Information & Security, Volume 15, Number 1

E-GOVERNMENT AND SECURITY OF INFORMATION

In the last few years, the term *e-Government* has been increasingly used to reflect the implementation of Information and Communications Technologies (ICT) in public administration in an attempt to ease access to governmental information and services for citizens, businesses, and government agencies. There has been a growing interest in the application of e-Government systems to various services such as e-Voting or e-Commerce, as well as to emergency management and related tasks. Therefore, information systems security becomes an essential management responsibility for e-Government.

To reflect the impact of security considerations on promoting e-Government concepts, the Editorial Board of *Information & Security: An International Journal* (I&S) announced the preparation of a special I&S issue on e-Government and Security of Information. The purpose of this special issue is to offer the opportunity for both academics and practitioners to share ideas, concepts, models, and experience. The topics include, but are not limited to:

- Information security challenges of e-Government;
- e-Government business model and risk analysis;
- Public Key Infrastructure (PKI) for e-Government;
- Strategy and policy of e-Government;
- Application of e-Government in the security sector;
- Discovery, promotion, and vision of e-Government in the security sector;
- Intrusion, denial of service, attack detection, etc.

In particular, based on the accepted publications, we have decided to organize the special issue on e-Government and Security of Information in two numbers. Volume 15, number 1 focuses on the following groups of topics:

- Strategic and Technology Policy Implications for e-Government;
- Secure Electronic Environment: Mail, PKI and Directory;
- User Authentication and Encryption in e-Government.

Volume 15, number 2 deals with: Secure e-Mail, e-Voting and e-Assistance.

This special issue provides also a comprehensive, up-to-date list with on-line resources on e-Government and Security of Information related research projects, journals, institutions, resource repositories, events, as well as some milestone publications.

The reader will not find answers to all related questions in this issue. We believe, though, that this I&S volume will provide novel ideas, analysis of experience, and description of advanced technological opportunities, that will be of service on the thorny path of e-Government introduction and further development.

Information & Security

CHALLENGES IN E-GOVERNMENT AND SECURITY OF INFORMATION

Min-Shiang HWANG, Chun-Ta LI, Jau-Ji SHEN, and Yen-Ping CHU

Abstract: Due to the advances made in Information and Communication Technologies (ICT), e-Government users can easily use the available services from places and at time that are convenient to them through WWW browsers. To easily and securely provide the required services through Information Technology (IT) has been an important issue in e-Government. In this article, the authors propose an explicit classification of e-Government applications and some challenges and obstacles in e-Government considered from four perspectives. Finally, a comprehensive view of some critical success factors in e-Government is proposed.

Keywords: e-Government; Critical Success Factor; Internet; Security.

Introduction

The time for the electronic-based society has arrived. E-Government has received more and more importance and it can provide a non-stop government information services to citizens, enterprises, public officers, government administrations and agencies over a network. There are many issues in e-Government which need a careful examination such as security issues,[1,2,3] service requirements of e-Government,[4,5,6] e-Government model, [7,8,9,10,11,12,13] strategy and policy for e-Government,[14,15,16,17] and domain of e-Government.[18]

In this article, we focus on the challenges, obstacles, and Critical Success Factors (CSFs)[19] in e-Government. First of all, we have to consider all of the participants in an e-Government system. According to the involved communities, an explicit classification of e-Government applications is proposed. It provides a way to an understanding of the challenges and CSFs in e-Government. Further detailed classification of e-Government applications is provided in a subsequent section. Then the challenges and obstacles in e-Government are considered from four perspectives. The CSFs of e-Government are described next. Finally, the last section provides conclusions and outlines future research directions.

An Explicit Classification of e-Government Applications

In order to develop an e-Government system, first, all of the users that may use the e-Government system have to be known. Therefore, the authors have defined four basic involved communities: Government, Officeholder, Citizens, and Business. All of the applications in an e-Government system will be developed in accordance with these four communities. An explicit classification of the e-Government applications is illustrated in Figure 1 and the detailed description of each e-Government application is as given below.

Government-to-Government e-Government (G-to-G e-Gov)

Government-to-Government e-Government (G-to-G e-Gov) supports the exchange of information between the inter-organizational governmental departments, such as the system of official documents received and dispatched.

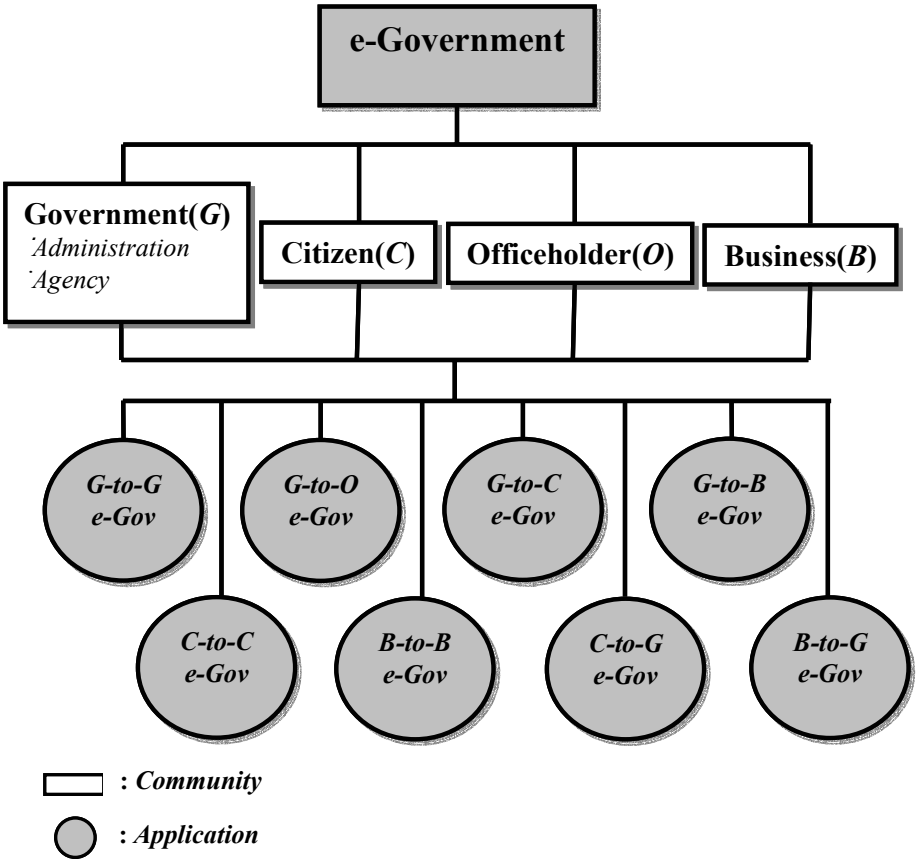


Figure 1: An Explicit Classification of e-Government Applications.

Government-to-Officeholder e-Government (G-to-O e-Gov)

Government-to-Officeholder e-Government (G-to-O e-Gov) supports intra-organizational government officeholders, public affair organizations, and secondary organizations' cooperative processes and procedures of public affairs.

Government-to-Citizen e-Government (G-to-C e-Gov)

Citizens are aware of the services provided by the government through the communication network and use the service with their personal identities through secure mechanisms. E-Voting and e-Assistance are two examples.

Government-to-Business e-Government (G-to-B e-Gov)

Businesses are aware of the services provided by the government through the communication network and use the service with a legal person's identity through secure mechanisms. Examples are on-line customs declaration of goods or on-line clearance of goods.

Citizen-to-Citizen e-Government (C-to-C e-Gov)

In Citizen -to- Citizen e-Government, the Government acts in a mediator role for the exchange of information. Typical examples are the following ones: the Government acts as a trouble-shooter in citizens' dispute or the Government offers temporary jobs to the victims of a disaster, so they could work in the public sector or private businesses. In this type of application the Government is a mediator that offers help in terms of manpower and information.

Business-to-Business e-Government (B-to-B e-Gov)

Similar to the above-described application of C-to-C e-Government, in Business-to-Business e-Government the Government plays an intermediary role in the exchange of information. For example, the Government could invite the business to bid for contracts that contain sensitive information. These businesses might produce the country's weaponry, such as tanks, warships, and warplanes.

Citizen-to-Government e-Government (C-to-G e-Gov)

These electronic communities are formed based on the demand of the citizens (demand aggregate-driven). Citizens request assistance or give suggestions to the citizenry, for example.

Business-to-Government e-Government (B-to-G e-Gov)

Similar to the above-mentioned application of C-to-G e-Government, electronic communities are formed on the basis of the demands of the business (demand aggregate-driven). Businesses ask for governmental patronage or proposals from other businesses, for example.

Challenges and Obstacles in e-Government

Considering the types of applications of e-Government described in the previous section, the authors demonstrate some challenges and obstacles to e-Government viewed from four perspectives: technical, political, cultural, and legal aspects. There is some difference between the aspects proposed here and the four aspects proposed by Wimmer and von Bredow[20]: social, political, cultural, and legal aspects. The challenges and obstacles in e-Government are illustrated in Figure 2 and further explanation of the challenges and obstacles in e-Government is provided below.

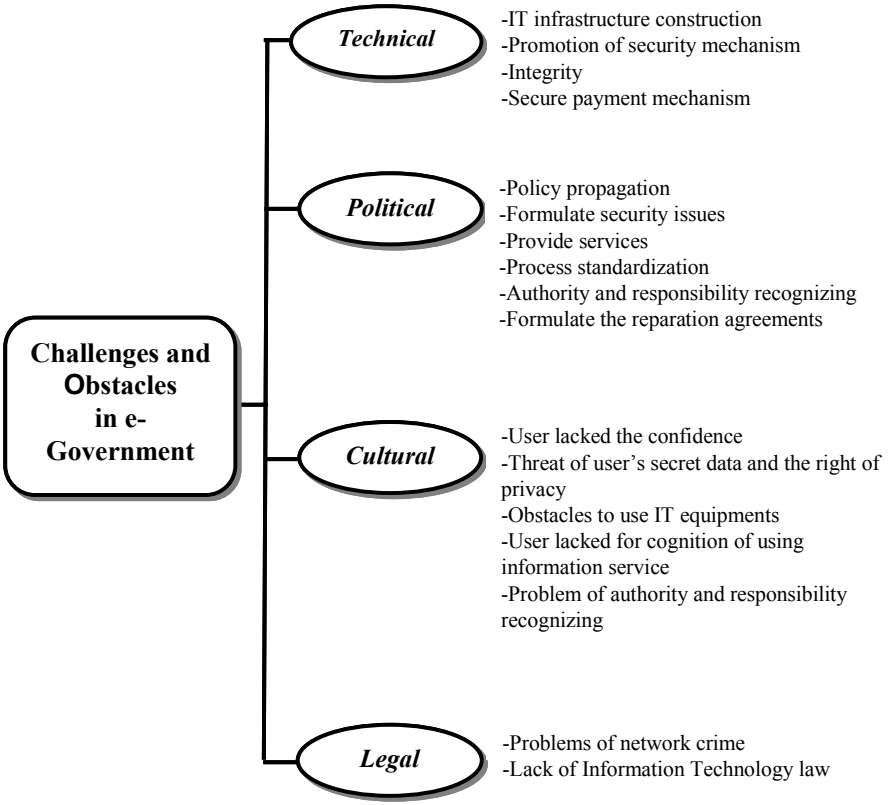


Figure 2: Challenges and Obstacles in e-Government.

Technical Impacts

In order to introduce and promote e-Government, the first and very important step is to construct the relevant IT infrastructure. This is a requirement very similar to the

relationship between advances in urban development and the construction of appropriate road infrastructure. Furthermore, system and security requirements, such as integrity, secure payment mechanism,[21,22,23,24] and promotion of security mechanism, are pertinent to e-Government as well.

Political Impacts

As is evident from Figure 2, there are many political issues that have to be considered. In this aspect, the services and processes need careful consideration. If the e-Government can provide a rich variety of different services (e-Justice for example) it will be more acceptable and convenient to users.

From the user's point of view, process standardization is a must and the simple principle "easy-to-use" has to be kept. Finally, the agreements of reparations, authority, and responsibilities have to be clearly formulated and recognized in order to protect the user's right.

Cultural Impacts

From this perspective, the challenges and obstacles in e-Government bring a lot of difficulty because it involves the human psychological factor. Therefore, the e-Government should not make any mistakes here, or otherwise it fails. Furthermore, the important principle—"easy-to-use"—has a great influence on the success of e-Government. This principle could advertise and promote e-Government and it will allow more people to use the e-Government services. In short, even illiterate people can use e-Government without any worries.

Legal Impacts

This aspect embraces a lot of problems related to networking crime and security threats,[25] such as hacker attacks, viruses, masquerades of unauthorized identity, and computer forgery. Furthermore, there is a shortage of relevant law in Information Technology.

Critical Success Factors in e-Government

In accordance with the e-Government challenges and obstacles described in the previous section, the critical success factors (CSF) in e-Government have to be investigated thoroughly. Therefore, we demonstrated thirteen CSFs in e-Government, as illustrated in Figure 3. These CSFs in e-Government are considered from a comprehensive view, including users, process, hardware/software, and legal views.

From the user's perspective, the government has to be greatly supportive and promoting first of all. Furthermore, it should have a high acceptance of users, clearly de-

fined authority and responsibility of users and it has to enhance the user's information technology skills. Besides, the diversification of electronic means is very helpful to e-Government, such as wireless communication, net-meeting, video conferencing, and video telephones. From the process view, high security, standardization and knowledge management are a must for e-Government; then come the provision of specific services and the emphasis of its quality. Furthermore, the establishment of national

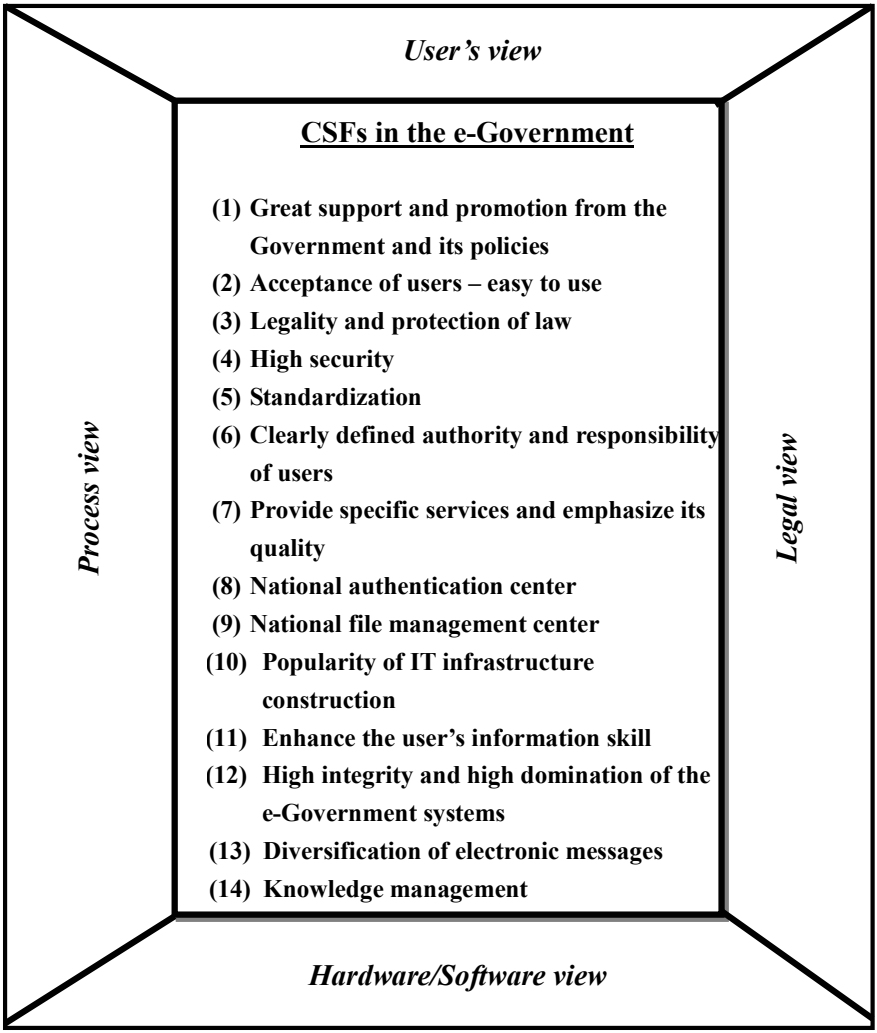


Figure 3: CSFs in e-Government from a Comprehensive View.

authentication centre is an essential requirement, so as the users could use the services with their personal identities and all transactions are recorded in the national file management centre in order to protect the electronic documents from any damage. From the legal point of view, it is necessary to legislate for legitimacy; hence all people are equal before the law. Finally, from the hardware/software point of view, popularizing the IT infrastructure construction is essential for e-Government. In addition, it is important to enhance the integrity and the dominance of the e-Government system.

Research Issues

As to the future research work, the authors have outlined some research issues for further detailed consideration as follows. Included are security issues, issues of services provided, and the e-Government model.

- Security issues:
  - Identification of security requirements[26]
  - Attribute Certificates (AC)[27]
  - Public Key Infrastructure (PKI)[28,29,30]
  - Certification/Authentication[31,32,33,34,35]
  - Risk analysis and Metrics for e-Government[36]
  - Database Security[37,38,39,40]
- Issues of services provided:
  - E-Learning in e-Government[41]
  - E-Procurement in e-Government[42]
  - Semantic Web for e-Government[43]
  - E-Voting in e-Government[44]
- E-Government model.[45,46,47,48]

Conclusion

In this article, the authors have proposed an explicit classification of e-Government applications according to the involved participants in an e-Government system. Further, the authors have demonstrated the challenges and obstacles in e-Government considered from four aspects: technical, political, cultural, and legal aspects. In addition to outlining the challenges and obstacles in e-Government, they have proposed thirteen CSFs in e-Government from a comprehensive view: user, process, legal and hardware/software views. Finally, developing practical solutions in e-Government is a very interesting subject for further investigation and discussion.

Notes:

[1] Dorothy E. Denning and Peter J. Denning, *Internet Besieged: Countering Cyberspace Scofflaws* (ACM Press, Addison Wesley Professional., 1998).

[2] Stefanos Gritzalis and Costas Lambrinoudakis, "Security Requirements of e-Government Services: An Organizational Framework," in *Proceedings of the International Conference on Parallel and Distributed Processing Techniques and Applications (PDPTA'2002)* (Las Vegas, Nevada, USA, 24-27 June 2002), Volume 1, ed. Hamid R. Arabnia (CSREA Press, 2002), 127-131.

[3] Spyros Ikonomopoulos, Costas Lambrinoudakis, Dimitris Gritzalis, Spyros Kokolakis, and Kostas Vassiliou, "Functional Requirements for a Secure Electronic Voting System," in *Proceedings of the IFIP TC11 17th International Conference on Information Security* (Cairo, 2002), 507-520.

[4] Stefanos Gritzalis, Sokratis K. Katsikas, Dimitrios Lekkas, Konstantinos Moulinos, and Eleni Polydorou, "Securing the Electronic Market: the KEYSTONE Public Key Infrastructure Architecture," *Computers and Security Journal* 19, no. 8 (2000): 731-746.

[5] Rolf Oppliger, "Managing Certificates in a Corporate Environment," *Annals of Telecommunication* 55, no. 7 (July 2000): 341-351.

[6] Michael Sonntag, "Improving Communication to Citizens and within Public Administration by Attribute Certificates," in *Knowledge Management in e-Government. KMGov-2001*, *Proceedings of the 2nd International Workshop on Knowledge Management and Electronic Government* (Siena, 2001), ed. Maria A. Wimmer (Linz: Universitätsverlag Rudolf Trauner, 2001), 207-217.

[7] Salah Benabdallah, Sihem Guemara EI Fatmi, and Noureddine Boudriga, "Security Issues in e-Government Models: What Governments Should Do?" in *2002 IEEE International Conference on Systems, Man and Cybernetics* (Hammamet, Tunisia, 6-9 October 2002), Volume 2, 398-403.

[8] Noureddine Boudriga and Salah Benabdallah, "Laying out the Foundation for a Digital Government Model, Case Study: Tunisia," in *Advances in Digital Government: Technology, Human Factors, and Policy*, ed. W. McIver and A. K. Elmagarmid (Boston: Kluwer Academic Publishers, 2002).

[9] Yumin Dong, Yannian Rui, and Dianxun Shuai, "The Researching of Constructing a Convenient, Safe, Credible, New e-Government System," in *Proceedings of 2003 IEEE Intelligent Transportation Systems*, Volume 2 (2003), 1719-1723.

[10] Karen Layne and Jungwoo Lee, "Developing Fully Functional e-Government: A Four Stage Model," *Government Information Quarterly* 18, no. 2 (2001): 122-136.

[11] Brahim Medjahed, Abdelmounaam Rezgui, Athman Bouguettaya, and Mourad Ouzzani, "Infrastructure for e-Government Web Services," *IEEE Internet Computing* 7, no. 1 (January/February 2003): 58-65.

[12] Tatyana Podgayetskaya and Wolffried Stucky, "A Model of Business Process Support System for e-Government," in *Proceedings of the 15th International Workshop on Database and Expert Systems Applications (DEXA'04)* (Zaragoza, Spain, 30 August-3 September 2004), (IEEE Computer Society, 2004),1007-1015.

[13] Christopher G. Reddick, "A Two-Stage Model of e-Government Growth: Theories and Empirical Evidence for U.S. Cities," *Government Information Quarterly* 21, no. 1 (2004): 51-64.

[14] Costas Lambrinoudakis, Stefanos Gritzalis, Fredj Dridi, and Günther Pernul, "Security Requirements for E-Government Services: A Methodological Approach for Developing a Common PKI-based Security Policy," *Computer Communications* 26, no. 16 (2003): 1873-1883; Reddick, "A Two-Stage Model of e-Government Growth."

[15] Thurman L. Whitson and Lynn Davis, "Best Practices in Electronic Government: Comprehensive Electronic Information Dissemination for Science and Technology," *Government Information Quarterly* 18, no. 2 (2001): 79-91.

[16] Maria Wimmer and Bianca von Bredow, "E-Government: Aspects of Security on Different Layers," in *Proceedings of 12th IEEE International Workshop on Database and Expert Systems Applications "On the Way to Electronic Government"* (Munich, Germany, 3-7 September 2001), ed. A. Min Tjoa and Roland Wagner (Los Alamitos, CA: IEEE Computer Society Press, 2001), 350-355.

[17] Maria Wimmer and Bianca von Bredow, "A Holistic Approach for Providing Security Solutions in e-Government," in *Proceedings of the 35th Hawaii International Conference on System Sciences (HICSS-35)* (Big Island of Hawaii, 7-10 January 2002), (IEEE Computer Society, 2002), 1715-1724.

[18] Michael Gisler and Dieter Spahni, eds., E-*Government: Eine Standortbestimmung* (Bern: Paul Haupt, 2000).

[19] John F. Rockart, "The Changing Role of the Information Systems Executive: A Critical Success Factors Perspective," *Sloan Management Review* 24, no. 1 (1982): 3-13.

[20] Wimmer and Bredow, "A Holistic Approach for Providing Security Solutions in e-Government."

[21] Min-Shiang Hwang, Iuon-Chung Lin, and Li-Hua Li, "A Simple Micro-payment Scheme," *Journal of Systems and Software* 55, no. 3 (January 2001), 221-229.

[22] Min-Shiang Hwang, Cheng-Chi Lee, and Yan-Chi Lai, "Traceability on Low-Computation Partially Blind Signatures for Electronic Cash," *IEICE Fundamentals on Electronics, Communications and Computer Sciences* E85-A, no. 5 (May 2002), 1181-1182.

[23] Min-Shiang Hwang, Eric Jui-Lin Lu, and Iuon-Chung Lin, "Adding Timestamps to the Secure Electronic Auction Protocol," *Data & Knowledge Engineering* 40, no. 2 (February 2002): 155-162.

[24] Min-Shiang Hwang, Cheng-Chi Lee, and Yan-Chi Lai, "An Untraceable Blind Signature Scheme," *IEICE Transactions on Foundations* E86-A, no. 7 (July 2003): 1902-1906.

[25] Ahti Saarenpää, Tuomas Pöysti, Mikko Saraja, Viveca Still, and Ruxandra Balboa-Alcoreza, "Data Security and Law: Perspectives on the Legal Regulation of Data Security," Executive Summary in English of the Research Report published by the Ministry of Finance under the title "Tietoturallisuusja laki, näkökohtia tietoturvallisuude oikeudellisesta sääntelystä," 1997.

[26] Noureddine Boudriga, "Technical Issues in Securing e-Government," in *2002 IEEE International Conference on Systems, Man and Cybernetics*, (Hammamet, Tunisia, 6-9 October 2002), Volume 2 (2002), 392-397; Gritzalis and Lambrinoudakis, "Security Requirements of E-Government Services."

[27] Sonntag, "Improving Communication to Citizens and within Public Administration by Attribute Certificates."

[28] Lambrinoudakis, Gritzalis, Dridi, and Pernul, "Security Requirements for e-Government Services."

[29] A. van Rensburg and Sebastiaan H. von Solms, "A Reference Framework for Certification Authorities/Trusted Third Parties," in *Proceedings of the 13th IFIP International Information Security Conference*, ed. L. Yngstromand and J. Carlsen (Chapman & Hall, 1996).

[30] Gwo-Chin Tai and Chung-Ming Ou "The Development of PKI Interoperability in Taiwan," in *Proceedings of 37th IEEE Annual 2003 International Carnahan Conference on Security Technology* (14-16 October 2003), 405-409.

[31] Franco Arcieri, Giovanna Melideo, Enrico Nardelli, and Maurizio Talamo, "Experiences and Issues in the Realization of e-Government Services," in *Proceedings of the 12th International Workshop on Research Issues in Data Engineering: Engineering e-Commerce/ e-Business Systems (RIDE'02)* (San Jose, California, USA, February 2002), (Washington, DC, USA: IEEE Computer Society, 2002), 143-150.

[32] Michael Caloyannides, Dennis R. Copeland, George H. Datesman Jr., and David S. Weitzel, "US e-Government Authentication Framework and Programs," *IT Professional* 5, no. 3 (May/June 2003), 16-21.

[33] Chin-Chen Chang, Kuo-Feng Hwang, and Min-Shiang Hwang, "A Digital Watermarking Scheme Using Human Visual Effects," *Informatica: An International Journal of Computing and Informatics* 24, no.4 (2000), 505-511.

[34] Fernando Galindo, "Public Key Certification Providers and e-Government Assurance Agencies. An Appraisal of Trust on the Internet," in *Proceedings of 12th IEEE International Workshop on Database and Expert Systems Applications "On the Way to Electronic Government"* (Munich, Germany, 3-7 September 2001), ed. A. Min Tjoa and Roland Wagner (Los Alamitos, CA: IEEE Computer Society Press, 2001), 345-349.

[35] Min-Shiang Hwang, Chin-Chen Chang, and Kuo-Feng Hwang, "Digital Watermarking of Images Using Neural Networks," *Journal of Electronic Imaging* 9, no. 4 (2000): 548-555.

[36] Benabdallah, Guemara EI Fatmi, and Oudriga, "Security Issues in e-Government Models: What Governments Should Do?"

[37] Min-Shiang Hwang and Wei-Pang Yang, "A Two-Phase Encryption Scheme for Enhancing Database Security," *Journal of Systems and Software* 31, no.12 (December 1995): 257-265.

[38] Min-Shiang Hwang and Wei-Pang Yang, "Multilevel Secure Database Encryption with Subkeys," *Data and Knowledge Engineering* 22, no. 2 (April 1997): 117-131.

[39] Min-Shiang Hwang and Chii-Hwa Lee, "Secure Access Schemes in Mobile Database Systems," *European Transactions on Telecommunications* 12, no. 4 (July 2001): 303-310.

[40] Min-Shiang Hwang and Wei-Pang Yang, "Integrating Different Semantics of Classification Levels in Heterogeneous Distributed Database Systems," *Pakistan Journal of Information and Technology* 1, no. 1 (April 2002): 1-4.

[41] Ranjit Bose, "Information Technologies for Education & Training in e-Government," in *Proceedings of the International Conference on Information Technology: Coding and Computing (ITCC'04)* (Las Vegas, Nevada, 05-07 April 2004), Volume 2 (IEEE Computer Society, 2004), 203-207.

[42] Steven Cohen and William Eimicke, "The Future of e-Government: A Project of Potential Trends and Issues," in *Proceedings of the 36th Hawaii International Conference on System Sciences (HICSS'03)* (Big Island, Hawaii, 6-9 January 2003), (IEEE Computer Society, 2003), 146-155.

[43] Ralf Klischewski and Martti Jeenicke, "Semantic Web Technologies for Information Management within e-Government Services," in *Proceedings of the 37th Hawaii International Conference on System Sciences (HICSS'04)* (Big Island, Hawaii, USA, 5-8 January 2004), (Los Alamitos, California: IEEE Computer Society, 2004), 119-128.

[44] Iuon-Chang Lin , Min-Shiang Hwang, and Chin-Chen Chang, "Security Enhancement for Anonymous Secure e-Voting over a Network," *Computer Standards & Interfaces* 25, no.2 (May 2003): 131-139.

[45] Layne and Lee, "Developing Fully Functional e-Government: A Four Stage Model."

[46] Medjahed, Rezgui, Bouguettaya, and Ouzzani, "Infrastructure for e-Government Web Services."

[47] Podgayetskaya and Stucky, "A Model of Business Process Support System for e-Government."

[48] Reddick, "A Two-Stage Model of e-Government Growth."

MIN-SHIANG HWANG was born on August 27, 1960 in Tainan, Taiwan, Republic of China (R.O.C.). He obtained a B.S. degree in Electronic Engineering from National Taipei Institute of Technology, Taipei, Taiwan, R.O.C, in 1980; a M.S. degree in Industrial Engineering from National Tsing Hua University, Taiwan, in 1988; and a Ph.D. in Computer and Information Science from National Chiao Tung University, Taiwan, in 1995. He studied also Applied Mathematics at National Cheng Kung University, Taiwan, from 1984 to 1986. Dr. Hwang passed the National Higher Examination in the field "Electronic Engineer" in 1988. He also passed the National Telecommunication Special Examination in the field "Information Engineering" and qualified as advanced technician first class in 1990. From 1988 to 1991, he was the leader of the Computer Center at Telecommunication Laboratories (TL), Ministry of Transportation and Communications, R.O.C. He was also a chairman of the Department of Information Management, Chaoyang University of Technology (CYUT), Taiwan, during the period 1999-2002. He was a professor and chairman of the Graduate Institute of Networking and Communications, CYUT, during 2002-2003. He obtained the 1997, 1998, 1999, 2000, and 2001 Outstanding Research Award of the National Science Council of the Republic of China. He is currently a professor at the department of Management Information Systems, National Chung Hsing University, Taiwan, R.O.C. He is a member of IEEE, ACM, and the Chinese Information Security Association. His current research interests include electronic commerce, database and data security, cryptography, image compression, and mobile computing. Dr. Hwang has published over 100 articles in the above research fields in international journals. *Address for correspondence:* Department of Management Information System, National Chung Hsing University, 250 Kuo Kuang Road, 402 Taichung, Taiwan, R.O.C.; *E-mail:* mshwang@nchu.edu.tw.

CHUN-TA LI received a B.S. degree in Management Information Science from Chia Nan University of Pharmacy & Science, Tainan county, Taiwan, Republic of China, in 2002. Two years later, he received a M.S. in Information Management from Chaoyang University of Technology, Taichung county, Taiwan. He is currently pursuing his Ph.D. degree in Computer Science from National Chung Hsing University. His current research interests include full text retrieval, information security, electronic government, and cryptography. *Address for correspondence:* Department of Computer Science, National Chung Hsing University, 250 Kuo Kuang Road, 402 Taichung, Taiwan, R.O.C. *E-mail:* phd9307@cs.nchu.edu.tw.

JAU-JI SHEN received a B.S. degree in Mathematics from Fu Jen University, Taipei county, Taiwan, Republic of China, in 1982. Two years later, he received a M.S. degree in Information Science program of Applied Mathematics from National Chung Hsing University, Taichung, Taiwan. In 1988, he received a Ph.D. in Information Engineering and Computer Science from National Taiwan University, Taipei, Taiwan. From 1988 to 1994, he was the leader of the software group at the Institute of Aeronautic, Chung Sung Institute of Science and Technology, R.O.C. He is currently an Associate Professor and Library Curator, National Formosa University, Taiwan, R.O.C. His current research interests include database techniques, algorithms, and software engineering. *Address for correspondence:* Department of Information Management, National Formosa University, 64 Wen-Hua Road Huwei, 632 Yunlin, Taiwan, R.O.C. *E-mail:* amitofo@sunws.nhust.edu.tw.

YEN-PING CHU is a Professor at the Department of Computer Science and the chair of Management Information Systems at National Chung Hsing University, Taiwan, R.O.C. His research interests include high-speed networks, operating systems, neural networks and computer-assisted learning. *E-mail:* ypchu@nchu.edu.tw.

STRATEGIC AND TECHNOLOGY POLICY IMPLICATIONS FOR E-GOVERNMENT: LESSONS FROM AN EMPIRICAL CASE STUDY ON INFORMATION SECURITY IN THAILAND

Donyaprueth KRAIRIT, Worraya CHOOMONGKOL, and Poondej KRAIRIT

Abstract: Smart card technology was first introduced in Thailand by the Thai government who planned to use the technology for the government's e-ID and e-Government projects in 2004. This situation is contrary to the introduction of smart cards by the private sector in developed countries. On the research front, this contrast provided an excellent opportunity to study the differences, if any, in factors affecting consumers' perceptions of smart card technologies. The study shows that, statistically, no demographic factors, except age, were found to have statistically significant effects on the users' decision to use smart cards. In addition, it was found that perceived convenience and security level of smart cards are the other two statistically significant factors found to affect Thai users' decisions to adopt smart card technologies. This study concludes that the key issue with respect to using smart cards in Thailand is not so much about which applications are the "right" ones to be put on the cards, but more on the matters of security of the cards. This issue is very important to Thai people as shown empirically by this study. As a result, the Thai government should put high emphasis on the security issue when planning for and implementing the smart card technologies in their e-ID and e-Government projects.

Keywords: Smart Cards, Thailand, Developing Countries, e-Government, Consumer Perception, Consumer Survey, Technology Policy Planning, Technology Implications.

In early 2002, the Thai government announced its e-Government policy, and subsequently, two of its most ambitious projects yet, the projects on e-ID and e-Citizen. For the e-ID project, the Thai government in 2004 introduced smart card technologies.

This research presents consumers' perceptions on information security in the deployment of smart cards in e-Government projects in developing countries using Thailand

as a case study. The paper is organized in the following manner. First, introduction on smart card technologies is presented. After that, the Technology Acceptance Model (TAM), on which a conceptual model for this research is based, is discussed and past research on the adoption of smart cards is reviewed. Subsequently, the conceptual framework is presented followed by the results from an empirical study. Finally, strategic implications for policy makers are discussed.

Smart Card Technologies

Smart card technologies have been revolutionizing telecommunications and financial transactions for many years. The major driving factors of the growth of smart card usage are the declining cost of smart cards and the added convenience that smart cards provide to users.

The majority of smart cards, by far, are used in the wireless telecommunications sector, where Subscriber Identity Modules (SIMs) are the major applications. Smart Cards have been specified as the access medium to the digital European mobile phone system (GSM). They are ideal because they provide secure access to the network by verifying the subscriber's identity, and they allow separation of sale of mobile phones from that of services by the network operator and service provider.[1]

There are many ways to categorize smart card technologies. However, for the purpose of this paper, only two major types of smart cards will be discussed. They are:

- "Simple" smart cards or Memory cards: These cards can store more data than the standard magnetic stripe cards. However, this type of card cannot process the information stored on it. This type of card is mainly used to store information only. The major applications of memory cards are the pre-paid pay-phone or store-valued cards.
- "Intelligent" smart cards: This type of card looks like standard plastic cards but are embedded with Integrated Circuit (IC) chip. They can securely store and process the information on the cards. This type of card cannot be reproduced and therefore is almost totally secure against fraud. Unlike the passive memory cards, "intelligent" smart cards can process, re-record, and update the information on real-time basis.

Literature Review

The framework for this research is developed based on Davis' Technology Acceptance Model (TAM).[2] According to Davis' framework, the intention to adopt new technologies (in his work, a software package) depends on two major factors, namely, perceived ease-of-use and perceived usefulness. Perceived ease-of-use reflects the extrinsic characteristics of the technology itself, while perceived usefulness reflects

the intrinsic characteristics of the technology based on the users' individual perceptions.

Over the years, the TAM framework has been revised and tailored to many specific new technologies, including the Internet, IT technologies, and many others. For this research, the TAM framework was selected because it deals directly with individual perceptions and new technologies, which are the main focus of this research.

In addition to Davis' TAM framework, this research has also incorporated other factors from previous studies on smart card adoption into its conceptual framework, including demographics and technology-specific concerns, i.e., information security, in order to test these factors in the context of developing countries.

Many of the past studies in smart cards dealt with unsuccessful attempts to introduce smart card technologies to consumers. Despite their usefulness and extensive applicability, smart cards have not gained popularity and acceptance worldwide as their supporters once claimed. In some locations, the trial implementation of smart cards was even deemed failure.[3,4,5] To this end, several researchers tried to give the explanation as to why smart cards were not accepted well in these cases.

One major case of failure in smart card implementation was the smart card trial in New York City, U.S.A., launched by Citibank, Chase, VISA and MasterCard. In an empirical study of this trial's failure, Truman, Sandoe, and Rifkin[6] found that despite the fact that the technology's relative advantages were significantly related to consumers' and merchants' acceptance, consumers and merchants were disposed against acceptance of smart card technology. In addition, they found that there was no evidence of any critical mass effects that can be used as a predictor of either consumers' or merchants' acceptance.

Another case where smart cards have failed was the case of the smart card-based retail point-of-sale system, called "Exact," which was test marketed for a full year in 1997 in the Canadian market. Plouffe, Vandenbosch, and Hulland[7] conducted a detailed case study of this trial and found that there is an unavoidable "synergistic" aspect to the diffusion of the smart card technology. Their research clearly indicates that the pure convenience and novelty elements of smart card payment are not enough in and of themselves to ensure the technology's longer-term viability and acceptance. Consumers only value smart cards if they are broadly accepted at a variety of merchants and service providers. They also found that there were no statistically significant differences in expressed adoption intent across either gender or highest achieved educational level.

In another study done by Kearns and Loy,[8] it was found that at the global level, there were still a number of issues that inhibit the widespread use of smart cards, especially

in open systems. These issues include the unsettled standards to be used for the Chip Operating System (COS), and the users' fears against security breaches and attacks of financial data which overweighed the benefits that facilitate adoptions of smart cards.

Other studies stated that obstacles to acceptance of smart cards include[9]:

- Present lack of infrastructure to support the smart card, particularly in the United States, necessitating retrofitting of equipment such as vending machines, ATMs, and telephones.
- Lack of standards to ensure interoperability among varying smart card programs.
- Unresolved legal and policy issues, such as those related to privacy and confidentiality or to consumer protection laws.

While the aforementioned empirical studies provided useful insights into the facilitators and inhibitors of smart card usage, the cases explored in these studies are mostly market trials of smart cards used in the financial and payment transactions. In addition, these past studies focused mainly on the cases of smart card usage in developed countries, such as the U.S., Canada, and the European countries.

Table 1 summarizes the factors studied in past research.

Table 1: Factors Affecting the Adoption of Smart Cards from Past Research.

Factors	Statistically Significant	Past Research
Gender	No	Plouffe, Vandenbosch, and Hulland,[10] Truman, Sandoe, and Rifkin[11]
Educational Level	No	Plouffe, Vandenbosch, and Hulland,[12] Truman, Sandoe, and Rifkin[13]
Age	Yes	Plouffe, Vandenbosch, and Hulland,[14] Truman, Sandoe, and Rifkin[15]
Income Level	Yes	Plouffe, Vandenbosch, and Hulland,[16] Truman, Sandoe, and Rifkin[17]
Security Concerns	Yes	Kearns and Loy[18]
Convenience	No	Truman, Sandoe, and Rifkin[19]

A Conceptual Framework

Unlike the past studies, this research hopes to shed some light on the consumers' perception and deployment of smart card technology in developing countries by using Thailand as a case study. In most developing countries, smart card technology was first introduced to consumers by the government, as opposed to the introduction by

the private sector in developed countries, through the implementation of electronic identification cards (e-ID). This is also the situation in Thailand, where the Thai government is currently planning for the deployment of e-ID and the implementation of electronic government regime.

This study intends to provide a unique perspective into the deployment of smart cards in developing countries. Being totally different from the optional usage of smart cards in developed countries; the usage of smart cards in Thailand was proposed to be "imposed" on all Thai citizens within the next few years. This situation does not only provide unique commercial implications for the private sector, but also important policy implications for the government and relevant stakeholders, and most importantly, to Thai citizens themselves.

This research is based on the conceptual framework presented in Figure 1.

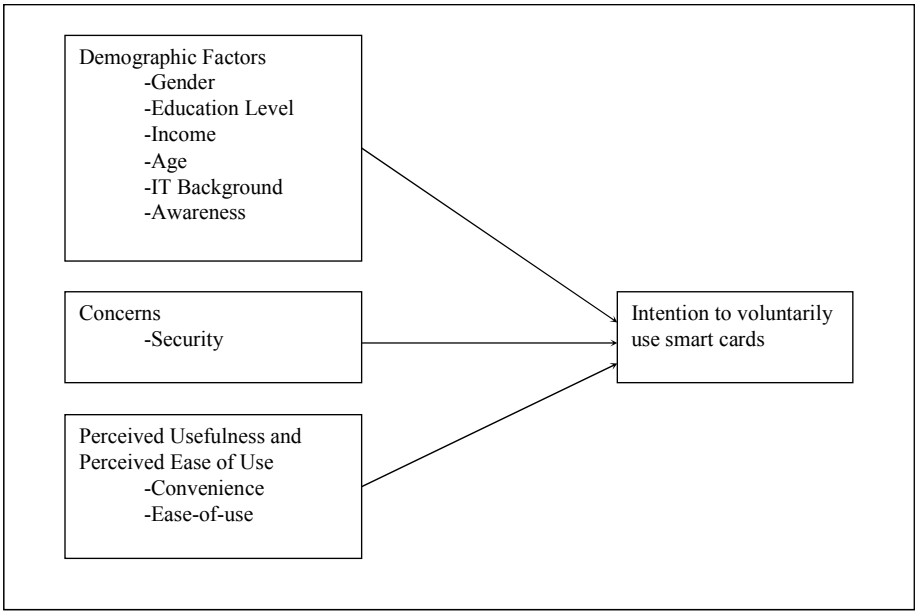


Figure 1: A Conceptual Model.

Thailand: A Background Review on e-Government and e-ID Policies

In early 2002, the Thai government announced the e-Government policy, and subsequently, the policies on e-ID and e-Citizen. In November 2002, the Information and Communications Technology (ICT) Ministry and the Bureau of Registration Administration (BORA) said they would introduce the country's first ID card equipped with

a chip to store personal data by April 2004. The smart card would be only issued on request.[20]

The government said it would launch a pilot scheme for electronic ID cards, "smart citizen e-card," that will cost taxpayers a mere 800 million Thai Baht to see if they actually work. The cards will have a 13-digit code exactly like now, be made of plastic exactly like now, contain health records such as blood group and allergies, and hold house registration and health-card details. The government estimated they would cost about 50 to 100 Thai Baht each to produce, depending on what the market will bear; the pilot project will cover about eight million people; if successful, everyone will have a smart card within three years. The government appointed Education Minister Suvit Khunkitti to run the e-Citizen card committee.

To date, magnetic ID cards have been provided to some citizens over 15-years-old in nine selected provinces: Bangkok, Chiang Mai, Phitsanulok, Chon Buri, Nakhon Pathom, Nakhon Ratchasima, Udon Thani, Songkhla and Surat Thani. The magnetic cards cannot store information but can be used with other services such as ATM machine.

BORA Director Surachai Srisarakham said government agencies would be able to select the information that would be stored. He added that the card might also be integrated with an e-signature, a driving license, job title, membership of any organizations or be used as an e-purse or e-passport in the future.[21]

BORA expects to set up a central server, separated from the central government database server, which would allow each government agency to select information to be stored in the card and update information.[22]

BORA director noted that the card would only be offered to those who ask for it. BORA will implement the ID smart card in selected provinces as a trial. There will be a 100 Thai Baht fee for the smart card to cover production expenses. One initial benefit is that the smart card could be used as an ID to access e-services of government agencies or as an e-signature with email.

In addition, the ICT Ministry expects to issue a smart card to newborn babies and students in the future. BORA forecasts that it will take at least three to five years before the smart card system is widely used.

BORA director claimed that the Thai public would be able to more easily access government services. The new smart ID card will be able to be used for any kind of government registration service. Currently, 505 district registration offices can provide an electronic registration service, covering nine provinces. The remaining 572 offices in 67 provinces were expected to be ready by the end of 2003.[23]

Once the Cabinet approves the agenda and all 572 offices are computerized, infrastructure will be completed nationwide. After that, BORA will link to other state agencies. BORA director claimed that the use of a single ID card would save costs and is more convenient for people. The public will be able to access the services via a one-stop gateway on the Web at khonthai.com.

The government is now amending existing laws so that it can offer the new services to the people. It is hoping that by using the 13-digit identification card number to apply for any service of the state agencies will eventually lead to e-Government.

BORA, meanwhile, will gradually redistribute jobs to the district government registration offices, while the BORA itself will be a center supporting those offices. District offices do not need to submit any documents to the center, rather they will have authority to issue documents themselves, such as ID cards. Also by next year, BORA will discontinue its census forms and will transfer information into the ID card itself.

The process will start in Bangkok and further eight provinces will be transferred to the electronic system, including Chiang Mai, Chonburi, Phitsanulok, Surat Thani, Songkhla, Udon Thani, Nakhon Ratchasima, and Nakhon Pathom.

However, the private sector has already voiced concerns over the privacy of personal information. The Association of Thai Computer Industry (ATCI) honorary president Manoo Ordeedolchet said that before the project is launched, the government should clearly outline what information will be stored on the card. He also stated that the information must not be used for further processing or linked to other database systems, such as healthcare or education systems, in order to protect consumers' privacy rights.[24]

Meanwhile, BORA has also developed systems that it hopes will help it to generate income. These include its database of population, investment, and so on, which can be used by businesses. It has been pointed out that BORA plans to offer those services to business by 2004. According to BORA director, the operational cost per year is around 1.3 billion Thai Baht ($29.64 million). By having businesses accessing the databases, BORA expected that 70-80 percent of the costs, or around 800 million Thai Baht ($18.24 million) would be returned in revenue. The revenue will be derived from service fees and transactions.[25]

This year BORA will set up the National Committee on Registration Administration with some 13 organizations that issue official registration documents, such as social welfare, healthcare, revenue, transportation, passports, military and education. The committee will be chaired by the Prime Minister and will comprise 24 members including the Interior Minister and selected experts.[26]

Table 2: Demographic Data of Respondents.

Characteristics	Description	Total %	Bangkok %	CM %
Location	Bangkok	48.8	--	--
	Chiang Mai	51.2	--	--
Age	15-25	20.8	19.5	22.1
	25-40	56.5	64.6	48.8
	40-60	20.8	15.9	25.6
	>60	1.8	0	3.5
Gender	Female	63.7	65.9	61.6
	Male	36.3	34.1	38.4
Education	< Bachelor	37.1	32.9	41.1
	Bachelor	47.3	52.4	42.4
	> Bachelor	15.6	14.7	16.5
Income	< 5,000	14.4	12.2	16.5
	5,001 - 10,000	29.3	35.4	23.5
	10,001 - 25,000	36.5	43.9	29.4
	25,001 - 50,000	16.2	7.3	24.7
	50,001 - 75,000	1.2	1.2	1.2
	> 75,000	2.4	0	4.7
IT Background	Have IT Background	32.3	40.2	24.7
	No IT Background	67.7	59.8	75.3
Heard about Smart Cards Before	Yes	68.5	65.9	70.9
	No	31.5	34.1	29.1
Total Response Rate	167 out of 200			83.5

Research Methodology and Settings

This study was conducted based on three types of data collection; namely, documentary research, expert interviews, and surveys. The surveys were conducted in two major cities of Thailand, Bangkok and Chiang Mai. Bangkok is the capital of Thailand and the country's largest city. Chiang Mai is a province in the northern part of Thailand and the second largest city in the country. Both locations are selected because they are among the first selected for the smart-card trials next year.

In both locations, the respondents were general consumers who were randomly selected by volunteers and asked to fill out the surveys. In total, 167 people answered

the survey making response rate of 83.5%. The demographic data of the respondents are summarized in Table 2.

Several interviews with experts in the technological and policy-making arena were also conducted over several months. Results of these in-depth interviews provide a crosscheck with the statistical results from the surveys and therefore are able to help ensure the integrity of data in this study.

It should also be noted here that although Thai people have never used the "intelligent" smart cards before, the idea of smart cards in general is not new to them. The government has promoted the ideas of pre-paid store-valued and telephone cards for quite some time already. Moreover, credit cards both in the forms of "simple" smart cards (Memory cards) and magnetic-stripe cards are being widely used in Thailand.

Results of the Study

The findings from the surveys are briefly presented in Table 3, after which descriptive findings are provided.

Table 3: Factors Affecting Respondents' Decisions to Use Smart Cards

Construct	β	S.E.	Wald	df	Significant
Security	***.446***	***.219***	***4.160***	***1***	***.041***
Convenience	***.953***	***.280***	***11.616***	***1***	***.001***
Card fees	-.183	.142	1.658	1	.198
Location	-.672	.390	2.960	1	.085
Age	***-.738***	***.333***	***4.916***	***1***	***.027***
Gender	-.241	.382	.398	1	.528
Income	.264	.224	1.391	1	.238
Have IT background	-.529	.462	1.309	1	.253
Smart card awareness	.150	.432	.120	1	.729
Education level	-.140	.303	.212	1	.645
Constant	***2.054***	***.971***	***4.475***	***1***	***.034***

Note: (1) Nagelkerk R Square value is 0.287.
(2) Cox & Snell R Square value is 0.210.
(3) The overall percentage of correct prediction is 72.6%.
(4) The bolded constructs are significant at the 95% confidence level.

Hypothesis Testing

Hypothesis 1

Demographic factors (Gender, Education Level, Income, Age, IT background, Smart card awareness) have significant relationships with the decision of users to adopt smart cards.

This hypothesis was set up to test the relationship between demographic constructs and the decision of users to adopt smart cards as mentioned in past literature to analyze if the relationships sustain in the context of Thailand.

It was found that the only demographic factor that has statistically significant effects on the decision of users to adopt smart cards is the "Age" of the respondents. The β value for "Age" construct is negative meaning that younger respondents were more likely to adopt smart cards than the older age group. No other demographic factors are found to have statistically significant effects on the decision of users to adopt smart cards.

Hypothesis 2

Perceived usefulness (i.e., convenience) has significant relationships with the decision of users to adopt smart cards.

This hypothesis was set up based on the TAM literature and conceptual framework mentioned earlier. It was found that the β value for the "Convenience" construct is positive and significant. This means that Hypothesis 2 is supported. In addition, this result shows that the higher the level of usefulness of smart cards perceived; the more likely people are to use it.

It should be mentioned that the perceived ease-of-use was not measured quantitatively since the Thai government has promoted the ease-of-use of smart cards continuously so the Thai people were strongly influenced about this factor. The brief interviews with the respondents about this factor confirmed that this influence truly exists as more than 90% of the respondents do not see the easiness of using smart cards as a potential problem.

Hypothesis 3

Security concern has significant relationships with the decision of users to adopt smart cards.

This hypothesis was established in order to test the specific feature and construct unique to smart card usage, security concerns. It was found that the β value for the "Security" construct is positive and significant. So, the Hypothesis 3 was supported.

This also shows that the higher the level of security of smart cards that people perceive; the more likely they are to use it.

Discussion

On Demographic Factors

Based on the results of this study, one interesting issue that emerged with respect to smart card adoption in every respondent group is that no demographic factors, except "Age," have statistically significant effects on the users' decision to adopt smart cards.

Young respondents tend to be more open to the idea than older respondents. This finding is consistent with previous research in this area, which found that age of consumers has statistically significant effects on the decision to adopt smart cards.

It is also worth noting that across all groups, neither gender, education level, awareness of smart card concepts, nor IT background, have statistically significant effects on the decision of users to adopt smart cards. This finding is along the line of previous research in smart card adoption.

One difference from previous research which was found in this study is the fact that, in Thailand, income levels have no statistically significant effect on the decision of users to adopt smart cards. This finding may be due to the fact that the government has continuously promoted and assured Thai people that smart card fees will be low.

On Perceived Usefulness

This research presents a different result from previous studies in terms of users' perception of usefulness of smart cards. While previous studies mentioned that users in other cases give more importance to security rather than convenience and that convenience may not contribute much to the decision of users to adopt smart cards. The result of this study shows that convenience is a statistically significant factor affecting users' decision to use smart cards.

In addition to the results of the survey, researchers also solicited respondents' comments on the government's e-ID project. More than 90% of the respondents think that the e-ID will provide convenience to them, in terms of reducing the paper work and the service time, when they use government services or deal with government agencies. Thus, the statistical finding could be supported by the fact that there is a longer waiting time to receive government services in developing countries.

On Security Concerns

While previous studies recognized that security could be an important factor in the adoption of smart cards, this research is among the first ones to show empirical evidence that security concern is a statistically significant factor influencing users' decision to adopt smart cards. This finding is important because it provides useful strategic implications for the implementation of the smart card projects in the future. It also shows that regardless of the level of development a country is at, security issue should be taken into account seriously when considering the introduction of smart cards.

Conclusion and Implications

Smart card technology was first introduced in Thailand by the Thai government who planned to use the technology for the government's e-ID and e-Government projects in 2004. This situation is contrary to the introduction of smart cards by the private sector in developed countries. On the research front, this contrast provided an excellent opportunity to study the differences, if any, in factors affecting consumers' perceptions of smart card technologies.

The study shows that, statistically, no demographic factors, except age, were found to have statistically significant effects on the users' decision to use smart cards. In addition, it was found that perceived convenience and security level of smart cards are the other two statistically significant factors found to affect users' decision to adopt smart card technologies.

To date, many government agencies in Thailand are still arguing about what information and applications should be put on the e-ID smart cards. The key issue with respect to using smart cards in Thailand is not so much about which information or applications are the "right" ones to be put on the cards, but more on the matters of security, ownership management, and privacy protection of the consumers' information on the cards. This issue is very important to Thai people as shown by this study. As a result, the Thai government should put high emphasis on the security issue when planning for and implementing the smart card technologies in their e-ID and e-Government projects.

References

"Making Smart Cards Work in the Enterprise," <http://www.findbiometrics.com/Pages/feature%20articles/smartcards_pg1.html> (11 November 2004).

Benoit A. Auber and Geneviève Hamel, "Adoption of Smart Cards in the Medical Sector: the Canadian Experience," *Social Science & Medicine* 53, no. 7 (October 2001): 879-894.

Elizabeth Blakey and Clare Saliba, "Smart Cards Stack the E-Commerce Deck," *E-Commerce Times* (http://www.ecommercetimes.com), 28 December 2000, <http://www.technewsworld.com/story/6323.html> (11 November 2004).

David Chadwick, "Smart Cards Aren't Always the Smart Choice," 1999, <http://sec.isi.salford.ac.th/download/smart.pdf> (11 November 2004).

Fred D. Davis, Richard P. Bagozzi, and Paul R. Warshaw, "User Acceptance of Computer Technology: A Comparison of Two Theoretical Models," *Management Science* 35, no. 8 (August 1989): 982-1003.

Fred D. Davis, Richard P. Bagozzi, and Paul R. Warshaw, "Extrinsic and Intrinsic Motivation to Use Computers in the Workplace," *Journal of Applied Social Psychology* 22 (1992): 1111-1132.

Digital Security Initiative Workgroup, "Executive Summary of Government Smart Card Interoperability Specification (GSC-IS)," 3 April 2002, <http://www.dsiw.org> (11 November 2004).

EC Strategic Factor, *Technology Diffusion in Services Electronic Commerce* (1999), <http://www.strategic.ic.gc.ca> (11 November 2004).

Roland Fournier, "IT and Facilities – Leveraging Smart Badges for PC, Network, VPN and Building," (paper presented at the RSA Security Web Seminar, 27 March 2002), <http://www.RSA.com> (11 November 2004).

International Engineering Consortium, *Smart Cards in Wireless Services* (2003), <http://www.iec.org/online/tutorials/ smartcard/>.

David Knights, Faith Noble, Theo Vurdubakis, and Hugh Willmott, "Chasing Shadows: Control, Virtuality and the Production of Trust," *Organization Studies* 22, no. 2 (March 2001): 311-340.

Tim Miller, "How Smart Are Smart Cards?," *Enterpreneur.com* (11 March 2002), <http://www.Enterpreneur.com> (11 November 2004).

Mintel International Group, *Smart Cards – UK* (June 2001), <http://reports. mintel.com/> (11 November 2004).

Phillips Semiconductors, *Information about Mifare Contactless Smart Card Chips* (2002), <http://www.semiconductors.phillips.com.markets/identification/products/ mifare> (10 November 2004).

US General Services Administration (GSA), *Smart Card Tutorial* (31 March 2002), <http://egov.gov/smartgov/tutorial/smartcard_foyer.htm> (11 November 2004).

VentureSolicitor.com, *Factors Accounting for Increasing Use of Smart Card Technology* (2003), <http://www.VentureSolicitor.com> (11 November 2004).

Notes:

[1] Cristopher R. Plouffe, Mark Vandenbosch, and John Hulland, "Why Smart Cards Have Failed: Looking to Consumer and Merchant Reactions to a New Payment Technology," *The International Journal of Bank Marketing* 18, no. 3 (2000): 112-122.

[2] Fred D. Davis, "Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology," *MIS Quarterly* 13, no. 3 (September 1989), 318-340.

[3] Gene Hinkle, "Hong Kong ID Project to Use Smart Card Management Software from ACI Worldwide," ACI Worldwide, 22 October 2002, <http://www.aciworldwide.com> (10 November 2004).

[4] Cristopher R. Plouffe, Mark Vandenbosch, and John Hulland, "Intermediating Technologies and Multi-Group Adoption: A Comparison of Consumer and Merchant Adoption Intentions toward a New Electronic Payment System," *The Journal of Product Innovation Management* 18, no.2 (2001): 65-71; Plouffe, Vandenbosch, and Hulland, "Why Smart Cards Have Failed."

[5] Gregory E. Truman, Kent Sandoe, and Tasha Rifkin, "An Empirical Study of Smart Card Technology," *Information & Management* 40, no. 6 (2003): 591-596.

[6] Truman, Sandoe, and Rifkin, "An Empirical Study of Smart Card Technology."

[7] Plouffe, Vandenbosch, and Hulland, "Intermediating Technologies and Multi-Group Adoption."

[8] Grover S. Kearns and Stephen Loy, "Global Acceptance of Stored-Value Smart Cards: Analysis of Inhibitors and Facilitators," *International Journal of Services Technology and Management* 3, no. 4 (2002): 417-423.

[9] Truman, Sandoe, and Rifkin, "An Empirical Study of Smart Card Technology."

[10] Plouffe, Vandenbosch, and Hulland, "Intermediating Technologies and Multi-Group Adoption."

[11] Truman, Sandoe, and Rifkin, "An Empirical Study of Smart Card Technology."

[12] Plouffe, Vandenbosch, and Hulland, "Intermediating Technologies and Multi-Group Adoption."

[13] Truman, Sandoe, and Rifkin, "An Empirical Study of Smart Card Technology."

[14] Plouffe, Vandenbosch, and Hulland, "Intermediating Technologies and Multi-Group Adoption."

[15] Truman, Sandoe, and Rifkin, "An Empirical Study of Smart Card Technology."

[16] Plouffe, Vandenbosch, and Hulland, "Intermediating Technologies and Multi-Group Adoption."

[17] Truman, Sandoe, and Rifkin, "An Empirical Study of Smart Card Technology."

[18] Kearns and Loy, "Global Acceptance of Stored-Value Smart Cards: Analysis of Inhibitors and Facilitators."

[19] Truman, Sandoe, and Rifkin, "An Empirical Study of Smart Card Technology."

[20] Sasiwimon Boonruang, "Electronic ID Key to Thailand's e-Govt Services," *Bangkok Post* (22 January 2002); Sasiwimon Boonruang, "Govt Envisions One-Stop Service – e-Citizen Initiative Showing Progress," *Bangkok Post* (9 October 2002); Sasiwimon Boonruang and Karnjana Karnjanatawe, "Cyber Laws Pass – but Confusion Reigns," *Bangkok Post* (30 August 2000); Sasiwimon Boonruang and Karnjana Karnjanatawe, "Thailand's Government

Services Move Online," *Bangkok Post* (9 January 2002), <http://www.bangkokpost.com>; "Government to Play the Smart Card Trick," *Bangkok Post* (22 May 2002), <http://www.bangkokpost.com>.

[21] "Government to Play the Smart Card Trick."

[22] Boonruang and Karnjanatawe, "Cyber Laws Pass – but Confusion Reigns."

[23] Boonruang, "Electronic ID Key to Thailand's e-Govt Services;" "Government to Play the Smart Card Trick."

[24] Boonruang and Karnjanatawe, "Cyber Laws Pass – but Confusion Reigns."

[25] Boonruang and Karnjanatawe, "Cyber Laws Pass – but Confusion Reigns;" "Government to Play the Smart Card Trick."

[26] Boonruang, "Electronic ID Key to Thailand's e-Govt Services;" Boonruang and Karnjanatawe, "Cyber Laws Pass – but Confusion Reigns;" "Government to Play the Smart Card Trick."

DONYAPRUETH KRAIRIT holds a Ph.D. from Massachusetts Institute of Technology (MIT) in Telecommunications Technology and Policy. She was a consultant in telecommunications and a guest speaker at Harvard and Tufts University. Her research has been in the field of telecommunications and sustainable development, economic and policy implications of technologies, and e-commerce, with particular focus on Asian countries and the U.S. She is now an assistant professor at the School of Management, Asian Institute of Technology (AIT), Thailand, and on the external evaluation committee working for the National Science and Technology Development Agency (NSTDA). *Address for Correspondence:* School of Management, Asian Institute of Technology (AIT), 58 Moo 9, Paholyothin Rd., Km. 42, Klong Luang, Pathumthani 12120, THAILAND; *E-mail:* donya@ait.ac.th, donya@alum.mit.edu.

WORRAYA CHOOMONGKOL is an independent IT trainer and consultant. She has an MBA degree from Thammasat University. She has been in the telecommunications industry for more than 10 years and worked with many international firms, including Nokia, on telecommunications issues in the Southeast Asian region. She has particular interests and much experience in wireless communications, smart cards, and telecommunication network planning. *E-mail:* cworraya@hotmail.com.

POONDEJ KRAIRIT is a doctoral student in the Computer and Engineering Management Program at Assumption University, Thailand. He has a Master's degree in telecommunications from Boston University. His current research is on the cost and demand modeling and cost-benefit analysis of integrated wireless network. *E-mail:* poondej@hotmail.com.

GOVERNMENT PKI DEPLOYMENT AND USAGE IN TAIWAN

Chung-Ming OU, Hwai-Ling SHAN, and Chuan-Te HO

Abstract: The ongoing e-Government Program in Taiwan started in 1997. It is based on the Government Service Network, which is the backbone infrastructure of the network transaction environment. During the first phase of this program in 1998, Taiwan established its first Certification Authority, namely, the Government Certification Authority (GCA), and this launched the electronic certification services in Taiwan. From 2001 to 2004, the Government Public Key Infrastructure (GPKI) has been established according to the planning set forth in the e-Government Program with the aim of strengthening electronic government infrastructure and establishing electronic certification and security applications for executive administration. Besides GPKI applications, PKI interoperability has become a major issue in Taiwan recently. Several interoperability schemes, such as strict hierarchy and Bridge Certificate Authority (BCA), have been deployed in different PKI domains. To achieve global PKI interoperability in Taiwan, BCA is being adapted as a major CA-CA interoperability engine, which will ensure trusted relationships between the different PKI domains.

Keywords: GPKI, GRCA, GCA, MOICA, MOEACA, Digital Signature.

PKI and Secure e-Taiwan

Taiwan was successful in shifting industry policies to focus on high-technology products, which is a strategy successfully transforming Taiwan into one of the largest hardware-exporting nations worldwide. This strategy has a major impact on national strategy in harnessing information and communication technologies for economic development and global competitiveness. To accelerate the transformation of traditional industries to a knowledge-based economy, the Cabinet had approved the e-Taiwan project (2002-2007), which is composed of e-Government, e-Industry and e-Society projects. Among these projects, e-Government will be the major driving force. There are several important plans under the "e-Taiwan Project" aim to build a more secure infrastructure for the information and communication security environment, and they are listed below[1]:

Natural Person Certificate Project

Object	• Assist e-Government to promote internet personal identification. • Issue over 3 million Natural Person Certificates by 2005.
Current Status	• Natural person CA was established and 50 register counters have been setup in registration offices in districts and counties. • More than 50 applications in 7 systems exploiting personal IDs have been developed by government agencies.
Period	2002~2007
Note	Electronic Signature Law was enacted on 31 October 2001 and became effective on 1 April 2002.

Establish Certificate Interoperability Mechanism

Object	• Build certificate interoperability mechanism between domestic and international domain. • Enhance CA industry development.
Current Status	• A PKI infrastructure interoperability committee has been setup and a Bridge CA which completed interoperability testing between two CA. • 28 PKI applications have been developed by private sectors under grant support from this project.
Period	2003~2007

Establish National Security Operation Center

Object	• Provide 24 hours/day network system monitoring and incident handling for 500 monitor points of important government agencies.
Current Status	• The design of monitor functions, SLA, common format of data exchange is under way. • A POC prototype is being developed.
Period	2003~2006

Information Security Product Certification Scheme

Object	• Create the security product certification scheme in Taiwan and plans of the testing laboratory construction.
Current Status	• Increase Information Security products testing and certification skill to provide consulting service. • Seek for the framework and its associated specifications for a CC-conformity testing laboratory. • Provide training courses for evaluators and assessors.
Period	2003~2006

The e-Government Program of Taiwan was initiated in 1997. The Government Service Network (GSN) was one of the sub-programs put to work since June 1997.[2,3,4] GSN is the fundamental infrastructure of the electronic government, providing network framework on which e-services are rendered. To establish a secure and trusted network transaction environment based on the GSN, Taiwan has launched electronic certification services. This involved establishing the e-government digital certification system, promoting Government PKI, and facilitating the development of government online information and service applications (see Figure 1). To promote e-government services, the Research, Development, and Evaluation Commission (RDEC) of the Executive Yuan (commonly known as the Cabinet) has since then instituted Government Electronic Certification Steering Committee so that opinions and ideas from experts and citizens can be efficiently and objectively reflected through the process.

The need of providing the GSN with an authentication/secure communication mechanism was the motive of building our GPKI. GPKI has been built according to the structure defined in the ITU-T X.509 standard, namely, there is a trust anchor for GPKI, a Government Root Certification Authority (GRCA), and underlying subordinate CAs for individual government sectors. The evolution of GPKI in Taiwan comprises two phases. In phase 1, RDEC has implemented a pilot certification authority (CA), namely, the "Government Certification Authority" (GCA), which served as a multi-purpose CA for issuing public key certificates to the government agencies, citizens, and application servers, as well as to corporations. In February 1998, RDEC commissioned Chunghwa Telecom, which is a major telecommunication company in Taiwan, to establish the GCA in phase 1, which provides electronic certification services so that users can be identified online. The GCA provides currently a variety of electronic certification services to government agencies, business organizations, and citizens. More than 536 000 electronic certificates of all classes have been issued

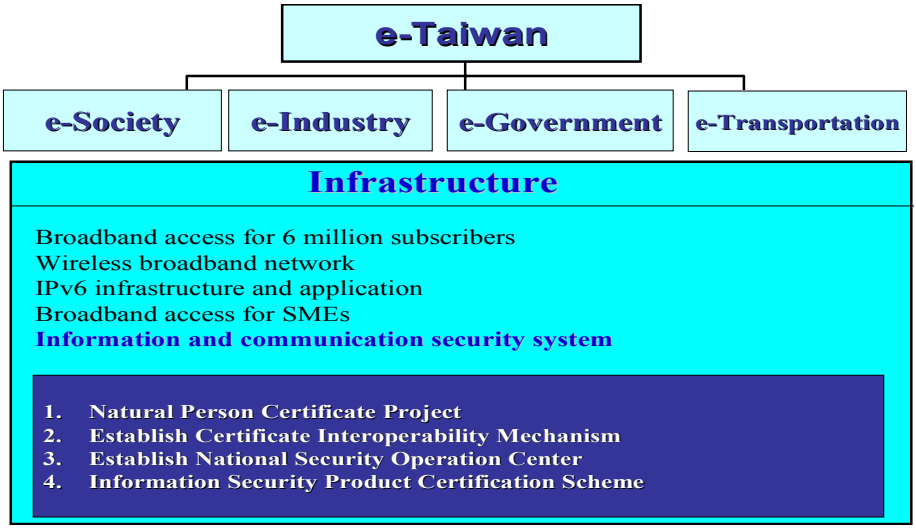


Figure 1: PKI and e-Taiwan Project.

since the establishment of GCA in 1998. The certificates have been used for such applications as online income tax filing, motor vehicle registration, electronic payment, electronic procurement, and official electronic document exchange.

In the mean time, as tremendous hands-on experience was gained, the acceptance of the PKI technology in Taiwan grew, and the relevant legislation such as the Electronic Signature Act was enacted, a clearer perspective appeared. RDEC recognized the need for "branching" the earlier multi-purpose GCA in response to more realistic and versatile applications. Hence, the objective of the *second phase* GPKI is to transform the earlier naive design into a full-fledged PKI based on the GPKI hierarchy and established GRCA, under which some government agencies acting as the proper authorities in corresponding fields will establish their CAs.

Framework and Services of GPKI

GPKI Framework

The GPKI in Taiwan is under the oversight of the Government Electronic Certification Steering Committee (GECSC). The responsibilities of the Steering Committee are as follows:

- To survey and review the Certificate Policy and Certification Practice Statements of CAs within the GPKI.
- To survey and review technical standards of digital certificates.

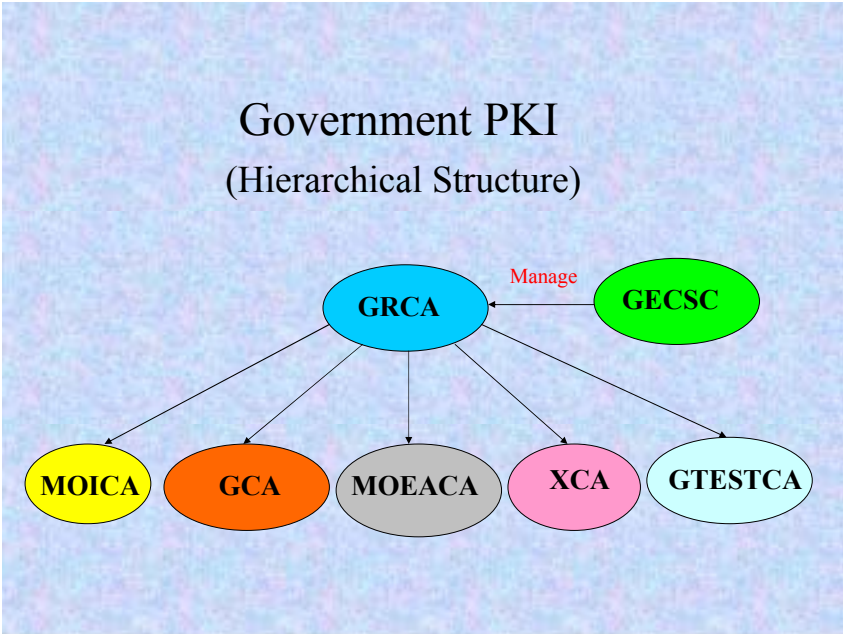


Figure 2: Framework of GPKI.

- To survey and review framework of digital certificates.
- To survey and review related administrative issues of digital certificates.

Following the hierarchical structure defined in the ITU-T X.509 standard,[5,6,7] GRCA is a trust anchor for GPKI. Other CAs within the GPKI are established by individual government sectors. They issue certificates to be used in applications of electronic government in order to provide more convenient Internet service for the citizens and business; this improves governmental administration efficiency and promotes applications development of electronic commerce. According to the e-Government Program (2001-2004), the designated organizations responsible for building corresponding CAs are illustrated in Figure 2; those CAs are responsible for providing certification services to government agencies, industry and business organizations, and citizens, which are named GCA, MOICA, MOEACA, XCA and GTestCA. The GRCA has issued certificates to these CAs since 2002. Table 1 lists the number of certificates issued by these CAs.

GCA (Phase 2)

Phase 2 of the GCA was initiated by RDEC in 2003, whose mission has switched from the phase 1 mission to issue certificates to all government sectors, which includes government organizations, government organizational units and server appli-

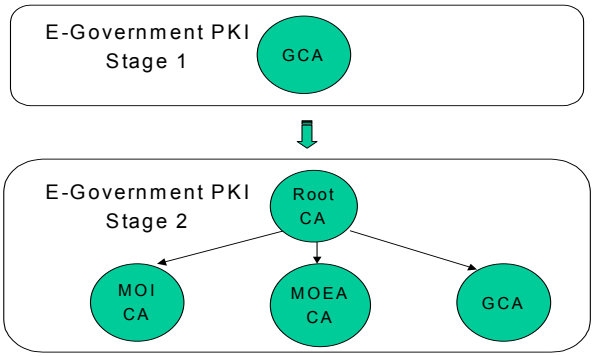


Figure 3: Evolution of E-Government PKI.

cations. It has issued more than 55 228 certificates so far.

MOEACA

The MOEACA was established by the Ministry of Economic Affairs (MOEA) in 2003. It issues certificates to all industry and business groups, which includes factories, companies and proprietors. So far there are around 3 493 certificates being issued. This MOEACA can be used for e-government applications such as industry and commerce registrations, bid getting and bid submitting, tax filing, and labor insurance updating.

MOICA

The MOICA was established by the Ministry of Interior in 2003. It issues certificates to all Taiwanese citizens and there are around 521 904 certificates being issued so far.

XCA

The XCA was established by RDEC in March 2004. It issues certificates to schools, juridical associations and consortiums. Total number of issued certificates is around 1 719.

GTestCA

The GTestCA was established by RDEC in 2003, which issues testing certificates to all GPKI applications. So far there are 4 056 certificates being issued.

Table 1: Certificates Issued by GPKI.

	GCA(old)	GCA(new)	XCA	MOEACA	MOICA	TOTAL
1998	33,901	0	0	0		33,901
1999	67,561	0	0	0		67,561
2000	104,854	0	0	0		104,854
2001	212,408	0	0	0		212,408
2002	418,178	0	0	0		418,178
2003	522,541	14,396	0	1,295	248,392	786,624
2004(Oct. 28)	530,490	55,228	1,719	3,493	521,904	1,112,834

GPKI Services

In RDEC's design of electronic certification applications (based on X.509 v3, year 2000 edition), the e-government electronic certification structure has the following components: Public Key Infrastructure (PKI) and Privilege Management Infrastructure (PMI). The former provides public certification services for authentication and non-repudiation with public key certificates stored in smart cards; the latter provides attribute certification service for authorization. PMI does not have a hierarchical structure in that, each Attribute Authority (AA) will issue attribute certificates within the scope of its authority independently and it is not subordinated to any other authority. Implementation of a functioning PMI which provides attribute certification services is expected to be completed in the near future. Therefore, we may conclude that the GPKI major services are as follows:

- To issue and manage certificate services;
- To manage certificate revocation and renewal;
- To publish certificates and certificate revocation list (CRL);
- To provide application programming interface (API) such as data encryption, digital signature, and digital envelope;
- To provide time stamp services;
- To provide testing certificates.

To support these services, the GPKI framework is designed to comprise the following components:

- A secure, trusted, and interoperable electronic certification mechanism. It supports secure and trusted government services;
- A variety of public key certification services. Their integrated and innovative functionalities will promote the widespread use of online applications;

- The PMI (Privilege Management Infrastructure), which will provide attribute certification services and satisfy various certification requirements for GPKI applications.

PKI-Enabled e-Services

According to Wang,[8] there are around 353 applications for GPKI and 45 companies are becoming solution providers for GPKI applications. Those applications can be divided into three categories, which are G2G, G2B, and G2C.

G2G Applications

e-Official Document Interchange

E-Official Document Interchange provides a portal for all governmental sectors to exchange electronic documents among them. GCA certificates are needed for those government sectors while adapting to this application. According to the future GPKI plan, each government official in charge of producing electronic documents will also need to append his/her digital signatures to those documents via his/her MOICA certificate. This so-called multi-signature document format will meet practical situations among government sectors in Taiwan.

e- Payment

E-Payment transforms the payment and fund-transferred information to non-reputable electronic forms, which are sent to the government payment center via GSN. This application requires the participating government sectors to apply their GCA certificates.

G2B Applications

e-Procurement

E-Procurement provides a portal to contractors and solution providers to get and submit governmental bids. This guarantees a fair bidding environment for every qualified contractor and service provider. All solution providers and contractors can purchase bid-offering documents and deliver bidding documents through Internet, after they have been issued MOEACA certificates. GPKI services guarantee that this application initiates a trusted and secure network transaction environment between government sectors and corporations.

e-Corporation

E-Corporation assists corporations in registering or updating their corporation information on-line. Corporations need to apply the MOEACA certificates first and this application can reduce lots of time-consuming paperwork.

e-Tax Refund

E-Tax Refund assists the Customs in returning taxes to foreign tourists while leaving Taiwan. This application provides a gateway for electronic information exchange between the tax bureau, corporations, the Customs, the Bank of Taiwan and the tax data center. Moreover, this application is a combination of a G2G and a G2B application, or we may refer it as a G2G2B application. GCA and MOEACA certificates are needed depending on the end-entities.

Customs e-Applying

An applicant for Customs e-Applying may be a person, a corporation, a Customs-applying company, or a special delivery company, among others. A Customs-application form is appended by a digital signature of a Customs-applicant. Depending on the entity, a Customs-applicant needs to provide either MOICA certificate or MOEACA certificate to this application.

Labor and Farmer Insurance On-Line System

The Labor and Farmer Insurance on-line system utilizes MOICA certificates to assist government officials in doing administrative work via Internet such as updating insurers' information. On the other hand, insurers can inquire about their insurance information using MOICA certificates.

G2C Applications

e- Household Registry

The e-Household Registry assists all residences in Taiwan in performing household services via Internet, such as completing general household information. The Ministry if Interior is planning to put most of the household registry services on-line.

Land Administration Electronic Gateway Information System

This is an on-line service for citizens who may file applications such as land price reporting, land registers' basic information update and land information update. A land register can also inquire about the rate of processing of his/her case on-line.

e-Motor-Vehicle Service

The e-Motor-Vehicle service assists all car owners who have MOICA certificates in requesting and renewing automobile registration licenses; it also assists car owners in requesting and paying traffic tickets.

e-Taxation Service

The e-Taxation service—the first G2C application of GPKI started in 1998—assists

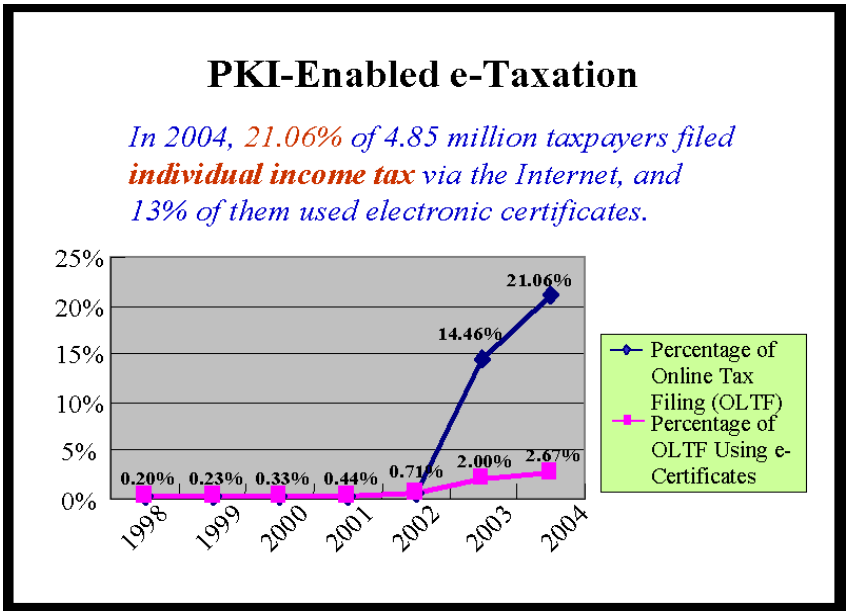


Figure 4: PKI-Enabled E-Taxation.

citizens and corporations filing income taxes and business taxes, respectively. This application has become one of the major achievements of Taiwanese GPKI for the past several years.

PKI Interoperability

PKI interoperability is identified as one of the most important obstacles to PKI deployment and usage. A survey conducted by OASIS in June 2003 highlights that the most serious interoperability problems are path validation, smart cards, unusual certificate content, cross-certification, certificate issuance, certificate revocation, and protocols. The most common problems[9] identified were standards: too many in some areas, too few in others, too ambiguous, poor implementations, no conformance testing, etc. Incompatible certificate policies were another concern. Due to the fact that PKI interoperability is especially complex, RDEC has allocated more resources and put a lot of effort in dealing with this issue.

Cross Certification with GRCA

There are three interoperability technologies deployed in Taiwan: cross certification, Bridge CA, and strict hierarchy. Basically, GRCA is in charge with the interoperabil-

ity of GPKI with other PKI (including foreign PKI).

A CA that interoperates with GRCA through cross-certification is referred to as an interoperating CA. To get GRCA's approval for cross-certification, the applicant CA must comply with the requirements of the assurance level defined in the cited Certificate Policy. Additionally, the applicant CA must have the capabilities to establish and manage the following aspects: Public Key Infrastructure; Digital signatures and certificate issuing technology; the corresponding responsibilities and obligations among CA, RA, and the relying party.

GRCA issues the certificate to the applicant CA if instructed by RDEC. After issuance, RDEC shall notify the applicant CA with formal official document, attached with the issued certificate. If RDEC decides not to issue the cross-certificate, the applicant CA shall also be notified by a formal official document along with the reason(s) for the rejection.

GRCA has its self-signed certificate (verified by RDEC) delivered to the applicant CA in accordance with the procedures of GRCA's Certificate Policy Statement (CPS). Upon receiving the notification of the approval delivered via formal official document, the applicant CA shall examine the attached certificate to ensure the correctness of its content. After the applicant CA verifies the correctness, it must sign a confirmation document, which shall be sent back to GRCA and RDEC by a formal official document. When GRCA receives a confirmation document, it shall post the newly issued certificates to the repository. If the applicant CA fails to respond within 30 days (upon receiving the approval notification), it is viewed as a refusal to accept the certificate. RDEC shall then authorize GRCA to revoke that certificate after verification. No additional announcement shall be made concerning the application.

Bridging GPKI and Commercial PKIs

The Ministry of Economic Affairs (MOEA), which is the authority in charge with PKI, has deployed Taiwanese BCA in 2004 as the major PKI interoperability platform. BCA will only issue cross certificate to a CA that becomes its member; BCA will not issue any certificates to end-users. Taiwanese BCA will not play a trust point for any PKI in order to respect the autonomy of each PKI.

Since there are distributed PKIs throughout different domains, such as government, finance and healthcare systems, BCA is regarded as a proper solution for Taiwanese PKI interoperability (see Figure 5) Furthermore, many foreign countries such as United States, Japan, Germany, China and Canada, have been either deployed or being planned for BCA interoperability.

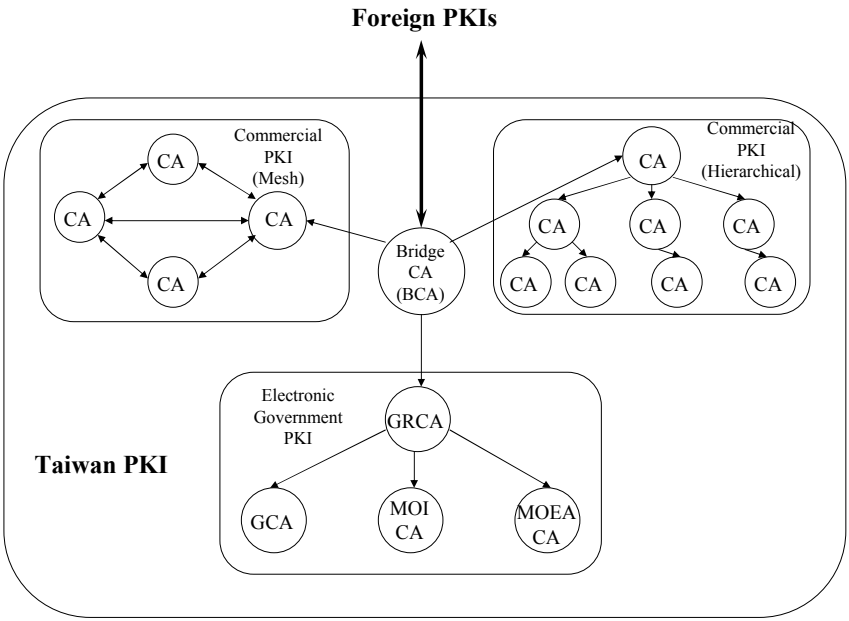


Figure 5: The Role of the Bridge CA in Taiwan PKI.

Currently, there are several companies acting as certification service providers for issuance of public-key certificates for commercial use. There are some end-entities the jurisdiction of which is out of the GPKI domain. Thus, the appearance of commercial PKI is a complement to a complete Taiwanese PKI. It is anticipated that there will be a need for cross certification between CAs in the GPKI and CAs in a commercial PKI. The rough draft, as shown in Figure 5, is to establish a Bridge CA (BCA)[10] as a bridge of trust that provides trust paths between the various PKIs in Taiwan. In addition, the BCA will also act as a bridge of trust that provides trust paths between Taiwanese PKI and foreign PKIs.

Each PKI has one principal CA that cross-certifies with the BCA. In the case of a PKI with hierarchical certification paths, it will be the root CA of the domain. In a mesh-organized PKI, the principal CA may be any CA in the domain. However, it will normally be one operated by, or associated with, the domain policy management authority. It is also anticipated that there will be a need for constituting a Policy Management Authority because cross certification will involve policy approval and policy mapping among different PKIs and the overall policies of the BCA. Thus, the main subject of phase 3 will comprise policy management, policy approval, policy map-

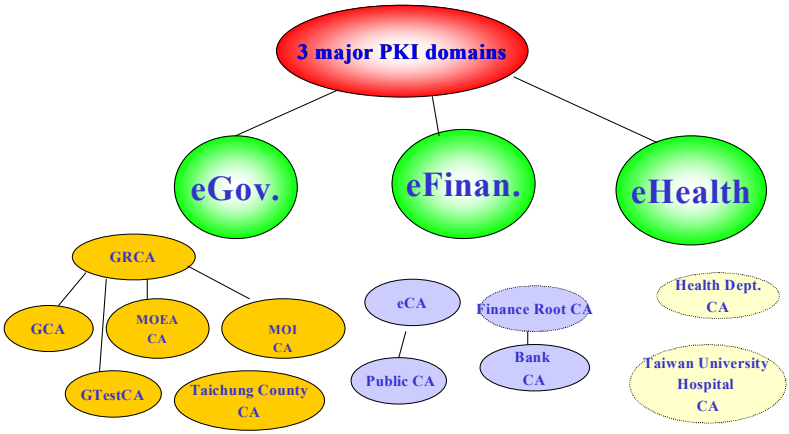


Figure 6: Three Major PKI Domains in Taiwan.

ping, and cross certification.

Global PKI Interoperability in Taiwan

The key for global PKI interoperability is to adapt the original certificate paths within each PKI domain. BCA will not influence any certificate path of each PKI domain. It is a better approach BCA to establish a peer-to-peer relationship; this means it is not superior to GRCA or the principal CA in each PKI domain. CAs do not need to connect to Taiwanese BCA unless they need to interoperate with CAs in different PKI domains.

Both from policy and technology point of view, the following four issues arise while considering adapting BCA as Global Taiwanese PKI Interoperability.

- *Establish the Policy Management Authority (PMA)*: PMA provides the operational guideline for BCA. PMA members should be those CAs which intend to interoperate with each other.
- *Establish the BCA Certificate Policy (CP)*: Before BCA issues a cross certificate to its member CA, this CA has to be audited by the BCA (actually, BCA can outsource this auditing task to some proper third-party organization). Furthermore, the assurance level of an issued certificate has to be mapped to that of BCA CP. Therefore, trust relationship between CAs can be built. The standard of the BCA CP may be referred to ANSI X9.79 and IETF RFC 2527.

- *BCA Technical Template*: After the CA-CA trusted relationship has been established, the technical details for interoperability will be a major issue.
- *Establish CA Auditing System*: CA has to be ensured that its operational and management security engine has passed the third–party inspection. One of the major auditing procedures is that CA must operate according to the assurance level acclaimed by its CPS.

Conclusions

GPKI is used in many e-services in Taiwan. As of October 2004, government agencies have promoted more than 900 online services. However, GPKI has not reached its full potentials in Taiwan. A number of barriers, including lack of applications, high cost, poor understanding of PKI, and interoperability issues have contributed to the limited use of Government PKI.

According to the survey conducted by OASIS in June 2003, respondents identified that the most important obstacles to PKI deployment and usage are (1) Software applications do not support IT; (2) Costs are too high; (3) PKI is poorly understood; (4) Too much focus on technology, not enough on need; and (5) Poor interoperability. The survey also indicated that the most important applications for PKI are document signing, secure e-mail, electronic commerce, and single sign-on. Document signing was further broken down into singing forms, signing contracts, and signing documents before dissemination. GPKI deployment and usage in Taiwan is facing the similar obstacles. In order to increase take-up of PKI, RDEC identified electronic document exchange and e-taxation as the most important applications. RDEC also adopts a free digital certificate policy, which means that every citizen, company and government agency can apply a digital certificate for free. This policy helps the users to set up a test PKI with little or no cost. It is useful for testing and as a way to encourage people to get started with PKI.

PKI was invented more than 20 years ago. Today, it is used in many important online services. But a number of barriers limit usage of PKI. Increasing take-up of GPKI was directly related to the value gained from a secure e-government program in terms of improved service, greater efficiency, costs saving, and trusted online services. Clearly, the full potential of GPKI will be realized only if citizens and business use it, but most governments still find themselves confronted with the challenge of low usage and the need for innovative methods to drive take-up. In Taiwan, promoting take-up of GPKI is taking hold, but the challenge remains. PKI involves many parties: customers and users, operators, software developers (for applications, auditors, and security experts). GPKI take-up needs support from all these parties.

Notes:

[1] National Information and Communication Security Taskforce (NICST), *Information and Communication Security Services for e-Government* (October 2003), <http://www.nicst.nat.gov.tw> (12 November 2004).

[2] The Executive Yuan of the Republic of China, *Note of the Executive Yuan Council No. 2557 Meeting* (1997), <http://www.ey.gov.tw> (12 November 2004).

[3] Research Development and Evaluation Commission of the Executive Yuan, *Introductory to the Electronic/Networked Government Program* (1998), <http://www.rdec.gov.tw>.

[4] Data Communication Group of Chunghwa Telecom Co. Ltd., *Proposal for Government Service Network (GSN) of the Electronic/Networked Government Program* (1998), <http://www.rdec.gov.tw> (12 November 2004).

[5] Russell Housley, Warwick Ford, W. Polk, and David Solo, "Internet X.509 Public Key Infrastructure, Certificate and CRL Profile," Internet Draft, The Internet Engineering Task Force (IETF), PKIX Working Group, RFC 2459, January 1999, <http://www.faqs.org/rfcs/rfc2459.html> (12 November 2004).

[6] Stefan Santesson, Tim Polk, Petra Barzin, and Magnus Nystrom, "Internet X.509 Public Key Infrastructure Qualified Certificates Profile", The Internet Engineering Task Force (IETF), RFC 3039, January 2001, <http://www.faqs.org/rfcs/rfc3039.html> (12 November 2004).

[7] William E. Burr, "Public Key Infrastructure (PKI) Technical Specifications: Part A - Technical Concept of Operations," NIST FPKI, Working Draft TWG-98-59, September 1998, < http://csrc.nist.gov/pki/twg/baseline/pkicon20b.PDF> (12 November 2004>.

[8] Wen-San Wang, "Current Status & Future Perspective of PKI Development in Taiwan," (paper presented at the International Conference of Collaboration of e-Commerce Applications and Security, Taipei, Taiwan, 14-15 September 2004).

[9] The OASIS PKI Technical Committee, *PKI Action Plan* (22 February 2004), <http://www.oasis-open.org/committees/pki/pkiactionplan.pdf> (12 November 2004).

[10] Burr, "Public Key Infrastructure (PKI) Technical Specifications."

CHUNG-MING OU received BS degree in Applied Mathematics in 1987 from Chung-Yuan Christian University, Taiwan, and MS and Ph.D. degrees in Applied Mathematics from Iowa State University, Ames, IA in 1994 and 1996 respectively. Dr. Ou was a MATLAB consultant and software engineer before he joined Chunghwa Telecommunications Lab as a researcher in 1997. His research focuses on cryptography, wireless security and PKI. Dr. Ou also assists in Government PKI e-Government project in Taiwan and PKI Interoperability within Asia PKI Forum. His area of specialty includes Cryptography, Information Security, Numerical Simulation, Computational Sciences and Applied Mathematics. *E-mail:* cou@cht.com.tw.

HWAI-LING SHAN received BS degree in Applied Mathematics in 1986 from Chung-Yuan Christian University, Taiwan, Ph.D. degree in Mathematics and MS degree in Computer Science from Pennsylvania State University, University Park, PA in 1995. She was a Post-doctoral Research Fellow within the Department of Computer Engineering, National Central University, Taiwan until 1998, when she joined Chunghwa Telecommunications Lab as a researcher. She focuses on cryptography, analyzing cryptographic algorithms and standards (including FIPS140, Common Criteria, etc). She also participates in the certification process of Hardware security module against FIPS140-2 and the development and establishment of Government PKI e-Government project in Taiwan. Her area of specialty includes Number Theory, Cryptographic Standards & Protocols, Applications & Services based on Public-Key Infrastructure and Telecommunication Products & Services. *E-mail:* shanhl@cht.com.tw.

CHUAN-TE HO received his master's degree from the Institute of Public Administration, National Chengchi University (Taiwan). Before assuming his present position as a Director of Department of Information Management, Research, Development, and Evaluation Commission of Executive Yuan in July 2004, he had served in the field of Information Management for over 20 years, during which he had participated in the planning or/and management of a number of IT-related projects, such as Electronic Government programs planning and promoting, Public Key Infrastructure policy planning, Government IT outsourcing policy planning, and Electronic Signature Law (as a drafter). He has also written a number of papers on information-related subjects and he has presented them at international workshops and conferences, including: A Study on Government Information Business Overall Outsourcing Systems, A Study on Government Information Security Management Systems, Secure and Trusted Infrastructure for e-Government, How to Establish an e-Government Information Security Mechanism, Electronic Signature and Electronic Authentication Mechanism, and Encryption Technology and Trust Mechanism in Digital Society. *E-mail:* chuan-te@rdec.gov.tw.

DESIGN OF A SECURE FINE-GRAINED OFFICIAL DOCUMENT EXCHANGE MODEL FOR E-GOVERNMENT

Yi-Hui CHEN and Eric Jui-Lin LU

Abstract: At present, the exchange of information via Internet is widely used in electronic government (e-Government). To securely and effectively exchange official documents among government agencies, an exchange model has been developed by the government of Taiwan. Although a RSA cryptosystem is used in the model to ensure security and XML is employed to increase interoperability, the current design does not take advantage of the rich structure of the XML documents, and it may result in possible security leaks due to the fact that, traditionally, the whole document is signed and encrypted. Considering the characteristic that it is easy to integrate encryption, signature and access control into XML documents, a fine-grained official document exchange model for e-Government is proposed in this article. In addition, the proposed model conforms to standards such as XML Encryption and XML Signature.

Keywords: e-Government, XML Encryption, XML Signature, Document Exchange.

The global acceptance of electronic commerce and the progress made in network technologies have great impact on the development of electronic government (e-Government). One of the main objectives of e-Government is to exchange information between government agencies in a timely manner.[1,2,3] In Taiwan, the e-Government program was initiated in 1997.[4] During the first phase of the program, Taiwan established the country's first certification authority – the Government Certification Authority (GCA). From 2001 until 2004, one of the major applications of the e-Government program enabled the secure and effective exchange of official documents between governmental agencies. As a result, an exchange model has been developed.[5,6,7] In the model, as illustrated in Figure 1, an official document is first transformed into XML format;[8,9] then the XML-based document is signed and encrypted; and finally the encrypted document is sent to the Official Document Exchange Center. Next time when the recipient logs in, the ciphered document will be retrieved

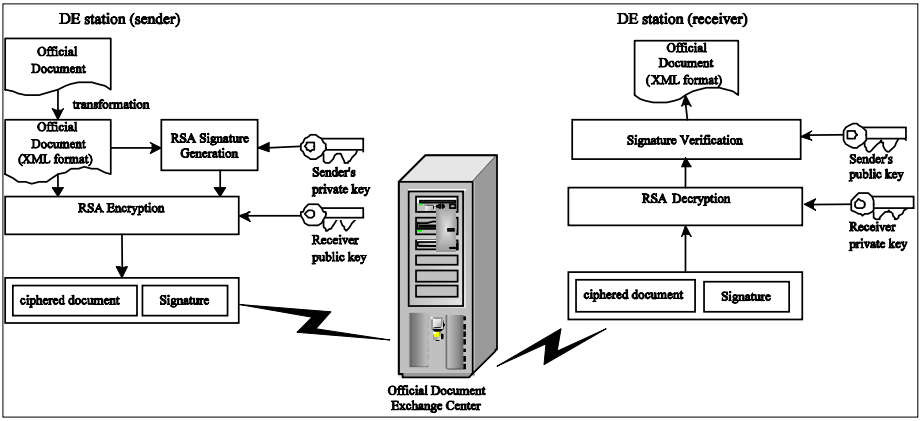


Figure 1: An Official Document Exchange Model.

from the center. The received ciphered document will then be decrypted and verified in order to obtain the original document.

Although the Rivest-Shamir-Adleman (RSA) cryptosystem[10] is used to ensure security and XML is employed to increase interoperability in the model, the current model does not take advantage of the rich structure of the XML documents and may result in possible security leaks due to the fact that, traditionally, the whole document is signed and encrypted. For example, in the current implementation, each agency assigns a specialized staff to send and receive official documents. When an official document, classified as "confidential," is received, the staff is still able to decrypt the whole document and read its content even though s/he is not authorized. Therefore, it is very important to design a secure official document exchange model with fine-grained control so that only designated recipients are allowed to read and process the received documents, while the staff that receives the incoming documents is only allowed to verify their validity.

To achieve these objectives, it is required that the official document contains all the information needed for encryption, signature, and access control. Traditional security mechanisms, in view of the fact that the target of access control is usually the whole document, require more than one file to accomplish these tasks. Fortunately, due to the rich structure of XML, *it is easy to integrate encryption, signature, and access control into one XML document*. Therefore, this article proposes a fine-grained official document exchange model for e-Government. Taking advantage of the rich structure of XML, the content of the XML documents can be encrypted at various security levels.[11] Example of an official document is given in Figure 2. The official document has two parts – header information and content of the document. The

header indicates that the document was issued on 2004/09/30, the official document is classified as "confidential," and the recipient is the Ministry of Defense. The body of the document describes the budget that is required to purchase missiles to enhance national security. The staff at the receiving desk will be able to read the header information of the received document. However, since the arriving document is classified as "confidential," s/he will not be able to read the content of the document. Instead, only the designated staff is allowed to decrypt and read the document.

```
<officialDocument>
 <headerInfo>
    <issueDate>2004/9/30</issueDate>
    <securityLevel> Confidential</securityLevel>
    <receiver>Ministry of Defence</receiver>
 </headerInfo>

 <content>
    <subject>Procurement of missiles</subject>
    <description>
       To enhance national security
    </description>
    <budget>250000000</budget>
 </content>
</officialDocument>
```

Figure 2: An Official Document Example.

The proposed model conforms to standards such as XML Signature[12] and XML Encryption.[13] The content of an official document can be encrypted by different keys based on the security level. And the staff can only decrypt and read the content of the document if s/he is authorized. In addition, due to the fact that the RSA cryptosystem is adopted in the proposed model, it is secure and can be easily incorporated into existing implementations.

The rest of the paper is organized as follows. First, a smartcard-based framework for secure document exchange, the XML Encryption, an XML Multi-signature scheme, and the XML Signature are briefly reviewed. Then the design of the secure fine-grained official document exchange model is described in detail. Afterwards, the authors analyze and summarize the advantages of the proposed model. Finally, some conclusions are provided in the last section.

Related Work

A Smartcard-Based Framework for Secure Document Exchange

A secure document exchange model was proposed by Yang, Ju, and Rao.[14] There are many Document Exchange (DE) Stations and a Security Management Center in the model, as shown in Figure 3. Each DE Station is responsible for sending and receiving documents and equipped with a smart card reader. Cryptographic algorithms are embedded in the smart card to provide security functions for digital signature and digital envelope. The Security Management Center is responsible for issuing smart cards, acting as a public-key certificate authority, regularly publishing certificate revocation list, and maintaining distribution lists. A distribution list contains a group of recipients that can be used as a mailing list to send and receive official documents.

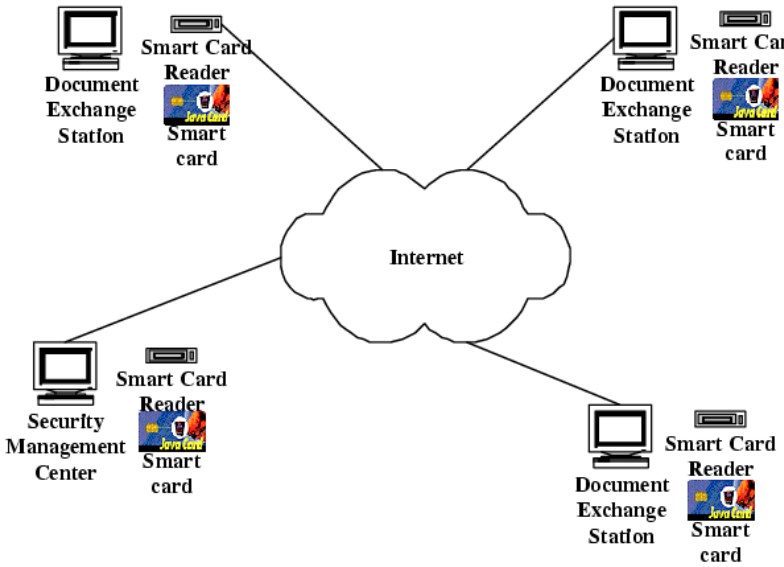


Figure 3: Yang-Ju-Rao's Secure Document Exchange Model.

An official document is first transformed into XML format, and the XML-based document is then signed and encrypted. Unlike the current implementation used in the Taiwanese official document exchange system, the ciphered document and its signature are sent directly to the recipient. Upon receiving the ciphered document, the recipient decrypts, verifies, and obtains the original document. Although the Yang-Ju-Rao's model is secure and XML is also adopted, there is still a possibility for security

leaks. The reason is identical to the one in the official document exchange model used by the government of Taiwan.

XML Signature

For ensuring the authenticity and the integrity of the data transmitted over the Internet, digital signature techniques are widely adopted. If the signature is validated, the transmitted document is integral and authentic. The digital signature is based on public-key cryptography in conjunction with one-way hash functions. After creating a one-way hash value (called message digest) from the document, the signer encrypts the digest value with her/his private key. In the traditional signature techniques, every participant signer signs the whole document rather than these portions of the document that s/he is responsible for. This brings two major drawbacks.[15] One is that it requires extra communication cost to transfer the whole document and extra computation time to generate personal signatures on the whole document. The other drawback is that it is difficult to achieve the principle of responsibility separation. It is extremely time consuming and tedious to read the whole document before signing it. In practice, every signer should sign these parts of the document that s/he is responsible for. To overcome these drawbacks, Lu and Chen[16] proposed a novel XML multi-signature scheme in 2003 that provides fine-grained control at element level.

The W3C XML Signature Working Group has worked on a standard called XML Signature.[17] The standard provides key developments based on various security strategies to support that the signer can sign only portions of the document.

```
<Signature>
  <SignedInfo>
  (CanonicalizationMethod)
     (SignatureMethod)
     (<Reference (URI=)?>
        (Transforms)?
        (DigestMethod)
        (DigestValue)
     </Reference>)+
  </SignedInfo>
  (SignatureValue)
  (KeyInfo)?
  (Object)*
</Signature>
```

Figure 4: Structure of the XML Signature.

The XML structure for representing digital signatures is shown in Figure 4.[18] Every XML Signature is enclosed within a `Signature` element. In the `Signature` element, there are several main elements including a `SignedInfo` element that contains all the information about the signed data and additional information required for signature validation.

The information how to locate the data object, the algorithm to generate the digest, and the digest value are included in the `Reference` element. For instance, the hashing function can be described in the `DigestMethod` element, whereas the digest is stored into the `DigestValue` element.

The `Reference` element can also encompass a `Transforms` element that contains a list of transformations (i.e. one or more `Transforms` elements) used by the signer to transform a document into a set of sub-documents. For example, the `Transforms` element can contain an XPath expression to identify the selected portions within the document.

Before utilizing digital signature, the `SignedInfo` element is transformed into a standard form called *canonical form*. The role of the canonical form is to eliminate additional symbols, such as white spaces, to avoid errors during the signature validation process. The canonical algorithm is specified in the `CanonicalizationMethod` element. After the canonical form has been generated, it is then encrypted with the key of the signer. The final step is to compute the digital signature of the whole `SignedInfo` element and the resulting value can be written in the `SignatureValue` element. All the information about the algorithm used for generation of the digital signature of `SignedInfo`, such as the encryption algorithm, is saved in the `SignatureMethod` element. The `Signature` element can also provide information on the keys used to validate the signature to the recipient. A `KeyInfo` element contains the keys used to validate the signature.

The XML Signature draft supports three different types of signatures which are shown in Figure 5 [19]:

- *Enveloping Signature*: The `Object` element includes the data object; therefore, it is a part of the `Signature` element.
- *Enveloped Signature*: The data object encloses the *Signature* element. Therefore, the *Signature* element is inserted into the XML document embracing the data object being signed.
- *Detached Signature*: The data object is either an external data object, or a local data object included as a sibling element in the XML document containing the *Signature* element.

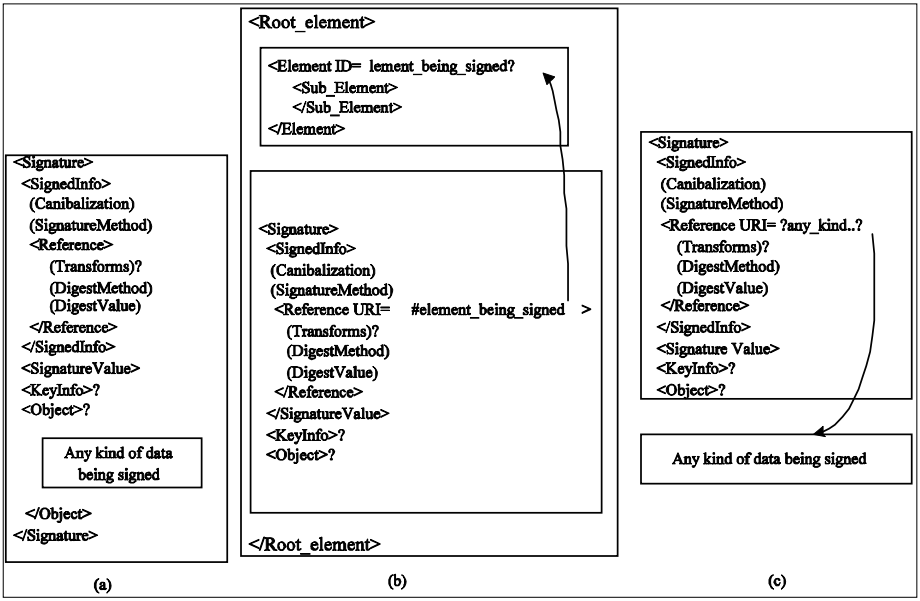


Figure 5: XML Signature Types: (a) Enveloping Signature (b) Enveloped Signature (c) Detached Signature.

An XML Multi-Signature Scheme

In the past, conventional multi-signature schemes allowed the participant signers to only sign on the whole document. This fact made the multi-signature schemes inefficient. To overcome the problem, Wu, Huang, and Guan[20] proposed a delegated multi-signature scheme in which the participant signers sign on the sub-documents that they are responsible for.

In Wu-Huang-Guan's delegated multi-signature scheme, a document is decomposed into a set of subdocuments and the subdocuments are assigned to qualified signers by means of a dispatch algorithm. There are four roles involved in this scheme: a group of signers, a system authority (SA), a document dispatcher (DD), and a signature collector (SC). SA provides services such as initialization of system parameters and generation of the secret and public keys for the individual users and the group. DD is responsible for document decomposition and sub-document delegation. SC collects and verifies the personal signatures generated by the delegated signers; it also constructs a multi-signature for the group. It is assumed that both SC and SD are trusted and only the cheating tricks plotted by DD are considered.

It is believed that XML is the *de facto* standard format for data interchange. To prevent the interchanged XML documents from being illegally modified or forged, digi-

tal signatures have to be incorporated in practical implementations.[21] Although software developers can directly apply Wu-Huang-Guan's multi-signature scheme or another multi-signature scheme to all XML documents, all of the schemes proposed so far do not consider the logical structure of XML and, thus, result in extra computation and communication overhead.

To overcome the described problems, an XML multi-signature scheme has been proposed by Lu and Chen.[22] The scheme is based on Wu-Huang-Guan's delegated multi-signature scheme and utilizes XPath, which is an official recommendation released by W3C, to transform an XML document into a set of sub-documents. In summary, the scheme inherits the advantages of Wu-Huang-Guan's scheme, further improves the efficiency in multi-signature generation by signing the rules rather than the sub-documents, provides fine-grained control at the element level, and is also compatible with the XML Signature standard.

XML Encryption

Various encryption techniques have been designed for encrypting a whole document, but they do not support selective encryption of a document. However, a requirement of many applications is that users have the ability to encrypt only selected portions within a document and encrypting different portions of the same document with different encryption keys. To meet this requirement, XML Encryption has been proposed by the W3C XML Encryption Working Group.[23] At time of writing, the XML Encryption is a working draft. It is mentioned in the draft that the granularity of encryption is limited to the element level as long as XML documents are concerned. Therefore, it is not possible to just encrypt selected attributes of an element.

An XML Encryption structure is composed of two parts and they are `EncryptedInfos` and `Objects`, as is illustrated in Figure 6. The information needed for a correct decryption is stored in the `EncryptedInfos` element, and the encrypted data are contained in the `Object` element.

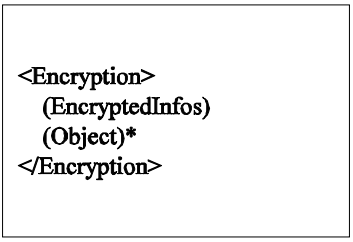


Figure 6: Structure of the XML Encryption.

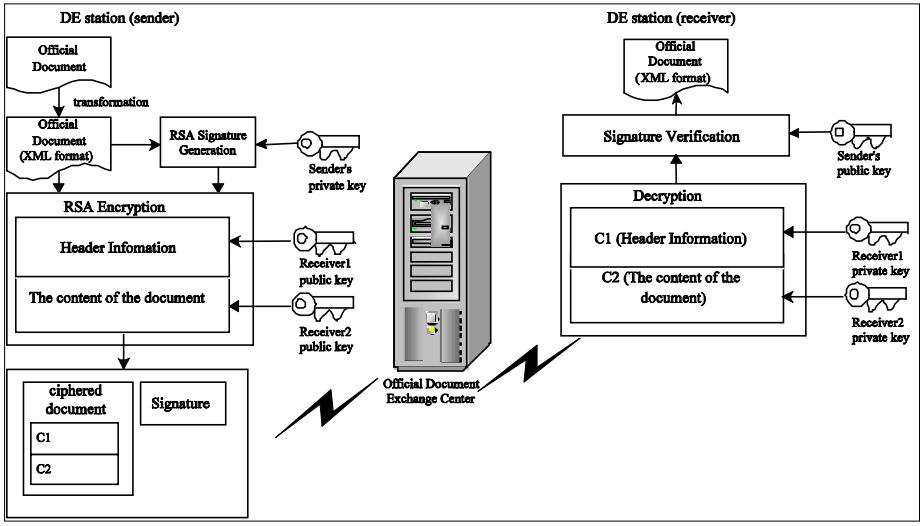


Figure 7: A Secure Fine-Grained Official Document Exchange Model.

Design of a Fine-Grained Official Document Exchange Model

The basic idea of the proposed model is that the originators or senders can sign and encrypt selective portions of a document with different keys based on the security policies. Therefore, only the designated recipients are allowed to read and process the received documents. A few issues have to be emphasized. First, the number of senders and the designated recipients can be one or more than one. Second, the granularity of the protected data object can be as small as a single element. This is due to the fact that any XML element or a set of XML elements can be identified by XPath[24] expressions. And last, the proposed model conforms to the XML Signature and the XML Encryption specification drafts.

The proposed secure fine-grained official document exchange model is shown in Figure 7. The model includes one sender side, one official document exchange center, and more than one receiving sides. First, each recipient has to register at the official document exchange center and the registration information is stored in a database. The registration information includes at least the recipient's name and her/his public-key certificate. Also, the role of the recipient in the government agency has to be registered. As stated earlier, for the reason that GCA has been established in Taiwan, all government agencies have their own public/private key pair. Additionally, with the roles employed in the proposed model, the management of recipients (or government agencies) is much easier.

```
<!ELEMENT Signature(SignedInfo+, SignatureValue, Object)>
<!ELEMENT SignedInfo (Reference , KeyInfo, CipherData)>
<!ELEMENT Reference (Transforms )>
<!ELEMENT Transforms (Transform )>
<!ELEMENT Transform (DataReference )>
<!ELEMENT Object (officialdc )>
<!ELEMENT officialdc (EncryptedData+)>
<!ATTLISTSignature xmlns CDATA #REQUIRED>
<!ATTLISTReference URI CDATA #REQUIRED>
<!ATTLISTTransform Algorithm CDATA #REQUIRED>
<!ATTLISTDataReference URI CDATA #REQUIRED>
<!ATTLISTDataReference xmlns CDATA #REQUIRED>
<!ATTLISTEncryptedData id CDATA #REQUIRED>
<!ATTLISTEncryptedData xmlns CDATA #REQUIRED>
```

Figure 8: The DTD of Signature.

Prior to sending an official document to the recipients, the sender can retrieve the recipients' certificates from the database of the official document exchange center. Once the certificates are obtained, the sender can sign the official document with her/his private key and encrypt the selected parts of the document with the recipients' public keys. The encrypted document and its signature will then be sent to the document exchange center. Upon logging into the official document exchange center, the staff at the receiving desk will receive official documents addressed to her/him. The received encrypted document will first be decrypted and verified. If the document is verified successfully, the staff at the receiving desk can check the header information to see if s/he is permitted to process the document. If the document is classified as "confidential," the document will then be forwarded to the designated recipient.

```
<!ELEMENT officialDocument( EncryptedData+)>
<!ELEMENT EncryptedData(EncryptionMethod, KeyInfo, CipherData)>
<!ELEMENT KeyInfo(KeyName)>
<!ELEMENT CipherData(CipherValue)>
<!ATTLIST EncryptedData id CDATA #REQUIRED>
<!ATTLIST EncryptedData xmlns CDATA #REQUIRED>
<!ATTLIST EncryptedData Type CDATA #REQUIRED>
<!ATTLIST EncryptionMethod Algorithm CDATA #REQUIRED>
<!ATTLIST KeyInfo xmlns CDATA #REQUIRED>
```

Figure 9: The DTD of Encryption.

```
<Signature xmlns= "http://www.w3.org/2000/09/xmldsig#">
  <SignedInfo>
    <Reference URI= "#officialdc"
      <Transforms>
        <Transform Algorithm="http://www.w3.org/2001/04/xmlenc#decryption">
          <DataReference URI="#enc2" xmlns= "http://www.w3.org/2001/04/xmlenc#"/>
        </Transform>
      </Transforms>
    </Reference>
  </SignedInfo>
  <SignatureValue>BC00025343</SignatureValue>
  <Object>
      <officialdc>
          <EncryptedData Id="enc1" xmlns="http://www.w3.org/2001/04/xmlenc#">…</EncryptedData>
          <EncryptedData Id="enc2" xmlns="http://www.w3.org/2001/04/xmlenc#">…</EncryptedData>
      </officialdc>
  </Object>
</Signature>
```

Figure 10: An Example XML Signature.

The signature and the encrypted document are encoded in XML, and their schemas are shown in Figure 8 and Figure 9, respectively. To keep the schemas as simple as possible, DTD has been chosen to describe the schemata. This should help in clarifying the concept. If necessary, the readers can choose the W3C XML Schema[25] to describe the schemata. In this article, the "enveloped signature" type of XML signature is adopted. The reason for this choice is that the schemata of the proposed model remains the same even when the structure of the official documents is revised. In Figure 8, the `officialdc` element is composed of more than one `EncryptedData` element, which are the ciphered sub-documents encrypted by a different security level. The `id` attribute of the `EncryptedData` element is used to establish the relationship between the signature and its associated encrypted document or sub-document. The value of the `id` attribute is unique for one official document. The `EncryptedData` element is composed of at least one `EncryptionMethod`, `KeyInfo`, and `CipherData` elements. The `EncryptionMethod` element has `Algorithm` attribute to specify the encryption algorithm. The `KeyInfo` element stores additional information enabling the recipient to obtain the keys for decryption. After a document or a sub-document is encrypted, the ciphered data is stored in `CipherData` element.

Consider for example that Bob wishes to send a confidential official document to Alice at the government agency "Ministry of Defense." The person at the receiving desk of the Ministry of Defense is Tom. The official document is denoted as D ; it is composed of header information H and the content of the document is denoted as

M. To ensure security, Bob classifies the document as "confidential" and signs the document. The signature of the document is $Sig(D)$. Also, the content of the official document is encrypted by Alice's private key. The encrypted content is denoted as $d_{Alice}(M)$. The sender (who can be either Bob or other staff at Bob's agency who is responsible for sending all outgoing documents) then signs H, $Sig(D)$, and $d_{Alice}(M)$, encrypts H using Tom's public key, and sends them to the official document exchange center. Once the document is received, Tom can only verify the document and decrypt the header information. The content of the document can not be read by Tom or anyone else. Alice is the only one who can verify the integrity and read the content of the document.

An example XML signature is shown in Figure 10. This signature is associated with an example ciphered document that is given in Figure 11 using the method of enveloping signature. As shown in Figure 11, the document was encrypted using two different public keys – *receiver*1 and *receiver*2. The header information was encrypted using *receiver1*'s public key and is shown in lines 2 to 12. And the content of the document was encrypted using *receiver*1's public key and is shown in lines 13 to 23.

When *receiver*1 gets the ciphered document through the official document exchange center, s/he can use her/his private key to decrypt the ciphered document and obtain

```
01 <officialDocument>
02  <EncryptedData id = " enc1"
03                  xmlns = "http://www.w3.org/2001/04/xmlenc#"
04                  Type = "http://www.w3.org/2001/04/xmlenc#Element"
05    <EncryptionMethod Algorithm="  http://www.w3.org/2001/04/xmlenc#tripledes-cbc1" />
06    <ds:KeyInfo xmlns:ds=" http://www.w3.org/2000/09/xmldsig1#"  >
07          <ds:KeyName> receiver1 </ds:KeyName>
08    </ds:KeyInfo>
09    <CipherData>
10          <CipherValue>AB123567</CipherValue>
11    <CipherData>
12  </EncryptedData>
13  <EncryptedData id = "enc2"
14                  xmlns = "http://www.w3.org/2001/04/xmlenc#"
15                  Type = "http://www.w3.org/2001/04/xmlenc#Element"
16    <EncryptionMethod Algorithm="  http://www.w3.org/2001/04/xmlenc#tripledes-cbc2"/>
17    <ds:KeyInfo xmlns:ds="  http://www.w3.org/2000/09/xmldsig2#"  >
18          <ds:KeyName> receiver2 </ds:KeyName>
19    </ds:KeyInfo>
20    <CipherData>
21          <CipherValue>QR156825</CipherValue>
22    <CipherData>
23  </EncryptedData>
24</officialDocument>
```

Figure 11: The Encrypted Official Document.

```
01 <officialDocument>
02  <headerInfo>
03     <issueDate>2004/9/30</issueDate>
04     <securityLevel> Confidential</securityLevel>
05    <receiver>Ministry of Defense</receiver>
06  </headerInfo>
07  <EncryptedData id = "enc2"
08                  xmlns="http://www.w3.org/2001/04/xmlenc#"
09                  Type="http://www.w3.org/2001/04/xmlenc#Element"
10    <EncryptionMethod Algorithm=" http://www.w3.org/2001/04/xmlenc#tripledes-cbc2" />
11    <ds:KeyInfo xmlns:ds=" http://www.w3.org/2000/09/xmldsig2#" >
12           <ds:KeyName>receiver2</ds:KeyName>
13     </ds:KeyInfo>
14     <CipherData>
15           <CipherValue>QR156825</CipherValue>
16      <CipherData>
17  </EncryptedData>
18 </ officialDocument>
```

Figure 12: The Official Document Decrypted by *Receiver*1.

the header information of the document. The official document decrypted by *receiver*1 is shown in Figure 12. As can be seen from the figure, the content of the document in lines 7 to 17 is still invisible to *receiver*1.

Analysis

Since public-key certificates are used to authenticate both senders and recipients, digital signatures are used to ensure the integrity of the official documents, and the documents are encrypted using the RSA cryptosystem, the proposed model is secure. In the rest of this section, the proposed model will be analyzed in terms of fine-grained control and issues related to open standards and system integration.

- *Fine-grained control*: Although, in the past many official document exchange models were developed,[26,27,28,29] the signed and encrypted documents have to be a whole file or a document. According to these models, it is not possible to selectively sign and/or encrypt segments of a document when the security level of each segment of the document is different. Since the proposed model is extended from the standard drafts of XML Signature and XML Encryption, an originator or a sender can sign and encrypt selected portions of the document that he or she is responsible for, and then the designated recipient can decrypt and read the content of the document for which s/he has permission. It should be noted that the granularity is limited to the element level.

- *Conforms to XML Signature and XML Encryption*: The XML Signature and the XML Encryption are specification drafts currently under development jointly by the W3C XML Signature Working Group and the W3C XML Encryption Working Group. Both specification drafts describe a set of XML elements and attributes which are used to store information such as the signature itself, the encrypted data, and the algorithm used to generate signatures and ciphered data.[30,31] Although the standard can be applied to an arbitrary document, it is best suited for XML documents. Due to the fact that the proposed model is designed based on such standards, it conforms to the XML Signature and XML Encryption standards.
- *Compatible with the official document exchange model in Taiwan*: The architecture of the proposed model, as shown in Figure 7, is almost identical to the architecture of the official document exchange model in Taiwan, given in Figure 1. The only difference is the schemata of the exchanged official documents. Although the structure of the official documents in government agencies may be different, the proposed model already illustrated the kernel design of the signature and the ciphered documents. As a result, the design of signature or encrypted document can be slightly modified to meet the requirements of the different agencies.

Conclusions

XML has become a standard format for data interchange on the web, and it is widely adopted by the governments to exchange official documents. Therefore, the development of a secure fine-grained official document exchange model is extremely important. Since the traditional document exchange models lack granular control on official documents, security leaks are possible. This article—taking advantage of the rich structure of XML, XML Signature, and XML Encryption—proposes a secure fine-grained official document exchange model for e-Government. Due to the fact that the RSA cryptosystem is also adopted in the proposed model, it is secure. Also, since the proposed model enhances the current model used in Taiwan and follows the XML Signature and XML Encryption specification drafts, it can be easily incorporated into existing implementations.

Acknowledgement

This research was partially supported by the National Science Council, Taiwan, R.O.C., under contract no. NSC93-2213-E-018-014.

Notes:

[1] Chung-Huang Yang, Shy-Ming Ju, and T.R.N. Rao, "A Smartcard-Based Framework for Secure Document Exchange," in *Proceedings of IEEE 32nd Annual 1998 International Carnahan Conference on Security Technology* (Washington D.C., USA, 12-14 October 1998), 93-96, <citeseer.ist.psu.edu/yang98smartcardbased.html> (23 November 2004).

[2] International Council for Information Technology in Government Administration, "E-Government Development in Taiwan," *ICA Information* 82 (The Executive Yuan, Taiwan, June 2004) <http://www.ica-it.org/docs/issue82/issue_82_2004_06.html> (23 November 2004).

[3] IDA, "Secure Exchange Infrastructure for e-Government Presented in France," *eGovernment News* (6 October 2004), <http://europa.eu.int/ida/en/document/3357/194> (23 November 2004).

[4] Chii-Wen Wu, Hwai-Ling Shan, Wen-Cheng Wang, Dung-Ming Shieh, and Ming-Hsin Chang, "E-Government Electronic Certification Services in Taiwan," (paper presented at the Second International Workshop for Asia Public Key Infrastructure, IWAP 2002) (Taipei, Taiwan, 30 October-01 November 2002), <http://dsns.csie.nctu.edu.tw/iwap/proceedings/proceedings/sessionC/25.pdf> (23 November 2004).

[5] *The Official Document Exchange System for e-Government in Taiwan*, <http://community.nat.gov.tw/> (23 November 2004).

[6] International Council for Information Technology in Government Administration, "E-Government Development in Taiwan."

[7] The Treasury Department of Taiwan, *Official Document Exchange Center for e-Government*, <http://210.241.98.149/ntact/index-1.htm> (23 November 2004).

[8] Charles F. Goldfarb and Paul Prescod, *The XML Handbook* (Englewood Cliffs: Prentice-Hall, 1998).

[9] Tim Bray, Jean Paoli, C. M. Sperberg-McQueen, Eve Maler, and François Yergeau, eds., *Extensible Markup Language (XML) Version 1.0* (W3C, February 1998), <http://www.w3.org/TR/REC-xml/> (22 November 2004).

[10] Ronald L. Rivest, Adi Shamir, and Leonard Adleman, "A Method of Obtaining Digital Signatures and Public-Key Cryptosystems," *Communications of the ACM* 21, no. 2 (February 1978): 120-126, <http://theory.lcs.mit.edu/~rivest/publications.html> (22 November 2004).

[11] Elisa Bertino, Barbara Carminati, and Elena Ferrari, "XML Security," *Information Security Technical Report* 6, no. 2 (2001): 44-58.

[12] *XML Signature* (W3C XML Signature Working Group, 2001), <http://www.w3.org/Signature> (22 November 2004).

[13] *XML Encryption* (W3C XML Encryption Working Group, 2001), <http://www.w3.org/Encryption/2001> (22 November 2004).

[14] Yang, Ju, and Rao, "A Smartcard-Based Framework for Secure Document Exchange."

[15] Eric Jui-Lin Lu and Rai-Fu Chen, "An XML Multisignature Scheme," *Applied Mathematics and Computation* 149, no. 1 (February 2004): 1-14.

[16] Lu and Chen, "An XML Multisignature Scheme."

[17] *XML Signature* (W3C XML Signature Working Group, 2001).

[18] Donald Eastlake, Joseph Reagle, and David Solo, eds., *XML-Signature Syntax and Processing* (W3C Working Draft, 2000), <http://www.w3.org/TR/2001/CR-xmldsig-core-20010419/> (22 November 2004).

[19] Bertino, Carminati, and Ferrari, "XML Security."

[20] Tzong-Chen Wu, Chih-Chan Huang, and D.-J. Guan, "Delegated Multisignature Scheme with Document Decomposition," *Journal of Systems and Software* 55, no. 3 (January 2001): 321-328.

[21] Bertino, Carminati, and Ferrari, "XML Security."

[22] Lu and Chen, "An XML Multisignature Scheme."

[23] *XML Encryption* (W3C XML Encryption Working Group, 2001).

[24] *XML Path Language (XPath) Version 1.0* (W3C, November 1999), <http://www.w3.org/TR/xpath> (22 November 2004).

[25] *XML Schema* (W3C, May 2001), < http://www.w3.org/XML/Schema.html> (22 November 2004).

[26] Chung-Huang Yang, So-Lin Yen, Hwang David Liu, Kuei Liu, Bor-Shenn Jeng, Kung-Yao Chang, Min-Shin Chang, Yu-Ling Cheng, Jo-Ling Liang, and Don-Min Shien "Secure Official Document Mail Systems for Office Automation," in *Proceedings of IEEE 31st Annual 1997 International Carnahan Conference on Security Technology* (Canberra, Australia, October 1997), 161-164.

[27] Shy-Ming Ju, "An SGML-Based Office Document Exchange and Management," in *Proceedings of SGML/XML Europe'98* (Paris, France, May 1998), 269-282.

[28] Yang, Ju, and Rao, "A Smartcard-Based Framework for Secure Document Exchange."

[29] *The Official Document Exchange System for e-Government in Taiwan*.

[30] Mark O'Neill, "XML and Security," *The XML Journal* 2, no. 12 (December 2001): 10-15.

[31] Bertino, Carminati, and Ferrari, "XML Security."

YI-HUI CHEN is currently a Ph.D. student at the Department of Computer Science and Information Engineering of the National Chung Chen University. She received her B.M. and M.S.I.M. degrees in Information Management from Chaoyang University of Technology, Taichung, Taiwan, in 1997 and 2004, respectively. Her research interests include XML, Access Control, Delegation, and Distributed System. *Address for correspondence:* Department of Computer Science and Information Engineering, National Chung Cheng University, 160 San-Hsing, Min-Hsiung, Chia-Yi, Taiwan, R.O.C.

ERIC JUI-LIN LU received his B.S. degree in Transportation Engineering and Management from the National Chiao Tung University, Taiwan, R.O.C., in 1982; a M.S. degree in Computer Information Systems from San Francisco State University, CA, USA, in 1990; and a Ph.D. degree in Computer Science from University of Missouri-Rolla, MO, USA, in 1996. In the period 1997-2004, he was a professor at the Department of Information Management and had served as Director of the Computer Center and Head of Graduate Institute of Networking and Communication Engineering at Chaoyang University of Technology, Taiwan, R.O.C. He is currently a professor at the department of Computer Science and Information Engineering at the National Changhua University of Education, Taiwan, R.O.C. His current research interests include electronic commerce, distributed processing, and security. *Address for correspondence:* Department of Computer Science and Information Engineering, National Changhua University of Education, No.1 Gin-Der Road, Changhua, Taiwan, R.O.C. *E-mail:* jlu@cc.ncue.edu.tw. *URL:* http://dns.csie.ncue.edu.tw/~jlu/.

AN EFFICIENT AND PRACTICAL REMOTE USER AUTHENTICATION SCHEME

Ya-Fen CHANG and Chin-Chen CHANG

Abstract: In 2000, Peyravian and Zunic proposed a simple and efficient password authentication scheme based on the collision-resistant hash function. Later, Hwang and Yeh indicated that Peyravian and Zunic's scheme is insecure and proposed an improvement by using the server's public key. Nevertheless, in practice, services that do not use public keys are quite often superior to PKIs. At the same time, Lee, Li and Hwang indicated that Peyravian and Zunic's scheme suffers from off-line password guessing attacks and presented an improved version. However, Lee-Li-Hwang's proposed scheme is still vulnerable to the same attacks and denial-of-service attacks. Therefore, this article presents a secure and efficient improvement.

Keywords: Password Authentication, Password Guessing Attacks.

Introduction

Several authentication methods have been proposed for electronic commerce environments (e.g., the authentication service Kerberos[1]). Among them, the password authentication scheme is the most common approach. In the password authentication scheme, a client is allowed to share an easy-to-remember password with a trusted server. Such concepts are applied in other applications as well.[2,3,4] Due to the characteristic of easy-to-remember password, these schemes may be broken with a little effort. Ding and Horster[5] divide the password-guessing attacks into three classes: (1) detectable on-line password guessing attacks, (2) undetectable on-line password guessing attacks, and (3) off-line password guessing attacks. In 2000, Peyravian and Zunic[6] proposed a novel password authentication scheme. The proposed scheme employs a collision-resistant hash function to protect the transmission of the password over an insecure network. No symmetric-key or public-key based authentication system is required in their method. Instead, only the hash value of the password is transmitted. In addition, random numbers are used to avoid eavesdropping and replay.

In 2002, Hwang and Yeh[7] pointed out that the security of Peyravian and Zunic's pass-

word authentication scheme is only based on the user password. Because of the features of the easy-to-remember passwords and the fact that no additional authentication approach is used, they pointed out that Peyravian and Zunic's password authentication schemes cannot resist password guessing attacks, server spoofing, and server data eavesdropping. As a result, they proposed an improvement to defend against the above-mentioned three types of attacks by using the server's public key. Notwithstanding, applying the server's public key puts a high burden on users since the server's public key needs to be verified before being used. In fact, in practice services that do not use public keys are quite often superior to PKIs.

At the same time, Lee, Li, and Hwang[8] also found the security flaws in the scheme proposed by Peyravian and Zunic. They presented another improvement and claimed that their scheme has the same features, such that still only the collision-resistant hash function is used to protect the transmission of the password. However, the Lee-Li-Hwang's scheme is still vulnerable to off-line password guessing attacks. Moreover, the authorized user will suffer from the denial-of-service attacks while changing his/her password. Consequently, the authors of this article propose a secure and efficient improved scheme where the computational load is low and the server's public key is not used.

This article is organized as follows. The next section reviews the scheme proposed by Hwang and Yeh. Then, the authors provide a review and cryptanalysis of the Lee-Li-Hwang's scheme. A novel improved scheme is presented afterwards, followed by a comprehensive discussion. Conclusions are drawn in the last section.

Review of Hwang and Yeh's Scheme

This section presents Hwang and Yeh's proposed improvement on Peyravian-Zunic's password authentication scheme. The initiation goes as follows. The client U_i with identity d_i and the trusted server S share a secret password p_i. S has a server public key KS. $H(p_i)$ is stored in the database by S for U_i, where $H()$ is a collision-resistant hash function. $EK()$ denotes an asymmetric encryption scheme with a public key K.

Hwang and Yeh's password authentication scheme consists of two phases: a password authentication phase and a password change phase. The password authentication phase is shown in Figure 1. The details are as follows:

Step1. U_i computes and sends $E_{K_S}(r_C, p_i)$ to S, where r_C is a random number, with d_i to S as a login request.

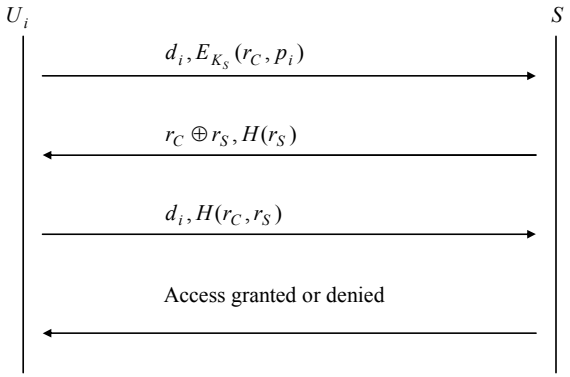


Figure 1: The Password Authentication Phase of Huang and Yeh's Scheme.

Step 2. After receiving the login request sent from U_i, S uses his/her own private key to retrieve r_C and p_i. Then S computes $H(p_i)$ for comparison with the corresponding item stored in the database. In case of equal values, S computes and sends $r_C \oplus r_S$ and $H(r_S)$ to U_i, where r_S is a random number chosen by S and $\oplus$ denotes XOR; otherwise, S terminates the protocol.

Step 3. Upon receiving the transmitted data, U_i computes $H(r_C \oplus (r_C \oplus r_S))$ and checks whether the result of this computation and $H(r_S)$ are equal. If it holds, U_i computes and sends $H(r_C, r_S)$ with d_i to S; otherwise, U_i may restart the scheme or ask S to retransmit the necessary information.

Step 4. After getting $(d_i, H(r_C, r_S))$, S computes and compares $H(r_C, r_S)$ with the received message. If they are equal, S grants U_i access request. Otherwise, S rejects the access request from U_i.

In the password change phase, the steps are almost the same as those of the password authentication scheme, except for an additional password change request in Step 3. In Step 3, U_i sends $d_i, H(r_C, r_S), H(p_i') \oplus H(r_C + 1, r_S)$ and the password change request to S, where p_i' is the new password chosen by U_i. Then, S computes $H(r_C + 1, r_S)$ and $H(r_C + 1, r_S) \oplus (H(p_i') \oplus H(r_C + 1, r_S))$ to get U_i's new verifier $H(p_i')$.

Review and Cryptanalysis of Lee-Li-Hwang's Scheme

First, the authors review the scheme proposed by Lee, Li and Hwang, followed by its cryptanalysis.

Review of Lee-Li-Hwang's Scheme

As stated in the previous section, U_i with identity d_i and the trusted server S share a secret password p_i. S stores $HPW_i = H(d_i, p_i)$ for U_i, where $H()$ is a collision-resistant hash function. The password authentication phase is shown in Figure 2. The details follow:

Step 1. U_i chooses a random number r_C. Then s/he computes and sends $r_C \oplus HPW_i$ with d_i to S as a login request, where $\oplus$ denotes XOR.

Step 2. After receiving the login request, S computes $HPW_i \oplus (r_C \oplus HPW_i)$. Then S computes and sends $r_S \oplus HPW_i$ to U_i, where r_S is a random number.

Step 3. Upon receiving the transmitted data, U_i computes $r_S = HPW_i \oplus (r_S \oplus HPW_i)$ and $AUTH = H(HPW_i, r_C, r_S)$. Then U_i sends d_i and $AUTH$ to S.

Step 4. After getting d_i and $AUTH$ from U_i, S computes and compares $H(HPW_i, r_C, r_S)$ with $AUTH$. If they are equal, S grants U_i the access request. Otherwise, S rejects the access request from U_i.

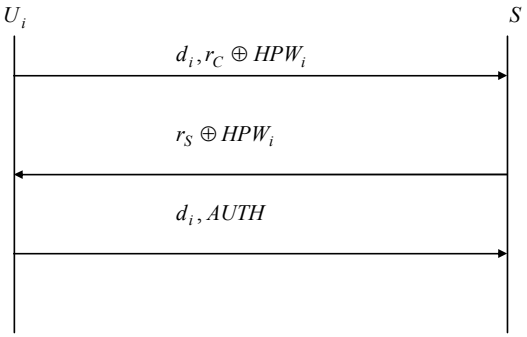


Figure 2: The Password Authentication Phase of Lee-Li-Hwang's Scheme.

The password changing phase of Lee-Li-Hwang's scheme follows the procedure illustrated in Figure 3. The steps are very similar to those of the password authentication phase, except for an additional password change request in Step 3. In Step 3, U_i computes $HPW_i' = H(d_i, p_i')$ and $Mask = HPW_i' \oplus H(HPW_i, r_C + 1, r_S)$, where p_i' is the new password chosen by U_i. Then U_i sends d_i, $AUTH$, and $Mask$ and the password change request to S. After getting the password change request, S first

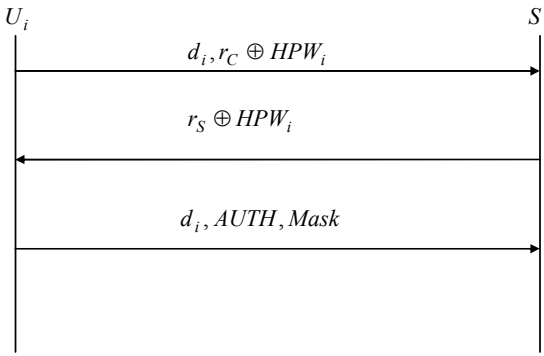


Figure 3: The Password Change Phase of Lee-Li-Hwang's Scheme.

authenticates U_i by comparing $H(HPW_i, r_C, r_S)$ with $AUTH$. If it does not hold, S denies the password change request; otherwise, S computes $HPW_i' = H(HPW_i, r_C + 1, r_S) \oplus Mask$ and updates U_i's verifier with HPW_i'.

Cryptanalysis of Lee-Li-Hwang's Scheme

Lee, Li and Hwang claimed that the scheme they propose can resist off-line password guessing attacks since r_C and r_S are random and the transmitted verifier is concealed. However, the authors will show that Lee-Li-Hwang's password authentication scheme still suffers from off-line password guessing. Even more, the proposed scheme cannot resist denial-of-service attacks when the authorized user changes his/her password. How to mount denial-of-service attacks on Lee-Li-Hwang's proposed scheme is shown afterwards.

Security Flaw 1: Lee-Li-Hwang's scheme suffers from off-line password guessing attacks

Consider the scenario when a malicious user Eve eavesdrops the data transmitted between U_i and S. As a result, Eve knows $r_C \oplus HPW_i$, $r_S \oplus HPW_i$, and $AUTH = H(HPW_i, r_C, r_S)$. Then, Eve performs the following operations:

Step 1. Eve guesses U_i's password to be pw and computes $HPW = H(d_i, pw)$.

Step 2. Eve computes $r_C'' = (r_C \oplus HPW_i) \oplus HPW$, $r_S'' = (r_S \oplus HPW_i) \oplus HPW$, and $AUTH'' = H(HPW_i, r_C'', r_S'')$.

Step 3. Eve checks whether $AUTH = AUTH''$ holds or not. If it holds, Eve is sure that pw is p_i. Otherwise, Eve repeats Steps 1 to 3.

According to the procedure described above, it is obvious that Eve can successfully get U_i's password p_i by performing off-line password guessing attacks.

Security Flaw 2: Lee-Li-Hwang's scheme suffers from denial-of-service attacks when the authorized user wants to change the password

When U_i wants to change her/his password, s/he follows the procedure as shown in Figure 3. Eve intercepts the transmitted data (d_i, $AUTH$, $Mask$) in Step 3 and replaces $Mask$ with a random number R, where $|R| = |Mask|$. Then Eve sends d_i, $AUTH$, and R and the password change request to S. After getting the request, S first authenticates U_i by comparing $H(HPW_i, r_C, r_S)$ with $AUTH$. It is obvious that U_i will be authenticated successfully since U_i indeed knows p_i. Then S computes $HPW_i'' = H(HPW_i, r_C + 1, r_S) \oplus R \neq HPW_i'$ and updates U_i's verifier with HPW_i''. Later, when U_i wants to access S, U_i will not be authenticated successfully.

An Efficient and Practical Remote User Authentication Scheme

In this section, the authors propose their novel remote user authentication scheme. To start with, the server S and the user U_i share a password p_i. There is one public system parameter $n = p \times q$, where p and q are two secret system parameters known only to S. S stores $(x \oplus p_i)$ in the database, where x is a system parameter kept concealed by S. The proposed scheme consists of two phases: a password authentication phase and a password change phase, which are described below.

Remote Password Authentication Phase

The password authentication phase is shown in Figure 4, and its description is given below:

Step 1. U_i sends access request containing her/his identity d_i and the timestamp.

Step 2. S uses x to retrieve p_i by computing $x \oplus (x \oplus p_i)$ and calculates $E1_{p_i}(r_S)$, where $E1()$ is a symmetric encryption algorithm and r_S is a random number. Then S sends $E1_{p_i}(r_S)$ to U_i.

Step 3. After getting the transmitted data, U_i computes $r_S = D1_{p_i}(E1_{p_i}(r_S))$, where $D1()$ is a symmetric decryption algorithm. Then U_i chooses $s_i \in_R Z_n$ and calculates $\alpha = H(r_S, s_i)$ and $z = s_i^2 \bmod n$. After that, U_i sends α and z to S.

Step 4. After getting α and z, S computes

$a_1 = z^{(p+1)/4} \bmod p$,

$a_2 = (p - z^{(p+1)/4}) \bmod p$,

$a_3 = z^{(q+1)/4} \bmod q$,

$a_4 = (q - z^{(q+1)/4}) \bmod q$,

$x = q(q^{-1} \bmod p)$, $y = p(p^{-1} \bmod q)$,

$\beta_1 = (x * a_1 + y * a_3) \bmod n$,

$\beta_2 = (x * a_1 + y * a_4) \bmod n$,

$\beta_3 = (x * a_2 + y * a_3) \bmod n$, and

$\beta_4 = (x * a_2 + y * a_4) \bmod n$.

For j = 1, 2, 3, and 4 let $s_i' = \beta_j$. S computes $\alpha' = H(r_S, s_i')$. Then S checks whether any α' and α are equivalent. If it does not hold, S terminates the protocol; otherwise, S accepts the access request and sends $H(d_i, s_i')$ to U_i.

Step 5. After getting $H(d_i, s_i')$ from S, U_i checks whether $H(d_i, s_i')$ and $H(d_i, s_i)$ are equivalent. If it holds, U_i is convinced that the communication party is indeed S.

Remote Password Change Phase

When U_i wants to update p_i with the new password p_i', the remote password change phase will look like as shown in Figure 5. The algorithm of the remote password change phase is as follows:

Step 1. U_i sends a password-change request containing her/his identity d_i and the timestamp.

Step 2. S computes $x \oplus (x \oplus p_i)$ to retrieve p_i and calculates $E1_{p_i}(r_S)$. Then S sends $E1_{p_i}(r_S)$ to U_i.

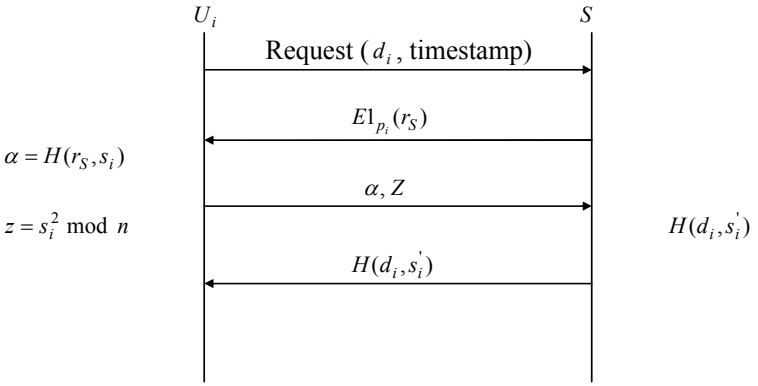


Figure 4: Proposed Remote Password Authentication Phase.

Step 3. After getting the transmitted data, U_i computes

$$r_S = D1_{p_i}(E1_{p_i}(r_S)).$$

Then U_i chooses the new password p_i' and calculates

$$\alpha = H(r_S, s_i),$$

$$Check = E1_{s_i}(p_i', r_S), \text{ and}$$

$$z = s_i^2 \bmod n.$$

Afterwards, U_i sends α, $Check$ and z to S.

Step 4. After getting α, $Check$ and z, S computes

$$a_1 = z^{(p+1)/4} \bmod p,$$

$$a_2 = (p - z^{(p+1)/4}) \bmod p,$$

$$a_3 = z^{(q+1)/4} \bmod q,$$

$$a_4 = (q - z^{(q+1)/4}) \bmod q,$$

$$x = q(q^{-1} \bmod p),\ y = p(p^{-1} \bmod q),$$

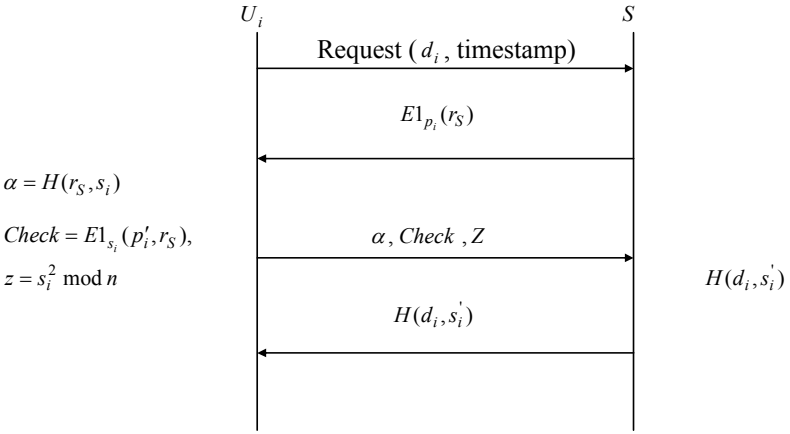


Figure 5: The Proposed Remote Password Change Phase.

$\beta_1 = (x * a_1 + y * a_3) \bmod n$,

$\beta_2 = (x * a_1 + y * a_4) \bmod n$,

$\beta_3 = (x * a_2 + y * a_3) \bmod n$, and

$\beta_4 = (x * a_2 + y * a_4) \bmod n$.

For j =1, 2, 3, and 4 let $s_i' = \beta_j$. S computes $\alpha' = H(r_S, s_i')$. Then S checks whether any α' and α are equivalent. If it does not hold, S terminates the protocol; otherwise, S computes $D1_{s_i}(Check)$ and checks whether the computation result contains r_S' . If it holds, S is convinced that p_i' is the new password and updates $(x \oplus p_i)$ with $(x \oplus p_i')$. From now on, S and U_i share the password p_i' . Then S computes and sends $H(d_i, s_i')$ to U_i .

Step 5. After getting $H(d_i, s_i')$ from S , U_i checks whether $H(d_i, s_i')$ and $H(d_i, s_i)$ are equal. If it holds, U_i is convinced that the communication party is indeed S .

Discussion

In this section, it will be shown that the proposed scheme is secure and efficient. First, security analysis is provided. Then, it will be demonstrated that the proposed

scheme is efficient by presenting performance analyses.

Security Analysis

Here, it will be demonstrated that the proposed scheme is secure. Moreover, the security drawbacks found in Lee-Li-Hwang's scheme are overcome.

Property 1: The proposed scheme can defend against the password guessing attacks

In Step 4 of the password authentication phase and the remote password change phase, S computes $a_1 = z^{(p+1)/4} \bmod p$, $a_2 = (p - z^{(p+1)/4}) \bmod p$, $a_3 = z^{(q+1)/4} \bmod q$, $a_4 = (q - z^{(q+1)/4}) \bmod q$, $x = q(q^{-1} \bmod p)$, $y = p(p^{-1} \bmod q)$, $\beta_1 = (x * a_1 + y * a_3) \bmod n$, $\beta_2 = (x * a_1 + y * a_4) \bmod n$, $\beta_3 = (x * a_2 + y * a_3) \bmod n$, and $\beta_4 = (x * a_2 + y * a_4) \bmod n$. For j = 1, 2, 3, and 4 let $s_i' = \beta_j$. S computes $\alpha' = H(r_S, s_i')$. Then S checks whether any α' and α are equivalent. If it does not hold, S will notice that there is the possibility that someone mounts attacks on the protocol. That is, it is impossible for undetectable on-line password guessing attacks to appear in the proposed protocol, and the proposed protocol is secure enough to defeat detectable on-line password guessing attacks.

With deep insight into the off-line password guessing attacks, meaningful information encrypted by the password will result in damage. The reason is that the attacker can guess the password and can decrypt the encrypted information by the guessed password. If the decryption result contains the meaningful information, it denotes that the attacker has already gotten the right password. In the proposed protocol, U_i's password is only involved in computing $E1_{p_i}(r_S)$, where r_S is a random number. No meaningful information, such as the identity or the timestamp, is contained in $E1_{p_i}(r_S)$. Hence, an attacker cannot determine whether the guessed password is correct according to $E1_{p_i}(r_S)$. In Step 3, U_i will send $\alpha = H(r_S, s_i)$ and $z = s_i^2 \bmod n$ to S. An attacker still cannot determine whether the guessed password is correct because of the following reasons: (1) $s_i \in_R Z_n$, (2) it is impossible to factor n to retrieve s_i, (3) it is impossible to know (r_S, s_i) from α for comparison since $H()$ is a one-way function. Due to the above reasons, we can sum up that the proposed scheme is secure to resist the password guessing attacks.

Property 2: The proposed scheme ensures mutual authentication

In Step 4 of both the password authentication phase and the remote password change phase, S authenticates U_i. In Step 5, U_i authenticates S by checking whether

$H(d_i, s_i')$ and $H(d_i, s_i)$ are equal. Consequently, mutual authentication is preserved in the proposed scheme. That is, server spoofing attacks cannot work in the proposed scheme.

Property 3: The proposed scheme can resist the denial-of-service attacks

In Step 3 of the remote password change phase, U_i chooses the new password p_i' and calculates $\alpha = H(r_S, s_i)$, $Check = E1_{s_i}(p_i', r_S)$, and $z = s_i^2 \bmod n$. Then, U_i sends α, $Check$ and z to S. In Step 4, S computes $a_1 = z^{(p+1)/4} \bmod p$, $a_2 = (p - z^{(p+1)/4}) \bmod p$, $a_3 = z^{(q+1)/4} \bmod q$, $a_4 = (q - z^{(q+1)/4}) \bmod q$, $x = q(q^{-1} \bmod p)$, $y = p(p^{-1} \bmod q)$, $\beta_1 = (x * a_1 + y * a_3) \bmod n$, $\beta_2 = (x * a_1 + y * a_4) \bmod n$, $\beta_3 = (x * a_2 + y * a_3) \bmod n$, and $\beta_4 = (x * a_2 + y * a_4) \bmod n$. For j =1, 2, 3, and 4 let $s_i' = \beta_j$. S computes $\alpha' = H(r_S, s_i')$. Then S checks whether any α' and α are equivalent. If it holds, S uses s_i' as the secret key to compute and checks whether the computation result contains r_S'. If it holds, S is convinced that p_i' is the new password and updates $(x \oplus p_i)$ with $(x \oplus p_i')$. The proposed approach first ensures that U_i is the authorized user and, second, makes sure that the new password is indeed the one chosen by U_i. Even though an attacker retransmits $Check$ from other iteration, S will not be cheated since s_i is a one-time used random number. Moreover, mutual authentication is confirmed in the proposed scheme. Furthermore, U_i can check whether the password is updated in Step 5 by authenticating S. As a result, the proposed scheme can withstand the denial-of-service attacks.

Performance Analysis

The well-known provable nonmalleable encryption scheme needs 5/3 exponentiations per en/decryption.[9] Since additional hash function operations are needed to transmit the new password in the password change phase, the number of hash operations needed in Hwang and Yeh's scheme and in the proposed scheme are shown as *a/b* in Table 1, where *a* denotes the number of operations needed in the password transmission phase, and *b* denotes the number of operations needed in the password change phase. Moreover, because additional symmetric encryption/decryption operations are also needed in the password change phase of the proposed scheme, the necessary number is represented as above.

The speed of en/decryption with symmetric encryption schemes is faster than that with asymmetric ones. For example, DES is faster than RSA by 1000 times in hardware and 100 times in software.[10] Further, the speed of hash operations is about 1000

Table 1: Number of Operations for Different Types of Computation in Hwang and Yeh's Password Authentication Scheme and the Proposed Authentication Scheme.

Party / Computation type	Hwang-Yeh		The proposed	
	U_i	S	U_i	S
Modular exponential	0(5)	0(3)	0	2
Public key en/decryption	1/0	0/1	0/0	0/0
Symmetric en/decryption	0	0	1/2	1/2
Random number	1	1	1	1
Hash operation	2/4	2/3	2/2	6/7

times faster than RSA operations.[11] Even though the needed number of hash operations in the proposed scheme is more than that needed in Hwang and Yeh's scheme, it is obvious that the scheme presented here is more efficient for the above described reasons. In addition, according to the comparison between Hwang and Yeh's scheme and the new one, it is obvious that the computation load of the user is quite low. That is, the proposed scheme is also suitable in imbalanced networks.

Conclusions

Peyravian and Zunic proposed a simple and efficient password authentication scheme in the year 2000. However, Peyravian and Zunic's scheme is insecure. Hwang and Yeh proposed an improved scheme that uses the server's public key. At the same time, Lee, Li and Hwang presented another improved version of Peyravian and Zunic's scheme. However, there are still security flaws in the scheme proposed by Lee, Li and Hwang. Therefore, this article presents an improvement without employing the server's public key. According to the analyses described above, it is unquestionable that the proposed scheme is secure, practical, and efficient. In addition, the proposed scheme is also suitable in imbalanced networks.

Notes:

[1] B. Clifford Neuman and Theodore Ts'o, "Kerberos: An Authentication Service for Computer Networks," *IEEE Communications Magazine* 32, no. 9 (September 1994): 33-38.

[2] Steven M. Bellovin and Michael Merrit, "Encrypted Key Exchange: Password-Based Protocols Secure against Dictionary Attacks" (paper presented at the 1992 IEEE Computer Society Symposium on Research in Security and Privacy, Oakland, California, May 1992), (IEEE Computer Society Press), 72-84.

[3] Chun-Li Lin, Hung-Min Sun, and Tzonelih Hwang, "Three-Party Encrypted Key Exchange: Attacks and a Solution," *ACM Operating Systems Review* 34, no. 4 (2000): 12-20.

[4] Chun-Li Lin, Hung-Min Sun, Michael Steiner, and Tzonelih Hwang, "Three-Party Encrypted Key Exchange without Server Public-Keys," *IEEE Communications Letters* 5, no. 12 (December 2001): 497-499.

[5] Yun Ding and Patrick Horster, "Undetectable On-Line Password Guessing Attacks," *ACM Operating Systems Review* 29, no. 4 (October 1995): 77-86.

[6] Mohammad Peyravian and Nevenko Zunic, "Methods for Protecting Password Transmission," *Computers and Security* 19, no. 5 (2000): 466-469.

[7] Jing-Jang Hwang and Tzu-Chang Yeh, "Improvement on Peyravian-Zunic's Password Authentication Schemes," *IEICE Transactions on Communications* E85-B, no. 4 (April 2002): 823-825.

[8] Cheng-Chi Lee, Li-Hua Li, and Min-Shiang Hwang, "A Remote User Authentication Scheme Using Hash Functions," *ACM SIGOPS Operating Systems Review* 36, no. 4 (October 2002): 23-29.

[9] Ronald Cramer and Victor Shoup, "A Practical Public Key Cryptosystem Provably Secure against Adaptive Chosen Cipher Attack," in *Proceedings of the 18th Annual International Cryptology Conference on Advances in Cryptology Crypto'98* (Santa Barbara, California, USA, August 1998), published also in *Lecture Notes in Computer Science* 1462 (London, UK: Springer-Verlag, 1998), 13-25.

[10] Bruce Schneier, *Applied Cryptography: Protocols, Algorithms, and Source Code in C*, Second Edition, (New York: John Wiley & Sons, 1995).

[11] Schneier, *Applied Cryptography: Protocols, Algorithms, and Source Code in C*.

YA-FEN CHANG received a B.S. degree in Computer Science and Information Engineering from National Chiao Tung University, Hsinchu, Taiwan, in 2000. She is currently pursuing her Ph.D. degree in Computer Science and Information Engineering from the National Chung Cheng University, Chiayi, Taiwan. Her current research interests include electronic commerce, information security, cryptography, and mobile communications. *Address for correspondence:* Department of Computer Science and Information Engineering, National Chung Cheng University, Chiayi 621, Taiwan, R.O.C.; *E-mail:* cyf@cs.ccu.edu.tw.

CHIN-CHEN CHANG received a B.S. degree in Applied Mathematics in 1977 and a M.S. degree in Computer and Decision Sciences in 1979, both from National Tsing Hua University, Hsinchu, Taiwan. He received his Ph.D. in Computer Engineering in 1982 from National Chiao Tung University, Hsinchu, Taiwan. During the academic years of 1980-1983, he was with the Department of Computer Engineering at National Chiao Tung University. From 1983 to 1989, he worked at the Institute of Applied Mathematics, National Chung Hsing University, Taichung, Taiwan. Since August 1989, he has worked as a professor at the Institute of Computer Science and Information Engineering at National Chung Cheng University, Chiayi, Taiwan. Since 2002, he has been a Chair Professor of National Chung Cheng University. His current research interests include database design, computer cryptography, image compression and data structures. Dr. Chang is a fellow of the IEEE, a fellow of the IEE, a research fellow of National Science Council of R.O.C., and a member of the Chinese Language Computer Society, the Chinese Institute of Engineers of the Republic of China, the International Association for Crypto-logic Research, the Computer Society of the Republic of China, and the Phi Tau Phi Honorary Society of the Republic of China. Dr. Chang was the chair and is a honorary chair of the executive committee of the Cryptography and Information Security Association of the Republic of China. *Address for correspondence:* Department of Computer Science and Information Engineering, National Chung Cheng University, 160, San-Hsing, Min-Hsiung, Chiayi 621, Taiwan. *Phone*: 886-5-2720411 ext. 33100; *Fax*: 886-5-2720859; *E-mail*: ccc@cs.ccu.edu.tw.

A NOVEL LOWER COST CRYPTO-SCHEME BASED ON THE THEORY OF SHARING SECRETS

Chao-Wen CHAN and Chin-Chen CHANG

Abstract: This article presents an information permutation and breaking scheme to construct a low-cost encryption scheme. The proposed encryption scheme preserves the security requirements of a general encryption scheme. The presented research uses information entropy to depict the one-way property and tries to use entropy to study the one-way property. The authors also present an estimation of the reasonable size of the seed set of a pseudo-random number generator.

Keywords: Entropy, One-Way Hash Function, One-Way Property, Pseudo-Random Number Generator.

Mobile computing continues to grow in importance. Machines that are designated to perform mobile computing are notebook PCs, PDAs, and mobile phones. In general, these machines have lower power than desktop PCs, and one of the main applications of these machines is communication. The owners of these machines communicate with each other or to some host machines. The business users of these lower power machines may need to exchange secret messages with other machines. The main technique to protect these secret messages is computer cryptography. The most popular cryptosystems are public-key cryptosystems.[1,2] However, encryption and decryption operations in these cryptosystems are expensive. It may take a long time to perform these operations. In addition, the length of the message that can be encrypted or decrypted is completely determined by the cryptosystem itself. However, the length of a general message is, in general, longer than the above mentioned length. The brute force method partitions the long message into blocks, so that each resulting block can be encrypted or decrypted using only one public-key operation. Thus, a message is partitioned into t blocks, then, we encrypt or decrypt it requiring t public-key operations. This will take a long time for a mobile machine.

A scheme to reduce the cost of the public-key encryption or decryption of a long message uses a session key of a symmetric-key cryptosystem to encrypt it. Then, we

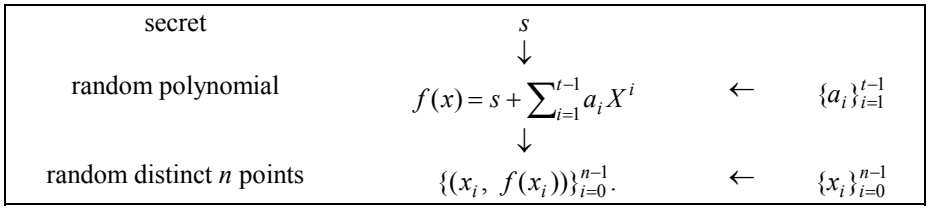
use a public-key cryptosystem to encrypt the session key. Finally, we send the encrypted session key and the message encrypted by the session key to the receiver. After receiving the encrypted message, the receiver uses a public-key operation to decrypt the encrypted session key, then, uses the session key to decrypt the encrypted message. In the scheme, the symmetric-key cryptosystem[3] reduces the public-key operation of a long message to a symmetric session key which can be properly operated by a public-key operation. However, the symmetric-key encrypted message contains all the information found in the original message. So, the public-key cryptosystem and the symmetric-key cryptosystem must prevent all attacks to ensure the security of the scheme.

The proposed scheme uses a permutation-like breaking information scheme to partition a long message into t blocks. By the interpolating theory and Shamir's (t,n)-threshold scheme,[4] we try to reduce the encryption of a long message into the encryption of some small blocks. Moreover, we will reduce the security problem of the encryption of a long message to that of a single public-key operation.

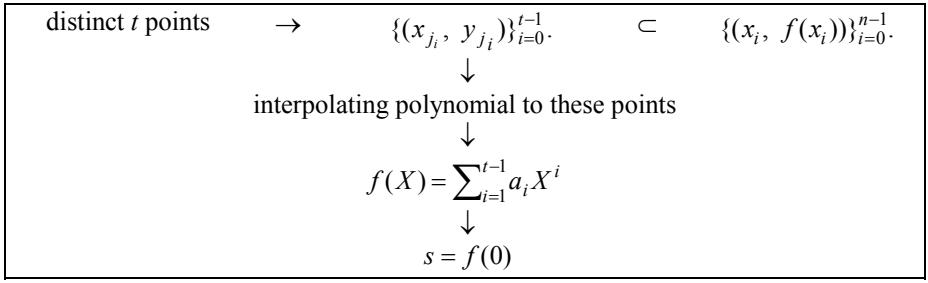
The section that follows presents the main idea of the proposed scheme. Then, the authors summarize the security problems of the main components of the scheme. Details of the proposed scheme are presented afterwards, followed by a comprehensive analysis. Conclusions of the presented research are given in the last section.

Main Idea

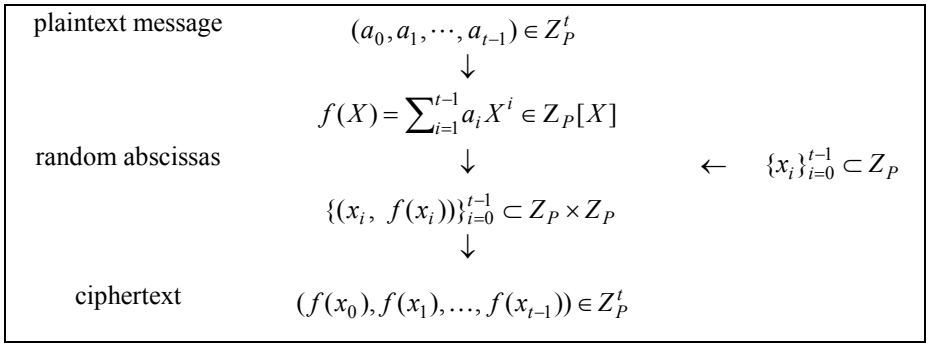
In the previous section, the authors point out that their approach to the problem of reducing the cost of a public-key encryption of a long message is to use a permutation-like information breaking mechanism to re-permute the long message and partition it into several blocks, say t blocks, such that no one can recover the original message unless s/he has all t blocks. It is a well-known scheme, called (t,n)-threshold secret sharing scheme. Using a (t,t)-threshold scheme, one can distribute, or partition, a secret into t shadows such that any $t' < t$ shadows can not recover the original secret and t distinct shadows can recover it. Let the secret be denoted by s. In Shamir's (t,n)-threshold scheme,[5] s is placed at the constant coefficient position of a polynomial of degree $t-1$ with other coefficients being randomly selected. We use the resulting random polynomial to generate n distinct points. Then, we can use any t out of these n distinct points to reconstruct the random polynomial, the unique interpolating polynomial of these t distinct points, and recover s by retrieving the constant coefficient of it. It should be noted that any point set of size less than t can not uniquely recover the random polynomial. The distribution of the secret in Shamir's scheme is depicted diagrammatically below:



With the property of modulo arithmetic operations, for instance $(\mathrm{mod}\, P)$ with P being prime, any change of a bit in s will be distributed over all bits of the resulting point set $\{(x_i,\ f(x_i))\}_{i=0}^{n-1}$. The recovering of the secret in Shamir's scheme is depicted diagrammatically below:



It is obvious that the secret s can be placed at the position of any coefficient of the random polynomial without loss of any security condition. And, a plaintext message seems to be a random number in general. With this insight, we may treat a plaintext message as a random polynomial function, and use it to generate a set of distinct points by giving a set of random distinct abscissas, $\{x_i\}_{i=0}^{t-1}$. The following diagram can be used to depict the permutation procedure:



It can be seen that any set of distinct abscissas, $\{x_i\}_{i=0}^{t-1} \subset Z_P$, uniquely determines an one-one linear transformation from Z_P^t to Z_P^t. Let denote the linear transformation by $F_{\vec{x}}$, then, the above permutation procedure can be written in the form of the following matrix equation:

$$\vec{y} \equiv F_{\vec{x}} \vec{a} \pmod{P}, \tag{1}$$

where $\vec{a}, \vec{y} \in Z_P^t$ and $y_j = \sum_{i=0}^{t-1} a_i x_j^i$. Note that $F_{\vec{x}}$ is a Vandermonde matrix. Let $\vec{A}$, and $\vec{Y}$ denote random vectors (or sequences of random variables). That is, $\vec{A} = (A_0, A_1, \ldots, A_{t-1})$, $\vec{Y} = (Y_0, Y_1, \ldots, Y_{t-1})$, and A_i, Y_i are random variables. Then Equation (1) implies

$$\mathrm{H}(\vec{Y} \mid \vec{A}, \vec{x}) = 0, \text{ or} \tag{2}$$

$$\mathrm{H}(\vec{A} \mid \vec{Y}, \vec{x}) = 0, \tag{3}$$

provided $\vec{x} = (x_0, x_1, \ldots, x_{t-1})$, ($x_i \neq x_j$ if $i \neq j$), where $H(|)$ denotes the conditional entropy function. It should be noted that if $\vec{a}$ happens to be an eigenvector of $F_{\vec{x}}$, then $\vec{y}$ is also an eigenvector of $F_{\vec{x}}$. In general, $\vec{a}$ is unlikely to be an eigenvector of $F_{\vec{x}}$, because $\vec{a}$ represents a plaintext message which can be seen as a randomly selected vector. In this situation, one can control the abscissa set $\{x_i\}_{i=0}^{t-1}$ to prevent it. Or, we will propose a scheme to make the probability of $\vec{a}$ being an eigenvector of $F_{\vec{x}}$ to be small. Given $\vec{x}$ and $\vec{y}$, one can determine whether $\vec{y}$ is an eigenvector of $F_{\vec{x}}$ or not. However, according to the theory of Shamir's threshold scheme, we have

$$H(A_i) = H(A_i \mid Y_1, \ldots, Y_{t-1}, \vec{X}). \tag{4}$$

That is, without the knowledge of Y_0, one cannot decide whether $\vec{Y}$ is an eigenvector of $F_{\vec{x}}$ or not.

In summary, we may permute a plaintext message by a linear transformation which is uniquely determined by randomly selecting a secret set of distinct abscissas. Without all the permuted information, one cannot learn any information about the original plaintext message. In the next section, we will briefly review the notions of pseudo-random number generator and a one-way hash function.

Related Topics

In this section, we will briefly review two important notions, one-way hash function and pseudo-random number generator. We shall use a one-way hash function to generate the message digest of a secret message and a pseudo-random number generator to generate a set of abscissas. Using a pseudo-random number generator by feeding a random number seed to generate a set of abscissas replaces the notion of the compression of a set of abscissas into a secret seed. A vector consists of the message digest and the chance that the original message is an eigenvector of a linear transformation will likely be decreased.

One-Way Hash Functions

Informally, a function $Y = f(X)$ has one-way property which means that given any $X = x$ in the domain of f, it is easy to compute a $Y = y$ in the co-domain of f such that $y = f(x)$, but it is hard to invert. That is, given a $Y = y$ in the co-domain of f, it is hard to compute a $X = x$ such that $y = f(x)$. To easily formulate the one-way property, we may assume that domain and co-domain of all functions are sets of binary strings $\{0,1\}^*$. Formally, a one-way function can be defined as follows:

Definition 1 One-way Function[6] *Let* $f : \{0,1\}^* \to \{0,1\}^*$ *be a function from binary strings to binary strings.* f *is called a* one-way function *if it satisfies the following conditions:*

1. f *is injective, and for all* $x \in \{0,1\}^*$, $|x|^{\frac{1}{k}} < |f(x)| < |x|^k$ *for some integer* $k > 0$, *where* $|x|$ *denotes the length of* x. *In other words,* $f(x)$ *is at most polynomially longer or shorter than* x.
2. f *is in* **FP**, *that is, given any* x, *the function value* $f(x)$ *can be computed in polynomial time.*
3. *The most important condition is that* f^{-1}, *the inverse of* f, *is not in* **FP**. *That is, there is no polynomial-time algorithm which, given a binary string y, either computes a* x *such that* $y = f(x)$ *or returns "no," if no* x *satisfies the equation* $y = f(x)$.

It can be noticed that, since a one-way function f is injective, x can be uniquely recovered from $f(x)$ by trying all x of appropriate length. The key point is that there is no polynomial-time algorithm that achieves this. Until now, no function can be proved to be a one-way function. However, there are two functions that many people

suspect are one-way functions. The first is the integer multiplication function and the second is the exponentiation function modulo a prime.

If $Y = f(X)$ is a one-way function, then $H(Y \mid X) = 0$ and $H(X \mid Y) = 0$, where $H(|)$ is the conditional entropy function. But, by the one-way property, the equation $H(X \mid Y) = 0$ provides no useful information to invert a one-way function.

A function is called a hash function if it can take a binary string of any length and produce a binary string of fixed length. That is, a hash function is of the following general form:

$$\mathtt{Hash}_m : \{0,1\}^* \rightarrow [0, m-1], \tag{5}$$

for some positive integer m and $[0, m-1]$ denotes the set of integers $\{0, 1, 2, \ldots, m-1\}$. It is obvious that $\mathtt{Hash}_m$ cannot be an injection for all possible integers m. In effect, $\mathtt{Hash}_m$ retrieves some attributes of its input and modifies or prunes them into a fixed length of $\lceil m \rceil$. Since we will use a hash function to generate a message digest in the proposed scheme, the hash function has to satisfy a security condition, which is called the collision-free property. It is impossible that a hash function satisfies the true collision-free properties. However, there are hash functions that can satisfy some pseudo-collision-free properties.

Definition 2 Weakly Collision-free Property[7] *A hash function* $\mathtt{Hash}_m$ *is* weakly collision-free *if, given* x*, there is no polynomial-time algorithm to compute a* $x' \neq x$ *such that* $\mathtt{Hash}_m(x') = \mathtt{Hash}_m(x)$.

Definition 3 Strong Collision-free Property[8] *A hash function* $\mathtt{Hash}_m$ *is* strong collision-free *if there is no polynomial-time algorithm to compute two* x *and* x' *such that* $x \neq x'$ *and* $\mathtt{Hash}_m(x) = \mathtt{Hash}_m(x')$.

Definition 4 One-way Hash Function[9] *A hash function* $\mathtt{Hash}_m$ *is* one-way *if, given a* y*, there is no polynomial-time algorithm to compute a* x *such that* $\mathtt{Hash}_m(x) = y$.

Note that a one-way hash function is not a one-way function. It has been proven that a strong collision-free hash function must be a one-way hash function. In this article, we will assume that if $Y = \mathtt{Hash}_m(X)$ is a one-way hash function, then

$$H(X) \geq H(X \mid Y) >> 0. \tag{6}$$

The above equation implies that directly computing X from Y might be of no use than directly trying out all possible appropriate X or directly guessing X.

Pseudo-Random Number Generators

A random number generator can generate a sequence of numbers, such that having observed the first $n-1$ generated numbers, we still cannot predict the n-th number to be generated by the generator. A random number generator can be illustrated by a sequence of random variables X_0, X_1, …, X_j, X_{j+1}, …, in which each random variable X_j obeys a probability distribution and they satisfy the following equation:

$$H(X_j) = H(X_j \mid X_0, X_1, \ldots, X_{j-1}). \tag{7}$$

That is, in a real random sequence, we learn no information about the future from the history of the random sequence. However, in a practical situation, we always assume that all X_j will obey the same probability distribution, $p(X)$, and assume that the history of such a random number sequence provides information about its sample space and probability distribution, i.e., $X_j = X$ for all j. Even in this ideal situation, Equation (7) still holds. Another problem of the real random number generators is that the generated random number sequence cannot be likely reproduced by the same random number generator. In our proposed scheme, we really need a pseudo-random number generator. A pseudo-random number generator can generate a set of number sequences indexed by a set of binary strings called random number seeds. Thus, the general functional form of a pseudo-random number generator is as follows:

$$\mathrm{PRNG}_m^{n_O} : Z_{n_O} \to Z_m^N, \tag{8}$$

where m and n_O are positive integers. The parameter m denotes the sample space, Z_m, of the pseudo-random sequences generated by $\mathrm{PRNG}_m^{n_O}$, and the parameter n_O depicts the set of the seeds, Z_{n_O}. Let $\mathrm{PRNG}_m^{n_O}(i) = x_{i,0}, x_{i,1}, \ldots, x_{i,j}, x_{i,j+1}, \ldots$. Suppose that the elements in $\mathrm{PRNG}_m^{n_O}[Z_{n_O}]$ are arranged such that

$$\frac{\sum_{(i \in Z_{n_O}) \wedge (x_{i,j} = x)} I}{n_O} \approx p(x) \text{ for each } j, x \text{ and} \tag{9}$$

$$\frac{\sum_{(0 \le j < l) \wedge (x_{i,j} = x)} I}{l} \to p(x) \text{ for each } i, x \text{ when } l \to \infty. \tag{10}$$

In Equation (9) PRNG_m^n is required to transform the uniformly distributed random variable I, the seed, into a random variable X'_j with probability distribution $p(X)$ for each j. We may use the random variable X'_j to simulate the random variable $X_j = X$. Now, we rewrite (8) as an equation of random variables.

$$\mathrm{PRNG}_m^{n_O}(I) = X'_0, X'_1, X'_2, \ldots, X'_j, X'_{j+1}, \ldots. \tag{11}$$

Based on the above equation and real pseudo-random number generators, we may reasonably assume that:

$$H(X'_0, X'_1, \cdots, | I) = 0, \tag{12}$$

$$H(X'_j) \geq H(X'_j \mid X'_0, \cdots, X'_{j-1}) >> 0, \text{ and} \tag{13}$$

$$H(I) \geq H(I \mid X'_0, \cdots, X'_j) >> 0, \tag{14}$$

for all $j < j_O$, where j_O is an integer description of the one-way property of $\mathrm{PRNG}_m^{n_O}$. The above assumptions state that a pseudo-random number generator will be assumed to behave like a one-way function if the corresponding j_O is sufficiently large. Now, we will discuss the parameter n_O of $\mathrm{PRNG}_m^{n_O}$. n_O is the size of the set of seeds or the size of $\mathrm{PRNG}_m^{n_O}[Z_{n_O}]$. By assumption $X'_0, X'_1, X'_2, \ldots$ are independent, identically distributed $\sim p(X)$, and we have

$$-\frac{1}{j} \lg p(X'_0, X'_1, \cdots, X'_j) \to H(X) \tag{15}$$

in probability.

The equation is the so-called Asymptotic Equipartition Property (AEP). In the following, we list a definition related to AEP[10]:

Definition 5 Typical Set *The typical set* $T_\varepsilon^{(j)}$ *with respect to* $p(X)$ *is the set of sequences* $(x_0, x_1, \ldots, x_{j-1}) \in (Z_m)^j$ *with the property:*

$$2^{-j(H(X)+\varepsilon)} \leq p(x_0, x_1, \ldots, x_{j-1}) \leq 2^{-j(H(X)-\varepsilon)}. \tag{16}$$

We can see that if $(x_0, x_1, \ldots, x_{j-1}) \in T_\varepsilon^{(j)}$ then

$$H(X) - \varepsilon \le -\frac{1}{j} \lg p(x_0, x_1, \cdots, x_{j-1}) \le \mathrm{H(X)} + \varepsilon. \qquad (17)$$

Obviously, we require that $\mathrm{PRNG}_m^{n_O}[Z_{n_O}] \subset T_\varepsilon^{(j_O)}$ for some reasonable small ε. However, the size of $T_\varepsilon^{(j_O)}$ is smaller than $2^{j_O H(X)+\varepsilon}$. Suppose that $\mathrm{PRNG}_m^{n_O}$ is injection. Then, we have:

$$n_O = |\,\mathrm{PRNG}_m^{n_O}[Z_{n_O}]\,| \le |\,T_\varepsilon^{(j_O)}\,| \le 2^{j_O H(X)+\varepsilon}. \qquad (18)$$

Thus, we may select n_O as close to $2^{j_O H(X)}$ as possible.

In the scheme proposed in this article, we will use a pseudo-random number generator to compress a set of secret abscissas, or as a secret abscissas generator. Suppose that $\mathrm{PRNG}(X,Q,N)$, $Q < \phi(N)$, is a random number generator that can generate a $(\phi(N), Q)$-combination sequence x_0, x_1, …, x_{Q-1}, where x_i's are distinct and $x_i \in Z_N^*$. $\mathrm{PRNG}(X,Q,N)$ can be implemented by selecting first Q items of $\mathrm{PRNG}_N^{n_O}(X)$ that are prime to N. Note that $|\mathrm{PRNG}(Z_{n_O},Q,N)| \le \binom{\phi(N)}{Q}$. Using Pascal's triangle, we may require $Q = \frac{\phi(N)}{2}$ or $Q \approx \frac{\phi(N)}{2}$ to make $|\mathrm{PRNG}(Z_{n_O},Q,N)|$ as large as possible. We call a pseudo-random number generator of the form $\mathrm{PRNG}(X,Q,N)$ secure if it satisfies the above-mentioned conditions.

In the next section, we will propose a low cost encryption scheme based on the notions elaborated here.

Proposed Scheme

To present the proposed scheme, we will first list the assumptions that will be used in the scheme.

1. Let P be a public large prime number.
2. Let $\mathrm{PRNG}(X,Q,N)$ be a public secure pseudo-random number generator. In addition, for each positive integer pair (t,n), $t < \phi(n)$, $\mathrm{PRNG}(x,t,n)$ will generate a $(\phi(n), t)$-combination integer sequence x_0, x_1, …, x_{t-1}, randomly selected from Z_n^* given a random seed $X = x$.

3. Suppose that the public-private key pairs of Alice, the sender, and Bob, the receiver, are (e_A, d_A) and (e_B, d_B), respectively. In addition, $E_e()$ and $D_d()$ are the associated encryption and decryption algorithms.

4. Let $\mathtt{Hash}_N(X, M)$ be a public secure one-way hash function that is unlikely to have occurred collisions, such that for all x, n and a positive integer m, $\mathtt{Hash}_n(x, m) \in Z_n$.

5. The sender, Alice, maintains a table to record the used hash values. The length of the table is at most L, where L reflects the security degree of the one-way hash function $\mathtt{Hash}_N(X, M)$.

Based on the above assumptions, we have the following properties:

1. By the assumption of $\mathtt{PRNG}(X, Q, N)$, we have $H(X) \geq H(X \mid X_0, X_1, \ldots, X_t, Q, N) >> 0$, where X denotes the random variable of random seed, the random variable vector $(X_0, X_1, \ldots, X_t) = \mathtt{PRNG}(X, t, N)$, $H()$ denotes the entropy function and $H(|)$ denotes the conditional entropy function. Or, given $N = P$ and $Q = t$, we have $H(X) \geq H(X \mid X_0, X_1, \ldots, X_t) >> 0$. However, by the assumption of PRNG() being secure, we have $H(X) \sim H(X \mid X_0, X_1, \ldots, X_t)$, where ~ denotes the "almost equal to" symbol.

2. Suppose that $Y = E_e(X)$ and $X = D_d(Y)$, where X denotes the random variable of plain-text, Y the random variable of cipher-text, e the random variable of the public key, and d the random variable of private key. We have $H(d) = H(d \mid e)$, $H(Y \mid X, e) = 0$ and $H(X \mid Y, d) = 0$.

3. Suppose that $Y = \mathtt{Hash}_N(X, M)$. In general, we have $H(Y \mid X, N, M) = 0$. But, by the assumption of $\mathtt{Hash}_N()$ being secure, we will have $H(X \mid Y, N, M) >> 0$ where >> denotes the "much greater than" symbol. Or, given $N = P$ and $M = m$, we have $H(X \mid Y) >> 0$.

Below, we first present the proposed encryption scheme, then, the proposed decryption scheme.

Proposed Encryption Sub-scheme

Suppose that Alice wants to send the secret message $(a_1, a_2, \ldots, a_t) \in Z_P^t$ to Bob secretly. Then, she performs the steps outlined in Algorithm 1.

Algorithm 1 Proposed Encryption Scheme

Input: The large prime number P, the pseudo random number generator $\mathtt{PRNG}(X,T,N)$, the hash function $\mathtt{Hash}_N(X,M)$, the public-key encryption algorithm $E_e(X)$, the decryption algorithm $D_d(X)$, the private key d_A, the public key e_B, the message $(a_1,a_2,\ldots,a_t)\in Z_P^t$, and a published m.

Output: The encrypted message $(y_0,y_1,\ldots,y_t)$ authenticated by the private key owner which is to be sent to the public key owner.

Step 1. [Compute the Message Digest] Compute the message digest $a_0=\mathtt{Hash}_P(a_1\|a_2\|\ldots\|a_t,m)$, where the expression $a_1\|a_2\|\ldots\|a_t$ denotes the catenation of a_1, a_2, …, a_{t-1} and a_t. (If a_0 had been used, Alice needs to modify the message $(a_1,a_2,\ldots,a_t)$ to compute a new a_0 that was never used. Alice, then, appends a_0 to a history table. If the length of the history table is bigger than L, Alice needs to publish a new m value, construct a new history table of length 0, and repeat the step again.)

Step 2. [Construct a Secret Polynomial] Use the secret message $(a_0,a_1,a_2,\ldots,a_t)$ to construct the secret polynomial $f(X)=a_0+a_1X+\cdots+a_tX^t \pmod P$.

Step 3. [Generate a Secret Random $(P-1,\ t+1)$-Combination Sequence] Randomly select a random seed x and generate a random sequence $\mathtt{PRNG}(x,t+1,P)=(\mathrm{x}_0,x_1,\ldots,x_t)$.

Step 4. [Generate Encrypted Message] Compute the encrypted message $[f(x_0),\ f(x_1),\ \ldots,\ f(x_t)]$.

Step 5. [Generate Encrypted Random Seed with $f(x_0)$] Use the private key d_A and the public key e_B to compute $E_{e_B}(D_{d_A}(x\|f(x_0)))$.

Step 6. [The Resulting Encrypted Message] $(y_0,y_1,\ldots,y_t)=[E_{e_B}(D_{d_A}(x\|f(x_0))),\ f(x_1),\ f(x_2),\ldots,\ f(x_t)]$.

Note that after performing Algorithm 1, the message $(a_1,a_2,\ldots,a_t)$ was first signed with the private key d_A owned by Alice. The authentication and integrity of the message can be verified by the public key e_B of the owner, Bob, using his private

key, d_B and Alice's public key e_A. Alice then sends the resulting encrypted message $(y_0, y_1, \ldots, y_t)$ to the receiver, Bob, over an insecure channel.

Proposed Decryption Sub-scheme

Upon receiving $(y_0, y_1, \ldots, y_t)$, Bob can use Algorithm 2 to decrypt the message. Algorithm 2 uses the public key e_A and the private key d_B to verify the encrypted message, i.e., that it was sent from the public key owner and the receiver is the private key owner. Algorithm 2 also uses the one-way hash function $\mathtt{Hash}_N(X, M)$ to verify the integrity of the secret message $(a_1, a_2, \ldots, a_t)$.

In the next section, the authors will analyze the security of the proposed scheme.

Algorithm 2 Proposed Decryption Scheme

Input: The large prime number P, the pseudo random number generator $\mathtt{PRNG}(X, T, N)$, the hash function $\mathtt{Hash}_N(X, M)$, the public-key encryption algorithm $E_e(X)$, the decryption algorithm $D_d(X)$, the private key d_B, the public key e_A, and the encrypted message $(y_0, y_1, \ldots, y_t)$.

Output: Reject the encrypted message or accept the decrypted message $(a_1, a_2, \ldots, a_t) \in Z_P^t$ whose authentication, sent from the public key owner, and integrity have been verified by the public key owner.

Step 1. [Recover the Secret Seed] Use the public key e_A and the private key d_B to decrypt the random seed $x \| f(x_0) = E_{e_A}(D_{d_B}(E_{e_B}(D_{d_A}(x \| f(x_0)))))$.

Step 2. [Recover the $(P-1,\ t+1)$-Combination Sequence] Use the seed x to generate the $(P-1,\ t+1)$-combination sequence, $\mathtt{PRNG}(x, P, t+1) = (\mathrm{x}_0, x_1, x_2, \ldots, x_t)$.

Step 3. [Recover the Secret Message] Compute the interpolating polynomial $f(x) \in Z_P[X]$ from the point sets $\{(x_0, f(x_0)),\ (x_1, f(x_1)),\ \ldots,\ (x_t, f(x_t))\} \subset Z_P \times Z_P$. The coefficients of the polynomial $f(x) \in Z_P[X]$ would be the secret message $(a_0, a_1, \ldots, a_t)$.

Step 4. [Verify the Message Digest] Check whether $a_0 = \mathtt{Hash}_P(a_1 \| a_2 \| \ldots \| a_t, m)$ or not. If the equality does not hold, reject the message. If it passes the verification, accept the message as being sent from the public key e_A owner and its integrity has not been destroyed.

Analysis

The attacks to the proposed scheme can be classified into the following classes:

1. Type 1 attack is eavesdropping or passive wiretapping. In general, the attack cannot be detected. This is the reason why we construct a cryptosystem to encrypt sensitive or secret message for preventing eavesdropping. In this attack we assume that the sender, Alice, and the receiver, Bob, are trusted parties. The eavesdropper, Eve, wants to learn the secret message from the encrypted message.
2. Type 2 attack is tampering or active wiretapping. The attacker, Mallory, modifies the encrypted message or forges an encrypted message to fool either Alice or Bob or the two of them.
3. Type 3 attack is an attack coming from the receiver. Bob forges a message and claims that it has been sent by Alice.
4. Type 4 attack is an attack coming from the sender. Alice wants to deny a message which she has sent to Bob.

It has to be noted that if the proposed scheme cannot prevent type 2 attacks, Alice can use the weak point to deny having sent a sensitive message and Bob can claim that he has received a message that Alice has never sent. However, types 3 and 4 attacks are more powerful than type 2 attacks because Alice and Bob have more key information than Mallory.

Below, we restate the assumptions listed in the previous section.

Let $(a_1, a_2, \ldots, a_t)$ represents the random vector of plain-text to be encrypted, and $(y_0, y_1, \ldots, y_t)$ - the random vector of the resulting encrypted cipher-text. Let x represents the random variable of the random number seed chosen by Alice, $(x_0, x_1, x_2, \ldots, x_t) = \mathrm{PRNG}(x, t+1, P)$. And, let (e, d) denote the random vector that represents the public-private key pair. In addition, let $y_{x,0} = D_{d_A}(x \| f(x_0))$ and $y_0 = E_{e_B}(y_{x,0})$.

1. $H(a_1', a_2', \ldots, a_t' \mid a_0, a_1, \ldots, a_t) >> 0$, where $H(a_0 \mid a_1, a_2, \ldots, a_t) = 0$ (i.e., $a_0 = \mathrm{Hash}_P(a_1 \| a_2 \| \ldots \| a_t, m)$) and $(a_1', a_2', \ldots, a_t')$ is the random vector, distinct from $(a_1, a_2, \ldots, a_t)$, such that $a_0 = \mathrm{Hash}_P(a_1' \| a_2' \| \ldots \| a_t', m)$.
2. $H(x \mid x_0, x_1, \ldots, x_t, t+1, P) >> 0$, where $H(x_0, x_1, \ldots, x_t \mid x, t+1, P) = 0$.
3. $H(e \mid d) = 0$ and $H(d \mid e) >> 0$.

4. $H(y_{x,0} \mid (x \| f(x_0))) >> 0$, where $H(y_{x,0} \mid (x \| f(x_0)), d_A) = 0$, and $H(y_{x,0} \mid y_0) >> 0$, where $H(y_{x,0} \mid y_0, d_B) = 0$.

Type 1 Attack to the Proposed Scheme

The type 1 attack is a ciphertext-only attack. The proposed scheme uses a random seed x to generate a linear transformation on Z_P^{t+1}, and the matrix representation of the linear transformation is the so-called Vandermonde matrix, such as the following:

$$\begin{pmatrix} 1 & x_0 & x_0^2 & \cdots & x_0^t \\ 1 & x_1 & x_1^2 & \cdots & x_1^t \\ & & \vdots & & \\ 1 & x_t & x_t^2 & \cdots & x_t^t \end{pmatrix} \begin{pmatrix} a_0 \\ a_1 \\ \vdots \\ a_t \end{pmatrix} = \begin{pmatrix} f(x_0) \\ f(x_1) \\ \vdots \\ f(x_t) \end{pmatrix}. \tag{19}$$

According to the assumption about the pseudo-random number generator $\mathtt{PRNG}(X, Q, N)$, the $(P-1, t+1)$-combination integer sequence $(x_0, x_1, \ldots, x_t)$ generated by $\mathtt{PRNG}(x, t+1, P)$ is a set of distinct integers, i.e. $x_i \neq x_j \in Z_P$ whenever $i \neq j$. Thus, the corresponding Vandermonde matrix is nonsingular. That is, given a random seed x and $(f(x_0), f(x_1), \ldots, f(x_t))$, Eve can determine a unique $(a_0, a_1, \ldots, a_t)$. Thus, we have

$$H(\vec{f}_x \mid \vec{a}', \vec{x}) = 0, \text{ and} \tag{20}$$

$$H(\vec{f}_x \mid \vec{x}) = H(\vec{a}' \mid \vec{x}), \tag{21}$$

where $\vec{f}_x = (f(x_0), f(x_1), \ldots, f(x_t))$, $\vec{a}' = (a_0, a_1, \ldots, a_t)$, and $\vec{x} = (x_0, x_1, \ldots, x_t)$. However, the secret random seed x and $f(x_0)$ are encrypted by the public-key e_B, and only Bob can decrypt it and no one else can do that providing the public key encryption cryptosystem is secure. Without x and $f(x_0)$, Eve cannot learn any information about the secret message $(a_0, a_1, \ldots, a_t)$. According to the theory of interpolating polynomials, we have

$$H(\vec{a}', \vec{x}) = H(\vec{a}', \vec{x} \mid \vec{y}'), \text{ or} \tag{22}$$

$$H(\vec{a}') = H(\vec{a}' \mid \vec{x}, \vec{y}'), \tag{23}$$

where $\vec{y'} = (y_1, y_2, \ldots, y_t) = (f(x_1), f(x_2), \ldots, f(x_t))$. Suppose that Alice uses the random seed x repeatedly. Then, Eve may have learnt the $(P-1, t+1)$-combination sequence $(x_0, x_1, \ldots, x_t)$. However, according to the theory of interpolating polynomials, without $f(x_0)$ Eve cannot uniquely determine the polynomial function $f(X)$. According to the theory of Shamir's (t, n)-threshold secret sharing scheme, the secret message $(a_0, a_1, \ldots, a_t)$ is protected by a perfect secret sharing scheme providing the public-key cryptosystem is secure. That is, Eve has to solve the following problem to perform the attack.

$$\begin{aligned} &\text{Given } y_0, \\ &\text{compute } x \| f(x_0) \text{ such that} \\ &y_0 = E_{e_B}(D_{d_A}(x \| f(x_0))). \end{aligned} \tag{24}$$

Not considering the signing operation, suppose that Alice uses a public-key cryptosystem to encrypt the secret message $(a_1, a_2, \ldots, a_t)$. It will need t encryption operations to perform the encryption of the message. In the proposed scheme, we use a pseudo-random number generator operation and a $(t+1) \times (t+1)$-linear transformation operation to replace the $t-1$ public-key operations. (Because the complexity of the public-key encryption operation is the same as the complexity of the public-key decryption operation, we call either one of them a public-key operation.) In general, a public-key operation is costly. So, the proposed scheme is less costly. For the same reason, the decryption operation of the proposed scheme uses a pseudo-random number generator operation and an interpolating polynomial operation to replace the $t-1$ public-key operations.

In conclusion, given a secure public-key cryptosystem and not considering the signing operation the proposed scheme can prevent the ciphertext-only attacks; it uses two pseudo-random number generator operations, a linear transformation operation and an interpolating polynomial operation to reduce the number of required public-key operations to two.

Type 2 Attack to the Proposed Scheme

If Mallory intercepts an encrypted message—simply replaces one y_i with y_i', and inserts it back into the message—Bob will discover the attack in Step 4 of Algorithm 2. To make such an attack meaningful, she has to perform an attack of type 1 to the encrypted message. However, without the help of Alice or Bob, she cannot compute the secret message $(a_0, a_1, \ldots, a_t)$ providing the public-key cryptosystem is secure. For this reason, we consider type 2 attack, a known-plaintext

attack, to the proposed scheme. In addition, Mallory cannot learn the sequence $(x_0, x_1, \ldots, x_t)$ from the two sequences $(a_0, a_1, \ldots, a_t)$ and $(y_0, y_1, \ldots, y_t)$ unless Alice repeatedly uses the same secret seed x. It is unlikely to happen. However, we assume that Mallory knows the three sequences $(x_0, x_1, \ldots, x_t)$, $(a_0, a_1, \ldots, a_t)$ and $(y_0, y_1, \ldots, y_t)$. And, she wants to change a_i to a_i', where $0 < i \le t$.

After computing the digest message $a_0' = \mathtt{Hash}_P(a_1 \| \ldots \| a_i' \| \ldots \| a_t, m)$, Mallory, then, computes:

$$\begin{pmatrix} f'(x_0) \\ f'(x_1) \\ \vdots \\ f'(x_t) \end{pmatrix} = \begin{pmatrix} 1 & x_0 & x_0^2 & \cdots & x_0^t \\ 1 & x_1 & x_1^2 & \cdots & x_1^t \\ & & \vdots & & \\ 1 & x_t & x_t^2 & \cdots & x_t^t \end{pmatrix} \begin{pmatrix} a_0' \\ a_1 \\ \vdots \\ a_i' \\ \vdots \\ a_t \end{pmatrix}, \tag{25}$$

where $f'(X) = a_0' + a_1 X + a_2 X^2 + \cdots + a_i' X^i + \cdots + a_t X^t$. Now, Mallory's attack is reduced to computing y_0' using the following equation:

$$y_0' = E_{e_B}(D_{d_A}(x \| f'(x_0))). \tag{26}$$

By the assumption about the security of the pseudo random number generator, Mallory cannot use the sequence $(x_0, x_1, \ldots, x_t)$ to learn the secret random seed x. Even though she uses a new random seed x' to compute a new sequence, ($f''(x_0')$, …, $f''(x_t')$), she still needs the private key d_A to compute a new $y_0'' = E_{e_B}(D_{d_A}(x' \| f''(x_0')))$. Mallory uses the following equation to compute $f(x_0)$ for learning the secret seed x.

$$\begin{pmatrix} f(x_0) \\ y_1 \\ \vdots \\ y_t \end{pmatrix} = \begin{pmatrix} 1 & x_0 & x_0^2 & \cdots & x_0^t \\ 1 & x_1 & x_1^2 & \cdots & x_1^t \\ & & \vdots & & \\ 1 & x_t & x_t^2 & \cdots & x_t^t \end{pmatrix} \begin{pmatrix} a_0 \\ a_1 \\ \vdots \\ a_t \end{pmatrix}. \tag{27}$$

Now, Mallory will obtain the following equation:

$$y_0 = E_{e_B}(D_{d_A}(x \| f(x_0))). \tag{28}$$

From the above equation, without Bob's help, Mallory cannot learn the secret random seed x either. Suppose that Mallory and Bob want to fool Alice. However, without the private key d_A, Mallory cannot compute y_0'. Thus, Mallory and Bob cannot fool Alice.

In conclusion, if the public-key cryptosystem is secure, only Alice can compute the value y_0; no one else can do that. Thus, the proposed scheme uses two public-key operations to prevent type 2 attacks. All the published information e_A, e_B, and $(y_0, y_1, \ldots, y_t)$ does not provide useful information to accomplish type 2 attacks even with the knowledge about the repeated uses of the same random seed x.

Type 3 Attack to the Proposed Scheme

Bob can perform all attacks that Mallory can perform. In addition, Bob has an additional piece of information, the private key d_B. Using this private key, Bob can easily get the secret random seed x. So, we suppose that Bob wants to forge a message $(a_1', a_2', \ldots, a_t')$, then claim that it was sent from Alice. Bob may use the hash function $\mathtt{Hash}_N(X, M)$ to compute $a_0' = \mathtt{Hash}_P(a_1' \| \ldots \| a_t', m)$. He randomly selects a seed x' and generates a $(P-1, t+1)$-combination sequence $(x_0', x_1', \ldots, x_t')$. Then, he computes

$$\begin{pmatrix} f'(x_0') \\ f'(x_1') \\ \vdots \\ f'(x_t') \end{pmatrix} = \begin{pmatrix} 1 & x_0' & x_0'^2 & \cdots & x_0'^t \\ 1 & x_1' & x_1'^2 & \cdots & x_1'^t \\ & & \vdots & & \\ 1 & x_t' & x_t'^2 & \cdots & x_t'^t \end{pmatrix} \begin{pmatrix} a_0' \\ a_1' \\ \vdots \\ a_t' \end{pmatrix}, \tag{29}$$

where $f'(X) = a_0' + a_1'X + a_2'X^2 + \cdots + a_t'X^t$. But, Bob does not have the private key d_A; he, therefore, cannot directly use the formula $y_0' = E_{e_B}(D_{d_A}(x' \| f'(x_0')))$ to compute y_0'. Consider the following equation,

$$x' \| f'(x_0') = E_{e_A}(D_{d_B}(y_0')). \tag{30}$$

Suppose that $\mathtt{Proj}_i(\mathtt{PRNG}(X, N)) = X_i$ is the *i*-th projection function. Equation (30) can be rewritten as:

$$x' \| f'(\mathtt{Proj}_0(\mathtt{PRNG}(x', P))) = E_{e_A}(D_{d_B}(y_0')). \tag{31}$$

Table 1: History of Messages that Alice has Sent.

$a_{0,i}$	$\bar{x}_i$	$\bar{x}_{0,i}$	$y_{0,i}$
$a_{0,1}$	$\bar{x}_1$	$\bar{x}_{0,1}$	$y_{0,1}$
$a_{0,2}$	$\bar{x}_2$	$\bar{x}_{0,2}$	$y_{0,2}$
$\vdots$	$\vdots$	$\vdots$	$\vdots$
$a_{0,ml}$	$\bar{x}_{ml}$	$\bar{x}_{0,ml}$	$y_{0,ml}$

Thus, Bob's attack is reduced to solving the following simultaneous equations:

$$X \| f'(\texttt{Proj}_0(\texttt{PRNG}(X,P))) = E_{e_A}(D_{d_B}(Y_0)), \tag{32}$$

$$f'(\texttt{Proj}_0(\texttt{PRNG}(X,P))) = \sum_{i=0}^{t} a'_i(\texttt{Proj}_0(\texttt{PRNG}(X,P)))^i \ (\text{mod P}) \tag{33}$$

$$a'_0 = \texttt{Hash}_P(a'_1 \| \ldots \| a'_t, m) \cdot b \tag{34}$$

For any $(a'_1, a'_2, \ldots, a'_t) \in Z_P^t$ and any random seed x', there should exist a solution (x', y'_0) of the above simultaneous equations since Alice can compute such a solution. However, given y'_0, Equation (32) uniquely determines a x'. But x' does not necessarily satisfy Equation (33). Note that if (x', y'_0) is a solution, the computation of y'_0 from x'_0 requires a one-way function $\texttt{PRNG}(X,T,N)$. Under our assumptions, Bob has to exhaustively search for y'_0 to compute x' such that it satisfies Equation (33). Suppose that Bob controls the value of a'_0 in order to find a proper sequence $(a'_1, a'_2, \ldots, a'_t)$ that satisfies Equation (33). However, in order to do that, Bob needs to break the secure one-way hash function $\texttt{Hash}_N(X,M)$. Now, we add one more assumption to increase Bob's abilities. Bob has collected all messages that Alice had sent to him and constructed Table 1, where $(a_{1,i}, a_{2,i}, \ldots, a_{t,i})$ is the i-th message that Alice has sent,

$$a_{0,i} = \texttt{Hash}_P(a_{1,i} \| a_{2,i} \| \ldots \| a_{t,i}, m),) \tag{35}$$

$$f_i(X) = \sum_{j=0}^{t} a_{i,j} X^j, \tag{36}$$

$\bar{x}_i$ is the i-th random seed, $\bar{x}_{0,i}$ is the first random number generated by $\mathtt{PRNG}(\bar{x}_i, t+1, P)$, and

$$y_{0,i} = E_{e_B}(D_{d_A}(x^i \,\|\, f_i(\bar{x}_{0,i}))). \tag{37}$$

It should be noted that the computation of $a_{0,i}$ is independent from the choice of the random seed $\bar{x}_i$. Thus, if ml is sufficiently large, there is a chance that Bob can change the value of $(a'_1, a'_2, \ldots, a'_t)$ such that a'_0 can be found in Table 1. Bob then selects the corresponding random seed $\bar{x}_i$ and uses the corresponding $y_{0,i}$ as y'_0. Alice cannot deny the resulting encrypted message $(y'_0, y'_1, \ldots, y'_t)$. However, Alice controls the length of the history table such that it is always smaller than L. So, we have $ml < L$. This means that ml can be too large and the new hash value will unlikely collide with the used hash values.

In conclusion, the proposed scheme can effectively prevent Bob's attack.

Type 4 Attack to the Proposed Scheme

Type 4 attack is performed by the sender, Alice. She wants to deny sending a secret message to Bob. If Bob can perform the type 3 attack, Alice can easily deny a message which she has sent. In a previous subsection, we have shown that without the help of Alice Bob is unlikely to perform a successful type 3 attack. Note that y_0 is protected by three one-way-like functions, $\mathtt{Hash}_N()$, $\mathtt{PRNG}()$, and $D_{d_A}()$, and only Alice can perform the public-key operation $D_{d_A}()$. Thus, the y_0 value of an encrypted message can be easily computed only by the sender, Alice. If Alice denies an encrypted message, Bob can publish the random seed x, y_0, and $D_{d_B}(y_0)$, ($f(x_0)$, $f(x_1)$, …, $f(x_t)$). Anyone can use the published information to prove that the encrypted message has been sent from Alice to Bob. Alice cannot deny it.

In summary, the proposed scheme provides undeniable services.

Conclusions

In this article, we use an information permutation scheme (a $(t+1, t+1)$-threshold scheme) to permute and break a message into a sequence of sub-blocks, such that without all sub-blocks we cannot recover the original message. The information breaking scheme is a polynomial-time operation. By encrypting a sub-block, we can protect the whole message. Thus, it is a low-cost scheme. In addition, we have shown that the proposed scheme preserves such cryptographic operations as information

authentication, information integrity, unforgeability, and undeniablility, while still maintaining a low cost.

First, the authors have presented the proposed information permutation and breaking scheme, and analyzed its security. The evidence for its efficiency is that it is a matrix multiplication modulo a prime. Next, the security requirements of one-way hash function and secure pseudo-random number generator have been given. An important contribution of the presented work is that the authors use information entropy to describe the notion of the one-way property that is believed to be a problem in computational complexity. This article has also established estimation of the size of the set of the random number seeds to a secure pseudo-random number generator that does not consider the algorithm that implements the generator.

Notes:

[1] Ronald L. Rivest, Adi Shamir, and Leonard M. Adleman, "A Method for Obtaining Digital Signatures and Public Key Cryptosystems," *Communications of the ACM* 21, no. 2 (February 1978): 120–126.

[2] Certificateless Public Key Cryptography.

[3] Joan Daemen and Vinvent Rijmen, "Advance Encryption Standard," (Computer Security Division of the Information Technology Laboratory at the National Institute of Standards and Technology, U.S. Department of Commerce's Technology Administration, October 2000), <http://csrc.nist.gov/CryptoToolkit/aes> (3 December 2004).

[4] Adi Shamir, "How to Share a Secret," *Communications of the ACM* 22, no. 11 (November 1979): 612–613.

[5] Shamir, "How to Share a Secret."

[6] Christos H. Papadimitriou, *Computational Complexity* (Reading, Massachusetts, Menlo Park, California: Addison-Wesley Publishing Company, 1994).

[7] Douglas R. Stinson, *Cryptography: Theory and Practice* (Boca Raton, London, Tokyo: CRC Press Inc., 1995).

[8] Stinson, *Cryptography: Theory and Practice*.

[9] Stinson, *Cryptography: Theory and Practice*.

[10] Thomas M. Cover and Joy A. Thomas, *Elements of Information Theory*, (New York, Chichester, Brisbane, Toronto, Singapore: John Wiley & Sons, Inc., 1991).

CHAO-WEN CHAN was born in Hsinchu, Taiwan, Republic of China, on 30 December 1957. He obtained a B.S. degree in Mathematics from National Tsing Hua University, Hsinchu, Taiwan, in 1981 and a M.S. degree in Mathematics from National Tsing Hua University, Hsinchu, Taiwan, in 1983. He is currently a Ph.D. candidate in Computer Science and Information Engineering at the National Chung Cheng University. His research interests include Cryptography, Image Processing, and Information Security. *Address for correspondence:* Department of Computer Science and Information Engineering, National Chung Cheng University, 160, San-Hsing, Min-Hsiung, Chiayi 621, Taiwan. *Phone*: 886-5-2720411 ext. 33100; *Fax*: 886-5-2720859; *E-mail*: ccwen@cs.ccu.edu.tw.

CHIN-CHEN CHANG see page 88.

CRYPTANALYSIS OF THE TSENG-JAN ANONYMOUS CONFERENCE KEY DISTRIBUTION SYSTEM WITHOUT USING A ONE-WAY HASH FUNCTION

Ting-Yi CHANG, Min-Shiang HWANG, and Wei-Pang YANG

Abstract: This paper mounts a conspiracy attack on the anonymous conference key distribution system without using a one-way hash function proposed by Tseng and Jan. The attack described in the article can reveal the participants' common key shared with the chairperson.

Keywords: Cryptography, Conference Key Distribution System, User Anonymity, One-way Hash Function, Discrete Logarithm.

A Conference Key Distribution System (CKDS) [1,2,3,4] guarantees that all and only the participants in a conference share a common conference key which can be used to hold a secure conference. In 1999, Tseng and Jan proposed two CKDSs with user anonymity based on the discrete logarithm problem.[5] One of their schemes requires a one-way hash function to hide the identity of the participants and to protect each participant's common key shared with the chairperson. The other scheme does not use a one-way hash function, but it can also achieve the same purposes. Tseng and Jan claim that both schemes are secure against the impersonation attack and the conspiracy attack. However, this paper will demonstrate that the claim made by Tseng and Jan,[6] that their scheme without using a one-way hash function is secure against conspiracy attack, is incorrect.

Brief Review of Tseng-Jan's Conference Key Distribution System

The conference key distribution scheme proposed by Tseng and Jan includes three stages:

- System set-up stage,
- Conference key distribution stage, and

- Conference key recovery stage.

During the system set-up stage, the system chooses two large primes p and q such that $q \mid (p-1)$ and generates g of order q in $GF(q)$. Then, the system assigns a secret key $x_i \in Z_q^*$ to user U_i over a secret channel and publishes the corresponding public key $y_i = g^{x_i} \bmod p$.

During the conference key distribution stage, U_c is appointed as a chairperson and $A = \{U_1, U_2, ..., U_n, n < m\}$ is the set of attending members. The chairperson U_c performs the following steps for distributing a conference key CK shared by the participants in the conference (A).

Step 1. Choose a random integer $r \in Z_q^*$ and get a time-sequence T from the system.

Step 2. Compute

$$R = g^r \bmod p$$
$$S = r + H(T \| R) \cdot x_c \bmod q$$

Here, $H(\cdot)$ denotes a one-way hash function and $\|$ denotes a concatenation.

Step 3. Compute the common secret key for each $U_i \in A$ as $k_{ci} = y_i^r \bmod p$.

Step 4. Randomly select a conference key $CK \in Z_q^*$ and construct a polynomial of degree n as

$$P(x) = \prod_{i=1}^{n} (x - k_{ci}) + CK \bmod p,$$
$$= x^n + c_{n-1}x^{n-1} + \cdots + c_0 \bmod p.$$

Step 5. Broadcast $\{R, S, T, c_{n-1}, c_{n-2}, \ldots, c_0\}$.

During the conference key recovery stage, each $U_i \in A$ receives $\{R, S, T, c_{n-1}, c_{n-2}, \ldots, c_0\}$ and performs the following steps for recovering the conference key CK.

Step 1. Verify T and the following equation

$$g^S = R \cdot y_c^{H(T\|R)} \bmod p .$$

Step 2. Compute the common secret key shared with U_c as $k_{ic} = R^{x_i} \bmod p$.

Step 3. Recover CK by computing

$$\begin{aligned} P(k_{ic}) &= (k_{ic})^n + c_{n-1}(k_{ic})^{n-1} + \cdots + c_1 k_{ic} + c_0 \bmod p \\ &= CK \bmod p. \end{aligned}$$

The Weakness of Tseng-Jan's Scheme

Tseng and Jan claim that their conference key distribution system is secure against the conspiracy attack. However, in this section, we will show that the participants' common secret key shared with the chairperson can be revealed with the conspiracy attack. Any $(n-1)$ attending members in A can conspire in order to reveal the remaining other member's common secret key shared with the chairperson.

For example, assume that $(n-1)$ attending members, U_i $(i = 1, 2, \ldots, n-1)$, intend to reveal the remaining other member U_n's common secret key k_{cn}. After substituting x with zero in Equation 1, we can obtain the equation:

$$\prod_{i=1}^{n-1} (-k_{ci}) \times (-k_{cn}) = c_0 - CK \bmod p .$$

Knowing the values c_0, CK and $\prod_{i=1}^{n-1}(-k_{ci})$, the common secret key k_{cn} can be computed. Thus, any $(n-1)$ attending members $U_1, U_2, ..., U_{n-1}$ can easily reveal U_n's common secret key k_{cn} shared with the chairperson U_c. Though k_{cn}, shared between U_c and U_n, is different at the next conference, if U_c and U_n use it to communicate with each other at this conference, $U_1, U_2, ..., U_{n-1}$ can eavesdrop confidential information exchanged between them.

Conclusion

In this article, the authors have shown that Tseng and Jan's claim that their conference key distribution system is secure against the conspiracy attack is wrong. Any $(n-1)$ attending members can conspire to reveal the remaining other member's common secret key shared with the chairperson.

Acknowledgment

This research was partially supported by the National Science Council, Taiwan, R.O.C., under contract no. NSC90-2213-E-324-004.

Notes:

[1] Shouichi Hirose and Katsuo Ikeda, "A Conference Distribution System for the Star Configuration Based on the Discrete Logarithm Problem," *Information Processing Letters* 62, no. 4 (May 1997): 189-192.

[2] Min-Shiang Hwang and Wei-Pang Yang, "Conference Key Distribution Protocols for Digital Mobile Communication Systems," *IEEE Journal on Selected Areas in Communications* 13, no. 2 (February 1995): 416-420.

[3] Ingemar Ingemarsson, Donald T. Tang, and C.K. Wong, "A Conference Key Distribution System," *IEEE Transactions on Information Theory* 28, no.5 (September 1982): 714-720.

[4] T.C. Wu, "Conference Key Distribution System with User Anonymity Based on Algebraic Approach," *IEE Proceedings – Computers and Digital Techniques* 144, no. 2 (March 1997): 145-148.

[5] Yuh-Min Tseng and Jinn-Ke Jan, "Anonymous Conference Key Distribution Systems Based on the Discrete Logarithm Problem," *Computer Communications* 22, no. 8 (1999): 749-754.

[6] Tseng and Jan, "Anonymous Conference Key Distribution Systems Based on the Discrete Logarithm Problem."

TING-YI CHANG received a B.S. degree in Information Management from Chaoyang University of Technology (CYUT), Taichung, Taiwan, Republic of China, in 2001, and a M.S. degree from the Department and Graduate Institute of Computer Science and Information Engineering of CYUT, in 2003. He is currently pursuing his Ph.D. in Computer and Information Science from the National Chiao Tung University, Taiwan, Republic of China. His current research interests include information security, cryptography, and mobile communications. *Address for correspondence:* Department of Computer and Information, National Chiao Tung University, 1001 Ta Hsueh Road, Hsinchu, Taiwan, R.O.C. *Email:* wpyang@cis.nctu.edu.tw.

MIN-SHIANG HWANG see page 20

WEI-PANG YANG was born on May 17, 1950 in Hualien, Taiwan, Republic of China. He received a B.S. degree in Mathematics from the National Taiwan Normal University in 1974, and a M.S. and a Ph.D. degrees from the National Chiao Tung University in 1979 and 1984, respectively, both in Computer Engineering. Since August 1979, he has been a member of the faculty of the Department of Computer Engineering at National Chiao Tung University, Hsinchu, Taiwan. In the academic year 1985-1986, he was awarded a National Postdoctoral Research Fellowship and was a visiting scholar at the Harvard University. From 1986 to 1987, he was Director of the Computer Center of the National Chiao Tung University. In August 1988, he joined the Department of Computer and Information Science at the National Chiao Tung University, and acted as Head of the Department for one year. Then, he joined IBM's Almaden Research Center in San Jose, California for another year as a visiting scientist. From 1990 to 1992, he was again Head of the Department of Computer and Information Science. His research interests include database theory, database security, object-oriented databases, image databases and Chinese database systems. Dr. Yang is a full professor and a member of IEEE, ACM, and the Tau Phi Society. He was the winner of the 1988 and 1992 Acer Long Term Award for Outstanding M.S. Thesis Supervision, and the winner of 1990 Outstanding Paper Award of the Computer Society of the Republic of China. He also obtained the 1991-1993 Outstanding Research Award of the National Science Council of the Republic of China. *Address for correspondence:* Department of Information Management, National Dong Hwa University, 1, Sec. 2, Da Hsueh Rd., Shou-Feng, Hualien, Taiwan, R.O.C. *Email:* wpyang@cis.nctu.edu.tw.

♦ I&S Internet Sources

I&S Monitor

.

E-GOVERNMENT AND SECURITY OF INFORMATION INTERNET SOURCES

E-GOVERNMENT AND SECURITY OF INFORMATION RELATED ORGANIZATIONS

E-GOVERNMENT RELATED ORGANIZATIONS

Institute for Electronic Government, IBM Corporation

http://www-1.ibm.com/industries/government/ieg/

Founded in 1994, the IEG focuses on issues including public policy as it relates to technology strategy and execution, economic development and education, online citizen and business services, and e-democracy. A collaborative network of related government and technology organizations, academics and other research institutions forms the backbone of the IEG.

The E-Gov Institute

http://www.e-gov.com/

E-Gov is an accomplished organization of marketing and education professionals who have worked with technology leaders from government and industry for more than twenty years. The E-Gov team produces events throughout the year and publishes the E-Gov Digest.

The Commonwealth Centre for Electronic Governance

http://www.electronicgov.net/

The Commonwealth Centre for e-Governance (CCEG) is a think tank operating under the auspices of an e-Governance program of the Commonwealth Secretariat in London, UK. CCEG is a legal entity incorporated in the United Kingdom and Canada

.

in November 2000. It operates on a global scale, with a board of Directors and Advisory Council from around the world. Members come from government, the private sector and civil society. The purpose of the Commonwealth Centre for e-Governance is to provide insight and knowledge on the changing nature of governments in the growing technology infrastructures. The CCEG is working to develop sets of best practices on how best to use technologies to implement the goals and objectives of public administration. It is the goal of CCEG to work with governments and international organizations to contribute to the growing knowledge base on e-Government, e-Governance and e-Democracy. Part of CCEG's mandate is to offer workshops and seminars in developing countries throughout the world on various aspects of e-Government. Much of the focus of CCEG will be on the multitude of information and administrative policies that will be needed as developing countries increasingly implement new technologies. The site features news and events, research papers, workshop reports, presentations.

E-Government – The World Bank Group

http://www1.worldbank.org/publicsector/egov/

This is the World Bank's e-Government website focusing on e-Government in developing countries. The site features case studies.

Digital Government Research Center

http://www.dgrc.org/

Digital Government Research Center is a joint research center of the Information Sciences Institute at the University of Southern California and the Department of Computer Science at Columbia University. The center conducts research on computer technologies towards generating and sharing knowledge for government agencies.

Center for Technology in Government

http://www.ctg.albany.edu/

The Center for Technology in Government (CTG) works with government to develop information strategies that foster innovation and enhance the quality and coordination of public services. It conducts applied research and partnership projects on the policy, management, and technology issues surrounding information use in the public sector. The results generated by each project add to a growing knowledge base designed to support the work of both government professionals and academic researchers. The site contains a toolbox with starter kits, executive briefings, and step-by-step guides.

Project output, research, demonstrations, publications and education programs are available on-line.

Public Technology Institute, Inc.

http://www.pti.org/

Public Technology Institute (PTI) is a U.S. non-profit technology research and development organization based in Washington, DC., representing local governments. The National League of Cities, the National Association of Counties, and the International City/County Management Association, three primary local government associations, provide PTI with its policy direction, while a select group of city and county members conduct applied R&D and technology transfer functions. The Institute's mission is to bring the benefits of technology to local governments. Membership in PTI is open to all local governments.

Kable

http://www.kablenet.com/

Kable helps suppliers to understand the government market better and to reach public sector decision-makers. The company also helps government organisations to research the context of policy-decisions and to promote official guidance or consultation. Kable offers a combination of subscription and bespoke research, online and print publications, and a series of conferences and exhibitions. The company also offers customised event, publishing and research services for both public and private sectors customers.

IDA

http://europa.eu.int/idabc/en/chapter/3

The IDA (interchange of data between administrations) mission is to support the implementation of Community policies and activities by co-ordinating the establishment of Trans-European telematic networks between administrations. As data needs to be exchanged throughout Europe, IDA also acts as an important vehicle for the re-engineering of the working processes of the administrations. The work within IDA is performed through several action lines:

- Promoting the implementation of sectoral networks in priority areas of work
- Developing interoperability measures, for use by sectoral networks
- Extending the benefits of the networks to Community industry and citizens

- Co-operating with national authorities and
- Co-operating with other EC services.

INFORMATION SECURITY RELATED ORGANIZATIONS AND RESEARCH INSTITUTIONS

Computer Security Institute

http://www.gocsi.com/

CSI is a leading membership organization specifically dedicated to serving and training the information, computer and network security professional. Since 1974, CSI has been providing education and aggressively advocating the critical importance of protecting information assets. CSI sponsors two conference and exhibitions each year: CSI NetSec in June; and the CSI Annual Computer Security Conference and Exhibition in November. CSI also offers a full schedule of training classes on encryption, intrusion management, Internet, firewalls, awareness, Windows and more.

International Association for Cryptologic Research (IACR)

http://www.iacr.org/

IACR is a non-profit scientific organization whose purpose is to further research in cryptology and related fields.

Information Security Forum (ISF)

http://www.securityforum.org/html/frameset.htm

ISF is a leading independent authority on information security. By harnessing world-renowned expertise and the collective knowledge and experience of its members—including 50% of Fortune 100 companies—the ISF delivers practical guidance and solutions to overcome wide- ranging security challenges impacting business information today.

Computer Security Group, Computer Laboratory, University of Cambridge

http://www.cl.cam.ac.uk/Research/Security/index.html

The Computer Security Group is an informal group of people with similar interests: mainly security, cryptology, and distributed systems. It holds meetings, seminars, and workshops. Computer security has been among the laboratory's research interests for many years, along with related topics such as cryptology, formal methods, medical

information security, electronic commerce, steganography and information hiding, and the robustness of distributed systems in general.

Computer Security Division, Information Technology Laboratory, National Institute of Science and Technology

http://csrc.nist.gov/

Computer Security Division's main focus areas are: Cryptographic Standards and Applications, Security Testing, Security Research/Emerging Technologies, and Security Management and Guidance.

Center for Education and Research in Information Assurance and Security (CERIAS) at Purdue University

http://ciac.llnl.gov/cstc/

CERIAS is currently viewed as one of the leading centers for research and education in areas of information security that are crucial to the protection of critical computing and communication infrastructure. CERIAS is quite unique in its multidisciplinary approach to the problems, ranging from purely technical issues (e.g., intrusion detection, network security, etc) to ethical, legal, educational, communicational, linguistic, and economic issues, and the subtle interactions and dependencies among them.

CSTC – Cyber Solutions Tools Center

http://ciac.llnl.gov/cstc/

CIAC's Cyber Solutions Tools Center (CSTC), located at the Lawrence Livermore National Laboratory, provides solutions to U.S. Government agencies facing today's security challenges in information technology. They maintain information protection core-competencies through high-tech, integrated INFOSEC incident response, product development, and consulting services. The CIAC is composed of three complementary business units: Operational Incident Response; Advanced Security Projects; and Secure Systems Services. The Operational Incident Response group assists the Department of Energy in its information protection efforts by providing computer security incident response related services. The CIAC is composed of security-cleared information security professionals with backgrounds in computer science, information systems, and engineering specializing in awareness, training, and education; Electronic Commerce security; electronic security assessment; firewall and web security; incident response; Internet and Intranet security; intrusion detection; malicious code detection and eradication; network security; policies and procedures; risk management; and system and software engineering.

E-GOVERNMENT AND SECURITY OF INFORMATION RELATED RESOURCES

E-GOVERNMENT RESOURCES

E-Government Observatory

http://europa.eu.int/idabc/en/chapter/140

The IDABC e-Government Observatory is a reference information tool on e-Government issues and developments across Europe. It provides the community of e-Government decision-makers and professionals with a unique set of information resources and with valuable insight into e-Government strategies, initiatives and projects in Europe and beyond.

The Victorian Government's Repository of over 27 000 e-Government Resources

http://www.egov.vic.gov.au/

The e-Government Resource Centre aggregates substantial knowledge as to how the Victorian Government is meeting the goals of providing e-Government services to citizens. It is a very dynamic site.

E-Government Resource Centre Canada

http://www.egov.vic.gov.au/International/TheAmericas/Canada/canada.htm

Downloads, Reports, Resources from the U.S. Federal Enterprise Architecture Program Management Office

http://www.feapmo.gov/fea_downloads.asp

The site provides links to files and information resources that the reader may download to gain a better understanding of the purpose, usage, and definition of the Federal Enterprise Architecture and associated reference models. These include standard text documents as well as files that one may download in XML format which contain the models of the Federal Enterprise Architecture. Data within the XML documents can be integrated into external datastores, data management systems or applications. As the Federal Reference Models evolve there will be subsequent releases of the Federal Enterprise Architecture in XML format. As new resources are created, the FEA-PMO will post these links to the "What's New" section on the FEA-

PMO homepage. These downloads have been organized by category of FEA-related information.

Piper Resources

http://www.statelocalgov.net/

State and Local Governments on the Web is a frequently updated directory of links to government sponsored and controlled resources on the Internet. It was created by Piper Resources, an Internet publishing firm, which has been providing the guide to the public for five years.

E-Government and e-Commerce Resources and Articles

http://www.mrsc.org/Subjects/InfoServ/egovresource.aspx

Asia-Pacific e-Government Portal

http://www.egovaspac.org/

UNPAN e-Government Theme

http://www.unpan.org/egovernment.asp

The site provides a very wide collection of presentations, links and resources, tools and papers.

International Telecommunication Union – e-Government

http://www.itu.int/osg/spu/wsis-themes/ict_stories/egovernment.html

Case studies on using information and communication technologies to bridge the digital divide.

SECURITY OF INFORMATION RESOURCES

Information Security Resource Centre

http://www.pnl.gov/isrc/

The Information Security Resource Capability (ISRC) is located at the Pacific Northwest National Laboratory (PNNL), in Richland, Washington. The ISRC provides support to the Department of Energy (DOE) Security Policy Staff in the Office of Security. The ISRC has served as a Center of Excellence for information security

issues for more than 12 years. The ISRC provides programmatic and technical support in the areas of Information Security, Facility Surveys and Approvals, Foreign Ownership, Control, or Influence, and maintains the DOE Incident Tracking and Analysis Capability (ITAC). These activities support the development of cost-effective, risk management-based security measures for incorporation into DOE Safeguards and Security Policies. The ISRC provides the DOE Security Policy Staff with expert technical assistance on critical Information Security matters across the DOE Complex, has developed effective Information Security training courses, provides subject matter expertise in policy planning and development, and provides an array of security technologies.

Research Resources on Authentication, Digital Signatures and PKI Issues

http://www.egov.vic.gov.au/Research/Authentication/authent.htm

Computer Security Resources from National Security Institute (NSI)

http://nsi.org/compsec.html

This web site features alerts and warnings, papers, programs, FAQs, government standards, mailing lists and newsgroups, computer security links, legislation, manager's guides, etc.

Computer Security Information

http://www.alw.nih.gov/Security/security.html

This page features general information about computer security. Information is organized by source and each section is organized by topic. The site includes FAQs, newsgroups, mailing lists, documents, programs, advisories, electronic magazines, newsletters, news sites, web sites, etc.

ITtoolbox Security

http://security.ittoolbox.com/

ITtoolbox Security offers forums for discussion, an integrated directory, daily news, and many other services geared towards security professionals and users of security products.

E-GOVERNMENT RELATED PROJECTS AND INITIATIVES

eEurope Awards

http://www.e-europeawards.org/

The eEurope Awards recognize innovative initiatives in the areas of e-Government and e-Health within Europe. The overall goal of the eEurope Awards is to promote best practice among the Member States of the enlarged European Union, the candidate countries as well as the EFTA countries. This will facilitate the sharing of experience and mutual learning from each other in order to meet the Lisbon targets and make Europe the most competitive knowledge-based economy by 2010.

The Official Web Site of the U.S. President's e-Government Initiative

http://www.whitehouse.gov/omb/egov/

"Secure e-Government" Project

http://www.bundonline2005.de

http://www.staat-modern.de

The "Secure e-Government" project interacts closely with the German government's BundOnline 2005 e-Government Initiative and the "Modern State – Modern Administration" program. Further information is available from the above sites.

New Zealand e-Government Programme Home Page

http://www.e-government.govt.nz/

3E Project at Harvard's Kennedy School of Government

http://www.ksg.harvard.edu/exec_ed/3e/

This is the homepage of the 3E Project at Harvard's Kennedy School of Government. The E-government Executive Education (3E) project at Harvard's John F. Kennedy School of Government is a collaborative effort among public- and private-sector organizations to inform and strengthen the leadership and cross-boundary relationships needed for 21st century government and governance. The project focuses on innovation through the use of information technologies. It offers services and content through a combination of traditional classroom interactions and network-enabled distance education.

Government Management Information Sciences (GMIS)

http://www.gmis.org/index.html

The purpose of GMIS is to provide a forum for the exchange of ideas, information, and techniques; to foster enhancement in hardware, software and communication developments as they relate to government activities.

Access e-Government – an Educational Program

http://www.access-egov.info/

The site is a starter kit for e-Government webmasters that shows local governments how to find resources and how to plan information-rich websites towards transact business and communicate with their citizens.

The National Science Foundation's Digital Government Research Program

http://www.diggov.org/

The Digital Government Program funds research at the intersection of computer information sciences and government information services, with the goal of bringing advanced information technology to the government information community. These Government/academic collaborations should contribute to government strategic planning for information services while providing interesting and unique new research problems and data sets for the academic research community. The site contains links to project demonstrations.

DigitalGovernance.org Initiative

http://216.197.119.113/artman/publish/index1.shtml

The site features models of digital governance, case studies, publications and events.

Global Business Dialogue on e-Commerce

http://www.gbde.org/egovernment/

This database contains projects, experiences and best practices on e-Government classified by region/country.