An IC-Card-Based and Flexible t-out-of-n Electronic Voting Mechanism

Chin-Chen Chang[1,*] and Ting-Fang Cheng[2]

[1]Department of Information Engineering and Computer Science
Feng Chia University
Taichung 407, Taiwan
ccc@cs.ccu.edu.tw

[2]Department of Computer Science
National Tsing-Hua University
Hsinchu, 30013, Taiwan
nthu.tiffany@gmail.com

Received 20 December 2008; Accepted 10 January 2009

Abstract. An electronic voting system must address essentials such as mobility, efficiency, verifiability, and robustness. Jan and Tai presented an electronic voting scheme using IC cards in 1997, and Chang and Lee proposed a *t*-out-of-*n* electronic voting protocol in 2006. According to their different traits of *t*-out-of-*n* and IC-card-based protocol, we consequently proposed a novel version to integrate these two protocols in this paper. By adopting IC cards, the authentication performance can be effectively promoted. The security of our scheme is based on symmetric and asymmetric cryptosystems. Our proposed scheme not only confirms most of the essentials of the general electronic voting scheme but also prevents potential malicious attacks. Furthermore, the computation overhead of the proposed scheme is less than that of the related methods.

Keywords: IC card, electronic voting, Citizen Digital Certificate, proxy server

References

[1] D. Chaum, "Blind Signature Systems," *Advances in Cryptology: Proceedings of Crypto'83*, New York, U.S.A., pp. 153, 1983.

[2] D. Chaum, "Blinding for Unanticipated Signatures," *Advances in Cryptology: Proceedings of EUROCRYPT'87*, Amsterdam, Netherlands, pp. 227-233, 1987.

[3] D. Chaum, "Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms," *Communications of the ACM*, Vol. 24, No. 2, pp. 84-88, 1981.

[4] D. Chaum, "Elections with Unconditional-Secret Ballots and Disruption Equivalent to Breaking RSA," *Advances in Cryptology: Proceedings of EUROCRYPT'87*, Davos, Switzerland, pp. 177-182, 1988.

[5] L. Cranor and R. Cytron, "Sensus: a Security-Conscious Electronic Polling System for the Internet," *Proceedings of the Thirtieth Hawaii International Conference on System Sciences*, Wailea, HI, U.S.A., Vol. 3, pp. 561-570, 1997.

[6] I. Damgard and M. Jurik, "A Generalization, a Simplification and Some Applications of Pailliers Probabilistic Public-Key System," *Proceedings of Public Key Cryptography*, Vol. 1992 of LNCS, pp. 119-136, 2001.

[7] A. Fujioka, T. Okamoto, and K. Ohta, "A Practical Secret Voting Scheme for Large Scale Elections," *Advances in Cryptology: Proceedings of ASIA CRYPT'92*, Gold Coast, Queensland, Australia, pp. 244-251, 1992.

[8] T. Elgamal, "A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms," *IEEE Transactions on Information Theory*, Vol. IT-31, No. 4, pp. 469-472, 1985.

[*] Correspondence author

[9] J.K. Jan and C.C. Tai, "A Secure Electronic Voting Protocol with IC Cards," *Journal of Systems and Software*, Vol. 39, pp. 93-101, 1997.

[10] C. Park, K. Itoh, K. Kurosawa, "Efficient Anonymous Channel and All/Nothing Election Scheme," *Advances in Cryptology: Proceedings of EUROCRYPT'93*, Lofthus, Norway, Vol. 765 of LNCS, pp. 248-259, 1994.

[11] K. Sako and J. Killian, "Receipt-Free Mix-Type Voting Scheme – a Practical Solution to the Implementation of a Voting Booth," *Advances in Cryptology: Proceedings of EUROCRYPT'95*, Berlin, Germany, Vol. 921 of LNCS, pp. 393-403, 1995.

[12] J. Benaloh, *Verifiable Secret-Ballot Elections, Ph.D. dissertation*, Yale University, Department of Computer Science, YALEU/CDS/TR-561, 1987.

[13] R. Cramer, R. Gennaro, and B. Schoenmakers, "A Secure and Optimal Efficient Multi-Authority Election Scheme," *Advances in Cryptology: Proceedings of EUROCRYPT'97*, Konstanz, Germany, Vol. 1233, pp. 103-118, 1997.

[14] I. Damgard, J. Groth, and G. Salomonsen, "The Theory and Implementation of an Electronic Voting System," *Advances in Information Security*, Vol. 7, pp. 77-100, 2003.

[15] C.C. Chang and J.S. Lee, "An Anonymous and Flexible *t*-out-of-*n* Electronic Voting scheme," *Journal of Discrete Mathematical Sciences & Cryptography*, Vol. 9, No. 1, pp. 133-151, 2006.

[16] C.C. Chang and J.S. Lee, "An Anonymous Voting Mechanism Based on the Key Exchange Protocol," *Computers & Security*, Vol. 25, pp. 307-314, 2006.

[17] J.J. Hwang, "A Conventional Approach to Secret Balloting in Computer Networks," *Computers & Security*, Vol. 15, No. 3, pp. 249-262, 1996.

[18] J.K. Jan, Y.Y. Chen, and Y. Lin, "The Design of Protocol for e-Voting on the Internet," *Proceedings of IEEE International Carnahan Conference on Security Technology*, London, England, pp. 180-189, 2001.

[19] W.S. Juang and C.L. Lei, "A Collision-Free Secret Ballot Protocol for Computerized General Elections," *Computers & Security*, Vol. 15, No. 4, pp. 339-348, 1996.

[20] H.T. Liaw, "A Secure Electronic Voting Protocol for General Elections," *Computers& Security*, Vol. 23, pp. 107-119, 2004.

[21] Y.Y. Chen, J.K. Jan, and C.L. Chen, "The Design of a Secure Anonymous Internet Voting System," *Computers & Security*, Vol. 23, No. 4, pp. 330-337, 2004.

[22] G. Dini, "A Secure and Available Electronic Voting Service for a Large-Scale Distribution System," *Future Generation Computer Systems*, Vol. 19, pp. 69-85, 2003.

[23] J.K. Jan and R.H. Lin, "A Secure Anonymous Voting by Employing Diffie-Hellman PKD Concept," *Proceedings of IEEE International Carnahan Conference on Security Technology*, Surrey, England, pp. 252-258, 1995.

[24] W.S. Juang and C.L. Lei, "A Secure and Practical Electronic Voting Scheme for Real World Environments," *IEICE Transactions on Fundamentals on Communications, Electronics, Information and Systems*, Vol. E80-A, No. 1, pp. 64-71, 1997.

[25] I.C. Lin, M.S. Hwang, and C.C. Chang, "Security Enhancement for Anonymous Secure e-Voting over a Network," *Computer Standards & Interfaces*, Vol. 25, No. 2, pp. 131-139, 2003.

[26] A. Zwierko and Z. Kotulski, "A Light-Weight e-Voting System with Distributed Trust," *Electronic Notes in Theoretical Computer Science*, Vol. 168, pp. 109-126, 2007.

[27] W. Rankl and W. Effing, *Smart Card Handbook*, John Wiley and Sons, 2nd Edition, 2000.

[28] C.T. Li, M.S. Hwang, and C.Y. Liu, "An Electronic Voting Protocol with Deniable Authentication for Mobile Ad Hoc Networks," *Computer Communications*, Vol. 31, No. 10, pp. 2534-2540, 2008.

[29] F. Rodríguez-Henríquez, D. Ortiz-Arroyo, and C. García-Zamora, "Yet Another Improvement over the Mu-Varadharajan e-Voting Protocol," *Computer Standards & Interfaces*, Vol. 29, No. 4, pp. 471-480, 2007.

[30] B. Schneier, *Applied Cryptography*, 2nd Edition, John Wiley and Sons, New York, U.S.A., 1996.

[31] Bruce Schneier, *Applied Cryptography, Protocols, Algorithms, and Source Code in C*, John Wiley and Sons Inc., 2nd Edition, New York, U.S.A., pp. 15, 1996.