A Scheme of Image-based Signature Verification upon Secret Sharing for Shopping in E-commerce Systems

Shiuh-Jeng Wang[1,*], Yuh-Ren Tsai[2], Pin-You Chen[2], and Chien-Chih Shen[2]

[1] Department of Information Management
Central Police University
Taoyuan, Taiwan 333
sjwang@mail.cpu.edu.tw

[2] Institute of Communications Engineering
National Tsing Hua University
Hsinchu, Taiwan 300

Received June 15 2009; Revised 10 July 2009; Accepted 15 July 2009

Abstract. Secret sharing protects a secret by distributing it to a group of participants/ nodes. The shared data, called shadows, are held by the nodes, and only certain authorized groups of nodes can reconstruct the secret from the shadows. In the (k, n) threshold secret sharing scheme, the secret is shared with n nodes, and more than k-1 nodes can collaborate to reconstruct the secret. There are many evolutions which involve threshold secret sharing, for examples, the proactive scheme, which periodically updates the shadows, and the mobile scheme, which can arbitrarily change the number of the nodes and the threshold. The size of the shadow is also an issue of interest: the sizes of the shadows which are held by a node are bigger, smaller than or equivalent to the secret. However, some schemes which have the size of the shadow smaller than the size of the secret do not have these advanced features. In this paper, we utilize polynomials and matrices to construct a new scheme, in which it not only has the property of having the size of the shadow smaller than the size of the secret, but also achieves proactive property. We apply furthermore the secret sharing to the verification systems when shopping to merchants for e-commerce.

Key words: Verification, secret sharing, projection matrix, linear independent, proactive, payments

References

[1] L. Bai, "A Strong Ramp Secret Sharing Scheme Using Matrix Projection," in *Proceedings of the 2006 International Symposium on World of Wireless, Mobile and Multimedia Networks*, pp. 652-656, 2006

[2] L. Bai, "A Reliable (k, n) Image Secret Sharing Scheme," *The 2nd IEEE International Symposium on Dependable, Autonomic and Secure Computing*, pp. 31-36, 2006

[3] G. Blakley, "Safeguarding Cryptographic Keys," in *Proceedings of the AFIPS 1979 National Computer Conference*, Vol.48, Arlington, VA, pp. 313-317 (1979)

[4] P. Feldman, "A practical Scheme for Non-interactive Verifiable Secret Sharing," in *Proceedings of the 28th IEEE Symposium on Foundations of Computer Science*, pp. 427-437, 1987

[5] A. Herzberg, S. Jarecki, H. Krawczyk, M. Yung, "Proactive Secret Sharing, or How to Cope with Perpetual Leakage," in *Proceedings of the 15th Annual International Cryptology Conference on Advances in Cryptology*, pp. 339-352, August 27-31, 1995

[6] T. P. Pederson, "Non-interactive and Information- Theoretic Secure Verifiable Secret Sharing," *Advances in Cryptology*, pp. 129-140, 1991

[7] A. Shamir, "How to Share a Secret," *Communications of the ACM*, Vol. 22, No.11, pp. 612-613, 1979

[8] C. C. Thien and J. C. Lin, "Secret Image Sharing," *Computers & Graphics*, Vol. 26, No. 5, pp. 765–770, 2002

[*] Correspondence author