

Dynamic Password Authentication Scheme for Multi-server Environments

王興翰、曹偉駿

E-mail: 9806264@mail.dyu.edu.tw

ABSTRACT

Recently, as the technology of Internet spread fast, all users have emphasized on information security issues. Thus, more and more security schemes have been developed and applied in various environments, in order to effectively ensure that the information can be securely transmitted via the network environments. Moreover, most of these schemes must satisfy at least two security requirements, including user authentication and data confidentiality. To do so, we use password-based mechanisms because they are popular with users, cost-efficient, easy to use. However, if current schemes are used in multi-server environments, then authentication messages must be stored in the server side, which are easily vulnerable to a variety of attacks. Most of approaches employ the public key cryptography or one-way hash function with smart card to solve this problem. Unfortunately, these approaches don't mention how to effectively add a new server to the system to provide service. Therefore, we propose a smart card based dynamic multi-server password authentication scheme using Bilinear Pairing and Newton interpolating polynomial, which has characteristics of high efficiency and security. Specially, we affirm that our proposed scheme will be able to save lots of costs when a new server is added and deleted.

Keywords : multi-server、 bilinear pairing、 password authentication、 smart card

Table of Contents

中文摘要	iii
英文摘要	iv
誌謝詞	v
內容目錄	vi
表目錄	vii
圖目錄	viii
第一章 緒論	1
第一節 研究背景	1
第二節 研究動機與目的	2
第三節 研究限制	2
第四節 研究流程	3
第五節 論文架構	5
第二章 文獻探討	6
第一節 雙線性配對	6
第二節 牛頓內插法	9
第三節 適用多伺服器密碼認證方法	10
第四節 小結	19
第三章 建構新型之多伺服器密碼認證機制	20
第四章 安全性與效能分析	28
第一節 安全性分析	28
第二節 效能分析	
第五章 結論與未來展望	32
38	
參考文獻	40

REFERENCES

- Boneh, D., & Franklin, M. (2001). Identity-based encryption from the weil pairing. *Crypto 2001*, LNCS , 2139, 213-229. Boneh, D., Lynn, B., & Shacham, H. (2001). Short signatures from the Weil pairing. *Crypto 2001 LNCS*, 17(4), 297-319. Chang, C. C., & Hwang, S. J. (1993). Using smart

cards to authenticate remote passwords. *Computers and Mathematics with Applications*, 26(7), 19-27.

Chang, C. C., & Wu, T. C. (1995). Remote scheme for password authentication based on theory of quadratic residues. *Computer Communications*, 936 – 942.

Chang, C. C. & Lee, S. J. (2004). An efficient and secure multi-server password authentication scheme using smart cards. *Proceedings of the 2004 International Conference on Cyberworlds* (pp. 417-422).

Du, H., & Wen, Q. (2009). Efficient and provably-secure certificateless short signature scheme from bilinear pairings. *Computer Standards & Interfaces*, 31(2), 390-394.

Galbraith, S. (2001). Supersingular curves in cryptography. *Proc. Of Asiacrypt' 01*, LNCS (pp. 495-513).

Galbraith, S. D., Paterson, K. G., & Smart, N. P. (2008). Pairings for cryptographers. *Discrete Applied Mathematics*. 156(1), 3113-3121.

Geng, J., & Zhang, L. (2008). A dynamic ID-based user authentication and key agreement scheme for multi-server environment using bilinear pairings. *Workshop on Power Electronics and Intelligent Transportation System*, 35(1), 33-37.

Hsiang, H. C., & Shih, W. K. (2009). Improvement of the secure dynamic ID based remote user authentication scheme for multi-server environment. *Computer Standards & Interfaces*, doi:10.1016/j.csi.2008.11.002.

Hwang, R. J., & Shiau, S. H. (2007). Provably efficient authenticated key agreement protocol for multi-servers. *The Computer Journal Advance Access published*, 50(5), 602-615.

Joux, A. (2002). The weil and tate pairings as building blocks for public key cryptosystems. LNCS (pp. 20-32).

Juang, W. S. (2004). Efficient multi-server password authenticated key agreement using smart cards. *IEEE Transactions on Consumer Electronics*, 50(1), 251-255.

Lee, N. Y., Wu, C. N., & Wang, C. C. (2008). Authenticated multiple key exchange protocols based on elliptic curves and bilinear pairings. *Computers and Electrical Engineering*, 34(1), 12-20.

Li, L., Lin, I., & Hwang, M. (2001). A remote password authentication scheme for multi-server architecture using neural networks. *IEEE Trans*, (pp. 1498-1504). *Neural Netw.*

Liao, Y. P., & Wang, S. S. (2009). A secure dynamic ID based remote user authentication scheme for multi-server environment. *Computer Standards & Interfaces*, 24-29.

Lin, I. C., Hwang, M. S., & Li, L. H. (2003). A new remote user authentication scheme for multi-server architecture. *Future Generation Computer Systems*, 13-22.

Menezes, A., Okamoto, T., & Vanstone, S. (1993). Reducing elliptic curve logarithms to logarithms in a finite field. *IEEE Transaction on Information Theory*, 1639-1646.

Menkus, B. (1989). Understanding the use of passwords. *Computer sand Security* 7, 132-136.

Mills, D. J. (1991). Internet time synchronization: The network time protocol, *IEEE Transactions on Communications*, 39(10), 1484-1493.

Mohammed, E., Emarah, A. E., & El-Shennawy, K. (2001). Elliptic curve cryptosystems on smart cards. 2001 IEEE 35th International Carnahan Conference, (pp. 213-222).

Paterson, K. G. (2002). ID-Based signatures from pairings on elliptic curves. *Electronics Letters*, pp. 1025-1026.

Pfleeger, C. P. (1997). *Security in computing*. (2nd edition), PrenticeHall. NJ.

Purdy, P. G. (1974). A high security login procedure. *Communications of the ACM* 17, (pp. 442-445).

Sauer, T. (2005). *Numerical Analysis*. Addison-Wesley.

Scott, M. N. Costigan & Abdulwahab, W. (2006). Implementing cryptographic pairings on smartcards. In *Cryptology ePrint Archive*. Available: <http://eprint.iacr.org/2006/144.pdf>

Smart, N. P. (2002). Identity-based authenticated key agreement protocol based on Weil pairing. *Electronic Letters*, 38(13), 630-632.

Tsaur, W. J. (2005). Several security schemes constructed using ECC-based self-certified public key cryptosystems. *Applied Mathematics and Computation*, 168(10), 447-464.

Tsaur, W. J., Wu, C. C., & Lee, W. B. (2004). A smart card-based remote scheme for password authentication in multi-server Internet services. *Computer Standards & Interfaces*, 27(4), 39-51.

Tseng, Y. M., Wu, T. Y., & Wu, J. D. (2008). A Pairing-based user authentication scheme for wireless clients with smart cards. *Institute of Mathematics and Informatics, Vilnius*, 19(2), 285-302.

Tsuar, W. J., Wu, C. C., & Lee, W. B. (2001). A flexible user authentication for multi-server internet services. *Networking-JCN2001* LNCS, (pp. 174-183).

Wang, S. B., Cao, Z., Raymond Choo, K. K., & Wang, L. (2009). An improved identity-based key agreement protocol and its security proof. *Information Sciences*, 179(30), 307-318.