## A Study of Proxy Signature Scheme based on the Elliptic Curve Cryptosystem

鍾玉芳、陳澤雄;余心淳

E-mail: 9225033@mail.dyu.edu.tw

## **ABSTRACT**

The technology of communication in the Internet changes with each passing day, it generalizes the interchanged phenomenon of on-line transaction and communication. Most probable the electronic commerce will be the current of business transaction activity in the future. Therefore, the importance of information security obviously becomes outstanding. In the current research of network security, a public-key cryptosystem is regarded as broadly approved. The implement of a public-key cryptosystem depends on the digital-signature technique. It is because that the digital-signature function can achieve a trusted Certification Authority (CA) in constructing a public key infrastructure. Along with the change in the general situations, the study correlated to the digital signature changes as well. The applications of digital signature can be extended to be various, including the proposed research of proxy signature in the thesis. The characteristic and function of the proxy-signature technique enable to solve the blind spots of digital signature in practice; accordingly, it is worthy for developing. The so-called proxy signature means that an original signer authorizes a proxy signer to sign messages on his/her behalf through some certain procedures. Being authorized, the proxy signer uses the authorized data to sign messages. Then, the side of receipt checks the validity of the received signatory messages by validating the proxy signature and the authorized data. Consequently, while the original signer disables to exercise authority for signing, then he enables to authorize the proxy signer on his/her behalf using the proxy signature scheme. Following the way, the possible loss from the delay of timing can be avoided for promoting the efficiency of performance. The related applications of proxy signature can be also devoted to the secure mobile agent, self-proxy signature, electronic-cash, and anonymous electronic-vote researches. Expectedly, the potential of proxy signature still needs to be further developed. The elliptic curve cryptosystem brings about shortening the key length and signature size, so that the required storage for the system parameters can be greatly lowered down. Accordingly, the elliptic curve cryptosystem is used in developing the proposed schemes. Since the thesis stresses the design on both security and efficiency at the same time, the proposals are based on an overall induction toward the related literature with the basic concepts. In summary, the proposals reach concrete and visible practicability in accord with the requirements of a proxy signature scheme.

Keywords: Cryptosystem; Digital Signature; Proxy Signature; Electronic Commerce Security

## **Table of Contents**

日 銶 封囬闪貝 僉名貝 按	性青 1	Ⅲ 授催書 2	Ⅳ 中义掲	
<b>要</b> 女	v 英文摘要	vii 誌謝	ix 目	
錄	x 圖目錄	xiii 表目錄	xiv	
Chapter 1 Introduction 01	1.1 Background and Motivation of t	he Research 01 1.2 Application	n of Public-Key	
Cryptosystem 04 1	.3 History of Proxy-Signature Resea	arch 05 1.4 Main Axes of th	ne Thesis08	3
1.4.1 Proxy-unprotected Pr	oxy Signature 08 1.4.2 Pr	oxy-protected Proxy Signature	09 1.5 Organization of	
the Thesis	09 Chapter 2 Elliptic Curve Cryptog	graphy11 2.1 Introductio	n to Elliptic Curve	
Cryptography 11 2.2	Theories of an Elliptic Curve	13 2.2.1 Definition of an Ellip	otic Curve 13 2.2.2	2
Elliptic Curve Additive Op	eration 14 2.2.3 Elliptic C	curve Multiplicative Operation	17 2.3 Elliptic Curve Discrete	Э
Logarithm Problem	18 Chapter 3 Application of Proxy-u	unprotected Proxy Multisignature Sch	neme 20	1
3.1 Background of Proxy-u	nprotected Proxy Multisignature Sch	neme 2	20 3.2 Related Work of	
Proxy-unprotected Proxy N	Multisignature Scheme of Sun	21 3.3 The Prop	osed Elliptic Curve	
Proxy-unprotected Proxy N	/Iultisignature Scheme	23 3.3.1 Initialization Proced	lure of the Elliptic Curve	
Cryptosystem	23 3.3.2 Procedures o	f Authorization, delegation, and		
	·	on of Proxy-protected Proxy Multisign		
		roxy-protected Proxy Multisignature		
		Proxy-protected Proxy Multisignatur		
	· · · · · · · · · · · · · · · · · · ·	rve Proxy-protected Proxy Multisign		
Scheme	31 4.3.1 Initialization Procedure	of the Elliptic Curve Cryptosystem	31	
4.3.2 Procedures of Author	ization, delegation, and Verification.	31 Chapt	er 5 Analyses of Performance	

and Security Concerns. 35 5.1	Analyses of Performance	35 5.2 Security Co	ncerns	41 5.2.1
Security Caused by Elliptic Cu	rve Discrete Logarithm Problem	41 5	2.2 Public Key Substitution	า
Attack 42 5.2.3 Se	election of the Elliptic Curve	43 5.3 Discussions on	Resultant Performance and	l Security
44 Chapter 6 Conclusions	46 6.1 Contribution	on of the Proposals	46 6.2 Perspective o	f
Proxy-Signature Research	47 Reference s	48		

## REFERENCES

References [1] B. C. Neuman, Proxy-based Authorization and Accounting for Distributed Systems, " Proc. 13th International Conference on Distributed Systems," 1993, pp.283-29157.

- [2] M. Mambo, K. Usuda, and E. Okamoto, Proxy Signatures for Delegation Signing Operation, "Proc. Third ACM Conf. on Computer and Communications Security," 1996, pp.48-57.
- [3] M. Mambo, K. Usuda, and E. Okamoto, Proxy Signatures: Delegation of the Power to Sign Messages, "IEICE Trans. Fundamentals," Vol.E79-A, No.9, Sep. 1996, pp.1338-1353.
- [4] S. Kim, S. Park, and D. Won, Proxy Signatures, Revisited, "ICICS'97, Lecture Notes in Computer Science 1334," Springer-Verlag, 1997, pp.223-232.
- [5] N. Y. Lee, T. Hwang, and C. H. Wang, On Zhang 's Nonrepudiable Proxy Signature Schemes, "Third Australasian Conference of ACISP '98," 1998, pp.415-422.
- [6] H. M. Sun, On Proxy (Multi-) Signature Schemes, "Proceedings of the International Computer Symposium," 2000, pp.65-72.
- [7] H. M. Sun and B. T. Hsieh, Remarks on two Nonrepudiable Proxy Signature Schemes, "Ninth National Conference on Information Security, "Taiwan, 1999, pp.241-246.
- [8] H. M. Sun, N. Y. Lee, and T. Hwang, Threshold Proxy Signatures, "IEE Proceedings Computers and Digital Techniques," Vol.146, No.5, 1999, pp.259-263.
- [9] S. M. Yen, C. P. Hung, and Y. Y. Lee, Remarks on Some Proxy Signature Schemes, "Proceedings of the International Computer Symposium, 2000, pp.54-59.
- [10] L. Yi, G. Bi and G. Xiao, Proxy Multi-signature Scheme: A New Type of Proxy Signature, "Electronics Letters," 2000, Vol.36, No.6, pp.527-528.
- [11] K. Zhang, Threshold Proxy Signature Schemes, "1997 Information Security Workshop," Japan, Sep. 1997, pp.191-199.
- [12] Sun, H. M., Lee, N. Y., and Hwang T., Nonrepudiable Threshold Proxy Signatures, "Proceedings of the Ninth National Conference on Information Security," 1999, pp. 254-261.
- [13] Sun, H. M., An Efficient Nonrepudiable Threshold Proxy Signature Scheme with Known Signers, "Computer Communications," Vol.22, No.8, 1999, pp.717-722.
- [14] Hsu C. L., Wu T. S., and Wu T. C., New Nonrepudiable Threshold Proxy Signature Scheme with Known Signers, "Journal of Systems and Software," 2001, Vol.58, No.2, pp.119-124.
- [15] Hsu C. L., Wu T. S., and Wu T. C., Improvement of Threshold Proxy Signature Scheme, accepted by "Applied Mathematics and Computation," 2001.
- [16] Hsu C. L., Wu T. S., and Wu T. C., Efficient Proxy Signature Schemes Using Self-certified Public Keys, submitted to "IEE Proceedings Computers and Techniques," 2001.
- [17] Okamoto T., Tada M., and Okamoto E., Extended Proxy Signatures for Smart Cards, "Workshop on Information Security ISW'99, Springer-Verlag," 1999, pp.247-258.
- [18] Sun H. M., Convertible Proxy Signature Scheme, "National Computer Symposium," 1999, pp.186-189.
- [19] Viswanathan K., Boyd C., and Dawson E., Publicly Verifiable Key Escrow with Limited Time Span, "Proceedings of the Fourth Australasian Conference on Information Security and Privacy ACISP, '99," Springer-Verlag, pp.36-50.
- [20] Hsu C. L., Wu T. S., He W. H., and Wu T. C., Efficient Proxy Multisignature Schemes, submitted to "Computer Systems Science and Engineering," 2000.
- [21] Itakura K. and Nakamura K., A Public-key Cryptosystem Suitable for Digital Multisignatures, "NEC Research and Development," Vol.71, 1983, pp.1-8.
- [22] Boyd C., Digital Multisignature, "Proceedings of Conference on Coding and Cryptography," 1986, pp. 15-17.
- [23] Okamoto T., A Digital Multisignature Scheme Using Bijective Public-key Cryptosystem, "ACM Transactions on Computer Systems," Vol.6, No.8, 1988, pp.432-441.
- [24] Harn L. and Kiesler T., New Scheme for Digital Multisignature, "Electronics Letters," Vol.25, No.15, 1989, pp.1002-1003.
- [25] Boyd C., Multisignatures based on Zero-knowledge Schemes, "Electronics Letters," Vol.27, No.22, 1991, pp.2002-2004.
- [26] Ohta K. and Okamoto T., A Digital Multisignature Scheme based on the Fiat-Shamir Scheme, "Advances in Cryptology

- ASIACRYPT'91, "Springer-Verlag, pp.139-148.
- [27] Harn L., Group-oriented (t, n) Threshold Digital Signature Scheme and Digital Multisignature, "IEE Proceedings Computer and Digital Techniques," Vol.141, No.5, 1994, pp.307-313.
- [28] Park S., Kim K., and Won D., Two Efficient RSA Multisignature Schemes, "Proceedings of the First International Conference on Information and Communications Security ICICS'97," 1997, pp.217-222.
- [29] Chang C. C., Leu J. J., Haung P. C., and Lee W. B., A Scheme for Obtaining a Message from the Digital Multisignature, "Workshop on Practice and Theory in Public Key Cryptography PKC' 98," Springer-Verlag, 1998, pp.154-163.
- [30] Harn L., Digital Multisignature with Distinguished Signing Authorities, "Electronics Letters," Vol.35, No.4, 1999, pp.294-295.
- [31] Lee N. Y., Hwang T., and Wang C. H., The security of two ID-based Multisignature Protocols for Sequential and Broadcasting Architectures, "Information Processing Letters," Vol.70, No.2, 1999, pp.79-81.
- [32] Harn L. and Yang S., Group-Oriented Undeniable Signature Schemes without the Assistance of a Mutually Trusted Party, "Advances in Cryptology AUSCRYPT, 92," Springer-Verlag, 1993, pp.133-142.
- [33] Li C. M., Hwang T., and Lee N. Y., Remark on the Threshold RSA Signature Scheme, "Advances in Cryptology CRYPTO' 93," Springer-Verlag, 1993, pp.413-419.
- [34] [LHL94] Li C. M., Hwang T., and Lee N. Y., Threshold-multisignature Schemes Where Suspected Forgery Implies Traceability of Adversarial Shareholders, "Advances in Cryptology EUROCRYPT' 94," Springer-Verlag, 1994, pp.194-203.
- [35] Langford S. K., Threshold DSS Signature without a Trusted Party, "Advances in Cryptology CRYPTO' 95," Springer-Verlag, 1995, pp.397-409.
- [36] Gennaro R., Jarecki S., Krawczyk H., and Rabin T., Robust Threshold DSS Signatures, "Advances in Cryptology EUROCRYPT '96," Springer-Verlag, 1996, pp.354-371.
- [37] Park C. and Kurosawa K., New ElGamal Type Threshold Digital Signature Scheme, "IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, Vol.E79-A, No.1, 1996, pp.86-93.
- [38] Wang C. T., Lin, C. H., and Chang C. C., Threshold Signature Schemes with Traceable Signers in Group Communications, "Computer Communications," Vol.21, No.8, 1998, pp.771-776.
- [39] Lee W. B. and Chang C. C., (t, n) threshold Digital Signature with Traceability Property, "Journal of Information Science and Engineering, "Vol.15, No.5, 1999, pp.669-678.
- [40] A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone, "Handbook of Applied Cryptography," CRC Press, Boca Raton, Florida, 1997.
- [41] N. Koblitz, Elliptic Curve Cryptosystems, "Mathematics of Computation," Vol.48, 1987, pp.203-209.
- [42] V. S. Miller, Uses of Elliptic Curves in Cryptography, "Advances in Cryptology Crypto' 85: Lecture Notes in Compute Science, New York, Springer-Verlag, No.218, 1985, pp.417-426.
- [43] N. Koblitz, "A Course in Number Theory and Cryptography," New York, Springer-Verlag, Second edition, 1994.
- [44] N. Koblitz, A. Menezes, and S. Vanstone, The State of Elliptic Curve Cryptography, "Designs, Codes and Cryptography," Vol.19, 2000, pp.173-193.
- [45] A. Menezes, T. Okamoto, and S. Vanstone, Reducing Elliptic Curve Logarithms to Logarithms in a Finite Field, "IEEE Transactions on Information Theory," Vol.39, 1993, pp.1639-1646.
- [46] N. Torii and K. Yokoyama, Elliptic Curve Cryptosystem, "FUJITSU Sci. Tech. J.," 36, 2, 2000, pp.140-146.
- [47] J. Guajardo and C. Paar, Efficient Algorithms for Elliptic Curve Cryptosystems, "Advances in Cryptology Crypto'97: Lecture Notes in Compute Science," Springer-Verlag, No.1294, 1997, pp.342-356.
- [48] G. Agnew, R. Mullin, and S. Vanstone, An Implementation of Elliptic Curve Cryptosystems over, "IEEE Journal on Selected Areas in Communications," Vol.11, 1993, pp.804-813.
- [49] J. Pollard, Monte Carlo Methods for Index Computation Mod p, "Mathematics of Computation," Vol.32, 1978, pp.918-924.
- [50] T. Satoh and K. Araki, Fermat Quotients and the Polynomial Time Discrete Log Algorithm for Anomalous Elliptic Curves, "Commentarii Mathematici Universitatis Sancti Pauli," Vol.47, 1998, pp.81-92.
- [51] I. Semaev, Evaluation of Discrete Logarithms in a Group of p-Torsion Points of an Elliptic Curve in Characteristic p, "Mathematics of Computation," Vol.67, 1998, pp.353-356.
- [52] IEEE P1363: Standard Specifications For Public Key Cryptography, http://grouper.ieee.org/groups/1363/.