4.3.2 Procedures of Authorization, delegation, and Verification

4.3.1 Initialization Procedure of the Elliptic Curve Cryptosystem

Chapter 5 Analyses of Performance Scheme

4.2 Related Work of Proxy-protected Proxy Multisignature Scheme

4.1 Background of Proxy-protected Proxy Multisignature Verification

Chapter 4 Application of Proxy-protected Proxy Multisignature Cryptosystem

3.3.2 Procedures of Authorization, delegation, and Proxy-unprotected Proxy Multisignature Scheme

3.3.1 Initialization Procedure of the Elliptic Curve Proxy-unprotected Proxy Multisignature Scheme of Sun

3.3 The Proposed Elliptic Curve

3.2 Related Work of Proxy-unprotected Proxy Multisignature Scheme

3.1 Background of Proxy-unprotected Proxy Multisignature Scheme

Chapter 3 Application of Proxy-unprotected Proxy Multisignature Scheme

3.3.2 Procedures of Authorization, delegation, and

3.2 Related Work of

3.1 Background of

Chapter 2 Elliptic Curve Cryptography

2.2.3 Elliptic Curve Multiplicative Operation

2.3 Elliptic Curve Discrete Cryptography

2.2 Theories of an Elliptic Curve

2.2.1 Definition of an Elliptic Curve

2.1 Introduction to Elliptic Curve

1.4.1 Proxy-unprotected Proxy Signature

1.4.2 Proxy-protected Proxy Signature

1.5 Organization of Cryptosystem

1.3 History of Proxy-Signature Research

1.2 Application of Public-Key

1.1 Background and Motivation of the Research

Chapter 1 Introduction

1.4.1 Proxy-unprotected Proxy Signature

1.4.2 Proxy-protected Proxy Signature

1.5 Organization of Cryptosystem

1.3 History of Proxy-Signature Research

1.2 Application of Public-Key

1.1 Background and Motivation of the Research

Chapter 1 Introduction

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

The proposed schemes are based on the elliptic curve cryptosystem. 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 order to achieve a balance between the security and signature size, so that the required storage for the system parameters can be greatly lowered down. Accordingly, the potential of proxy signature still needs to be further developed. The elliptic curve cryptosystem brings about shortening the key length and signature size, which makes the system parameters be shorter. The delay of timing can be avoided for promoting the efficiency of performance. The related applications of proxy signature can be expectedly also devoted to the secure mobile agent, self-proxy signature, electronic-cash, and anonymous electronic-vote researches. Expectedly, 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 signature in practice; accordingly, it is worthy for developing. 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 signature in practice; accordingly, it is worthy for developing.

The technology of communication in the Internet changes with each passing day, it generalizes the interchanged phenomenon of on-line transaction and communication. Most probably 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 the current research. The study correlated to the digital signature is integrally considered to be the core of the network security. Along with the change in the general situations, the study correlated to the digital signature is integrally considered to be the core of the network security. The digital-signature technique is of the basic security and key tune in the current research of network security.
Chapter 5 Performance and Security Concerns

5.1 Analyses of Performance............................. 35
5.2 Security Concerns................................... 41

5.2.1 Security Caused by Elliptic Curve Discrete Logarithm Problem....................................... 41
5.2.2 Public Key Substitution.................... 42
5.2.3 Selection of the Elliptic Curve................... 43

5.3 Discussions on Resultant Performance and Security... 44

Chapter 6 Conclusions................................... 46

6.1 Contribution of the Proposals....................... 46
6.2 Perspective of Proxy-Signature Research............. 47

References............................................. 48

REFERENCES

References
[26] Ohta K. and Okamoto T., A Digital Multisignature Scheme based on the Fiat-Shamir Scheme, "Advances in Cryptology
[27] Harn L., Group-oriented (t, n) Threshold Digital Signature Scheme and Digital Multisignature, "IEE Proceedings─Computer and Digital


[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


[31] Lee N. Y., Hwang T., and Wang C. H., The security of two ID-based Multisignature Protocols for Sequential and Broadcasting Architectures,

[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

[35] Langford S. K., Threshold DSS Signature without a Trusted Party, "Advances in Cryptology─CRYPTO'95," Springer-Verlag, 1995,
pp.397-409.


[37] Park C. and Kurosawa K., New ElGamal Type Threshold Digital Signature Scheme, "IEICE Transactions on Fundamentals of Electronics,


[39] Lee W. B. and Chang C. C., (t, n) threshold Digital Signature with Traceability Property, "Journal of Information Science and Engineering,


