Information for each entry item is restricted to the designated pages. However, the applicant may decide how much page space to assign for any individual entry item.

Receipt Number	

Cryptographic Techniques Overview

1. Name of Cryptographic Technique

ESIGN

Categories
[✓ 1.Asymmetric Cryptographic Schemes]
2.Symmetric Ciphers
3.Hush Functions
4.Pseudo-random Number Generators

Security Functions of Asymmetric Cryptographic Schemes
1.confidentiality 2. Authentication [✓ 3. signature] 4. key- sharing

Subcategories of Symmetric Ciphers
1. stream ciphers 2. 64-bits block ciphers 3. 128-bits block ciphers

2. Cryptographic Techniques Overview

2.1 Design policy

(1) Criteria of Security:

(a) We adopt the strongest security notion of security for a digital signature scheme-- existentially unforgeable against adaptively-chosen message attacks.

(b) Security in the above sense must be proven in a cryptosystem, that is to say, a digital signature scheme that is called a provably secure one, can, theoretically, be proven secure under some reasonable assumptions.

(2) Performance:

(a) At least as efficient as the well-known previously-proposed schemes such as EC-based schemes and RSA-based schemes.

To achieve provable security (in the strongest sense), we adopt the random oracle paradigm along with a reasonable intractable assumption. In the random oracle paradigm, security of a cryptosystem is proved assuming hash functions are modeled as random oracles. This paradigm was originally proposed by Bellare and Rogaway in ¥cite{BelRog93}, and is rapidly becoming a standard approach to achieve a provably-secure cryptosystem. Security of ESIGN, in the random oracle model, can be assured under an intractable assumption, which we name the approximate e-th root assumption, an approximate version of RSA assumption.

As for efficiency, signature generation with ESIGN is ten times more efficient than that achieved with RSA-based signature schemes, while their verification performances are comparable. Compared to EC(Elliptic Curve)-based signature schemes, ESIGN is several times faster in terms of signature and verification performance.

2.2 Intended applications

ESIGN is applicable to any circumstances in which digital signature schemes are available. In particular, it fits a batch procession of a huge number of signatures.

2.3 Basic theory and techniques

(1) ESIGN was originally proposed in [1] in 1985. Since then, both problems, factoring $n=p^2q$ and approximate e-th root problem (AERP), have been extensively investigated by many excellent researchers such as Adleman, Bleichenbacher, Brickell, DeLaurentis, Girault, McCurley, Odlyzko, Peralta, Pollard, Shamir, Toffin, Vall{¥'e}e. The authors have also communicated with Lenstra and Buchmann on these problems. The fact that no efficient algorithms on both problems have been found since they were raised implies that these problems can be considered to be almost as intractable as factoring $n =pq$ and the RSA problem.

(2) ESIGN can be proven secure in the random oracle model under the approximate e-th root assumption.

Information for each entry item is restricted to the designated pages. However, the applicant may decide how much page space to assign for any individual entry item.	Receipt Number	

Reference:

[1] Okamoto, T. and Shiraishi, A.: A Fast Signature Scheme Based on Quadratic Inequalities, Proc. of the ACM Symposium on Security and Privacy, ACM Press (1985).
[2] Okamoto, T.: A Fast Signature Scheme Based on Congruential Polynomial Operations, IEEE Trans. on Inform. Theory, IT-36, 1, pp.47-53 (1990).
[3] Brickell, E. and DeLaurentis, J.:An Attack on a Signature Scheme Proposed by Okamoto and Shiraishi, Proc. of Crypto'85, LNCS 218, Springer-Verlag, pp.28-32 (1986)
[4] Brickell, E. and Odlyzko: Cryptanalysis: A Survey of Recent Results, Chap.10, Contemporary Cryptology, Simmons (Ed.), IEEE Press, pp.501--540 (1991).
[5] Girault, M., Toffin, P. and Vall{\'e}e, B.: Computation of Approximate L-th Roots Modulo n and Application to Cryptography, Proc. of Crypto'88, LNCS 403, Springer-Verlag, pp.100-117 (1990)
[6] Vall{\'e}e, B., Girault, M. and Toffin, P.: How to Guess L-th Roots Modulo n by Reducing Lattice Bases, Proc. of Conference of ISSAC-88 and AAECC-6 (1988)
[7] Peralta, R.: Bleichenbacher's improvement for factoring numbers of the form $N=PQ^{2}$ (private communication) (1997).
[8] Peralta, R. and Okamoto, E.: Faster Factoring of Integers of a Special Form, IEICE Trans. Fundamentals, E79-A, 4, pp.489-493 (1996).
[9] Pollard, J.L.: Manuscript (1997).
[10] Okamoto, T., Fujisaki, E. and Morita, H.: TSH-ESIGN: Efficient Digital Signature Scheme Using Trisection Size Hash, submission to P1363a (1998).

Previous use: None