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 identification

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

``ESIGN identification'' is an identification scheme based on ``ESIGN signatures''. Suppose a system that a server checks the validity of a user.In the initial (registration) phase, a user registers his/her public-key of ESIGN signatures to the server. In the authentication phase when the server checks the validity of a user, the server sends a random string to the user, then the user makes the signature of the random string (as message) by using the secret key and sends it to the server. The server checks the validity of the signature using the public-key. If the signature is valid, then the sever acknowledge the validity of the user.

``ESIGN identification'' satisfies the following criteria under reasonable assumption.

(1) It should be proven to be secure in the strongest sense (i.e., impersonation is hard even against adaptive attacks) under reasonable assumptions (and in the random oracle model).

(2) Its performance in the light of speed and round complexity should be better than practical zero-knowledge identification (at least four moves) and three-move identification schemes.

2.2 Intended applications

(1) Identification (user authentication):
A server checks the validity of a user through network, where, in the initial (registration) phase, a user should register his/her public-key to the server.

(2) Mutual authentication:
The identification protocol executed in both ways (i.e., two parties identify each other).

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	

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.

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:

- Smart card payment system in Japan (Internet cash)
- Adopted in ISO/IEC 14888-3 (Digital Signature Algorithm with Appendix)