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
PSEC

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

Security ~~Functions of A~~symmetric 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

The design target of PSEC is as follows:

(1) It should be proven to be secure in the strongest sense (i.e., semantically secure against adaptively chosen-ciphertext attacks) under reasonable assumptions (and in the random oracle model).
(2) Its performance should be comparable to the elliptic curve ElGamal and other practical encryption schemes based on the elliptic curve discrete logarithm assumption.
(3) Its hybrid usage with a symmetric encryption should be also proven to be secure in the strongest sense (i.e., semantically secure against adaptively chosen-ciphertext attacks) under reasonable assumptions (and in the random oracle model).

Our approach to construct PSEC is based on the random oracle model [1], in which a primitive public-key encryption function is converted to an encryption scheme provably secure in the strongest sense if the underlying hash functions are assumed truly random functions.

Our primitive encryption function is the elliptic curve ElGamal function. There are three conversions based on the random oracle model [2,3,4], therefore we have three versions of PSEC: PSEC-1, PSEC-2 and PSEC-3.These schemes satisfy the above-mentioned target (security, performance and hybrid security). (except PSEC-1 for the hybrid security)

2.2 Intended applications

(1) PSEC-1:
- Key distribution for a symmetric encryption (at most 128 bit key size)
- Encrypted communication for small size data (at most 128 bit data size)

(2) PSEC-2:
- Key distribution for a symmetric encryption (no restriction on the size)
- Encrypted communication in a hybrid usage with symmetric encryption, especially envelope type (key distribution and data transmission are synchronized)

(3) PSEC-3:
- Key distribution for a symmetric encryption (no restriction on the size)
- Encrypted communication in a hybrid usage with symmetric encryption, especially ``envelope type'' (key distribution and data transmission are synchronized)
- Encrypted communication in a hybrid usage with symmetric encryption, especially ``session type'' (only once key distribution in the opening phase of a session, and many times data transmissions during the session)

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) The elliptic curve ElGamal encryption function as a primitive encryption function.
(2) Our novel three conversion methods [2,3,4], by which we have three versions: PSEC-1, PSEC-2, PSEC-3. Especially PSEC-2 and PSEC-3 are the first public-key encryption schemes whose hybrid usages with symmetric encryption are proven to be secure in the strongest sense under reasonable assumptions and random oracle model.
(3) In the conversion of PSEC-3 [4], ``session type'' (only once key distribution in the opening phase of a session, and many times data transmissions during the session) of a hybrid usage with symmetric encryption is available. In addition, the overhead of the conversion is almost nothing if practical hash functions such as SHA-1 are employed, namely the conversion is optimal in the performance.

References:

[1] Bellare, M. and Rogaway, P. : Optimal Asymmetric Encryption, Proc. of Eurocrypt'94, LNCS 950, Springer-Verlag, pp.92-111 (1995).
[2] Fujisaki, E. and Okamoto, T.: How to Enhance the Security of Public-Key Encryption at Minimum Cost, Proc. of PKC'99, Springer-Verlag, LNCS 1560, pp. 53--68 (1999).
[3] Fujisaki, E. and Okamoto, T.: Secure Integration of Asymmetric and Symmetric Encryption Schemes, Proc. of Crypto'99, Springer-Verlag, LNCS 1666, pp. 535--554 (1999).
[4] Okamoto, T. and Pointcheval, D.: OCAC: an Optimal Conversion for Asymmetric Cryptosystems, manuscript (2000).