Report on Present State of PSEC-KEM Cryptosystem Evaluation (screening evaluation)

January 28, 2002

Natsume Matsuzaki, Member

Public-Key Cryptography Subcommittee

PSEC-KEM cryptosystem

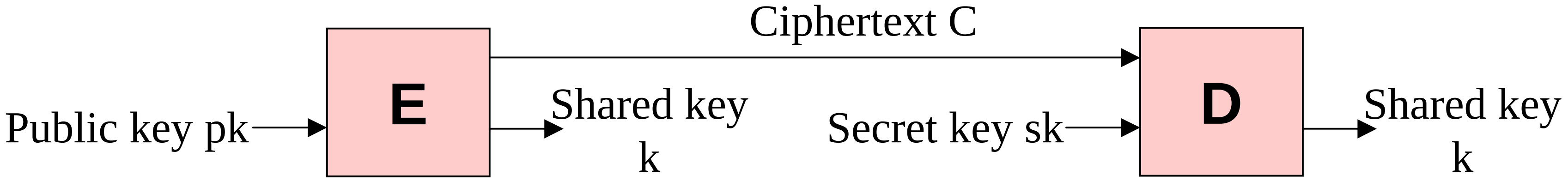
(submitter’s claims)

- Category:Key agreement – Proposes key generations, E, and D in the illustration.
- Provable security: Provides the strongest security based on random oracle model.

  (a) IND-CCA2 security definition for key encapsulation mechanism (by Dr.Shoup)

  (b) Proof that the scheme is reduced to EC-CDH under random oracle model.
- SW implementation:

  Key generation: 5.64ms, encryption: 11.09ms, decryption: 10.97ms (Pentium III 600MHz)



Evaluation methods

- PSEC-KEM:
  - Submitted as a modification of PSEC-2 (cryptosystem submitted to CRYPTREC2000).
  - Based on a study by this Subcommittee, a decision was made to evaluate the cryptosystem as a *new submission*.
- In addition to a screening evaluation, the relationship between this cryptosystem and PSEC-2 was also evaluated for reference purposes.

Screening evaluation

While no major problems were discovered, the following issues were observed.

<Category>

The cryptographic technique specifications describe the scheme as a key agreement scheme, while the self-evaluation describes it as a key encapsulation mechanism used in a hybrid cryptosystem. Thus consistency and associations are unclear.

<Cryptographic technique specifications>

- The primitive section does not contain elliptic curve recommended parameters.
- It is unclear what level of security is attained by the recommended parameters in the scheme section.

<Self-evaluation>

The security definition for key encapsulation is satisfactory, and there are no deficiencies in the security proofs. However, the claim that they have proved that the strongest security is provided by IND-CCA2 could be misunderstood.

(Reference information) Evaluation of PSEC-KEM as a modification of PSEC-2 in response to issues in PSEC-2 (CRYPTREC2000 submission)

Category		PSEC-2		PSEC-KEM
		Issues noted at CRYPTREC2000	Appropriateness of criticism	Modification
Scheme	1	“hLen ≤ k” is written where “hLen≅k” should be written. (hLen: hash output bit length; k: security parameter which is the bit length of order of the base point).	Appropriate	Omission; correction needed.
	2	“rLen ≤ qLen” was written where “rLen≅qLen” should have been written. (rLen：random number bit length; qLen: bit length of the size of the definition field)	Appropriate	Change in specifications; not applicable
Primitive	3	Typographical errors Elliptic curve parameter values and elliptic curve conditions are missing.	Appropriate	Omission; addition needed.
	4	The exclusion of characteristic 3 field is not explicitly stated.	Appropriate	Solved
	5	If the first coordinate of an element on the elliptic curve is used as a mask, is there a possibility that semantic security will be adversely affected?	Not reviewed	Change in specifications; not applicable

(Reference Information) Relationship between PSEC-KEM and PSEC-2, and comparison with other methods

- Relationship with PSEC-2: PSEC-KEM may be considered a separate scheme for the following reasons.
  - PSEC-2 has plaintext input, whereas PSEC-KEM does not.
  - Their categories and definitions of security are different.
  - They are similar in that they both use secret random number r, but PSEC-2 involves plaintext, whereas PSEC-KEM does not.

- Comparison with ECIES-KEM and ACE-KEM

Compared parameters		PSEC-KEM	ACE-KEM	ECIES-KEM
Processing time (elliptic curve additions)	Encryption	2	5	2
	Decryption	2	3	1
Provable security	Security	IND-CCA2		
	Model	Random oracle model	Standard model	Random oracle model
	Security hypothesis	CDH	DDH	Gap-DH