# Report on Present State of HIME(R) Cryptosystem Evaluation (screening evaluation)

January 28, 2002

Seigo Arita, Member

Public-Key Cryptography Subcommittee

# HIME(R)
## (submitter's claims)

- **Category:** Confidentiality
- **Security basis:** Difficulty of $N=p^dq$ type factoring problem
- **Provable security: IND-CCA2** in random oracle model
- **Characteristics of system:**
  - Extremely high-speed encryption processing
  - Decryption processing approximately 2.5 times as fast as RSA-OAEP
- **SW implementation information:**

  Encryption: 0.6 ms; decryption: 37.0 ms (Pentium III 800MHz)

# Screening evaluation

- Three evaluators were requested to evaluate the cryptosystem.
- Cryptographic technique specifications:
  - There are problems at the textual (descriptive) level.
  - In general, there are no problems.
- Self-evaluation:
  - No problems were discovered in relation to the security proof.

# Evaluator comments

- Rabin-OAEP using modulus $N = p^d q$
- Decryption method (i.e., square root computation method using modulus $N=p^d q$ type)
  - Isn't this on par with the method which uses CRT (CRYPTO'98 Takagi)?
- Provable security
  - No particular conflicts with past results from others.
- $N = p^d q$ type factoring problem
  - The analysis in the self-evaluation is not sufficient.
- Other issues
  - There is no description of cases other than d = 2,3.