Report on Present State of EPOC-2 Cryptosystem Evaluation (full evaluation)

January 28, 2002

Hajime Watanabe, Member

Public-Key Cryptography Subcommittee

EPOC-2 cryptosystem (submitter's claims)

- Category: Confidentiality
- Security basis:
  - Difficulty of $n=p^2q$ type factoring problem
- Provable security:
  - Strongest security under random oracle model.
- Characteristics:
  - Decryption is faster than encryption (faster than RSA-OAEP)
  - Security proof based on a assumption which is more general than the RSA assumption
  - Enables more efficient security reduction than general security reductions do
- Other issues
  - Hybrid cryptosystem which is combined with symmetric-key cipher

Full evaluation

- Specifications changed slightly from the cryptosystem submitted last year (treated as continual evaluation)
- Four evaluators were requested to evaluate the cryptosystem from the following perspectives:
  - Cryptographic primitive
  - Cryptographic scheme
  - (Relationship between last year's evaluation results and this year's submitted cipher)
  - Other issues (e.g., difficulty of $n=p^2q$ type prime factor decomposition problem)

Evaluation comments

– Difficulty of $n=p^2q$ type factoring problem –

- **No particular problems were discovered (security is almost exactly the same as with n=pq).**
- The size of the prime factors (composite number consisting thereof) being used should be determined in consideration of the estimated size of the composite number undergoing factoring by the Number Field Sieve (NFS) (according to preliminary calculations, 1024 bits could be factored by the year 2018).
  - The same issue should be considered for other cryptosystems as well.
- In order to make the difficulty of factoring problems for NFS equal to the difficulty level for the symmetric-key cipher being used (128 bits), larger prime factors (composite number consisting thereof) should be used (according to preliminary calculations).
  - The same issue should be considered for other cryptosystems as well.
- The factoring problem was evaluated separately. In that evaluation, it was pointed out that this problem is slightly easier than the problem for n=pq type factoring.

Evaluation comments

– Cryptographic primitives –

The remarks regarding primitives affect the scheme's security proof.

- The primitives used have different parameter conditions from the original function presented at Eurocrypt '98. Therefore, provable security could not be confirmed based on the self-evaluation alone (according to multiple evaluators).
  - Parameter h_0 conditions, order of h, etc.
  - Addition of other conditions, or lowered reduction efficiency may allow provable security?
- The evaluators who raised the issue report that under the same conditions as the Eurocrypt '98 function, there would be provable security (due to efficient reduction).

Evaluation comments

– Scheme –

- **No significant problems were noted. (Strongest security is provided under random oracle model.)**
- When a block cipher is used as a symmetric-key cipher, IND-CPA may not be fulfilled depending on the usage method, so caution is necessary. Provable security may be lost as a result.