Report on Present State of RSA Cryptosystem/Signature Evaluation (full evaluation)

January 28, 2002

Kazuo Ohta, Member

Public-Key Cryptography Subcommittee

RSA signature, RSA-PSS, RSA-OAEP

- Category:
  Signature, confidentiality
- Security basis:
  Difficulty of n=pq type factoring problem
- Provable security:
  Equivalence with the difficulty of n=pq type factoring problems has not been shown, but the cryptosystem is believed to be secure heuristically.
- Characteristics:
  Track record of use over a broad range

  Security evaluation based on a broad range of perspectives
- SW implementation information:
  Celeron 450 MHz 1 ms (e=3)

  (key size: 1024 bits) 27 ms (CRT used)

Full evaluation

- Multiple evaluators were requested to evaluate the cryptosystem based on the following perspectives:
  - Cryptographic primitives: Have we overlooked anything in terms of our understanding of this area? Is there a possibility that known attack methods will become more advanced?
  - Cryptographic scheme: Are there any errors in terms of proofs, etc. published in academia?
  - Other issues: Has the theoretical proof been accurately reflected in the proposed system?

Comments on RSA primitives

No problem with the self-evaluation on the textual (descriptive) level (all evaluators)

- Comments on usage constraints

  Under typical conditions

    Modulus value sharing   When secret key d is small

    Calculation of entire information from partial key information

  When used as cryptosystem

    When public key e is small   Broadcast communication environment, etc.

The noted constraint conditions were all already known.

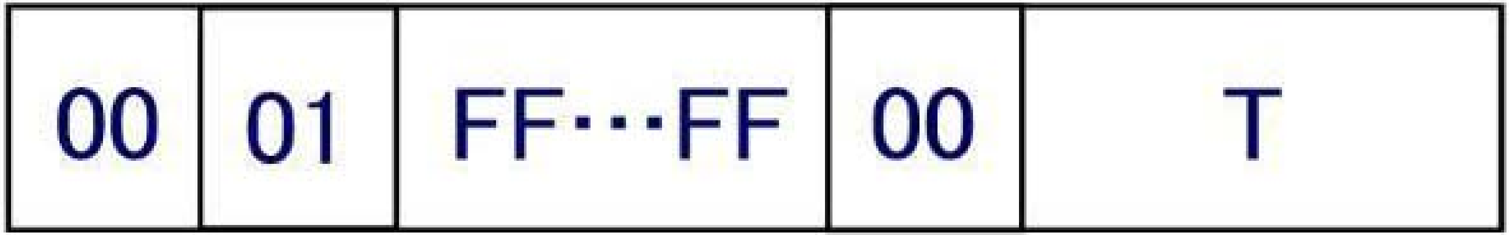
Comments on RSA signature (PKCS#1 v1.5)

(one of the signature systems included in
guidelines for electronic signature law)

No security issues noted (multiple responses)

- There was a comment stating that RSA-PSS should be used because provable security was not shown.
- There was a comment that we should check with the submitting company on the definition of "textbook RSA", because the submitting company does not recommend use due to security constraint conditions for "textbook RSA".
- Discussion must take into consideration factors such as usage conditions and the life of the system.

PKCS#1 v1.5 format



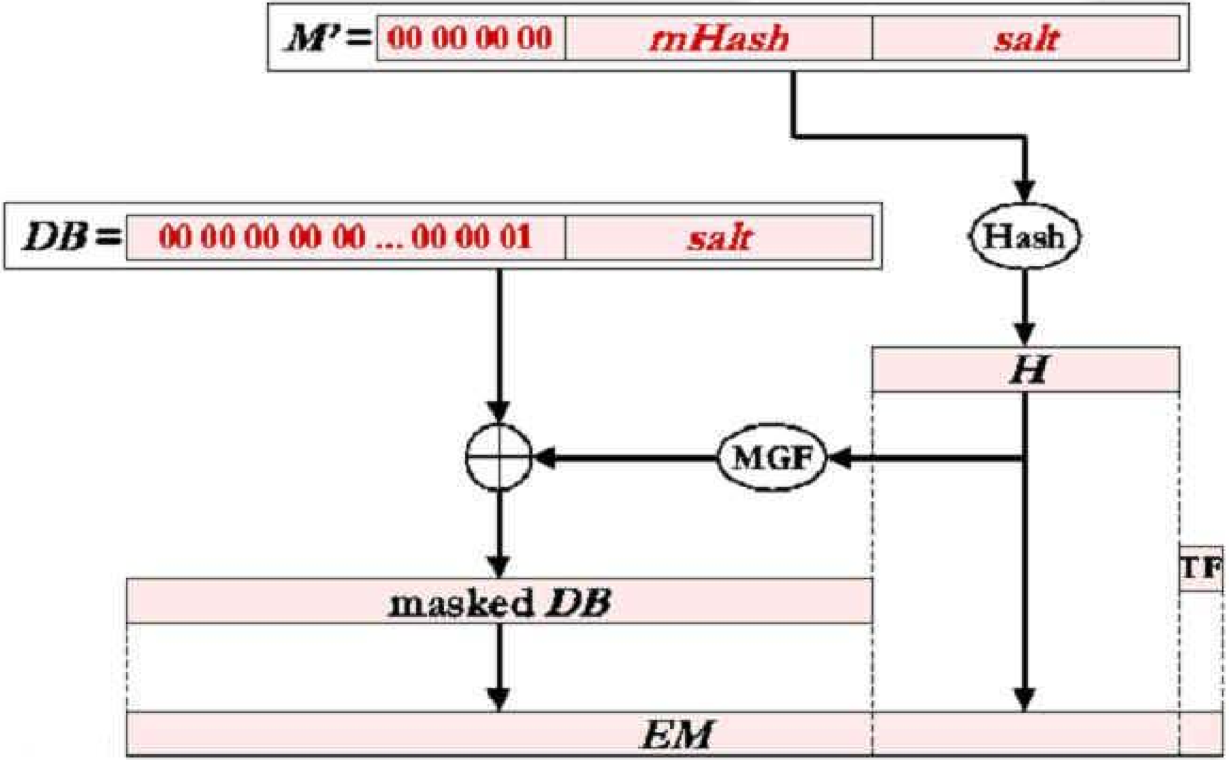
00	01	FF···FF	00	T

Comments on RSA-PSS

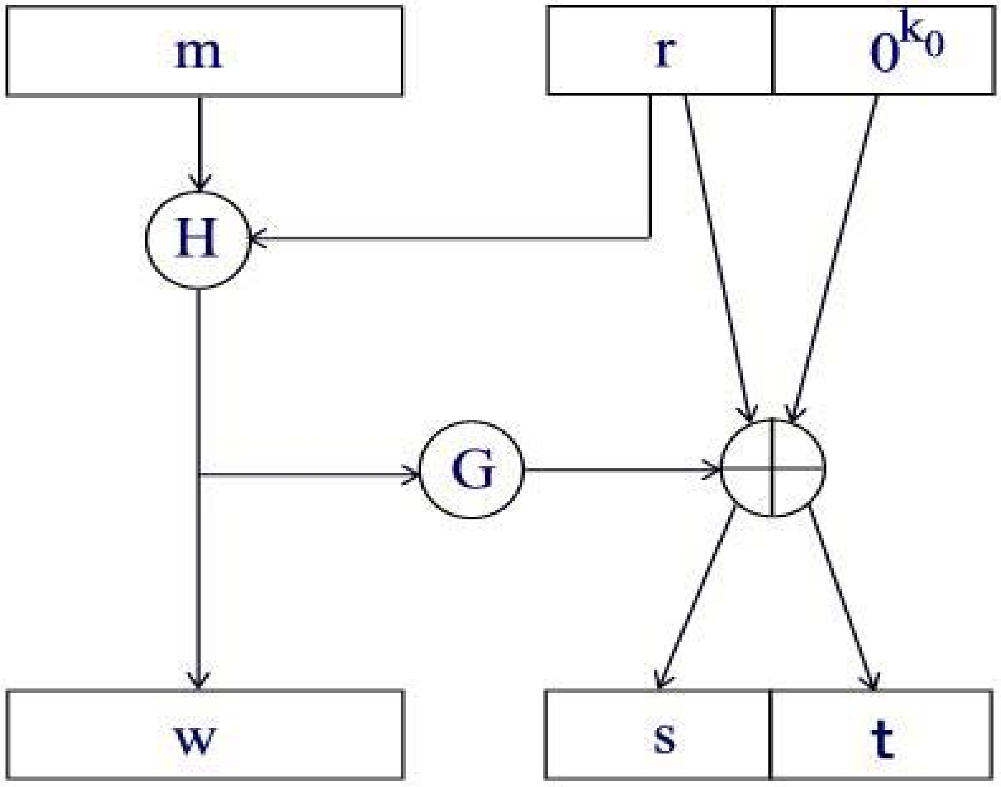
Provable security is reliable (note that this is for the RO Model).

- Jonsson’s proof, while not applied to hash-id, is reliable because security has been evaluated for attacks that exploit the variable length of the random number component (salt), as well as cases where there is a correlation between the two functions used in encoding.
- It is necessary to continue studying the possibility of exploiting hash-ids that are newly introduced due to specification changes (noted by multiple evaluators).
- Reduction efficiency is reduced by the introduction of parameters. Therefore, care must be taken in selecting the modulus size.

PSS Diagram


M' = 00 00 00 00
mHash
salt
DB = 00 00 00 00 00 ... 00 00 01
salt
Hash
H
MGF
TF
masked DB
EM

The probabilistic signature scheme



Comments on RSA-OAEP

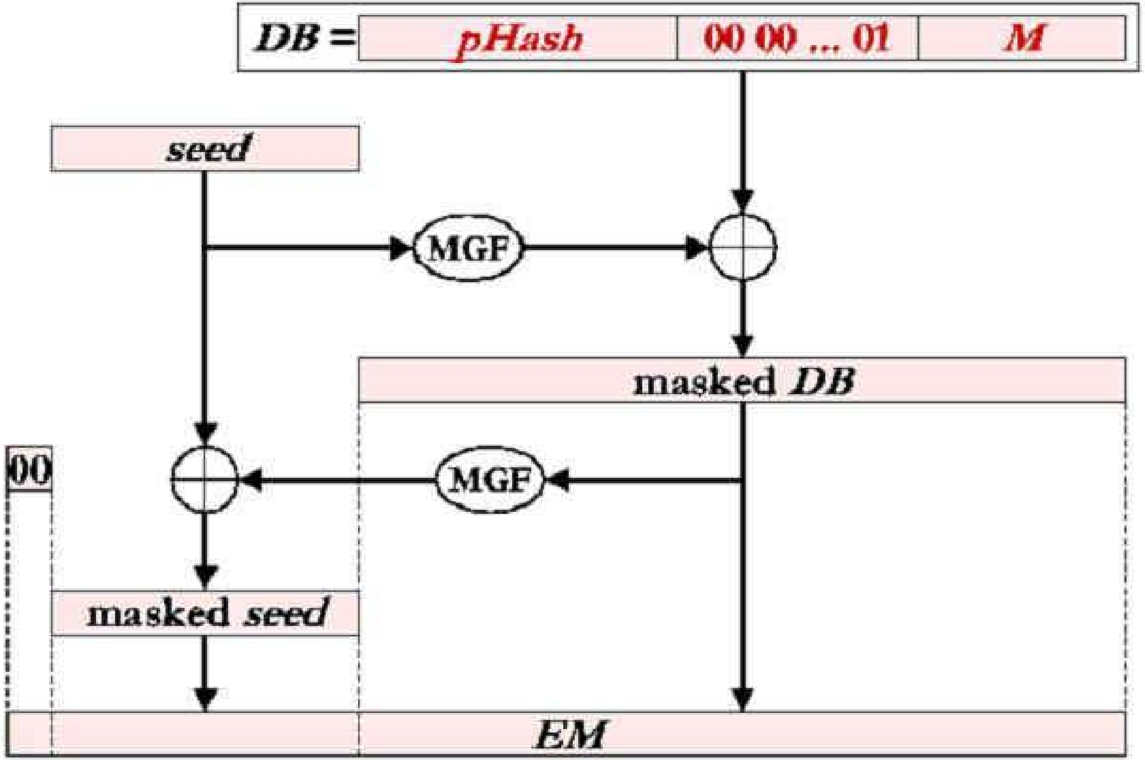
Provable security is reliable (note that this is for the RO Model).

- The proposed system differs slightly from the text where the proof is given in the paper. Design parameters need to be selected based on an understanding of the relationship between them.
- From the perspective of reduction efficiency, RSA-OAEP+ is recommended by one evaluator.

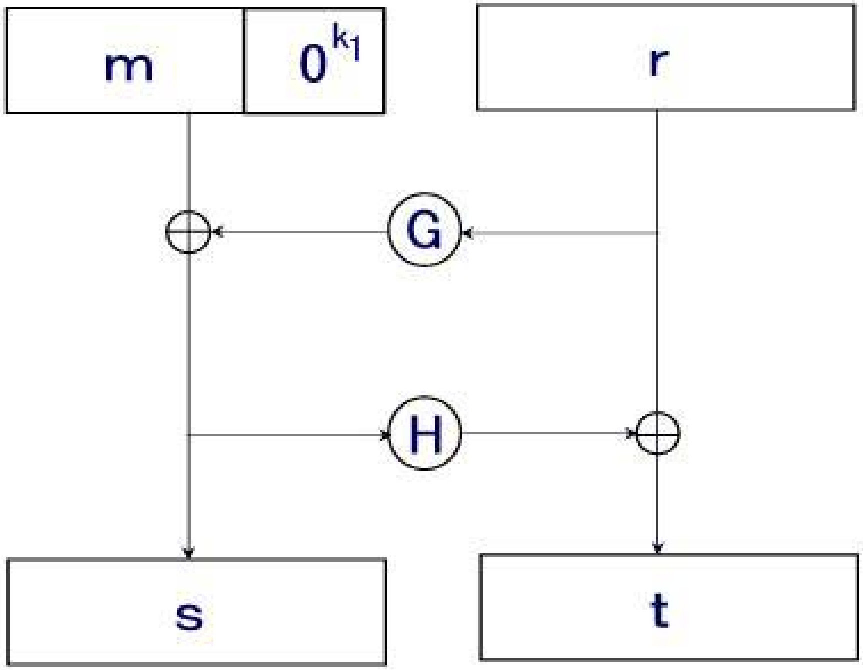
  → This needs to be studied.
- There is a possibility that the data lengths presented in the specifications are typographical errors.

  → This needs to be checked.

OAEP Diagram



Optimal asymmetric encryption padding



Issues going forward

- RSA signature (PKCS#1 v1.5):

  Discussion with consideration for usage conditions, system life, etc.
- RSA-PSS:

  Continual study of potential for exploiting hash-id

  Selection of modulus size with consideration for decline in reduction efficiency
- RSA-OAEP:

  Design parameter selection

  Comparison with RSA-OAEP+