# *Report on FY2002 Evaluation of Public-Key Cryptographic Techniques*

*May 22, 2003*

*Tsutomu Matsumoto*

*Chair of*

*Public-Key Cryptography Sub-Committee*

*CRYPTREC Evaluation Committee*

# *Outline of This Presentation*

- ***Tasks and Results***
- ***Outline of Evaluation***
  - ***Policy***
  - ***Targets***
  - ***Method***
- ***Result of Evaluation***
  - ***List of Recommended Public-key Cryptographic Schemes for Electronic Government***
  - ***Intractability of Number-theoretic Problems***
- ***For details, please refer to CRYPTREC Report 2002***

## *FY2002 Plan of Public-Key Cryptography Sub-Committee*

- ***Mission 1 Drafting***

  ***The List of Recommended Public-Key Cryptographic Schemes for Electronic Government.***

- ***Mission 2 Following-up***

  ***The Electronic Signature Schemes***

  ***Listed for Electronic Signature Law.***

- ***Mission 3 Others***

## *FY2002 Result of Public-Key Cryptography Sub-Committee*

### ◆*Regarding Mission 1*

***The Drafted List became the***

***List of Recommended Public-Key Cryptographic Schemes for Electronic Government***

***on 28 February 2003.***

### ◆ *Regarding Mission 2*

***The Electronic Signature Schemes***

***listed for Electronic Signature Law was revised on***

***11 November 2002.***

# *Evaluation Policy*

- ***Complete Specification* of the scheme including *Parameter Selecting Method* should be available.**
- ***Consensus based on Sufficient Evidence* should be presented that the scheme is *Currently Secure* enough and preferably *kept secure in 10 years* .**
  - ***Requirement for Widely Used Scheme***
  - ***Requirement for Young Schemes***
- ***Comprehensive security evaluation should be conducted regarding intractability of number-theoretic problems on which primitives depends, how to select recommended parameters, etc.***

## *Requirement for Widely Used Schemes*

- ***With regard to widely used schemes, namely, public-key cryptographic techniques that have a firm track record of use and evaluation over relatively long period of time, and whose specifications cannot be changed easily from the viewpoint of interoperability, only empirical evidence on security is required and provable security is preferably presented.***

## *Requirement for Young Schemes*

- ***With regard to young schemes,***

  ***namely, public-key cryptographic techniques that have a short-time track record,***

  ***it was required that reasonable level of provable security under reasonable assumption is provided as a minimum requirement because they can be specified independently of existing cryptographic techniques.***

# *Public-Key Schemes Evaluated in FY2002*

| *Security Basis*<br><br>*Function* | *Integer Factoring* | *Discrete Logarithm* | *Elliptic Curve Discrete Logarithm* |
|---|---|---|---|
| *Signature* | **ESIGN**<br>**TSH-ESIGN**<br>**RSA-PSS**<br>**RSASSA-PKCS1- v1_5** | **DSA** | **ECDSA**<br>**(ANSI X9.62, SEC1)** |
| *Confidentiality* | **HIME(R)**<br>**RSA-OAEP**<br>**RSAES-PKCS1- v1_5** | | **ECIES** |
| *Key Agreement or Distribution* | | **DH** | **ECDH**<br>**PSEC-KEM** |

# *How the target schemes are selected*

- ***Review the Results of FY2001 Evaluation***

# *Public-Key Schemes Evaluated in FY2001*

| *Security Basis* / *Function* | *Integer Factoring* | *(Elliptic Curve) Discrete Logarithm* | *Lattice* |
|---|---|---|---|
| *Signature* | **ESIGN**<br>**RSA-PKCS#1 v1.5**<br>**RSA-PSS** | **DSA**<br>**ECDSA(ANSI X9.62)**<br>**ECDSA in SEC1**<br>**OK-ECDSA** | |
| *Confidentiality* | **EPOC-2**<br>**HIME(R)**<br>**RSA-OAEP** | **ECIES in SEC1** | **NTRU** |
| *Key Agreement or Distribution* | | **DH**<br>**ECDH in SEC1**<br>**OK-ECDH**<br>**PSEC-KEM** | |

*Target of Specific Evaluation with respect to Electronic Signature Law*

*Target of Screening*

*Targets in Follow-up Phase*

■ *Others:* **COCK System, CVCRT, MKS**

## *FY2001 Conclusion I* *Schemes in the Follow-up Phase*

| *Security Basis* / *Function* | *Integer Factoring* | *(Elliptic Curve) Discrete Logarithm* | *Lattice* |
|---|---|---|---|
| *Signature* | **RSA-PKCS#1 v1.5**<br>**RSA-PSS** | **DSA**<br>**ECDSA(ANSI X9.62)**<br>**ECDSA in SEC1** | |
| *Confidentiality* | **RSA-OAEP** | | |
| *Key Agreement or Distribution* | | **DH**<br>**ECDH in SEC1** | |

## *FY2001 Conclusion II* *Candidate Targets of FY2002 Evaluation*

| *Security Basis* / *Function* | *Integer Factoring* | *(Elliptic Curve) Discrete Logarithm* | *Lattice* |
|---|---|---|---|
| *Signature* | **ESIGN** | | |
| *Confidentiality* | **HIME(R)** | **ECIES in SEC1** | |
| *Key Agreement or Distribution* | | **PSEC-KEM** | |

# *Public-Key Schemes Evaluated in FY2002*

| *Security Basis* / *Function* | *Integer Factoring* | *Discrete Logarithm* | *Elliptic Curve Discrete Logarithm* |
|---|---|---|---|
| *Signature* | **ESIGN**<br>**TSH-ESIGN**<br>**RSA-PSS**<br>**RSASSA-PKCS1- v1_5** | **DSA** | **ECDSA**<br>**(ANSI X9.62, SEC1)** |
| *Confidentiality* | **HIME(R)**<br>**RSA-OAEP**<br>**RSAES-PKCS1- v1_5** | | **ECIES** |
| *Key Agreement or Distribution* | | **DH** | **ECDH**<br>**PSEC-KEM** |

# Method of Evaluation

## Specific OR Deep OR Follow-up Evaluation

- ***Whole Scheme***
- ***Special***
  - ***Decompose the targets into several sub-targets***
  - ***Synthesize the evaluation results for the sub-targets***
  - ***Security Basis: Factoring, Discrete Log, …***

# *Human Resources*

## *CRYPTREC Evaluation Committee*

- ***Public-Key Cryptography Sub-Committee***
  - ***Members***
  - ***A Number of Anonymous and Onymous External Experts***

***An Expert means a team consisting of one or more World Class Cryptographers***

# *Public-Key Cryptography Sub-Committee*

- *Seigo ARITA (NEC Corporation)*
- *Jun KOGURE (Fujitsu Laboratories Ltd.)*
- *Tsutomu MATSUMOTO (Chair, Yokohama National University)*
- *Natsume MATSUZAKI (Matsushita Electric Industrial Co.,Ltd.)*
- *Kazuo OHTA (The University of Electro-Communications)*
- *Yasuyuki SAKAI (Mitsubishi Electric Corporation)*
- *Atsushi SHIMBO (Toshiba Corporation)*
- *Hiroki SHIZUYA (Tohoku University)*
- *Seiichi SUSAKI (Hitachi, Ltd.)*
- *Hajime WATANABE (National Institute of Advanced Industrial Science and Technology)*

## *Security Evaluation Items Regarding the Intractability of Number-theoretic Problems*

# i) Integer factoring problem

- *Investigation of known algorithms and comparison of their efficiency*
- *Comparison between pq type and (p^d)q type (d ≥2)*
- *Validity and feasibility of research that realizes the number field sieve method on a hardware circuit*

# ii) Discrete logarithm problem

- *Investigation of known algorithms and comparison of their efficiency*

# iii) Elliptic curve discrete logarithm problem

- *Investigation of known algorithms and comparison of their efficiency*
- *Investigation of problems regarding several restricted curves(such as Koblitz curve)*

## *Selection of Parameters and Their Security*

- ***Differences in elliptic curve parameters between SEC1 and ANSI and their security***
- ***Parameter selecting method used for RSA***

# i) DSA

- ***Security evaluation of primitives and schemes***
- ***Defects of random number generation given by FIPS186-2 Appendix 3***

# ii) ECDSA

- ***Adequacy and significance of provable security of existential unforgeability in a generic group model***
- ***Problems in generating a key and DSKS characteristics***
- ***Security evaluation of Koblitz curve***

## iii) ESIGN, TSH-ESIGN

- *Adequacy of the size of recommended parameters*
- *Approximate e-th root problem and ppq type integer factoring problem*
- *Provable security in SO-CMA model*

## iv) RSA

- ***Security evaluation of RSASSA-PKCS1-v1_5, RSAES-PKCS1-v1_5***
- ***Provable security of RSA-PSS, RSA-OAEP and the reduction efficiency***

## v) ECIES

- ***Investigation of vulnerability regarding MAC and KDF functions***

## vi) HIME( R )

- *Verification of total security including provable security*
- *ppq type integer factoring problem*

## vii) DH

- *Security evaluation of scheme (ANSI X9.42-2001)*

## viii)ECDH

- *Security evaluation of scheme (SEC1)*

# ix) PSEC-KEM

- *Provable security required for KEM-DEM construction*
- *Security of hybrid-type public-key ciphers by KEM-DEM configuration method*
- *Security in usage methods other than KEM*

# *Public-Key Schemes Evaluated in FY2002*

| *Security Basis* / *Function* | *Integer Factoring* | *Discrete Logarithm* | *Elliptic Curve Discrete Logarithm* |
|---|---|---|---|
| *Signature* | **ESIGN**<br>**TSH-ESIGN**<br>**RSA-PSS**<br>**RSASSA-PKCS1- v1_5** | **DSA** | **ECDSA**<br>**(ANSI X9.62, SEC1)** |
| *Confidentiality* | **HIME(R)**<br>**RSA-OAEP**<br>**RSAES-PKCS1- v1_5** | | **ECIES** |
| *Key Agreement or Distribution* | | **DH** | **ECDH**<br>**PSEC-KEM** |

# *FY2002 Result* (1)

***No problems in the use of Electronic Government are currently observed for these schemes with appropriate parameters and auxiliary functions.***

| *Security Basis* / *Function* | *Integer Factoring* | *Discrete Logarithm* | *Elliptic Curve Discrete Logarithm* |
| --- | --- | --- | --- |
| *Signature* | **RSA-PSS**<br>**RSASSA-PKCS1- v1_5** | **DSA** | **ECDSA (ANSI X9.62, SEC1)** |
| *Confidentiality* | **RSA-OAEP** | | |
| *Key Agreement or Distribution* | | **DH** | **ECDH** |

*has Provable Security* (RSA-PSS, RSA-OAEP)

*has Empirical Evidence on Security* (RSASSA-PKCS1- v1_5, DSA, ECDSA, DH, ECDH)

# *FY2002 Result* (2)

| *Security Basis* / *Function* | *Integer Factoring* | *Discrete Logarithm* | *Elliptic Curve Discrete Logarithm* |
| --- | --- | --- | --- |
| *Signature* | | | |
| *Confidentiality* | | | |
| *Key Agreement or Distribution* | | | **PSEC-KEM** |

**PSEC-KEM** ***should be used in the Key Encapsulation Mechanism - Data Encapsulation Mechanism construction. Provable Security has been shown in that sense.***

***Use of elliptic curve parameters specified by SEC1 is recommended.***

# *FY2002 Result* (3)

| *Security Basis* / *Function* | *Integer Factoring* | *Discrete Logarithm* | *Elliptic Curve Discrete Logarithm* |
|---|---|---|---|
| *Signature* | | | |
| *Confidentiality* | **RSAES-PKCS1- v1_5** | | |
| *Key Agreement or Distribution* | | | |

***Use of* RSAES-PKCS1-v1_5 *is allowed for the time being because it has been used in SSL3.0/TLS1.0.***
***It is not likely that* RSA-PKCS1-v1_5 *has provable security. Measures against attacks should be carefully adopted in the real operational environment.***

# *FY2002 Result* (4) and (5)

| *Security Basis* <br> *Function* | *Integer Factoring* | *Discrete Logarithm* | *Elliptic Curve Discrete Logarithm* |
|---|---|---|---|
| *Signature* | **ESIGN** <br> **TSH-ESIGN** | | |
| *Confidentiality* | | | |
| *Key Agreement or Distribution* | | | |

***The FY2002 evaluation made clear that*** **ESIGN(*****the version formerly listed for Electronic Signature Law) has a flaw in the specification of signature verification procedure and contains parameters permitting signature forgery: Thus*** **ESIGN** ***does not have provable security.***

**TSH-ESIGN** ***evaluated for reference to*** **ESIGN** ***has only provable security of lower level than that required for submitted schemes.***

# *FY2002 Result* (6)

| *Security Basis* / *Function* | *Integer Factoring* | *Discrete Logarithm* | *Elliptic Curve Discrete Logarithm* |
|---|---|---|---|
| *Signature* | | | |
| *Confidentiality* | | | **ECIES** |
| *Key Agreement or Distribution* | | | |

***The proposed* ECIES *has problems regarding input to the KDF function and MAC handling, and does not have high security, which allows adaptive chosen-ciphertext attacks.***
***Also, it does not have provable security required for submitted schemes.***

# *FY2002 Result (7)*

| *Security Basis* / *Function* | *Integer Factoring* | *Discrete Logarithm* | *Elliptic Curve Discrete Logarithm* |
|---|---|---|---|
| *Signature* | | | |
| *Confidentiality* | **HIME(R)** | | |
| *Key Agreement or Distribution* | | | |

***The specification of* HIME(R) *contains some flaws.***

***Regarding* HIME(R), *it was judged that the proof described in the submitted document was incorrect. Provable security can be proven through accurate discussions, but this had not been confirmed as of September 2002.***

# *Summary of the FY2002 Evaluation Result*

## *The List of Recommended Public-Key Cryptographic Schemes*

| *Security Basis*<br><br>*Function* | *Integer Factoring* | *Discrete Logarithm* | *Elliptic Curve Discrete Logarithm* |
|---|---|---|---|
| *Signature* | **RSA-PSS**<br>**RSASSA-PKCS1- v1_5** | **DSA** | **ECDSA** |
| *Confidentiality* | **RSA-OAEP**<br>**RSAES-PKCS1- v1_5** | | |
| *Key Agreement or Distribution* | | **DH** | **ECDH**<br>**PSEC-KEM** |

# *Result on Integer Factoring*

- *In 2001, Factoring Problem of $n = pq$ is "secure" if $|p| = |q|$ and $|n|$ is 1024 or more.*
- *In 2001, Factoring Problem of $n = ppq$ is "secure" if $|p| = |q|$ and $|n|$ is 1024 or more.*
- *The condition $|n| = 1024$ gives different margins for $n = pq$ and $n = ppq$.*
- *Transition of security of Integer Factoring is estimated.*

# *Result on Discrete Logarithm*

- ***In 2001, Discrete Logarithm Problem in subgroup of order q of a multiplicative group of finite field Fp (p: prime) is "secure" if p is 1024 bit or more and q is 160 bit or more.***
- ***Transition of security of Discrete Logarithm is estimated.***

# *Result on Elliptic Curve Discrete Logarithm*

- ***In 2001, except for particular classes of elliptic curves, Elliptic Curve Discrete Logarithm Problem is "secure" if the order of the base point has a prime factor of 160 bit or more.***
- ***Transition of security of Elliptic Curve Discrete Logarithm is estimated.***

# *Thanks to All who Supported and Gave Pressures*

***including***

- ***Applicants to CRYPTREC Call for Submission,***
- ***External Experts,***
- ***Observers from Kasumigaseki and Ichigaya,***
- ***Members and Staffs of***

  ***Public-Key Cryptography Sub-Committee,***

  ***Symmetric-Key Cryptography Sub-Committee,***

  ***CRYPTREC Evaluation Committee, and***

  ***CRYPTREC Advisory Committee.***