Report on FY2001 Evaluation of Public-Key Cryptographic Techniques

April 16, 2002

Tsutomu Matsumoto

Chair of

Public-Key Cryptography Sub-Committee

CRYPTREC Evaluation Committee

Tasks2

Specific Evaluation

- Signature Schemes Listed for Japanese Electronic Signature Law
- SSL/TLS Research
  1. How RSA schemes are used in the Protocol
  2. Survey of Vulnerability of the Protocol

General Evaluation --- for Use in Electronic Government

- Follow-up
- Deep Evaluation
- Newly Submitted Schemes
  1. Screening in FY 2001
  2. Deep Evaluation in FY 2002 for Selected Targets

Evaluated Public-Key Schemes

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

Target of Specific Evaluation with respect to Electronic Signature Law: ESIGN, RSA-PKCS#1 v1.5, DSA, ECDSA(ANSI X9.62)

Target of Screening: OK-ECDSA, HIME(R), NTRU, OK-ECDH, PSEC-KEM, COCK System, CVCRT, MKS

Targets in Follow-up Phase: ECIES in SEC1, DH, ECDH in SEC1

■ *Others*: COCK System, CVCRT, MKS

Requirement to a Public-Key Cryptographic Scheme for the Use in Electronic Government

- ***Complete Specification of the scheme including Parameter Selecting Method is available.***
- ***Consensus based on Sufficient Evidence is available that the scheme is Currently Secure enough and will be Kept Secure in 10 years .***
  - ***Widely Used Schemes***
    - ***- must have Empirical Evidence on Security***
    - ***- preferably have Provable Security***
  - ***Young Schemes***
    - ***- must have Provable Security under reasonable assumption***

Method of Evaluation

Screening

- Based on the submitted documents
  - Examination of Completeness of Submission
  - Implementability by third parties
  - Security or Performance is superior to those in the FY2000 list

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 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)***

Number of External Experts for Screening

Target	*Overseas*	*Domestic*	*Total*
OK-ECDSA	-	*3*	*3*
HIME (R)	-	*3*	*3*
NTRU	-	*3*	*3*
OK-ECDH	-	*3*	*3*
PSEC-KEM	*1*	*2*	*3*

Number of External Experts for Deep Evaluation of Computational Intractability

Target	*Overseas*	*Domestic*	*Total*
Integer Factoring - Experimental Study	*-*	*1*	*1*
Integer Factoring - Survey	*-*	*1*	*1*
Integer Factoring - Special Type Factors	*3*	*1*	*4*
Discrete Logarithm	*2*	*1*	*3*
Elliptic Curve Discrete Logarithm	*2*	*-*	*2*

Number of External Experts for Deep Evaluation of Schemes

Target	*Overseas*	*Domestic*	*Total*
DSA	*3*	*2*	*5*
ECDSA	*3*	*1*	*4*
ESIGN **ESIGN(Electronic Signature Law), TSH-ESIGN**	*3*	*1*	*4*
RSA **RSA-PKCS#1 v1.5, RSA-PSS, RSA-OAEP**	*2*	*2*	*4*
EPOC-2	*2*	*2*	*4*

Number of External Experts for Research of SSL/TLS

Target	*Overseas*	*Domestic*	*Total*
How RSA schemes are used	*-*	*1*	*1*
Vulnerability of the Protocol	*-*	*2*	*2*

Evaluated Public-Key Schemes

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

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.***

Result on Schemes (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*	*(Elliptic Curve) Discrete Logarithm*	*Lattice*
Signature	**RSA-PKCS#1 v1.5** **RSA-PSS**	**DSA** **ECDSA (ANSI X9.62)** **ECDSA in SEC1**	
Confidentiality	**RSA-OAEP**		
Key Agreement or Distribution		**DH** **ECDH in SEC1**	

Use of MD5 is not recommended.

Adding RSA-PSS to the List for Electronic Signature Law should be examined.

Result on Schemes **(2)**

ESIGN ***is currently not recommended for the use in Electronic Government.***

Security Basis / *Function*	*Integer Factoring*	*(Elliptic Curve) Discrete Logarithm*	*Lattice*
Signature	**ESIGN**		
Confidentiality			
Key Agreement or Distribution			

ESIGN(***Listed for Electronic Signature Law*****)** ***has a flaw in the specification of signature verification procedure and contains parameters permitting signature forgery.***
Example: ***e = 8 and |n| = 2048 with*** **SHA-1**

Change of the List for Electronic Signature Law with respect to **ESIGN** ***should be examined.***

Result on Schemes (3)

ECIES in SEC1 ***is currently not recommended for the use in Electronic Government.***

Security Basis / *Function*	*Integer Factoring*	*(Elliptic Curve) Discrete Logarithm*	*Lattice*
Signature			
Confidentiality		**ECIES in SEC1**	
Key Agreement or Distribution			

Some security problem has emerged.

***Result on Schemes* (4)**

EPOC-2 *is not recommended for the use in Electronic Government.*

Security Basis / ***Function***	***Integer Factoring***	***(Elliptic Curve) Discrete Logarithm***	***Lattice***
Signature			
Confidentiality	**EPOC-2**		
Key Agreement or Distribution			

Claimed proof of* EPOC-2'*s provable security was found to be wrong.

Result on Schemes (5)

Decision on the use of* HIME(R) *in Electronic Government cannot be made without deep evaluation.

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

Claimed proof of HIME(R)*'s provable security is not confirmed.*

Result on Schemes (6)

Decision on the use of* PSEC-KEM *in Electronic Government needs further examination since the technique Key Encapsulation Mechanism is relatively young.

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

Claimed proof of* PSEC-KEM*'s provable security as a KEM seems correct.

Result on Schemes (7)

NTRU, OK-ECDSA, ***and*** **OK-ECDH** ***are not recommended for the use in Electronic Government.***

Security Basis / *Function*	*Integer Factoring*	*(Elliptic Curve) Discrete Logarithm*	*Lattice*
Signature		*Young but No proof of Provable Security is given.* OK-ECDSA	
Confidentiality	*Young but the status on Provable Security is the same as* ECDSA		NTRU *Resistance against Side Channel Attacks is not sufficiently confirmed by the contents of the self evaluation report.*
Key Agreement or Distribution	*Young but the status on Provable Security is the same as* ECDH	OK-ECDH	

Result on Other Schemes

COCK System, CVCRT, ***and*** **MKS** ***are not recommended for the use in Electronic Government.***

Security Basis / *Function*	*Integer Factoring*	*(Elliptic Curve) Discrete Logarithm*	*Lattice*
Signature			
Confidentiality			
Key Agreement or Distribution			

Screening of these schemes was terminated earlier

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

Survey of RSA in SSL/TLS

- ***Key distribution and signature protocols of SSL/TLS using RSA schemes are basic and simple enough to avoid almost protocol failures.***
- ***RSA schemes in SSL/TLS have no problems if appropriate parameters and auxiliary functions are adopted.***

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** **RSA-PSS**	**DSA** **ECDSA(ANSI X9.62)** **ECDSA in SEC1**	
Confidentiality	**RSA-OAEP**		
Key Agreement or Distribution		**DH** **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	

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***

Thanks to All who Supported and Gave Pressures

including

- *Applicants to CRYPTREC Call for Submission,*
- *Anonymous 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.