CRYPTREC2001
Report on Present State of Asymmetric-Key Cryptographic Technique Evaluations

January 28, 2002

Tsutomu Matsumoto,

Yokohama National University, Graduate School

Chairman, Public-Key Cryptography Subcommittee

Tasks

- Specific evaluation
  - Signature algorithms for Electronic Signature Law
  - SSL ((1) RSA-related matters, (2) Protocol)
- General evaluation --- for e-government use
  - Follow-up OR deep evaluation
  - Newly submitted systems
  - FY 2001 screening
  - FY 2002 deep evaluation

Targets of specific evaluation (Electronic Signature Law)

Security basis Function	Integer factoring	(Elliptic curve) Discrete logarithm	Lattice	Others
Signature	**ESIGN** **RSA** RSA-PSS	**DSA** **ECDSA** ECDSA in SEC1 OK-ECDSA		
Confidentiality	EPOC-2 HIME(R) RSA-OAEP	ECIES in SEC1	NTRU	
Key agreement		DH ECDH in SEC1 OK-ECDH PSEC-KEM		COCK System
Miscellaneous				CVCRT MKS

Newly submitted targets

Security basis / Function	Integer factoring	(Elliptic curve) Discrete logarithm	Lattice	Others
Signature	ESIGN RSA RSA-PSS	DSA ECDSA ECDSA in SEC1 **OK-ECDSA**		
Confidentiality	EPOC-2 **HIME(R)** RSA-OAEP	ECIES in SEC1	**NTRU**	
Key agreement		DH ECDH in SEC1 **OK-ECDH** **PSEC-KEM**		**COCK System**
Miscellaneous				**CVCRT** **MKS**

Targets of follow-up OR deep evaluation

Security basis / Function	Integer factoring	(Elliptic curve) Discrete logarithm	Lattice	Others
Signature	ESIGN RSA **RSA-PSS**	DSA ECDSA **ECDSA in SEC1** OK-ECDSA		
Confidentiality	**EPOC-2** HIME(R) **RSA-OAEP**	**ECIES in SEC1**	NTRU	
Key agreement		**DH** **ECDH in SEC1** OK-ECDH PSEC-KEM		COCK System
Miscellaneous				CVCRT MKS

Method and points

- Screening
  - Based on the submitted documents
    - Submission completeness examination
    - Implementability by third parties
    - Security or Performance ≥ FY2000
- Specific OR deep OR follow-up evaluation
  - Whole
  - 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 Subcommittee
    - Members
    - A Number of anonymous external experts (world class cryptographers)

Public-Key Cryptography Subcommittee

Seigo Arita (NEC Corporation)
Jun Kogure (Fujitsu Laboratories Ltd.)
Tsutomu Matsumoto (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 reviewers for screening evaluation

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

Number of external reviewers for deep evaluation of primitives

Target	Overseas	Domestic	Total
Integer factoring (Experimental)		1	1
IF survey		1	1
Special IF	3	1	4
DLP	2	1	3
ECDLP	2		2

Number of external reviewers for deep evaluation of schemes

Target	Overseas	Domestic	Total
EPOC-2 (conversion)		1	1
EPOC-2 (new)	2	1	3
RSA-OAEP, RSA-PSS, etc	2	2	4
ESIGN	3	1	4
DSA	3	2	5
ECDSA	3	1	4

Number of external reviewers for SSL evaluation

Target	Overseas	Domestic	Total
How RSA is used		1	1
Protocol		2	2

Things to do

- Examine the gathered knowledge
- Synthesize the evaluation results for the sub-targets
- Settle ECIES issues
- Summarize the evaluation for CRYPTREC REPORT 2001
- Complete remaining evaluation
- Establish the list of recommended schemes