The CRYPTREC Policy to Evaluate the Submitted Public Key Systems

October 10, 2001

Tsutomu Matsumoto

Chair, Public-Key Subcommittee

Graduate School of Environment and Information Sciences

Yokohama National University

Tasks

- Specific Evaluation
  - Signature Algorithms for Electronic Signature Law
  - Others
- 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

Possible Targets of 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
  - Submission completeness examination
  - Based on the submitted documents
    - 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 Sub-Committee
    - Members
    - A Number of

      Anonymous External Experts

      (World Class Cryptographers)

Public-Key Cryptography Sub-Committee

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)

Call for Comments

- Any comments are welcome to all aspects of the CRYPTREC Projects.
- Let us know any results on the security and performance evaluation of the submitted cryptographic systems.
- E-mail:

cryptrec-comment@ipa.go.jp