Trends and Challenges for Securer Cryptography

December 16, 2005

Hideki Imai
Institute of Industrial Science, University of Tokyo
Research Center for Information Security,
National Institute of
Advanced Industrial Science and Technology
What Can Happen Will Happen — Prepare for Cryptanalysis —

• Imminent Crises
  – WEP Vulnerability, Hash Function Crisis, Threats of Implementation-related Attacks, Y-00 Affaire

• Crisis in the Near Future
  – Cryptanalysis of 1024-bit RSA Cryptosystem

• Future Crisis
  – Cryptosystems of Long-term Security
Imminent Crises

- Serious flaws are found in many IT systems in practice or development.
- Some of them can be easily fixed. (The prevalence may be the problem.)
- Some of them require challenges.
- Some of them should be carefully treated to avoid disturbance.
- Some of them can never be fixed and should be discarded.
• WEP (Wired Equivalent Privacy) : A specification for protecting wireless access, especially of 802.11 (WEP provides protection only for wireless part, but not for wired part.)
• Serious attack was discovered in 2001
• WEP is available for almost all wireless LAN equipments and easy to handle. Therefore, WEP is still popular and continue to be used if it can be secured at small cost.
History of Battles over WEP

Kobara, Yoshida and Imai analyzes the attacks and identifies more advanced patterns of IVs and WEP keys to skip.

- **2001~**: New specs, TKIP and AES (Not interoperable with WEP)
- **2001~**: Some chip makers started skipping certain IVs, but they are incomplete yet
- **1999**: WEP was standardized

Attack

- **2001**: The key recovery attack was presented by Fluhrer, Mantin and Shamir., and then implemented

Prevention

Implemented tools are being improved

Keys can be recovered
**Hash Function Crisis**

- Hash function is a fundamental element of cryptographic techniques.
  - MD4, MD5; RIPEMD-160, SHA-1, SHA-256, SHA-384, SHA-512; Whirlpool

- Hash function must have at least onewayness and for high security collision (a pair of two input sequences generating the same hashed value) intractability.

  - Collision of MD5 (not in the CRYPTREC List, but widely used) can be found in eight hours on 1.6GHz computer.
  - Collision of SHA-1 can be found by computation of at most $2^{63}$ operations. This attack may not be a practical threat yet, but it will in the near future.
  - Flaw of MD5 can be a reason for invalidating evidence.
MD5 flaw pops up in Australian traffic court

Suspected flaws in a computer algorithm have invalidated a fine issued by a speed camera in Australia.

It turns out that a Sydney magistrate tossed out a speeding ticket after the Roads and Traffic Authority, a government agency, failed to prove in court that the algorithm was cryptographically sound.

In other words, the argument goes, the photos could have been altered along the way. "The integrity of all speed-camera offences has been thrown into serious doubt and it appears that the RTA is unable to prove any contested speed camera matter because of a lack of admissible evidence," one defense lawyer boasted. The algorithm in question, called MD5, is one of the standard choices that programmers use when creating digital signatures. But some research has suggested attacks on MD5 (though those attacks remain largely impractical).

It's not clear what happens next. Australia's RTA could switch to a more secure algorithm (SHA-1 would be a contender) to digitally sign photographs -- or simply mount a more aggressive defense of its technique the next time this comes up in traffic court.

Posted by Declan McCullagh
Threats of Implementation-related Attacks

• Attacks based on defects of implementation
• Tampering modules that are critical to the security of the system
  – Invasive analysis
  – Non-invasive analysis
    • Side-channel attack
# Examples of Tampering Techniques

<table>
<thead>
<tr>
<th>Invasive Analysis</th>
<th>Non-invasive Analysis</th>
<th>Side-channel attack</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Probing</strong></td>
<td><strong>Fault-based Analysis</strong></td>
<td></td>
</tr>
<tr>
<td>A technique to probe signal after exposing surface of chips and removing protective coating</td>
<td>A technique to derive internal confidential information using the difference between normal output and faulty output caused artificially</td>
<td></td>
</tr>
<tr>
<td><strong>Timing Analysis</strong></td>
<td><strong>Power Analysis</strong></td>
<td></td>
</tr>
<tr>
<td>A technique to estimate confidential information by analyzing processing time</td>
<td>A technique to estimate confidential information by observing power consumption</td>
<td></td>
</tr>
</tbody>
</table>
Vulnerability of Smart Card Systems

- Smart cards are not necessarily tamper-resistant against skillful attackers.
- A smart card system relying on the tamper resistance of the smart card may be eventually broken.
- The system should be designed so that the damage caused by leakage of secret data stored in the smart card may be limited and compensated.
- Comprehensive evaluation of security of the system including tamper resistant property of the smart card is essential.
Quantum Cryptography

- Based on one of the most fundamental laws of the universe (QT: quantum theory)
- Achieves unconditional security (if the adversary can attack only the channel and QT is correct)

Almost unique practical solution to achieve the unconditional security

Numerous R&D are going on, including commercialization

- Mainly based on BB84: QKD (Quantum Key Distribution) system proposed by Bennett and Brassard in 1984
The Y-00 Affair

Difficulty of quantum cryptography brought about the Y-00 affair. Y-00 is a QKD protocol proposed by Yuen’s group in 2000, but its principle is totally different from that of BB84.

Yuen et al. are claiming that the Y-00 is superior to BB84
  Direct encryption with unconditional security is possible
  Good compatibility with existing photonic network technology

Their propaganda was very misleading

Example of Misled Argument: The Y-00 protocol is the most suitable for the developing broadband and long-distance communication technologies, since it can be proved by quantum detection theory that the protocol is unconditionally secure and is as efficient as the speed of the photonic telecommunication technology. (S. Tsujii: “Cryptographic technology for e-society” IPSJ Magazine, vol.45, Nov. 2004, originally in Japanese)
Security of the Y-00

• Yuen and his supporters claimed that “unconditional security” of the protocol could be proved on the basis of the following:
  – Unavoidable error exists when one tries to distinguish two non-orthogonal quantum states.
  – The error of legitimate user who is privy to an optimal way of the distinction is always less than that of attackers who are not privy to it.

• However, they missed the fact that there was another way to attack Y-00.
  – The real problem is that they do not have a good cryptographer.

• Through our analysis, the Y-00 proved to be a simple classical stream cipher
  – Their claim was simply based on their adversary model which was so restricted that they could prove the security against such an adversary.
  For the details, see also [Nishioka-Hasegawa-Ishizuka-Imafuku-Imai04] (PLA 327), and [Nishioka-Hasegawa-Ishizuka-Imafuku-Imai05] (to appear in PLA)
What We Learned from the Y-00 Affair

• For developers and users, to get reliable information is often difficult.
  – Feature of quantum cryptography
    • A good physicist is not always a good cryptographer.
  – Cryptographic approach involving good cryptographers is essential for the research on quantum cryptography.

• Wrong information sounds sweet, and spreads fast (and is difficult to correct them.)

• Framework for evaluation is crucial as well as classical one.
Crisis in the Near Future

• Cryptography is becoming weaker year by year due to the progress of cryptanalysis and computers, changes of technical environment, etc.
• Some cryptographic techniques will be broken before 2020.
• The most serious threat is the attack to 1024-bit RSA, which is used as users’ digital signature schemes in almost all practical public-key cryptosystems.
Cryptanalysis of 1024-bit RSA Cryptosystem

- It is reasonable to predict that 1024-bit RSA will be broken within 10 years.
  - Progress of computing technology
  - TWIRL: The Wizezman Institute Relation Locator; $10M Dedicated HW to compute one 1024-bit key/year
  - Wafer Scale Integration, 582 wafers (30cm, 0.13 \( \mu \)m rule, 1GHz Clock) Shamir, Tromer … CRYPTO’03

- We have substitutes: 2048-bit RSA, elliptic curve cryptosystems
Number of digits of $n = pq$ ($p, q$: primes of similar size) that can be factored

Insecure RSA Key-length

Quantum Computer

TWIRL

<table>
<thead>
<tr>
<th>512 bits</th>
<th>1024 bits</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td></td>
</tr>
<tr>
<td>50</td>
<td></td>
</tr>
<tr>
<td>100</td>
<td></td>
</tr>
<tr>
<td>150</td>
<td></td>
</tr>
<tr>
<td>200</td>
<td></td>
</tr>
<tr>
<td>250</td>
<td></td>
</tr>
<tr>
<td>300</td>
<td></td>
</tr>
<tr>
<td>350</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>year</th>
<th>number of digits</th>
</tr>
</thead>
<tbody>
<tr>
<td>1960</td>
<td>0</td>
</tr>
<tr>
<td>1970</td>
<td>50</td>
</tr>
<tr>
<td>1980</td>
<td>100</td>
</tr>
<tr>
<td>1990</td>
<td>150</td>
</tr>
<tr>
<td>2000</td>
<td>200</td>
</tr>
<tr>
<td>2010</td>
<td>250</td>
</tr>
<tr>
<td>2020</td>
<td>300</td>
</tr>
<tr>
<td>2030</td>
<td>350</td>
</tr>
<tr>
<td>2040</td>
<td>?</td>
</tr>
</tbody>
</table>
• For the future we must assume the emergence of practical quantum computers.
• Quantum computers can do super-parallel computing in use of quantum effects.
• If practical quantum computers appeared, almost all current public-key cryptosystems such as RSA and elliptic-curve cryptosystems would be broken.
• It may take 50 years to realize practical quantum computers.（It requires some breakthrough.）
• Challenge is to create efficient cryptosystems of long-term security.
Cryptosystems of Long-term Security

There are various possibilities of constructing cryptosystems of long-term security, which will survive after the emergence of practical quantum computers. They are divided into four types from the aspect of the basis for their security:

• Computational security
  – Public-key cryptosystems based on computational assumptions other than the integer factoring problem and discrete logarithm problem.
  – McEliece, Lattice, SFLASH,…
  – Still depend on unproven assumptions.
• **Physical security (Security based on physics)**
  – Based on tamper-resistant modules (TRM) (A TRM is a module (HW or SW) for which information stored in it is protected from improper access)
  – Evaluating the security of TRM is difficult
  – Quantum physics ⇒ unconditional security

• **Human-oriented security**
  – Based on the memory shared among many people (or a few people who can be trusted for a long time)
  – Mostly hash functions are used (Based also on computational security)
  – Difficult to prove the security
• **Information-theoretic security (Unconditional security)**
  – Based on only the difference of pre-distributed information owned by the authorized users and the adversaries.
  – Ultimate security, but requires much cost.
2005 IEEE Information Theory Workshop on Theory and Practice in Information-Theoretic Security (ITW05 Japan)
October 16-19, 2005, Awaji Island, Japan

[Place] Awaji Yumebutai International Conference Center
[Participants (expected number)] 85 people
[Significance] The purpose of this workshop is to further develop and disseminate research area of information-theoretic security which is the boundary area between information theory and information security.

Topics include (but are not limited to)
Theoretical and practical topics concerning information-theoretic security
Information theory applicable to information security
Applications of information theory to computational security
Topics in the bounded storage model and the noisy channel model
Quantum information theory applicable to information security
Quantum cryptography
Technical Program of ITW’05 Japan

Authenticated Encryption and Steganography in Unconditional Security Setting
Tsutomu Matsumoto

Unconditionally Secure Signatures and its Related Schemes
Goichiro Hanaoka

The Commitment Capacity of the Gaussian Channel is Infinite
Kirill Morozov

How to Attain the Ordinary Channel Capacity Securely in Wiretap Channels
Hirosuke Yamamoto

A Brief History of Quantum Cryptography
Gilles Brassard

Quantum Reverse Shannon Theorem - beyond IID sources
Charles Bennett

A New Approach in Quantum Cryptography - Achieving Provable Security by Restricting the Attacker’s Quantum Memory
Serge Fehr

Cryptographic Primitives from Einstein-Podolsky-Rosen Correlations
Stefan Wolf

Temporary Assumptions -Quantum and Classical
Joern Mueller-Quade
Michael Rabin

Hyper-Encryption via Virtual Satellite, a Poor Person's Unbreakable Encryption

Chi-Jen Lu

Randomness Extractors in Cryptography

Yvo Desmedt

Unconditionally Private and Reliable Communication in an Untrusted Network

Matthias Fitzi

Broadcast and Secure Computation Under Reduced Setup Assumptions

Moti Yung

Cryptography and Reed-Solomon Codes as a Hard Problem

Anne Canteaut

Fast Correlation Attacks Against Stream Ciphers and Related Open Problems

Kaoru Kurosawa

Some Topics Related to Resilient Functions

Keith Martin

Dynamic Access Policies for Unconditionally Secure Secret Sharing Schemes

Hiroki Koga

Coding Theorems on the Threshold Scheme for a General Source

Tatsuaki Okamoto

Relationship of Three Cryptographic Channels in the UC Framework

Yevgeniy Dodis

On Extractors, Error-Correction and Hiding All Partial Information

Carlo Blundo

Self-Healing Key Distribution Schemes

Rei Safavi-Naini

Bounds on Authentication Systems in Query Model

Rafail Ostrovsky

Cryptography from Anonymity
Guardian of Cryptography — CRYPTREC —

- CRYPTOgraphy Research and Evaluation Committees

- Background of CRYPTREC
  - e-JAPAN Priority Policy Program (2001)

- Main Purpose
  to make and maintain a list of cryptographic techniques for the common security basis to the Japanese e-Government (List of the e-Government Recommended Cryptographic Techniques)
From April 2000 to March 2003

- Open calls for cryptographic techniques in 2000 and 2001
- Received 61 submissions
- Add 24 cryptographic techniques as the cryptographic techniques to be evaluated
- Evaluated 85 cryptographic techniques
  - Entrusted the evaluation to top cryptographers in the world
  - Discussed the selection at the CRYPTREC meetings on the basis of 173 reports from the entrusted cryptographers
- Selected 29 cryptographic techniques
- Published the CRYPTREC List in March 2003
- The ministries agreed to use ciphers in the CRYPTREC List for e-Government

http://www.cryptrec.jp/
CRYPTREC e-Government
Recommended Ciphers List (1/4)

- Asymmetric Ciphers
  - Signature
    - DSA
    - ECDSA
    - RSASA-PKCS1-v1 *1
    - RSA-PSS
  - Confidentiality
    - RSA-OAEP
    - RSAES-PKCS1-v1 *1
  - Key Agreement
    - DH
    - ECDH
    - PSEC-KEM *2
CRYPTREC e-Government
Recommended Ciphers List (2/4)

- Symmetric Ciphers
  - 64-bit block ciphers
    - CIPHERUNICORN-E
    - Hierocrypt-L1
    - MISTY
    - 3-key Triple DES *4
  - 128 bit block ciphers
    - AES
    - Camellia
    - CIPHERUNICORN-A
    - Hierocrypt-3
    - SC2000
CRYPTREC e-Government
Recommended Ciphers List (3/4)

- **Stream ciphers**
  - MUGI
  - MULTI-S01
  - 128-bit RC4 *5

- **Others**
  - **Hash Functions**
    - RIPEMD-160 *6
    - SHA-1 *6
    - SHA-256
    - SHA-384
    - SHA-512

- **Pseudo-random number generators**
  - Omitted
*1 Use of this is permitted for the time being because it was used in SSL3.0/TLS1.0.

*2 On the assumption that this is used in the KEM (Key Encapsulation Mechanism)-DEM (Data Encapsulation Mechanism) construction.

*3 When constructing a new e-Government system, 128-bit block ciphers are preferable if possible.

*4 Using the 3-key Triple DES is permitted for the time being under the following conditions:
   1) It is specified as FIPS 46-3.
   2) It is positioned as the de facto standard.

*5 It is assumed that the 128-bit RC4 will be used only in SSL3.0/TLS(1.0 or later). If any other cipher listed above is available, it should be used instead.

*6 If any ciphers with a longer hash value are available when constructing a new e-Government system, it is preferable that a 256-bit (or more) hash function be selected. However, this does not apply in cases where the hash function to be used has already been designated according to the public-key cryptographic specifications.
CRYPTREC Committees
(March 2003-Present)

CRYPTREC Advisory Committee
Chair: Hideki Imai
(Secretariat: MIC and METI)

Cryptographic Technique Monitoring Committee
(Chair: Hideki Imai)
(Secretariat: NICT and IPA)
(1) Monitoring e-Government recommended ciphers
(2) Research and examination focusing on cryptographic algorithms, etc.
(3) Research and examination related to the revisions of e-Government recommended ciphers list

Cryptographic Module Committee
(Chair: Tsutomu Matsumoto)
(Secretariat: NICT and IPA)
(1) Creation of evaluation criteria and test requirements for cryptographic modules
(2) Research and examination focusing on Cryptography implementation related technology
(Preparation for CMVP)

Cryptographic Technique Research WG

MIC: Ministry of Internal Affairs and Communications
METI: Ministry of Economy, Trade and Industry
NICT: National Institute of Information and Communications Technology
IPA: Information-technology Promotion Agency, Japan
Japanese Cryptographic Module Validation Program (J-CMVP)

- Cryptographic algorithms from CRYPTREC List and ISO Standards
- Conformance test based on FIPS 140-2, ISO/IEC 19790 and our research results
- Preparing for
  - Regulations, Rules, etc.
  - Training Validator and Testers
- In April 2007, validation will start.
  - Certification body : IPA Security Center
  - Independent testing laboratories based on ISO/IEC 17025
Future Plan of CRYPTREC

CRYPTREC (2000-2002FY)
NESSIE E
AES

CRYPTREC (From 2003FY)

ISO15408(CC)
ISO17799(ISMS)

Quantum Cryptography

Algorithm Evaluation

Standardization

Implementation

Cryptographic Modules

Cryptographic Protocols

Application Systems

Compound Systems
For achieving information security there is no case where you may neglect cryptography.

- Cryptography can be applied to improve information security in every information system.
- Concepts and methods of cryptography can be foundation of the design of information security.

⇒ Cryptographic Approach
Cryptographic Approach

- Modern cryptology is the science treating information security in the most rigid manner and has been successful in securing cryptosystems. It is natural to apply concepts and techniques produced in cryptology to problems concerning information security.

This is cryptographic approach to information security.

- Cryptographic approach will provide strategy to information security measures

- Fundamental remedy to root out the attacks (in the assumed adversary model), rather than temporal countermeasure for each attack to IT systems
**Typical Cryptographic Approach (1)**

- **Definition of models**
  - System model (+Trust model)
  - Adversary model (Be proactive)
    (eg assumptions on the information and computing capability owned by the adversary in case of encryption for confidentiality)

- **Definitions of security**
  - Extracted from security requirements
  - Should be treated mathematically
  - With clear assumptions
    - **computational assumption**, information theoretical assumption, physical assumption etc.
      (eg factoring the product of two prime integers of more than 155 digits is intractable)
Typical Cryptographic Approach (2)

• Evaluation of security
  – **Theoretical evaluation**
    • Computational approach, Information theoretic approach, Formal approach, etc.
    • Proof of security is required
      – Newly proposed public-key cryptography must be provably secure (CRYPTREC)
    • Impossible to evaluate every system theoretically
  – Empirical evaluation
    • Security of symmetric ciphers depends on empirical evidence
  – Hybrid evaluation
    • Theoretical to generic attacks
  – Compound systems
    • Theory for theoretical evaluation is making progress
Why Cryptographic Approach?

• Cryptographic approach is the most important basis of information security techniques.
• Cryptography has advanced and systematic theory.
  – Concepts of security are established
  – Many theoretical tools to prove the security
• Cryptographers are skilled in finding vulnerabilities from every aspect.
Contribution of Cryptographers to Other Areas of Information Security

- Experiments of Prof. Tsutomu Matsumoto (Yokohama National Univ.) to impersonate against identification systems using fingerprints.
  - One of the most important research results in the area of biometrics identification.
  - R & D of biometrics identification has been conducted from the aspect of pattern recognition, where no intelligent adversary exists.
  - Cryptographers are trained to believe that human nature is essentially bad.

To Err Is Human…
—Fait-Safe Techniques for Information Security—

• IT security measures are being developed.
  – Many IT-related laws have been enacted.
  – Government structure for information security has been improved.
  – IT security evaluation and certification schemes have been developed.
  – Systems for collecting and distributing vulnerability information have been created.

• But problems keep occurring.
Because

- IT-related systems are prone to be sacrificed for convenience. Thus, the security level becomes low.
  → Shoring up of IT-related laws and enlightenment
- Difficult to determine the reliable source of security information
  → Creation of reliable distributors of security information
- Although problems are solved at some point, new problems keep occurring.
  → Continuous monitoring
These are issues still to be tackled, and what’s more…
- Human factor plays a big role (It is impossible to prevent human errors and insider attacks completely)
  ⇒ Humancrypt (Key to achieve safety)
**Humancrypt (Human Crypto+)**

- Humancrypt means cryptographic approach to information security issues concerning relation between human beings and computers.
  - Cryptographic techniques to make authentic user’s access to computers secure and easy
  - Human interface techniques to make cryptosystems easy to use
  - Techniques to generate confidence in the use of cryptosystems
  - Techniques to incorporate human factors into cryptosystems (typical human-oriented cryptography)
  - ...
  - Techniques to tolerate human errors in information security

⇒ Fail-safe information security technology
Fail-Safe Information Security Technology

- Technology that may fundamentally change the present state of cryptographic infrastructures such as PKI
- In designing cryptographic infrastructures, we should give up the conventional assumption that classified information won’t leak, and instead, should develop technology that will minimize the damage when the information is leaked, and secure the continuity of cryptographic infrastructure.
- A wide range of applications: measure against leakage of personal data; protection against unauthorized usage of the contents on the site; medical information protection; securing business continuity; disaster recovery, etc.
Core Techniques of Fail-Safe Information Security Technology

- It is essential to develop core techniques to efficiently protect the system from leakage of stored secrets.
  - Authenticated key establishment robust against leakage of stored secrets (LR-AKE: Shin-Kobara-Imai04) [Leakage of stored secrets does not damage the password (that may be short) or the session keys of past and future]
  - Public key cryptosystems robust against leakage of stored secrets (Attrapadung-Hanaoka-Imai04: generalization and unification)
  - Implementation techniques robust against leakage of stored secrets (Hanaoka-Hanaoka-Shikata-Imai05)
**LR-AKE (Leakage-Resilient Authenticated Key Exchange)**

- **Password**: Client
- **Server 1**: LR-AKE
  - Secret Data 1
  - Verification Data 1
  - SK1
- **Server 2**: LR-AKE
  - Secret Data 2
  - Verification Data 2
  - SK2

**Leakage-Tolerant (LT) Data**
- (Renewed every time to generate a new session key)
- Leakage of LT-data does not reveal the other session keys unless it happens at both client and server.

**Session Key**
Toward Higher Level of Security — RCIS/AIST —

An Introduction to Research Center for Information Security (RCIS)
National Institute of Advanced Industrial Science and Technology (AIST)
http://unit.aist.go.jp/rcis/
RCIS

- Research Center for Information Security (RCIS), National Institute of Advanced Industrial Science and Technology (AIST)
- Founded in April 2005
- Location: 11th floor, Akihabara DAIBIRU, Tokyo

![map of Akihabara Station and RCIS location]
Organization of RCIS (Oct. 2005)

Director: Prof. H. Imai (Invited, U. of Tokyo)

Research Advisors:
Prof. I. Nakajima (Invited, Tohoku U.)
Prof. T. Matsumoto (Invited, Yokohama National U.)

Deputy Directors:
Prof. A. Yonezawa (Invited, U. of Tokyo)
Dr. H. Watanabe

Administrative Staffs

RT for Security Fundamentals (6)
Leader: Dr. K. Kobara (Invited, U. of Tokyo)

RT for Physical Analysis (3)
Leader: Dr. K. Imafuku

RT of Software Security (6)
Leader: Prof A. Yonezawa (double)
Sub Leader: Prof. E. Shibayama (Invited, Tokyo Institute of Tech)

Full-Time Researchers: 12 (to 20 in next April)
Part-Time Researchers: 6
Post-Doctoral Research Scientist: 0 (to 2 or 3, now planning)
Researchers from Companies: 1 (to 2 or 3, now planning)
The Roles of the RCIS

• Creating a core information security research center in order to release the world-level research results constantly
  – Establishing a new academic area of information security
  – Developing theory for applying information security techniques in practice
  – Conducting top-level researches in the world
  – Promoting the coordination to create synergism
  – Representing the security research organizations of Japan

• Supporting information security-related government policy execution
  – Providing reliable information on information security researches
  – Developing security evaluation techniques for critical infrastructures

• Training high-level experts
Teams of RCIS

Security Technology for **Hardware Products** ⇒ Research Team for Physical Analysis
Security Technology for **Software Products**
  ⇒ Research Team for Software Security
Security Technology Used in Those Products
  ⇒ Research Team for Security Fundamentals

There are rare research bases treating such three areas.

**Collaboration** of these team creates new security technology.
Study on Cryptographic Techniques

1. New cryptographic technology with high functionality
   – Anonymous authentication
   – Information leakage resilient technique...

2. Security evaluation for cryptographic technologies
   – Mathematical security proof of public key cryptography...
Research Team for Physical Analysis

Study for Developing Secure Hardware Products

1. Security evaluation in implementation of secure hardware module such as IC cards

2. New information security technology based on physical laws
   - Quantum cryptography
   - Quantum information and communication theory…

3. Security evaluation of quantum information security technology
Research Team for Software Security

Study for Developing Secure Software Products

1. Secure software system
   - Secure C, C++ language compilers
   - Secure and practical programming languages
   - Analyzing technique of computer viruses/worms
   - Formal security verification of software products

2. Pragmatic security verification system
   - Vulnerability checking tool for Web servers
   - Vulnerability checking tool for Web applications
Position of the Research Center

RCIS

Government

Security-related Public Organizations (IPA, NITE, JQA, JEITA etc.)

Standardization Organizations

Providing Information

Information Sharing

Think Tanks

Security-related Public Research Institutes (NICT etc.)

CRYPTREC

Standardization Activities

Projects

Collaboration Research

Academic Societies

Presenting Results

Universities (The University of Tokyo etc.)

Industry
Conclusion

• It is a big challenge to keep cryptosystems secure
• Cryptographic approach will become more and more important
• When you want to solve an information security problem, you must look for a good cryptographer.
• If you cannot find a good cryptographer around you, we are pleased to help you.