What Can Cryptography Guarantee?

Que peut nous garantir la cryptographie ?

David Pointcheval
Ecole normale supérieure
Fondation Sciences Mathématiques de Paris
September 27th, 2011

Security of Communications

One ever wanted to exchange information securely

With the all-digital world, security needs are even stronger...

In your pocket

But also at home

First Encryption Mechanisms

The goal of encryption is to hide a message

Scytale
Permutation

Alberti’s disk
Mono-alphabetical Substitution

Wheel – M 94 (CSP 488)
Poly-alphabetical Substitution

Substitutions and permutations

Security relies on the secrecy of the mechanism

⇒ How to widely use them?

Common Parameter

A shared information (secret key) between the sender and the receiver parameterizes the public mechanism

Enigma:
choice of the connectors and the rotors

Security looks better: but broken (Alan Turing et al.)

⇒ Security analysis is required
Practical Secrecy

Perfect Secrecy vs. Practical Secrecy

- No information about the plaintext $m$ can be extracted from the ciphertext $c$, even for a powerful adversary (unlimited time and/or unlimited power): perfect secrecy
- In practice: adversaries are limited in time/power ⇒ complexity theory

We thus model all the players (the legitimate ones and the adversary) as Probabilistic Polynomial Time Turing Machines:

Computational Security Proofs

- a formal security model (security notions)
- a reduction: if one (Adversary) can break the security notions, then one (Simulator + Adversary) can break a hard problem
- acceptable computational assumptions (hard problems)

Integer Factoring

**Records**

Given $n = pq$ → Find $p$ and $q$

<table>
<thead>
<tr>
<th>Digits</th>
<th>Date</th>
<th>Bit-Length</th>
</tr>
</thead>
<tbody>
<tr>
<td>130</td>
<td>April 1996</td>
<td>431 bits</td>
</tr>
<tr>
<td>140</td>
<td>February 1999</td>
<td>465 bits</td>
</tr>
<tr>
<td>155</td>
<td>August 1999</td>
<td>512 bits</td>
</tr>
<tr>
<td>160</td>
<td>April 2003</td>
<td>531 bits</td>
</tr>
<tr>
<td>200</td>
<td>May 2005</td>
<td>664 bits</td>
</tr>
<tr>
<td>232</td>
<td>December 2009</td>
<td>768 bits</td>
</tr>
</tbody>
</table>

**Complexity**

- $768$ bits $\rightarrow 2^{54}$ op.
- $1024$ bits $\rightarrow 2^{80}$ op.
- $2048$ bits $\rightarrow 2^{112}$ op.
- $3072$ bits $\rightarrow 2^{128}$ op.
- $4096$ bits $\rightarrow 2^{150}$ op.
- $7680$ bits $\rightarrow 2^{192}$ op.

- Lossy reduction: $T = k^3 \times t$
  
  - Adversary running time $t$
  - Algorithm running time $T = f(t)$

- Tight reduction: $T \approx t$
  
  With $k = 2048$ and $t < 2^{110}$, one gets $T < 2^{110}$

Proof by contradiction
Public-Key Encryption

Goal: Privacy/Secrecy of the plaintext

RSA-OAEP (PKCS #1 v2.1)

The Plain RSA Encryption

\[ \mathcal{G}(1^k) : n = pq, sk \leftarrow d = e^{-1} \mod \varphi(n) \text{ and } pk \leftarrow (n, e) \]

\[ \mathcal{E}(pk, m) = c = m^e \mod n ; D(sk, c) = m = c^d \mod n \]

Deterministic and malleable: \textbf{randomness and redundancy}

- \( m \) is the message to encrypt
- \( r \) is the additional randomness to make encryption probabilistic
- \( 00 \ldots 00 \) is redundancy to be checked at decryption time

Then, \( c = RSA(X \| Y) \)

Theorem (IND-CCA Security) [Fujisaki-Okamoto-Pointcheval-Stern – Crypto ’01]

\( RSA-OAEP \) is IND-CCA secure under the RSA assumption

RSA-OAEP Security Proof [Fujisaki-Okamoto-Pointcheval-Stern – Crypto ’01]

\[ c = f(X \| Y) \]

To get information on \( m, H(X) \) queried

\[ \implies \text{ partial inversion of } f \]

\[ c = RSA(X \| Y) \]

RSA: partial inversion and full inversion are equivalent (but at a loss)

If an adversary breaks IND-CCA within time \( t \), one can break RSA within time \( T \approx 2t + 3qH^2k^3 \) (\( qH \) = number of Hashing queries \( \approx 2^{60} \))

\[ k = 2048 \quad (2^{112}) \quad t < 2^{110} \quad T < 2^{155} \]

\[ k = 4096 \quad (2^{150}) \quad t < 2^{110} \quad T < 2^{158} \]

\[ \implies \text{ large modulus:} \]

\[ > 4096 \text{ bits!} \]

\[ \mathcal{E}(pk, m, r) = (c_1 = r^e \mod n, c_2 = G(r) \oplus m, c_3 = H(r, m, c_1, c_2)) \]

Security reduction between IND – CCA and the RSA assumption:

\[ T \approx t \implies 2048\text{-bit RSA moduli provide } 2^{110} \text{ security} \]
**Lattice-Based Cryptography**

- **Lattice Problems**
  - Shortest Vector
  - Small Basis (Reduced)
  - Closest Vector

- **Properties**
  - Worst-case/Average-case Reductions
  - No quantum attack known

- **Related Problems**
  - Learning With Errors
  - Knapsack Problem

- **Cryptographic Primitives**
  - Identity Based Encryption
  - Fully Homomorphic Encryption

---

**Conclusion**

With provable security, one can precisely get:
- the security games one wants to resist against any adversary
- the security level, according to the resources of the adversary

But, it is under some assumptions:
- the best attacks against the underlying problems
- no leakage of information excepted from the given oracles

Cryptographers’ goals are thus
- analysis of the underlying problems / new problems
- realistic and strong security notions (games)
- accurate model for leakage of information (oracle access)
- tight security reductions

**Implementations and uses must satisfy the constraints!**