RSA-OAEP and Cramer-Shoup

Olli Ahonen
Laboratory of Physics, TKK

11th Dec 2007
T-79.5502 Advanced Cryptology
Part I: Outline

- RSA, OAEP and RSA-OAEP
- Preliminaries for the proof
- Proof of IND-CCA2 security for RSA-OAEP
  - Setup and process
  - Decryption oracle service
  - Likelihood of success
  - Fujisaki's method
- Safe modulus size
Basic RSA

- Random primes $p$ and $q$
- Public $N = pq$; private $\Phi(N) = (p - 1)(q - 1)$
- Random public $e \in \mathbb{Z}_{\Phi(N)}^*$
- Private $d$ such that $ed \mod \Phi(N) = 1$
- Ciphertext $c = m^e \mod N$
- Decryption: $m = c^d \mod N$
- IND-CPA (i.e., semantically) secure
Basic RSA: not secure enough

- Assume: Alice acts as a decryption oracle, if the message appears random
- Malice wishes to decrypt $c = m^e \mod N$
  - Picks random $r \in \mathbb{Z}_N^*$
  - Sends to Alice $c' = r^e c \mod N$
  - Receives $rm \mod N$
  - Learns $m$ by division $\mod N$
Optimal asymmetric encryption padding (OAEP)

- M. Bellare and P. Rogaway in 1994
  - Add randomness
  - Mix the input
  - Encrypt with a one-way trapdoor permutation (OWTP), e.g., RSA

- IND-CCA2 secure
  - Assuming the OWTP really is one-way

- Practically efficient
OAEP structure

- $k_0 < |N|/2$
- Hash functions $G$ and $H$
- $s||t$ input to encryption
- E.g:
  - $|N| = 2048$
  - $k_0 = k_1 = 160$

RSA-OAEP algorithm

- $|N| = |m| + k_1 + k_0$; $2^{-k_0}$ and $2^{-k_1}$ negligible
- Encryption
  - $r = \text{rand}(k_0)$; $s = (m||0..0) \oplus G(r)$; $t = r \oplus H(s)$
  - $c = (s||t)^e \mod N$
- Decryption
  - $s||t = c^d \mod N$; $|s| = |m| + k_1$; $|t| = k_0$
  - $u = t \oplus H(s)$; $v = s \oplus G(u)$
  - If $v == m||0^{k_1}$, extract $m$; else reject
IND-CCA2 game

- Oracle provides PPT Malice with requested decryptions (except for $c^*$).
- Malice is capable if he guesses which of the two plaintexts $c^*$ encrypts.
- Required: non-negligible $\text{Adv} = 2 \Pr[\text{"correct guess" | history}] - 1$.
Random oracle

- Idealized hash function $G: \{0,1\}^k \rightarrow \{0,1\}^n$
- Output
  - Uniformly random (really!)
  - Deterministic
  - Efficient
- Imaginary
- Computationally indistinguishable from a good real-world hash function
Simulating a random oracle

- At startup, initialize $\mathcal{G}$-list to empty
- When value $\mathcal{G}(a)$ is queried
  - Lookup $a$ in $\mathcal{G}$-list
  - If not found
    - Generate random value for $\mathcal{G}(a)$
    - Store $(a, \mathcal{G}(a))$ in the $\mathcal{G}$-list
  - Return the stored value
- Precise local simulation in PPT
Proof of IND-CCA2 security

- General idea:
  - \( \exists \) algorithm \( A \) that is IND-CCA2 capable
  - \( \Rightarrow \) OWTP \( f \) (e.g., RSA) can be inverted
  - \( \Leftrightarrow \)
    - OWTP \( f \) is not invertible
    - \( \Rightarrow \) IND-CCA2 security
- "Reduction to contradiction"
- PPT algorithms, non-negligible advantages
RSA-inverting algorithm $M$

- Input: Random point $c^* = f(w^*)$
- Output: Preimage $w^* = f^{-1}(c^*)$
- Encapsulates IND-CCA2 capable $A$
- Random-oracle simulator of the OAEP hash functions $G$ and $H$ for $A$
- Decryption oracle for $A$
  - Based on the $G$- and $H$-lists
  - May reject even if $A$ submits a valid ciphertext
Inversion process

- $M$ plays two IND-CCA2 games with $A$
  - Round 1: $M$ challenges $A$ with $c^*$
    - $c^*$ has nothing to do with $(m_0, m_1)$!
  - Round 2: $M$ challenges $A$ with $c^*_2 = c^* \alpha^e \mod N$
    - Random $\alpha \in \mathbb{Z}_N^*$ (probability of bad $\alpha$ negligible)

- If $A$ queries $H(s^*)$ and $H(s^*_2)$, $M$ finds $f^{-1}(c^*)$
  - PT lattice method by Fujisaki et al.

- How probable are the queries?
- What if $A$ discovers $c^*$ is a hoax?
Decryption oracle service

- Maintain a list of potential ciphertext-plaintext tuples \( \{(f(w_i), w_i, v_i)\}_i \)
  
  For each \((g, G(g))\) for each \((h, H(h))\)
  
  \[ w = h || (g \oplus H(h)); \quad v = G(g) \oplus h \]

- If \( f(w_i) = c^* \), \( w_i = w^* = f^{-1}(c^*) \); success!

- To decrypt \( c \)
  - If \( c = f(w_i) \) and \( v_i = \Delta || 0..0 \), return \( \Delta = m \)
  - Else reject
Quality of the decryption service

- If $A$ creates a valid $c$ without $G$ or $H$, $M$ rejects $c$ illegally
- $(s, H(s))$ missing $\Rightarrow \Pr["r correct"] = 2^{-k_0}$
  $\Rightarrow \Pr[s \oplus G(r) = \Delta || 0^{k_1}] = 2^{-k_1}$
- Similarly for missing $(r, G(r))$
- If $G(r)$ or $H(s)$ not queried, reject is correct except for (negligible) $\Pr \sim 2^{-k_0} + 2^{-k_1}$
- Good decryption quality
Likelihood of successful inversion

- Define the following events
- **DBad** = $M$ rejects a valid ciphertext
- **AskH** = $A$ has queried for $H(s^*)$
- **AskG** = $A$ has queried for $G(r^*)$
- **AskH** or **AskG** may reveal the deception in $c^*$
  - **Bad** = **AskH** $\cup$ **AskG** $\cup$ **DBad**
- **AWins** = $A$ can correctly guess the IND-CCA2 game challenge bit $b$

$s^*||t^* = f^{-1}(c^*)$
$r^* = t^* \oplus H(s^*)$
$m^*||0..0 = s^* \oplus G(r^*)$
Likelihood of successful inversion

- \( \Pr[AWins | \neg Bad] \)
  \[ \equiv \frac{\Pr[AWins, \neg Bad]}{\Pr[\neg Bad]} = \frac{1}{2} \]
  \[ \Rightarrow \Pr[AWins, \neg Bad] = \frac{(1 - \Pr[Bad])}{2} \]

- \( \text{Adv} + \frac{1}{2} = \Pr[AWins] \)
  \[ \equiv \Pr[AWins, \neg Bad] + \Pr[AWins, Bad] \]
  \[ \leq \Pr[AWins, \neg Bad] + \Pr[Bad] \]
  \[ = \frac{\Pr[Bad]}{2} + \frac{1}{2} \]

- \( \Rightarrow \Pr[Bad] \geq 2\text{Adv} \)
Pr[A U B]
= Pr[A] + Pr[B] – Pr[A, B]
≤ Pr[A] + Pr[B]

Likelihood of successful inversion

- \( \Pr[\text{Bad}] \leq \Pr[\text{AskH} \cup \text{AskG}] + \Pr[\text{DBad}] \)
  
  = \( \Pr[\text{AskH}] + \Pr[\neg \text{AskH}, \text{AskG}] + \Pr[\text{DBad}] \)
  
  \leq \Pr[\text{AskH}] + \Pr[\text{AskG} | \neg \text{AskH}] + \Pr[\text{DBad}] 

- \( \text{AskG} | \neg \text{AskH} = G(r^*) \) has been queried when \( H(s^*) \) has not \( \Rightarrow \) \( \Pr[\text{AskG} | \neg \text{AskH}] = 2^{-k_0} \)

- \( \Pr[\text{AskH}] \geq 2(\text{Adv} – (2^{-k_0} + 2^{-k_1-1})) \)

- \( M \) obtains \( s^* \) with non-negligible probability
  - After this, \( M \) can let \( A \) know the truth about \( c^* \)
Fujisaki's method

- $|s^*| > |w^*|/2; \text{Int}(t^*) < \sqrt{N}$
- Use $s^*$ and $s^*_2$ to solve for $\text{Int}(t^*)$ in
  $$(2^{k_0} \text{Int}(s^*) + \text{Int}(t^*))^e \equiv c^* \pmod{N}$$
- $q = \text{larger H-list length}$
- For each pair $(s,s^*_2)$, solve for $\text{Int}(t)$ twice
- $\Rightarrow$ Inversion takes time $2\tau_A + q^2O((\log_2 N)^3)$
  $\tau_A = \text{running time of IND-CCA2 on RSA-OAEP}$
Practically safe parameters

- Evaluating $H$ and $G$ is very efficient in reality
- Dedicated attacker may make $q \approx 2^{50}$ queries
- Now RSA inversion time $> 2^{100} \gg 2^{86}$ for the Number Field Sieve method, if $|N| = 1024$
- $|N| = 2048$ considered safe
  - NFS takes time $2^{116}$
- $k_0 = k_1 = 160$ considered safe
- Up to 84% of $s||t$ can be actual message $m$
Part II: Outline

- Decisional Diffie-Hellman problem
- Cramer-Shoup scheme
  - Key setup
  - Encryption and decryption
- Overview of proof of IND-CCA2 security
  - DDH reduction
Decisional Diffie-Hellman problem

- Given
  - Description of an abelian group $G$
  - $(g, g^a, g^b, g^c) \in G^4; g = \text{gen}(G)$
- Is $ab \equiv c \pmod{\text{ord}(G)}$?
- Easy in supersingular elliptic-curve groups
- Hard in groups of finite fields
Cramer-Shoup

- R. Cramer and V. Shoup in 1998
  - CCA2-enhanced ElGamal encryption
  - More public and private parameters
  - Hashing
- IND-CCA2 secure
  - Assuming Finite-Field Decisional D-H is hard
- Data integrity check
- Resource need ~ twice that of ElGamal
Cramer-Shoup key setup

- Large prime $q = \text{ord}(G)$; $G = \text{plaintext space}$
- Pick random $g_1, g_2 \in G$
- Pick random $x_1, x_2, y_1, y_2, z \in [0,q)$
- $c = g_1^{x_1}g_2^{x_2}$; $d = g_1^{y_1}g_2^{y_2}$; $h = g_1^z$
- Choose a hash function $H: G^3 \rightarrow [0,q)$
- Public key: $(g_1, g_2, c, d, h, H)$
- Private key: $(x_1, x_2, y_1, y_2, z)$
Cramer-Shoup operation

● Encryption
  - Message $m \in G$; Pick random $r \in [0,q)$
  - $u_1 = g_1^r$; $u_2 = g_2^r$; $e = h^r m$
  - $\alpha = H(u_1, u_2, e)$; $\nu = c^r d^{r \alpha}$
  - The ciphertext is $(u_1, u_2, e, \nu)$

● Decryption
  - $\alpha = H(u_1, u_2, e)$
  - If $u_1^{x_1 + y_1 \alpha} u_2^{x_2 + y_2 \alpha} = \nu$, $m = e / u_1^z$
  - Else reject
Proof of IND-CCA2 security

- Same general idea as with RSA-OAEP:
  - ∃ algorithm $A$ that is IND-CCA2 capable
  - $\Rightarrow$ Finite-Field Decisional Diffie-Hellman can be answered efficiently by $M_A$
  - $\Leftrightarrow$
    - FFDDH is hard $\Rightarrow$ IND-CCA2 security

- Better than the proof for RSA-OAEP
  - No need for controversial random oracles
  - Reduction DDH $\rightarrow$ IND-CCA2 is linear
Reduction

- $M_A$: Can the arbitrary input $(g_1, g_2, u_1, u_2) \in G^4$ be a Diffie-Hellman quadruple? (DDH)
- Play the IND-CCA2 game with $A$
  - Receive chosen $(m_0, m_1)$, challenge with $C^*$
- Input is a DHq $\Rightarrow C^*$ encrypts $m_b$
- Input is not a DHq $\Rightarrow C^*$ uniformly distributed
- Based on $A$'s guess on $b$, $M_A$ can decide whether $(g_1, g_2, u_1, u_2)$ is a DHq or not