Provable Security and Ideal Models

Workshop on Provable Security eCrypt – AZTEC

Versailles – France – November 2004

David Pointcheval
CNRS-ENS, Paris, France

Summary

- Introduction to Provable Security
- The Random-Oracle Model
- The Ideal-Cipher Model
- The Generic Model
- Comparisons

Summary

- **Introduction to Provable Security**
- The Random-Oracle Model
- The Ideal-Cipher Model
- The Generic Model
- Comparisons

Algorithmic Assumptions *necessary*

- $n=pq$: **public modulus**
- e : **public exponent**
- $d=e^{-1} \bmod \varphi(n)$: **private**

RSA Encryption

- $\mathbf{E}(m) = m^e \bmod n$
- $\mathbf{D}(c) = c^d \bmod n$

If the RSA problem is easy,
privacy is not satisfied:
anybody may recover m from c

Algorithmic Assumptions *sufficient?*

Security proofs give the guarantee that the assumption is **enough** for security:

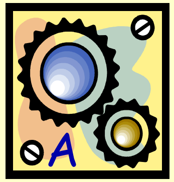
- if an adversary can break the security
- one can break the assumption

⇒ "reductionist" proof

Proof by Reduction

Reduction of a problem **P** to an attack *Atk*:

- Let *A* be an adversary that breaks the scheme
- Then *A* can be used to solve **P**

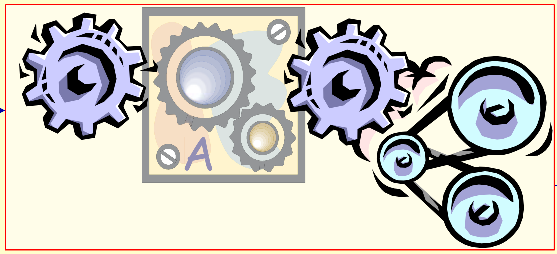


Proof by Reduction

Reduction of a problem **P** to an attack *Atk*:

- Let *A* be an adversary that breaks the scheme
- Then *A* can be used to solve **P**

Instance **I** of **P** →



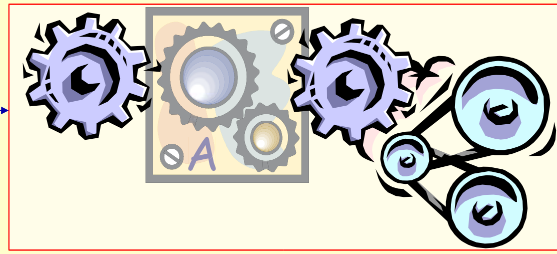
→ Solution of **I**

Proof by Reduction

Reduction of a problem **P** to an attack *Atk*:

- Let *A* be an adversary that breaks the scheme
- Then *A* can be used to solve **P**

Instance **I** of **P** →

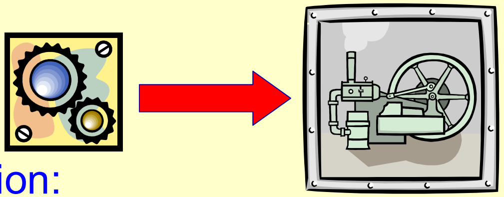


→ Solution of **I**

P intractable ⇒ scheme unbreakable

Complexity Theory

Adversary within t



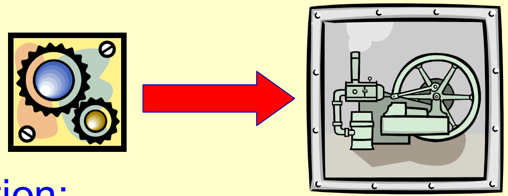
Algorithm against **P** within $t' = T(t)$

- Assumption:
  - **P** is hard = no polynomial algorithm
- Reduction:
  - polynomial = T is a polynomial
- Security result:
  - no polynomial adversary

  ⇒ no attack for parameters **large enough**

Exact Security

Adversary within t



Algorithm against **P** within $t' = T(t)$

- Assumption:
  - Solving **P** requires N operations (or time τ)
- Reduction:
  - Exact cost for T,
    in t, and some other parameters
- Security result:
  - no adversary within time t such that $T(t) \leq \tau$

Strong Security Notions

- Strong security (IND-CCA2, EF-CMA, ...)
  hard to achieve under standard assumptions
- There are candidates, but they are not
  as efficient as one would like
- Efficiency
  - is a requirement

    security must be transparent
  - also means

    efficient reduction

    bad reduction ⇒ larger parameters ⇒ inefficient in practice

Ideal Models

→ One makes some ideal assumptions:

- ideal random hash function:
  - random-oracle model (ROM)
- ideal symmetric encryption:
  - ideal-cipher model (ICM)
- ideal group:
  - generic model (GM = generic adversaries)

→ They help to prove efficient schemes
or to get efficient reductions

Summary

The Random-Oracle Model

Bellare-Rogaway 1993

- The most admitted model
- It consists in considering some functions
  as perfectly random functions,
  or replacing them by random oracles:
  - each new query is returned a random answer
  - a same query asked twice receives twice
    the same answer

f-OAEP Construction

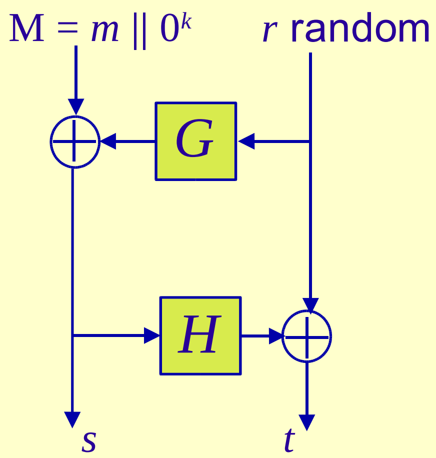
Bellare-Rogaway 1994

E(m) : $c = f(s \,||\, t)$

D(c) : $s \,||\, t = f^{-1}(c)$

then invert OAEP,

if the redundancy
is satisfied, one returns m



G, H: hash functions

f-OAEP IND-CCA2: Result

Fujisaki-Okamoto-Pointcheval-Stern 2001

- In the ROM for G and H,
  for any partial-domain T-OWP f :

$$\mathrm{Adv}^{ind}(t) \leq 2 q_H \times \mathrm{Succ}_f^{pd-ow}(t + q_G q_H T_f, q_H) + 2 \times \left(\frac{q_D}{2^k} + \frac{q_G + q_D + q_G q_D}{2^\ell} \right)$$

- Main contribution in the cost: the simulation of the decryption oracle on c' is in quadratic time
  - For all 4-tuples $(r, g{=}G(r), s, h{=}H(s))$: $q_G\, q_H$ possibilities
    - Complete into $(r, g, s, h, c{=}f(s,t))$ for $t = r \oplus h$
    - On c', look for (r', g', s', h', c'), get/check $M = s' \oplus g' = m \,||\, 0^k$

f-OAEP IND-CCA2: Exact Security

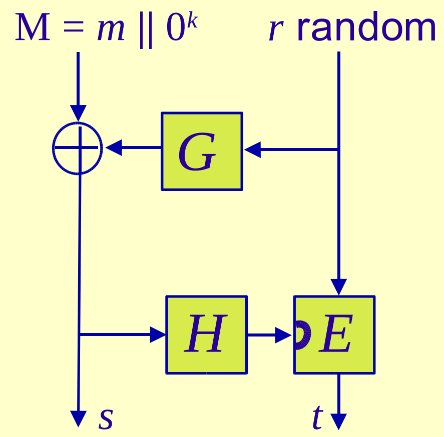
$$\mathrm{Adv}^{ind}(t) \leq 2 \times \sqrt{\mathrm{Succ}_f^{ow}\left(2t + q_H(2q_G + q_H)K^3, q_H\right)}$$

- Security bound: 2^{75}, and 2^{55} hash queries
- If one can break the scheme within time T, one can invert f within time T'
  $\leq 2T + 2q_H(2q_G + q_H)K^3$
  (or just $2T + 2q_H(2q_G + q_H)K^2$ with small e)
  $\leq 2^{76} + 6 \cdot 2^{110} K^2 \leq 2^{113} K^2$
- RSA: 1024 bits $\rightarrow 2^{133}$ (NFS: 2^{80}) ✘
  2048 bits $\rightarrow 2^{135}$ (NFS: 2^{111}) ✘
  4096 bits $\rightarrow 2^{137}$ (NFS: 2^{149}) ✔

Improvement: OAEP++

Jonsson 2002

The one-time pad is replaced by a strong block cipher E



G, H: hash functions
E: block cipher

Summary

- Introduction to Provable Security
- The Random-Oracle Model
- **The Ideal-Cipher Model**
- The Generic Model
- Comparisons

The Ideal-Cipher Model

It consists in considering a cipher E_k as a family of perfectly random and independent permutations:

- For each key k, E_k is a random permutation:
  - Maintain of a list $\Lambda_E = \{(k,m,c = E_k(m))\}$ set to empty
  - For each query $E_k(m)$, check whether there is c such that $(k,m,c) \in \Lambda_E$, answer c
  - For each query $D_k(c) = E_k^{-1}(c)$, check whether there is m such that $(k,m,c) \in \Lambda_E$, answer m
  - Answer a random element and update Λ_E

f-OAEP^{++}: Decryption Simulation

- ICM + ROM ⇒ the simulation of the decryption oracle on c becomes linear:

  For all 4-tuples (s,h,r,t) such that $h=H(s)$ and $t = E_h(r)$
  less than q_E possibilities (unless H-collision)

  - Complete into $(s,h,r,t,c = f(s,t))$
  - Upon receiving c', look for (s', h', r', t', c'),
    get/check $M = s' \oplus g' = m \,\|\, 0^k$

f-OAEP^{++} IND-CCA2: Exact Security

- Security bound: 2^{75}, and 2^{55} hash queries
- If one can break the scheme within time T, one can invert f within time T'
  $\leq T + q_E K^2 \leq 2^{75} + 2^{55} K^2$
- RSA:
  - 1024 bits → 2^{75} (NFS: 2^{80}) ✔
  - 2048 bits → 2^{77} (NFS: 2^{111}) ✔
  - 4096 bits → 2^{79} (NFS: 2^{149}) ✔

Summary

- Introduction to Provable Security
- The Random-Oracle Model
- The Ideal-Cipher Model
- **The Generic Model**
- Comparisons

Schnorr Signature (1989)

G, g and q: **common** elements
x: **private** key $y=g^x$: **public** key

- Signing m:
  - choose $k \in \mathbb{Z}_q$
  - compute $r=g^k$ as well as $e=H(m,r)$
  - and $s = k - xe \bmod q$

  $\sigma = (r,e,s)$
- Verifying (m,σ):
  - $u = g^s y^e \ \ (= g^{k-xe} g^{xe})$

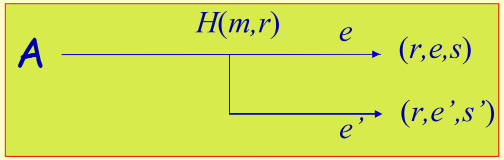
  test if $e=H(m,r)$ and $r=u$

The Forking Lemma

Pointcheval-Stern 1996

In the ROM, EF-CMA = DL problem

- Run *A* until one gets a success:
  on average = $1/\varepsilon$ iterations
- Run *A* again with same beginning, but random end until a success: on average q_H / ε times
- On average: $T' \approx (q_H + 1)\, t / \varepsilon$



$g^s y^e = r = g^{s'} y^{e'}$

$g^{s-s'} = y^{e'-e}$

Security Result

- Security bound: 2^{75}
  - and 2^{55} hash queries
- If one can break the scheme
  within time $T = t/\varepsilon$,
  one can extract two tuples within time
  $$T' \leq q_H\, t/\varepsilon = q_H\, T \leq 2^{130}$$
- Discrete Log (with same bounds as Fact)
  - 1024 bits → 2^{130} (NFS: 2^{80}) ✘
  - 2048 bits → 2^{130} (NFS: 2^{111}) ✘
  - 4096 bits → 2^{130} (NFS: 2^{149}) ✔

The Generic Model

Naechev 1994 – Shoup 1997

- It consists in considering the underlying group as a generic one: $(\mathbf{G},+) \approx (\mathbf{Z}_q,+)$
- But the adversary has access to the encoding $E(\mathbf{Q})$ of elements via an oracle
- If one assumes that $\mathbf{G} = \langle \mathbf{P} \rangle$,
  we define $\sigma(x) = E(x.\mathbf{P})$
  $$\sigma(x \pm y) = E((x \pm y).\mathbf{P}) = E(x.\mathbf{P} \pm y.\mathbf{P})$$

Generic group: the encoding is a random oracle

Schnorr Signature in ROM+GM

- If the group is of prime order q:
  one cannot break the scheme with less than $\sqrt{q}$ queries to the group-law oracle
- If q is a 160-bit prime, then $T \geq 2^{80}$
  - ***as soon as*** the best attack in the group is a generic one

Summary

- Introduction to Provable Security
- The Random-Oracle Model
- The Ideal-Cipher Model
- The Generic Model
- Comparisons

The Random-Oracle Model

Canetti-Goldreich-Halevi 1998

The ROM is strictly stronger
than the standard model

- Several counter-examples
  - Canetti-Goldreich-Halevi '98 (signature scheme)
  - Nielsen '02 (non-committing encryption scheme)
  - Goldwasser-Tauman '03 (signature scheme)
  - Bellare-Boldyreva-Palacio '03 (IND-CCA-preserving encryption)
- But still no practical attack against a "reasonable" scheme "provably secure in the random-oracle model"

The Generic Model

Stern-Pointcheval-Malone-Lee-Smart 2002

"*Generic group: the encoding is a random oracle*"

⇒ a stronger assumption than the ROM

Several counter-examples

- Index-calculs = non-generic attacks

  But not available everywhere:
  on some well-chosen elliptic curves
- ECDSA [Stern-Pointcheval-Malone-Lee-Smart '02]:
  - Provably non-malleable in the generic model
  - Malleable with any elliptic curve

⇒ to be used very carefully

The Ideal-Cipher Model

- Seems to be stronger than the ROM
  - a family of random permutations vs. a random function
- Maybe more realistic, when one looks at
  the goals in the design of a block cipher

But no formal result in either direction

- Candidates (none is proven):
  - ideal cipher → random oracle: CBC-MAC
  - random oracle → ideal cipher: Luby-Rackoff (Feistel)

Feistel Network: Not That Easy!

- Luby-Rackoff 1988: a 4-round Feistel network
  - a family of pseudo-random functions
    → a family of super pseudo-random permutations
    - i.e. indistinguishable from a random permutation, with access to both the permutation and its inverse but as **black boxes**
  - in the ROM, the adversary has access to the inner functions!
- Coron 2002: no black-box reduction
  - from an attack in the ICM
  - into an attack in the ROM
    if the cipher is instantiated with less than 6 rounds of random oracles

Conclusion

- Improvements to combine the standard model with efficient schemes
  - Cramer-Shoup 1998 (IND-CCA encryption
    EF-CMA signature)
  - Boneh-Boyen 2004 (EF-CMA signature)
- Still
  - either not as efficient as schemes proven in the ROM
  - or under stronger algorithmic assumptions

stronger model vs.
stronger algorithmic assumption