TOPIC: 6.857 - Computer & Network Security

DATE: 4/8/13

FILE UNDER:

PAGE: L16.1

**Admin:**

Quiz 4/17 open notes

3 crypto lectures this week (see email)

meet with TA's this week re projects

**Today:**

Making RSA IND-CCA2 secure (OAEP)

Other aspects of RSA security

Digital signatures & security defns

El Gamal digital signatures

RSA digital signatures (PSS)

DSS (Digital signature standard)

# Security of RSA

## Factoring attacks:

If any adversary can factor $n$, then the adversary can compute $\varphi(n)$, and thus compute $d = e^{-1} \pmod{\varphi(n)}$.

## How hard is factoring?

- time $\exp\{c \cdot (\ln n)^{1/3} (\ln \ln n)^{2/3}\}$
- RSA keys of length 768 factored (2009); can expect RSA key of length 1024 bits to be factored in the "near future".
- RSA keys of length 2048 secure for a very long time, unless there are algorithmic breakthroughs on problem of factoring.

Is (basic) RSA semantically secure?

No. (It's not even randomized...)

$\therefore$ not IND-CCA2 secure either...

How to make RSA IND-CCA2 secure?

OAEP = "Optimal asymmetric encryption padding" [BR 94]

Let message $m$ be $t$ bits in length.
Add $k_0$ bits of randomness $|r| = k_0$
Add $k_1$ bits of 0's $0^{k_1}$ (to check)

Assume $G: \{0,1\}^{k_0} \rightarrow \{0,1\}^{t+k_1}$

$H: \{0,1\}^{t+k_1} \rightarrow \{0,1\}^{k_0}$

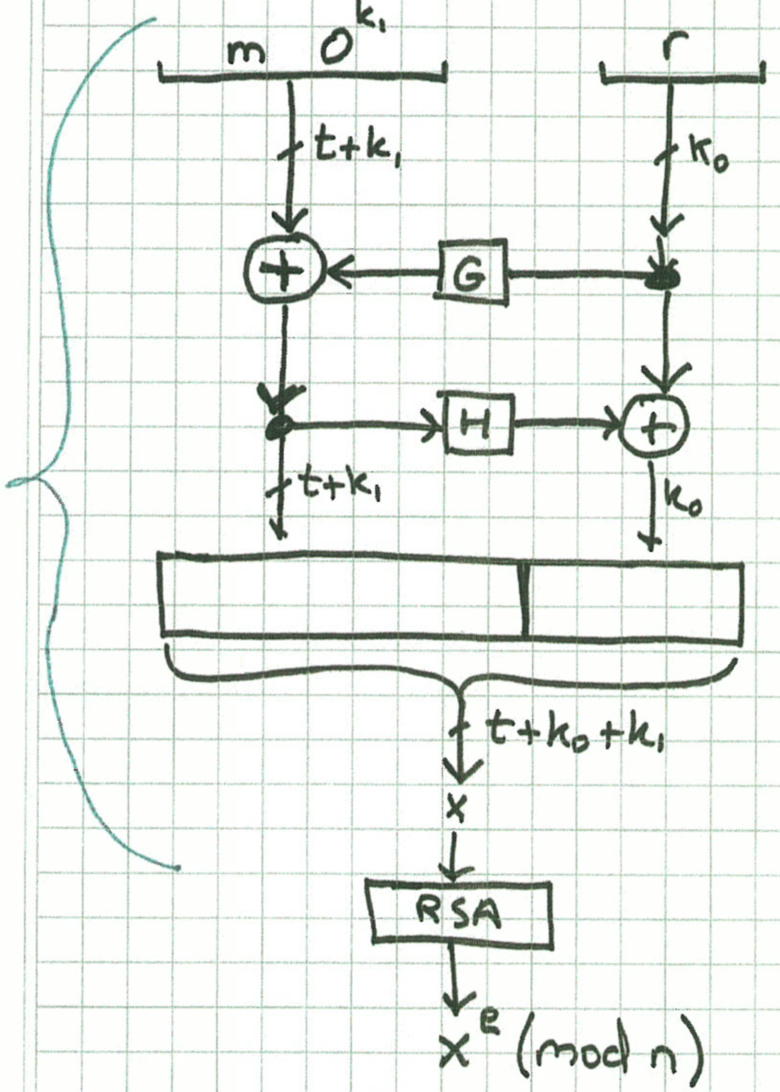
$G, H$ "random oracles"

[Compare to UFE of Desai for symmetric encryption]

PAGE: L16.8

# OAEP Encryption

OAEP




On decryption:
- invert RSA
- invert OAEP
- reject if $0^{k_1}$ not present
- else output m

TOPIC:

DATE:

FILE UNDER:



**Theorem:** RSA with OAEP is IND-CCA2 secure, assuming ROM for G & H, and assuming RSA hard to invert on random inputs.

[Bug in original proof, but OK with very slightly modified assumptions (or OAEP$^+$)]

OAEP used in practice

(But in practice we don't really have random oracles!)

TOPIC:

DATE:

FILE UNDER:



## Other aspects of RSA security:

[ref Boneh paper: 20 years of attacks on RSA]

**Weak keys:** small $d$ is insecure

($d < n^{1/4}$ allows adversary to factor $n$)

**Implementation issues:**

- Power analysis } "side channel attacks"
- Timing attacks }
- Fault injection (introduce power supply glitch)

  (esp. if device is using CRT)

**Quantum computing**

Peter Shor (MIT) has shown that factoring in polynomial time is possible on a "quantum computer"

PAGE: L16.11

# Digital Signatures

- Invented by Diffie & Hellman in 1976
  ("New Directions in Cryptography")
- First implementation: RSA (1977)
- Initial idea: switch PK/SK
  (enc with secret key ⟹ signature)
  (if PK decrypts it & looks ok then sig ok??)

## Current way of describing digital signatures

- $\mathrm{Keygen}(1^\lambda) \longrightarrow (\underline{PK}, \underline{SK})$
  verification key (PK) — signing key (SK)
- $\mathrm{Sign}(SK, m) \rightarrow \underbrace{\sigma_{SK}(m)}_{\text{signature}}$ [may be randomized]
- $\mathrm{Verify}(PK, m, \sigma) = $ True/False (accept/reject)

## Correctness:

$$(\forall m)\ \mathrm{Verify}(PK, m, \mathrm{Sign}(SK, m)) = \mathrm{True}$$

TOPIC:

DATE:

FILE UNDER:



## Security of digital signature scheme:

**Def:** (weak) existential unforgeability under adaptive chosen message attack.

① Challenger obtains $(PK, SK)$ from $Keygen(1^\lambda)$

Challenger sends PK to Adversary

② Adversary obtains signatures to a sequence

$$m_1, m_2, \ldots, m_q$$

of messages of his choice. Here $q = poly(\lambda)$, and $m_i$ may depend on signatures to $m_1, m_2, \ldots, m_{i-1}$.

Let $\sigma_i = Sign(SK, m_i)$.

③ Adversary outputs pair $(m, \sigma_*)$

Adversary wins if $Verify(PK, m, \sigma_*) = True$

and $m \notin \{m_1, m_2, \ldots, m_q\}$

Scheme is secure (i.e. weakly existentially unforgeable under adaptive chosen message attack) if

$$Prob[Adv\ wins] = negligible$$

TOPIC:

DATE:

FILE UNDER:

PAGE: L16.13

Scheme is strongly secure if adversary can't even produce new signature for a message that was previously signed for him.

I.e. Adv wins if $\text{Verify}(PK, m, \sigma_*) = \text{True}$ and $(m, \sigma_*) \notin \{(m_1, \sigma_1), (m_2, \sigma_2), \ldots, (m_q, \sigma_q)\}$.