PUBLIC KEY ENCRYPTION AND SIGNATURES

- RSA security
- RSA-OAEP for ACCA security
- Digital signatures
- Signing with RSA
- EL Gamal signatures

RSA Security

RSA is homomorphic (like El Gamal)

$$E(m_1) \cdot E(m_2) = E(m_1 m_2)$$
$$= (m_1 m_2)^e \pmod{n}$$

RSA is not even semantically secure
- Adversary can tell $E(m_0)$ from $E(m_1)$ since their values are fixed in deterministic RSA.

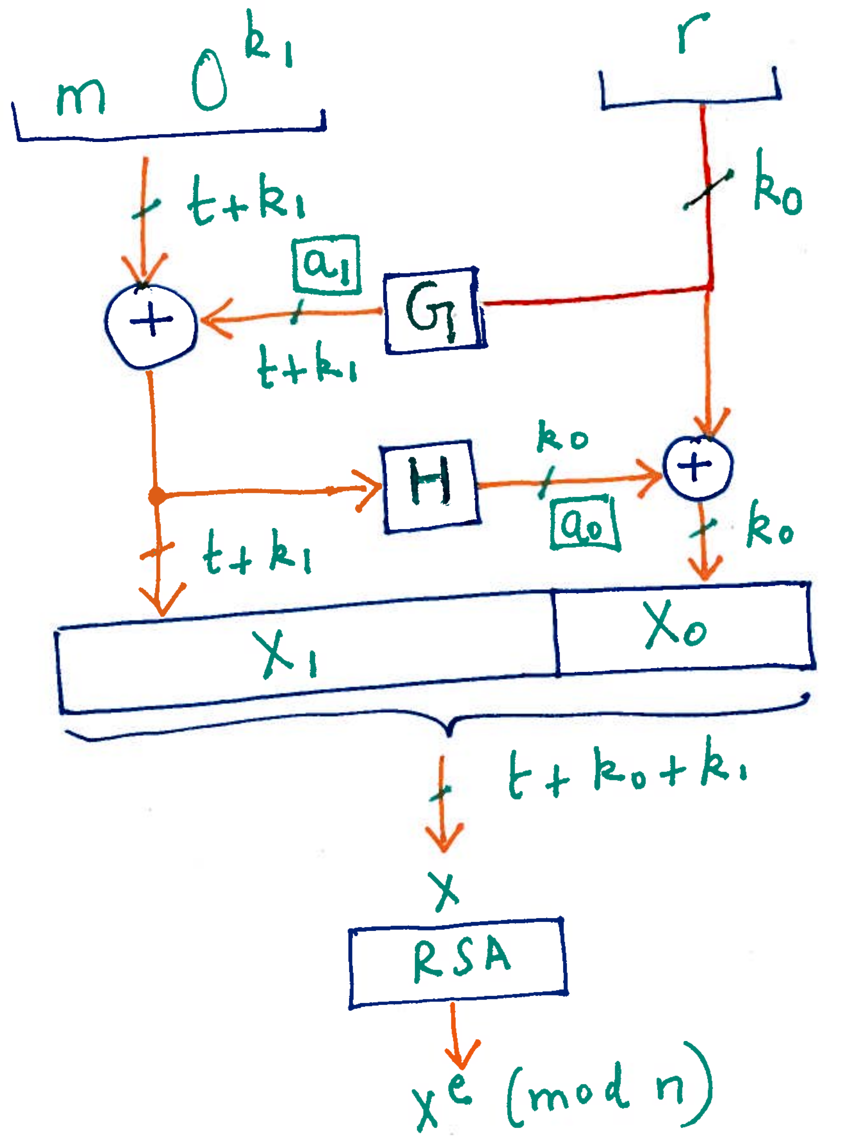
How to make RSA IND-CCA2 secure?

"OAEP" = Optimal Asymmetric Encryption Padding

Bellare, Rogaway 1994

Given m, $|m| = t$ bits

Pick r at random, $|r| = k_0$



G, H: random oracles

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

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

On decryption: Invert RSA

Invert OAEP

reject if 0^{k_1} not present

Inverting OAEP

$$X_1 = m0^{k_1} + a_1 \quad \xleftarrow{(4)} \quad \xleftarrow{(3)} G(r)$$

$$X_0 = r + a_0 \quad \xleftarrow{(1)} H(X_1)$$

(2) get this in step 2

Thm: RSA with OAEP secure against ACCA, assuming RO model & that RSA hard to invert on random inputs

replace with SHA-x

Digital Signatures

- Invented by Diffie-Hellman in 1976
- First implementation: RSA (1977)
- Initial idea: Switch PK/SK
  Encrypt with secret key to get signature
  If PK decrypts it, then sig OK
  (compare decrypted result to original)

Digital Signatures

Keygen $\rightarrow$ (PK, SK)

verification key (PK), signing key (SK)

Ignore "PKI" issue for now: Knowing that you have the "right" PK

$\mathrm{Sign}(SK, M) \rightarrow \sigma_{SK}(M)$ (may be randomized)

$M \in \{0,1\}^*$

$\mathrm{Verify}(PK, M, \sigma) = \mathrm{True}/\mathrm{False}$

Correctness: $(\forall M)\ \mathrm{Verify}(PK, M, \mathrm{Sign}(SK, M)) = \mathrm{True}$

Signing with RSA.

Hash and sign with PKCS

Let $H(M) = \mathrm{SHA256}(M)$

Let $H'(M) = 0x\,00\,01\,FF \ldots FF\,00 \,\|\, \mathrm{ASN.1} \,\|\, H(M)$

padding (FF … FF); name of hash (ASN.1)

$\sigma(M) = (H'(M))^d \bmod n, \quad M' = (\sigma(M))^e \bmod n$

Some issues with $e=3$ but appears secure

No proofs even assuming collision-resistant H and RSA hard to invert.

SECURITY OF SIGNATURES

(Weak) existential unforgeability under adaptive chosen message attack

Game: Challenger | Adversary

$(PK, SK) \leftarrow \text{Keygen}$

$\longrightarrow$

M_1 $\longleftarrow$

$\sigma(M_1)$ $\longrightarrow$

$\vdots$

M_k $\longleftarrow$

$\sigma(M_k)$ $\longrightarrow$

M, σ^* $\longleftarrow$

Adv wins if $\text{Verify}(PK, M, \sigma^*) = \text{True}$
& $M \notin \{M_1, \ldots M_k\}$

Scheme is weakly existentially unforgeable under adaptive chosen message attack if
Prob [Adv wins] is negligible

RSA-PSS weakly secure

Scheme is strongly secure if Adversary can't produce new signature for previously signed message.
Adv wins if $\text{Verify}(PK, M, \sigma^*) = \text{True}$
& $(M, \sigma_*) \notin \{(M_1, \sigma_1), \ldots (M_k, \sigma_k)\}$

EL Gamal Signatures

Public system parameters $\quad p$ prime
$\qquad g$ generator

Keygen: $\quad x \in_R \{0, 1, \ldots p-2\} \quad sk = x$
$\qquad y = g^x \qquad pk = y$

Sign(M): $\quad m = h(M) \quad m \in \mathbb{Z}_p$
$\qquad k \in_R \mathbb{Z}_{p-1}^* \quad [\gcd(k, p-1) = 1]$
$\qquad r = g^k \bmod p$
$\qquad s = k^{-1}(m - rx) \pmod{p-1}$
$$\boxed{\sigma(M) = (r, s)}$$

Verify: Check $0 < r < p$
$\qquad$ " $\quad y^r r^s = g^m \pmod p$
Return True if both checks pass, else False

Correctness: $\quad g^{xr} g^{ks} = g^{xr+ks}$

Since $s = k^{-1}(m - rx) \pmod{p-1}$ & $\gcd(k, p-1) = 1$

we have $xr + ks = m \pmod{p-1} = m + u(p-1)$

$\therefore \quad g^{xr+ks} = g^m \pmod p$
$\qquad = g^{m+u(p-1)}$

Original El Gamal is existentially forgeable

Without $h()$ function or collision-resistant identity $h()$

Let $e \in_R \mathbb{Z}_{p-1}$

$$r \leftarrow g^e y \pmod{p}$$

$$s \leftarrow -r \pmod{p-1}$$

(r, s) is signature for message $m = es \pmod{p-1}$

$$y^r r^s = g^{xr}(g^e y)^{-r} = g^{-er} = g^{es}$$

$$= g^m \quad \text{for } m = es \pmod{p-1}$$

Easy to fix!

Modified El Gamal

Sign(M): $k \in_R \mathbb{Z}_p^*$

$$r = g^k \pmod{p}$$

$$m = h(M \| r)$$

$$s = k^{-1}(m - rx) \pmod{p-1}$$

$$\sigma(M) = (r, s)$$

Verify: check $0 < r < p$

check $y^r r^s = g^m$ where $m = h(M \| r)$

Thm: Modified El Gamal is existentially unforgeable against adaptive chosen message attack, in ROM, assuming DLP is hard.