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, $|r| = k_0$

On decryption: Invert RSA
Invert OAEP
reject if $0^{k_1}$ not present
Inverting OAEP

\[ X_1 = m^{0^1} + a_1 \]
\[ X_0 = r + a_o \]

get this in step 2

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

Digital Signatures

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

\[ \text{keygen} \rightarrow (PK, SK) \]

\[ \text{verification key} \]

\[ \text{signing key} \]

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

\[ \text{Sign} (SK, M) \rightarrow \sigma_{SK} (M) \]

\[ M \in \{0, 1\}^* \] (may be randomized)

\[ \text{Verify} (PK, M, \sigma) = \text{True/False} \]

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

Signing with RSA.

Hash and sign with PKCS

Let \( H(M) = \text{SHA256}(M) \)

Let \( H'(M) = 0x00001 \text{ FF... FF 00 11 ASN.1 II } H(M) \)

Let \( \sigma(M) = (H'(M))^d \mod n, \ M' = (\sigma(M))^e \mod n \)

Some issues with \( e = 3 \) but appears secure

No proofs even assuming collision-resistant \( H \) and RSA hard to invert
(Weak) existential unforgeability under adaptive chosen message attack

\[ (PK, SK) \leftarrow \text{Keygen} \]

\[ M_1, \sigma(M_1) \]

\[ \vdots \]

\[ M_k, \sigma(M_k) \]

\[ M, \sigma_x \]

Adv wins if \( \text{Verify} (PK, M, \sigma_x) = \text{True} \)

\& \( M \notin \{ M_1, \ldots, M_k \} \)

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

RSA-PSS weakly secure

Scheme is strongly secure if
Adversary can't produce new signature for previously signed message.
Adv wins if \( \text{Verify} (PK, M, \sigma_x) = \text{True} \)

\& \( (M, \sigma_x) \notin \{ (M_1, \sigma_1), \ldots, (M_k, \sigma_k) \} \)
EL Gamal Signatures

Public system parameters

\[ p \text{ prime} \]
\[ g \text{ generator} \]

Keygen:

\[ X \in \mathbb{Z}_p \setminus \{0, 1, \ldots, p-2\} \]
\[ \text{SK} = x \]
\[ y = g^x \]
\[ \text{PK} = y \]

Sign \( M \):

\[ m = h(M) \in \mathbb{Z}_p \]
\[ k \in \mathbb{Z}_{p-1}^* \quad \left[ \text{gcd}(k, p-1) = 1 \right] \]
\[ r = g^k \mod p \]
\[ s = k^{-1} (m-rx) \mod (p-1) \]
\[ \sigma(M) = (r, s) \]

Verify:

Check \( 0 < r < p \)
\[ y^r r^s = g^m \mod p \]
Return True if both checks pass, else False

Correctness:

\[ g^{xr} g^{ks} = g^{xr+ks} \]

Since \[ s = k^{-1} (m-rx) \mod (p-1) \quad \text{and} \quad \text{gcd}(k, p-1) = 1 \]
we have \[ xr + ks = m \mod (p-1) = m + u(p-1) \]
\[ \Rightarrow \]
\[ g^{xr+ks} = g^m \mod p \]
Original El Gamal is existentially forgeable

Without hash function or collision-resistant identity h(.)

Let \( e \in \mathbb{Z}_{p-1} \)

\[ r \leftarrow g^e y \pmod{p} \]
\[ s \leftarrow r \pmod{p-1} \]

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

\[ y^rrs = g^{xr} (gey)^r = g^{-er} = ges \]
\[ = g^m \text{ for } m = es \pmod{p-1} \]

Easy to fix!

Modified El Gamal

\[ \text{Sign}(M): \quad k \in \mathbb{Z}_{p}^* \]

\[ r = g^k \pmod{p} \]

\[ m = h(M \| r) \]

\[ s = k^{-1} \left( m - rx \right) \pmod{p-1} \]

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

Verify:

check \( 0 < r < p \)

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

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