Identity-Based Cryptography

Ratna Dutta

Associate Professor

Department of Mathematics

Indian Institute of Technology, Kharagpur

November 9-13, 2020

Public Key Cryptosystem

- Public keys are used for encryption and digital signature verification.
- Private keys are used for decryption and digital signature generation.
- Public keys are accessible to all parties.
- Private keys are to be kept secret.

- How to associate entities with their respective public keys?
- An attacker may present a harmful key as the public key of a victim.
- Before using a public key, one should verify that the key belongs to the claimed party.

Public Key Certificates

- There is a trusted Certification Authority (CA).
- CA issues public-key certificates to parties.
- A certificate contains a public key, some identifying information of the party to whom the key belongs, a period of validity.
- The certificate is digitally signed by the CA.
- Key compromise and/or malicious activities may lead to revocation of certificates.
- The CA maintains a list of revoked certificates.

Use of Public Key Certificates

- Alice wants to send an encrypted message to Bob.
- Alice obtains Bob's public-key certificate.
- Alice verifies the signature of the CA on the certificate.
- Alice confirms that Bob's identity is stored in the certificate.
- Alice checks the validity of the certificate.
- Alice ensures that the certificate does not reside in the revocation list maintained by the CA.
- Alice then uses Bob's public key for encryption.

Problems of Public Key Certificates

- A trusted CA is needed.
- Every certificate validation requires contact with the CA for the verification key and for the revocation list.

Identity-Based Public Keys

- Alices identity (like e-mail ID) is used as her public key.
- No contact with the CA is necessary to validate public keys.
- A trusted authority is still needed: Private-Key Generator (PKG) or Key-Generation Center (KGC).
- Each party should meet the PKG privately once (registration phase).
- **Limitation:** Revocation of public keys may be difficult.

Historical Remarks

- Shamir (Crypto 1984) introduces the concept of identity-based encryption (IBE) and signature (IBS). He gives a concrete realization of an IBS scheme.
- In early 2000, bilinear pairing maps are used for concrete realizations of IBE schemes.
- Sakai, Ohgishi and Kasahara (SCIS 2000) propose an identity-based key-agreement scheme and an IBS scheme.

- Boneh and Franklin (Crypto 2001) propose an IBE scheme. Its security is proved in the random-oracle model.
- Boneh and Boyen (Eurocrypt 2004) propose an IBE scheme whose security can be proved without random oracles.

Cryptographic Bilinear Map

- G_1, G_2 two groups of a large prime order q.
- $G_1 = \langle P \rangle$ additive, G_2 multiplicative, DLP hard.
- Bilinear Map $\quad e : G_1 \times G_1 \rightarrow G_2$
  1. Bilinearity : $e(aP, bQ) = e(P, Q)^{ab}$ for all $P, Q \in G_1$ and $a, b \in Z_q^*$.
  2. Non-degeneracy : $e(P, P) \neq 1$.
  3. Computable : e can be efficiently computed.
- Examples : Modified Weil, Tate Pairing.

Sakai-Ohgishi-Kasahara [2000] Key Agreement

- public key $ID \in \{0,1\}^*$ (like e-mail addresses)
  1. *Setup*: $params = \langle G_1, G_2, e, P, q, H \rangle$, $G_1 =< P >$, s is the master key. (G_1 additive, G_2 multiplicative group of prime order q, DLP is hard in both)
  2. *Extract*: $Q_{ID_U} = H(ID_U) \in G_1$, $d_{ID_U} = sQ_{ID_U}$.
  3. *Key Agreement*:
     Alice computes $SK_{ID_{\mathsf{Alice}}} = e(d_{ID_{\mathsf{Alice}}}, Q_{ID_{\mathsf{Bob}}})$
     Bob computes $SK_{ID_{\mathsf{Bob}}} = e(d_{ID_{\mathsf{Bob}}}, Q_{ID_{\mathsf{Alice}}})$
- security: hardness of BDH problem.

Identity-Based Encryption (IBE) Scheme

- Shamir [1984]
- public key $ID \in \{0,1\}^*$
- An ID-based encryption scheme has four algorithms.
  1. *Setup:* Creates system parameters and *master key*.
  2. *Extract:* Uses master key to generate the private key corresponding to an arbitrary public key string ID.
  3. *Encrypt:* Encrypts messages using the public key ID.
  4. *Decrypt:* Decrypts the message using the corresponding private key of ID.

Motivation for ID-based encryption

- To simplify certificate management in e-mail system
- No need to keep a large database for public keys
- System derives the public keys by user names

Boneh-Franklin [2001] IBE Scheme

- *Setup*: $params = \langle G_1, G_2, e, P, q, n, P_{pub}, H_1, H_2 \rangle$, $P_{pub} = sP$, s is the master key, message space $\mathcal{M} = \{0,1\}^n$.
- *Extract*: $Q_{ID} = H_1(ID) \in G_1$, $d_{ID} = sQ_{ID}$.
- *Encrypt*: $r \in Z_q^*$, $m \in \mathcal{M}$,

$$C = \langle rP, m \oplus H_2(e(Q_{ID}, P_{pub})^r) \rangle$$

- *Decrypt*: $C = \langle U, V \rangle$, recover

$$m = V \oplus H_2(e(d_{ID}, U))$$

- Security of Boneh-Franklin's (BF) IBE scheme depends on hardness of BDH problem in $\langle G_1, G_2, e \rangle$.
- BDH (Bilinear Diffie-Hellman) Problem in $\langle G_1, G_2, e \rangle$:
  - given $\langle P, aP, bP, cP \rangle$ for some $a, b, c \in Z_q^*$, compute $e(P, P)^{abc}$.
- This version of BF scheme is IND-ID-CPA secure in the random oracle model.

- **Fujisaki-Okamoto transformation** has been used to extend IND-ID-CCA security.
- Let $\mathcal{E}$ be a probabilistic public key encryption scheme. We denote by $\mathcal{E}_{pk}(M; r)$ the encryption of M using the random bits r under the public key pk.
- Fujisaki-Okamoto define the hybrid scheme $\mathcal{E}^{hy}$ as:

$$\mathcal{E}^{hy}_{pk}(M) = \langle \mathcal{E}_{pk}(\sigma; H_3(\sigma, M)), H_4(\sigma) \oplus M \rangle$$

  where σ is generated at random and H_3, H_4 are cryptographic hash functions.

- Fujisaki-Okamoto (FO) show that if $\mathcal{E}$ is an IND-CPA secure encryption scheme, then $\mathcal{E}^{hy}$ is an IND-CCA secure encryption scheme in the random oracle model.
- So after applying FO transformation, the resulting ciphertext is

$$C = \langle rP, \sigma \oplus H_2(e(Q_{ID}, P_{pub})^r), m \oplus H_4(\sigma) \rangle$$

where $r = H_3(\sigma, m)$.

Selective Model

- Boneh and Boyen gave selective ID model, namely IND-sID-CCA, which is slightly weaker than the model described above.
- In selective model the adversary must commit ahead of the time to the identity that it intends to attack.
- In the standard model described earlier, the adversary is allowed to choose this identity adaptively.

Boneh-Boyen's IBE Without Random Oracle

- *Setup* : $params = \langle G_1, G_2, e, P, q \rangle$,
  $P_{pub} = (U = xP, V = yP)$, (x, y) is the master key.
- *Extract* : Given a public key $\mathsf{ID} \in Z_q^*$, the private key $d_{\mathsf{ID}} = (r, K)$, where $r \in Z_q^*$ and $K = \frac{1}{\mathsf{ID}+x+ry} P \in G_1$.
- *Encrypt* : Message $M \in G_1$, $s \in Z_q^*$, ciphertext is

$$C = \langle s(\mathsf{ID})P + sU, sV, e(P, P)^s \ M \rangle$$

- *Decrypt* : $C = \langle X, Y, Z \rangle$, recover $M = \frac{Z}{e(X+rY,K)}$

Security : IND-sID-CCA secure without random oracles under k-DBDHI assumption.

k-DBDHI Problem

- The k-Decisional Bilinear Diffie-Hellman Inversion (k-DBDHI) problem in $\langle G_1, G_2, \hat{e} \rangle$:

  Instance : $(P, yP, y^2P, \ldots, y^kP, r)$ for some $y \in Z_q^*$, $r \in_R G_2$.

  Output : yes if $r = e(P, P)^{\frac{1}{y}} \in G_2$ and output no otherwise.

Identity-Based Signature (IBS) Scheme

- Shamir's IBS
- Sakai-Ohgishi-Kasahara (SOK) IBS

Shamir's IBS

- *Setup*: Uses RSA setup.
  - PKG generates an RSA modulus $n = pq$ and computes $\phi(n) = (p-1)(q-1)$.
  - PKG chooses $e \geq 3$ such that $\mathsf{gcd}(e, \phi(n)) = 1$ and computes $d \equiv e^{-1} \pmod{\phi(n)}$.
  - PKG fixes a hash function $H : \{0,1\} \rightarrow Z_n$.
  - PKG publishes n, e, H.
  - $p, q, \phi(n), d$ are kept secret.

- *Extract*:
  - Bob's public key: $Q_{ID_{Bob}} = H(ID_{Bob})$.
  - Bob's private key: $S_{ID_{Bob}} \equiv Q_{ID_{Bob}}^{d} \pmod{n}$.
- *Sign*: Bobs signature on message M is the pair (s, t) with

$$s \equiv x^e \pmod{n}, x \in Z_n$$

$$t \equiv S_{ID_{Bob}}.x^{H(s,M)} \pmod{n}$$

- *Verify*:

$$t^e \equiv Q_{ID_{Bob}}.(x^e)^{H(s,M)} \equiv Q_{ID_{Bob}}.s^{H(s,M)} \pmod{n}.$$

Security:

– A forger can generate $x, s, H(s, M)$.

– Generating the correct t is equivalent to knowing $S_{ID_{Bob}}$.

– Getting $S_{ID_{Bob}}$ from $Q_{ID_{Bob}}$ is the RSA problem.

Sakai-Ohgishi-Kasahara (SOK) IBS

- *Setup*: $params = \langle G_1, G_2, e, P, q, P_{pub}, H \rangle$, $G_1 =< P >$, $P_{pub} = sP$, s is the master key. (G_1 additive, G_2 multiplicative group of prime order q)
- *Extract*: $Q_{ID_U} = H(ID_U) \in G_1$, $d_{ID_U} = sQ_{ID_U}$.
- *Sign*: Bob's signature on message M is (U, V) with

$$U = rP, r \in Z_q,$$

$$V = d_{ID_{Bob}} + rH(Q_{ID_{Bob}}, M, U) \in G_1$$

- *Verify*: Check if

$$e(P, V) = e(P_{pub}, Q_{ID_{Bob}})e(U, H(Q_{ID_{Bob}}, M, U).$$