Short signatures

Ratna Dutta

Department of Mathematics

Indian Institute of Technology, Kharagpur

November 9-13, 2020

Outline

- Boneh-Lynn-Schcham's short signature
- Boneh-Boyen's signature
- Water's signature

Public Key Cryptosystem

- Public key cryptosystems, also called asymmetric cryptosystems, derive their security from some computationally hard mathematical problems.
- The most popular ones are based mainly over two such problems:
  - Integer factorization problem
  - Discrete logarithm problem (DLP)

Integer factorization problem

- it is very easy to create at will quite large prime numbers (for instance 1024 bit is a typical cryptographic size for reasonable security),
- but it is totally impossible (at the current state of art), except by some incredible stroke of luck (or a bad choice of the prime) to factor the product of two primes of this size (a 2048-bit number).
- The RSA cryptosystem, Paillier's homomorphic encryption are based on the hardness of integer factoring problem.

Discrete logarithm problem (DLP)

- if G is a large cyclic group (multiplicative, say) with a generator g, then given any element $y = g^a$ in the group, computing a is called the DLP over G.
- Cryptosystems those derive their security from the hardness of DLP:
  - Diffie-Hellman (DH) key exchange
  - ElGamal encryption
  - Digital Signature Algorithm (DSA)
  - Many more ....

- many groups have been identified on which the DLP is believed to be hard:
  - the multiplicative group of a finite field of characteristic 2 ($F_{2^n}, n \geq 1$, facilitates “carry-free” arithmetic)
  - the group of units of Z_n where n is a composite integer
  - the multiplicative subgroup of the prime field Z_p
  - the group of points on an elliptic curve defined over a finite field
  - the Jacobian of an hyperelliptic curve over a finite field

Short signature scheme

- When a person is asked to manually key in the signature, the shortest possible signature is required.
- 1024 bit modulus RSA signature is 1024 bit long.
- Standard DSA or ECDSA signatures are 320 bit long.
- Boneh, Lynn, Shacham (BLS) signature scheme provides a feasible signature of length approximately 170 bit providing the same level of security similar to that of 320 bit DSA signature.

<u>**Boneh, Lynn, Shacham**</u> (BLS) [2001]

- KeyGen : $params = \langle G_1, G_2, \hat{e}, q, P_{pub}, H \rangle$, s is the private key and $P_{pub} = sP$ is the corresponding private key.
  - G_1 is a Gap Diffie-Hellman (GDH) group.
- Signing : $m \in \{0,1\}^*$, compute $P_m = H(m) \in G_1$, $S_m = sP_m \in G_1$.
  - signature is σ, the x-co-ordinate of S_m.

- Verification : given m, σ and $params$, find a point $S \in G_1$ with x-co-ordinate σ.
  - if no such point, reject the signature as invalid
  - else check whether $\langle P, P_{pub}, P_m, \pm S_m \rangle$ is a valid Diffie-Hellman tuple.

$$i.e.\ \ \hat{e}(P, \pm S_m) = \hat{e}(P_{pub}, P_m)$$

  - if so accept the signature,
  - otherwise reject.

- BLS short signature scheme is secure against *existential forgery under adaptive chosen message attack* assuming the hardness of CDH problem in G_1 using random oracle model.

Random Oracle Model

- Assume that all random values are indeed random
- Assume Adversary does not exploit any properties of the hash function
- Assume that hash functions behave idealistically (random public functions)
- Assumptions reduce the strength of a proof

- A random oracle is a function $H : X \to Y$ chosen uniformly at random from the set of all functions $\{h : X \to Y\}$ (we assume Y is a finite set)
- An algorithm can query the random oracle at any point $x \in X$ and receive the value $H(x)$ in response
- Random oracles are used to model cryptographic hash functions such as SHA-1.
- Security in the random oracle model does not imply security in the real world
- Nevertheless, the random oracle model is a useful tool for validating natural cryptographic constructions.

Boneh-Boyen's Short Signature (Without ROM)

- Protocol Description :

  KeyGen : The secret key is $(x, y) \in_R Z_q^* \times Z_q^*$ and the public key is $(P, U = xP, V = yP)$ for a signer.

  Sign : Given a secret key (x, y), a message $m \in Z_q^*$, choose a random $r \in Z_q^*$ and compute $\sigma = \frac{1}{x+m+yr}P$.

  Verify : Given a public key (P, U, V), a message $m \in Z_q^*$ and a signature (σ, r), verify

$$e(\sigma, U + mP + rV) = e(P, P).$$

- **Security** : Secure against existential forgery under chosen message attack assuming q-SDH problem is hard without using the random oracle model.
- k-Strong Diffie-Hellman (k-SDH) problem in G_1 :

  $Instance$: $(P, yP, y^2P, \ldots, y^kP)$ for a random $y \in Z_q^*$.

  $Output$: $(c, \frac{1}{y+c}P)$ where $c \in Z_q^*$.
- **Existential Unforgeability against Weak Chosen Message Attack:** The adversary submits all signature queries before seeing the public key.

Water's Signature (Without ROM)

1. *Setup*: $\mathsf{params} = \langle p, G, G_T, e, g\rangle$, $|G| = p$, $G = \langle g\rangle$
   - $g_1 = g^{\alpha}, \alpha \in_R Z_p^*$
   - $g_2, f', f_1, f_2, \ldots, f_n \in_R G$
   - $\mathsf{SK} = g_2^{\alpha}$, $\mathsf{VK} = \langle \mathsf{params}, g_1, g_2, f', f_1, f_2, \ldots, f_n\rangle$
2. *Sign*: $M = M_1 M_2 \ldots M_n \in \{0,1\}^n$, $S = \{i | M_i = 1\}$

$$\sigma_M = \left(\mathsf{SK}\ \left(f' \prod_{i \in S} f_i\right)^r, g^r\right), r \in_R Z_q^*$$

3. *Verify*: $M = M_1 M_2 \ldots M_n \in \{0,1\}^n$, $S = \{i | M_i = 1\}$, $\sigma_M = (\sigma_1, \sigma_2)$, $\mathsf{VK} = \langle \mathsf{params}, g_1, g_2, f', f_1, f_2, \ldots, f_n \rangle$

$$e(\sigma_1, g) \stackrel{?}{=} e(g_1, g_2) e\left(f' \prod_{i \in S} f_i, \sigma_2\right)$$

Correctness: $e(\sigma_1, g) = e\left(g_2^{\alpha}\left(f' \prod_{i\in S} f_i\right)^r, g\right)$

$$= e(g_2^{\alpha}, g) e\left(\left(f' \prod_{i \in S} f_i\right)^r, g\right) = e(g_2, g_1) e\left(f' \prod_{i \in S} f_i, \sigma_2\right)$$

Security : Secure against existential forgery under chosen message attack assuming CDH problem is hard without using the random oracle model.