Anonymous Threshold Signatures

Petar Hlad Colic

Universitat Politècnica de Catalunya

July 2018

1. Preliminaries
   - Oblivious Polynomial Evaluation
   - Bilinear Pairings

PKE scheme

A public key encryption scheme $PKE = (KG, \mathcal{E}, \mathcal{D})$ consists of three probabilistic and polynomial time algorithms:

- Key generation KG:
  - Input: Security parameter
  - Output: Pair (sk, pk) of secret and public keys.
- Encription $\mathcal{E}$:
  - Input: Plaintext m
  - Output: Ciphertext $c = \mathcal{E}_{pk}(m)$
- Decryprtion $\mathcal{D}$:
  - Input: Ciphertext c
  - Output: Plaintext $m = \mathcal{D}_{sk}(c)$

For any pair (sk, pk) and any plaintext m, it must hold

$$m = \mathcal{D}_{sk}\left(\mathcal{E}_{pk}(m)\right)$$

Homomorphic PKE

Definition 1.1 (Homomorphic PKE).

Let $\mathcal{M}$ be the set of plaintexts s.t. it is closed under an operation $\bullet$. Let $\mathcal{C}$ be the set of ciphertexts s.t. it is closed under an operation $\circ$. A PKE scheme $(KG, \mathcal{E}, \mathcal{D})$ has the homomorphic property if

$$\mathcal{D}_{sk}\left(\mathcal{E}_{pk}(m_1) \circ \mathcal{E}_{pk}(m_2)\right) \;=\; m_1 \bullet m_2 \quad \forall m_1, m_2 \in \mathcal{M}.$$

Remark 1.2.

If we write $\mathcal{M}$ additively and $\mathcal{C}$ multiplicatively, for $a \in \mathbb{Z}^+$ we have:

$$\mathcal{D}_{sk}\left(\mathcal{E}_{pk}(m)^a\right) = a \cdot m$$

Oblivious Polynomial Evaluation

Oblivious Polynomial Evaluation is a protocol involving a sender who knows a polynomial $P \in \mathbb{F}[x]$ and a receiver who knows a value $\alpha \in \mathbb{F}$. At the end of the protocol, the receiver learns $P(\alpha)$ and the sender learns nothing.

	Sender	Receiver
Input	$P \in \mathbb{F}[x]$	$\alpha \in \mathbb{F}$
Output	-	$P(\alpha)$

Bilinear Pairings

Problem name	Input	Output
Decisional DH (DDH)	$g, g^a, g^b, g^c \in G_1$	TRUE iif $c = ab$
Computational DH (CDH)	$g, g^a, g^b \in G_1$	g^{ab}
Decisional Co-DH (co-DDH)	$h, h^b \in G_1$ $g_2, g_2^a \in G_2$	TRUE iif $a = b$
Computational Co-DH (co-CDH)	$h \in G_1$ $g_2, g_2^a \in G_2$	h^a

Bilinear Pairings

Definition 1.3 (Bilinear map).

Let G_T be an additional group s.t. $|G_1| = |G_2| = |G_T|$.
A **bilinear map** *is a map $e : G_1 \times G_2 \to G_T$ s.t.:*

- *Is bilinear:* $\forall u \in G_1, \forall v \in G_2, \forall a, b \in \mathbb{Z}$,

$$e(u^a, v^b) = e(u, v)^{ab}$$

- *Is non-degenerate:* $e(g_1, g_2) \neq 1$.