CS6115: Structure versus Hardness in Cryptography	Oct 7, 2021
Lecture 19 : Identity Based Encryption	
Lecturer: *Shweta Agrawal*	Scribe: *Satvinder*

1 Identity Based Encryption

We describe the IBE scheme given by Boneh and Franklin in 2001.

Setup(1^λ): Choose groups G and G_T of prime order $p > 2^\lambda$ along with a bilinear map $e : G \times G \to G_T$ and a generator g. Choose random $\alpha \in \mathsf{Z}_p^*$ and define the master secret key $\mathsf{MSK} = \alpha$. Define the public parameters

$$\mathsf{PP} = (G, G_T, g, g_1 = g^\alpha, H)$$

where H is a hash function treated as a random oracle in the security proof. Output $(\mathsf{MSK}, \mathsf{PP})$.

KeyGen$(\mathsf{PP}, \mathsf{MSK}, \mathsf{ID})$: Output the secret key

$$d_{\mathsf{ID}} = (H(\mathsf{ID}))^\alpha$$

Encrypt$(\mathsf{PP}, \mathsf{ID}, M)$: Sample random $r \in \mathbb{Z}_p^*$. Output $C = (C_1, C_2)$ where

$$C_1 = g^r$$
$$C_2 = M.e\Big(g_1,\ H(\mathsf{ID})\Big)^r$$

Decrypt$(\mathsf{PP}, d_{\mathsf{ID}}, C)$: Parse C as (C_1, C_2) and output

$$M = \frac{C_2}{e(C_1, d_{\mathsf{ID}})}$$

Correctness: We now prove correctness of the encryption scheme described above.

$$\begin{aligned} e(C_1, d_{\mathsf{ID}}) &= e(g^r, H(\mathsf{ID})^\alpha) \\ &= e(g, H(\mathsf{ID}))^{\alpha r} \\ &= e(g^\alpha, H(\mathsf{ID}))^r \\ &= e(g_1, H(\mathsf{ID}))^r \end{aligned}$$

Now,

$$\frac{C_2}{e(C_1, d_{\mathsf{ID}})} = \frac{M.e(g_1, H(\mathsf{ID}))^r}{e(g_1, H(\mathsf{ID}))^r} = M$$

Security

Theorem: The Boneh-Franklin IBE is IND-ID-CPA secure in the Random Oracle Model if the DBDH assumption holds in (G, G_T).

Proof: Assume there exists an adversary $\mathcal{A}$ for the IBE scheme described earlier. We construct an adversary $\mathcal{B}$ for a DBDH challenger as follows:

1. $\mathcal{B}$ is given (g, g^a, g^b, g^c) and T by the DBDH challenger where T is either $e(g,g)^{abc}$ or $e(g,g)^d$ where $a, b, c, d \leftarrow \mathbb{Z}_p$.
2. $\mathcal{B}$ provides $\mathcal{A}$ with the public parameters $\mathsf{PP} = (G, G_T, g, g_1 = g^a, H)$. Implicitly, $\mathsf{MSK} = a$
3. Initialize $L = \{\}$
4. When $\mathcal{A}$ queries $H(\mathsf{ID})$, $\mathcal{B}$ does the following:
   (a) Return previously defined $H(\mathsf{ID})$ if it exists
   (b) Flip a coin $b_{\mathsf{ID}} \in \{0, 1\}$ with probabilities
   $$\Pr(b_{\mathsf{ID}} = 0) = \frac{q}{q+1}$$
   $$\Pr(b_{\mathsf{ID}} = 1) = \frac{1}{q+1}$$
   where q is the number of hash queries.
   (c) If $b_{\mathsf{ID}} = 0$, sample random $\beta_{\mathsf{ID}} \in \mathbb{Z}_p$ and define $H(\mathsf{ID}) = g^{\beta_{\mathsf{ID}}}$
   (d) If $b_{\mathsf{ID}} = 1$, sample random $\beta_{\mathsf{ID}} \in \mathbb{Z}_p$ and define $H(\mathsf{ID}) = \left(g^b\right)^{\beta_{\mathsf{ID}}}$
   (e) Store $(\mathsf{ID}, b_{\mathsf{ID}}, \beta_{\mathsf{ID}}, H(\mathsf{ID}))$ in L
5. When $\mathcal{A}$ queries secret key of an ID, $\mathcal{B}$ does the following: (Without loss of generality, we assume that every private key query was preceded by the corresponding hash query)
   (a) If $b_{\mathsf{ID}} = 1$, $\mathcal{B}$ fails and outputs a random bit.
   (b) If $b_{\mathsf{ID}} = 0$, $\mathcal{B}$ computes and returns $d_{\mathsf{ID}} = \left(g^a\right)^{\beta_{\mathsf{ID}}}$ to $\mathcal{A}$
6. Generation of challenge ciphertext and proof of security of reduction shall be covered in the next lecture.

References

[BF01] Dan Boneh and Matthew K. Franklin. Identity-based encryption from the weil pairing. In Advances in Cryptology - CRYPTO 2001, 21st Annual International Cryptology Conference, Santa Barbara, California, USA, August 19-23, 2001, Proceedings, pages 213–229, 2001.