CS6115: Structure versus Hardness in Cryptography Oct 13, 2021

Lecture 20 : IBE from Pairings

Lecturer: *Shweta Agrawal* Scribe: *Somnath Bhattacharjee*

Identity Based Encryption

We will continue the proof of the security theorem discussed in the last class

Theorem. [BF01] The Boneh-Franklin IBE is IND-ID-CPA secure in the Random Oracle Model if the DBDH assumption holds in (G, G_T).

Proof(continued): Till now the form of reduction we have

1. $\mathcal{B}$ is given (g, g^a, g^b, g^c) and the Target element $T = e(g,g)^{abc}$, or a random $e(g,g)^d$ (slightly different from the previous scribe) by the challenger.
2. **PP:** a will be treated as MSK. Hence the PP is $(G, G_T, g, g_1 = g^a, H)$
3. **Hash queries:** With a biased coin toss, $b_{id} \in \{0,1\}$ we will determine $H(\mathsf{ID})$ by
$$\begin{cases} H(\mathsf{ID}) = g^{\beta_{id}} & \text{if } b_{id} = 0 \\ H(\mathsf{ID}) = (g^b)^{\beta_{id}} & \text{if } b_{id} = 1 \end{cases}$$
L will store these information.
4. **Public key queries:** for any ID $\mathcal{B}$ will return
$$\begin{cases} \mathcal{B} \text{ fails and returns a random value} & \text{if } b_{id} = 1 \\ (g^a)^{\beta_{id}} & \text{if } b_{id} = 0 \end{cases}$$

Now the task is to generate cipher text. It will also depend on the value of b_{id^*}. (id^* is the identity used as secret key)

1. If $b_{id^*} = 0$ then $\mathcal{B}$ fails and outputs a random value. (as we know how to generate secret key for that particular id, follows from the construction of β)
2. if $b_{id^*} = 1$ then c will be treated as r, since we have the access of g^c, we will set $c_1 = g^c$ (c_1, r are the same parameters defined in discussion of the IBE scheme)
Now construction of c_2 will be straight forward
$$\begin{aligned} c_2 &= M_\gamma e\big(g^a, H(\mathsf{ID}^*)\big)^c && (\gamma \text{ is a random bit}) \\ &= M_\gamma e\big(g^a, g^{b\beta_{\mathsf{ID}^*}}\big)^c \\ &= M_\gamma e\big(g,g\big)^{(abc)\beta_{\mathsf{ID}^*}} \\ &= M_\gamma T^{\beta_{\mathsf{ID}^*}} \end{aligned}$$
(M_0, M_1 are the msg required for the security game)

Now that can be either completely random value or our desired target element.
If T is random then the adversary can only guess randomly for the msg bit (since the msg has been wiped out, so M_γ and hence γ is information theoretically hidden from the IBE Adv)
Now if T is not random and adv can guess γ correctly then actually during the reduction it can distinguish between $e(g,g)^{abc}$ and random element which contradicts the DBDH assumption.

Success Probability:

Say if $\mathcal{B}$ outputs 1, T is real (i.e., $= e(g,g)^{abc}$), $\mathcal{B}$ outputs 0 otherwise.
Let us call the event that $\mathcal{B}$ fails as FAILS. Now not FAILing can occur by both challenger coin comes with 1 (w.p. $\frac{1}{q+1}$) and q many key coins comes with 0 (w.p. $\left(\frac{q}{1+q}\right)^q$). Hence

$$Pr(\neg \mathsf{FAIL}) = \frac{1}{q+1}\left(\frac{q}{1+q}\right)^q$$

$$\approx \frac{1}{exp(1)(q+1)} \qquad \text{(for large } q\text{)}$$

Now we have

$$\begin{aligned}
&\Pr(B = 1 \,\big|\, \mathsf{T\ \ Real}) \\
=&\frac{\Pr(B = 1 \wedge \mathsf{T\ \ Real})}{\Pr(\mathsf{T\ \ Real})} \\
=&\frac{\Pr(B = 1 \wedge \neg\mathsf{FAIL} \wedge \mathsf{T\ \ Real}) + \Pr(B = 1 \wedge \mathsf{FAIL} \wedge \mathsf{T\ \ Real})}{\Pr(\mathsf{T\ \ Real})} \\
=&\frac{\Pr(B = 1 \wedge \neg\mathsf{FAIL} \wedge \mathsf{T\ \ Real})}{\Pr(\mathsf{T\ \ Real})} \times \frac{\Pr(\neg\mathsf{FAIL} \wedge \mathsf{T\ \ Real})}{\Pr(\neg\mathsf{FAIL} \wedge \mathsf{T\ \ Real})} \\
&\quad + \frac{\Pr(B = 1 \wedge \mathsf{FAIL} \wedge \mathsf{T\ \ Real})}{\Pr(\mathsf{T\ \ Real})} \times \frac{\Pr(\mathsf{FAIL} \wedge \mathsf{T\ \ Real})}{\Pr(\mathsf{FAIL} \wedge \mathsf{T\ \ Real})} \\
=&\Pr(B = 1 \,\big|\, \neg\mathsf{FAIL} \wedge \mathsf{T\ \ Real}) \times \Pr(\neg\mathsf{FAIL} \,\big|\, \mathsf{T\ \ Real}) \\
&\quad + \Pr(B = 1 \,\big|\, \mathsf{FAIL} \wedge \mathsf{T\ \ Real}) \times \Pr(\mathsf{FAIL} \,\big|\, \mathsf{T\ \ Real}) \\
=&\Pr(B = 1 \,\big|\, \neg\mathsf{FAIL} \wedge \mathsf{T\ \ Real}) \times \Pr(\neg\mathsf{FAIL}) \\
&\quad + \Pr(B = 1 \,\big|\, \mathsf{FAIL} \wedge \mathsf{T\ \ Real}) \times \Pr(\mathsf{FAIL}) \\
&\qquad\qquad \text{(Since FAILing and T being real are independent)} \\
=&\Pr(B = 1 \,\big|\, \neg\mathsf{FAIL} \wedge \mathsf{T\ \ Real}) \times \Pr(\neg\mathsf{FAIL}) + \frac{1}{2}\Pr(\mathsf{FAIL}) \\
&\qquad\qquad \text{(whenever the reduction fails it outputs a random bit)} \\
=&\frac{1}{2} + \Pr(\neg\mathsf{FAIL})\Big(\Pr(B = 1 \,\big|\, \neg\mathsf{FAIL} \wedge \mathsf{T\ \ Real}) - \frac{1}{2}\Big) \\
=&\frac{1}{2} + \Pr(\neg\mathsf{FAIL})\varepsilon \qquad \text{(say)}
\end{aligned}$$

Now note ε is indeed the "advantage" that $\mathcal{B}$ has over a random guess.

Now similarly for random T case we have

$$\Pr(B=1\Big|\mathsf{T\ \ Random}) = \frac{1}{2} + \Pr(\neg\mathsf{FAIL})\Big(\Pr(B=1\Big|\neg\mathsf{FAIL}\wedge\mathsf{T\ \ Random}) - \frac{1}{2}\Big) = \frac{1}{2}$$

(when T is random it can only guess, hence there is no advantage
or $\Pr(B=1\Big|\neg\mathsf{FAIL}\wedge\mathsf{T\ \ Random}) = \frac{1}{2}$)

So the advantage of the reduction $\mathcal{B}$ over the DBDH challenger

$$\begin{aligned} &= \Big|\Pr(B=1\Big|\mathsf{T\ \ Real}) - \Pr(B=1\Big|\mathsf{T\ \ Random})\Big| \\ &= \frac{1}{2} + \Pr(\neg\mathsf{FAIL})\varepsilon - \frac{1}{2} \\ &= \frac{1}{exp(1)(q+1)}\varepsilon \end{aligned}$$

Which is non-negligible if ε is non-negligible.

References

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