Application Model

Lecture 10

DNA encryption

- Review

1. DLP and ElGamal Cryptosystem
2. Paillier Cryptosystem
3. Weil-pairing

The simplest case: $(s_1,s_2)==(t_1,t_2)$?

Let $z=(s1-t1)(s2-t2)$, $(s_1,s_2)==(t_1,t_2) \Leftrightarrow z==0$

Using ElGamal (public=(g,g^{α}), secret=(α,r))

. T sends $(y_1=g^{t_1}g^{\alpha r}, y_2=g^{t_2}g^{\alpha r}, y_3=g^{t_1 t_2}g^{\alpha r})$

. S computes $z_1=(y_1)^{-s_2}, z_2=(y_2)^{-s_1}, z_3=g^{s_1 s_2}$

and $u=z_1z_2z_3y_3=g^z g^{\alpha r(-s_1-s_2+1)}$

. S sends $(v_1=g^z g^{\alpha r(-s_1-s_2+1)}, v_2=g^{(-s_1-s_2+1)}$

Note

1/ suppose that $s_2=t_1$ then

(i) gz=1 and

(ii) With $g^{(-s_1-s_2+1)}$ we can get s1.

2/ S sends only one value

$v=(g^z g^{\alpha r(-s_1-s_2+1)})^{(1/(-s_1-s_2+1))}$

if (z=0) then T will have $g^{\alpha r}$.

The simplest case: $(s_1,s_2)==(t_1,t_2)$?

Let z=(s1-t1)(s2-t2), $(s_1,s_2)==(t_1,t_2) \Leftrightarrow z==0$

Using Weil-pairing (public=(P, αP), secret=(α,r))

. $z = 0 \Leftrightarrow s_1 s_2 - s_1 t_2 - s_2 t_1 + t_1 t_2 = 0 \Leftrightarrow s_1 s_2/t_1 t_2 - s_1/t_1 - s_2/t_2 + 1=0 \pmod{p}$

Set $\mu_i=s_i/t_i$, we have $\mu_1+\mu_2-\mu_1\mu_2=1 \pmod{p}$

. T computes $(y_1=g^{r/t_1}, y_2=g^{r/t_2}, y_3=g^{r/t_1 t_2})$

and sends (y_1,y_2,y_3) to S.

. S computes $v_1=(y_1)^{s_1}$, $v_2=(y_2)^{s_2}$, $v_3=(y_3)^{-s_1 s_2}$, $v=v_1 v_2 v_3$

and sends v to T

Note

1/ if $(z_1=1)$ then T receives g^r.

2/ we can use hash values of s_i, t_i.

DNA tests

(1) *Identity test*

$$\bigwedge_{i=1}^{N}\left[\{s_{i,1}, s_{i,2}\} - \{t_{i,1}, t_{i,2}\}\right] = TRUE$$

(2) *Common ancestor test on the Y chromosome*

$$\bigvee_{C\subseteq[N],|C|\geq n-t}\ \bigwedge_{i\in C}\left[\{s_i\} - \{t_i\}\right] = TRUE$$

(3) *Paternity test with one parent*

$$\bigwedge_{i=1}^{N}\left[\{s_{i,1}, s_{i,2}\} \cap \{t_{i,1}, t_{i,2}\} \neq \emptyset\right] = TRUE$$

(4) *Paternity test with two parents*

$$\bigwedge_{i=1}^{N} \begin{array}{c} \left[\left(\{c_{i,1} = m_{i,1}\} \vee \{c_{i,2}, m_{i,2}\}\right) \wedge \left(\{c_{i,2} = f_{i,1}\} \vee \{c_{i,2}, f_{i,2}\}\right)\right] \vee \\ \left[\left(\{c_{i,1} = f_{i,1}\} \vee \{c_{i,2}, f_{i,2}\}\right) \wedge \left(\{c_{i,2} = m_{i,1}\} \vee \{c_{i,2}, m_{i,2}\}\right)\right] \\ = TRUE \end{array}$$

Implementing: let $\bar{a}_{ij} = H_i(a_{ij})$

$$\textbf{(1)}\ Z_I = \sum(\bar{s}_{i1} + \bar{s}_{i2}) - \sum(\bar{t}_{i1} + t_{i2})$$

$$\textbf{(2)}\ Z_C = \sum_{i,j\in[N],i<j} (\bar{s}_i - \bar{t}_i)(\bar{s}_j - \bar{t}_j)$$

$$\textbf{(3)}\ Z_O = \sum_{i=1}^{N} z_i\,, z_i = (\bar{s}_{i1} - \bar{t}_{i1})(\bar{s}_{i1} - \bar{t}_{i2})(\bar{s}_{i2} - \bar{t}_{i1})(\bar{s}_{i2} - \bar{t}_{i2})$$

$$\textbf{(4)}\ Z_T = \sum_{i=1}^{N}[(\bar{c}_{i1} - \bar{m}_{i1})\,(\bar{c}_{i1} - \bar{m}_{i2}) + (\bar{c}_{i2} - \bar{f}_{i1})(\bar{c}_{i2} - \bar{f}_{i2})] +$$
$$[(\bar{c}_{i1} - \bar{f}_{i1})(\bar{c}_{i1} - f_{i2}) + (\bar{c}_{i2} - \bar{m}_{i1})(\bar{c}_{i2} - \bar{m}_{i2})]$$

Blockchain database

- Discussing