CS152-11

Hongchen Cao 2019533114

2020/12/03

1

From

$$\begin{cases} k\delta_1 & = x_1 - a\gamma_1 \; mod\, (p-1) \\ k\delta_2 & = x_2 - a\gamma_2 \; mod\, (p-1) \end{cases}$$

We have

$$k = 9421 \times 10915^{-1} \; mod\, 31846 = 1165$$

Then, from

$$a = \gamma_1^{-1}(x_1 - k\delta_1) \; mod\, (p-1)$$

We have

$$a = 11852 \times 11986^{-1} \; mod\, 15923 = 7459$$

Therefore,

$$a = 7459 \text{ or } 23382$$

From,

$$\alpha^{7459} \; mod\, p = 25703 = \beta$$
$$\alpha^{23382} \; mod\, p = 6144 \neq \beta$$

Thus,

$$k = 1165 \quad a = 7459$$

2

2.1

From,

$$k_i\delta_1 \equiv x_1 - a\gamma_1 (\operatorname{mod} p-1)$$
$$\left(k_i+2\right)\delta_2 \equiv x_2 - a\gamma_2 (\operatorname{mod} p-1)$$

So, we have

$$a\left(\gamma_2\delta_1 - \gamma_1\delta_2\right) \equiv x_2\delta_1 - x_1\delta_2 - 2\delta_1\delta_2 (\operatorname{mod} p-1)$$

Then, by calculate $\gcd\left(\gamma_2\delta_1 - \gamma_1\delta_2, p-1\right)$ Bob can get a.

2.2

From the equation in 2.1, we have

$$14396a \equiv 9964 (\operatorname{mod} 28702)$$
$$\gcd(14396, 28702) = 2$$

So,

$$a = 4982 \times 7198^{-1} \bmod 14351 = 5324$$

Therefore, we have $a = 5324$ or $a = 5324 + 14351 = 19675$
From,

$$5^{5324} \bmod 28703 = 17364 \neq \beta$$
$$5^{19675} \bmod 28703 = 11339 = \beta$$

Thus, $a = 19675$

3

First, we have

$$\gamma = (\alpha^k \; mod\, p) \; mod\, q = 59$$
$$\delta = (SHA3 - 224(x) + a\gamma)k^{-1} \; mod\, (p-1) = 79$$

Then

$$e_1 = SHA3 - 224(x)\gamma^{-1} \; mod\, q = 16$$
$$e_2 = \gamma\delta^{-1} \; mod\, q = 57$$

So,

$$(\alpha^{e_1}\beta^{e_2} \; mod\, p) \; mod\, q = 59 = \gamma$$

4

If $k = k_1 = k_2$,

$$\gamma_1 = \gamma_2 = h(x||\alpha^k \; mod\, p)$$

Let $\gamma = \gamma_1 = \gamma_2$ Thus, we have

$$a \equiv (\delta_1 - \delta_2)(\gamma_1 - \gamma_2)^{-1} \; (mod\, q)$$

So, Schnorr Signature Scheme is broken