Identity based cryptography

Veřejný klíč je hash nějaké identity

TA (trusted authority) — důvěryhodná autorita / orgán

Boneh-Franklin naše schéma

Veřejné parametry

$e: G_1 \times G_1 \to G_2$

$P \in G_1$

hash $H_1 : \{0,1\}^* \to G_1$

$H_2 : G_2 \to \{0,1\}^*$

TA zvolí svůj hlavní tajný klíč S (master key)

$Q = [S]P \in G_1$ veřejný klíč

Příjemce

$Q_i = H_1(ID_i)$ je jeho veřejný klíč

i-tý uživatel

Soukromý klíč $S_i = [S]Q_i$ SPOČÍTÁ PŘÍJEMCE

pošle spolehlivým kanálem uživateli

$Q_i \quad S_i = [s] Q_i$ s je master key

Uživateli i se posílá zpráva M jako dvojice

$$\Big([t] P_1 ,\ M \oplus H_3\big(\underbrace{e(Q, Q_i)^t}_{\text{prvek grupy } G_3} \big) \Big)$$

(C_1, C_2)

t zvoleno náhodně

P_1 generátor G_1 známý

Uživatel i zná $S_i = [s] Q_i$

$$e(C_1, S_i) = e([t] P, [s] Q_i) = e(P, [s] Q_i)^t = e([s] P, Q_i)^t = \boxed{e(Q, Q_i)^t}$$

$$M = C_2 \oplus H_3(e(C_1, S_i))$$

Výpočet hodnoty $\boxed{f(\mathcal{O})}$, kde $f \in K(x_1, x_2)$ je representant

$K(C)$, $C = V_w$, $w(x_1, x_2) = 0$ $w(x_1, x_2) = x_2^2 - (x_1^3 + ax_1 + b)$

$f \in K[x, y]$ $a(x) + y\,b(x)$ — y^2 se v členech vyjádří záměnou $x^3 + ax + b$

$\deg(f) = \max\{2\,st(a), 3 + 2\,st(b)\}$

$\deg(f) = \sum v_\alpha(f)$ $\bar{K} = K$ $= \sum_{P \neq \mathcal{O}} v_P(f) \deg(P)$

α probíhá všechny afinní body

$\deg(f) = -v_{\mathcal{O}}(f)$

Budeme chvíli uvažovat ještě polynomy jen s malým ohledem na křivku.

$y^2 \longrightarrow x^3+ax+b$

$f \in K[x,y]$ lze substitucí dostat ke tvaru $a(x)+y\,b(x)$

Také můžeme dostat substituce $x^3 \longrightarrow y^2-ax-b$

z toho vyjde tvar $u(y)+x\,v(y)+x^2 w(y)$

Řekneme, že f má <u>dominantní term</u> jestliže v zápisu f jako $\sum a_{ij} x^i y^j$ existuje jediné (i,j), že $a_{ij} \neq 0$ a pro toto (i,j) je $2i+3j > 2i'+3j'$, kde (i',j') je ~~[illegible]~~ takové, že $(i',j') \neq (i,j)$ a $a_{i'j'} \neq 0$

$\boxed{\begin{matrix}\lambda x^i y^j \\ \lambda \neq 0\end{matrix}} \longleftarrow$ dominantní term

Budeme chvíli uvažovat spíše polynomy jen s malým ohledem na křivku.

$y^2 \longrightarrow x^3 + ax + b$

$f \in K[x,y]$ bez substituci dostaneš to tvaru $a(x) + y\,b(x)$

Taky můžeme dostat substituce $x^3 \longrightarrow y^2 - ax - b$

z toho dostaneme vyjádření $u(y) + x\,v(y) + x^2 w(y)$

Řekneme, že f má dominantní term jestliže v zápise f jako $\sum a_{ij} x^i y^j$ existuje jediné (i,j), že $a_{ij} \neq 0$ a pro toto (i,j) je $2i + 3j > 2i' + 3j'$, kde (i',j') je ~~libovolné~~ takové, že $(i',j') \neq (i,j)$ a $a_{i'j'} \neq 0$

$$\boxed{\begin{array}{l} \lambda x^i y^j \\ \lambda \neq 0 \end{array}} \longleftarrow \text{dominantní term}$$

Lemma: Pokud má zápis f dominantní člen, tak ho má i po substituci $x^3 \longrightarrow$

$y^2 \longrightarrow$

D: Při úpravě termu odlišného od dominantního se žádný člen s max. hodnotou $2i+3j$ neobjeví

$$x^i y^j \quad \text{člen}$$

$$x^{i-3} y^j (y^2 - ax - b) = x^{i-3} y^{2+j} - \dots$$

stejná

menší $2i+3j$ hodnoty

$$x^i y^{j-2} (x^3 + ax + b) \longrightarrow x^{i+3} y^{j-2} + \dots$$

menší

$f \in K(x_1, x_2)$

bez omezení

$$\frac{ya(x)+b(x)}{y\,c(x)+d(x)} \cdot \frac{y\,c(x)-d(x)}{y\,c(x)-d(x)} = \frac{\ldots}{y^2c^2(x)+d^2(x)}$$

(x^3+ax+b)

$$\frac{ya(x)+b(x)}{c(x)}$$

$v_0(f) = \deg(c(x)) - \deg(ya(x)+b(x))$

$> 0 \;-\; f(0) = 0$

$v_0(f) < 0 \to f(0)$ nedefinováno

$= 0 \quad \deg(b(x)) > \deg(ya(x))$

$$f(0) = \frac{\ell(b)}{\ell(c)}$$

$$\frac{ya(x)+b(x)}{c(x)} \quad [YZ^2A(X,Z)+B(X,Z) : C(X,Z)]$$

$(0:1:0)$

nedefinováno $(0:0)$

Rozšíření f: hodnoty x^i, $0 \le i \le 2$ algebraicky dodají: $\frac{ya(x)+b(x)}{c(x)}$ $st(c)=st(b)=3k$

$ya(x)+b(x)$ má dominantní člen $\lambda(b)x^{3k}$

$\lambda(c)x^{3k}$

$ya(x)+b(x)$ univerzálně převést na $u_0(y)+xu_1(y)+x^2u_2(y)$

λy^{2k}, $k=st(u_0)$ jsou dominantní člen.

$st(u_1)\le k-1$ plyne z $6k>3\deg u_1+2$

$st(u_2)\le k-2$ $\quad 6k>3\deg u_2+4$

$c(x)$ jako $v_0(y)+xv_1(y)+x^2v_2(y)$

$$f(x_1,x_2)=\frac{u_0(y)+xu_1(y)+x^2u_2(y)}{v_0(y)+xv_1(y)+x^2v_2(y)}$$

$\lambda(u_0)=\lambda(b)$

$\lambda(v_0)=\lambda(c)$

$$[U_0(Y,Z)+XU_1(Y,Z)+X^2U_2(Y,Z):V_0(Y,Z)+XV_1(Y,Z)+X^2V_2(Y,Z)]$$

$(0:1:0)=[\lambda(b):\lambda(c)]=\frac{\lambda(b)}{\lambda(c)}$ STEJNĚ ~~JAKO~~ V „TECH." POPISU