Tutorial 9 SVK

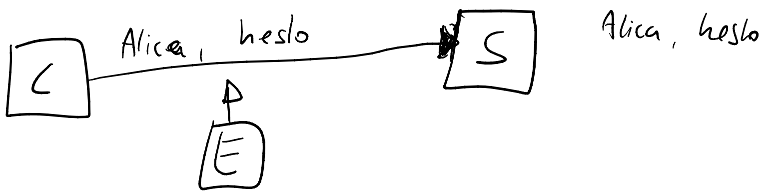
10 November 2021 17:56

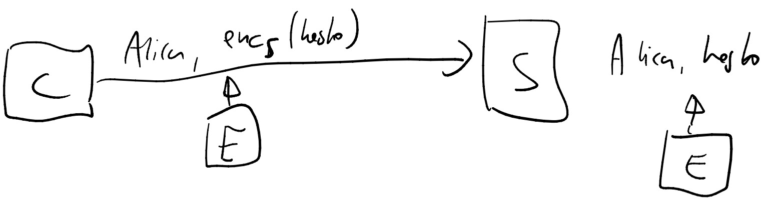
Identifikácia

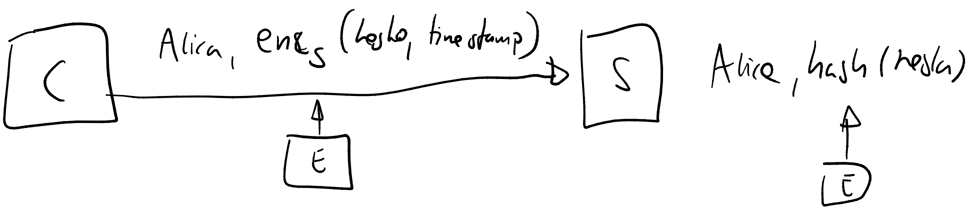
Zdieľanie tajomstva

Ortogonálne polia a autentizácia správ

Identifikácia







Tieto ↑ riešenia fungujú len pre server, ktorý je dôveryhodný

Riešenia, ktoré si ukážeme sú tzv. zero-knowledge identifikačné protokoly

Klient svoju identitu serveru preukáže pomocou demonštrácie znalosti hesla, bez toho aby heslo ukázal.

Klient = Alica = dokazovateľ

Server = Bob = verifikátor

1.) Commitment $A \to B$

2.) Challenge $B \to A$

3.) Response $A \to B$

4.) Verifikácia

Fiat-Shamir

↳ založená na zložitosti výpočtu $\sqrt{c}$ mod n, ak $n = pq$

p, q sú prvočísla a nepoznáme faktorizáciu n.

Tajný kľúč $\quad s \in \{1, \dots, n-1\}$

Verejný kľúč $\quad n, \; v = s^2 \mod n$

1.) Commitment: Alice zvolí náhodné číslo $1 \le r < n$ a pošle B.

$$x = r^2 \mod n$$

2.) Challenge: Bob zvolí náhodný bit $b \in \{0, 1\}$ a pošle ho Alici

3.) Response: Alica pošle $y = r \cdot s^b \mod n$

4.) Verifikácia: Bob overí že $y^2 = x \cdot v^b \mod n$

Opakujeme t krát. Ak dokazovateľ je schopný splniť každý t-krát, Bob si je istý s pravdepodobnosťou $1 - 2^{-t}$, že dokazovateľ je Alica

→ Ak vie útočník uhádnuť $b = 0$, verifikácia bude $y^2 = x \mod n$

Dokáže útočník nájsť také x a y?

1.) zvolí y 2.) spočítaj $x = y^2 \mod n$

→ Ak vie útočník uhádnuť $b = 1$, verifikácia bude $y^2 = x \cdot v \mod n$

vie útočník nájsť také x a y?

Vie útočník nájsť také x a z?

1.) zvoľ z 2.) spočítaj $x = z^2 \cdot v^{-1} \mod n$

TRANSCRIPT

(x, b, z) je platný iff $z^2 = x \cdot v^b \mod n$

$\boxed{n = 15, v = 4}$

$z^2 = x$

$11^2 = x \mod 15$

$x = 1$

$(x, 0, z) \rightsquigarrow (1, 0, 11)$

$(x, 1, z) \rightsquigarrow (6, 1, 3)$

$z^2 = x \cdot 4 \mod 15 \quad / \cdot (4^{-1}) = 4$

$4 \cdot 3^2 = x$

$36 \equiv 6 \equiv x \mod 15$

$\left.\begin{array}{l}(x, 0, z_0) \\ (x, 1, z_1)\end{array}\right\}$ nájdenie takýchto dvoch transcriptov je ekvivalentné výpočtu s_0

$z_0^2 = x \mod n$

$z_1^2 = x \cdot v \mod n$

$z_0 = \sqrt{x} \mod n$

$z_1 = \sqrt{x} \cdot s \mod n$

$z_1 = z_0 \cdot s \mod n$

$s \equiv z_1 \cdot z_0^{-1} \mod n$

Shnorr identifikácia

↳ založený na diskrétnom logaritme

ťažký je diskrétny logaritmus

Verejné informácie: p – veľké prvočíslo

p ·· [illegible]

Verejné informácie: p – veľké prvočíslo

q – prvočíslo, ktoré delí $(p-1)$ $[q \approx 140 \text{ bitov}]$

$\alpha \in \mathbb{Z}_p^*$ rádu q $\quad [\alpha^q \equiv 1 \mod p]$

$\boxed{\text{bezpečnostný parameter } t}$ s.t. $2^t < q$ → Ako ťažké je uhádnuť challenge

$$\vartheta = \alpha^{-a} \mod p \equiv \alpha^{q-a} \mod p$$

Správa Podpísaná autoritou: $\boxed{\mathrm{Sig}_{TA}(\text{"Alica"}, \vartheta, p, q, \alpha)}$

Tajná informácia: $1 < a \leq q-1$

1.) <u>Commitment:</u> Alica náhodne zvolí $1 \leq k \leq q-1$
a pošle $\gamma = \alpha^k \mod p$

2.) <u>challenge:</u> Bob náhodne zvolí $1 \leq r \leq 2^t - 1$

3.) <u>response:</u> Alica pošle $y = (k + a \cdot r) \mod q$

4.) <u>verifikácia:</u>

$$\gamma = \alpha^y \vartheta^r \mod p$$

$$\alpha^k = \alpha^{k+ar} \alpha^{-a \cdot r} \mod p$$

$$\alpha^k = \alpha^k \mod p$$

1.) k musí byť náhodné a tajné, ak Bob zistí k, vie spočítať
$a = (y-k) \cdot r^{-1} \mod q$.

2.) r musí byť náhodné a tajné, až do momentu keď dokazovateľ pošle γ.

[illegible]

[illegible] y.

Inak dokazovateľ vie nájsť γ a y také že

$$\gamma = \alpha^{y} v^{r} \mod p$$

1.) vyber y 2.) $\boxed{\text{spočítaj } \gamma = \alpha^{y} \cdot v^{r}}$ mod p

Po 1 kole Bob vie s pravdepodobnosťou $1-2^{-t}$, že sa rozpráva s Alicou.

TRANSCRIPTS

(γ, r, y) je platný $\gamma = \alpha^{y} \cdot v^{r} \mod p$

Vytvoriť platné transkripty je jednoduché

$\nexists$

$$\left.\begin{array}{l}(\gamma, r_1, y_1) \\ (\gamma, r_2, y_2)\end{array}\right\}$$ spočítanie je také ťažké ako výpočet a.

$$\alpha^{y_1} v^{r_1} = \gamma = \alpha^{y_2} v^{r_2} \mod p$$

$$\alpha^{y_1} \alpha^{-a r_1} = \alpha^{y_2} \alpha^{-a r_2} \mod p$$

$$y_1 - a r_1 \equiv y_2 - a r_2 \mod q$$

$$a \equiv (y_2 - y_1)(r_2 - r_1)^{-1} \mod q$$

$$z_2 = f(z_1)$$

$$\alpha^{z_1} = \alpha^{y_1} v^{r_1}$$

$$\alpha^{z_2} = \alpha^{y_2} v^{r_2}$$

$z_2 = 4 z_1 + 3 \mod q$

Zdieľanie tajomstva

U - množina užívateľov $\quad U = \{1, \dots, n\}$

A - prístupová štruktúra $\quad A \subseteq P(U) = 2^U$

$P(U) = \{\emptyset, \{1\}, \{2\}, \dots, U\}$

$U = \{A, B, C, D\}$

$A = \{\{A,B\}, \{B,C,D\}, \{A,C,D\}\}$ ✗

$A = \{\{A,B\}, \{A,B,C\}\}$

Prahové schémy (n,t)

n - počet užívateľov

t - veľkosť autorizovanej množiny

$(4,2)$ schéma

$U = \{1, 2, 3, 4\}$

$A = \{\{1,2\}, \{1,3\}, \{1,4\}, \{2,3\}, \{2,4\}, \{3,4\}\}$

Shamirovo prahové zdieľanie tajomstva

1.) p - veľké prvočíslo

2.) každý užívateľ dostane $x_i \in \mathbb{Z}_p$ $(x_i = i$ typicky$)$

3.) pre zdieľanie tajomstva $S \in \mathbb{Z}_p$ pošli každému užívateľovi

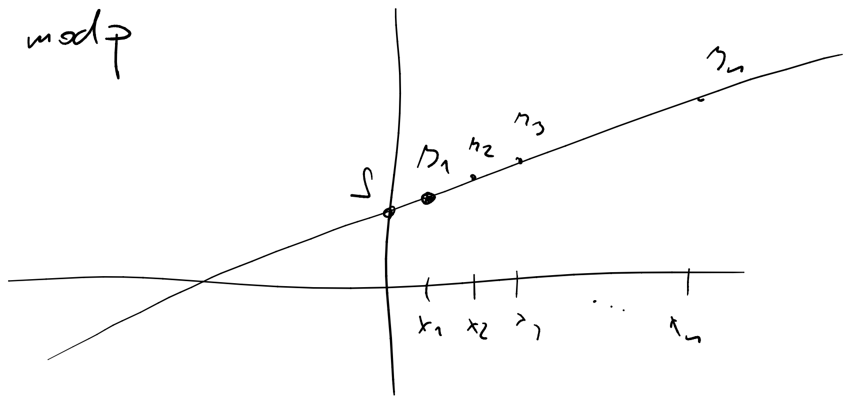
$$y_i = a(x_i)$$

kde $a(x) = \sum_{j=1}^{t-1} a_j x^j + S \mod p$

a čísla $a_i \in \mathbb{Z}_p$ sú vybrané náhodne a tajné

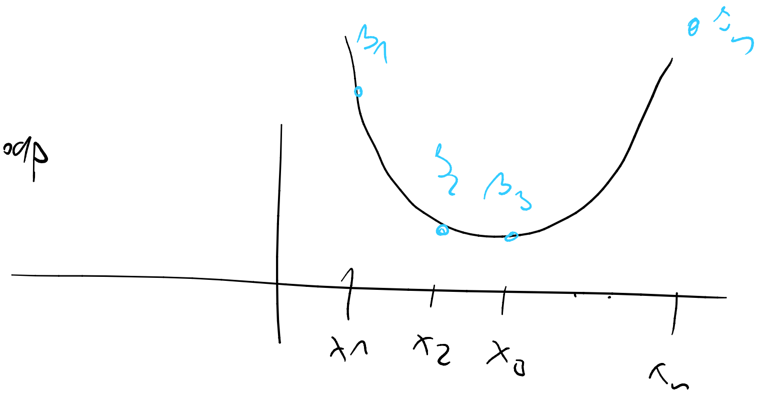
$t=2$ a je lineárna funkcia

$a(x) = a_1 x + S \mod p$



$t=3$ a je kvadratická funkcia

$a(x) = a_2 x^2 + a_1 x + S \mod p$



Pre prahovú hodnotu t, $a(x)$ má stupeň $t-1$ a je potrebných t bodov na rekonštrukciu $a(x)$ $a(0) = S$.

Príklad $(3,3)$ schéma

$a(1) = 9 \mod 11$ $a(x)$ má stupeň 2

$a(1) = 9 \mod 11$ $\quad$ $a(x)$ má stupeň 2

$a(2) = 9 \mod 11$ $\quad$ a tvar

$a(3) = 4 \mod 11$ $\quad$ $a(x) = ax^2 + bx + c$

$$\boxed{\begin{aligned} a + b + c &\equiv 9 \mod 11 \\ 4a + 2b + c &\equiv 9 \mod 11 \\ 9a + 3b + c &\equiv 4 \mod 11 \end{aligned}}$$

Ortogonálne polia

$OA(n, k, \lambda)$ → pole veľkosti $(\lambda n^2) \times (k)$ obsahuje n znakov a každá dvojica stĺpcov obsahuje každú z n^2 dvojíc znakov presne λ krát.

$OA(3, 3, 1)$

stĺpce

symboly

opakovania párov

$\lambda n^2 \times k$

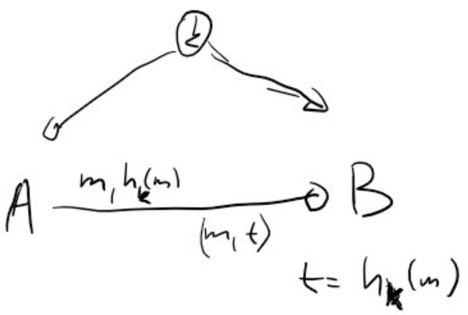
$1 \cdot 3^2 \times 3$

9×3

	m_1	m_2	m_3
h_1	0	0	0
h_2	1	1	1
h_3	2	2	2
h_4	0	1	2
h_5	2	0	1
h_6	1	2	0
h_7	0	2	1
h_8	1	0	2
h_9	2	1	0

1.) útočník chce poslať správnu dvojicu (m, t), bez toho aby Alica niečo poslala

2.) Alica pošle $m, h_2(m)$
Útočník chce modifikovať na $[m', h_2(m')]$



$(m', h_2(m'))$

$t-(n,k,\lambda)$ OA $\quad t$ počet stĺpcov

$\lambda n^t \times k \quad$ pole n znakov s k stĺpcami, taký že v každej t-tici stĺpcov sa každá z n^t možných t-tíc n znakov vyskytuje presne λ krát

$2-(n,k,\lambda)$ OA