Tutorial IX

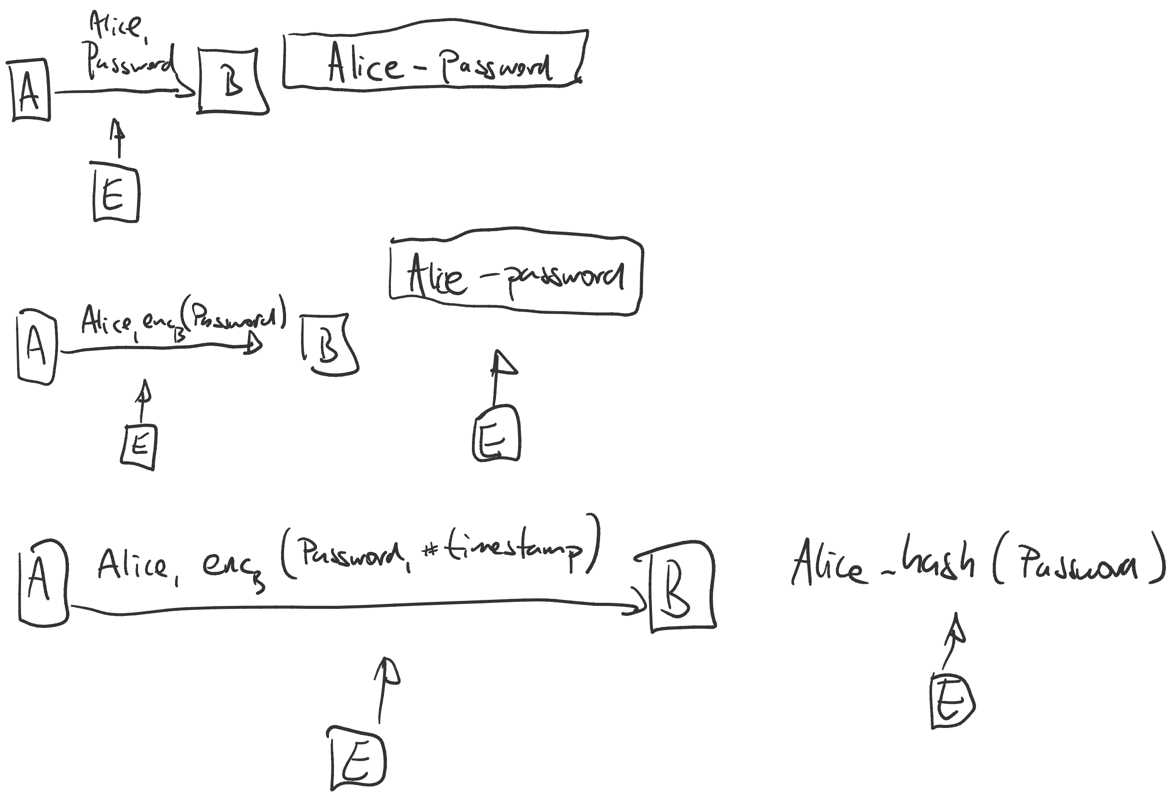
04 December 2020 14:53

Identification

Secret sharing

Orthogonal arrays → message authentication with shared key

Identification



These ↑ work only for trusted $\boxed{B}$ (he knows the password)

Here ↓ we learn about zero-knowledge identification protocols

Alice proves her identity to Bob by demonstrating knowledge of her password without revealing it.

Alice - Prover

Bob - Verifier

Eve - Evesdropper

1.) Commitment $A \to B$

2.) Challenge $B \to A$

3.) Response $A \to B$

4.) Verification

Fiat-Shamir identification

↳ based on hardness of calculating $\sqrt{c}$ mod n, for $n = p \cdot q$, without the knowledge of p, q.

Private: $s \in \{1, \dots, n-1\}$

Public: n, $v = s^2 \bmod n$

1.) commitment part: Alice chooses random $1 \leq r < n$ and sends

$\to x = r^2 \bmod n$ to Bob

→ 2.) challenge: Bob chooses a random bit $b \in \{0, 1\}$ and sends it to Alice

3.) response: Alice sends $y = r \cdot s^b \bmod n$ to Bob

4.) verification: Bob verifies whether $y^2 = x \cdot v^b \bmod n$

→ r needs to be secret – random and unknown to Bob. Why?

if Bob knows r, he can choose $b = 1$, then $y = r \cdot s$ and if Bob knows r_i he can choose $b=1$, then $y = r \cdot s$ and Bob can calculate $s = y \cdot r^{-1} \mod n$

→ If Prover can guess $b=0$ they can pass the protocol

In this case verification will be $y^2 = x \mod n$

Can you find such x and y

1.) Choose y 2.) calculate x (order is important this is why the commitment is sent before the challenge)

→ If Prover can guess $b=1$. Verification will be

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

Can you find such x and y?

$$x = y^2 \cdot v^{-1} \mod n$$

1.) choose y 2.) calculate $x = y^2 \cdot v^{-1} \mod n$

TRANSCRIPT

(x, b, y) valid iff $y^2 = x \cdot v^b \mod n$

$\boxed{n = 15,\ v = 4}$ $11^2 = x \cdot v^0$

$(x, 0, y) \rightsquigarrow (1, 0, 11)$ $\quad \overset{y^2}{11^2} = \overset{x}{1} \mod 15$

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

$y^2 = x \cdot v$

$3^2 = x \cdot 4 \mod 15 \qquad 1 \cdot 4^{-1} (=4)$

$4 \cdot 5 = x \mod 15$

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

$(x, 0, y_0)$
$(x, 1, y_1)$ } ↳ calculating two transcripts is as hard as finding s

$y_0^2 = x \mod n$

$y_1^2 = x \cdot v \mod n$

$y_0 = \sqrt{x} \mod n$

$y_1 = \sqrt{x} \cdot s \mod n$

$y_1 = y_0 \cdot s \mod n$

$s = y_1 \cdot y_0^{-1} \mod n$

After n correct rounds Bob knows he is talking to Alice w.p. $1 - \frac{1}{2^n}$

Shnorr identification

↳ based on discrete log problem

Public information: p - large prime

q - a prime dividing $(p-1)$ [q - is 140 bits] σ

$\alpha \in \mathbb{Z}_p^*$ of order q $[\alpha^q = 1 \mod p]$

$\boxed{\text{Security parameter } t}$ s.t. $2^t < q$ → how hard it is to guess a challenge.

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

Signed by public authority: $Sig_{TA}(ALICE, v, p, q, \alpha)$ σ

Private: $1 \leq a \leq q-1$

1.) <u>commitment</u> Alice randomly chooses $1 \leq k \leq q-1$ and sends $\gamma = \alpha^k \mod p$

2.) <u>challenge:</u> Bob chooses randomly $1 \leq r \leq 2^t - 1$ and sends it to Alice

3.) <u>response</u> Alice sends $y = (k + ar) \mod q$ σ

4.) verification:

$$\gamma = \alpha^y \cdot v^r \mod p$$

$$\alpha^k = \alpha^{(k+ar)} \alpha^{-ar} \mod p$$

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

→ k should be random and secret (unknown to Bob) if Bob learns k then $a = (y - k) r^{-1} \bmod q$

$\Rightarrow$ r should be random and unknown to Prover before she sends her commitment γ.

Otherwise Prover can find two numbers γ and y for which $\gamma = \alpha^{y} v^{r} \bmod p$.

Easy: 1.) choose y 2.) calculate $\gamma = \alpha^{y} v^{r} \bmod p$.

After 1 round Bob knows he is talking to Alice w.p. $1 - 2^{t}$

TRANSCRIPTS

(γ, r, y) valid iff $\gamma = \alpha^{y} v^{r} \bmod p$

$$\left.\begin{array}{l}(\gamma, r_1, y_1) \\ (\gamma, r_2, y_2)\end{array}\right\}$$ calculating is as hard as calculation of a

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

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

$$y_1 - a r_1 = y_2 - a r_2 \bmod q$$

$r_2 = f(r_1)$

$$a = (y_2 - y_1) \cdot (r_2 - r_1)^{-1} \bmod q$$

$$\alpha^{y_1} v^{r_1} = f(\alpha^{y_2} v^{r_2})$$

$$h^{\beta_1 v_1}_{v} = f(\alpha^{\beta_2 v_2}_{v})$$

Secret sharing

U = user set $\qquad U = \{1, \dots, n\}$

A - access structure $\qquad A \subseteq P(U) = 2^U$

$$P(U) = \{\emptyset, \{1\}, \{2\}, \dots, \{1,2\}, \{1,3\}, \dots, U\}$$

$$|P(U)| = 2^{|U|}$$

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

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

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

Threshold schemes (n,t)

n - number of users

t - size of the authorized set

$(4,2)$-scheme

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

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

Shamir threshold secret sharing

1.) p - a large prime

2.) to each user send $x_i \in \mathbb{Z}_p$ (typically $x_i = i$)

3.) to share a secret $S \in \mathbb{Z}_p$ send to each user

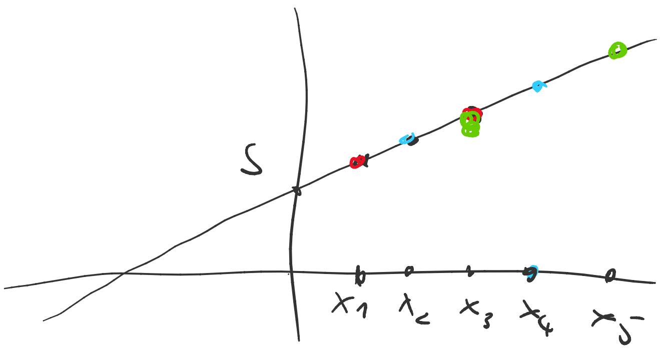
$$y_i = a(x_i)$$

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

and $a_i \in \mathbb{Z}_p$ are chosen at random and kept secret.

for $t=2$ a is a linear function

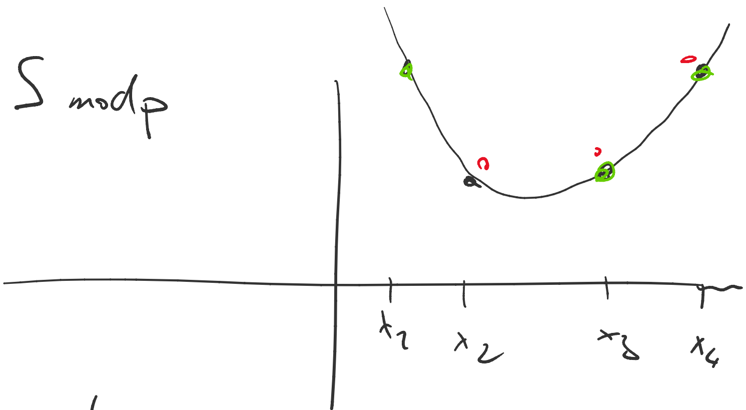
$$a(x) = a_1 x + S \mod p$$



for $t=3$

a is quadratic

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



for threshold t a is of degree $t-1$

for thershold t a is of degree $t-1$

and t points are needed to reconstruct $a(x)$ and find $a(0) = S$.

Example of $(3,3)$ scheme

$f(1) = 9 \mod 11$ degree of f is 2

$f(2) = 9 \mod 11$

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

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

ORTHOGONAL ARRAYS

$OA(n,k,\lambda)$ is a $\lambda n^2 \times k$ array of n symbols s.t.

in any two columns of the array each of the n^2 possible pairs of symbols appear exactly λ-times.

$OA(3,3,1)$ → repetition of pairs

symbols columns

$\lambda n^2 \times k$

$1 \cdot 3^2 \times 3$

9×3

$$\begin{array}{c|ccc} & m_1 & \boxed{m_2} & m_3 \\ \hline h_1 & 0 & 0 & 0 \\ \boxed{h_2} & 1 & 1 & 1 \\ h_3 & 2 & 2 & 2 \\ \boxed{h_4} & 0 & \boxed{1} & 2 \\ h_5 & 1 & 2 & 0 \\ \boxed{h_6} & 2 & 0 & 1 \\ \boxed{h_7} & 0 & 2 & 1 \\ h_8 & 1 & 0 & 2 \\ h_9 & 2 & 1 & 0 \end{array}$$

1.) Adversary wants to send a message to Bob without seeing Alice's message first

2.) Alice sends a valid pair $m, h_k(m)$

And adversary wants to change it to $m', h_k(m')$

$m \neq m'$

$$\overset{k}{A} \xrightarrow[(m,t)]{(m, h_k(m)) \to} \overset{k}{B}$$

$m \quad h_k(m) = t$

$m', h_k(m')$

$m', h_k(m')$

E

$m', h_l(m)$

$m \neq m'$

$3-(3,3,1)-OA$

Generalization – strength of OA t

$t-(n,k,\lambda)$ OA   Consider tuples instead of pairs

$\lambda n^t \times k$ array such that each of n^t tuples (of n symbols) appear in every subset of t columns exactly λ-times

$2-(n,k,\lambda)$ OA are 'plain' OAs