Tutorial 9 ENG

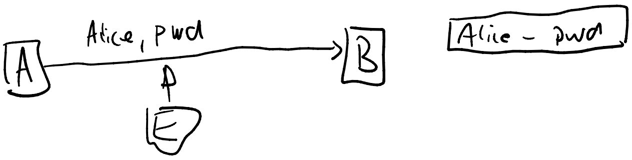
10 November 2021 13:50

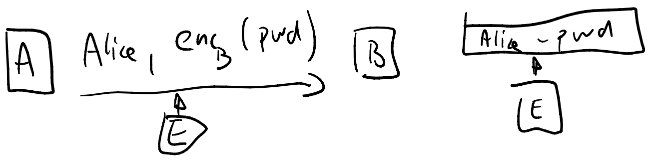
Identification

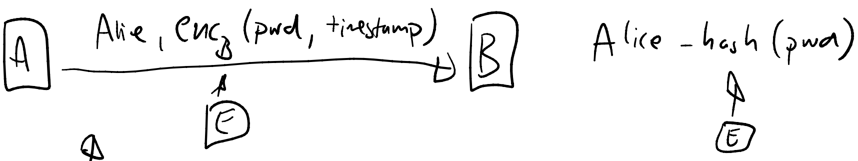
Secret sharing

Orthogonal arrays → message authentication

Identification







This works only for trusted B (they know 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 → eavesdropper

1.) Commitment A → B

2.) Challenge B → A

3.) Response A → B

4.) Verification

Fiat-Shamir indentification

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

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

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

1.) commitment: Alice chooses a random number $1 \leq r < n$ and
→ sends $\boxed{x = r^2 \mod n}$ to Bob

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

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

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

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

→ r needs to be secret → random and unknown to Bob. Why?
if Bob knows r he can choose $b = 1$, then $y = r \cdot s \mod n$
and $s = y \cdot r^{-1} \mod n$

→ Impersonator who does not know s can guess $b = 0$, then $y = r$ and
$y^2 = x \mod n$

Can impersonator find such x and r?

1.) choose r (y) 2.) calculate $x = r^2$ ← Order is important! this is why the commitment is sent before challenge

→ Impersonator can guess $b = 1$, Verification is
$y^2 = x \cdot v \mod n$

Can you find such x and y?
$x = y^2 \cdot v^{-1} \mod n$

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

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

$11^2 = x \mod 15 \Rightarrow x = 1$

$121 \equiv 1 \mod 15$

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

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

$y^2 = x \cdot v$

$3^2 \equiv 4x \mod 15 \quad / 4^{-1} (4)$

$4 \cdot 9 = x \mod 15$

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

$(x, 0, y_0)$

$(x, 1, y_1)$

finding two transcripts like this is as hard as finding s.

$y_0^2 = x \mod n$

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

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

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

$y_1 = y_0 \cdot s \mod n$

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

Shnorr identification

↳ discrete logarithm problem

discrete log problems

Site

Public information: p - large prime

q - a prime dividing $(p-1)$ $\{q$ - is $\underline{140}$ bits$\}$

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

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

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

Signed by public trusted authority: $\boxed{Sig_{TA}(\text{"ALICE"}, v, p, q, \alpha)}$

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

$\boxed{k_2 = 3\,5\,1\,4 \mod q}$

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

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

3.) response: Alice sends $y = (k + ar) \mod q$

4.) verification: $\gamma = \alpha^y \cdot v^r \mod p$

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

$$\alpha^k \equiv \alpha^k \mod p$$

→ k needs to be secret (unknown to Bob) otherwise $a = (y - t) \cdot r^{-1} \mod q$

$\to$ t should be secret (unknown to Prover) before they commit

Otherwise impersonator can find two numbers γ and y for which $\gamma = \alpha^{y} \cdot \vartheta^{r} \mod p$

1.) Choose y 2.) calculate $\gamma = \alpha^{y} \vartheta^{r} \mod p$

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

TRANSCRIPTS

(γ, r, y) valid iff $\gamma = \alpha^{y} \cdot \vartheta^{r} \mod p$

(γ, r_1, y_1)
(γ, r_2, y_2) calculating is as hard as calculation of a

$$\boxed{\begin{aligned}
&\alpha^{y_1} \vartheta^{r_1} \equiv \gamma \equiv \alpha^{y_2} \cdot \vartheta^{r_2} \mod p \\
&\alpha^{y_1} \cdot \alpha^{-ar_1} \equiv \alpha^{y_2} \alpha^{-ar_2} \mod p \\
&y_1 - a r_1 \equiv y_2 - a r_2 \mod q \\
&a \equiv (y_2 - y_1) \cdot (r_2 - r_1)^{-1} \mod q
\end{aligned}}$$

$\gamma_2 = f(\gamma_1)$

$$\alpha^{y_1} \vartheta^{r_1} = f(\alpha^{y_2} \vartheta^{r_2}) \mod p$$

$$\boxed{\alpha^{\beta_1} v^{v_1} = f(\alpha^{\beta_2} v^{v_2}) \mod p}$$

Secret sharing

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

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

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

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

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

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

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

Threshold schemes $\quad (n,t)$

n - num of users

t - size of authorized set

$(4,2)$-scheme

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

Shamir threshold secret sharing

1.) p - a large prime

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

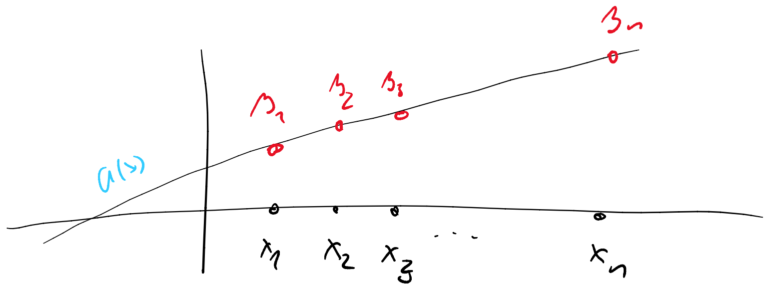
3.) to share a secret $S \in \mathbb{Z}_p$ send to each user

$$y_i = a(x_i)$$

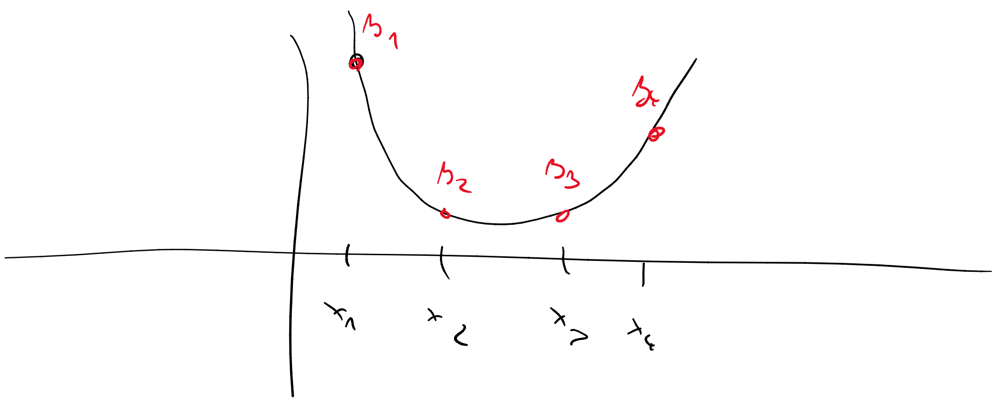
where $$a(x) = \sum_{j=1}^{t-1} a_j x^j + S \mod p$$

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

for $t=2$ $\quad a(x) = a_1 x + S \quad \Rightarrow$ a is a linear function



$t=3$ $\quad a(x) = a_1 x + a_2 x^2 + S \mod p \quad \Rightarrow$ $a(x)$ is quadratic



for threshold 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

$$\boxed{\begin{aligned} a(1) &= 9 \mod 11 \\ a(2) &= 9 \mod 11 \\ a(3) &= 4 \mod 11 \end{aligned}}$$

degree of $a(x)$ is 2

and $a(x) = ax^2 + bx + c$

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

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

3 symbols, 3 columns

$\lambda n^2 \times k$

$1 \cdot 3^2 \times 3$

9×3

$$A \xrightarrow[(m,t)]{m, h_2(m)} B \qquad h_2(m) = t$$

$m', h_2(m')$

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

1.) wants to send message to Bob without seeing alice's message first.

2.) Alice sends a valid pair $m, h_2(m)$. and Adversary wants to change it to m' $[m', h_2(m')]$.

Generalization – strength of OA t

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

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