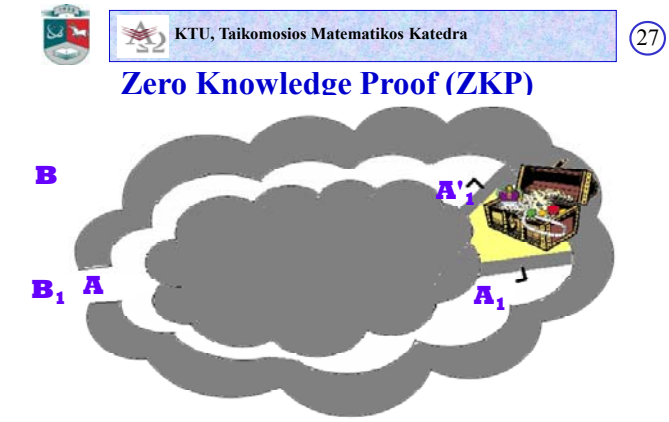
2009 m. sausio 29 d.
10:45

Zero Knowledge Proof Identifications - Neatskleidžianti Žinių Identifikacija



$P = \frac{1}{2^8} = \frac{1}{2} \cdot \frac{1}{2} \cdot \ldots \frac{1}{2}$

L. Guilou & J-J. Quisquater : iliustracija

$\mathcal{A} \equiv \mathcal{P}$: Prover, Pirkėjas (Peggy)

$\mathcal{B} \equiv \mathcal{V}$: Verifier, Verslininkas (Victor)

$\mathcal{A} : \sigma$ ("Aš esu Aldona") $= S_A$

$PR_A = x$

$\mathcal{A} \longleftrightarrow \mathcal{B}$

VR šifrav. metodas $\mathcal{E}_{VR_A}(t) = c$

$\mathcal{D}_{PR_B}(c) = t$

1) $\mathcal{B}$: $R_B \in_r \{0,1\}^*$; $com_B(R_B) \longrightarrow \mathcal{A}$

2) $\mathcal{A}$: $R_A \in_r \{0,1\}^*$; $R_A \longrightarrow \mathcal{B}$

3) $\mathcal{B}$: VR_A ; $c = \mathcal{E}_{VR_A}(com(R_B) \oplus R_A) \longrightarrow \mathcal{A}$

4) $\mathcal{A}$: $\mathcal{D}_{PR_A}(c) = com_B(R_B) \oplus R_A$ Turi būti teisingai dešifruotas com_B ir R_A

$com_A(com_B(R_B) \oplus R_A) \longrightarrow \mathcal{B}$

5) $\mathcal{B}$: atskleidžia $R_B \longrightarrow \mathcal{A}$

6) $\mathcal{A}$: patikrina, ar R_B teisingas ir $R_A \longrightarrow \mathcal{B}$

6) $\mathcal{A}$: patikrina, ar R_B teisingas ir $R_A \longrightarrow \mathcal{B}$

7) $\mathcal{B}$: patikrina R_A ir jei jis teisingas, priima Irodyma

Protokolas turi 6 komunikacijas.

L. Guilou & J-J. Quisquater IDENTIFICATION

$\mathcal{A}$: ▭ IK - (smart card)

IK atributai : {Nr, Galiojimo laikas, A/S ...} = J

TTP - Operatorius :

1. Sugeneruoja slaptus pirm. sk. p, q ir apsk. $n = pq$
   Atsit. parenka ν
   Apskaičiuoja X : $JX^{\nu} \equiv 1 \bmod n$

$PR_A = (X)$ $\qquad$ $VR_A = (\nu, n)$

$\mathcal{A}$ nori įrodyti $\mathcal{B}$, kad atributai J priklauso jai $\Rightarrow$
$\mathcal{A}$ reikia įrodyti, kad ji žino X.

1. $\mathcal{A}$ atsit. parenka $r \in_r [1, n-1]$, apsk. $a = r^{\nu} \bmod n$
   $\mathcal{A} \xrightarrow{a} \mathcal{B}$ $\qquad$ $r = \sqrt[\nu]{a} \bmod n$
2. $\mathcal{B}$ atsit. parenka $s \in_r [0, \nu - 1]$
   $\mathcal{A} \xleftarrow{s} \mathcal{B}$
3. $\mathcal{A}$ apskaič. $A = rX^s \bmod n$
   $\mathcal{A} \xrightarrow{A} \mathcal{B}$
4. $\mathcal{B}$ apskaič. $b = A^{\nu} J^s$: Jeigu $a = b \bmod n \Rightarrow +$

Patikrinimas

$$b = A^{\nu} J^s = (rX^s)^{\nu} J^s = r^{\nu} X^{s\nu} J^s = r^{\nu} \underbrace{(JX^{\nu})^s}_{=1} =$$
$$= r^{\nu} \bmod n = a \bmod n$$

Jei protokolas vykdomas t kartų, klastojimo tikimybė yra $\nu^{-t} = 1/\nu^t$

C. Schnorr