2009 m. sausio 29 d.
10:45

# Zero Knowledge Proof Identifications - Neatskleidžianti Žinių Identifikacija

## ZKP Identification Nr 2: Claus Schnorr Identification

Parenkam pirminį sk. $p = kq + 1$ // $q$ - pirminis

Pvz. $p = 11 = 2 \cdot 5 + 1 = 11$ // $q = 5$

$\mathcal{Z}_{11}^* = \{1, 2, 3 \ldots, 10\}$ // $\mathcal{Z}_{11}^* = \mathcal{Z}_{11} \setminus \{0\}$

Sudarykime $\mathcal{Z}_{11}^*$ eksponenčių lentelę:

>> dexp_lent(11) >> daug_lent(11)

ans =

| $i$ | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| $2^i$ | 2 | 4 | 8 | 5 | 10 | 9 | 7 | 3 | 6 | 1 | $g \in \mathcal{Z}_{11}^*$ |
| $3^i$ | 3 | 9 | 5 | 4 | 1 | 3 | 9 | 5 | 4 | 1 | $g \in G_q \subset \mathcal{Z}_{11}^*$ |
| | 4 | 5 | 9 | 3 | 1 | 4 | 5 | 9 | 3 | 1 | |
| | 5 | 3 | 4 | 9 | 1 | 5 | 3 | 4 | 9 | 1 | |
| | 6 | 3 | 7 | 9 | 10 | 5 | 8 | 4 | 2 | 1 | |
| | 7 | 5 | 2 | 3 | 10 | 4 | 6 | 9 | 8 | 1 | |
| | 8 | 9 | 6 | 4 | 10 | 3 | 2 | 5 | 7 | 1 | |
| | 9 | 4 | 3 | 5 | 1 | 9 | 4 | 3 | 5 | 1 | DSA |
| $10^i$ | 10 | 1 | 10 | 1 | 10 | 1 | 10 | 1 | 10 | 1 | |

$q=5$: $G_q = \{1, 3, 4, 5, 9\}$ : aibė uždara · in ^ atžv.

$\forall g \in G_q : g^q \equiv 1 \bmod p \ \& \ g^a \not\equiv 1 \bmod p; a < q.$

Schnorr Identification : Viešieji param.: $p$, $g \in G_q$

$\mathcal{A}$ : $x \in_r (1, q)$

PR = $x$ VR = $a = g^{-x} \bmod p$

1) $\mathcal{A}$ : $r \in_r (1, q)$; $b = g^r \bmod p$; $\mathcal{A} \xrightarrow{b} \mathcal{B}$

2) $\mathcal{B}$ : $e \in_r [1, 2^t - 1]$; $2^t < q$; $\mathcal{A} \xleftarrow{e} \mathcal{B}$

3) $\mathcal{A}$ : $c = r + ex \bmod q$ $\mathcal{A} \xrightarrow{c} \mathcal{B}$

4) $\mathcal{B}$ : $b \stackrel{?}{=} g^c a^e \bmod q$

$$g^c a^e = g^{r+ex} (g^{-x})^e = g^r \cancel{g^{ex}} \cancel{g^{-ex}} = g^r = b$$

Lo ataka: a) atspėja $e$, kuris bus atsiųstas iš $\mathcal{B}$ (2) etape

atsiųstas iš $\mathcal{B}$ (2) etape

b) parenka bet kokį $c'$

1) $\mathcal{Lo}$ : $b' = g^{c'} a^{e}$ $\quad \mathcal{Lo} \xrightarrow{b'} \mathcal{B}$

2) $\mathcal{B}$ : vykdo protokolą $\quad \mathcal{Lo} \xleftarrow{e} \mathcal{B}$

3) $\mathcal{Lo}$ : nieko neskaičiuoja $\quad \mathcal{Lo} \xrightarrow{c'} \mathcal{B}$

4) $\mathcal{B}$ : patikrinimas teisingas $\mathcal{Lo} = \mathcal{A}$

Tikimybė atspėti $e$ yra $1/2^t$ $\quad P = 1/2^{72}$

Param. reikšmės : $|t| = 72\,b$ ; $|q| = 140\,b$ ; $|p| = 512\,b$.

Schnorr Signature : pranešimas $M$ ; H-funkcija.

$PR = x$ $\qquad VR = a = g^{-x} \bmod p$

$\mathcal{A}$ : $r \in_R (1, q)$ ; $\quad b = g^r \bmod p$ ;

$\mathcal{A}$ : $s = H(M \| b)$ ; $\quad c = r + xs \bmod q$

$S = (s, c)$

$\mathcal{A} \xrightarrow{M, S} \mathcal{B}$

$\mathcal{B}$ : $b' = g^c a^s = g^r g^{xs} g^{-xs} = g^r = b$

$s \stackrel{?}{=} H(M \| b')$

JAV patentas:

C. Schnorr, Method for Identifying Subscribers and for Generating and Verifying Electronic Signaturs in a Data Exchange System, U. S. Patent #4,995,082, 19 Feb 1991.

1993 m. Kompanija PKP – Public Key Partners iš CA įgijo pasaulines teises šiam patentui.

Patento galiojimo laikas baigėsi 19 Feb 2008.

Identifikacijos metodas ⟶ Parašo schema :

$\mathcal{B}$ pakeičiamas H-funkcija

Prieš pasirašymą $M$ ne H-uojamas

H-avimas įdedamas į parašo schemą.