Liet. matem. rink, **47**, *spec. nr.*, 2007, 197–201

Rakto apsikeitimo protokolas Braid grupės įvaizdžio lygmenyje

Povilas TVARIJONAS, Eligijus SAKALAUSKAS,
Gediminas Simonas DOSINAS (KTU)
el. paštas: povilas.tvarijonas@ktu.lt, esakal@asi.lt, gediminas.dosinas@ktu.lt

1. Įvadas

Rakto apsikeitimo protokolas (RAP) labai svarbus kuriant kriptografines sistemas. Darbe siūloma RAP realizacija remiasi baigtine multiplikacine grupe $<G, \cdot>$.

Tegu $GL(n, \boldsymbol{Z})$ – n-tosios eilės neišsigimusių matricų apibrėžtų žiede $\boldsymbol{Z}$ multiplikacinė grupė. φ – šių grupių homomorfizmas [1], t.y. φ: $G \to GL(n, Z)$.

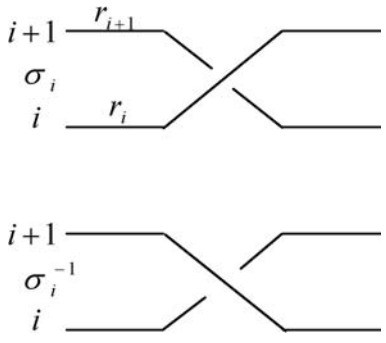
2. Raktų apsikeitimo protokolas

Naudosimės tokiu raktų apsikeitimo protokolu [2]. Tegu $\theta \in G$, θ – žinomas, G_1 ir G_2 tarpusavyje komutatyvūs grupės G poaibiai, t.y. $\forall a_1 \in G_1 \subset G, \forall a_2 \in G_2 \subset G$, $a_1 \cdot a_2 = a_2 \cdot a_1$.

1. „Aldona“ laisvai pasirenka $\alpha \in G_1$ ir suformuoja žodį
   $\omega_1 = \alpha \cdot \theta \cdot \alpha^{-1}$,
   kurį homomorfizmo pagalba atvaizduoja į matricą
   $V_1 = \varphi(\omega_1) = \varphi(\alpha) \cdot \varphi(\theta) \cdot \varphi(\alpha^{-1}) = AQA^{-1}$.
2. Pasirinkusi $r \in N$ apskaičiuoja
   $V_1^r = AQ^rA^{-1}$
   ir siunčia V_1^r „Broniui“.
3. „Bronius“ pasirenka $\beta \in G_2$ ir konstruoja žodį
   $\omega_2 = \beta\theta\beta^{-1}$,
   kuris homomorfizmo pagalba atvaizduojamas į matricą
   $V_2 = \varphi(\omega_2) = BQB^{-1}$.
4. Pasirinkęs $s \in N$ „Bronius“apskaičiuoja
   $V_2^s = BQ^sB^{-1}$ ir siunčia V_2^s „Aldonai“.
5. „Aldona“ apskaičiuoja
   $K_A = A \cdot (V_2^s)^r \cdot A^{-1} = ABQ^{sr}B^{-1}A^{-1}$.
   „Bronius“ apskaičiuoja
   $K_B = B \cdot (V_1^r)^s \cdot B^{-1} = BAQ^{rs}A^{-1}B^{-1}$.
   Aibių G_1 ir G_2 elementai komutuoja, taigi komutuoja ir atitinkamos matricos A ir B, todėl $K_A = K_B$.

3. Braid grupė ir jos įvaizdžiai

Tarkime, kad turime n sruogų r_i, tuomet elementai



σ_i, $i = 1, 2, ..., n-1$ apibrėžia Braid grupę [3].

$$Br_n = \{\sigma_1, \sigma_2, \ldots, \sigma_{n-1}\colon\ \sigma_i\sigma_{i+1}\sigma_i = \sigma_{i+1}\sigma_i\sigma_{i+1},\ i = \overline{1, n-2};$$
$$\sigma_i\sigma_j = \sigma_j\sigma_i\ \ |i-j| \geqslant 2\ \ i, j = \overline{1, n-1}\}.$$

Pasirodo, kad žodžiai

$$d = \sigma_1 \cdot \sigma_2 \cdot \ldots \cdot \sigma_{n-1},$$
$$\overline{d} = \sigma_{n-1} \cdot \sigma_{n-2} \cdot \ldots \cdot \sigma_1,$$
$$\Delta = \sigma_1(\sigma_2\sigma_1)(\sigma_3\sigma_2\sigma_1) \cdot \ldots \cdot (\sigma_{n-1}\sigma_{n-2} \cdot \ldots \cdot \sigma_1)$$

pasižymi tuo, kad $d, \overline{d}, \Delta, \overline{\Delta}$ tenkina šias tapatybes [4]

$$d\sigma_i = \sigma_{i+1}d, \quad i = \overline{1, n-2},$$
$$\overline{d}\sigma_i = \sigma_{i-1}\overline{d}, \quad i = \overline{1, n-1},$$
$$\Delta = \overline{\Delta} = (\sigma_1 \cdot \sigma_2 \cdot \ldots \cdot \sigma_{n-1}) \ldots (\sigma_1\sigma_2)\sigma_1,$$
$$\Delta\sigma_i = \sigma_{n-i}\Delta, \quad i = \overline{1, n-1}.$$

Tada $\Delta^2\sigma_i = \Delta(\Delta\sigma_i) = \Delta(\sigma_{n-i} \cdot \Delta) = (\Delta\sigma_{n-i})\Delta = \sigma_i\Delta^2$, $\forall i = \overline{1, n-1}$, taigi Δ^2 yra Braid grupės centras.

Burau homomorfizmo pagalba [4] Braid grupė gali būti atvaizduota į $M_n(Z[t, t^{-1}])$, čia $Z[t, t^{-1}]$ yra polinomų virš žiedo Z nuo kintamųjų t ir t^{-1} aibė.

$$\varphi\colon\ \sigma_i \to E_{i-1} \oplus \begin{pmatrix} 1-t & t \\ 1 & 0 \end{pmatrix} \oplus E_{n-i-1}$$

$$= \left(\begin{array}{c|ccc|c} E_{i-1} & 0 & 0 & 0 \\ \hline 0 & 1-t & t & 0 \\ 0 & 1 & 0 & 0 \\ \hline 0 & 0 & 0 & E_{n-i-1} \end{array}\right), \quad i = \overline{1, n-1},$$

E_i – i-tosios eilės vienetinė matrica, parametrui t parenkama konkreti reikšmė ($t \notin \{0, 1\}$).

Tai neredukuojamas Braid grupės įvaizdis. Egzistuoja redukuojamas Braid grupės Burau įvaizdis

$$\varphi*\colon \sigma_1 \to \begin{pmatrix} -t & 0 \\ -1 & 1 \end{pmatrix} \oplus E_{n-3},$$

$$\varphi*\colon \sigma_i \to E_{i-2} \oplus \begin{pmatrix} 1 & -t & 0 \\ 0 & -t & 0 \\ 0 & -1 & 1 \end{pmatrix} \oplus E_{n-i-2}, \quad i = \overline{2, n-2},$$

$$\varphi*\colon \sigma_{n-1} \to E_{n-3} \oplus \begin{pmatrix} 1 & -t \\ 0 & -t \end{pmatrix}.$$

4. Raktų apsikeitimo protokolo taikymas, naudojant Braid grupės įvaizdį

Pasirinkus grupę $G = Br_{2n}$,

$$G_1 = \{\sigma_i\colon i \leqslant n-1\} \subset G,$$
$$G_2 = \{\sigma_i\colon i \geqslant n+1\} \subset G,$$

galime taikyti pasiūlytą raktų apsikeitimo protokolą.

I atvejis

Atsižvelgus į matricų A ir B blokinę struktūrą

$$A_{2n\times 2n} = \begin{pmatrix} A^*_{n\times n} & 0_{n\times n} \\ 0_{n\times n} & E_{n\times n} \end{pmatrix},$$

$$B_{2n\times 2n} = \begin{pmatrix} E & 0 \\ 0 & B^* \end{pmatrix},$$

atakos iš „Broniaus“ pusės atveju, gali pasirodyti, kad protokolo saugumas remiasi tik matricinio logaritmo problema, nes

$$AQ^rA^{-1} = \begin{pmatrix} A & 0 \\ 0 & E \end{pmatrix}\begin{pmatrix} Q_1 & Q_2 \\ Q_3 & Q_4 \end{pmatrix}\begin{pmatrix} A^{-1} & 0 \\ 0 & E \end{pmatrix} = \begin{pmatrix} AQ_1A^{-1} & AQ_2 \\ Q_3A^{-1} & Q_4 \end{pmatrix}.$$

Tačiau, keldami matricą $Q = \begin{pmatrix} M_1 & N_1 \\ C_1 & D_1 \end{pmatrix}$ laipsniu, gauname

$$Q^{i+j} = Q^i \cdot Q^j = \begin{pmatrix} M_i & N_i \\ C_i & D_i \end{pmatrix} \cdot \begin{pmatrix} M_j & N_j \\ C_j & D_j \end{pmatrix}$$

$$= \begin{pmatrix} M_i M_j + N_i C_j & M_i N_j + N_i D_j \\ C_i M_j + D_i C_j & C_i N_j + D_i D_j \end{pmatrix} = \begin{pmatrix} M_{i+j} & N_{i+j} \\ C_{i+j} & D_{i+j} \end{pmatrix}.$$

Mažiausiai apsaugotas blokas Q_4 su pradinės matricos Q laipsniais susijęs rekurentine priklausomybe

$$D_{i+j} = C_i \cdot N_j + D_i \cdot D_j \text{ ir t.t.}$$

Taigi, norint nustatyti r, tiesiogiai pasinaudoti matricine diskrečiojo logaritmo problema negalima. Išsprendus šią problemą ir radus r dar tektų spręsti matricinę lygtį

$$XQ^rX^{-1} = B^* \Leftrightarrow XQ^r = BX.$$

Šiuo atveju ataką galima išskaidyti į du uždavinius:

1. Rasti r: $Q^r = \begin{pmatrix} M_1 & N_1 \\ C_1 & D_1 \end{pmatrix}^r = \begin{pmatrix} Q_1 & Q_2 \\ Q_3 & Q_4 \end{pmatrix}$.
2. Rasti X: $XQ^r = BX$.

II atvejis

Norėdami užtikrinti papildomą saugumo laipsnį imame

$$\alpha = \sigma_{i_1}^{k_1} \cdot \sigma_{i_2}^{k_2} \cdot \ldots \cdot \sigma_{i_{n_1}}^{k_{n_1}} \cdot \Delta^{2k} \xrightarrow{\phi} X^* = A^* C_A,$$

čia $\sigma_{i_p} \in G_1, k, k_p \in N$,

$$\beta = \sigma_{j_1}^{l_1} \cdot \sigma_{j_2}^{l_2} \cdot \ldots \cdot \sigma_{j_{n_2}}^{l_{n_2}} \cdot \Delta^{2l} \xrightarrow{\phi} Y^* = B^* C_B,$$

čia $\sigma_{j_q} \in G_2, l, l_q \in N$.

Tuomet, pavyzdžiui, žinant

$$X^* Q^r (X^*)^{-1} = \begin{pmatrix} A & 0 \\ 0 & E \end{pmatrix} \begin{pmatrix} U & V \\ Z & X \end{pmatrix} \begin{pmatrix} Q_1 & Q_2 \\ Q_3 & Q_4 \end{pmatrix} \begin{pmatrix} U' & V' \\ Z' & X' \end{pmatrix} \begin{pmatrix} A^{-1} & 0 \\ 0 & E \end{pmatrix}$$

$$= \begin{pmatrix} ((AUQ_1+AVQ_3)U'+(AUQ_2+AVQ_4)Z')A^{-1} & (AUQ_1+AVQ_3)V'+(AUQ_2+AVQ_4)X' \\ ((ZQ_1+XQ_3)U'+(ZQ_2+XQ_4)Z')A^{-1} & (ZQ_1+XQ_3)V'+(ZQ_2+XQ_4)X' \end{pmatrix}$$

matome, kad netgi „mažiausiai“ apsaugotas elementas turi išraišką

$$(ZQ_1 + XQ_3)V' + (ZQ_2 + XQ_4)X'.$$

Taigi, šiuo atveju protokolo saugumas grindžiamas matricine lygtimi $XQ^r = B \cdot X$, kai X – nežinoma matrica, r – nežinomas natūralusis skaičius ir šių dviejų uždavinių atskirti negalima.

5. Išvados

1. Siūlomo protokolo atsparumo laipsnį atakoms užtikrina su šiuo protokolu susijusios kartu sprendžiamos dvi problemos: matricinio diskretinio logaritmo problema ir matricinės lygties $XQ^r = B^*X$ sprendinio suradimo problema, kurių negalima atskirti.

2. Nežinomi polinominio laiko funkcijos algoritmai, leidžiantys spręsti matricinę diskretinio logaritmo problemą, nors ir egzistuoja polinominiai algoritmai matricinei lygčiai spręsti, sprendžiant šias problemas kartu tenka naudotis perrinkimo metodu, kurio laiko funkcija yra eksponentinė, todėl šių problemų pagrindu sudaryta funkcija pasižymi vienkryptiškumo savybe.

Literatūra

1. A. Matuliauskas, *Algebra*, Mokslas, Vilnius (1985).
2. E. Sakalauskas, P. Tvarijonas, A. Raulynaitis, Key agreement protocol (KAP) using conjugacy and discrete logarithm problems in group representation level, *Informatica*, **18**(1), 115–124 (2007).
3. I.S. Birman, Braids, links and mapping class groups, *Annals of Mathematic Studies*, **82**, Princeton University Press (1974).
4. G. Dietz, The Braid group representation on intersection, in: *Matrices and Monodromy of Singularities*, Universitat Munster (2005), `http://www.gdietz.de`.

SUMMARY

P. Tvarijonas, E. Sakalauskas, G.S. Dosinas. Key agreement protocol in Braid group representation level

In this paper the key agreement protocol is given and the application of it in Braid groups is suggested. The one way of protocol is being justified.

Keywords: key agreement protocol, Braid groups.