Liet. matem. rink., **47**, *spec. nr.*, 2007, 168–172

Rakto apsikeitimo protokolas begalinės pusgrupės įvaizdžio lygmenyje

Artūras KATVICKIS, Eligijus SAKALAUSKAS,
Kastytis RATKEVIČIUS (KTU)
el. paštas: arturas.katvickis@ktu.lt, eligijus.sakalauskas@ktu.lt, kastytis.ratkevicius@ktu.lt

1. Įvadas

Raktų apsikeitimo protokolai, kaip ir šifravimas bei elektroninis parašas, yra vieni pagrindinių kriptografinių primityvų. Tokie protokolai leidžia dviems arba grupei asmenų apsikeisti informacija naudojantis viešais ir neapsaugotais kanalais, bei susitarti dėl bendro rakto, kuris būtų naudojamas tolimesniam kriptografiškai saugiam informacijos apsikeitimui.

Pirmas paskelbtas raktų apsikeitimo protokolas yra Diffie–Hellman protokolas [1], kuris sukėlė revoliucija šiuolaikinėje kriptografijoje ir pradėjo asimetrinės kriptografijos vystimosi erą. Diffie–Hellman protokolo pagrindu buvo sukurta daugybė raktų apsikeitimo protokolų, pridedant autentifikavimą. Tačiau vėliau daugelyje tokių protokolų buvo pastebėtos saugumo spragos.

1993 m. atsirado naujos idėjos viešo rakto kriptografijoje, kurių pagrindu buvo pristatytas raktų apsikeitimo protokolas begalinėse nekomutatyviose grupėse [2]. Pagrindinė idėja buvo panaudoti žinomas sunkias algoritmines problemas šiose grupėse, kuriant vienkryptes funkcijas. Viena tokių problemų yra jungtinuko suradimo problema.

Paskelbtos idėjos buvo apibendrintos [3] ir realizuotos Braid grupėse – [4] paskelbtas raktų apsikeitimo protokolas, panaudojant jungtinuko suradimo problemą grupės raiškos lygmenyje (presentation level).

2004 metais pradėta abejoti ar jungtinuko suradimo problema Braid grupėse užtikrina pakankama saugumo lygį [5] ir plačiau pradėtos nagrinėti kitos sunkios algoritminės problemos įvairiose algebrinėse struktūrose. Buvo paskelbtas porinimu pagrįstas raktų apsikeitimo protokolas [7], triguba dekompozicijos problema pagrįstas protokolas [8], priklausomybės pogrupiui problema pagrįstas protokolas [6]. Taip pat buvo pasiūlytos sistemos realizuotos sudėtingesnėse algebrinėse struktūrose [9] ir algoritmai, pagrįsti keliomis sunkiomis algoritminėmis problemomis vienu metu [10].

Nagrinėjamu atveju, rakto apsikeitimo protokolas yra paremtas sunkia algoritmine problema, suformuluota begalinės nekomutatyvios pusgrupės įvaizdžio lygmenyje (representation level).

2. Matematiniai pagrindai

Braid grupė yra begalinė nekomutatyvi grupė, kurios raiškos lygmuo nusakomas tokiais generatoriais ir ryšiais tarp jų [4]:

$$B_n = \langle\, \delta_1, \delta_2, \ldots, \delta_{n-1} |\, \delta_i \delta_j = \delta_j \delta_i \;\; (|i-j| \geq 2)\,,$$
$$\delta_i \delta_{i+1} \delta_i = \delta_{i+1} \delta_i \delta_{i+1} \;\; (i = 1, \cdots, n-2) \,\rangle.$$

Viena svarbių Braid grupės savybių yra fundamentalaus ir centro elementų egzistavimas. Fundamentalus Braid grupės elementas $\Delta = \delta_1 \delta_2 \cdots \delta_n \delta_1 \cdots \delta_{n-1} \cdots \delta_1 \delta_2 \delta_1$, o centras yra Δ^2[11]. Fundamentalus elementas pasižymi „skvarbos“ savybe, t.y. tenkinama lygybė $\delta_i \Delta = \Delta \delta_{n-i}$, o centras yra komutatyvus su bet kurio grupės elementu.

Egzistuoja keli Braid grupių homomorfiniai įvaizdžiai vektorinėse erdvėse. Vienas tokių yra Burau įvaizdis, kuris nusakomas homomorfizmu φ: $B_n \to GL(n, Z[t])$:

$$\delta_i \to \begin{pmatrix} I_{i-1} & 0 & 0 & 0 \\ 0 & 1-t & t & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & I_{n-i-1} \end{pmatrix},$$

čia I_n yra n-tos eilės vienetinė matrica, $Z[t]$ yra daugianarių žiedas su kintamuoju t virš sveikųjų skaičių žiedo Z.

Šiame darbe nagrinėjama ne Braid grupė, o Braid monoidas, sudarytas iš visų teigiamų Braid grupės žodžių, t.y. elementų kuriose nėra generatorių neigiamais laipsniais, kurį žymėsime B_n^+ .

Matricų dekompozicijos problema.

Uždavinio formulavimas: duotos dvi n-tos eilės kvadratinės matricos A ir B virš sveikųjų skaičių žiedo. Reikia rasti tokias dvi matricas X ir Y virš sveikųjų skaičių žiedo, kad galiotų lygybė $XAY = B$.

Pasirenkama tokia sprendinio ieškojimo metodika:

1) parenkama matrica virš sveikų skaičių žiedo $Y = Y_0$;

2) apskaičiuojama matrica $Z = AY_0$;

3) sprendžiama matricinė lygtis $XZ = B$.

Ieškant sprendinio yra iškyla dvi problemos:

1) Kaip parinkti Y_0? Laisvai pasirenkant matricą Y_0, nėra užtikrinamas sprendinio egzistavimas nagrinėjamame žiede. Suformuluoti kokius nors reikalavimus ar bent jau rekomendacijas, užtikrinančias sprendinio virš sveikų skaičių žiedo egzistavimą, matricos Y_0 parinkimui bendru atveju yra neįmanoma. Todėl lieka tik atsitiktinis sveikų skaičių matricos generavimas, tikintis palankaus scenarijaus.

2) Kaip išspręsti lygtį $XZ = B$? Nagrinėjamame žiede matricos neturi atvirkštinių elementų. Iš kitos pusės, skaitmeniniai tiesinių lygčių sprendimo metodai taip pat netinka, nes jų pagalba gaunami sprendiniai nėra sveikaskaitiniai.

Tokiu būdu suformuluotas uždavinys turi kriptografijoje naudojamų vienkrypčių funkcijų (VKF) požymius.

3. Rakto apsikeitimo protokolas

Naudojantis aukščiau išvardintomis sąvokomis bei gautais rezultatais galime sukonstruoti rakto apsikeitimo protokolą tarp dviejų kriptografinių subjektų $\boldsymbol{A}$ ir $\boldsymbol{B}$.

Sistemos viešasis parametras yra n-tos eilės matrica M virš sveikųjų skaičių žiedo.

Slaptieji subjektų parametrai yra: subjektui $\boldsymbol{A}$ – n-tos eilės matricos X ir Y; subjektui $\boldsymbol{B}$ – matricos U ir V. Šie slaptieji parametrai turi tenkinti komutatyvumo savybę, t.y. $XU = UX$ ir $YV = VY$.

Rakto apsikeitimas vykdomas tokiais žingsniais:

1) Subjektas $\boldsymbol{A}$ apskaičiuoja $A = XMY$ ir gautą rezultatą siunčia subjektui $\boldsymbol{B}$, o subjektas $\boldsymbol{B}$ apskaičiuoja $B = UMV$ ir gautą rezultatą siunčia subjektui $\boldsymbol{A}$.

2) Pasinaudoję gautais pranešimais subjektai apskaičiuoja bendrąjį slaptąjį raktą K. Subjektas $\boldsymbol{A}$ gauna $K_A = XUMVY$, subjektas $\boldsymbol{B}$ – $K_B = UXMYV$. Gauti subjektų raktai sutampa dėl iškeltų reikalavimų slaptiesiems raktams (atitinkamų matricų komutatyvumas), t.y. $K_A = K_B = K$.

Užtikrinant šio algoritmo funkcionalumą, siūlomas toks vartotojų slaptųjų raktų generavimo mechanizmas:

1) Braid monoide B_n^+ išskiriamos dvi struktūros B_l^+ ir B_r^+ , tokios kad bet kuris elementas iš B_l^+ komutuotų su bet kurio elementu iš B_r^+, t.y. $\forall a \in B_l^+,\ \forall b \in B_r^+$: $ab = ba$.

2) Subjektas $\boldsymbol{A}$ atsitiktinai parenka (sugeneruoja) elementus $x \in B_l^+$ ir $y \in B_r^+$ bei suranda jų įvaizdžius vektorinėje erdvėje, t.y. matricas X ir Y, naudojant Burau atvaizdavimą.

3) Subjektas $\boldsymbol{B}$ atsitiktinai parenka (sugeneruoja) elementus $u \in B_r^+$ ir $v \in B_l^+$ bei suranda jų įvaizdžius vektorinėje erdvėje, t.y. matricas U ir V, naudojant Burau atvaizdavimą.

Toks slaptųjų parametrų pasirinkimas užtikrina iškeltą komutatyvumo sąlygą.

4. Kriptografinio saugumo analizė

Pateikto rakto apsikeitimo protokolo saugumas pagrįstas matricų dekompozicijos problema – sistemos viešasis parametras yra matrica M, o neapsaugotais ryšio kanalais perduodamas dydis yra pavidalu $A = XMY$. Taigi, jei potencialus kenkėjas, žinodamas A ir M, galėtų lengvai gauti X ir Y, tuomet rakto apsikeitimo protokolas būtų pažeidžiamas. Nes matricos X ir Y yra vartotojo slaptasis raktas, kuris negali būti žinomas kitiems asmenims.

Nagrinėkime bendros matricinės lygties $AX = B$ sprendimą virš sveikųjų skaičių žiedo. Šią lygtį sprendžiame naudojantis Gauso eliminavimo schema. Tam kad gauti sveikaskaitinį sprendinį neatliekamos jokios dalybos operacijos. Dėl šios priežasties atlikus Gauso eliminavimo schema labai išauga matricų elementų eilė. Gaunamų elementų eilę galima sumažinti atliekant prastinimo veiksmus, t.y. kiekviename Gauso metodo žingsnyje kiekviena eilutę padalinti iš visų eilutės elementų bendro didžiausio daliklio. Atliekant tokį veiksmą bus užtikrintas tarpinių rezultatų sveikaskaitinės reikšmės ir galima tikėtis ženkliai sumažinti elementų eilę. Tačiau tikimybė kad n sveikų skaičių turės nevienetinį bendrą didžiausią daliklį

yra $P(BDD(m_1, m_2, \ldots, m_n) \neq 1) \approx 1 - \zeta^{-1}(n)$, čia $\zeta(n) = \sum_{k \geq 1} \frac{1}{k^n}$ Rymano ζ-funkcija. Ši tikimybė sparčiai artėja prie nulio didėjant n, todėl visos eilutės prastinimo galimybė atmetama, kaip praktiškai neįmanoma.

Nagrinėkime vieną Gauso algoritmo žingsnį. Kad užtikrinti matricų elementų priklausymą sveikųjų skaičių žiedui, veiksmai atliekami tokiu būdu:

$$\begin{pmatrix} a_{11}\, a_{12}\, a_{13} \ldots \\ a_{21}\, a_{22}\, a_{23} \ldots \\ \ldots\ \ldots\ \ldots\ \ldots \end{pmatrix} \to \begin{pmatrix} a_{11} & a_{12} & a_{13} & \ldots \\ 0 & a_{22}a_{11} - a_{12}a_{21} & a_{23}a_{11} - a_{13}a_{21} & \ldots \\ \ldots & \ldots & \ldots & \ldots \end{pmatrix}.$$

Pastebėkime, kad jeigu pradinės matricos elementų eilė buvo a, tai po pertvarkymo didžiausio elemento eilė bus a^2. Be to, jeigu $BDD(a_{11}, a_{21}) \neq 1$, tai rezultatų eilutėje visi elementai bus kartotiniai $BDD(a_{11}, a_{21})$. Bendro didžiausio daliklio vidurkį pažymėkime $\mathrm{E}(BDD(a_{11}, a_{21})) = \gamma$, tuomet, atlikus Gauso eliminavimo schema, didžiausias elementas turės būti $\frac{a^{2^n}}{\gamma^{2^n-1}}$ eilės.

Apytiksliai vertinant dydį γ, nagrinėkime tikimybes $\mathrm{P}(BDD(a, b) = d)$, kur $d = 1, 2, 3, ..., 10$ ir $\mathrm{P}(BDD(a, b) > 10)$. Apskaičiavę gauto skirstinio vidurkį, turėsime dydžio γ artinį.

Pritaikius šią metodiką gauname $\gamma \approx 4$ ir matricos didžiausias elementas, atlikus Gauso eliminavimo schemą, būtų $\frac{a^{2^n}}{4^{2^n-1}}$ eilės. T.y. Jei pradinės matricos elemento saugojimui kompiuterio atmintyje skiriama k bitų, tai galimas matricos didžiausias elementas, atlikus Gauso eliminavimo schemą, būtų $\frac{(2^k)^{2^n}}{4^{2^n-1}} = 2^{k2^n - 2\cdot 2^n + 2} = 2^{2+(k-2)2^n}$ ir šio elemento saugojimui kompiuterio atmintyje turėtų būti skirta $2 + (k-2) \cdot 2^n$ bitų.

5. Išvados

1. Nagrinėjamas uždavinys yra eksponentinio sudėtingumo uždavinys naudojamų atminties resursų atžvilgiu. Be to, vertinant šio uždavinio sudėtingumą buvo nagrinėjama tik lygtis $AX = B$, o į matricos Y_0 pasirinkimą nebuvo atsižvelgta. Tačiau Y_0 pasirenkamas atsitiktiniai, t.y. šios matricos parinkimas yra perrinkimo uždavinys aibėje turinčioje $n^2 2^b$ elementų (čia n – matricos eilė, b – bitų skaičius, skirtas vienam matricos elementui saugoti).
2. Darbe pristatytas rakto apsikeitimo protokolas, paremtas matricų dekompozicijos problema.

Literatūra

1. W. Diffe, M. Hellman, New directions in cryptography, in: *IEEE Transaction on Information Theory*, IT-22, **6**, 644–654 (1976).
2. V. Sidelnikov, M. Cherepnev, V. Yaschenko, Systems of open distribution of keys on the basis of non-commutative semigroups, . *Russian Acad. Sci. Dokl. Math.*, **48**(2), 566–567 (1993).
3. I. Anshel, M. Anshel, D. Goldfeld, An algebraic method for public key cryptography, *Mathematical Research Letters*, **6**, 1–5 (1999).
4. K.H. Ko, S.J. Lee, J.H. Cheon, J.W. Han, J.S. Kang, C. Park, New public key cryptosystem using Braid groups, *Advances in Cryptology, Proc. Crypto 2000*, LNCS **1880**, Springer-Verlag, 166–183 (2000).
5. V. Shpilrain, G. Zapata, *Combinatorial Group Theory and Public Key Cryptography* (2004). `http://www.iacr.org`

6. V. Shpilrain, G. Zapata, *Using The Subgroup Membership Search Problem In Public Key Cryptography* (2004). http://www.iacr.org
7. R. Lu, Z. Cao, R. Su, J. Shao, *Pairing-Based Two-Party Authenticated Key Agreement Protocol* (2005). http://www.iacr.org
8. Y. Kurt, *A New Key Exchange Primitive Based on the Triple Decomposition Problem* (2006). http://www.iacr.org
9. E. Sakalauskas, One digital signature scheme in semimodule over semiring, *Informatica*, **16**(3), 383–394 (2005).
10. E. Sakalauskas, P. Tvarijonas, A. Raulynaitis, Key agreement protocol using conjugacy and discrete logarithm problems in group representation level, *Informatica*, **18**(1), 115–124 (2007).
11. J. Gonzalez–Meneses, B. Wiest, *On the Structure of the Centralizer of a Braid*. http://www.arxiv.org/PS_cache/math/pdf/0305/0305156v2.pdf

SUMMARY

A. Katvickis, E. Sakalauskas, K. Ratkevičius. Key agreement protocol in infinite semigroup representation level

Matrix decomposition problem over integer ring is presented. Solving methods are discussed and it is showed, that this problem is hard computational problem regard to computer memory resources**.** A key agreement protocol based on matrix decomposition problem is presented.

Keywords: key agreement protocol, representation level, Braid group.