Problematika využití neasociativních algebraických struktur pro kryptografické účely

Eliška Ochodková

Katedra informatiky, FEI, VŠB - Technická Univerzita Ostrava,
17. listopadu 15, 708 33, Ostrava-Poruba
eliska.ochodkova@vsb.cz

Abstrakt. V tomto článku uvádím jednu z možností využití neasociativní algebraické struktury kvazigrupa v kryptografii. Je zde prezentován algoritmus pro generování velkých kvazigrup a jejich použití pro konstrukci hashovací funkce. Na konci článku je uveden seznam publikací týkajících se této problematiky, ale jiných oblastí, jimiž se autorka zabývá.

Klíčová slova: kvazigrupa, kryptografická hashovací funkce, Latinský čtverec

1 Úvod

Jednou z oblastí, kterou se zabývám, je kryptografie a problematika využití neasociativních algebraických struktur pro kryptografické účely. Zajímavými algebraickými strukturami jsou tzv. kvazigrupa a neofield, jejichž vlastnosti jsou takové, že se tyto struktury jeví být v kryptografii použitelné. Blíže jsem se, spolu s kolegy, zatím zabývala kvazigrupami, jejich využitím v šifrovacích algoritmech (viz např. [3]) a kryptografických hashovacích funkcích (viz např. [6]). Stručné přiblížení problematiky obsahují další kapitoly.

Kvazigrupy jsou ekvivalentní známějším Latinským čtvercům. Tabulka násobení nad kvazigrupou řádu n je Latinský čtverec (dále LS) řádu n a naopak, každý LS řádu n je tabulkou násobení pro kvazigrupu řádu n.

Kryptografie se zabývá transformací otevřeného textu na šifrový text prostřednictvím šifrování a transformací šifrového textu na otevřený text prostřednictvím dešifrování. Ideální kryptosystémy podporují tři nejdůležitější bezpečnostní funkce, a to utajení, autentizaci, integritu, a popřípadě nepopiratelnost.

Existují dva typy šifrovacích algoritmů:

1. algoritmy, které používají dvojici klíčů, veřejný a soukromý klíč - asymetrické algoritmy (např. RSA, ElGamal),
2. algoritmy, které používají tajný klíč - symetrické algoritmy (např. AES, DES).

Hashovací funkce jsou matematické funkce, které se v informačních technologiích používají velice často, jsou to funkce, které mapují vstup proměnné délky na

výstup pevné délky. Jako příklad lze uvést databázové zpracování, kdy technika hashování umožňuje na základě hodnoty vyhledávacího klíče určit umístění odpovídajícího záznamu. Kryptografické hashovací funkce jsou důležitými nástroji pro kryptografické aplikace jakými jsou například digitální podpis, klíčované hashovací funkce (MAC - Message Authentication Code).

2 Hashovací funkce založená na kvazigrupě

2.1 Kryptografické hashovací funkce

Kryptografické hashovací funkce jsou většinou iterační procesy, které hashují vstup proměnné délky (t-bitové bloky) na výstup pevné délky (r-bitové bloky). Vstup M je nejprve zarovnán na násobek délky bloku a poté je rozdělen na t-bitové bloky M_i. Hashovací funkce H může být popsána takto:

$$MD_0 = IV, MD_i = f(MD_{i-1}, M_i), 1 \leq i \leq n, H(M) = MD_n,$$

kde IV je inicializační hodnota, f je kompresní funkce, MD_i jsou r-bitové buffery.

Důležitou vlastností kryptografických hashovacích funkcí je to, že jsou to funkce jednocestné a odolné proti kolizím. Tyto vlastnosti musí každá hashovací funkce mít, aby byla použitelná právě pro kryptografické účely.

Definice 1. *Funkce $H()$ se nazývá jednocestnou hashovací funkcí (JHF), jestliže splňuje následující vlastnosti:*

1. *argument (zpráva) M může mít libovolnou délku,*
2. *výsledek $H(M)$ má pevnou délku (charakteristika),*
3. *funkci $H(M)$ lze relativně snadno realizovat jak hardwarově, tak softwarově,*
4. *funkce $H(M)$ je jednocestná, tj. pro daný vstup M a danou funkci H je snadné vypočítat $H(M)$, ale pro danou $H(M)$ je nesnadné vypočítat M.*

Definice 2. *Jednocestná hashovací funkce $H()$ se nazývá jednocestnou hashovací funkcí odolnou kolizím (JHFOK), jestliže splňuje následující vlastnosti:*

1. *funkce $H(M)$ je odolná proti kolizím, tj. pro daný vstup M a danou hodnotu $H(M)$ je těžké (nemožné) najít takové $M'(M \neq M')$, aby platilo $H(M) = H(M')$,*
2. *funkce $H(M)$ je silně odolná proti kolizím, je-li těžké (nemožné) najít jakýkoliv pár M, M' (pro $M \neq M'$) takový, aby platilo $H(M) = H(M')$.*

2.2 Kvazigrupa

Definice 3. *Grupoid $(Q, *)$ se nazývá kvazigrupou (algebrou s jednou binární operací), jestliže splňuje podmínku:*

$$(\forall u, v \in Q)(\exists! x, y \in Q)(u * x = v \wedge y * u = v).$$

Z toho vyplývá:

1. $x * y = x * z \vee y * x = z * x \Rightarrow y = z$,
2. rovnosti $a * x = b, y * a = b$ mají stejná řešení x, y pro každé $a, b \in Q$.

Definice 4. *Nechť $A = \{a_1, a_2, \ldots, a_n\}$ je abeceda. Latinský obdélník velikosti $k \times n$ je matice s prvky $a_{ij} \in A$, $i = 1, 2, \ldots, k$, $j = 1, 2, \ldots, n$, taková, že každý její prvek se nachází v každém řádku a každém sloupci právě jednou. Jestliže $k = n$ hovoříme o Latinském čtverci (LS).*

Říkáme, že Latinský čtverec je ve standardní formě (redukovaný), jestliže první řádek a nejlevější sloupec jsou určitým způsobem uspořádány, nejčastěji v alfabetickém pořadí.

Tabulka 1. Počet všech různých redukovaných Latinských čtverců řádu n pro $n \leq 10$.

n	L_n
1	1
2	1
3	1
4	4
5	56
6	9 408
7	16 942 080
8	535 281 401 856
9	377 597 570 964 258 816
10	7 580 721 483 160 132 811 489 280

Problém určení přesného počtu všech LS řádu $n > 10$ stále vyřešen není. Existuje však nejméně $n!(n-1)!...2!$ LS řádu n. Pokud $A = \{0, ..., 255\}$, potom existuje $256!255!...2! > 10^{58000}$ různých kvazigrup. Tento velký počet různých kvazigrup činí případnou hashovací funkci založenou na kvazigrupě odolnou proti útoku hrubou silou a proti narozeninovému útoku.

Velmi důležitá vlastnost násobení v kvazigrupách je následující: Je možno ukázat, že každý prvek kvazigrupy Q řádu n se vyskytuje právě n-krát mezi všemi dvouprvkovými součiny prvků z Q, n^2-krát mezi všemi tříprvkovými součiny prvků z Q atd. až n^{t-1}-krát mezi všemi t-prvkovými součiny prvků z Q. Existuje n^t možných uspořádaných součinů t prvků z Q, to znamená, že všechny prvky se vyskytují stejně často (se stejnou pravděpodobností) mezi těmito n^t součiny.

2.3 Konstrukce jednoduché hashovací funkce

Definice 5. *Zobrazení $H_Q : Q \to Q$ definované následujícím předpisem:*

$$H_Q(q_1 q_2 \ldots q_n) = ((\ldots(a * q_1) * q_2 * \ldots) * q_n)$$

se nazývá hashovací funkce nad kvazigrupou $(Q, *)$. *Prvek* a *je pevně zvolený prvek z kvazigrupy* $(Q, *)$.

Neformálně řečeno hodnotu hashovací funkce vypočteme tak, že vynásobíme postupně všechny znaky ze kterých se skládá slovo.

Příklad 1. Tabulka kvazigrupy modulárního odčítaní vypadá následovně:

0	3	2	1
1	0	3	2
2	1	0	3
3	2	1	0

To že tato tabulka definuje kvazigrupu je dáno tím, že splňuje podmínky pro Latinský čtverec, to znamená, že každý prvek se v řádku a sloupci vyskytuje právě jednou. Násobení v této kvazigrupě je definováno předpisem $a * b = (a + 4 - b) \bmod 4$. Je zřejmé, že tato kvazigrupa není komutativní $1 * 2 = 3, 2 * 1 = 1$. Neobsahuje jednotkový prvek a tudíž není ani asociativní. Kdyby byla asociativní musí obsahovat i jednotkový prvek, protože by byla grupou. Hodnota hashovací funkce $H_2(0013) = (((2 * 0) * 0) * 1) * 3 = 2$.

Příklad 2. Tabulka kvazigrupy homotopická s kvazigrupou modulárního odčítaní:

0	3	2	1
2	1	0	3
1	0	3	2
3	2	1	0

Tato tabulka vznikla prohozením druhého a třetího řádku v tabulce násobení kvazigrupy modulárního odčítaní. Permutace π, ρ jsou identity a $\omega = [0213]$. Například $1 * 0 = \omega(1) * 0 = 2 * 0 = 2$. Tento příklad je možno považovat za návod jak konstruovat nové kvazigrupy.

Definice 6. *Kvazigrupy* $(Q, *)$ *a* $(R, *)$ *nazveme homotopické, jestliže existují permutace takové, že platí :*

$$(\forall u, v \in R)(u * v = \pi(\omega(u) * \rho(v))).$$

Homotopii kvazigrup si můžeme snadno představit jako permutování sloupců a řádků tabulky násobení kvazigrupy.

Déle budeme používat kvazigrupy homotopické kvazigrupě modulárního odčítání. Tyto kvazigrupy můžeme generovat tak, že vygenerujeme tři náhodné permutace a pomocí těchto permutací upravíme tabulku násobení. Takto vzniklé kvazigrupě budeme říkat tabulková kvazigrupa. Nevýhodou tohoto postupu je velká paměťová náročnost. Je potřeba uložit n^2 prvků. Homotopie nám dává možnost výsledek násobení v kvazigrupě počítat analyticky a to tak, že zvolíme předpis pro výpočet permutací π, ρ, ω. Násobení v této kvazigrupě je definováno takto:

$$a * b = \pi((\omega(a) + n - \rho(b)) \bmod n).$$

Uvedený postup nám dává možnost pracovat s kvazigrupami velkých rozměrů. Hypotézy jsme o věřili experimentálně a výsledky experimentu jsou dostupné např. v [3]. Některé další kryptograficky důležité vlastnosti takto navržené hashovací funkce jsou ověřeny v [6].

3 Závěr

Použití neasociativních algebraických struktur pro kryptografii je široké. Tyto existují pro všechny řády, jejich implementace je snadná a mají další kryptograficky výhodné vlastnosti. Existuje celá řada publikací, které se zabývají využitím kvazigrup v kryptografii, ty však pracují s kvazigrupami malých řádů. My se ale zabýváme použitím kvazigrup velkých řádů a jejich realizací pomocí výpočetní metody nevyžadující žádnou pomocnou paměť. Pro velká čísla je potřeba pro výpočet hodnoty hashovací funkce používat aritmetiku pro práci s velkými čísly. Popis dalšího použití kvazigrup v kryptografii lze nalézt v [4].

V současnosti blíže zkoumám strukturu neofield, zatím jsem však žádné výsledky týkající se neofield nepublikovala. Dalším tématem, kterým se v současnosti zabývám je problematika bezpečnosti XML (viz [12]).

Reference

1. Černohorský J., Kovář P., Ochodková E., Hrudka G. Implementace grafově teoretických algoritmů v SW architektuře typu framework a jejich aplikace při návrhu řídicích systémů. *Moderní matematické metody v inženýrství, Ostrava, vol. 10, 37-41.* VŠB Technická universita Ostrava, 2001. ISBN 80-248-0013-6.
2. Černohorský J., Hrudka G., Kovář P., Ochodková E. Extensible Development Framework for Implementation of Graphically Expressed Design Tools. *PDS2001 IFAC WORKSHOP on Programmable Devices and Systems, 237-241.* Gliwice, 2001.
3. Ochodková E., Snášel V. Using Quasigroups for Secure Encoding of File System. *NATO PfP Conference Security and Protection of Information, p. 173-180.* Brno, 2001.
4. Ochodková E., Snášel V. Cryptographic Algorithms with Uniform Statistics. *NATO Regional Conference on Military Communications and Informations Systems, p. 165-172.* Zegrze, Poland, 2001.
5. Ochodková E., Dvorský J., Snášel V. Hashovací funkce založená na kvazigrupách. *Workshop Mikulášská kryptobesídka.* Praha, 2001. ISBN 80-903083-0-9.
6. Ochodková E., Dvorský J., Snášel V. Hash function based on large quasigroups, continuation. *Workshop Velikonoční kryptologie 2002.* Brno, 2002. ISBN 80-903083-1-7.
7. Ochodková E. Podpora výuky grafově orientovaných předmětů na Internetu. *Information and Communication Technology in Education.* Rožnov p. R., 2002. ISBN 80-7042-828-7.
8. Ochodková E., Dvorský J., Snášel V. Generation of large quasigroups: An application in cryptography. *Arbeitstagung Allgemeine Algebra-Workshop on General Algebra.* Olomouc, 2002.

9. Snášel V., Ochodková E., Dvorský J. Využití neasociativních algebraických struktur v kryptografii. *Kybernetika - história, perspektívy, teória a prax.* Žilina, 2002. ISBN 80-967609-7-1.
10. Černohorský J., Ochodková E., Hrudka G. The Experimental Extensible Framework for Support of Control System Development. *Sborník vědeckých prací VŠB-TUO, p. 21-28.* VŠB - TUO, 2003.
11. Šeptáková E., Snášel V., Ochodková E. Vyhledávání na základě podobnosti v XML dokumentech. *Znalosti 2003, p. 368-373.* Ostrava, 2003. ISBN 80-248-0229-5.
12. Ochodková E.: Introduction to Security Assertion Markup Language. *NATO Regional Conference on Military Communications and Informations Systems.* Zegrze, Poland, 2003.

Anotation. This paper covers possibilities of quasigroup usage for cryptographic purposes. An algorithm for large quasigroup generation and its usage for hash function generation is presented here. The list of publications that are concerned with non-associative algebraic structures and its usage in cryptography is mentioned at the end of this article.