VEDECKÁ RADA FAKULTY ELEKTROTECHNIKY
A INFORMATIKY SLOVENSKEJ TECHNICKEJ
UNIVERZITY V BRATISLAVE

Milan Vojvoda

Autoreferát dizertačnej práce

PRÚDOVÉ ŠIFRÁTORY A HAŠOVACIE FUNKCIE – ANALÝZA NIEKTORÝCH NOVÝCH NÁVRHOV

na získanie vedecko-akademickej hodnosti philosophiae doctor
v odbore doktorandského štúdia:

11-14-9 Aplikovaná matematika

Bratislava, Júl 2004

Dizertačná práca bola vypracovaná v externej forme doktorandského štúdia na Katedre matematiky Fakulty elektrotechniky a informatiky Slovenskej technickej univerzity v Bratislave.

Predkladateľ: Ing. Milan Vojvoda
Katedra matematiky STU FEI
Ilkovičova 3, 812 19 Bratislava 1

Školiteľ: Prof. RNDr. Otokar Grošek, PhD.
Katedra aplikovanej informatiky STU FEI
Ilkovičova 3, 812 19 Bratislava 1

Oponenti: Prof. RNDr. Štefan Porubský, DrSc.
Ústav informatiky, Akademie věd České republiky
Pod Vodárenskou věží 2
182 07 Praha 8 - Libeň, Česká republika

RNDr. Karol Nemoga, PhD.
Matematický ústav SAV
Štefánikova 49, 814 73 Bratislava

Doc. RNDr. Karol Macák, PhD.
Národný bezpečnostný úrad SR
Budatínska 30, 850 07 Bratislava 57

Autoreferát bol rozoslaný dňa .....

Obhajoba dizertačnej práce sa koná dňa ..... o ..... hod. pred komisiou pre obhajobu dizertačnej práce v odbore doktorandského štúdia, vymenovanou predsedom spoločnej odborovej komisie .....
11-14-9 Aplikovaná matematika
na .....

Predseda spoločnej odborovej komisie:
Prof. RNDr. Zdenka Riečanová, PhD.
Katedra matematiky STU FEI
Ilkovičova 3, 812 19 Bratislava 1

1 Úvod

Kryptografia je dnes neoddeliteľnou súčasťou našich každodenných aktivít, aj keď si to možno vôbec neuvedomujeme. Medzi najznámejšie aplikácie kryptografických techník patria Internet, bankové prevody, mobilné telefóny, a i. Hlavnými cieľmi kryptografie sú: zabezpečenie privátnosti, integrity údajov, autenticity a nepopierateľnosti [36].

V dizertačnej práci sa zaoberáme prúdovými šifrátormi a hašovacími funkciami, t.j. algoritmami na zabezpečenie privátnosti a integrity.

Prúdové šifry sú obľúbené pre svoju vysokú rýchlosť a zvyčajne jednoduché a lacné hardvérové riešenie. Jadrom prúdových šifier sú generátory (pseudo)náhodných postupností. Skutočne náhodné postupnosti sú zvyčajne získavané z fyzikálnych procesov. Tie sú však pomalé a generovanie je nereprodukovateľné, čo je nevýhodou pre určité aplikácie. Tieto dôvody viedli k intenzívnemu výskumu v oblasti pseudonáhodných postupností. Tie, napriek svojmu deterministickému vytvoreniu, vykazujú znaky typické pre náhodné postuposti a môžu byť veľmi rýchlo i efektívne vytvárané. Navyše sú reprodukovateľné, pokiaľ sú známe niektoré počiatočné hodnoty.

Úlohou hašovacích funkcií je vytvoriť digitálny odtlačok (bitový reťazec fixnej dĺžky) z ľubovoľnej správy (bitový reťazec ľubovoľnej dĺžky). Tento digitálny odtlačok potom danú správu "jednoznačne" reprezentuje. (Analogickým príkladom je odtlačok prsta u ľudí.) S hašovacími funkciami sa možno stretnúť v informatike (optimalizovaný prístup k uloženým údajom) a prirodzene aj v kryptografii (ochrana integrity údajov, digitálne podpisové schémy).

2 Súčasný stav problematiky

Prúdové šifrátory tvoria významnú časť symetrických kryptosystémov. Jednotlivé symboly (znaky, bity) otvoreného textu šifrujú v čase meniacou sa transformáciu.

Významnou schémou je tzv. binárny aditívny prúdový šifrátor.

Definícia 1 *Nech* $P = (p_0, p_1, \ldots, p_{N-1})$ *je otvorený text,* $C = (c_0, c_1, \ldots, c_{N-1})$ *zašifrovaný text a* $z = (z_0, z_1, \ldots, z_{N-1})$ *prúdový kľúč. Binárny aditívny prúdový šifrátor je synchrónny prúdový šifrátor, ktorého šifrovacia transformácia je daná vzťahom* $c_i = p_i \oplus z_i, \quad i = 0, 1, \ldots, N-1$. *Znak* $\oplus$ *značí sčítanie modulo 2. Dešifrovacia transformácia je potom:* $p_i = c_i \oplus z_i, \quad i = 0, 1, \ldots, N-1$.

Jadrom binárneho aditívneho prúdového šifrátora je generátor (pseudo)náhodnej postupnosti – prúdového kľúča. Takýto generátor musí vytvárať postupnosti s veľkou periódou, veľkou lineárnou zložitosťou a s dobrými štatistickými vlastnosťami.

V minulosti boli skúmané viaceré generátory založené na rôznych modifikáciách lineárneho kongruenčného generátora. Tieto návrhy však boli úspešne narušené [29], [30], [31]. Ako ďalšie boli skúmané lineárne spätnoväzobné registre (LFSR), resp. lineárne rekurentné postupnosti. Pri vhodnom návrhu LFSR možno vytvoriť postupnosti s veľkou periódou a dobrými štatistickými vlastnosťami, avšak s malou lineárnou zložitosťou, čo umožňuje útok [34]. Samotný LFSR je preto nevhodný ako generátor, ale je bežne používaným stavebným blokom komplikovanejších generátorov. Tie sú často založené na použití viacerých LFSR, ktorých výstupy sú vstupmi vhodnej Booleovskej funkcie, ktorá vytvára prúdový kľúč. Skúmané boli aj viaceré modifikácie LFSR: zmena výstupnej funkcie a zmena časového riadenia [45], [46], [19]. Novým typom generátorov sú spätnoväzobné registre s prenosom – FCSR [26], [27], [9], založené na teórii 2-adických čísel. Veľmi málo prebádanou oblasťou sú zatiaľ stále registre s nelineárnou spätnou väzbou. Dnes sa však dostávajú do popredia generátory založené na báze blokových šifrátorov. Väčšinou ide o návrhy efektívnych prúdových šifrátorov pre softvérové aplikácie (Seal, Scream).

Vyhodnocovanie bezpečnosti generátorov je realizované kombináciou teoretického a experimentálneho prístupu. Perióda a lineárna zložitosť sú zvyčajne skúmané teoreticky, štatistické vlastnosti sú skúmané experimentálne [29], [16], [47]. Na záver sa prirodzene vyšetruje odolnosť generátora voči útokom.

Okrem klasických útokov typu: útok hrubou silou, výmenou času za pamäť, príp. rozdeľuj-a-panuj sa pri prúdových šifrátoroch (založených na LFSR) stretávame najmä s tzv. korelačnými útokmi [51], [35], [7], [61], [?], [23], [25], [24]. Rozpracované bolo aj použitie diferenciálnej kryptoanalýzy [9]. V poslednom období, najmä pri generátoroch založených na báze blokových šifier, sa možno stretnúť s útokmi založenými na odlíšiteľnosti prúdového kľúča od dokonale náhodnej postupnosti.

Úlohou hašovacích funkcií (angl. Manipulation Detection Codes – MDCs) je vytvoriť digitálny odtlačok (bitový reťazec fixnej dĺžky) z ľubovoľnej správy (bitový reťazec ľubovoľnej dĺžky) [39], [40]. Tento digitálny odtlačok potom danú správu "jednoznačne" reprezentuje. (Analogickým príkladom je odtlačok prsta u ľudí.) S hašovacími funkciami sa možno stretnúť v informatike (optimalizovaný prístup k uloženým údajom) a prirodzene aj v kryptografii (ochrana integrity údajov, digitálne podpisové schémy). V prípade, že vstupom hašovacej funkcie je okrem správy aj tajný kľúč, hovoríme

o autentifikačných kódoch (angl. Message Authentication Codes – MACs).

Definícia 2 *([40], neformálna) Jednocestná hašovacia funkcia odolná voči kolíziám je funkcia* $h : \{0,1\}^* \to \{0,1\}^m$, *kde* $\{0,1\}^*$ *je množina všetkých konečných binárnych reťazcov a* m *je dané prirodzené číslo*[1], *spĺňajúca nasledovné podmienky:*

1. *K danej funkčnej hodnote* y *hašovacej funkcie* h *je "ťažké" (t.j. výpočtovo nerealizovateľné v reálnom čase) nájsť takú správu* x, *že* $h(x) = y$.
2. *K danej správe* x *je "ťažké" nájsť takú správu* $x' \neq x$, *že* $h(x') = h(x)$.
3. *Je "ťažké" nájsť také dve rôzne správy* x, x', *že* $h(x) = h(x')$.

Väčšina hašovacích funkcií je založená na kompresnej funkcii so vstupmi fixnej dĺžky [40]. Digitálny odtlačok sa potom počíta nasledovne:

- Správa x sa rozdelí na bloky $x_1, x_2, \ldots, x_t$ fixnej dĺžky. Posledný blok sa doplní podľa dopĺňacieho pravidla na žiadanú dĺžku.
- $H_0 = IV$,
  $H_i = f(x_i, H_{i-1}), \qquad i = 1, 2, \ldots, t,$
  $h(x) = g(H_t)$.
  IV je daný inicializačný vektor, f je kompresná funkcia a g je výstupná funkcia (zvyčajne identita).

Podľa návrhu kompresnej funkcie rozlišujeme hašovacie funkcie založené na blokových šifrátoroch, na matematických problémoch a "netypických" algebraických štruktúrach (v ostatných rokoch sa objavili návrhy založené na kvázigrupách [1], [14], [15] - kryptoanalýzu posledných dvoch prác možno nájsť v časti 4.4 predloženej dizertačnej práce). Takmer všetky v praxi používané hašovacie funkcie (MD5, SHA-1, RIPEMD-160) spadajú do posledne menovanej kategórie.

Základnými útokmi na hašovacie funkcie sú útoky nezávislé na algoritme. Ich úspech závisí len od veľkosti digitálneho odtlačku (m bitov). Medzi ne patrí náhodné hádanie správy a útok založený na narodeninovom paradoxe [40]. Ďalšie útoky sú závislé na konštrukcii samotnej hašovacej funkcie, resp. na tzv. reťazení. Medzi ne patria napr. útok s pevnými bodmi a útok typu "stretnutie uprostred" (angl. meet-in-the-middle attack), ktorý vychádza z narodeninového paradoxu.

Aktuálny stav v oblasti kryptológie možno najlepšie sledovať na viacerých projektoch na výber kryptografických primitív. Medzi už ukončené

[1] Dnes sa pre m používajú hodnoty 128, 160, 196, 256, 512.

projekty patria NESSIE (New European Schemes for Signatures, Integrity and Encryption) [43] a japonský CRYPTREC [41]. V Európe, ako nový projekt 6-teho rámcového programu, začína ECRYPT (European Network of Excellence in Cryptology) [42].

3 Ciele dizertačnej práce

Predložená dizertačná práca sa zaoberá vlastnosťami niektorých, špeciálne konštruovaných, pseudonáhodných postupností ako z pohľadu kryptografie tak aj kryptoanalýzy. Zároveň sa zaoberá aj relatívne novým trendom v kryptografii – použitím kvázigrúp pri návrhu prúdových šifrátorov a hašovacích funkcií.

Ciele práce možno formulovať nasledovne:

1. uviesť potrebné základné pojmy týkajúce sa generátorov pseudonáhodných postupností a hašovacích funkcií v kryptografii;
2. preskúmať kryptografické vlastnosti spájania periód viacerých ml-postupností;
3. urobiť kryptoanalýzu prúdových šifier založených na spájaní transformovaných iterácií z dvoch ml-postupností;
4. kryptoanalyzovať prúdový šifrátor založený na kvázigrupe, ktorý bol navrhnutý v [38],
5. preskúmať bezpečnosť hašovacej funkcie založenej na kvázigrupe, ktorá bola publikovaná v [14], [15].

4 Výsledky dizertačnej práce

4.1 Nová konštrukcia úplne rovnomerne rozdelenej postupnosti

Táto časť je založená na autorových prácach [55] a [56].

Nech $A(b,k)$ je konečná k-rovnomerne rozdelená b-árna postupnosť, pozostávajúca z jej prvých b^k členov, pričom každý jej člen je vydelený číslom b. Každý člen $A(b,k)$ je teda reálne číslo z $[0,1)$. Ďalej nech $A(b,k)^n$ označuje n-krát zopakovanú postupnosť $A(b,k)$.

Vôbec prvú konštrukciu úplne rovnomerne rozdelenej postupnosti publikoval Knuth [28] a je ukázaná v nasledujúcej vete.

Veta 3 *Postupnosť reálnych čísel*

$$A(2,1)^{1.2^2}, A(2^2,2)^{2.2^4}, A(2^3,3)^{3.2^6}, \ldots$$

je úplne rovnomerne rozdelená.

Zistili sme, že síce tzv. Fordove a Knuthove postupnosti vykazujú rovnomerné rozdelenie vzorov, majú aj niektoré slabiny (pozri [55]). Fordova k-rovnomerne rozdelená b-árna postupnosť nie je odolná voči diferenciálnej kryptoanalýze. Jej diferenčné parametre sú nerovnomerne rozdelené a vzdialenosti medzi ich extrémami sú rovné práve k. Podobné slabiny sa objavujú aj v konečnej časti Knuthovej úplne rovnomerne rozdelenej postupnosti. Z technického hľadiska, obe postupnosti sú náročné na vytváranie (najmä pomocou hardvérových generátorov). Pre použitie v praktických aplikáciách preto nie sú tieto postupnosti vhodné.

Vhodné štatistické vlastnosti úplne rovnomerne rozdelených postupností boli pre nás motiváciou pre hľadanie novej (praktickejšej) konštrukcie takejto postupnosti. Náš návrh je založený na tzv. *ml*-postupnostiach.

Veta 4 *(Theorem 4.1.3) Nech p je prvočíslo, $l \in \mathbb{N}$ a $b = p^l$. Ďalej nech $ML'(b,k)$ je konečná b-árna ml-postupnosť, pozostávajúca z jej prvých $b^k - 1$ členov, generovaná nejakým primitívnym polynómom nad $GF(b)$. Nech $ML(b,k)$ je vytvorená z $ML'(b,k)$ vydelením každého jej člena číslom b. Potom postupnosť reálnych čísel*

$$ML(2,1)^{1.2^2}, ML(2^2,2)^{2.2^4}, ML(2^3,3)^{3.2^6}, \ldots$$

je úplne rovnomerne rozdelená.

Z praktických dôvodov sme študovali lokálne vlastnosti, konkrétne spájanie dvoch, príp. viacerých, *ml*-postupností nad $GF(2)$. Naše analýzy ukazujú, že postupnosti tvorené spájaním períód *ml*-postupností majú veľkú lineárnu zložitosť a iba mierne extrémy autokorelačnej funkcie. Veľkosť periódy takto vytvorených postupností je vyjadrená v nasledujúcich dvoch Vetách.

Veta 5 *(Theorem 4.1.4) Nech $u = u_0, u_1, \ldots, u_{2^{\deg c_1(x)}-2}$, resp. $v = v_0, v_1, \ldots, v_{2^{\deg c_2(x)}-2}$ je jedna perióda postupnosti tvorenej primitívnym polynómom $c_1(x)$, resp. $c_2(x) \in GF(2)[X]$, $\deg c_1(x), \deg c_2(x) > 1$, $\deg c_1(x) \neq \deg c_2(x)$, $\deg c_1(x) \neq 2$ a $\deg c_2(x) \neq 3$ alebo naopak. Potom perióda postupnosti $u, v, u, v, \ldots$, vytvorenej spájaním postupností u a v, je $(2^{\deg c_1(x)} - 1) + (2^{\deg c_2(x)} - 1)$.*

Veta 6 *(Theorem 4.1.5) Nech* $u^1 = u_0^1, u_1^1, \ldots, u_{2^{\deg c_1(x)}-2}^1$, $u^2 = u_0^2, u_1^2, \ldots$ $u_{2^{\deg c_2(x)}-2}^2$, $\ldots$, $u^n = u_0^n, u_1^n, \ldots, u_{2^{\deg c_n(x)}-2}^n$ *je jedna perióda postupnosti vytvorenej primitívnym polynómom* $c_1(x), c_2(x), \ldots, c_n(x) \in GF(2)[X]$, $3 < \deg c_1(x) < \deg c_2(x) < \cdots < \deg c_n(x)$ *alebo* $\deg c_1(x) > \deg c_2(x) > \cdots > \deg c_n(x) > 3$. *Potom perióda postupnosti* $u^1, u^2, \ldots, u^n, u^1, u^2, \ldots, u^n, \ldots$, *vytvorenej spájaním postupností* $u^1, u^2, \ldots, u^n$, *je* $\sum_{i=1}^{n}(2^{\deg c_i(x)} - 1)$.

4.2 Spájanie iterácií z dvoch *ml*-postupností

Táto časť je založená na autorových prácach [53] a [54].

Majme generátor G tvorený dvoma LFSR, $L1$ a $L2$. Kľúčom je počiatočné naplnenie $L1$ a $L2$. Nech polynómy $c_1(x), c_2(x) \in GF(2)[X]$ asociované s $L1$, resp. $L2$ sú primitívne. Ďalej nech $\tilde{a} = \tilde{a}_0, \tilde{a}_1, \ldots$, resp. $\tilde{b} = \tilde{b}_0, \tilde{b}_1, \ldots$ sú binárne postupnosti produkované časovo-riadenými registrami $L1$, resp. $L2$.

Algoritmus generátora G:

1. Vytvorenie bitu prúdového kľúča: $z_t = L1(t) \oplus L2(t) = \tilde{a}_t \oplus \tilde{b}_t$.
2. Zmena vnútorného stavu generátora: ak $z_t = 1$, tak sa $L1$ posunie, inak sa posunie $L2$.

Pozorovanie 7 *(Observation 4.2.2) Vytváranie prúdového kľúča možno charakterizovať ako spájanie transformovaných iterácií z dvoch ml-postupností, vytvorených charakteristickými polynómami* $c_1(x)$, *resp.* $c_2(x)$.

Veta 8 *(Theorem 4.2.7) Nech registre* $L1$, *resp.* $L2$ *majú asociované primitívne polynómy* $c_1(x)$, *resp.* $c_2(x)$, $\deg c_1(x), \deg c_2(x) > 1$ *a nenulové počiatočné naplnenie. Potom perióda generátorom* G *vytvoreného prúdového kľúča je daná vzťahom*

$$(2^{\max\{\deg c_1(x), \deg c_2(x)\}} - 1) + 2^{|\deg c_1(x) - \deg c_2(x)|}(2^{\min\{\deg c_1(x), \deg c_2(x)\}} - 1).$$

Nasledujúce Vety charakterizujú štatistické vlastnosti prúdového kľúča, vytváraného generátorom G.

Veta 9 *(Theorem 4.2.8) Nech registre* $L1$, *resp.* $L2$ *s asociovanými primitívnymi polynómami* $c_1(x)$, *resp.* $c_2(x)$, $\deg c_1(x), \deg c_2(x) > 1$ *majú nenulové počiatočné naplnenie. Potom počet jednotiek* n_1 *a núl* n_0 *v jednej perióde prúdového kľúča je nasledovný:*

1. *ak* $\deg c_1(x) \geq \deg c_2(x)$ *tak*
   $n_1 = 2^{\deg c_1(x)} - 1, \qquad n_0 = 2^{|\deg c_1(x) - \deg c_2(x)|}(2^{\deg c_2(x)} - 1)$;

2. *ak* $\deg c_1(x) < \deg c_2(x)$ *tak*
$n_1 = 2^{|\deg c_1(x) - \deg c_2(x)|}(2^{\deg c_1(x)} - 1), \qquad n_0 = 2^{\deg c_2(x)} - 1.$

Veta 10 *(Theorem 4.2.9) Nech L1, resp. L2 s asociovanými primitívnymi polynómami* $c_1(x)$, *resp.* $c_2(x)$, $\deg c_1(x), \deg c_2(x) > 1$, $|\deg c_1(x) - \deg c_2(x)| \leq 1$ *majú nenulové počiatočné naplnenie. Potom prúdový kľúč, vytváraný generátorom G, spĺňa prvý Golombov postulát. Navyše, ak* $\deg c_1(x) = \deg c_2(x)$, *tak potom prúdový kľúč spĺňa aj druhý Golombov postulát.*

Veta 11 *(Theorem 4.2.10) Prúdový kľúč vytváraný generátorom G vyhovuje kritériu dlhých iterácií (FIPS 140-1, long run test), ak* $1 < \|L1\|, \|L2\| < 34$ *(a registre L1, resp. L2 majú nenulové počiatočné naplnenie).*

Z vykonaných experimentov na 1 000 postupnostiach vyplýva, že prúdový kľúč má veľkú lineárnu zložitosť (blízku perióde) a aj vhodný profil lineárnej zložitosti. Všetky testované prúdové kľúče úspešne prešli všetkými testami podľa normy FIPS 140-1, 95% z nich prešlo testom na sériovú koreláciu [29], avšak všetky zlyhali na teste medzier [29]. Z výsledkov tzv. Maurerovho univerzálneho štatistického testu vyplýva, že prúdový kľúč nemožno výrazne skomprimovať.

Generátor G nie je odolný voči útoku so známym otvoreným textom. Algoritmus narušenia generátora je uvedený v predloženej práci.

4.3 Útoky na prúdový šifrátor založený na kvázigrupe

Táto časť je založená na autorových prácach [57] a [58].

Nech $(Q, *)$ je konečná kvázigrupa a jednotlivé znaky otvoreného textu $p_1, p_2, \ldots, p_k$, $p_i \in Q$, $1 \leq i \leq k$. Rovnako nech jednotlivé znaky zašifrovaného textu $c_i \in Q$, $1 \leq i \leq k$. Kľúčom študovaného prúdového šifrátora (pozri [38], veľmi podobný šifrátor bol publikovaný aj v [33]) je definícia operácie $*$ na Q, t.j. Caleyho tabuľka tejto operácie. Autori šifrátora ho prehlásili za odolný voči ľubovoľným útokom [38].

Šifrovanie:
$encrypt(p_1, p_2, \ldots, p_k) = c_1, c_2, \ldots, c_k$.
$c_1 = l * p_1$, kde $l \in Q$ je dané (a známe).
$c_{i+1} = c_i * p_{i+1}$, $i = 1, 2, \ldots, k-1$.

Dešifrovanie:
$decrypt(c_1, c_2, \ldots, c_k) = p_1, p_2, \ldots, p_k$.
$p_1 = l \backslash c_1$.
$p_{i+1} = c_i \backslash c_{i+1}$, $i = 1, 2, \ldots, k-1$.

Analyzovaný prúdový šifrátor nie je odolný voči útoku s vybranými zašifrovanými textami. Nech $Q = \{q_1, q_2, \ldots, q_n\}$. Predpokladajme, že útočník má prístup k dešifrovaciemu zariadeniu, v ktorom je vložený neznámy dešifrovací kľúč. Potom môže vložiť nasledujúci zašifrovaný text do dešifrovacieho zariadenia:

$q_1, q_1, q_1, q_2, q_1, q_3, \ldots, q_1, q_n,$
$q_2, q_1, q_2, q_2, q_2, q_3, \ldots, q_2, q_n,$
$\vdots$
$q_n, q_1, q_n, q_2, q_n, q_3, \ldots, q_n, q_n$

Z dešifrovacieho zariadenia získa nasledovný otvorený text:

$l\backslash q_1, q_1\backslash q_1, q_1\backslash q_1, q_1\backslash q_2, q_2\backslash q_1, q_1\backslash q_3, \ldots, q_1\backslash q_n,$
$\vdots$
$q_n\backslash q_n, q_n\backslash q_1, q_1\backslash q_n, q_n\backslash q_2, q_2\backslash q_n, q_n\backslash q_3, \ldots, q_n\backslash q_n.$

Ako je vidieť, Caleyho tabuľka operácie $\backslash$ definovanej na Q je úplne nájdená. Z nej možno dopočítať Caleyho tabuľku operácie $*$. Použitý zašifrovaný text je tvorený $2n^2$ znakmi. Prezentovaný útok vyžaduje $2n^2$ operácií $\backslash$.

Útok s vybranými otvorenými textami možno aplikovať podobným spôsobom. Taktiež možno použiť útok so známymi zašifrovanými textami, avšak v tomto prípade nemožno zaručiť nájdenie celého kľúča.

Zistili sme, že skúmaný prúdový šifrátor je možné narušiť dokonca aj pomocou útoku so znalosťou iba zašifrovaného textu. Tento útok je založený na frekvenčnej analýze, dobre známej z kryptoanalýzy klasických kryptosystémov. Útok sme úspešne prakticky vykonali na otvorenom texte (kniha "SLOVENSKO. Európske súvislosti ľudovej kultúry" od Rastislavy Stoličnej et al., VEDA Bratislava 1997), napísanom v slovenskom jazyku v rozšírenej telegrafnej abecede a pozostávajucom z 291 041 znakov. Rád použitej kvázigrupy bol 27.

4.4 Útoky na hašovaciu funkciu založenú na kvázigrupe

Táto časť je založená na autorových prácach [59] a [60].

Konštrukcia 12 *([14], [15].) Nech $(Q, *)$ je konečná kvázigrupa a Q^* množina všetkých konečných postupností prvkov z Q. Nech správa je postupnosť prvkov $\{m_1, m_2, \ldots, m_k\}$ z Q. Pre dané $a \in Q$ definujeme hašovaciu funkciu $H_a : Q \times Q^* \to Q$ ako*

$$H_a(m_1, m_2, \ldots, m_k) = ((\ldots((a * m_1) * m_2) * \ldots) * m_{k-1}) * m_k,$$

kde $m_i \in Q$, $1 \leq i \leq k$.

O počte správ danej dĺžky s rovnakým digitálnym odtlačkom hovorí nasledujúca Veta. Jej zrejmým dôsledkom je balansovanosť študovanej hašovacej funkcie.

Veta 13 *(Theorem 4.4.7) Nech* $(Q, *)$ *je konečná kvázigrupa a* H_a *hašovacia funkcia daná Konštrukciou 12. Potom počet správ* $\{m_1, m_2, \ldots m_k\}$, $m_i \in Q$, $1 \leq i \leq k$ *dĺžky* k *s rovnakým digitálnym odtlačkom je* $\|Q\|^{k-1}$.

V ďalšom ukážeme konštrukciu falošných správ, vedúcich k narušeniu študovanej hašovacej funkcie.

Nech $a \in Q$ je známy parameter hašovacej funkcie a $\{m_1, m_2, \ldots m_k\}$, $m_i \in Q$, $1 \leq i \leq k$ je správa. Jej digitálny odtlačok je potom $H_a(m_1, m_2, \ldots, m_k) = (\ldots((a * m_1) * m_2) * \ldots) * m_k = d$. Vytvoríme správu $x_1, x_2, \ldots, x_v$, $x_i \in Q$, $1 \leq i \leq v$, ktorej digitálny odtlačok bude taktiež d. $x_1, x_2, \ldots, x_{v-1}$ môžu byť ľubovoľné. Zostáva už len vhodne zvoliť x_v. (Vo všeobecnosti to nemusí to byť posledný symbol správy.) V prípade, že operácia definovaná na kvázigrupe je daná (uloženou) Caleyho tabuľkou, je tento problém riešiteľný hrubou silou. (Ak jeden prvok kvázigupy reprezentujeme 18-timi bitmi, potom $\|Q\| = 2^{18}$ a na uloženie Caleyho tabuľky operácie pre túto kvázigrupu treba $18.2^{18}.2^{18} > 1$ TB, čo je na hranici dnešných možností. Druhým problémom je malá dĺžka digitálneho odtlačku, čo umožňuje útok pomocou narodeninového paradoxu.)

Problémy s pamäťovými nárokmi navrhli autori hašovacej funkcie v [14], [15] vyriešiť použitím kvázigrupy modulárneho odčítania. Operácia *, definovaná na Q, je potom daná vzťahom $a * b = a + (n - b) \bmod \|Q\|$. V tomto prípade však možno pre vyššie uvedenú konštrukciu falošnej správy použiť vzťah $x_v = d' + (\|Q\| - d) \bmod \|Q\|$.

Veta 14 *(Theorem 4.4.12) Hašovacia funkcia* H_a *s použitím kvázigrupy modulárneho odčítania nie je odolná voči kolíziám ani voči nájdeniu falošnej správy k danej správe.*

Útok sa skomplikuje, pokiaľ sa pri konštrukcii hašovacej funkcie použije izotopná kvázigrupa s kvázigrupou modulárneho odčítania. Operáciu v takejto kvázigrupe $(Q, .)$ možno potom zapísať ako $a.b = \psi^{-1}(\theta(a) + (\|Q\| - \varphi(b)) \bmod \|Q\|)$, kde ψ, θ, φ sú zobrazenia, ktoré definujú izotopizmus medzi kvázigrupou modulárneho odčítania a kvázigrupou $(Q, .)$. V tomto prípade konštrukcia falošnej správy vedie k rovnici $d = a.b = \psi^{-1}(\theta(a) + (\|Q\| - \varphi(b)) \bmod \|Q\|)$ pre danú kvázigrupu, kde a a d sú známe, b je neznáma.

Bezpečnosť študovanej hašovacej funkcie teda výrazne závisí od "náročnosti" invertovania zobrazení φ a ψ^{-1}.

Potenciálnym bezpečnostným problémom pri použití kvázigrupy $(Q, .)$ izotopnej s kvázigrupou modulárneho odčítania $(Q, *)$ je možná existencia viacerých trojíc zobrazení θ, φ, ψ, ktoré definujú izotopizmus medzi $(Q, .)$ a $(Q, *)$. Z vykonaných experimentov úplným prehľadávaním (pre $\|Q\| = 3, 4, 5,$ a 6) plynie hypotéza, že existuje práve $2\|Q\|^2$ trojíc zobrazení θ, φ, ψ, ktoré definujú izotopizmus medzi $(Q, .)$ a $(Q, *)$.

Skúmali sme aj modifikáciu tejto hašovacej funkcie, kedy sme parameter a považovali za tajný kľúč (H_a je v tomto prípade MAC).

Veta 15 *(Theorem 4.4.16) Konštrukcia falošných správ pre H_a, keď je použitá ako MAC, s tajným kľúčom a, je iba tak ťažká ako konštrukcia falošných správ pre hašovaciu funkciu H_a samotnú, t.j. keď je a verejné.*

5 Závery pre ďalší rozvoj disciplíny

V predloženej práci sú skúmané vlastnosti špeciálne konštruovaných pseudonáhodných postupností tak z hľadiska kryptografie ako aj kryptoanalýzy. Práca sa taktiež zaoberá relatívne novým trendom v kryptografii – použitím kvázigrúp pri návrhu prúdových šifrátorov a hašovacích funkcií.

Hlavnými výsledkami práce sú:

- nová konštrukcia úplne rovnomerne rozdelenej postupnosti reálnych čísel, popis periódy výslednej postupnosti pri spájaní períod *ml*-postupností,
- popis kryptografických vlastností prúdového šifrátora, založeného na spájaní iterácií *ml*-postupností a jeho následná kryptoanalýza,
- kryptoanalýza prúdového šifrátora založeného na kvázigrupe,
- kryptoanalýza hašovacej funkcie založenej na kvázigrupe.

Využitie kvázigrúp pri návrhu kryptografických primitív je pomerne novým smerom a zatiaľ nie je známych veľa výsledkov. Návrh prúdových šifrátorov sa v poslednom období začína orientovať na návrh špeciálnych prúdových šifrátorov, využívajúc pritom známe poznatky z návrhu blokových šifrátorov. Návrh hašovacích funkcií sa v poslednom období venuje zlepšovaniu známych používaných návrhov, pričom niektoré hašovacie funkcie boli použité aj ako základ pre návrh blokových šifrátorov.

Referencie

[1] Bakhtiari, S., Safavi-Naini, R., Pieprzyk, J.: A Message Authentication Code Based on Latin Squares, Proceedings of ACISP '97, LNCS 1270, Springer-Verlag 1997, pp.194–203.

[2] Beth, T., Piper, F.C.: The Stop–and–go Generator, Advances in Cryptology – EUROCRYPT '84 Proceedings, LNCS 209, Springer–Verlag 1985, pp.88–92.

[3] Biryukov, A., Shamir, A., Wagner, D.: Real Time Cryptanalysis of A5/1 on PC, FSE 2000, LNCS 2365, Springer–Verlag, pp.1–18.

[4] Blum, L., Blum, M., Shub, M.: A Simple Unpredictable Pseudo-Random Number Generator, SIAM Journal on Computing, Vol.15 (1986), No.2, pp.364–383.

[5] den Boer, B., Bosselaers, A.: Collision for the Compression Function of MD5, Advances in Cryptology - EUROCRYPT '93 Proceedings, LNCS 765, Springer–Verlag 1994, pp.293–304.

[6] Boyar, J.: Inferring Sequences Produced by Pseudo-Random Number Generators, J.Assoc.Comput.Mach., Vol.36 (1989), pp.129–141.

[7] Chepyzhov, V., Smeets, B.: On a Fast Correlation Attack on Certain Stream Ciphers, Advances in Cryptology – EUROCRYPT '91 Proceedings, LNCS 547, Springer–Verlag 1991, pp.176–185.

[8] Coppersmith, D., Halevi, S., Jutla, C.: Cryptanalysis of Stream Ciphers with Linear Masking, `http://eprint.iacr.org/2002/020.ps`, 15.4.2004.

[9] Cusick, T.W., Ding, C., Renvall, A.: Stream Ciphers and Number Theory, Elsevier Science B.V. 1998.

[10] Damgård, I.B.: A Design Principle for Hash Functions, Advances in Cryptology - CRYPTO '89 Proceedings, LNCS 435, Springer–Verlag 1990, pp.416–427.

[11] Dénes, J., Keedwell, A.D.: Latin Squares and Their Applications, Academic Press, NY 1974.

[12] Dobbertin, H., Bosselaers, A., Preneel, B.: RIPEMD-160: A Strengthened Version of RIPEMD, Fast Software Encryption, LNCS 1039, Springer-Verlag 1996, pp.71–82.

[13] Dobbertin, H.: Cryptanalysis of MD4, Journal of Cryptology, Vol.11 (1998), No.4, pp.253–271. See also Fast Software Encryption, LNCS 1039, Springer-Verlag 1996, pp.53–69.

[14] Dvorský, J., Ochodková, E., Snášel, V.: Hash Function Based on Quasigroups ("Hashovací funkce založená na kvazigrupách"), *Proc. of Mikulášská kryptobesídka*, Praha, pp. 27-36, 2001 (in Czech).

[15] Dvorský, J., Ochodková, E., Snášel, V.: Hash Functions Based on Large Quasigroups, *Proc. of Velikonoční kryptologie*, Brno, pp. 1-8, 2002.

[16] FIPS PUB 140–2, Federal Information Processing Standard Publication, Security Requirements for Cryptographic Modules, National Institute of Standards and Technology (NIST), U.S. Department of Commerce, Washington D.C., May 25, 2001.

[17] FIPS PUB 180–1, Federal Information Processing Standard (FIPS), Secure Hash Standard, National Institute of Standards and Technology (NIST), U.S. Department of Commerce, Washington D.C., April 17, 1995.

[18] Ford, L.R.Jr.: A Cyclic Arrangement of m-Tuples, Rand Corporation, Santa Monica, California, 1957, report 1071.

[19] Gollmann, D.: Pseudo Random Properties of Cascade Connections of Clock Controlled Shift Registers, Advances in Cryptology – EUROCRYPT '84 Proceedings, LNCS 209, Springer–Verlag 1985, pp.93–98.

[20] Grošek, O.: On the Stability of Stream Ciphers (O stabilite prúdových šifier), Proceedings of the conference "Jesenný seminár z kryptoanalýzy", Liptovský Mikuláš, October 9–11, 1996, pp.14–26 (in Slovak).

[21] Grošek, O., Horák, P., van Tran, T.: On Non-Polynomial Latin Squares, accepted for publication in Design, Codes and Cryptography, Kluwer Academic Publishers.

[22] Grošek, O., Porubský, Š.: Cryptology - Algorithms, Methods, Practice (Šifrovanie - algoritmy, metódy, prax), Praha, Grada 1992 (in Slovak).

[23] Johansson, T., Jönsson, F.: Improved Fast Correlation Attacks on Stream Ciphers via Convolutional Codes, Advances in Cryptology – EUROCRYPT '99, LNCS 1592, Springer–Verlag 1999, pp.347–362.

[24] Johansson, T., Jönsson, F.: Fast Correlation Attacks Based on Turbo Code Techniques, Advances in Cryptology – CRYPTO '99, LNCS 1666, Springer–Verlag 1999, pp.181–197.

[25] Johansson, T., Jönsson, F.: Fast Correlation Attacks through Reconstruction of Linear Polynomials, Advances in Cryptology – CRYPT0 '2000, LNCS 1880, Springer–Verlag 2000, pp.300–315.

[26] Klapper, A.: Feedback with Carry Shift Registers over Finite Fields, K.U.Leuven Workshop on Cryptographic Algorithms, Springer-Verlag 1995, pp.170–178.

[27] Klapper, A., Goresky, M.: Large Period Nearly de Bruijn FCSR Sequences, Advances in Cryptology - EUROCRYPT '95 Proceedings, LNCS 921, Springer-Verlag 1995, pp.263–273.

[28] Knuth, D.E.: Construction of a Random Sequence, Nordisk tidskrift for informationbehandling, Vol.5 (1965), No.4, pp.246–250.

[29] Knuth, D.E.: The Art of Computer Programming, Vol.2 Seminumerical Algorithms, Addison-Wesley 1969.

[30] Knuth, D.E.: Deciphering a Linear Congruential Encryption, IEEE Transactions on Information Thoery, Vol.IT–31 (January 1985), No.1.

[31] Krawczyk, H.: How to Predict Congruential Generators, J.Algorithms, Vol.13 (1992), pp.527–545.

[32] Lidl, R., Niederreiter, H.: Introduction to Finite Fields and Their Applications, Cambridge University Press, 1994, Revised Edition.

[33] Markovski, S., Gligoroski, D., Andova, S.: Using Quasigroups for One–One Secure Encoding, Proceedings of LIRA '97 – Novi Sad Yugoslavia.

[34] Massey, J.L.: Shift-Register Synthesis and BCH Decoding, IEEE Transactions on Information Theory, Vol.IT–15 (January 1969), No.1.

[35] Meier, W., Staffelbach, O.: Fast Correlation Attacks on Certain Stream Ciphers, Journal of Cryptology, Vol.1 (1989), pp.159–176.

[36] Menezes, A., van Oorschot, P., Vanstone, S.: Handbook of Applied Cryptography, CRC Press 1996, `http://www.cacr.math.uwaterloo.ca/hac`.

[37] Nemoga, K.: Linear Recurring Sequences (Lineárne rekurentné postupnosti), Proceedings of the conference "Jesenný seminár z kryptoanalýzy", Liptovský Mikuláš, October 9–11, 1996, pp.1–13 (in Slovak).

[38] Ochodková, E., Snášel, V.: Using Quasigroups for Secure Encoding of File System, Proceedings of the International Scientific NATO PfP/PWP Conference "Security and Information Protection 2001", May 9–11, 2001, Brno, Czech Republic, pp.175–181.

[39] Preneel, B.: Analysis and Design of Cryptographic Hash Functions, Doctoral Dissertation, Katholieke Universiteit Leuven, 1993.

[40] Preneel, B.: The State of Hash Functions, Cryptology and Information Security, Proceedings of VI RECSI, Teneriffe, Spain, September 2000, RA-MA, Madrid, 2000, pp. 3-27.

[41] Project CRYPTREC, `http://www.ipa.go.jp/security/enc/CRYPTREC/index-e.html`, (April 19, 2004).

[42] Project ECRYPT - European Network of Excellence in Cryptology, `http://www.ecrypt.eu.org`, (April 19, 2004).

[43] Project NESSIE, `http://www.cryptonessie.org`.

[44] Rogaway, P., Coppersmith, D.: A Software-Optimized Encryption Algorithm, Fast Software Encryption Proceedings, LNCS 809, Springer–Verlag 1994, pp.56–63.

[45] Rueppel, R.A.: The Analysis and Design of Stream Ciphers, Berlin, Heidelberg, Springer–Verlag, 1986.

[46] Rueppel, R.A.: When a Shift Registers Clock Themselves, Advances in Cryptology – EUROCRYPT '87 Proceedings, LNCS 304, Springer–Verlag 1988, pp.53–64.

[47] Rukhin, A. et al.: A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications. NIST Special Publication 800–22, May 15, 2001.

[48] Satko, L.: Correlation attack of Siegenthaler and Rueppel (Korelačný útok Siegenthalera a Rueppela), Proceedings of the conference "Jesenný seminár z kryptoanalýzy", Liptovský Mikuláš, October 9–11, 1996, pp.27–35 (in Slovak).

[49] Schneier, B.: Applied Cryptography. Protocols, Algorithms, and Source Code in C, John Wiley & Sons, Inc. 1996, Second Edition.

[50] Siegenthaler, T.: Correlation-Immunity of Nonlinear Combining Functions for Cryptographic Applications, IEEE Transactions on Information Theory, Vol.IT-30 (September 1984), No.5, pp.776–780.

[51] Siegenthaler, T.: Decrypting a Class of Stream Ciphers Using Ciphertext Only, IEEE Transactions on Computers, Vol.34 (January 1985), No.1, pp.81–85.

[52] Stinson, D.R.: Cryptography: Theory and Practice, CRC Press 1995.

[53] Vojvoda, M.: Cryptanalysis of a Clock-Controlled Running Key Generator, Journal of Electrical Engineering, Vol.50 (1999), No.10/s, pp.16–18.

[54] Vojvoda, M.: Enhanced Cryptanalysis of a Clock-Controlled Running Key Generator, Journal of Electrical Engineering, Vol.51 (2000), No.12/s, pp.81–84.

[55] Vojvoda, M., Šimovcová, M.: Some Properties of Uniformly Distributed Sequences, Abstracts of the conference "Elitech 2000", FEI-STU, 2000.

[56] Vojvoda, M., Šimovcová, M.: On Concatenating Pseudorandom Sequences, Journal of Electrical Engineering, Vol.52 (2001), No.10/s, pp.36–37.

[57] Vojvoda, M.: Cryptanalysis of a File Encoding System Based on Quasigroup, Journal of Electrical Engineering, Vol.54 (2003), No.12/s, pp.69–71.

[58] Vojvoda, M.: Attacks on a File Encryption System Based on Quasigroup, Proceedings of the 6th Scientific Conference on Electrical Engineering and Information Technology for PhD students – Elitech 2003, FEI-STU 2003, pp.54–56.

[59] Vojvoda, M.: Cryptanalysis of One Hash Function Based on Quasigroup, accepted for publication in Tatra Mountains Mathematical Publications.

[60] Vojvoda, M.: On One Hash Function Based on Quasigroup, Proceedings of the Conference "Mikulášská kryptobesídka", ecom-monitor.com 2003, pp.23-28.

[61] Zeng, K.C., Huang, M.: On the Linear Syndrome Method in Cryptanalysis, Advances in Cryptology – CRYPTO '88, LNCS 403, Springer–Verlag 1990, pp.469–478.

6 Zoznam prác dizertanta

Vedecké články

- Vojvoda, M.: Cryptanalysis of a Clock-Controlled Running Key Generator, Journal of Electrical Engineering, Vol. 50 (1999), No. 10/s, pp.16-18.
- Vojvoda, M.: Enhanced Cryptanalysis of a Clock-Controlled Running Key Generator, Journal of Electrical Engineering, Vol. 51 (2000), No. 12/s, pp. 81-84.
- Vojvoda, M., Šimovcová, M.: Some Properties of Uniformly Distributed Sequences, Proceedings of abstracts from the conference Elitech 2000, (Vojvoda 50%, Šimovcová 50%).
- Vojvoda, M., Šimovcová, M.: On Concatenating Pseudorandom Sequences, Journal of Electrical Engineering, Vol. 52 (2001), No. 10/s, pp.36-37, (Vojvoda 70%, Šimovcová 30%).
- Vojvoda, M.: A Survey of Security Mechanisms in Mobile Communication Systems, Tatra Mountains Mathematical Publications, Vol. 25 (2002), pp. 101-117.
- Vojvoda, M.: A Probabilistic Approach to Weight Complexity of Binary Sequences, Proceedings of Elitech 2001, FEI STU, Bratislava, 2002, pp.91-92.
- Šimovcová, M., Vojvoda, M.: Symmetric and Complementary Boolean Functions, Proceedings of Elitech 2001, FEI STU, Bratislava, 2002, pp. 89-90, (Vojvoda 30%, Šimovcová 70%).
- Vojvoda, M.: Cryptanalysis of a File Encoding System Based on Quasigroup, Journal of Electrical Engineering, Vol.54 (2003), No.12/s, pp.69-71.
- Vojvoda, M.: Cryptanalysis of One Hash Function Based on Quasigroup, accepted for publication in Tatra Mountains Mathematical Publications.
- Vojvoda, M.: Attacks on a File Encryption System Based on Quasigroup, Proceedings of the 6th Scientific Conference on Electrical Engineering and Information Technology for PhD students - Elitech 2003, FEI-STU 2003, pp.54-56.

- Vojvoda, M.: On One Hash Function Based on Quasigroup, Proceedings of the Conference "Mikulášská kryptobesídka", ecom-monitor.com 2003, pp.23-28.

Učebné materiály

- Akantis,D., Grošek,O., Nemoga,K., Satko,L., Vojvoda,M.: KRYPTOLÓGIA: Základy a aplikácie v bankovníctve VIII., FEI-STU 2001, 86 s.
- Grošek,O., Nemoga,K., Satko,L., Strnád,O., Šrámka,M., Vojvoda,M.: KRYPTOLÓGIA: Základy a aplikácie v bankovníctve IX., FEI-STU 2002, 152 s.
- Grošek,O., Nemoga,K., Oravec,P., Satko,L., Šiška,J., Vávra,A., Vojvoda,M., Zanechal,M.: KRYPTOLÓGIA: Základy a aplikácie v bankovníctve X., FEI-STU 2003, 123 s.

Granty a výskumné správy

- Spoluriešiteľ grantu "Metódy a prostriedky získavanie, reprezentácie, prezentácie a vyhľadávania informácií a znalostí", VEGA 1/7611/20, Zodpovedný riešiteľ: Prof. Ing. Vladimír Vojtek, PhD. (2001 – 2002).
- Spoluriešiteľ grantu "Spracovanie informácií v distribuovanom prostredí mobilných agentov", VEGA 1/0161/03, Zodpovedný riešiteľ: Prof. Ing. Vladimír Vojtek, PhD. (od r.2003).
- Spoluriešiteľ 9 výskumných úloh a spoluautor 9 výskumných správ pre Národný bezpečnostný úrad SR a Ministerstvo vnútra SR (od r.2001).

7 Summary

In this dissertation there are properties of some specifically constructed pseudorandom sequences studied both from the point of view of cryptography and cryptanalysis. This dissertation deals also with a relatively new direction in cryptography – the usage of quasigroups in the design of stream ciphers and hash functions.

The state of the art in stream ciphers and hash fuctions is given in Chapter 3. It covers the design principles of stream ciphers, their evaluation and the

attacks against them as well. There are also the design principles of hash functions and known attacks against them described in this Chapter.

The results of the research are presented in Chapter 4. This Chapter is based on the author's papers [53], [54], [55], [56], [57], [58], [59] and [60].

Cryptographic properties of the concatenation of periods of several *ml*-pseudorandom sequences are studied in Section 4.1. The length of the period of a sequence obtained by periodic concatenation of two or more *ml*-sequences is determined. Moreover, a new construction of a completely equidistributed real valued sequence based on concatenation of *ml*-sequences is presented.

Section 4.2 deals with cryptanalysis of one stream cipher based on the concatenation of transformed runs of two *ml*-sequences. There are several theorems determining the number of runs in an *ml*-sequence presented in this section. The period of the keystream sequence of the cryptanalysed generator is determined as well as its basic statistical properties. The keystream sequence possesses good cryptographic properties such as long period and large linear complexity. The results of statistical tests are outlined. A known plaintext attack on the studied running key generator is proposed. The security of the generator against the known plaintext attack is generalized.

There are three successful attacks, namely chosen ciphertext, chosen plaintext and ciphertext-only attacks, against the self-synchronizing stream cipher (proposed in [38]) presented in Section 4.3. These attacks rank among the standard basic cryptanalyst techniques. Each of these attacks is much faster than the brute-force attack. We conclude that the cryptanalysed self-synchronizing stream cipher is insecure due to its vulnerability to the presented attacks.

The properties of one hash function based on a quasigroup (proposed in [14], [15]) are studied in Section 4.4. Some possible attacks against this hash function are presented. Attacks are studied in a setting when a general (storable, i.e. small) quasigroup is used and also when a special (large) quasigroup, namely the quasigroup of modular subtraction is used. The security of the construction of a hash functions is studied both in the MDC and also in the MAC scenario. In all the cases it was possible to create false messages. It was demostrated which mappings play an important role in the security of the studied hash function when a quasigroup isotopic to the quasigroup of modular subtraction is used. A possible weakness of isotopic mappings was found.