VEDECKÁ RADA FAKULTY ELEKTROTECHNIKY
A INFORMATIKY SLOVENSKEJ TECHNICKEJ
UNIVERZITY V BRATISLAVE

Július Šiška

Autoreferát dizertačnej práce

Diskrétny logaritmus a jeho zovšeobecnenia

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

11–14–9 Aplikovaná matematika

Bratislava, február 2003

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

Predkladateľ: Július Šiška
Národná banka Slovenska
Imricha Karvaša 1
813 25 Bratislava

Školiteľ: Prof. RNDr. Otokar Grošek, PhD.
Fakulta elektrotechniky a informatiky STU Bratislava

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

RNDr. Jozef Vyskoč, PhD.
VaF, s.r.o.
Bebravská 1,
821 07 Bratislava

RNDr. Karol Nemoga, PhD.
Matematický ústav
Slovenská akadémia vied
Štefánikova 49
814 73 Bratislava

Autoreferát bol rozoslaný dňa

Obhajoba dizertačnej práce sa koná dňa ..... o ..... h. pred komisiou pre obhajobu dizertačnej práce v odbore doktorandského študia, vymenovanej predsedom spoločnej odborovej komisie ..... 11–14–9 Aplikovaná matematika
v

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

1 Úvod

V súčasnosti kryptografia nachádza stále širšie pole uplatnenia v civilnom živote aj mimo bezpečnostných zložiek, kde bola používaná už dlho. Kryptografia sa používa v Internete (podpora posielaní šifrovaných emailov, zabezpečenie home bankingu, bezpečnosť pri internetových platbách za tovar), vo finančných službách (elektronické peňaženky, operácie s kreditnými kartami), v mobilných telefónoch, aj v telekomunikáciách (šifrované faxové správy, bezpečné telefóny a šifrovaná platená TV). Na tieto účely sa používajú rôzne druhy kryptografických algoritmov. V tejto práci sa zaoberáme iba jedným z mnohých typov kryptografických algoritmov – algoritmami založenými na verejných kľúčoch a probléme diskrétneho logaritmu.

Vôbec prvým zverejneným kryptografickým algoritmom s verejnými kľúčmi bola Diffie-Hellmanova schéma na výmenu kľúčov. Bola založená práve na predpoklade, že diskrétny logaritmus sa v konečnom poli ťažko počíta. Obtiažnosť problému diskrétneho logaritmu nie je dokázaná, no napriek tomu kryptológovia veria, že kryptosystémy na ňom založené sú dostatočne bezpečné, ak sa ich parametre vhodne zvolia.

Hoci kryptografické algoritmy sú založené na viacerých ťažkých problémoch, najpopulárnejšie a všeobecne v odbornej verejnosti akceptované ako najdôveryhodnejšie sú dva ťažké problémy vhodné pre kryptosystémy s verejným kľúčom - problém faktorizácie veľkých čísiel (využitého napr. v RSA) a druhým je problém diskrétneho logaritmu. Ostatné použité problémy boli buď zlomené, sú menej efektívne implementovateľné, alebo neboli ešte podrobené dôkladnej kryptoanalýze.

V súčasnosti je na probléme diskrétneho logaritmu založených niekoľko rozšírených kryptografických algoritmov. Ak by sa ukázal predpoklad o jeho obtiažnosti ako nesprávny, všetky tieto schémy by prestali byť bezpečné.

Jeden z dôvodov, prečo sa stále problém diskrétneho logaritmu skúma je ten, že veľa nových kľúčových myšlienok v oblasti faktorizácie a diskrétneho logaritmu pochádza od jedinej osoby - Johna Pollarda. Navyše, pre cyklické grupy bez ďalšieho využitia znalostí o ich štruktúre nebol urobený žiaden podstatný pokrok za posledných 25 rokov. Boli vyvinuté iba modifikácie a efektívnejšie verzie tzv. index calculus algoritmov pre konečné polia.

2 Súčasný stav problematiky

Diffie-Hellmanova schéma, ElGamalova podpisová schéma, GOST, DSA, ECDSA, všetky popísané v [Schn96, MOV96], sú kryptografické schémy založené na probléme diskrétneho logaritmu. Tento problém je možné zaviesť nasledujúcim spôsobom.

Problém 2.1 (Problém 2.4). *Problém diskrétneho logaritmu (ďalej aj skratkou DLP) je nasledujúci: pre konečnú cyklickú grupu G rádu n, jej generátor $g \in G$*

a prvok $y \in G$, je treba nájsť číslo x, $0 \leq x < n$ také, že $g^x = y$ a zapisujeme $x = \log_g y$.

Problém 2.2 (Problém 2.5). *Zovšeobecnený problém diskrétneho logaritmu (GDLP) je nasledujúci: pre konečnú grupu G rádu n (tu sa nevyžaduje, aby grupa bola cyklická), jej prvok $g \in G$ rádu q a prvok $y \in G$, je treba nájsť číslo x, $0 \leq x \leq q-1$ také, že $g^x = y$, ak také číslo existuje.*

Veľkosť používaných algebraických štruktúr vo všetkých uvedených algoritmoch závisí od známych algoritmov na riešenie DLP. Sú to hlavne algoritmy Shanksov, Pollardov rho a Pohlig-Hellmanov, pracujúce v ľubovoľných cyklických grupách a index calculus algoritmus, ktorý pracuje iba v niektorých grupách.

Z algoritmov, ktoré sú založené na obtiažnosti riešenia DLP uvedieme DSA [FIPS186]. Parametre algoritmu (môžu byť zdieľané celou doménou subjektov) sú nasledujúce:

- prvočíslo p dĺžky, ktorá je násobok 64 a je z rozmedzia 512 až 1024 bitov,
- prvočíslo q, ktoré je 160 bitový prvočíselný faktor čísla $p-1$,
- $g = h^{(p-1)/q} \pmod p$, kde h je ľubovoľné číslo menšie ako $p-1$, pre ktoré $h^{(p-1)/q} \pmod p$ nie je rovné 1.

DSA využíva pri vytváraní digitálneho podpisu hašovaciu funkciu $h : \{0,1\}^* \to \mathbb{Z}_q$ pre zvolené q. DSS (štandard FIPS 186) vyžaduje použitie 160 bitovej hašovacej funkcie SHA-1.

Algoritmus 2.3 (Algoritmus 3.8) DSA podpisová schéma

A si zvolí náhodné číslo $x_A \in \mathbb{Z}_q$, ktoré bude jeho súkromný kľúč a zverejní číslo $y_A = g^{x_A} \pmod p$ ako verejný kľúč.

1. *Podpísanie správy.* Na podpísanie správy m vykoná subjekt A nasledujúce kroky:
   (a) Zvolí náhodné tajné číslo $k \in \mathbb{Z}_q$.
   (b) Vypočíta $r = g^k \pmod p$.
   (c) Vypočíta
   $$s = k^{-1}(h(m) + xr) \pmod q . \tag{1}$$
   Trojica (m, r, s) tvorí podpis správy m.
2. *Overenie podpisu.* Subjekt B podpis overí takto:
   (a) Vypočíta $w = s^{-1} \pmod q$ a $h(m)$.
   (b) Vypočíta $u_1 = w \cdot h(m) \pmod q$ a $u_2 = rw \pmod q$.

(c) Vypočíta $v = (g^{u_1} y_A^{u_2} \pmod p) \pmod q$.

(d) Podpis akceptuje jedine ak platí $v = r$.

Dizertačná práca sa zaoberá aj algoritmom AES, ktorý bol schválený ako šifrový štandard [FIPS197] v roku 2000. AES má jednoduchý algebraický popis. Na algoritmus zverejnili Courtois a Pieprzyk [CoP02] XSL útok vychádzajúci z toho, že S-box AES algoritmu je možné popísať viacerými kvadratickými booleovskými funkciami. Potom je možné zostrojiť sústavu kvadratických booleovských rovníc nad $GF(2)$ a jej riešením určiť kľúč.

Murphy a Robshaw [MuR02] zovšeobecnili algoritmus AES na nový algoritmus BES, v ktorom sa všetky operácie vykonávajú iba nad prvkami poľa $GF(2^8)$, namiesto bitovo reprezentovaných (tabulovaných) S-boxov. BES má 1024 bitový blok a rovnako dlhý kľúč. XSL útok je možné aplikovať aj na BES, pričom rovnice sú nad poľom $GF(2^8)$ a sústava rovníc je riedka. Aplikovateľnosť tohto útoku je však otázna. Výhodou je, že BES algoritmus má ešte jednoduchší algebraický popis ako AES.

V roku 1999 boli prezentované ďalšie dva systémy odvodzujúce svoju bezpečnosť (nepriamo) od DLP. Prvý bol GH systém, publikovaný autormi Gongovou a Harnom v práci [GoH98]. Druhý bol XTR systém publikovaný, Lenstrom a Verheulom v prácach [LeV00, LeV02]. Ich výhodou je, že pri rovnakej bezpečnosti ako u predchádzajúcich kryptografických schém, pracujú nad oveľa menšími algebraickými štruktúrami.

3 Ciele dizertácie

Úlohou predkladanej práce je podať samotnú problematiku DLP a algoritmy, ktoré je možné použiť na riešenie tohto problému.
Ďalšie ciele práce sú:

(i) uviesť kryptografické schémy, ktoré odvodzujú svoju bezpečnosť od skúmaného problému a ich rôzne známe modifikácie;

(ii) prezentovať známe vlastnosti 3 rôznych pologrúp matíc;

(iii) uviesť modifikáciu DSA podpisovej schémy na pologrupy matíc;

(iv) uviesť také modifikácie algoritmov na riešenie DLP, aby boli použiteľné aj nad pologrupami;

(v) uviesť možnú modifikáciu symetrického šifrovacieho algoritmu AES;

(vi) prezentovať poznatky o systémoch GH a XTR a preskúmať frekvenčné vlastnosti postupností, ktoré sú nimi generované.

V neposlednom rade, je cieľom podať aj súčasný stav našej legislatívy týkajúcej sa digitálnych podpisov, ktoré využívajú aj algoritmy založené na DLP.

4 Výsledky dizertačnej práce

Dosiahnuté výsledky sme rozdelili do troch podkapitol, ktoré z dôvodu ucelenosti autoreferátu presne nezodpovedajú členeniu dizertačnej práce. Takisto niektoré z literatúry známe výsledky uvádzame kvôli súvislosti výkladu až v tejto časti. Pri každom novom výsledku je kvôli referencii uvedené aj jeho číslo v dizertačnej práci.

4.1 Podpisová schéma na maticiach

Východiskom pre matematické rovnice potrebné na overenie digitálneho podpisu je zovšeobecnená Euler-Fermatova veta pre pologrupy.

Definícia 4.1. *Nech S je konečná pologrupa a definujme K, D a R nasledujúcim spôsobom:*

$$K = \max\{k(x) \mid x \in S\} \tag{2}$$
$$D = \operatorname{lcm}\{d(x) \mid x \in S\}, \tag{3}$$

a R je jednoznačne určené číslo také, že $K \leq R < K + D$ a $D|R$.

Veta 4.2 (Euler-Fermatova veta pre konečné pologrupy [Sch70]). *Pre každé $x \in S$ a K, D, R definované vyššie platí*

$$x^{K+D} = x^K$$

a x^R je idempotentný prvok. Naviac K, D a R sú najmenšie čísla majúce takéto vlastnosti.

Čísla K, D a R sa nazývajú univerzálne exponenty pologrupy a sú známe iba pre obmedzený počet používaných pologrúp. Ich hodnoty pre 3 špeciálne pologrupy matíc sú uvedené v nasledujúcich vetách.

Symbolom B_Ω označujeme pologrupu booleovských matíc typu $n \times n$. Sú to matice s prvkami 0,1, kde platia nasledujúce pravidlá počítania: $0 + 0 = 0$, $0 + 1 = 1 + 0 = 1 + 1 = 1$ a $0.0 = 0.1 = 1.0 = 0$ a $1.1 = 1$. Univerzálne exponenty K, D pre túto pologrupu udávajú nasledujúce 2 vety.

Veta 4.3 (Schwarz, [Sch74]). *Pre pologrupu B_Ω booleovských matíc typu $n \times n$ platí $K = (n-1)^2 + 1$. Toto maximum sa dosahuje napríklad pre Wielandtove matice.*

Veta 4.4 (Schwarz [Sch80], Ecker [Eck83]). *Nech $n = n_1+n_2+\ldots+n_k$ je partícia čísla n. Potom v pologrupe booleovských matíc je $D = \max \mathrm{lcm}(n_1, n_2, \ldots, n_k)$, kde maximum sa berie cez všetky možné partície čísla n. Inak povedané, D je najväčší rád prvku symetrickej grupy permutácií n prvkov.*

Symbolom $\mathcal{M}_n$ označujeme pologrupu matíc typu $n \times n$ s prvkami z okruhu $\mathbb{Z}_m$. Symbolom $p\{n\}$ pre ľubovoľné čísla prirodzené p, n označme hodnotu minimálnu hodnotu z postupnosti $1, p, p^2, p^3, p^4, \ldots$, pre ktorú je $p^t \geq n$. Univerzálne exponenty K, D udáva nasledujúca veta.

Veta 4.5 (Davis, [Dav51]). *Nech $m = p_1^{\alpha_1} \ldots p_s^{\alpha_s}$ je ľubovoľné prirodzené číslo s rôznymi prvočíslenými deliteľmi $p_1, \ldots, p_s$ a*

$$\lambda_i(n) = p_i\{n\}\mathrm{lcm}(p_i^n - 1, p_i^{n-1} - 1, \ldots, p_i - 1), \quad i = 1, 2, \ldots, s. \tag{4}$$

Ďalej nech

$$D_N = \mathrm{lcm}(\lambda_1(n)p_1^{\alpha_1-1}, \ldots, \lambda_s(n)p_s^{\alpha_s-1}). \tag{5}$$

Potom pre každú $n \times n$ maticu $A \in \mathcal{M}_n$, ktorej determinant je nesúdeliteľný s m (teda A je nesingulárna matica) platí

$$A^{D_N} = I,$$

a $D = D_N$ je najmenší kladný exponent, ktorý má túto vlastnosť.

Nech S_n označuje pologrupu matíc typu $n \times n$ s prvkami z poľa $GF(q)$. Potom univerzálne exponenty pre túto pologrupu udáva nasledujúca veta.

Veta 4.6 (Schwarz, [Sch85]).

1. *Nech $A \in S_n$ je ľubovoľná matica typu $n \times n$ s rádom $rank(A) = h, h < n$. Potom*

   $$A^{h+1} = A^{h+1+\lambda(h)}$$

   a toto je najlepší možný výsledok.

2. *Nech $A \in S_n$ je ľubovoľná $n \times n$ matica s rádom $rank(A) < n$. Potom*

   $$A^n = A^{n+\lambda(n-1)},$$

   a toto je najlepší možný výsledok.

3. *Pre ľubovoľnú maticu $A \in S_n$ platí*

   $$A^n = A^{n+\lambda(n)},$$

   a je to najlepší možný výsledok. Z toho vyplýva, že $K = n$, $D = \lambda(n) = p\{n\}\mathrm{lcm}(q^n - 1, q^{n-1} - 1, \ldots, q - 1)$.

Všetky matice uvedené v podpisovej schéme budú patriť k pologrupe $\mathcal{S}$, ktorá bude označovať jednu pevne zvolenú pologrupu z pologrúp $B_\Omega, \mathcal{M}_n$ alebo S_n (alebo ľubovoľnú inú pologrupu so známymi univerzálnymi exponentami). Použité hodnoty k a d označujú univerzálne exponenty zvolenej pologrupy $\mathcal{S}$.

Algoritmus 4.7 (Algoritmus 4.15) Nová podpisová schéma pre pologrupu

---

Subjekt A podpisuje binárnu správu m ľubovoľnej dĺžky a má zvolené číslo $1 \leq x_A < d$ ako tajný kľúč. A zverejní hodnoty $G \in \mathcal{S}, W(= G^k), X_A(= G^{x_A}), d(= d(G))$ ako svoj verejný kľúč, kde h je vhodná funkcia $h : \{0,1\}^* \to \langle 0, d)$, f je funkcia, ktorá matice zobrazuje na bitové reťazce, teda $f : \mathcal{S} \to \{0,1\}^*$. Parametre G, W, d, k, h, f môžu byť zvolené dôveryhodnou treťou stranou a spoločné pre celú doménu subjektov.

1. *Podpísanie správy.* Subjekt A musí vykonať nasledujúce kroky:
   (a) Zvolí náhodné tajné číslo s, $1 \leq s \leq d-1$, pre ktoré platí $\gcd(s, d) = 1$.
   (b) Vypočíta $Y = G^s, h(m)$.
   (c) Vypočíta $a = h(f(Y))$. Ak $a = 0$ potom sa vráti ku kroku (a).
   (d) Nájde číslo b také, že platí
   $$h(m) = x_A a + sb \pmod{d}. \tag{6}$$
   (e) Dvojica (Y, b) je podpisom subjektu A pre správu m.
2. *Overenie podpisu.* Na verifikáciu podpisu (Y, b) subjektu A správy m musí B vykonať nasledujúce kroky:
   (a) Získa autentifikačný verejný kľúč W, X_A, d, f, h subjektu A, má správu m a podpis (Y, b).
   (b) Vypočíta $h(m), a = h(f(Y))$.
   (c) Vypočíta $V_1 = WX_A^a Y^b (= G^{k+ax+sb})$.
   (d) Vypočíta $V_2 = WG^{h(m)} (= G^{k+h(m)})$.
   (e) Podpis akceptuje práve vtedy, keď platí $V_1 = V_2$.

Korektnosť schémy ľahko vidieť zo vzťahu (6). Funkcia f môže matici priradiť reťazec bitov napríklad tak, že berie postupne prvky matice ako bitové reťazce a tieto reťazce ukladá za sebou. Funkcia h môže byť hašovacia funkcia, napríklad SHA-1. Táto podpisová schéma sa od DSA podpisovej schémy líši zakomponovaním predperiódy potrebnej pre počítanie v pologrupe.

Z vlastností jednotlivých pologrúp vyplývajú možnosti ich použitia v praxi. Použitie booleovských matíc je nepraktické kvôli ich veľkosti, ak chceme, aby

bola zachovaná bezpečnosť. Matice nad konečným poľom $GF(q)$ sú z hľadiska bezpečnosti ekvivalentné podpisovej schéme používajúcej konečné pole, ktoré je malým rozšírením poľa $GF(q)$. Použiteľné sú teda matice modulo m a matice nad konečným poľom. Na rozdiel od RSA schémy sú pomalšie, dokážu však naraz spracovať väčší objem údajov. Podrobná analýza je uvedená v článku [GrS02].

4.2 Modifikácia AES algoritmu

Jedna z operácií algoritmu AES je operácia `mixColumn`, ktorá je lineárnym zobrazením bloku šifry a dá sa reprezentovať násobením 4-bytového bloku, zapísaného ako stĺpec, cirkulantnou maticou

$$A = \begin{pmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{pmatrix}.$$

Kritériá kladené na túto maticu boli:

1. *invertibilnosť* - k transformácii musí existovať inverzná transformácia,
2. *symetria* - transformácia musí byť symetrická pre všetky stĺpce,
3. *rozmery* - transformácia mieša 4 bytové stĺpce,
4. *linearita* - transformácia musí byť lineárna nad $GF(2)$,
5. *difúzia* - musí mať dostatočnú difúziu, t.j. diferenciálne vetvenie podľa definície uvedenej v [DaR02] je rovné 5,
6. *rýchlosť* - musí sa dať vykonať dostatočne rýchlo na 8-bitových procesoroch.

Ak $\mathbb{F}$ označuje pole $GF(2^8)$, Murphy a Robshaw [MuR02] ukázali, že AES možno vnoriť do poľa $\mathbb{F}^{128}$. Potom sa všetky operácie vykonávajú iba nad prvkami poľa $\mathbb{F}$, namiesto bitovo reprezentovaných (tabulovaných) S-boxov. Šifru, ktorá takto vznikne nazvali BES. Matica A má rád 4, čo je príčinou aj algebraickej jednoduchosti algoritmu BES a existencie hypoteticky ľahšieho útoku naň.

Preto sme algoritmus AES modifikovali tak, že sme zamenili `mixColumn` maticu inou invertibilnou maticou spĺňajúcou kritériá 1. až 5. s mierne horším výsledkom pre 6. a pridáme navyše ďalšie kritérium:

7. *vysoký rád matice* - rád matice rovný aspoň počtu kôl AES algoritmu, ktorý je 10, 12, alebo 14 kôl v závislosti od parametrov algoritmu.

Nová `mixColumn` matica je

$$C = \begin{pmatrix} 02 & 05 & 01 & 01 \\ 01 & 02 & 05 & 01 \\ 01 & 01 & 02 & 05 \\ 05 & 01 & 01 & 02 \end{pmatrix}$$

a zodpovedá polynómu $05x^3+01x^2+01x+02$ nad poľom $GF(2^8)$. Jej diferenciálne vetvenie je 5. Rád matice C je 340, teda matica spĺňa nové kritérium. Nevýhodou jej použitia je, že operácia dešifrovania k nej inverznou maticou je približne o 7/25-krát pomalšia ako v prípade použitia matice inverznej k matici A.

4.3 DLP v XTR a GH systémoch

Oba systémy využívajú polynóm $f(x)$ tretieho stupňa ireducibilný nad poľom $GF(q)$ a s koreňom $\alpha \in GF(q^3)$. $f(x)$ je možné brať ako charakteristický polynóm LFSR. Ten potom generuje postupnosť, ktorej členy je možné matematicky vyjadriť ako

$$s_k = Tr_{E/F}(\alpha^k) = \alpha^k + \alpha^{kq} + \alpha^{kq^2}, \quad k = 0, 1, 2, \ldots. \tag{7}$$

Systémy sú navrhnuté tak, že počítajú efektívne iba v poli $GF(q)$ bez nutnosti počítania v poli $GF(q^3)$. XTR systém používa $q = p^2$, kde p je prvočíslo.

Pre charakteristické postupnosti sme zaviedli nový typ problému diskrétneho logaritmu. Nech $\mathbb{F}$ je konečné pole s q prvkami a prvočíselnou charakteristikou p, označme jeho konečné rozšírenie ako $\mathbb{E} = GF(q^n)$ a majme nejakú funkciu $f : \mathbb{E} \to \mathbb{F}$.

Problém 4.8 (Problém 5.9). *Nech $G \subset \mathbb{E}$ je multiplikatívna podgrupa generovaná prvkom $g \in \mathbb{E}$. Pre dané $x \in \mathbb{F}$ problém nájdenia množiny všetkých exponentov i, $0 \leq i < |G|$ takých, že platí $f(g^i) = x$ budeme nazývať f-DLP. Množinu všetkých exponentov i, ktoré spĺňajú predchádzajúcu rovnicu označujeme $\log_g(x)$. $\log_g$ je vo všeobecnosti relácia, podmnožina kartézskeho súčinu $\mathbb{F} \times \mathbb{Z}_{|G|}$.*

Ak by nejaké množiny dikrétnych logaritmov boli omnoho väčšie ako iné, bolo by možné "hádať" členy postupnosti, a tak útočiť na schémy využívajúce GH alebo XTR systémy.

Nech $s_0, s_1, s_2, \ldots$ je charakteristická postupnosť generovaná systémom GH alebo XTR podľa vzťahu (7) a má periódu r. Nech $Z_s(b)$ označuje počet výskytov prvku $b \in GF(q)$ medzi prvými r prvkami tejto postupnosti. Nasledujúce vety dávajú ohraničenia hodnôt $Z_s(b)$.

Veta 4.9 (Veta 5.11). *Nech $\{s_k\}_{k\geq 0}$ je GH charakteristická postupnosť nad poľom $GF(q)$ s periódou $r = q^2 + q + 1$ pre $q \geq 2$ a $b \in GF(q) \setminus \{0\}$. Ak* $\gcd(q^2 + q + 1, q - 1) = 1$, *potom platí*

$$Z(0) = q + 1 \tag{8}$$

$$\left| Z(b) - (q+1) - \frac{1}{q-1} \right| \leq q - 1 - \frac{1}{q-1}, \tag{9}$$

ak $\gcd(q^2 + q + 1, q - 1) = 3$, *potom platí*

$$|Z(0) - (q+1)| \leq 2q^{1/2} \tag{10}$$

$$|Z(b) - (q+1)| \leq q + 3, \tag{11}$$

Pre XTR postupnosti je možné získať ohraničenia podobným spôsobom. Pre nenulové prvky postupnosti je však odhad zhodný s triviálnym ohraničením - periódou.

Veta 4.10 (Veta 5.12). *Pre XTR charakteristickú postupnosť s periódou* $r|(p^2 - p + 1)$ *a* b *ľubovoľný nenulový prvok* $GF(q) \setminus \{0\}$ *platí*

$$\left| Z(0) - \frac{r}{p^2 - 1} \right| \leq p \tag{12}$$

$$\left| Z(b) - \frac{p^4 r}{p^6 - 1} \right| \leq p^2 \tag{13}$$

Ak máme zvolené dva rôzne charakteristické polynómy postupností a ich korene majú rovnaký rád, potom nasledujúca veta a dôsledok hovoria, že rovnaké prvky v postupnostiach síce môžu byť na rôznych miestach, ale počty ich výskytov sú v oboch postupnostiach rovnaké.

Veta 4.11 (Veta 5.14). *Pre ľubovoľné* $a \in GF(q)$ *a všetky prvky* β, $\gamma \in GF(q^3)$ *také, že majú rovnaký rád* $\mathrm{ord}(\beta) = \mathrm{ord}(\gamma)$ *platí*

$$\left| \{i \,|\, Tr(\beta^i) = a\} \right| = \left| \{j \,|\, Tr(\beta^j) = a\} \right|$$

Priamy dôsledok tejto vety je nasledujúci.

Dôsledok 4.12. *Nech* $\{s_k\}_{k \geq 0}$ *a* $\{t_k\}_{k \geq 0}$ *sú dve charakteristické postupnosti 3. rádu (GH alebo XTR char. postupnosti) nad tým istým poľom* $GF(q)$ *s rovnakou periódou. Potom ich frekvenčné vlastnosti nezávisia na výbere charakteristických polynómov (pre polynómy s periódou rovnou perióde postupnosti) a pre všetky prvky* $a \in GF(q)$ *platí* $Z_s(a) = Z_t(a)$.

Jedným z dôležitých kritérií kryptografickej odolnosti sú hodnoty autokorelačnej funkcie postupnosti. Autokorelačná funkcia postupnosti $\{s_k\}_{k \geq 0} = s_0, s_1, \ldots$ nad poľom $\mathbb{F}$ s periódou N je definovaná ako

$$AC_s(l) = \sum_{i=0}^{N-1} \chi(s_i - s_{i+l}),$$

kde χ je tzv. kanonický aditívny charakter s hodnotami

$$\chi(g) = \exp\left(\frac{2\pi i}{p} Tr_{F/K}(g)\right)$$

a $\mathbb{K}$ je prvopole poľa $\mathbb{F}$.

Pre GH postupnosti je možné odvodiť nasledujúci odhad. Pre XTR postupnosti odhad nie je odvodený, opätovne z dôvodu, že ich perióda je menšia ako p^3.

Veta 4.13 (Veta 5.18). *Pre ľubovoľnú GH charakteristickú postupnosť* $\{s_k\}_{k\geq 0}$ *platí*

$$AC_s(l) \leq p^3$$

pre každé $l \neq 0$.

Uskutočnili sme niekoľko testov, aby sme zistili správanie sa GH a XTR postupností na malých inštanciách týchto systémov a porovnali ho s teoreticky očakávanými hodnotami podľa viet 4.9 a 4.10. Testy boli implementované v jazyku C++ a bola využitá Shoupova knižnica NTL [NTL].

Z testov pre XTR postupnosti vyplynula nasledujúca hypotéza.

Hypotéza 4.14 (Hypotéza 5.19). *Pre XTR charakteristické postupnosti platí* $Z(3) = 1$ *a* $Z(b) \in \{0, 3\}$ *pre každé* $b \in GF(p^2)$, $b \neq 3$.

Pre GH postupnosti sme našli postupnosť, ktorá dosahuje horné ohraničenie vo vzťahoch vety 4.9 pre počet výskytov prvku 0 v postupnosti. Z toho vyplýva, že tento odhad nemožno vo všeobecnosti vylepšiť.

5 Závery pre ďalší rozvoj disciplíny

Hlavnými výsledkami práce sú:

- digitálna podpisová schéma na pologrupách
- návrh modifikácie algoritmu AES
- zistenie frekvencií výskytov prvkov v postupnostiach GH a XTR systémov

Práca sa zaoberala vlastnosťami systémov, ktoré sú z kryptografického hľadiska nové a málo prebádané (AES je štandardom 2 roky a GH a XTR sú verejne publikované 3 roky). Preto v týchto oblastiach stále prebieha intenzívny výskum.

Zdá sa, že trend vývoja systémov s verejnými kľúčmi smeruje k systémom so zložitejšou algebraickou štruktúrou, ktorá však umožňuje používať menšie kľúče. Oproti tejto praktickej výhode sa objavuje nevýhoda ťažšej kryptoanalýzy takýchto kryptosystémov. Naopak, v prípade symetrických šifier sa začínajú používať jednoduché algebraické operácie (viď AES, predtým IDEA).

Referencie

[AbS70] M. Abramowitz, I.A. Stegun (eds): Handbook of Mathematical Functions. Dover, New York 1970.

[BBL95] D. Bleichenbacher, W. Bosma, A. K. Lenstra: Some remarks on Lucas based cryptosystems, Advances in Cryptology-CRYPTO '95, pp. 386-396, 1995.

[CoP02] N. Courtois, J. Pieprzyk: Cryptanalysis of Block Ciphers with Overdefined Systems of Equations, Proceedings of Asiacrypt'02, Lecture Notes in Computer Science, Springer-Verlag, 2002.

[CDR98] T. Cusick, C. Ding, A. Renvall: Stream Ciphers and Number Theory. Elsevier, 1998.

[DaR02] J. Daemen, V. Rijmen: The Design of Rijndael. AES - The Advanced Encryption Standard, Springer-Verlag, 2002.

[DaR99] J. Daemen, V. Rijmen: The Rijndael Block Cipher, AES Proposal: Rijndael, 1999

[Dav51] R.M. Davis: The Euler–Fermat theorem for matrices. Duke Math. J., 18, 1951, pp. 613–617.

[Dif88] W. Diffie: The First Ten Years of Public Key Cryptography, Proceedings of the IEEE, v. 76, n. 5, pp. 560-577, May 1988.

[DiH76] W. Diffie, M. E. Hellman: New directions in cryptography, IEEE Trans. Inform. Theory, IT-22, pp. 644-654, 1976.

[Eck83] A. Ecker: Finite semigroups and the RSA-cryptosystem. EuroCrypt'82, LNCS 149, Springer-Verlag, pp. 353–369, 1983.

[FIPS186] National Institute of Standards and Technology, NIST FIPS PUB 186, "Digital Signature Standard," U.S. Department of Commerce, May 1994.

[FIPS197] National Institute of Standards and Technology, NIST FIPS PUB 197, "Advanced Encryption Standard," U.S. Department of Commerce, 26th november 2001.

[Gan88] F.R. Gantmacher: The Theory of Matrices, Volumes I. and II. Chelsea, New York, 1959. (In Russian: 4th edition, Naukha, Moscow, 1988.)

[GiG00] K. Giuliani, G. Gong: Generating Large Instances of the Gong-Harn Cryptosystem

[GoH98] G. Gong, L. Harn: A new approach on public key distribution, ChinaCRYPT '98, pp. 50-55, 1998.

[GoH99] G. Gong, L. Harn: Public-Key Cryptosystems Based on Cubic Finite Field Extensions, IEEE Transactions on information theory, vol. 45, No. 7, Nov 1999.

[GHW01] G. Gong, L. Harn, H. Wu: The GH Public-Key Cryptosystem, Lecture Notes in Computer Science, vol. 2259, pp. 284, 2001.

[HMP94] P.Horster, M.Michels, H.Petersen: Meta-ElGamal signature schemes, Proc. 2. ACM conference on Computer and Communications security, Fairfax, Virginia, pp. 96 – 107, 2.-4. Nov 1994.

[ECDSA] D. Johnson, A. Menezes: The Elliptic Curve Digital Signature Algorithm (ECDSA), Tech. Report CORR 99-34, Dept. of C&O, Univ. of Waterloo, Canada, Feb 24, 2000.

[Jun92] D. Jungnickel: Finite Fields. Structure and Arithmetics, Wissenschaftverlag, 1992.

[Knu2] D. E. Knuth: The Art of Computer Programming, Volume 2 - Seminumerical Algorithms, Addison-Wesley Longman, 3rd edition, pp. 379-417, 1998.

[Knu3] D. E. Knuth: The Art of Computer Programming, Volume 3 - Sorting and Searching, Addison-Wesley Reading, Massachussets, 1973.

[LmO91] B. A. LaMacchia, A. M. Odlyzko: Computation of discrete logarithms in prime fields, Designs, Codes and Cryptography 1 (1991), pp. 47-62, 1991.

[LaP96] M. Laššák, Š. Porubský: Fermat–Euler theorem in algebraic number fields. J. Number Theory 60, pp. 254–290, 1996.

[LeV00] A. K. Lenstra, E. R. Verheul: The XTR public key system, Advances in Cryptology - Crypto 2000, Lecture Notes in Computer Science 1880, pp. 1-20, Springer-Verlag 2000.

[LeV02] A. K. Lenstra, E. R. Verheul: An overview of the XTR public key system, The proceedings of the Public Key Cryptography and Computational Number Theory Conference 2002.

[LiN86] R. Lidl, H. Niederreiter: Introduction to finite fields and their applications. Oxford University Press, 1986.

[LiN97] R. Lidl, H. Niederreiter: Finite Fields, Cambridge University Press, Cambridge, 1997.

[Maple] Maple 7.00, Waterloo Maple Inc.

[Mar41] I. B. Marshall: On the extension of Fermat's theorem to matrices of order n, Proceedings of the Edinburgh Math. Soc. 6, pp. 85-91, 1939-41.

[Max51] M.W. Maxfield: The order of a matrix under multiplication (modulo m). Duke Math. J. 18, pp. 619–621, 1951.

[McC90] K. S. McCurley: The discrete logarithm problem, Cryptography and Computational Number Theory, editor C. Pomerance, Proc. Symp. Appl. Math. 42, pp. 49-74, 1990.

[Men93] A. Menezes: Elliptic Curve Public Key Cryptosystems, Kluwer Academic Publishers, ISBN 0-7923-9368-6, 1993.

[MeWu98] A. Menezes, Yi-Hong Wu: The Discrete Logarithm Problem in $GL(n, q)$. Ars Combinatoria 47, pp. 23–32, 1998.

[MOV96] A. Menezes, P. van Oorschot and S. Vanstone: Handbook of Applied Cryptography. CRC Press, Inc. 1996.

[MNP96] M. Michels, D. Naccache, H. Petersen: GOST 34.10 - A Brief Overview of Russia's DSA, Computers & Security 15(8):725:732, 1996.

[MoMo66] J. W. Moon and L. Moser, Almost all (0,1) matrices are primitive, Studia Scientiarum Mathematicarum Hungarica 1 (1966), 153-156, 1966.

[MuR02] S. Murphy, M. J. B. Robshaw: Essential Algebraic Structure within the AES, CRYPTO 2002, LNCS 2442, pp. 1–16, Springer-Verlag, 2002.

[Niv48] I. Niven: Fermat's theorem for matrices. Duke Math. J. 15, pp. 823–826, 1948.

[NTL] V. Shoup: "NTL: A library for doing Number Theory", *http://shoup.net/ntl*

[NyR94] K. Nyberg, R. Rueppel: Message recovery for signature schemes based on the discrete logarithm problem, LNCS 950, Advances in Cryptology: Proc. Eurocrypt '94, Springer, pp. 182 – 193, 1994.

[Odl84] A. M. Odlyzko: Discrete logarithms in finite fields and their cryptographic significance, in Lecture Notes in Computer Science 209, pp. 224–316, Springer-Verlag, Berlin, 1984.

[Odl00] A. M. Odlyzko: Discrete logarithms: The past and the future. Designs, Codes, and Cryptography, 19:129-145, 2000.

[PoH78] Pohlig S.C., M. Hellman: An improved algorithm for computing logarithms over *GF(p)* and its cryptographic significance, pp. 106-110, IEEE Trans. Inform. Theory IT-24, 1978.

[Pol78] J. Pollard: Monte Carlo methods for index computations (mod p), Math. Comp. 32, pp. 106-110, 1978.

[Rue86] R. A. Rueppel: Design and Analysis of Stream Ciphers. Springer–Verlag, 1986.

[Schn96] B. Schneier: Applied Cryptography Second Edition: protocols, algorithms, and source in C, John Wiley & Sons, 1996.

[Sch70] Š. Schwarz: On the Semigroup of Binary Relations on a Finite Set. Czech. Math. J. 20(95), pp. 632-679, 1970.

[Sch74] Š. Schwarz: Sums of powers of Binary Relations. Mat. Čas. 2(24), pp. 161–171 (in Russian), 1974.

[Sch80] Š. Schwarz: The Euler-Fermat Theorem for the Semigroup of Circulant Boolean Matrices, Czechoslovak Mathematical Journal, 1980.

[Sch85] Š. Schwarz: Fermat's Theorem for Matrices Revisited. Math. Slovaca 4(35) 1985, pp. 343–347.

[Sho97] V. Shoup: Lower bounds for discrete logarithms and related problems. Proc. Eurocrypt'97, LNCS 1233 (1997), Springer Berlin, pp. 256–266. 1997.

[Shp00] I. E. Shparlinski, On the generalized hidden number problem and bit security of XTR, Preprint, pp. 1–14, 2000.

[Sim93] G. J. Simmons: Subliminal Channels of the U.S. Digital Signature Algorithm (DSA), Proc. of the Third Symposium on: State and Progress of Research in Cryptography, Rome, pp. 33–54, 1993.

[Sim94] G. J. Simmons: Subliminal Communication is Easy Using the DSA, EUROCRYPT '93 Proceedings, Springer-Verlag, pp. 218–232, 1994.

[Tes01] E. Teske. Square-root algorithms for the discrete logarithm problem (a survey). In Public Key Cryptography and Computational Number Theory, Walter de Gruyter, pp. 283-301, 2001.

[VaO85] V. Varadharajan, R. Odoni: Extension of RSA Cryptosystems to Matrix Rings. Cryptologia 2(9), pp. 140–153, 1985.

[Var85] V. Varadharajan: Trapdoor rings and their use in cryptography. Advances in Cryptology - CRYPTO '85, LNCS 218, Springer-Verlag, pp. 369–395, 1986.

[Ver00] E. Verheul: Certificates of Recoverability with Scaleable Recovery Agent Security. In Proceedings of PKC2000, LNCS 1751. Springer-Verlag, 2000.

6 Zoznam prác dizertanta

6.1 Zoznam prác dizertanta priamo súvisiacich z dizertačnou prácou

[GS02] O. Grošek, J. Šiška: Signature schemes based on matrices. Accepted for publication in Congressus Numerantium. (2002), pp. 154-159.

[GrS02] O. Grošek, J. Šiška: Signature schemes based on matrices. Abstracts of the 33rd Southeastern International Conference on Combinatorics, Graph Theory and Computing, Florida Atlantic University, March 4-8, 2002, p. 87.

[GrS03a] O. Grošek, J. Šiška: Semigroup of matrices over $GF(2^s)$ and its relation to AES. 8 pages. Submitted to PU.M.A – Pure Mathematics and Applications, Budapest, Sien.

[GrS03b] O. Grošek, J. Šiška: Frequentative properties of GH and XTR schemes. 8 strán, zaslané do Mathematica Slovaca.

6.2 Zoznam ďalších prác dizertanta

[Sis02] J. Šiška: Aplikácie booleovských funkcií na polenej hyperkocke, rigorózna práca, FMPHI UK, Bratislava, 2002.

[HlS98] L. Hluchý, J. Šiška: Parallel Algoritmhs of an Object Reconstruction for 3D X-ray Tomography, Modeling and Simulation of Systems MOSIS 1998, Sv.Hostýn-Bystrice pod Hostýnem, pp. 237-242, ISBN 80-85988-23-2, 1998.

[HlS97a] L. Hluchý, J. Šiška: Počítačová simulácia tomografie v distribuovanom prostredí ASIS 97 - Advanced Simulation of Systems, XIXth International Workshop, Krnov, pp. 393-401, ISBN 80-85988-20-8, 1997.

[HlS97b] L. Hluchý, J. Šiška: Počítačová simulácia tomografie v distribuovanom prostredí Proc. of Modelling and Simulation in Management and Control, Súľov, pp. 89-97, 1997.

[GHS97a] M. Gažák and L. Hluchý, J. Šiška: WaTor - neregulárny distribuovaný simulačný problém a jazyk Java Proc. of Modelling and Simulation in Management and Control, Súl'ov, pp. 78-83, 1997.

[GHS97b] M. Gažák, L. Hluchý, J. Šiška: WaTor - neregulárny distribuovaný simulačný problém a jazyk Java ASIS 97 - Advanced Simulation of Systems, XIXth International Workshop, Krnov, pp. 387-392, ISBN 80-85988-20-8, 1997.

7 Summary

A discrete logarithm problem (DLP) is one of the supposed to be hard problems used in cryptography. The first cryptosystem based on DLP was Diffie-Hellman's key exchange scheme published in 1976. Since then, this problem was also used to involve digital signature schemes, such as ElGamal, DSA, ECDSA or GOST 34.10 [MNP96], and some encryption schemes. They utilize various algebraic structures like general groups, finite fields or elliptic curves. The main goal of this thesis is to show some of possible generalizations – especially using framework of DSA, and changing underlying group to semigroup, or change of equations. It also deals with some fast and memory efficient cryptosystems like GH and XTR.

First three chapters of the thesis introduce the DLP itself, and some basic facts about it. In the second chapter there are shown known algorithms solving the DLP, such as Shanks', Pollard's rho and Pohlig-Hellman's generic algorithms, and index calculus algorithm respectively. These algorithms put constraints on the sizes of parameters of cryptographic algorithms. DH scheme, ElGamal, DSA, and ECDSA respectively are presented in the third chapter. That chapter contains some of possible known modifications of these algorithms. It also presents state of the art of the Slovak legislative for digital signatures.

The core of the thesis is put into chapters 4 and 5. The fourth chapter deals with a new digital signature scheme on a semigroup of matrices. The generalized Euler-Fermat theorem is needed, and it uses a concept of so called universal exponent. Known values of the universal exponents are given for three special semigroups: 1. boolean matrices, 2. matrices over the ring modulo m, 3. matrices over the finite field $GF(q)$. We introduce a modification of DSA on these semigroups. This modification utilizes universal preperiod needed in the generalized Euler-Fermat theorem. The second chapter's algorithms solve DLP on groups only. We present their modifications in such a way that they are able to work on any semigroup.

As a side result of universal exponents, we propose another criterion for the selection of a matrix in the `mixColumn` operation in the new enciphering standard AES. This criterion is connected with the order of the used circulant matrix. We suggest to replace it with another matrix.

The fifth chapter deals with GH and XTR systems proposed in 1999. After a brief description as the 3rd order linear feedback shift registers we describe them as a DLP problem. It is known that these systems allow to build up cryptographic schemes like DH scheme, various digital signature algorithms, and a modification of RSA. Here we focus on occurrence of different elements of the sequences produced by these systems, and try to obtain a bound for number of elements in one period of GH and XTR sequences respectively. It seems, that XTR sequences have a very stable frequentative spectrum with maximum of 3 occurrences of an element in one period.

GH has also a quite stable spectrum, though number of occurrences of elements is higher to expected values. By experiments we found an instance of GH sequence

showing, that it is not possible to improve some of the obtained bounds. For GH sequences an upper bound for its autocorrelation function is obtained.