Ministerstvo financií
Slovenskej republiky

EFQM
Recognised for excellence
5 star - 2012

Súčasný stav v riešení faktorizácie a diskrétneho logaritmu

Marek Sýs

29. október 2014

KPMG
cutting through complexity™

Obsah

Kryptosystémy verejného kľúča

- Charakteristika.
- Ťažké výpočtové problémy

Generické metódy

- Metódy na faktorizáciu
- Metódy na riešenie diskrétneho logaritmu

Sitá číselných polí

- Kvadratické sito
- Index calculus
- Zložitosť
- Súčasný stav

PKC - Kryptosystémy verejného kľúča

Dešifrovanie so znalosťou tajnej informácie
- ťažký výpočtový problém

Problém faktorizácie - RSA, Rabinov

Problém diskrétneho logaritmu –
ElGamal, DSA, Eliptické krivky

Diffie-Hellman problém - Diffie-Hellman protokol

Ťažké výpočtové problémy

- Faktorizácia celých čísel:

  Pre celé číslo **n** = p.q nájdi p,q

- Diskrétny logaritmus

  Pre prvočíslo $\boldsymbol{p}$ a **g**,**h** z [1,**p**-1] nájdi x aby

  $$\boldsymbol{g}^{x} = \boldsymbol{h}\ mod\ \boldsymbol{p}$$

- Diffie-Hellman

  Pre prvočíslo **p** a $\boldsymbol{g}$, $\boldsymbol{g}^{\boldsymbol{x}}$, $\boldsymbol{g}^{\boldsymbol{y}}$ z [1,p-1] nájdi g^{xy}

Ťažké výpočtové problémy

- Faktorizácia celých čísel:

  Pre celé číslo **221** = p.q nájdi p,q

- Diskrétny logaritmus

  Pre prvočíslo $\boldsymbol{p}$ a **g**,**h** z [1,**p**-1] nájdi x aby

  $$\boldsymbol{g}^{x} = \boldsymbol{h}\ mod\ \boldsymbol{p}$$

- Diffie-Hellman

  Pre prvočíslo **p** a $\boldsymbol{g}$, $\boldsymbol{g}^{\boldsymbol{x}}$, $\boldsymbol{g}^{\boldsymbol{y}}$ z [1,p-1] nájdi g^{xy}

Ťažké výpočtové problémy

- Faktorizácia celých čísel:

  Pre celé číslo **221** = 13.17 nájdi p,q

- Diskrétny logaritmus

  Pre prvočíslo $\boldsymbol{p}$ a **g**,**h** z [1,**p**-1] nájdi x aby

  $$\boldsymbol{g}^{x} = \boldsymbol{h}\ mod\ \boldsymbol{p}$$

- Diffie-Hellman

  Pre prvočíslo **p** a $\boldsymbol{g}$, $\boldsymbol{g}^{\boldsymbol{x}}$, $\boldsymbol{g}^{\boldsymbol{y}}$ z [1,p-1] nájdi g^{xy}

Ťažké výpočtové problémy

- Faktorizácia celých čísel:

  Pre celé číslo **221** = 13.17 nájdi p,q

- Diskrétny logaritmus

  Pre prvočíslo $\boldsymbol{p}$ a **g**,**h** z [1,**p**-1] nájdi x aby

  $$\mathbf{2}^{x} = \mathbf{5}\ mod\ \mathbf{11}$$

- Diffie-Hellman

  Pre prvočíslo **p** a $\boldsymbol{g}$, $\boldsymbol{g^x}$, $\boldsymbol{g^y}$ z [1,p-1] nájdi g^{xy}

Ťažké výpočtové problémy

- Faktorizácia celých čísel:

  Pre celé číslo **221** = 13.17 nájdi p,q

- Diskrétny logaritmus

  Pre prvočíslo $\boldsymbol{p}$ a **g**,**h** z [1,**p**-1] nájdi x aby

  $$\mathbf{2}^{4} = \mathbf{5}\ mod\ \mathbf{11}$$

- Diffie-Hellman

  Pre prvočíslo **p** a $\boldsymbol{g}$, $\boldsymbol{g^x}$, $\boldsymbol{g^y}$ z [1,p-1] nájdi g^{xy}

Ťažké výpočtové problémy

- Faktorizácia celých čísel:

  Pre celé číslo **221** = 13.17 nájdi p,q

- Diskrétny logaritmus

  Pre prvočíslo $\boldsymbol{p}$ a **g**,**h** z [1,**p**-1] nájdi x aby

  $$\mathbf{2}^{4} = \mathbf{5}\ mod\ \mathbf{11}$$

- Diffie-Hellman

  Pre prvočíslo **p** a $(\boldsymbol{g}, \boldsymbol{g}^{\boldsymbol{x}}, \boldsymbol{g}^{\boldsymbol{y}})$ = (2,5,9) nájdi 2^{xy}

Ťažké výpočtové problémy

- Faktorizácia celých čísel:

  Pre celé číslo **221** = 13.17 nájdi p,q

- Diskrétny logaritmus

  Pre prvočíslo $\boldsymbol{p}$ a **g**,**h** z [1,**p**-1] nájdi x aby

  $$\mathbf{2}^{4} = \mathbf{5}\ mod\ \mathbf{11}$$

- Diffie-Hellman

  Pre prvočíslo **p** a (**2**, $\mathbf{2}^{4}$=**5**, $\mathbf{2}^{6}$=**9**) nájdi 2^{24}

Generické algoritmy

Generické – nevyužívajú špecifické vlastnosti grupy

Faktorizácia – Pollard Rho, Pollard p-1, Lenstrov alg.

Zložitosť: Pollard Rho $O(\sqrt{p})$

(p – najmenší faktor n)

DLP – Shanks, Pollard Rho, Pohlig-Hellman

Pohlig-Hellman + Pollard Rho

Zložitosť: $O(\sqrt{p})$

(p – najväčší faktor rádu grupy)

Voľba parametrov.

RSA – p,q také aby p-1 malo veľké faktory

p = 59, p – 1 = 29.2 (Sophie Germain)

DLP – $\boldsymbol{g}$ generátor grupy [1,…, p-1]

generátor grupy: M = { $\boldsymbol{g}^1$, $\boldsymbol{g}^2$,…, $\boldsymbol{g}^m$=1 }

$(Z_{11}, .)$ $\boldsymbol{g}$ = 2 2,4,8,16=5,10,9,7,3,6,1=$2^{\mathbf{10}}$

4 nieje 4,5,9,3,1= 2^5

(rád grupy teda 5 nie **10** !!!)

Kvadratické sito - základná myšlienka

$$a^2 = b^2 \mod n$$

n delí $a^2 - b^2 = (a-b).(a+b)$
$p.q$ delí $(a-b).(a+b)$

1. p, q delí $(a-b)$
2. len p delí $(a-b)$ tj. $gcd(a-b, n) = p$
   (Euklidov algoritmus)

Kvadratické sito - naivný prístup

$a_i = \sqrt{n} + i$

$a_i{}^2 \; mod \; n \quad ? = b^2$

"stačí" prehľadať
$[\sqrt{n}, (p+q)/2]$

(17+ 83)/2

a_i	$b_i = a_i{}^2 \; mod \; 1411$
38	33
39	110
40	189
41	270
42	353
43	438
44	525
…	
50	1089 = 33*33

Kvadratické sito – skladanie relácií

Cieľ: získať rovnosť $a^2 = b^2 \ mod\ n$

Možno použiť viaceré $\boldsymbol{b}_i$

$$a_i{}^2 = \boldsymbol{b}_i \ mod\ n \qquad 40^2 = 189\ mod\ 1411$$
$$a_j{}^2 = \boldsymbol{b}_j \ mod\ n \qquad 44^2 = 525\ mod\ 1411$$

$$a_i{}^2 . \ a_j{}^2 = \ \boldsymbol{b}_i . \boldsymbol{b}_j mod\ n \qquad 189.525 = 315^2$$

Kvadratické sito – skladanie relácií

Idea: rozložiť do malých prvočísel (prvočíselná báza **B**)

a vynásobiť vhodné

189 = 3.3.3.7

525 = 3.5.5.7

$189.525 = 3^4 5^2 7^2$

a_i	b_i	rozklad
38	33	3.11
39	110	2.5.11
40	189	3.3.3.7
41	270	2.3.3.3.5
42	353	
43	438	2.3.
44	525	3.5.5.7

Kvadratické sito – skladanie relácií

Idea: rozložiť do malých prvočísel (prvočíselná báza B)

a vynásobiť vhodné

189 = 3.3.3.7

525 = 3.5.5.7

189.525 = $3^4 5^2 7^2$

a_i	b_i	2	3	5	7	11
38	33		1			1
39	110	1		1		1
40	189		3		1	
41	270	1	3	1		
44	525		1	2	1	

Kvadratické sito – skladanie relácií

Idea: rozložiť do malých prvočísel (prvočíselná báza B)
a vynásobiť vhodné

189 = 3.3.3.7

525 = 3.5.5.7

$189.525 = 3^4 5^2 7^2$

33.110.189.270.525 =
$2^2 3^8 5^4 7^2 11^2$

a_i	b_i	2	3	5	7	11
38	33		1			1
39	110	1		1		1
40	189		3		1	
41	270	1	3	1		
44	525		1	2	1	

Báza

Prvočíselná báza B = {2,3,5,…, p_N}

Hľadáme len čísla $\boldsymbol{b}_i$ – rozložiteľné do prvočísel z B
(B-hladké čísla)

B= {2,3,5}

6 = 2.3 (B-hladké) 21 = 3.7 (nie je B-hladké)

Kvadratické sito – lineárna algebra

Hľadáme riadky matice M, ktorých súčet nám dá riadok s párnymi číslami.

Systém:

- xM = **0** mod 2

a_i	b_i
38	33
39	110
40	189
41	270
44	525

2	3	5	7	11
	1			1
1		1		1
	3		1	
1	3	1		
	1	2	1	

- riedky systém – málo $\boldsymbol{d}$ nenulových riadkov
  - Wiedemann, Block Lanczos O($\boldsymbol{d}.N^2$)

Kvadratické sito

Voľba prvočíselnej faktorovej bázy B = {2,3,5,…, p_N}
veľkosti N.

1. Hľadanie relácií -

   B-hladké $\boldsymbol{b}_i = {a_i}^2 \, mod \, n$ (preosievanie, sito)

   malé N ťažko nájsť B-hladké

   veľké N ľahko nájsť B-hladké

2. Lineárna algebra – riešenie sústavy mod 2

   – aspoň N relácií (zložitosť O($\boldsymbol{d}.N^2$))

Index calculus – základná myšlienka

Hľadáme x pre $\boldsymbol{g^x = h \; mod \; p}$

Pre

$$g^{a_i} = b_i \; mod \; p$$

hľadáme také $\boldsymbol{b_i}$ aby ich súčin bol h

$$g^{a_0+a_1} = b_0 b_1 = h \; mod \; p$$

x = $a_0 + a_1 \; mod \; p - 1$

Index calculus – základná myšlienka

Hľadáme x pre $\boldsymbol{g^x = h \; mod \; p}$ $\quad 2^x = 5 \; mod \; 11$

Pre

$$g^{a_i} = b_i \; mod \; p \qquad 2^8 = 3 \; mod \; 11$$

$$2^6 = 9 \; mod \; 11$$

hľadáme také $\boldsymbol{b_i}$ aby ich súčin bol h

$g^{a_0+a_1} = b_0 b_1 = h \; mod \; p$ $\quad 2^{14} = 3.9 = 5 \; mod \; 11$

x = $a_0 + a_1 \; mod \; p - 1$ $\quad$ x = 14 mod 10 =4

Index calculus - postup

Podobný – kvadratickému situ

Počítame $13^{x} = 11 \; mod \; 37$ pre B = {2,3,5,7}

1. Hľadanie relácií
   hladké $\boldsymbol{b}_i = g^{a_i} \; mod \; p$
2. Lineárna algebra
   počítanie DLP pre prvky bázy– $\boldsymbol{g}^{x} = p_i \; mod \; \boldsymbol{p}$
3. Počítanie individuálneho logaritmu pre $\boldsymbol{h}$

Index calculus – hľadanie relácií

Idea: Nájsť logaritmy prvkov bázy

$\boldsymbol{b}_i = g^{a_i} \; mod \; p$ $\qquad\qquad$ $\boldsymbol{b}_i = 13^{a_i} \; mod \; 37$

a_i	b_i
2	21
3	14
4	34
5	35
6	11
7	32

2	3	5	7
	1		1
1			1
1			
		1	1
5			

$13^2 = 3.7$ zlogaritmujem

2 = log(3)+log(7)

Index calculus – lineárna algebra

Cieľ: Výpočet DLP pre prvky faktorovej bázy B

Riedky systém:

- Mx = **a** mod p-1

log 2	log 3	log 5	log 7	a_i
	1		1	2
1			1	3
		1	1	5
5				7

Mx = **a** mod 36

x = (23,22,25,16)

tj. $2 = 13^{23}\ mod\ 37$

$3 = 13^{22}\ mod\ 37$

$5 = 13^{25}\ mod\ 37$

$7 = 13^{16}\ mod\ 37$

Index calculus – individuálny logaritmus

$2 = 13^{23}\ mod\ 37$ $\qquad$ $3 = 13^{22}\ mod\ 37$

$5 = 13^{25}\ mod\ 37$ $\qquad$ $7 = 13^{16}\ mod\ 37$

$$13^{x} = \mathbf{11}\ mod\ 37$$

$\boldsymbol{h} = 11$ sa nedá rozložiť do B (nie je B-hladké)

Vynásobíme prvkom z B a zistíme hladkosť

11.7 = 3 $\qquad$ tj. $\qquad$ log(11) = log(3) –log(7)

log(11) = 22 – 16 = 6

Sitá polí (Field sieve) - prehľad

Pracujú v iných štruktúrach –

ľahšie hľadanie B-hladkých čísel

Všeobecné číselné (GNFS)

Špeciálne číselné (SNFS) – vhodné pre špeciálne čísla

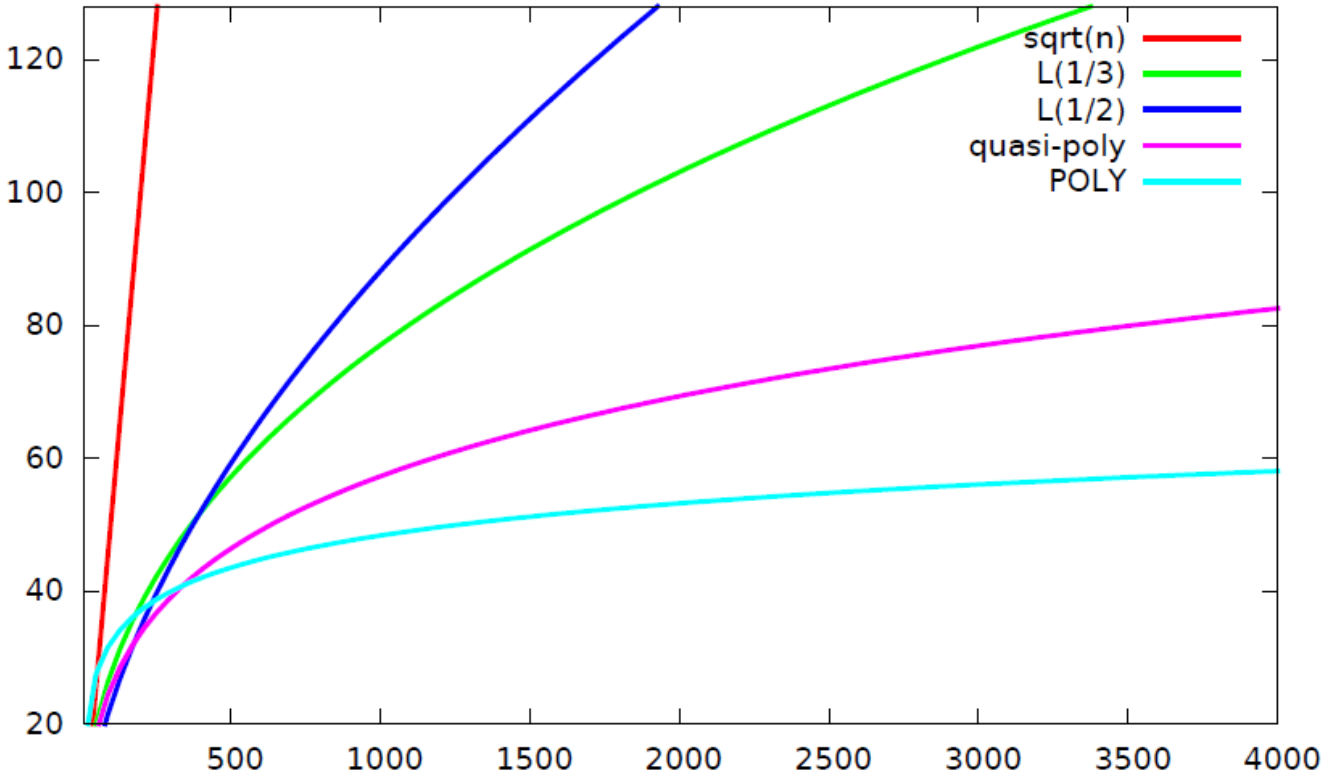
$$p^N - 1, p^N + 1$$

Násobné číselné (MNFS)

Funkčné (FFS)

Sitá – prehľad zložitosti

Zložitosť pre číslo n - L[a,c] = $e^{c\,(\log n)^{a}(\log\log n)^{1-a}}$



Sitá – prehľad zložitosti

Faktorizácia - L(1/3, 1.92) pre GNFS

Konečné polia – zovšeobecnenie poľa Z_p

DLP – malá charakteristika poľa - L(1/3, 1.52)
stredná charakteristika - L(1/3, 2.42)
veľká charakteristika - L(1/3, 1.92)

Faktorizácia rekordy

Číslo	číslic	Dátum	čas	Sito
C158	158	2002	3.4 CPU rokov	GNFS
RSA-160	160	2003	2.7 CPU rokov	GNFS
RSA-576	174	2003	13.2 CPU rokov	GNFS
C176	176	2005	48.6 CPU rokov	GNFS
RSA-200	200	2005	121 CPU rokov	GNFS
RSA-768	232	2009	3,300 CPU rokov	GNFS
$6^{353}-1$	275	2005	0,5 roka*	SNFS
$2^{1039}-1$	313	2006	0,7 roka*	SNFS
$2^{1061}-1$	320	2012	1,5 roka*	SNFS

CPU = 1Ghz pentium

Faktorizácia RSA-768

Relácií - 64 334 489 730 (5 TB)

- 47 762 243 404 (bez duplicít)
- 1.75 roka

Faktorová báza - 35 288 334 017 (ideálov)

Nezávislých relácií - 2 458 248 361

(1 697 618 199 ideálov)

- Systém - 192 796 550 x 192 795 550 (105 GB)
  - hustota - 144 čísel na riadok
  - 119 dní

DLP rekordy

Číslo	číslic	Dátum	Čas - hod	Sito
431	130	2005	8000	NFS
530	160	2007	??	NFS
596	180	2014	130 (rokov)	NFS
2^{6168}	4080		550	NFS
$3^{6.137}$	1303	2014	920	NFS
2^{9234}	9234		398 000	NFS
ECC – 112 bit prvočíslo	34	2009	876 000*	Pollard
Koblitz ECC-113 bit	34	2014	10 368’	Pollard

* PlayStation, ’Virtex-6 FPGA

Bezpečnosť a veľkosti kľúčov

Útočník	Cena $	Hardware	Min. bezpečnosť
Hacker	0	PC	53
Malá organizácia	10K	PC	64
Stredná	300K	FPGA	68
Veľká organizácia	10M	FPGA	78
Tajná služba	300M	ASIC	84

Veľkosť kľúča RSA / DL	Bezpečnosť
1024	73
1536	89
2048	103

Odporúčané veľkosti kľúčov

RSA/DL kryptosystémy

- 1024 sa nepovažuje za bezpečné
- 2048 bezpečné do 2030
- 3072 bezpečné po 2030

ECC
- 160 sa nepovažuje za bezpečné
- 224 bezpečné do 2030
- 256 bezpečné po 2030

Otázky a diskusia

Ďakujem za pozornosť