Ministerstvo financií
Slovenskej republiky

EFQM
Recognised for excellence
5 star - 2012

Kryptoanalýza prúdových šifier

Milan Vojvoda

2. október 2014

KPMG
cutting through complexity™

Obsah

Prúdová šifra

- Binárny aditívny prúdový šifrátor.
- Lineárny spätnoväzobný register.

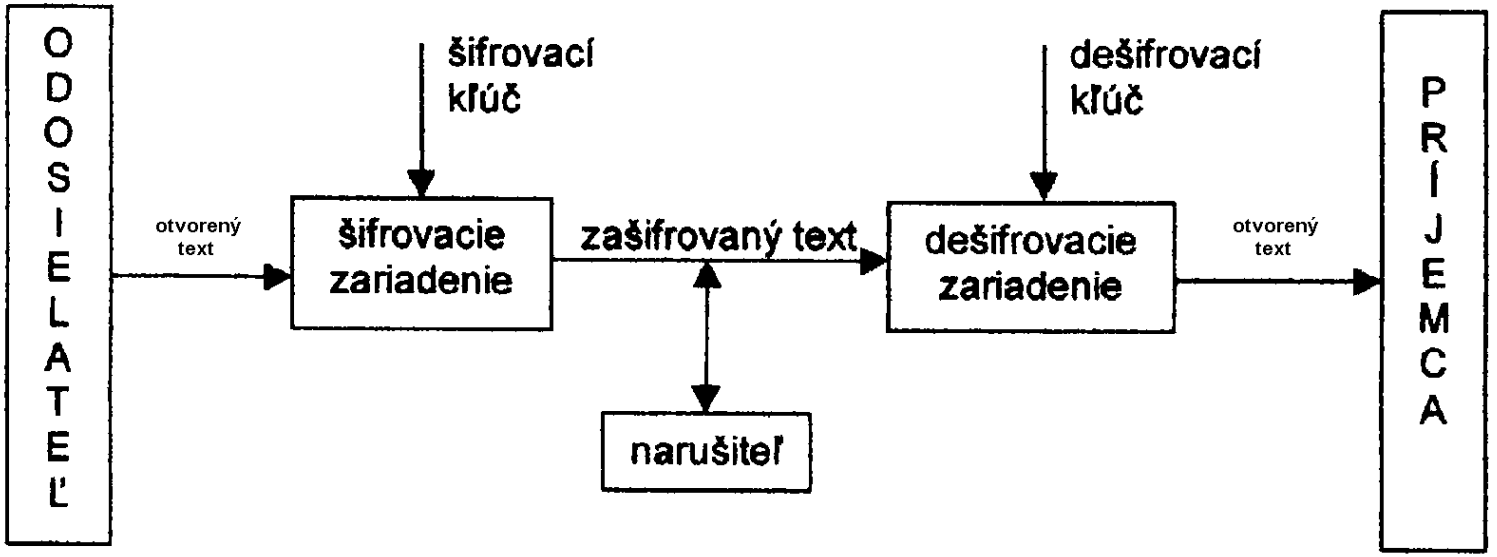
Útoky na šifry

- Ciele útokov.
- Druhy útokov.

Útoky na prúdové šifry

- Útok hrubou silou.
- Útok „rozdeľuj a panuj“.
- Korelačné útoky.
- Ďalšie útoky.

Schéma komunikácie so šifrovaním



Binárny aditívny prúdový šifrátor

- p_i – bity otvoreného textu (OT)
- z_i – bity prúdového kľúča
  - z_i – bity samotného kľúča = Vernamova šifra
- c_i – bity zašifrovaného textu (ZT)

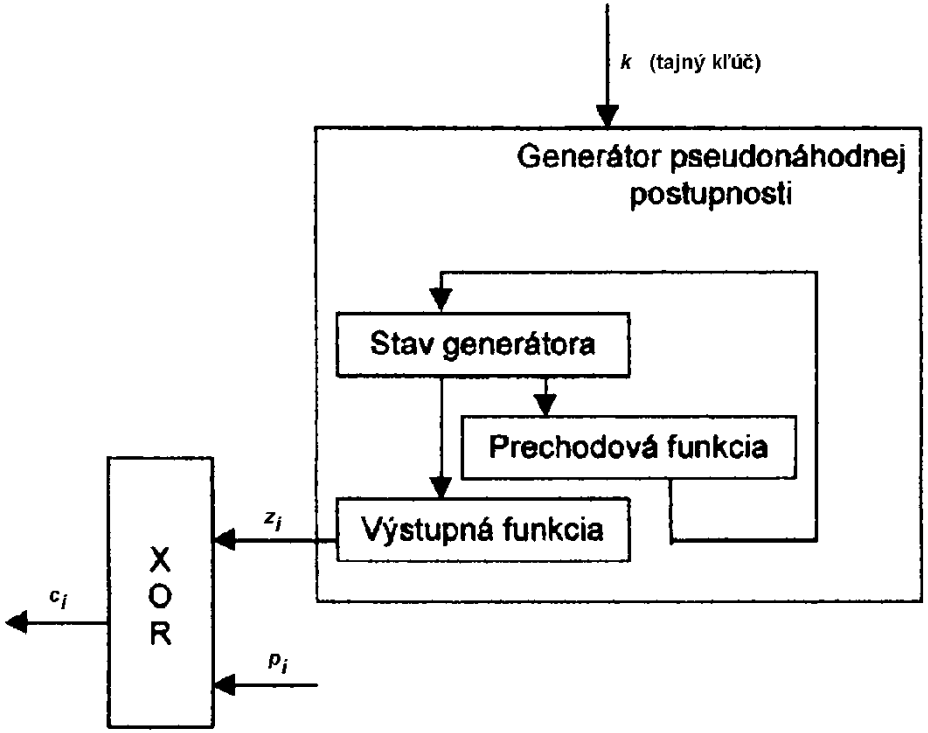
Šifrovacia transformácia:

$c_i = p_i \oplus z_i$

Dešifrovacia transformácia:

$p_i = c_i \oplus z_i = p_i \oplus z_i \oplus z_i = p_i$

Binárny aditívny prúdový šifrátor



Lineárny spätnoväzobný register

- Lineárna diferenčná rovnica (homogénna).
- Charakteristický polynóm.
- Perióda postupnosti.
- Lineárna zložitosť.
- Štatistické vlastnosti.

Ciele útokov

- **Úplné prelomenie šifry:** nájdenie kľúča analyticky...
- **Globálna dedukcia:** alternatívny algoritmus na nájdenie ľubovoľného OT...
- **Lokálne dedukcia:** alternatívny algoritmus na nájdenie konkrétneho OT...
- **Informačná dedukcia:** v texte je istá informácia, ktorá nám pomôže...

- **Kompromitácia kľúča:** často najľahšie...

Druhy útokov

Podľa aktivity útočníka:

- pasívny,
- aktívny.

Podľa toho, čo poznáme:

- len so znalosťou ZT,
- so znalosťou niekoľkých párov OT-ZT,
- s (adaptívnou) možnosťou voľby OT a získania zodpovedajúceho ZT,
- s (adaptívnou) možnosťou voľby ZT a získania zodpovedajúceho OT.

Útoky postrannými kanálmi:

- získanie informácií z konkrétnej (zlej) implementácie šifry.

Kerckhoffsov princíp

- 19. storočie.

- Kryptoanalytik má k dispozícii úplný popis šifrovacieho algoritmu so všetkými jeho detailami,vrátane jeho technickej implementácie.

- Bezpečnosť šifry má byť založená na utajení kľúča a nie na utajení šifry samotnej.

Útok hrubou silou

- Preverenie všetkých možných kľúčov kryptosystému → dostatočná mohutnosť množiny kľúčov.

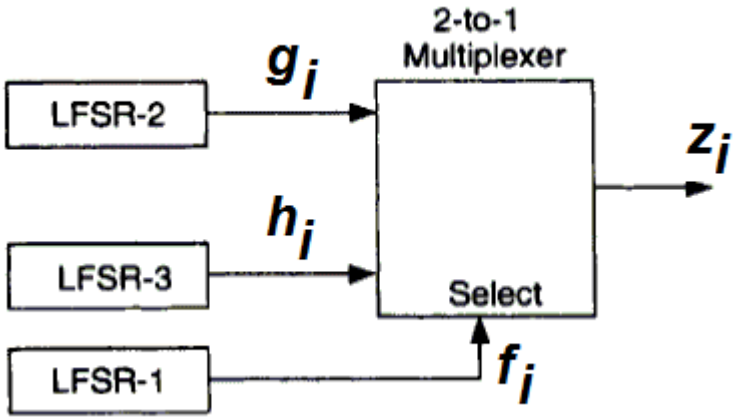
- Útok rýchlejší než hrubou silou = zlomenie šifry.

Útok „rozdeľuj a panuj“

- Rozdeliť kľúč na jednotlivé časti.
- Nájsť jednotlivé časti.
- Skonštruovať celý kľúč.

- Zvyčajne sa kombinuje s inými útokmi.

Geffeho generátor



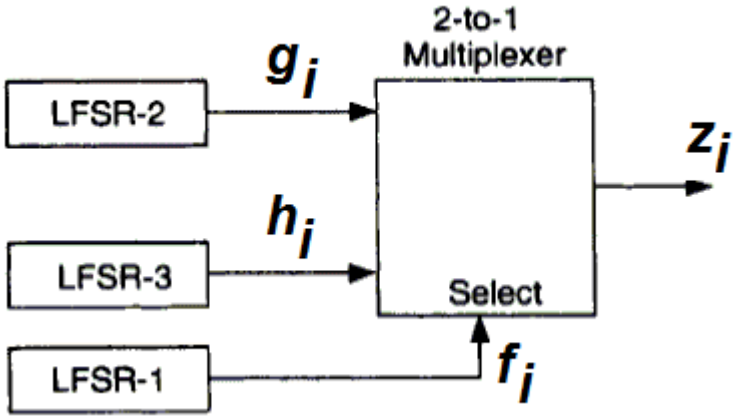
$$f_i + f_{i-1} + f_{i-2} = 0$$

$$g_i + g_{i-1} + g_{i-3} = 0$$

$$h_i + h_{i-1} + h_{i-4} = 0$$

$$z_i = f_i g_i \oplus (1 \oplus f_i) h_i$$

Geffeho generátor



$$f_i + f_{i-1} + f_{i-2} = 0$$

$$g_i + g_{i-1} + g_{i-3} = 0$$

$$h_i + h_{i-1} + h_{i-4} = 0$$

$$z_i = f_i g_i \oplus (1 \oplus f_i) h_i$$

i	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
f_i	**0**	**1**	1	0	1	1	0	1	1	0	1	1	0	1	1
g_i	**0**	**0**	**1**	1	1	0	1	0	0	1	1	1	0	1	0
h_i	**0**	**0**	**0**	**1**	1	1	1	0	1	0	1	1	0	0	1
z_i	0	0	1	1	1	0	1	0	0	0	1	1	0	1	0

Geffeho generátor – útok „rozdeľuj a panuj“

Poznáme výstup generátora – z_i

Cieľ: nájsť poč.naplnenia LFSR1,2,3

$$f_i + f_{i-1} + f_{i-2} = 0$$

$$g_i + g_{i-1} + g_{i-3} = 0$$

$$h_i + h_{i-1} + h_{i-4} = 0$$

$$z_i = f_i g_i \oplus (1 \oplus f_i) h_i$$

i	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
f_i															
g_i															
h_i															
z_i	0	0	1	1	1	0	1	0	0	0	1	1	0	1	0

Geffeho generátor – útok „rozdeľuj a panuj“

Zvolím naplnenie LFSR1

Dopočítam naplnenia LFSR2 a LFSR3

$$f_i + f_{i-1} + f_{i-2} = 0$$

$$g_i + g_{i-1} + g_{i-3} = 0$$

$$h_i + h_{i-1} + h_{i-4} = 0$$

$$z_i = f_i g_i \oplus (1 \oplus f_i) h_i$$

i	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
f_i	**1**	**0**	1	1	0	1	1	0	1	1	0	1	1	0	1
g_i	**0**		**1**	1		0	1		0	**0**		1	0		0
h_i		**0**			1			0			1			1	
z_i	0	0	1	1	1	0	1	0	0	0	1	1	0	1	0

Geffeho generátor – útok „rozdeľuj a panuj“

Zvolím naplnenie LFSR1

Dopočítam naplnenia

LFSR2 a LFSR3

$$f_i + f_{i-1} + f_{i-2} = 0$$

$$g_i + g_{i-1} + g_{i-3} = 0$$

$$h_i + h_{i-1} + h_{i-4} = 0$$

$$z_i = f_i g_i \oplus (1 \oplus f_i) h_i$$

i	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
f_i	**0**	**1**	1	0	1	1	0	1	1	0	1	1	0	1	1
g_i		**0**	**1**		1	0		0	0		1	1		1	0
h_i	**0**			**1**			1			0			0		
z_i	0	0	1	1	1	0	1	0	0	0	1	1	0	1	0

Geffeho generátor – útok „rozdeľuj a panuj“

Zvolím naplnenie LFSR1

Dopočítam naplnenia

LFSR2 a LFSR3

$$f_i + f_{i-1} + f_{i-2} = 0$$

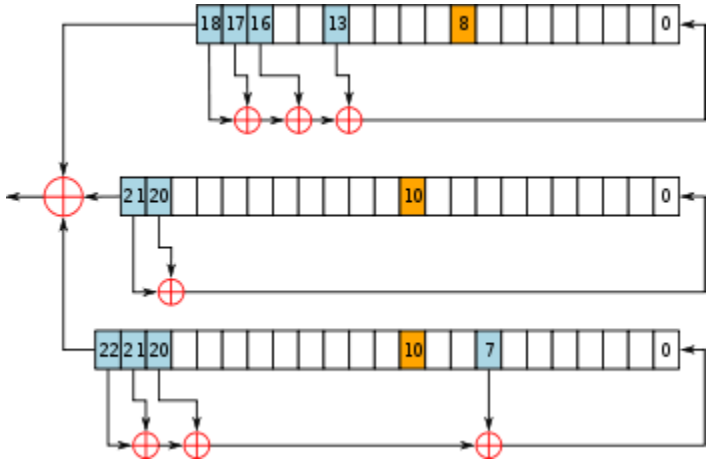
$$g_i + g_{i-1} + g_{i-3} = 0$$

$$h_i + h_{i-1} + h_{i-4} = 0$$

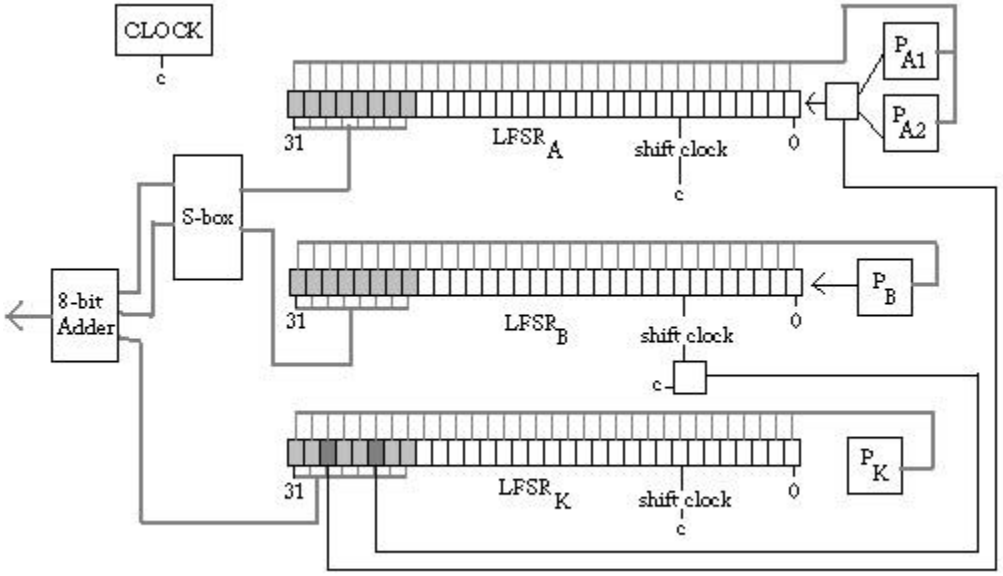
$$z_i = f_i g_i \oplus (1 \oplus f_i) h_i$$

i	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
f_i	**0**	**1**	1	0	1	1	0	1	1	0	1	1	0	1	1
g_i	**0**	**0**	**1**	1	1	0	1	0	0	1	1	1	0	1	0
h_i	**0**	**0**	**0**	**1**	1	1	1	0	1	0	1	1	0	0	1
z_i	0	0	1	1	1	0	1	0	0	0	1	1	0	1	0

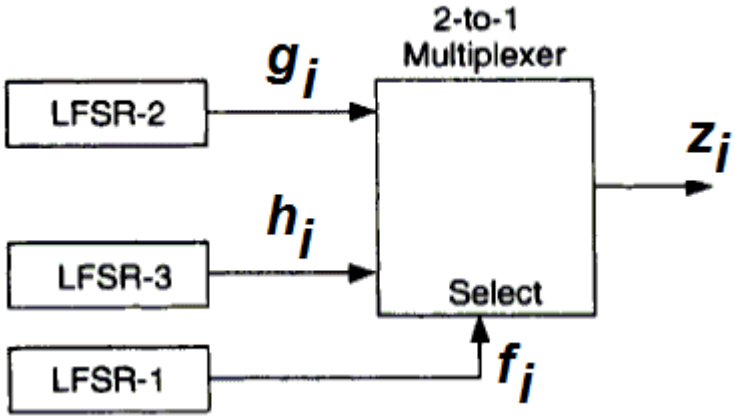
A5/1 – útok „rozdeľuj a panuj“



ORYX – útok „rozdeľuj a panuj“



Geffeho generátor

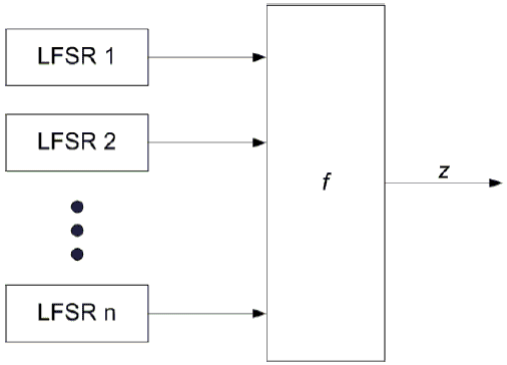


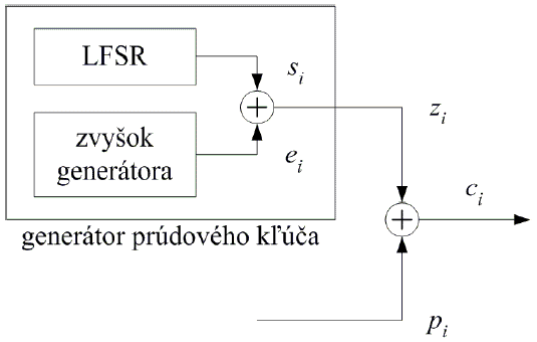
$$z_i = f_i g_i \oplus (1 \oplus f_i) h_i$$

f_i	g_i	h_i	z_i
0	0	0	0
0	0	1	1
0	1	0	0
0	1	1	1
1	0	0	0
1	0	1	0
1	1	0	1
1	1	1	1

$$\Pr(z_i = g_i) = \Pr(z_i = h_i) = 3/4$$

Korelačný útok - model





e_i ... šum

$p = \Pr(s_i = z_i) \neq 1/2 \rightarrow$ korelačný útok

Siegenthalerov korelačný útok na LFSR

- Dané: LFSR, prúdový kľúč, pravdep.zhody
- Cieľ: poč. napln. LFSR
- Opakuj pre všetky počiatočné naplnenia:
  - Vytvor postupnosť z LFSR
  - Urči pravdepodobnosť zhody s bitmi prúd.kľ.
- Zostav zoznam kandidátov (porovnaj očakávanú pravdepodobnosť zhody a skutočnú pravdep. zhody pre jednotl. postupnosti).

Siegenthalerov korelačný útok na Geffeho generátor

$g_i + g_{i-1} + g_{i-3} = 0$

i	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	p.z.	a.h.o.
z_i	0	0	1	1	1	0	1	0	0	0	1	1	0	1	0		
g_i	**0**	**0**	**1**	1	1	0	1	0	0	1	1	1	0	1	0	14	0,183
g_i	**0**	**1**	**0**	0	1	1	1	0	1	0	0	1	1	1	0	8	0,217
g_i	**0**	**1**	**1**	1	0	1	0	0	1	1	1	0	1	0	0	6	0,350
g_i	**1**	**0**	**0**	1	1	1	0	1	0	0	1	1	1	0	1	7	0,283
g_i	**1**	**0**	**1**	0	0	1	1	1	0	1	0	0	1	1	1	5	0,417
g_i	**1**	**1**	**0**	1	0	0	1	1	1	0	1	0	0	1	1	7	0,283
g_i	**1**	**1**	**1**	0	1	0	0	1	1	1	0	1	0	0	1	5	0,417

p.z.-počet zhôd z_i a g_i v riadku, a.h.o.= |p.z./15 - 3/4|

Rýchle korelačné útoky - ako zisťovať chybné bity?

- Nepoužívajú úplné prehľadávanie
- Posun (bit s_i môže v rekurencii vystupovať na viacerých pozíciách).
- Ďalšie rekurencie:
  - napr. postupné umocňovanie ľavého char. polynómu:
    $a(x)$, $a^2(x)$, $a^4(x)$, $a^8(x)$, ...

Rýchle korelačné útoky

- Dva základné prístupy:
  - Vyber bity s veľa splnenými vzťahmi, vypočítaj z nich poč. naplnenie LFSR, over ho, ak nesedí, tak zmeň vybrané bity
  - Zmeň bity s málo splnenými vzťahmi, znova urči koľko vzťahov je prednotlivé bity splnených, ...

Ďalšie útoky

- Rýchle korelačné útoky pomocou turbo kódov, konvolučných kódov, rekonštrukcie lineárnych polynómov, ...
- Diferenciálna kryptoanalýza.
- Odlišovače.
- Útoky vnútením chyby.
- Útoky skenovaním.
- Špeciálne útoky na konkrétne prúdové šifry.

Otázky a diskusia

Ďakujem za pozornosť