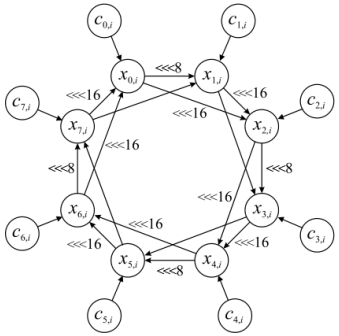
České vysoké učení technické v Praze
Fakulta elektrotechnická
Katedra telekomunikační techniky



A7B32KBE – 6.přednáška

Proudové šifry

Ing. Tomáš Vaněk, Ph.D. tomas.vanek@fel.cvut.cz

Osnova

- Proudové šifry
  - synchronní
  - asynchronní
- RC4
- A5
- E0
- Projekt eSTREAM

Opakování

- Moderní symetrické šifry
  - Blokové – viz. přednáška č.3 a 4
    - Šifrovací schéma rozděluje zprávu OT do řetězců pevné délky *t* nad abecedou *A* zvaných bloky. BŠ šifruje v jeden okamžik pouze jeden blok OT.
    - šifry bez paměti (neuvažujeme režimy činnosti)
  - Proudové
    - šifry s pamětí
    - OT je zpracováván po jednotlivých bitech
    - Proudová šifra aplikuje jednoduchou šifrovací transformaci (XOR) v závislosti na použitém proudovém klíči. Klíč je generován náhodně, nebo pomocí algoritmu, který jej generuje z malého inicializačního proudového klíče zvaného jádro/semínko (seed), nebo z jádra a předchozích šifrovaných symbolů. Tento algoritmus se nazývá generátor proudového klíče.

Proudové šifry

Vernamova šifra

- pracuje nad abecedou A={0,1}
- $c_1 = m_i \oplus k_i, \quad 1 \leq i \leq t$
- dvě substituční šifry (E_0, E_1) na množině A
  - E_0 mapuje $0_{OT} \rightarrow 0_{ŠT}$ a $1 \rightarrow 1_{ŠT}$
  - E_1 mapuje $0_{OT} \rightarrow 1_{ŠT}$ a $1_{OT} \rightarrow 0_{ŠT}$
  - pokud klíč obsahuje 0, aplikuje se E_0 na daný symbol OT
  - pokud klíč obsahuje 1, aplikuje se E_1 na daný symbol OT

One-time pad

- Vernamova šifra s náhodným klíčem
- nepodmíněně bezpečná vůči útoku na ŠT, protože entropie zprávy $H(M|C) = H(M)$
- ŠT neobsahuje žádnou informaci o OT

Proudové šifry

Shannonova podmínka nepodmíněné bezpečnosti:

- entropie klíče > entropie zprávy
  - $H(\kappa) \geq H(M)$
- toto je omezující podmínka použití proudových šifer
  - nelze ji dodržet
  - pro šifry s $H(\kappa) << H(M)$ – výpočetní složitost
- další problém – distribuce klíčů

Proudové šifry

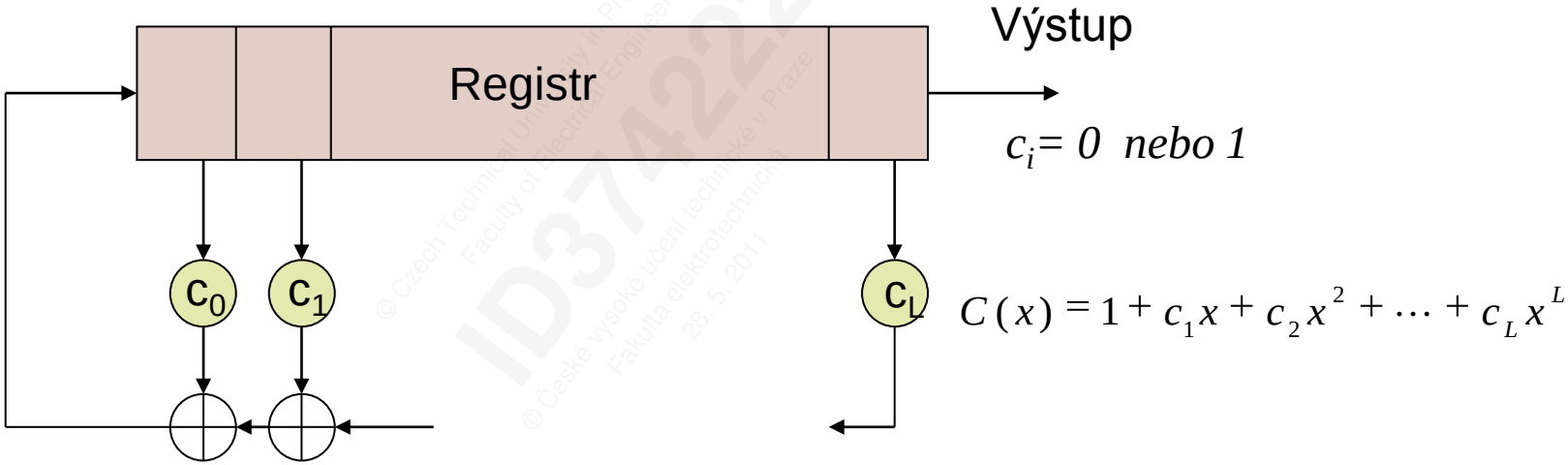
- šifry s pamětí (též stavové šifry)
- výměna prokazatelné bezpečnosti za jednoduchou realizaci (konstrukci)
- proudové šifry jsou inicializovány krátkým klíčem (**seed**)
- klíč je „natažen“ do dlouhého proudu klíče (**keystream**)
- proud klíče se používá stejně jako one-time pad
  - XOR s OT / ŠT
- proudová šifra je generátor proudu klíče
  - obvykle generuje proud klíče po bitech, někdy bajtech

Posuvné registry

- Klasické proudové šifry byly založeny na posuvných registrech (shift register)
- posuvný registr obsahuje
  - množina stavů každý obsahující jeden bit
  - zpětnovazební funkci
- lineární zpětnovazební registr (LFSR) má lineární zpětnovazební funkci
- dnes se využívá mnohem širší spektrum metod :
  - LFSR (jednoduchá konstrukce, dobré statistické vlastnosti)
  - S-boxy (vnášejí nelinearitu),
  - Booleovy funkce (nelinearita a zvýšení lineární složitosti),
  - sčítání mod 2^n (nelinearity a rušení asociativity)

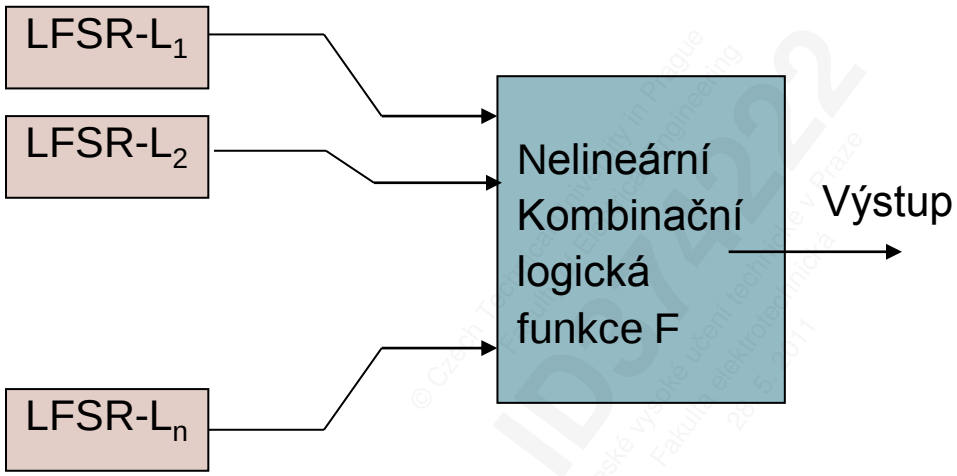
LFSR – Linear Feedback Shift Register

- jeden ze základních bloků proudových šifer
- nutno kombinovat s nějakou nelineární části



- *n*-bitový čítač vykazující náhodné chování
- Pokud je polynom $C(x)$ primitivní, má výstupní posloupnost LFSR periodu $T = 2^L - 1$.
- Taková výstupní posloupnost má dobré statistické vlastnosti, ale je předvídatelná.

Nelineární kombinování LFSR



Kombinační funkce má mít následující vlastnosti:

1. vyvážená,
2. silně nelineární,
3. nekorelující výstup s obsahem LFSR

9

Nelineární kombinování LFSR

Příklad: 3 LFSR s nelineární funkcí F

$$F(x_1, x_2, x_3) = x_1 x_2 \oplus x_2 x_3 \oplus x_3$$

Pravdivostní tabulka funkce F

x_1	x_2	x_3	$z = F(x_1,x_2,x_3)$
0	0	0	0
0	0	1	1
0	1	0	0
0	1	1	0
1	0	0	0
1	0	1	1
1	1	0	1
1	1	1	1

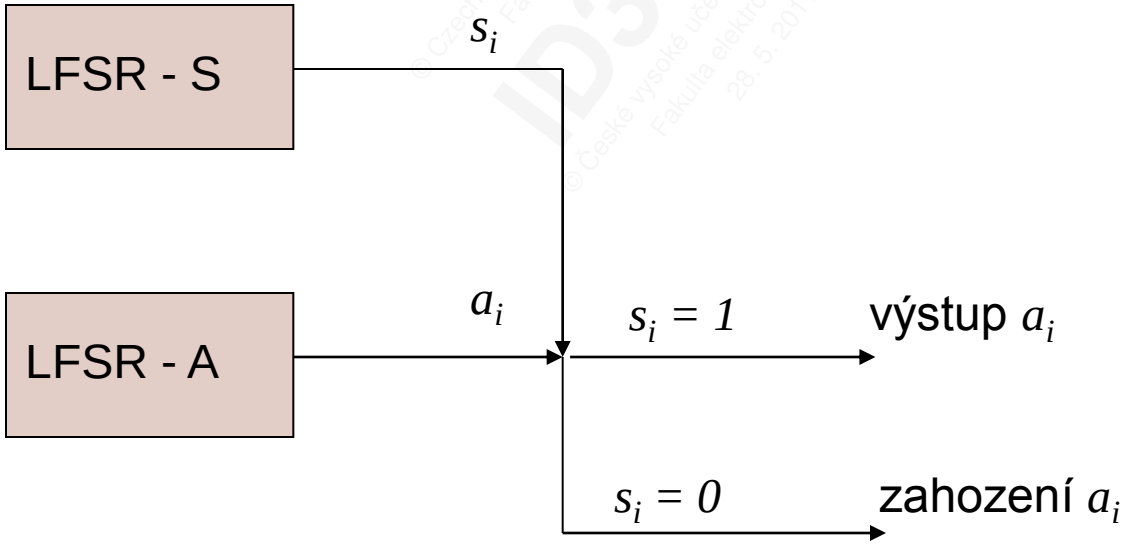
- funkce F kombinující tři LFSR je vyvážená
- existuje velká korelace mezi x_1 a z, protože

$$P(z = x_1) = 3/4.$$

Proto funkce F není bezpečná (jako proudová šifra).

LFSR řízené hodinovým taktem

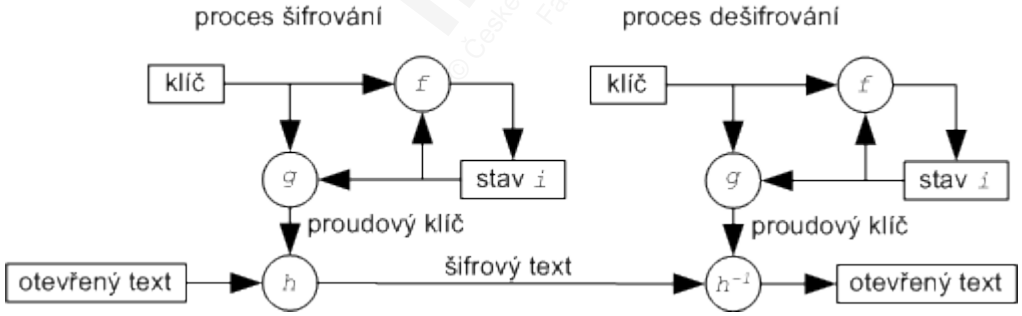
- Clock-controlled Generator
- LFSR je taktován z výstupu jiného LFSR
- Nelinearita vytvořena nepravidelnostmi v taktování jednotlivých LFSR
- Příklad:



11

Synchronní proudová šifra

- SSC – Synchronous Stream Cipher
- proud klíče (key stream) je generován nezávisle na OT a K
- SSC šifra vyžaduje, aby odesílatel a příjemce byli synchronizováni při použití proudu klíče a operací na shodné pozici
- ztráta/přidání bitu → dešifrování znemožněno a je nutná resynchronizace obou stran

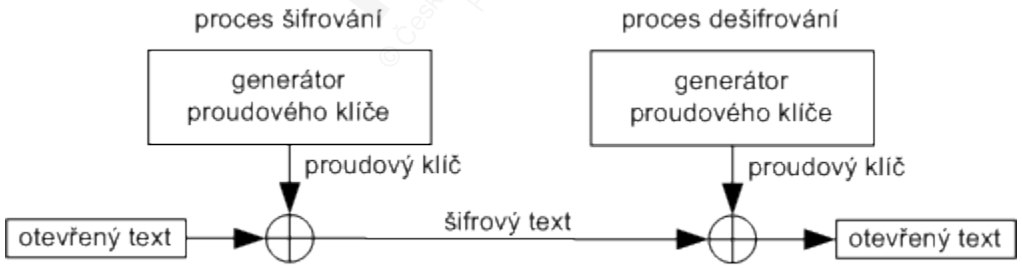


Synchronní proudová šifra

- resynchronizace spočívá ve vkládání speciálních značek do šifrového textu, které reinicializují ztracenou synchronizaci
- kladnou vlastností SSC je nešíření chyb
- změna bitu ŠT neovlivní dešifrovací proces, pouze bit OT
- SSC jsou náchylné na útoky typu mazání, vložení či opakování bitů - důsledkem je ztráta synchronizace
- v praxi je nezbytné tyto situace detekovat a zavést mechanizmy pro zajištění autentizace a integrity dat

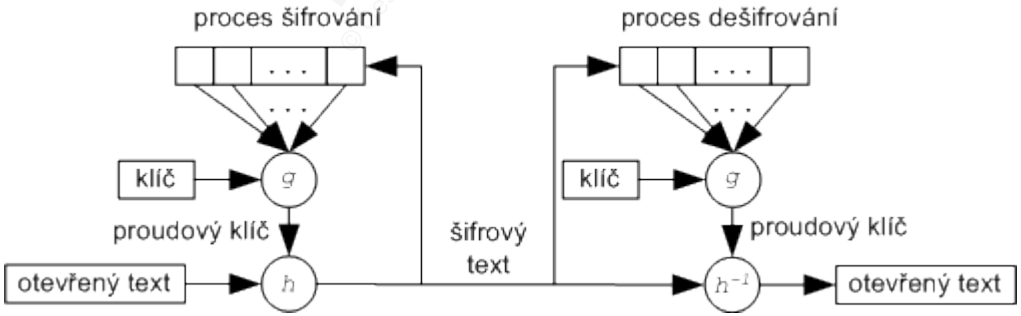
Binární aditivní proudová šifra

- BASC – Binary Additive Stream Cipher
- speciální případ synchronní proudové šifry
- binární reprezentace OT a ŠT (bity)
- výstupní funkce je funkce XOR
- počítačové aplikace



Asynchronní proudové šifry

- proud klíče závisí na OT/ŠT
- také „proudové šifry s vlastní synchronizací“ nebo „samosynchronizující se šifry“
- Self-synchronnizing Stream Cipher
- proudový klíč je generován v závislosti na klíči K a pevně daném počtu předchozích šifrovaných bitů
- v praxi se nejčastěji používají v režimu jednobitové zpětné vazby (CFB – viz 4.přednáška)



Asynchronní proudové šifry

- vlastní synchronizace je možná, i když jsou některé bity smazané či vložené, protože dešifrovací mapování závisí na pevném počtu předchozích zašifrovaných bitů
- po ztrátě synchronizace se automaticky obnoví správná činnost - ztratí pouze pevný počet bitů otevřeného textu.
- pokud stav asynchronního proudu šifry závisí na *t* předchozích šifrovaných bitech a je-li jeden šifrovaný bit modifikován (smazán nebo vložen) během přenosu, potom může být dešifrování maximálně *t* následujících bitů šifrového textu nesprávných, než nastane opět správné dešifrování
- omezené šíření chyb
- lepší statistické vlastnosti ŠT (každý znak OT ovlivňuje následující znak ŠT)-> odolnější než synchronní šifry

Současné proudové šifry

- vyskytují se v běžných technologiích
  - WiFi – IEEE 802.11
  - Bluetooth – IEEE 802.15
  - GSM – ETSI GSM 09.01
- HW implementace

Proudová šifra RC4

- autor Ron Rivest
- 1987 (!) ve firmě RSA Data Security Inc.
- nemá IV → pro každí spojení se používá nový klíč
- šifra nebyla nikdy oficiálně publikována
- 09/1994 anonymní hacker uveřejnil zdrojový kód získaný pomocí technologie *reverse engineering*
- dostupná verze se označuje *ARCFOUR*
  - RC4 je ochranná známka RSA Data Security Inc.
- volitelná délka klíče 8..2048b
  - nejčastěji128 bitů
- v jednom kroku algoritmus vygeneruje 1B proudu klíče
- 1997 J. Golic - statistická slabina generátoru klíče ARC4
  - GOLIĆ, J. *Linear Statistical Weakness of Alleged RC4 Key stream Generator.* In Advances in Cryptology, Eurocrypt'97, Lecture Notes in Computer Science 1233. Springer-Verlag Berlin, 1997. ISBN 3-540-62975-0

Proudová šifra RC4

- rychlý algoritmus
- základem je tabulka o velikosti 255 bajtů
- v každém kroku RC4 dojde k
  - prohození prvků v současné tabulce
  - výběru bajtu klíče z tabulky
- počáteční nastavení (permutace) je dána klíčem
- na počátku je tabulka prázdná → naplní se klíčem
- určitý počet kroků algoritmu bez výstupu
- v každý krok RC4 produkuje 8 bitů proudu klíče
- OT se přičítá (XOR) na generovaný proud klíče
- efektivní SW implementace na PC (žádné LFSR; operace s celými bajty, operace mod 256 = AND 255)

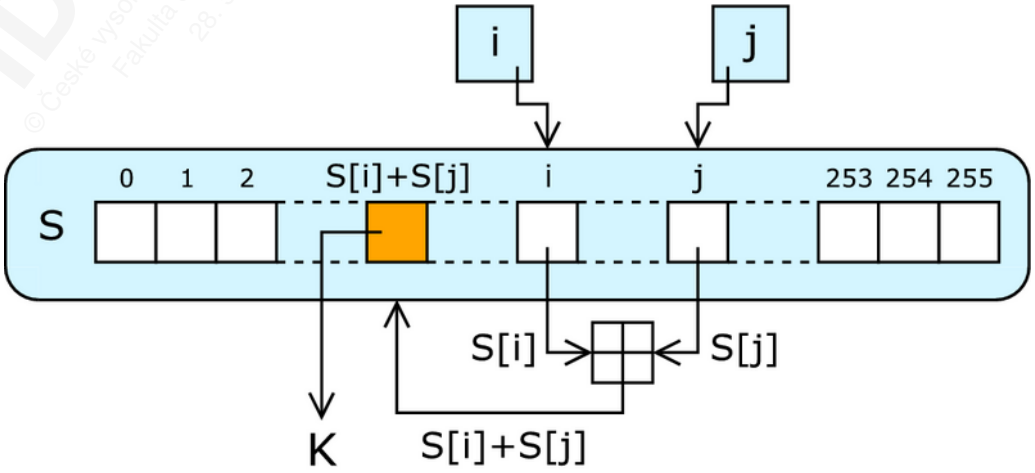
Proudová šifra RC4

- rychlý algoritmus
- základem je tabulka o velikosti 255 bajtů
- v každém kroku RC4 dojde k
  - prohození prvků v současné tabulce
  - výběru bajtu klíče z tabulky
- počáteční nastavení (permutace) je dána klíčem
- na počátku je tabulka prázdná → naplní se klíčem
- určitý počet kroků algoritmu bez výstupu
- v každý krok RC4 produkuje 8 bitů proudu klíče
- OT se přičítá (XOR) na generovaný proud klíče
- efektivní SW implementace na PC (žádné LFSR; operace s celými bajty, operace mod 256 = AND 255)

Proudová šifra RC4

V každém kroku se prohodí prvky tabulky a vybere bajt:

i = (i + 1) mod 256
j = (j + S[i]) mod 256
swap(S[i], S[j])
t = (S[i] + S[j]) mod 256
keystreamByte = S[t]



Proudová šifra RC4 - využití

- bezdrátové sítě IEEE 802.11
  - WEP
  - WPA
- BitTorrent protokol
- MPPE - Microsoft Point-to-Point Encryption
  - volitelné zabezpečení PPP od Microsoftu
- SSL - Secure Sockets Layer (jedna z protokolových sad)
- SSH - Secure shell (jeden z možných algoritmů)
- RDP - Remote Desktop Protocol
- Kerberos (jeden z možných algoritmů)
- SASL - Simple Authentication and Security Layer (jeden z možných algoritmů)
  - framework pro autentizaci spojově orientovaných protokolů, RFC4422
- virus Gpcode.AK pro MS Windows (06/2008
  - šifroval dokumenty pomocí RC4 a RSA-1024 – klíč k dispozici po zaplacení
- PDF

Proudová šifra RC4 - bezpečnost

- pokud se stejný klíč má použít ke generování více proudů, je nutné použít další parametr - nonce (náhodné číslo) k jejich rozlišení
- kryptosystém musí mít mechanismus, jak dlouhodobý klíč a nonce bezpečně kombinovat
- dobrý způsob generování proudových klíčů :
  - hash z klíče a nonce
- v praxi často používaný způsob (špatný):
  - pouhé spojení klíče a nonce
  - vzhledem ke způsobu inicializace RC4 to způsobuje vážné bezpečnostní problémy
  - viz přednáška o zabezpečení bezdrátových sítí (WEP)

Proudová šifra RC4 - bezpečnost

- 1995 – Andrew Roos experimentálně zjistil, že
  - existuje korelace mezi prvním bajtem proudu klíče a prvními třemi bajty klíče
  - několik prvních bajtů permutace je lineární kombinací vybraných bajtů klíče
  - v 2007 potvrzeno (obě tvrzení)
  - problém je v KSA (Key Scheduling Algorithm)
  - nalezen pravděpodobnostní algoritmus
    - zjistí počáteční klíč pouze ze znalosti „permutovaného pole“ po KSA
    - konstatní PRST úspěchu v čase sqrt(x), kde x je doba nutná k prolomení pomocí brute-force
- 2001 – Fluhrer, Mantin, Shamir (FMS útok)
  - prvních několik bajtů proudu klíče má velmi NEnáhodný charakter -> prolomení WEPu

Proudová šifra RC4 - bezpečnost

- 2005 - Andreas Klein
  - další korelace mezi proudem klíče a klíčem
  - výsledek - urychlení útoků na WEP
  - výrazně snížen počet zachycených paketů nutných k prolomení WEPu
    - FMS ~ 10^7 rámců
    - Klein ~ 40.000 rámců …PRST úspěchu 50%
    - Klein ~ 85.000 rámců …PRST úspěchu 95%

Proudová šifra A5

- 1987 USA
- algoritmus utajován
- 1994 – únik informací o obecné struktuře (LFSR)
- 1990 – rekonstrukce algoritmu (*reverse engineering*)
- A5/1 klíč délky 64 bitů + číslo TDMA rámce (veřejně známé)
  - 10 bitů vždy nastaveno na log.0
  - efektivní délka klíče 54bitů
- 1997 – teoretický útok J. Golić
  - na stejné konferenci, kde popsal útok na RC4 ☺
- 1999 - A5/2 vyvinuta pro oblast Asie a východní Evropy
  - výrazně slabší
  - kryptoanalýza uveřejněná ve stejném měsíci, kdy byla publikována ukázala vážné slabiny
- od 2006 GSMA zákaz podpory A5/2 v mobilních telefonech
- v doporučeních 3GPP je A5/2 dodnes jako volitelný algoritmus

Proudová šifra A5

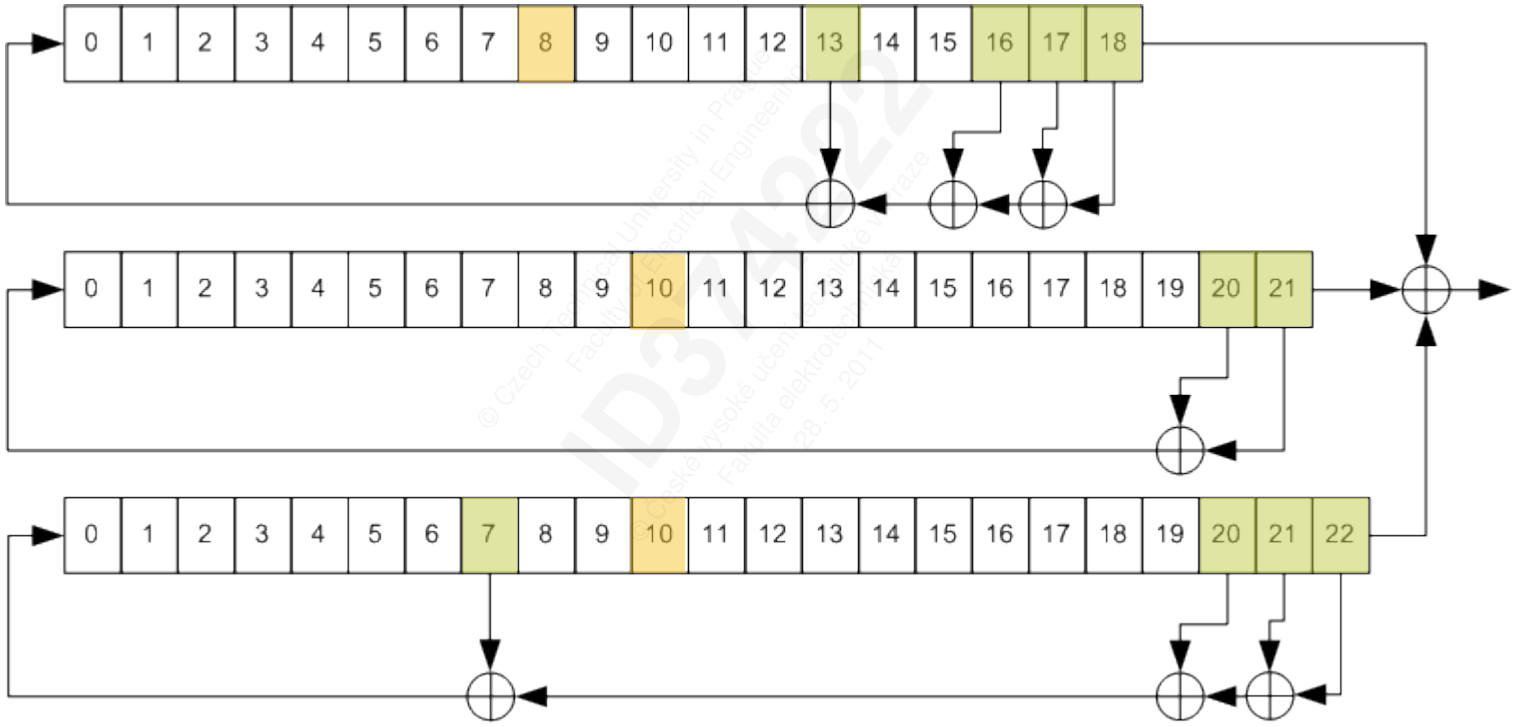
- šifrování na rádiovém rozhraní sítě mezi MS a BTS
  - šifrovací algoritmus A5 je uložen v MS
  - je stejný pro všechny operátory (proč ?)
  - klíč generován pomocí A8 uloženým na SIM kartě
- specifikace A5 nebyla nikdy oficiálně publikována
- vstup do A5:

  relační klíč K_c = A8(RAND, K_i) délky 64 bitů

  číslo TDMA rámce (22 bitů)

  výstup: 114 bitů
- šifra produkuje vždy 228 bitů proudu klíče
  - 114 bitů se používá pro šifrování komunikace od telefonu k základové stanici
  - 114 bitů pro šifrování komunikace v opačném směru
- více viz přednáška o zabezpečení GMS/UMTS sítí

Proudová šifra A5



Proudová šifra A5

- algoritmus A5/1 je založen na kombinaci tří lineárních registrů se zpětnou vazbou (LFSR) a nepravidelného taktování
- A5/1 obsahuje of 3 LFSR
  - X: 19 bitů (x_0,x_1, …,x_{17},x_{18})
  - Y: 22 bitů (y_0,y_1, …,y_{20},y_{21})
  - Z: 23 bitů (z_0,z_1, …,z_{21},z_{22})
- klíčem je počáteční hodnota registrů
- každá buňka obsahuje jeden bit (srovnej s RC4)
- v každém kroku se každý registr posune nebo zůstane stát
- registr se posune pokud hodnota jeho „hodinového bitu“ (oranžový) souhlasí s většinovou hodnotou všech „hodinových bitů“
- proud klíče vzniká XORem výstupu tří registrů

Proudová šifra A5 – inicializace v GSM

1) všechny jsou registry vynulovány

2) v 64 krocích je namixován 64bitový tajný klíč K_i podle následujícího principu:

Pro 0<i<64, je *í-tý* bit klíče přidán do každého registru pomocí operace XOR : R[i]=R[i] XOR K[i]

3) Po načtení klíče se do systému přičte 22 bitů čísla TDMA rámce a poté je systém provozován 100 hodinovým taktů s odpojeným výstupem

Nyní je systém připraven vyprodukovat 228 bitů výstupního proudu klíče.

Varianty A5

Existuje několik verzí algoritmu A5, které poskytují různou úroveň zabezpečení:

- A5/0 – neposkytuje žádné zabezpečení
- A5/1 – původní algoritmus A5 používaný v Evropě
  - prvních deset bitů klíče je nulových
  - efektivní délka klíče – 54 bitů (horší než DES!)
- A5/2 – kryptograficky oslabená varianta algoritmu vytvořená pro export (Čína…)
- A5/3 – silný šifrovací algoritmus vytvořený jako součást 3rd Generation Partnership Project (3GPP), základem je japonská bloková šifra KASUMI ( )

Varianty A5

Existuje několik verzí algoritmu A5, které poskytují různou úroveň zabezpečení:

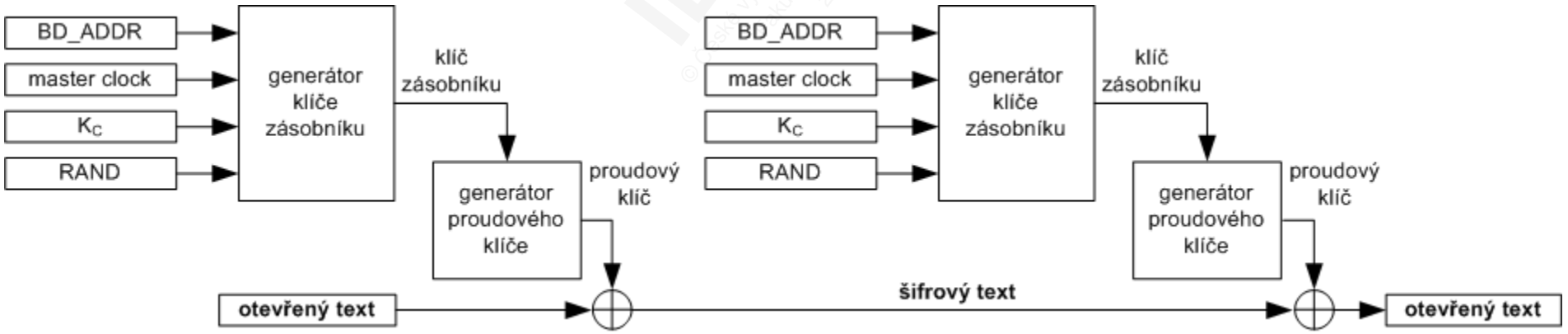
- A5/0 – neposkytuje žádné zabezpečení
- A5/1 – původní algoritmus A5 používaný v Evropě
  - prvních deset bitů klíče je nulových
  - efektivní délka klíče – 54 bitů (horší než DES!)
- A5/2 – kryptograficky oslabená varianta algoritmu vytvořená pro export (Čína…)
- A5/3 – silný šifrovací algoritmus vytvořený jako součást 3rd Generation Partnership Project (3GPP), základem je japonská bloková šifra KASUMI ( )

Proudová šifra E0

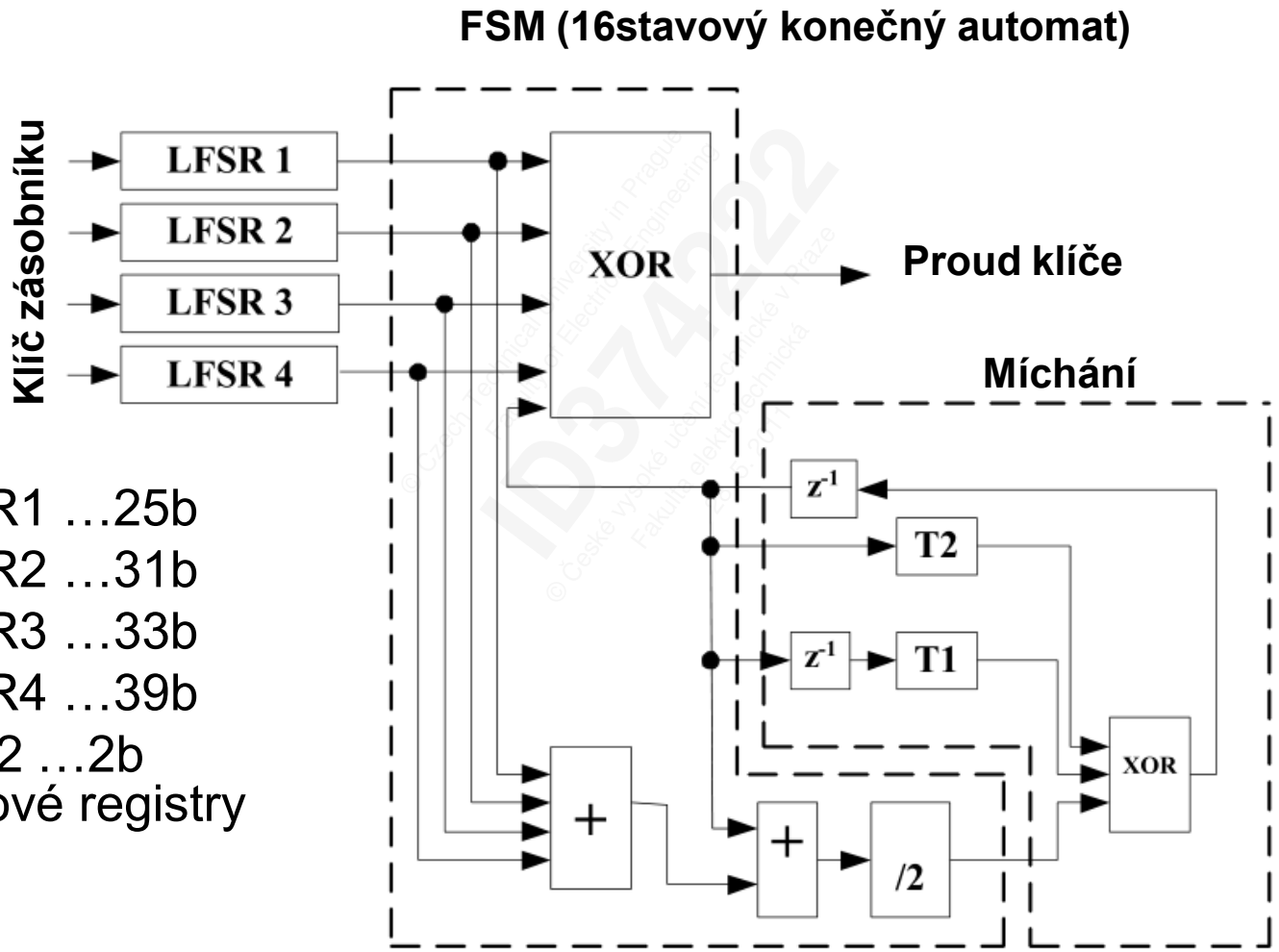
- šifrování datového toku technologie Bluetooth
  - IEEE 802.15
- Tři fáze
  - incializační - generování klíče pro blok dat
  - generování proudu klíče na principu Massey-Rueppelova generátoru klíče
  - vlastní šifrování
- Massey-Rueppelův algoritmus generování klíče je náchylný na korelační útoky
- PRST úspěšného útoku je je snížena vysokou resynchronizační frekvencí (nastává po odeslání každého bloku dat).

Proudová šifra E0

- Parametry algoritmu:
  - BD_ADDR – 48 bitů – fyzická adresa zařízení (unikátní)
  - KC - šifrovací klíč – 8-128bitů
  - master clock - 26 bitů
  - RAND – 128 bitů - náhodně vygenerovaná hodnota



E0 – generátor proudového klíče



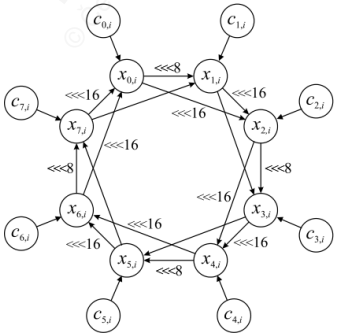
- LFSR1 …25b
- LFSR2 …31b
- LFSR3 …33b
- LFSR4 …39b
- T1,T2 …2b stavové registry

E0 - bezpečnost

- existuje několik útoků na E0 (a Bluetooth)
- 1999 - nalezena možnost prolomení E0 v 2^{64} krocích (místo 2^{128}) se znalostí 2^{64} bitů výstupu
- maximální bezpečnost E0 odpovídá algoritmu s 65bitovým klíčem – delší klíče nezvyšují bezpečnost
- 2004 – statistický útok se znalostí 24 prvních bitů z 2^{35} Bluetooth rámců (rámec má 2745b). Celková složitost útoku vedoucí k získání klíče je 2^{40}
  - útok zdokonalen – potřebuje pouze 2^{37} kroků pro pomocné výpočty (před útokem) a 2^{39} kroků pro nalezení klíče
- 2005 – podmíněný korelační útok - útok se znalostí 24 prvních bitů z $2^{23,8}$ rámců a dále 2^{38} kroků pro výpočet klíče - nejrychlejší známý útok

Projekt eSTREAM

- od 2004
- hledání nových proudových algoritmů
  - rychlejší než AES
  - bezpečnější než AES
- projekt organizovaný evropským konsorciem výzkumných organizací ECRYPT (European Network of Excellence for Cryptology)



Projekt eSTREAM

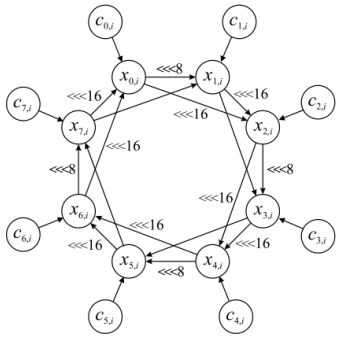
3 fáze výběrového řízení

- 1. fáze do 02/2006
  - rámcová analýza všech kandidátů
- vytvoření dvou profilů
  - Profil 1
    - SW implementace
    - vysoká propustnost
    - přijaty pouze algoritmy efektivnější než AES128 -CTR
  - Profil 2
    - HW implementace
    - omezené zdroje
      - počet hradel, množství paměti

Projekt eSTREAM

2. fáze od 06/2006 -09/2007
  - podrobné testy kandidátů přijatých z fáze 1
  - pro oba profily byly dodatečně přijaty nové algoritmy
  - kandidáti fáze 2 byly každých šest měsíců reklasifikováni
3. fáze
  - celkem osm kandidátů v Profile1 a Profile2
  - 08/2008 - z kandidátů byly vybrány algoritmy:

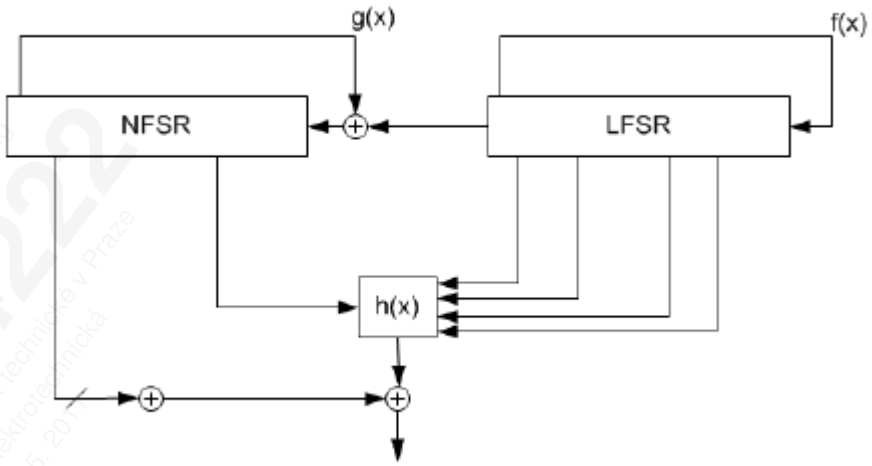
Profil 1	**Profil 2**
HC-128	Grain v1
Salsa 20/12	MICKEY v2
SOSEMANUK	Trivium
Rabbit	F-FCSR (později vyřazen)



- každých 6 měsíců revize

E-stream Profile 2 - Grain

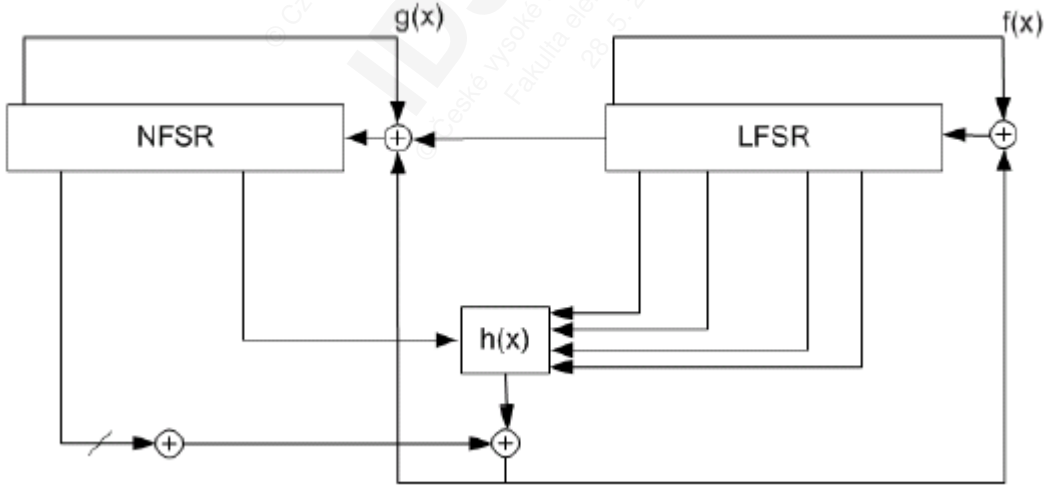
- IV …64 bitů
- K … 80 bitů
- vnitřní struktura
  - 80bitový LFSR
  - 80bitový NLFSR
- vnitřní stav celkem 160 bitů
- perioda 2^{80}-1



- 4 bity LFSR a 1 bit NLFSR vstupují do nelineární Booleovy funkce *h(x)* (5 vstupů, 1 výstup), výstup je dále znovu zkombinován se 7 bity NLFSR a tvoří výstup z generátoru klíče
- 10/2006 – útok typu „related key“ – pro pár (K,IV) s PRST 1:22 existuje pár (K’,IV’), který generuje proud klíče posunutý o jeden bit vůči proudu z (K,IV)

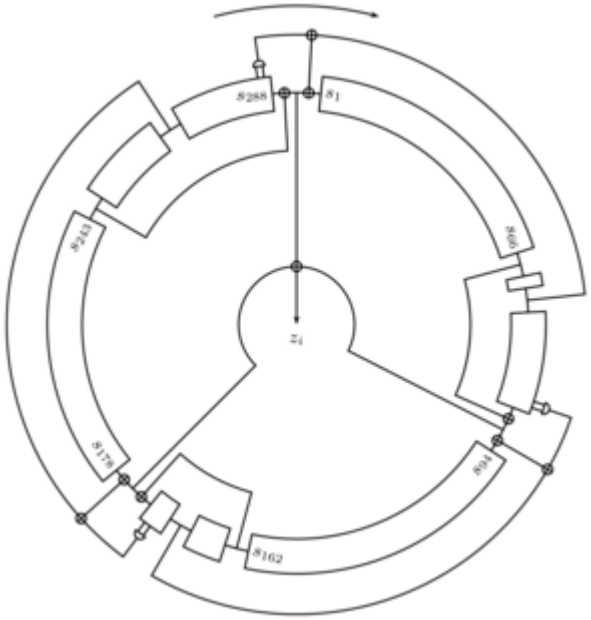
E-stream Profile 2 - Grain

- Inicializace algoritmu
  - naplnění NFSR bity klíč
  - naplnění LFSR bity IV
    - zbytek LFSR je naplněn log.1
  - 160 taktů probíhá inicializace s výstupem zapojeným zpět do obou registrů



E-stream Profile 2 - Trivium

- synchronní proudová šifra
- IV … 80 bitů
- K … 80 bitů
- 3 FSR různé délky
- vnitřní stav celkem 288 bitů
- nejjednodušší návrh ze všech algoritmů v E-stream projektu
- 9/2010 – nejlepší útok na odhalení vnitřního stavu šifry vyžaduje $2^{89.5}$ kroků



$$X_i = Z_{i-66} \oplus Z_{i-111} \oplus Z_{i-110} \otimes Z_{i-109} \oplus X_{i-69}$$
$$Y_i = X_{i-66} \oplus X_{i-93} \oplus X_{i-92} \otimes X_{i-91} \oplus Y_{i-78}$$
$$Z_i = Y_{i-69} \oplus Y_{i-84} \oplus Y_{i-83} \otimes Y_{i-82} \oplus Z_{i-87}$$

$\otimes$ … AND

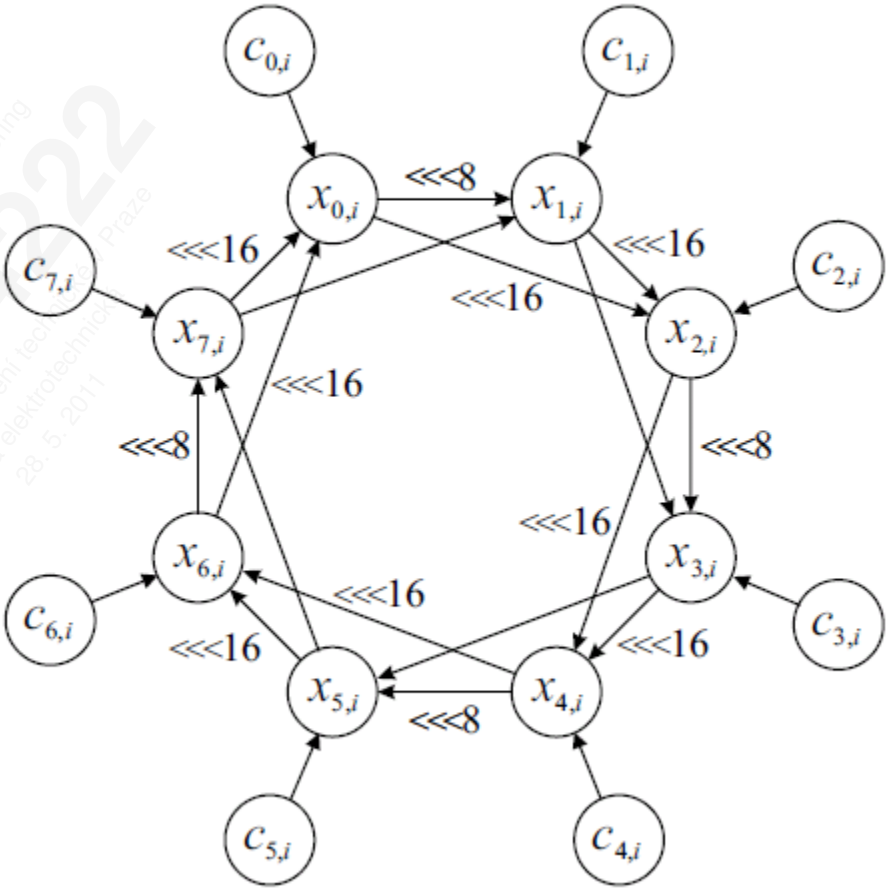
$\oplus$ … XOR

E-stream Profile 2 – MICKEY v2

- IV … 0-80 bitů
- K … 80 bitů
- pro daný pár (K,IV) lze vygenerovat max. 2^{40} bitů
- dva registry *R,S* o velikosti 100b
  - R - lineární
  - S - nelineární
  - změna obsahu R/S na základě aktuálních v registrech a pomocných bitů (feedback_bit, control_bit)

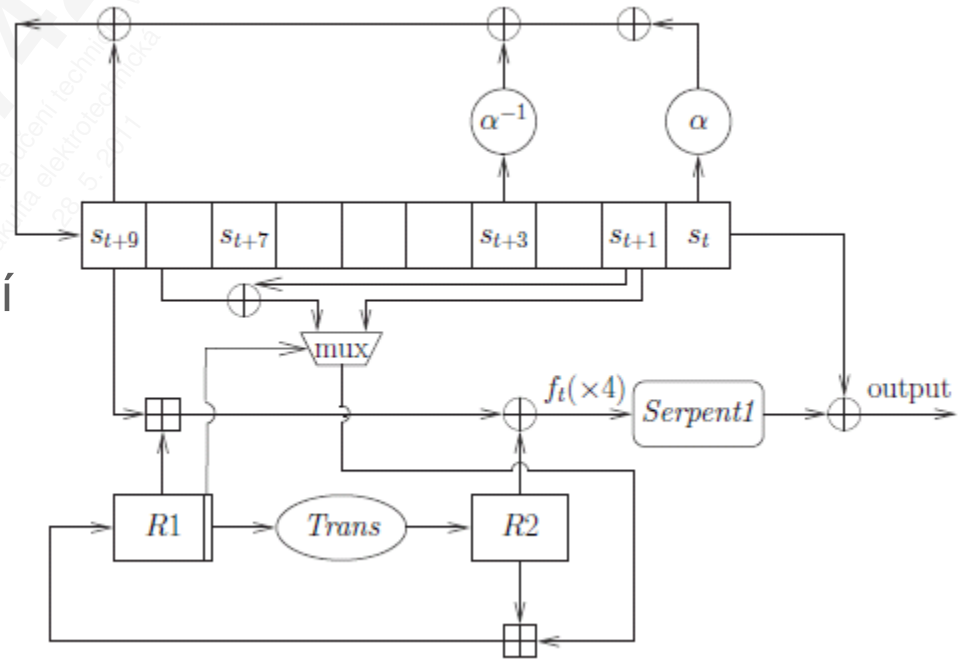
E-stream Profile 1 - Rabbit

- K …128 bitů
- IV … 64 bitů
- SW implementace
- RFC 4503
- s *(K,IV)* lze zašifrovat 2^{64} 128bitových bloků
- vnitřní stav …513b
  - osm 32bitových registrů *x*
  - osm 32bitových čítačů *c*
  - jeden „carry“ bit



E-stream Profile 1 - SOSEMANUK

- K …128 bitů
- IV …128 bitů
- SOSEMANUK = „snow snake“ v jazyce kmene Cree
  - LFSR
    - deset 32bitových čísel
    - operace v F_2^{32}
  - modifikovaný Serpent
    - bez přičítání klíčů
    - bez lineárních transformací
  - FSM - 64b paměti
    - realizováno registry R1,R2
    - v každém kroku FSM vezme data z LSFR, aktualizuje R1,R2 a vygeneruje 32b výstupu

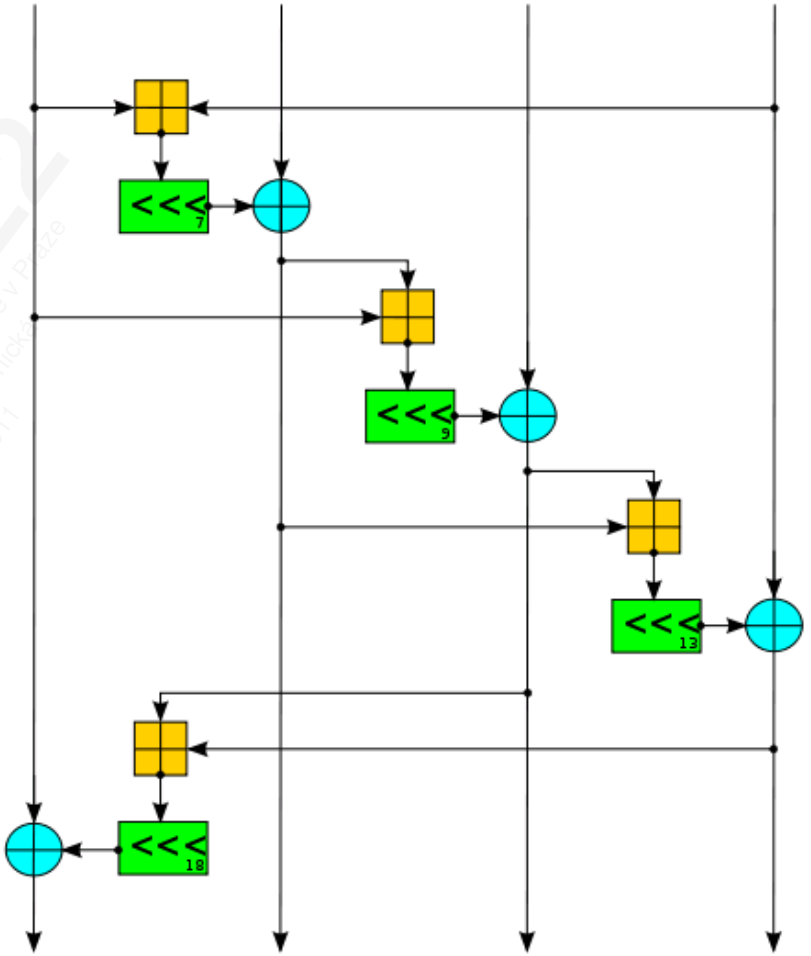


E-stream Profile 1 – HC128

- K …128 bitů
- IV …128 bitů
- pro (K,IV) lze vygenerovat 2^{64}b proudu klíče
- dvě tabulky P,Q – každá obsahuje 512 32bitových prvků
- operace v mod 2^{32} a mod512
- šest nelineárních funkcí
  - dvě funkce realizují stejné operace jako v SHA-256
  - dvě funkce realizují jiné nelineární operace podobného typu jako v SHA-x (ale ne stejné)
  - dvě funkce používají tabulku P reps. Q jako S-box

E-stream Profile 1 – Salsa20/12

- K…256 bitů
- nonce … 64bitů
- číslo bloku … 64 bitů
- výstup…512 bitů
- Salsa 20/12 používá 12 rund z 20
- jádrem Salsa 20 je hashovací funkce s 64B vstupem/výstupem
- hashovací funkce je použita v CTR režimu, kdy se chová jako proudová šifra



Dotazy