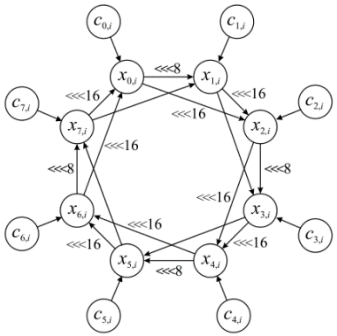
České vysoké učení technické v Praze
Fakulta elektrotechnická
Katedra telekomunikační techniky



Proudové šifry

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

Osnova

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

Proudové 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

Proudové šifry

Shanonnova 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

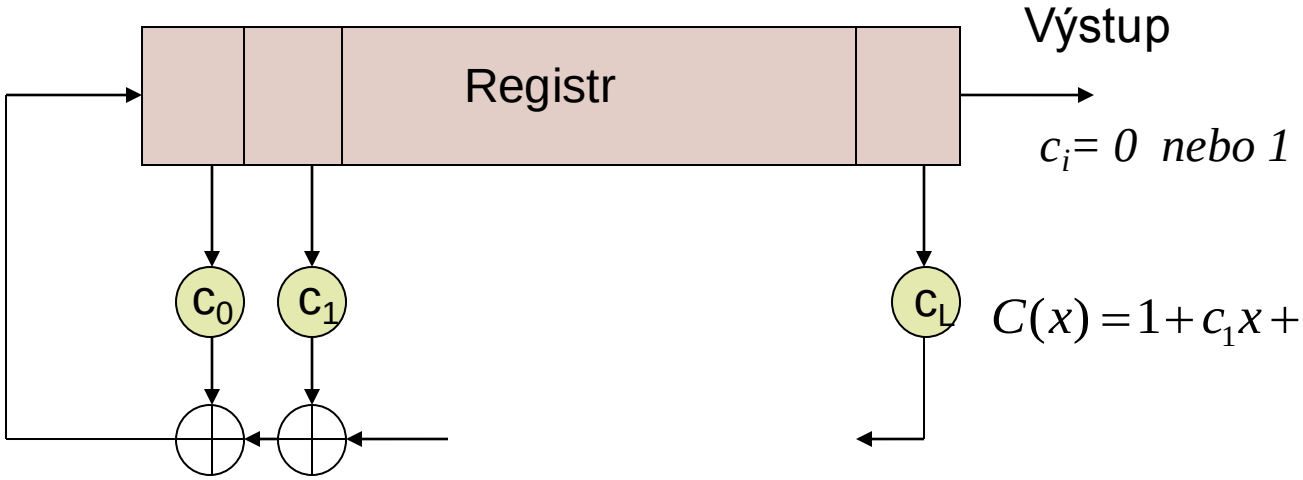
Posuvné registry

- Klasické proudové šifry byly založeny na posuvných registrech (shift register)
- posuvný registr obsahuje
  - množina stavů každý obsahující jeden bit
  - zpětnovazební funkci

- dnes se využívají i jiné přístupy:
  - 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



$$C(x) = 1 + c_1 x + c_2 x^2 + \cdots + c_L x^L$$

- *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.

Kryptograficky silné posloupnosti

- Posloupnost (sekvence) čísel je **kryptograficky silná**, pokud může realizovat „dobrý“ proud klíče (keystream)
  - slovo „dobrý“ se vztahuje k určitým kvalitativním kritériím
- Kryptograficky silné posloupnosti musí být **nepředvídatelné**
  - Známy OT odhalí část proudu klíče (keystream)
  - Útočník nesmí být schopný získat větší část proudu klíče z kratšího zachyceného segmentu
- Nízká lineární složitost generátoru implikuje předvídatelnost výstupu
  - Berlekamp-Massey algoritmus
  - **Dobrý proud klíče musí mít velkou lineární složitost!**

Proudové šifry založené na LFSR

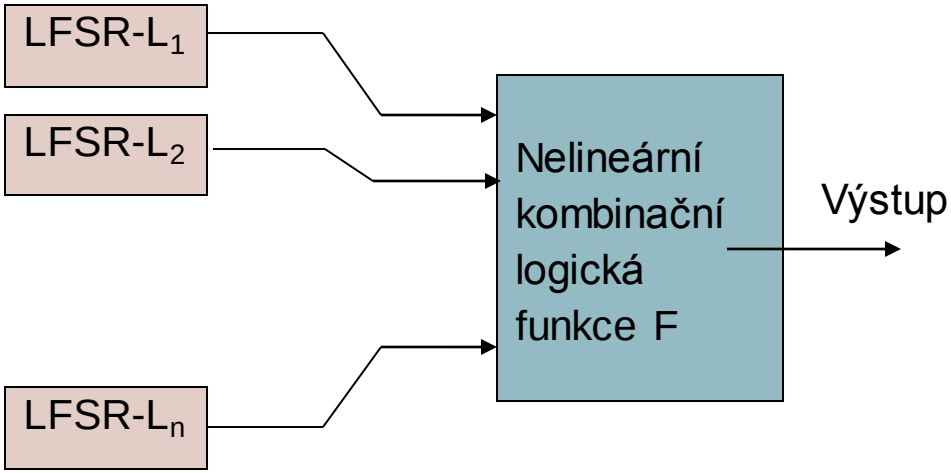
Existují dva základní přístupy, jak realizovat proudovou šifru založenou na LFSR:

- jeden LFSR s nějakou nelineární kombinační funkcí
- více LFSR propojených nelineární funkcí

V obou případech slouží klíč K k počátečnímu naplnění LFSR.

Proud klíče je výstup z nelineární funkce.

Nelineární kombinování LFSR



Kombinační funkce má mít následující vlastnosti:

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

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

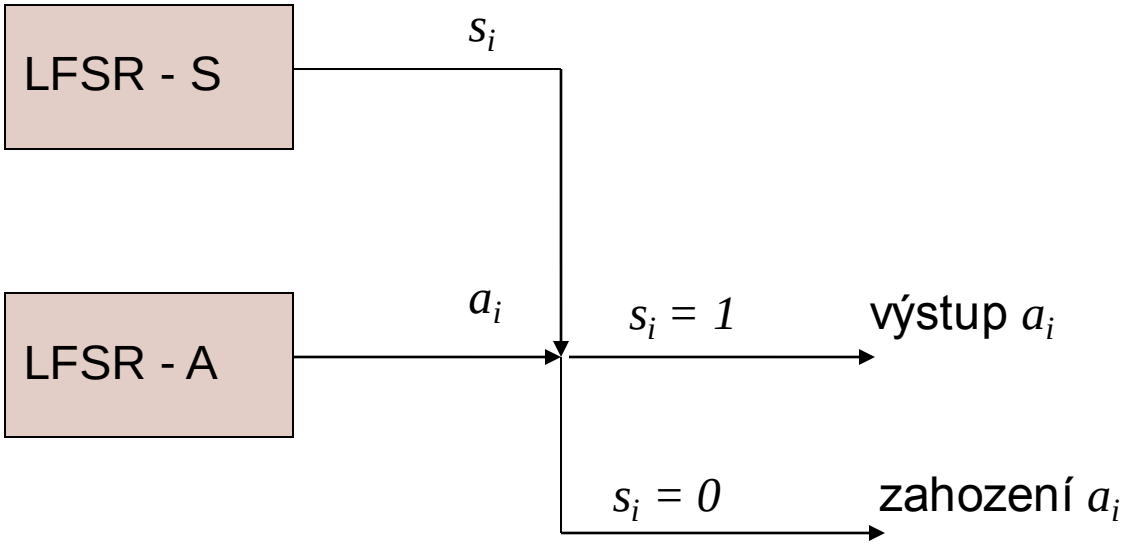
- funkce F kombinující tři LFSR je vyvážená
- existuje velká korelace mezi x_1 a z, protože

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

Proto funkce F není bezpečná (jako proudová šifra).

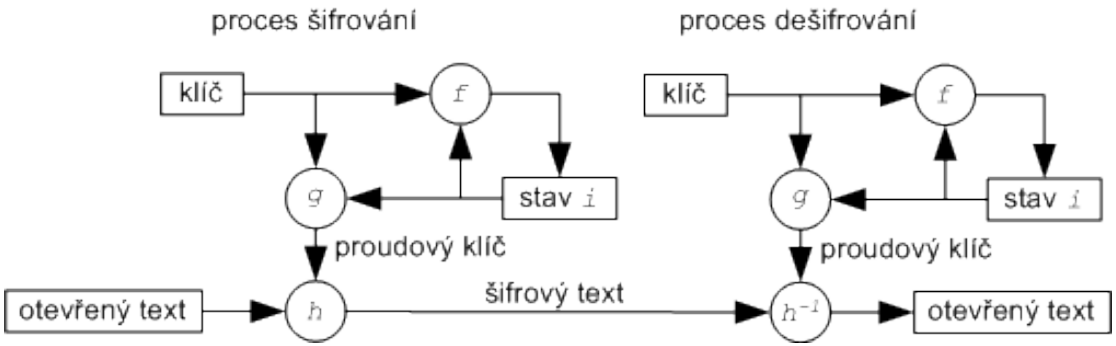
LFSR řízené hodinovým taktem

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



Synchronní proudová šifra

- SSC – Synchronous Stream Cipher
- proud klíče (key stream) je generován nezávisle na OT/ŠT
- 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

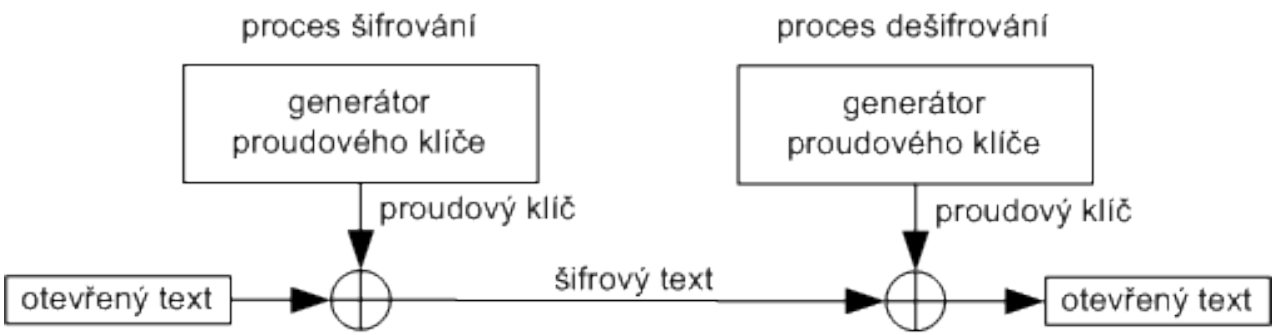


Synchronní proudová šifra

- 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

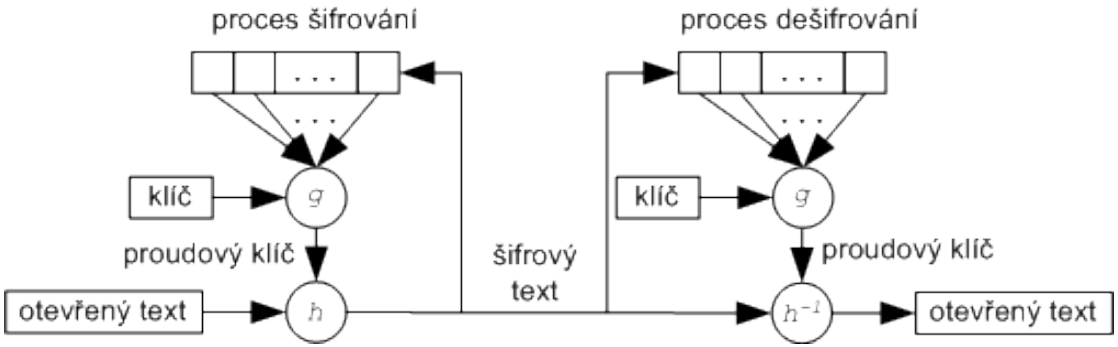
Binární aditivní proudová šifra

- BASC – Binary Additive Stream Cipher
- speciální případ synchronní proudové šifry
- binární reprezentace OT a ŠT (bity)
- výstupní funkce *h* je funkce XOR
- RC4, A5



Asynchronní proudové šifry

- SSC - Self-synchronnizing Stream Cipher
  - proudové šifry s vlastní synchronizací nebo
  - samosynchronizující se šifry nebo
  - CTAK – Cipher Text Auto Key
- proud klíče závisí na OT/ŠT
- proudový klíč je generován v závislosti na
  - klíči K
  - pevně daném počtu bitů předchozího ŠT



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
- Příklady:
  - CFB režim blokových šifer

Současné proudové šifry

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

- časté HW implementace

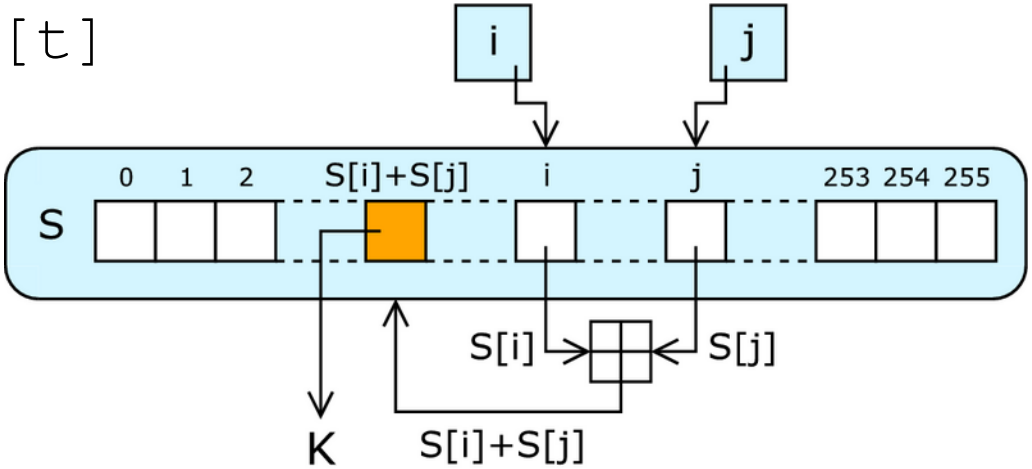
Proudová šifra RC4

- 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

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 - 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
    - konstantní 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 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 → prolomení v řádu ms
  - 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

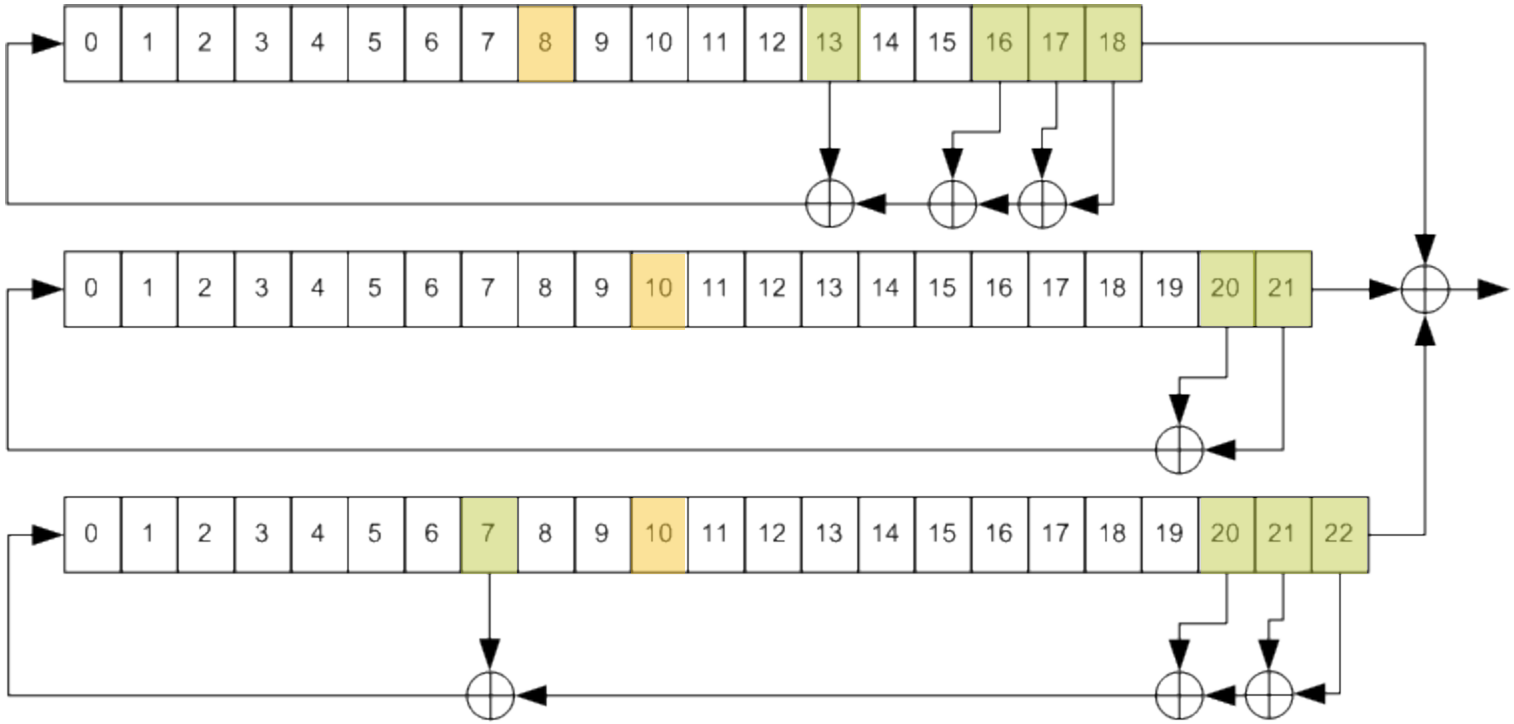
- šifrování na rádiovém rozhraní sítě mezi MS a BTS
  - šifrovací algoritmus A5 je uložen v MS
  - je stejný pro všechny operátory (proč ?)
  - klíč generován pomocí A8 uloženým na SIM kartě
- specifikace A5 nebyla nikdy oficiálně publikována
- vstup do A5:

  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 ($x_0, x_1, \ldots, x_{17}, x_{18}$)
  - Y: 22 bitů ($y_0, y_1, \ldots, y_{20}, y_{21}$)
  - Z: 23 bitů ($z_0, z_1, \ldots, z_{21}, z_{22}$)
- 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

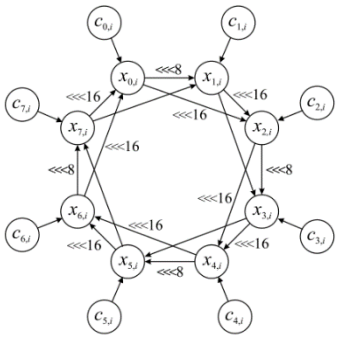
Varianty A5

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 (霞)

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)
- kniha New Stream Cipher Designs
  - The eSTREAM Finalists
  - ISBN 978-3-540-68351-3



Projekt eSTREAM

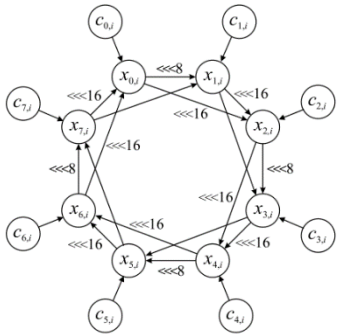
3 fáze výběrového řízení

- 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:

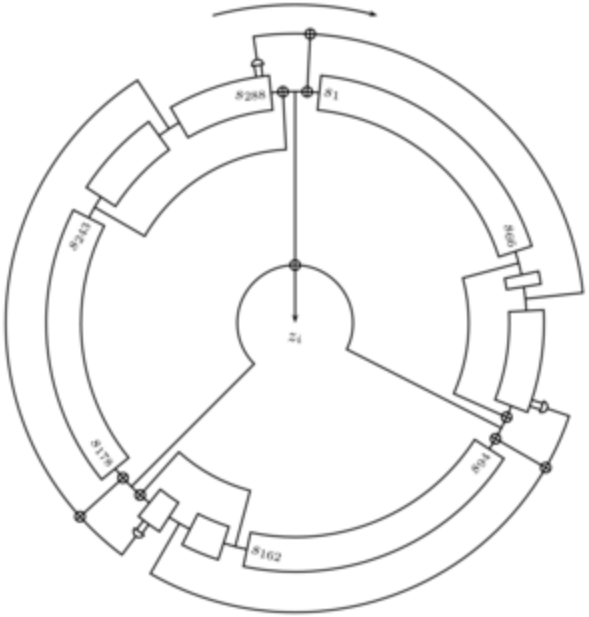
Profil 1	**Profil 2**
HC-128	Grain v1
Salsa 20/12	MICKEY v2
SOSEMANUK	Trivium
Rabbit	F-FCSR (později vyřazen)



- každých 6 měsíců by měl být revidován

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



$$X_i = Z_{i-66} \oplus Z_{i-111} \oplus Z_{i-110} \otimes Z_{i-109} \oplus X_{i-69}$$

$$Y_i = X_{i-66} \oplus X_{i-93} \oplus X_{i-92} \otimes X_{i-91} \oplus Y_{i-78}$$

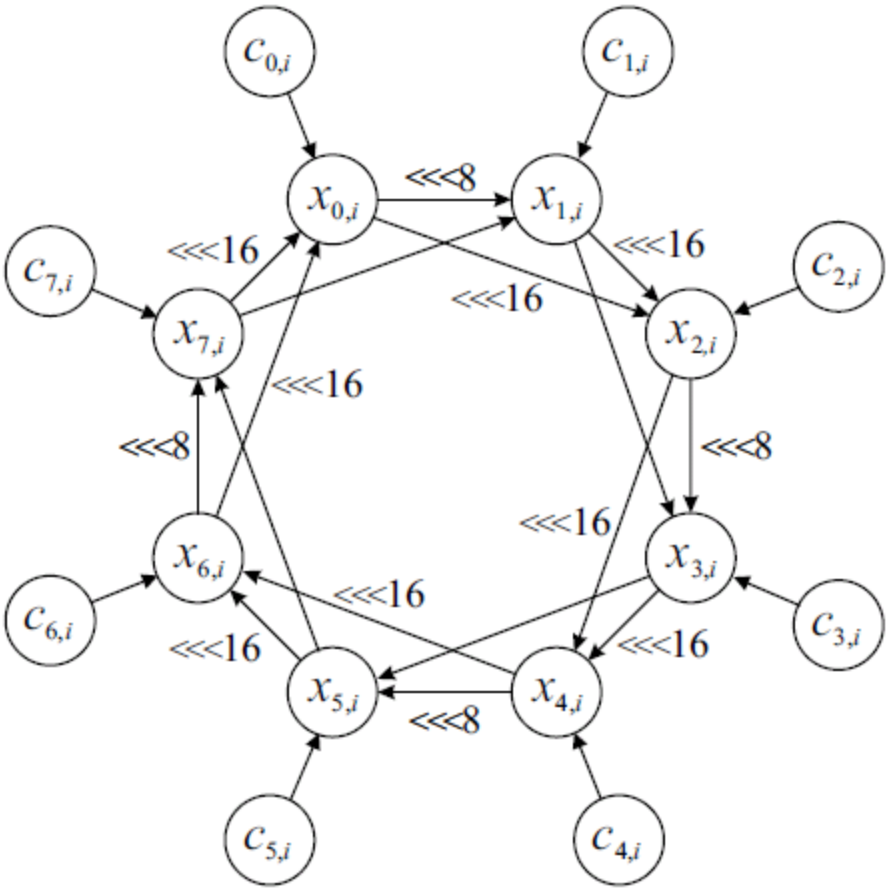
$$Z_i = Y_{i-69} \oplus Y_{i-84} \oplus Y_{i-83} \otimes Y_{i-82} \oplus Z_{i-87}$$

$\otimes$ … AND

$\oplus$ … XOR

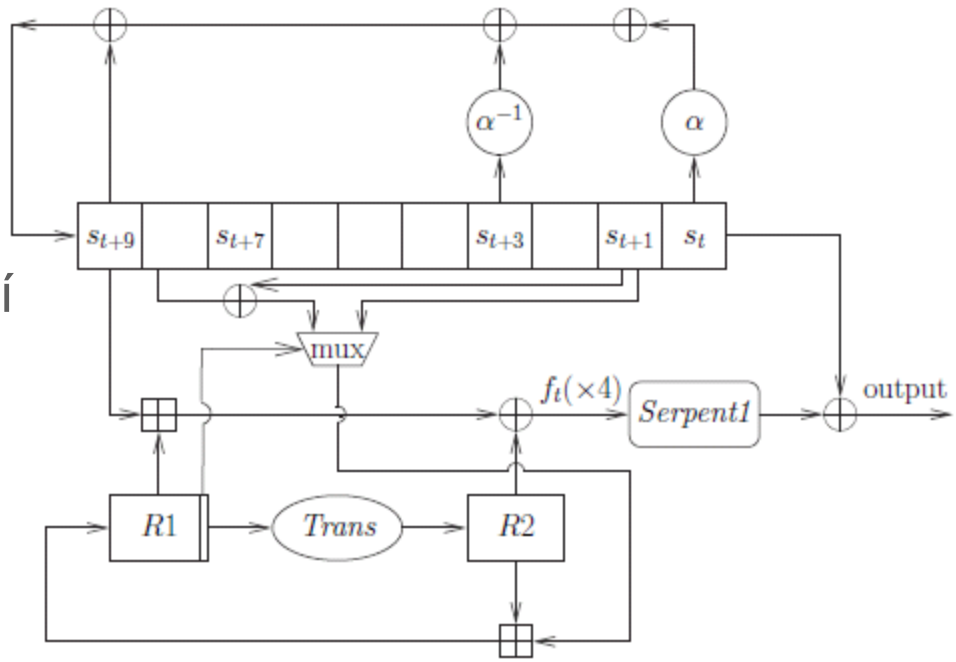
E-stream Profile 1 - Rabbit

- 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



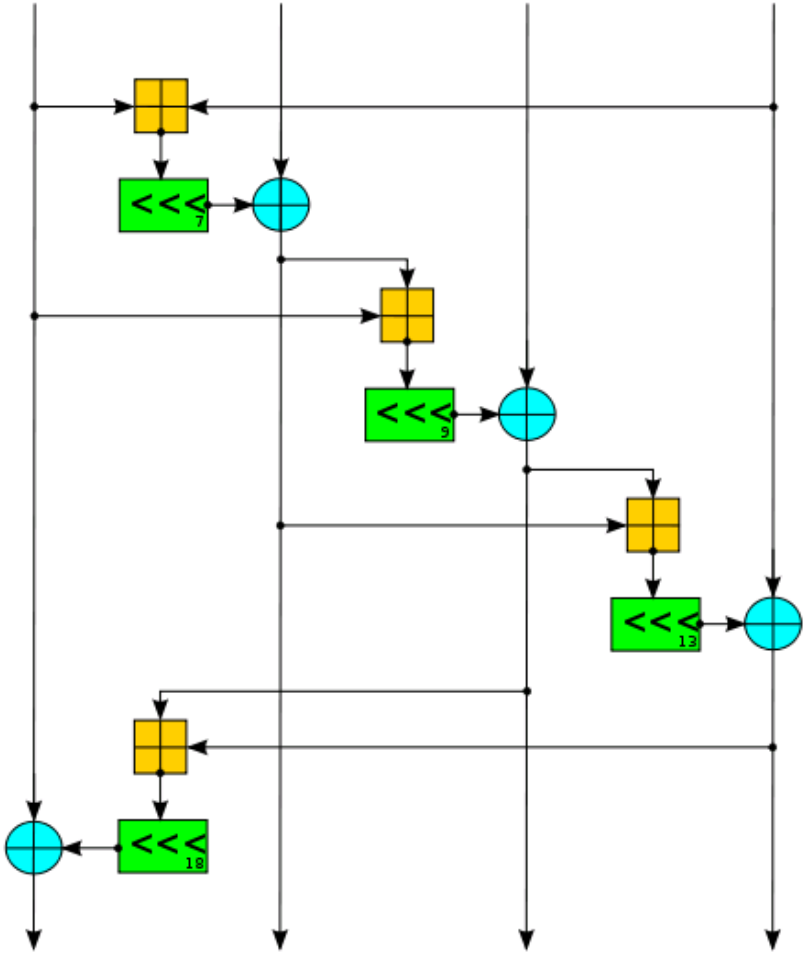
E-stream Profile 1 - SOSEMANUK

- 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 – 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



ChaCha20

- odvozena z šifry Salsa
- „The ChaCha20 cipher is designed to provide 256-bit security.“
  - efektivnější než AES (bez AES-NI)

- použití v konstrukcích typu AEAD
  - AEAD - Authenticated Encryption with Aditional Data
  - spolu s algoritmem Poly1305
    - varianta MAC (Message Authentication Code)

ChaCha20

- RFC 7539 - ChaCha20 and Poly1305 for IETF protocols
  - status „Informational“
  - 07/2015
- RFC 7905 – ChaCha20-Poly1305 CipherSuites for TLS
  - 06/2016
- podporována v TLS 1.2
  - v Chrome od verze 32 (cca 11/2013)
  - ve Firefoxu od verze 47 (06/2016)
- alternativa k AES-GCM

Dotazy