Útoky na šifru HBB

Vlastimil Klíma

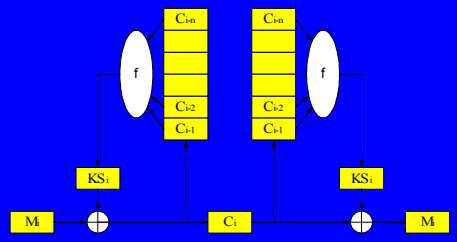
LEC, s.r.o.
Národní 9, 110 00 Praha 1

v.klima@volny.cz, http://cryptography.hyperlink.cz

Mikulášská kryptobesídka, 6. - 7. prosinec 2004, Hotel STEP, Praha

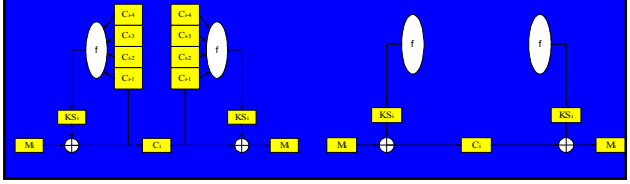
Úvod

- HBB – INDOCRYPT 2003, autorem Palash Sarkar
- Asynchronní šifry – velmi málo návrhů



Základní údaje o HBB

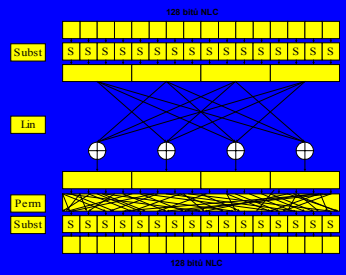
- HBB měla vyplnit mezeru – dva mody B (synchronní), SS (asynchronní)
- Synchronizace na úrovni 128bitových bloků
- Základ HBB je lineární a nelineární blok (NLC 128b, LC 512b – 4 bloky šifrového textu), NLC a LC tvoří funkci f
- V obou modech nalezeny velké slabiny



Základní údaje

- Klíč - 128 nebo 256 bitů
- Inicializační fáze - naplní LC a NLC klíčovým materiálem
- Pracuje se s bloky 128 bitů (heslo, otevřený i šifrový text)
- V každém kroku šifrování (modus B i SS) se pomocí klíče (a eventuelně šifrového textu) aktualizuje LC a NLC a vytvoří se heslo KS
- Přínos HBB byl spatřován v návrhu LC a NLC a jejich kombinaci

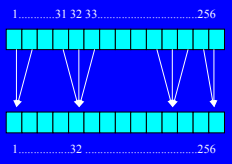
Nelineární blok F



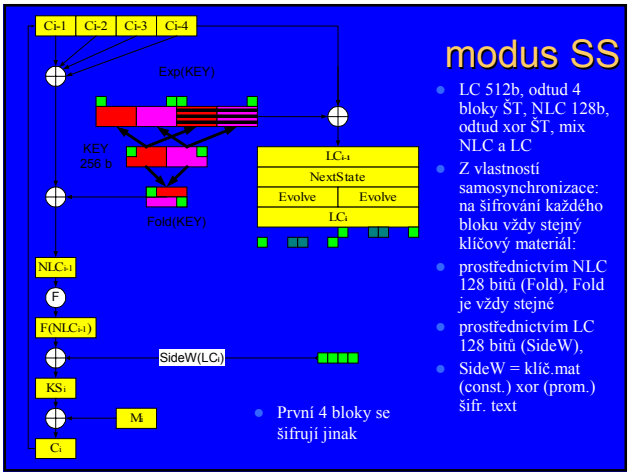
- Vstup klíče je mimo nelineární blok – je součást schématu

Lineární blok, 512 bitů

- 512 bitů, zpracovává se zvlášť po 256 + 256
- $LC_i = NextState(LC_{i-1}) = Evolve_{C1}(LC_{lo}) \parallel Evolve_{C2}(LC_{hi})$
- Evolve = CA:



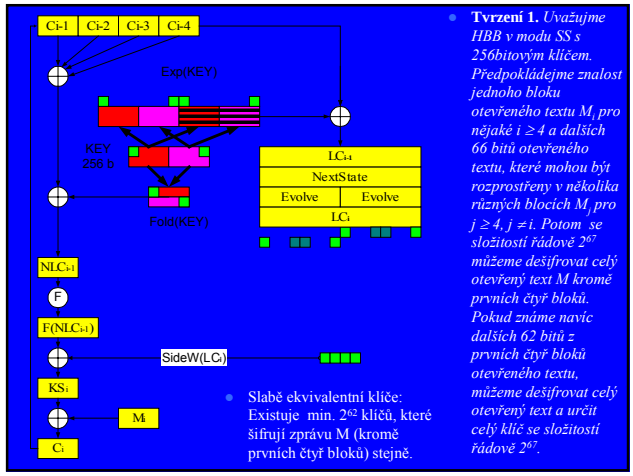
$$S_1 = c_1 s_1 \oplus s_2,$$
$$S_2 = s_1 \oplus c_2 s_2 \oplus s_3,$$
$$S_3 = s_2 \oplus c_3 s_3 \oplus s_4,$$
$$\ldots$$
$$S_{255} = s_{254} \oplus c_{255} s_{255} \oplus s_{256},$$
$$S_{256} = s_{255} \oplus c_{256} s_{256}.$$



modus SS

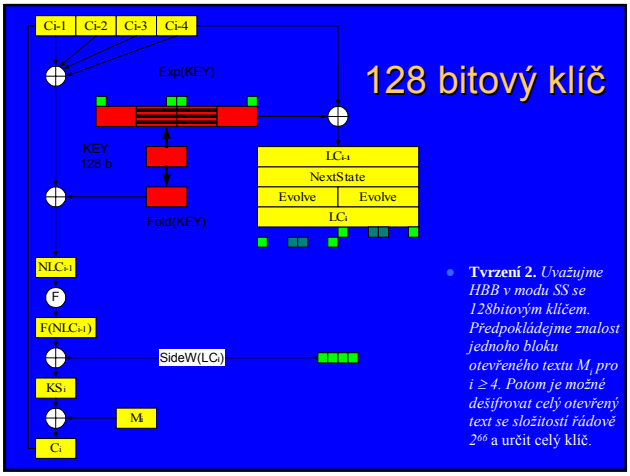
- LC 512b, odtud 4 bloky ŠT, NLC 128b, odtud xor ŠT, mix NLC a LC
- Z vlastností samosynchronizace: na šifrování každého bloku vždy stejný klíčový materiál:
- prostřednictvím NLC 128 bitů (Fold), Fold je vždy stejné
- prostřednictvím LC 128 bitů (SideW),
- SideW = klíč.mat (const.) xor (prom.) šifr. text

- První 4 bloky se šifrují jinak



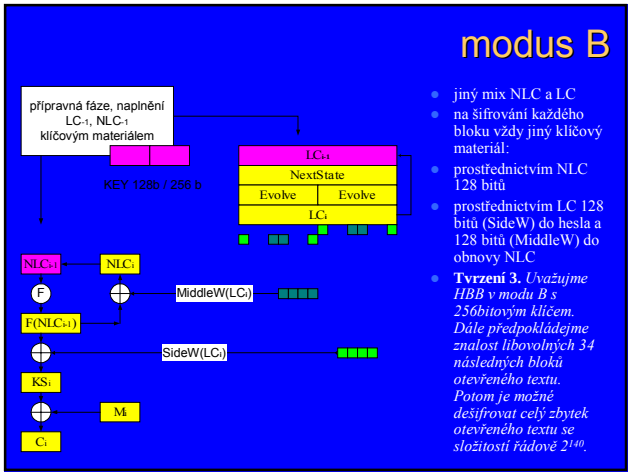
- Slabě ekvivalentní klíče: Existuje min. 2^{62} klíčů, které šifrují zprávu M (kromě prvních čtyř bloků) stejně.

- **Tvrzení 1.** *Uvažujme HBB v modu SS s 256bitovým klíčem. Předpokládejme znalost jednoho bloku otevřeného textu M_i pro nějaké $i \geq 4$ a dalších 66 bitů otevřeného textu, které mohou být rozprostřeny v několika různých blocích M_j pro $j \geq 4, j \neq i$. Potom se složitostí řádově 2^{67} můžeme dešifrovat celý otevřený text M kromě prvních čtyř bloků. Pokud známe navíc dalších 62 bitů z prvních čtyř bloků otevřeného textu, můžeme dešifrovat celý otevřený text a určit celý klíč se složitostí řádově 2^{67}.*



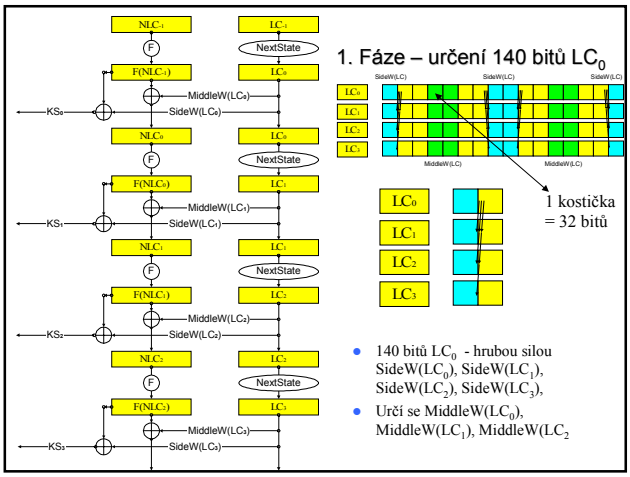
128 bitový klíč

- **Tvrzení 2.** *Uvažujme HBB v modu SS se 128bitovým klíčem. Předpokládejme znalost jednoho bloku otevřeného textu M_i pro $i \geq 4$. Potom je možné dešifrovat celý otevřený text se složitostí řádově 2^{66}* a určit celý klíč.



modus B

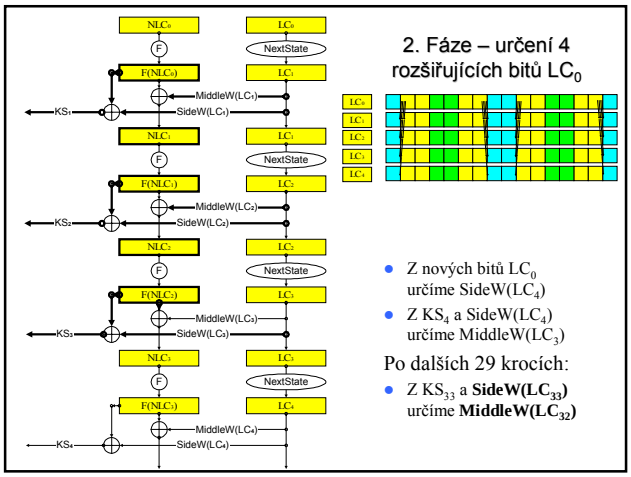
- jiný mix NLC a LC
- na šifrování každého bloku vždy jiný klíčový materiál:
- prostřednictvím NLC 128 bitů
- prostřednictvím LC 128 bitů (SideW) do hesla a 128 bitů (MiddleW) do obnovy NLC
- **Tvrzení 3.** *Uvažujme HBB v modu B s 256bitovým klíčem. Dále předpokládejme znalost libovolných 34 následných bloků otevřeného textu. Potom je možné dešifrovat celý zbytek otevřeného textu se složitostí řádově 2^{140}.*



1. Fáze – určení 140 bitů LC_0

1 kostička = 32 bitů

- 140 bitů LC_0 - hrubou silou $SideW(LC_0)$, $SideW(LC_1)$, $SideW(LC_2)$, $SideW(LC_3)$,
- Určí se $MiddleW(LC_0)$, $MiddleW(LC_1)$, $MiddleW(LC_2$

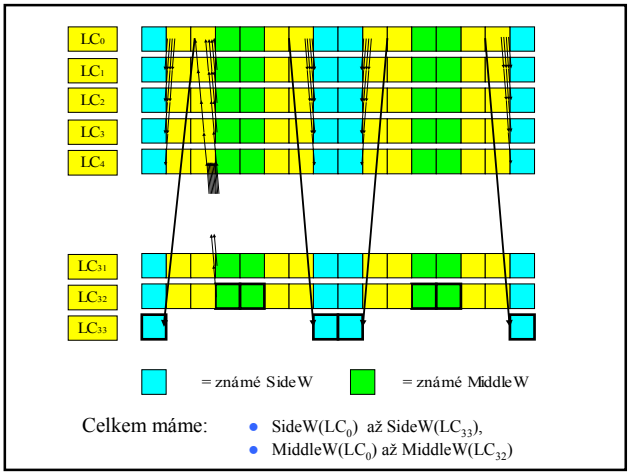


2. Fáze – určení 4 rozšiřujících bitů LC_0

- Z nových bitů LC_0 určíme $SideW(LC_4)$
- Z KS_4 a $SideW(LC_4)$ určíme $MiddleW(LC_3)$

Po dalších 29 krocích:

- Z KS_{33} a **$SideW(LC_{33})$** určíme **$MiddleW(LC_{32})$**



Literatura

- Sarkar, P.: Hiji-bij-bij: A New Stream Cipher with a Self-synchronizing Mode of Operation, in *Proc. Of Progress in Cryptology - INDOCRYPT 2003*, Dec. 2003, Springer-Verlag, Lecture Notes in Computer Science, Vol. 2904, pp. 36 - 51, 2003.