O speciálních blokových šifrách a speciálních hašovacích funkcích

Vlastimil Klíma

Nezávislý kryptolog,
v.klima (at) volny.cz, http://cryptography.hyperlink.cz

Mikulášská kryptobesídka 2007, Praha, Hotel Olympik,
6. – 7. prosinec 2007, http://mkb.buslab.org/

V tomto příspěvku prezentujeme část výsledků projektů NBÚ Bezpečná hašovací funkce (ST20052005017) a Speciální bloková šifra (ST2005006018)

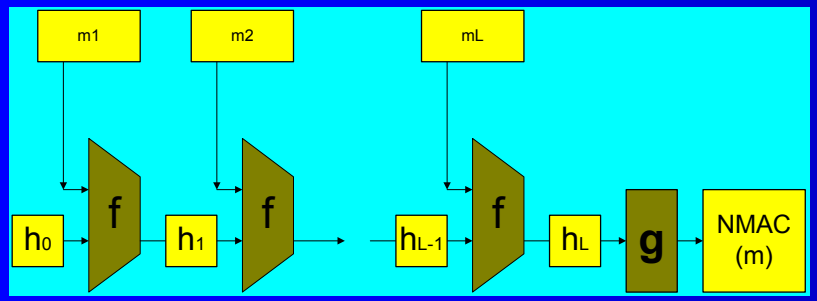
Cíl

- Seznámit s koncepcí, motivací, konstrukčními prvky SBŠ a SHF
- Ukázat širší souvislosti mezi blokovými šiframi a hašovacími funkcemi
- Podnítit kritiku konceptu, vyvolat diskusi, návrh nových variant

Vznik

- 2004: Generické problémy hašovacích funkcí
- 2005: Projekt NBÚ: NEvylepšovat a NEzesilovat existující hašovací funkce a jejich principy, ALE nový princip, vysokou bezpečnost, prokazatelná tvrzení. NE čistě teoretický koncept s vysokou bezpečností, ALE funkce, skutečně použitelné
- 2005: Koncept hašovacích funkcí jako speciálních vnořených autentizačních kódů (SNMAC), v nichž navíc bude použita nikoli klasická, ale speciální bloková šifra, nové důkazy vlastností [CDMP05] [Kli06]
- 2006: Koncept speciálních blokových šifer. Konkrétní instance (třídy) DN, HDN. [Kli07]

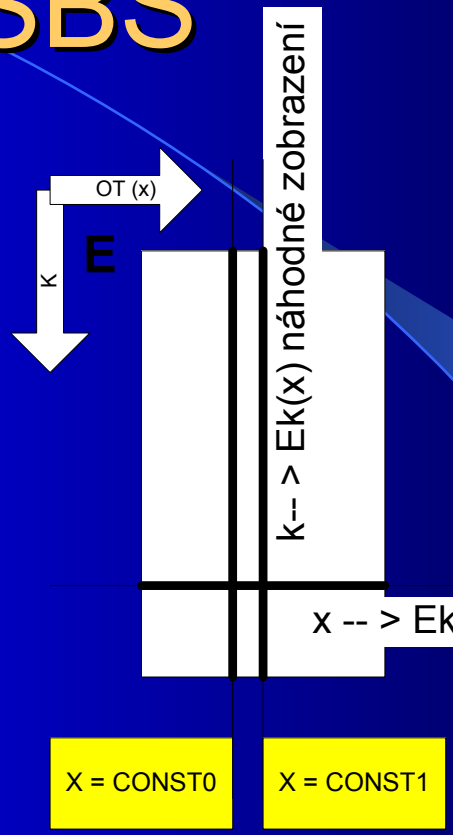
SNMAC se SBŠ

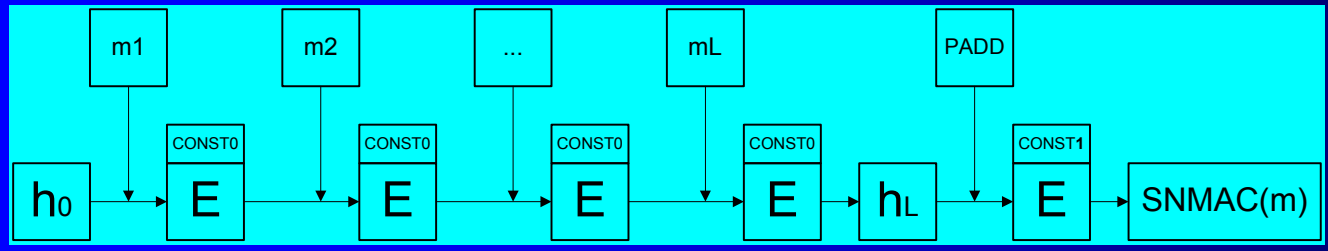


Náhodná orákula

$f: k \rightarrow E_k(Const0)$

$g: k \rightarrow E_k(Const1)$





Výhoda průchodu přes klíč:
jednosměrnost

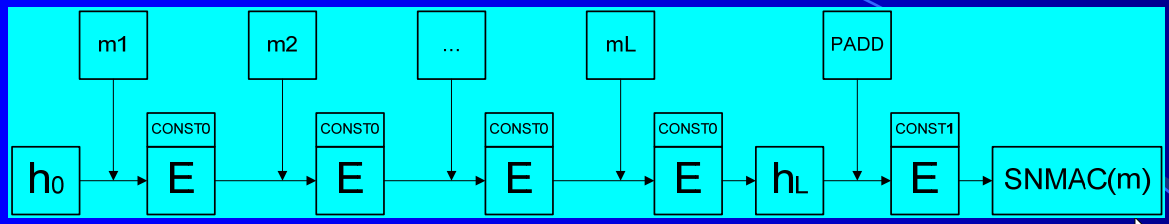
homogenita, náhodnost,

Komprese

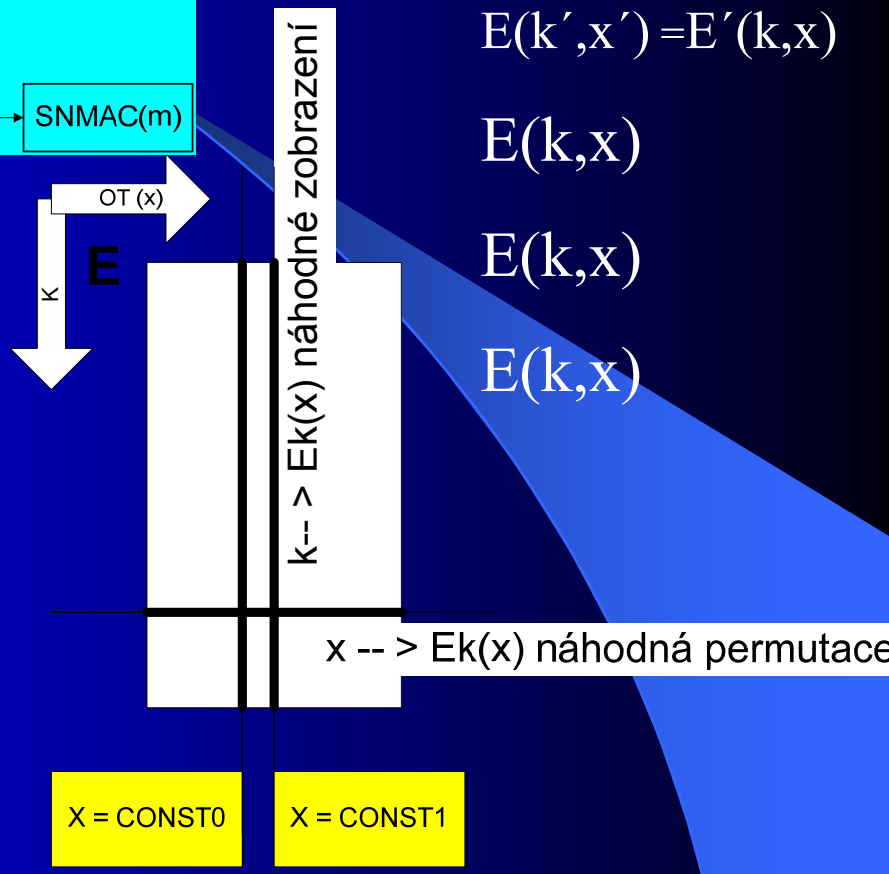
Nutno ještě zajistit odolnost proti DC,LC ***přes klíč***

SNMAC se SBŠ se chová jako náhodné orákulum, máme důkazy odolnosti proti nalezení kolize a vzoru, víc nepotřebujeme → nutnost držet se této konstrukce

Požadavky na SBŠ



- Jako klasická BŠ byla odolná proti různým (diferenčním, lineárním a tisíci dalším) útokům, vedeným z OT, nyní SBŠ stejně odolná proti útokou vedenému (zejména) z klíčového vstupu
- A ponecháme i … ze vstupu OT, neboť chceme, aby SBŠ byla náhodné zobrazení pro 2 konstantní OT … → raději pro všechny řezy OT, a tudíž i pro jejich vztahy (je to BR)
- Vzhledem k vlastnosti homogenity chceme více:
- Mezi (k, x, $y=E_k x$) nesmí existovat využitelné vztahy (LC, DC samozřejmé, ale nejen ty)
- Tedy:….Bloková šifra musí být kvalitní „v ploše, dvojrozměrně, lokálně i globálně“, nejen v řezech klíčem nebo otevřeným textem
- Lapidární minimum: … Klíč musí být zpracováván stejně kvalitně jako OT



Poznámka: Komplementárnost

$E(k',x') = E'(k,x)$

$E(k,x)$

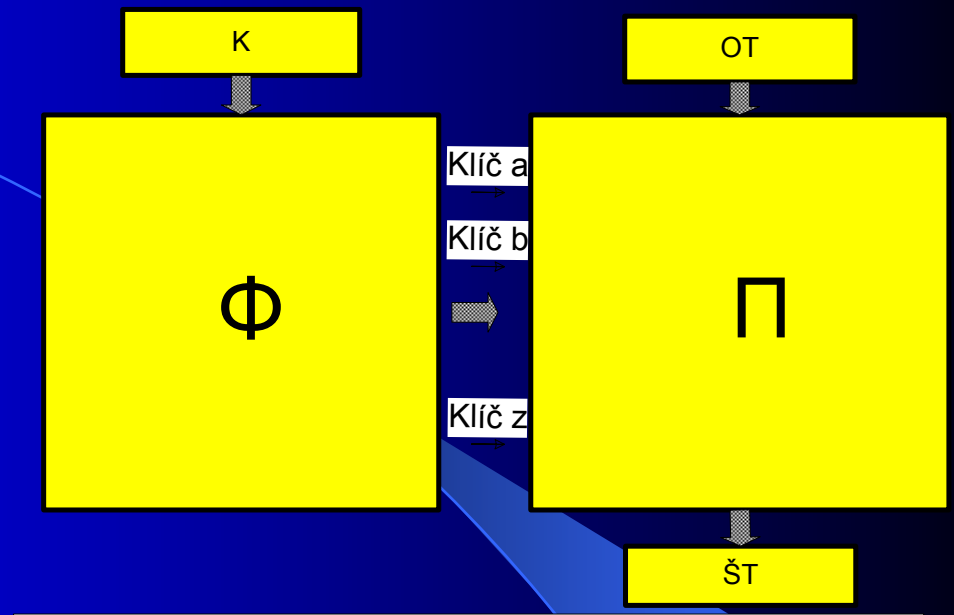
$E(k,x)$

$E(k,x)$

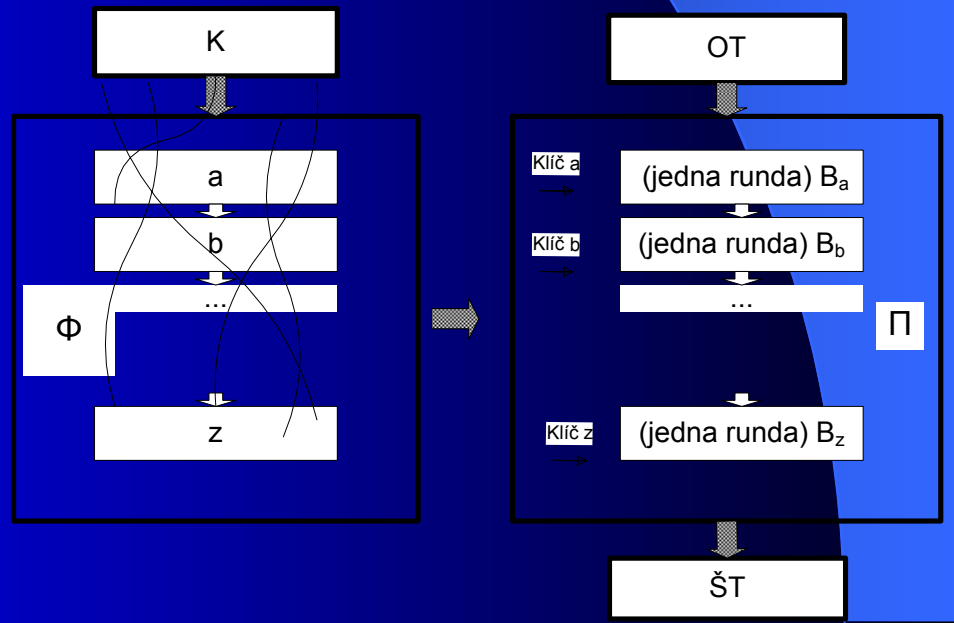
Poznámka: Komplementárnost – lineární vztah v ploše, (z jiného úhlu pohledu „Lin. vztah, prostupující schématem“)

Dvojitá síť

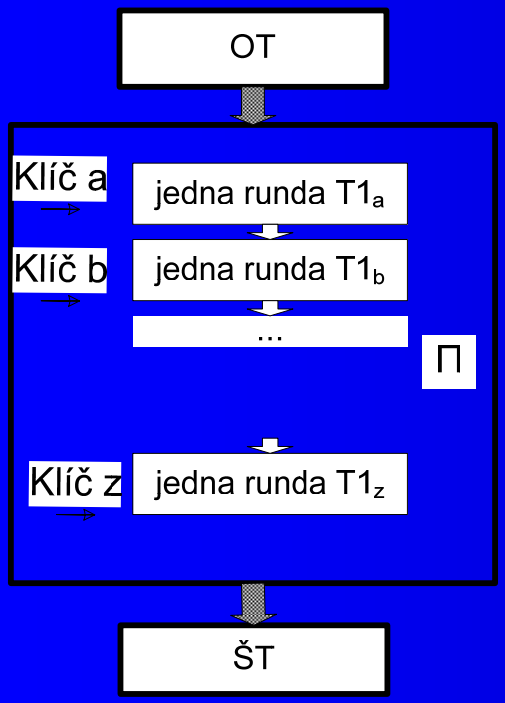
- Většina současných blokových šifer má strukturu „dvojité sítě“ – odráží „dva přístupy“ ke zpracování vstupů
- FI je expanze klíče, PI je součinová šifra
- Drtivá většina z nich má funkci PI silnou a funkci FI slabou

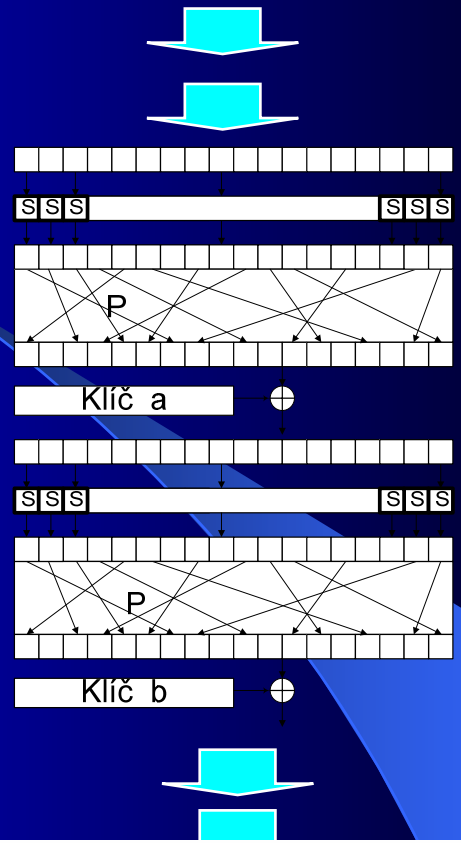


DES: Funkce Φ = „COPY BIT“, Funkce B = jedna runda
Diference v klíči se propagují přímo do proměnných a,b,…,z



Funkce PI





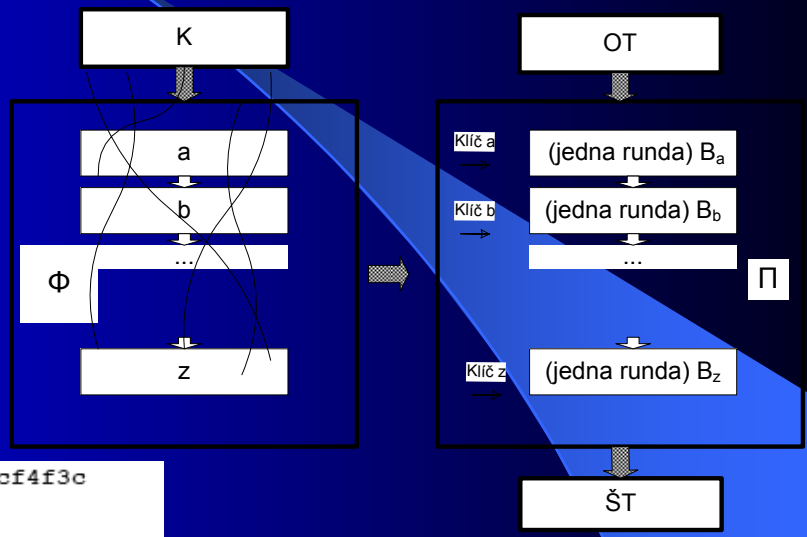
$$B_k = T1_{k16} \bullet \ldots \bullet T1_{k9} \bullet T1_{k8} \bullet T1_{k7} \bullet T1_{k6} \bullet T1_{k5} \bullet T1_{k4} \bullet T1_{k3} \bullet T1_{k2} \bullet T1_{k1}$$

- Součinové šifry, předpoklad nezávislosti rundovních klíčů
- Závislé klíče se mohou „vyrušit“ nebo jinak negativně působit
- Předpoklad nezávislosti rundovních klíčů (nutný k důkazům) opomíjen u moderních BŠ

Závislost klíče u DES, AES

- AES: Pouze 4 nové nelineární bajty ze 16 v každém rundovním klíči
- (mírné zesložitění v mezích tržního zákona, neřeší problém důsledně) – do diskuse
- Velká závislost v rundovních klíčích, nesložité vztahy

DES: Funkce Φ = „COPY BIT“, Funkce B = jedna runda
Diference v klíči se propagují přímo do proměnných a,b,…,z



$w_0 = 2b7e1516$ $w_1 = 28aed2a6$ $w_2 = abf71588$ $w_3 = 09cf4f3c$

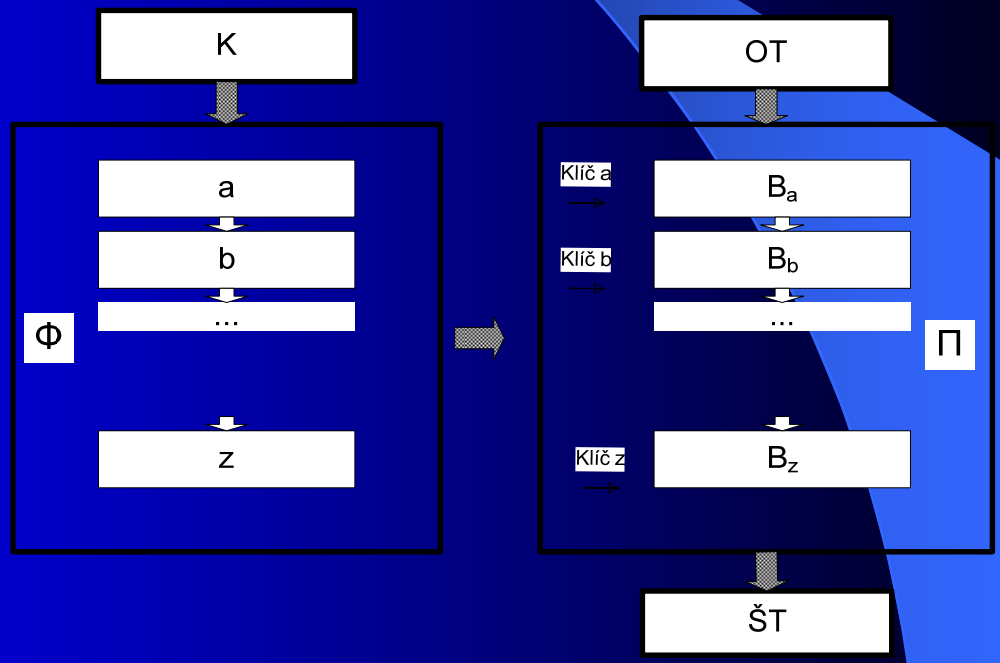
i (dec)	temp	After RotWord()	After SubWord()	Rcon[i/Nk]	After XOR with Rcon	w[i-Nk]	w[i]= temp XOR w[i-Nk]
4	09cf4f3c	cf4f3c09	8a84eb01	01000000	8b84eb01	2b7e1516	a0fafe17
5	a0fafe17					28aed2a6	88542cb1
6	88542cb1					abf71588	23a33939
7	23a33939					09cf4f3c	2a6c7605
8	2a6c7605	6c76052a	50386be5	02000000	52386be5	a0fafe17	f2c295f2
9	f2c295f2					88542cb1	7a96b943
10	7a96b943					23a33939	5935807a
11	5935807a					2a6c7605	7359f67f

- Výmluva:
- utajenost klíče – nemožné u hašovacích funkcí

Princip dvojité sítě DN

$$\Pi = B_z \bullet \ldots \bullet B_b \bullet B_a$$

- Předpokládejme blokové šifry B místo transformací T1
- Chceme nezávislé klíče a, b, …, z



Nezávislost u dvojité sítě DN

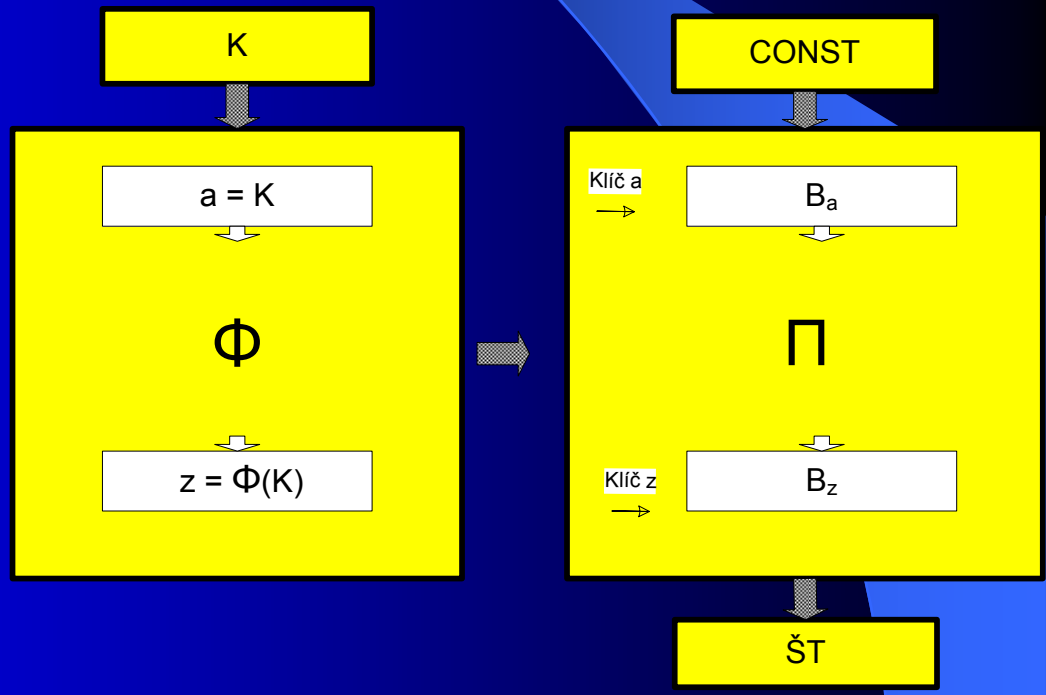
- Nejjednodušší varianta :

$$\Pi = B_z \bullet B_a$$

- Předpokládejme dva nezávislé klíče: a, z

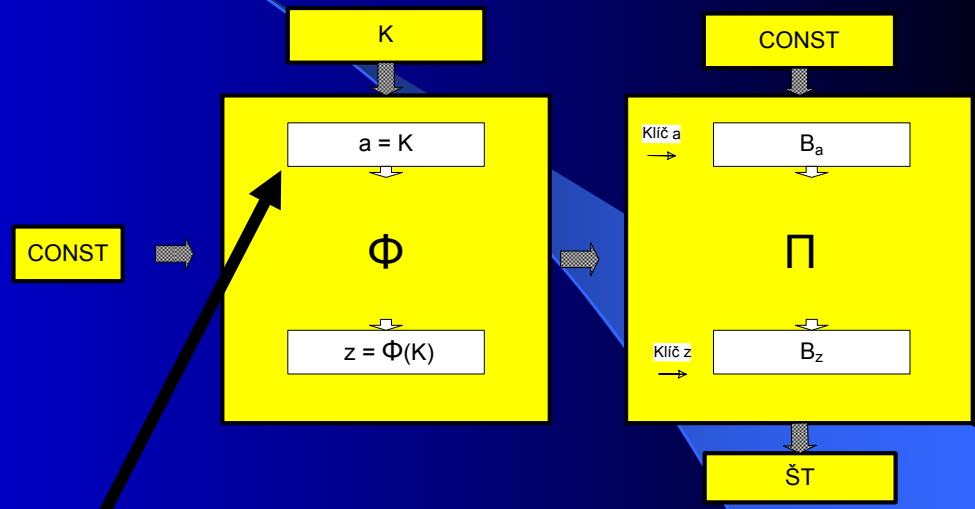
a (=K) a *z* (=Φ(K)) nezávislé

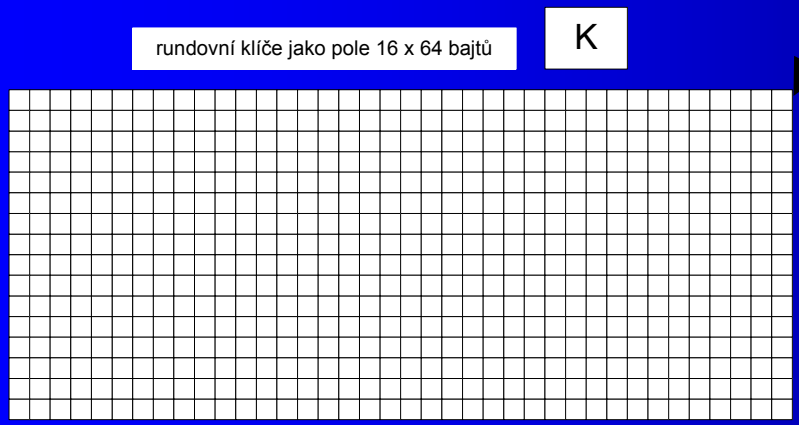
B_z (B_a(Const))



Konstrukce FI a rozměry DN

- Hašový kód 512 bitů
- ..16 rund B
- Rozměry pole klíčů 16 x 64 bajtů = 8192 bitů
- Bloková šifra s délkou bloku 8192 bitů ?



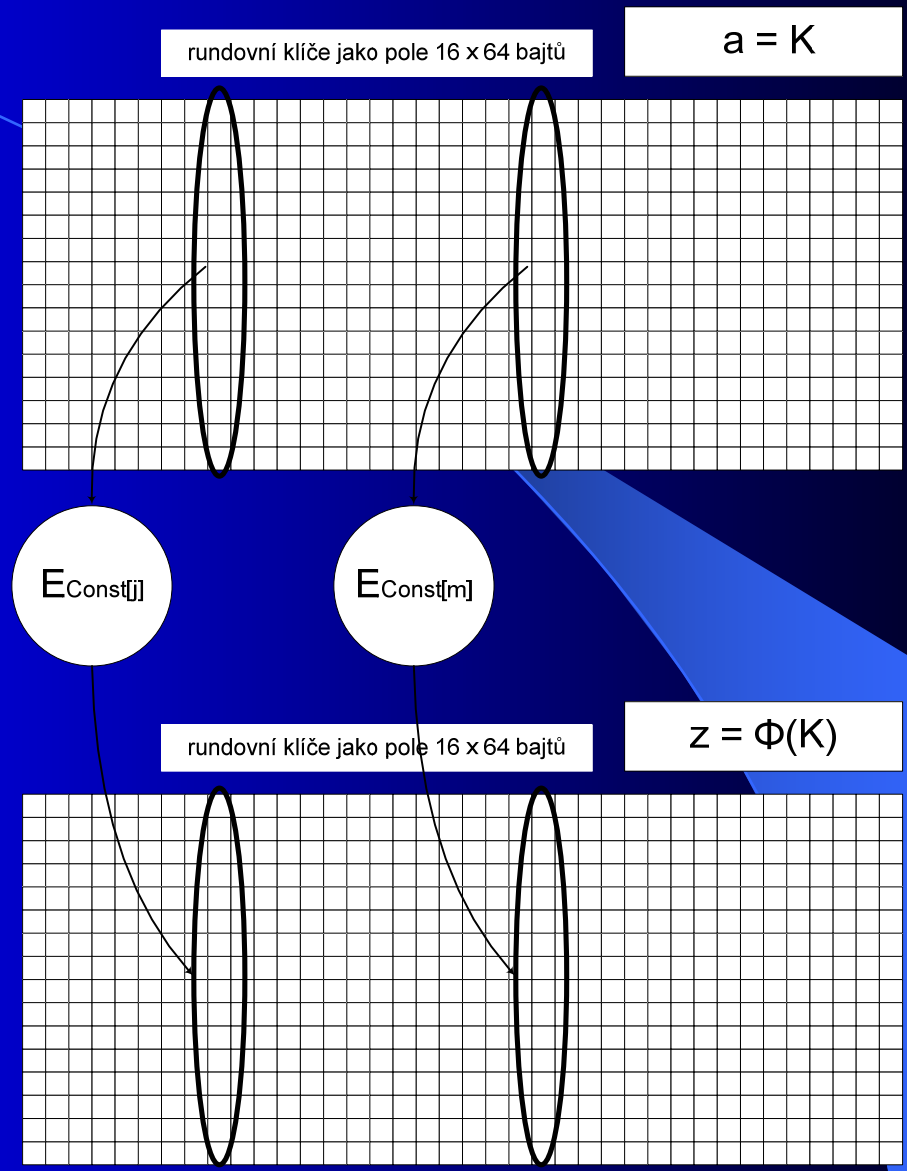


Sloupcová transformace

zvolíme nezávislé náhodné permutace

$E_{Const[1]}(*)$,
$E_{Const[2]}(*)$,
… ,
$E_{Const[64]}(*)$

aplikujeme je na sloupce pole K



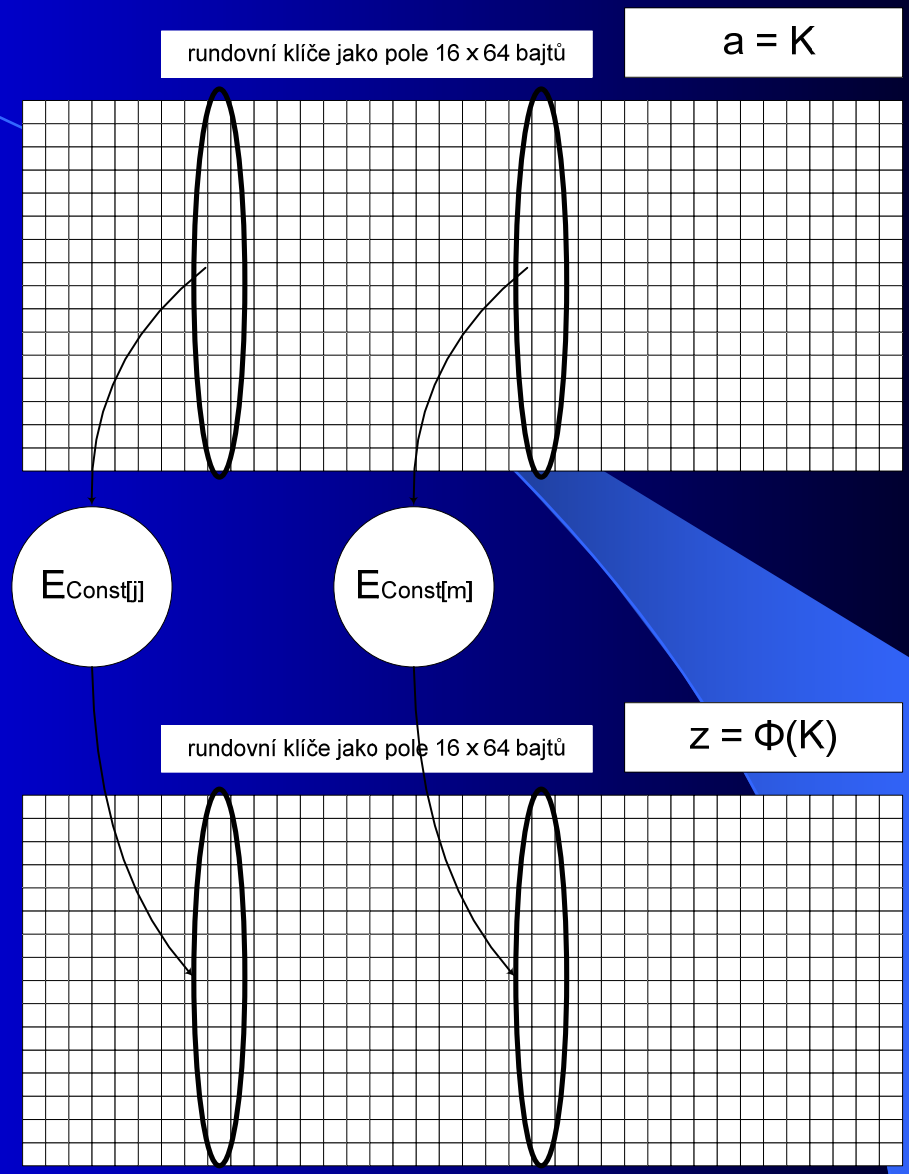
Potom $z = \Phi(K) = (E_{Const[1]}(sloupec_1(K)), E_{Const[2]}(sloupec_2(K)), \ldots, E_{Const[64]}(sloupec_{64}(K))$ je nezávislá na K

Sloupcová transformace

nezávislé náhodné permutace

$AES_{Const[1]}(*)$,
$AES_{Const[2]}(*)$,
… ,
$AES_{Const[64]}(*)$

128 bitů šíře, 10 rund



Potom $z = \Phi(K) = (E_{Const[1]}(sloupec_1(K)), E_{Const[2]}(sloupec_2(K)), \ldots, E_{Const[64]}(sloupec_{64}(K))$ je nezávislá na K

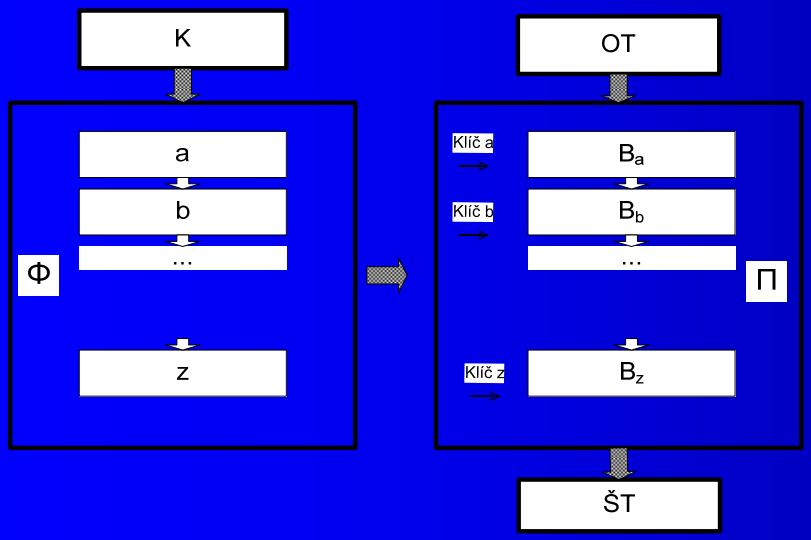
Praktická realizace funkce FI

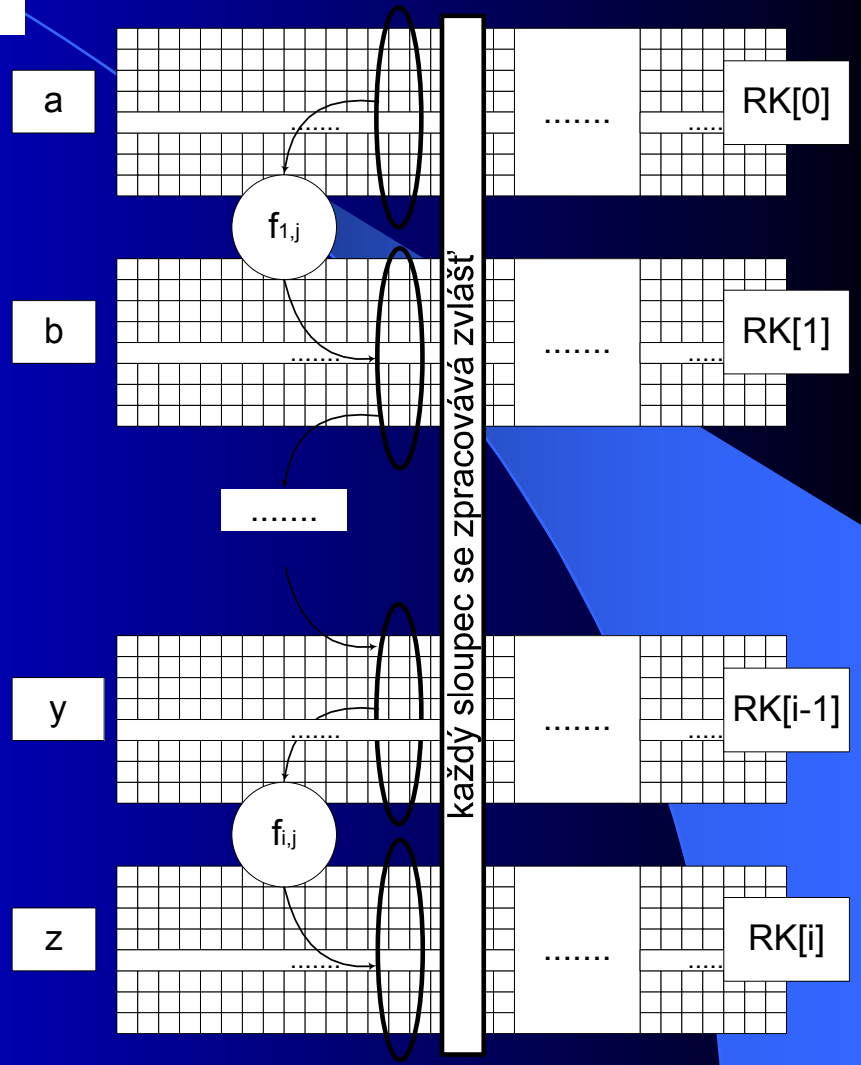
$$\Pi = B_z \bullet \ldots \bullet B_b \bullet B_a$$

DN – parametry n, k, **rho**

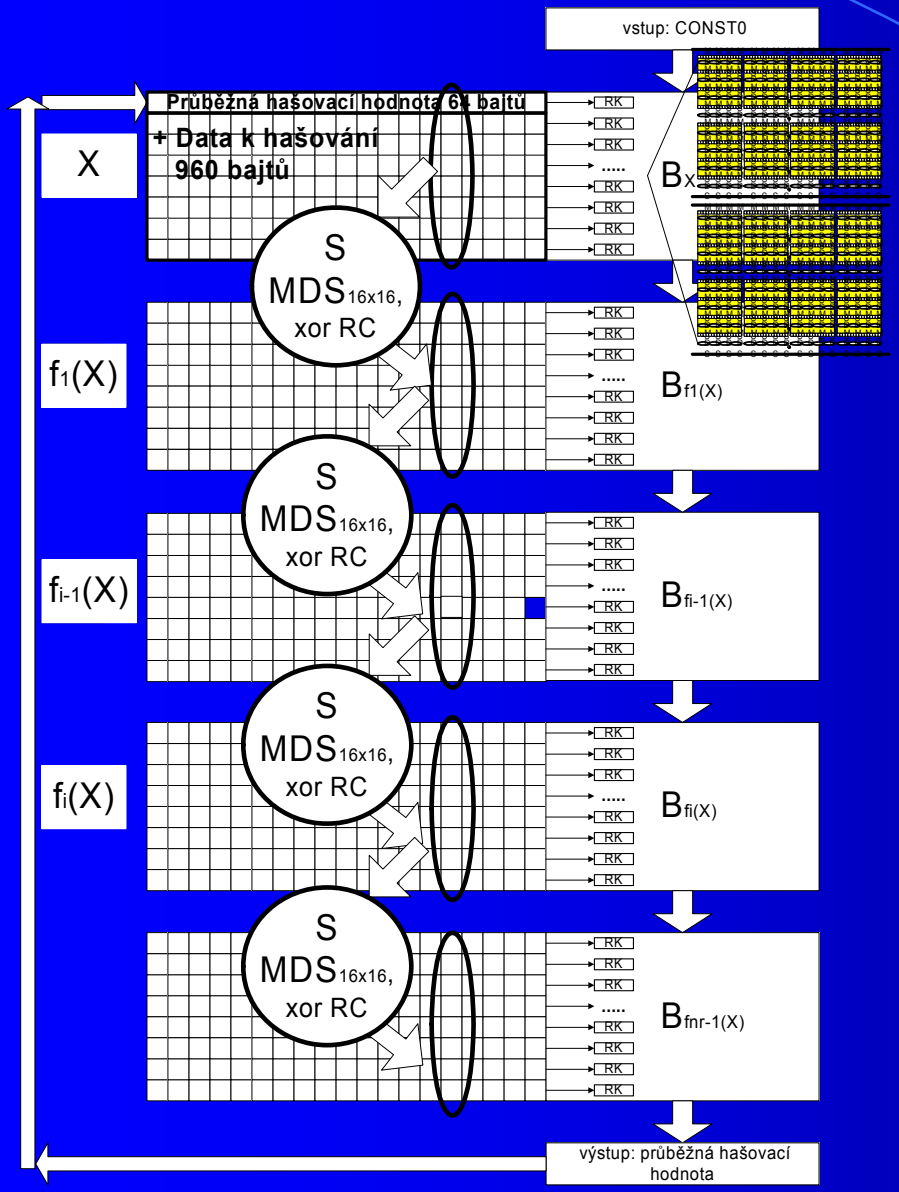
Pole rundovních klíčů – operace probíhají v jednom registru, paralelně (HW, MIL)

Využití zbylých klíčů (HW realizace - čekání, SW – musí se provést, BR)





Praktická realizace funkce PI

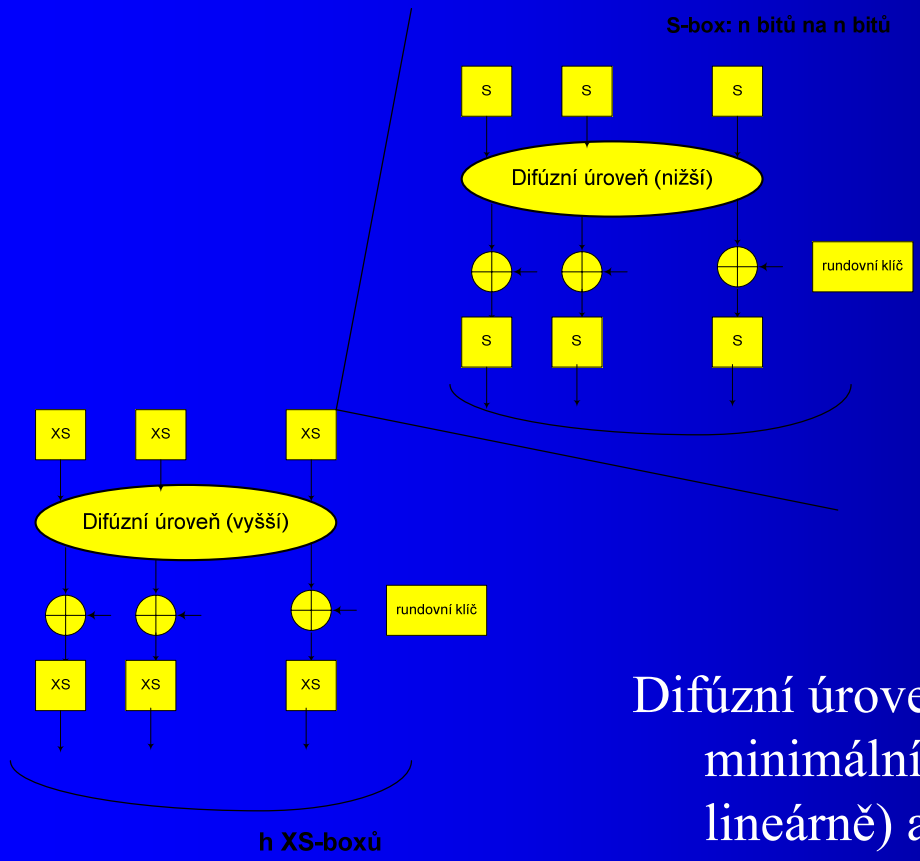


Potřebujeme blokovou šifru B

Šířka 64 bajtů

Připraveno pole rundovních klíčů

Praktická realizace funkce PI



Šířka bloku 512 bitů:

1 bajt, S box – diferenciál p

4 bajty, XS box – dif. $\leq p^4$

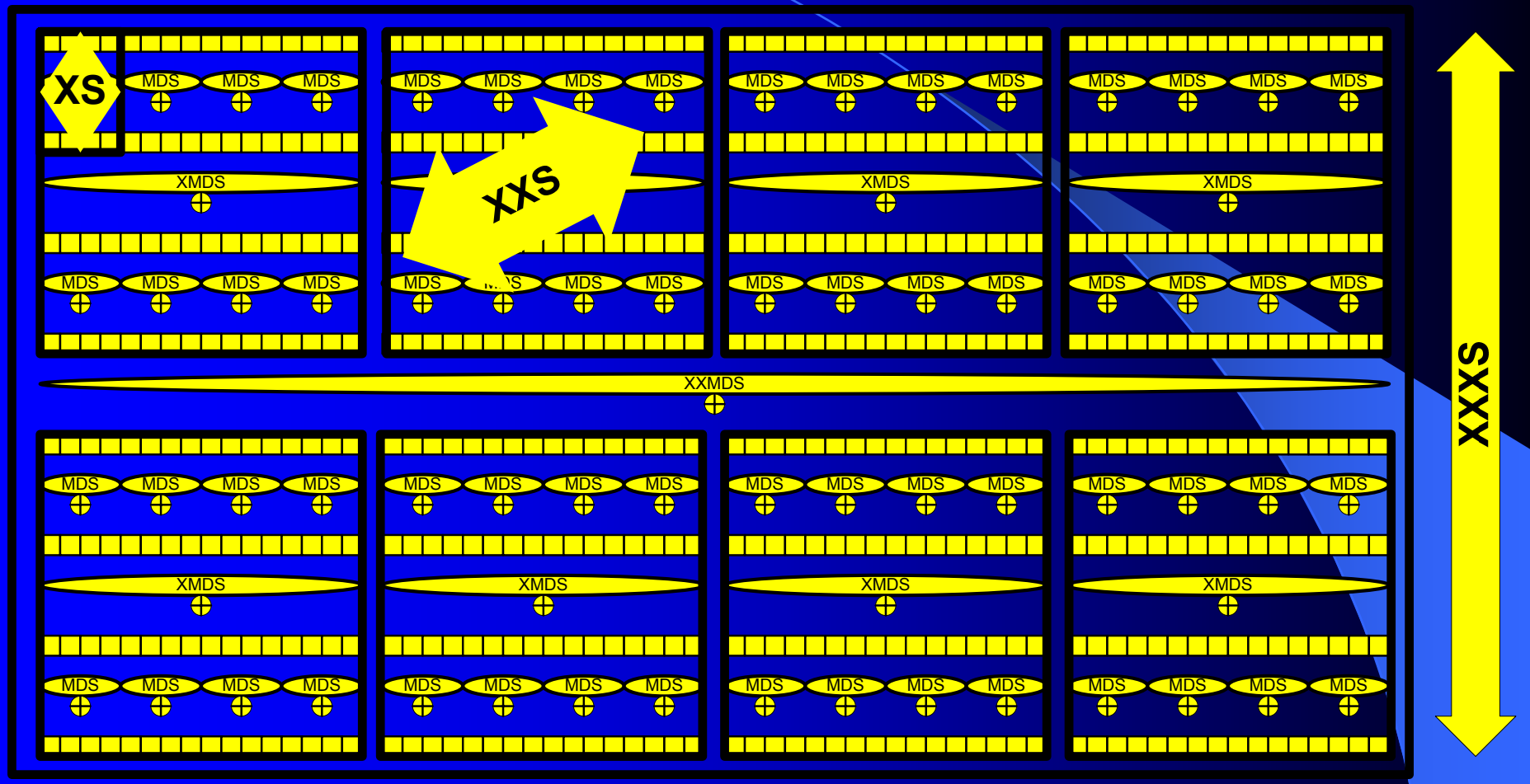
16 bajtů, XXS box – dif. $\leq p^{16}$

64 bajtů, XXXS box - dif. $\leq p^{64}$

(podobný odhad pro lineární obal)

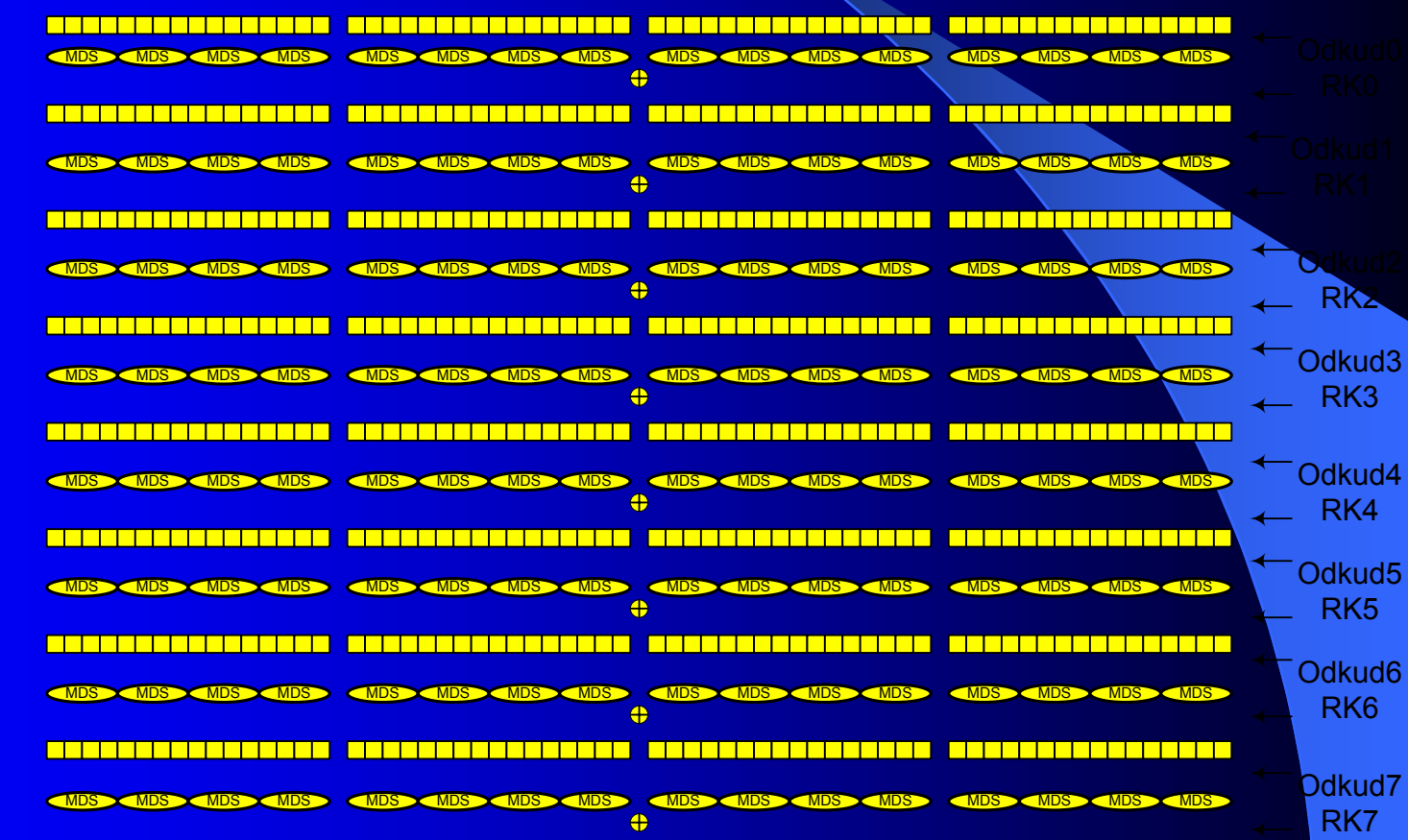
Difúzní úroveň nazýváme maximální, jestliže minimální počet diferenciálně (ekviv. lineárně) aktivních boxů je roven N + 1.

XXXS box (8 rund sítě PI)



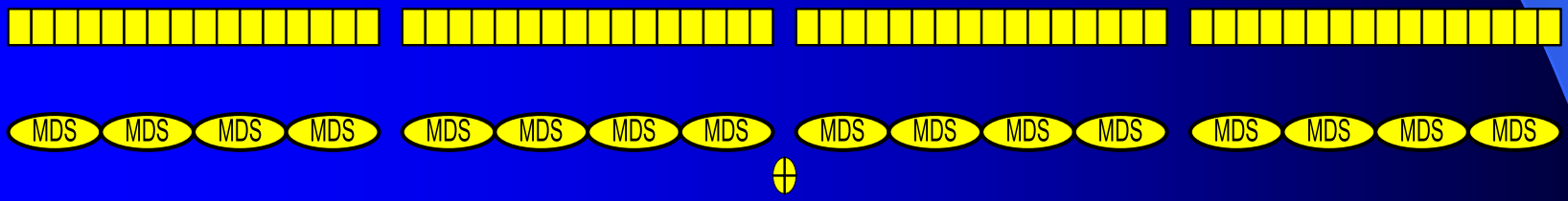
- Problém velkých lineárních matic MDS 16 x 16 bitů, XMDS 128 x 128 bitů, XXMDS 512 x 512 bitů

Konstrukce XiMDS

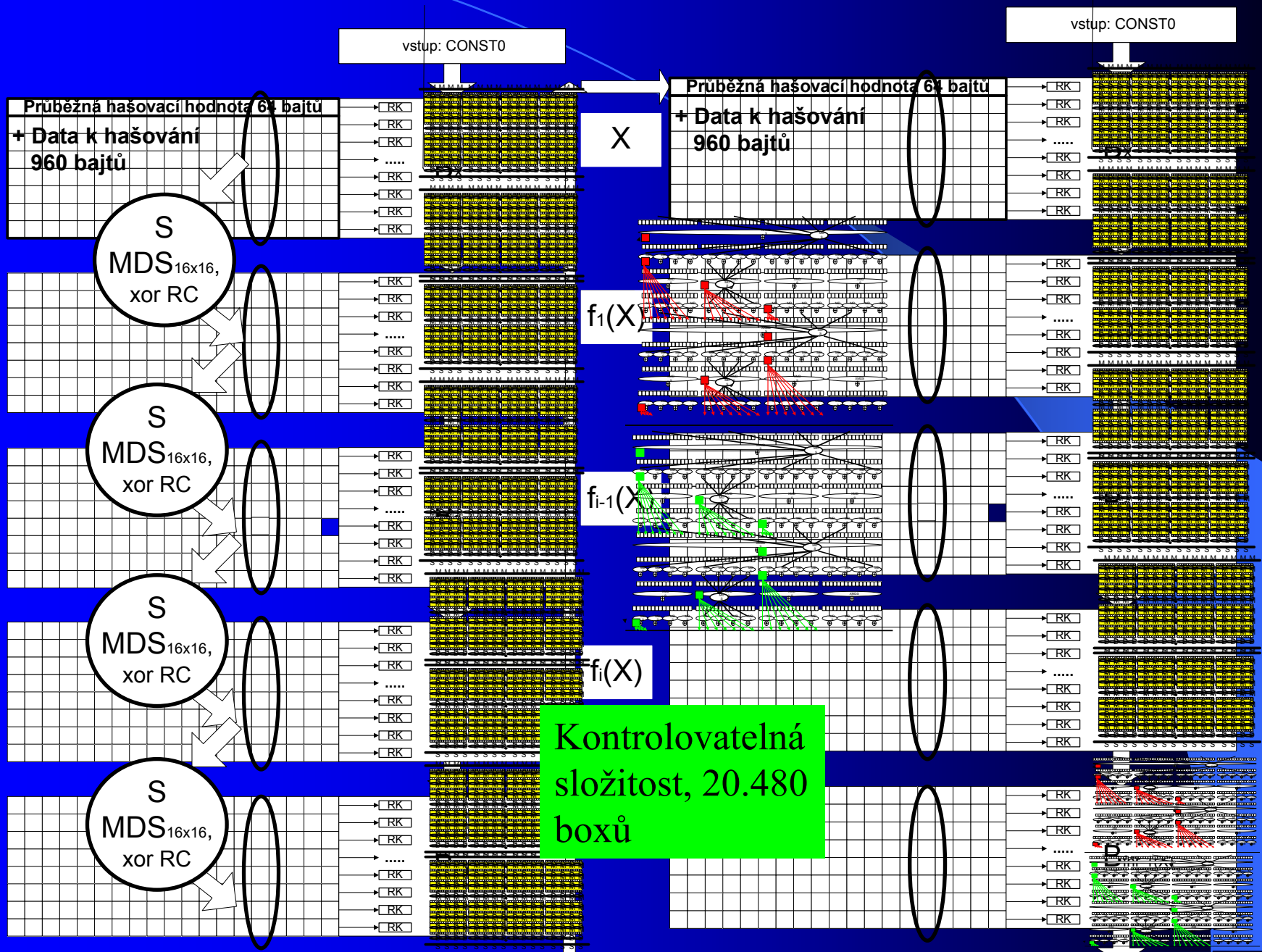


Transformace T1

S
P
(L)
K



Celkové schéma HDN



Co je DN ?

- Obecná myšlenka dvou sítí, stejně kvalitních, homogenita proměnných, nezávislost proměnných v síti FI, sloupcová transformace
- Rozměry a další prvky – vysoká volnost, stavebnice
- Můžeme pomocí DN šifrovat ?

Závěr

- DN(512, 8192)-10 a HDN(512, 8192)-10, prakticky použitelné funkce, rychlost cca 2-3 krát nižší než SHA-512
- DN prokazatelně odolné proti diferenciální a lineární kryptoanalýze
- HDN mají dokazatelné vlastnosti odolnosti proti nalezení kolize a vzoru a limitně jsou neodlišitelné od náhodných orákul
- Nadstandardní úroveň bezpečnostní rezervy

Literatura

- [BCK96] M. Bellare, R. Canetti and H. Krawczyk. Keying hash functions for message authentication. Advances in Cryptology – CRYPTO ’96, Lecture Notes in Computer Science Vol. 1109, pp. 1-15, Springer-Verlag, 1996.
- CDMP05] J. S. Coron, Y. Dodis, C. Malinaud and P. Puniya. Merkle-Damgard Revisited: how to construct a hash-function. Advances in Cryptology – CRYPTO 2005, Lecture Notes in Computer Science Vol. 3621, pp. 430 - 448, Springer-Verlag, 2005.

Literatura

- [Kli06] V. Klima: A New Concept of Hash Functions SNMAC Using a Special Block Cipher and NMAC/HMAC Constructions, IACR ePrint archive Report 2006/376 , October, 2006, http://cryptography.hyperlink.cz/SNMAC/SNMAC_EN.html (English, Czech).
- [Kli07] V. Klima: Special block cipher family DN and new generation SNMAC-type hash function family HDN, IACR ePrint archive Report 2007/050 , February, 2007, http://cryptography.hyperlink.cz/SNMAC/SNMAC_EN.html (English, Czech).