O návrhu speciálních blokových šifer a speciálních hašovacích funkcí[1]

Vlastimil Klíma

nezávislý kryptolog
v.klima@volny.cz,

http://cryptography.hyperlink.cz

Abstrakt

Generické problémy hašovacích funkcí vyvolaly potřebu návrhu nového konceptu hašovacích funkcí. U hašovacích funkcí, využívajících blokové šifry v kompresní funkci, má útočník možnost manipulace s otevřeným textem i klíčem. Základním cílem klasických blokových šifer však není odolnost proti útokům, založeným na změně nebo znalosti (nějaké části) šifrovacího klíče. Proto byly navrženy speciální blokové šifry DN a na jejich základě hašovací funkce třídy HDN [Kli07a]. V příspěvku ukazujeme motivaci a postup, kterým byly tyto funkce navrhovány. Technické detaily obsahují práce [Kli06a,c] a [Kli07a].

DN jsou prokazatelně odolné proti diferenciální a lineární kryptoanalýze. HDN mají dokazatelné vlastnosti odolnosti proti nalezení kolize a vzoru a limitně jsou neodlišitelné od náhodných orákul.

Jako příklad uvádíme DN(512, 8192)-10 a HDN(512, 8192)-10. Jedná se o prakticky použitelné funkce, jejichž rychlost je jen 2-3 krát nižší než rychlost SHA-512 a Whirlpool.

Klíčová slova: Speciální bloková šifra, speciální hašovací funkce, DN, HDN, NMAC, SNMAC.

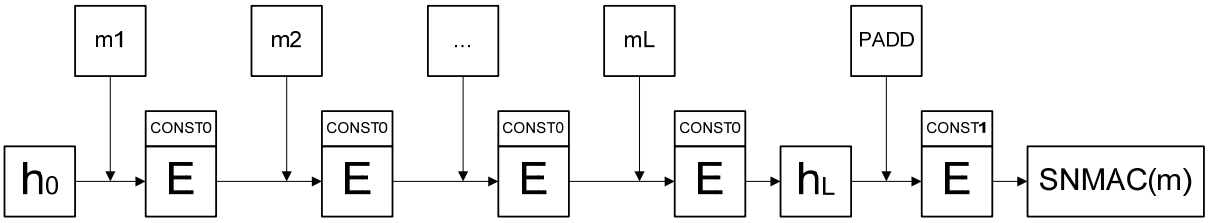
1 Úvod

Speciální blokové šifry DN a speciální hašovací funkce HDN vznikly na základě projektů, vypsaných NBÚ krátce poté, co byly objeveny generické slabiny moderních hašovacích funkcí. Smyslem těchto projektů nebylo vylepšovat a zesilovat existující hašovací funkce a jejich principy, ale navrhnout (pokud možno) nový princip a funkci, která bude mít vysokou bezpečnost, založenou (pokud možno) na prokazatelných tvrzeních. Současně ale nebyly preferovány čistě teoretické koncepty s vysokou bezpečností, které nelze naprogramovat, ale funkce, skutečně použitelné v současných i budoucích reálně existujících systémech ochrany dat. Připomeňme, že v době zadání projektu takové funkce nebyly známy a do současnosti není známo mnoho jiných alternativ. Z časového hlediska vznikly nejprve teoretické koncepty speciálních vnořených autentizačních kódů (SNMAC) a speciálních blokových šifer (SBŠ). V druhé fázi byla navržena konkrétní speciální bloková šifra DN a na její bázi hašovací funkce HDN.

Teoretický koncept SNMAC byl prezentován na MKB 2006 [Kli06a]. Soustředíme se proto na koncept SBŠ (technické detaily viz [Kli06a,c] a [Kli07a]).

Při návrhu SBŠ jsme vyšli z faktu, že blokové šifry byly vyvíjeny desítky let tak, aby ze znalosti šifrového a otevřeného textu nebylo možné určit klíč, tj. byla přirozeně zajišťována jednocestnost vzhledem ke klíči. Dále byly vyvíjeny tak, aby splňovaly tzv. ideální model blokové šifry, tj. že při náhodné volbě klíče *k* je transformace E_k náhodně vybranou permutací z množiny všech permutací nad prostorem otevřených zpráv. Využili jsme tohoto faktu a definovali kompresní funkci hašovací funkce přirozeně jako $f(X) = E_X(Const_0)$, tedy všechny proměnné vedeme do klíče speciální blokové šifry, zatímco otevřený text je konstantní. V tomto modelu je pak f náhodným orákulem. E nazýváme speciální blokovou šifrou. Tento název si E určitě zaslouží, protože je použita pouze se dvěma různými konstantními otevřenými texty - $Const_0$ pro orákulum f a $Const_1$ pro orákulum g (g je tzv. závěrečná operace hašovací funkce). Nyní můžeme definovat hašovací funkci SNMAC na bázi NMAC [BCK96] a SBŠ tak, jak ilustruje obr. 1.

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



Obr. 1: Definice SNMAC, založená na SBŠ a NMAC

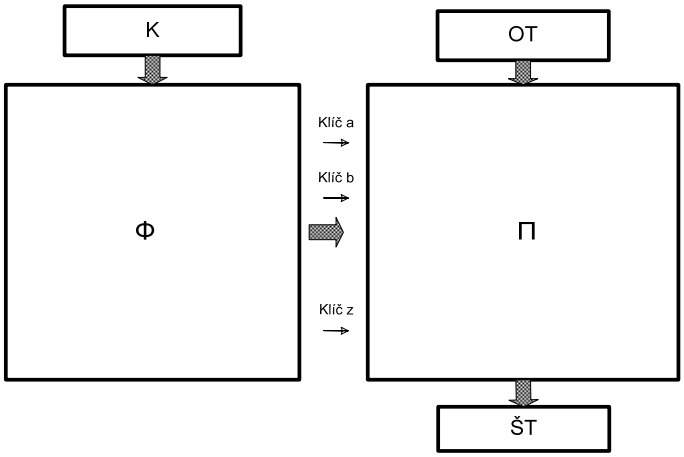
Všechny diferenční a lineární útoky, které byly úspěšné u hašovacích funkcí, se u SBŠ převádí na diferenční a lineární útoky s využitím klíče. Proto na rozdíl od běžných blokových šifer bude od speciální blokové šifry požadováno, aby byla odolná proti různým diferenčním a lineárním útokům, vedeným zejména z klíčového vstupu.

Požadujeme tedy, aby mezi proměnnými (k, x) a $y = E_k(x)$ neexistovaly žádné diferenční a lineární vztahy s využitelnou pravděpodobností. Jinými slovy, požadavky na SBŠ jsou stejné jako na klasickou blokovou šifru a navíc se požaduje silnější zpracování klíče.

Cíl útočníka. U klasických blokových šifer byl hlavním cílem útočníka klíč. U speciální blokové šifry může útočník s klíčem dokonce libovolně manipulovat. Vzniká otázka, co je nyní jeho cílem. Protože hašovací funkce SNMAC je založena na SBŠ, jeho cílem bude zejména nalézt vzor nebo kolizi SBŠ. Obecněji bude jeho cílem možnost jakýmkoliv způsobem řídit vztah mezi vstupem a výstupem SBŠ, což by mohlo vést k nalezení vlastností odlišujících hašovací funkci od náhodného orákula.

2 Dvojitá síť DN

Nyní popíšeme principy konstrukce třídy speciálních blokových šifer DN (Double Net). Prozatím víme, že

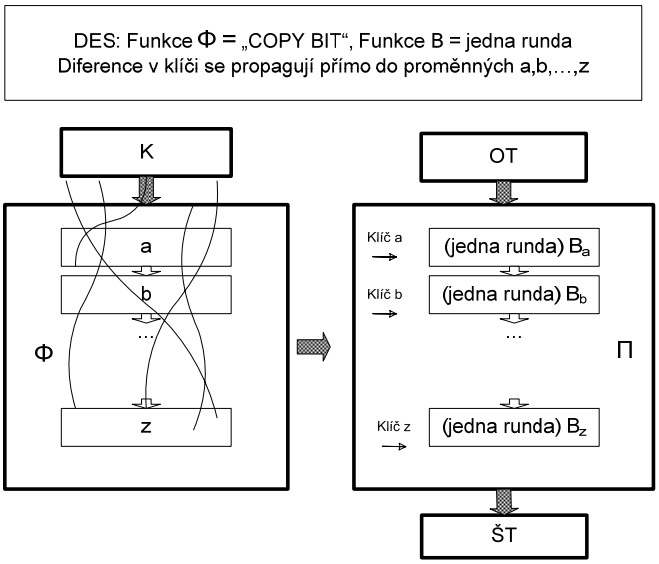


Obr. 2: Základní schéma speciální blokové šifry DN

se DN skládá ze dvou funkcí, expanze klíče Φ a součinové šifry Π a že funkci Φ by měla být věnována stejná pozornost jako funkci Π, odtud název dvojitá síť (DN, Double Network), neboť Φ je právě ta část DN, která zpracovává klíčový vstup. Síť Φ poskytuje síti Π nějaké proměnné, které označíme a, b, ..., z.

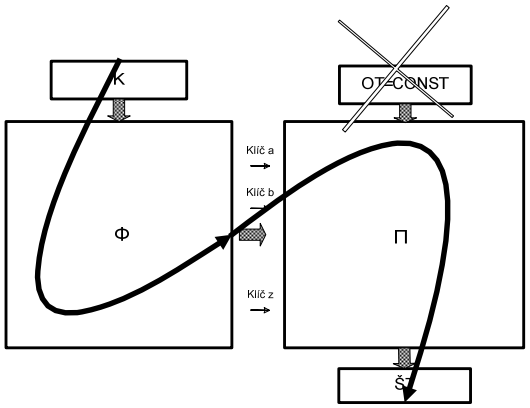
Podívejme se, jak pracují současné blokové šifry.

DES - Funkce Φ poskytuje 16 proměnných a,b, ..., z, které jsou kopií vybraných bitů klíče K. Funkce Π je součinová šifra 16 rund, v nichž proměnné a,b,...,z působí jako rundovní klíče.



Obr. 3: Schéma DES jako dvojitá síť

Nevýhoda DES je, že proměnné a,b,...,z jsou jednoduchou funkcí klíče K. Funkci Φ potřebujeme nepoměrně kvalitnější. Uvědomme si, jak používáme DN v konstrukci hašovací funkce - všechna data (průběžný kontext i aktuální hašovaný datový blok) jdou do zpracování prostřednictvím klíčového vstupu. Tudíž diference v klíči se nemohou jednoduše projevovat v proměnných a,b,...,z. Pak by šly také jednoduše řídit vnitřní proměnné při hašování ve funkci Π.



Obr. 4: Základní použití speciální blokové šifry DN ve speciální hašovací funkci

AES - oproti DES mírně zesložitila přípravu klíče. Proč? V blokové šifře Π by totiž rundovní klíče měly být nezávislé. Na tom závisí důkaz kvality blokové šifry. Tento předpoklad se však v důkazech šifer obvykle považuje za splněný, i když u drtivé většiny blokových šifer evidentně splněný není. U šifrovacích funkcí je však klíč tajný, rundovní klíče také, a proto se předpoklad nezávislosti "omlouvá" tím, že závislost rundovních klíčů je útočníkem obtížně zjistitelná nebo obtížně využitelná. U hašovacích funkcí tuto omluvu nelze akceptovat, neboť to, co vystupuje v roli klíče, je útočníkovi známo a může s tím dokonce libovolně manipulovat.

U speciálních blokových šifer bude nutné ve funkci Φ použít takové funkce, které poskytnou síti Π proměnné a,b...,z pokud možno skutečně nezávislé a bez možnosti v nich jednoduše řídit změny pomocí změn v klíči K.

Princip skládání šifer

Předpoklad nezávislosti rundovních klíčů byl u blokových šifer potřeba k tomu, aby jednoduché rundovní transformace (označujeme je $T1_k$), z nichž se skládá celá bloková šifra, byly nezávislé a jejich součin mohl tvořit kvalitní blokovou šifru. Kdyby byly závislé, mohlo by se také mohlo stát, že následující transformace obsahuje doplňkový poloslabý klíč k předchozímu klíči a odšifruje to, co předchozí transformace zašifrovala. U DES a AES máme tento vzorec (liší se pouze počtem 10 až 16 rund):

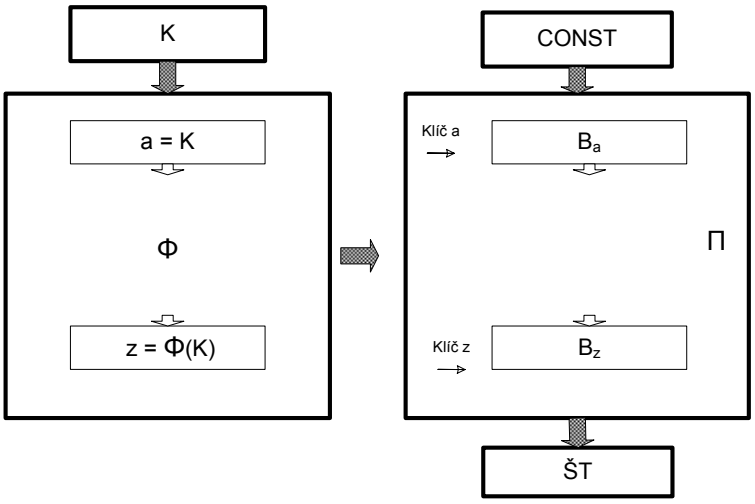
$B_k = T1_{k16} \bullet T1_{k15} \bullet T1_{k14} \bullet T1_{k13} \bullet T1_{k12} \bullet T1_{k11} \bullet T1_{k10} \bullet T1_{k9} \bullet T1_{k8} \bullet T1_{k7} \bullet T1_{k6} \bullet T1_{k5} \bullet T1_{k4} \bullet T1_{k3} \bullet T1_{k2} \bullet T1_{k1}$.

Bohužel ani u DES, ani u AES nemůžeme tvrdit, že rundovní klíče k1, ..., k16 jsou nezávislé. Nezávislost rundovních klíčů je velký problém, který nebyl v moderních šifrách uspokojivě vyřešen.

Nezávislost klíčů se řeší na vyšší úrovni, a to skládáním (nikoli jednotlivých rund, ale) blokových šifer, u nichž skutečně můžeme volit nezávislé klíče. Například u trojnásobné DES je možné použít tři různé nezávislé (náhodné) klíče: $DES_{k1} \bullet DES_{k2} \bullet DES_{k3}$.

Šifra Π

Šifru Π v DN definujeme jako součin blokových šifer B s rundovními klíči a, ..., z, tj. $\Pi = B_z \bullet ... \bullet B_b \bullet B_a$. Pokud jsou rundovní klíče *a* a *z* nezávislé, postačilo by z hlediska nezávislosti klíče (nikoli například z hlediska difúze) definovat $\Pi = B_z \bullet B_a$, kde $a = K$ a *z* je nějaká transformace klíče K taková, že *a* a *z* jsou nezávislé.

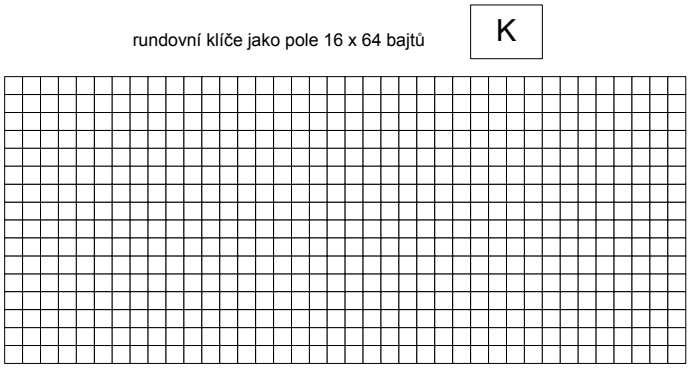


Obr. 4: Základní použití speciální blokové šifry DN ve speciální hašovací funkci

Pokud jsou klíče *a* (=K) a *z* (=Φ(K)) nezávislé, pak šifra $\Pi = B_z \bullet B_a$, není ani horší než B_a, ani horší než B_z. Výsledkem hašování je pak hodnota $B_z \bullet B_a$(Const). V tomto výrazu můžeme volit vstupní data *a* (= K), tím ovšem nějakým nezávislým způsobem také vznikne hodnota z. Hodnotu B_a(Const) můžeme tedy ovlivnit, čili můžeme ovlivnit vstup do transformace B_z. Transformace B_z je ovšem vybrána nezávisle na B_a, a tak nejsme schopni ovlivnit hodnotu B_z (B_a(Const)).

Pole rundovních klíčů

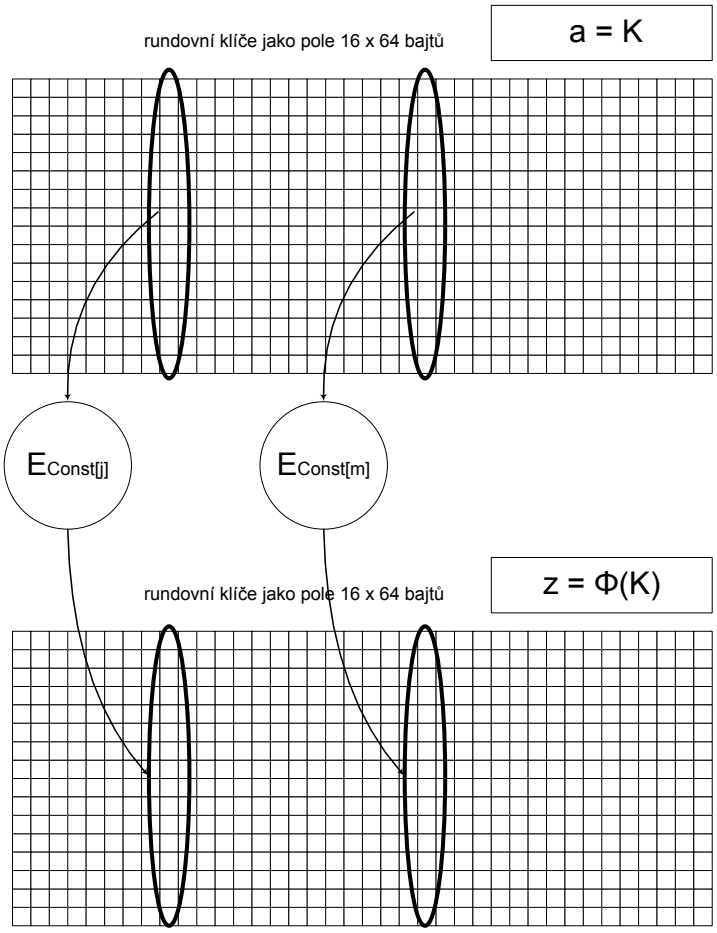
Nyní uvažujme o velikosti proměnné *a* a *z*. Hašovací kód HDN byl zvolen 512 bitů, bloková šifra B, která zpracovává 512 bitů bude mít pro tuto šíři bloku odhadem cca 16 rund. Proto budeme potřebovat cca 16x512 bitů rundovních klíčů, a tudíž proměnná *a* bude mít řádově tisíce (8192) bitů. Proměnnou *a* si můžeme zapsat do pole o rozměrech 16 x 64 bajtů (tzv. pole rundovních klíčů), kde řádky nazýváme malé rundovní klíče a odpovídající rundy blokové šifry B nazýváme malé rundy. Velké rundy nazýváme bloky B, tj. 16 malých rund. Použijeme-li $\Pi = B_z \bullet B_a$, máme dvě velké rundy, resp. 32 malých rund.



Obr. 5: Pole rundovních klíčů

Sloupcová transformace

Klíčovým bodem je vytvoření hodnoty z (=Φ(K)), nezávislé na K. Ideálně bychom potřebovali blokovou šifru Φ s délkou bloku 8192 bitů, což je velmi náročné. Mnohem efektivnější je využít nezávislosti hodnoty z (=Φ(K)) po částech, v tomto případě po sloupcích v poli rundovních klíčů. Označme E blokovou šifru s délkou bloku 16 bajtů a aplikujme ji s 64 různými klíči Const[1], Const[2], ..., Const[64] na jednotlivé sloupce pole K. Potom z = Φ(K) = ($E_{Const[1]}$(sloupec$_1$(K)), $E_{Const[2]}$(sloupec$_2$(K)), ..., $E_{Const[64]}$(sloupec$_{64}$(K)) je nezávislá na K. Je-li totiž bloková šifra E kvalitní, pak i permutace $E_{Const[1]}$(*), $E_{Const[2]}$(*), ... , $E_{Const[64]}$(*) jsou nezávislé náhodné permutace.

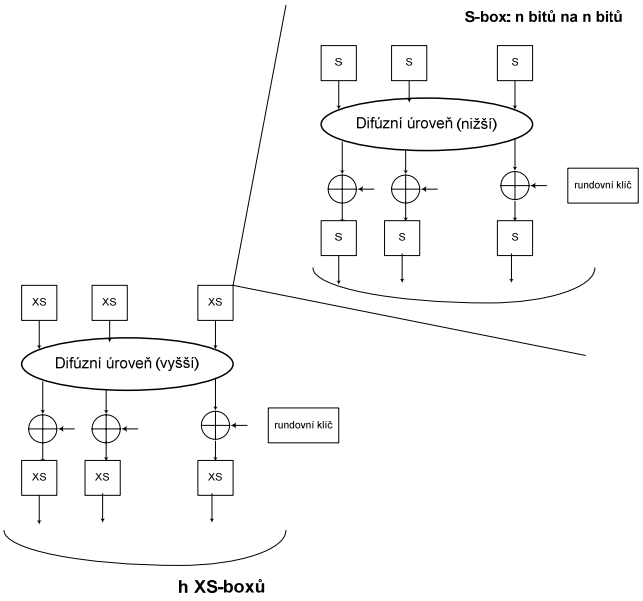


Obr. 6: Sloupcová transformace

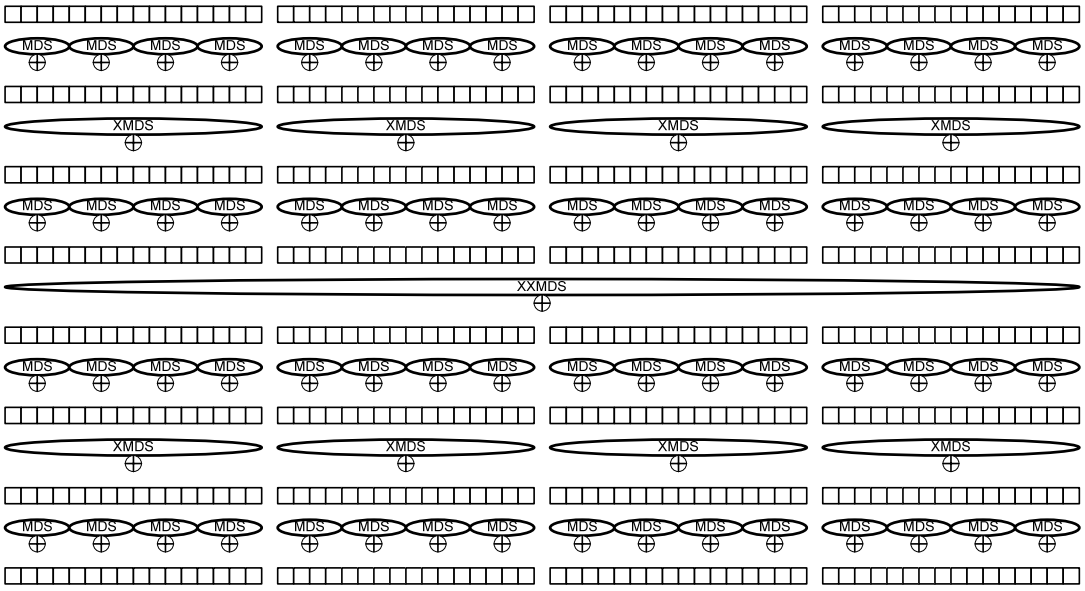
V konkrétní funkci DN má bloková šifra E 9 rund, takže je použito deset velkých rundovních klíčů, které (když už jsou vypočteny) můžeme využít také jako bloky rundovních klíčů b, c, .., y pro funkci $\Pi = B_z \bullet B_y \bullet ... \bullet B_b \bullet B_a$. Zařazení $B_y \bullet ... \bullet B_b$ má význam z hlediska dosažení lepší difúze a dále jako bezpečnostní rezerva.

Funkce Π

Funkci **Π** i sloupcovou transformaci **E** jsme jako blokové šifry konstruovali na základě vnořených SP sítí. Nejnižším prvkem je substituční box S (převádějící bajt na bajt), ten je stavební částí první SP sítě (XS-box). XS-box se skládá z vrstvy 4 S-boxů, lineárně-difúzní úrovně (tvořené maticí typu MDS typu 4x4 bajty), přičtení rundovního klíče a další vrstvy 4 S-boxů. Vzniklý XS-box je stavebním prvkem XXS-boxu, ten XXXS-boxu atd. Vnořováním vytváříme větší a větší SP sítě až do potřebného rozměru - šíře 64 bajtů, viz obrázek.



Obr. 7: Vnořené SP sítě



Obr. 8: Funkce Π na bázi vnořených sítí

Díky tomu, že matice všech použitých typů lze složit pouze z matic MDS typu 4x4, je možné celou funkci $\Pi = B_z \bullet ... \bullet B_b \bullet B_a$ vyjádřit jako složení jedné elementární transformace T1, která se skládá ze substituční vrstvy, permutace (složení bajtové permutace v celé šíři 64 bajtů a jednoduchých matic MDS typu 4x4 vytváří matice XMDS a XXMDS) a přičtení rundovního klíče.

Kód, který realizuje funkci Π je proto velmi kompaktní. Ve vnitřním cyklu pseudokódu je T1 (malá runda).

```
d = inputdata
for(i=0;i<rho; step 1)for(j=0;j<16; step 1)
{
   for(k=0; k<64; step 4)
   tmp[k+0,k+1,k+2,k+3]= MDS(S[P[d[k+0]]],S[P[d[k+1]]],S[P[d[k+2]]],S[P[d[k+3]]]);
   for(k=0; k<64; step 1)d[k] = RK[i][j][k] ^ tmp[k];
}
outputdata = d;
```

Podobně bloková šifra E je konstruována jako SP síť. SP-sítě umožňují dokázat odolnost E a Π vůči diferenciální a lineární kryptoanalýze. Například pravděpodobnost maximálního diferenciálu sítě Π je menší nebo rovna p^{64}, kde p je maximální diferenciál nejhoršího použitého S-boxu v Π (p může být 2^{-4} resp. 2^{-6}).

3 Závěr

Generické problémy hašovacích funkcí vyvolaly potřebu návrhu nového konceptu hašovacích funkcí. Navrhli jsme koncept SNMAC na bázi speciálních blokových šifer a dokázali o něm kvalitativní i kvantitativní vlastnosti odolnosti proti nalezení vzoru a kolize [Kli06a,b,c]. Dále jsme navrhli třídu speciálních blokových šifer DN a na jejich základě hašovací funkce třídy HDN [Kli07a,b]. V příspěvku ukazujeme motivace a postup, kterým byly tyto funkce navrhovány.

4 Literatura

Seznam použité literatury obsahuje mnoho desítek položek. Posloužily jako podklad pro dále uvedené práce, které je citují v plném rozsahu. Vzhledem k omezenému prostoru na příspěvek odkazujeme laskavého čtenáře na seznamy literatury v [Kli06a,c] a [Kli07a].

[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.

[Kli06a] V. Klima: New generation of hash functions SNMAC, Santa´s Crypto Get-Together, MKB 2006, Prague, Hotel Olympik, December, 7. – 8., 2006.

[Kli06b] SNMAC homepage http://cryptography.hyperlink.cz/SNMAC/SNMAC.html

[Kli06c] 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.pdf.

[Kli07a] 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://eprint.iacr.org/2007/050.pdf, source codes on [Kli06b].

[Kli07b] V. Klima: About a new generation of block ciphers and hash functions - DN and HDN, SPI 2007, Security and Protection of Information, May 2 – 4, 2007, Brno, Czech Republic, http://cryptography.hyperlink.cz/2007/Klima_SPI_2007_EN.pdf.