Acta Informatica Pragensia, 2017, 6(2): 162–173
DOI: 10.18267/j.aip.107
Peer-reviewed paper

Vliv nelinearity na vybraná kryptografická kritéria 8x8 S-boxů

Influence of Non-Linearity on Selected Cryptographic Criteria of 8x8 S-Boxes

Petr Tesař*

Abstrakt

V článku jsou definována standardně používaná kritéria charakterizující kryptografickou kvalitu S-boxu: regulárnost, nelinearita, autokorelace, propagace změny a imunita proti diferenční kryptoanalýze. Jsou porovnány hodnoty autokorelace, propagace změny a imunity proti diferenční kryptoanalýze pro regulární 8x8 S-boxy s nelinearitou 98, a regulárních 8x8 S-boxů s nelinearitou 104. Je statisticky ověřeno, že vyšší nelinearita zlepšuje, v kryptograficky výhodném smyslu, hodnoty těchto kritérií.

Klíčová slova: Kryptografie, regulární 8x8 S-box, kritérium nelinearity, vliv nelinearity na ostatní kryptografická kritéria.

Abstract

The article defines standard criteria used to characterize the cryptographic quality of the S-box: regularity, non-linearity, autocorrelation, avalanche and immunity against differential cryptanalysis. The values of autocorrelation, avalanche and immunity against differential cryptanalysis for regular 8x8 S-boxes with non-linearity 98 and regular 8x8 S-boxes with non-linearity 104 are compared. It is statistically verified that higher non-linearity improves the values of these criteria in a cryptographically advantageous sense.

Keywords: Cryptography, Regular 8x8 S-box, Non-linearity criterion, Effect of non-linearity on other cryptographic criteria.

1 Úvod

Jeden z hlavních stavebních prvků současných symetrických kryptografických algoritmů je záměnný box, neboli S-box. Záměnné boxy (anglicky substitution boxes – S-boxes) jsou obecně libovolná zobrazení vstupních N-rozměrným binárních vektorů na M-rozměrné výstupní binární vektory.

Z matematického hlediska každý NxM S-box definuje zobrazení množiny B^N na množinu B^M, kde $B = \{0,1\}$ je Booleovská 1-dimenzionální množina. Formálně se na S-box typu NxM můžeme dívat jako na systém M Booleovských funkcí $f_1,f_2,\ldots,f_M$, každé o N proměnných.

* Department of Computer Science and Mathematics, Faculty of Economic Studies,
University of Finance and Administration, Estonská 500, 101 00 Prague 10, Czech Republic
✉ 22901@mail.vsfs.cz

Potom *NxM* S-box *T* můžeme zapsat v analytickém tvaru $[f_1(x_1,x_2,\ldots,x_N),\ldots,f_M(x_1,x_2,\ldots,x_N)]$, kde každá Booleovská funkce je vyjádřena jako formule pomocí operace logického součinu a součtu mod 2 (= logická funkce XOR).

Libovolný vstupní vektor $x = (x_1,x_2,\ldots x_N)$ je pomocí S-boxu *T* zobrazen na výstupní vektor

$y = T(x) = (y_1,y_2,\ldots,y_M)$ v souladu se vztahy $y_i = f_i(x_1,x_2,\ldots,x_N)$ pro $i = 1,2,\ldots,M$.

Splněním dalších podmínek lze u S-boxu dosáhnout vlastností, které z kryptologického hlediska významným způsobem ovlivňují kryptologickou kvalitu celého šifrového algoritmu.

Nejčastěji používanými jsou S-boxy s $N = M = 8$. Regulární 8x8 S-box je použit i v nejpoužívanější šifře AES. Dalším používaným formátem, zejména v tzv. lehkých šifrách, jsou S-boxy s $N = M = 4$.

Cílem této práce je pomocí statistických metod dokázat existenci vztahu mezi nelinearitou regulárního 8x8 S-boxu a dalšími standardně používanými kryptografickými kritérii: autokorelací, propagací změny a imunity proti diferenční kryptoanalýze. Statistická analýza a provedený experiment, které jsou uvedeny v odstavci 4, jsou vlastním přínosem autora k problematice kryptografických kritérií regulárních 8x8 S-boxů. Definice termínů a všech kritérií je uvedena v odstavci 3.

2 Rešerše aktuálního stavu a výzkumné metody

Vědecké práce k problematice S-boxů jsou nejvíce publikovány na specializovaném webu Mezinárodní asociace pro kryptografický výzkum (IACR) a na velkých mezinárodních kryptologických konferencích, jakými jsou například CRYPTO pořádané každoročně v Santa Barbaře v USA nebo Eurocrypt, pořádaný každoročně v různých městech Evropy. Značná část těchto prací se týká způsobů generování S-boxů, s co nejvyšší nelinearitou, případně vyhovujícím dalším kryptografickým kritériím. Jsou to práce (Zhang et al., 2017), (Farwa et al., 2016), (Ivanov et al., 2016), (Spain & Varia, 2016), (Guo et al., 2016), (Stoffelen, 2016), (Biryukov & Perrin, 2015), (Canteaut et al., 2015), (Das, 2014), (Kazymyrov et al., 2014), (Mazumdar et al., 2013), (Nawaz et al., 2009), (Tran et al., 2008), (Cui & Cao, 2007) a (Sakalauskas & Luksys, 2007). Dále jsou práce, které porovnávají konkrétní S-box s publikovanými S-boxy. Jde o práce (Farwa et al., 2016) a (Rostovtsev, 2013).

Další problematika je rozbor kryptoanalytických metod na šifry, které využívají S-boxy jako hlavní nelineární komponentu. Jsou to práce (Ghosal, 2017), (Khanoki et al., 2017), (Goudarzi et al., 2017), (Borissov et al., 2016), (Guo et al., 2016), (Selvam et al., 2016), (Gologlu et al., 2016), (Biryukov & Perrin, 2015), (Leventi-Peetz & Peetz, 2015), (Guo et al., 2012), (Gilbert & Peyrin, 2010), (Canright & Batina, 2009), (Youssef et al., 2006), (Courtois et al., 2006) a (Carlet, 2005).

V práci (Parker, 2003) je rozšířen pojem nelinearity S-boxu, za účelem zvýšení rezistence S-boxu proti lineární kryptoanalýze. V práci (Mishra et al., 2017) je navržen algoritmus výpočtu stupně algebraické normální formy pro S-box. Stupeň algebraické normální formy Booleovské funkce je rovněž jedno z kryptografických kritérií. V práci (Carlet & Ding, 2004) je přehled o poznatcích z oblasti vysoce nelineárních Booleovských funkcí do roku 2003. Nový indikátor upřesňující meze pro nelinearitu S-boxu je navržen v (Carlet & Ding, 2007). V práci (Zhang et al., 2015) je provedena klasifikace regulárních 4x4 S-boxů, které jsou vedle 8x8 S-boxů nejčastěji používanými S-boxy, zejména v tzv. lehkých šifrách.

Z prací, ve kterých jsou k daným S-boxům uvedeny i hodnoty dalších kryptografických kritérii vyplývá, že vyšší nelinearita ovlivňuje hodnoty dalších kritérií kryptograficky výhodným směrem. Nicméně tyto vztahy nejsou v publikované literatuře statisticky ověřeny na větších množinách regulárních 8x8 S-boxů. Tento fakt byl výchozím bodem k provedení experimentu s větším počtem S-boxů s různou nelinearitou za účelem ověření vztahu mezi nelinearitou a třemi rozšířenými kryptografickými kritérii.

K ověření cíle práce, uvedeného v Úvodu, byl použit následující postup:

- Byly vygenerovány dvě množiny regulárních 8x8 S-boxů s různými nelinearitami. V první množině měly všechny S-boxy nelinearitu 98. Tato hodnota nelinearity je maximální, kterou lze dosáhnout generováním regulárních 8x8 S-boxů náhodným výběrem z množiny všech možných regulárních 8x8 S-boxů. Ve druhé množině měly všechny S-boxy nelinearitu 104. Tato hodnota je maximální, kterou lze dosáhnout generováním regulárních 8x8 S-boxů originální autorovou metodou, uvedenou v (Tesař, 2010). V literatuře jsou popsány i regulární 8x8 S-boxy s nelinearitou 112 viz například v (Farwa et al., 2016). Jde ovšem o speciální případy v jednotkovém množství a publikovaný počet takto nelineárních S-boxů je nedostatečný pro statistické testování.
- U všech S-boxů byly spočítány hodnoty autokorelace, propagace změny a imunity proti diferenční kryptoanalýze. Pro obě množiny byly dále vypočítány výběrové průměry, směrodatné odchylky, šikmosti a špičatosti všech tří sledovaných kritérií.
- Dvouvýběrovým *t*-testem byly porovnány výběrové průměry kritérií se stanovenou hypotézou, že průměry kritérií u S-boxů s nelinearitou 98 jsou stejné jako průměry u S-boxů s nelinearitou 104. Ve všech případech byla stanovena alternativní hypotéza, že průměry kritérií u S-boxů s nelinearitou 104 jsou menší než průměry u S-boxů s nelinearitou 98. Hypotézy byly testovány na hladině významnosti 0.01. U všech kritérií je menší hodnota kryptograficky výhodnější.

3 Kryptografická kritéria kvality S-boxu

Zavedeme nejdříve kryptografická kritéria kvality Booleovské funkce s jedním výstupem, která potom přirozeným způsobem rozšíříme na *NxM* S-box. Definice zde uvedených kryptografických kritérii jsou uvedeny v mnoha pracích. Při citaci v tomto odstavci byla snaha uvádět ty zdroje, ve kterých se daný pojem vyskytl poprvé.

3.1 Booleovská funkce s 1 výstupem

Definice v této kapitole jsou převzaty z (Clark et al., 2005).

Definice 1 – Hammingova váha

Hammingova váha $w_t(f)$ Booleovské funkce f s jedním výstupem, je počet jedniček v množině výstupních hodnot. Hammingova vzdálenost dvou Booleovských funkcí f a g je definována jako Hammingova váha $w_t(f \oplus g)$, kde $\oplus$ je logická funkce XOR.

Definice 2 – Vybalancovaná Booleovská funkce

Booleovskou funkci f o N proměnných nazveme vybalancovanou, pokud splňuje podmínku

(1) $$w_t(f) = 2^{N-1}$$

Definice 3 – Lineární Booleovská funkce

Lineární Booleovskou funkci příslušnou vektoru $\alpha \in B^N$ označíme

(2) $$L_\alpha(x) = \alpha_1 x_1 \oplus \alpha_2 x_2 \oplus ... \oplus \alpha_N x_N$$

kde $\alpha_i x_i$ značí logickou funkci AND i-tého bitu vektorů α a x.

Definice 4 – Afinní Booleovská funkce

Množina afinních Booleovských funkcí je složena z množiny lineárních Booleovských funkcí a jejich komplementů

(3) $$A_{\alpha,c}(x) = L_\alpha(x) \oplus c$$

kde $c \in B$.

Definice 5 – Nelinearita Booleovské funkce

Míru nelinearity Booleovské funkce *f* (na bitové úrovni) vyjadřujeme hodnotou N_f, která je definována jako minimum Hammingovy vzdálenosti w_t mezi danou funkcí *f* a prostorem afinních funkcí.

(4) $$N_f = \min_{d \in A_{\alpha,c}} (w_t(f \oplus d))$$

Definice 6 – Autokorelační transformace

Autokorelační transformaci Booleovské funkce *f* definujeme výrazem:

(5) $$\hat{r}_f(\alpha) = \sum_{x \in B^N} \hat{f}(x) \hat{f}(x \oplus \alpha)$$

Kde $\alpha \in B^N$ a $\hat{f}(x) = (-1)^{f(x)}$ je tak zvaná polaritní reprezentace funkce *f*.

Autokorelací funkce *f* budeme označovat hodnotu AC_f, kde

(6) $$AC_f = \max_{\alpha \in B^N} \left| \sum_{x \in B^N} \hat{f}(x) \hat{f}(x \oplus \alpha) \right|$$

Definice 7 – Booleovská diference

Nechť je dána Booleovská funkce *f*. Potom výraz

(7) $$\frac{df}{dx_i} = f(x_1,...,x_i = 0,...,x_N) \oplus f(x_1,...,x_i = 1,...,x_N)$$

nazveme Booleovskou diferencí funkce *f* podle proměnné x_i. Definice je převzata z (McCluskey, 1986).

Je zřejmé, že Booleovskou diferencí funkce *f* podle proměnné x_i je Booleovskou funkcí *N-1* proměnných, a to $x_1,...,x_{i-1},x_{i+1},...,x_N$. Jestliže Booleovská funkce *f* nezávisí na proměnné x_i platí, že $\frac{df}{dx_i} = 0$ pro všechny (*N-1*)-bitové vektory hodnot proměnných $x_1,...,x_{i-1},x_{i+1},...,x_N$.

Na druhé straně, jestliže Booleovská funkce *f* závisí na proměnné x_i, existuje *(N-1)* bitový vektor hodnot proměnných $x_1,...,x_{i-1},x_{i+1},...,x_N$ pro který $\frac{df}{dx_i} = 1$.

Definice 8 – Přísná propagace změny

Booleovská funkce *f* vyhovuje přísné propagaci změny podle proměnné x_i *i=1,...,N,* jestliže na množině (*N-1*)-bitových vektorů platí:

(8) $$w_t(\frac{df}{dx_i}) = 2^{N-2}$$

Definice 9 – Kritérium propagace změny Booleovské funkce

Hodnotou propagace změny Booleovské funkce *f* pro proměnnou x_i nazýváme veličinu

(9) $$w_t(\frac{df}{dx_i}).$$

Kritériem propagace změny Booleovské funkce *f* (angl. Avalanche criterion) s *N* proměnnými nazveme veličinu

(10) $$\vartheta(f) = \sum_{i=1}^{N} \left| w_t(\frac{df}{dx_i}) - 2^{N-2} \right|$$

Čím je menší hodnota definovaná vztahem (10), tím kryptologicky kvalitnější je Booleovská funkce. Kritérium je popsáno např. v (McCluskey, 1986) nebo v (Webster, 1985).

3.2 Booleovské funkce s více výstupy - vlastní S-boxy

Booleovské funkce s $M > 1$ výstupy reprezentují vlastní *NxM* S-boxy. Následující definice jsou rozšířením obdobných definic pro booleovské funkce.

Definice 10 – Regulární S-box

NxM S-box nazýváme *regulárním,* pokud platí, že všechny *M*-tice na výstupu mají stejnou četnost.

Regularita S-boxu je obdobou vybalancovanosti u Booleovské funkce s jedním výstupem. Regularita zajišťuje, že se nebude snižovat relativní entropie vstupní posloupnosti při průchodu S-boxem. V případě, že *N=M,* můžeme regulární S-box *T* reprezentovat permutací čísel *0, ..., 2^{N-1},* zapsaných ve formě *N*-bitových vektorů. V tomto případě jde o bijektivní zobrazení a existuje inverzní S-box T^{-1}. Regulární S-boxy jsou zvláště významnou skupinou stavebních prvků moderních šifer.

Definice 11 – Nelinearita S-boxu

Nelinearitou *NxM* S-boxu *T* budeme nazývat hodnotu

(11) $$N_T = \min_{\alpha \in \{B^M - \{0\}\}}(N_{f_\alpha})$$

kde f_α je lineární kombinací *M* výstupů S-boxu *T* danou nenulovým vektorem $\alpha \in B^M$ a je Booleovskou funkcí s jedním výstupem a *N* vstupy.

Tedy

(12) $$f_\alpha(x) = \alpha_1 f_1(x) \oplus \alpha_2 f_2(x) \oplus .... \oplus \alpha_M f_M(x)$$

A dále N_{f_α} je nelinearita Booleovské funkce f_α definovaná výrazem (4).

Nelinearita S-boxu je minimální nelinearitou ze všech nelinearit 2^M-1 netriviálních funkcí, získaných lineárními kombinacemi *M* výstupních funkcí S-boxu *T*.

Tato, dnes používaná definice nelinearity S-boxu, byla poprvé publikována v (Nyberg, 1992).

Horní mez nelinearity *NxM* S-boxu je potom stejná jako u Booleovské funkce s jedním výstupem a *N* vstupy.

Definice 12 – Autokorelace S-boxu

Autokorelací *NxM* S-boxu *T* budeme nazývat hodnotu

(13) $$AC_T = \max_{\alpha \in \{B^M - \{0\}\}}(AC_{f_\alpha})$$

Kde f_α je Booleovská funkce definována výrazem (12) a její autokorelace AC_{f_α} je definována výrazem (6).

Definice 13 – Přísná propagace změny v S-boxu

Řekneme, že *NxM* S-box má vlastnost přísné propagace změny, jestliže každá jeho Booleovská funkce f_j vyhovuje přísné propagaci změny podle proměnné x_i pro *j=1, ...,M* a *i=1, ...,N.*

Z uvedené definice vyplývá, že v *NxM* S-boxu *T*, který vyhovuje přísné propagaci změny, se jedna změna vstupního bitu projeví v *M/2* bitech na výstupu.

Definice 14 – Kritérium propagace změny v S-boxu

Kritériem propagace změny *NxM* S-boxu T nazýváme veličinu

(14) $$\vartheta(T) = \sum_{j=1}^{M} \vartheta(f_j)$$

kde $\vartheta(f_i)$ pro jednotlivé Booleovské funkce $f_1, ..., f_M$ S-boxu *T* jsou definovány výrazem (10).

Kryptologický význam tohoto kritéria pro S-boxy je popsán v práci (Pieprzyk, 1989).

Vysoká hodnota propagace změny $\vartheta(T)$ pro *NxM* S-box *T* je z kryptologického hlediska nevhodná, protože buď jednotlivé bity výstupního vektoru *T(x)* jsou v průměru málo závislé na bitech vstupního vektoru *x* nebo naopak, je tato závislost příliš silná, což je rovněž špatně.

Poznamenejme, že v případě S-boxu T s vlastností přísné propagace platí

(15) $\vartheta(T) = 0$

Jako poslední kritérium uvedené v této práci je speciální kritérium zaměřené proti využití diferenční luštící metody popsané Bihamem. V době uvedení šlo o velmi revoluční luštící metodu typu CPA, aplikovatelnou na všechny DES-podobné blokové šifry, která se v různých variacích využívá dodnes. Ochrana proti diferenční metodě musí být při konstrukci kryptograficky kvalitních S-boxů ošetřena již při jejich návrhu. Jako nejdůležitější kritéria zvyšující odolnost S-boxů proti diferenční metodě jsou vysoká nelinearita a nízká autokorelace.

Diferenční metoda je obecně založena na nerovnoměrném rozdělení v tzv. Input-Output maticí diferencí, uvedené v práci (Dawson & Tavares, 1991). V této práci je navržena speciální baterie kritérií založených na teorii informací, které ohodnocují odolnost S-boxu proti diferenční metodě. Z této baterie byl vybrán test hodnoty maximálního prvku v Input-Output matici diferencí (mimo první řádek).

Nechť T je NxM S-box. Potom matice Input-Output diferencí MIO má rozměr $2^N x 2^M$, kde každý prvek této matice $MIO[i,j]$ obsahuje počet případů, kdy pro vstupní vektory x_k a x_p

platí: $x_k \oplus x_p = i$ a současně platí $T(x_k) \oplus T(x_p) = j$.

Pokud matice MIO má následující hodnoty, je příslušný S-box imunní proti diferenční metodě.

(16) $MIO[0,0] = 2^N$

$MIO[0,j] = 0$ pro $j=1, \ldots, 2^M-1$

$MIO[i,j] = A$ pro $i=1, \ldots, 2^N-1$ a pro $j=0, \ldots, 2^M-1$

kde $A = \frac{2^N}{2^M}$

Všechny prvky matice MIO jsou sudá čísla. V případě S-boxu, kde $N=M$ dostáváme $A=1$ což však není možné. Nejlepší možný případ bude proto směs hodnot 0 a 2.

Definice 15 – Kriterium MIO-Max S-boxu

Nechť T je NxM S-box. Spočteme jeho matici Input-Output diferencí MIO. Kritérium MIO-Max je vyjádřeno vzorcem

(17) $\psi(T) = \max_{i=1,\ldots,2^N-1,\, j=0,\ldots,2^M-1}(MIO[i, j])$

Nižší hodnota $\psi(T)$ je kryptologicky výhodnější. V anglické literatuře, například v (Farwa et al., 2016), je také používáno jako Differential approximation probability (DP), kde $DP=\psi(T)/256$ (pro 8x8 S-box).

Za kryptologicky kvalitní považujeme S-boxy, které mají dobré hodnoty požadovaných kritérií. Vysoká nelinearita S-boxu a nízká hodnota autokorelace zvyšují odolnost šifer proti dnes již klasickým kryptoanalytickým útokům – lineární a diferenční kryptoanalýze.

Pro zde uvedená kritéria bude na základě vyhodnocení experimentu ukázáno, že hodnoty těchto kritérií souvisí s nelinearitou v tom smyslu, že pokud má S-box vysokou nelinearitu, má i dobré hodnoty v těchto kritériích.

4 Výsledky experimentu

V reálných kryptosystémech jsou nejčastěji používány regulární S-boxy s $N = M = 8$, a proto byl experiment prováděn s tímto formátem S-boxů.

Metodou náhodného výběru bylo vygenerováno 300 regulárních 8x8 S-boxů s nelinearitou 98, pro které byly vypočteny hodnoty výše popsaných kritérii. Nelinearita 98 je maximální nelinearita regulárních 8x8 S-boxů dosažitelná generováním metodou náhodného výběru.

- Autokorelace podle vzorce (13) (zkratka AKOR) nižší hodnota je lepší
- Propagace změny podle vzorce (14) (zkratka AVAL) nižší hodnota je lepší
- MIO-Max podle vzorce (17) (zkratka MIOX) nižší hodnota je lepší

Rozdělení hodnot těchto kritérií pro 300 náhodně vygenerovaných regulárních 8x8 S-boxů s nelinearitou 98 je v následující tabulce 1.

Kritérium	Průměr	Odchylka	Šikmost	Špičatost	Min.	Max.	Normalita
AKOR	99.09	6.113	0.699	3.477	80	120	ne
AVAL	286.13	29.265	0.160	2.797	216	382	ano
MIOX	11.09	1.122	0.496	2.919	10	16	ne

Tab. 1. *Hodnoty výběrových statistik kritérií. Zdroj: Autor.*

Metodou GaT popsanou v (Tesař, 2010) bylo vygenerováno 300 regulárních 8x8 S-boxů s nelinearitou 104, pro které byly vypočteny hodnoty výše popsaných kritérii. Metoda GaT je schopná generovat regulární 8x8 S-boxy s nelinearitou maximálně 104. Rozdělení hodnot těchto kritérií pro 300 vygenerovaných regulárních 8x8 S-boxů s nelinearitou 104 je v následující tabulce 2.

Kritérium	Průměr	Odchylka	Šikmost	Špičatost	Min.	Max.	Normalita
AKOR	93.49	6.309	0.371	2.928	80	112	ne
AVAL	271.35	27.766	0.081	2.599	198	346	ano
MIOX	9.80	1.039	-0.128	3.519	8	12	ano

Tab. 2. *Hodnoty výběrových statistik kritérií. Zdroj: Autor.*

U všech kritérií byla ověřována normalita výběru pomocí testu kombinace výběrové šikmosti a špičatosti uvedeného v (Meloun & Militký, 1998, s. 95). Výsledky testu normality na hladině významnosti 0.01 jsou v pravém sloupci tabulek.

Pro všechna kritéria byla stanovena nulová hypotéza a alternativní hypotéza:

H_0: výběrový průměr množiny S-boxů s nelinearitou 104 je rovný výběrovému průměru množiny S-boxů s nelinearitou 98.

H_1: výběrový průměr množiny S-boxů s nelinearitou 104 je menší než výběrový průměr množiny S-boxů s nelinearitou 98.

Protože *F*-test shodnosti rozptylů uvedený v (Anděl, 1978, s. 94), přijal ve všech případech hypotézu o rovnosti rozptylů na hladině významnosti 0.01, byl pro testování hypotéz H_0 použit dvouvýběrový *t*-test uvedený v (Anděl, 1978, s. 91). Použití dvouvýběrového *t*-testu je i při porušení normality rozdělení přijatelné, viz (Anděl, 1978, s. 93). Výsledky testů jsou v tabulce 3. V testech je kritická hodnota testu na hladině významnosti 0.01 rovna 2.58408. Hypotéza H_0 se na hladině významnosti 0.01 zamítne, pokud je výsledná hodnota *t*-testu vyšší než kritická hodnota.

Kritérium	***t* - test**	**Hypotéza** H_0
AKOR	11.02283	Zamítá se
AVAL	6.33526	Zamítá se
MIOX	14.58698	Zamítá se

Tab. 3. *Výsledky dvouvýběrových t testů. Zdroj: Autor.*

Pro všechna kritéria se nulová hypotéza H_0 o rovnosti průměrů zamítá. Protože ve všech případech je výběrový průměr množiny S-boxů s nelinearitou 104 menší než výběrový průměr množiny S-boxů s nelinearitou 98, přijímá se alternativní hypotéza H_1. U všech těchto kritérií je menší hodnota lepší pro kryptografickou kvalitu S-boxu.

5 Závěr

Provedený experiment prokázal, že vyšší nelinearita u regulárních 8x8 S-boxů pozitivně (ve smyslu kryptograficky výhodně) ovlivňuje autokorelaci, propagaci změny a kritérium MIO-Max. Pro další představu o hodnotách výše uvedených kritérií byly spočítány jejich velikosti pro několik speciálních 8x8 S-boxů s extrémní nelinearitou rovnou 112.

S-box použitý v šifře AES: AKOR = 32, AVAL = 216, MIOX = 4

S-box APA (Cui & Cao, 2007): AKOR = 32, AVAL = 226, MIOX = 4

S-box Gray (Tran et al., 2008): AKOR = 32, AVAL = 226, MIOX = 4

S-box autorů práce (Farwa et al., 2016): AKOR = 32, AVAL = 248, MIOX = 4.

Kritéria zpracovaná v této práci slouží zejména k hodnocení odolnosti S-boxu proti diferenční a lineární kryptoanalýze. Vedle těchto klasických luštitelských metod jsou v literatuře popsány další metody jako například algebraická analýza a nebo v poslední době zkoumaná DPA (Differential Power Analysis). V odborné literatuře jsou prezentována kritéria odolnosti S-boxů proti těmto kryptoanalytickým útokům. Testování vztahů mezi těmito kritérii, včetně klasických kritérií jako nelinearita a další, jsou možná témata, kterými by se mohly zabývat návazné práce na tuto studii.

Seznam použité literatury

Anděl, J. (1978). *Matematická statistika*. Praha: SNTL.

Biryukov, A. & Perrin, L. (2015). On Reverse-Engineering S-Boxes with Hidden Design Criteria or Structure. In *CRYPTO 2015* (pp. 116-140). Berlin: Springer. doi: 10.1007/978-3-662-47989-6_6

Borissov, Y., Boyvalenkov, P. & Tsenkov, R. (2016). On a Linear Cryptanalysis of a Family of Modified DES Ciphers with Even weight S-boxes. *Cybernetics and Information Technologies*, 16(4), 3-12. doi: 10.1515/cait-2016-0063

Canright, D. & Batina, L. (2009, January 14). *A Very Compact „Perfectly Masked" S-Box for AES* (corrected). Retrieved from https://eprint.iacr.org/2009/011.pdf

Canteaut, A., Duval, S. & Leurent, G. (2015). Construction of Lightweight S-Boxes Using Feistel and MISTY Structures. In *International Conference on Selected Areas in Cryptography – SAC 2015* (pp. 373-393). Berlin: Springer. doi: 10.1007/978-3-319-31301-6_22

Carlet, C. & Ding, C. (2007). Nonlinearities of S-boxes. *Finite Fields and Their Applications*, 13(1), 121-135. doi: 10.1016/j.ffa.2005.07.003

Carlet, C. (2005). On highly nonlinear S-boxes and their inability to thwart DPA attacks. In *International Conference on Cryptology – INDOCRYPT 2005* (pp. 49-62). Berlin: Springer. doi: 10.1007/11596219_5

Carlet, C. & Ding, C. (2004). Highly nonlinear mappings. *Journal of Complexity*, 20(2-3), 205–244. doi: 10.1016/j.jco.2003.08.008

Clark, J. A., Jacob, J. L. & Stepney, S. (2005). The design of S-Boxes by simulated annealing. *New Generation Computing*, 23(3), 219-231. doi: 10.1007/BF03037656

Courtois, N.T., Debraize, B. & Garrido, E. (2006). On Exact Algebraic [Non-]Immunity of S-boxes Based on Power Functions. In *Australasian Conference on Information Security and Privacy – ACISP 2006* (pp. 76-86). Berlin: Springer. doi: 10.1007/11780656_7

Cui, L. & Cao, Y. (2007). A New S-Box Structure Named Affine-Power-Affine. *International Journal of Innovative Computing, Information and Control*, 3(3), 751–759. Retrieved from http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.129.8337

Das, S. (2014, January 7). *Ultra-lightweight 8-bit Multiplicative Inverse Based S-box Using LFSR*. Retrieved from https://eprint.iacr.org/2014/22.pdf

Dawson, M. H. & Tavares, S. E. (1991). An Expanded Set of S-box Design Criteria Based on Information Theory and its Relation to Differential-Like Attacks. In *EUROCRYPT '91* (p. 352-367). Berlin: Springer. doi: 10.1007/3-540-46416-6_30

Farwa, S., Shah, T. & Idrees, L. (2016). A highly nonlinear S-box based on a fractional linear transformation. *SpringerPlus*, 5, 1658. doi: 10.1186/s40064-016-3298-7

Ghosal, R. (2017, June 13). *Analysing Relations involving small number of Monomials in AES S-Box*. Retrieved from https://eprint.iacr.org/2017/580.pdf

Gilbert, H. & Peyrin, T. (2010). Super-Sbox Cryptanalysis: Improved Attacks for AES-like permutations. In *International Workshop on Fast Software Encryption – FSE 2010* (pp. 365-383). Berlin: Springer. doi: 10.1007/978-3-642-13858-4_21

Gologlu, F., Rijmen, V. & Wang, Q. (2016, February 23). On the division property of S-boxes. Retrieved from https://eprint.iacr.org/2016/188.pdf

Goudarzi, D., Rivain, M., Vergnaud, D. & Vivek, S. (2017, June 27). *Generalized Polynomial Decomposition for S-boxes with Application to Side-Channel Countermeasures*. Retrieved from https://eprint.iacr.org/2017/632.pdf

Guo, J., Jean, J., Nikolić, I., Qiao, K., Sasaki, Y. & Sim, S.M. (2016). Invariant Subspace Attack Against Midori64 and The Resistance Criteria for S-box Designs. *IACR Transactions on Symmetric Cryptology*, 2016(1), doi: 10.13154/tosc.v2016.i1.33-56

Guo, X., Xu, K., Sun, T. & Fan, X. (2012). Analysis of Minimum Numbers of Linearly Active S-Boxes of a Class of Generalized Feistel Block Ciphers. *Journal of Systems Science and Complexity*, 25(5), 1014-1031. doi: 10.1007/s11424-012-0238-7

Ivanov, G., Nikolov, N. & Nikova, S. (2016). Reversed Genetic Algorithms for Generation of Bijective S-boxes with Good Cryptographic Properties. *Cryptography and Communications*, 8(2), 247-276. doi: 10.1007/s12095-015-0170-5

Kazymyrov, O., Kazymyrova, V. & Oliynykov, R. (2014). A Method For Generation Of High-Nonlinear S-Boxes Based On Gradient Descent. *Mathematical Aspects of Cryptography*, 5(2), 71-78.

Khanoki, H.A., Sadeghiyan, B. & Pieprzyk, J. (2017, January 8). *Algebraic Attack Efficiency versus S-box Representation.* Retrieved from https://eprint.iacr.org/2017/007.pdf

Leventi-Peetz, A.M. & Peetz, J.V. (2015, July 13). Generating S-Box Multivariate Quadratic Equation Systems And Estimating Algebraic Attack Resistance Aided By SageMath. Retrieved from https://eprint.iacr.org/2015/589.pdf

Mazumdar, B., Mukhopadhyay, D. & Sengupta, I. (2013). Constrained Search for a Class of Good S-Boxes with Improved DPA Resistivity. *IEEE Transactions on Information Forensics and Security*, 8(12), 2154-2183. doi: 10.1109/TIFS.2013.2285522

McCluskey, E. J. (1986). *Logic design principles*. New Jersey: Prentice-Hall

Meloun, M. & Militký, J. (1998). *Statistické zpracování experimentálních dat*. Praha: East Publishing.

Mishra, P.R., Sarkar,S. & Gupta, I. (2017, April 4). *Determining the Minimum Degree of an S-box*. Retrieved from https://eprint.iacr.org/2017/376.pdf

Nawaz, Y., Gupta, K.C. & Gong, G. (2009). Algebraic Immunity of S-boxes Based on Power Mappings: Analysis and Construction. *IEEE Transactions on Information Theory*, 55(9), 4263-4273. doi: 10.1109/TIT.2009.2025534

Nyberg, K. (1992). On the Construction of Highly Nonlinear Permutations. In *EUROCRYPT '92*, (pp. 92-98). Berlin: Springer. doi: 10.1007/3-540-47555-9_8

Parker, M.G. (2003). *Generalised S-Box Nonlinearity*. Retrieved from http://www.ii.uib.no/~matthew/SBoxLin.pdf

Pieprzyk, J. (1989). Error propagation property and application in cryptography. *IEE Proceedings E – Computers and Digital Techniques*, 136(4), 262-270.

Rostovtsev, A. (2013, March 12). *AES-like ciphers: are special S-boxes better then random ones?*. Retrieved from https://eprint.iacr.org/2013/148.pdf

Sakalauskas, E. & Luksys, K. (2007, June 5). *Matrix Power S-Box Construction*. Retrieved from https://eprint.iacr.org/2007/214.pdf

Selvam, R., Shanmugam, D., Annadurai, S. & Rangasamy, J. (2016). Decomposed S-Boxes and DPA Attacks: A Quantitative Case Study using PRINCE. In *International Conference on Security, Privacy, and Applied Cryptography Engineering – SPACE 2016* (pp. 179-193). Berlin: Springer. doi: 10.1007/978-3-319-49445-6_10

Spain, M. & Varia, M. (2016, October 18). *Evolving S-Boxes with Reduced Differential Power Analysis Susceptibility*. Retrieved from https://eprint.iacr.org/2016/1145.pdf

Stoffelen, K. (2016). Optimizing S-box Implementations for Several Criteria using SAT Solvers. In *International Conference on Fast Software Encryption – FSE 2016* (pp. 140-160). Berlin: Springer. doi: 10.1007/978-3-662-52993-5_8

Tesař, P. (2010). A New Method for Generating High Non-linearity S-Boxes. *Radioengineering*, 19(1), 23-26. Retrieved from https://www.radioeng.cz/fulltexts/2010/10_01_023_026.pdf

Tran, M.T., Bui, D.K. & Duong A.D. (2008). Gray S-Box for Advanced Encryption Standard. In *International Conference on Computational Intelligence and Security 2008 - CIS ´08* (pp. 253-258). New York: IEEE. doi: 10.1109/CIS.2008.205

Webster, A. F. (1986) Plaintext/Ciphertext Bit Dependencies in Cryptographic Systems. Master's thesis, Department of Electrical Engineering, Queen's University.

Youssef, A.M., Tavares, S.E. & Gong, G. (2006). On some probabilistic approximations for AES-like S-boxes. *Discrete Mathematics*, 306(16), 2016-2020. doi: 10.1016/j.disc.2006.03.055

Zhang, W., Bao, Z., Rijmen, V. & Liu, M. (2015). A New Classification of 4-bit Optimal S-boxes and its Application to PRESENT, RECTANGLE and SONGENT. In *International Workshop on Fast Software Encryption* (pp. 494-515). Berlin: Springer. doi: 10.1007/978-3-662-48116-5_24

Zhang, W., Li, L. & Pasalic., E. (2017). Construction of resilient S-boxes with higher-dimensional vectorial outputs and strictly almost optimal nonlinearity. *IET Information Security*, 11(4), 199-203. doi: 10.1049/iet-ifs.2016.0168