# Aplikace moderních kryptoanalytických metod

Bc. Martin Mikala

Bakalářská práce
2019

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2018/2019

# ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

| | |
|---|---|
| Jméno a příjmení: | **Bc. Martin Mikala** |
| Osobní číslo: | **A16097** |
| Studijní program: | **B3902 Inženýrská informatika** |
| Studijní obor: | **Bezpečnostní technologie, systémy a management** |
| Forma studia: | **kombinovaná** |
| Téma práce: | **Aplikace moderních kryptoanalytických metod** |
| Téma anglicky: | **The Application of Modern Cryptanalysis Methods** |

Zásady pro vypracování:

1. **Vypracujte literární rešerši na dané téma.**
2. **Popište základní principy lineární a diferenciální kryptoanalýzy.**
3. **Demonstrujte použití lineární kryptoanalýzy na vlastním zvoleném příkladu šifry.**
4. **Proveďte dále demonstraci pomocí diferenciální kryptoanalýzy.**
5. **Porovnejte dosažené výsledky kryptoanalýzy a proveďte závěr.**

Rozsah bakalářské práce:

Rozsah příloh:

Forma zpracování bakalářské práce: **tištěná/elektronická**

Seznam odborné literatury:


1. **ZELENKA, Josef. Ochrana dat: kryptologie. Vyd. 1. Hradec Králové: Gaudeamus, 2003, 198 s. ISBN 80-704-1737-4.**
2. **SWENSON, Christopher. Modern cryptanalysis: techniques for advanced code breaking. Indianapolis: Wiley, c2008, xxviii, 236 s. ISBN 978-0-470-13593-8.**
3. **VONDRUŠKA, Pavel. Kryptologie, šifrování a tajná písma. 1. vyd. Praha: Albatros, 2006, 340 s. Oko. ISBN 80-000-1888-8.**
4. **KATZ, Jonathan a Yehuda LINDELL. Introduction to modern cryptography. Boca Raton: Chapman, 2008, xviii, 534 s. ISBN 978-1-58488-551-1.**
5. **PIPER, F a Sean MURPHY. Kryptografie. 1. vyd. v českém jazyce. Překlad Pavel Mondschein. Praha: Dokořán, 2006, 157 s. ISBN 80-736-3074-5.**


Vedoucí bakalářské práce: **doc. Ing. Roman Šenkeřík, Ph.D.**
Ústav informatiky a umělé inteligence

Datum zadání bakalářské práce: **21. prosince 2018**

Termín odevzdání bakalářské práce: **15. května 2019**

Ve Zlíně dne 21. prosince 2018

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ
Fakulta aplikované informatiky
L.S.

doc. Mgr. Milan Adámek, Ph.D.
*děkan*

Ing. Jan Valouch, Ph.D.
*ředitel ústavu*

**Prohlašuji, že**

- beru na vědomí, že odevzdáním bakalářské práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že bakalářské práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk bakalářské práce bude uložen v příruční knihovně Fakulty aplikované informatiky. Univerzity Tomáše Bati ve Zlíně a jeden výtisk bude uložen u vedoucího práce;
- byl/a jsem seznámen/a s tím, že na moji bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – bakalářskou práci nebo poskytnout licenci k jejímu využití jen připouští-li tak licenční smlouva uzavřená mezi mnou a Univerzitou Tomáše Bati ve Zlíně s tím, že vyrovnání případného přiměřeného příspěvku na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše) bude rovněž předmětem této licenční smlouvy;
- beru na vědomí, že pokud bylo k vypracování bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky bakalářské práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem bakalářské práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

**Prohlašuji,**

- že jsem na bakalářské práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze bakalářské práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně .....

podpis autora

**ABSTRAKT**

Hlavním cílem této Bakalářské práce je popsat metody lineární a diferenciální kryptoanalýzy a principy, na kterých jsou založeny. Druhým cílem je demonstrovat použití obou metod na zvolené blokové šifře a odhalit tak tajný klíč použitý k zašifrování otevřeného text. V závěrčné části pak proběhne srovnání výsledků obou metod.

Klíčová slova: lineární kryptoanalýza, diferenciální kryptoanalýza, bloková šifra, substitučně-permutační síť

**ABSTRACT**

Main goal of this Bachelor thesis is to describe methods of linear and differential cryptanalysis and principles they are based on. Second goal is to demonstrate usage of both methods on chosen block cipher to find secret key used to cipher plaintext. In last part there is comparision of outcome of both methods.

Keywords: linear cryptanalysis, differential cryptanalysis, block cipher, substitution-permutation network

*„Jaký smysl by mělo šifrovat zprávy tak, že by je velmi chytrý nepřítel nedokázal rozluštit? Nakonec by člověk skončil s tím, že byste nevěděl, co si nepřítel myslí, že si myslíte, že si myslí...“*

Terry Pratchett, Pátý elefant

## OBSAH

# ÚVOD

Tato práce si klade za cíl představit a na praktické ukázce demonstrovat dva nástroje moderní kryptografie zaměřené primárně na prolamování blokových šifer, a to lineární a diferenciální kryptoanalýzu. Obě metody byly oficiálně objeveny v 90. letech 20. století jako nástroj k prolomení tehdejšího šifrovacího standardu DES, minimálně metoda diferenciální kryptoanalýzy byla autorům šifry DES známa již o téměr 20 let dříve, ale byla držena v přísném utajení z důvodu národní bezpečnosti.

Tato práce demonstruje pouze základní úroveň obou kryptoanalýz, v praxi již bylo objeveno mnoho způsobů, jak učinit tyto nástroje ještě silnějšími.

První část práce je věnována obecnému úvodu do kryptologie. Cílem je definice pojmů nutných k pochopení problematiky lineární a diferenciální kryptoanalýzy. Následuje popis kryptoanalytických principů, na kterých tyto metody staví.

Druhá část práce se věnuje teoretickému popisu obou kryptoanalýz s praktickými ukázkami jednotlivých kroků.

Poté následuje demonstrace tříkolové mnohonásobné lineární a diferenciální kryptoanalýzy na vzorové šifře, jejíž cílem je odhalit použitý klíč, a poukázat na podobnosti a rozdíly obou metod.

V závěru následuje srovnávací analýza výkonu obou metod na zvolené šifře s cílem porovnat pravděpodobnost úspěchu útoku v závislosti na počtu známých otevřených textů, a demonstrace vhodnosti použití mnohonásobných kryptoanalýz oproti jednoduchých kryptoanalýzám.

# I. TEORETICKÁ ČÁST

# 1 Kryptografie

„Kryptologie je vědní obor zabývající se šifrováním a dešifrováním zpráv. Zahrnuje v sobě kryptografii a kryptoanalýzu. Kryptografie označuje nauku o šifrování, kryptoanalýza se pak zabývá lámáním šifer (tj. luštěním bez znalosti klíče).“[1]

## 1.1 Rozdělení kryptografie

Za základní způsob rozdělení kryptografie je považováno dělení na klasickou kryptografii a moderní kryptografii. K přechodu na moderní kryptografii došlo zhruba v období 2. světové války s rozvojem výpočetní techniky. Tato práce je věnována výhradně metodám moderní krypografie.

Moderní kryptografie je dělena dle stavby klíče na symetrickou, kde je stejný klíč použit pro šifrování i dešifrování, a asymetrickou, také označovanou jako kryptografie s veřejným klíčem. Při ní jsou k šifrování a dešifrování zprávy použity rozdílné klíče.

## 1.2 Asymetrická kryptografie

První praktické použití asymetrické kryptografie bylo představeno roku 1976 na konferenci pořádané federací AFIPS[1)]. Autory jsou dva američtí kryptologové, Whitfield Diffie a Martin E. Hellman. Ve svém díle Multiuser cryptographic techniques[2)] představují dvě techniky distribuce klíčů. „Druhá technika je stále ve fázi konceptu, ale slibuje úplně eliminovat potřebu bezpečného kanálu pro distribuci klíče tím, že je zasilatelova informace o klíči veřejná. Je zde také ukázáno, jak by takový kryptosystém s veřejným klíčem umožnil vývoj autentizačního systému, který by generoval nepadělatelný digitální podpis závisející na zprávě.“[3)][2] Tento systém je známý pod jménem Diffie-Helmanova výměna klíče.

„Podle informací britské vlády byla asymetrická kryptografie objevena v britské tajné instituci GCHQ. Práce na této technologii zahájil v roce 1965 James Ellis, který načrtl základní principy. Roku 1973 nový pracovník „Clifford Cocks“ navrhl reálný systém AK. Z důvodů utajení nebyl tento objev veřejně publikován a byl odhalen až několik let po uvedení RSA.“[3]

Dle dnes již odtajněného memoranda NSAM 160 z června 1962 měla americká NSA již tehdy k dispozici systémy asymetrické kryptografie.[4]

[1)] American Federation of Information Processing Societies

[2)] Kryptografické techniky pro mnoho uživatelů

[3)] The second technique is still in the conceptual phase, but promises to eliminate completely the need for a secure key distribution channel, by making the sender's keying information public. It is also shown how such a public key cryptosystem would allow the development of an authentication system which generates an unforgeable, message dependent digital signature.

„Při asymetrickém šifrování (asymetrický = nesouměrný), jsou použity dva klíče. První, veřejný klíč (public key) pro zašifrování zprávy (je přístupný komukoliv, kdo chce šifrovaně odeslat data příjemci zprávy) a druhý, soukromý klíč (private key), pro dešifrování.“[5]

Nejznámějším asymetrickým šifrovacím systémem je RSA pojmenovaný podle jmen autorů (Rivest, Shamir, Adelman) a vydaný roku 1977.

## 1.3 Symetrická kryptografie

„Šifry symetrické jsou šifrovací algoritmy, které používají pro zašifrování i rozšifrování sdílený klíč.“[6] Z tohoto pohledu většina moderních a všechny historické šifry spadají do této kategorie. Symetrické šifry se dělí do dvou skupin na základě toho, zda je současně šifrován jeden nebo více znaků.

### 1.3.1 Proudové šifry

U proudových šifer probíhá šifrování postupně po jednotlivých znacích. U historických šifer (např. Vigenérova šifra) jde o jednotlivá písmena, u moderních šifer pak o jednotlivé bity. Na základě toho, zda je ke generování klíče použit předchozí již zašifrovaný text se tyto šifry dělí dále na synchronní (kde je klíč nezávislý na zašifrovaném textu) a asynchronní.

Mezi nejznámější moderní proudové šifry patří Vernamova šifra, jinak také známá jako jednorázová tabulková šifra, či A5 sloužící k šifrování GSM signálu.

### 1.3.2 Blokové šifry

„Blokové šifry zašifrovávají současně celý blok dat“.[7] Vstupem šifry je vždy $n$ bitů, počet bitů výstupu je zpravidla stejný. Na rozdíl od proudových šifer změna jednoho bitu vstupu ovlivní šifrování celého bloku.

Mezi nejznámější blokové šifry patří například FEAL, DES a jeho varianta 3DES, AES či IDEA.

## 1.4 Provozní režimy blokových šifer

V praxi je stejně jako použitá šifra důležitý způsob její implementace. Na základě způsobu, jakým daná šifra využívá (nebo nevyužívá) data zašifrovaná v předchozích krocích, a jakým způsobem probíhá generování klíče, je možno rozlišit několik provozních režimů.

Těmito provozními režimy blokových šifer se zabývá norma ISO/IEC 10116:2017 - Information technology – Security techniques – Modes of operation for an n-bit block

cipher. [8] Norma se zabývá provozními režimy ECB, CBC, CFB, OFB a CTR.

### 1.4.1 Elektronická kódová kniha (ECB - Electronic Code Book)

Jedná se o základní a nejjednodušší provozní režim moderních šifer, kdy je každý blok otevřeného textu šifrován nezávisle na předchozích blocích. Systém je odolný proti chybám při šifrování, dešifrování či přenosu dat, neboť každá chyba znemožní dešifrování pouze jednoho bloku textu. „Díky rychlosti a možnosti paralelního zpracování bývá tento režim použit v databázích, kde umožňuje přidávat nebo mazat záznamy nezávisle na ostatních.“[4)][9]

Nevýhodou tohoto systému režimu je fakt, že shodný otevřený text dá za použití stejného klíče totožný šifrovaný text, z čehož vyplývá zranitelnost režimu proti celé řadě útoků, například analýze provozu, frekvenční analýze či substitučnímu útoku. Tento režim také generuje velké množství dat nutných pro lineární i diferenciální kryptoanalýzu. [9]

### 1.4.2 Řetězení šifrových bloků (CBC - Cipher Block Chaining)

Na rozdíl od režimu ECB se při šifrování každého bloku otevřený text exkluzivně binárně sečte se šifrovým textem předchozího bloku, zbytek šifrování se nemění. Tím dojde k „řetězení“, kdy změna jednoho bitu otevřeného textu ovlivní nejen šifrování současného bloku, ale také všech následujících. Stejný otevřený text je v rámci šifry pokaždé šifrován jinak, čímž se zvyšuje bezpečnost.

Nevýhodou tohoto režimu je nemožnost provozovat šifrování ani dešifrování paralelně a také větší náchylnost na chyby, kdy „pokud je jeden bit otevřeného textu poškozený (například kvůli chybě při přenosu), všechny následující bloky šifry budou poškozeny a nebude nikdy možné získat otevřený text z tohoto šifrovaného textu“.[5)][10]

### 1.4.3 Šifrová zpětná vazba (CFB - Cipher Feedback)

„V tomto režimu se prakticky jedná o proudovou šifru. Bloková šifra zde slouží jako generátor pseudonáhodné posloupnosti, která je pak použita pro zašifrování otevřeného textu (zprávy) operací XOR (součet mod 2). Generátor je ovlivňován zpětnou vazbou získanou ze zašifrovaného textu. Zpětná vazba dala tomuto režimu i název - Ciphertext FeedBack.“[11]

[4)] Due to its speed and parallelization advantages, it has been used in database applications; addition or deletion of entries can be done independently of other records.

[5)] If one bit of a plaintext message is damaged (for example because of some earlier transmission error), all subsequent ciphertext blocks will be damaged and it will be never possible to decrypt the ciphertext received from this plaintext.

Jde o režim podobný CBC, s tím rozdílem, že zatímco u řetězení šifrových bloků se zašifrovaný text minulého kola binárně sečte s otevřeným textem a poté šifruje, v tomto případě se nejprve zašifruje šifrovaný text z minulého kola a až poté proběhne binární součet s otevřeným textem kola.

Tento režim využívá stejného algoritmu k šifrování i dešifrování. Ačkoli šifrování musí probíhat postupně, dešifrování je možné provést paralelně.

### 1.4.4 Výsledková zpětná vazba (OFB - Output Feedback)

Tento mód provozu generuje na základě inicializačního vektoru a klíče hlavní klíč, který po binárním součtu s otevřeným textem teprvé dává šifrovaný text. Z tohoto pohledu simuluje proudovou šifru, neboť samotné šifrování probíhá po jednotlivých bitech.

Výhodou této metody je, že šifrování i dešifrování probíhá na základě stejného postupu. Hlavní klíč také může být nachystán před začátkem šifrování. Poškození jednoho bitu textu při přenosu ovlivní čitelnost pouze jednoho bitu. „Největší nevýhodou OFB je, že opakované šifrování inicializačního vektoru může vygenerovat již dříve vygenerovaný text. Jde o nepravděpodobnou situaci, ale v takovém případě začne být otevřený text šifrován již použitým klíčem.“[6)][10]

### 1.4.5 Čítač (CTR - Counter)

Poslední metodou zmíněnou v normě ISO je čítačový režim. Jde o metodu připomínající přecházející v tom, že pomocí vstupu a klíče generuje hlavní klíč, který se exkluzivně binárně sčítá s otevřeným textem. Rozdíl je v tom, že šifrovaný text nezávisí na informaci z předchozího kola. Namísto toho se před započtením šifrování vygeneruje náhodné či pseudonáhodné číslo unikátní pro každý šifrovaný text. K tomuto číslu se připojí čítač, který se u každého bloku navyšuje o 1. Tím se dosáhne stavu, kdy je každý blok šifrován jiným hlavním klíčem.

Šifrování i dešifrování může probíhat paralelně, poškození 1 bitu otevřeného či šifrového textu ovlivní pouze výsledek 1 bitu. „Může být dokázáno, že čítačový režim poskytuje vysokou úroveň bezpečnosti a klíč je nutno měnit méně často než u metody CBC.“[7)][10]

[6)] The biggest drawback of OFB is that the repetition of encrypting the initialization vector may produce the same state that has occurred before. It is an unlikely situation but in such a case the plaintext will start to be encrypted by the same data as previously.

[7)] It can be proved that the CTR mode generally provides quite good security and that the secret key needs to be changed less often than in the CBC mode.

# 2 Stavba moderních šifer

Americký informatik Claude Elwood Shannon definuje ve svém díle „Communication theory of secrecy systems“[12] dvě vlastnosti šifry, které zvyšují odolnost šifry proti metodám statistické analýzy. Tyto vlastnosti pojmenovává „zmatení“[1)] a „difúze“[2)].

## 2.1 Zmatení

„Metodou zmatení je myšleno učinit vztah mezi jednoduchým rozložením šifrovaného textu a jednoduchým popisem klíče velmi komplexním a složitým.“[3)][12]

Zmatení u blokových šifer je dosaženo pomocí substituce, neboli sboxů.

### 2.1.1 Substituce

Termínem substituce je myšleno nahrazení jednoho prvku jiným. U historických šifer šlo zpravidla o záměnu na úrovni jednotlivých písmen, případně jejich dvojic. V moderní kryptografii probíhá substituce zpravidla na úrovni několika bitů. Například vzorová šifra z praktické části provádí substituci na úrovni 4 bitů, což znamená, že nahrazuje čtyřbitovou hodnotu vstupu čtyřbitovou hodnotou výstupu. Seznam jednotlivých možných substitucí v rámci jedné operace bývá označován jako sbox.

## 2.2 Difúze

„Difúze znamená, že změna jednoho znaku otevřeného textu změní několik znaků šifrovaného textu, a stejně tak, změníme-li jeden znak šifrovaného textu, mělo by se změnit několik znaků otevřeného textu“[4)][13]

Dostatečné úrovni difúze je dosaženo permutací, neboli pboxy.

### 2.2.1 Permutace

V kryptografii je permutací myšlena změna pořadí jednotlivých znaků podle předem určeného pořadí. U historických šifer šlo zpravidla o písmena, u moderních šifer pak jde o jednotlivé bity.

---

[1)] confusion

[2)] diffusion

[3)] The method of confusion is to make the relation between the simple statistics of $E$ and the simple description of $K$ a very complex and involved one.

[4)] Diffusion means that if we change a character of the plaintext, then several characters of the ciphertext should change, and similarly, if we change a character of the ciphertext, then several characters of the plaintext should change.

### 2.3 Přičtení klíče

U moderních šifer probíhá přičtení klíče na úrovni bitů. Konkrétně jde o „exkluzivní disjunkci“ daného bitu šifrovaného textu a odpovídajícího bitu klíče. Pravdivostní tabulka exkluzivní disjunkce dvou proměnných je následující:

Tab. 2.1 Exkluzivní dijunkce

| $A$ | $B$ | $A \oplus B$ |
|---|---|---|
| 1 | 1 | 0 |
| 1 | 0 | 1 |
| 0 | 1 | 1 |
| 0 | 0 | 0 |

### 2.4 Substitučně - permutační síť

„Substitučně-permutační sít je iterovaná šifra, která následuje Shannonovy pravidla zmatení a difúze. Jak již bylo řešeno zmatení a difúze jsou dosaženy použitím substituční fáze a permutační fáze u šifry. Kolo šifry se tak skládá ze tří částí - substituce, permutace a přičtení klíče.“[5)][14]

## 3 Kryptoanalýza

Druhou částí kryptologie je kryptoanalýza, která se zabývá prolamováním šifer bez znalosti použitého klíče. Jde o velmi důležitý doplňek kryptografie, neboť pouze při znalosti silných kryptoanalytických metod je možno tvořit a používat šifry bezpečně.

### 3.1 Druhy útoků

Ačkoli je hlavním cílem kryptoanalýzy získat otevřený text pouze ze znalosti šifrovaného textu, je možno útoky provádět i na nižších úrovních, kde může existovat vyšší pravděpodobnost úspěšného provedení útoku. V závislosti na známých proměnných můžeme definovat několik druhů kryptoanalytických útoků.

#### 3.1.1 Známý šifrovaný text (Known-ciphertext)

Cílem tohoto toku je odhalit otevřený text a případně použité heslo pouze na základě znalosti šifrovaného textu. „Při tvorbě šifrovacích algoirmů je velmi důležité zabezpečit je proti útokům se známým šifrovaným textem, neboť jsou nejvíce zřejmým vstupním

[5)] An SPN is an iterated cipher that follows Shannon's rules of confusion and diffusion. As stated previously confusion and diffusion are achieved by using a substitution phase and a permutation phase in this network. A round in this iterated cipher consists of three phases - substitution, permutation and key mixing.

bodem pro každou kryptoanalýzu. Proto nejsou dobře připravené a revidované šifry zpravidla příliš zranitelné tímto typem útoků.“[1)][15]

### 3.1.2 Známý otevřený text (Known-plaintext)

„Útok se známým otevřených textem neboli „tahákem“ je model kryptoanalytického útoku, kde zná útočník vzorky otevřeného textu a jemu odpovdající šifrovaný text, a může je použít k odhalení dalších tajných informací, jako jsou tajné klíče a kódové knihy. Termín „tahák“ pochází z Bletchley Parku, kde byla za 2. světové války vedena britská dešifrovací operace.“[2)][16]

### 3.1.3 Zvolený otevřený text (Chosen-plaintext)

„Během útoku se zvoleným otevřeným textem si kryptoanalytik může vybrat libovolný otevřený text k zašifrování a tím získá odpovídající zašifrovaný text. Pokouší se získat tajný klíč nebo případně vytvořit algorimus, který by mu umožnil dešifrovat libovolné šifrované zprávy zašifrované tímto klíčem (ale bez znalosti samotného klíče). “[3)][15]

„Útoky se zvoleným otevřeným textem jsou extrémně důležité v kontextu kryptografie s veřejným klíčem, kde je šifrovací klíč veřejný a útočník může zašifrovat libovolně zvolený otevřený text.“[4)][16]

### 3.1.4 Zvolený šifrovaný text (Chosen-ciphertext)

V tomto případě si útočník může zvolit šifrovaný text, ke kterému získá odpovídající otevřený text. Cílem je odhalit klíč, kterým byl tento otevřený text zašifrován.

„Mnoho jinak bezpečných schémat může být prolomeno útokem se zvoleným šifrovaným textem. Například kryptosystém El Gamal je sémanticky bezpečný[5)] proti útoku se zvoleným otevřeným textem, tato sémantická bezpečnost může být jednoduše

[1)] While designing encryption algorithms, it is particularly important to secure them against ciphertext-only attacks, as they are the most obvious starting point for every cryptanalysis. That is why well prepared and reviewed ciphers are usually not very vulnerable to these kinds of attacks.

[2)] The known-plaintext attack (KPA) or crib is an attack model for cryptanalysis where the attacker has samples of both the paintext and its encrypted version (ciphertext), and is at liberty to make use of them to reveal further secret information such as secret keys and code books. The term „crib“ originated at Bletchley Park, the British World War II decryption operation.

[3)] During the chosen-plaintext attack, a cryptanalyst can choose arbitraty plaintext data to be encrypted and then he receives the corresponding ciphertext. He tries to acquire the secret encrytion key or alternatively to create an algorithm which would allow him to decrypt any ciphertext messages encrypted using this key (but without actually knowing the secret key).

[4)] Chosen-plaintext attacks become extremely important in the context of public key cryptography, where the encryption key is public and attackers can encrypt any plaintext they choose.

[5)] „Sémanticky bezpečný kryptosystém je takový, kdy je možno ze šifrovaného textu odvodit pouze zanedbatelné množství informací o otevřeném textu“[6)][17]

prolomena při útoku se zvoleným šifrovaným textem.“[7)][16]

## 4 Principy útoku

Existuje velké množství principů, na základě kterých může být kryptoanalytický útok veden, ať už se jedná o útok přímo na šifru či na její implementaci. Níže jsou představeny pouze principy, na kterých je postavena lineární a diferenciální kryptoanalýza.

### 4.1 Útok hrubou silou

Základním kryptografickým principem je útok hrubou silou, označovaný také jako „kompletní prohledání“. Útok probíhá postupným testováním všech možných klíčů. Ačkoli je touto metodou teoreticky možno prolomit prakticky každou šifru, v praxi to vzhledem k výpočetní náročnosti a délce klíče reálně používaných šifer není možné. Šifra s klíčem délky 128 bitů umožňuje zhruba $3,4 \cdot 10^{38}$ možných klíčů.

Šifru s dostatečně krátkým klíčem je nicméně možno tímto klíčem prolomit. Tento princip využívají metody lineární i diferenciální kryptoanalýzy, které nejprve omezí počet možných bitů klíče, které je možno testovat samostatně, a na tuto část klíče je poté veden útok hrubou silou.

### 4.2 Meet-in-the-middle

„Meet-in-the-middle (MITM) je obecný kryptoanalytický přístup původně vyvinut pro kryptoanalýzu blokových šifer. Vývoj začíná s kryptoanalýzou DES, který se datuje do roku 1977.“[1)][18] Za touto kryptoanalýzou stojí již zmiňovaná dvojice kryptologů Diffie a Helman.

Je-li otevřený text šifrován dvěma nezávislými klíči $K$, $K'$ délky $n$ bitů, je možno počet možných kombinací klíčů spočítat jako $2^{2n}$. V případě útoku hrubou silou je nutno otestovat toto množství klíčů.

Známe-li zároveň otevřený a jemu odpovídající šifrovaný text, můžeme začít provádět útok hrubou silou na klíč $K$ šifrováním otevřeného textu a zapisováním všech kombinací použitý klíč $K$:částečně zašifrovaný text. Zároveň je možno provádět druhý útok hrubou silou na klíč $K'$ dešifrováním šifrovaného textu a zapisováním všech kombinací použitý klíč $K'$:částečně dešifrovaný text. V okamžiku, kdy je objevena stejná hodnota v obou tabulkách je nalezen potenciální kombinace klíčů $K, K'$.

[7)] A number of otherwise secure schemes can be defeated under chosen-ciphetext attack. For example, the El Gamal cryptosystem is semantically secure under chosen-plaintext attack, but this semantic security can be trivially defeated under a chosen-ciphertext attack.

[1)] Meet-in-the-middle (MITM) is a generic cryptanalytic approach originally developed from cryptanalysis of block cipher. Early development start with cryptanalysis of DES, which dates back to 1977.

V tomto případě je nutno ověřit pouze $2^{n+1}$ možností, zároveň je ale nutno toto množství informací uložit do databáze. Tento princip je nazýván space-time tradeoff (výměna místa za čas).

Na principu MITM útoku, tedy současném útoku z obou stran šifry, jsou postaveny metoda lineární i diferenciální kryptoanalýzy.

## 5 Lineární kryptoanalýza

V roce 1992 představili Mitsuru Matsui a Atsuhiro Yamagishi na konferenci EUROCRYPT 1992 „Novou metodu pro útok na šifru FEAL se známým otevřeným textem.“[1)] Autoři tuto metodu popisují slovy: „Naše metoda je druh meet-in-the-middle útoku s částečným útokem hrubou silou; tím můžeme odvodit rozšířený klíč přímo a úplně.“[2)][19]

O rok později představil Matsui útok touto metodou na šifru DES. „Je možné prolomit osmikolovou DES šifru při $2^{21}$ známých otevřených textů a šestnáctikolovou DES šifru s $2^{47}$ známých otevřených textů. Navíc je tato metoda za určitých okolností použitelná ve formě útoku se známým šifrovaných textem (known-ciphertext). Například, pokud se otevřený text skládá pouze z obyčejných anglických vět kódovaných v ASCII, osmikolová DES šifra je prolomitelá při znalosti pouze $2^{29}$ šifrovaných textů.“[3)][20]

V dalším roce pak Matsui metodu ještě vylepšil a úspěšně provedl experimentální útok na plný šestnáctikolový DES, ke kterému potřeboval $2^{43}$ otevřený textů a odpovídajících šifrovaných textů. Experiment trval 50 dní na 12 počítačích, kdy 40 dní zabralo generování požadovaného množství dat a 10 dní samotný útok. [21]

### 5.1 Princip použití

„Prvním cílem lineární kryptoanalýzy je nalezení následující rovnice lineární aproximace, která platí s pravděpodobností $p \neq 1/2$ pro náhodně zvolený otevřený text P a odpovídající šifrovaný text C a tajný klíč K, kde $i_1, i_2, ..., i_a, j_1, j_2, ..., j_b$ a $k_1, k_2, ..., k_c$ značí fixní lokace bitů.“[4)] [20]

---

[1)] A New Method for Known Plaintext Attack of FEAL Cipher

[2)] Our method is a kind of meet-in-the-middle attack with a partial exhaustive search; hence we can derive the extended key directly and definitely.

[3)] As a result, it is possible to break 8-round DES cipher with $2^{21}$ known-plaintexts and 16-round DES cipher with $2^{47}$ known-plaintexts, respectively. Moreover, this method is applicable to an only-ciphertext atack in certain situations. For example, if plaintexts consist of natural English sentences represented by ASCII codes, 8-round DES cipher is breakable with $2^{29}$ ciphertexts only.

[4)] The first purpose of linear cryptanalysis is to find the following linear approximate expression which hodls with probability $p \neq 1/2$ for randomly given plaintext P, the corresponding ciphertext C and the fixed secret key K, where $i_1, i_2, ..., i_a, j_1, j_2, ..., j_b$ and $k_1, k_2, ..., k_c$ denote fixed bit locations.

$$P[i_1, i_2, ..., i_a] \oplus C[j_i, j_2, ..., j_b] = K[k_1, k_2, ..., k_c] \tag{5.1}$$

Zápis $P[i_1, i_2, ..., i_a]$ značí exkluzivní binární součet 1.,2.,...,a-tého bitu otevřeného textu (to stejné platí pro $C[...]$ i $K[...]$), neboli:

$$\begin{aligned} P[i_1, i_2, ..., i_a] &= P_{i_1} \oplus P_{i_2} \oplus ... \oplus P_{i_a} \\ P[i_1, i_2, ..., i_a] &= P_1 \oplus P_2 \oplus ... \oplus P_a \end{aligned} \tag{5.2}$$

Exkluzivní binární součet náhodně zvolených sčítanců je roven 0 s pravděpodobností $p = 1/2$, z čehož vyplývá, že neexistuje-li závislost mezi zvolenými bity, bude výše zmíněná rovnice platit v $1/2$ případů.

Protože $k_1 \oplus k_2 \oplus ... \oplus k_c = 0$ platí v $1/2$ případů a zároveň je v rámci jedné aproximace konstantní, některé zdroje (např. [22]) tuto část z rovnice rovnou vypouští:

$$P[i_1, i_2, ..., i_a] \oplus C[j_i, j_2, ..., j_b] = 0 \tag{5.3}$$

Jinými slovy hledáme takovou kombinaci bitů otevřeného textu a bitů šifrovaného textu, jejíž binární součet je roven 0 s pravděpodobností $p$, kde $|p - 1/2| > 0$. Tato pravděpodobnost se označuje jako lineární bias.

### 5.1.1 Lineární bias

„Bias je systematická chyba ve sběru, analýze a interpretaci dat, která vede ke zkreslení konečných výsledků.“[23] Právě tuto systematickou chybu lineární kryptoanalýza využívá.

Vzhledem k tomu, že jak permutace tak přičtení klíče jsou lineární prvky, je jediným nelineárním prvkem, který je nutné aproximovat, substituce. Cílem je tedy nalézt pro daný sbox řešení následující binární rovnice pro všechna $X$,$Y$, $a$ a $b$, kde $X_1X_2X_3X_4$ značí binární zápis vstupu do sboxu, $Y_1Y_2Y_3Y_4$ binární zápis výstupu, $a_1a_2a_3a_4$ vstupní masku a $b_1b_2b_3b_4$ výstupní masku.[22]

$$a_1X_1 \oplus a_2X_2 \oplus a_3X_3 \oplus a_4X_4 = b_1Y_1 \oplus, b_2Y_2 \oplus b_3Y_3 \oplus b_4Y_4 \tag{5.4}$$

Rovnici je možno zobecnit pro $m$ bitů vstupu a $n$ bitů výstupu sboxu:

$$\sum_{i=0}^{m-1} a_iX_i = \sum_{j=0}^{n-1} b_jY_j \tag{5.5}$$

Výsledky se zpravidla interpretují v tabulce, kde řádky značí jednotlivé hexadecimálně vyjádřené vstupy $a_1a_2a_3a_4$, sloupce výstupy $b_1b_2b_3b_4$ a v odpovídajících buňkách počet platných rovnic ponížený o polovinu počtu rovnic.

### 5.1.2 Ukázka lineární aproximace sboxu

Pro ukázku byl vybrán sbox1 z praktické části práce. Zvolíme-li $a_1a_2a_3a_4 = 1000$ a $b_1b_2b_3b_4 = 0110$ dostaneme následující rovnici:

$$X_1 \oplus Y_2 \oplus Y_3 = 0 \tag{5.6}$$

Vyhodnotíme rovnici pro všechny kombinace vstupů a výstupů do sboxu:

Tab. 5.1 Lineární aproximace pro danou vstupní a výstupní masku

| $X_D$ | $Y_D$ | $X_B$ | $Y_B$ | $X_1$ | $Y_2$ | $Y_3$ | $X_1 \oplus Y_2 \oplus Y_3$ |
|---|---|---|---|---|---|---|---|
| 0 | 15 | 0000 | 1111 | 0 | 1 | 1 | 0 |
| 1 | 1 | 0001 | 0001 | 0 | 0 | 0 | 0 |
| 2 | 7 | 0010 | 0111 | 0 | 1 | 1 | 0 |
| 3 | 0 | 0011 | 0000 | 0 | 0 | 0 | 0 |
| 4 | 9 | 0100 | 1001 | 0 | 0 | 0 | 0 |
| 5 | 6 | 0101 | 0110 | 0 | 1 | 1 | 0 |
| 6 | 2 | 0110 | 0010 | 0 | 0 | 1 | 1 |
| 7 | 14 | 0111 | 1110 | 0 | 1 | 1 | 0 |
| 8 | 11 | 1000 | 1011 | 1 | 0 | 1 | 0 |
| 9 | 8 | 1001 | 1000 | 1 | 0 | 0 | 1 |
| 10 | 5 | 1010 | 0101 | 1 | 1 | 0 | 0 |
| 11 | 3 | 1011 | 0011 | 1 | 0 | 1 | 0 |
| 12 | 12 | 1100 | 1100 | 1 | 1 | 0 | 0 |
| 13 | 13 | 1101 | 1101 | 1 | 1 | 0 | 0 |
| 14 | 4 | 1110 | 0100 | 1 | 1 | 0 | 0 |
| 15 | 10 | 1111 | 1010 | 1 | 0 | 1 | 0 |

Index $D$ značí dekadickou hodnotu, $B$ pak tuto stejnou hodnotu vyjádřenou ve dvojkové soustavě. Při neexistenci závislosti mezi zvolenými bity je očekávána platnost rovnice v 8 (16/2) případech, namísto toho rovnice platí pro 14 případů. Rozdíl mezi těmito dvěma hodnotami, $(14 - 8)/(16/2)$ neboli $0,75$ je lineární bias této kombinace masek $a$ a $b$. Výsledkem provedení těchto operací pro všechny masky je tabulka lineární aproximace pro sbox1, kterou je možno nalézt v příloze.[5)]

[5)] V rámci útoku z praktické části je pracováno pouze s velikostí biasu a nikoli z jeho směrem, proto jsou v této tabulce uvedeny pouze absolutní hodnoty výsledků

## 5.2 Aproximace více sboxů

„Nechť jsou $X_i(1 \leq i \leq n)$ nezávislé náhodné proměnné jejichž hodnota je 0 s pravděpodobností $p_i$ nebo 1 s pravděpodobností $1 - p_i$. Pak je pravděpodobnost, že $X_1 \oplus X_2 \oplus ... \oplus X_n = 0$:“[6)][20]

$$\frac{1}{2} + 2^{n-1} \prod_{i=1}^{n} (p_i - \frac{1}{2}) \tag{5.7}$$

Toto tvrzení nazývá Matsui Lemma o skládání[7)]. Rovnici můžeme uvést ve tvaru:

$$\epsilon = \frac{1}{2} \prod_{i=1}^{n} \frac{2a_i}{x} \tag{5.8}$$

Kde $a_i$ je hodnota z tabulky lineární aproximace $i$-tého sboxu a $x$ počet možných kombinací vstup/výstup daného sboxu.

Se zvyšujícím se počtem zapojených sboxů klesá bias, čímž se zvyšuje počet různých otevřených textů nutných k provedení útoku na šifru. Matsui uvádí v [20] pro výpočet pravděpodobnosti úspěchu útoku v závislost na velikosti biasu následující vzorec:

$$\int_{-2\sqrt{N}|p-\frac{1}{2}|}^{\infty} \frac{1}{\sqrt{2\pi}} e^{-\frac{x}{2}} dx \tag{5.9}$$

Ze vzorce dle Matsuiho vyplývá, že provedení lineární aproximace se stejnou pravděpodobností úspěchů u rovnice s polovičním biasem vyžaduje čtyřnásobný počet různých otevřených textů.

## 5.3 Varianta útoku se známým šifrovaným textem

Matsui se ve svém díle také zmiňuje o možnosti eskalace útoku na útok se znalostí šifrovaného textu (known-ciphertext). „Obecně řečeno, pro daný šifrový algoritmus existuje mnoho rovnic lineární aproximace. Navíc, pokud není otevřený text náhodný, můžeme najít výraz, který v sobě nemá žádný bit otevřeného textu. Toto naznačuje, že naše metoda v konečném důsledku vede k útoku se znalostí pouze šifrovaného textu.“[8)][20]

Předpokládejme, že se otevřený text skládá pouze z velkých a malých písmen, mezer, čárek a teček, a že je kódován osmibitovým kódem (například ASCII). Z použitých

[6)] Let $X_i(1 \leq i \leq n)$ be independent random variables whose values are 0 with probability $p_i$ or 1 with probability $1 - p_i$, Then the probability that $X_1 \oplus X_2 \oplus ... \oplus X_n = 0$ is

[7)] Piling-up Lemma

[8)] Generally speaking, there exist many linear approximate expressions for a given cipher algorithm. Moreover, if plaintexts are not random, we may even find an expression which has no plaintext bit in it. This suggests that our method finally leads to an only-ciphertext attack.

znaků má největší hodnotu znak „z“ - 122, binárně 01111010. Z toho vyplývá, že první bit každého znaku bude 0, tento bit připadne na pozice s indexem 0,8 a 16. Vezměme následující rovnici šifry z praktické části platnou s biasem 3/1024:

$$P_0 \oplus C_4 \oplus C_{14} = 0 \tag{5.10}$$

Bylo odvozeno, že $P_0 = 0$. Dosazením do rovnice dostaneme $C_4 \oplus C_{14} = 0$, neboli rovnici lineární aproximace pouze z bitů šifrovaného textu. Dále útok pokračuje stejným způsobem jako v případě známého otevřeného textu.

### 5.4 Odvození bitů klíče

„Pro všechny možné hodnoty cílového částečného klíče kola, odpovídající bity šifrovaného textu jsou XORovány s bity testovaného klíče kola a výsledek je veden od konce skrze odpovídající sboxy. Toto je provedeno pro všechny vzorky otevřeného textu/šifrovaného textu a pro každou hodnotu testovaného klíče je veden záznam. “[9)][22]

U špatného klíče předpokládáme, že rovnice bude platit v 1/2 případů. Čím větší kladný či záporný rozdíl od 1/2, tím větší šance, že daný klíč je správný. Při vyhodnocení se tedy hodnoty jednotlivých testovaných klíčů upraví tak, aby reflektovaly rozdíl od 50% pravděpodobnosti:

$$H_i = |h_i - \frac{x}{2}| \tag{5.11}$$

Kde $x$ je počet testovaných rovnic a $h_i$ počet platných rovnic u klíče $i$.

## 6 Diferenciální kryptoanalýza

Metoda diferenciální krytoanalýzy byla představena roku 1990 izraelskými kryptografy Eli Binhamem a Adi Shamirem jako útok na šifru DES. Roku 1993 byl popis této metody vydán knižně v díle „Diferenciální kryptoanalýza DES“. Kniha se kromě aplikace na šifru DES věnuje také kryptoanalýze šifry FEAL a dalších.

V úvodu autor uvádí: „Krátce před odeslání knihy vydavatelům, Don Coppersmith (člen týmu, který navrhoval DES ve firmě IBM na začátku 70.let) potvrdil, že si byl jeho tým vědom diferenciální kryptoanalýzy již v roce 1974, a navrhovali S boxy a permutaci

[9)] For all possible values of the target partial subkey, the corresponding ciphertext bits are exclusive-ORed with the bits of the target partial subkey and the result is run backwards through the corresponding S-boxes. This is done for all known plaintext/ciphertext samples and a count is kept for each value of the target partial subkey.

tak, aby jej co nejvíce znemožnili. Tuto informaci museli držet v tajnosti 18 let z důvodu národní bezpečnosti, neboť šlo o velmi silnou formu kryptoanalýzy, ale rozhodli se ji zvěřejnit poté, co jsme metodu znovuobjevili a publikovali.“[1)][24]

Název metody vychází z faktu, že „analyzuje vývoj diferencí (rozdílů), když jsou dva souvisící otevřené texty zašifrovány stejným klíčem.“[2)][24] „Diferenciální kryptoanalýza je prvním publikovaným útokem schopný rozlomit plný 16ti kolový DES s komplexitou menší než $2^{55}$. Při analýze dat se analyzuje zhruba $2^{36}$ šifrovaných textů v čase $2^{37}$.“[3)][24]

Nejčastěji je používán jako útok se zvoleným otevřeným textem, jde ale teoreticky využít i pro útok se známým otevřeným textem.

## 6.1 Princip použití

Cílem metody je nalezení pravděpodobné diference výstupu na základě diference vstupů. Mějme dva vstupy $X'(X'_1X'_2X'_3X'_4)$ a $X''(X''_1X''_2X''_3X''_4)$, k nim odpovídající výstupy $Y'(Y'_1Y'_2Y'_3Y'_4)$ a $Y''(Y''_1Y''_2Y''_3Y''_4)$. Pak platí:

$$\begin{aligned} \Delta X(\Delta X_1\Delta X_2\Delta X_3\Delta X_4) &= X'(X'_1X'_2X'_3X'_4) \oplus X''(X''_1X''_2X''_3X''_4) \\ \Delta Y(\Delta Y_1\Delta Y_2\Delta Y_3\Delta Y_4) &= Y'(Y'_1Y'_2Y'_3Y'_4) \oplus Y''(Y''_1Y''_2Y''_3Y''_4) \end{aligned} \tag{6.1}$$

U ideální šifry je pravděpodobnost všech $\Delta Y$ v závislosti na $\Delta X$ stejná, tedy $1/2^n$, kde $n$ je počet bitů. Útok cílí na ty kombinace $\Delta X, \Delta Y$, kde je pravděpodobnost výskytu co největší. [22]

### 6.1.1 Tvorba tabulky diferencí

Jako příklad byl zvolen sbox1. Pro každý vstup do sboxu a pro zvolenou vstupní diferenci najdeme výstupní diferenci. Následují rovnice pro diferenci $\Delta X = 0111$:

---

[1)] Shortly before this book was sent to the publishers, Don Coppersmith (who was a member of the DES design team at IBM in the early 70's) revealed that his team was aware of differential cryptanalysis back in 1974, and designed the S boxes and the permutation in order to optimally defeat it. They had to keep this information secret for 18 years for´national security reasons since it was such a potent form of cryptanalysis, but decided to break the silence after we rediscovered and published it

[2)] it analyzes the evolution of differences when two related plaintexts are encrypted under same key.

[3)] Differential cryptanalysis is the first published attack which is capable of breaking the full 16-round DES in less than $2^{55}$ complexity. The data analysis phase computes the key by analyzing about $2^{36}$ ciphertexts in $2^{37}$ time.

Tab. 6.1 Výstupní diference pro danou vstupní diferenci

| $X'_D$ | $Y'_D$ | $X'_B$ | $X''_B$ | $Y'_B$ | $Y''_B$ | $\Delta Y_B$ |
|---|---|---|---|---|---|---|
| 0 | 15 | 0000 | 0111 | 1111 | 1110 | 0001 |
| 1 | 1 | 0001 | 0110 | 0001 | 0010 | 0011 |
| 2 | 7 | 0010 | 0101 | 0111 | 0110 | 0001 |
| 3 | 0 | 0011 | 0100 | 0000 | 1001 | 1001 |
| 4 | 9 | 0100 | 0011 | 1001 | 0000 | 1001 |
| 5 | 6 | 0101 | 0010 | 0110 | 0111 | 0001 |
| 6 | 2 | 0110 | 0001 | 0010 | 0001 | 0011 |
| 7 | 14 | 0111 | 0000 | 1110 | 1111 | 0001 |
| 8 | 11 | 1000 | 1111 | 1011 | 1010 | 0001 |
| 9 | 8 | 1001 | 1110 | 1000 | 0100 | 1100 |
| 10 | 5 | 1010 | 1101 | 0101 | 1101 | 1000 |
| 11 | 3 | 1011 | 1100 | 0011 | 1100 | 1111 |
| 12 | 12 | 1100 | 1011 | 1100 | 0011 | 1111 |
| 13 | 13 | 1101 | 1010 | 1101 | 0101 | 1000 |
| 14 | 4 | 1110 | 1001 | 0100 | 1000 | 1100 |
| 15 | 10 | 1111 | 1000 | 1010 | 1011 | 0001 |

Z rovnic vyplývá, že této diferenci $\Delta X = 0111$ odpovídá výstupní diference $\Delta Y_B = 0001$ v 6 případech, pravděpodobnost této diference je tedy 6/16. Zbylých 10 případů je rovnoměrně rozděleno mezi $\Delta Y_D = 3, 8, 9, 12, 15$. Na rozdíl od lineární aproximace, kde je možno ověřením jedné vstupní masky a jedné výstupní masky získat hodnotu jedné buňky tabulky, výsledkem ověření jedné vstupní diference je celý řádek tabulky diferencí.

Po provedení výpočtu pro všechny vstupní diference se výsledky zpravidla interpretují v tabule diferencí. Tabulku diferencí pro 1.sbox je možno najít v příloze.

### 6.1.2 Vliv klíč na diferenciální charakteristiku

Nechť $K$ je klíč ovlivňující bity vstupu do sboxu $X'$, $X''$, kde $X'' \oplus X' = \Delta X$. Pak platí:

$$\begin{aligned} X'_K &= X' \oplus K \\ X''_K &= X'' \oplus K \\ X''_K \oplus K \oplus X'_K \oplus K &= \Delta X \\ X''_K \oplus X'_K &= \Delta X \\ \Delta X_K &= \Delta X \end{aligned} \tag{6.2}$$

Vstupní diference tedy není závislá na použitém klíči.

## 6.2 Diferenciální charakteristika více sboxů

Mějme jev $A$ pravdivý s pravděpodobností $Q(A)$[4] a k němu nezávislý jev $B$ s pravděpodobností $Q(B)$. Pravděpodobnost, že oba jevy platí zároveň, je $Q(A \cap B) = Q(A) \cdot Q(B)$. Pro současné působení $n$ jevů s pravděpodobností $Q_1, Q_2, ..., Q_n$ pak platí:

$$Q_n = \prod_{i=1}^{n} Q_i \tag{6.3}$$

Ze vztahu vyplývá, že pravděpodobnost průchodu více sboxy je součin pravděpodobností jednotlivých sboxů.

## 6.3 Varianta útoku se známým otevřeným textem

Teoreticky je možno provést diferenciální útok v režimu známého otevřeného textu. Problémem je v tomto případě získat dostatečné množství otevřených textů se stejným vstupním diferenciálem. Jsou-li otevřené texty náhodně generovány, je diferenciál dvou náhodně vybraných otevřených textů také náhodný a pravděpodobnost, že jde o požadovaný diferenciál, je $2^{-n}$, kde $n$ je počet bitů oteveného textu.

Při šifrování smysluplného textu kódovaného například osmibitovým ASCII kódem se počet možných diferencí snižuje. U 24bitové šifry použité v praktické části je počet možných vstupních diferencí $x^3$, kde $x$ je počet možných reálně použitých znaků. Obsahuje-li otevřený text například 30 různých znaků, je počet možných vstupních diferencí roven 27000, z čehož vyplývá nutnost menšího počtu známých otevřených textů k získání dostatečného počtu dvojic se stejnou diferencí, než u náhodně generovaného otevřeného textu.

## 6.4 Odvození bitů klíče

„Pro každý pár šifrovaných textů a jim odpovídajících otevřených textů použitých ke generování vstupní diference $\Delta P$ se provede částečné dešifrovaní pro všechny možné hodnoty cíleného subklíče.“[5][22] Pro každou hodnotu subklíče se vede záznam, kolik vypočítaných výstupních diferencí odpovídá očekávané výstupní diferenci. S rostoucí hodnotou pak roste pravděpodobnost správnosti klíče.

[4] Vzhledem k tomu, že v této práci je písmenem $P$ označován otevřený text, bude z důvodu přehlednosti označena pravděpodobnost zkratkou $Q$ namísto obvyklé $P$

[5] A partial decryption is executed for each pair of ciphertexts corresponding to the pairs of plaintexts used to generate the input difference $\Delta P$ for all possible target partial subkey values.

# II. PRAKTICKÁ ČÁST

Cílem praktické části této práce je provést vzorový útok lineární a diferenciální kryptoanalýzou. K tomuto účelu bylo nutné zvolit vhodnou šifru, dostatečně jednoduchou ke srozumitelné a praktické ukázce a zároveň dostatečně složitou k představení síly obou metod. Zvolená šifra je upravenou verzí šifry použité při soutěži picoCTF 2014.

## 7 Popis šifry

Jde o šestikolovou šifru využívající jednoduchou substitučně-permutační síť, kdy se každé kolo šifry skládá z fáze substituce, permutace a přičtení klíče. Výjimkou je poslední kolo, kde je vynechána permutace. Do šifry vstupuje otevřený text délky 24 bitů rozdělených do 6 různých sboxů se čtyřbitovým vstupem i výstupem. Permutace i pořadí sboxů v jednotlivých kolech zůstává stejné. První 4 bity kola tedy vstupují do sboxu1, další 4 bity do sboxu2 atd. Použité sboxy jsou shrnuty v tabulce níže:[1)]

Tab. 7.1 Definice sboxů použitých v šifře

| index | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| sbox1 | 15 | 1 | 7 | 0 | 9 | 6 | 2 | 14 | 11 | 8 | 5 | 3 | 12 | 13 | 4 | 10 |
| sbox2 | 3 | 7 | 8 | 9 | 11 | 0 | 15 | 13 | 4 | 1 | 10 | 2 | 14 | 6 | 12 | 5 |
| sbox3 | 4 | 12 | 9 | 8 | 5 | 13 | 11 | 7 | 6 | 3 | 10 | 14 | 15 | 1 | 2 | 0 |
| sbox4 | 2 | 4 | 10 | 5 | 7 | 13 | 1 | 15 | 0 | 11 | 3 | 12 | 14 | 9 | 8 | 6 |
| sbox5 | 3 | 8 | 0 | 2 | 13 | 14 | 5 | 11 | 9 | 1 | 7 | 12 | 4 | 6 | 10 | 15 |
| sbox6 | 14 | 12 | 7 | 0 | 11 | 4 | 13 | 15 | 10 | 3 | 8 | 9 | 2 | 6 | 1 | 5 |

Následuje pbox:

Tab. 7.2 Definice permutace

| vstupní bit | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| výstupní bit | 13 | 3 | 15 | 23 | 6 | 5 | 22 | 21 | 19 | 1 | 18 | 17 |
| vstupní bit | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 |
| výstupní bit | 20 | 10 | 7 | 8 | 12 | 2 | 16 | 9 | 14 | 0 | 11 | 4 |

Šifra využívá 56bitový klíč, z něhož je vygenerováno 6+1(inicializační vektor) klíčů kola o délce 24 bitů. Subklíče jsou generovány tak, aby ve dvou po sobě jdoucích kolech nemohl být použit stejný bit klíče. K vytvoření klíčů pro jednotlivá kola byl použit následující postup:

- Prvních 24 bitů pomocného klíče (v prvním kole je totožný s reálným klíčem) je označeno jako pracovní klíč

[1)] Vzhledem k tomu, že k šifrování a kryptoanalýze byl použit algoritmus psaný v programu Python, který indexuje od 0, má první znak textu index 0 a nikoli 1. Stejně tak poslední znak má index 15 a nikoli 16, případně 23 místo 24

- Je provedena permutace pracovního klíče pomocí permutační tabulky klíče
- Jako klíč kola je použit pracovní klíč
- Je vytvořen nový pomocný klíč jako 25. - 56. bit předchozího pomocného klíče následovaný pracovním klíčem

Tab. 7.3 Permutace klíče pro tvoření klíčů kola

| vstupní bit | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| výstupní bit | 15 | 16 | 17 | 12 | 13 | 14 | 3 | 4 | 5 | 21 | 22 | 23 |
| vstupní bit | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 |
| výstupní bit | 9 | 10 | 11 | 18 | 19 | 20 | 0 | 1 | 2 | 6 | 7 | 8 |

Tabulka níže shrnuje vztah jednotlivých bitů klíčů kola a celkového klíče:

Tab. 7.4 Přehled použitých klíčů kola

| index | $K_{(0,i)}$ | $K_{(1,i)}$ | $K_{(2,i)}$ | $K_{(3,i)}$ | $K_{(4,i)}$ | $K_{(5,i)}$ | $K_{(6,i)}$ |
|---|---|---|---|---|---|---|---|
| 0 | 18 | 42 | 13 | 37 | 8 | 32 | 18 |
| 1 | 19 | 43 | 14 | 38 | 21 | 45 | 4 |
| 2 | 20 | 44 | 3 | 27 | 51 | 16 | 40 |
| 3 | 6 | 30 | 54 | 10 | 34 | 20 | 44 |
| 4 | 7 | 31 | 55 | 11 | 35 | 6 | 30 |
| 5 | 8 | 32 | 18 | 42 | 13 | 37 | 8 |
| 6 | 21 | 45 | 4 | 28 | 52 | 17 | 41 |
| 7 | 22 | 46 | 5 | 29 | 53 | 9 | 33 |
| 8 | 23 | 47 | 0 | 24 | 48 | 1 | 25 |
| 9 | 12 | 36 | 7 | 31 | 55 | 11 | 35 |
| 10 | 13 | 37 | 8 | 32 | 18 | 42 | 13 |
| 11 | 14 | 38 | 21 | 45 | 4 | 28 | 52 |
| 12 | 3 | 27 | 51 | 16 | 40 | 23 | 47 |
| 13 | 4 | 28 | 52 | 17 | 41 | 12 | 36 |
| 14 | 5 | 29 | 53 | 9 | 33 | 19 | 43 |
| 15 | 0 | 24 | 48 | 1 | 25 | 49 | 2 |
| 16 | 1 | 25 | 49 | 2 | 26 | 50 | 15 |
| 17 | 2 | 26 | 50 | 15 | 39 | 22 | 46 |
| 18 | 15 | 39 | 22 | 46 | 5 | 29 | 53 |
| 19 | 16 | 40 | 23 | 47 | 0 | 24 | 48 |
| 20 | 17 | 41 | 12 | 36 | 7 | 31 | 55 |
| 21 | 9 | 33 | 19 | 43 | 14 | 38 | 21 |
| 22 | 10 | 34 | 20 | 44 | 3 | 27 | 51 |
| 23 | 11 | 35 | 6 | 30 | 54 | 10 | 34 |

K zašifrování byl použit následující pseudonáhodně vygenerovaný klíč:
01101001001100010101000100110101001011110001010001001101.

## 8 Příprava útoku

Lineární kryptoanalýza byla provedena v režimu známý otevřený text, prvním krokem tedy bylo vygenerování dostatečného množství párů otevřený text - šifrovaný text k úspěšné analýze. Z existujících $2^{24}$ možných vstupů bylo pseudonáhodně vygenerováno 100000 a tyto byly zašifrovány.

Diferenciální kryptoanalýza proběhla v režimu zvolený otevřený text. Bylo použito stejných 100000 výchozích otevřených textů, pro každou diferenci byl ke každému výchozímu textu vypočítán druhý otevřený text a ten následně zašifrován.

Ačkoli byly obě kryptoanalýzy provedeny na sobě nezávisle, v praxi byl pro obě použit stejný algoritmus, který byl pro potřeby jednotlivých kryptoanalýz jen mírně upraven. Následující část je věnována popisu obecného postupu se zdůrazněním podobností a rozdílů obou kryptoanalýz. Není-li uvedeno jinak, je v této části termínem „aproximace“ myšlena jak zvolená lineární aproximace, tak vybraná diference. Stejně tak je termínem „bias“ myšlen jak lineární bias, tak diferenciální pravděpodobnost.

### 8.1 Výpočet tabulek aproximací

Ačkoli se pro výpočet tabulky lineární aproximace sboxu používá jiný vzorec, než pro tabulku diferencí, výsledná tabulka je podobná s tím rozdílem, že u lineární aproximace dosahují jednotlivé buňky hodnot v intervalu $< 0, n/2 >$, zatímco u tabulky diferencí $< 0, n >$.

Pro jednotlivé sboxy byly vypočítány tabulky lineární aproximace a tabulky diferencí. Na rozdíl od běžně používaných tabulek lineární aproximace byly tyto pro účely útoku zjednodušeny tak, že je v nich uvedena pouze absolutní hodnota. Na provedení útoku nemá tato úprava vliv, jediným rozdílem oproti běžnému použití je nemožnost určit, zda jde o bias kladný či záporný. Vzhledem k tomu, že k vyhodnocení útoku je použita pouze absolutní hodnota odchylky, výsledek bude stejný. Díky tomu je možno k hledání aproximací i diferencí použít totožný alogritmus.

Tabulky lineárních aproximací i tabulky diferencí pro všechny použité sboxy je možno najít v příloze.

### 8.2 Nalezení cest

Cestami jsou myšleny rovnice lineární aproximace a rovnice diferencí. Ačkoli vyjadřuje lineární bias jinou hodnotu, než diferenciální pravděpodobnost, je možno s nimi pra-

covat totožným způsobem, s následujícími rozdíly:

- Základní hodnota lineárního biasu je 0.5, zatímco základní pravděpodobnost diference je 1
- Hodnota jmenovatele u lineární aproximace je $n/2$, u diference je $n$

Jmenovatel se rovná maximální možné hodnotě v tabulce. Stejná hodnota je uvedena v prvním řádku a sloupci tabulky. Čitatelem je pak hodnota z odpovídajícího řádku a sloupce tabulky aproximace.

Obecně se při výpočtu biasu vynásobí základní hodnota poměrem hodnot čitatele a jmenovatele pro každý zapojený sbox.

Logika hledání optimálních cest byla rozdělena na 2 části - cesta 1. kolem a cesta ostatními koly. Pro všechna kola byla z důvodu zrychlení výpočtu a odstranění slabých cest experimentálně určena minimální úroveň biasu, který musí výstup dosáhnout, aby „postoupil“ do dalšího kola.

Tab. 8.1 Minimální bias pro lineární aproximaci

| kolo | minimální bias |
|---|---|
| 1 | 0,150 |
| 2 | 0,060 |
| 3 | 0,030 |
| 4 | 0,012 |
| 5 | 0,006 |

Diferenciální pravděpodobnost dosahuje obecně nižších hodnot, než lineární bias, proto bylo nutno upravit tabulku minimálních pravděpodobností pro jednotlivá kola.

Tab. 8.2 Minimální pravděpodobnost diference v kole

| kolo | minimální pravděpodobnost |
|---|---|
| 1 | 0,15000 |
| 2 | 0,00240 |
| 3 | 0,00120 |
| 4 | 0,00048 |
| 5 | 0,00024 |

### 8.2.1 Rozšíření rovnic v prvním kole aproximace

Ze znalosti rovnice aproximace pro požadovaný počet kol je možno odvodit další rovnice se stejnými bity výstupu. Tuto rovnici je možno vytvořit při zachování stejného výstupu z prvního kola aproximace pro každý vstup, kde je hodnota nebo jejich součin (v případě

více zapojených sboxů) větší než 0. Nový bias se vypočítá jako podíl původního biasu a původní hodnoty z prvního kola vynásobený novou hodnotou.

Tohoto je možno využít v případě mnohonásobné lineární i diferenciální kryptoanalýzy, kdy nahradíme malé množství kvalitních rovnic větším množstvím rovnic s menším biasem s cílem dosáhnout spolehlivějšího výsledku.

### 8.2.2 Rozšíření rovnic v posledním kole aproximace

Stejného efektu lze využít i v posledním kole aproximace, kdy zůstanou bity otevřeného textu $P$ zachovány a bity výstupu $C$ jsou nahrazeny.

Na rozdíl od rozšíření v prvním kole změna v posledním kole může změnit zapojené sboxy, čímž je možno útok rozšířit na více bitů klíče.

## 8.3 Aproximace 1.kola

Pro všechny možné výstupy každého sboxu byla nalezena 1 maximální hodnota biasu. V případě, že tuto hodnotu sdílelo více vstupů, byl použit pouze ten první - v této fázi hledání aproximace je toto dostačující a případě nutnosti je možno aproximace v prvním kole rozšířit dle pravidel výše.

Pro každý z $2^{24}$ možných výstupů 1. kola aproximace byl spočítán bias 1. kola. Pokud byl tento bias větší, než minimální bias pro 1. kolo, a zároveň tento výstup zapojil méně, než 4 sboxy, byl výstup permutován a výsledek spolu s biasem byl uložen jako vstup do dalšího kola.

## 8.4 Aproximace $n$-tého kola

Pro každý vstup z předchozího kola bylo vyhodnoceno množství zapojených sboxů. Byla-li tato hodnota menší než 4, byly otestovány všechny možné výstupy. Byl-li bias větší, než minimální požadovaný, byla tato hodnota porovnána s předchozími hodnotami tohoto kola. Mohly nastat následující možnosti:

- Výstup již byl v tabulce, ale s menším biasem → byl nahrazen novou cestou a biasem
- Výstup již byl v tabulce s větším nebo stejným biasem → nová cesta byla zahozena
- Výstup ještě nebyl v tabulce → cesta byla přidána do tabulky

Po prozkoumání všech vstupů byla provedena permutace výstupu, čímž byla získána vstupní tabulka do dalšího kola aproximace.

### 8.5 Výběr vhodných aproximací

Výstupem předchozích kroků byl seznam aproximací s dostatečným biasem. Tyto aproximace byly rozděleny do skupin dle počtu použitých sboxů na výstupu. Protože v dalším kroku probíhálo testování všech možných hodnot klíče, a protože těchto možných hodnot bylo $2^{4n}$, kde $n$ je počet zapojených sboxů, byly jako nejvhodnější aproximace určeny ty, do kterých bylo zapojeno co nejméně sboxů.

Ačkoli při zapojení 2 sboxů je možno odhalit 8 bitů klíče namísto 4, je za stejnou dobu možno otestovat 16 aproximací pro 1 sbox, tedy 2-3 pro každý použitý sbox v daném kole. Proto byla většina aproximací použitých k reálnému útoku zacílena jen na 1 sbox, útok na 2 sboxy zároveň byl proveden pouze v nejasných případech a aproximace s více než dvěma zapojenými sboxy v posledním kole nebyly použity.

## 9 Lineární kryptoanalýza

Tato část je věnována ukázce praktického provedení lineární kryptoanalýzy. Cílem je získat všech 56 bitů klíče použitého k zašifrování otevřených textů.

### 9.1 Odvození rovnice lineární aproximace

Níže je uveden příklad postupu hledání rovnice lineární aproximace $n-1$ kol šifry.[1)] Pro první kolo je možno odvodit následující rovnice:

$$\begin{aligned} Y_{(1,14)} &= X_{(1,13)} \oplus X_{(1,14)} \oplus X_{(1,15)} \\ X_{(1,13)} \oplus X_{(1,14)} \oplus X_{(1,15)} &= (P_{13} \oplus K_{(0,13)}) \oplus (P_{14} \oplus K_{(0,14)}) \oplus (P_{15} \oplus K_{(0,15)}) \\ Y_{(1,14)} &= P_{13} \oplus P_{14} \oplus P_{15} \oplus (K_{(0,13)} \oplus K_{(0,14)} \oplus K_{(0,15)}) \end{aligned} \tag{9.1}$$

V tabulce lineární aproximace pro sbox 4 je možno najít hodnotu 6, bias se tedy spočítá dosazením do rovnice:

$$\epsilon_1 = \frac{1}{2} \cdot \frac{2 \cdot 6}{16} = \frac{3}{8} \tag{9.2}$$

Druhé kolo aproximace je možno vyjádřit takto:

$$\begin{aligned} Y_{(2,7)} &= X_{(2,7)} \\ X_{(2,7)} &= Y_{(1,14)} \oplus K_{(1,7)} \\ Y_{(2,7)} &= P_{13} \oplus P_{14} \oplus P_{15} \oplus (K_{(0,13)} \oplus K_{(0,14)} \oplus K_{(0,15)} \oplus K_{(1,7)}) \end{aligned} \tag{9.3}$$

[1)] Význam jednotlivých zápisů viz Seznam použitých symbolů

První z trojice rovnic značí substituci v rámci sboxů. Druhá permutaci (od druhého kola) a přičtení klíče, poslední rovnice vznikne dosazením druhé rovnice z tohoto kola a třetí rovnice z předchozího kola do první rovnice.

V tomto kole je použita lineární aproximace 2.sboxu, hodnota z tabulky je 2:

$$\epsilon_2 = \frac{1}{2} \cdot \frac{2 \cdot 6}{16} \cdot \frac{2 \cdot 2}{16} = \frac{3}{32} \tag{9.4}$$

Následují třetí kolo:

$$\begin{aligned} Y_{(3,22)} &= X_{(3,22)} \\ X_{(3,22)} &= Y_{(2,7)} \oplus K_{(2,22)} \\ Y_{(3,22)} &= P_{13} \oplus P_{14} \oplus P_{15} \oplus (K_{(0,13)} \oplus K_{(0,14)} \oplus K_{(0,15)} \oplus K_{(1,7)} \oplus K_{(2,22)}) \end{aligned} \tag{9.5}$$

Z tabulky pro 6.sbox je získána hodnota 4. Vzhledem k tomu, že sboxy použité v předchozích kolech aproximace a jejich spočítány bias zůstává stejný, je možno bias vyjádřit jako ten z předchozího kola upravený pouze o sboxy použité v tomto kole:

$$\epsilon_3 = \epsilon_2 \cdot \frac{4 \cdot 2}{16} = \frac{3}{64} \tag{9.6}$$

Ve 4. kole byly zapojeny 2 bity na výstupu z sboxu, postup to ale neovlivní:

$$\begin{aligned} Y_{(4,8)} \oplus Y_{(4,11)} &= X_{(4,11)} \\ X_{(4,11)} &= Y_{(3,22)} \oplus K_{(3,11)} \\ Y_{(4,8)} \oplus Y_{(4,11)} &= P_{13} \oplus P_{14} \oplus P_{15} \oplus K \\ K &= K_{(0,13)} \oplus K_{(0,14)} \oplus K_{(0,15)} \oplus K_{(1,7)} \oplus K_{(2,22)} \oplus K_{(3,11)} \end{aligned} \tag{9.7}$$

Spočteme bias s hodnotou 4 z tabulky 3.sboxu:

$$\epsilon_4 = \epsilon_3 \cdot \frac{4 \cdot 2}{16} = \frac{3}{128} \tag{9.8}$$

Provedeme poslední kolo lineární aproximace:

$$\begin{aligned} Y_{(5,17)} \oplus Y_{(5,18)} &= X_{(5,17)} \oplus X_{(5,19)} \\ X_{(5,17)} &= Y_{(4,11)} \oplus K_{(4,17)} \\ X_{(5,19)} &= Y_{(4,8)} \oplus K_{(4,19)} \\ Y_{(5,17)} \oplus Y_{(5,18)} &= P_{13} \oplus P_{14} \oplus P_{15} \oplus K' \end{aligned} \tag{9.9}$$

Kde $K'$ je rovno:

$$K' = K_{(0,13)} \oplus K_{(0,14)} \oplus K_{(0,15)} \oplus K_{(1,7)} \oplus K_{(2,22)} \oplus K_{(3,11)} \oplus K_{(4,17)} \oplus K_{(4,19)} \tag{9.10}$$

Nyní byl zapojen 5. sbox, opět z hodnotou 4.

$$\epsilon_5 = \epsilon_4 \cdot \frac{4 \cdot 2}{16} = \frac{3}{256} \tag{9.11}$$

V posledním kroku musí být vyřešena poslední permutace a přičtení klíče:

$$\begin{aligned} X_{(6,2)} &= Y_{(5,17)} \oplus K_{(5,2)} \\ X_{(6,16)} &= Y_{(5,18)} \oplus K_{(5,16)} \\ P_{13} \oplus P_{14} \oplus P_{15} \oplus C_2 \oplus C_{16} &= K' \end{aligned} \tag{9.12}$$

Kde $K'$ značí binární součet všech relevantních bitů klíče.

$$K' = K_{(0,13)} \oplus K_{(0,14)} \oplus K_{(0,15)} \oplus K_{(1,7)} \oplus K_{(2,22)} \oplus K_{(3,11)} \oplus K_{(4,17)} \oplus K_{(4,19)} \oplus K_{(5,2)} \oplus K_{(5,16)} \tag{9.13}$$

Máme rovnici lineární aproximace, která závisí pouze na bitech vstupního textu, bitech posledního kola aproximace, a proměnné $K'$. Ta může nabývat pouze hodnot 0 nebo 1. Dále víme, že tato rovnice je pravdivá s biasem $3/256 \approx 0.1172$.

Vzhledem k tomu, že pro úspěch lineární aproximace je nutné najít rovnici, která má velikost biasu co největší, ale není důležité, zda je kladný nebo záporný, a vzhledem k tomu, že hodnota $K$ výsledek nezmění nebo změní pro všechny testované hodnoty, můžeme všechny bity klíče z rovnice vypustit a rovnici zjednodušit:

$$P_{13} \oplus P_{14} \oplus P_{15} \oplus C_2 \oplus C_{16} = 0 \tag{9.14}$$

### 9.1.1 Alternativní rovnice

Stejným způsobem odvodíme následující rovnici:

$$P_{13} \oplus P_{14} \oplus P_{15} \oplus C_2 \oplus C_{16} = K \tag{9.15}$$

Kde $K$ je:

$$K = K_{(0,13)} \oplus K_{(0,14)} \oplus K_{(0,15)} \oplus K_{(1,7)} \oplus K_{(2,22)} \oplus K_{(3,11)} \oplus K_{(4,18)} \oplus K_{(5,2)} \oplus K_{(5,16)} \quad (9.16)$$

Spočteme bias této rovnice:

$$\epsilon_5 = \frac{1}{2} \cdot \frac{2 \cdot 6}{16} \cdot \frac{2 \cdot 2}{16} \cdot \frac{2 \cdot 4}{16} \cdot \frac{2 \cdot 2}{16} \cdot \frac{2 \cdot 2}{16} = \frac{3}{1024} \quad (9.17)$$

Po zjednodušení rovnice vypuštením $K$ je možno vidět, že jde o stejnou aproximaci jako v předchozím příkladu, spočtený bias je ale čtvrtinový. Vzhledem k tomu, že při hledání aproximace nebyly testovány všechny možné rovnice, je možné, že pro danou kombinaci bitů vstupu a výstupu existuje rovnice s biasem ještě větším.

Po zjednodušení rovnice vypuštěním bitů klíče je tedy biasem myšlen spíše „minimální bias“ ve smyslu, že může existovat cesta s vyšším biasem, která doposud nebyla objevena. Pro úspěšné provedení útoku na šifru je postačující dostatečný minimální bias, není nutné hledat maximální bias pro danou kombinaci vstupních a výstupních bitů. Proto není v ukázkovém útoku při vyhodnocení aproximací brán na uvedený bias ohled.

Na předchozí rovnici je možno aplikovat pravidla o rozšíření rovnic v prvním i posledním kole. V prvním kole je možno nahradit výše odvozenou rovnici například rovnicí $P_{15} \oplus C_2 \oplus C_{16} = 0$ s třetinovým minimálním biasem tedy 1/256. Stejným způsobem a se stejným biasem je možno v tomto případě vytvořit dalších 6 rovnic.

Dle rozšíření v posledním kole je z rovnice možno vytvořit například rovnici $P_{13} \oplus P_{14} \oplus P_{15} \oplus C_{16} = 0$ se stejným biasem 3/256 a dalších 8 rovnic s biasem polovičním.

Obě pravidla je možno použít současně. Výsledkem může být například rovnice $P_{15} \oplus C_{16} = 0$ se stejným biasem 1/256.

## 9.2 Vzorový útok

Pro uvedenou šifru existuje lineární aproximace $P[12, 13, 15] \oplus C[1]$ s biasem 3/256. Vzhledem k tomu, že je zapojen bit 1 z výstupu, znamená to, že je možno provést útok na 1.sbox a pokusit se tak odhalit první 4 bity klíče kola. Je testováno 16 možných klíčů. K tomuto účelu bylo použito všech 100000 vygenerovaných dvojic otevřený text - šifrovaný text.

Pro každou dvojici textů a každý možný klíč bylo provedeno následující:

- Relevantní bity šifrovaného textu byly odšifrovány testovaným klíčem
- Byla ověřena platnost rovnice $P[12, 13, 15] \oplus C[1] = 0$
- Platila-li rovnice, bylo provedeno $h_i = h_i + 1$ kde $i$ je index ověřovaného klíče

Poté byly spočítány $H_i$ dle vzorce výše a výsledek byl uveden do tabulky:

Tab. 9.1 Vyhodnocení útoku lineární kryptoanalýzy

| Klíč | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|---|---|---|---|---|---|---|---|---|
| $h_i$ | 49662 | 50083 | 50074 | 49500 | 49702 | 49774 | 50204 | 49461 |
| $H_i$ | 338 | 83 | 74 | 500 | 298 | 226 | 204 | 539 |
| Pořadí | 5 | 12 | 13 | 3 | 6 | 8 | 10 | 2 |
| Klíč | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
| $h_i$ | 49927 | 50597 | 50225 | 50110 | 49967 | 50288 | 50355 | 50071 |
| $H_i$ | 73 | 597 | 225 | 110 | 33 | 288 | 355 | 71 |
| Pořadí | 14 | 1 | 9 | 11 | 16 | 7 | 4 | 15 |

Z tabulky je patrno, že nejvíce se od očekávané hodnoty 50000 odchýlily možný klíč 9 (50597 platných rovnic) a možný klíč 7 (49461 platných rovnic). Toto jsou nejpravděpodobnější kandidáti na první 4 bity klíče posledního kola.

### 9.2.1 Rozšířené vyhodnocení

Vzhledem k tomu, že tato práce demonstruje mnohonásobnou lineární kryptoanalýzu, kdy je klíč každého sboxu odvozen z více rovnic, bylo nutné stanovit metriku pro porovnání jednotlivých lineárních aproximací. Při tvorbě této metriky bylo vycházeno z předpokladu, že čísla $H_i$ nejsou mezi jednotlivými aproximacemi vzájemně porovnatelná, proto byla každá hodnota aproximace vyjádřena jako násobek průměru dané aproximace.

Druhou myšlenkou byla snaha ocenit v rámci jednotlivých aproximací hodnoty, které extrémně převyšují průměr, u kterých byl předpoklad, že tento rozdíl byl způsobený volbou správného klíče. Proto byl násobek průměru mocněn. Rozšířené hodnoty byly určeny takto:

$$G_i = (H_i / \sum_{j=0}^{n-1} H_j)^2 \tag{9.18}$$

Kde $n$ je celkový počet uvažovaných klíčů (tedy 16). Hodnoty byly v rámci aproximací cílící na stejné sboxy sečteny.

## 9.3 1. kolo útoku

V předchozí fázi bylo nalezeno 5 aproximací, které cílí pouze na 1.sbox. Po provedení útoku pro těchto 5 rovnic dostaneme výsledky shrnuté v tabulce níže.

Vzhledem k tomu, že je vždy testováno nejméně 16 možných klíčů, měla by celá tabulka vždy více než 16 sloupců. Proto je tabulek vždy uvedeno 5 nejpravděpodob-

nějších hodnot. Je-li sloupec tabulky nadepsán $X$. a je-li v daném řádku hodnota $i : G_i$, znamená to, že $X$-tý nejpravděpodobnější klíč daného sboxu je $i$, s hodnotou rovnou $G_i$. Nejpravděpodobnější klíč v prvním řádku následující tabulky je tedy 4, druhý nejpravděpodobnější 10 apod.

Jsou-li na místě $i$ uvedeny 2 hodnoty oddělené čárkou, jde zároveň o dva klíče odpovídajících sboxů.

Tab. 9.2 Útok na 1.sbox - jednotlivé aproximace

| rovnice | min. bias | 1. | 2. | 3. | 4. | 5. |
|---|---|---|---|---|---|---|
| P[12, 13, 15] ⊕ C[1] | 0,0117 | 4 : 7,29 | 10 : 3,24 | 13 : 3,06 | 15 : 2,16 | 7 : 2,04 |
| P[22]⊕ C[2] | 0,0078 | 11 : 7,67 | 4 : 6,86 | 12 : 4,33 | 0 : 3,20 | 1 : 2,40 |
| P[4, 5, 7, 22] ⊕ C[0] | 0,0088 | 4 : 2,92 | 14 : 2,92 | 2 : 1,06 | 8 : 1,06 | 7 : 1,04 |
| P[4, 5, 7, 22] ⊕ C[2] | 0,0088 | 1 : 6,86 | 11 : 5,02 | 8 : 3,06 | 7 : 2,10 | 13 : 2,10 |
| P[9, 10] ⊕ C[1] | 0,0078 | 4 : 3,65 | 10 : 3,57 | 13 : 3,10 | 15 : 2,50 | 8 : 2,31 |

Rovnice nebudou vyhodnocovány zvlášť, výsledek bude agregován tak, aby pro každou kombinaci sboxů byla pouze jeden řádek. Toho je dosaženo sečtením hodnot pro jednotlivé klíče. Spolehlivost ($S$) je poměr mezi dvěma největšími hodnotami daného sboxu. Čím větší spolehlivost, tím větší šance, že klíč s největší hodnotou je skutečně správný. Za dostatečnou spolehlivost je v rámci této práce považována hodnota větší než 1,8.

Tab. 9.3 Agregace útoků na 1. sbox

| sbox | rovnic | S | 1. | 2. | 3. | 4. | 5. |
|---|---|---|---|---|---|---|---|
| 100000 | 5 | 1,47 | 4 : 21,65 | 11 : 14,71 | 1 : 12,18 | 10 : 9,54 | 13 : 9,52 |

Z tabulky vyplývá, že mezi pravděpodobné subklíče pro 1.sbox patří klíč 4 a dále 11 a 1. Hodnota spolehlivosti 1,47 není dostatečná k určení klíče, ten by měl být ověřen dalšími aproximacemi.

Stejným způsobem provedeme lineární aproximaci zbylých 20 nalezených rovnic pro 1 sbox. Jednotlivé aproximace shrnuje příloha, zde jsou uvedeny agregované výsledky:

Tab. 9.4 První kolo útoku (všechny sboxy)

| sbox | rovnic | S | 1. | 2. | 3. | 4. | 5. |
|---|---|---|---|---|---|---|---|
| 100000 | 5 | 1,47 | 4 : 21,65 | 11 : 14,71 | 1 : 12,18 | 10 : 9,54 | 13 : 9,52 |
| 010000 | 5 | 1,27 | 0 : 14,05 | 11 : 11,07 | 12 : 10,39 | 5 : 10,31 | 14 : 8,53 |
| 001000 | 4 | 1,06 | 15 : 11,66 | 1 : 11,03 | 8 : 9,03 | 13 : 8,84 | 11 : 8,81 |
| 000100 | 3 | 1,12 | 13 : 8,90 | 7 : 7,95 | 5 : 6,29 | 10 : 6,27 | 4 : 5,59 |
| 000010 | 5 | 1,76 | 10 : 17,37 | 15 : 9,87 | 6 : 8,02 | 1 : 7,40 | 7 : 7,03 |
| 000001 | 3 | 1,24 | 7 : 6,62 | 9 : 5,35 | 11 : 4,33 | 0 : 4,30 | 5 : 4,30 |

Jak je vidět, u žádného sboxu není dostatečně spolehlivý výsledek k učinění závěru. Nejslibnější výsledek je pro 1. a 5. sbox, proto nyní provedeme útok na oba sboxy zároveň. Připraveny máme 4 rovnice aproximace:

- $P[17, 18] \oplus C[1, 18] = 0$
- $P[16, 18] \oplus C[1, 17] = 0$
- $P[13, 14, 15] \oplus C[2, 16] = 0$
- $P[12, 13, 15] \oplus C[1, 17, 19] = 0$

Následuje agregovaná tabulka pro tyto rovnice:

Tab. 9.5 Nalezení klíče 1. a 5. sboxu

| sbox | rovnic | S | 1. | 2. | 3. | 4. | 5. |
|---|---|---|---|---|---|---|---|
| 100010 | 4 | 2,18 | 4,10 : 132,8 | 4,7 : 60,9 | 4,6 : 53,3 | 1,8 : 43,5 | 4,14 : 42,5 |

Spolehlivost této aproximace je 2,18 můžeme tedy nejpravděpodobnější výsledek považovat za správný klíč. Usuzujeme tedy, že do 1.sboxu vstupuje klíč 4 a do 5. klíč 10 - stejný výsledek jako při aproximaci každého sboxu zvlášť.

Využijeme znalosti 1.sboxu a pokusíme se najít aproximaci pro 1. a 3. sbox zároveň. Zde můžeme využít znalosti klíče 1.sboxu a vést útok pouze na 16 možných klíčů 3.sboxu.

Tab. 9.6 Útok na 3. sbox se znalostí klíče 1. sboxu

| sbox | rovnic | S | 1. | 2. | 3. | 4. | 5. |
|---|---|---|---|---|---|---|---|
| 101000 | 2 | 2,68 | 1 : 52,38 | 11 : 19,58 | 4 : 9,69 | 6 : 8,85 | 12 : 8,78 |

Ze spolehlivosti 2,68 usuzujeme, že klíčem 3.sboxu je 1, což je až 3. nejpravděpodobnější hodnota z jednosboxového hodnocení.

Nyní se zaměříme na 2. a 6. sbox:

Tab. 9.7 Odhalení klíče 2. a 6.sboxu

| sbox | rovnic | S | 1. | 2. | 3. | 4. | 5. |
|---|---|---|---|---|---|---|---|
| 010001 | 3 | 1,56 | 0,9 : 31,21 | 6,9 : 19,98 | 0,4 : 15,94 | 7,9 : 15,68 | 6,1 : 15,43 |

Provedená aproximace nevede k výsledku s dostatečnou spolehlivostí. V tomto případě je možno pokusit se použít jinou kombinaci sboxů nebo si pomoci výsledky z aproximace jednotlivých sboxů, zde bude demonstrována druhá možnost.

Výsledky pro jednotlivé sboxy a pro jejich kombinaci nejsou momentálně vzájemně porovnatelné. Jako referenční hodnotu každého sboxu použijeme poměr hodnoty aproximace daného klíče k maximální hodnotě dané aproximace.

$$G_i' = \frac{G_i}{G_{max}} \tag{9.19}$$

Tím dostaneme vyjádření jednotlivých hodnot v procentech maxima. Vynásobením získaných hodnot pro 2., 6. a oba sboxy získáme následující hodnoty: [2)]

Tab. 9.8 Klíč 2. a 6. sboxu - kombinace útoku na dvojici sboxů a jednotlivé sboxy

| sbox | rovnic | S | 1. | 2. | 3. | 4. | 5. |
|---|---|---|---|---|---|---|---|
| 010001 | 3 | 2,29 | 0,9 : 8,09 | 0,7 : 3,53 | 5,9 : 2,29 | 7,9 : 2,24 | 0,13 : 2,20 |

Ze spolehlivosti 2,29 je možno odvodit klíč pro oba sboxy, tedy 0 pro 2.sbox a 9 pro 6.sbox.

Posledním neodhaleným sboxem je 4. sbox. K odhalení využijeme kombinace 1 rovnice pro 4. a 5. sbox (kde známe klíč 5. sboxu) a 2 rovnic pro 4. a 6. sbox (kde známe klíč 6. sboxu). Efektivně jde tedy o 3 rovnice o 1 sboxu, které můžeme přičíst ke třem již provedeným rovnicím:

Tab. 9.9 Odhalení klíče 4. sboxu

| sbox | rovnic | S | 1. | 2. | 3. | 4. | 5. |
|---|---|---|---|---|---|---|---|
| 000100 | 6 | 2,12 | 7 : 29,83 | 9 : 14,09 | 11 : 10,83 | 5 : 10,66 | 13 : 9,91 |

S dostatečnou mírou spolehlivosti je klíčem 4. sboxu 7.

Tímto je první kolo útoku hotovo. Výsledný klíč kola je $4, 0, 1, 7, 10, 9$, tedy 010000000001011110101001.

## 9.4 2. kolo útoku

Na počátku druhého kola útoku je nutno upravit zašifrovaný text - provede se odstranění právě odhaleného klíče, odstranění jednoho kola substituce a odstranění jednoho kola permutace.[3)] Takto upravený šifrový text bude vstupovat do rovnic v tomto kole.

Pro daný počet kol bylo vygenerováno 21 rovnic lineárních aproximací cílící na 1 sbox. Agregace výsledků proběhla stejně jako v předchozím kole:

[2)] z důvodu přehlednosti jsou hodnoty vynásobeny deseti

[3)] Vzhledem k tomu, že při dešifrování proběhne první přičtení klíče a až po té permutace, tedy v opačném pořadí, bude výsledkem těchto rovnic permutovaný klíč.

Tab. 9.10 Útok na jednotlivé sboxy (2.kolo)

| sbox | rovnic | S | 1. | 2. | 3. | 4. | 5. |
|---|---|---|---|---|---|---|---|
| 100000 | 5 | 3,80 | 3 : 40,80 | 6 : 10,74 | 7 : 9,98 | 10 : 8,96 | 2 : 8,93 |
| 010000 | 5 | 1,96 | 15 : 26,87 | 11 : 13,74 | 6 : 11,39 | 7 : 10,16 | 10 : 8,27 |
| 001000 | 3 | 2,03 | 6 : 19,88 | 5 : 9,78 | 7 : 6,44 | 2 : 5,50 | 11 : 4,98 |
| 000100 | 3 | 1,19 | 4 : 8,67 | 9 : 7,30 | 6 : 6,20 | 15 : 6,15 | 13 : 6,13 |
| 000010 | 3 | 3,07 | 9 : 22,39 | 14 : 7,30 | 8 : 6,20 | 5 : 6,00 | 15 : 4,79 |
| 000001 | 2 | 2,35 | 8 : 12,55 | 6 : 5,35 | 0 : 4,88 | 11 : 4,20 | 5 : 1,86 |

Z tabulky je patrná větší spolehlivost než v prvním kole útoku. Toto je dáno v průměru zhruba dvojnásobným biasem oproti předchozímu kolu. Je možno spolehlivě určit klíč pro 1., 2., 3., 5., a 6. sbox $(3, 15, 6, 9, 8)$.

K odhalení klíče 4. sboxu použijeme útok na 4. a 6. sbox se znalostí klíče 6.sboxu:

Tab. 9.11 Klíč 4. sboxu v závislosti na klíči 6.sboxu

| sbox | rovnic | S | 1. | 2. | 3. | 4. | 5. |
|---|---|---|---|---|---|---|---|
| 000101 | 2 | 2,13 | 9 : 49,83 | 6 : 23,35 | 8 : 22,42 | 0 : 13,44 | 7 : 11,62 |

S dostatečnou mírou spolehlivosti můžeme určit klíč 4.sboxu jako 9.

Permutovaným klíčem kola je tedy $3, 15, 6, 9, 9, 8$, neboli:

001111110110100110011000.

Po provedení permutace dostaneme klíč kola:

010001101100101100101111.

### 9.4.1 Vyhodnocení stavu po 2. kole

S odhaleným klíčem 2 kol je známých 48 bitů. Na základě rozdělení klíčů kola uvedených v tabulce je možno získat následující klíč:

$$K = ?11?1?0?001100?10101000100?10101001011?000101000100 11?1 \tag{9.20}$$

Kde ? je prozatím neznámý bit klíče. Z toho odvodíme klíč pro 4. kolo:

$0001, 0011, 0101, 0000, ????, ????$.

Jde o opravdový klíč kola, k získání testovaného klíče kola je nutné odstranit permutaci: $010?, 10??, ?0??, ?010, 00?1, 0010$.

V tomto případě by bylo možno upravit aproximace tak, aby byly provedeny pouze pro neznámé bity klíče. V rámci demonstrace použijeme útok na celé kolo, čímž si ověříme správnost již odhalených bitů klíče.

### 9.5 3. kolo aproximace

Z upraveného šifrovaného textu odstraníme další kolo klíče, substituce a permutace. Poté provedeme útok na 19 rovnic cílících na 1 sbox:

Tab. 9.12 Poslední kolo lineární kryptoanalýzy (všechny sboxy)

| sbox | rovnic | S | 1. | 2. | 3. | 4. | 5. |
|---|---|---|---|---|---|---|---|
| 100000 | 4 | 2,34 | 4 : 22,05 | 1 : 9,42 | 8 : 7,20 | 12 : 5,87 | 11 : 5,08 |
| 010000 | 3 | 1,42 | 1 : 13,87 | 8 : 9,78 | 12 : 7,54 | 0 : 6,83 | 9 : 6,06 |
| 001000 | 4 | 3,04 | 1 : 31,40 | 8 : 10,32 | 0 : 10,07 | 9 : 8,21 | 3 : 6,40 |
| 000100 | 3 | 1,03 | 5 : 9,33 | 13 : 9,07 | 4 : 8,83 | 12 : 7,66 | 10 : 5,41 |
| 000010 | 3 | 3,70 | 3 : 21,54 | 15 : 5,82 | 7 : 4,69 | 2 : 4,22 | 0 : 4,18 |
| 000001 | 2 | 2,42 | 2 : 16,84 | 12 : 6,95 | 1 : 4,40 | 15 : 4,07 | 7 : 3,77 |

S dostatečnou spolehlivostí dokážeme určit klíč pro 1., 3., 5. a 6. sbox.

Pro odhalení 4. sboxu je se známým klíčem ?010 jsou možné klíče 8,10. Z této skupiny je se spolehlivostí 3,52 nejpravděpodobnější klíč 8.

K ověření 2. sboxu použijeme výše zmíněné již odhalené bity. Odhalený klíč je 10??, tomuto zadání odpovídají klíče $8, 9, 10, 11$. Z těchto klíčů je nejpravděpodobnější 8 (se spolehlivostí 1,61). Ačkoli je spolehlivost tohoto klíče menší, než očekávaná, budeme tento klíč považovat za dostatečný. Pokud při pokusu o dešifrování celé šifry nezískáme správný výsledek, použijeme pro další pokus 2. nejpravděpodobnější klíč pro tento sbox.

Získaným klíčem tohoto kola je $4, 8, 1, 10, 3, 2$, tedy: 010010000001101000110010, po permutaci: 000100110101000011001000.

#### 9.5.1 Vyhodnocení po 3. kole

Po přidání posledních 8 získaných bitů klíče získáme celý klíč šifry, který je možno použít k dešifrování šifrovaných textů. Po doplnění posledních bitů klíče kola dostaneme následující celkový klíč:

011010010011000101010001001101010010111100010100010011 01

Získaný klíč je skutečně použitý klíč při šifrování, z čehož vyplývá, že útok pomocí metody lineární kryptoanalýzy byl úspěšný.

#### 9.5.2 Alternativní útok

Po druhém kole útoku zbývá na odhalení posledních 8 bitů klíče, tedy $2^8$ možností. Proto je jednodušší a rychlejší provést útok hrubou silou pro 256 zbývajících kombinací.

# 10 Diferenciální kryptoanalýza

Na tomto místě začíná část věnovaná diferenciální kryptoanalýze. Ačkoli je použit stejný klíč, jako u lineární kryptoanalýzy, a získáváné výsledky tak budou totožné, proběhla tato kryptoanalýza nezávisle a výsledku je dosaženo čistě pomocí metody diferenciální kryptoanalýzy.

## 10.1 Odvození rovnice diferencí

Hledáme vhodné vstupní a výstupní diferenciály pro $n-1$ kol šifry. V prvním kole zvolíme diferenciál pro sbox6 s $\Delta X = 1$ a $\Delta Y = 2$. S tabulky diferencí zjistíme, že tento diferenciál platí s pravděpodobností $Q_1 = 4/16$. Tyto diferenciály můžeme označit jako $X_{(1,23)}$ a $Y_{(1,22)}$, kde $X_{(1,23)} = P_{23}$.

Po provedení permutace tento výstupní diferenciál odpovídá diferenciálu $X_{(2,11)}$. Jde o 3.sbox se vstupem $\Delta X = 1$ a výstupem $\Delta Y = 8$, tedy $Y_{(2,8)}$ s pravděpodobností 4/16, tedy $Q_2 = (4/16)^2 = 1/16$.

Pro 3. kolo platí následující rovnice:

$$\begin{aligned} Y_{(2,8)} &= X_{(3,19)} \\ X_{(3,19)} &= Y_{(3,18)} \\ Q_3 &= Q_2 \cdot \frac{4}{16} = \frac{1}{64} \end{aligned} \tag{10.1}$$

Ve 4. kole odvodíme stejným způsobem rovnice:

$$\begin{aligned} Y_{(3,18)} &= X_{(4,16)} \\ X_{(4,16)} &= Y_{(4,17)} \\ Q_4 &= Q_3 \cdot \frac{2}{16} = \frac{1}{512} \end{aligned} \tag{10.2}$$

V posledním kole hledání získáme:

$$\begin{aligned} Y_{(4,17)} &= X_{(5,2)} \\ X_{(5,2)} &= Y_{(5,0)} \\ Q_5 &= Q_4 \cdot \frac{6}{16} = \frac{3}{4096} \end{aligned} \tag{10.3}$$

Po provedení poslední permutace zjistíme, že $Y_{(5,0)} = C_{13}$. Odvodili jsme tedy, že pro vstupní diferenciál $P_{23}$ dostaneme výstupní diferenciál $C_{13}$ s pravděpodobností $3/4096 \approx 0.000732$.

### 10.1.1 Alternativní rovnice

Výše rozepsanou diferenci můžeme napsat takto:

$$\begin{aligned} P_{23} \xrightarrow{s} Y_{(1,22)} \xrightarrow{p} X_{(2,11)} \xrightarrow{s} Y_{(2,8)} \xrightarrow{p} X_{(3,19)} \xrightarrow{s} Y_{(3,18)} \xrightarrow{p} \\ X_{(4,16)} \xrightarrow{s} Y_{(4,17)} \xrightarrow{p} X_{(5,2)} \xrightarrow{s} Y_{(5,0)} \xrightarrow{p} C_{13} \end{aligned} \tag{10.4}$$

Následující rovnice cílí na stejnou vstupní i výstupní diferenci:

$$\begin{aligned} P_{23} \xrightarrow{s} Y_{(1,22)} \xrightarrow{p} X_{(2,11)} \xrightarrow{s} Y_{(2,8)} \xrightarrow{p} X_{(3,19)} \oplus X_{(3,1)} \xrightarrow{s} \\ Y_{(3,18)} \oplus Y_{(3,3)} \xrightarrow{p} X_{(4,16)} \oplus X_{(4,23)} \xrightarrow{s} Y_{(4,17)} \oplus Y_{(4,21)} \xrightarrow{p} \\ X_{(5,0)} \oplus X_{(5,2)} \xrightarrow{s} Y_{(5,0)} \xrightarrow{p} C_{13} \end{aligned} \tag{10.5}$$

Spočtěme pravděpodobnost této rovnice:

$$Q_n = \prod_{i=1}^{n} Q_i = \frac{4 \cdot 2 \cdot 2 \cdot 4 \cdot 2 \cdot 4 \cdot 2}{16^7} = \frac{1}{262144} \tag{10.6}$$

Z nalezení druhé diference cílící na stejný vstupní a výstupní diferenciál, i když s mnohem menší pravděpodobností, je možno vyvodit, že může existovat i nenalezená rovnice s větší pravděpodobností. Proto i v tomto případě uvažujeme o nejlepší nalezené diferenci jako o „minimální diferenci“ a proto také při samotné diferenciální kryptoanalýze na nalezené pravděpodobnosti není brán zřetel.

## 10.2 Vzorový útok

Byla nalezena závislost výstupní diference $C[12]$ na vstupní diferenci $P[16, 18]$ s minimální pravděpodobností 3/8192. Tato výstupní diference odpovídá 4.sboxu, bude tedy testováno 16 možností. Postup útoku je následující:

- Vygenerovat 100000 různých otevřených textů $X'$
- Pro každé $X'$ spočítat $X''$ tak, že $X'' = X' \oplus \Delta X$
- Zašifrováním všech $X', X''$ získat odpovídající $Y', Y''$
- Pro každý testovaný klíč a každou dvojici odpovídajících otevřených textů $X', X''$ provést částečné dešifrování odpovídajících šifrovaných textů subklíčem $i$
- Vypočítat diferenci částečně dešifrovaných šifrovaných textů $\Delta Y_t = Y'_t \oplus Y''_t$
- Pokud se vypočítaná diference rovná požadované diferenci, pak hodnotu daného testovaného klíče zvýšit o 1

Po provedení těchto kroků pro všechny otevřené texty a testované klíče získáme následující tabulku:

Tab. 10.1 Vyhodnocení útoku diferenciální kryptoanalýzou

| Klíč | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $h_i$ | 43 | 77 | 31 | 90 | 34 | 111 | 43 | 149 | 121 | 43 | 112 | 31 | 86 | 34 | 102 | 43 |
| Pořadí | 9 | 8 | 15 | 6 | 13 | 4 | 9 | 1 | 2 | 9 | 3 | 15 | 7 | 13 | 5 | 9 |

Z provedené kryptoanalýzy tedy vyplývá, že nejpravděpodobnější klíč pro daný sbox je 7.

### 10.2.1 Rozšířené vyhodnocení

Pro útok mnohonásobnou diferenciální kryptoanalýzou je nutno stanovit, jakým způsobem porovnat výsledky jednotlivých útoků cílících na jeden sbox. Při hledání vhodného srovnání se vycházelo z předpokladu, že s rostoucím množstvím shodných diferencí pro daný klíč roste pravděpodobnost správnosti klíče. Druhým předpokladem bylo, že s rostoucím množstvím shodných diferencí bez ohledu na správnost klíče roste věrohodnost daného útoku. K ohodnocení této věrohodnosti byla stanovena logaritmická škála se základem 10. Hodnoty ke srovnání více útoků na stejný sbox se tedy spočítají následujícím vzorcem:

$$G_i = h_i \cdot \log\left(\frac{1}{n}\sum_{j=0}^{n-1} h_j\right) \tag{10.7}$$

Jde tedy o dekadický logaritmus aritmetického průměru hodnot pro daný útok.

## 10.3 1. kolo útoku

Pro první kolo útoku bylo zvoleno 23 rovnic cílících na 1 sbox. Po provedení útoků a agregaci dat pomocí metody popsané výše dostaneme následující tabulku:

Tab. 10.2 1. kolo diferenciální kryptoanalýzy (všechny sboxy)

| sbox | rovnic | S | 1. | 2. | 3. | 4. | 5. |
|---|---|---|---|---|---|---|---|
| 100000 | 4 | 2,98 | 4 : 212,13 | 1 : 71,15 | 5 : 69,82 | 15 : 59,30 | 0 : 56,40 |
| 010000 | 3 | 1,91 | 0 : 87,19 | 3 : 45,76 | 8 : 45,75 | 4 : 32,83 | 1 : 31,38 |
| 001000 | 3 | 3,04 | 1 : 269,97 | 0 : 88,80 | 8 : 82,25 | 4 : 79,65 | 9 : 72,59 |
| 000100 | 5 | 1,63 | 7 : 622,60 | 14 : 382,38 | 5 : 349,24 | 12 : 267,49 | 8 : 227,50 |
| 000010 | 6 | 2,25 | 10 : 442,88 | 7 : 196,60 | 14 : 186,50 | 4 : 171,95 | 1 : 168,00 |
| 000001 | 2 | 1,66 | 9 : 100,19 | 10 : 60,49 | 11 : 52,83 | 14 : 48,57 | 13 : 44,46 |

Za dostatečnou spolehlivost z pohledu diferenciální kryptoanalýzy považujeme hodnotu 1,6. Jak je možno vidět z tabulky, dostatečnou spolehlivost máme u všech sboxů. Z toho je možno odvodit klíč kola: $4, 0, 1, 7, 10, 9$.

### 10.4 2.kolo útoku

Stejně jako u lineární kryptoanalýzy odstraníme z šifrovaného textu $Y'$ klíč 1. kola, substituci a jedno kolo permutace. Stejnou úpravu provedeme pro každý $Y''$, který v rámci diferenciálního útoku použijeme.

Ve druhém kole útoku použijeme opět 22 rovnic. Výsledky 2. kola aproximace shrnuje následující tabulka:

Tab. 10.3 2. kolo diferenciálního útoku (všechny sboxy)

| sbox | rovnic | S | 1. | 2. | 3. | 4. | 5. |
|---|---|---|---|---|---|---|---|
| 100000 | 4 | 1,38 | 3 : 257 | 2 : 186 | 8 : 149 | 9 : 141 | 11 : 99 |
| 010000 | 3 | 1,67 | 15 : 745 | 7 : 445 | 12 : 427 | 3 : 276 | 11 : 275 |
| 001000 | 3 | 1,94 | 6 : 393 | 10 : 202 | 8 : 143 | 4 : 138 | 3 : 134 |
| 000100 | 4 | 1,52 | 9 : 6 057 | 0 : 3 983 | 6 : 3 740 | 11 : 3 645 | 13 : 3 469 |
| 000010 | 6 | 1,93 | 9 : 1 251 | 12 : 648 | 11 : 516 | 8 : 501 | 3 : 473 |
| 000001 | 2 | 2,06 | 8 : 1 968 | 11 : 954 | 15 : 935 | 12 : 812 | 9 : 683 |

S dostatečnou spolehlivostí jsme tedy schopni určit klíč pro 2., 3., 5. a 6. sbox. K získání klíče 1. a 4. kola použijeme rovnici cílící na tyto dva sboxy.

Tab. 10.4 Útok na 1. a 4. sbox

| sbox | rovnic | S | 1. | 2. | 3. | 4. | 5. |
|---|---|---|---|---|---|---|---|
| 100100 | 1 | 1 | 3,9 : 26,19 | 3,0 : 26,19 | 3,1 : 17,61 | 3,2 : 13,54 | 3,4 : 11,29 |

Ze spolehlivosti výsledku 1 vyplývá, že dva různé výsledky mají stejnou pravděpodobnost výskytu. Proto použijeme k podrobnějšímu vyhodnocení výsledky z útoků na jednotlivé sboxy. Převedeme tedy výsledky útoku na 1., 4., a současně oba sboxy na procenta maxima a tyto mezi sebou vynásobíme.[1)]

Tab. 10.5 Rozšíření útoku na 1. a 4. sbox

| sbox | rovnic | S | 1. | 2. | 3. | 4. | 5. |
|---|---|---|---|---|---|---|---|
| 100100 | 1 | 1,52 | 3,9 : 10,00 | 3,0 : 6,58 | 3,2 : 2,47 | 3,4 : 2,21 | 3,1 : 1,70 |

Ačkoli je spolehlivost útoku pouze 1.52, což je pro naše účely nedostatečné, můžeme po bližším zkoumání největších výsledků určit klíč 1. kola jako 3. Výsledek 4. sboxu nám tento útok nepomohl potvrdit ani vyvrátit, vzhledem ke stavu útoku jej budeme považovat za správný s předpokladem, že na případnou chybu způsobenou použitím špatného klíče narazíme v příštím kole útoku.

Klíčem kola je tedy $3, 15, 6, 9, 9, 8$, po permutaci a převedení na bitový zápis:

010001101100101100101111.

[1)] Stejný postup jako v prvním kole lineární kryptoanalýzy, včetně násobení výsledku deseti z důvodu větší přehlednosti

### 10.4.1 Vyhodnocení po 2. kole

Vzhledem k tomu, že postup, mezivýsledky i finální výsledek lineární a diferenciální kryptoanalýzy je u stejné šifry se stejným klíčem totožný, odvodíme stejným způsobem již známý klíč pro další kolo útoku: 010?, 10??, ?0??, ?010, 00?1, 0010.

## 10.5 3.kolo útoku

Po odstranění dalšího kola klíče, substituace a permutace provedeme poslední kolo útoku diferenciální kryptoanalýzou. Pro toto použijeme 20 rovnic:

Tab. 10.6 Finální kolo útoku (všechny sboxy)

| sbox | rovnic | S | 1. | 2. | 3. | 4. | 5. |
|---|---|---|---|---|---|---|---|
| 100000 | 4 | 1,58 | 4 : 2629 | 5 : 1666 | 15 : 1092 | 14 : 1090 | 12 : 812 |
| 010000 | 3 | 2,72 | 8 : 6427 | 12 : 2366 | 0 : 1325 | 11 : 1226 | 4 : 1203 |
| 001000 | 3 | 2,27 | 1 : 3278 | 0 : 1444 | 12 : 1332 | 13 : 1093 | 15 : 906 |
| 000100 | 4 | 1,86 | 10 : 15395 | 3 : 8278 | 8 : 6916 | 5 : 6682 | 14 : 5617 |
| 000010 | 4 | 2,49 | 3 : 16765 | 9 : 6739 | 7 : 6518 | 11 : 5584 | 0 : 5386 |
| 000001 | 2 | 1,94 | 2 : 3554 | 1 : 1837 | 3 : 1428 | 5 : 1416 | 6 : 1085 |

S dostatečnou spolehlivostí jsme získali klíč pro všechny sboxy kromě 1. Očekávaný klíč je tedy 4 nebo 5. Bohužel jde o dva nejravděpodobnější klíče, v tomto případě tedy nemůžeme použít již známý klíč k rozhodnutí.

Dvě ze čtyř rovnic, které jsme testovali pro první sbox, jsou $P[11], C[0]$ a $P[11], C[2]$. U obou rovnic je prvním kole zapojen 4. sbox: $X_{(1,11)} = Y_{(1,9)}$. Hodnota v odpovídajícím řádku a sloupci 4. sboxu je 4. Za každý sloupec tohoto sboxu, ve kterém je ve stejném řádku hodnota 4, můžeme z každé rovnice vytvořit jednu další se stejnou pravděpodobností. V tomto případě tedy existuje $X_{(1,10)} = Y_{(1,9)}$, můžeme tedy vytvořit dvě další rovnice: $P[10], C[0]$ a $P[10], C[2]$. Po provedení útoku na tyto dvě rovnice a sloučení s hodnotami z předchozího pokusu dostaneme následující tabulku:

Tab. 10.7 Rozšířený útok na 1.sbox

| sbox | rovnic | S | 1. | 2. | 3. | 4. | 5. |
|---|---|---|---|---|---|---|---|
| 100000 | 6 | 1,80 | 4 : 3 334,8 | 5 : 1 847,8 | 15 : 1 164,3 | 14 : 1 085,9 | 0 : 957,8 |

S dostatečnou spolehlivostí můžeme prohlásit 4 jako klíč 1. sboxu. Tímto byl odhalen poslední chybějící bit klíče.Získaným klíčem tohoto kola je $4, 8, 1, 10, 3, 2$, tedy 010010000001101000110010, po permutaci 000100110101000011001000.

### 10.5.1 Vyhodnocení po 3. kole

Po přidání posledních 8 získaných bitů klíče získáme celý klíč šifry, který je možno použít k dešifrování šifrovaných textů. Po doplnění posledních bitů klíče kola dostaneme

následující celkový klíč:

01101001001100010101000100110101001011110001010001001101

Získaný klíč je skutečně použitý klíč při šifrování, z čehož vyplývá, že útok pomocí metody diferenciální kryptoanalýzy byl také úspěšný.

### 10.5.2 Alternativní útok

Kromě provedení útoku hrubou silou na počátku kola je možno použít tento útok na poslední neznámý bit klíče. V takovém případě zbývají pouze 2 možnosti, které je nutno otestovat. Cílem práce je demonostrovat diferenciální kryptoanalýzu, proto nebyla tato metoda použita.

## 11 Srovnání metod

Jak bylo demonstrováno, obě metody nezávisle na sobě vedly k prolomení šifry. Tato část je věnována srovnání výsledků obou metod. Cílem bylo zhodnotit výsledky obou kryptoanalýz za co nejpodobnějších možných podmínek.

Z hlediska lineární kryptoanalýzy není rozdíl mezi útokem se zvoleným nebo se známým otevřeným textem, diferenciální kryptoanalýza by pro útok se známým otevřeným textem potřebovala mnohonásobně více vzorků než útok se zvoleným otevřeným textem. Proto byl pro srovnání zvolen útok se zvoleným otevřeným textem.

Pro srovnání bylo zvoleno celkem 6 rovnic pro lineární a 6 pro diferenciální kryptoanalýzu. Tyto rovnice jsou rozděleny do dvou skupin po třech, kde první trojice útočí na 1. sbox a druhá trojice na 5. sbox. Rovnice byly zvoleny na základě reálných výsledků kryptoanalýzy, linearního biasu a diferenciální pravděpodobnosti tak, aby bylo srovnání co nejprůkaznější. Srovnání probíhá na všech kolech výše popsané šifry (tedy na úrovni 1.kola kryptoanalýzy). Byly zvoleny následující rovnice:

Tab. 11.1 Rovnice pro srovnání

| Typ | Sbox | B/P | Rovnice |
|---|---|---|---|
| L | 1 | 0,0117 | $P[12, 13, 15] \oplus C[1]$ |
| L | 1 | 0,0078 | $P[22] \oplus C[2]$ |
| L | 1 | 0,0088 | $P[4, 5, 7, 22] \oplus C[0]$ |
| L | 5 | 0,0078 | $P[12] \oplus C[17]$ |
| L | 5 | 0,0078 | $P[17, 18] \oplus C[17]$ |
| L | 5 | 0,0176 | $P[4, 5, 7, 22] \oplus C[16]$ |
| D | 1 | 0,0002441 | $P[21] \oplus C[0]$ |
| D | 1 | 0,0003662 | $P[14, 15] \oplus C[2]$ |
| D | 1 | 0,0003662 | $P[0, 3] \oplus C[0]$ |
| D | 5 | 0,0004119 | $P[0, 1, 2] \oplus C[18]$ |
| D | 5 | 0,0004119 | $P[0, 1, 2] \oplus C[17]$ |
| D | 5 | 0,0004882 | $P[0] \oplus C[16]$ |

Pro každé kolo srovnání bylo pseudonáhodně vygenerováno 50000 otevřených textů. V případě diferenciální kryptoanalýzy byla pro každý otevřený text a každou rovnici vypočítán další text s požadovanou diferencí (celkem tedy 1 otevřený text použitý při lineární kryptoanalýzy odpovídá 6 otevřeným textům pro diferenciální kryptoanalýzu[1)]).

Částečné výsledky byly pořízeny v intervalu každých 2500 otevřených textů. Tyto jsou použity pro srování metod v závislosti na počtu použitých otevřených textů. Celkem bylo provedeno 10 kol srovnání.

Cílem této části bylo provést:

- srovnání lineární a diferenciální kryptoanalýzy na úrovni jednotlivých rovnic
- srovnání mnohonásobné lineární a diferenciální kryptoanalýzy pro trojice zároveň použitých rovnic
- srovnání výsledků kryptoanalýz pro jednotlivé rovnice a pro trojice rovnic

## 11.1 Srovnání jednotlivých útoků

Prvním krokem bylo nezávislé srovnání jednotlivých útoků. Jak již bylo zmíněno, šlo celkem o 60 útoků lineární a 60 diferenciální kryptoanalýzou. Cílem bylo zjistit, u kolika rovnic byl korektně vyhodnocen správný klíč jako ten nejpravděpodobnější, alternativně zda byl alespoň mezi prvními třemi.

[1)] 1 vygenerovaný + 5 pro rovnice diferenciální kryptoanalýzy, neboť dvě rovnice mají stejnou vstupní diferenci

Tab. 11.2 Srovnání jednotlivých útoků

| | Lineární | | | | Diferenciální | | | |
|---|---|---|---|---|---|---|---|---|
| Textů | 1. | 1.-3. | %1. | % 1.-3. | 1. | 1.-3. | %1. | % 1.-3. |
| 2500 | 23 | 35 | 38,33% | 58,33% | 28 | 38 | 46,67% | 63,33% |
| 5000 | 25 | 44 | 41,67% | 73,33% | 39 | 44 | 65,00% | 73,33% |
| 7500 | 30 | 48 | 50,00% | 80,00% | 43 | 53 | 71,67% | 88,33% |
| 10000 | 38 | 52 | 63,33% | 86,67% | 46 | 54 | 76,67% | 90,00% |
| 12500 | 40 | 53 | 66,67% | 88,33% | 47 | 57 | 78,33% | 95,00% |
| 15000 | 34 | 53 | 56,67% | 88,33% | 51 | 58 | 85,00% | 96,67% |
| 17500 | 38 | 53 | 63,33% | 88,33% | 50 | 58 | 83,33% | 96,67% |
| 20000 | 41 | 55 | 68,33% | 91,67% | 50 | 60 | 83,33% | 100,00% |
| 22500 | 42 | 54 | 70,00% | 90,00% | 52 | 58 | 86,67% | 96,67% |
| 25000 | 41 | 56 | 68,33% | 93,33% | 53 | 58 | 88,33% | 96,67% |
| 27500 | 41 | 57 | 68,33% | 95,00% | 54 | 57 | 90,00% | 95,00% |
| 30000 | 44 | 54 | 73,33% | 90,00% | 53 | 60 | 88,33% | 100,00% |
| 32500 | 45 | 56 | 75,00% | 93,33% | 53 | 59 | 88,33% | 98,33% |
| 35000 | 45 | 57 | 75,00% | 95,00% | 54 | 59 | 90,00% | 98,33% |
| 37500 | 44 | 57 | 73,33% | 95,00% | 55 | 59 | 91,67% | 98,33% |
| 40000 | 44 | 56 | 73,33% | 93,33% | 56 | 59 | 93,33% | 98,33% |
| 42500 | 44 | 55 | 73,33% | 91,67% | 57 | 59 | 95,00% | 98,33% |
| 45000 | 45 | 57 | 75,00% | 95,00% | 57 | 59 | 95,00% | 98,33% |
| 47500 | 43 | 58 | 71,67% | 96,67% | 57 | 59 | 95,00% | 98,33% |
| 50000 | 45 | 58 | 75,00% | 96,67% | 56 | 59 | 93,33% | 98,33% |

Sloupec označený 1. značí, v kolika případech byl jako korektní klíč vyhodnocený ten správný, sloupec 1. – 3. ukazuje v kolika případech byl korektní klíč alespoň mezi prvními třemi nejpravděpodobnějšími, sloupce s % analogicky vyjadřují procentovou úspěšnost.

Ze srovnání vyplývá mírná převaha výsledků diferenciální kryptoanalýzy. V rámci objektivity je nutno vzít v potaz dvojnásobné množství testovaných otevřených textů u diferenciální kryptoanalýzy, korektní srovnání je tedy například diferenciální útok na 5000 otevřených textů oproti lineárnímu útoku na 10000 otevřených textů. I přes tuto změnu vycházejí výsledky diferenciální kryptoanalýzy mírně lépe.

Za zmínku zde stojí významně větší rozdíly mezi 1. v pořadí a 1.-3. v pořadí u lineární kryptoanalýzy. Toto je způsobeno jiným charakterem statistické analýzy, kde jde o binomické rozdělení s velmi podobnými pravděpodobnostmi.

### 11.2 Srovnání mnohonásobného útoku

Při mnohonásobném útoku byly vždy 3 odpovídající rovnice vyhodnoceny společně. Rovnice byly přepočteny vzorcem, výsledky odpovídajících rovnic pro odpovídající klíče byly sečteny a tyto výsledky byly vyhodnoceny.

Rovnice pro lineární kryptoanalýzu:

$$G_i = (H_i / \sum_{j=0}^{n-1} H_j)^2 \tag{11.1}$$

Rovnice pro diferenciální kryptoanalýzu:[2)]

$$G_i = h_i \cdot \log\left(1 + \frac{1}{n} \sum_{j=0}^{n-1} h_j\right) \tag{11.2}$$

Tab. 11.3 Srovnání mnohonásobného útoku na sbox

| | Lineární | | | | Diferenciální | | | |
|---|---|---|---|---|---|---|---|---|
| Textů | 1. | 1.-3. | %1. | % 1.-3. | 1. | 1.-3. | %1. | % 1.-3. |
| 2500 | 10 | 16 | 50,00% | 80,00% | 18 | 20 | 90,00% | 100,00% |
| 5000 | 14 | 18 | 70,00% | 90,00% | 20 | 20 | 100,00% | 100,00% |
| 7500 | 17 | 20 | 85,00% | 100,00% | 20 | 20 | 100,00% | 100,00% |
| 10000 | 19 | 20 | 95,00% | 100,00% | 20 | 20 | 100,00% | 100,00% |
| 12500 | 19 | 19 | 95,00% | 95,00% | 20 | 20 | 100,00% | 100,00% |
| 15000 | 19 | 20 | 95,00% | 100,00% | 20 | 20 | 100,00% | 100,00% |
| 17500 | 19 | 20 | 95,00% | 100,00% | 20 | 20 | 100,00% | 100,00% |
| 20000 | 19 | 20 | 95,00% | 100,00% | 20 | 20 | 100,00% | 100,00% |
| 22500 | 20 | 20 | 100,00% | 100,00% | 20 | 20 | 100,00% | 100,00% |
| 25000 | 20 | 20 | 100,00% | 100,00% | 20 | 20 | 100,00% | 100,00% |
| 27500 | 20 | 20 | 100,00% | 100,00% | 20 | 20 | 100,00% | 100,00% |
| 30000 | 20 | 20 | 100,00% | 100,00% | 20 | 20 | 100,00% | 100,00% |
| 32500 | 20 | 20 | 100,00% | 100,00% | 20 | 20 | 100,00% | 100,00% |
| 35000 | 20 | 20 | 100,00% | 100,00% | 20 | 20 | 100,00% | 100,00% |
| 37500 | 20 | 20 | 100,00% | 100,00% | 20 | 20 | 100,00% | 100,00% |
| 40000 | 20 | 20 | 100,00% | 100,00% | 20 | 20 | 100,00% | 100,00% |
| 42500 | 20 | 20 | 100,00% | 100,00% | 20 | 20 | 100,00% | 100,00% |
| 45000 | 20 | 20 | 100,00% | 100,00% | 20 | 20 | 100,00% | 100,00% |
| 47500 | 20 | 20 | 100,00% | 100,00% | 20 | 20 | 100,00% | 100,00% |
| 50000 | 20 | 20 | 100,00% | 100,00% | 20 | 20 | 100,00% | 100,00% |

[2)] Rovnice byla na rozdíl od praktické části upravena přidáním části „$1 + \ldots$“, aby platila i pro rovnice, kde je suma $h_j$ menší než 16.

Z tabulky vyplývá, že pro danou šifru a dané kombinace rovnic je potřeba zhruba 10000 otevřených textů pro dosažení 90% úspěšnosti v určení správného klíče. U diferenciální kryptoanalýzy je dostačujících 2500 rovnic. Jak bylo již řečeno, u agregovaného útoku odpovídá jeden otevřený text diferenciální šesti otevřeným textům pro lineární kryptoanalýzu. Srovnatelné číslo je tedy 15000 otevřených textů. V případě agregovaných útoků je tedy úspěšnost srovnatelná.

Vzhledem k tomu, že byly rovnice vybírány ručně tak, aby byl výsledek co nejlepší, je pravděpodobné, že v případě náhodného výběru rovnic ze všech použitých by výsledky poukazovaly na nižší úspěšnost útoků.

## 11.3 Srovnání jednotlivého a mnohonásobného útoku lineární kryptoanalýzou

Pro praktickou část byl zvolen model mnohonásobné lineární kryptoanalýzy s hypotézou, že takto zvolený model a metrika pro srovnání jednotlivých útoků na stejný sbox zvýší pravděpodobnost úspěšného útoku. Následuje tabulka srovnání úspěšnosti jednotlivých útoků oproti agregovaným výsledkům:

Tab. 11.4 Mnohonásobný útok lineární kryptoanalýzou

| | Jednotlivý | | | | Agregovaný | | | |
|---|---|---|---|---|---|---|---|---|
| Textů | 1. | 1.-3. | %1. | % 1.-3. | 1. | 1.-3. | %1. | % 1.-3. |
| 2500 | 23 | 35 | 38,33% | 58,33% | 10 | 16 | 50,00% | 80,00% |
| 5000 | 25 | 44 | 41,67% | 73,33% | 14 | 18 | 70,00% | 90,00% |
| 7500 | 30 | 48 | 50,00% | 80,00% | 17 | 20 | 85,00% | 100,00% |
| 10000 | 38 | 52 | 63,33% | 86,67% | 19 | 20 | 95,00% | 100,00% |
| 12500 | 40 | 53 | 66,67% | 88,33% | 19 | 19 | 95,00% | 95,00% |
| 15000 | 34 | 53 | 56,67% | 88,33% | 19 | 20 | 95,00% | 100,00% |
| 17500 | 38 | 53 | 63,33% | 88,33% | 19 | 20 | 95,00% | 100,00% |
| 20000 | 41 | 55 | 68,33% | 91,67% | 19 | 20 | 95,00% | 100,00% |
| 22500 | 42 | 54 | 70,00% | 90,00% | 20 | 20 | 100,00% | 100,00% |
| 25000 | 41 | 56 | 68,33% | 93,33% | 20 | 20 | 100,00% | 100,00% |
| 27500 | 41 | 57 | 68,33% | 95,00% | 20 | 20 | 100,00% | 100,00% |
| 30000 | 44 | 54 | 73,33% | 90,00% | 20 | 20 | 100,00% | 100,00% |
| 32500 | 45 | 56 | 75,00% | 93,33% | 20 | 20 | 100,00% | 100,00% |
| 35000 | 45 | 57 | 75,00% | 95,00% | 20 | 20 | 100,00% | 100,00% |
| 37500 | 44 | 57 | 73,33% | 95,00% | 20 | 20 | 100,00% | 100,00% |
| 40000 | 44 | 56 | 73,33% | 93,33% | 20 | 20 | 100,00% | 100,00% |
| 42500 | 44 | 55 | 73,33% | 91,67% | 20 | 20 | 100,00% | 100,00% |
| 45000 | 45 | 57 | 75,00% | 95,00% | 20 | 20 | 100,00% | 100,00% |
| 47500 | 43 | 58 | 71,67% | 96,67% | 20 | 20 | 100,00% | 100,00% |
| 50000 | 45 | 58 | 75,00% | 96,67% | 20 | 20 | 100,00% | 100,00% |

Z tabulky vyplývá výrazné zlepšení pravděpodobnosti určení správného klíče na všech úrovních.

## 11.4 Srovnání jednotlivého a mnohonásobného útoku diferenciální kryptoanalýzou

Stejně jako u lineární kryptoanalýzy provedeme srovnání jednotlivých a agregovaných útoků u diferenciální kryptoanalýzy.

Tab. 11.5 Mnohonásobný útok diferenciální kryptoanalýzou

| | Jednotlivý | | | | Agregovaný | | | |
|---|---|---|---|---|---|---|---|---|
| Textů | 1. | 1.-3. | %1. | % 1.-3. | 1. | 1.-3. | %1. | % 1.-3. |
| 2500 | 28 | 38 | 46,67% | 63,33% | 18 | 20 | 90,00% | 100,00% |
| 5000 | 39 | 44 | 65,00% | 73,33% | 20 | 20 | 100,00% | 100,00% |
| 7500 | 43 | 53 | 71,67% | 88,33% | 20 | 20 | 100,00% | 100,00% |
| 10000 | 46 | 54 | 76,67% | 90,00% | 20 | 20 | 100,00% | 100,00% |
| 12500 | 47 | 57 | 78,33% | 95,00% | 20 | 20 | 100,00% | 100,00% |
| 15000 | 51 | 58 | 85,00% | 96,67% | 20 | 20 | 100,00% | 100,00% |
| 17500 | 50 | 58 | 83,33% | 96,67% | 20 | 20 | 100,00% | 100,00% |
| 20000 | 50 | 60 | 83,33% | 100,00% | 20 | 20 | 100,00% | 100,00% |
| 22500 | 52 | 58 | 86,67% | 96,67% | 20 | 20 | 100,00% | 100,00% |
| 25000 | 53 | 58 | 88,33% | 96,67% | 20 | 20 | 100,00% | 100,00% |
| 27500 | 54 | 57 | 90,00% | 95,00% | 20 | 20 | 100,00% | 100,00% |
| 30000 | 53 | 60 | 88,33% | 100,00% | 20 | 20 | 100,00% | 100,00% |
| 32500 | 53 | 59 | 88,33% | 98,33% | 20 | 20 | 100,00% | 100,00% |
| 35000 | 54 | 59 | 90,00% | 98,33% | 20 | 20 | 100,00% | 100,00% |
| 37500 | 55 | 59 | 91,67% | 98,33% | 20 | 20 | 100,00% | 100,00% |
| 40000 | 56 | 59 | 93,33% | 98,33% | 20 | 20 | 100,00% | 100,00% |
| 42500 | 57 | 59 | 95,00% | 98,33% | 20 | 20 | 100,00% | 100,00% |
| 45000 | 57 | 59 | 95,00% | 98,33% | 20 | 20 | 100,00% | 100,00% |
| 47500 | 57 | 59 | 95,00% | 98,33% | 20 | 20 | 100,00% | 100,00% |
| 50000 | 56 | 59 | 93,33% | 98,33% | 20 | 20 | 100,00% | 100,00% |

I zde je patrné zvýšení pravděpodobnosti úspěchu agregovaného útoku, obzvláště u nižšího množství použitých rovnic.

## 11.5 Vyhodnocení

Ačkoli se ve srovnávacích testech lépe jevila diferenciální kryptoanalýza, je nutno připomenout fakt, že na lineární kryptoanalýza běžně pracuje o úroveň výše, než bylo srovnání provedeno, a této úrovni by diferenciální kryptoanalýza mohla být provedena jen velmi těžko.

Na provedených kryptoanalýzách je možno vidět, že ačkoli jde o dvě odlišné metody, mají velmi mnoho společného a jejich pracovní postup je velmi podobný. I proto lze metody jednoduše kombinovat v lineárně-diferenciální kryptoanalýze, díky které je možno prolomit šifry, se kterými by samostatná lineární i diferenciální kryptoanalýza měla potíže.

# ZÁVĚR

Cílem práce bylo demnostrovat metody lineární a diferenciální kryptoanalýzy a jejich použití na jednoduché blokové šifře.

První část práce se věnovala definici kryptologických pojmů nutných k pochopení problematiky, a také k popsání obecných kryptoanalytických principů, ze kterých útoky vychází.

Další část byla věnována teoretickému popisu obou metod a praktickým ukázkám jednotlivých kroků.

Poté následuje samotná tříkolová demonstrace obou mnohonásobných útoků na zvolené šifře s cílem odhalit celý klíč použitý k zašifrování otevřeného textu.

Poslední část byla věnována srovnání podobností obou metod, a také porovnání jejich výkonu s cílem srovnat pravděpodobnost úspěšného odhalení klíče v závislosti na počtu známých otevřených textů.

## SEZNAM POUŽITÉ LITERATURY

[1] Úvod do kryptologie. *Mendelova univerzita v Brně* [online]. [cit. 2019-05-26]. Dostupné z: https://is.mendelu.cz/eknihovna/opory/zobraz_cast.pl?cast=7021

[2] DIFFIE, Whitfield a Martin E. HELLMAN. Multiuser cryptographic techniques. *Proceedings of the June 7-10, 1976, national computer conference and exposition* [online]. [cit. 2019-05-26]. Dostupné z: https://dl.acm.org/citation.cfm?id=1499815

[3] Asymetrická kryptografie. *Mendelova univerzita v Brně* [online]. [cit. 2019-05-26]. Dostupné z: https://is.mendelu.cz/eknihovna/opory/zobraz_cast.pl?cast=7027

[4] PINKAVA, Jaroslav. Základy kryptografie III. *Crypto-world* [online]. [cit. 2019-05-26]. Dostupné z: http://crypto-world.info/pinkava/uvod/bulletin3.pdf

[5] Asymetrické šifry. *Střední škola - Centrum odborné přípravy technické Kroměříž* [online]. [cit. 2019-05-26]. Dostupné z: https://coptkm.cz/portal/reposit.php?action=0&id=40950&revision=-1&instance=1

[6] Úvod do kryptografie. *EARCHIVACE.CZ* [online]. [cit. 2019-05-26]. Dostupné z: http://www.earchivace.cz/technologie/uvod-do-kryptografie/

[7] Symetrické šifry. *Střední škola - Centrum odborné přípravy technické Kroměříž* [online]. [cit. 2019-05-26]. Dostupné z: https://coptkm.cz/portal/reposit.php?action=0&id=40940&revision=-1&instance=1

[8] ISO/IEC 10116:2017: Modes of operation for an n-bit block cipher. *International Organization for Standardization* [online]. [cit. 2019-05-26]. Dostupné z: https://www.iso.org/obp/ui/#iso:std:iso-iec:10116:ed-4:v1:en

[9] BUJARI, Diedon a Erke ARIBAS. *Comparative Analysis of Block Cipher Modes of Operation.* [online]. [cit. 2019-05-26]. Dostupné z: https://www.researchgate.net/publication/322294203_Comparative_Analysis_of_Block_Cipher_Modes_of_Operation

[10] Block Ciphers Modes of Operation. *Crypto-IT* [online]. [cit. 2019-05-26]. Dostupné z: http://www.crypto-it.net/eng/theory/modes-of-block-ciphers.html

[11] VONDRUŠKA, Pavel. Režimy činností kryptografických algoritmů. *Crypto-World* [online]. **2002**(78) [cit. 2019-05-26]. Dostupné z: http://crypto-world.info/casop4/crypto78_02.pdf

[12] SHANNON, C.E. Communication Theory of Secrecy Systems. *University of Wisconsin-Madison* [online]. [cit. 2019-05-26]. Dostupné z: http://pages.cs.wisc.edu/~rist/642-spring-2014/shannon-secrecy.pdf

[13] CHRISTENSEN, Chris. Diffusion and Confusion. *Northern Kentucky University* [online]. [cit. 2019-05-26]. Dostupné z: https://www.nku.edu/~christensen/diffusionandconfusion

[14] YELLA, Vijay. Linear and Differential Cryptanalysis of Substitution Permutation Networks. *Rochester Institute of Technology* [online]. [cit. 2019-05-26]. Dostupné z: https://www.cs.rit.edu/usr/local/pub/GraduateProjects/2165/vy8970/Report.pdf

[15] Ciphertext-Only (Known Ciphertext) Attack. *Crypto-IT* [online]. [cit. 2019-05-26]. Dostupné z: http://www.crypto-it.net/eng/attacks/known-ciphertext.html

[16] SADKHAN, S.B. Methods of cryptanalysis. *University of Babylon* [online]. [cit. 2019-05-26]. Dostupné z: http://www.uobabylon.edu.iq/eprints/paper_5_7264_649.pdf

[17] Semantic security. *Wikipedia: the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation, 2001- [cit. 2019-05-26]. Dostupné z: https://en.wikipedia.org/wiki/Semantic_security

[18] WEI, Lei, Christian RECHBERGER, Jian GUO, Hongjun WU, Huaxiong WANG a San LING. Improved Meet-in-the-Middle Cryptanalysis of KTANTAN. *Grøstl – a SHA-3 candidate* [online]. [cit. 2019-05-26]. Dostupné z: http://www.groestl.info/rechberger/AdvancedMITMPreimage.pdf

[19] MATSUI, Mitsuru a Atsuhiro YAMAGISHI. A New Method for Known Plaintext Attack of FEAL Cipher. *Advances in Cryptology — EUROCRYPT' 92* [online]. [cit. 2019-05-26]. Dostupné z: https://link.springer.com/chapter/10.1007/3-540-47555-9_7

[20] MATSUI, Mitsuru. Linear Cryptanalysis Method for DES Cipher. *Advances in Cryptology — EUROCRYPT '93* [online]. [cit. 2019-05-26]. Dostupné z: https://link.springer.com/chapter/10.1007/3-540-48285-7_33

[21] MATSUI, Mitsuru. The First Experimental Cryptanalysis of the Data Encryption Standard. *Advances in Cryptology — CRYPTO '94* [online]. [cit. 2019-05-26]. Dostupné z: https://link.springer.com/chapter/10.1007/3-540-48658-5_1

[22] HEYS, Howard M. *A Tutorial on Linear and Differential Cryptanalysis* [online]. [cit. 2019-05-26]. Dostupné z: https://www.engr.mun.ca/~howard/PAPERS/ldc_tutorial.pdf

[23] Bias. *WikiSkripta* [online]. [cit. 2019-05-26]. Dostupné z: https://www.wikiskripta.eu/w/Bias

[24] BIHAM, Eli a Adi SHAMIR. Differential Cryptanalysis of the Data Encryption Standard. *Technion - Israel Institute of Technology* [online]. [cit. 2019-05-26]. Dostupné z: http://www.cs.technion.ac.il/~biham/Reports/differential-cryptanalysis-of-the-data-encryption-standard-biham-shamir-authors-latex-version.pdf

## SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

| | |
|---|---|
| P | otevřený text |
| C | šifrovaný text |
| K | klíč |
| X | vstup do sboxu |
| Y | výstup z sboxu |
| $K_i$ | $i$-tý bit klíče |
| $K_{(j,i)}$ | $i$-tý bit klíče $j$-tého kola |
| $P$[i,j,k] | $P_i \oplus P_j \oplus P_k$ |

## SEZNAM TABULEK

## SEZNAM PŘÍLOH

# PŘÍLOHA P I. TABULKY LINEÁRNÍ APROXIMACE 1. A 2.SBOXU

Lineární aproximace 1.sboxu

| X\|Y | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 8 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 1 | 0 | 2 | 0 | 2 | 2 | 0 | 2 | 4 | 0 | 2 | 0 | 2 | 2 | 4 | 2 | 0 |
| 2 | 0 | 2 | 2 | 0 | 0 | 2 | 2 | 0 | 4 | 2 | 2 | 4 | 0 | 2 | 2 | 0 |
| 3 | 0 | 0 | 2 | 2 | 2 | 2 | 0 | 0 | 4 | 0 | 2 | 2 | 2 | 2 | 0 | 4 |
| 4 | 0 | 4 | 0 | 4 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 0 | 0 | 0 | 0 |
| 5 | 0 | 2 | 4 | 2 | 4 | 2 | 0 | 2 | 2 | 0 | 2 | 0 | 2 | 0 | 2 | 0 |
| 6 | 0 | 2 | 2 | 0 | 2 | 0 | 0 | 2 | 2 | 0 | 4 | 2 | 0 | 2 | 2 | 4 |
| 7 | 0 | 0 | 2 | 2 | 0 | 0 | 2 | 2 | 2 | 6 | 0 | 0 | 2 | 2 | 0 | 0 |
| 8 | 0 | 0 | 2 | 2 | 0 | 0 | 6 | 2 | 2 | 2 | 0 | 0 | 2 | 2 | 0 | 0 |
| 9 | 0 | 2 | 2 | 0 | 2 | 4 | 0 | 2 | 2 | 0 | 4 | 2 | 0 | 2 | 2 | 0 |
| 10 | 0 | 2 | 0 | 2 | 0 | 2 | 0 | 2 | 2 | 0 | 2 | 0 | 2 | 4 | 2 | 4 |
| 11 | 0 | 0 | 4 | 0 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 0 | 0 | 4 | 0 |
| 12 | 0 | 0 | 2 | 2 | 2 | 2 | 0 | 4 | 0 | 0 | 2 | 2 | 2 | 2 | 4 | 0 |
| 13 | 0 | 2 | 2 | 4 | 4 | 2 | 2 | 0 | 0 | 2 | 2 | 0 | 0 | 2 | 2 | 0 |
| 14 | 0 | 2 | 0 | 2 | 2 | 0 | 2 | 0 | 0 | 2 | 0 | 2 | 6 | 0 | 2 | 0 |
| 15 | 0 | 4 | 0 | 0 | 0 | 4 | 0 | 0 | 0 | 0 | 0 | 4 | 0 | 0 | 0 | 4 |

Lineární aproximace 2.sboxu

| X\|Y | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 8 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 1 | 0 | 2 | 2 | 4 | 0 | 2 | 2 | 0 | 4 | 2 | 2 | 0 | 0 | 2 | 2 | 0 |
| 2 | 0 | 0 | 2 | 2 | 0 | 4 | 2 | 2 | 4 | 0 | 2 | 2 | 0 | 0 | 2 | 2 |
| 3 | 0 | 2 | 0 | 2 | 0 | 2 | 4 | 2 | 0 | 2 | 0 | 2 | 0 | 2 | 4 | 2 |
| 4 | 0 | 0 | 0 | 0 | 4 | 0 | 0 | 4 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 |
| 5 | 0 | 2 | 2 | 0 | 0 | 2 | 2 | 4 | 2 | 0 | 0 | 2 | 2 | 4 | 0 | 2 |
| 6 | 0 | 4 | 2 | 2 | 4 | 0 | 2 | 2 | 2 | 2 | 0 | 0 | 2 | 2 | 0 | 0 |
| 7 | 0 | 2 | 0 | 2 | 0 | 2 | 0 | 2 | 2 | 4 | 2 | 0 | 2 | 0 | 2 | 4 |
| 8 | 0 | 4 | 0 | 4 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 0 | 0 | 0 | 0 |
| 9 | 0 | 2 | 2 | 0 | 2 | 0 | 0 | 2 | 2 | 0 | 0 | 6 | 0 | 2 | 2 | 0 |
| 10 | 0 | 0 | 2 | 2 | 2 | 2 | 4 | 0 | 2 | 2 | 0 | 0 | 0 | 4 | 2 | 2 |
| 11 | 0 | 2 | 0 | 2 | 2 | 4 | 2 | 0 | 2 | 0 | 2 | 0 | 0 | 2 | 4 | 2 |
| 12 | 0 | 0 | 0 | 0 | 2 | 2 | 2 | 2 | 0 | 4 | 4 | 0 | 2 | 2 | 2 | 2 |
| 13 | 0 | 2 | 2 | 0 | 2 | 0 | 0 | 2 | 0 | 2 | 2 | 0 | 6 | 0 | 0 | 2 |
| 14 | 0 | 0 | 6 | 2 | 2 | 2 | 0 | 0 | 0 | 0 | 2 | 2 | 2 | 2 | 0 | 0 |
| 15 | 0 | 2 | 0 | 2 | 2 | 0 | 2 | 0 | 0 | 2 | 4 | 2 | 2 | 0 | 2 | 4 |

## PŘÍLOHA P II. TABULKY LINEÁRNÍ APROXIMACE 3. A 4.SBOXU

Lineární aproximace 3.sboxu

| X\|Y | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 8 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 1 | 0 | 0 | 2 | 2 | 0 | 0 | 2 | 2 | 0 | 4 | 2 | 2 | 4 | 0 | 2 | 2 |
| 2 | 0 | 2 | 2 | 0 | 4 | 2 | 2 | 0 | 2 | 0 | 0 | 2 | 2 | 4 | 0 | 2 |
| 3 | 0 | 2 | 0 | 2 | 4 | 2 | 4 | 2 | 2 | 0 | 2 | 0 | 2 | 0 | 2 | 0 |
| 4 | 0 | 4 | 0 | 0 | 0 | 4 | 0 | 0 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 |
| 5 | 0 | 0 | 2 | 2 | 0 | 0 | 2 | 2 | 2 | 2 | 0 | 4 | 2 | 2 | 4 | 0 |
| 6 | 0 | 2 | 2 | 4 | 0 | 2 | 2 | 0 | 4 | 2 | 2 | 0 | 0 | 2 | 2 | 0 |
| 7 | 0 | 2 | 0 | 2 | 0 | 2 | 0 | 2 | 0 | 2 | 0 | 2 | 0 | 2 | 0 | 6 |
| 8 | 0 | 2 | 4 | 2 | 2 | 0 | 2 | 0 | 2 | 0 | 2 | 0 | 4 | 2 | 0 | 2 |
| 9 | 0 | 2 | 2 | 0 | 2 | 4 | 0 | 2 | 2 | 0 | 4 | 2 | 0 | 2 | 2 | 0 |
| 10 | 0 | 4 | 2 | 2 | 2 | 2 | 4 | 0 | 0 | 0 | 2 | 2 | 2 | 2 | 0 | 0 |
| 11 | 0 | 0 | 0 | 0 | 2 | 2 | 2 | 2 | 4 | 4 | 0 | 0 | 2 | 2 | 2 | 2 |
| 12 | 0 | 2 | 4 | 2 | 2 | 0 | 2 | 4 | 0 | 2 | 0 | 2 | 2 | 0 | 2 | 0 |
| 13 | 0 | 2 | 2 | 0 | 2 | 0 | 0 | 2 | 0 | 2 | 2 | 4 | 2 | 0 | 4 | 2 |
| 14 | 0 | 0 | 2 | 2 | 2 | 2 | 0 | 4 | 2 | 2 | 4 | 0 | 0 | 0 | 2 | 2 |
| 15 | 0 | 0 | 0 | 4 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 0 | 4 | 0 | 0 |

Lineární aproximace 4.sboxu

| X\|Y | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 8 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 1 | 0 | 2 | 2 | 0 | 4 | 2 | 2 | 0 | 2 | 4 | 0 | 2 | 2 | 0 | 0 | 2 |
| 2 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 4 | 0 | 4 | 0 | 4 | 0 | 4 |
| 3 | 0 | 2 | 2 | 0 | 4 | 2 | 2 | 0 | 2 | 0 | 0 | 2 | 2 | 4 | 0 | 2 |
| 4 | 0 | 2 | 0 | 2 | 2 | 0 | 6 | 0 | 2 | 0 | 2 | 0 | 0 | 2 | 0 | 2 |
| 5 | 0 | 0 | 2 | 2 | 2 | 2 | 0 | 0 | 0 | 4 | 2 | 2 | 2 | 2 | 0 | 4 |
| 6 | 0 | 2 | 0 | 2 | 2 | 0 | 2 | 0 | 2 | 4 | 2 | 4 | 0 | 2 | 0 | 2 |
| 7 | 0 | 0 | 6 | 2 | 2 | 2 | 0 | 0 | 0 | 0 | 2 | 2 | 2 | 2 | 0 | 0 |
| 8 | 0 | 2 | 0 | 2 | 2 | 4 | 2 | 4 | 2 | 0 | 2 | 0 | 0 | 2 | 0 | 2 |
| 9 | 0 | 0 | 2 | 2 | 2 | 2 | 0 | 4 | 0 | 0 | 2 | 2 | 2 | 2 | 4 | 0 |
| 10 | 0 | 2 | 0 | 2 | 2 | 0 | 2 | 0 | 2 | 0 | 6 | 0 | 0 | 2 | 0 | 2 |
| 11 | 0 | 4 | 2 | 2 | 2 | 2 | 0 | 0 | 0 | 0 | 2 | 2 | 2 | 2 | 4 | 0 |
| 12 | 0 | 4 | 0 | 4 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 4 | 0 | 4 | 0 |
| 13 | 0 | 2 | 2 | 0 | 0 | 2 | 2 | 0 | 6 | 0 | 0 | 2 | 2 | 0 | 0 | 2 |
| 14 | 0 | 0 | 0 | 0 | 0 | 4 | 0 | 4 | 0 | 0 | 0 | 0 | 4 | 0 | 4 | 0 |
| 15 | 0 | 2 | 2 | 4 | 0 | 2 | 2 | 4 | 2 | 0 | 0 | 2 | 2 | 0 | 0 | 2 |

## PŘÍLOHA P III. TABULKY LINEÁRNÍ APROXIMACE 5. A 6.SBOXU

Lineární aproximace 5.sboxu

| X\|Y | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 8 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 1 | 0 | 2 | 2 | 0 | 0 | 2 | 2 | 0 | 2 | 0 | 0 | 6 | 2 | 0 | 0 | 2 |
| 2 | 0 | 0 | 2 | 2 | 0 | 4 | 2 | 2 | 0 | 0 | 2 | 2 | 0 | 4 | 2 | 2 |
| 3 | 0 | 2 | 0 | 2 | 0 | 2 | 4 | 2 | 2 | 4 | 2 | 0 | 2 | 0 | 2 | 0 |
| 4 | 0 | 0 | 2 | 2 | 4 | 0 | 2 | 2 | 2 | 2 | 4 | 0 | 2 | 2 | 0 | 0 |
| 5 | 0 | 2 | 4 | 2 | 0 | 2 | 4 | 2 | 0 | 2 | 0 | 2 | 0 | 2 | 0 | 2 |
| 6 | 0 | 4 | 0 | 0 | 4 | 0 | 0 | 0 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 |
| 7 | 0 | 2 | 2 | 4 | 0 | 2 | 2 | 0 | 0 | 2 | 2 | 0 | 0 | 2 | 2 | 4 |
| 8 | 0 | 0 | 0 | 0 | 2 | 2 | 2 | 6 | 0 | 0 | 0 | 0 | 2 | 2 | 2 | 2 |
| 9 | 0 | 2 | 2 | 0 | 2 | 0 | 0 | 2 | 2 | 0 | 0 | 2 | 4 | 2 | 2 | 4 |
| 10 | 0 | 0 | 2 | 2 | 2 | 2 | 0 | 0 | 4 | 4 | 2 | 2 | 2 | 2 | 0 | 0 |
| 11 | 0 | 2 | 4 | 2 | 2 | 0 | 2 | 0 | 2 | 0 | 2 | 0 | 0 | 2 | 4 | 2 |
| 12 | 0 | 4 | 2 | 2 | 2 | 2 | 0 | 0 | 2 | 2 | 0 | 0 | 0 | 4 | 2 | 2 |
| 13 | 0 | 2 | 0 | 2 | 2 | 4 | 2 | 0 | 0 | 2 | 4 | 2 | 2 | 0 | 2 | 0 |
| 14 | 0 | 0 | 0 | 4 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 4 | 0 | 0 | 0 |
| 15 | 0 | 2 | 2 | 0 | 2 | 0 | 0 | 2 | 4 | 2 | 2 | 0 | 2 | 0 | 4 | 2 |

Lineární aproximace 6.sboxu

| X\|Y | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 8 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 1 | 0 | 0 | 2 | 2 | 2 | 2 | 0 | 0 | 2 | 2 | 0 | 0 | 0 | 0 | 2 | 6 |
| 2 | 0 | 4 | 4 | 0 | 0 | 4 | 4 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 3 | 0 | 0 | 2 | 2 | 2 | 2 | 0 | 0 | 2 | 2 | 4 | 0 | 0 | 4 | 2 | 2 |
| 4 | 0 | 2 | 0 | 2 | 2 | 0 | 2 | 0 | 2 | 4 | 2 | 4 | 0 | 2 | 0 | 2 |
| 5 | 0 | 2 | 2 | 0 | 4 | 2 | 2 | 0 | 0 | 2 | 2 | 0 | 4 | 2 | 2 | 0 |
| 6 | 0 | 2 | 0 | 2 | 2 | 0 | 2 | 0 | 2 | 4 | 2 | 0 | 4 | 2 | 0 | 2 |
| 7 | 0 | 2 | 2 | 4 | 0 | 2 | 2 | 0 | 0 | 2 | 2 | 4 | 0 | 2 | 2 | 0 |
| 8 | 0 | 0 | 0 | 4 | 4 | 0 | 0 | 0 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 |
| 9 | 0 | 4 | 2 | 2 | 2 | 2 | 0 | 4 | 0 | 0 | 2 | 2 | 2 | 2 | 0 | 0 |
| 10 | 0 | 0 | 4 | 0 | 0 | 4 | 0 | 0 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 |
| 11 | 0 | 0 | 2 | 2 | 2 | 2 | 4 | 4 | 0 | 0 | 2 | 2 | 2 | 2 | 0 | 0 |
| 12 | 0 | 2 | 0 | 2 | 2 | 0 | 2 | 0 | 4 | 2 | 0 | 2 | 2 | 4 | 2 | 0 |
| 13 | 0 | 2 | 2 | 0 | 0 | 2 | 2 | 4 | 2 | 0 | 0 | 2 | 2 | 0 | 4 | 2 |
| 14 | 0 | 2 | 0 | 2 | 2 | 0 | 2 | 0 | 4 | 2 | 4 | 2 | 2 | 0 | 2 | 0 |
| 15 | 0 | 2 | 2 | 0 | 0 | 2 | 2 | 4 | 2 | 0 | 0 | 2 | 2 | 0 | 4 | 2 |

## PŘÍLOHA P IV. TABULKY DIFERENCÍ 1. A 2.SBOXU

Tabulka diferencí 1.sboxu

| X\|Y | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 16 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 1 | 0 | 2 | 0 | 2 | 0 | 0 | 2 | 2 | 0 | 0 | 0 | 0 | 2 | 0 | 4 | 2 |
| 2 | 0 | 2 | 0 | 0 | 0 | 0 | 0 | 2 | 6 | 0 | 0 | 4 | 0 | 0 | 2 | 0 |
| 3 | 0 | 0 | 0 | 0 | 2 | 0 | 4 | 2 | 2 | 2 | 0 | 0 | 0 | 2 | 0 | 2 |
| 4 | 0 | 2 | 0 | 0 | 0 | 4 | 2 | 4 | 0 | 2 | 0 | 0 | 0 | 0 | 2 | 0 |
| 5 | 0 | 0 | 2 | 0 | 2 | 0 | 2 | 2 | 2 | 4 | 0 | 0 | 0 | 0 | 0 | 2 |
| 6 | 0 | 0 | 2 | 0 | 0 | 0 | 2 | 0 | 0 | 2 | 0 | 0 | 0 | 2 | 4 | 4 |
| 7 | 0 | 6 | 0 | 2 | 0 | 0 | 0 | 0 | 2 | 2 | 0 | 0 | 2 | 0 | 0 | 2 |
| 8 | 0 | 0 | 2 | 2 | 4 | 2 | 2 | 0 | 0 | 2 | 0 | 2 | 0 | 0 | 0 | 0 |
| 9 | 0 | 0 | 0 | 0 | 4 | 2 | 0 | 2 | 2 | 0 | 6 | 0 | 0 | 0 | 0 | 0 |
| 10 | 0 | 0 | 2 | 2 | 0 | 0 | 0 | 0 | 2 | 0 | 2 | 0 | 4 | 2 | 2 | 0 |
| 11 | 0 | 0 | 4 | 2 | 2 | 0 | 0 | 0 | 0 | 0 | 0 | 2 | 2 | 0 | 0 | 4 |
| 12 | 0 | 0 | 2 | 4 | 0 | 0 | 0 | 2 | 0 | 0 | 2 | 0 | 2 | 2 | 2 | 0 |
| 13 | 0 | 4 | 2 | 0 | 2 | 0 | 0 | 0 | 0 | 0 | 0 | 2 | 0 | 6 | 0 | 0 |
| 14 | 0 | 0 | 0 | 0 | 0 | 2 | 2 | 0 | 0 | 2 | 0 | 6 | 2 | 2 | 0 | 0 |
| 15 | 0 | 0 | 0 | 2 | 0 | 6 | 0 | 0 | 0 | 0 | 6 | 0 | 2 | 0 | 0 | 0 |

Tabulka diferencí 2.sboxu

| X\|Y | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 16 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 1 | 0 | 2 | 2 | 0 | 2 | 2 | 0 | 0 | 4 | 2 | 0 | 2 | 0 | 0 | 0 | 0 |
| 2 | 0 | 0 | 2 | 4 | 2 | 0 | 0 | 0 | 0 | 0 | 0 | 2 | 0 | 2 | 4 | 0 |
| 3 | 0 | 0 | 0 | 0 | 0 | 0 | 4 | 0 | 0 | 0 | 4 | 4 | 0 | 0 | 0 | 4 |
| 4 | 0 | 0 | 0 | 0 | 2 | 0 | 2 | 8 | 2 | 0 | 2 | 0 | 0 | 0 | 0 | 0 |
| 5 | 0 | 0 | 2 | 2 | 0 | 2 | 2 | 0 | 0 | 0 | 0 | 0 | 2 | 0 | 2 | 4 |
| 6 | 0 | 0 | 0 | 2 | 6 | 0 | 0 | 0 | 2 | 2 | 2 | 0 | 2 | 0 | 0 | 0 |
| 7 | 0 | 2 | 2 | 0 | 0 | 0 | 0 | 0 | 4 | 0 | 0 | 0 | 4 | 2 | 2 | 0 |
| 8 | 0 | 0 | 2 | 2 | 0 | 2 | 4 | 2 | 2 | 0 | 0 | 2 | 0 | 0 | 0 | 0 |
| 9 | 0 | 2 | 2 | 4 | 0 | 0 | 0 | 0 | 0 | 0 | 4 | 0 | 0 | 2 | 2 | 0 |
| 10 | 0 | 2 | 0 | 0 | 0 | 4 | 0 | 2 | 2 | 2 | 0 | 2 | 2 | 0 | 0 | 0 |
| 11 | 0 | 2 | 0 | 2 | 0 | 0 | 0 | 0 | 0 | 4 | 0 | 0 | 2 | 4 | 2 | 0 |
| 12 | 0 | 4 | 0 | 0 | 2 | 2 | 0 | 0 | 0 | 0 | 0 | 0 | 2 | 2 | 0 | 4 |
| 13 | 0 | 0 | 0 | 0 | 2 | 4 | 0 | 2 | 0 | 2 | 2 | 0 | 0 | 4 | 0 | 0 |
| 14 | 0 | 2 | 4 | 0 | 0 | 0 | 2 | 0 | 0 | 0 | 0 | 2 | 2 | 0 | 0 | 4 |
| 15 | 0 | 0 | 0 | 0 | 0 | 0 | 2 | 2 | 0 | 4 | 2 | 2 | 0 | 0 | 4 | 0 |

## PŘÍLOHA P V. TABULKY DIFERENCÍ 3. A 4.SBOXU

Tabulka diferencí 3.sboxu

| X\|Y | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 16 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 1 | 0 | 2 | 2 | 0 | 2 | 2 | 0 | 0 | 4 | 0 | 0 | 0 | 2 | 0 | 2 | 0 |
| 2 | 0 | 2 | 0 | 0 | 2 | 0 | 0 | 0 | 0 | 0 | 2 | 0 | 2 | 6 | 2 | 0 |
| 3 | 0 | 0 | 2 | 2 | 0 | 2 | 2 | 0 | 2 | 2 | 0 | 0 | 2 | 0 | 0 | 2 |
| 4 | 0 | 4 | 4 | 0 | 0 | 0 | 0 | 0 | 2 | 2 | 0 | 0 | 0 | 0 | 2 | 2 |
| 5 | 0 | 0 | 0 | 2 | 0 | 0 | 0 | 2 | 0 | 4 | 2 | 0 | 4 | 0 | 2 | 0 |
| 6 | 0 | 0 | 0 | 2 | 2 | 4 | 0 | 0 | 0 | 0 | 0 | 2 | 2 | 0 | 0 | 4 |
| 7 | 0 | 4 | 0 | 2 | 2 | 0 | 2 | 2 | 0 | 0 | 0 | 2 | 0 | 2 | 0 | 0 |
| 8 | 0 | 0 | 2 | 2 | 0 | 0 | 2 | 2 | 0 | 2 | 2 | 0 | 2 | 0 | 0 | 2 |
| 9 | 0 | 0 | 4 | 0 | 2 | 2 | 0 | 4 | 0 | 0 | 2 | 2 | 0 | 0 | 0 | 0 |
| 10 | 0 | 0 | 2 | 0 | 2 | 0 | 2 | 2 | 0 | 0 | 0 | 2 | 0 | 2 | 2 | 2 |
| 11 | 0 | 0 | 0 | 0 | 0 | 2 | 2 | 0 | 2 | 0 | 6 | 0 | 0 | 0 | 2 | 2 |
| 12 | 0 | 2 | 0 | 2 | 0 | 0 | 0 | 0 | 2 | 2 | 0 | 4 | 0 | 2 | 2 | 0 |
| 13 | 0 | 0 | 0 | 2 | 0 | 4 | 2 | 0 | 0 | 2 | 2 | 2 | 0 | 2 | 0 | 0 |
| 14 | 0 | 0 | 0 | 2 | 2 | 0 | 4 | 0 | 0 | 2 | 0 | 0 | 2 | 2 | 0 | 2 |
| 15 | 0 | 2 | 0 | 0 | 2 | 0 | 0 | 4 | 4 | 0 | 0 | 2 | 0 | 0 | 2 | 0 |

Tabulka diferencí 4.sboxu

| X\|Y | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 16 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 1 | 0 | 0 | 0 | 0 | 0 | 0 | 2 | 2 | 0 | 0 | 2 | 2 | 0 | 0 | 4 | 4 |
| 2 | 0 | 2 | 2 | 2 | 0 | 0 | 4 | 2 | 2 | 0 | 0 | 0 | 0 | 0 | 0 | 2 |
| 3 | 0 | 2 | 0 | 0 | 0 | 0 | 0 | 2 | 6 | 0 | 0 | 0 | 4 | 0 | 2 | 0 |
| 4 | 0 | 0 | 2 | 0 | 0 | 2 | 0 | 0 | 0 | 2 | 4 | 4 | 0 | 0 | 2 | 0 |
| 5 | 0 | 0 | 0 | 2 | 4 | 6 | 0 | 0 | 0 | 2 | 0 | 0 | 0 | 0 | 0 | 2 |
| 6 | 0 | 0 | 0 | 2 | 0 | 2 | 0 | 0 | 4 | 0 | 0 | 2 | 0 | 6 | 0 | 0 |
| 7 | 0 | 0 | 4 | 2 | 0 | 2 | 2 | 2 | 0 | 0 | 2 | 0 | 0 | 2 | 0 | 0 |
| 8 | 0 | 0 | 2 | 0 | 2 | 0 | 0 | 0 | 0 | 10 | 0 | 0 | 0 | 0 | 0 | 2 |
| 9 | 0 | 0 | 0 | 2 | 2 | 0 | 4 | 4 | 0 | 2 | 0 | 0 | 0 | 0 | 2 | 0 |
| 10 | 0 | 2 | 0 | 0 | 0 | 0 | 2 | 0 | 2 | 0 | 2 | 2 | 0 | 0 | 2 | 4 |
| 11 | 0 | 6 | 0 | 0 | 0 | 4 | 0 | 2 | 2 | 0 | 0 | 0 | 0 | 0 | 2 | 0 |
| 12 | 0 | 0 | 4 | 4 | 0 | 0 | 2 | 2 | 0 | 0 | 0 | 0 | 2 | 2 | 0 | 0 |
| 13 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 2 | 2 | 6 | 6 | 0 | 0 |
| 14 | 0 | 4 | 2 | 0 | 6 | 0 | 0 | 0 | 0 | 0 | 2 | 0 | 2 | 0 | 0 | 0 |
| 15 | 0 | 0 | 0 | 2 | 2 | 0 | 0 | 0 | 0 | 0 | 2 | 4 | 2 | 0 | 2 | 2 |

## PŘÍLOHA P VI. TABULKY DIFERENCÍ 5. A 6.SBOXU

Tabulka diferencí 5.sboxu

| X\|Y | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 16 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 1 | 0 | 0 | 4 | 2 | 0 | 2 | 0 | 0 | 2 | 0 | 0 | 4 | 0 | 0 | 2 | 0 |
| 2 | 0 | 0 | 0 | 2 | 0 | 2 | 0 | 0 | 2 | 2 | 2 | 0 | 0 | 2 | 4 | 0 |
| 3 | 0 | 2 | 0 | 0 | 0 | 2 | 4 | 0 | 2 | 0 | 0 | 4 | 2 | 0 | 0 | 0 |
| 4 | 0 | 0 | 0 | 2 | 0 | 2 | 2 | 2 | 0 | 2 | 0 | 0 | 0 | 4 | 2 | 0 |
| 5 | 0 | 0 | 0 | 0 | 0 | 4 | 2 | 2 | 2 | 0 | 0 | 2 | 0 | 2 | 0 | 2 |
| 6 | 0 | 0 | 0 | 6 | 0 | 0 | 2 | 0 | 0 | 0 | 2 | 0 | 2 | 2 | 2 | 0 |
| 7 | 0 | 2 | 0 | 0 | 0 | 0 | 2 | 0 | 4 | 0 | 0 | 2 | 0 | 2 | 2 | 2 |
| 8 | 0 | 0 | 0 | 0 | 2 | 0 | 0 | 2 | 2 | 4 | 2 | 0 | 0 | 0 | 2 | 2 |
| 9 | 0 | 4 | 2 | 0 | 0 | 2 | 0 | 0 | 0 | 0 | 4 | 2 | 2 | 0 | 0 | 0 |
| 10 | 0 | 4 | 0 | 2 | 4 | 0 | 0 | 2 | 0 | 2 | 0 | 0 | 0 | 2 | 0 | 0 |
| 11 | 0 | 2 | 2 | 2 | 2 | 0 | 0 | 0 | 0 | 0 | 0 | 2 | 0 | 0 | 0 | 6 |
| 12 | 0 | 0 | 2 | 0 | 2 | 0 | 0 | 4 | 0 | 0 | 2 | 0 | 0 | 2 | 2 | 2 |
| 13 | 0 | 0 | 0 | 0 | 0 | 2 | 0 | 2 | 2 | 2 | 0 | 0 | 6 | 0 | 0 | 2 |
| 14 | 0 | 0 | 2 | 0 | 4 | 0 | 0 | 2 | 0 | 2 | 4 | 0 | 2 | 0 | 0 | 0 |
| 15 | 0 | 2 | 4 | 0 | 2 | 0 | 4 | 0 | 0 | 2 | 0 | 0 | 2 | 0 | 0 | 0 |

Tabulka diferencí 6.sboxu

| X\|Y | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 16 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 1 | 0 | 2 | 4 | 0 | 4 | 0 | 0 | 2 | 0 | 2 | 0 | 0 | 0 | 0 | 0 | 2 |
| 2 | 0 | 0 | 2 | 4 | 0 | 0 | 2 | 0 | 0 | 2 | 2 | 2 | 2 | 0 | 0 | 0 |
| 3 | 0 | 0 | 0 | 2 | 2 | 0 | 0 | 4 | 0 | 2 | 0 | 4 | 0 | 0 | 2 | 0 |
| 4 | 0 | 0 | 0 | 0 | 0 | 4 | 0 | 0 | 4 | 2 | 2 | 0 | 2 | 0 | 0 | 2 |
| 5 | 0 | 2 | 0 | 0 | 0 | 0 | 0 | 2 | 4 | 0 | 2 | 0 | 2 | 4 | 0 | 0 |
| 6 | 0 | 0 | 0 | 4 | 2 | 0 | 2 | 0 | 0 | 0 | 2 | 2 | 2 | 0 | 0 | 2 |
| 7 | 0 | 4 | 2 | 2 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 4 | 0 | 0 | 2 | 2 |
| 8 | 0 | 0 | 2 | 0 | 2 | 0 | 0 | 0 | 0 | 4 | 2 | 0 | 2 | 0 | 0 | 4 |
| 9 | 0 | 0 | 0 | 0 | 0 | 0 | 4 | 0 | 4 | 0 | 0 | 0 | 0 | 4 | 4 | 0 |
| 10 | 0 | 2 | 0 | 2 | 0 | 2 | 2 | 0 | 0 | 2 | 2 | 0 | 0 | 2 | 0 | 2 |
| 11 | 0 | 0 | 0 | 0 | 4 | 2 | 0 | 2 | 0 | 0 | 2 | 2 | 0 | 2 | 2 | 0 |
| 12 | 0 | 2 | 0 | 0 | 0 | 4 | 4 | 2 | 0 | 0 | 2 | 0 | 2 | 0 | 0 | 0 |
| 13 | 0 | 2 | 2 | 0 | 2 | 0 | 0 | 2 | 4 | 0 | 0 | 0 | 0 | 0 | 4 | 0 |
| 14 | 0 | 0 | 0 | 2 | 0 | 2 | 2 | 2 | 0 | 2 | 0 | 0 | 2 | 2 | 0 | 2 |
| 15 | 0 | 2 | 4 | 0 | 0 | 2 | 0 | 0 | 0 | 0 | 0 | 2 | 2 | 2 | 2 | 0 |

## PŘÍLOHA P VII. POUŽITÉ ROVNICE LINEÁRNÍ KRYPTOANALÝZY

| tabulka | sbox | Rovnice |
|---|---|---|
| 9.4 | 010000 | $P[1,2] \oplus C[6], P[22] \oplus C[5], P[22] \oplus C[6], P[4,5,7,13,14,15] \oplus C[5], P[4,5,7,22] \oplus C[4]$ |
| 9.4 | 001000 | $P[12] \oplus C[10], P[12] \oplus C[8], P[16,18] \oplus C[8,10], P[4,5,7,22] \oplus C[9]$ |
| 9.4 | 000100 | $P[1,2] \oplus C[13], P[22] \oplus C[13], P[4,5,7,22] \oplus C[14]$ |
| 9.4 | 000010 | $P[12] \oplus C[17], P[13,14,15] \oplus C[16], P[17,18] \oplus C[17], P[4,5,7,22] \oplus C[16], P[9,10] \oplus C[18]$ |
| 9.4 | 000001 | $P[12] \oplus C[20], P[17] \oplus C[23], P[21,23] \oplus C[23]$ |
| 9.6 | 101000 | $P[4,5,7,22] \oplus C[0,11], P[4,5,7,22] \oplus C[2,9]$ |
| 9.7 | 010001 | $P[22] \oplus C[5,21,22], P[22] \oplus C[5,21], P[4,5,7,13,14,15] \oplus C[5,21,22]$ |
| 9.9 | 000110 | $P[22] \oplus C[12,16]$ |
| 9.9 | 000101 | $P[22] \oplus C[13,15,23], P[21,23] \oplus C[15,23]$ |
| 9.10 | 100000 | $P[4,5,6] \oplus C[0], P[4,5,6] \oplus C[2], P[17] \oplus C[1], P[9,10] \oplus C[2], P[21,23] \oplus C[1]$ |
| 9.10 | 010000 | $P[13,14,15] \oplus C[6], P[4,5,7] \oplus C[5], P[4,5,6] \oplus C[4], P[5] \oplus C[5], P[7] \oplus C[6]$ |
| 9.10 | 001000 | $P[4,5,6] \oplus C[9], P[9] \oplus C[8], P[12] \oplus C[8,10]$ |
| 9.10 | 000100 | $P[12] \oplus C[13], P[4,5,6] \oplus C[14], P[11] \oplus C[13]$ |
| 9.10 | 000010 | $P[17] \oplus C[18], P[9] \oplus C[17], P[4,5,6] \oplus C[16]$ |
| 9.10 | 000001 | $P[9] \oplus C[20], P[1,3] \oplus C[23]$ |
| 9.11 | 000101 | $P[11] \oplus C[15,23], P[1,3] \oplus C[15,23]$ |
| 9.12 | 100000 | $P[22] \oplus C[0], P[1,3] \oplus C[1], P[22] \oplus C[2], P[17,18] \oplus C[2]$ |
| 9.12 | 010000 | $P[5] \oplus C[5], P[22] \oplus C[4], P[7] \oplus C[6]$ |
| 9.12 | 001000 | $P[17] \oplus C[10], P[17] \oplus C[8], P[22] \oplus C[9], P[9] \oplus C[8,10]$ |
| 9.12 | 000100 | $P[17,19] \oplus C[13], P[9] \oplus C[13], P[22] \oplus C[14]$ |
| 9.12 | 000010 | $P[22] \oplus C[16], P[2] \oplus C[18], P[16,18] \oplus C[17]$ |
| 9.12 | 000001 | $P[17] \oplus C[20], P[15] \oplus C[23]$ |

## PŘÍLOHA P VIII. POUŽITÉ ROVNICE DIFERENCIÁLNÍ KRYPTOANALÝZY

| tabulka | sbox | Rovnice |
|---|---|---|
| 10.2 | 100000 | $P[21] \oplus C[0], P[21,22,23] \oplus C[3], P[14,15] \oplus C[2], P[0,3] \oplus C[0]$ |
| 10.2 | 010000 | $P[23] \oplus C[7], P[11] \oplus C[6], P[11] \oplus C[7]$ |
| 10.2 | 001000 | $P[23] \oplus C[10], P[11] \oplus C[8,10], P[0,3] \oplus C[11]$ |
| 10.2 | 000100 | $P[23] \oplus C[13], P[16,19] \oplus C[13], P[16,18] \oplus C[12], P[4,5] \oplus C[14], P[0] \oplus C[12]$ |
| 10.2 | 000010 | $P[0,1,2] \oplus C[18], P[0,1,2] \oplus C[17], P[19] \oplus C[18,19], P[21,22,23] \oplus C[16], P[1,2,3] \oplus C[18,19], P[0] \oplus C[16]$ |
| 10.2 | 000001 | $P[23] \oplus C[23], P[0] \oplus C[23]$ |
| 10.3 | 100000 | $P[23] \oplus C[2], P[7] \oplus C[3], P[13,14,15] \oplus C[0], P[12,13,14] \oplus C[0]$ |
| 10.3 | 010000 | $P[11] \oplus C[7], P[19] \oplus C[7], P[19] \oplus C[6]$ |
| 10.3 | 001000 | $P[11] \oplus C[10], P[19] \oplus C[8,10], P[12,13,14] \oplus C[11]$ |
| 10.3 | 000100 | $P[11] \oplus C[13], P[2] \oplus C[12], P[1,2,3] \oplus C[12], P[21] \oplus C[14]$ |
| 10.3 | 000010 | $P[4,5,6] \oplus C[16], P[16,18] \oplus C[18,19], P[13,15,23] \oplus C[17], P[13,15,23] \oplus C[18], P[1,2,3] \oplus C[16], P[23] \oplus C[18,19]$ |
| 10.3 | 000001 | $P[11] \oplus C[23], P[1,2,3] \oplus C[23]$ |
| 10.4 | 100100 | $P[6] \oplus C[3,13,15]$ |
| 10.6 | 100000 | $P[11] \oplus C[0], P[11] \oplus C[2], P[7] \oplus C[0], P[6] \oplus C[3]$ |
| 10.2 | 100000 | $P[16,18] \oplus C[7], P[17,18,19] \oplus C[6], P[19] \oplus C[7]$ |
| 10.6 | 001000 | $P[11] \oplus C[11], P[16,18] \oplus C[8,10], P[19] \oplus C[10]$ |
| 10.6 | 000100 | $P[23] \oplus C[12], P[19] \oplus C[13], P[13,14,15] \oplus C[14], P[13,15] \oplus C[12]$ |
| 10.6 | 000010 | $P[8,10,11] \oplus C[17], P[8,10,11] \oplus C[18], P[23] \oplus C[16], P[0,1,2] \oplus C[18,19]$ |
| 10.6 | 000001 | $P[19] \oplus C[23], P[23] \oplus C[23]$ |
| 10.7 | 100000 | $P[10] \oplus C[0], P[10] \oplus C[2]$ |