Návrh polymorfních struktur v symetrické kryptografii

Ing. Petr Žáček, Ph.D.

Teze disertační práce

Univerzita Tomáše Bati ve Zlíně

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Teze disertační práce

Návrh polymorfních struktur v symetrické kryptografii

Design of the Polymorphous Structures in the Symmetric Cryptography

Autor: **Ing. Petr Žáček, Ph.D.**

Studijní program: Inženýrská informatika (P3902)
Studijní obor: Inženýrská informatika (3902V023)

Školitel: prof. Mgr. Roman Jašek, Ph.D., DBA
Konzultant: Ing. David Malaník, Ph.D.

Oponenti: doc. RNDr. Martin Kotyrba, Ph.D.
doc. Dr. Ing. Oldřich Kodym
prof. Ing. Ivan Zelinka, Ph.D.

Zlín, Květen 2021

Vydala **Univerzita Tomáše Bati ve Zlíně** v edici **Doctoral Thesis Summary.**

Publikace byla vydána v roce 2021.

Klíčová slova: *kryptologie, symetrická kryptografie, kryptografický systém, blokové šifra, režim činnosti blokových šifer, šifrovací funkce, runda, délka bloku, délka klíče, polymorfismus.*

Key words: *cryptology, symmetric-key cryptography, cryptography system, block cipher, block cipher mode of operation, encryption function, round, block length, key length, polymorphism.*

Práce je dostupná v Knihovně UTB ve Zlíně.

ISBN 978-80-7678-034-7

ABSTRAKT

Disertační práce se věnuje polymorfním strukturám v symetrické kryptografii. Součástí textu je přehled zabývající se symetrickou kryptografií blokových šifer a aktuálnímu stavu dané problematiky. Mezi hlavní cíle patří vymezení termínu polymorfních struktur v symetrické kryptografii, uvedení příkladů stávajících algoritmů a šifrovacích principů na základě vymezení.

Práce je dále souborem výsledků, kterých bylo dosaženo v rámci doktorského studia a navrhuje jednotný šifrovací systém založený na rozebraných principech s důrazem na polymorfní struktury.

Celkové řešení obsahuje i praktickou implementaci všech navržených struktur v komplexní polymorfní šifrovací systém s ukázkou fungování. Práce dále prezentuje zhodnocení kvality návrhu včetně otestování systému.

ABSTRACT

The disertation is focused on polymorphous structures in symmetric cryptography. The text includes an overview of symmetric cryptography of block ciphers and the actual state of that field. The main objectives are definition of the term polymorphic structures in symmetric cryptography, introducing examples of existing algorithms and principles based on definition.

The work is further a set of results achieved under Doctoral Study and proposes a single encryption system based on describes and designed principles with emphasis to the polymorphic structures.

The overal solution also includes the practical show of implementation of all proposed structures in a comprehensive polymorphous cryptographic system with a demonstration of functioning. The work further presents an evaluation of the design quality, including the testing of the system.

OBSAH

ÚVOD

Většina hlavních zástupců blokových šifer (viz kapitola 4 disertační práce) má společnou jednu vlastnost, a to statické algoritmy. Jejich bezpečnost je postavena výhradně na vstupním klíči, případně na vstupních datech v závislosti na situaci použití režimů činnosti. Princip činnosti, struktura a další parametry zůstávají během celého procesu šifrování neměnné. Existuje však několik výjimek mezi zástupci blokových šifer, které jsou rozvedeny podrobněji v rámci textu disertační práce v kapitole 4.

Výše uvedené důvody posloužily jako hlavní motivace pro tvorbu nové polymorfního kryptografického systému, který by byl vhodnou alternativou ke stávajícím šifrám/systémům. Hlavním cílem disertační práce byla tvorba kryptografického systému, u kterého by nebylo předem možné určit strukturu šifrování nebo její parametry bez znalosti vstupních dat nebo nastavení uživatele → šifrovacího klíče. Systému, kde by všechny aspekty byly založeny na závislostech jednotlivých části odvíjejících se od vstupních dat, parametrů a klíče. Navíc kde by se i proces šifrování a parametry pro šifrování následujících bloků odvíjel od aktuálního průběhu.

Výsledný návrh rozepsaný v disertační práci tyto vlastnosti splňuje a rozšiřuje o využití náhodných dat, kdy dochází ke změně systému v závislosti na jeho spuštění. A to bez nutnost změny uživatelského vstupu. Výsledkem disertační práce je navržený ucelený kryptografický systém TSS s náhodně polymorfním chováním.

1 CÍLE DISERTAČNÍ PRÁCE

Hlavním cílem disertační práce je výzkum v oblasti symetrické kryptografie blokových šifer a následný návrh vlastního komplexního kryptografického systému na základě tvorby jeho dílčích částí. Samotný návrh by měl být řešen v souladu s principem polymorfních struktur. To znamená volbu vhodných parametrů a částí kryptografického systému blokových šifer a jejich následnou modifikaci tak, aby chování výsledného systému bylo polymorfní. To celé při zachování základní filozofie kryptologie, že žádný algoritmus by neměl být tajný, ale jeho bezpečnost je současně matematicky podložená.

Součástí disertační práce bude také praktická implementace polymorfního kryptografického systému, který bude v co nejvyšší míře závislý na polymorfním chování – označený Smallie (ve variantě Triply Salted Smallie). Proto v rámci disertační práce bude vytvořených systém označen zkratkou TSS. Systém, který bude vytvořen z navržených jednotlivých části, jako výsledek dílčích cílů disertační práce. Bude provedena implementace a otestování v jazyce Python 3.x.

1.1 Dílčí cíle disertační práce

Cíle disertační práce lze rozdělit následovně:

1. Nastudování teoretického základu pro tvorbu blokových šifer a analýzu aktuálního stavu na poli polymorfních struktur v symetrické kryptografii.
2. Výběr parametrů, operací a vlastností blokových šifer vhodných pro polymorfizaci.
3. Návrh vlastního způsobu polymorfizace vybraných parametrů, operací a vlastností.
4. Praktická implementace polymorfních struktur v symetrické kryptografii (vlastní kryptografický systém TSS).
5. Analýza a případná optimalizace navržených a implementovaných polymorfních struktur z hlediska bezpečnosti.
6. Zhodnocení výsledků a popis budoucího výzkumu, či aplikaci v praxi.

2 SOUČASNÝ STAV ŘEŠENÉ PROBLEMATIKY

Následující kapitola je věnována současnému stavu problematiky kryptografii blokových šifer a struktur.

2.1 Fixní versus „polymorfní“

Z definice (popisu) v rámci kapitoly 4.1 disertační práce můžeme odvodit, že blokové šifry můžeme rozdělit do následujících kategorií:

- Klasické šifry s fixní strukturou (většina algoritmů)
- Polymorfní šifry s proměnlivými strukturami

V následujících částech si tyto dvě kategorie rozebereme a ukážeme si jejich zástupce.

2.2 Shrnutí současného stavu řešené problematiky

Na základě výše popsaného lze současný stav řešené problematiky shrnout následovně.

Existuje celá řada algoritmů v oblasti kryptografie blokových šifer, která je prakticky využívána. S tím existují režimy činnosti, algoritmy pro odvození klíčů a nespočet praktických implementací v kryptografické nástroje, systémy a protokoly. Nicméně drtivá většina z nich má fixní → časově či parametrově nezávislé chování, strukturu a průběh.

Existují i zástupci algoritmů, které lze alespoň částečně zařadit mezi polymorfní. Každopádně se jedná pouze o částečnou polymorfizaci.

Dále lze narazit i na komplexněji polymorfní systémy či teorie, které ovšem nenašli praktického uplatnění či aplikace.

Rozhodně lze říci, že problematika polymorfních struktur, nejen v oblasti symetrické kryptografie, by zasluhovala hlubší pozornost a výzkum. Lze se jen domnívat, proč tomu tak není, kdy jeden z možných důvodů je velmi obtížná (až nereálná) analýza těchto systémů/algoritmů. Což znemožňuje potvrzení bezpečnosti či standardizaci.

V porovnání se systémem TSS, který je navržen v disertační práci, tak nebylo možné dohledat systém, který by principy polymorfnosti využíval v takové míře. Systém, který ve svém komplexním návrhu kombinuje všechny prostředky nutné pro postavení kryptografického systému včetně šifrovacího jádra → polymorfní blokové šifry.

Další informace a podrobnosti o řešené problematice je možné dohledat v rámci podkapitol kapitoly 4 v textu disertační práce.

3 ZÁKLADNÍ MYŠLENKA VYBUDOVÁNÍ POLYMORFNÍHO ŠIFROVACÍHO SYSTÉMU

V rámci této kapitoly je rozebrána základní myšlenka pro vybudování polymorfního šifrovacího systému. Rozebírání možnosti a způsoby, jakými by bylo možné transformovat blokové šifry v polymorfní. V rámci kapitoly jsou vybrány jednotlivé části blokových šifer, které budou následně upraveny a změněny na polymorfní struktury.

Jak už bylo uvedeno výše, v rámci moderní kryptologie se využívají nebo byly navrženy algoritmy, které jsou výhradně navrženy tak, že celý průběh šifrování je znám a jediná tajná informace je šifrovací klíč. Tento fakt vychází ze základní myšlenky, že algoritmus musí být veřejný. Bez pochyby se jedná o validní a velmi důležitý faktor, který je potřebné dodržet, jak se ukázalo v minulosti. Jedná se o problematiku „Security through obscurity“, problematika rozebrána výše, v rámci kapitoly 2.4.1. Odborná komunita se výhradně shodne, že šifrovací systém by měl být založen na matematických principem s ohledem na otevřenost systému. Neměl by spoléhat pouze na utajení algoritmu šifrovacího systému. Nicméně, pokud se systém navržen na matematických principech, lze v tomto případě ještě doplnit bezpečnost o neveřejnost algoritmu. To ovšem za předpokladu, že je algoritmus dostatečně bezpečný a byl podroben kvalitní kryptoanalýze. V opačném případě je jeho veřejnost výhodou z důvodu, že

komunita, uživatelé a kryptoanalytici mají možnost provést testování těchto šifrovacích systémů. Protože jakákoliv chyba může být odhalena kýmkoliv a vzápětí odstraněna/opravena. Celkově nelze nikdy vyloučit absenci chyb v rámci systému, ale můžeme tvrdit, že pokud byl systém podroben více testů, bez nalezeného bezpečnostního problému, tak jej lze považovat za bezpečnější.

Z výše uvedených podmínek je právě šifra AES natolik oblíbená a i využívaná, protože bylo provedeno nespočet pokusů o prolomení. Nespočet vědeckých prací se zabýval její kryptoanalýzu a doposud nebyl nalezen žádný efektivní způsob na prolomení či snížení bezpečnosti této šifry. Lze uvést i příklad z jiné oblasti – zobecněná teorie relativity je čím dál více potvrzována pokusy vědců a jejich snahami o její vyvrácení. Tím můžeme říct, že jakýkoliv negativní pokus o prolomení šifry je zároveň vhodný prostředek pro potvrzení bezpečnosti.

Výhoda otevřenosti šifrovacího systému je nezpochybnitelná a v rámci této disertační práce je navržen kryptografický systém, který je v souladu s tímto pravidlem. Nicméně, tato disertační práce se snaží tuto problematiku prohloubit a rozšířit o následující možnost; konkrétně o návrh systému, který by ve své podstatě byl otevřený, veřejný a postaven na matematických principech. Zároveň aby jeho šifrovací proces byl tajný stejně jako využití tajného šifrovacího klíče. Navržený systém tedy je vybudován na známých operacích a má veřejnou podobu, ale konkrétní nastavení a vlastnosti se budou měnit spolu se vstupními podmínkami. Můžeme tedy mluvit o tom, že celkový proces šifrování, včetně parametrů a vlastností šifrovacího systému, se polymorfně mění v závislosti na změnách počátečních/aktuálních hodnot v rámci systému. Výsledkem je šifrovací systém, který kombinuje výhody otevřenosti systému, ale zároveň jeho konkrétní průběh je proměnlivý. Bez nadsázky můžeme říci, že vytvořený kryptografický systém v sobě zahrnuje složku t – čas. Neboli při každém šifrování se průběh a jednotlivé parametry mění v závislosti na čase, i když nedojde ke změně vstupních dat/otevřeného textu nebo klíče/klíčového souboru.

V rámci disertační práce byl vybudován kompletní systém, který je na základě uživatelských vstupních parametrů nastaven a inicializován pro šifrování prvního bloku dat a následně je před šifrováním dalšího bloku dat na základě aktuální parametrů modifikován a upraven. Návrh je proveden tak, aby šifrování aktuálního bloku dat bylo neznámé, a to bez znalosti vstupních parametrů a klíče. Celkově, aby před samotným šifrováním nebylo známé, za jakých podmínek a parametrů je šifrování prováděno. Proces a parametry jsou tak v maximální míře závislé na tajném klíči, ale i na dalších parametrech, jako jsou náhodná vstupní data či otevřená data.

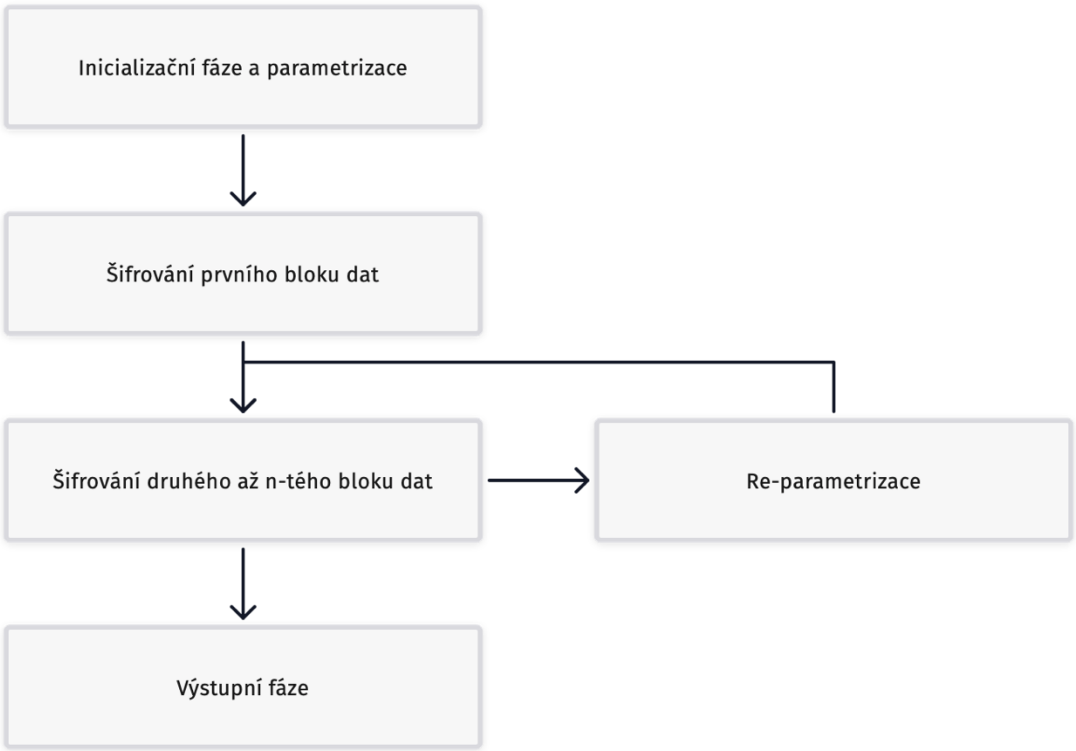
Pro navržený kryptografický systém bylo vymyšlené kódové označení TSS, kdy nejnovější verze nese název s adaptací – „Triply Salted Smallie“ („Trojitě nasolené Smallie). V rámci disertační práce je rozepsána hlavně verze „Triply Salted Smallie“. Jedná se o variantu, kdy v rámci solení bylo využito tří samostatně generovaných solí.

Volba vlastností a parametrů je rozebrána podrobně v rámci kapitoly 5.2 disertační práce.

4 VYTVOŘENÝ KRYPTOGRAFICKÝ SYSTÉM - TSS

Tato kapitola pojednává o vytvořeném polymorfním kryptografickém systému. Systém byl navržen v souladu s popisem výše. Tvorba systému probíhala v několika fázích a systém byl několikrát upraven a vylepšen. Kapitola popisuje a ukazuje finální návrh. Systém je i částečně postaven na základě šifrovacího jádra diplomové práce autora [1], kdy bylo zmíněné šifrovací jádro upraveno a vylepšeno. Jednotlivým částem systému a jejich popisu se věnuje text v podkapitolách.

V základu jde výsledný polymorfně založený šifrovací systém znázornit následujícím diagramem.



Obrázek 1 - Schéma polymorfního kryptografického systému – TSS

Na základě výše zobrazeného schématu lze průběh šifrování pomocí výsledného šifrovacího systému rozdělit na pět základních částí. Jednotlivé části budou blíže popsané v následujících kapitolách.

Jedná se o části:

1. Inicializace a první parametrizace.
2. Šifrování prvního bloku dat.
3. Re-parametrizace – příprava klíče a parametrů pro šifrování dalšího bloku.
4. Šifrování dalších bloků otevřeného textu.
5. Výstupní fáze – tvorba finálního šifrového textu.

Je důležité poznamenat, že šifrování prvního nebo jakéhokoliv dalšího bloku probíhá stejně (aplikování šifrovacího jádra/nosné šifrovací funkce), ale každý blok je šifrován/dešifrován za pomocí jiného klíče a na základě jiných parametrů a dochází k adaptaci šifrovacího jádra na základě předchozích podmínek/parametrů. Rozdíl je v prvotní parametrizaci a pak následné re-parametrizaci mezi šifrováním dalších bloků.

V rámci dešifrování se postupuje prakticky stejně, akorát rozdíl je v inicializační fázi a parametrizaci a dále ve výstupní fázi. Hlavní rozdílem je manipulace se solemi a úprava otevřeného/šifrového textu. V případě šifrování se soli používají na „předsolení“ a „zasolení“ – připojení k otevřenému textu zepředu a zezadu.

Tyto soli jsou dále šifrovány, takže v rámci dešifrování je možné „odsolení“ – odstranění soli zepředu a zezadu až po dešifrování všech dat. Obdobně je to se solí, která slouží k „nasolení“ inicializačního vektoru. Při šifrování dochází v závěrečné fázi k vmísení soli pro „nasolení“ to výsledného šifrového textu na základě pravidel inicializačního vektoru a parametrů. Při dešifrování je ale nutné ještě před započetím dešifrování patřičnou sůl pro „nasolení“ získat ze šifrového textu, což probíhá opět na základě inicializačního vektoru a parametrů.

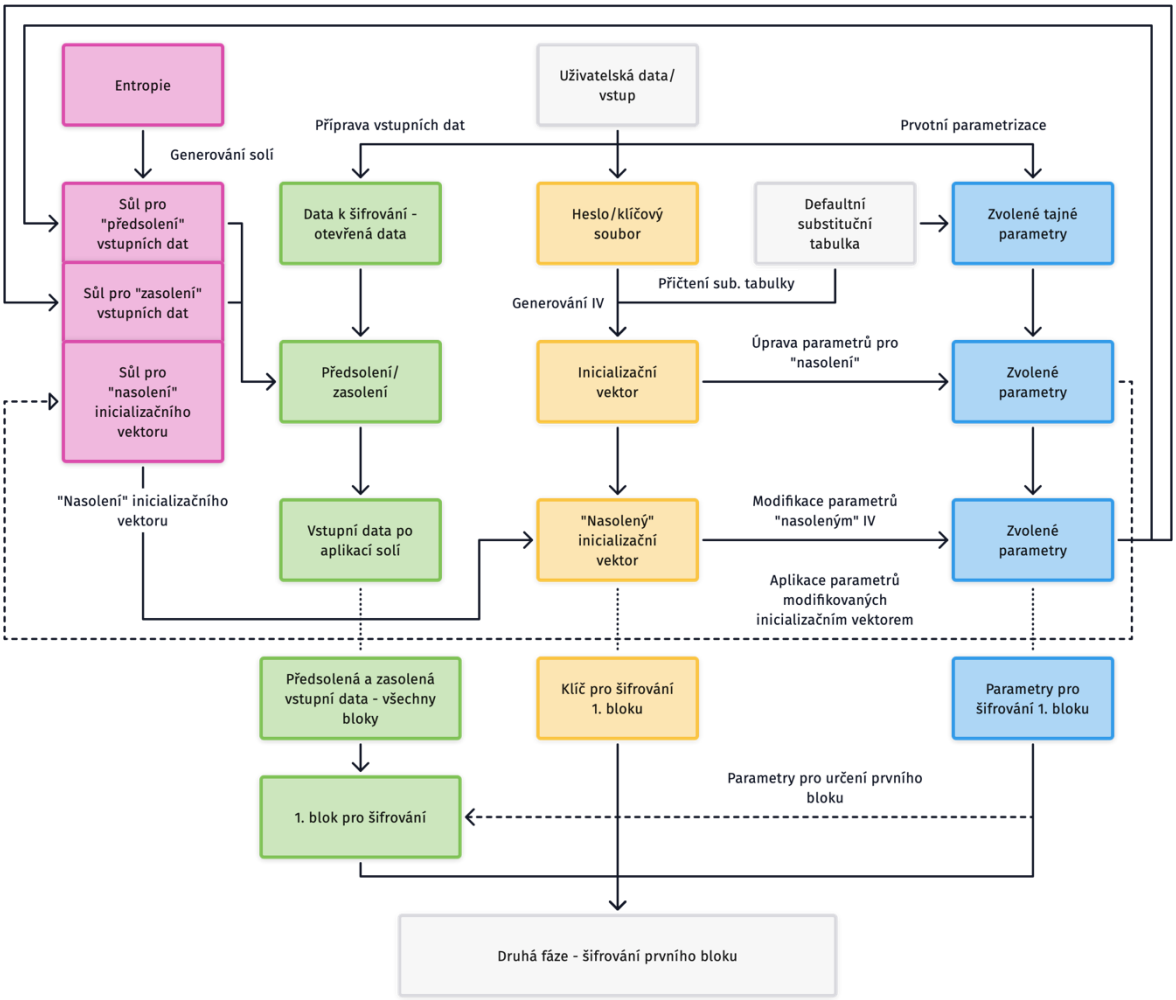
4.1 První část – inicializace fáze a úvodní parametrizace

V rámci první fáze dochází k následujícím krokům:

1. Získání vstupních dat od uživatele – otevřená data
2. Získání parametrů od uživatele – tajné nastavení vstupních parametrů

3. Získání dat pro potřeby vygenerování prvního šifrovacího klíče – inicializačního vektoru
4. Sběr entropie a generování náhodných dat – modifikace parametrů a inicializačního vektoru

Proces lze znázornit pomocí následujícího diagramu.



Obrázek 2 - Schéma fáze první - příprava na šifrování prvního bloku dat

Výsledkem je zpracování uživatelského vstupu pro určení:

- Prvního blok data pro šifrování
- Klíče pro šifrování prvního bloku dat
- Parametrů pro šifrování prvního bloku dat (zahrnující substituční tabulku)

Jednotlivé fáze a části jsou pro přehlednost barevně odlišeny:

- Růžová barva reprezentuje sběr entropie a přípravu solí pro „předsolení“, „zasolení“ a „nasolení“ vstupních dat, konkrétní postup „předsolení“, „zasolení“ a „nasolení“ je rozveden v kapitole 7.4.
- Zelená barva reprezentuje postup manipulace se vstupními daty až po odvození prvního bloku dat pro šifrování.
- Žlutá barva reprezentuje proces a kroky pro určení klíče pro šifrování první bloku dat.
- Modrá barva reprezentuje proces a průběh určení parametrů, které jsou použité pro šifrování prvního bloku.

4.2 Dešifrování

Při dešifrování se postupuje v rámci první fáze obdobně. Odvození klíče pro dešifrování prvního bloku je naprosto stejné. Jako první jsou načtena uživatelská data pro jeho odvození (heslo/klíčový soubor) a dále tajné parametry. Vypočte se inicializační vektor, který slouží pro získání soli k „nasolení“, který byl při šifrování začleněn do šifrových dat. Tento inicializační vektor je použitý k výpočtu parametrů pozice soli k „nasolení“. Jakmile je známá pozice soli, lze tuto sůl extrahovat a „nasolit“ inicializační vektor. Ten je následně využitý k výpočtu parametrů pro dešifrování prvního bloku a výpočtu parametrů solí k „předsolení“ a „zasolení“, které bude nutné v rámci poslední fáze z dešifrovaných dat odstranit. V rámci dešifrování dat se postupuje stejně, pouze s rozdílem aplikace inverzních funkcí v rámci šifrovacího jádra. Odvození klíčů pro další bloky dat je naprosto stejné jako při procesu šifrování.

4.3 Shrnutí vlastností polymorfního kryptografického systému TSS

Na základě předchozích kapitol lze tvrdit, že všechny vlastnosti, součásti i chování kryptografického systému TSS jsou polymorfní a chovají se polymorfně, a to nejen v souvislosti na uživatelském vstupu, ale i ve vazbě na náhodně vygenerovaná data → soli. Celý proces šifrování a kryptografický systém TSS je tudíž náhodně polymorfní, kdy pro každý šifrovaný blok je proces modifikován. Pro shrnutí jsou následující vlastnosti a součásti TSS polymorfní a náhodné:

- Odvození IV → dle klíčových dat
- Délka šifrovaného bloku
- Klíče pro šifrování
  - Režimy činnosti, včetně generátoru (PM-DC-LM)
- Počet rund
- Pořadí operací
- Operace šifrování

- Solení → podrobně viz kapitola 7.2 disertační práce
    - Délky solí pro „předsolení“, „zasolení“ a „nasolení“
    - Proces solení
    - Pozice soli pro „nasolení“ v rámci šifrových dat
- Substituční tabulka

Podrobnější informace o vlastnostech vytvořeného kryptografického systému TSS je možné najít v rámci textu disertační práce.

5 NÁVRH POLYMORFNÍCH SKTRUKTUR BLOKOVÝCH ŠIFER

Kapitola se věnuje jednomu ze stěžejních cílů disertační práce a v rámci doktorského studia mu byla věnována největší pozornost. V rámci předchozí kapitoly by předveden komplexní systém jako celek. V této kapitole bude rozebrán výzkum a návrh jednotlivých části systému v souladu s terminologií problematiky návrhu blokových šifer. Zároveň byly všechny části navrženy v souladu s tématem práce tak, aby bylo vše co nejvíce polymorfní – závislé na aktuálních podmínkách a vstupních datech.

V rámci problematiky návrhu komplexního polymorfního šifrovacího systému byly řešeny následující části blokových šifer a šifrování dat; tyto části se běžně využívají při šifrování pomocí blokových šifer či při návrhu blokových šifer:

- Odvození a tvorba inicializačního vektoru z tajných dat uživatele
- Bloková šifra – samotné šifrovací funkce
- Správa klíčů
- Režim činnosti blokových šifer
    - Proces zahrnutí entropie – solení

Dále v rámci doktorského studia proběhl návrh parametrizace systému a vlastností šifrování, které běžně v kryptografii není řešeno, viz kapitola věnující se současnému stavu řešené problematiky.

5.1 Princip solení a zahrnutí entropie do procesu šifrování

V průběhu tvorby kryptografické systému a při jeho výzkumu se projevovaly nedostatky v difúzi při šifrování. V závislosti na změnách v rámci otevřených dat bylo možné pozorovat konkrétní změny v šifrových datech. Toto nastávalo při změně pouze otevřených dat. Za další nedostatek bylo možné považovat přílišnou fixaci průběhu šifrování na vstupní podmínky → otevřená data, klíčová data a vstupní nastavení parametrů. Již ve variantě kryptografického

systému bez využití solí bylo možné pozorovat polymorfní chování v souvislosti se vstupním nastavením, což potvrzují výsledky testování v rámci kapitoly 8.1 disertační práce. Nicméně, zvýšení difúze šifrovacího systému byl jeden ze základních požadavků, který bylo nutné vyřešit.

Podrobný popis solení, včetně dalších informací je rozveden v rámci textu disertační práce. Níže uvedená kapitola slouží jako shrnutí a vymezení bezpečnosti a možností vytvořeného systému solení TSS.

5.1.1 Vymezení bezpečnosti solení a shrnutí

Proces solení je prakticky nezávislý na uživatelském vstupu, a proto i bezpečnost je z většiny nezávislá na uživatelských datech. Hlavní část bezpečnosti je proto spojená s kvalitou generování náhodných dat a souvisí s danou problematikou. Tudíž pokud jsou generovaná data náhodná, tak lze považovat TSS za náhodný. Ideální je využít tak zvaných „true-random" generátorů → využití atmosférického šumu, kvantových generátorů apod. Pro praktické testování je nyní generování náhodných solí v rámci systému TSS založené na základní funkci *urandom()* v rámci jazyka Python 3.x, ale není problém využití jakéhokoliv jiného generátoru.

Jediná část v rámci solení, která nejméně souvisí s náhodnými daty a více s uživatelským vstupem je výpočet pozice soli v rámci šifrových dat. Ta, jak bylo uvedeno v rámci podkapitole výše, souvisí zejména s klíčovými daty a vstupními uživatelskými parametry. Tato funkce je nicméně polymorfní v souvislosti s klíčovými daty a uživatelskými parametry, a tudíž je jen částečně náhodná. Za částečně náhodnou ji lze považovat, protože pozice souvisí s délkou otevřených dat, která zahrnují soli pro „předsolení" a „zasolení" → délky solí souvisí s nasoleným *IV*. Tedy i pozice soli v rámci šifrových dat se chová částečně náhodně. Prakticky to znamená, že i když bychom šifrovali pomocí stejného IV, pomocí stejných parametrů, tak i tak se může pozice soli měnit v souvislosti s délkami solí pro „předsolení" a „zasolení" → 512 různých pozic. Jak bylo naznačeno v úvody kapitoly, tak by šlo využít generování čtvrté soli, která vy sloužila pouze pro potřeby výpočty pozice soli.

Celkově tedy bezpečnost části TSS pro solení souvisí zejména s kvalitou a náhodností generovaných solí. Nicméně díky funkcionalitě solení lze považovat systém TSS za **náhodně polymorfní**.

5.2 Návrh způsobu generování šifrovacího klíče na základě tajných dat

V rámci této kapitoly je navržen princip nového způsobu generování klíče → polymorfního generování klíče. V rámci klasických způsobů generování klíče, viz kapitola 2.5, se postupuje obvykle následovně. Na vstupu jsou data pro odvození klíče – například heslo, soubor apod., která jsou vstupem pro fixní funkci, která na jejich základě vygeneruje klíč. Pokud se změní data pro odvození klíče, proces výpočtu klíče zůstává vždy stejný.

V rámci článku prezentovaného na konferenci (viz reference autora [A.7]) byl navržen a otestován odlišný přístup. Přístup, který postupuje polymorfně v závislosti na datech, z kterých má být odvozen klíč. Proces výpočtu klíče lze shrnout následovně. Samotná implementace je navržena pro potřeby šifrovacího systému. Tedy pro tvorbu šifrovacího klíče délky 111 bajtů.

Podrobný popis algoritmu a analýza byla provedena v rámci článku [A.7].

5.3 Parametrizace vlastností systému

Při návrhu šifrovacího systému TSS byly zvoleny vhodné parametry a byl navržen proces parametrizace. Celkově lze parametrizaci rozdělit na dvě části:

- Parametrizace vlastností šifrování – variabilita (9 parametrů)
  - Speciální parametrizace režimu činnosti PM-DC-LM pro inicializaci hodnot (2 parametry)
- Parametrizace solení (8 parametrů)

Celkově bylo doposud navrženo 19 parametrů (viz podrobněji disertační práce), které do šifrování vstupují a může je uživatel na začátku nastavit a které následně upravují celý proces šifrování. V budoucnu se mohou tyto parametry ještě rozšířit. Některé z parametrů jsou nastaveny pouze na začátku a ovlivňují šifrování a vlastnosti v prvotních fázích šifrování, jiné ovlivňují průběh šifrování v rámci celého procesu.

Parametry jsou navrženy tak, že mají hlavní složku → hodnota parametru, dále mají řídící složku, která slouží k manipulaci a přepočtu parametru pomocí klíče → který bajt klíče bude využitý k přepočtu.

V neposlední řadě jsou zde parametry, které ovlivňují solení, tyto parametry mají obdobně hodnotu parametru a hodnotu řídícího parametru. Většina parametrů má svou funkci na přepočet pomocí klíče.

Parametrizace byla sice zvolena tak, aby zapadala do kontextu celého šifrovacího systému TSS, ale spousta parametrů by bylo možné využít i stávajících šifrovacích algoritmů, jako je AES. Tyto možnosti a porovnání jsou rozebrány v rámci podkapitol věnovaných jednotlivým navrženým parametrům.

Podrobný popis parametrizace je možné dohledat v rámci textu disertační práce. Každopádně je zde uvedeno shrnutí.

5.3.1 Shrnutí a možnosti do budoucna

Jak bylo uvedeno v úvodu kapitoly, tak doposud bylo vytvořeno 19 parametrů, které lze v rámci uživatelského nastavení před započetím šifrování nastavit. Jedná se o parametry pro změnu variability šifrování (9), parametry pro nastavení solení (8) a parametry speciálně pro potřeby režimu činnosti PM-DC-LM (2). Celková režie parametrizace a přepočítávání parametrů je jeden z důvodů, který velmi pozitivně ovlivňuje bezpečnost systému TSS a inovativně rozšiřuje problematiky symetrické kryptografie, ale bohužel je i jeden z důvodů, který má negativní dopad na dobu šifrování.

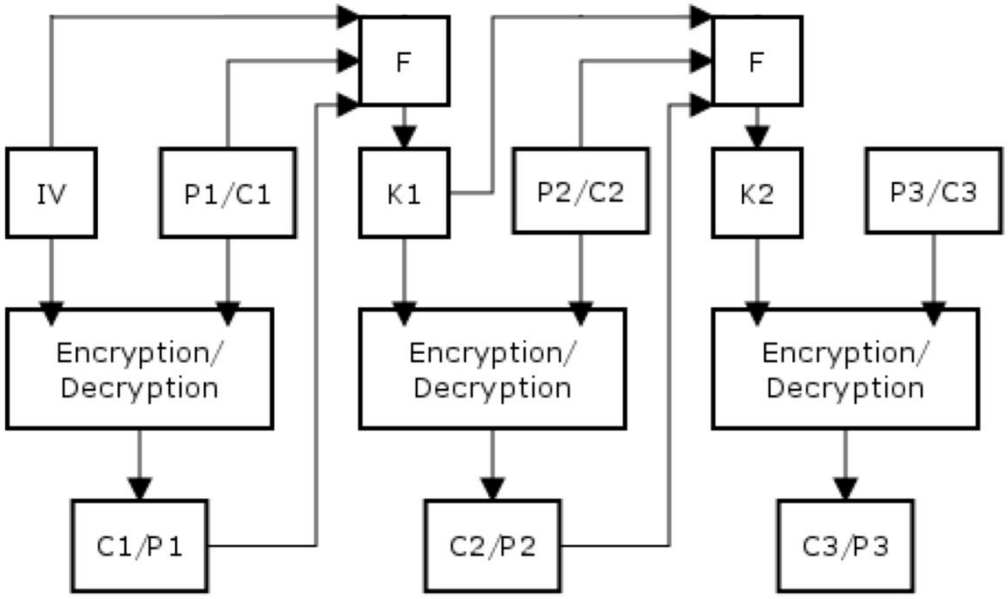
Nicméně tyto parametry lze dle potřeby měnit → ubírat i přidávat a parametrizovat další části/vlastnosti systému. Pro potřeby vylepšení systému TSS je v plánu přidání dalších parametrů, například:

- Parametricky odvozená pozice hodnot d a g v CPRNG režimu činnosti PM-DC-LM (aktuálně jsou fixní)
- Parametrické vyjádření pozice soli pro „nasolení“ v šifrovém textu
- Parametry pro šifrovací jádro → indexování či omezení přičítání klíče

5.4 Návrh správy klíčů a tvorba režimu činnosti blokové šifry

Výsledky tvorby režimů činnosti v rámci doktorského studia byly i z velké části prezentované a publikované v rámci vědeckých konferencí. Režimy činnosti vytvořené v rámci doktorského studia lze označit jako skupinu režimů činnosti → Skupina polymorfních režimů činnosti PM (Polymorphous Modes)

V porovnání s aktuálně používanými režimy činnosti, které využívají pouze jednu složku z předchozích dat (otevřená data nebo šifrová data) k modifikaci aktuálních dat (opět otevřená nebo šifrová data), polymorfní režim činnosti mění klíč, který byl použit k zašifrování bloku dat na jiný, který bude použit pro šifrování dat následující bloku. To zachycuje následující diagram.



Obrázek 3 – Diagram režimu činnosti ze skupiny PM (vlastní)

- *IV* – označuje inicializační vektor („nasolené“ *IV* v rámci TSS)
- P_i – označuje otevřený blok dat
- C_i – označuje šifrový blok dat
- K_i – označuje klíč pro šifrování/dešifrování bloku dat
- F – Funkce, která na základě složek – parametr N (viz kapitola 7.4.3), P_i, C_i a K_i odvodí klíč K_{i+1}

Diagram zachycuje obecnou strukturu polymorfního režimu činnosti. Na základě uvedeného diagramu je možné měnit funkci F a tím vytvořit či optimalizovat režim činnosti dle potřeby. Uveďme si tři základní návrhy polymorfního režimu činnosti → varianta 1, varianta 2 a varianta 3. Popíšeme si ještě speciální modifikaci jako variantu 4 s označením „PM-PolyUltra“. První je přímou implementací v diplomové práci a druhá varianta je jeho vylepšenou verzí v rámci náplně disertační práce → vylepšení pravděpodobnostní distribuce volby rovnic. Ukázky a testy jsou provedeny implementací v programovacím jazyce Python 3.x. V neposlední řádě byla navržená varianta číslo 5, která zahrnují vlastní implementaci polymorfního chaotického pseudo-náhodného generátoru čísel. Podobnosti z tvorby a samotný popis všech navržených variant režimů činnosti je možné dohledat v rámci disertační práce (viz kapitola 7.5), kde jsou všechny varianty zároveň i otestovány. V rámci textu disertační práce lze najít i shrnutí.

6 TESTOVÁNÍ KRYPTOGRAFICKÉHO SYSTÉMU TSS

Následující kapitola se věnuje testování vytvořeného systému TSS jako souhrnu všech součásti systému jako celku. Kapitolu jde rozdělit do testování systému TSS bez využití solení (bez generování solí a za využití solí pouze s nulovými bajty) a na testování kompletního systému TSS včetně solení. Další podkapitoly se věnují testování rychlosti šifrování v porovnání se šifrou AES a jako poslední podkapitola je sumarizace výsledků testování systému TSS.

Konkrétní podmínky testování a obsah testů jsou uvedeny v rámci jednotlivých podkapitol. Všechny entropie jsou vypočteny z hexadecimálního tvaru dat, a tudíž entropie v rámci následujících podkapitol a provedených testů může nabývat hodnotu reálného čísla na intervalu $\langle 0; 4 \rangle$.

6.1 Testování TSS bez využití solení a využití klíčových dat

Testování systému TSS bez využití solení jako demonstraci změny šifrových dat v souvislosti se změnou vstupních parametrů lze podrobně najít v textu disertační práce. Zde následuje sumarizační tabulka vypočtených entropií šifrových dat pomocí systému TSS bez využití solení.

Tabulka 1 - Výpočet entropie TSS s nulovými solemi a se změnou parametrů

Entropie -> TSS s nulovými solemi a změnou parametrů		
Varianta	Entropie - celá data	Entropie - bez "nasolení"
TSS + PM - parametry 0	3,6005585670	3,9890066218
TSS + PM-PolyUltra - parametry 0	3,6104553882	3,9889534982
TSS + PM-DC-LM - parametry 0	3,5979363475	3,9892705569
TSS + PM - parametry 11	3,6013654878	3,9824469681
TSS + PM-PolyUltra - parametry 11	3,6104553882	3,9788065314
TSS + PM-DC-LM - parametry 11	3,5893556851	3,9740693394

6.2 Testování entropie systému TSS včetně solení

Podrobný postup a parametry testování je možné vidět v rámci kapitoly 8.2 disertační práce. Zde jsou uvedené souhrnné výsledky.

Výsledky jsou vidět v následujících dvou tabulkách. Všechny entropie byly vypočteny z hexadecimální reprezentace šifrových dat a jsou zobrazeny s přesností na 11 platných číslic. V souvislosti s výpočtem entropie z hexadecimálního tvaru dat lze očekávat, že by se hodnoty entropií měly blížit k maximální hodnotě 4.

Tabulka 2 - Testování entropie TSS vs. AES - nulové hodnoty OT a klíče (vlastní)

Entropie -> nulové hodnoty OT a klíče					
Varianta	Počet iterací	Délka OT (B)	Entropie - průměr	Entropie - min	Entropie - max
TSS + PM	111	1111111	3,9999950574	3,9999897006	3,9999982711
TSS + PM-PolyUltra	111	1111111	3,9999948037	3,9999889434	3,9999983851
TSS + PM-DC-LM	111	1111111	3,9999952784	3,9999873040	3,9999980147
AES256-ECB	111	1111111	3,2807236356	3,2807236356	3,2807236356
AES256-CBC	111	1111111	**3,9999952832**	3,9999896777	3,9999986514
AES256-CTR	111	1111111	3,9999948563	3,9999899455	3,9999982716
AES256-CFB	111	1111111	3,9999952179	3,9999899586	**3,9999989392**
AES256-OFB	111	1111111	3,9999951129	3,9999892935	3,9999983596
AES256-CCM	111	1111111	3,9999948921	3,9999898791	3,9999985659
AES256-GCM	111	1111111	3,9999952123	3,9999895944	3,9999985018
AES256-EAX	111	1111111	3,9999949681	3,9999899133	3,9999981307
AES256-OCB	111	1111111	3,9999947250	3,9999898085	3,9999980943
Maximální průměrná entropie -> **AES256-CBC**			**3,9999952832**		
Maximální entropie -> **AES256-CFB**					**3,9999989392**

Jak je možné vidět z první tabulky, tak s nejlepší průměrnou entropii při šifrování nulových hodnot bylo šifrování pomocí kombinace **AES256-CBC**. Maximální entropie bylo dosaženo při šifrování kombinací **AES256-CFB**.

Tabulka 3 - Testování entropie TSS vs. AES vs. náhodné generátory - náhodné hodnoty OT a klíčů (vlastní)

Entropie -> náhodné hodnoty OT a klíče					
Varianta	Počet iterací	Délka OT (B)	Entropie - průměr	Entropie - min	Entropie - max
TSS + PM	111	1111111	3,9999950738	3,9999908275	3,9999984169
TSS + PM-PolyUltra	111	1111111	3,9999949853	3,9999896968	3,9999979634
TSS + PM-DC-LM	111	1111111	3,9999952609	3,9999903583	**3,9999989922**
AES256-ECB	111	1111111	3,9999948387	3,9999903530	3,9999982111
AES256-CBC	111	1111111	3,9999952414	3,9999891625	3,9999986157
AES256-CTR	111	1111111	3,9999950330	3,9999885891	3,9999978544
AES256-CFB	111	1111111	3,9999951390	3,9999890055	3,9999983995
AES256-OFB	111	1111111	3,9999949671	3,9999904922	3,9999982140
AES256-CCM	111	1111111	3,9999951344	3,9999872249	3,9999983546
AES256-GCM	111	1111111	3,9999951228	3,9999907588	3,9999987934
AES256-EAX	111	1111111	3,9999953396	3,9999888946	3,9999989337
AES256-OCB	111	1111111	3,9999950577	3,9999897997	3,9999981906
Random PyCryptodome	111	1111111	3,9999951461	3,9999896907	3,9999981823
Random urandom()	111	1111111	**3,9999953764**	3,9999910962	3,9999987336
Maximální průměrná entropie -> **urandom()**			**3,9999953764**		
Maximální entropie -> **TSS + PM-DC-LM**					**3,9999989922**

V případě šifrování náhodných dat, náhodným klíčem vyšla „lépe“ kombinace **TSS + PM-DC-LM** s dosaženou maximální entropií 3,9999989922.

Nejlepší průměrná entropie byla po 111 iteracích dosažena při generování náhodných dat pomocí funkce *urandom()*.

Na základě entropií jde usuzovat kvalitní míru difúze a konfúze systému TSS, zejména při šifrování nulových bajtů otevřených dat. Dále lze říci, že se šifrová data blíží datům náhodným, kdy náhodnost dat by byla ještě nutná podrobněji otestovat, například za využití Diehard testů. Celkově z testování lze říci, že jak systém TSS a AES jsou na srovnatelné úrovni. Rozdíly v dosažených entropiích jsou nepatrné a nelze tvrdit, že by byl jeden z testovaných lepší či horší. Při dalším spuštění testů by mohl být výsledek jiný. Každopádně TSS i AES dosahují výsledných entropií srovnatelných s entropií náhodně generovaných dat, viz entropie náhodně generovaných dat funkce *urandom()* a *get_random_bytes()* a hodnoty blížící se 4. Jediná kombinace AES256-ECB nedosahovala kvalitní entropie šifrovaných dat při šifrování nulových bloků, což je ale z principu fungování ECB pochopitelné. Výsledná vypočtená entropie znamená vyjádření entropie jednoho zašifrovaného bloku otevřených dat. Zbývající šifrované bloky vypadaly stejně.

6.3 Shrnutí

Systém TSS, jak bylo ukázáno výše poskytuje velmi kvalitní pravděpodobnostní distribuci hodnot bajtů šifrových dat → difúzi a konfúzi. Lze vidět, že systém TSS je schopen znemožnit určení jakékoliv vazby mezi šifrovými daty a otevřenými daty či šifrovacím klíčem.

Bylo ukázáno, že i když jsou systémem TSS šifrována otevřená data s velmi nízkou entropií, tak výstupní šifrová data se svou entropií blíží té maximální. Bylo demonstrováno, že systém TSS se chová náhodně polymorfně. To znamená, parametry systému a průběh šifrování probíhají rozdílně i bez nutnosti měnit vstupní šifrovací klíč (*IV*), uživatelské parametry či otevřená data.

Lze tvrdit, že systém TSS je schopen odolat základním známým kryptoanalytickým metodám, které jsou výhradně aplikovatelné na šifrovací algoritmy a systémy s fixní strukturou. Lze očekávat, že systém je díky jeho náhodně polymorfnímu chování schopen odolat i pokročilým kryptoanalytickým metodám založených na postranních kanálech, útocích založených na časování a v neposlední řadě i aplikaci kvantových počítačů. Teoreticky lze systém TSS brát jako post kvantový symetrický šifrovací algoritmus. To vše za předpokladu další hlubší analýzy → což je možné, při rozsáhlosti faktorů ovlivňující chování systému a jeho komplexnosti, vidět jako zároveň výhodu i nevýhodu.

V neposlední řadě lze vidět výhodu TSS v možnosti flexibilně měnit systém a manipulovat s jeho parametry → délka klíče je pouze jeden z parametrů,

který lze jednoduše kdykoliv změnit a s tím související fungování a nastavení celého systému. Jako výhodu a současně nevýhodu je možné považovat výpočetní náročnost (doba šifrování) a nemožnost škálovatelnosti. Výhodu v obtížné aplikaci HW prostředků pro prolomení a nevýhodu v době šifrování.

7 PŘÍNOS PRO VĚDU A PRAXI

Problematikou polymorfních struktur v symetrické kryptografii se věnuje omezené množství publikací. V rámci existujících řešení je pouze malé množství algoritmů, které by byly navrženy v souladu s polymorfním chováním, a i ty jsou polymorfní jen z části – generování substituční tabulky, využití *nonce*/*IV*/tweaku, využití proměnlivé délky bloků, využití variabilních operací (permutace, posun, rotace). Aktuálně využívané šifry, mezi které patří AES, Camellia, TDES/TDEA, Blowfish, Serpent, Twofish, ARIA, IDEA, GOST, RC6 a další mají z většiny fixní průběh – nezávislý na vstupních podmínkách a je nutné je kombinovat s dalšími režimy činností. Například se jedná o klasické režimy činnosti CBC, OFB, CTR, XTS nebo tzv. moderní režimy činnosti CCM, EAX, GCM, SIV a OCB, které ovšem mají fixní strukturu a nejsou uzpůsobeny potřebám šifry. Lze nalézt pouze omezené množství příkladů algoritmů (systémů), kde je polymorfní chování aplikované ve větší míře (viz kapitola 4 disertační práce). Tyto systému jsou buď teoretickým konceptem nebo nebyly nikdy využity v praxi.

Navržený a vytvořený kryptografický systém TSS v rámci disertační práce je v tomto směru unikátní. Nejen že byly jeho dílčí části navrženy, aby jejich princip byl polymorfní, ale také s důrazem, aby bylo možné všechny vytvořené části sjednotit v komplexně fungující kryptografický systém. Systém, který polymorfně odvozuje *IV*. Systém s polymorfně odvozenými parametry pro šifrování, jako substituční tabulka, počet rund, délka šifrovaných bloků. Systém, jenž samotné jádro šifrování se chová polymorfně (operace šifrování včetně pořadí operací). Poskytuje výběr z více druhů polymorfních režimů činnosti (režimu odvození klíče pro šifrování či klíčového managementu). V neposlední řadě systém využívající polymorfně a parametricky založené solení pomocí tří náhodných solí.

Většina existujících algoritmů v rámci bezpečnosti spoléhá v základu na délku klíče a s tím spojenou velikostí klíčového prostoru. V případě využití *nonce*/*IV*/tweaku/soli pro šifrování nebo režim činnosti je nutné tyto parametry vhodně sdílet, podobně jako u tajného klíče. V praxi je nutné využití asymetrické kryptografie pro jejich přenos stejně jako u klíče nebo připojení k šifrovým datům na začátek.

Navržený systém TSS nevyužívá pouze tajný klíč k zajištění bezpečnosti, ale rozšiřuje množinu klíčů, která je při délce 111 bajtů dostačující v odolání

útoku hrubou silou, o uživatelsky vstup ve formě nastavení parametrů. Délka klíče 111 bajtů neboli 888 bitů byla zvolena nejen z důvodu počtu možných kombinací klíčů, ale i pro možnost odvozování parametrů a vlastností systému. Můžeme říci, že i když uživatel bude šifrovat stejným klíčem stejná otevřená data, tak při využití odlišného uživatelské nastavení parametrů budou mít šifrová data jiný tvar. Další věc, která lze považovat za tajnou jsou vygenerované soli, protože soli k „předsolení“ a „zasolení“ jsou zašifrovány a součástí výstupních šifrových dat a sůl pro „nasolení“ *IV* je algoritmicky začleněna do šifrových dat, kdy pozice soli je variabilní, závislá na tajném klíči, uživatelském nastavení a délce otevřených dat. V porovnání se stávajícími algoritmy není nutné sdílení solí či připojení solí na začátek šifrových dat. Tato nutnost přenosu opět zůstává pro tajný klíč a tajné vstupní nastavení parametrů. Celkově se v souvislosti s aplikací solí chová systém náhodně a jeho fungování je závislé na složce *t* – čas. Protože i když budou na vstupu stejná otevřená data, stejná klíčová data pro odvození *IV*, stejné tajné uživatelské nastavení vstupních parametrů, tak sůl je vždy generována náhodně a při všech vzájemných vazbách lze tvrdit, že i výstupní šifrová data mají polymorfně náhodný tvar. V souvislosti s parametrizací, která je opět závislá i na obsahu solí, lze říci, že otevřená data jsou šifrované polymorfně náhodným způsobem. Množina způsobů šifrování je dána navrženým systémem. Vše za možnosti šifrová data zpětně dešifrovat a bez nutnosti sdílení solí.

Na základě výše uvedeného lze vidět přínos pro praxi, kdy je množina stávajících algoritmů rozšířena o nové. Zároveň je poskytnuta i potenciální možnost odolání blížícím se kvantovým počítačům → bez znalostí tajných dat, nastavení parametrů a solí nelze určit konkrétní algoritmus použitý k šifrování otevřených dat. Tato skutečnost komplikuje využití kvantových počítačů pro prolomení systému. Systém TSS poskytuje vyšší míru bezpečnosti, ale je nutné říct, že za cenu výpočetní náročnosti → rychlost při testování byla přibližně 800 krát a více pomalejší než AES (viz kapitola 8.3 disertační práce), proto jeho využití lze doporučit se zaměřením na šifrování menších objemů dat (cca do velikosti MB) – ochrana klíčů, hesel, kritických dokumentů apod. Dalším praktickým přínosem je potenciální využití jednotlivých části na rozšíření bezpečnosti stávajících algoritmů – využití parametrizace, polymorfního režimu činnosti nebo „obalením“ systému pomocí vytvořeného solení. Celý systém lze teoreticky využít s náhradou/změnou blokové šifry. To umožní zvýšení bezpečnosti blokových šifer – protože systém solení zvyšuje znatelně difúzi a konfúzi. Zároveň znemožňuje určení důležitých parametrů z výsledných šifrových dat – délka vstupních otevřených dat, parametry a další.

Problematika polymorfních struktur v rámci symetrické kryptografie by zasloužila větší vědeckou pozornost. Jak bylo ukázané v rámci disertační práce,

tak není složité aplikovat polymorfní chování na kteroukoliv oblast symetrické kryptografie. Teoreticky by šla nejen symetrická kryptografie převést na polymorfní chování, ale například hashovací algoritmy nebo i asymetrická kryptografie. Složitější problematikou, než samotná tvorba polymorfních struktur je jejich následné vyhodnocení a podrobná analýza. Disertační práce poskytuje solidní základy a prostor pro další bádání na poli polymorfních struktur. Zároveň práce poskytuje prostor pro podrobnější analýzu a následnou optimalizaci navržených struktur a je inspirací pro další tvorbu, aplikaci a zkoumání problematiky polymorfních struktur v kryptografii.

8 ZÁVĚR

Výzkum provedený v rámci disertační práce lze shrnout na základě cílů disertační práce viz kapitola 1.

Na základě myšlenky (viz kapitola 3) byly zvoleny parametry, algoritmy a části problematiky kryptografie blokových šifer za cílem návrhu komplexního šifrovacího systému TSS. Systém TSS je tedy vytvořen plně v souladu s výše uvedenou myšlenkou, kdy velká část chování, funkcí včetně parametrů a průběhu šifrování jsou odvozeny od tajného uživatelského klíče. TSS lze označit jako „systém šifrovacích systémů“.

Na základě této myšlenky bylo šifrovací funkce a šifrování parametrizováno, kdy výčet parametrů lze dohledat v rámci textu disertační práce zejména v kapitolách 5.2, 7.2 a 7.4. Aktuálně je systém parametrizován na základě 19 parametrů, kdy je počítáno s budoucím možných rozšířením těchto parametrů.

V neposlední řadě byl navržený systém TSS doplněn o funkcionalitu solení → zahrnutí náhodných dat do procesu šifrování a lze říct že se celý systém včetně parametrů chová „náhodně“ v závislosti na těchto datech. Systém TSS chová nejen polymorfně, ale i polymorfně „náhodně“ → pseudo-náhodně. Proto, pokud budeme šifrovat stejná otevřená data, stejným tajným klíčem a za stejně nastavených vstupních parametrů, tak výstupem budou rozdílná šifrová data. A to při každém spuštění šifrování. V souvislosti s tím dojde i ke změně vnitřních funkcí a parametrů systému, takže lze říci, že při každém šifrování jsou otevřená data šifrované jinak (jiným šifrovacím systémem).

V sedmé kapitole disertační práce se lze dočíst o konkrétnímu návrhu jednotlivých částí systému TSS včetně popisu tvorby a implementace těchto řešení. Jsou zde popsány návrhy polymorfního odvození klíče z tajných dat, tvorba polymorfních režimů činnosti blokových šifer a správa klíčů (vytvořena skupina režimů činností PM), polymorfní šifrovací jádro → bloková šifra,

polymorfní parametrizace systému a vlastností a polymorfní solení. Všechny součásti systému TSS byly navrženy polymorfně.

V rámci osmé kapitoly disertační práce bylo ukázáno, že systém disponuje vysokou mírou difúze (změny i beze změny otevřených dat), konfúze a pravděpodobnostní distribuce znaků (výsledná entropie šifrových dat) byla blížící se maximální hodnotě. To i v případě, že byla šifrována otevřená data reprezentující hodnoty nulových bajtů.

Výstupem práce je ucelený komplexní kryptografický polymorfní šifrovací systém TSS jako demonstrace polymorfních struktur v symetrické kryptografii. Dalším přínosem práce jsou vytvořené jednotlivé návrhy polymorfních struktur, které je možné využít jako podklad pro budoucí výzkum. Je důležité poznamenat, že vytvořený systém TSS, i když vykazuje velmi dobré výsledky, je pouze konceptuálním řešením a nelze jej považovat za plnohodnotně bezpečné a aplikovatelné řešení do praxe. Pro využití systému v praxi by bylo potřebné jej podrobit podrobnější analýze, včetně rozsáhlejšímu testování.

SEZNAM POUŽITÉ LITERATURY

[1] ŽÁČEK, Petr. Návrh nové symetrické šifry pro mobilní zařízení. Zlín, 2014. Diplomová práce. Univerzita Tomáše Bati ve Zlíně. Vedoucí práce Ing. David Malaník, Ph. D.

[2] Symmetric ciphers: Modern modes of operation, 2020. PyCryptodome - documentation: Revision ca247079 [online]. [cit. 2021-5-2]. Dostupné z: https://pycryptodome.readthedocs.io/en/latest/src/cipher/modern.html

[3] https://docs.python.org/3/library/os.html

SEZNAM POUŽITÝCH ZKRATEK

AEAD	Authenticated Encryption with Associated Data
AES	Advanced Encryption Standard
CBC	Cipherblock Chaining
CCM	Counter with CBC-MAC
CFB	Cipher Feedback
CPRNG	Chaotic Pseudo-Random Number Generator
DC	Deterministic Chaos
ECB	Electronic Codebook
GCM	Galois/Counter mode
GOST	Gosudarstvenii Standart
HW	Hardware
IDEA	International Data Encryption Standard
IV	Inicializační Vektor
LM	Logistic Maps
OCB	Offset CodeBook mode
OFB	Output Feedback

OT	Otevřený text (otevřená data)
PM	Polymorphous Mode
SIV	Synthetic Initialization Vector
TDES/TDEA	Triple Data Encryption Standard / Triple Data Encryption Algorithm
TSS	Triply Salted Smallie
XTS	XEX-based tweaked-codebook mode with ciphertext stealing

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

PUBLIKAČNÍ ČINNOST AUTORA

Mezinárodní patentová přihláška

Jašek R. [25], Oulehla M. [35], Žáček P. [6], Krňávek J. [14], Lázecký V. [5], Makowski J. [5], Malík T. [5], Malík J. [5] Identity and License Verification System for Working with Highly Sensitive Data

Konference a časopisy

[A.1] ŽÁČEK, Petr, JAŠEK, Roman, MALANÍK, David. Using the Deterministic Chaos in Variable Mode of Operation of Block Ciphers. In *Artificial Intelligence Perspectives and Applications*. Heidelberg: Springer-Verlag Berlin, 2015, s. 347-354. ISSN 2194-5357. ISBN 978-3-319-18475-3.

[A.2] ŽÁČEK, Petr, JAŠEK, Roman, MALANÍK, David. Group of the Polymorphous Modes of Operation - PM. In *Proceedings of the 2016 Future*

Technologies Conference (FTC). New Jersey, Piscataway: IEEE, 2016, s. 1314-1315. ISBN 978-1-5090-4171-8.

[A.3] ŽÁČEK, Petr, JAŠEK, Roman, MALANÍK, David. Improvement of CPRNG of the PM-DC-LM Mode and Comparison with its Previous Version. In *Tenth International Conference on Emerging Security Information, Systems and Technologies*. Wilmington: IARIA XPS Press, 2016, s. 57-62. ISBN 978-1-61208-493-0.

[A.4] ŽÁČEK, Petr, JAŠEK, Roman, KRÁLÍK, Lukáš, MALANÍK, David, HOLBÍKOVÁ, Petra. Analysis of the chaotic pseudo-random generator of the PM-DC-LM mode based on the position of the returned numbers. In *2017 International Conference on Logistics, Informatics and Service Sciences (LISS)*. New Jersey, Piscataway: IEEE, 2017, s. nestrankovano. ISBN 978-1-5386-1047-3.

[A.5] ŽÁČEK, Petr, JAŠEK, Roman, MALANÍK, David. A Comparison of the PM-DC-LM Mode With Other Common Operational Block Cipher Modes. In *The Ninth International conference on Emerging Security Information, Systems and Technologies*. Wilmington: IARIA, 2015, s. 44-48. ISSN 2162-2116. ISBN 978-1-61208-427-5.

[A.6] ŽÁČEK, Petr, JAŠEK, Roman, MALANÍK, David. Possibilities and Testing of CPRNG in Block Cipher Mode of Operation PM-DC-LM. In *Proceedings of PPS-30: The 30th International Conference of the Polymer Processing Society*. Melville: American Institute of Physics Publising Inc., 2016, s. "nestrankovano". ISSN 0094-243X. ISBN 978-0-7354-1309-2.

[A.7] ŽÁČEK, Petr, JAŠEK, Roman, MALANÍK, David, KRÁLÍK, Lukáš, HOLBÍKOVÁ, Petra. Using the SHA-3 to Derive Encryption Keys Based on Key-file. *Proceedings - 2018 2nd European Conference on Electrical Engineering and Computer Science, EECS 2018*. Piscataway, New Jersey: Institute of Electrical and Electronics Engineers Inc., 2019, s. 348-351. ISBN 978-1-72811-929-8.

ODBORNÝ ŽIVOTOPIS AUTORA

OSOBNÍ ÚDAJE Ing. Petr Žáček

Kŕiby 4713, 76005 Zlín (Česká republika)

+420 734 304 234

PRACOVNÍ ZKUŠENOSTI

01/10/2017–do současnosti

Asistent

Univerzita Tomáše Bati ve Zlíně, Zlín (Česká republika)

1. Výuka předmětů
   - Bezpečnost informačních systémů, Kryptologie, Testování software, Programování
2. Člen laboratoře pro penetrační testování PTLab
   - Penetrační testování sítí, webových stránek
   - Konzultační činnost v oblasti kybernetické bezpečnosti
   - Etický hacking

VZDĚLÁNÍ, ODBORNÁ PŘÍPRAVA A KURZY

2012–2014

Vysokoškolské vzdělání II. stupně

Univerzita Tomáše Bati ve Zlíně, Fakulta aplikované informatiky; Bezpečnostní technologie, systémy a management – technické zaměření, Zlín (Česká republika), Zlín (Česká republika)

Diplomová práce – Návrh nové symetrické šifry pro mobilní zařízení v jazyce Python 3.x

2014–do současnosti

Vysokoškolské vzdělání III. stupně

Univerzita Tomáše Bati ve Zlíně, Fakulta aplikované informatiky; Inženýrská informatika, Zlín (Česká republika), Zlín (Česká republika)

OSOBNÍ DOVEDNOSTI

Mateřský jazyk: Čeština

Další jazyky

	POROZUMĚNÍ		MLUVENÍ		PÍSEMNÝ PROJEV
	Poslech	Čtení	Ústní interakce	Samostatný ústní projev	
Angličtina	B2	B2	B1	B2	B2

Úrovně: A1 a A2: základní uživatel - B1 a B2: samostatný uživatel - C1 a C2: zkušený uživatel
Společný evropský referenční rámec pro jazyky

Certifikáty

The Complete Ethical Hacking Course: Beginner to Advanced! - UC-5W8MTNLZ
Programming for Everybody (Python)
Cryptography I.
ISTQB - Certified Tester Foundation Level - 00153/15
ISTQB - Certified Tester Foundation Level - Agile Tester Extension - 00013/16

DOPLŇUJÍCÍ INFORMACE

Projekty

IGA/FAI/2015/047 - Variabilní struktura v režimu činnosti blokových šifer (Hlavní řešitel)

IGA/FAI/2016/028 - Rozšíření a možnosti vylepšení polymorfních režimů činnosti blokových šifer ze skupiny PM (Hlavní řešitel)

IGA/CebiaTech/2017/007 - Softwarová podpora pro školení a testování správců IT (Spoluřešitel)

IGA/CebiaTech/2018/007 - Softwarová podpora pro školení a testování správců IT- II. (Hlavní řešitel)

FAI2A/2019 - Kvantový generátor náhodných čísel ve výuce předmětu Kryptologie (A3KRY) (Spoluřešitel)

RVO/CEBIA/2018/001 - Aplikace inženýrské informatiky (Spoluřešitel)

RVO/CEBIA/2019/001 - Aplikace inženýrské informatiky (Spoluřešitel)

CZ.01.1.02/0.0/0.0/15_019/0004580 – Platforma INFOS (Spoluřešitel)

CZ.02.2.69/0.0/0.0/16_015/0002204 – Strategický project UTB ve Zlíně (Spoluřešitel)

CZ.01.1.02/0.0/0.0/17_107/0012503 - Výzkum a vývoj eHealth Integrované aplikační platformy Telemedicíny (Spoluřešitel)

CZ.02.2.69/0.0/0.0/18_056/0012951 - DUO UTB: Strategický projekt UTB ve Zlíně II. (Spoluřešitel)

Penetrační testování pro soukromý sektor – roky 2016 až současnost (Spoluřešitel)

Ing. Petr Žáček, Ph.D.

Návrh polymorfních struktur v symetrické kryptografii

Design of the Polymorphous Structures in the Symmetric Cryptography

Teze disertační práce

Vydala Univerzita Tomáše Bati ve Zlíně
nám. T. G. Masaryka 5555, 760 01 Zlín.

Náklad: vyšlo elektronicky
Sazba: Ing. Petr Žáček, Ph.D.
Publikace neprošla jazykovou ani redakční úpravou.

Rok vydání 2021
První vydání.

ISBN 978-80-7678-034-7

30