OPONENTNÍ POSUDEK DOKTORSKÉ DISERTAČNÍ PRÁCE

Téma disertační práce:	Návrh polymorfních struktur v symetrické kryptografii
Vypracováno na pracovišti:	Univerzita Tomáše Bati ve Zlíně, Fakulta aplikované informatiky
Autor práce:	Ing. Petr Žáček
Školitel – vedoucí práce:	prof. Mgr. Roman Jašek, Ph.D., DBA

Aktuálnost tématu disertační práce

Předložená disertační práce zaměřená do oblasti symetrické kryptografie, což se může zdát být v dnešní době anachronismem. Autor toto svou aplikací polymorfních postupů do symetrického šifrování překonává a činí symetrické šifrování opět aktuálním. Není jediným autorem, který se předloženým tématem zabývá, autorů, kteří te tímto tématem zabývají, je ale velmi málo.

Práce je svým přístupem k řešení problému unikátní. Její výstupy odrážejí současný stav ve zkoumané oblasti a jsou přínosné pro cílovou skupinu potenciálních příjemců. Jako významný a přínosný hodnotím i postup řešení práce, který je možným vzorovým postupem i pro další výzkumníky. I v této oblasti tedy vnímám aktuálnost tématu a jeho řešení.

Splnění stanovených cílů v disertační práci

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.

Naplněním autorem uvedených 6 dílčích cílů (od teoretického základu přes definici jednotlivých vlastností, operací a parametrů, návrh vlastního řešení a jeho praktickou implementaci včetně optimalizace až po diskuzi dosažených výsledků a pohled do budoucnosti) pak plní hlavní cíl disertační práce.

Metody použité při vypracování disertační práce

Metody použité v práci jsou vhodně zvolené a odpovídají tématu práce. Volba metod prokazuje schopnost autora práce systematicky teoreticky vědecky pracovat a výsledky konfrontovat se stavem praxe.

V rámci volby metod a přístupů vnímám velmi významně a výrazně roli školitele jako konzultanta a kritického oponenta průběžného řešení zadání práce. Uvedené hodnotím jako významné pro schopnost autora týmově vědecky pracovat.

Postup řešení problému a výsledky disertační práce, přínos doktoranda

Práce je rozdělena (kromě úvodních a závěrečné) do 8 kapitol (Úvod do řešené problematiky, Terminologie a vymezení pojmů disertační práce, Současný stav řešené problematiky, Základní myšlenka vybudování polymorfního šifrovacího systému, Vytvořený kryptografický systém – TSS, Návrh polymorfních sktruktur blokových šifer, Testování kryptografického systému tss a Přínos pro vědu a praxi).

Způsob řešení práce odpovídá požadavkům na řešení zadaného problému vědeckou metodou a hodnotím jej jako optimálně zvolený. Kapitoly jsou srozumitelné a logicky na sebe navazují. Autor v dostatečném rozsahu provedl srovnání práce s dosavadním stavem výzkumu ve světě.

Význam pro praxi a pro rozvoj vědního oboru

Význam pro praxi i rozvoj vědního oboru „Inženýrská informatika" vnímám nejen v autorově tvůrčím přístupu k řešenému tématu ale i v úvodních teoretických kapitolách, kde ze svého odborného pohledu rekapituluje aktuální „state-of-the-art".

Výsledky autorovy disertační práce nerozvíjejí mainstreamové téma, ale naopak téma mimo tento mainstream. Zpracované téma má ale potenciál významným způsobem vytvářet prostředí pro využívání všech informačních a komunikačních technologií.

Zpracovaní tématu není uzavřené, byť všechny dílčí, a i hlavní cíl disertační práce je naplněn. Autor sám uvádí, co dalšího by mělo následovat.

Formální úprava disertační práce

Rozsah práce odpovídá standardní disertační práci. Kapitoly na sebe logicky navazují. Práce je psána většinou srozumitelně, některé formulace jsou ale komplikovanější, resp. Méně přehledné, což v daném místě poněkud snižuje srozumitelnost a přehlednost popisu řešeného problému. Příklady autorova programového kódu jsou uváděny zbytečně inverzně a jako obrázky, což opět snižuje přehlednost a srozumitelnost. Závěrečnou redakci předložené práce autor poněkud podcenil.

Rovněž je škoda, že autor v disertační práci téměř vše uvádí především textově. Tím ztěžuje čtenáři orientaci v řešené problematice. Teprve v podkapitole 7.5 je jednoduchý diagram činnosti, který takovou orientaci usnadňuje.

Předložená práce splňuje požadavky na doktorskou disertační práci v uvedeném oboru.

Dotazy k obhajobě:

- Může být zvýšení výpočetní náročnosti v případě nasazení popisovaného systému (požadované zvýšení výkonu výpočetního systému nebo prodloužení doby zpracování) významnou překážkou pro nasazení prezentovaného systému? Jak je to s náročností dešifrování?
- Jaký význam v práci mají definované hypotézy a co je třeba, aby je bylo možné požadovat za prokázané?
- Jak vidí autor budoucnost polymorfních šifrovacích systémů obecně i systému TSS konkrátně?

Závěrečné vyjádření

Práci **doporučuji** k obhajobě před příslušnou komisí.

Oldřich Kodym Digitálně podepsal Oldřich Kodym Datum: 2021.06.13 18:44:40 +02'00'

V Přerově dne: 31. 5. 2021

doc. Dr. Ing. Oldřich Kodym

Kontaktní informace:
Vysoká škola logistiky o.p.s. Přerov, Palackého 1381, Přerov. mail: oldrich.kodym@vslg.cz, tel.: 604 933 595

OSTRAVSKÁ UNIVERZITA
PŘÍRODOVĚDECKÁ FAKULTA

POSUDEK DISERTAČNÍ PRÁCE

Uchazeč: Ing. Petr Žáček
Fakulta aplikované informatiky
Univerzita Tomáše Bati ve Zlíně
Studijní program:

Téma práce: Návrh polymorfních struktur v symetrické kryptografii

Oponent: doc. RNDr. Martin Kotyrba, Ph.D.
Přírodovědecká fakulta
Katedra informatiky a počítačů
Ostravská univerzita

Předložená dizertační práce Ing. Petra Žáčka se věnuje polymorfním strukturám v symetrické kryptografii včetně vymezení samotného termínu polymorfních struktur v oblasti symetrické kryptografii. Výstupem práce je jednotný šifrovací systém založený na rozebraných principech s důrazem na polymorfní struktury. Dále je součástí práce i praktická implementace všech navržených struktur v komplexní polymorfní šifrovací systém s ukázkou fungování včetně zhodnocení kvality návrhu a otestování systému. Práce je dělena na 10 kapitol mimo úvod a má 132 stran včetně příloh.

Splnění cílů, zhodnocení
Hlavním cílem disertační práce je návrh vlastního komplexního kryptografického systému TSS na základě tvorby jeho dílčích částí. Samotný návrh je 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. Z tohoto úhlu pohledu se dá usuzovat, že všechny hlavní a dílčí cíle stanoveny v kapitole 1 byly splněny.

Postup řešení, konkrétní přínos
Problematice polymorfních struktur v symetrické kryptografii se věnuje omezené množství publikací. Lze nalézt pouze omezené množství příkladů algoritmů, kde je polymorfní chování implementované ve větší míře a ve většině případů nebyly tyto systémy nikdy využity v praxi. Navržený a vytvořený kryptografický systém TSS v rámci disertační práce je v tomto směru značně unikátní. Nejen že byly jeho dílčí části navrženy tak, aby jejich princip byl polymorfní, ale také kladně hodnotím, že bylo kladen důraz na sjednocení všech dílčích částí v jeden komplexně fungující kryptografický systém. Struktura práce je definovaná první částí, kde byly vymezeny základní pojmy spojené s kryptologií s důrazem na problematiku symetrickou kryptografii blokových šifer. V další části se autor věnoval krátkému vymezení terminologie z oblasti symetrické kryptografie. Dále autor provedl analýza aktuálního stavu problematiky spojené se symetrickou kryptografií, kde byl kladen důraz na blokové šifry a s nimi souvisejícími algoritmy. Následně je vymezena základní myšlenka problematiky tvorby polymorfních struktur ve vazbě na blokové šifry. Jádrem je navržený systém TSS doplněný o funkcionalitu solení, tedy zahrnutí náhodných dat do procesu šifrování a lze konstatovat, že se celý systém včetně parametrů chová nahodile v závislosti na těchto datech. Nedílnou součástí práce je i testování navrženého systému,

kde lze vidět, že i při vyřazení funkcionality šifrování, při použité stejného klíče a jen na základě změny nastavení parametrů se systém chová rozdílně a stejná vstupní otevřená data jsou zašifrována rozdílně, tak výstupem jsou rozdílná šifrová data.

Rozvoj vědního oboru a význam pro praxi

Práce má významný dopad pro praxi, avšak je zatím pouhým konceptem, proto prosím autora, aby se v rámci obhajoby vyjádřil, co brání finálnímu nasazení do praxe. Navržený systém TSS nevyužívá pouze tajný klíč k zajištění bezpečnosti, ale rozšiřuje množinu klíčů, která je dostačující pro odolání útoku hrubou silou o uživatelsky vstup ve formě nastavení potřebných parametrů. Unikátní zároveň je, že i když uživatel bude šifrovat stejným klíčem stejná otevřená data, tak při využití odlišného uživatelské nastavení parametrů budou mít šifrová data jiný tvar. V porovnání se stávajícími algoritmy není nutné sdílení solí či připojení solí na začátek šifrových dat. Tuto nutnost přenosu autor implementoval pro tajný klíč a tajné vstupní nastavení parametrů. Na základě výše uvedeného lze jasně konstatovat praktický přínos a možnou potencionální uplatnitelnost, pokud by byl systém rozsáhleji testován.

Formální úprava

Celá práce je psaná přehledně, kapitoly strukturou i logikou plynule navazují. Práce obsahuje drobné překlepy a gramatické chyby. Jako drobnou formální výtku uvádím, že citační norma není vždy použita jednotně. Disertant nepoužil číslování vzorců ani odkazovaní, ale díky kvalitnímu popisu terminologie se při studování práce čtenář neztrácí. Práce je doplněna vysvětlujícími obrázky, avšak zase některé z nich jsou v horší kvalitě a zdrojové kódy ve formě obrázku nejsou jednotné a za černým pozadím nepůsobí dobře, viz. obr.32 vs obr 34. Text obsahuje i množství zkratek, které musí čtenář vždy vyhledat v seznamu, osobně bych volil spíše přímé vysvětlení v textu. Vhodnost výběru a množství použité literatury je dostatečný a je v souladu s požadavky na disertační práci. Jako výtku vnímám seznam publikací autora, na které se nikde v textu neodkazuje.

Publikační aktivita

Publikační aktivita dizertanta je na průměrné úrovni. Byl spoluautorem 7 článků indexovaných ve sbornících konferencí evidovaných na WoS nebo Scopus, ale poslední z nich je z roku 2018, což bych chtěl osvětlit v rámci obhajoby, cožpak disertant od té doby již v oblasti publikační činnosti nic nedělal? Na druhou stranu podotýkám, že autor je jeden z 8 spoluautorů mezinárodní patentové přihlášky.

Na dizertanta mám následující otázky:

1. Proč jste výsledky své práce nepublikoval nikde v mezinárodním časopise s IF nebo ano, ale výsledky byly zamítnuty?
2. Jak by mohl být systém využít s náhradou/změnou blokové šifry?
3. Jak bude zajištěno další uplatnění systému v praxi?
4. Váš systém využívá parametricky založené solení pomocí tří náhodných solí, proč tří?
5. Jak byste hashovacímu algoritmu nebo i asymetrické kryptografii pomohl k polymorfnímu chování?

OSTRAVSKÁ UNIVERZITA
PŘÍRODOVĚDECKÁ FAKULTA

Závěrečné doporučení

Přes výše uvedené připomínky dizertační práce Ing. Petra Žáčka přináší zajímavé poznatky a splňuje kritéria na dizertační práci, a proto ji doporučuji k obhajobě.

Jestliže uchazeč uspokojivě zodpoví uvedené otázky a bude vhodně reagovat v rámci veřejné rozpravy, doporučuji mu udělit vědecko-akademickou hodnost "Philosophiae Doctor" (zkratka Ph.D.).

V Ostravě, dne 27. 5. 2021

Martin Kotyrba

Přírodovědecká fakulta Ostravské univerzity / 30. dubna 22 701 03 Ostrava / Česká republika
e-mail: martin.kotyrba@osu.cz / telefon: +420 597 092 255
prf.osu.cz

VŠB–TECHNICAL UNIVERSITY OF OSTRAVA

Faculty of Electrical Engineering and Computer Science

Ostrava, 11.6.2021

Posudek disertační práce

Autor: Ing. Petr Žáček, UTB
Název: Návrh polymorfních struktur v symetrické kryptografii

K vyhodnocení důležitosti a dopadu jakékoli vědecké činnosti je nutné ji vyhodnotit z několika hledisek, zkontrolovat její životaschopnost, důležitost atd. Disertační práce předložená uchazečem jako výsledek několikaletého výzkumu musí být hodnocena tímto způsobem. Shrnutí všech těchto bodů nám může celkem poskytnout optimální hodnocení disertační práce.

Důležitost daného tématu
Disertační práce je zaměřena na návrh polymorfních struktur v symetrické kryptografii (dále už jen NPSSK) s aplikacemi ve firemních procesech. Úroveň důležitosti kandidátské práce pochází přímo z této oblasti samotné.
Prezentovaný stav a jeho rozvoj dizertantem v NPSSK je použitelný pro širokou třídu různých problémů. Kryptologie, zvláště v poslední době je životně důležitá součást IT technologií a průmyslových aplikací. Úroveň kvality ochrany dat a komunikace je alfou a omegou jak v ochraně průmyslových, tak státních či armádních oblastech.
Z tohoto pohledu je zřejmé, že téma disertační práce má velký význam s vysoce pravděpodobným dopadem na průmyslové aplikace.

Relevantnost
V zásadě řečeno relevance a důležitost jsou vzájemně spojené body, které nelze tak snadno oddělit. Z hlediska hodnocení je nejvhodnější vyhodnotit relevantnost metod použitých v doktorské práci. Přesněji řečeno, páteř doktorské práce je založena na NPSSK a výzkumu v této oblasti. Zvolené metody jsou vědeckou komunitou ale hlavně i praxí plně akceptovatelné. Z tohoto pohledu bych chtěl říci, že v disertační práci jsou vhodným způsobem vybrány relevantní metody. Nicméně, o jejich rozpracování a přínosu lze diskutovat.

Contact:
Faculty of Electrical Engineering and Computer Science, VŠB–TU Ostava
17.listopadu 15/2172, 708 33 Ostrava-Poruba
tel.: +420 596 919 353, fax: +420 596 919 597, e-mail: ivan.zelinka@vsb.cz

Vědecký formalismus
Výzkum a následné vědecké zprávy obecně musí dodržovat některá formální pravidla. Jedná se v zásadě o to, jak psát vědecké zprávy, jak psát reference z literatury, jak počítat rovnice atd. Na základě mých zkušeností s disertační prací z různých univerzit konstatuji, že jsem v doktorské práci nenašel žádné vážné chyby, a proto lze práci považovat v principu za vědeckou práci. Práce je psána uspokojivě.
Připomínky:

- Jen bych vytkl velmi špatnou úroveň obrázků a screenshotů, jejichž kvalita je velmi špatná. Nechápu proč. Tohle přece nebylo nutné.
- Dále cíle v práci jsou definovány v 6. očíslovaných bodech, zatím co v závěru jsou jen 4 a nečíslované. Znamená to tedy, že 2 cíle nebyly splněny?
- První cíl: Nastudování teoretického základu..... mi přijde absurdní, to student začínal doktorát symetrickou kryptografií nepolíben?

Použitelnost
Na základě výsledků a aplikací NPSSK je zřejmé, že navrženou metodu v disertační práci lze aplikovat. Ty jsou omezeny pouze schopnostmi uživatele a limity vycházejícími ze samotného řešení problémů.

Obsah a struktura
V disertační práci je diskutován NPSSK s demonstrací funkcionality. Práce se skládá z doložených a diskutovaných výsledků, které ukazují, že NPSSK je vhodným tématem. K práci jsou připojeny také výsledky výzkumu kandidáta ve formě publikací. K publikacím mám však vážné výhrady, viz sekce otázek níže.
Na základě současného stavu práce lze konstatovat, že práce zřejmě představuje posun v NPSSK. Přínos dizertanta je nejasný a podpořen jen několika konferenčními příspěvky z nichž jeden (A6) je zřejmě obskurní.

Kvalita a definované cíle
Kvalitu kandidátské práce lze hodnotit po grafické i formální stránce. Z obou pohledů lze konstatovat, že úroveň kvality je uspokojivá. Cíle práce jsou dostatečně jasné, nicméně s několika nedostatky, viz můj komentář výše.

Vybrané metody
V navrhované diplomové práci uchazeč použil standardní metody a jeho výzkum se řídí standardními vědeckými kritérii a postupy.

Navrhované návrhy pro budoucí práci a otázky
V navrhované práci bych měl následující návrhy pro budoucí práci:

- Můžete ještě jednou v pár větách jasně vyjádřit Váš přínos v dané problematice?
- Ve Vámi uváděných publikacích vidím jen koference a možná jednu kapitolu. Co z toho jsou časopisy? V jakém jsou kvartilu se nachází a jaký IF mají?
- Publikace [A.6], chápu správně, že IT publikace je ve sborníku "společnosti pro zpracování polymer (plastů)" ??? Jaký má pak taková publikace význam?

Závěr

Doktorand Ing. Petr Žáček, publikoval své výsledky na několika málo konferencích a workshopech s různou úrovní kvality. Bohužel musím konstatovat, že u doktoranda bych očekával alespoň 2 – 3 časopisy s kryptologickou tématikou. To tu bohužel nevidím. Tyto publikace byly zřejmě přijaty vědeckou komunitou (i tou polymerní, [A.6]). V navrhované práci Ing. Petr Žáček jasně prokázal schopnost samostatné vědecké práce. Navrhovaná práce až na mé výhrady splňuje všechna důležitá kritéria, a proto by měla být připuštěna k obhajobě.

prof. Ing. Ivan Zelinka, Ph.D.
Department of Computer Science
Faculty of Electrical Engineering and
Computer Science VŠB-TUO
17. listopadu 2172/15
708 00 Ostrava-Poruba
Czech Republic

IT4Innovations
National Supercomputing Centre
senior researcher
Big Data Analysis Lab
www.it4i.cz

Phone: +420 597 325 863

www.ivanzelinka.eu
Member of BCS, Certified IT Professional, www.bcs.org/
http://www.springer.com/series/10624
IEEE SMC Big Data Computing