VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ

Oponentní posudek dizertační práce

Uchazeč: Ing. Peter Cíbik

Název dizertační práce: HARDWARE-ACCELERATED CRYPTOGRAPHY

Oponent: doc. Dr.-Ing, Martin Novotný

Pracoviště oponenta: ČVUT v Praze, Fakulta informačních technologií

Oponent se v posudku vyjádří dle Studijního a zkušebního řádu VUT zejména:
a) k aktuálnosti tématu dizertační práce,
b) zda dizertační práce splnila stanovený cíl,
c) k postupu řešení problému a k výsledkům dizertační práce s uvedením konkrétního přínosu doktoranda,
d) k významu pro praxi nebo rozvoj oboru,
e) k formální úpravě dizertační práce a její jazykové úrovni,
f) zda dizertační práce splňuje podmínky uvedené v § 47 odst. 4 zákona,
g) zda student prokázal nebo neprokázal tvůrčí schopnosti v dané oblasti výzkumu a zda práce splňuje nebo nesplňuje požadavky standardně kladené na dizertační práce v daném oboru. Bez tohoto závěru je posudek neplatný.
Ke každému z níže uvedených bodů je nutno doplnit stručný komentář.

Ad a) Aktuálnost tématu dizertační práce

Téma dizertační práce je velmi aktuální.

Komentář:
Disertační práce se věnuje návrhu hardwarových kryptografických komponent pro šifrovaný přenos dat ve vysokorychlostních sítích. Téma je aktuální z několika hledisek:

1. Součástí práce je efektivní implementace postkvantových schémat pro digitální podpis i pro zapouzdření klíče. Tato schémata byla standardizována v roce 2022.
2. Práce se dotýká i kvantového schématu dohody na klíči.
3. Práce míří na vysokorychlostní sítě s přenosovou rychlostí 100 Gbps.

Ad b) Splnění stanoveného cíle dizertační práce

Cíl dizertační práce byl splněn.

Komentář:
Cílem práce bylo implementovat vysokorychlostní šifrátor síťového provozu. K tomu bylo potřeba vytvořit bloky pro zapouzdření klíče (algoritmus ML-KEM, CRYSTALS-Kyber), digitální podpis (algoritmus ML-DSA, CRYSTALS-Dillithium), vysokovýkonné jádro pro kvantově odolnou šifru AES-256-GCM (Galois-Counter Mode) a vše bylo integrováno do jednoho celku. Životaschopnost řešení byla ověřena empirickým testováním, které zahrnovalo mezinárodní projekt na velkou vzdálenost a vysokorychlostní laboratorní měření.

Ad c) Postup řešení problému a výsledky disertační práce s uvedením konkrétního přínosu doktoranda

Postup řešení problému a výsledky dizertační práce jsou nadprůměrné.

Komentář:
Práce zahrnuje implementace soudobých postkvantových schémat pro digitální podpis (CRYSTALS-Dillithium) i pro dohodu na klíči (CRYSTALS-Kyber). Pro šifrování přenášených dat byl implementován algoritmus AES-256-GCM, který zajišťuje i jejich autentizaci. Všechny části byly integrovány do jednoho celku a funkčnost celku byla ověřena na reálném hardwaru. Představuje tedy proof-of-concept proveditelnosti řešení při přenosových rychlostech 100 Gbps.

Předložená disertační práce je postavena na pěti recenzovaných publikacích, konkrétně čtyřech konferenčních příspěvcích a jednom časopiseckém článku. Každá publikace má kromě autora DP a jeho školitele ještě další čtyři až šest spoluautorů (Sara Ricci a Lukáš Malina jsou spoluautory všech publikací), a proto není jednoduché posoudit přínos doktoranda. Autor sám svoje podíly v disertační práci nezmiňuje, a proto bude dobré, když se autor a jeho školitel k této otázce vyjádří při obhajobě práce. Autor disertační práce je prvním autorem dvou publikací (časopisecký článek a jeden konferenční příspěvek).

RICCI, S.; MALINA, L.; JEDLIČKA, P.; SMÉKAL, D.; HAJNÝ, J.; CÍBIK, P.; DZURENDA, P.; DOBIÁŠ, P. Implementing CRYSTALS-Dilithium Signature Scheme on FPGAs. In *ARES 2021: The 16th International Conference on Availability, Reliability and Security*. 2021. p. 1-10. ISBN: 978-1-4503-9051-4.

RICCI, S.; JEDLIČKA, P.; CÍBIK, P.; DZURENDA, P.; MALINA, L.; HAJNÝ, J. Towards CRYSTALS-Kyber VHDL Implementation. In *Proceedings of the 18th International Conference on Security and Cryptography (SECRYPT 2021)*. Science and Technology Publications, 2021. p. 760-765. ISBN: 978-989-758-524-1.

MALINA, L.; SMÉKAL, D.; RICCI, S.; HAJNÝ, J.; CÍBIK, P.; HRABOVSKÝ, J. Hardware-Accelerated Cryptography for Software-Defined Networks with P4. In *Innovative Security Solutions for Information Technology and Communications. Lecture Notes in Computer Science*. Springer, 2021. no. 2021, p. 271-287. ISSN: 0302-9743.

CÍBIK, P.; DOBIÁŠ, P.; RICCI, S.; HAJNÝ, J.; MALINA, L.; JEDLIČKA, P.; SMÉKAL, D. Pushing AES-256-GCM to Limits: Design, Implementation and Real FPGA Tests. In *Lecture Notes in Computer Science - Applied*

Cryptography and Network Security Workshops. Lecture Notes in Computer Science. Berlin: Springer, 2024. p. 303-318. ISBN: 978-3-031-61486-6. ISSN: 0302-9743.

CÍBIK, P.; RICCI, S.; DOBIÁŠ, P.; HAJNÝ, J.; MALINA, L.; HAVLÍN, J. Quantum-resistant hardware-accelerated IoT traffic encryptor. *Internet of Things*. 2025, vol. 31, no. 6, 18 p. ISSN: 2542-6605.

Ad d) Význam pro praxi nebo rozvoj oboru

Význam pro praxi nebo rozvoj oboru je nadprůměrný.

Komentář:
V disertační práci vidím zejména její praktický a experimentální význam. Autor práce (spolu)navrhnul a (spolu)vytvořil implementace state-of-the-art kryptografických primitiv, které jsou optimalizované pro vysoké přenosové rychlosti, (spolu)integroval je do jednoho funkčního celku a (spolu)ověřil funkčnost tohoto řešení při soudobých vysokých přenosových rychlostech.
Bude zajímavé prodiskutovat případný teoretický přesah předložené práce.

Ad e) Formální úprava dizertační práce a její jazyková úroveň

Formální úprava dizertační práce a její jazyková úroveň je nadprůměrné.

Komentář: Práce je psaná velmi dobrou, čitelnou angličtinou. Výklad je srozumitelný. Pouze na několika místech došlo k drobným opomenutím (nedokončená věta, zavlečené překlepy při kopírování z originálního textu), které by bylo dobré případně opravit.

Ad f) Dizertační práce splňuje podmínky uvedené v § 47 odst. 4 zákona

Dizertační práce podmínky uvedené v § 47 odst. 4*) zákona č. 111/1998 sb. o vysokých školách splňuje.

((4) Studium se řádně ukončuje státní doktorskou zkouškou a obhajobou dizertační práce, kterými se prokazuje schopnost a připravenost k samostatné činnosti v oblasti výzkumu nebo vývoje nebo k samostatné teoretické a tvůrčí umělecké činnosti. Dizertační práce musí obsahovat původní a uveřejněné výsledky nebo výsledky přijaté k uveřejnění.*

Ad g) Prokázání tvůrčí schopnosti studenta v dané oblasti výzkumu a zda práce splňuje nebo nesplňuje požadavky standardně kladené na dizertační práce v daném oboru.

Doktorand prokázal tvůrčí schopnosti v dané oblasti výzkumu a práce splňuje požadavky standardně kladené na dizertační práce v daném oboru.

Komentář:
Předložená práce představuje enormní objem prací, od implementace jednotlivých primitiv, jejich integraci, přes nasazení v provozu a provedení příslušných experimentů, až po publikaci získaných výsledků.

Celkové hodnocení:

Otázky oponenta:

1. **Práce je založena na pěti článcích, které mají po šesti až osmi spoluautorech a není jasné, na jakých částech se který autor podílel. Vyzdvihněte, prosím, svoje podíly na jednotlivých částech práce.**
2. **Na jakém hardwaru (FPGA, síťové karty, síťová infrastruktura) byly prováděny experimenty a měření?**
3. **Vyplývají z Vaší práce nějaké obecné (teoretické) poznatky?**

Dizertační práci k obhajobě ☒**doporučuji** ☐**nedoporučuji.**

Dne: 09.03.2026

Podpis: …… [redacted] ..