ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE

POSUDEK OPONENTA ZÁVĚREČNÉ PRÁCE

I. IDENTIFIKAČNÍ ÚDAJE

Název práce:	**Securing Quantum Key Distribution: Architecture, Threats, and Deployment Strategies**
Jméno autora:	**Sebastian Štefko**
Typ práce:	diplomová
Fakulta/ústav:	Fakulta elektrotechnická (FEL)
Katedra/ústav:	**Department of Computer Science**
Oponent práce:	Prof. Ing. Miroslav Vozňák, Ph.D.
Pracoviště oponenta práce:	Fakulta elektrotechniky a informatiky, VŠB – Technická univerzita Ostrava

II. HODNOCENÍ JEDNOTLIVÝCH KRITÉRIÍ

Zadání **průměrně náročné**

Hodnocení náročnosti zadání závěrečné práce.

Předložená práce je víceméně kompilačního charakteru, představuje studii shrnující současný stav poznání v oblasti QKD v kombinaci s vlastními návrhy, nicméně osobně bych u inženýrského díla mnohem raději viděl praktickou či experimentální část.

Splnění zadání **splněno**

Posuďte, zda předložená závěrečná práce splňuje zadání. V komentáři případně uveďte body zadání, které nebyly zcela splněny, nebo zda je práce oproti zadání rozšířena. Nebylo-li zadání zcela splněno, pokuste se posoudit závažnost, dopady a případně i příčiny jednotlivých nedostatků.

Předložená práce zadání splňuje, student se zabýval ve své práci všemi body dílčími body. Své připomínky uvádím v části "Další komentáře a hodnocení."

Zvolený postup řešení **správný**

Posuďte, zda student zvolil správný postup nebo metody řešení.

Práce má charakter studie, z čehož vyplývá i zvolený postup k jejímu vytvoření.

Odborná úroveň **C - dobře**

Posuďte úroveň odbornosti závěrečné práce, využití znalostí získaných studiem a z odborné literatury, využití podkladů a dat získaných z praxe.

Práce obsahuje řadu faktických chyb a nesprávných závěrů, které zmiňuji v části hodnocení, což je dle mého názoru způsobeno tím, že záběr studenta byl příliš velký. Pokud by se zaměřil na jednu specifickou oblast, např. DoS/DDoS útoky na KMS, tak by měl větší šanci téma obsáhnout lépe, navrhnout řešení vč. implementace a přispět tak k bezpečnosti QKD systémů.

Formální a jazyková úroveň, rozsah práce **A - výborně**

Posuďte správnost používání formálních zápisů obsažených v práci. Posuďte typografickou a jazykovou stránku.

Práce se četla velmi dobře, nenacházel jsem v ní prohřešky vůči anglickému jazyku, nicméně není to pohled rodilého mluvčího, čili nemůžu vyloučit, že zde chyby jsou.

Výběr zdrojů, korektnost citací **A - výborně**

Vyjádřete se k aktivitě studenta při získávání a využívání studijních materiálů k řešení závěrečné práce. Charakterizujte výběr pramenů. Posuďte, zda student využil všechny relevantní zdroje. Ověřte, zda jsou všechny převzaté prvky řádně odlišeny od vlastních výsledků a úvah, zda nedošlo k porušení citační etiky a zda jsou bibliografické citace úplné a v souladu s citačními zvyklostmi a normami.

Práce obsahuje osmdesát odkazů, přičemž použitá literatura zahrnuje články jak z poslední doby, tak původní přelomové práce od významných autorů jako např. Shannon, Feynman, Bennet, Brassard, atd. a to mi udělalo radost, že si student dal

práci a články dohledal, přečetl a použil. Dále je zde řada článků od velmi výkonných vědců současné doby, práce s literaturou se mi líbí. Mrzí mne jen, že nenašel knihu vydanou nakladatelstvím Springer s titulem "Quantum Key Distribution Networks" z roku 2022, viz https://www.springerprofessional.de/en/quantum-key-distribution-networks/23479114 , která je přímo k tématu jeho diplomky a kapitole sedmá v ní je věnována Security in QKD, myslím, že by pomohla.

Další komentáře a hodnocení

Vyjádřete se k úrovni dosažených hlavních výsledků závěrečné práce, např. k úrovni teoretických výsledků, nebo k úrovni a funkčnosti technického nebo programového vytvořeného řešení, publikačním výstupům, experimentální zručnosti apod.

Několik vybraných postřehů, kdy nesouhlasím s tvrzením v DP:

Kap. 2.3.2 "the technology is not available for implementing quantum repeaters."
Jedno z řešení kvantového opakovače je zde, https://journals.aps.org/prl/abstract/10.1103/PhysRevLett.130.213601
Btw. koncept pro QKD repeater s využitím entanglovaných fotonů je znám již poměrně dlouho.

Kap. 2.1 o QKD Networks nezahrnuje stav posledních cca deseti let, doporučuji si přečíst tento článek, https://dl.acm.org/doi/pdf/10.1145/3402192 a podívat se rovněž na případy užití z projektu OpenQKD, dke byla postavena řada zajímavých užití QKD sítí, viz zde https://openqkd.eu/openqkd-in-action/

Kap. 1.1.4. Cituji:"To successfully break RSA, factorising a 2048-bit long number, which is currently the most commonly used modulus..."
2048 bitů pro RSA je již málo, viz. https://www.johndcook.com/blog/2019/05/23/nsa-recommendations/ , doporučuji se podívat na minimální požadavky na kryptografické algoritmy od NÚKIB, pro RSA klíče je požadováno 3072 bitů https://nukib.gov.cz/download/uredni_deska/Minimalni%20pozadavky%20na%20kryptograficke%20algoritmy.pdf

Conclusion. Cituji: "In Chapter 4, we suggested several improvements for the quantum networks .... and enhancing security practice by combining keys from a quantum key distribution with other key exchange methods.
Koncept kombinování klíčů je nejen znám ale rovněž prosazován v souvislosti s PQC. Zajímavější by bylo provést implementaci a ještě lépe integraci s některými stávajícími řešeními často využívanými jako IPsec, TLS či SSH, to je hot topic, inspirace např. zde https://atos.net/wp-content/uploads/2023/04/Cybersecurity-Trustway-Paper-Hybridation-Cryptography-EN.pdf .

III. CELKOVÉ HODNOCENÍ, OTÁZKY K OBHAJOBĚ, NÁVRH KLASIFIKACE

Shrňte aspekty závěrečné práce, které nejvíce ovlivnily Vaše celkové hodnocení. Uveďte případné otázky, které by měl student zodpovědět při obhajobě závěrečné práce před komisí.

Otázka:

1. V práci je akcentován opakovaně problém konvenčních algoritmů asymterické kryptografie v době kvantových počítačů, což je správně, nicméně mi chybí alespoň zmínka o symetrické. Dokázal byste říci, jak ohrožuje Groverův algoritmus bezpečnost AES?

2. Mohl byste provést analýzu na jakou vzdálenost bychom se mohli dostat na jednom QKD spoji, vemte v úvahu např. ultra loss fibers, Twin field a současné možnosti výrobců (např. Toshiba uvádí, že zvládá link budget až 30 dB).

Předloženou závěrečnou práci hodnotím klasifikačním stupněm **C - dobře.**

Datum: 20.6.2024

Podpis: prof. Ing. Miroslav Vozňák, Ph.D.

Digitálně podepsal prof. Ing. Miroslav Vozňák, Ph.D.
Datum: 2024.06.20 17:19:11 +02'00'