Slovenská technická univerzita v Bratislave

FAKULTA ELEKTROTECHNIKY A INFORMATIKY

HQC kryptosystém

ponuka

tímový projekt

2017/2018

Vedúci projektu:

- Tomáš Fabšič
- Viliam Hromada

Vypracovali:

- Michal Zelenčík
- Samuel Podhorec
- Peter Kiska
- Tomáš Kubinec

Obsah:

1.Zloženie tímu

Michal Zelenčík
Samuel Podhorec
Peter Kiska
Tomáš Kubinec

Michal Zelenčík

Má maturitu z Gymnázia Jána Chalupku v Brezne, po ktorej absolvoval bakalárske štúdium na FEI STU v Bratislave. Už počas bakalárskeho štúdia si vybral špecializáciu na Bezpečnosť informačných systémov. V bakalárskej práci sa venoval postkvantovej kryptografii, konkrétne naprogramoval kryptosystém založený na probléme riešenia sústavy nelineárnych rovníc viacerých premenných s HFE trapdoorom. Počas tohto štúdia nadobudol pokročilé znalosti z oblasti informatiky, programovania a matematiky.

Samuel Podhorec

Absolvoval bakálárske štúdium na FEI STU odbor Aplikovaná informatika, pododbor Bezpečnosť informačných systémov. Zaujíma sa o objektové programovanie, penetračné testovanie a zabezpečovania systémov. Vo voľnom čase, mimo školských povinností, sa zaujíma o slaboprúdovú elektrotechniku a programovanie mikrokontrolérov. Daný projekt považuje za vhodnú príležitosť na získanie znalostí ohľadom postkvantovej kryptografie.

Peter Kiska

Zmaturoval na kežmarskom gymnáziu, odkiaľ jeho kroky viedli na Fakultu elektrotechniky a informatiky v Bratislave, odbor aplikovaná informatika. Pre zvýšený záujem o kryptografiu sa blizšie špecializoval na pododbor Bezpečnosť informačných systémov, ktorého je úspešným bakalárskym absolventom. V bakalárskej práci sa venoval transpozícií pomocou Rubikovej kocky. Nadobudnuté vedomosti z predmetov ako Klasické šifry, Základy kryptografie, Teória kódovania či Úvod do počítačovej bezpečnosti chce využiť v prospech riešenia tímového projektu, takisto ďaľšie nadobudnuté vedomosti ohľadom tejto témy sú vítané pre ďalší osobný rozvoj.

Tomáš Kubinec

Je absolventom bakalárskeho štúdia na Fakulte elektrotechniky a informatiky Slovenskej Technickej Univerzity v Bratislave v študijnom programe Aplikovaná informatika odbor Bezpečnosť informačných systémov. Bakalárske štúdium úspešne dokončil vypracovaním práce s názvom Návrh modelu slnečnej sústavy vo virtuálnej realite. Jeho práca sa zaoberala modelovaním v programe Unity a scriptovaním pohybov planét v jazyku C#. Má skúsenosti napríklad s jazykmi Java, C, C#, Python, Javascript. Zaujíma sa o zabezpečovanie systémov, umelú inteligenciu, kvantové počítače a v tomto projekte by mal využiť svoje dosiahnuté poznatky. Počas nasledujúcich mesiacov by rád získal skúsenosti v oblasti neurónových sietí a šifrátorov odolných voči kvantovým počítačom.

2.Motivácia

Tému tímového projektu s názvom „HQC Kryptosystém“ sme si zvolili, pretože nás zaujíma otázka budúceho vývoja šifier na zabezpečenie komunikácie v dobe post kvantovej výpočtovej techniky. Táto oblasť nám ponúka možnosť v praxi si overiť teoretické vedomosti, ktoré sme si osvojili úspešným absolvovaním Bakalárskeho štúdia v odbore bezpečnosť informačných systémov. Naším cieľom je nadviazať na knižnicu BitPunch, vyvinutú predošlými generáciami študentov a na jej základe implementovať funkčný HQC Kryptosystém. Knižnica je vyvinutá v programovacom jazyku C, v ktorom majú všetci členovia tímu skúsenosti z predošlého štúdia.

Všetci členovia tímu sa v minulosti efektívne podieľali na spoločných zadaniach, čo je dobrý základ pre úspešné dosiahnutie stanoveného cieľa.

3.Zadanie projektu

V roku 1999 dokázal P. W. Shor, že s využitím kvantového počítača je možné riešiť problémy prvočíselnej faktorizácie a diskrétneho logaritmu v polynomiálnom čase. Dôsledkom tohto zistenia je, že v prípade, že technologický pokrok umožní postavenie dostatočne výkonného kvantového počítača, nebudú v súčasnosti používané asymetrické kryptosystémy môcť byť považované za bezpečné. Mnoho vedcov sa v súčasnosti domnieva, že postavenie výkonného kvantového počítača je už iba otázkou času a niektorí odborníci dokonca predpovedajú, že do 20 rokov budú existovať kvantové počítače s výkonom dostatočným na prelomenie akejkoľvek momentálne používanej asymetrickej šifry. V roku 2016 vyhlásil americký národný inštitút štandardov a technológie (National Institute of Standards and Technology, NIST) súťaž, z ktorej majú vzísť návrhy štandardov pre asymetrické kryptosystémy odolné voči útokom kvantovými počítačmi (takzvané postkvantové kryptosystémy). Do 30-teho novembra 2017 prijíma NIST návrhy postkvantových kryptosystémov. Prijaté návrhy budú v nasledujúcich 3-5 rokoch verejne analyzované, s cieľom vybrať najlepšie kryptosystémy a tie odporučiť ako štandardy pre postkvantovú kryptografiu.

Na nedávnej konferencii PQcrypto 2017 oznámili francúzski výskumníci Aguilar, Blazy, Deneuville, Gaborit a Zemor, že plánujú do NIST súťaže zaslať svoj kryptosystém HQC. HQC kryptosystém je založený na teórii kódovania a bol zverejnený v článku https://eprint.iacr.org/2016/1194.pdf . Cieľom tímového projektu je implementovať

tento kryptosystém v jazyku C. Vytvorenie implementácie HQC kryptosystému by umožnilo testovanie tohto kryptosystému na FEI STU.

4.Čo môžeme poskytnúť

Naším cieľom, počas nasledujúcich 2 semestrov bude oboznámiť sa s problematikou kvantových počítačov, spôsobe ich fungovania a ich výpočotov. Oboznámime sa s kryptografiou súvisiacou s HQC kryptosystémom, naštudujeme matimetické pozadie fungovania šifier ktoré budeme implementovať a to hlavne QCLDPC a QCMDPC šifry.

Ďalším naším cieľom bude implementovanie QCLDPC šifrovania pomocou knižnice BitPunch, z ktorého využijeme Genrovanie Matíc a čistenie zašumenéj správy. Následne budeme pracovať na implentácii dešifrovania.

Následne by sme sa chceli venovať protokolu Ouroboros, ktorý slúži na bezpečnú a efektívnu výmenu kľúča medzi komunikujúcimi stranami. Toto by sme taktiež chceli implementovať za pomoci knižnice BitPunch.

Každej ďalšej čiastkovej úlohe sme otvorení a radi sa jej budeme venovať, keďže táto téma je pre nás veľmi zaujímavá.

5.Zdroje projektu

Vývoj bude prebiehať na zariadeniach členov tímu. Na vývoj budeme používať knižnicu BitPunch vyvinutú v jazyku C#. Vývoj bude prebiehať na operačnom systéme Linux, s ktorým je spomínaná knižnica kompatibilná.

6.Priestory

Tým sa bude pravidelne raz týždenne stretávať v priestoroch FEI STU. Ostatný vývoj bude prebiehať vzdialene, komunikáciu cez AIS a sociálne siete.

7.Čas konzultácii

Po preštudovaní a porovnaní rozvrhov členov tímu a zadávateľov projektu, sme sa zhodli ako na najlepšom termíne konzultácii určenom na štvrtok 12:00. Stretávať sa budeme pravidelne každý týždeň v prípade, že bude potrebné prekonzultovať čiastkové úlohy, alebo doplniť na riešenie ďalšie úlohy.