Projekt MPC-KRY

Zabezpečení dat pomocí algoritmů postkvantové kryptografie

Autoři: Dušan Sýkora, Richard Stupka, Vojtěch Svoboda, Martin Dundálek

Obsah

Úvod

Tento projekt se zabývá návrhem a implementací peer-to-peer aplikace umožňující zabezpečenou komunikaci pomocí technik postkvantové kryptografie. S nástupem kvantových počítačů budou tradiční kryptografické algoritmy, jako jsou RSA a ECC, považovány za nedostatečně bezpečné, jelikož kvantové algoritmy (zejména Shorův algoritmus) mohou efektivně řešit problémy faktorizace celých čísel a diskrétního logaritmu, na kterých jsou tyto algoritmy založeny.

Aplikace umožní uživatelům navazovat přímá spojení s jinými uživateli v síti, bez nutnosti centrálního serveru, a provádět tři základní kryptografické operace:

1. Výměna tajného klíče prostřednictvím postkvantových algoritmů založených na veřejném klíči

2. Důvěrný přenos dat šifrovaný pomocí symetrických algoritmů

3. Podepisování dat s využitím postkvantových podpisových algoritmů

Aplikace bude nabízet **více algoritmů** pro každou z těchto operací, takže uživatelé si budou moci vybrat konkrétní algoritmus podle svých potřeb. Operace budou logovány a logy i klíče budou bezpečně uloženy.

Cíle projektu

Hlavní cíle projektu jsou:

1. **Vytvořit funkční P2P komunikační síť**, která umožní přímou komunikaci mezi uživateli bez centrálního serveru

2. **Implementovat postkvantové algoritmy** pro výměnu klíčů a digitální podpisy

3. **Umožnit důvěrnou komunikaci** prostřednictvím symetrických šifrovacích algoritmů

4. **Poskytnout uživatelsky rozhraní** pro výběr kryptografických algoritmů a správu komunikace

5. **Implementovat bezpečné logování** kryptografických operací s důrazem na ochranu citlivých informací

6. **Zajistit bezpečné ukládání klíčů a logů** na lokálním zařízení

Měřitelné cíle projektu:

- Úspěšná implementace minimálně dvou algoritmů pro každou z kryptografických operací
- Dosažení přenosové rychlosti dostatečné pro běžnou komunikaci a přenos souborů
- Vytvoření intuitivního uživatelského rozhraní s možností volby algoritmů a parametrů zabezpečení
- Implementace robustního systému logování s vhodnou granularitou informací

Teoretická část

V této části je popsána teorie týkající se projektu.

Postkvantová kryptografie

Postkvantová kryptografie (PQC) označuje kryptografické systémy, které jsou považovány za odolné vůči útokům pomocí kvantových počítačů. Tradiční kryptografické algoritmy, jako jsou RSA, DSA a ECC, jsou založeny na matematických problémech, které lze efektivně řešit pomocí kvantových algoritmů, zejména Shorova algoritmu. Aby byly kryptografické systémy bezpečné i v éře kvantových počítačů, je nutné je postavit na jiných matematických problémech, které jsou považovány za obtížné i pro kvantové počítače. Hlavní směry postkvantové kryptografie jsou popsany dále ve studii.

Kryptografie založená na mřížkách (Lattice-based Cryptography)

Kryptografické systémy založené na mřížkách využívají obtížnost problémů spojených s mřížkami v n-dimenzionálním prostoru. Mezi tyto problémy patří problém nejkratšího vektoru (SVP), problém nejbližšího vektoru (CVP) a Learning With Errors (LWE). Výhodou těchto systémů je jejich relativní efektivita a silná matematická základna. Algoritmy jako CRYSTALS-KYBER a NTRU patří do této kategorie.

CRYSTALS-KYBER je algoritmus pro ustanovení klíče založený na problému Module Learning With Errors (MLWE). Tento problém je variantou problému LWE, která využívá modulární strukturu pro zlepšení efektivity. KYBER nabízí dobrou rovnováhu mezi velikostí klíčů, rychlostí a bezpečností.

NTRU (N-th degree TRUncated polynomial ring) je jeden z nejstarších postkvantových kryptosystémů. Byl vyvinut v roce 1996 a je založen na problému hledání krátkých vektorů v mřížkách. NTRU je rychlý a má relativně malé veřejné klíče ve srovnání s jinými postkvantovými algoritmy.

FrodoKEM je konzervativnější přístup, který nepřidává další algebraickou strukturu k problému LWE. Tím se vyhýbá potenciálním slabinám strukturovaných variant, ale za cenu větších klíčů a nižší efektivity.

ML-DSA je postkvantový algoritmus pro digitální podpisy založený na module-lattice problémech. Používá podobnou strukturu jako Dilithium a poskytuje silnou bezpečnost s efektivními podpisy a relativně malou velikostí veřejných klíčů.

ML-KEM je postkvantový algoritmus pro výměnu klíčů, který je založen na module-lattice (mřížkových) problémech, což jej činí odolným vůči kvantovým útokům. Používá metody podobné Kyberu a je jedním z finalistů v NIST standardizaci.

Kryptografie založená na kódech (Code-based Cryptography)

Tyto systémy jsou založeny na obtížnosti dekódování náhodných lineárních kódů. Nejznámějším příkladem je McElieceův kryptosystém, který byl navržen již v roce 1978. Systémy založené na kódech mají obvykle velké veřejné klíče, ale nabízejí rychlé šifrování a dešifrování.

Classic McEliece je moderní implementace McElieceova kryptosystému, která používá Goppaovy kódy. Jedná se o jeden z nejdéle studovaných postkvantových algoritmů s velmi silnými bezpečnostními zárukami.

HQC je asymetrický šifrovací algoritmus založený na problémech s kódy v teorii kódování (code-based cryptography). Nabízí vysokou úroveň bezpečnosti a je odolný proti kvantovým útokům díky své konstrukci založené na dekódování chybových vzorů v kódech.

Kryptografie založená na hashovacích funkcích (Hash-based Cryptography)

Podpisové systémy založené na hashovacích funkcích, jako jsou Lamportův jednorazový podpis, Merkleovy stromy a jejich modernější varianty (XMSS, SPHINCS+), nabízejí silné bezpečnostní záruky. Jejich bezpečnost je založena pouze na vlastnostech hashovacích funkcí, což je činí velmi důvěryhodnými.

SPHINCS+ je bezstavový hashovací podpisový systém, který kombinuje několik různých technik k vytvoření praktického podpisového schématu. Jeho bezpečnost závisí pouze na vlastnostech použitých hashovacích funkcí.

Kryptografie založená na multivariantních polynomech (Multivariate Cryptography)

Tyto systémy jsou založeny na obtížnosti řešení systémů multivariantních polynomiálních rovnic nad konečnými tělesy. Jsou obecně efektivní pro ověřování podpisů, ale mají velké veřejné klíče.

Rainbow je multivariantní podpisové schéma, které nabízí velmi rychlé ověřování podpisů a krátké podpisy. Je založeno na struktuře olejovo-octových polynomů (Oil and Vinegar).

Kryptografie založená na izogeniích (Isogeny-based Cryptography)

Systémy založené na izogeniích mezi supersingulárními eliptickými křivkami představují novější směr v postkvantové kryptografii. Nabízejí nejmenší velikosti klíčů ze všech postkvantových kandidátů, ale jsou výpočetně náročnější.

SIKE (Supersingular Isogeny Key Encapsulation) je algoritmus pro ustanovení klíče založený na problému hledání izogenií mezi supersingulárními eliptickými křivkami. Vyniká velmi malými veřejnými klíči, ale je výpočetně náročnější než jiné metody

Symetrická kryptografie v post-kvantovém prostředí

I když je symetrická kryptografie považována za relativně odolnou vůči kvantovým útokům, Groverův algoritmus může poskytnout kvadratické zrychlení při hledání klíčů hrubou silou. Proto je doporučeno zdvojnásobit délku klíčů pro symetrické algoritmy v postkvantovém prostředí.

AES-256-GCM je moderní symetrická šifra s 256bitovým klíčem, která kombinuje blokovou šifru AES a autentizační režim GCM pro zajištění jak důvěrnosti, tak integrity dat. Je široce používána v bezpečnostních protokolech, jako je TLS nebo IPsec.

ChaCha20-Poly1305 je moderní alternativní šifra k AES, která kombinuje ChaCha20 jako proudovou šifru a Poly1305 pro autentizaci zpráv. Je optimalizovaná pro výkon na procesorech bez AES akcelerace a nabízí vysokou odolnost vůči útokům díky své jedinečné konstrukci**.**

Standardizace postkvantové kryptografie

Národní institut standardů a technologie USA (NIST) zahájil proces standardizace postkvantových kryptografických algoritmů v roce 2016. Tento proces je podobný předchozím soutěžím pro standardizaci AES a SHA-3. V červenci 2022 NIST oznámil první algoritmy vybrané pro standardizaci.

CRYSTALS-KYBER pro ustanovení klíče

CRYSTALS-DILITHIUM, FALCON a SPHINCS+ pro digitální podpisy Proces standardizace pokračuje pro další kandidáty, včetně algoritmů založených na kódech a dalších přístupech

Peer-to-Peer sítě

Peer-to-peer (P2P) sítě jsou distribuované systémy, kde každý uzel může fungovat jako klient i jako server.

Hlavní charakteristiky P2P sítí zahrnují:

- **Decentralizace**: Neexistuje centrální server, který by řídil komunikaci
- **Škálovatelnost**: Síť se může efektivně rozrůstat s počtem uzlů
- **Robustnost**: Selhání jednoho uzlu neovlivní celou síť Autonomie: Uzly mohou nezávisle rozhodovat o svých zdrojích

Aktuální stav řešení

Projekt je ve fázi analýzy a návrhu, byla nastudovaná a popsána problematika k projektu a postkvantové kryptografie.

Klíčové komponenty a požadavky na systém jsou:

1. Byly vybrány vhodné kryptografické algoritmy pro implementaci:
    - Pro ustanovení klíče: **ML-KEM, HQC a FrodoKEM**
    - Pro symetrické šifrování: **AES-256-GCM a ChaCha20-Poly1305**
    - Pro digitální podpisy: **ML-DSA a SPHINCS+**
2. Byla navržena základní architektura aplikace:
    - Síťová vrstva pro P2P komunikaci
    - Kryptografická vrstva pro implementaci kryptografických algoritmů
    - Aplikační vrstva pro logiku aplikace
    - Prezentační vrstva pro uživatelské rozhraní
3. Byly identifikovány vhodné knihovny pro implementaci v Pythonu:
    - liboqs (Open Quantum Safe) pro postkvantové algoritmy
    - pyca/cryptography pro symetrické algoritmy
    - socket a asyncio pro síťovou komunikaci PyQt5 pro uživatelské rozhraní

Plán dalšího postupu

Další postup vývoje projektu zahrnuje následující kroky:

- **Fáze I:** Implementace základních komponent, včetně vývoje síťové vrstvy pro P2P komunikaci a integrace kryptografických knihoven. Dále bude navrženo API pro kryptografickou vrstvu a vytvořeno základní testovací rozhraní. (*Tato fáze je již dokončena.*)
- **Fáze II**: Implementaci kryptografických funkcí, jako je výměna klíčů, šifrovaný přenos dat a digitální podpisy, včetně bezpečného ukládání klíčů a logů. (*Tato fáze je již dokončena.*)
- **Fáze III:** Návrh a implementaci uživatelského rozhraní, včetně interaktivních prvků pro výběr algoritmů a vizualizace informací o bezpečnosti a operacích. (*Tato fáze je již dokončena.*)
- **Fáze IV:** Testování a optimalizaci, což zahrnuje testování funkčnosti, bezpečnosti, optimalizaci výkonu a zátěžové testování v simulovaném prostřed

- **Fáze V:** finalizace projektu, včetně vytvoření uživatelské a vývojářské dokumentace a přípravy na předání projektu a jeho zhodnocení.

Závěr

Projekt zaměřený na zabezpečení dat pomocí postkvantové kryptografie se soustředí na vývoj aplikace pro bezpečnou komunikaci mezi uživateli v peer-to-peer síti, která využívá algoritmy odolné vůči kvantovým počítačům. S nárůstem kvantových technologií bude důležité přejít na nové kryptografické metody, které zaručí bezpečnost komunikace v nadcházející kvantové éře. V projektu byly implementovány postkvantové algoritmy pro výměnu klíčů a digitální podpisy, což umožňuje vysoce bezpečnou a efektivní výměnu informací.

Aplikace navržená v tomto projektu spojuje principy postkvantové kryptografie se symetrickým šifrováním pro zajištění důvěrnosti komunikace, zatímco všechny kryptografické operace jsou bezpečně logovány a uchovávány. Projekt se nachází ve fázi vývoje a již byly vybrány klíčové kryptografické algoritmy a navržena architektura aplikace. Dalšími kroky vývoje budou implementace kryptografických funkcí, vývoj uživatelského rozhraní a optimalizace celého systému.

Autoři a jejich přínos

Všichni členové týmu se podíleli na **návrhu samotné aplikace**, vzájemných konzultacích a testování. **Programování** bylo týmovou aktivitou, kde měl hlavní podíl **Dušan Sýkora**, ale ostatní členové se aktivně podíleli na různých částích aplikace.

Dušan Sýkora – programovaní, dokumentace, testování a ladění

Richard Stupka – dokumentace, organizace práce, testování a ladění

Martin Dundálek – ladění kódu, dokumentace, testování a optimalizace

Vojtěch Svoboda – optimalizace, dokumentace, testování a ladění

Reference

1.Bernstein, D. J., & Lange, T. (2017). Post-quantum cryptography. Nature, 549(7671), 188-194.

2. NIST (2019). Status Report on the First Round of the NIST Post-Quantum Cryptography Standardization Process. NISTIR 8240.

3. Alagic, G., et al. (2022). Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardization Process. NISTIR 8413.

4. Chen, L., et al. (2016). Report on Post-Quantum Cryptography. NISTIR 8105.

5. Grassl, M., et al. (2016). Applying Grover's algorithm to AES: quantum resource estimates. In Post-Quantum Cryptography (pp. 29-43).

6. Hoffstein, J., Pipher, J., & Silverman, J. H. (1998). NTRU: A ring-based public key cryptosystem. In Algorithmic number theory (pp. 267-288).

7. Paquin, C., Stebila, D., & Tamvada, G. (2020). Benchmarking post-quantum cryptography in TLS. In PostQuantum Cryptography (pp. 72-91).