

|  |  |
| --- | --- |
| VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ  BRNO UNIVERSITY OF TECHNOLOGY  FAKULTA ELEKTROTECHNIKY  A KOMUNIKAČNÍCH TECHNOLOGIÍ  FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION  ÚSTAV TELEKOMUNIKACÍ  DEPARTMENT OF TELECOMMUNICATIONS  Zabezpečené úložiště pomocí postkvantové  kryptografie | |
| SEMESTRÁLNÍ PRÁCE  SEMESTRAL THESIS |  |
| AUTOŘI PRÁCE  AUTHOR | Tadeáš Zachoval, Adam Turek,  Tomáš Závada, Nguyễn Phúc |
| BRNO 2023 |  |

Obsah

[Úvod 1](#_bookmark0)

[Cíle 2](#_bookmark1)

[Teoretická část 2](#_bookmark2)

[Zabezpečené uložiště 2](#_bookmark3)

[Komunikace peer to peer 2](#_bookmark4)

[Symetrická kryptografie 2](#_bookmark5)

[Advanced Encryption Standard (AES) 3](#_bookmark6)

[Postkvantová kryptografie 3](#_bookmark7)

[Aktuální stav 5](#_bookmark8)

[Navázání peer-to-peer za pomocí serveru 5](#_bookmark9)

[Spojení P2P 5](#_bookmark10)

[Formát komunikace 5](#_bookmark11)

[Grafické uživatelské rozhraní 6](#_bookmark12)

[Vývojový diagram 6](#_bookmark13)

[Následující kroky 6](#_bookmark14)

[Závěr 7](#_bookmark15)

[Příloha 8](#_bookmark16)

[Literatura 9](#_bookmark17)

# Úvod

V posledních třech desetiletích se kryptografie s veřejným klíčem stala nedílnou součástí globální digitální komunikační infrastruktury. Bezpečnost mnoha dnes používaných důležitých komunikačních protokolů se opírá o tři základní kryptografické funkce: šifrování s veřejným klíčem, digitální podpisy a výměnu klíčů. V současné době se tyto funkce realizují především pomocí Diffie- Hellmanovy výměny klíčů, kryptosystému RSA a kryptosystému eliptických křivek. Bezpečnost těchto kryptosystémů je založena na obtížných problémech, jako je numerická analýza, diskrétní logaritmy.

V roce 1994 Peter Shor z Bellových laboratoří ukázal, že kvantové počítače, nová technologie, která využívá fyzikální vlastnosti hmoty a energie pro výpočty, mohou řešit složité problémy efektivněji než výpočty pomocí tradičních počítačů. To vytváří riziko, že všechny informační systémy využívající kryptografii s veřejným klíčem přestanou být bezpečné. Stojíme před otázkou: Můžeme se ubránit útočníkovi, který používá klasické a kvantové výpočty?

Vznik kvantových počítačů přilákal vědce zabývající se kryptografií k řešení problému budoucího zabezpečení informací, které by bylo odolné vůči útokům pomocí kvantových počítačů. Tato věda se nazývá postkvantová kryptografie. Výsledkem této vědy jsou různé přístupy ke kvantovému šifrování. Za zmínku stojí např: Algoritmus učení s chybami (LWE), McElieceův kryptosystém, NTRU kryptosystém, Kvantová distribuce klíčů a Merkle-Damgårdova konstrukce hashe. **Chyba! Nenalezen zdroj odkazů.**

V tomto projektu přezkoumáme a vyhodnotíme přístup využívající algoritmus McEliece. Poté bude algoritmus aplikován na sestavení databáze s vlastnostmi kompletní aplikace. Projekt je založen na dostupných knihovnách v kombinaci s programovacím jazykem Python s cílem ověřit teoretický základ a demonstrovat použití postkvantové kryptografie v praxi.

# Cíle

Cílem našeho semestrálního projektu je vytvořit zabezpečené úložiště pomocí postkvantové kryptografie. Aplikace bude schopná vytvořit zabezpečené spojení typu klient-klient (peer-to-peer), které bude šifrováno pomocí symetrického šifrovacího algoritmu. K výměně/ustanovení symetrického klíče mezi klienty využijeme algoritmus postkvantové kryptografie. Úložiště bude ovládáno pomocí grafického rozhraní. Při přenosu dat mezi úložištěm a uživatelem bude zajištěna důvěrnost, integrita a autentičnost přenášených dat.

Úložiště bude vytvářet logy o přístupu a akcích uživatele (kdy byl autentizován, jaké soubory četl, změnil, kopíroval, smazal, stahoval, nahrával apod.) a informace o provedených akcích (čas, činnost, použitý algoritmus, velikost zpracovávaného souboru atd.). Logy o přístupu a akcích uživatele budou chráněny proti jejich změně.

# Teoretická část

## Zabezpečené uložiště

Zabezpečené úložiště [(1)](#_bookmark18)je důležitou součástí bezpečnosti informací, která se týká chráněného ukládání cenných nebo citlivých dat. Data mohou zahrnovat osobní nebo finanční informace, duševní vlastnictví, obchodní tajemství nebo jiné důvěrné informace. Zabezpečené úložiště je tak nezbytné pro zajištění důvěrnosti, integrity a pro dostupnost informací. Potřeba zabezpečeného úložiště vzniká v důsledku rostoucí závislosti na ukládání digitálních dat a stále rostoucích hrozeb kybernetických útoků a narušení bezpečnosti dat.

## Komunikace peer to peer

Peer-to-peer (P2P) [(3)](#_bookmark19)je model komunikace, ve které disponují jednotlivé strany rovnoměrnými možnostmi a kterákoli z nich může iniciovat komunikační relaci. Při tomto typu komunikace každý počítač funguje jako klient i server zároveň a umožňuje přímou výměnu dat mezi nimi. U komunikace klient-klient je nevýhodou, že soubory nejsou centrálně zálohovány a uspořádány v konkrétní sdílené oblasti, ale jsou ukládány v samostatných počítačích. Výhodou je že sítě pracují bez serveru, kde díky tomu není nutnost správce serveru, jelikož každý uživatel má ve správě svůj počítač

Klienti přitom působí jako pracovní stanice, přičemž nesdílejí informační a komunikační zdroje. Také mohou lépe provádět aktualizaci aplikací a souborů, protože tyto soubory jsou ukládány pouze na jednom jediném počítači

## Symetrická kryptografie

Symetrická kryptografie [(4)](#_bookmark20) využívá k šifrování i dešifrování elektronické informace pouze jeden klíč (tajný klíč). Subjekty komunikující prostřednictvím symetrického šifrování si musí vyměnit klíč, aby jej bylo možné použít při dešifrování. Využíváním algoritmů symetrického šifrování jsou data "zakódována" takovým způsobem, že je nemůže rozpoznat žádná osoba, která nedisponuje tajným

klíčem k dešifrování. Po obdržení zprávy určeným příjemcem, který vlastní klíč, algoritmus obrátí svůj postup tak, aby se zpráva vrátila do své původní čitelné podoby.

Symetrická kryptografie je účinným nástrojem pro bezpečnou komunikaci, ale zároveň není nezranitelná. Mezi hlavní zranitelnosti symetrické kryptografie patří: Distribuce klíčů, Správa klíčů, Opakované použití klíče, Kryptoanalýza, Hrozby zevnitř

#### Rozdělení:

* Blokové šifry
  + Advanced Encryption Standard (AES)
  + Blowfish
  + Data Encryption Standard (DES)
  + Rivest Cipher 2 (RC2)
  + RC5
  + Triple DES
* Proudové šifry
  + FISH
  + RC4

## Advanced Encryption Standard (AES)

AES [(5)j](#_bookmark21)e nejrozšířenější symetrická šifra v současné době. Na rozdíl od DES, mohou být klíč a bloky nezávisle zvoleny. Velikosti klíče mohou být 128, 192 nebo 256 bitu a velikost bloku 128 bitu.

#### Rundovní operace:

* substituce (S-box): matice obsahující všechny možné kombinace po 8bitové sekvenci,
* row shift (bajtová permutace): jedná se o permutaci, kdy:
  + První řádek stavu se nepozmění.
  + Druhý řádek je posunut o 1 bajt doleva kruhovým způsobem.
  + Třetí řádek je posunut o 2 bajty doleva kruhovým způsobem.
  + Čtvrtý řádek je posunut kruhovým způsobem o 3 bajty doleva.
* column mix (lineární transformace): jedná se o substituci s využitím aritmetiky Gaisového pole (28). S každým sloupcem se pracuje jednotlivě a každá byte je namapován na novou hodnotu.
* key addition: bitový XOR s rundovním klíčem.

I když existují útoky na oslabené verze AES (nižší počet rund a menší velikost klíčů), jde o bezpečný protokol, který je využitý v TLS, OpenSSH a většině ostatních současných protokol.

## Postkvantová kryptografie

Postkvantová kryptografie [(6)](#_bookmark22)je oblast kryptografie, jejímž cílem je vývoj kryptografických algoritmů, které jsou odolné vůči útokům kvantových počítačů. Podnětem pro postkvantovou kryptografii je potenciální hrozba, kterou kvantové počítače představují pro klasické kryptografické algoritmy. Pro kvantové počítače se předpokládá, že jsou schopny řešit některé výpočetní problémy, jako je faktorizace velkých čísel a výpočet diskrétních logaritmů, mnohem rychleji než klasické počítače. Zmíněné problémy reprezentují základ mnoha klasických kryptografických algoritmů, včetně těch, které se používají pro výměnu klíčů. Počet klíčů generovaných v postkvantové kryptografii závisí na konkrétním použitém algoritmu. Například algoritmy založené na mřížce (Lattice), jako jsou NTRUEncrypt a

NewHope, používají klíče o délce obvykle 256 až 512 bitů. Jiné algoritmy, jako je podepisování na základě hašování (XMSS) a kryptografie na základě kódu (McEliece), používají delší klíče, například 768 až 1536 bitů.

V oblasti výzkumu postkvantové kryptografie se v současné době pracuje především se čtyřmi hlavními typy přístupů:

* Kryptografie založena na mřížkách [(7)](#_bookmark23): toto kryptografické schéma je postaveno na matematických problémech kolem mřížek. Mřížka v tomto kontextu připomíná mřížku grafického papíru – využívá množinu bodů umístěných na průsečících mřížky přímek. Tato mřížka není v žádném smyslu konečná. Místo toho mřížka popisuje vzor, který pokračuje do nekonečna. K odvození soukromého klíče z veřejného klíče by bylo nutné prohledat všechny možnosti hrubou silou, a i když kvantové počítače mohou toto prohledávání urychlit, stále by trvalo značně dlouho a nereálně. Předpokládá se, že ani kvantový počítač není schopen vyřešit těžké problémy založené na mřížkách v rozumném čase. Jako příklad algoritmů na bázi mřížky lze uvést CRYSTALS-KYBER a CRYSTALS-Dilithium.
* Multivariační kryptografie [(8)](#_bookmark24): je založena na řešení soustav vícerozměrných rovnic. V multivariační kryptografii je veřejným klíčem vícerozměrný polynom a soukromým klíčem je řešení příslušné soustavy rovnic. Proces šifrování je transformaci zprávy s otevřeným textem na polynom, který je poté vyhodnocen pomocí polynomu veřejného klíče. Výsledná hodnota je šifrovaný text, který lze dešifrovat pomocí soukromého klíče. Jako příklad algoritmů na bázi multivariační kryptografie lze uvést například Rainbow Scheme.
* Kryptografie založena na kódování [(9)](#_bookmark25): kryptosystémy, v nichž algoritmické primitivum (základní jednosměrná funkce) pracuje s kódem pro opravu chyb C. Toto primitivum spočívá v přidání chyby ke slovu C nebo ve výpočtu relativního syndromu k matici kontroly parity C.

Jedním z nejznámějších kryptografických algoritmů založených na kódech je schéma McEliece. Soukromý klíč je náhodný binární neredukovaný Goppa kód a veřejným klíčem je náhodná generátorová matice z náhodně permutované verze tohoto kódu. Šifrovaný text je kódové slovo, do kterého byly přidány některé chyby, a pouze vlastník soukromého klíče (Goppa kódu) může tyto chyby odstranit. Není znám žádný útok, který by pro tento systém představoval vážnou hrozbu

* Kryptografie založená na supersingulárních eliptických křivkách [(10)](#_bookmark26): s použitím supersingulárních křivek, jsou křivky generovány během výměny klíčů. Při této variantě metody jsou tajné klíče izogenické. Z toho vyplývá, že body jedné eliptické křivky mohou být mapovány na jinou křivku při zachovaní vrcholů křivek a samotné struktury křivky. To využivá skutečnost, že lze namapovat více bodů do jednoho bodu. Veřejným klíčem je pak samotná supersingulární eliptická křivka. Jako příklad algoritmů na bázi supersingulárních eliptických křivkách lze uvést například Diffie-Hellman key echange (SIDH), nebo Supersingular isogeny Key Encapsulation (SIKE).

# Aktuální stav

V této kapitole se zaměříme na aktuální stav semestrálního projektu. V rámci realizace projektu je vytvořen GitHub repositář (<https://github.com/ChybaYg/Projekt-Krypto>). Jako programovací jazyk byl zvolen Python.

Členové: Tomáš Závada – Navázání peer-to-peer spojení, Tadeáš Zachoval – Grafické uživatelské rozhraní a propojení GUI se serverem, Adam Turek – Grafické uživatelské rozhraní a kontrolní studie, Nguyễn Phúc – kontrolní studie

Projekt tvoříme jako skupina. Na pravidelných společných schůzkách na něm pracujeme, každý přichází se svými nápady a návrhy.

## Navázání peer-to-peer za pomocí serveru

K vytvoření spojení peer-to-peer je v naší implementaci využito serveru, který oběma klientům následně předá informace o druhém klientovi. Z počátku je tak třeba počkat, než se na server oba klienti připojí. Jakmile je tohoto dosaženo, každému z nich pošle zprávu obsahující cílovou IPv4 adresu a port. Po ustanovení spojení mezi klienty, je možno server vypnout, jelikož v komunikaci mezi klienty není nadále zapojený.

### Spojení P2P

Po získání adresy a portu je na každého z klientů odeslán testovací paket s daty o velikosti 0 byte, pro zjištění, zda je skutečně možné se s druhým klientem spojit. Každý z klientů má od tohoto bodu jinou funkcionalitu. V naší práci rozlišujeme uživatelského klienta a klienta úložiště. Uživatelský klient má vytvořené UI a zadává klientovi úložiště, povely pro práci se soubory. Prozatím nejsou implementovány všechny funkce, které je potřeba k plnohodnotnému využívání úložiště.

Funkce, které jsou již implementovány:

* CreateFile
* ReadFile
* DeleteFile
* DeleteDirectory
* CreateDirectory

### Formát komunikace

V tuto chvíli je komunikace přenášena nezabezpečeně jako byte array. K převodu do byte array je využito funkce encode a zpětný převod do formátu string zajišťuje funkce decode. Data jsou rozdělena do tří skupin, které jsou ve formátu string odděleny středníkem.

Jednotlivé části by se daly pojmenovat takto:

* Název funkce
* Parametry funkce
* Přenášená data

V rámci parametrů funkce je potřebné oddělit více parametrů. Tohoto je dosaženo oddělením jednotlivých parametrů čárkou.

## Grafické uživatelské rozhraní

Při vytváření základní kostry grafického uživatelského rozhraní (GUI) byl využito vývojového prostředí Qt designer jenž usnadňuje tvorbu GUI a je provázán s multiplatformním frameworkem Qt pro python. V tomto programu byl prvně vytvořen vzhled všech nezbytných oken, které jsou nutné k chodu aplikace. Následně byl kód implementován do vývojového prostředí.

Jmenovitě jsou to okna pro připojení k serveru skrz IP adresu verze 4 a port. V tomto okně je ošetřeno vkládání správného tvaru IP adresy a port je nastaven na maximální hodnotu 65536. Dalším oknem aplikace je přihlašovací okno, které slouží pro přihlášení či vytvoření nového uživatele. V tuto chvíli není vytvořen žádný uživatel, ani heslová politika, který by byl autentizován do datového uložiště.

Momentálně je vstup do aplikace možný bez ověření uživatele. V případě nevyplnění IP adresy a portu ve správném rozsahu nebo přihlašovacího pole je uživatel informován o chybě a vyzván k jeho vyplnění. Informace o vložených údajích do přihlašovacího pole zatím nejsou nijak ochráněna. Poslední okno je samotné uložiště, kde je naprogramováno pět funkčních tlačítek (home, upload, download, about us a sign out). Tlačítko „home“ pracuje ke zobrazení současného stavu uložistě, v současné době je zatím zobrazováno místní uložiště. Tlačítko „upload“ a „download“ pracuje k nahrání či stažení souborů do/z uložiště, kdy jejich funkcionalita bude doplněna. V případě tlačítka

„about us“ je zobrazena informační tabule s odkazem na náš GitHub a informacích o projektu. Poslední tlačítko je pro odhlášení uživatele, kdy v případě jeho stisknutí dojde k zavření aplikace a přechodu na přihlašovací okno.

Nyní jsme ve fázi, kdy se nám povedlo propojit GUI se serverem a tím ustanovit spojení mezi klienty.

## Vývojový diagram

Viz [**Příloh**](#_bookmark16)**a**.

## Následující kroky

V následujících krocích bude v aplikaci naimplementováno symetrické šifrování pomocí AES s délkou klíče 128 bitů, pro zabezpečení spojení. Následně pro výměnu těchto klíčů bude využito postkvantové kryptografie založené buď na supersingulárních eliptických křivkách (algoritmus

SIDH/SIKE), nebo na teorii kódování vůči kvantovým útokům (algoritmus McEliece). Pro implementaci AES budeme v Pythonu využívat knihovnu Crypto. Knihovna pro postkvantovou kryptografii je

v procesu výběru.

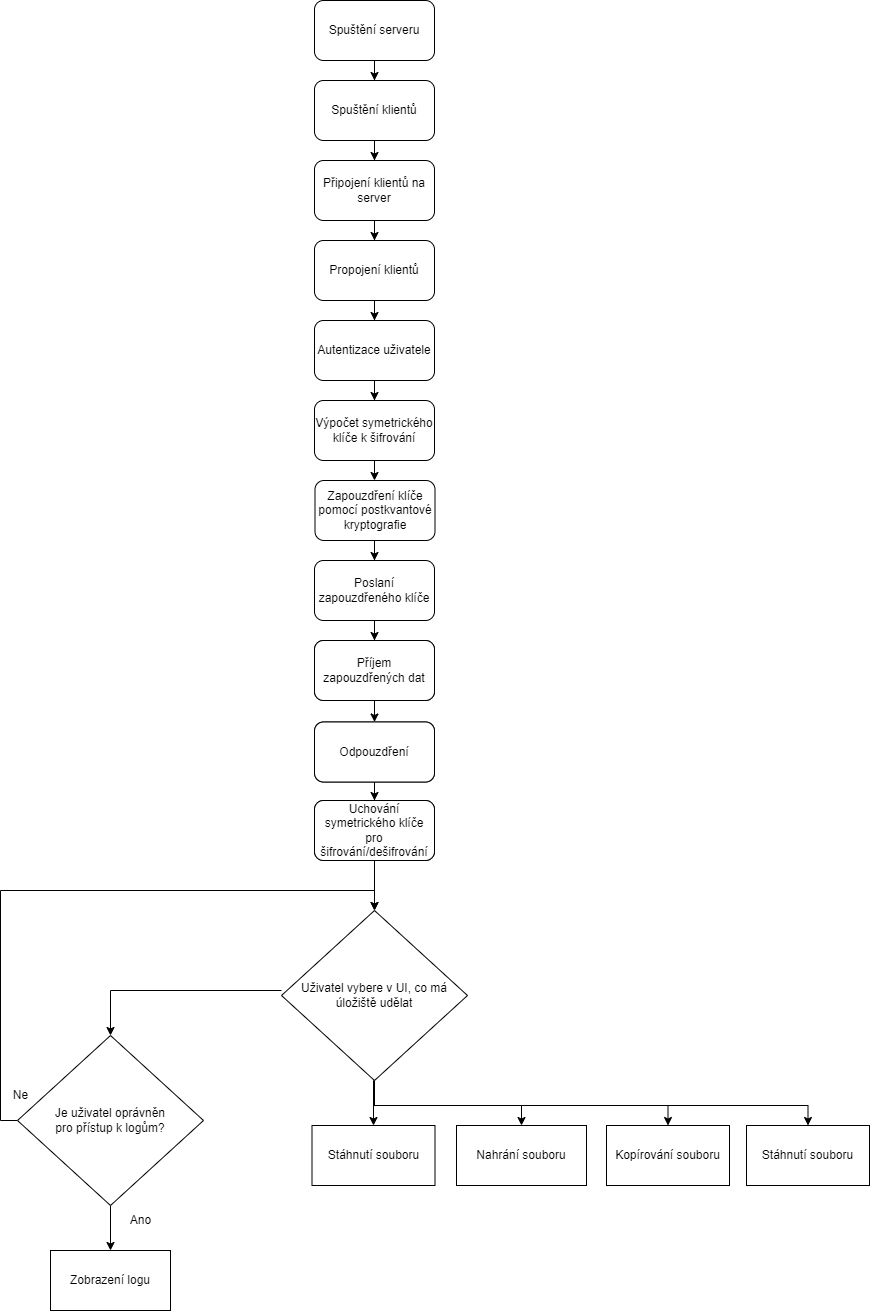
V případě GUI bude nutné vytvořit dvě funkční tlačítka (COPY, PASTE). A také v přihlašovacím okénku vytvořit možnost na vytváření nového uživatele. Kromě těchto malých úprav považujeme GUI z designové stránky za hotové. Bude nutné napárovat všechna tlačítka s požadovanými funkcemi aplikace.

Dále bude nutné vytvořit databázi v MS SQL. Databáze bude sloužit pro možnost vytváření uživatelů, přidělovaní jejich práv a autentizaci. Do databáze se také budou ukládat logy o proběhlých akcích, ke kterým budou mít přístup jen privilegovaní uživatelé.

# Závěr

V průběhu projektu jsme vytvořili jednoduchou aplikaci pro komunikační účely. Aplikace umožňuje navázat spojení mezi uživateli na základě intuitivního uživatelského rozhraní. Uživatelské rozhraní také umožňuje uživateli přizpůsobit různé parametry relace. Aplikace také zajišťuje základní funkce informačního systému, jako je čtení, změna, kopírování, mazání a zobrazování, ... na základě ověření přístupových práv.

Vzhledem k tomu, že je aplikace omezena na jeden semestr, je stále omezená. Poskytla však přehled o praktickém využití postkvantové kryptografie. V budoucnu bude aplikace pravděpodobně dále rozvíjena, aby vznikl hotový produkt.

Příloha

# Literatura

1. PINTO, Jose. *Post-Quantum Cryptography* [online]. 2022 [cit. 2023-03-26]. Dostupné z: <https://www.researchgate.net/publication/367100840_Post-Quantum_Cryptography>
2. *Storage Security Professional’s Guide to Skills and Knowledge* [online]. 2008 [cit. 2023-03-21]. Dostupné z: [https://www.snia.org/sites/default/files/Storage-Sec-Prof-](https://www.snia.org/sites/default/files/Storage-Sec-Prof-Guidance.081015.Final_.pdf)

[Guidance.081015.Final\_.pdf](https://www.snia.org/sites/default/files/Storage-Sec-Prof-Guidance.081015.Final_.pdf)

1. ROSENCRANCE, Linda. *Peer-to-peer (P2P)* [online]. 2022 [cit. 2023-03-22]. Dostupné z: <https://www.techtarget.com/searchnetworking/definition/peer-to-peer>
2. SMIRNOFF, Peter a Dawn M. TURNER. *Symmetric Key Encryption - why, where and how it’s used in banking* [online]. 2020 [cit. 2023-03-22]. Dostupné z: [https://www.cryptomathic.com/news-events/blog/symmetric-key-encryption-why-where-](https://www.cryptomathic.com/news-events/blog/symmetric-key-encryption-why-where-and-how-its-used-in-banking) [and-how-its-used-in-banking](https://www.cryptomathic.com/news-events/blog/symmetric-key-encryption-why-where-and-how-its-used-in-banking)
3. *The Advanced Encryption Standard (AES)* [online]. [cit. 2023-03-24]. Dostupné z: <http://www.facweb.iitkgp.ac.in/~sourav/AES.pdf>
4. *Post-quantum cryptography* [online]. [cit. 2023-03-22]. Dostupné z: <https://en.wikipedia.org/wiki/Post-quantum_cryptography>
5. *What is Lattice-based Cryptography?* [online]. [cit. 2023-03-22]. Dostupné z: [https://utimaco.com/products/technologies/post-quantum-cryptography/what-lattice-based-](https://utimaco.com/products/technologies/post-quantum-cryptography/what-lattice-based-cryptography) [cryptography](https://utimaco.com/products/technologies/post-quantum-cryptography/what-lattice-based-cryptography)
6. *Multivariate cryptography* [online]. [cit. 2023-03-22]. Dostupné z: [https://utimaco.com/products/technologies/post-quantum-cryptography/what-lattice-based-](https://utimaco.com/products/technologies/post-quantum-cryptography/what-lattice-based-cryptography) [cryptography](https://utimaco.com/products/technologies/post-quantum-cryptography/what-lattice-based-cryptography)
7. Overbeck, R., Sendrier, N. (2009). *Code-based cryptography*. In: Bernstein, D.J., Buchmann, J., Dahmen, E. (eds) Post-Quantum Cryptography. Springer, Berlin, Heidelberg. <https://doi.org/10.1007/978-3-540-88702-7_4>

(10) MATULA, Lukáš. *POST-KVANTOVÁ KRYPTOGRAFIE NA OMEZENÝCH ZAŘÍZENÍCH*. BRNO, 2019. Dostupné také z: <https://www.vut.cz/www_base/zav_prace_soubor_verejne.php?file_id=194065>. Bakalářská práce. Vysoké učení technické.