NEW CHALLENGES TO MODERN CLASSICAL CRYPTOGRAPHY IN A WORLD WITH QUANTUM COMPUTING

Zhaneta N. Savova, Rosen A. Bogdanov

**Computer Systems and Technologies Department, Faculty of Artillery, Air Defense and Communication and Information Systems/National Military University, Shumen, Bulgaria, zh.savova@yahoo.com*
***Communication Networks and Systems Department, Faculty of Artillery, Air Defense and Communication and Information Systems/National Military University, Shumen, Bulgaria, rabogdanov@nvu.bg*

***Abstract**: The current state of classical cryptosystems and quantum computing is examined in the paper. The possibility of the influence of quantum computing from a large-scale quantum computer on the classical cryptographic algorithms is analyzed. As a result, the challenges for the scientific community working on postquantum cryptography have been identified.*

***Keywords**: Postquantum Cryptography, Postquantum Cryptography Primitives, Quantum Computing*

НОВИ ПРЕДИЗВИКАТЕЛСТВА ПРЕД СЪВРЕМЕННАТА КЛАСИЧЕСКА КРИПТОГРАФИЯ В СВЯТ С КВАНТОВИ ИЗЧИСЛЕНИЯ

Жанета Н. Савова, Росен А. Богданов

Въведение

В съвременния свързан свят способността на хората, предприятията и правителствата да комуникират сигурно е от изключително значение. За да поддържа множество приложения, които са важни за икономиката, сигурността и начина на живот, като мобилни телефони, интернет търговия, социални мрежи, облачни изчисления и др., глобалната комуникационна цифрова инфраструктура използва криптография с публичен ключ през последните три десетилетия. Много от комуникационните протоколи разчитат главно на три основни криптографски функционалности: криптиране с публичен ключ, цифрови подписи и обмен на ключове. Понастоящем тези функционалности се прилагат предимно с помощта на обмен на ключове на Дифи-Хелман, криптосистемата RSA (Rivest-Shamir-Adleman) и криптосистеми с елиптични криви. Тяхната сигурност зависи от трудността за решаване на някои теоретико-числови проблеми, като например факторизация на големи цели съставни числа или проблем с дискретен логаритъм върху различни групи.

Още през 1994 г. Питър Шор от лаборатория Бел показа, че квантовите компютри като нова технология, използваща физическите свойства на материята и тяхната енергия за извършване на изчисления, могат ефективно да решат всеки от тези теоретико-числови проблеми, като по този начин правят всички криптосистеми с публичен ключ използващи тези проблеми безсилни [14], [15] . По този начин достатъчно мощен квантов компютър ще постави в опасност много форми на съвременна комуникация - от обмен на ключове до криптиране и цифрово удостоверяване.

Откритието, че квантовите компютри могат да се използват за решаване на определени проблеми по-бързо от класическите компютри, предизвика голям интерес към квантовите изчисления сред изследователите. Понастоящем теоретичните разработки в областта изпреварват реалните технологични разработки. Отговорът на въпроса „Кога ще бъдат разбити съвременните криптосистеми с открит ключ?" зависи от отговора на въпроса „Кога ще бъдат построени мащабни квантови компютри?". За да бъде готова за този момент криптографската научна общност през последните десетилетия работи върху въпросите за намиране на начини за противопоставяне на противник използващ както квантови, така и класически изчисления.

Във връзка с горе поставените въпроси в статията се разглежда съвременното състояние на класическите криптосистеми и квантовите изчисления. Анализира се възможността за въздействие на квантовите изчисления от мащабен квантов компютър върху класическите криптографски алгоритми. В резултат са изведени предизвикателства към научната общност работеща по въпросите на постквантовата криптография.

1. Съвременно състояние на квантовите изчисления и класическите криптосистеми

Анализирано е съвременното състояние на квантовите изчисления и влиянието им върху съвременните криптографски алгоритми

1.1. Състояние на квантовите изчисления

Изследванията на възможността за изграждане на мащабни квантови компютри започнаха сериозно след откриването от Питър Шор през 1994 г. на квантов алгоритъм, който със сложност от полиномиално време реализира целочислено факторизиране [14]. По това време не беше ясно дали квантовите изчисления някога ще бъдат реална технология. Много водещи експерти предполагаха, че квантовите състояния са твърде неустойчиви и подлежат на натрупване на грешка, за да може някога да се реализират мащабни квантови изчисления. Тази ситуация се промени в края на 90-те години с развитието на кодове за коригиране на квантови грешки и прагови теореми [12]. Тези прагови теореми показват, че ако степента на грешка за логическа операция в квантов компютър може да бъде поддържана под фиксиран праг, тогава произволно дългите квантови изчисления могат да бъдат извършени по надежден и толерантен към грешки начин чрез включване на стъпки за корекция на квантовата грешка по време на изпълнението на квантовото изчисление [5]. През годините постепенно е разработен подобрен хардуер с все по-ниски проценти на квантова грешки. Едновременно с това теоретиците разработват нови процедури за коригиране на квантови грешки, които дават по-високи прагове за устойчивост на грешки. Някои експерименти, използващи йонни капани и свръхпроводящи вериги, демонстрираха универсални набори от квантови порти, които номинално са под най-високите теоретични прагове за устойчивост на грешки (около 1 %) [3], [7]. Това е важен етап, който стимулира увеличаването на инвестициите както от правителството, така и от промишлеността за преминаване от лабораторни демонстрации, включващи няколко кюбита, до мащабни квантови компютри, включващи хиляди логически кюбита, кодирани в може би стотици хиляди или милиони физически кюбита.

Успоредно с развитието на цифрови квантови компютри с общо предназначение, бяха положени усилия за разработване на аналогови квантови компютри със специално предназначение,

като квантови D-Wave машини, аналогови квантови симулатори и устройства за вземане на проби от бозони. Някои от тези устройства са изградени от много по-голям брой кюбита, отколкото цифровите квантови компютри. Въпреки това, поради техния специализиран характер, се смята, че тези аналогови квантови устройства не са от значение за криптоанализа.

Днес Google, IBM, Intel и други са изградили първите реални цифрови квантови компютри, но тези системи все още са в начален етап на разработка и не могат да изпълняват полезни търговски приложения. Въпреки това има забележим напредък с квантовите изчисления, който е различен от класическите изчислителни системи.

В класическите изчисления информацията се съхранява в битове, които могат да бъдат „0" или „1". В квантовите изчисления информацията се съхранява в квантови битове или кюбита (q-bit), които могат да съществуват като „0" или „1" или комбинация от двете. Състоянието на суперпозиция позволява на квантовия компютър да извършва множество изчисления наведнъж, което му позволява да надмине традиционната изчислителна система. Но технологията е изправена пред редица предизвикателства и много индустриални експерти смятат, че тези системи все още са десетилетие далеч от практическото им приложение.

Понастоящем, китайският университет за наука и технологии USTC (University of Science and Technology of China) през юни 2021 г. демонстрира най-бързият според изследователите процесор за квантови изчисления в света, надминавайки предишния неофициален рекорд, държан от 53-кюбитно устройство на Google от 2019 г. USTC процесорът, който съдържа 66 кюбита извършвайки сложно изчисление за 1,2 часа, което би отнело на съвременните суперкомпютри 8 години.

Според Джеймс Кларк, директор на отдела за квантов хардуер в Intel, е още рано да се обявява победител, тъй като технологията все още е в начален стадий. „Когато се обръщам към първите приложения, ще са ни необходими няколко хиляди, ако не и 100 000 кюбита, за да направим нещо полезно. Ако днес са реализирани от 50 до 60 кюбита, ще е необходимо време, преди да стигнем до 100 000 кюбита. Ще мине известно време, преди да стигнем до 1 милион кюбита, което би било необходимо за криптографията." [10].

Все пак пазарът е обещаващ. Очаква се пазарът на квантови компютри да нарасне от 320 милиона долара през 2020 г. на 830 милиона долара до 2024 г., според Hyperion Research [13].

1.2. Въздействие на квантовите изчисления върху криптографските алгоритми

След откриването на алгоритъма на Шор теорията за квантовите алгоритми се е развила значително. Открити са квантови алгоритми, постигащи експоненциално ускорение, за няколко проблема, свързани с теорията на числата, симулацията на физически процеси и топологията. Въпреки това, списъкът с проблеми, допускащи експоненциално ускоряване чрез квантови изчисления, остава сравнително малък. По-скромни ускорения са постигнати за широк клас от проблеми, свързани с търсене, намиране на сблъсък и оценка на булеви функции. По-специално, алгоритъмът за търсене на Гровър [8], [9] предлага квадратично ускоряване на неструктурирани проблеми за търсенето. Въпреки че подобно ускорение не прави криптографските технологии остарели, това може да доведе до изискване на по-големи размери на ключовете, дори в симетричните криптосистеми. Все още не е известно докъде могат да приложат реално тези квантови предимства, нито колко голяма е разликата в реалното осъществяване на класическите и квантовите криптографски модели.

Въпросът кога ще бъде построен мащабен квантов компютър е сложен и спорен. Докато в миналото беше ясно, че големите квантови компютри са физическа възможност, то сега много учени смятат, че това е просто значително инженерно предизвикателство. Някои експерти дори прогнозират, че в рамките на следващите 20 и повече години ще бъдат изградени достатъчно големи квантови компютри, които да разбият по същество всички схеми с публичен ключ, които се използват в момента. Модерната инфраструктура за криптография с публичен ключ също бе

внедрена за почти 20 години. Ще са необходими значителни усилия, за да се осигури гладка и сигурна миграция от настоящите широко използвани криптосистеми към новите криптосистеми, устойчиви на квантовите изчисления. Следователно, независимо от това дали може да се прецени точното време на настъпване на ерата на квантовите изчисления, сега трябва да се започне подготовка за информационна сигурност, която да устои на квантовите изчисления.

Таблица 1 обобщава въздействието на мащабните квантови компютри върху класическите криптографски алгоритми, като AES, RSA, SHA-2, SHA-3, ESDCA, ECDH и DSA.

Таблица 1. *Въздействие на квантовите изчисления от мащабен квантов компютър върху криптографските алгоритми*

Криптографски алгоритъм	**Тип**	**Предназначение**	**Въздействие**
AES	Симетрична криптосистема	Криптиране	Необходими са по-големи размери на ключовете
SHA-2, SHA-3	Семейство хеш функции	Еднопосочно преобразование	Необходим е по-голям изход
RSA	Асиметрична криптосистема	Цифров подпис, размяна на ключове, криптиране	Вече не е защитен
ECDSA, ECDH (Криптография с елиптична крива)	Асиметрична криптосистема	Цифров подпис, размяна на ключове	Вече не е защитен
DSA (Криптография с крайно поле)	Асиметрична криптосистема	Цифров подпис, размяна на ключове	Вече не е защитен

Появи се голяма международна общност, която да реши проблема с информационната сигурност в бъдеще на квантовите изчисления, с надеждата, че инфраструктурата с публичен ключ може да остане непокътната, като използва нови квантово устойчиви примитиви. В академичния свят тази нова наука носи името „Постквантова криптография". Това е активна област на изследване със собствена серия конференции PQCrypto, която стартира през 2006 г. Тя получи значителна подкрепа от националните агенции за финансиране в Европа и Япония, чрез проектите на Европейския съюз PQCrypto и SAFEcrypto, и проекта CREST Crypto-Math в Япония.

Най-важните употреби на криптографията с публичен ключ днес са за цифрови подписи и размяна на ключове. Както се вижда от Таблица 1 изграждането на мащабен квантов компютър би направило много от тези криптосистеми с публичен ключ несигурни. По-специално, това включва криптосистемите, които се основават на трудността на цялочислена факторизация, като RSA, както и такива, основани на трудността на проблема на дискретния логаритъм, като ECDSA, ECDH и DSA. Въздействието върху симетричните криптосистеми няма да бъде толкова драстично (виж Таблица 1). Алгоритъмът на Гроувър осигурява квадратично ускоряване на алгоритмите за квантово търсене в сравнение с алгоритмите за търсене на класическите компютри. Не се знае кога алгоритъмът на Гроувър ще бъде практически реализиран, но ако това стане, удвояването на размера на ключа ще бъде достатъчно за запазване на сигурността. Освен това е показано, че експоненциалното ускоряване на алгоритмите за търсене е невъзможно, което предполага, че симетричните алгоритми и хеш функциите трябва да бъдат използваеми в квантовата ера [4].

Следователно търсенето на алгоритми, за които се смята, че са устойчиви на атаки както от класически, така и от квантови компютри, се фокусира върху алгоритми с публичен ключ.

2. Предизвикателства пред постквантовата криптография

Изглежда невероятно, че някой от известните понастоящем криптографски алгоритми може да послужи като заместител на това, което се използва днес. Едно предизвикателство, което вероятно ще трябва да бъде преодоляно, е, че повечето от квантово устойчивите алгоритми имат по-големи размери на ключовете от алгоритмите, които ще заменят. Това може да доведе до необходимост от промяна на различни интернет протоколи, като протокола за защита на транспортния слой (TLS) или обмена на интернет ключове (IKE). Начините, по които това трябва да се направи,

трябва да бъдат внимателно обмислени. Може да се отбележи като второ предизвикателство, че нито едно от горните предложения не е доказано, че гарантира сигурност срещу всички квантови атаки. Може да бъде открит нов квантов алгоритъм, който нарушава някои от тези схеми. Това обаче е подобно на днешното състояние. Въпреки че повечето криптосистеми с публичен ключ идват с доказателство за сигурност, тези доказателства се основават на недоказани предположения. По този начин липсата на известни атаки се използва, за да се оправдае сигурността на криптографията с публичен ключ, която се използва в момента.

Затова според националния институт по стандартизация и технологии NIST на САЩ, ще са необходими повече изследвания и анализи, преди някой от постквантовите алгоритми да може да бъде препоръчан за използване. Те не са достатъчно изследвани от криптографската общност, колкото алгоритмите, използвани в момента. Като изключение могат да се посочат подписите, базирани на хеш функции, чиято сигурност е добре изследвана. За някои специфични приложения, като например подписване на цифрова информация, подписите на базата на хеш могат потенциално да бъдат стандартизирани през следващите няколко години.

Основните семейства криптографски примитиви, които са предложени за приложение в постквантовата ера са примитиви, базирани на решетки, базирани на кодове и многовариантни полиноми, както и няколко други варианти [6].

Криптография, базирана на решетки. Криптосистемите, базирани на проблеми с решетки, са получили интерес по няколко причини. Повечето базирани на решетки алгоритми за установяване на ключове са относително прости, ефективни и могат да се изпълняват като паралелни алгоритми. Също така, сигурността на някои системи, базирани на решетки, е доказано сигурна при предположение за сигурност в най-лошия случай, а не в средния случай. Някои нови приложения на криптографските примитиви, базирани на решетки, са напълно хомоморфно криптиране, замъгляване на кода и криптиране, базирано на атрибути. Като техен недостатък може да се посочи, че е трудно да се дадат точни оценки за сигурността на решетъчните схеми срещу известни в момента техники на криптоанализ.

Криптография, базирана на код. Представител на това семейство криптографски примитиви е криптосистемата McEliece, която е предложена през 1978 г. и оттогава не е разбита. Оттогава до сега са предложени и други системи, базирани на кодове за коригиране на грешки. Характерно за тях е, че са доста бързи, но изискват доста големи размери на ключовете. За да се избегне този недостатък се премина към по-новите варианти, които въведоха повече структури в кодовете, но доведе до реализирани успешни атаки срещу някои предложения. Въпреки че са предложени и схеми за подписи, базирани на код, криптографията, базирана на код, постигна по-голям успех със схемите за криптиране.

Криптография, базирана на многовариантни полиноми. Тези примитиви се основават на трудността при решаването на системи от многовариантни полиноми над крайни полета. През последните няколко десетилетия бяха предложени няколко многовариантни криптосистеми, като много от тях бяха разбити. Въпреки че има някои предложения за многовариантни схеми за криптиране, многовариантната криптография исторически е по-успешна като подход към реализация на цифрови подписи.

Подписи, базирани на хеш функции. Хеш базираните подписи са цифрови подписи, конструирани с помощта на хеш функции. Тяхната сигурност, дори срещу квантови атаки, е добре изследвана. Много от по-ефективните схеми за подпис, базирани на хеш, имат недостатъка, че подписващият трябва да води запис на точния брой на предварително подписаните съобщения и всяка грешка в този запис може да доведе до несигурност. Друг недостатък е, че те могат да дадат само ограничен брой подписи. Броят на подписите може да бъде увеличен, но това води също и до увеличаване на размера на подписа.

Други криптографски примитиви. Предложени са различни криптосистеми, които не попадат в горните семейства. Едно такова предложение се основава на оценяването на изогения върху свръхсингулярни елиптични криви. Докато проблемът с дискретния логаритъм на елиптични

криви може да бъде ефективно решен чрез алгоритъма на Шор на квантов компютър, проблемът с изогенията на свръхсингулярни криви няма известна подобна квантова атака. Подобно на някои други предложения, например тези, които се основават на проблема с търсенето на конюгация и свързаните с него проблеми в групи плитки (braid group), все още няма достатъчно анализ, за да се има голямо доверие на тяхната сигурност.

За да се реши проблема със стандартизиране на постквантови примитиви, националният институт по стандарти и технологии е в процес на избор на един или повече криптографски алгоритми с публичен ключ чрез публичен конкурсен процес. Новите стандарти за криптография с публичен ключ ще определят един или повече допълнителни цифрови подписи, криптиране на публичен ключ и алгоритми за установяване на ключ. Представените алгоритми трябва да отговарят на следните изисквания [11]:

1. Алгоритмите се оповестяват публично и се предоставят за обществен преглед по време на процеса на оценяване и за стандартизация, ако са предназначени за обществеността.
2. Алгоритмите не трябва да включват основни компоненти, за които се смята, че са несигурни срещу квантовите компютри.
3. Алгоритмите трябва да осигуряват поне една от следните функционалности: криптиране на публичен ключ, размяна на ключове или цифров подпис:

a. Схемите за криптиране с публичен ключ включват алгоритми за генериране на ключове, криптиране и декриптиране. Алгоритъмът за генериране на ключове трябва да генерира публични и частни ключове, такива че криптираните с публичния ключ съобщения или симетрични ключове се възстановяват чрез декриптиране със съответния частен ключ. Ако е възможна грешка при декриптиране, тя трябва да се случи в размер, съответстващ на претенциите, подадени от подателя. Като минимум, схемата трябва да поддържа криптиране и декриптиране на съобщения, които съдържат симетрични ключове с дължина най -малко 256 бита.

b. Механизмите за капсулация на ключове KEM (Key Encapsulation Mechanism) включват алгоритми за генериране на ключове, капсулиране и декапсулация. Алгоритъмът за генериране на ключове генерира двойки публични и частни ключове, такива че капсулирането с публичния ключ и декапсулирането с частния ключ произвежда една и съща споделена тайна, когато капсулираният шифротекст е подаден като вход за декапсулиращата функция. Ако се е възможна грешка при капсулирането, тя трябва да се случи в размер, съответстващ на претенциите, направени от подателя. Като минимум функционалността на KEM трябва да поддържа установяване на споделени ключове с дължина най-малко 256 бита.

c. Схемите за цифров подпис включват алгоритми за генериране на ключове, подпис и проверка. Алгоритъмът за генериране на ключове генерира публични и частни ключове, така че съобщението, подписано с частния ключ, успешно да бъде проверено със съответния публичен ключ. Схемата трябва да бъде способна да поддържа размер на съобщението до 2^{63} бита.

4. Пакетът за подаване трябва да предоставя конкретни стойности за всички параметри и настройки, необходими за постигане на заявените свойства на сигурност на примитивите.

Предполага се, че тези алгоритми ще могат да защитават чувствителна информация в обозримо бъдеще, включително след появата на квантовите компютри. През ноември 2017 г. 82 алгоритми кандидати бяха изпратени на NIST за разглеждане. Сред тях 69 отговарят на минималните критерии за приемане и на изискванията за подаване и са приети като кандидати за първи кръг на 20 декември 2017 г. На 30 януари 2019 г. за преминаване към втория кръг на конкурса са избрани 17 алгоритми за криптиране на публичен ключ и установяване на ключ: BIKE, Classic McEliece, CRYSTALS-KYBER, FrodoKEM, HQC, LAC, LEDAcrypt (сливане на LEDAkem/LEDApkc), NewHope, NTRU (сливане на NTRUEncrypt/NTRU- HRSS-KEM), NTRU Prime, NTS-KEM, ROLLO (сливане на LAKE/LOCKER/Ouroboros-R), Round5 (сливане на Hila5/Round2), RQC, SABER, SIKE и Three Bears. Избраните примитиви за цифрови подписи са 9: CRYSTALS-DILITHIUM, FALCON, GeMSS, LUOV, MQDSS, Picnic, qTESLA, Rainbow и SPHINCS+ [1].

Алгоритмите за криптиране на публичен ключ и установяване на ключ от третия кръг са Classic McEliece, CRYSTALS-KYBER, NTRU и SABER. Финалистите от третия кръг за цифрови подписи са CRYSTALS-DILITHIUM, FALCON и Rainbow. Тези финалисти ще бъдат разглеждани за стандартизация в края на третия кръг. В допълнение, осем алтернативни алгоритми за кандидатстване също ще преминат към третия кръг: BIKE, FrodoKEM, HQC, NTRU Prime, SIKE, GeMSS, Picnic и SPHINCS+. Тези допълнителни кандидати все още се разглеждат за стандартизация, въпреки че това е малко вероятно да се случи в края на третия тур. NIST се надява, че обявяването на тези финалисти и допълнителни кандидати ще послужи за фокусиране на вниманието на криптографската общност през следващия кръг [2].

References

1. Alagic, G. et al. (2019). NISTIR 8240. Status Report on the First Round of the NIST Post-Quantum Cryptography Standardization Process. Retrieved from https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=927303
2. Alagic, G. et al. (2020). NISTIR 8309. Status Report on the Second Round of the NIST Post-Quantum Cryptography Standardization Process. Retrieved from https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8309.pdf
3. Barends, R., Kelly, J., Megrant, A., Veitia, A., Sank, D., Jeffrey, E., ... & Martinis, J. M. (2014). Superconducting quantum circuits at the surface code threshold for fault tolerance. Nature, 508(7497), 500-503.
4. Bennett, C. H., Bernstein, E., Brassard, G., & Vazirani, U. (1997). Strengths and weaknesses of quantum computing. SIAM journal on Computing, 26(5), 1510-1523
5. Brun, T. A. (2019). Quantum error correction. arXiv preprint arXiv:1910.03672. Retrieved from https://arxiv.org/ftp/arxiv/papers/1910/1910.03672.pdf
6. Campagna, M. et al. (2015) European Telecommunications Standards Institute White Paper No. 8, Quantum Safe Cryptography and Security: An Introduction, Benefits, Enablers and Challenges. June 2015. ISBN No. 979-10-92620-03-0. Retrieved from https://www.etsi.org/images/files/ETSIWhitePapers/QuantumSafeWhitepaper.pdf
7. Fawzi, O., Grospellier, A., & Leverrier, A. (2018, October). Constant overhead quantum fault-tolerance with quantum expander codes. In 2018 IEEE 59th Annual Symposium on Foundations of Computer Science (FOCS) (pp. 743-754). IEEE
8. Grover, L. K. (1997). Quantum computers can search arbitrarily large databases by a single query. Physical review letters, 79(23), 4709.
9. Grover, L. K. (1997). Quantum mechanics helps in searching for a needle in a haystack. Physical review letters, 79(2), 325.
10. Lapedus M. (2021, July). The Great Quantum Computing Race. Retrieved from https://semiengineering.com/the-great-quantum-computing-race/
11. NIST. (2016) Submission Requirements and Evaluation Criteria for the Post-Quantum Cryptography Standardization Process. Retrieved from https://csrc.nist.gov/csrc/media/projects/post-quantum-cryptography/documents/call-for-proposals-final-dec-2016.pdf
12. Preskill, J. (1998). Reliable quantum computers. Proceedings of the Royal Society of London. Series A: Mathematical, Physical and Engineering Sciences, 454(1969), 385-410
13. Russell, J. (2021, May). Hyperion Offers Snapshot of Quantum Computing Market. Retrieved from https://www.hpcwire.com/2021/05/13/hyperion-offers-snapshot-of-quantum-computing-market/
14. Shor, P. W. (1994). Algorithms for quantum computation: discrete logarithms and factoring. In Proceedings 35th annual symposium on foundations of computer science (pp. 124-134). IEEE.
15. Shor, P. W. (1999). Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM review, 41(2), 303-332.