Дослідження криптосистем на основі кодів хеш функцій

Ілля Жеков, Володимир Караваєв

Кафедра безпеки інформаційних технологій, Харківський національний університет радіоелектроніки, УКРАЇНА,
м.Харків, пр. Науки, 14,
E-mail: illia.zhekov@nure.ua,
E-mail: volodymyr.karavaiev@nure.ua

Коротка анотація – This article is devoted to information security in post quantum epoch. The article discusses the security problems which could appear with quantum computer appearing and describes what have world's best minds do to prevent information's collapse.

Ключові слова – квантовий комп'ютер, хеш-функція, алгоритм Шора, дискретний логарифм, NIST, криптоаналіз, криптосистема, стандартизація.

I. Вступ

В наш час багато провідних учених і експертів активно працюють над створенням квантових комп'ютерів. Кожний додатковий кубіт у два рази збільшує площу пошуку даних, отже, значно підвищується й швидкість їх обчислення.

Квантові комп'ютери ймовірно зможуть зруйнувати більшу частину, якщо не абсолютно всі традиційні криптосистеми, які широко використовуються в практиці. Конкретно, системи, засновані на завданні факторизації цілих чисел (наприклад, RSA).

Саме тому вже зараз ведеться робота над створенням криптосистем стійких до квантового криптоаналізу.

II. Актуальність проблеми

На сьогоднішній день майже всі технології в мережі інтернет містять у собі асиметричне шифрування. Це передбачене необхідністю мати захищений канал передачі між вузлами[1].

Мільярди людей щодня використовують протокол TLS коли вони входять в акаунти соціальних мереж, форумів, електронної пошти або будь-якого іншого ресурсу де має місце структура логін-пароль. Це вже не говорячи про технологію електронного цифрового підпису, який широко використовується у фінансовій сфері й на рівнях державних таємниць.

Також користувачі сучасних комп'ютерів, смартфонів досить часто завантажують нові програми для своїх гаджетів. Про це може свідчити величезний ринок цифрових продуктів, який тільки продовжує рости. Але для завантаження будь-якого додатка або програми, що використовують інтернет при роботі, потрібне залучення технологій шифрування.

Тому криптографія з відкритим ключем і тут є невід'ємною частиною. У зв'язку із цим має місце постійна необхідність підтвердження надійності й відмовостійкості сучасних криптографічних систем.

Достовірність будь-якого файлу, що завантажується з інтернету повинна бути підтверджена за допомогою цифрового підпису, щоб ви могли бути впевнені в тому, що ніде не була порушена цілісність. Така структура впроваджена у всіх ведучих постачальників електронних продуктів таких як: Appstore, Googleplay, Amazon, Tesla, Microsoft, Ubuntu і т.д.

Втративши свій рівень безпеки, будь-який файл можна вважати скомпрометованим і неприпустимим для використання, тому провідні компанії постійно поліпшують свої продукти, надаючи людям упевненість у безпеці. Одним з варіантів підвищення якості послуг безпеки є використання сучасних криптосистем, і зокрема на основі кодів хеш функцій.

III. Аналіз проблеми

В 1994 році Шор [3] запропонував квантові алгоритми дискретного логарифмування в групі точок еліптичної кривої і факторизації чисел. В 2001 році в IBM продемонстрували працездатність алгоритму Шора, розклавши число 15 на множники 3 і 5 на 7-кубітному квантовому комп'ютері. По оцінці Proos і Zalka відновлення секретного ключа ECDSA довжиною 256 біт зажадає близько 1500 кубіт і 6*109 (~232) операцій. По оцінці фахівців Microsoft для цього буде потрібно 2330 кубіт і $1.26*10^{11}$ ($\sim 2^{36}$) операцій.

У звіті Національного Інституту Стандартів і Технологій США (The National Institute of Standards andTechnology, NIST) за квітень 2016 року відзначається, що більшість асиметричних криптографічних примітивів, широко використовуваних сьогодні в різних сферах суспільного життя, і які базуються на завданнях факторизації та дискретного логарифмування в різних групах, будуть скомпрометовані.

У силу всього вище сказаного, очевидною стає необхідність подальшого розвитку пост-квантової криптографії. Тому що схеми електронного підпису повністю втратять свою криптостійкість у випадку появи квантового комп'ютера, на відміну від шифрування й обміну ключами, саме для цих криптографічних функцій першорядною необхідністю є пошук нових пост-квантових аналогів.

Пост-квантова криптографія на даний момент містить у собі наступні основні підходи:теорія ґрат; багатомірні квадратичні системи; електронні підписи на хеш-функціях; теорія алгебраїчного кодування; ізогенії еліптичних кривих.

Розглянемо коротко переваги й недоліки кожного підходу, приведемо приклади конкретних реалізацій.

Криптографія на ґратах. Даний розділ криптографії почав активно розвиватися з 1990-х років і містить у собі велику кількість важко обчислювальних завдань, деякі з яких уважаються Np-повними . Більшість схем прості в розумінні, забезпечують гарну швидкодію й мають властивість розпаралелювання обчислень. Крім шифрування й підпису, на ґратах можуть бути побудовані інші цікаві додатки (повністю гомоморфне шифрування, шифрування й підпис із використанням атрибута, обфускація кодів і інші). Деякі системи із цього розділу мають складність у

найгіршому випадку, а не в середньому, як більшість криптосистем. До мінусів можна віднести відсутність точного методу оцінки складності алгоритмів на ґратах до існуючих видів атак. Найбільш відомою схемою є криптосистема NTRU (Nth-degree Truncated polynomial ring), запропонована в 1998 році. На базі криптосистеми NTRU можна реалізувати алгоритми шифрування й електронному підпису.

Модифікована версія даного алгоритму була взята за основу стандарту для фінансових організацій ANSI X9.98-2010 «Lattice-Based Polynomial Public Key Establishment Algorithm for the Financial Services Industry». В 2008 році криптосистема NTRU була включена в стандарт IEEE 1363.1 «Lattice-based public-key cryptography».

Криптографія, заснована на багатомірних квадратичних системах. Стійкість цього розділу криптографії ґрунтується на складності розв'язку системи багатомірних квадратичних багаточленів над кінцевим полем. Дане завдання вважається Np-повним. Системи із цього розділу мають гарну швидкість і невеликі вимоги до обчислювальних ресурсів, однак, довжини відкритих ключів досить великі.

Криптографія на кодах, що виправляють помилки (теорія алгебраїчного кодування). До плюсів такого роду систем можна віднести швидкість обчислень. До мінусів - занадто велику довжину ключів. На теорії алгебраїчного кодування базуються класичні криптосистеми McEliece і Niederreiter.

Ізогенії суперсингулярної еліптичної кривої. Найбільш популярний протокол SIDH (Supersingular isogeny Diffie-Hellman, SIDH) дозволяє зробити обмін ключами по незахищеному каналу зв'язку. Цей факт і є його відмінною рисою, що гарантує досконалу таємність. З урахуванням стиснення SIDH має найменшу довжину ключа із усіх постквантових протоколів обміну ключами. Однак повноцінної криптосистеми на ізогеніях поки реалізовано не було.

Криптографія, заснована на хеш-функціях з нашої точки зору є досить перспективним напрямом. У даний розділ входять електронні підписи, побудовані за допомогою хеш-функцій, у силу чого забезпечується їхня стійкість до квантових обчислень.

IV. Розв’язання проблеми

Криптостійкість цифрового підпису, заснованого на гешуванні, зводиться до стійкості хеш-функції до відновлення першого й другого прообразу. Відновлення прообразу хеша довжиною n біт на класичному комп'ютері зводиться до повного перебору (складність $O(2^n)$), на квантовому — до перебору алгоритмом Гровера (складність $O(2^{n/2})$). Таким чином, можна вибрати стійку хеш-функцію, що забезпечує необхідну класичну й пост-квантову криптостійкість. Інші підходи до постквантової криптографії ґрунтуються на математичних проблемах, які вважаються квантово-стійкими, але можливо можуть бути вирішені класичним комп'ютером у випадку прориву в розвитку математики.

Згідно з рекомендаціями PQCRYPTO для досягнення 128-бітної постквантової криптостійкості на практиці може використовуватись схема цифрового підпису XMSS [4,5] з параметрами з RFC 8391. Недолік схеми XMSS полягає в тому, що вона може генерувати обмежене число підписів, яке залежить від висоти використовуваного дерева Меркла.

Поряд з XMSS рекомендації PQCRYPTO містять у собі схему SPHINCS [6], яка позбавлена обмеження на кількість підписів, але для 128-бітної криптостійкості розмір такого підпису становить близько 41 кілобайт, тому більшою мірою цей алгоритм придатний для використання в системах автентифікації.

В цій схемі замість OTS (One Time Signature) використовується FTS (Few Time Signature), що дозволяє зменшити ймовірність виникнення колізії шляхів та зменшити висоту дерева. По-друге, внутрішні вузли дерева замінюються деревами Мерклє. За допомогою використання такої конструкції зменшується необхідний на генерації підпису час та розмір підпису, адже до самого підпису входить менша кількість реалізацій OTS.

Висновки

У даній роботі був проведений аналіз існуючих пост-квантових підходів, відзначені переваги й недоліки даних підходів. Також були розглянуті пост-квантові схеми криптосистем на основі геш-функцій, одна з них SPHINCS пройшла в другий тур конкурсу NIST на створення нових пост-квантових стандартів. Проведений порівняльний аналіз даних кандидатів. Нові стандарти підсилять FIPS 186-4, стандарт цифрового пыдпису (DSS), а також 800-56A.

Література

[1] PQCrypto 2017. Netherlands, 26-28 June 2017. [Електронний ресурс] – Режим доступа: URL: https://2017.pqcrypto.org/conference/ - 02.06.2018.

[2] Bernstein D. J., Buchmann J., Dahmen E.: Post-Quantum Cryptography. — Springer. — 2009.

[3] Shor P. W. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer//Foundations of Computer Science: Conference Publications. — 1997. — P. 1484–1509.

[4] PQCRYPTO. Initial recommendations of long-term secure post-quantum systems. http://pqcrypto.eu.org /docs/initial-recommendations.pdf.

[4] J. Buchmann, E. Dahmen, A. Hülsing. XMSS – A Practical Forward Secure Signature Scheme based on Minimal Security Assumptions. https://eprint.iacr.org /2011/484.pdf

[5] SPHINCS: practical stateless hash-based signatures. http://sphincs.cr.yp.to/