УДК 004.056.55

О. В. Потій, д-р. техн. наук, професор,
К. В. Ісірова, аспірантка

Харківський національний університет імені В. Н. Каразіна, м. Харків

АНАЛІЗ ВИМОГ ТА МОДЕЛЕЙ БЕЗПЕКИ ДЛЯ ПОСТКВАНТОВОЇ КРИПТОГРАФІЇ

Сформульовані проблеми та ризики класичних систем в галузі криптографічного захисту інформації у зв'язку із розвитком квантових обчислень. Обґрунтована задача необхідності пошуку нових рішень. Доповідь містить аналіз останніх вимог, які були висунуті двома найпотужнішими організаціями зі стандартизації: NIST та ETSI відносно криптографічних алгоритмів у пост квантовий період.

Ключові слова: *пост квантова криптографія, вимоги до крипто алгоритмів у пост квантовий період, вимоги NIST та ETSI.*

Вступ. Успіхи в сфері квантових обчислень є важливим викликом сучасній криптографії. Швидка еволюція квантових комп'ютерів, а як наслідок зростання швидкості обчислень обумовлюють нові ризики для існуючих криптографічних систем. Зокрема, алгоритми Шнора та Гровера становлять реальну загрозу для асиметричних систем, побудованих на основі RSA, Diffie-Hellman, Elliptic Curves.

В найближчий час довіра до інформаційних систем, які обробляють критичну інформацію, без засобів квантово-захищеної криптографії буде неможлива.

На шляху побудови нових рішень важливим етапом є розробка та формування вимог та характеристик, що мають бути пред'явлені до нових кандидатів та можливих умов їхнього застосування.

В роботі проведений аналіз вимог двох найбільших організацій: NIST та ETSI. Також наведені моделі безпеки та порушника для криптографічних примітивів в умовах пост квантової криптографії.

Аналіз вимог NIST. NIST розуміє необхідність пошуку нових примітивів, які будуть актуальні у пост квантовий період. Відповідні роботи здійснюються у рамках відкритого конкурсу Post-Quantum crypto Project [1, 2].

Проведений аналіз показав, що всі вимоги можна поділити на такі групи:

1) вимоги з безпеки, основними з яких є використання криптографії з відкритим ключем, схема «семантично безпечного шифрування», відповідність моделям безпеки IND-CCA2 та EUF-CMA;

«perfect forward secrecy». (удосконалена випереджаюча безпека), стійкість до атак сторонніми каналами;
2) техніко-економічні вимоги, такі як: орієнтація на розмір пакетів інтернет-протоколів, гешування ключової інформації, забезпечення ефективності як апаратної, так і програмної реалізації, відповідність розмірів ключа до обраної системи;
3) техніко-експлуатаційні вимоги: кросплатформеність, можливість розпаралелювання, зрозумілість побудови.

Аналіз вимог ETSI. Європейський союз також розпочав активну роботу з підготовки нових пост квантових стандартів. Європейською організацією зі стандартизації ETSI у кластері «Безпека» сформований новий напрямок «Квантово-захищена криптографія» («Quantum-Safe Cryptography») [3].

До основних сформульованих ними вимог безпеки належать наступні:

- надійне підтвердження стійкості;
- актуальність моделі безпеки;
- висока складність можливих атак;
- можливість поєднання кількох функцій безпеки (наприклад, встановлення ключів і схеми автентифікації);
- зручність кількісної оцінки заявлених класичних і квантових рівнів безпеки;
- визначеність рекомендованих ключових розмірів для заданого рівня безпеки (наприклад, 80-біт, 112 біт, 128 біт або 256 біт);
- стійкість, як проти класичних атак, так і проти «квантових» атак, зокрема, стійкість до алгоритму Гровера (подвоєння розміру ключа);
- можливість використання у протоколах типу TLS 1.3 з підтримкою forward secure cipher suites;
- відносно малий об’єм необхідної пам'яті під час виконання (можливість реалізації на пристрої з обмеженими ресурсами);
- сумісність (наприклад, гнучкість у виборі ґеш-функції в схемах дерева Меркле).

Обґрунтування моделей безпеки для пост квантової криптографії. Обґрунтування стійкості криптографічних примітивів має базуватися на складних обчислювальних задачах для квантових комп’ютерів. На сьогоднішній день визначені основні напрямки розробок нових квантово-захищених алгоритмів: CB-криптографія, HB-криптографія, LB-криптографія, MQ-перетворення, використання ізогеній еліптичних кривих.

Вимоги до стійкості мають бути сформульовані у відповідності до таких моделей загроз:

- для шифрування — в умовах моделі IND-CCA2 (Indistinguishability under Adaptive Chosen Ciphertext Attack), стійкість до адаптивної атаки на основі обраного шифртексту;

- для цифрового підпису — в умовах моделі EUF-CMA (Existentially unforgeable under adaptive chosen message attacks), тобто забезпечення захисту від екзістенціональної підробки в умовах адаптивного вибору повідомлення.

Для ймовірнісного алгоритму асиметричного шифрування стійкість до атаки на основі обраного шифротексту/до адаптивної атаки на основі обраного шифртексту (IND-CCA1/ IND-CCA2) визначається «грою» між претендентом (легітимним користувачем) та противником (криптоаналітиком). Необхідно ввести наступне визначення: $E(PK, M)$ — шифрування повідомлення M ключем PK. Умова: противник моделюється поліноміальним часом машини Тюрінга. Він має доступ до відкритого ключа (оракула за шифрування у симетричному випадку), а також до оракула розшифрування, який розшифровує довільні шифротексти на вимогу противника, повертаючи відкритий текст.

«Гра» складається з таких кроків:

1) претендент генерує ключову пару PK, SK, що базується на параметрі безпеки k (наприклад, розмір ключа у бітах), та видає PK противнику. Претендент зберігає SK;
2) противник може виконувати будь-яке число зашифрувань, викликати оракула розшифрування, що заснований на довільних шифротекстах або інших операціях;
3) зрештою, противник представляє два різні обрані відкриті тексти M_0, M_1 претенденту;
4) претендент обирає біт $b \in \{0, 1\}$ рівномірно у випадковому порядку та відправляє «виклик» шифротексту $C = E(PK, M_b)$ назад противнику;
5) противник може вільно виконувати будь-яку кількість додаткових обчислень або зашифрувань:
   а) у *неадаптивному* випадку (IND-CCA1) порушник може *не* виконувати подальших викликів оракула розшифрування;
   б) у *адаптивному* випадку (IND-CCA2) порушник може виконувати подальші виклики оракула розшифрування, але може не відправляти виклик шифротексту C;
6) нарешті, противник виводить припущення для значення b.

Схема є IND-CCA1/IND-CCA2 безпечною, якщо жоден противник не має жодної, хоча б малої, переваги для перемоги у грі.

Модель безпеки EUF-CMA. Поняття (або рівень) безпеки повністю визначається співвідношенням між метою (ціллю) порушника та моделлю порушника. В залежності від контексту, в якому використовується дана схема підпису (або криптосистема), можна формально визначити поняття безпеки системи, задавши цілі порушника, які він намагатиметься досягти та методи / засоби, які йому доступні (модель порушника).

Введемо позначення можливий цілей порушника.

UB (стійкість) — зловмисник відновлює секретний ключ *sk* з відкритого ключа *pk* (або еквівалентного ключа, якщо такий існує). Вона неявно з'явилася з виникненням схем підпису з відкритим ключем (криптографії з відкритим ключем).

UUF (універсальна нерозрізнювальність) — зловмисник може згенерувати дійсний підпис *S* будь-якого повідомлення *M* без розкриття секретного ключа *sk.*

EUF (екзистенційна нерозрізнюваність) — зловмисник створює повідомлення *M* і його дійсний підпис *S* (хоча не має ніякого контролю над повідомленням).

Моделі порушника можуть бути наступні.

KOA (ключова атака) — зловмисник має доступ тільки до відкритого ключа *pk*. Цей випадок неминучий для схем підпису з відкритим ключем (криптографії з відкритим ключем).

KMA (атака на основі відомого повідомлення) — зловмисник має доступ до підписів безлічі відомих повідомлень.

CMA (атака на основі вибраного повідомлення) — зловмисник має змогу використовувати в якості підписувача Оракул (повний доступ), і може запросити підпис будь-якого повідомлення на свій вибір (кілька запитів одного і того ж повідомлення дозволені).

Наведемо графічне представлення (рисунок), для цього перенесемо показники цілей порушника на вісь *Y*, а показники моделей порушника на вісь *X*. Таким чином, точки перетину показників цілей порушника та моделей формалізуватимуть поняття безпеки або рівень безпеки.

Схема підпису є екзистенційно непідробною, якщо зловмисник не може згенерувати будь-яку пару повідомлень підпису.

При реалізації атаки адаптивно підібраного повідомлення, зловмисник має доступ до оракула підпису, за допомогою якого він може підписувати повідомлення за своїм вибором.

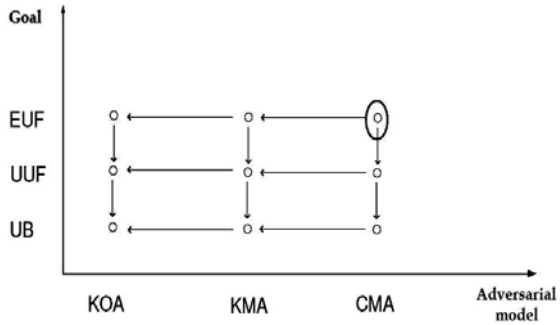

Рисунок. *Поняття безпеки схеми цифрового підпису [6]*

Нехай, $\Pi = (K, T, V)$ — код автентифікації повідомлення та, нехай, *Aeuf* — ймовірнісний алгоритм, який виконується за поліноміальний час. Розглянемо послідовність атаки.

1. Обчислення секретного стану $K \xleftarrow{\$} K(1^k)$.
2. Порушнику *Aeuf* надається необмежений доступ до міток оракула генерації *OT* та оракула перевірки *OV* виконання *TK* та *VK*.
3. Зрештою, *Aeuf* виводить пару повідомлення/мітка (M, T).

Нехай *QueriedEarlier* буде подією, що A^{euf} виводить повідомлення M, що буде вже запитувати мітку оракула генерації O_T. Ймовірність успіху A^{euf} $Succ_A^{euf} = Succ_A^{euf}(k)$ визначається:

$$Succ_{Aeuf} = Pr\left[v_{pk}(M, \sigma) = true \ and \ \neg Queried \ \ Earlier \right]$$

і ми маємо у вигляді КАП П як безпечне в змісті EUF-CMA, якщо $Succ_A^{euf}$ мізерно мале для всіх імовірнісних порушників поліноміального часу A^{euf}.

Висновки. Останні досягнення технологій у частині квантових обчислень формують нові виклики для сучасної криптографії та обумовлюють необхідність пошуку нових шляхів забезпечення безпеки інформації та її основних властивостей — конфіденційності, цілісності, автентичності та неспростовності. Важливою задачею для розгортання досліджень та розробки квантво-захищених алгоритмів є визначення вимог до них. В результаті проведеного аналізу, можна побачити, що такі вимоги формуються за цільовим призначенням стійкості, техніко-економічні та техніко-експлуатаційні вимоги. За результатами досліджень можна зробити висновки, що моделі безпеки допускають найвищий ступень обізнаності порушника.

Список використаних джерел:

1. NISTIR 8105 (DRAFT) Report on Post-Quantum Cryptography.
2. NISTIR (DRAFT) Proposed Submission Requirements and Evaluation Criteria for the Post-Quantum Cryptography Standardization Process.
3. ETSI GR QSC 001 V.1.1.1 (2016-07). Quntum-Safe Cryptography (QSC); Quantum-safe algorithmic framework.
4. Lindell, Y.: A Simpler Construction of CCA2-Secure Public-Key Encryption Under General Assumptions. In: Biham, E. (ed.) EUROCRYPT 2003. LNCS, Vol. 2656. P. 241–254. Springer, Heidelberg (2003).
5. Nojima R., Imai H., Kobara K., Morozov K.: Semantic security for the mceliece cryptosystem without random oracles. Des. Codes Cryptography 49(1-3), 289–305 (2008).
6. Faust S., Kiltz E., Pietrzak K., Rothblum G. Leakage-resilient signatures, Cryptology ePrint Archive: Report 2009/282, June, 2009, http://eprint.iacr.org/2009/282.

7. Madeline Gonzarlez Mun˜iz, Rainer Steinwandt: Security of signature schemes in the presence of key-dependent messages. In Tatra Mt. Math. Publ. 47 (2010), 15–29.

In the paper problems and risks for classical systems in the field of cryptographic protection of information in connection with the development of quantum computing are formulated. Problems the need to finding new solutions are grounded. The paper includes analysis of requirements of two major organizations NIST and ETSI. There are security models for cryptographic primitives offered in terms of post quantum cryptography.

Key words: *post quantum cryptography, requirements for crypto algorithms in post quantum period, NIST requirements, ETSI requirements, security models for post quantum cryptography.*

Одержано 15.02.2017

УДК 519.1:004

І. А. Ревенчук, канд. техн. наук, доцент

Харківський національний університет радіоелектроніки, м. Харків

МАТЕМАТИЧНА МОДЕЛЬ АГРЕГАЦІЇ ДАНИХ В СОЦІАЛЬНИХ МЕДІА

В роботі представлена математична модель агрегації даних соціальних мереж за допомогою узагальнення графа, що може в подальшому використовуватися в галузі інтернет маркетингу і створення необхідних пакетів даних для користувача соціальних мереж.

Ключові слова: *агрегація даних, соціальні мережі, платформи агрегації, узагальнення графу, медіа данні.*

Вступ. Акаунти у соціальних мережах мають мільйони користувачів, і кожен середній користувач має профіль у більш ніж одній з цих мереж. Деякі дані з профілю користувача соціальної мережі є конфіденційними, а деякі — відкритими. Існує величезна кількість загальнодоступних даних, які можуть бути об'єднані і використані для створення профілю користувача, а також визначення способу комунікації з ним.

Агрегація даних на основі веб-платформи включає агрегування загальнодоступних даних про людину з веб-сайтів соціальних мереж.

Інтерес представляють такі функціональні можливості: пошук, побудова профілю з агрегованими даними користувача, якого шукають;список контактів або взаємодій користувача в мережі; галузь наукових інтересів; індивідуальний маркетинг.

Аналіз методів агрегації даних, як концепція може бути розширена до формування змісту профілю користувача соціальної мережі. Відомос-

