Список використаних джерел:

1. URL: https://csrc.nist.gov/projects/post-quantum-cryptography/round-2-submissions.
2. URL: https://ntruprime.cr.yp.to.
3. URL: https://groups.google.com/a/list.nist.gov/forum/#!forum/pqc-forum.
4. URL: https://sourceforge.net/ projects/threebears/
5. URL: https://eprint.iacr.org/2012/230.pdf.
6. URL: https://eprint.iacr.org/2012/688.
7. URL: https://newhopecrypto.org.
8. URL: https://eprint.iacr.org/2017/634.pdf.
9. URL: https://eprint.iacr.org/2018/230.pdf.
10. URL: https://round5.org.
11. URL: https://cryptojedi.org/papers/sphincs-20141001.pdf.

ACTUAL ISSUES ANALYSIS REGARDING PERSPECTIVE PUBLIC-KEY CRYPTOGRAPHY

An analysis of current research on cryptography on lattices is given. The analysis takes place in accordance with the most relevant algorithms that have gone through the second stage of the US NIST competition. Some of them are combined — include several similar algorithms from the past stage. For a detailed consideration of them, a number of relevant topics for post-quantum algorithms are presented, which allows them to be described and categorized more substantially.

Key words: *lattice, post-quantum algorithm, LWE, ring, encapsulation.*

Одержано 02.12.2018

УДК 004.056.55
DOI: 10.32626/2308-5916.2019-19.49-55

М. В. Єсіна, канд. техн. наук

АТ «Інститут інформаційних технологій»,
Харківський національний університет імені В. Н. Каразіна, м. Харків

МОДЕЛІ БЕЗПЕКИ ПОСТКВАНТОВИХ КРИПТОГРАФІЧНИХ ПРИМІТИВІВ

У даній роботі розглядається сутність та досліджуються моделі безпеки щодо асиметричних постквантових криптографічних примітивів різного типу. За основу взяті моделі безпеки, які рекомендовані NIST США у вимогах конкурсу PQC до кандидатів на постквантові криптографічні примітиви. До таких алгоритмів відносяться асиметричні криптографічні перетворення типу асиметричне шифрування, цифровий підпис та механізм інкапсуляції ключів. Рекомендованими є наступні моделі безпеки, які стосуються: щодо асиметричного шифрування — IND-CCA2 (IND-CPA, IND-CCA); щодо цифрового підпису — EUF-CMA (та її варіації); щодо механізмів інкапсуляції ключів —

СК-модель. У роботі розглядається основна сутність таких моделей безпеки. Використання моделей безпеки при дослідженнях криптографічних примітивів є відносно новим. Потрібне узагальнення щодо кожної із вказаних моделей та визначення необхідності та умов, і наслідків їх застосування. У таких моделях враховується середовище застосування, в якому може діяти неавтентифікований чи автентифікований порушник. У роботі розглядається поняття нерозрізнюваності (невизначеності) та моделі безпеки постквантових асиметричних шифрів на її основі. Визначається властивість нерозрізнюваності (невизначеності) при атаці на основі підібраного (вибраного) відкритого тексту. Розглядається поняття семантичної безпеки. Наводяться види найпоширеніших атак на основі нерозрізнюваності (невизначеності). Розглядаються існуючі різновиди моделі безпеки EUF-CMA — SUF-CMA і т. д. Даються визначення понять «пряма секретність» (forward security, forward secrecy) та «досконала пряма секретність» (perfect forward secrecy (PFS)). Також у роботі розглядаються особливості застосування щодо перспективних асиметричних перетворень «теорії ігор». Надається визначення поняття «теорія ігор».

Ключові слова: *атака, інкапсуляція ключів, модель безпеки, семантична безпека, шифротекст, електронний підпис.*

Вступ. У критеріях відбору, які висуваються NIST США до кандидатів на постквантові стандарти криптографічного захисту інформації [1], визначено моделі безпеки, яким повинні відповідати кандидати. Відповідно до трьох кандидатів — асиметричний шифр (АСШ), цифровий підпис та протокол інкапсуляції ключів (ПІК), визначено три моделі безпеки. Стосовно АСШ — IND-CCA2 (IND-CPA, IND-CCA), для підпису — EUF-CMA-модель та для ПІК — СК-модель [1].

На наш погляд, на сьогоднішній день проблемними є питання, що стосуються узагальненого визначення та дослідження моделей безпеки постквантових криптопримітивів різного типу, але з урахуванням основних положень та пропозицій, що викладені у [2–5]. На відміну від традиційного застосування тільки моделей порушника та загроз, при створенні кандидатів на перспективні асиметричні криптографічні перетворення запропоновано використовувати моделі безпеки. Але, ні досвіду, ні рекомендацій щодо їх застосування практично немає чи вони є формальними. Тому, на наш погляд, актуальною є проблема узагальненого визначення та дослідження моделей безпеки взагалі, в першу чергу на рівні сутності, умов та можливостей застосування при оцінці кандидатів щодо їх вразливості щодо класичного та квантового криптоаналізу.

Мета цієї роботи — узагальнене визначення, класифікація та попереднє дослідження моделей безпеки, зокрема, визначення можливостей та умов застосування постквантових криптопримітивів при протидії із сторони класичного чи квантового порушника [2–5].

Модель безпеки постквантових алгоритмів асиметричного шифрування. Нерозрізнюваність (невизначеність) зашифрованого тексту — це важлива властивість безпеки багатьох схем шифрування. Якщо криптосистема володіє властивістю нерозрізнюваності, то зловмисник не зможе відрізнити пари шифрованих текстів на основі повідомлення, що вони шифрують [6].

Властивість нерозрізнюваності при атаці на основі підібраного відкритого тексту вважається основною вимогою для більшості достовірно захищених криптосистем з відкритим ключем, хоча деякі схеми також забезпечують нерозрізнюваність при атаці на основі підібраного зашифрованого тексту та атаці на основі адаптивно підібраного зашифрованого тексту. Нерозрізнюваність при атаці на основі підібраного відкритого тексту еквівалентна властивості семантичної безпеки, і багато криптографічних доказів використовують ці визначення як еквівалентні [6].

Криптосистема вважається «безпечною з точки зору нерозрізнюваності», якщо жоден зловмисник A, отримавши зашифроване повідомлення, довільно вибране з двоелементного простору повідомлень, визначеного зловмисником, не може ідентифікувати вибір повідомлення з ймовірністю значно краще, ніж при випадкових вгадуваннях (½). Якщо будь-який зловмисник може вдало відрізнити вибраний шифрований текст з ймовірністю значно більше, ніж ½, тоді цей зловмисник вважається таким, що має «перевагу» в розрізнені шифрованого тексту, і схема «не» вважається безпечною з точки зору нерозрізнюваності [6].

Безпека з точки зору нерозрізнюваності представляється як гра, де криптосистема вважається безпечною, якщо жоден із зловмисників не може виграти гру зі значно більшою ймовірністю, ніж зловмисник, який повинен вгадати випадковим чином. Найпоширеніші визначення, що використовуються у криптографії [6, 7]: нерозрізнюваність при атаці на основі підібраного відкритого тексту (IND-CPA безпека); нерозрізнюваність при атаці на основі підібраного шифртексту (IND-CCA безпека); нерозрізнюваність при атаці на основі адаптивно підібраного шифртексту (IND-CCA2 безпека).

Безпека за будь-яким з останніх визначень означає безпеку за попередніми [6]: схема, яка є IND-CCA безпечною, також є IND-CPA безпечною; схема, яка є IND-CCA2 безпечною, є як IND-CCA безпечною, так і IND-CPA безпечною. Таким чином, IND-CCA2 є найстрогішим з цих трьох визначень безпеки.

Семантична безпека — поняття, яке описує безпеку схеми шифрування, позначається як SEM-CPA та фіксує ідею, що безпечна схема шифрування повинна приховувати всю інформацію про невідомий відкритий текст. Зловмиснику дозволяється вибирати між двома відкритими текстами m_0 та m_1, і він отримує зашифрування будь-якого з відкритих текстів. Схема шифрування є семантично безпечною, якщо

зловмисник не може здогадуватися з кращою ймовірністю, ніж ½, чи даний шифртекст є зашифруванням повідомлення m_0 або m_1. Семантична безпека вимагає, щоб те, що можна ефективно обчислювати щодо деяких відкритих текстів з їх шифртекстів, можна обчислювати так само легко за відсутності цих шифртекстів [8].

Модель безпеки постквантових цифрових підписів. Сьогодні пропонується як модель безпеки стосовно постквантових підписів застосовувати EUF-CMA модель. EUF-CMA визначає екзистенційну непідроблюваність від атак на основі адаптивно вибраних повідомлень. Зокрема, безпека в сенсі EUF-CMA не дозволяє криптоаналітику виробляти підпис для повідомлень, що залежать від ключів, наприклад, підпис при застосуванні повного особистого *sk* ключа. Якщо є хоча б один запит повідомлення, що залежить від ключів, безпека механізму підпису порушується [9–12].

Існує два загальних формальних визначення для забезпечення безпеки схеми цифрового підпису. Кожне з цих визначень представлено як «гра», або експеримент, який виконується між атакуючим (attacker) та деяким чесним претендентом (challenger).

Теорія ігор — теорія математичних моделей прийняття оптимальних рішень в умовах конфлікту. Оскільки сторони, що беруть участь у більшості конфліктів, зацікавлені в тому, щоб приховати від противника власні наміри, прийняття рішень в умовах конфлікту, зазвичай, відбувається в умовах невизначеності.

Неформально, експеримент EUF-CMA працює так [9–12]:

1. Претендент генерує дійсну пару ключів (*pk, sk*) і надає *pk* атакуючому.
2. Атакуючий тепер може повторно запросити підписи на підібраних повідомленнях (M_1,...,M_q) за своїм вибором, і отримує дійсні підписи (σ_1,...., σ_q) у відповідь.
3. По завершенню експерименту зловмисник повинен вивести повідомлення та підпис M^*, σ^* такі, що (1) повідомлення було не одним із повідомлень, які вимагали попереднього кроку, і (2) повідомлення/підпис перевіряється правильно з відкритим ключем.

Схема вважається безпечною, якщо жоден зловмисник не має ні найменшої переваги у виконанні вищезазначених умов. Зазвичай кількість повідомлень q обмежується лише часом виконання атакуючого, однак для спеціального випадку одноразових підписів, зловмисник обмежується запитом лише одного підпису на кроці (2).

Це визначення досить сильне, але не настільки сильне, наскільки це можливо. Дещо сильнішим є визначення SUF-CMA.

Неформально, експеримент SUF-CMA працює так [9–12]:

1. Аналогічно попередньому експерименту.

2. Аналогічно попередньому експерименту.
3. Після завершення експерименту, атакуючий повинен вивести повідомлення та підпис M^*, σ^* такі, що (1) пара (M^*, σ^*) не була одним із запитаних повідомлень, а підпис повернувся на попередньому кроці, (2) повідомлення/підпис перевіряється на відкритому ключі.

Головна відмінність полягає у тому, що це більш сильне визначення гарантує, що атакуючий не зможе підібрати підпис [8].

Модель безпеки постквантових протоколів інкапсуляції ключів. Модель СК включає у себе три основні компоненти: модель неавтентифікованого порушника (UM), модель автентифікованого порушника (AM) та механізм автентифікації (автентифікатор) (MT). Модель безпеки СК використовується для автентифікації обміну ключами (AKE) [2]. СК-модель стосується безпеки ключа сеансу, що використовується на сеансі зв'язку. При її оцінці використовується формальна модель для протоколів обміну ключами та можливостей криптоаналітика. Поняття безпеки, яке називається безпекою ключа сеансу (або SK-безпека), направлене на забезпечення безпеки окремих ключів сеансу. Її порушення являє собою компрометацію сеансового ключа. У випадку безпечності ключа, зловмисник «нічого не дізнається про значення ключа», коли він перехвачує дані протоколу обміну ключами та здійснює атаки на інші сеанси та сторони, що взаємодіють. Такий підхід є стандартним для моделі семантичної безпеки, коли криптоаналітик не може відрізнити реальне значення ключа від незалежного випадкового значення [2].

Поняття досконалої прямої безпеки (PFS) відноситься до властивості протоколів обміну ключами (KE), за допомогою якої розкриття довгострокових ключів, що використовується у протоколі для автентифікації та узгодження ключів сеансу, не ставить під загрозу секретність ключів сеансу, встановлених до розкриття [2].

Висновки. 1. На сьогодні запропоновано три моделі безпеки: асиметричне шифрування — IND-CPA, IND-CCA/CCA2, цифровий підпис — EUF-CMA, та механізми інкапсуляції ключів — СК. Моделі безпеки усіх асиметричних криптоперетворень засновуються на понятті «теорії ігор».

2. Сьогодні актуальна — проблема узагальненого визначення та дослідження моделей безпеки, визначення сутності, умов їх застосування при криптоаналізі та використання при оцінці захищеності від відомих класичних та квантових атак.

3. Відповідно до моделі безпеки на основі нерозрізнюваності, безпека за будь-яким з наступних визначень означає безпеку за попередніми, тобто: схема, яка є IND-CCA безпечною, є IND-CPA безпечною; схема, яка є IND-CCA2 безпечною, є як IND-CCA безпечною,

так і IND-CPA безпечною. Тобто, IND-CCA2 є найстрогішим з цих трьох визначень безпеки. Нерозрізнюваність при атаці на основі підібраного відкритого тексту (IND-CPA) еквівалентна властивості семантичної безпеки (SEM-CPA).

4. Як модель безпеки щодо постквантових криптоперетворень типу підпис застосовується EUF-CMA-модель. EUF-CMA-модель визначає екзистенційну непідроблюваність від атак на основі адаптивно вибраних повідомлень. Зокрема, безпека в сенсі EUF-CMA не дозволяє зловмиснику виробляти підписи для повідомлень, що залежать від ключів, наприклад, підпис при застосуванні повного особистого *sk* ключа. При наявності хоча б одного запиту повідомлення, що залежить від ключів, безпека механізму підпису порушується.

5. CK модель безпеки включає у себе три основні складові компоненти: модель неавтентифікованого порушника (UM), модель автентифікованого порушника (AM) та механізм автентифікації (автентифікатор) (MT). Як правило модель безпеки CK використовується для автентифікації обміну ключами (AKE).

6. Модель безпеки CK стосується безпеки ключа сеансу, що використовується на сеансі зв'язку. При оцінці протоколів обміну ключами та можливостей криптоаналітика використовується формальна модель. Поняття безпеки, яке називається безпекою ключа сеансу (або SK-безпека), направлене на забезпечення безпеки окремих ключів сеансу. Її порушення може призвести до компрометації ключа сеансу.

Список використаних джерел:

1. Post-Quantum Cryptography. URL: https://csrc.nist.gov/projects/post-quantum-cryptography/round-1-submissions.
2. Ran Canetti, Hugo Krawczyk Analysis of Key-Exchange Protocols and Their Use for Building Secure Channels. URL: http://iacr.org/archive/eurocrypt2001/20450451.pdf.
3. Shoup V. On Formal Models for Secure Key Exchange, Theory of Cryptography Library, 1999. URL: http://philby.ucsd. edu/cryptolib/1999/9912.html.
4. Yoshida Y., Morozov K., Tanaka K. CCA2 Key-Privacy for Code-Based Encryption in the Standard Model. Post-Quantum Cryptography. PQCrypto 2017. Lecture Notes in Computer Science, Vol. 10346. Springer, Cham.
5. Bellare M., Boldyreva A., Desai A., Pointcheval D. Key-privacy in public-key encryption. ASIACRYPT 2001. LNCS. Vol. 2248. P. 566–582. Springer, Heidelberg (2001). doi:10.1007/3-540-45682-1 33.
6. Ciphertext indistinguishability. URL: http://cse.iitkgp.ac.in/~debdeep/-courses_iitkgp/FCrypto/scribes/scribe8.pdf.
7. Henk C.A. van Tilborg, Sushil Jajodia (Eds.) Encyclopedia of Cryptography and Security Springer, 2011. 1416 p.
8. Bellare M. Symmetric encryption. URL: https://cseweb.ucsd.edu/~mihir/-cse207/w-se.pdf.

9. EUF-CMA and SUF-CMA. URL: https://blog.cryptographyengineering.com/-euf-cma-and-suf-cma.
10. Haitner I., Holensteiny T. On the (im) possibility of key dependent encryption, in: TCC'09 — Theory of Cryptography, 6th Theory of Cryptography Conference, San Francisco, CA, USA, 2009, Lecture Notes in Comput. Sci. Vol. 5444, Springer, Berlin, 2009, P. 202–219.
11. Hofheinz D., Unruh D. Towards key-dependent message security in the standard model. *EUROCRYPT'08 — Advances in Cryptology*, 27th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Istanbul, Turkey, 2008, Lecture Notes in Comput. Sci., Vol. 4965, Springer, Berlin, 2008. P. 108–126.
12. Applebaum B., Cash D., Peikert C., Sahai A. Fast cryptographic primitives and circular-secure encryption based on hard learning problems. *Advances in Cryptology — CRYPTO'09*, 29th Annual International Cryptology Conference, Santa Barbara, CA, USA, 2009. Lecture Notes in Comput. Sci. Vol. 5677, Springer, Berlin, 2009. P. 595–618.

SECURITY MODELS OF POST-QUANTUM CRYPTOGRAPHIC PRIMITIVES

In this paper, the essence is considered and security models of asymmetric post-quantum cryptographic primitives of different types are investigated. The basis taken security models that are recommended by NIST USA in the requirements of the PQC competition for candidates for post-quantum cryptographic primitives. Such algorithms include asymmetric cryptographic transformations such as asymmetric encryption, digital signature, and key encapsulation mechanism. The following security models are recommended, which are related to: the asymmetric encryption — IND-CCA2 (IND-CPA, IND-CCA); the digital signature — EUF-CMA (and its variations); the key encapsulation mechanisms — CK-model. In this paper, the basic essence of such security models is considered. The use of security models in research of cryptographic primitives is relatively new. A generalization of each of these models and a definition of the necessity and conditions, and the consequences of their application are required. Such models take into account the application environment in which an unauthenticated-links adversarial model and authenticated-links adversarial model can operate. The paper considers the concept of indistinguishability and security model of post-quantum asymmetric ciphers on its basis. The property of indistinguishability under chosen plaintext attack is determined. The concept of semantic security is considered. The types of most common attacks based on indistinguishability are given. Existing versions of the EUF-CMA security model — SUF-CMA, etc. are considered. Definitions of «forward security, forward secrecy» and «perfect forward secrecy (PFS)» are given. In addition, the paper considers the peculiarities of the application regarding to perspective asymmetric transformations of the «game theory». The definition of concept «game theory» is given.

Key words: *attack, key encapsulation, security model, semantic security, ciphertext, signature.*

Одержано 26.01.2019