СЛУЖБА БЕЗПЕКИ УКРАЇНИ

ІНСТИТУТ ПІДГОТОВКИ ЮРИДИЧНИХ КАДРІВ
ДЛЯ СЛУЖБИ БЕЗПЕКИ УКРАЇНИ
НАЦІОНАЛЬНОГО ЮРИДИЧНОГО УНІВЕРСИТЕТУ
ІМЕНІ ЯРОСЛАВА МУДРОГО

АКТУАЛЬНІ ПИТАННЯ ЗАБЕЗПЕЧЕННЯ СЛУЖБОВО-БОЙОВОЇ ДІЯЛЬНОСТІ СИЛ СЕКТОРУ БЕЗПЕКИ І ОБОРОНИ

Матеріали Всеукраїнського круглого столу
(м. Харків, 23 квітня 2021 року)

Випуск 5

Харків
2021

УДК 351.74-057.36
ББК 67.9(4УКР)301.1
А43

Рекомендовано до видання Вченою радою
Інституту підготовки юридичних кадрів для Служби безпеки України
Національного юридичного університету імені Ярослава Мудрого,
протокол засідання від 28.04.2021 № 10

Редколегія може не поділяти погляди, викладені у збірнику. Автори опублікованих матеріалів несуть відповідальність за їх зміст.

А43 Актуальні питання забезпечення службово-бойової діяльності сил сектору безпеки і оборони : матеріали всеукр. круг. столу (м. Харків, 23 квіт. 2021 р.) / редкол.: Є.О. Меленті, І.В. Євтушенко, О.А. Гарбузов, В.О. Пономарьов – Х.: ФОП Бровін О.В., 2021. – Вип. 5. – 412 с.
ISBN 978-617-8009-14-4

До збірника увійшли тези доповідей науковців, практичних працівників та курсантів, присвячені проблемам забезпечення службово-бойової діяльності складових сектору безпеки і оборони України в умовах сьогодення.

Для співробітників сил безпеки і оборони, науковців, викладачів, курсантів та студентів закладів вищої освіти.

УДК 351.74-057.36
ББК 67.9(4УКР)301.1

Адреса Інституту: м. Харків, вул. Мироносицька, 71,
телефон/факс (057) 700-34-55
E-mail: ipuk@ssu.gov.ua

ISBN 978-617-8009-14-4

7. ІНШІ ПИТАННЯ, ПОВ'ЯЗАНІ З ТЕМОЮ ВСЕУКРАЇНСЬКОГО КРУГЛОГО СТОЛУ

Гаврилова А.А., завідувач навчальної лабораторії кафедри кібербезпеки та інформаційних технологій Харківського національного економічного університету імені Семена Кузнеця, старший викладач

АНАЛІЗ КРИПТОГРАФІЧНИХ АЛГОРИТМІВ ПОДАНИХ ДО ТРЕТЬОГО ТУРУ КОНКУРСУ NIST

Пошук криптографічно стійкого алгоритму проводиться в рамках конкурсу NIST в три етапи відповідно до такими критеріями оптимальності: первинне вивчення алгоритму, проведення криптоаналітичних досліджень вразливостей конкретного алгоритму і проведення порівняння алгоритмів за критеріями швидкодії і мінімальності вимог до обчислювальних ресурсів.

Рішення, подані для участі в конкурсі NIST, реалізують такі механізми [1]: цифровий підпис, шифрування, інкапсуляцію ключів і вироблення загального ключа.

З огляду на досвід раніше проведених NIST конкурсів на створення блокового шифру (AES) і геш-функції (SHA-3), комплекс робіт з аналізу пропозицій і створенню нових стандартів може тривати до п'яти років.

NIST висуває вимоги по стійкості до учасників конкурсу як формальні (строго доказові на основі припущення про складність рішень деякої задачі), так і практичні. Серед строго доказових вимог на основі припущення про складність рішень деякої задачі виділяють вимоги до асиметричних систем шифрування і електронного підпису [2].

Для асиметричних систем шифрування характерні такі вимоги, як:

- стійкість до загрози розрізнення шифртекстів щодо атаки на основі підібраного відкритого тексту (Indistinguishability Against Chosen Plaintext Attack, IND-CPA);
- стійкість до загрози розрізнення шифртекстів щодо атаки на основі підібраного шифрованого тексту (Indistinguishability Against Chosen Ciphertext Attack, IND-CCA);
- стійкість до загрози розрізнення шифртекстів щодо атаки на основі (неадаптивно) підібраного відкритого тексту (Indistinguishability Against (non-adaptive) Chosen Plaintext Attack, IND-CPA1);
- стійкість до загрози розрізнення шифртекстів щодо атаки на основі (неадаптивно) підібраного шифрованого тексту (Indistinguishability Against (non-adaptive) Chosen Ciphertext Attack, IND-CCA1);

- стійкість до загрози розрізнення шифртекстів щодо атаки на основі адаптивно підібраного відкритого тексту (Indistinguishability Against Adaptive Chosen Plaintext Attack, IND-CPA2);

- стійкість до загрози розрізнення шифртекстів щодо атаки на основі адаптивно підібраного шифрованого тексту (Indistinguishability Against Adaptive Chosen Ciphertext Attack, IND-CCA2).

Для схем електронного підпису інтерес представляють наступні поняття стійкості:

- сильна стійкість до підробки щодо атак на основі підібраних повідомлень (Strong Unforgeability under Chosen Message Attacks, SUF-CMA);

- стійкість до екзистенціальної підробки щодо атак на основі підібраних повідомлень (Existentially Unforgeability under Chosen Message Attacks, EUF-CMA).

Визначення практичної стійкості, задані вимогами NIST, передбачають п'ять рівнів стійкості [2]: 1) визначення ключа 128-бітового блокового шифру; 2) пошук колізії 256-бітової геш-функції; 3) визначення ключа 256-бітового блокового шифру; 4) пошук колізії 384-бітової геш-функції; 5) визначення ключа 384-бітового блокового шифру.

Основні рішення, що застосовуються конкурсантами NIST, відносять до шести груп [3]:

- використання теорії цілочисельних решіток – засновані на ряді складних завдань, в їх числі NP-задачі пошуку найкоротшого вектора (SVP) і пошуку найближчого вектора (CVP);

- задача навчання з помилками (LWE; RLWE) і завдання пошуку найменшого цілочисельного рішення системи лінійних алгебраїчних рівнянь (SIS);

- використання кодів, що виправляють помилки – схема Мак-Еліса за умови використання кодів Гоппи залишається стійкою;

- використання многочленів від багатьох змінних – досліджується з точки зору синтезу кріптосхем;

- використання криптографічних геш-функцій – використовують одноразові підписи Лампорта і Вінтерніца, адаптуючи їх для побудови багаторазової схеми підпису на основі деревовидної структури геш-значень спеціального виду;

- використання ізогеній на суперсінгулярних еліптичних кривих – в основу покладено вирішення складної задачі пошуку шляху в графі ізогеній між суперсінгулярними еліптичними кривими;

- вузькоспеціалізовані задачі (проблеми сполученого пошуку (Search Problem) або операції в групах кіс (Braid Groups), алгебра октоніонів, многочлени Чебишева і т.д.

У першому етапі взяли участь 69 алгоритмів, до другого етапу вийшли 15 алгоритмів, а для участі в третьому етапі виділено 7 основних та 8 альтернативних алгоритмів, які потенційно можуть бути стандартизовані. З досвіду раніше проведених NIST аналогічних конкурсів з вибору блочного шифру (AES) і функції гешування (SHA-3), процес стандартизації квантово-стійких алгоритмів може завершитися в 2022 році.

22 липня 2020 року, були оголошені фіналісти другого етапу, які пройшли далі. Залишилося всього 4 кандидати на асиметричне шифрування і 3 кандидати на цифровий підпис [2]. Результат розгляду основних властивостей і характеристик обраних алгоритмів [4 – 8] наведено в табл. 1.

Таблиця 1

Визначення основних характеристик криптографічних алгоритмів-переможців другого етапу конкурсу NIST

Алгоритм	Синтезні рішення	Основа	Криптоаналіз	Переваги	Недоліки
Постквантовий стандарт цифрового підпису					
CRYSTALS-DILITHIUM	Криптографія на решітках	схема Фіата-Шаміра з перериваннями	Рішення задач Module-LWE та Module-SIS	Задовільнапродуктивність; реалізація на малоресурсному пристрої	Відсутність загальносистемних параметрів для 5 рівня безпеки
FALCON	Криптографія на решітках	Фрейм-ворк GPV	Рішення задач SIS на NTRU-решітках (алгебраїчних)	Невразливий до атак: відно-влення ключів, підробка підпису, комбінаторна атака, гібридна атака, щільна підрешітка високого ран-	Складна програмна та апаратна реалізація; відсутність аналізу стійкості до атак за сторонніми каналами; складна реалізація для малоресурс-

				гу	них пристроїв
Rainbow	Криптографія на мультиваріативних перетвореннях	Схема UOV	Рішення специфічних задач	Розмір цифрового підпису не великий	Великий розмір ключа
Асиметричне шифрування					
Classic McEliece	Криптографія на ко-дах, які виправляють помилки	Теорія алгебраїчного кодування	Рішення специфічних задач	Невеликі розміри шифртекстів	Дуже великий розмір ключа
CRYSTALS-KYBER	Криптографія на решітках	Перетворення Фуджисакі-Окамо-то	Рішення задач Module-LWE	Гарна продуктивність та безпечність	Module-LWE мало вивчен та вимагає більш деталь-ного крипто-аналізу
NTRU	Криптографія на решітках	Схема NTRU-Encryt	Технологічний стандарт для фінансових транзакцій	Висока швидкість асиметричного шифрування, гарна паралелізація, протистояння ата-кам з використанням квантових комп'ютерів	-
SABER	Криптографія на решітках	Перетворення Фуджисакі-Окамо-то	Рішення задач Module-LWE (використовується округлення за меншим модулем)	Висока пропускна здатність та час обчислень	Висока вартість випадкової генерації чисел на платформах з обмеженими ресурсами

За твердженням NIST тільки одна з двох схем нових постквантових стандартів цифрового підпису (CRYSTALS-DILITHIUM і FALCON) буде стандартизована. Таким чином, для цифрового підпису скоріше за все в майбутньому будуть використовуватися схеми на основі криптографії на

решітках. Але для більш специфічних завдань можна буде застосовувати і алгоритм Rainbow.

Щодо асиметричного шифрування - для загального використання рекомендуються схеми на основі решіток, але тільки одна з схем на решітках (CRYSTALS-KYBER, NTRU і SABER) буде стандартизована.

В результаті проведеного аналізу рішень конкурсу NIST можна зробити висновок про те, що він справив значний вплив на розвиток методів синтезу і аналізу нових квантово-стійких криптографічних схем, змушує ретельно перевіряти нові стандарти, що розробляються в рамках програм цієї організації. Таким чином, необхідність розробки сімейства постквантових криптографічних механізмів є важливим завданням, але, з огляду на обсяг витрат на ці заходи, рішення про перехід до використання постквантової криптографії має прийматися зважено, на основі точного прогнозу розвитку потужності квантових обчислювачів.

Список використаних джерел:

1. NIST объявило о начале третьего этапа стандартизации постквантовой криптографии URL: https://habr.com/ru/post/512410/ (дата обращения: 24.07.2020).
2. Гребнев С. О некоторых тенденциях развития постквантовой криптографии URL: https://www.itsec.ru/articles/o-nekotoryye-tendentsii-razvitiya-postkvantovaya-kriptografiya (дата обращения: 31.05.2019).
3. История криптографии. Часть 1. Первый стандарт криптографии URL: https://www.angaratech.ru/press-center/novosti/istoriya-kriptografii-chast-1-pervyy-standart-kriptografii_972 (дата обращения: 21.02.2020).
4. Falcon: Fast-Fourier Lattice-based Compact Signatures over NTRU. Specifications v1.0. PierreAlain Fouque, Jeffrey Hoffstein, Paul Kirchner, Vadim Lyubashevsky, Thomas Pornin, Thomas Prest, Thomas Ricosset, Gregor Seiler, William Whyte, Zhenfei Zhang URL: https://falcon-sign.info/falcon.pdf (accessed on: 15.02.2021).
5. Черниш Д., Янко А. Обгрунтування стійкості алгоритму ЕЦП FALCON *«GLOBAL CYBER SECURITY FORUM 2019» 14 – 16 НОЯБРЯ 2019*, Харьков, Украина, 2019. С. 108 – 109.
6. Усатюк В.С. Реализация параллельных алгоритмов ортогонализации в задаче поиска кратчайшего базиса целочисленной решетки. *Прикладная дискретная математика. Приложение*, 2012, № 5. С. 120-122.
7. Хачатуров Р. В. Основные свойства решеток кубов, алгоритмы их построения и возможности применения в дискретной оптимизации. *Ж. вычисл. матем. и матем. физ.*, 2015, том 55, № 1, С. 121–134.
8. Шокуров А.В, Кузюрин Н.Н, Фомин С.А. Решетки, алгоритмы и современная криптография. URL: https://www.ispras.ru/courses/book-lattice-cryptography.pdf (дата обращения: 02.03.2021).