УДК 004.056.55 **DOI:10.30837/rt.2020.3.202.02**

Ю.І. ГОРБЕНКО, канд. техн. наук, О.В. ПОТІЙ, д-р техн. наук,
В.В. ОНОПРІЄНКО, канд. техн. наук, М.В. ЄСІНА, канд. техн. наук, Г.А. МАЛЄЄВА

ОСНОВНІ ПОЛОЖЕННЯ ЩОДО МОДЕЛІ БЕЗПЕКИ ДЛЯ АСИМЕТРИЧНИХ ПЕРЕТВОРЕНЬ ТИПУ ЕП З УРАХУВАННЯМ ВИМОГ ТА ЗАГРОЗ ПОСТКВАНТОВОГО ПЕРІОДУ

Вступ

Стосовно криптографічної стійкості (безпеки) асиметричних криптоперетворень, як і симетричних криптоперетворень, для оцінки використовуються існуючі методи, методики та різні системи криптоаналізу. Такий вузький підхід при аналізі стійкості залишає без необхідного врахування можливі моделі порушника, моделі загроз, а також не дає можливих варіантів протидії. На наш погляд, продуктивним може бути введення та використання узагальненої (комплексної) моделі криптографічної стійкості. Приймемо в якості складових комплексної моделі безпеки щодо асиметричних криптоперетворень типу ЕП такі часткові моделі:

- порушника щодо асиметричних криптоперетворень типу ЕП;
- загроз щодо асиметричних криптоперетворень типу ЕП;
- безпеки щодо асиметричних криптоперетворень типу ЕП.

При викладенні сутності, призначення, можливостей застосування та обмежень щодо такої комплексної моделі будемо орієнтуватись та використовувати результати теоретичного обґрунтування та розробки вказаних часткових моделей безпеки та комплексної моделі безпеки у цілому. Метою цієї статі є обґрунтування та розробка пропозицій щодо побудування комплексної моделі безпеки стосовно асиметричних криптоперетворень типу перспективний ЕП, що може та повинен застосовуватись в постквантовий період.

1. Визначення моделей порушника, загроз та безпеки щодо перспективного ЕП

Побудова моделі порушника необхідна для того, щоб розробити комплекс заходів із забезпечення захищеності механізмів ЕП, в тому числі з урахуванням вимог та умов їх застосування в постквантовий період. Така модель порушника може бути побудована з урахування різних критеріїв.

Звичайно модель порушника розробляється з метою отримання відповідей на наступні питання:

- від кого необхідно захищати інформацію?
- якою є мета порушника?
- якими знаннями володіє порушник?
- які повноваження в системі має потенційний порушник?
- які методи, системи та засоби використовує порушник?

По суті модель порушника – це опис можливих дій порушника, який формується на основі аналізу типу зловмисника, рівня його повноважень, знань, теоретичних та практичних можливостей. У якості порушника розглядається особа, що може отримати доступ до роботи з включеними до складу відповідної комп'ютерної системи (КС) засобами.

Модель загроз ЕП (далі – модель загроз) повинна бути документом, яким закріплено найбільш повний перелік загроз щодо існуючих та перспективних ЕП, що може застосовуватись в постквантовий період. Відповідно до Законів України "Про захист інформації в інформаційно-телекомунікаційних системах", "Про електронні довірчі послуги" та "Про захист персональних даних". Перелік можливих загроз безпеці застосування існуючих та перспективних ЕП сформований з числа загроз, наявних у IT-Grundschutz Catalogues [10] з урахуванням апаратних, програмних та апаратно-програмних ресурсів, технологій обробки даних та механізмів криптографічного захисту при застосуванні ЕП, в тому числі з урахуванням вимог та умов синтезу перспективних ЕП та застосування ЕП в постквантовий період.

Основними загрозами (атаками) з застосуванням квантових математичних методів, які можуть бути реалізованими на квантовому комп'ютері (звичайно, якщо він буде побудований та доступний для застосування), є такі:

- квантовий алгоритм факторизації Шора;
- квантовий алгоритм Гровера;
- квантовий алгоритм Шора вирішення дискретного логарифму в полі;
- квантовий алгоритм Шора вирішення дискретного логарифму в групі точок еліптичної кривої;
- квантовий алгоритм криптоаналізу для перетворень в фактор-кільці тощо.

Стосовно перспективного ЕП можливо виділити та необхідно, як мінімум, розглядати наступні атаки (загрози):

1. Атака грубої сили, тобто повного перебору.
2. Традиційна атака зустріч посередині.
3. Атака на основі алгоритму Arora-Ge.
4. Диференційні атаки.
5. BKW, коли LWE зводиться до SIS атаки.
6. Primal attack (Search-LWE зводиться до BDD атаки).
7. Dual attack (Decision-LWE зводиться до SIS).
8. Зведення до uSVP атаки пошуку короткого вектора.

Для однозначного розуміння та використання також введемо поняття щодо моделі безпеки (криптографічної стійкості) стандартизованих криптографічних примітивів ЕП. Модель безпеки (криптографічної стійкості) криптографічних примітивів (в тому числі типу ЕП) – це сукупність організаційно-технічних, програмно-технічних та логічних механізмів (методів) та заходів, законодавчих та нормативно-правових норм та правил, що визначають вимоги до методів синтезу, оцінки криптографічної стійкості та застосування стандартизованих криптографічних примітивів (типу ЕП), з урахуванням умов їх реалізації при інтенсивній протидії порушника 4-го рівня [8, 9] із застосуванням методів, систем та засобів класичного та квантового криптоаналізу.

Аналіз показує, що NIST США планує стандартизувати один чи декілька стандартизованих криптопримітивів типу ЕП, що будуть забезпечувати екзистенційну стійкість ЕП щодо атак на основі адаптивно підібраного повідомлення. Така безпека позначається в науковій літературі як EUF-CMA безпека [1, 2]. Представлені кандидати ЕП оцінюються на підставі того, наскільки такі можливості існують для кандидата на постквантовий стандарт, щоб забезпечити таку його властивість. Але така вимога не є обов'язковою, заявники не зобов'язані надавати докази безпеки щодо атаки на основі адаптивно підібраного повідомлення, хоча такі докази вже розглядаються та розглядатимуться при подальших дослідженнях, якщо вони будуть наявні (доступні).

Важливим є те, що у якості апріорних даних запропоновано вважати, що зловмисник має доступ не більш, ніж до 2^{64} обраних повідомлень. Проте, атаки за умови більшої кількості повідомлень також можуть розглядатись. Крім того, скоріше всього NIST розглядає як класичні, так і квантові атаки.

2. Загальні положення щодо моделі безпеки перспективного ЕП

Модель безпеки EUF-CMA визначає екзистенційну непідроблюваність від атак на основі адаптивно вибраних повідомлень [1, 2, 5]. Зокрема, безпека в сенсі EUF-CMA повинна протидіяти порушнику 4-го рівня виробляти ЕП для повідомлень, що залежать від ключів (застосуванні особистого sk ключа). По суті, при застосуванні механізму безпечного ЕП, згідно моделі EUF-CMA, вона є безпечною для EUF-CMA у випадку, коли не застосовуються запити повідомлення. Але, при наявності хоча б одного запиту повідомлення, що залежить від ключів, безпека механізму ЕП порушується.

Існує два загальних формальних визначення для забезпечення безпеки схеми ЕП [7]. Кожне з цих визначень представлено як експеримент, який виконується між атакуючим (attacker) та деяким чесним претендентом (challenger).

Експеримент щодо моделі EUF-CMA (екзистенційна непідроблюваність при атаці на основі підібраних повідомлень) виконується у такій послідовності:

1. Претендент генерує дійсну пару ключів (pk, sk) і надає pk атакуючому.

2. Далі атакуючий може повторно запросити підписи на підібраних (вибраних) 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 одне повідомлення було не одним із повідомлень, які вимагали попереднього кроку (1), і (2) повідомлення/підпис перевіряється правильно з відкритим ключем.

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

Така властивість є досить сильною, але не настільки як можливо. Дещо сильнішим визначенням є визначення моделі безпеки SUF-CMA [7].

Експеримент із застосуванням моделі SUF-CMA (сильна екзистенційна непідроблюваність при атаці на основі підібраних) повідомлень) виконується у такій послідовності:

1. Те саме, що і в попередньому експерименті.

2. Те саме, що і в попередньому експерименті.

3. Після завершення п. 2 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 правильно з відкритим ключем.

Атакуючий виграє, якщо вона задовольняє вищенаведеним умовам.

Головна відмінність моделі SUF-CMA полягає в тому, що це більш сильне визначення гарантує, що атакуючий не зможе підібрати підпис. Так, схема, в якій атакуючий може повторно рандомізувати дійсний підпис, щоб він залишався дійсним, але виглядав інакше, ніж вихідне значення, не задовольнила би умові SUF-CMA.

Введемо визначення 1 гри між зловмисником та схемою підпису використовуючи [7].

Нехай EUF–CMA–GAME(Gen, Sign, Ver, A, n), причому виконуються пункти 1 – 7.

1. Gen(1n) (sk, vk);

2. A отримує vk;

3. A створює повідомлення m;

4. A отримує s Sign(sk, m);

5. A повторює кроки 3 та 4, якщо це необхідно;

6. A виводить (m*, s*);

7. A виграє, якщо Ver(vk, m*, s*)=accept та m* не було раніше підписано Sign.

Тоді дійсним є визначення 1.

Визначення 1. Схема підпису є EUF-CMA безпечною, якщо для будь-якого зловмисника A, що виконується за поліноміальний час, ймовірність виграшу EUF-CMA-GAME є незначною.

3. Попередні дані та визначення

Як вже зазначалося і як буде показано далі, для цілей безпеки вкрай важливо допустити алгоритм підпису з відслідковуванням стану (stateful).

Це забезпечується на основі використання та врахування наступного:

- KDM – повідомлення, залежне від ключа;
- KD – залежність від ключа;
- KDS – підписи, залежні від ключів;

- EUF-CMA – екзистенційна непідроблюваність при атаці на основі адаптивно підібраних (вибраних) повідомлень;
- Aeuf – зловмисник (імовірнісний алгоритм поліноміального часу) при EUF-CMA
- Akds – зловмисник (імовірнісний алгоритм поліноміального часу) при KDS-CMA;
- Akd – зловмисник (імовірнісний алгоритм поліноміального часу) при KD-EUF;
  OS – оракул підпису при Aeuf.
- безпека розглядається в сенсі KDS-CMA означає безпеку в сенсі EUF-CMA;
- CMA – атака на основі адаптивно підібраних (вибраних) повідомлень.

Також використовується «пряма» секретність (forward security, forward secrecy), як властивість криптосистем зберігати конфіденційність минулих сеансових ключів при компрометації довгострокового ключа.

Також застосовується досконала пряма секретність (perfect forward secrecy (PFS)), яка означає, що сеансовий ключ, який генерується з використанням довгострокових ключів, не буде скомпрометований при умові, якщо один або декілька з цих довгострокових ключів будуть скомпрометовані у майбутньому.

Аналіз показав [6, 7], що моделі безпеки щодо підписів засновуються на принципах та понятті теорії ігор. Поняття теорії ігор може використовуватись у такому змісті.

Теорія ігор – це теорія математичних моделей прийняття оптимальних рішень в умовах конфлікту. Оскільки сторони, що беруть участь в більшості конфліктів, зацікавлені в тому, щоб приховати від супротивника власні наміри, прийняття рішень в умовах конфлікту, зазвичай, відбувається в умовах невизначеності. Фактор невизначеності можна інтерпретувати як противника суб'єкта, який приймає рішення. Логічною основою теорії ігор є формалізація трьох понять, які входять в її визначення і є фундаментальними для всієї теорії: конфлікт; приймання рішення у конфлікті; оптимальність прийнятого рішення.

4. Аналіз схем підписів та екзистенційна непідроблюваність

Подальший аналіз можна провести засобом використання визначень 2 та 3 із [7].

Визначення 2 [7] (Схема підпису). Схема підпису S є трійкою поліноміальних алгоритмів S=(K, S, V):

K − імовірнісний алгоритм генерації ключа, який при введенні параметру безпеки 1k повертає пару (sk, pk) ключів − відкритий ключ перевірки pk з відповідним секретним ключем підпису sk {0,1}*. У випадку підписувача з відслідковуванням стану (stateful) sk інтерпретуємо як початковий стан підписувача, тобто вся секретна інформація підписувача є частиною його стану;

S − імовірнісний алгоритм підпису, який при введенні повідомлення M {0,1}* та стану sk − який у випадку підписувача без стану (stateless) є лише секретним ключем − повертає підпис σ {0,1}* на M або символ помилки. Крім того, оновлюється стан значення sk;

V − це детерміністичний алгоритм перевірки, який при введенні відкритого ключа pk, повідомлення M та підпису кандидата σ для M повертає true або false, вказуючи, чи є σ дійсним підписом для M при відкритому ключі pk.

Далі, для пар ключа (sk, pk), що виводяться за допомогою K, вимагаємо, щоб із переважною ймовірністю мала місце очевидна умова правильності – для всіх повідомлень M маємо Vpk(M, Ssk(M))=true.

Стандартна вимога до безпеки для схем підписів – EUF-CMA, що означає екзистенційну непідроблюваність при атаці адаптивно підібраних повідомлень.

Визначення 3 [7]. (EUF-CMA). Нехай S=(K, S, V) буде схемою підпису, і Aeuf – імовірнісним алгоритмом, що виконується за поліноміальний час. Сценарій атаки буде такий:

1. Обчислити пару ключів (sk, pk) K(1k) та pk як вхідні дані Aeuf.

2. Зловмиснику Aeuf надається необмежений доступ до оракулу підпису OS для виконання Ssk( ).

3. Зрештою, Aeuf виводить повідомлення M та підпис σ.

Зауваження 1. Вищезгадане визначення безпеки EUF-CMA є дійсними одноразовими схемами підпису в очевидний спосіб – єдиною модифікацією є те, що Aeuf може запитувати оракул підпису OS лише один раз.

Зокрема, безпека в сенсі EUF-CMA не дозволяє зловмиснику отримувати підписи повідомлень, залежних від ключів, як підпис на повному секретному ключі (стані) sk. Фактично, враховуючи EUF-CMA-безпечну схему підпису, легко скласти схему підписів, яка все ще є EUF-CMA-безпечною, але один запит на повідомлення, залежного від ключів, порушує безпеку схеми.

5. Аналіз безпеки за наявності підписів, залежних від ключів

В ряді випадків схема підпису S=(K, S, V) називається KDS-CMA-безпечною, якщо вона є захищеною, незважаючи на здатність зловмисника отримувати підписи на довільних (таких, що ефективно обчислюються) функціях g стану sk підписувача. Зокрема, g має доступ до секретного ключа, що зберігається під час підписування.

Визначення 4 [7] (KDS-CMA). Нехай трійка S=(K, S, V) буде схемою підпису, і Akds – це імовірнісний алгоритм поліноміального часу. Нехай реалізується такий сценарій атаки:

1. Обчислити пару ключів (sk, pk) K(1k) та pk – як вхідні дані до Akds.

2. Зловмисник Akds отримує необмежений доступ до оракула підпису. Оракул приймає як вхідну функцію g, представлену як логічна схема поліноміального розміру, і виконує алгоритм підпису S із поточним станом sk і повідомлення g(sk) як вхідними даними (у моделі випадкового оракула g може викликати випадковий оракул).

3. Зрештою, Akds виводить повідомлення M {0,1}* і підпис σ.

Необхідно відмітити, що оцінка ефективності моделі безпеки KDS-CMA в сенсі KDS-CMA означає безпеку в сенсі EUF-CMA, і виникає питання, чи/як може бути досягнута безпека в сенсі *Визначення* 3.

6. Неможливість KDS-CMA з алгоритмом підпису без стану (stateless)

Як перший (негативний) результат необхідно відмітити, що жодна схема підпису з алгоритмом підписування без стану не може відповідати цілі безпеки KDS-CMA-безпечності.

Зауваження 2[7]. Нехай S=(K, S, V) буде схемою підпису з алгоритмом підписування без стану S, тобто секретний ключ підпису sk не змінюється шляхом виконання S. Тоді схема підпису S не є безпечною в сенсі KDS-CMA.

Незважаючи на свою простоту, атака в доказі зауваження 2[7] є досить руйнівною, і це може виявитися незрозумілим.

Як правило для моделі прямої безпеки розглядаються так звані схеми підпису з ключами, що розвиваються, та компрометація поточного секретного ключа не дозволяє зловмиснику підроблювати попередні підписи. Підписи для повідомлень, підписаних раніше при фіксованому відкритому ключі, дійсні, навіть, якщо поточний секретний ключ розкрито. Крім того, зловмисник не може підробити підпис з "датою" перед розголошенням ключа.

7. Схеми підпису з ключами, що розвиваються, та пряма безпека

Визначення 5. Схема підпису з ключем, що модифікується. Схема підпису з ключем, що «розвивається». Така схема Sf є кортежем з чотирьох елементів поліноміальних алгоритмів S=(Kf, Uf, Sf, Vf):

1. Kf – імовірнісний алгоритм генерації ключа, у якому при введенні параметра безпеки 1k, загальна кількість періодів часу T (і, можливо, інші параметри) повертає пару (sk0, pk) ключів – відкритий ключ перевірки pk з відповідним (базовим) секретним ключем підпису sk0.

2. Uf – детермінований алгоритм оновлення секретного ключа, який приймає в якості вхідних даних секретний ключ підпису sk_{j-1} попереднього періоду j−1 і повертає секретний ключ підпису sk_j для періоду j.

3. Sf – імовірнісний алгоритм підпису, у якого вхідними даними є повідомлення M {0, 1}* та секретний ключ підпису sk_j поточного періоду часу j повертає підпис для M для періоду j або повертає символ помилки.

4. Vf – це детермінований алгоритм перевірки, у якого вхідними даними є відкритий ключ pk, повідомлення M і підпис, повертає true або false, що вказує на те, що підпис прийнято або відхилено відповідно.

Можна припустити, що sk_j зберігає саме значення j для періоду j {1,...,T}, а також загальне число T періодів часу. Далі, приймається рішення про те, що skT+1 – це порожній рядок і, що Uf(skT) повертає skT+1. І поточний період часу j, і загальна кількість періодів T є загальновідомими та доступними для зловмисника Afwd разом із атакованим відкритим ключем pk. Фактична гра атаки, яка використовується для визначення прямої безпеки схеми підпису з ключем, що «розвивається», включає в себе три етапи – етап атаки підібраного повідомлення (cma), етап розриву (breakin) та етап підробки (forge).

Визначення 6 (FWD-CMA – пряма безпека). Нехай Sf=(Kf, Uf, Sf, Vf) – це схема підпису з ключем, що розвивається, і нехай Afwd – це імовірнісний поліноміальний алгоритм. Тоді важливим для рішення є сценарій.

1. CMA стадія

Встановити j←0, і згенерувати пару ключів (sk0, pk) Kf(1k,...,T). (Тут '...' вказує, що додаткові вхідні параметри можуть бути присутніми).

repeat
  j←j+1; skj←Uf(skj−1)
 (cma, pk)
until (d = breakin) or (j = T)
if d ≠ breakin and j = T
 then j = T + 1
end if

2. Breakin стадія

Зловмиснику Afwd передається поточний секретний ключ sk_j.

3. Forge стадія

Зрештою, Afwd виводить повідомлення M та підпис з b<j.

Нехай QueriedEarlier – це подія, що Afwd виводить повідомлення M, яке вже було запитано до оракула підпису.

Процес у *визначенні* 5 суворо упорядкований тим, що як тільки зловмисник відмовляється від оракула підпису для sk_j, він не може знову отримати доступ до цього оракула. У якийсь момент зловмисник Afwd вирішує скористатися своїм привілеєм розриву, і повертає поточний секретний ключ sk_j. Щоб бути успішним Afwd повинен підробити підпис з sk_b для деяких b<j і нового повідомлення M.

Зауваження 3 [7]. За визначенням безпечна схема FWD-CMA дозволяє зловмиснику Afwd подавати поліноміальну кількість запитів до його оракула підпису протягом одного часового періоду j. Таким чином, за наявності повідомлень залежних від ключів, атака, як показано в доказі *зауваження* 2, може розкрити повний секретний ключ, перед тим як з'явиться оновлення секретного ключа. Іншими словами, безпека у сенсі FWD-CMA не передбачає сильних гарантій безпеки при наявності повідомлень залежних від ключів.

На противагу вищезазначеному негативному твердженню після застосування деяких технічних модифікацій для отримання синтаксично правильної схеми підпису з ключем, що «розвивається», компілятор (який був розроблений для забезпечення безпеки KDS-CMA) може бути використаний для безпеки EUF-CMA одноразової схеми підпису S, включно до прямої безпеки схеми підпису з ключем, що розвивається, Sf.

Висновки

1. В результаті проведених досліджень визнано, що продуктивним може бути введення та використання узагальненої (комплексної) моделі криптографічної стійкості ЕП.

2. В якості складових узагальненої (комплексної) моделі криптографічної стійкості асиметричних криптоперетворень типу ЕП обґрунтовані та визначені такі часткові моделі:

- порушника щодо асиметричних криптоперетворень типу ЕП;
- загроз щодо асиметричних криптоперетворень типу ЕП;
- безпеки щодо асиметричних криптоперетворень типу ЕП.

3. Побудова моделі порушника необхідна для того, щоб розробити комплекс заходів із забезпечення захищеності механізмів ЕП, в тому числі з урахуванням вимог та умов їх застосування в постквантовий період. Така модель порушника може бути побудована з урахування різних критеріїв.

4. Порушники класифікуються за рівнем можливостей, що надаються їм штатними засобами КС, в тому числі для класичного та квантового криптоаналізу. Виділяються чотири рівні таких можливостей. Класифікація є ієрархічною – кожний наступний рівень включає в себе функціональні можливості попереднього рівня [5]. Прийнято, що щодо перспективного ЕП для постквантового періоду безпека повинна бути забезпечена в умовах протидії порушнику 4 рівня.

5. У найгіршому випадку безпека повинна бути забезпечена проти криптоаналітика 4-го рівня можливостей, він знає все про метод синтезу перспективного ЕП, криптографічні властивості методу ЕП, а також всі механізми безпеки, що виконуються під час синтезу та застосування. Виключенням є те, що криптоаналітик не знає особистого ключа чи відповідним чином обґрунтовану частину особистого ключа. У найкращому випадку порушник не знає нічого про системні параметри та ключі. У нашому випадку можливі варіанти є рівноймовірними.

6. Модель загроз щодо криптоперетворення ЕП повинна бути документом, яким закріплено найбільш повний перелік загроз щодо існуючих та перспективних ЕП. Відповідно до Законів України інформація у основних інформаційних ресурсах поділяється на відкриту і конфіденційну. Інформація у підтримуючих інформаційних ресурсах є технологічною інформацією.

7. При застосуванні ЕП, незалежно від видів додатків, використовуються асиметричні пари ключів, для кожної пари особистий та відкритий. В подальшому при реальному застосуванні ЕП відкритий ключ, як правило, є сертифікатом відкритого ключа та є доступним усім користувачам інфраструктури відкритого ключа.

8. Стосовно відкритого ключа ЕП повинна бути можливість забезпечення його цілісності, справжності, доступності, неспростовності та захист від несанкціонованих дій, які можуть привести до випадкової чи умисної модифікації, нав’язування хибного чи знищення.

9. Стосовно особистого ключа повинна забезпечуватись його цілісність, справжність, доступність, неспростовність та захист від несанкціонованих дій, а також його захист від несанкціонованого та неконтрольованого ознайомлення, модифікації, знищення, копіювання та поширення, тобто конфіденційність.

10. Перелік можливих загроз безпеці застосування існуючих та перспективних ЕП сформований з числа загроз, що визначені у IT-Grundschutz Catalogues Германії з урахуванням апаратних, програмних та апаратно-програмних ресурсів, технологій обробки даних та механізмів криптографічного захисту при застосуванні ЕП, в тому числі з урахуванням вимог та умов синтезу перспективних та застосуванні ЕП в постквантовий період.

11. Безумовно, що щодо обґрунтованої та вибраної на основі IT-Grundschutz Catalogues бази Германії моделі загроз, при синтезі та застосуванні існуючих стандартизованих та перспективних ЕП, повинне бути зроблено перекриття названих загроз з необхідною якістю. Для цього, у залежності від механізмів та засобів, що застосовуються для протидії, повинні бути розробленими відповідні нормативно-правові документи.

12. Детально загрози щодо застосування класичного криптоаналізу при синтезі та застосуванні ЕП розглянуті в [1 - 9]. Їх перекриття повинне бути зроблене на всіх етапах синтезу та застосування перспективних ЕП. Вказані загрози з точки зору застосування математичних

методів синтезу та застосування перспективних методів ЕП залежать від математичних методів, що застосовуються, та умов їх функціонування.

13. Загрози (атаки) сторонніми каналами є виділеним класом атак, основною особливістю яких є спрямованість на вразливості практичної реалізації криптосистем, тобто, на відміну від теоретичного криптоаналізу. Загрозою такого класу атак над традиційними є менша потужність та більш висока дієвість.

14. Загрози (атаки) сторонніми каналами є надзвичайно небезпечними, якщо їх не перекривати. Концепція цих атак існує доволі тривалий час, але реалізація захищеності від них вимагає знань не лише у сфері криптографії, а й у сферах технічного характеру. Тому переважна більшість перспективних ЕП розрахована на використання у пристроях, які не можуть захистити від сторонніх атак, бо не мають відповідних програмних рішень щодо захисту від витоку сторонніми каналами.

15. Основними загрозами (атаками) з застосуванням квантових математичних методів, які можуть бути реалізованими на квантовому комп'ютерові (звичайно, якщо він буде побудований), є такі: квантовий алгоритм факторизації Шора; квантовий алгоритм Гровера; квантовий алгоритм Шора вирішення дискретного логарифму в полі; квантовий алгоритм Шора вирішення дискретного логарифму в групі точок еліптичної кривої; квантовий алгоритм криптоаналізу для перетворень в фактор кільці.

16. У залежності від математичних методів, що застосовуються для синтезу та застосування ЕП, можуть застосовуватись різні методи, системи та засоби. Наприклад, для криптоперетворень на алгебраїчних решітках необхідно вирішувати проблему навчання з помилками (LWE).

17. Наразі в постквантовій криптології актуальними є завданнями забезпечення криптографічної стійкості щодо квантових атак.

18. Стосовно атак на LWE можливо виділити та необхідно розглядати наступні атаки (загрози): атаки грубої сили, тобто повного перебору; традиційні атаки зустріч посередині; атаки на основі алгоритму Arora-Ge; BKW, коли LWE зводиться до SIS атаки; Primal attack (Search-LWE зводиться до BDD атаки); Dual attack (Decision-LWE зводиться до SIS); зведення до uSVP атаки пошуку короткого вектора.

19. Для однозначного розуміння та використання пропонується ввести та використовувати нове поняття щодо моделі безпеки (криптографічної стійкості) стандартизованих криптографічних примітивів.

20. Модель безпеки (криптографічної стійкості) криптографічних примітивів (в тому числі типу ЕП) – це сукупність організаційно-технічних, програмно-технічних та логічних механізмів (методів) та заходів, законодавчих та нормативно-правових норм та правил, що визначають вимоги до методів синтезу, оцінки криптографічної стійкості та застосування стандартизованих криптографічних примітивів (типу ЕП), з урахуванням умов їх реалізації при інтенсивній протидії порушника 4-го рівня із застосування методів, систем та засобів класичного та квантового криптоаналізу.

21. Модель безпеки EUF-CMA визначає екзистенційну непідроблюваність від атак на основі адаптивно вибраних повідомлень [7]. Зокрема, безпека в сенсі EUF-CMA повинна протидіяти порушнику 4-го рівня виробляти ЕП для повідомлень, що залежать від ключів (застосуванні особистого sk ключа). По суті, при застосуванні механізму безпечного ЕП, згідно моделі EUF-CMA, вона є безпечною для EUF-CMA випадку.

22. Головна відмінність моделі SUF-CMA полягає в тому, що це більш сильне визначення гарантує, що атакуючий не зможе підібрати підпис. Так, схема, в якій атакуючий може повторно рандомізувати дійсний підпис, щоб він залишався дійсним, але виглядав інакше, ніж вихідне значення, не задовольнила би умові SUF-CMA.

23. В ряді випадків схема підпису S=(K, S, V) називається KDS-CMA-безпечною, якщо вона є захищеною, незважаючи на здатність зловмисника отримувати підписи на довільних

(таких, що ефективно обчислюються) функціях g стану sk підписувача. Зокрема, g має доступ до секретного ключа, що зберігається під час підписування.

24. Оцінка ефективності моделі безпеки KDS-CMA в сенсі KDS-CMA означає безпеку в сенсі EUF-CMA, і виникає питання, чи може бути досягнута за цих умов безпека.

25. Після застосування деяких технічних модифікацій для отримання синтаксично правильної схеми підпису з ключем, що «розвивається», компілятор може бути використаний для безпеки EUF-CMA одноразової схеми підпису S, включно до «прямої» безпеки схеми підпису з ключем, що розвивається, Sf.

Список літератури:

1. Lily Chen Report on Post-Quatum Cryptography. NISTIR 8105 (DRAFT) / Lili Chen, Stephen Jordan, Yi-Kai-Liu, Dustin Moody, Rene Peralta, Ray Perlner, Daniel Smith-Tone // Access mode: http://csrc.nist.gov/publications/drafts/nistir-8105/nistir_8105_draft.pdf.
2. Moody D. Post-Quntum Cryptography: NIST's Plan for the Future. The Seventh International Conference on Post-Quntum Cryptography [Електронний ресурс] // Moody. 2016. Режим доступу: https://pqcrypto2016.jp/data/pqc2016_nist_announcement.pdf.
3. ETSI GR QSC 001 V.1.1.1 (2016-07). Quantum-Safe Cryptography (QSC); Quantum-safe algorithmic framework. Режим доступу: https://www.etsi.org/deliver/etsi_gr/QSC/001_099/001/01.01.01_60/gr_QSC001v010101p.pdf.
4. ETSI Quantum safe cryptography and security // White Paper №8, 2015. Режим доступу: https://www.etsi.org/images/files/ETSIWhitePapers/QuantumSafeWhitepaper.pdf.
5. NIST. Post-Quantum Cryptography Standardization. National Institute of Standards and Technology Internal, Report 8105 [Електронний ресурс] // NIST Режим доступу: https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Post-Quantum-Cryptography-Standardization.
6. Gorbenko I., Ponomar V. Examining a possibility to use and the benefits of post-quantum algorithms dependent on the conditions of their application // Eastern-European Journal of Enterprise Technologies. 2017. Vol. 2 NO 9 (86). P.21–32. Available at: http://journals.uran.ua/
7. EUF-CMA and SUF-CMA. [Електронний ресурс]. Режим доступу: https://blog.cryptographyengineering.com/euf-cma-and-suf-cma/.
8. Горбенко І. Д., Кузнєцов О. О., Олійников Р. В., Горбенко Ю. І., Ганзя Р. С., Пономар В. А. Аналіз проблем криптографічного захисту інформації у постквантовий період та можливі шляхи їх вирішення // V Міжнар. Наук.-техн. конф. "Захист інформації і безпека інформаційних систем" : Праці Наук.-техн. конф., 02–03 червня 2016 р. Львів : Нац. ун-т "Львівська політехніка", 2016. С. 110-111.
9. Горбенко Ю.І. Методи побудування та аналізу, стандартизація та застосування криптографічних систем ; за заг. ред.. І.Д. Горбенка. Харків : Форт, 2015. 959 с.
10. IT-Grundschutz Catalogues. [Електронний ресурс]. Режим доступу: https://www.bsi.bund.de/EN/Topics/ITGrundschutz/ITGrundschutzCatalogues/itgrundschutzcatalogues_node.html.

Надійшла до редколегії 07.08.2020

Відомості про авторів:

Горбенко Юрій Іванович – канд. техн. наук, АТ «Інститут інформаційних технологій», перший заступник головного конструктора, Україна, e-mail: gorbenkou@iit.kharkov.ua, ORCID: https://orcid.org/0000-0003-0073-9107

Потій Олександр Володимирович – д-р техн. наук., професор, заступник Голови Державної служби спеціального зв'язку та захисту інформації України, e-mail: potav@ua.fm, ORCID: https://orcid.org/0000-0002-2366-0541

Онопрієнко Віктор Васильович – канд. техн. наук, генеральний директор АТ «Інститут інформаційних технологій», Україна.

Єсіна Марина Віталіївна – канд. техн. наук, Харківський національний університет імені В. Н. Каразіна, доцент кафедри безпеки інформаційних систем і технологій, факультет комп'ютерних наук, Україна, e-mail: rinayes20@gmail.com, ORCID: https://orcid.org/0000-0002-1252-7606

Малєєва Ганна Андріївна – Харківський національний університет радіоелектроніки, аспірант кафедри безпеки інформаційних технологій, Україна, e-mail: hanna.malieieva@nure.ua