УДК 004.056.5 **DOI:10.30837/rt.2022.4.211.01**

Є.В. ОСТРЯНСЬКА, С.О. КАНДІЙ, І.Д. ГОРБЕНКО, д-р техн. наук,
М.В. ЄСІНА, канд. техн. наук

КЛАСИФІКАЦІЯ ТА АНАЛІЗ ВРАЗЛИВОСТЕЙ СУЧАСНИХ ІНФОРМАЦІЙНИХ СИСТЕМ ВІД КЛАСИЧНИХ ТА КВАНТОВИХ АТАК

Вступ

Завдяки останнім досягненням у квантових технологіях та потенціалу того, що практичні квантові комп'ютери можуть стати реальністю у майбутньому, відновився інтерес до розробки криптографічних технологій, захищених від звичайних та квантових атак. Наразі практично всім асиметричним криптографічним схемам, які сьогодні використовуються, загрожує потенційна розробка потужних квантових комп'ютерів. Постквантова криптографія є одним із способів боротьби із цією загрозою. Її безпека базується на складності математичних проблем, які наразі вважаються нерозв'язними ефективно – навіть за допомогою квантових комп'ютерів.

Безпека інформаційних систем забезпечується через захист від різноманітних загроз, що використовують вразливості системи. Загроза – це потенційне порушення безпеки, тоді як атака – це погроза, яка виконується. Процеси безпеки стосуються вибору та реалізації засобів контролю безпеки (так звані контрзаходи), які допомагають зменшити ризик, спричинений вразливостями.

Протоколи безпеки є будівельними блоками безпечного зв'язку. Вони реалізують механізми безпеки для надання послуг безпеки. Протоколи безпеки вважаються абстрактними під час аналізу, але вони можуть мати додаткові вразливості у реалізації. Ця робота містить цілісне дослідження протоколів безпеки. Розглядаються основи протоколів безпеки, таксономія атак на протоколи безпеки та їх впровадження, а також різні методи та моделі аналізу безпеки протоколів. Зокрема, уточнюються відмінності між інформаційно-теоретичною та обчислювальною безпекою, обчислювальними та символьними моделями. Крім того, надано огляд моделей обчислювальної безпеки для автентифікованого обміну ключами (AKE) і протоколів обміну ключами з автентифікацією пароля (PAKE).

Також було описано найважливіші моделі безпеки для протоколів AKE і PAKE. З появою нових технологій, які можуть мати інші вимоги до безпеки, а також завдяки збільшеним можливостям змагальності, завжди виникає потреба в розробці нових протоколів.

Для майбутнього використання постквантової криптографії недостатньо стандартизувати криптографічні алгоритми. Швидше, необхідно також адаптувати криптографічні протоколи до нових алгоритмів. Це пов'язано, наприклад, з тим, що в багатьох протоколах дозволена довжина відкритих ключів обмежена і більше недостатня для нових алгоритмів. Однак істотним моментом є те, що постквантові алгоритми, як правило, не слід використовувати окремо, а лише в гібридному режимі, тобто в поєднанні з класичною процедурою. Зміни в протоколах і стандартах повинні бути ініційовані та спільно розроблені галуззю. Ця робота вже триває для багатьох протоколів.

Метою статті є огляд, класифікація, аналіз та дослідження вразливостей інформаційних систем від класичних, квантових та спеціальних атак, виконані з урахуванням прогнозу щодо можливостей здійснення атак на постквантові криптографічні перетворення; вивчення моделей для оцінки безпеки для існуючих криптографічних протоколів, а також огляд та по-

рівняльний аналіз моделей безпеки та надання пропозицій щодо захисту від існуючих потенційних атак.

1. Попередні визначення квантово-безпечної криптографії

В останні роки спостерігається стійкий прогрес у створенні квантових комп'ютерів. У разі реалізації великомасштабних квантових комп'ютерів вони будуть загрожувати безпеці багатьох широко використовуваних криптосистем з відкритим ключем. Щоб протистояти загрозі сучасної асиметричної криптографії з боку квантових комп'ютерів, виникла нова галузь криптографічних досліджень – постквантова криптографія.

Постквантова криптографія займається розробкою та дослідженням асиметричних криптосистем, які, згідно із сучасними знаннями, не можуть бути зламані навіть потужними квантовими комп'ютерами. Тобто квантово-стійка криптографія – це криптографія, яка спрямована на надання криптографічних функцій і протоколів, які залишаються безпечними, навіть, якщо створено великомасштабні відмовостійкі квантові комп'ютери [1]. Ці методи базуються на математичних задачах, для розв'язання яких на сьогодні невідомі ані ефективні класичні алгоритми, ані ефективні квантові алгоритми. У сучасних дослідженнях застосовуються різні підходи до реалізації постквантової криптографії. До них належать, серед іншого:

- Криптографія на основі кодів: безпека схем на основі кодів ґрунтується на труднощах ефективного декодування загальних кодів з виправленням помилок.
- Криптографія на основі решітки: безпека схем на основі решітки базується на складності вирішення певних обчислювальних проблем на математичних решітках.
- Криптографія на основі гешування: безпека схем підпису на основі гешування базується на властивостях безпеки використаної геш-функції.
- Криптографія на основі ізогенії: схеми на основі ізогенії базують свою безпеку на тому факті, що важко знайти ізогенію між двома суперсингулярними еліптичними кривими, якщо така існує.
- Багатовимірна криптографія: безпека багатовимірної криптографії базується на припущенні, що багатовимірні поліноміальні системи рівнянь над скінченними полями важко вирішити.

Далі будуть розглянуті лише перші три класи, оскільки постквантові схеми, рекомендовані BSI, а також ті, що пройшли до фіналу конкурсу NIST та будуть стандартизовані, належать до цих класів. Багатоваріантні схеми мають довгу історію атак і виправлень. Криптографія, заснована на ізогеніях (відображення між еліптичними кривими зі спеціальними властивостями), є цікавою темою дослідження, яку, на думку BSI, слід вивчити далі, перш ніж розглядати рекомендацію.

Реалізація загроз, що спрямовані на програмні ресурси, може призводити до порушення вимог безпеки первинних інформаційних ресурсів, вплинути на інше ПЗ та, в окремих випадках, на функціонування апаратних ресурсів. А також порушити цілісність, справжність, доступність, неспростовність даних, що мають бути захищеними від несанкціонованих дій, які можуть привести до випадкової або умисної модифікації чи знищення. Саме тому у розд. 2 буде розглянуто основні атаки на постквантові криптографічні алгоритми.

2. Класифікація та аналіз основних атак на постквантові криптографічні перетворення

У цьому розділі коротко розглянуті деякі атаки на протоколи, схеми шифрування та їх реалізації.

Загрози в інформаційній безпеці можна розділити на чотири великі класи: розкриття або несанкціонований доступ до інформації; обман або прийняття неправдивих даних; порушення, переривання або запобігання коректній роботі; узурпація або несанкціонований контроль деякої частини системи [2]. Атаки також можна розділити на пасивні та активні [3].

Прослуховування є різновидом розкриття та несанкціонованого перехоплення інформації. Це пасивна атака, яка може бути або видаленням вмісту повідомлення, аналізом трафіку або переглядом файлів чи системної інформації. Маскування або підробка має місце, коли сутність видає себе за іншу сутність. Це можна вважати як вид обману та узурпації.

Несанкціонована зміна інформації є активною атакою, яка може бути обманом, або зривом і узурпацією. Затримка і відмова в обслуговуванні (DoS) є тимчасовими і довгостроковими гальмуваннями послуги відповідно. Хоча їх і можна вважати узурпацією, вони можуть грати допоміжну роль в обмані. Вони можуть бути результатом прямих атак або інших проблем, які не стосуються безпеки.

Під атаками впровадження маємо на увазі атаки, які використовують інформацію, яка отримана через витік через криптографічний примітив або його конкретне використання в протоколі безпеки. Наприклад, вимірювання споживання енергії або часу, необхідного для шифрування того самого повідомлення з різними секретними ключами може надати певну інформацію про секретні ключі.

2.1. Атаки на протоколи

Атака на протокол визначається та виконується відповідно до цілей безпеки або вимог безпеки протоколу, або моделі безпеки, в якій безпека протоколу доведена. Атака відбувається, коли порушується будь-яка властивість протоколу. Як зазначається в [42] атаки на протоколи безпеки можна в цілому розділити на пасивні та активні атаки. Також можна класифікувати атаки на протоколи безпеки на основі їх недоліків експлуатації [4].

У цьому розділі представлено неповний список стандартних атак на протоколи [5 – 8]. Це найпоширеніші типи атак, засновані на практичних сценаріях, завдяки чому зловмисник може спричинити збій протоколу. Список неповний, тому що в теорії є необмежені способи взаємодії криптоаналітика з одним або кількома (наприклад, паралельними) протоколами. Наведений нижче список не включає атаки, засновані на недоліках апаратного забезпечення або реалізації програмного забезпечення. Отже, найпоширенішими атаками на протоколи є:

- Атака з уособленням: це активна атака, спрямована на порушення автентичності. У цій атаці криптоаналітик намагається видати себе за одну або більше сутностей. Відповідно до змагальної моделі у відповідній моделі безпеки атака з уособленням може мати слабші варіанти обміну автентифікованими ключами (AKE) або протоколи обміну ключами з автентифікацією на основі пароля (PAKE), які будуть розглянуті у розд. 3. Ключова атака з уособленням компромісу (KCI) і атака з уособленням компрометації тимчасового ключа є слабшими варіантами атаки з уособленням у протоколах AKE, які потребують знання статичного секретного ключа та тимчасового секретного ключа (випадкове число) відповідно. Мета в таких варіантах – видати себе за іншу особу або іншу сутність скомпрометованій сутності [9].
- Атака «Людина посередині» (MITM): це варіант атаки з уособленням, де криптоаналітик знаходиться між двома сутностями та переконливо видає себе за обидві жертви. Практичні приклади включають атаку MITM на стільниковий зв'язок GSM мережі [10], протокол HTTPS [11] і EMV (Europay, MasterCard і Visa) протокол [12]. MITM можливий, коли протоколу бракує (взаємної) автентифікації.
- Атака зі спільним використанням невідомого ключа (UKS): це варіант атаки уособлення в протоколах AKE. Під час атаки UKS дві сутності мають спільний ключ сеансу, але вони мають різні представлення сеансу [13]. Атака UKS можлива коли протокол обміну ключами не може забезпечити автентифіковане зв’язування між сеансовим ключем та ідентифікаторами чесних об’єктів. Як правило, є два типи атак UKS [14, 15]: у першому типі, який називається Public UKS, атака замінює ключ, зловмисник реєструє відкритий ключ іншої сутності як власний відкритий ключ. У атаці UKS другого типу криптоаналітик має дійсний публічно-секретний ключ, сертифікований центром сертифікації, і намагається здійснити атаку UKS.

- Атака повтору: це активна атака, під час якої криптоаналітик втручається в запуск протоколу шляхом вставки деяких повідомлень із попередніх запусків протоколу або паралельно сесії. Це можна розглядати як комбінацію атак прослуховування та модифікації. Протокол вразливий до атаки відтворення, якщо він не забезпечує свіжість (freshness). Актуальність можна забезпечити за допомогою часових позначок, одноразових номерів або маркерів сеансу, а також лічильники [16].
- Атака Preplay: під час атаки Preplay супротивник готується до атаки шляхом імітації виконання протоколу та виконання набору операцій. Криптоаналітик виконує справжню атаку пізніше, коли є ймовірність здійснити той самий ряд операцій, що й у симуляції. Атака Preplay можлива, коли передбачуваний виклик у протоколах є виклик-відповідь [16, 17].
- Атака на відмову в обслуговуванні (DoS): DoS-атаки відносяться до широкого класу атак, які направлені на порушення доступності систем [18]. З точки зору протоколів, вони відносяться до атак, у яких зловмисник перешкоджає законним особам завершити протокол. На практиці вони можуть відбуватися проти серверів, які взаємодіють з багатьма клієнтами. Зловмисник може використати обчислювальні ресурси передбачуваного сервера (атака виснаження ресурсу) або перевищити кількість дозволених підключень до сервера (атака з розривом з'єднання). Неможливо повністю запобігти DoS-атакам, але можна зменшити їх вплив. Протоколи, які відкладають автентифікацію до кінця протоколу, набагато більш уразливі до атак DoS, ніж протоколи, які забезпечують автентифікацію на ранніх етапах.
- Атаки на дефекти: у атаках на дефекти зловмисник використовує відсутність належної перевірки типу повідомлення. Зловмисник надсилає повідомлення іншого типу, ніж очікується. Об'єкт-жертва не може виявити невідповідність типу та неправильно інтерпретує вміст повідомлення або поводиться неочікувано. Заходи протидії до атаки дефектів полягають у зміні порядку елементів повідомлення в наступному використанні одного й того самого повідомлення та гарантуванні того, що кожен ключ шифрування використовується один раз.
- Криптоаналіз: у протоколах безпеки криптографічні примітиви вважаються абстрактними та захищеними від атак. Однак є виняток, коли відомо, що ключ слабкий. Ці ситуації не повинні розкривати верифікатори або докази, які можуть бути використані для розкриття ключа. Важливо, щоб протоколи PAKE протистояли таким атакам:
  - офлайн-атака за словником: під час атаки за словником в автономному режимі, яка є пасивною, зловмисник підслуховує зв'язок між двома чесними об'єктами та отримує верифікатор, який можна використовувати для вилучення пароля за допомогою словника найбільш імовірних паролів. Зловмисник застосовує кожен пароль зі словника до отриманого верифікатора, поки не знайде правильний пароль, який задовольняє рівнянню верифікатора;
  - онлайн-атака за словником: під час онлайн-атаки за словником зловмисник використовує словник найбільш вірогідних паролів, але отримує верифікатор через онлайн-взаємодію з цільовою сутністю. Як контрзахід сервери зазвичай блокують обліковий запис користувача після кількох невдалих спроб.
- Атака за вибраним протоколом: під час атаки за вибраним протоколом новий протокол призначений для взаємодії з існуючим протоколом і створення вразливості. Ця атака заснована на сценарії взаємодії протоколу, де ключ використовується для кількох програм, наприклад, смарт-карти.
- Внутрішні недоліки дій: група атак заснована на відсутності деяких операцій, які є вирішальними для гарантування властивості безпеки. Прикладом є відсутність перевірки повідомлення, отриманого на третій фазі протоколу трьох проходів [19].

2.2. Атаки на алгоритми шифрування

Наївний спосіб атакувати схему шифрування полягає в атаці грубої сили або вичерпному пошуку ключа, коли зловмисник пробує всі можливі ключі в просторі ключів на парі

відкритий текст-шифртекст, доки не знайде ключ. Метою зловмисника є систематичне відновлення відкритого тексту із зашифрованого тексту або виведення ключа [5]. За класифікацією з [42] атаки на схеми шифрування можна розділити на наступні моделі атак:

- Під час атаки лише зашифрованим текстом криптоаналітик має лише зашифрований текст. Схема шифрування є абсолютно небезпечною, якщо вона вразлива до цієї атаки.
- Під час атаки з відомим відкритим текстом криптоаналітик також має певну кількість відкритого тексту та відповідного зашифрованого тексту.
- У атаці обраного відкритого тексту (CPA) криптоаналітик вибирає відкритий текст, а потім отримує відповідний зашифрований текст. Зловмисник використовує виведену інформацію, щоб відновити відповідний відкритий текст зашифрованого тексту, який раніше не бачив. Схеми шифрування з відкритим ключем є прикладом, коли зловмисник може зашифрувати будь-яке повідомлення за своїм вибором під відкритим ключем жертви. Адаптивна атака обраного відкритого тексту (CPA2) – це атака CPA, у якій вибір відкритого тексту зловмисником може залежати від зашифрованого тексту, створеного під час попередніх зашифрувань.
- Під час атаки за допомогою обраного зашифрованого тексту (CCA) зловмисник може розшифрувати довільні зашифровані тексти, наприклад за допомогою доступу до обладнання для розшифрування з надійно вбудованим ключем розшифрування. Мета полягає в тому, щоб вивести відкритий текст із раніше невидимого зашифрованого тексту. CCA має два спеціальні варіанти: у неадаптивній атаці зашифрованого тексту (CCA1) [20] зловмисник може мати доступ до системи лише протягом обмеженого часу або обмеженої кількості пар відкритий текст-зашифрований текст. Атаку називають неадаптивною, оскільки зловмисник не може адаптувати свої запити до оракула дешифрування відповідно до зашифрованого тексту виклику. В адаптивній атаці обраного зашифрованого тексту (CCA2) [21], яка є сильнішою, ніж CCA1, зловмисник має доступ до оракула розшифрування навіть після отримання виклику зашифрованого тексту.

Більшість із наведених атак можуть стосуватися до схем цифрового підпису та кодів автентифікації повідомлень (MAC), де метою зловмисника є підробка повідомлень або MAC. На основі наведених вище моделей атак у літературі представлено різні методи криптоаналізу. Найбільш широко використовуваними методами для криптоаналізу схем шифрування з симетричним ключем є диференціальний криптоаналіз [22, 23], лінійний криптоаналіз [24] і алгебраїчний криптоаналіз [25]. Інші методи включають комбіновані атаки [26], атаку «зустріч посередині» [27], інтегральний криптоаналіз [28], атаку з пов’язаним ключем [29] і атаку за визначенням [30].

Схеми шифрування з асиметричним ключем побудовані на нерозв'язності деяких складних проблем. Складні задачі, які використовуються в криптографії з відкритим ключем, включають факторизацію цілих чисел, задачу дискретного логарифмування (DLP) у відповідних групах, таких як мультиплікативні групи скінченних полів або адитивні групи еліптичних кривих над скінченними полями, задачі про рюкзак і задачі решітки, проблеми кодування та багатовимірні поліноміальні рівняння над малими кінцевими полями. Для схем шифрування було введено кілька понять безпеки, а саме:

- Нерозрізнюваність (IND), яка формалізує нездатність зловмисника дізнатися будь-яку інформацію про відкритий текст, що лежить в основі зашифрованого тексту виклику.
- Неподатливість (NM), яка формалізує нездатність супротивника перетворити даний зашифрований текст на інший зашифрований текст, щоб їхні відповідні відкриті тексти були «значуще пов’язані».
- Розпізнавання відкритого тексту [31, 32], яке формалізує нездатність криптоаналітика створити зашифрований текст, не знаючи базових повідомлень.

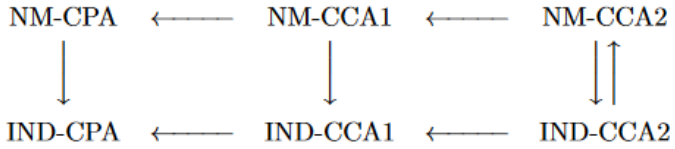

Рис. 1. Зв'язки між поняттями безпеки для схем шифрування з відкритим ключем [42]

Нерозрізнення є важливою властивістю для збереження конфіденційності. Однак у деяких випадках це може означати інші властивості безпеки, такі як цілісність, яка так чи інакше пов'язана з неподатливістю. На рис. 1 зображено співвідношення між поняттями нерозрізнення та неподатливості для схем шифрування з відкритим ключем під час атак CPA, CCA1 та CCA2 [31]. Стрілки позначають наслідки. Наприклад, якщо схема шифрування безпечна NM-CCA2, вона також безпечна NM-CCA1. Однак, якщо схема шифрування захищена NM-CCA1, вона може бути зламана в сенсі NM-CCA2. IND-CCA2 передбачає всі інші поняття. Поняття {IND-CPA, IND-CCA1, IND-CCA2} і {NM-CPA, NM-CCA1, NM-CCA2} можна визначити наступним чином (визначення 1 та визначення 2).

В и з н а ч е н н я 1. IND-CPA, IND-CCA1, IND-CCA2. Нехай $\Pi = (Gen, Enc, Dec)$ позначає схему шифрування з відкритим ключем, а $A = (A_1, A_2)$ позначає криптоаналітика з двома підалгоритмами. Для атаки $atk \in \{cpa, cca1, cca2\}$ і параметра безпеки $n \in \mathbb{N}$ ймовірність успіху криптоаналітика визначається як

$$Adv_{A,\Pi}^{ind-atk}(n) = \Pr\left[Exp_{A,\Pi}^{ind-atk-1}(n) = 1\right] - \Pr\left[Exp_{A,\Pi}^{ind-atk-0}(n) = 1\right], \quad (1)$$

для $b \in \{0,1\}$. Експеримент $Exp_{A,\Pi}^{ind-atk-b}(n) = b'$ визначається як

$$\begin{array}{ccc} (pk, sk) & \leftarrow & Gen(1^n) \\ (m_0, m_1, s) & \rightarrow & Gen(1^n) \\ b & \in_R & \{0,1\} \\ c & \leftarrow & Enc_{pk}(m_b) \\ b' & \leftarrow & A_2^{O_2}(m_0, m_1, s, c) \\ \text{Повернути} & b' & \end{array},$$

де

$$atk = cpa \Rightarrow O_1(\cdot) = \varepsilon, O_2(\cdot) = \varepsilon,$$
$$atk = cca1 \Rightarrow O_1(\cdot) = O_{Dec}(\cdot), O_2(\cdot) = \varepsilon,$$
$$atk = cca2 \Rightarrow O_1(\cdot) = O_{Dec}(\cdot), O_2(\cdot) = O_{Dec}(\cdot).$$

Схема шифрування безпечна в сенсі IND-ATK, якщо $Adv_{A,\Pi}^{ind-atk}(\cdot)$ є незначним у n [31].

В и з н а ч е н н я 2. NM-CPA, NM-CCA1, NM-CCA2. Нехай $\Pi = (Gen, Enc, Dec)$ позначає схему шифрування з відкритим ключем, а $A = (A_1, A_2)$ позначає криптоаналітика з двома підалгоритмами. Для атаки $akt \in \{cpa, cca1, cca2\}$ і параметра безпеки $n \in \mathbb{N}$ ймовірність успіху криптоаналітика визначається як

$$Adv_{A,\Pi}^{nm-atk}(n) = \Pr\left[Exp_{A,\Pi}^{nm-atk-1}(n) = 1\right] - \Pr\left[Exp_{A,\Pi}^{nm-atk-0}(n) = 1\right], \quad (2)$$

у якому для $b \in \{0,1\}$ експеримент $Exp_{A,\Pi}^{nm-atk-b}(n) = b'$ визначається як

$$
\begin{array}{ccc}
(pk, sk) & \leftarrow & Gen(1^n) \\
(m_0, m_1, s) & \leftarrow & A_1^{O_1}(pk) \\
c & \leftarrow & Enc_{pk}(m_1) \\
(R, c') & \leftarrow & A_2^{O_2}(m_0, m_1, s, c) \\
m' & \leftarrow & Dec_{sk}(c') \\
c \notin c' \wedge \perp \notin m' \wedge R(m_b, m') & \text{Тоді} & b' \leftarrow 1 \\
\text{Інакше} & & b' \leftarrow 1 \\
\text{Повернути} & b' &
\end{array},
$$

де m і c позначають вектори відкритих і зашифрованих текстів, $\perp$ позначає результат дешифрування, $R(\cdot)$ представляє поняття «значуще пов'язаних» і

$$
\begin{array}{l}
atk = cpa \Rightarrow O_1(\cdot) = \varepsilon, O_2(\cdot) = \varepsilon \\
atk = cca1 \Rightarrow O_1(\cdot) = O_{Dec}(\cdot), O_2(\cdot) = \varepsilon \\
atk = cca2 \Rightarrow O_1(\cdot) = O_{Dec}(\cdot), O_2(\cdot) = O_{Dec}(\cdot)
\end{array}.
$$

Схема шифрування безпечна в сенсі NM-ATK, якщо $Adv_{A,\Pi}^{nm-atk}(\cdot)$ є незначним у n [31].

Уявлення про безпеку в схемах шифрування з симетричним ключем також можна моделювати як ігри з криптоаналітиком [33].

2.3. Атаки на реалізацію

Криптографічні примітиви та протоколи зазвичай вважаються абстрактними, коли вони розроблені. Ця математична абстракція є корисною для дослідження, але вона не охоплює всього сценарію, який може статися на практиці. Криптографічні алгоритми завжди реалізуються в програмному або апаратному забезпеченні фізичних пристроїв, на які впливає середовище. Зловмиснику може не знадобитися безпосередньо брати на себе обчислювальну складність зламу алгоритмів, щоб отримати відкритий текст або ключ. Інформація, отримана під час спостереження за обчисленнями або комунікацією конкретної реалізації, може дуже допомогти в криптоаналізі та може значно зменшити обчислювальну складність зламу криптосистеми. Далі коротко розглянемо деякі атаки на впровадження криптосистем.

Атаки з бічного каналу недорогі, реалістичні та зазвичай вважаються найнебезпечнішим типом фізичних атак. Обчислювальні пристрої пропускають інформацію не лише через взаємодію вводу-виводу, а й через фізичні характеристики обчислень, такі як енергоспоживання, час або електромагнітне випромінювання. Такий витік інформації може зламати багато криптосистем, які зазвичай використовуються. Атаки з бічного каналу можна розділити на пасивні та активні. У пасивних атаках по бічному каналу зловмисник не втручається в роботу цільової системи; в той час як під час активних атак бічним каналом (або атак через помилки) криптоаналітик має певний вплив на поведінку цільової системи. Атаки бічних каналів також можна класифікувати як інвазивні, неінвазивні та напівінвазивні. Інвазивні атаки вимагають розпакування, щоб отримати прямий доступ до внутрішніх компонентів пристрою. Неінвазивні атаки використовують лише зовнішню інформацію. Напівінвазивні атаки включають доступ до пристрою без пошкодження шару пасивації або електричного контакту з несанкціонованою поверхнею. Нижче наведено неповний список [42] атак бічними каналами. Таким чином, відомі атаки з бічних каналів включають такі:

- Атака за часом: під час атаки за часом деяка інформація про ключ або секретний параметр виводиться з часу роботи криптографічного алгоритму або пристрою. Тобто, атаки за часом використовують різницю в часі, необхідну пристрою для виконання конкретних операцій, наприклад, непостійний час для виконання двох різних інструкцій.

- Атака з аналізом потужності: в атаках з аналізом потужності цінну інформацію про операції або параметри отримують шляхом спостереження за енергоспоживанням криптографічного пристрою або модуля. Тобто, вони використовують той факт, що електронні пристрої споживають електроенергію під час роботи. Атаки з аналізом потужності можна розділити на простий аналіз потужності (SPA), де вимірювання енергоспоживання безпосередньо інтерпретуються, і диференціальний аналіз потужності (DPA), де статистичні функції застосовуються до вимірювань енергоспоживання.
- Атака електромагнітного аналізу: під час атаки електромагнітного аналізу певна інформація отримується шляхом вимірювання електромагнітних полів, що випромінюються пристроєм.
- Акустичний криптоаналіз: акустичні випромінювання можна розглядати як джерело інформації для атак бічними каналами. Приклади включають вилучення 4096-бітних ключів RSA з програмного забезпечення GnuPG за допомогою звуку, створеного комп'ютером під час розшифрування деяких вибраних зашифрованих текстів, або розпізнавання натиснутої клавіші за допомогою акустичного випромінювання клавіатури.
- Атаки на пам'ять: інформація бічного каналу з геш-значення процесора і DRAM може бути використано для криптоаналізу програмно реалізованих шифрів. Геш-значення центрального процесора знаходиться між процесором і основною пам'яттю, щоб прискорити час роботи. Атаки на основі геш-значення використовують вимірювання затримки, викликаної промахом гешу, який виникає, коли ЦП отримує доступ до даних, які не зберігалися в геш-значенні, і використовується для криптоаналізу шифрів, включаючи DES і AES [34].
- Атаки з ін'єкцією помилки: атаки з ін'єкцією помилки є активним аналогом атак із бічного каналу, коли зловмисник отримує інформацію про внутрішні стани алгоритму, провокуючи помилки в обчисленнях і порівнюючи правильний і помилковий результат. Збій може бути постійним, що незворотно пошкоджує криптографічний пристрій, або він може бути тимчасовим. Несправність може бути викликана зміною напруги, тактової частоти чи температури, або використанням світла, рентгенівського та мікрохвильового випромінювання, або вихрових струмів, викликаних магнітними полями тощо.

Пропоновані заходи протидії атакам із бічного каналу включають спеціальні рішення щодо впровадження, які пропонують лише часткове вирішення проблеми, і теоретичні рішення, які формально вирішують проблему. Стійка до витоків криптографія є активною областю досліджень, яка стосується обчислень за наявності витоку інформації та розглядає математичні рішення для вирішення атак бічними каналами. Стійка до витоків криптосистема залишається безпечною, навіть, якщо довільна, але обмежена інформація про секретний ключ і, можливо, інша інформація про внутрішній стан, потрапляє до зловмисника.

3. Моделі безпеки для криптографічних протоколів

Дійсні атаки на протоколи визначаються за допомогою моделей безпеки, а докази безпеки надають міркування щодо їх надання, часто шляхом зведення до передбачуваної складної проблеми. Важкі проблеми в більшості популярних криптографічних протоколів і примітивів відкритого ключа – це теоретико-числові проблеми, такі як проблема дискретного логарифмування та розкладання на множники, які неможливо здійснити цифровими комп'ютерами, але які можуть бути здійснені за допомогою квантового комп'ютера. При виборі параметрів безпеки для криптосистем необхідно розуміти та оцінювати вартість найвідоміших атак. Розробка захищених протоколів, які забезпечують певні бажані функції або служби безпеки для різних програм, є основною частиною сучасної криптографії.

Багато криптографічних протоколів можна сформулювати як багатостороннє обчислення (MPC). Наприклад, у протоколах обміну ключами кожен принципал має деякі секретні значення та хоче безпечно обчислити ключ сеансу без шкоди для секретних значень. У безпечному MPC набір із m сторін, кожна з яких має секретне значення x_i, хоче обчислити

спільну функцію $f(x_1,...,x_m)$, не розкриваючи жодної інформації про x_i. Правильність обчислень і конфіденційність вхідних даних є двома важливими цілями для безпечного МРС.

Поняття безпеки були визначені для протоколів МРС як в обчислювальній, так і в інформаційно-теоретичній безпеці [35].

Ідеальна модель для протоколів МРС складається з довіреної сторони, яка приватно отримує вхідні дані від учасників і обчислює для них функцію f. У реальній моделі учасники обчислюють f без довіреної сторони. Протокол вважається безпечним, якщо реальні параметри емулюють ідеальні параметри, тобто все, що криптоаналітик може отримати в реальних налаштуваннях, також можна отримати в ідеальних налаштуваннях. Хоча моделі безпеки, розроблені для загальних протоколів, будуть використовуватися для будь-якого криптографічного протоколу, простіше та ефективніше працювати з моделями безпеки, які спеціально розроблені для певного типу протоколу. Найбільш спеціалізовані та добре розроблені моделі захисту для аналізу криптографічних протоколів у обчислювальних налаштуваннях присвячені протоколам AKE та PAKE, які будуть розглянуті далі.

3.1. Моделі безпеки для AKE протоколів

Протоколи AKE є найбільш добре вивченим типом протоколів безпеки. У 1976 р. Діффі та Геллман [36] представили протокол узгодження ключів, який є вразливим до атак MITM через відсутність автентифікації.

Протоколи AKE повинні забезпечувати певні атрибути безпеки, і вони повинні протистояти добре відомим атакам, представленим у підрозд. 2.1. Актуальність є важливим атрибутом у протоколах обміну ключами. Встановлений ключ має бути новим, а не повторним з попередніх сеансів. Актуальність може бути забезпечена за допомогою часових позначок, nonces або лічильників [16]. Спираючись на роботу [42] очікується, що протокол узгодження ключів забезпечить пряму секретність, безпеку відомого ключа та спільний контроль ключів і буде стійким до атаки Деннінга – Сакко [6]. Попередня секретність зберігає безпеку ключів сеансу після розкриття матеріалу ключів, який використовується в протоколі для узгодження ключів сеансу. Безпека відомого ключа означає, що кожен запуск протоколу повинен створювати унікальний ключ сеансу. Злом сеансового ключа не повинен загрожувати іншим сеансовим ключам. Спільний контроль ключів гарантує, що всі передбачувані учасники залучені до генерації сеансового ключа, і гарантує, що жодна сутність не зможе змусити сеансовий ключ потрапити у заздалегідь визначений інтервал. Стійкість до атак Деннінга – Сакко не дозволяє зловмиснику відновити або вгадати секретні параметри, які використовуються в протоколі, після розкриття ключа сеансу.

Хоча протоколи AKE можна розглядати як особливі випадки МРС, багато моделей безпеки були спеціально розроблені для протоколів AKE в обчислювальних налаштуваннях. Першою ігровою моделлю безпеки для протоколів AKE була модель Bellare-Rogaway (BR93) [37], яка охоплювала взаємну автентифікацію та обмін ключами від попередньо спільних симетричних ключів. Пізніше Bellare і Rogaway представили модель BR95, яка є розширенням моделі BR93 і охоплює обмін ключами на основі сервера. У моделях BR безпека протоколу KE визначається в термінах розрізнення встановлених ключів сеансу від випадкових значень під час гри з криптоаналітиком PPT. Зловмисник має доступ до будь-яких публічних даних і контролює всі комунікації, взаємодіючи з набором оракулів, кожен з яких представляє екземпляр принципала в певному виконанні протоколу. Зловмисник взаємодіє з принципалами за допомогою запитів, які в основному є Send, Reveal, Corrupt і Test. Send дозволяє криптоаналітику змусити принципалів запускати протокол. Reveal моделює здатність зловмисника знаходити старі ключі сеансу. Corrupt моделює інсайдерські атаки криптоаналітика, повертає внутрішній стан оракула та встановлює довгостроковий ключ принципала на значення, вибране зловмисником. Потім зловмисник може контролювати поведінку пошкодженого принципала за допомогою надсилання запитів. Успіх зловмисника вимірюється з точки зору його переваги в розрізненні ключа сеансу від випадкового непов'язаного значення після

виконання тестового запиту. Моделі BR стали важливою віхою та призвели до появи інших моделей безпеки. Блейк-Вілсон і Менезес розширили моделі BR, щоб охопити відкриті ключі та угоду ключів. Bellare, Pointcheval і Rogaway розширили та модифікували модель BR95, а також представили модель BPR для протоколів на основі паролів. Далі наведено основні моделі безпеки для AKE протоколів:

- Модель CK01: Белларе, Канетті та Кравчик запровадили загальну структуру та модульний підхід для розробки та аналізу протоколів автентифікації та обміну ключами, який іноді називають моделлю BCK98. Згодом Канетті та Кравчик представили модель CK01 [38], яка вирішила проблеми з моделлю BCK98 і забезпечила прототип сучасної моделі безпеки шляхом поєднання моделей BR і BCK98. Основні ідеї в моделі CK01 подібні до ідей моделей BR, але модель CK01 дозволяє розкривати стани сеансу, що фіксує більше атрибутів безпеки. Після моделі BCK98 у моделі CK01 визначено дві змагальні моделі, а саме конкурентну модель неавтентифікованих посилань (UM) і змагальну модель автентифікованих посилань (AM). У моделі UM супротивник є активним і має повний контроль над комунікаційними лініями; у той час як у моделі AM супротивник не може фабрикувати повідомлення і може доставляти лише повідомлення, справді створені сторонами, без будь-яких змін чи доповнень.

Модель CK01 використовувалася для аналізу безпеки багатьох протоколів AKE. Однак вона отримала певну критику. Модель CK01 не надає конкретного визначення ідентифікаторів сесії. Крім того, визначення стану сеансу залежить від розробників протоколів, що може спричинити неоднозначність у доказах безпеки протоколів та їх реалізації. Будь-яка реалізація, в якій локальний стан (як показано супротивнику) містить більше інформації, ніж відповідне визначення в доказах, виходить за межі доказу. Інша проблема полягає в тому, що модель CK01 не фіксує деякі важливі атаки, такі як атака KCI та її варіанти.

- Модель HMQV: вирішує проблему того, що модель безпеки CK01 не фіксує атаки KCI. Докази конструкції та безпеки протоколу HMQV базувалися на новій формі підписів виклик-відповідь, яка була отримана зі схеми ідентифікації Шнорра. Для досягнення кращої продуктивності перевірки відкритого ключа, обов'язкові в протоколах MQV, були виключені з протоколів HMQV. Це робить протокол HMQV вразливим до атак малих підгруп, що дозволяє зловмиснику відновити статичний особистий ключ жертви. Хоча модель безпеки HMQV якимось чином ігнорувала модульний підхід у моделі безпеки CK01, але вона враховувала деякі інші поняття, такі як стійкість до атаки KCI та слабка ідеальна пряма секретність (wPFS).
- Модель eCK (extended-CK) була представлена LaMacchia та ін. [40] і є розширенням моделі CK01. Він усуває деякі недоліки в моделях BR і CK01. Зокрема, криптоаналітик може отримати тимчасові секрети, які належать до тестової сесії. Криптоаналітик може отримати довгостроковий ключ тестової сесії та свого партнера ще до завершення сесії. Модель eCK допускає різні комбінації для витоку довгострокових і тимчасових секретних ключів, але не обидва витоки відбуваються в одній сутності.

Порівняння між моделями CK01, HMQV і eCK наведено в [39], де зроблено висновок, що ці моделі непорівнянні, тобто безпека в кожній із цих трьох моделей не означає безпеку в двох інших моделях.

Кілька протоколів було запропоновано як вдосконалення протоколів MQV і HMQV, і для цих протоколів було представлено кілька моделей безпеки. Приклади включають протокол CMQV у моделі eCK, протокол UP у моделі Менезеса-Устаоглу (eCK+), протокол SMQV у моделі seCK, протокол FHMQV у моделі FHMQV і протокол UP+ у моделі vCK.

3.2. Моделі безпеки для протоколів PAKE

Протоколи AKE (PAKE) на основі паролів дозволяють двом або більше об'єктам автентифікувати один одного та спільно використовувати криптографічний ключ на основі попереднього спільного пароля, який запам'ятовує людина. Через низьку ентропію паролів такі

протоколи схильні до онлайн-атак підбору пароля, яким можна запобігти, обмеживши кількість невдалих спроб на стороні сервера. Мета протоколів PAKE полягає в тому, щоб єдиною реальною атакою була атака підбору пароля в режимі онлайн. Протоколи PAKE повинні бути стійкими до атак з підбіркою пароля в режимі офлайн і невиявлених онлайн [6].

Більшість існуючих протоколів PAKE мають докази або в моделі BPR, або в моделі BMP. Хоча ці моделі забезпечують певний рівень безпеки, вони мають обмеження щодо розповсюдження паролів. Тоді Канетті запропонував ідеальну функціональність для протоколів PAKE в універсально складеній (UC) структурі, де середовище емулює будь-який розподіл, неправильні паролі та пов'язані паролі. Однак він все ще не в змозі зафіксувати деякий витік інформації, який може статися в реальності.

Модель BPR була представлена як варіант моделі BR95 для протоколів PAKE. Він мав на меті боротися з вгадуванням пароля, секретністю пересилання, компрометацією сервера та втратою ключів сеансу. Подібно до моделі безпеки BR, перевага криптоаналітика в атаці визначається як подвоєна ймовірність того, що він виграє мінус один. Модель BPR забезпечує гарантії автентифікації. Зловмисник порушує автентифікацію клієнт-сервер, якщо якийсь серверний оракул завершує роботу, не маючи оракула-партнера. Зловмисник порушує автентифікацію між серверами, якщо якийсь клієнтський оракул завершує роботу, не маючи оракула-партнера. Криптоаналітик порушує взаємну автентифікацію, якщо якийсь оракул завершує роботу, не маючи оракула-партнера. Однак показано, що модель BPR є найслабшою моделлю безпеки серед моделей безпеки BR93, BR95 і CK01. Вона не фіксує деякі атаки, включаючи атаку UKS.

4. Формальна верифікація протоколів безпеки

Формальна перевірка коректності програмного забезпечення є важливою частиною практичної та теоретичної інформатики [42]. Оскільки протоколи безпеки можна розглядати як короткі програми або алгоритми, можна адаптувати методи коректності програмного забезпечення та інструменти для перевірки протоколів безпеки. Однак міркування про складність, важливість протоколів безпеки та той факт, що проблему безпеки за наявності зловмисника неможливо виявити за допомогою функціонального тестування програмного забезпечення, вказують на те, що існує потреба в спеціалізованих інструментах.

Перевірка протоколу безпеки означає перевірку того, що протокол правильний і працює відповідно до своїх цілей безпеки. Перевірка може вказувати на приклади збоїв або недоліків у аналізованому протоколі. Одночасне виконання протоколів, де об'єкт може мати різні ролі у різних виконаннях (наприклад, як ініціатор або відповідач), а також багатопротокольні атаки, згадані в підрозд. 2.1, роблять аналіз дуже складним, що не може бути охоплено евристичною перевіркою. Проблема верифікації є нерозв'язною в найзагальнішому вигляді. Для необмеженого розміру повідомлення за наявності активного супротивника або необмеженої кількості сеансів простір станів для дослідження є нескінченним, а проблема нерозв'язною. Однак збереження секретності є NP-складним для обмеженої кількості сеансів протоколу щодо моделі Долева – Яо [41] і вирішальним для необмеженої кількості сеансів за деяких додаткових обмежень.

Формальні методи, як визначено Медоузом, – це комбінація математичної або логічної моделі системи та її вимог разом із ефективною процедурою для визначення того, чи є доказ того, що система задовольняє вимоги, правильним. Формальна перевірка протоколів безпеки може розглядатися відповідно до специфікацій протоколу або реалізацій. Ідеальною метою є мати повністю автоматизований інструмент, який перевіряє безпеку реалізованого протоколу, але ця мета ще далека від досягнення.

Формальні методи перевірки протоколів безпеки відповідно до їх специфікацій можна загалом розділити на перевірку моделі та доведення теорем. У підході перевірки моделі будується кінцевий автомат, стани якого є всіма можливими проміжними станами виконання протоколу. Потім усі можливі виконання перевіряються на відповідність набору умов корек-

тності, щоб знайти атаку на протокол. Цей метод перевіряє, чи не досягнуто стану з небажаною властивістю, яка може вказувати на атаку. Правильність визначається просто через невдачу в пошуку атаки. Методи перевірки моделі, як правило, більше підходять для пошуку атак на протоколи, а не для підтвердження їх правильності. Через можливий паралельний сеанс протоколи безпеки загалом мають нескінченну кількість станів. Таким чином, відсутність атаки в кінцевій моделі не обов'язково означає відсутність атаки в нескінченному стані. Крім того, кількість станів у скінченній моделі може бути занадто великою і може сильно збільшуватися зі збільшенням кількості учасників і виконаних кроків. Методи перевірки моделі можуть забезпечити атаку, якщо виявлено, що протокол не задовольняє умові коректності. Однак вони не дають символічного доказу безпеки протоколу, якщо атаку не виявлено. У підході доведення теореми розглядаються та перевіряються всі можливі варіанти виконання протоколу на відповідність набору умов коректності. Ці методи, як правило, більше підходять для підтвердження правильності, а не для пошуку атаки на протоколи. Вони можуть використовувати аксіоматичний (дедуктивний) або індуктивний підхід.

Формальні методи перевірки протоколів безпеки іноді називають символьними моделями. У символьних моделях криптографічні примітиви розглядаються як ідеальні чорні скриньки. Однак вони мають ту перевагу, що спрощують створення інструментів автоматичної перевірки, а також існують численні ефективні інструменти для аналізу символьного протоколу.

На відміну від символьних моделей, криптоаналітик в обчислювальних моделях не виконує заздалегідь визначених дій для аналізу повідомлень, а моделюється як довільний алгоритм PPT. Обчислювальні моделі визначили сильнішу здатність змагатися, яка ближче до реального виконання протоколів. Вони дозволяють вибірково порушувати принципали під час виконання протоколу, наприклад, їх короткострокові чи довгострокові секрети або результати проміжних обчислень.

Таким чином, обчислювальні моделі забезпечують надійніші гарантії безпеки, наприклад, ідеальну пряму секретність або стійкість до атак із розкриттям стану. Однак вони здебільшого розроблені лише для протоколів ключових угод. Крім того, докази в обчислювальній моделі важче автоматизувати.

Висновки

1. Розробка потужних квантових комп'ютерів є загрозою для криптографії з відкритим ключем, яка використовується сьогодні. Постквантова криптографія пропонує квантово безпечну альтернативу криптосистемам із відкритим ключем, які зараз використовуються. Ці схеми можуть бути реалізовані на звичайних апаратних засобах.

2. Загрози в інформаційній безпеці можна розділити на чотири великі класи: розкриття або несанкціонований доступ до інформації; обман або прийняття неправдивих даних; порушення, переривання або запобігання коректній роботі; та узурпація або несанкціонований контроль деякої частини системи. Атаки також можна розділити на пасивні та активні.

3. Існує велика кількість можливих векторів атаки, які повинні бути враховані при реалізації криптографічної схеми. З часом ці атаки стали доступнішими для криптоаналітиків, оскільки вартість обладнання, для здійснення різних видів атак, продовжувала знижуватися. Обробка великих наборів вимірів також може потребувати значних обчислювальних ресурсів. З появою хмарних сервісів тепер стало набагато простіше застосовувати масштабований ресурс обробки на вимогу без вкладень у початкові витрати на інфраструктуру.

4. Захист від переліку атак, наведених у розд. 2, не гарантує безпеку протоколу, але можна очікувати, що новий протокол не успадковує помилки попередніх проєктів протоколів. Крім того, модель безпеки розглядає найважливіші атаки, які відбуваються в реальності. Це хороший вимір для оцінки моделей безпеки: якщо модель безпеки не дозволяє зловмиснику виконувати атаки, які можуть мати місце в реальності, докази безпеки будуть марними,

тому що будуть практичні сценарії порушення протоколу, які не зафіксовані у модель безпеки.

5. Потужність і складність атак покращилися завдяки вдосконаленню методів аналізу, які розвивалися від простих компараторів, таких як різниця середніх, за допомогою диференційного аналізу з використанням кореляції Пірсона, до новітніх математичних методів обробки та статистичних методів, таких як аналіз інформації. Оскільки вдосконалення атак продовжуються, як нові, так і існуючі контрзаходи потребуватимуть постійної оцінки, щоб гарантувати, що вони продовжують забезпечувати необхідний рівень захисту. Таким чином, у розд. 3 було розглянуто моделі безпеки, які були запропоновані для оцінки безпеки та боротьби з постійною загрозою від перерахованих в розд. 2 класів атак.

6. Розробка захищених протоколів, які забезпечують певні бажані функції або служби безпеки для різних програм, є основною частиною сучасної криптографії. З іншої точки зору, конструкцію будь-якої криптографічної схеми можна розглядати як проєкт безпечного протоколу для реалізації відповідної функціональності.

7. Протокол вважається безпечним, якщо реальні параметри емулюють ідеальні параметри, тобто все, що криптоаналітик може отримати в реальних налаштуваннях, також можна отримати в ідеальних налаштуваннях. Хоча моделі безпеки, розроблені для загальних протоколів, будуть використовуватися для будь-якого криптографічного протоколу, простіше та ефективніше працювати з моделями безпеки, які спеціально розроблені для певного типу протоколу.

8. Обчислювальні моделі забезпечують надійніші гарантії безпеки, наприклад, ідеальну пряму секретність або стійкість до атак із розкриттям стану. Однак вони здебільшого розроблені лише для протоколів ключових угод. Крім того, докази в обчислювальній моделі важче автоматизувати.

9. Найбільш спеціалізовані та добре розроблені моделі безпеки для аналізу криптографічних протоколів у обчислювальних налаштуваннях присвячені протоколам AKE та PAKE, були розглянуті в даній статті.

10. Також досі залишається багато відкритих питань щодо постквантової криптографії. З одного боку, стійкість до атак бічними каналами і безпека впровадження цих криптосистем ще недостатньо досліджені. З іншого боку, необхідні подальші дослідження можливих криптоаналітичних досягнень, як з класичними, так і з квантовими комп’ютерами. З огляду на ці питання у Європейському союзі було створено багато проєктів та ініціатив щодо дослідження багатьох питань, що стосуються постквантової криптографії та зокрема побудови великомасштабного квантового комп’ютера. Також досі залишається багато відкритих питань щодо постквантової криптографії. З одного боку, стійкість до атак бічними каналами і безпека впровадження цих криптосистем ще недостатньо досліджені. З іншого боку, необхідні подальші дослідження можливих криптоаналітичних досягнень, як з класичними, так і з квантовими комп’ютерами. З огляду на ці питання у Європейському союзі було створено багато проєктів та ініціатив щодо дослідження багатьох питань, що стосуються постквантової криптографії та зокрема побудови великомасштабного квантового комп’ютера.

Список літератури:

1. John Preuß Mattsson, Ben Smeets and Erik Thormarker Quantum-Resistant Cryptography. Ericsson Security Research. [Електронний ресурс]. Режим доступу: https://arxiv.org/ftp/arxiv/papers/2112/2112.00399.pdf.

2. M. Bishop, Introduction to computer security. Prentice Hall PTR, 2004.

3. W. Stallings. Cryptography and Network Security: Principles and Practice, 6th ed. Pearson Education, 2014.

4. S. Gritzalis, D. Spinellis Cryptographic protocols over open distributed systems: A taxonomy of flaws and related protocol analysis tools, in Safe Comp 97. Springer London, 1997, pp. 123–137. [Електронний ресурс]. Режим доступу: http://dx.doi.org/10.1007/978-1-4471-0997-6.

5. A. J. Menezes, P. C. Van Oorschot, S. A. Vanstone, Handbook of applied cryptography. CRC press, 1996.

6. M. Toorani Cryptanalysis of a new protocol of wide use for email with perfect forward secrecy // Security and Communication Networks, vol. 8, no. 4, pp. 694-701, 2015.

7. R. Bird, I. Gopal, et al. Systematic design of a family of attack-resistant authentication protocols, Selected Areas in Communications // IEEE Journal on, vol. 11, no. 5, pp. 679–693, Jun 1993.

8. C. Boyd, A. Mathuria. Protocols for authentication and key establishment // Springer Science & Business Media, 2003.

9. M. Toorani. On vulnerabilities of the security association // IEEE 802.15.6 standard, in Financial Cryptography and Data Security, ser. Lecture Notes in Computer Science. Springer Berlin Heidelberg, 2015, vol. 8976, pp. 245–260.

10. M. Toorani, A. Beheshti. Solutions to the GSM security weaknesses // Proceedings of the Second International Conference on Next Generation Mobile Applications, Services, and Technologies (NGMAST'08), Sept 2008, pp. 576–581.

11. H. Xia, J. C. Brustoloni. Hardening web browsers against man-in-the-middle and eavesdropping attacks // Proceedings of the 14th International Conference on World Wide Web. New York, 2005, pp. 489–498. [Електронний ресурс]. Режим доступу: http://doi.acm.org/10.1145/1060745.1060817.

12. S. Murdoch, S. Drimer, R. Anderson, M. Bond Chip and pin is broken // Security and Privacy (SP), 2010 IEEE Symposium on, May 2010, pp. 433–446.

13. M. Toorani. Cryptanalysis of a robust key agreement based on public key authentication // Security and Communication Networks, vol. 9, no. 1, pp. 19–26, 2016.

14. B. S. Kaliski. An unknown key-share attack on the MQV key agreement protocol // ACM Transactions on Information and System Security (TISSEC), vol. 4, no. 3, pp. 275–288, 2001.

15. S. Blake-Wilson, A. Menezes. Unknown key-share attacks on the station-to-station (sts) protocol // Public Key Cryptography, ser. Lecture Notes in Computer Science. Springer Berlin Heidelberg, 1999, vol. 1560, pp. 154–170. [Електронний ресурс]. Режим доступу: http://dx.doi.org/10.1007/3-540-49162-7 12.

16. L. Gong Variations on the themes of message freshness and replay // Proceedings of the Computer Security Foundations Workshop VI, vol. 6. Citeseer, 1993, pp. 131–126.

17. C. J. Mitchell, L. Chen. Comments on the s/key user authentication scheme // ACM SIGOPS Operating Systems Review, vol. 30, no. 4, pp. 12–16, Oct. 1996.

18. M. Eian, S. F. Mjølsnes. The modeling and comparison of wireless network denial of service attacks // Proceedings of the 3rd ACM SOSP Workshop on Networking, Systems, and Applications on Mobile Handhelds (MobiHeld'11), 2011, pp. 7:1–7:6. [Електронний ресурс]. Режим доступу: http://doi.acm.org/10.1145/2043106.2043113.

19. A. Shamir, R. Rivest, L. Adleman Mental poker // The Mathematical Gardner. Springer US, 1981, pp. 37–43. [Електронний ресурс]. Режим доступу: http://dx.doi.org/10.1007/978-1-4684-6686-7.

20. M. Naor, M. Yung Public-key cryptosystems provably secure against chosen ciphertext attacks // Proceedings of the 22nd Annual ACM Symposium on Theory of Computing (STOC'90). New York, NY, USA: ACM, 1990, pp. 427–437.

21. C. Rackoff, D. R. Simon. Non-interactive zero-knowledge proof of knowledge and chosen ciphertext attack // Advances in Cryptology – CRYPTO'91, ser. Lecture Notes in Computer Science. Springer Berlin Heidelberg, 1992, vol. 576, pp. 433–444.

22. E. Biham, A. Shamir. Differential cryptanalysis of des-like cryptosystems // Advances in Cryptology-CRYPTO'90, ser. Lecture Notes in Computer Science. Springer Berlin Heidelberg, 1991, vol. 537, pp. 2–21. [Електронний ресурс]. Режим доступу: http://dx.doi.org/10.1007/3-540-38424-3.

23. H. Wu, B. Preneel. Differential cryptanalysis of the stream ciphers Py, Py6 and Pypy // Advances in Cryptology – EUROCRYPT 2007, ser. Lecture Notes in Computer Science. Springer Berlin Heidelberg, 2007, vol. 4515, pp. 276–290. [Електронний ресурс]. Режим доступу: http://dx.doi.org/10.1007/978-3-540-72540-4.

24. M. Matsui, A. Yamagishi. A new method for known plaintext attack of feal cipher, in Advances in Cryptology – EUROCRYPT'92, ser. Lecture Notes in Computer Science. Springer Berlin Heidelberg, 1993, vol. 658, pp. 81–91. [Електронний ресурс]. Режим доступу: http://dx.doi.org/10.1007/3-540-47555-9.

25. G. Bard. Algebraic cryptanalysis // Springer Science & Business Media, 2009.

26. E. Biham, O. Dunkelman, N. Keller. New combined attacks on block ciphers // Fast Software Encryption, ser. Lecture Notes in Computer Science. Springer Berlin Heidelberg, 2005, vol. 3557, pp. 126–144. [Електронний ресурс]. Режим доступу: http://dx.doi.org/10.1007/11502760.

27. B. Zhu, G. Gong. Multidimensional meet-in-the-middle attack and its applications to katan32/48/64 // Cryptography and Communications, vol. 6, no. 4, pp. 313–333, 2014.

28. L. Knudsen, D. Wagner. Integral cryptanalysis // Fast Software Encryption, ser. Lecture Notes in Computer Science. Springer Berlin Heidelberg, 2002, vol. 2365, pp. 112–127. [Електронний ресурс]. Режим доступу: http://dx.doi.org/10.1007/3-540-45661-9.

29. E. Biham. New types of cryptanalytic attacks using related keys // Advances in Cryptology – EUROCRYPT'93, ser. Lecture Notes in Computer Science. Springer Berlin Heidelberg, 1994, vol. 765, pp. 398–409. [Електронний ресурс]. Режим доступу: http://dx.doi.org/10.1007/3-540-48285-7.

30. M. Hell, T. Johansson, L. Brynielsson An overview of distinguishing attacks on stream ciphers // Cryptography and Communications, vol. 1, no. 1, pp. 71–94, 2009.

31. M. Bellare, A. Desai, D. Pointcheval, P. Rogaway. Relations among notions of security for public-key encryption schemes // Advances in Cryptology – CRYPTO'98, ser. Lecture Notes in Computer Science. Springer Berlin

Heidelberg, 1998, vol. 1462, pp. 26–45. [Електронний ресурс]. Режим доступу: http://dx.doi.org/10.1007/BFb0055718.

32. M. Bellare, P. Rogaway. Optimal asymmetric encryption – how to encrypt with RSA // Advances in Cryptology – EUROCRYPT'94, ser. Lecture Notes in Computer Science. Springer Berlin Heidelberg, 1995, vol. 950, pp. 92–111.

33. J. Katz, Y. Lindell. Introduction to modern cryptography. Chapman & Hall / CRC, 2008.

34. D. A. Osvik, A. Shamir, E. Tromer. Cache attacks and countermeasures: The case of AES // Topics in Cryptology – CT-RSA 2006, ser. Lecture Notes in Computer Science. Springer Berlin Heidelberg, 2006, vol. 3860, pp. 1–20.

35. R. Cramer, I. Damgard, J. B. Nielsen. Secure multiparty computation and secret sharing – an information theoretic approach. Book Draft, 2013.

36. W. Diffie, M. Hellman. New directions in cryptography // IEEE Transactions on Information Theory, vol. 22, no. 6, pp. 644–654, Nov 1976.

37. M. Bellare, P. Rogaway. Entity authentication and key distribution // Advances in Cryptology – CRYPTO'93, ser. Lecture Notes in Computer Science. Springer Berlin Heidelberg, 1994, vol. 773, pp. 232–249. [Електронний ресурс]. Режим доступу: http://dx.doi.org/10.1007/3-540-48329-2.

38. R. Canetti, H. Krawczyk. Analysis of key-exchange protocols and their use for building secure channels // Advances in Cryptology – EUROCRYPT'01, ser. Lecture Notes in Computer Science. Springer Berlin Heidelberg, 2001, vol. 2045, pp. 453–474. [Електронний ресурс]. Режим доступу: http://dx.doi.org/10.1007/3-540-44987-6.

39. C. Cremers. Examining indistinguishability-based security models for key exchange protocols: the case of CK, CK-HMQV, and eCK // Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security, ser. ASIACCS'11. New York, NY, USA: ACM, 2011, pp. 80–91.

40. B. LaMacchia, K. Lauter, A. Mityagin. Stronger security of authenticated key exchange // Provable Security, ser. Lecture Notes in Computer Science. Springer Berlin Heidelberg, 2007, vol. 4784, pp. 1–16.

41. D. Dolev, A. C. Yao. On the security of public key protocols // IEEE Transactions on Information Theory, vol. 29, no. 2, pp. 198–208, Mar 1983.

42. M. Toorani Security Protocols in a NutShell, Department of Informatics, University of Bergen, Norway, arXiv preprint arXiv:1605.09771, 2016. [Електронний ресурс]. – Режим доступу: https://arxiv.org/pdf/1605.09771.pdf.

Надійшла до редколегії 03.11.2022

Відомості про авторів:

Острянська Єлизавета Вадимівна – аналітик з систем захисту інформації, АТ «Інститут Інформаційних технологій», Україна; e-mail: antelizza@gmail.com

Кандій Сергій Олегович – Харківський національний університет імені В. Н. Каразіна, аспірант кафедри безпеки інформаційних систем і технологій, факультет комп'ютерних наук, АТ «Інститут Інформаційних технологій», технік-конструктор, Україна; e-mail: sergeykandy@gmail.com

Горбенко Іван Дмитрович – д-р техн. наук, професор, Харківський національний університет імені В. Н. Каразіна, професор кафедри безпеки інформаційних систем і технологій, факультет комп'ютерних наук, АТ "Інститут Інформаційних Технологій", головний конструктор, Україна; e-mail: gorbenkoi@iit.kharkov.ua; ORCID: https://orcid.org/0000-0003-4616-3449

Єсіна Марина Віталіївна – канд. техн. наук, Харківський національний університет імені В.Н. Каразіна, доцент кафедри безпеки інформаційних систем і технологій, факультет комп'ютерних наук; науковий співробітник-консультант АТ «Інститут Інформаційних технологій»; Україна; e-mail: m.v.yesina@karazin.ua; ORCID: https://orcid.org/0000-0002-1252-7606