КІБЕРНЕТИКА та КОМП'ЮТЕРНІ ТЕХНОЛОГІЇ

УДК 004.056 DOI:10.34229/2707-451X.20.3.7

В.Ю. КОРОЛЬОВ, М.І. ОГУРЦОВ, О.М. ХОДЗІНСЬКИЙ

БАГАТОРІВНЕВЕ ДЕРЖАВНЕ ВПІЗНАВАННЯ ОБ'ЄКТІВ ТА АНАЛІЗ ЗАСТОСОВНОСТІ ПОСТ-КВАНТОВИХ КРИПТОГРАФІЧНИХ АЛГОРИТМІВ ДЛЯ ЗАХИСТУ ІНФОРМАЦІЇ

Широке застосування безпілотних систем спонукає до модернізації існуючої системи державного впізнавання. Запропоновано новий алгоритм захисту інформації для системи державного впізнавання (СДВ) для військових об'єктів, що забезпечуватиме достатню масштабованість, стійкість, надійність та багаторівневість впізнавання. Проаналізовано загрози для сучасних криптографічних алгоритмів, викликані реалізацією алгоритмів Гровера і Шора на квантових комп'ютерах (КК). Досліджено криптографічні алгоритми, стійкі до атак за допомогою КК та надано рекомендації до застосування класичних алгоритмів – нові довжини ключів шифрування для СДВ.

Ключові слова: *державне впізнавання, квантові комп'ютери, пост-квантова криптографія.*

Вступ. Зростання кількості рухомих роботизованих систем у сучасних збройних конфліктах потребує вдосконалення систем впізнавання військових об'єктів за якісними і кількісними показниками. Широке застосування безпілотних літальних апаратів (БПЛА) та їх роїв у новітніх гібридних конфліктах потребує розробки мережевих алгоритмів державного впізнавання та передачі інформації, що можуть ґрунтуватись на методах захисту інформації, а саме симетричних і асиметричних алгоритмах шифрування даних та інших методах криптографії [1–2].

Система державного впізнавання (ДВ) [3] є складовою частиною автоматизованої системи «Ореанда» [4], яка керує військовою авіацією, протиповітряною обороною, взаємодіє з цивільними системами керування повітряним рухом, військовими системами радіотехнічної та авіаційної розвідки. «Ореанда» – це складова частина багаторівневої Єдиної системи автоматизованого управління (ЄАСУ) Збройними Силами України (ЗСУ) (рис. 1) та взаємодія з системами керування рівня бригади «Дзвін», системами керування рівня батальйону «Простір», а також системами NATO C4ISR (Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance) за стандартом Link-1. Для криптографічного захисту передачі інформації на всіх рівнях та у всіх перелічених системах застосовуються симетричні й асиметричні криптографічні алгоритми.

Сьогодні в ЗСУ для ДВ об'єктів військової техніки (ОВТ) за принципом «свій-чужий» використовується комплекс «Пароль-М», який є модифікацією радянської системи, розробленої у 80-х роках минулого століття. Комплекс «Пароль» передбачає, що у тактичній зоні може бути до 110 запитувачів і 110 відповідачів [5], аналогічна система в країнах блоку NATO – MarkXII виконує в номінальному режимі 400 опитувань в секунду [6].

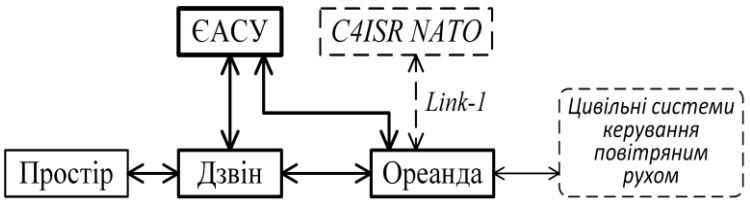

РИС. 1. Багаторівнева організація обміну даними в АСУ ЗСУ

Після відповіді на кожен запит передавач відповідача на деякий час вимикається за допомогою замикаючого пристрою [7]. Цим запобігають відповіді на радіосигнали, які відбиті від прилеглих місцевих предметів у тих випадках, коли частоти запиту і відповіді збігаються, а коди подібні. При дуже великій частоті запитів число відповідей кожному запитувачу зменшується і може досягти рівня, при якому порушується нормальна робота системи. Для запобігання цьому у відповідачах застосовується автоматичне обмеження максимального числа відповідей. Воно здійснюється шляхом інтегрування дешифрованих сигналів запиту і використання напруги отриманого сигналу для регулювання швидкості роботи каналу формування відповідей. Пристрій обмеження частоти відповідей дозволяє також запобігти тепловому перевантаженню генератора відповідача при великому числі запитів [5, 7].

Новітні засоби керування високоточною зброєю окрім радіотехнічних способів підвищення точності впізнавання об'єктів [5, 7] мають забезпечувати: зменшення кількості об'єктів у промені радіолокатора, звуження діаграми спрямованості радіолокатора, запобігання прийому відбитих сигналів за бічними пелюстками від радіолокатора багатоканальних приймачів, когерентний прийом і передачу сигналів впізнавання. Вони мають використовувати також технології розпізнавання військових об'єктів [7], техніки та солдат супротивника для віднесення об'єкта до «своїх» або «чужих» на базі розпізнавання образів.

Застосування роїв БПЛА у збройних конфліктах на Близькому сході, оснащення засобами впізнавання новітніх екіпірувань солдат показує, що впізнавання 110 об'єктів у зоні відповідальності військового підрозділу може виявитись недостатнім. Цю проблему можна вирішити розробкою нових систем кодування і шифрування сигналів ДВ ОВТ, які відповідатимуть сучасному рівню вимог.

Сучасні комплекси розпізнавання цілей для військових літальних апаратів (ЛА) [7] складаються з декількох систем, до переліку яких входить система державного впізнавання, що об'єднуються системою підтримки прийняття рішень пілота для застосування засобів ураження. Алгоритми ДВ ОВТ ЗСУ, які використовуються системами автоматичного впізнавання за принципом «свій-чужий», з точки зору інформаційної безпеки є алгоритмами зі змінними параметрами для ідентифікації технічних об'єктів на базі паролів з ротацією їх у часі [5 – 7]. У роботі пропонується розробити алгоритми для системи ДВ ОВТ на базі криптографічних алгоритмів.

Розвиток алгоритмів, що використовуються у системах ДВ ОВТ [5, 7], подібний до еволюції систем автентифікації користувачів комп'ютерних систем і мереж [8, 9], де відбувся поступовий перехід від однофакторних систем ідентифікації до багатофакторних систем автентифікації з резервними варіантами авторизації доступу, що застосовують асиметричні криптографічні алгоритми для надання дистанційного доступу до інформаційних сервісів у мережі Інтернет.

Системи радіолокаційного впізнавання (системи вторинної радіолокації) [1, 5 – 7] – це комплекс наземної, літакової, корабельної та космічної апаратури (відповідачів та запитувачів), що забезпечує впізнання об'єктів державної належності у всіх родах Збройних сил на основі Єдиної системи кодування сигналів.

Склад системи радіолокаційного впізнання. Система радіолокаційного розпізнавання будується за принципом радіолокаційної системи з активною відповіддю. Вона являє собою єдиний радіотехнічний комплекс, що складається з запитувача і відповідача, утворюють два канали зв'язку (канал запиту і канал відповіді), які називають лінією впізнання (рис. 2).

Механізм впізнавання можна представити наступним чином. Запитувач по каналу запиту випромінює кодований спеціальним кодом сигнал (сигнал запиту). Відповідач приймає цей сигнал, декодує його і в разі рівності отриманої кодової послідовності сигналу встановленим на даний час значенням виробляє сигнал відповіді, структура якого теж відповідає встановленому на даний час коду. При активній відповіді по каналу відповіді крім інформації державної приналежності може передаватися інша корисна (в тому числі й не радіолокаційна) інформація: висота польоту (бортовим висотоміром вона визначається більш точно, ніж наземною РЛС), відомості про кількість палива, бортовий номер об'єкта і т. д., а за часом приходу відповідного сигналу і його напрямом визначаються відповідно дальність і кутові координати об'єкта (див. рис. 3).

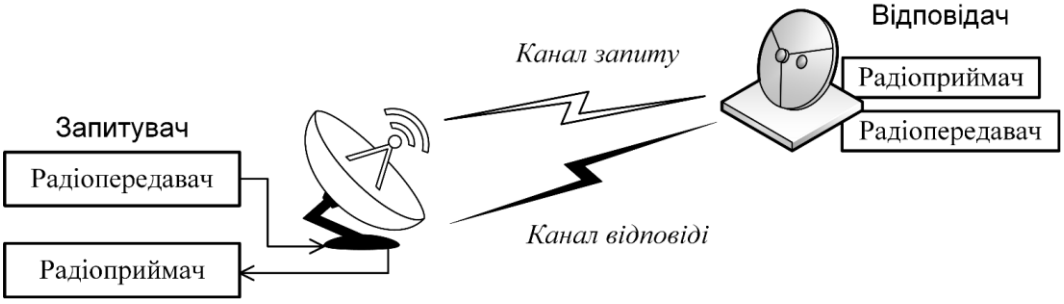

РИС. 2. Принцип побудови системи ДВ

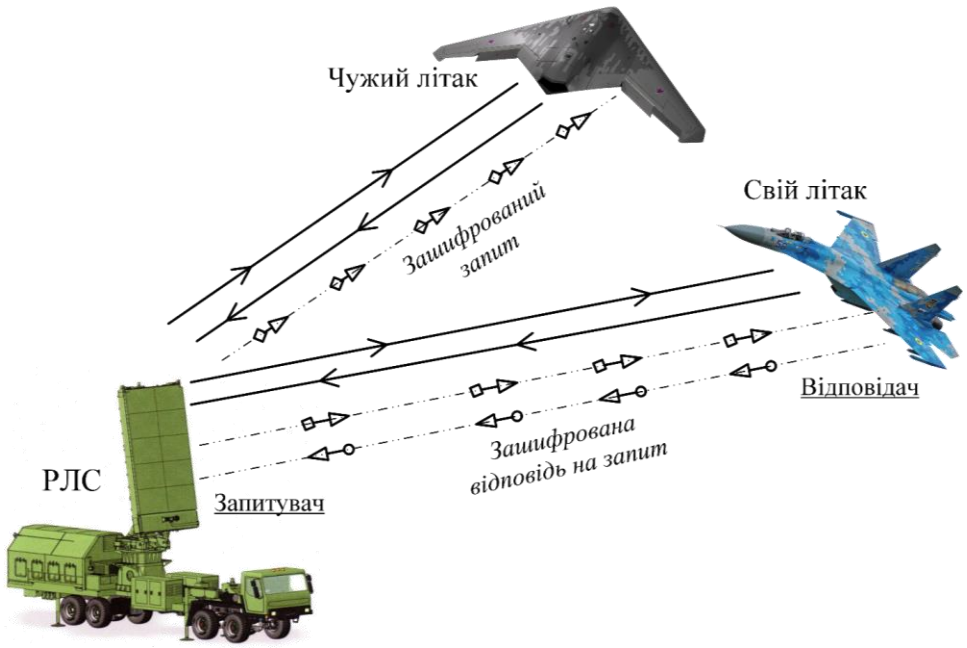

РИС. 3. Принцип роботи системи державного впізнавання

Сигнал відповіді приймається запитувачем, також декодується, і результат декодування висвічується у вигляді відповідної позначки на екрані РЛС. Таким чином, якщо об'єкт свій, то на індикаторі РЛС від даного об'єкта висвічуються дві позначки:

- відмітка, обумовлена відлунням сигналу РЛС від об'єкта;
- додаткова відмітка, що показує державну приналежність об'єкта.

Інформація про державну приналежність використовується на всіх етапах організації та ведення бойових дій і тому є вкрай важливою. Для вирішення завдань сучасного бою система ДВ має відповідати ряду загальних вимог:

- мати високу перешкодозахищеність як по запитному каналу, так і по каналам відповіді;
- мати достатню стійкість до імітації противником відповідних сигналів;
- мати високу пропускну здатність (надійно працювати за наявності в тактичній зоні великого числа запитувачів і відповідачів);
- мати досить точні характеристики, що забезпечуються розрізнювальною здатністю за дальністю і кутовими координатами;
- мати високу експлуатаційну надійність і малий час відновлення;
- характеристики системи мають бути узгоджені з характеристиками РЛС, з якою вона пов'язана. При цьому максимальна дальність розпізнавання має бути більшою або дорівнювати максимальній дальності виявлення РЛС.

У системах ДВ [1, 5–7] сигнал запиту – це комбінація з високочастотних сигналів РЛС і передавача запитувача, що передаються на різних частотах (рис. 2, 3).

Прийом і розшифровка сигналів відповіді здійснюються у спеціальному пристрої – запитувачі [8, 9]. Сигнал відповіді генерується передавачем об'єкта, що перевіряється, тільки тоді, коли його приймальний пристрій отримає обидва сигнали як РЛС, так і запитувача. Завдяки цьому система не створює зайвого демаскуючого випромінювання та забезпечує зменшення завантаження відповідачів об'єктів впізнавання, тобто збільшується пропускна здатність системи.

Захист інформації для системи ДВ

Суть роботи алгоритмів ДВ – це обробка запитів і відповідей ОВТ, які зашифровані симетричним криптографічним алгоритмом. Такий підхід обрано тому, що потрібна максимальна продуктивність такої системи, а обмін публічними ключами за асиметричною системою може не спрацювати в умовах дії природніх шумів або навмисних завад, створених комплексами радіоелектронної боротьби супротивника. Іншим рекомендованим підходом є використання асиметричного криптографічного алгоритму лише для шифрування ключа симетричного алгоритму для його відправлення до передачі сигналів запиту/відповіді. В цьому випадку можливість розшифрувати та використати ключ симетричного алгоритму автоматично означає наявність ключа асиметричного алгоритму.

За аналогією з цивільними системами керування повітряним рухом у відповідь військовий технічний об'єкт може надати не тільки свій ідентифікатор, але і дані про координати, тип літака та інше, що може бути додатково використано для запобігання підміні сигналу відповіді та перевірці справжності отриманого коду. ОВТ, включений у підсистеми ЄАСУ ЗСУ, може також використовувати інформацію від цивільних систем для верифікації даних, отриманих через спеціальні мережі, що застосовують симетричні і асиметричні криптографічні алгоритми для захисту інформації для забезпечення багаторівневого ДВ ОВТ.

Алгоритм захисту інформації системи ДВ

Розглянемо один з можливих варіантів роботи системи ДВ:

1) перед виконанням задач державного впізнавання у центрі керування повітряним рухом заздалегідь генерується відкритий довготерміновий ключ K для асиметричного алгоритму шифрування та копіюється на кожний ОВТ. Він зберігається і на кожному об'єкті, і у центрі керування повітряним рухом для подальшого тривалого використання. Пара до цього відкритого ключа – закритий ключ $K_з$ – зберігається виключно у центрі керування повітряним рухом;

2) кожному ЛА призначається свій унікальний ідентифікатор I_i, що зберігається в його довготерміновій пам'яті. База усіх ідентифікаторів I також зберігається у центрі керування повітряним рухом;

3) для кожного ЛА генерується унікальна пара ключів Q_o та Q_z. Відкритий ключ Q_o зберігається в центрі керування повітряним рухом, а закритий Q_z – в пам'яті ЛА;

4) за необхідності виконання процедури впізнавання центр керування повітряним рухом надсилає невпізнаному літальному об'єкту (НЛО) відкритий (не зашифрований) запит на впізнавання B_i, що містить позначку дати та часу (включаючи секунди) T_i;

5) НЛО, отримавши запит на впізнавання B_i, шифрує отриману позначку дати та часу T_i закритим ключем Q_z. Після цього він шифрує свій ідентифікатор I_i та попередньо зашифровану позначку дати та часу довготерміновим ключем K. Після цього НЛО передає зашифровану відповідь до центру керування повітряним рухом. Зашифрована відповідь НЛО на запит впізнавання має вигляд

$$\{I_i,\{T_i\}Q_z\}K; \tag{1}$$

6) центр керування повітряним рухом отримує зашифровану відповідь від НЛО. Він розшифровує її довготерміновим закритим ключем $K_з$ – і отримує ідентифікатор об'єкта I_i. Далі в своїй базі даних центр керування знаходить відповідний об'єкту I_i відкритий ключ Q_o, та використовує його для розшифровки позначки дати та часу T_i. Якщо розшифрована позначка дати та часу співпадає з тою, що була відправлена НЛО на кроці 4, то це підтверджує, що НЛО – той ЛА, за який він себе видає (апарат з ідентифікатором I_i або «свій»);

7) за необхідності повторити процедуру впізнавання кроки 4 – 6 повторюються.

У випадку, якщо інформація про захоплені супротивником/втрачені/знищені ЛА буде вчасно оновлюватись у базі даних центру керування повітряним рухом, то така система ДВ забезпечуватиме достатню стійкість та надійність впізнавання. Інакше супротивник, захопивши ЛА, може просто перемістити систему відповіді на запит впізнавання на один зі своїх ЛА. В цьому випадку система впізнавання буде давати правильні відповіді на запити від центру керування повітряним рухом.

За необхідності виконувати захищений обмін даними після завершення процедури впізнавання, в алгоритм слід ввести такі зміни:

1) п. 5) НЛО генерує сеансовий ключ для симетричного криптографічного алгоритму KS_i. Далі НЛО шифрує ключем Q_z не лише позначку дати та часу T_i, але й ключ KS_i. Вигляд відповіді на запит від системи впізнавання (зашифрована відповідь НЛО із симетричним ключем на запит впізнавання) в цьому випадку описується залежністю

$$\{I_i,\{T_i,KS_i\}Q_z\}K; \tag{2}$$

2) п. 6) центр керування повітряним рухом розшифровує відповідь послідовно ключами $K_з$ та Q_o і отримує ключ KS_i, який застосовує для подальшого обміну даними з літальним апаратом, використовуючи симетричний алгоритм шифрування.

Вибір асиметричних алгоритмів шифрування даних для систем військового зв'язку і ДВ ОВТ з урахуванням розвитку квантових комп'ютерів

Зростання продуктивності квантових комп'ютерів [10 – 12] у виконанні алгоритму Гровера для пошуку і алгоритму Шора для факторизації простих чисел ставить питання перегляду довжин ключів застосованих криптографічних алгоритмів та запровадження нових протоколів захисту інформації у наступні 5 – 10 років, що приблизно відповідає часу постановки на озброєння нових систем в Україні. У 2016 році Національний інститут стандартів і Агентство Національної безпеки США рекомендувало збільшити довжини ключів криптографічних алгоритмів [9]. Оскільки квантові комп'ютери розвиваються не тільки в демократичних країнах блоку NATO, то Україні варто розглянути доцільність створення альтернативних протоколів на базі пост-квантових криптографічних алгоритмів, які стійкі до зламу квантовими комп'ютерами. Проаналізуємо можливості квантових алгоритмів, що прискорюють злам алгоритмів шифрування та розроблені алгоритми пост-квантової криптографії з метою формування переліку рекомендацій за їх вибору і застосуванню для задач державного впізнавання та захисту інформації у спеціальних мережах.

Алгоритм Гровера [13] показує, що отримати розв'язок будь-якої задачі пошуку можна набагато швидше за допомогою квантових комп'ютерів. Замість того, щоб послідовно чи паралельно перебирати всі можливі N рішень на класичних процесорах, квантовий комп'ютер з $\log(N) + 1$ кубітами прискорює продуктивність розв'язування пропорційно квадратному кореню з N. Тобто алгоритм Гровера забезпечує поліноміальне прискорення продуктивності обчислень. Алгоритм Гровера прискорює головним чином підбір ключів симетричних шифрів та в меншій мірі пошук криптографічних ключів асиметричних шифрів і деяких типів криптографічних геш-функцій. Експерти рекомендують [13] збільшити принаймні вдвічі довжину ключів для симетричних криптографічних алгоритмів і гешів відносно таких, що рекомендують застосовувати на сьогоднішній день, для забезпечення захисту інформації при появі квантових комп'ютерів.

Алгоритм Шора [13] теоретично забезпечує поліноміальне поліпшення часу для факторингу великих простих чисел. Цей алгоритм дозволяє розкласти на множники дуже великі рівняння з простих чисел на квантовому комп'ютері зі стабільними (без шуму і помилок обчислень) кубітами за час, що оцінюється секундами або хвилинами.

Нині є алгоритми факторизації для квантових комп'ютерів, швидші за алгоритм Шора, наприклад, GEECM (Grover Lenstra elliptic-curve factorization method) [14]. Це означає, що алгоритм Шора надає нижню межу швидкості обчислення рівнянь з великими простими числами тобто вони можуть бути вирішені навіть швидше або з меншою кількістю кубітів.

Криптографічні технології, засновані на асиметричних алгоритмах шифрування та стійкі до алгоритму Шора

Асиметрична криптографія зі збільшеною довжиною ключа [13] – це криптографічні алгоритми, засновані на факторизації великих простих чисел, задачі пошуку дискретного логарифма або задачі пошуку дискретного логарифма еліптичної кривої. Такі алгоритми можуть бути зламані, коли квантові комп'ютери матимуть достатньо стабільних кубітів та зв'язків між ними [10], щоб реалізувати алгоритми розкладання чисел на множники.

Криптографія на основі алгебраїчного коду з виправленням помилок [13] – це набір алгоритмів шифрування і підпису, заснований на кодах Гоппи (Goppa codes), які навмисно генерують «помилки» у відкритому тексті, щоб зашифрувати вихідні дані. На двійкових кодах Гоппи базується ряд шифрів: BIKE, Classic McEliece, HQC, LEDAcrypt, NTS-KEM, Rollo, and RQC McEliece. Побудова криптографічної системи за алгоритмами виправлення помилок має два значних недоліки: значно більший розмір відкритих ключів порівняно з RSA (приблизно 300 000 біт) та є теоретична імовірність, що внесені «помилки» не будуть виправлені. Таким чином, на сьогоднішній день цей набір алгоритмів не може практично застосовуватись у реальних умовах.

Криптографія на базі граткових математичних структур [13] базується на формулах, які за побудовою важко факторизувати, як відомі обчислювальні граткові задачі. Граткові криптографічні алгоритми вважаються стійкими до алгоритму Шора та інших квантових алгоритмів факторизації. Найбільш поширені граткові задачі, що використовуються в криптографії, відомі як навчання з помилками (Learning With Errors – LWE), кільцеве навчання з помилками (Ring Learning With Errors – RLWE), модульне навчання з помилками (Module Learning With Errors – MLWE),
навчання з округленням (Learning With Rounding – LWR). Кожен різновид граткових задач має свої переваги і недоліки для застосування у криптографії. Проте, алгоритми на базі LWE, що використовують алгебраїчні кільця, швидші та мають менші довжини ключів у порівнянні з іншими варіантами. До недоліків граткової криптографії відносять відносно великі розміри ключів у порівнянні з іншими типами шифрів. Найбільш відомими гратковими шифрами є: Round5, LAC, NewHope, ThreeBears, NTRU, NTRUPrime, CRYSTAL-Kyber, SABER, FRODO-KEM. Таким чином, їх можна застосовувати для захисту даних – але на даний момент вони поступаються за характеристиками надійним криптографічним алгоритмам, що використовуються на сьогоднішній день.

Криптографія на базі суперсингулярних ізогеній еліптичних кривих [13] використовує математичні рівняння та алгоритми, які утворюють суперсингулярні еліптичні криві та графіки ізогенії для побудови алгоритмів шифрування. Еліптичні криві є алгебраїчними кривими, які не перетинаються або є несингулярними. Всі суперсингулярні криві є несингулярними, а «супер» означає, що кільця є надзвичайно великими. Ізогенія відноситься до окремих алгебраїчних груп, які поділяють перетин пов’язаних значень між собою.

В ізогенній криптографії два різних рівняння алгоритму створюють ізогенний зв’язок, який використовується для шифрування і дешифрування. Відповідно відкритим ключем є пара еліптичних кривих, а закритий ключ – це ізогенія між ними. Знаходження цієї ізогенії, знаючи лише пару суперсингулярних еліптичних кривих, є обчислювально складною задачею. До переваг ізогенної криптографії відносять малі розміри ключів, а також підтримку частої зміни сеансових ключів. Ізогенна криптографія відносно нова, тому вона перебуває у процесі досліджень і тестувань. Єдиний відомий криптографічний алгоритм на базі алгоритмів ізогенної суперсингулярної криптографії, поданим до розгляду у Національний інститут стандартів США, – SIKE. Цей напрям є перспективним, але, оскільки на сьогоднішній день єдиний відомий криптографічний алгоритм недостатньо вивчений та досліджений, то його зарано називати надійним альтернативним існуючим алгоритмом шифрування.

Криптографія багатопараметрична (множинність змінних) [13] відноситься до асиметричних алгоритмів шифрування і цифрового підпису, які засновані на багатовимірних поліноміальних математичних рівняннях, таких як $x + y + z = n$, щоб сформувати криптографічні примітиви. Правильно побудована багатовимірна криптографія не може бути зламана за поліноміальний час та не використовує великі прості числа для захисту від алгоритмів факторизації, тому вважається квантово-стійкою. Для алгоритмів багатопараметричної криптографії відомі продуктивні апаратні реалізації на спеціалізованих процесорах і програмованих логічних матрицях. Багатовимірна криптографія включає у себе HFE, Gui, Balanced Oil & Vinegar (BOV), Unbalanced Oil & Vinegar (UOV) і Tame Transformation Signature. Відомі багатовимірні схеми цифрового підпису включають GeMSS, LUOV, MQDSS і Rainbow. Rainbow – це багатошарова реалізація UOV.

Для більшості з цих алгоритмів існують відомі атаки. Для алгоритму HFE – отримання закритого ключа (Шамір-Кіпніс) та атака, розроблена Жаном-Чарльзом Фужером на основі алгоритму Гребнера [15]. Алгоритми UOV та BOV використовують дуже великі ключі (ці ключі містять цілі системи рівнянь), що значно обмежує їх практичне застосування. Крім того, вони є молодими та недостатньо дослідженими (хоча певний ряд атак – наприклад, отримання закритого ключа (Шамір-Кіпніс) для них вже відомий). Відомі також загальні для цих криптографічних алгоритмів атаки методами повторної лінеаризації та використанням XL алгоритму. Тому зарано застосовувати їх в реальних випадках, що потребують значного рівня захисту інформації.

Аналіз застосування квантових комп'ютерів до зламу криптографічних алгоритмів

На даний час можна стверджувати, що для низки квантових комп'ютерів існує аналог закономірності Мура, принаймні деякі розробники заявляють про це [10, 12, 16] – тобто число кубітів подвоюється приблизно раз на рік. Але складності розв'язування задачі збільшення кількості кубітів [10] додає факт, що квантові обчислення потребують калібрування, виконуються з помилками, котрі виправляють за допомогою багатократних запусків задач (100 – 1000 разів), а потім обирають результат з найбільшою ймовірністю.

В результаті прогноз від IBM про виконання закономірності Мура для універсальних квантових комп'ютерів здається занадто оптимістичним і не точним. Наприклад, ще у 2016 році компанія IBM представила квантовий комп'ютер на 16 кубітів [17]. А на момент середини 2020 року максимальна кількість кубітів у працюючому квантовому комп'ютері досягла лише 20 [18] – і ця кількість кубітів була досягнута за 4 роки роботи компанії IBM (тобто, приріст склав лише 25 % за 4 роки). Та й в цілому результат в 20 кубітів був досягнутий лише за десятиріччя роботи над квантовими комп'ютерами в усьому світі. В Російській Федерації на сьогоднішній день вдалося створити лише квантовий комп'ютер з двома кубітами. Крім того, зростання складності розробки та налаштування квантових комп'ютерів (калібрування, помилки – [10]) через зростання кількості кубітів у їх складі є близьким до експоненційного.

Тобто можна прогнозувати, що в найближчі десятиріччя закон Мура для універсальних квантових комп'ютерів не буде виконуватись [19], зростання кількості кубітів у їх складі ще сповільниться, або навіть зупиниться. Для спеціалізованих квантових комп'ютерів фірми D-wave закономірність Мура виконується, у 2020 році прогнозується поява обчислювального пристрою з 5000 [16] кубіт, але алгоритм Шора для них не підходить [20] і поліноміальний час виконання не гарантується. На момент написання статті є повідомлення про факторизацію на множники чисел з максимальним значенням до 291311 [21].

Отже, обчислювальна продуктивність, досягнута багатьма різними типами квантових комп'ютерів і відповідними алгоритмами, вказує на нездатність зламати різні типи систем криптографічного захисту інформації у найближчий час. Деякі квантові комп'ютери ймовірно досягнуть квантової переваги протягом наступного року або двох років і будуть здатні розв'язувати задачі, які класичні комп'ютери не можуть розв'язати за прийнятний час. Але алгоритми асиметричного шифрування, що ґрунтуються на низькій ефективності класичних комп'ютерів у розв'язуванні задач факторизації простих чисел і подібних для побудови систем захисту інформації, не стануть менш надійними у найближчі 5 – 10 років. Рекомендації збільшити вдвічі довжину ключів для симетричних та асиметричних криптографічних алгоритмів є більш ніж достатньо для захисту від квантових комп'ютерів, що можуть застосовуватись у криптоаналізі впродовж щонайменше наступних 10-ти років. Алгоритми, що теоретично є стійкими до квантових методів криптоаналізу, потребують більш детальних досліджень, щоб визначити, чи не мають вони інших вразливостей. Лише після проведення таких досліджень їх можливо буде рекомендувати для застосування для захисту критично важливої інформації.

Квантові методи захищеної передачі інформації вже технічно реалізовані для оптоволоконних ліній, а способи передачі даних, які використовують закони квантової фізики, перейшли в стадію польових випробувань. Нещодавно виконано передачу інформації за допомогою зв'язаних фотонів через ретранслятори та низку БПЛА [13], а також квантову телепортацію спінових станів фотонів на супутник на навколоземній орбіті [13]. Тому напрямками подальшої роботи може бути створення квантових алгоритмів захисту інформації та передачі даних.

Результати. У статті запропоновано новий багаторівневий алгоритм державного впізнавання на базі сучасних криптографічних методів захисту інформації, який дозволяє виконувати надійну автоматизовану ідентифікацію об'єктів, масштабувати систему за допомогою використання даних про потенційні цілі з інших джерел через захищені мережі та обмінюватись власними даними з іншими системами через спеціальні мережі.

Алгоритм пошуку Гровера на сьогоднішній день не дає сильного приросту в продуктивності пошуку ключів для алгоритмів симетричного шифрування, тому немає потреби збільшувати довжини ключів для цього типу алгоритмів захисту інформації.

Пост-квантові алгоритми асиметричного шифрування потребують додаткового вивчення і всебічного тестування захисту інформації або збільшення довжин ключів криптографічних алгоритмів, яке відповідає кількості кубітів, тобто більше ніж у два рази. Найбільш перспективним є сімейство асиметричних пост-квантових алгоритмів заснованих на *криптографії на базі суперсингулярних ізогеній еліптичних кривих*.

Висновки. Розроблено алгоритм державного впізнавання об'єктів, що є більш захищеним порівняно з існуючими алгоритмами та орієнтований на використання сучасних бортових комп'ютерів та програмованих радіомодемів. Алгоритм Шора та подібні стануть суттєвою загрозою для сучасних алгоритмів асиметричної криптографії лише коли кількість кубітів квантових комп'ютерів буде перевищувати кількість бітів у публічних ключах більше ніж у два рази.

Напрямом подальших досліджень може бути вдосконалення алгоритму роботи системи ДВ, наприклад, шляхом шифрування першого запиту від наземного центру керування. В цьому випадку не маючи правильного ключа, НЛО не зможе навіть визначити вміст запиту, що він отримав.

Список літератури

1. Rudinskas D., Goraj Z., Stankūnas J. Security Analysis Of UAV Radio Communication System. *Aviation*. 2009. **13** (4). P. 116–121. https://doi.org/10.3846/1648-7788.2009.13.116-121
2. Огурцов М.І. Розробка протоколу захищеного обміну даними для спеціальних мереж. *Математичне та комп'ютерне моделювання. Серія: Технічні науки: зб. наук. праць*. Кам'янець-Подільський національний університет ім. Івана Огієнка, 2019. **19**. С. 108–113. https://doi.org/10.32626/2308-5916.2019-19.108-113
3. ДСТУ 4550:2006. Система державного впізнавання об'єктів. Впізнавання радіолокаційне. Терміни та визначення понять. [Чинний від 2007-08-01]. Вид. офіц. Київ : Держспоживстандарт України, 2007. 21 с.
4. Заболоцький В. Цифровий вимір ЗСУ. За яких умов це можливо? URL: http://opk.com.ua/цифровий-вимір-зсу-за-яких-умов-це-можл/ (дата звернення: 06.08.2020)
5. Ермак С.Н., Касанин О.А., Хожевец С.Н. Устройство и эксплуатация наземных средств системы государственного опознавания. Минск: БГУИР, 2017. 230 с.
6. STANAG 4193. Technical Characteristics Of The IFF Mk XIIA System. NATO, 2016. p. 45.
7. Канащенков А.И., Меркулов В.И. Радиолокационные системы многофункциональных самолетов. М.: Радиотехника, 2006. 656 с.
8. Королев В.Ю., Полиновский В.В. Комбинаторная модель украинского ключа-аутентификатора и считывателя. *Управляющие системы и машины*. 2013. **3** (245). С. 61–80. http://nbuv.gov.ua/UJRN/USM_2013_3_8
9. Корольов В.Ю., Поліновський В.В., Ходзінський О.М. Математична модель українського ключа-автентифікатора. *Компьютерная математика*. 2013. **2**. С. 12–23. http://nbuv.gov.ua/UJRN/Koma_2013_2_3
10. Корольов В.Ю., Ходзінський О.М. Розв'язування задач комбінаторної оптимізації на квантових комп'ютерах. *Кібернетика і комп'ютерні технології*. 2020. **2**. С. 5–13. https://doi.org/10.34229/2707-451X.20.2.1
11. Commercial National Security Algorithm Suit and Quantum Computing FAQ. Assurance Directorate. National Security Agency / Central Security Agency. MFQ U / OO / 815099-15 January 2016. URL: https://cryptome.org/2016/01/CNSA-Suite-and-Quantum-Computing-FAQ.pdf (дата звернення: 06.08.2020)
12. IBM Achieves Highest Quantum Volume to Date, Establishes Roadmap for Reaching Quantum Advantage URL: https://newsroom.ibm.com/2019-03-04-IBM-Achieves-Highest-Quantum-Volume-to-Date-Establishes-Roadmap-for-Reaching-Quantum-Advantage (дата звернення: 06.08.2020)
13. Grimes R.A. Cryptography Apocalypse. Preparing for the Day When Quantum Computing Breaks Today's Crypto. John Wiley & Sons, Hoboken. 2020. p. 272. https://doi.org/10.1002/9781119618232
14. Grover-Lenstra elliptic-curve factorization method. URL: https://cr.yp.to/papers/pqrsa-20170419.pdf (дата звернення: 06.08.2020)
15. Faugère J.C., Joux A. Algebraic Cryptanalysis of Hidden Field Equation Cryptosystems Using Gröbner Bases. *Advances in Cryptology. CRYPTO 2003*. Berlin: Springer, 2003. P. 44–60. https://doi.org/10.1007/978-3-540-45146-4_3

16. List of quantum processors. URL: https://en.wikipedia.org/wiki/List_of_quantum_processors (дата звернення: 06.08.2020)
17. Wang Y., Li Y., Yin Z. *et al.* 16-qubit IBM universal quantum computer can be fully entangled. *npj Quantum Inf.* 2018. **4 (**46). https://doi.org/10.1038/s41534-018-0095-x
18. IBM-Q - Online Quantum Computing Platform. URL: https://digital.csic.es/bitstream/10261/212957/1/IBM-Q.pdf (дата звернення: 06.08.2020)
19. Bhupesh B. Quantum-Computation and Applications. URL: https://arxiv.org/abs/2006.02799 (дата звернення: 06.08.2020)
20. Andriyash E., Bian Z., Chudak F., Drew-Brook M., King A.D., Macready W.G. Technical Report. Boosting integer factoring performance via quantum annealing offsets. 2016. URL: https://www.dwavesys.com/sites/default/files/14-1002A_B_tr_Boosting_integer_factorization_via_quantum_annealing_offsets.pdf (дата звернення: 06.08.2020)
21. Anschuetz E., Olson J., Aspuru-Guzik A., Cao Y. Variational Quantum Factoring. *Quantum Technology and Optimization Problems. Lecture Notes in Computer Science*. Vol. 11413. March 18, Springer: Munich, 2019. P. 74–85. https://doi.org/10.1007/978-3-030-14082-3_7

Одержано 02.09.2020

Корольов В'ячеслав Юрійович,
кандидат технічних наук, старший науковий співробітник
Інституту кібернетики імені В.М. Глушкова НАН України, Київ,
https://orcid.org/0000-0003-1143-5846

Огурцов Максим Ігоревич,
науковий співробітник Інституту кібернетики імені В.М. Глушкова НАН України, Київ,
https://orcid.org/0000-0002-6167-5111

Ходзінський Олександр Миколайович,
кандидат фізико-математичних наук, старший науковий співробітник
Інституту кібернетики імені В.М. Глушкова НАН України, Київ.
okhodz@gmail.com

УДК 004.056

В.Ю. Королев, М.И. Огурцов, А.Н. Ходзинский

Многоуровневое государственное опознавание объектов и анализ применимости пост-квантовых криптографических алгоритмов для защиты информации

Институт кибернетики имени В.М. Глушкова НАН Украины, Киев
Переписка: okhodz@gmail.com

Введение. Широкое применение беспилотных аппаратов в гражданской и военной сферах требует разработки новых алгоритмов государственного опознавания объектов по принципу «свой-чужой», поскольку используемые в Вооруженных Силах Украины (ВСУ) устройства системы «Пароль» рассчитаны на опознавание до 110 единиц объектов военной техники. Системы автоматизации ВСУ позволяют использовать дополнительные источники информации о различных объектах, получаемые через гражданские или специальные сети передачи данных, которые могут быть основой для построения объединенной в сеть многоуровневой системы государственного опознавания. Прогнозы развития квантовых компьютеров предрекают возможность взлома современных алгоритмов защиты информации за полиномиальное время в ближайшие 5 – 10 лет, что требует разработки и внедрения новых алгоритмов шифрования и пересмотра параметров современных.

Цель работы заключается в разработке нового алгоритма государственного опознавания объектов, который предоставляет возможность масштабирования системы для обработки нужного количества пилотируемых и беспилотных аппаратов. Также исследовались потенциальные угрозы для классических алгоритмов криптографической защиты сетей передачи данных, которые повлечет выполнение алгоритмов типа Гровера и Шора на квантовых компьютерах.

Результаты. Предложен новый многоуровневый алгоритм государственного опознавания на базе современных криптографических методов защиты информации, позволяющий выполнять надежную автоматизированную идентификацию объектов, масштабировать системы с помощью данных о потенциальных целях из других источников через защищенные специальные сети. Алгоритм поиска Гровера не дает сильного прироста в производительности поиска ключей для алгоритмов симметричного шифрования, поэтому нет необходимости увеличивать длины ключей для этого типа алгоритмов защиты информации. Пост-квантовые алгоритмы асимметричного шифрования требуют дополнительного изучения и всестороннего тестирования защиты информации или увеличение длин ключей классических криптографических алгоритмов, которое соответствует количеству кубитов, то есть не менее чем в два раза. Наиболее перспективным является семейства асимметричных пост-квантовых криптографических алгоритмов основанных на суперсингулярных изогенных эллиптических кривых.

Выводы. Разработан алгоритм государственного опознавания объектов более защищен сравнительно с существующими методами и ориентирован на использование современных бортовых компьютеров и программируемых радиомодемов. Алгоритм Шора и подобные станут существенной угрозой для современных алгоритмов асимметричной криптографии когда количество кубитов квантовых компьютеров будет превышать количество битов в публичных ключах больше чем в два раза.

Ключевые слова: государственное опознавание, симметричное шифрование, асимметричная криптография, квантовый компьютер, пост-квантовая криптография.

UDC 004.056

V. Korolyov, M. Ogurtsov, A. Khodzinsky

Multilevel Identification Friend or Foe of Objects and Analysis of the Applicability of Post-Quantum Cryptographic Algorithms for Information Security

V.M. Glushkov Institute of Cybernetics of the NAS of Ukraine, Kyiv
Correspondence: okhodz@gmail.com

Introduction. Widespread use of unmanned aerial vehicles in the civilian and military spheres requires the development of new algorithms for identification friend or foe of targets, as used in the Armed Forces of Ukraine (AFU) devices of the "Parol" system are designed to service approximately 110 objects military equipment. AFU automation systems allow the use of additional sources of information about various objects from civil or special data transmission networks, which can be the basis for building a networked multi-level system of state recognition. Predictions of the development of quantum computers foresee the possibility of breaking modern algorithms for information security in polynomial time in the next 5-10 years, which requires the development and implementation of new encryption algorithms and revision of modern parameters.

The purpose of the article is to develop a new algorithm for state recognition of objects, which can be scaled to process the required number of manned and unmanned aerial vehicles. Potential threats to classical cryptographic protection algorithms for data networks, which will result in the execution of algorithms such as Grover and Shore on quantum computers, were also discussed.

Results. The article proposes a new multilevel algorithm of state recognition based on modern cryptographic methods of information protection, which allows to perform reliable automated identification of objects, scale systems using data on potential targets from other sources through secure special networks. Grover's search algorithm does not give a strong increase in key search performance for symmetric encryption algorithms, so there is no need to increase the key lengths for this type of information security algorithms. Post-quantum asymmetric encryption algorithms require additional study and comprehensive testing of information security or increasing the key lengths of cryptographic algorithms, which corresponds to the number of qubits, i.e. more than twice. The most promising is the family of asymmetric post-quantum cryptographic algorithms based on supersingular isogenic elliptic curves.

Conclusions. The developed algorithm of identification friend or foe of objects is more secure compared to existing algorithms and is focused on the use of modern on-board computers and programmable radio modems. Shore's algorithm and the like will be a significant threat to modern asymmetric cryptography algorithms when the number of qubits of quantum computers exceeds the number of bits in public keys more than twice.

Keywords: identification friend or foe, symmetric encryption, asymmetric cryptography, quantum computer, post-quantum cryptography.