УДК 004.056.5

д.т.н. Чевардін В.Є. (ВІТІ)
Шкіцькій В.В. (ВІТІ)
Пономарьов О.А. (ВІТІ)

ПЕРСПЕКТИВИ РОЗВИТКУ КРИПТОГРАФІЧНИХ ГЕНЕРАТОРІВ ПСЕВДОВИПАДКОВИХ ПОСЛІДОВНОСТЕЙ СТІЙКИХ ДО КВАНТОВОГО КРИПТОАНАЛІЗУ

Визначені загрози сучасним криптосистемам з появою квантових комп'ютерів. Представлені основні види перспективних постквантових криптографічних алгоритмів. Представлена класифікація відомих генераторів псевдовипадкових послідовностей. Представлені результати порівняння часу необхідного для квантового та класичного криптоаналізу асиметричних криптосистем. Запропоновано альтернативний шлях розвитку перспективних генераторів псевдовипадкових послідовностей, побудованих на основі ізоморфних перетворень еліптичних кривих.

Чевардин В.Е., Шкицкий В.В., Пономарев А.А. Перспективы развития криптографических генераторов псевдослучайных последовательностей стойких к квантовому криптоанализу. *Определены угрозы современным криптосистемам с появлением квантовых компьютеров. Представлены основные виды перспективных постквантовых криптографических алгоритмов. Представлена классификация известных генераторов псевдослучайных последовательностей. Представлены результаты сравнения времени необходимого для квантового и классического криптоанализа асимметричных криптосистем. Предложен альтернативный путь развития перспективных генераторов псевдослучайных последовательностей, построенных на основе изоморфных преобразований эллиптических кривых.*

V. Chevardin, V. Shkitskii, A. Ponomarev Perspectives of the cryptographic deterministic random bit generators development who resisted to quantum cryptanalysis. *The threats of quantum cryptanalysis for modern crypto algorithms were identified. Main mathematics types which are using for building of postquantum algorithms were shown. Classification of known random bit generators was presented. The results of estimation of quantum and classical cryptanalyzes of asymmetric cryptosystems were presented. The alternative way of development of perspective deterministic random bit generators based on elliptic curves isomorphic transformations was proposed.*

Ключові слова: *генератор псевдовипадкових послідовностей, еліптична крива, ізоморфні перетворення еліптичної кривої, квантовий комп'ютер.*

Постановка проблеми та актуальність дослідження

Криптографія є найважливішим напрямком розвитку всесвітньої науки, що містить в собі багато методів, алгоритмів та криптографічних механізмів, які потребують постійної оцінки їх надійності, стійкості до зламу, можливості реалізації на новітніх зразках телекомунікаційного обладнання, комплексів та систем. Величезна кількість сучасних телекомунікаційних послуг, які не можуть бути реалізовані без використання криптографії, відрізняються вимогами до обчислювальної складності процедур гешування, шифрування, цифрового підпису, генерації ключів, а також до їх криптографічної стійкості.

За останні 10 років, з часу прийняття шифру Rejndal в якості стандарту *AES*, криптографія стала застосовуватись практично в усіх системах: банківських, системах електронного уряду E-Government, електронної торгівлі E-Commerce, системах інтелектуальних будинків, системах екстреної медичної допомоги та інших системах управління або надання телекомунікаційних та інформаційних послуг. Це призвело до залежності надійності та захищеності зазначених систем від криптографічної стійкості та швидкодії класичних криптосистем (геш-функцій, електронного цифрового підпису, методів та алгоритмів симетричного і асиметричного шифрування, схем та алгоритмів генерації та розповсюдження криптографічних ключів). А враховуючи, що створення систем захисту інформації в критичній інфраструктурі є тривалим і повільним процесом, зміна алгоритмічної частини такої системи пов'язана з значними матеріальними та часовими втратами, що робить на певний час систему уразливою до нових криптоаналітичних або інших атак, особливо якщо це стосується алгоритмів генерації криптографічних ключів.

Безумовно, серед усіх складових криптосистем генератори псевдовипадкових послідовностей (ПВП) грають значну роль в забезпеченні стійкості та надійності більшості

сучасних методів криптографічного захисту інформації, тому їх розробці та вдосконаленню приділяють особливу увагу, як для інформаційних систем критичної інфраструктури, так і для програмних додатків не великої ресурсної ємності. Для генерації ключів шифрування широко використовуються алгоритми гешування (*MD5, SHA1, SHA2* та інші), блочно-симетричні шифри (*DES, AES* та інші), асиметричні шифри *RSA*, перетворення на основі на еліптичній кривій. На рис. 1 наведені, як існуючі алгоритми генерації ПВП, так і перспективні варіанти використання існуючих шифрів або геш-функцій для модернізації існуючих стандартизованих алгоритмів генерації ПВП. Наприклад, використання алгоритму ДСТУ 7624:2014 в режимі лічильника може використовуватись в якості генератора ПВП.

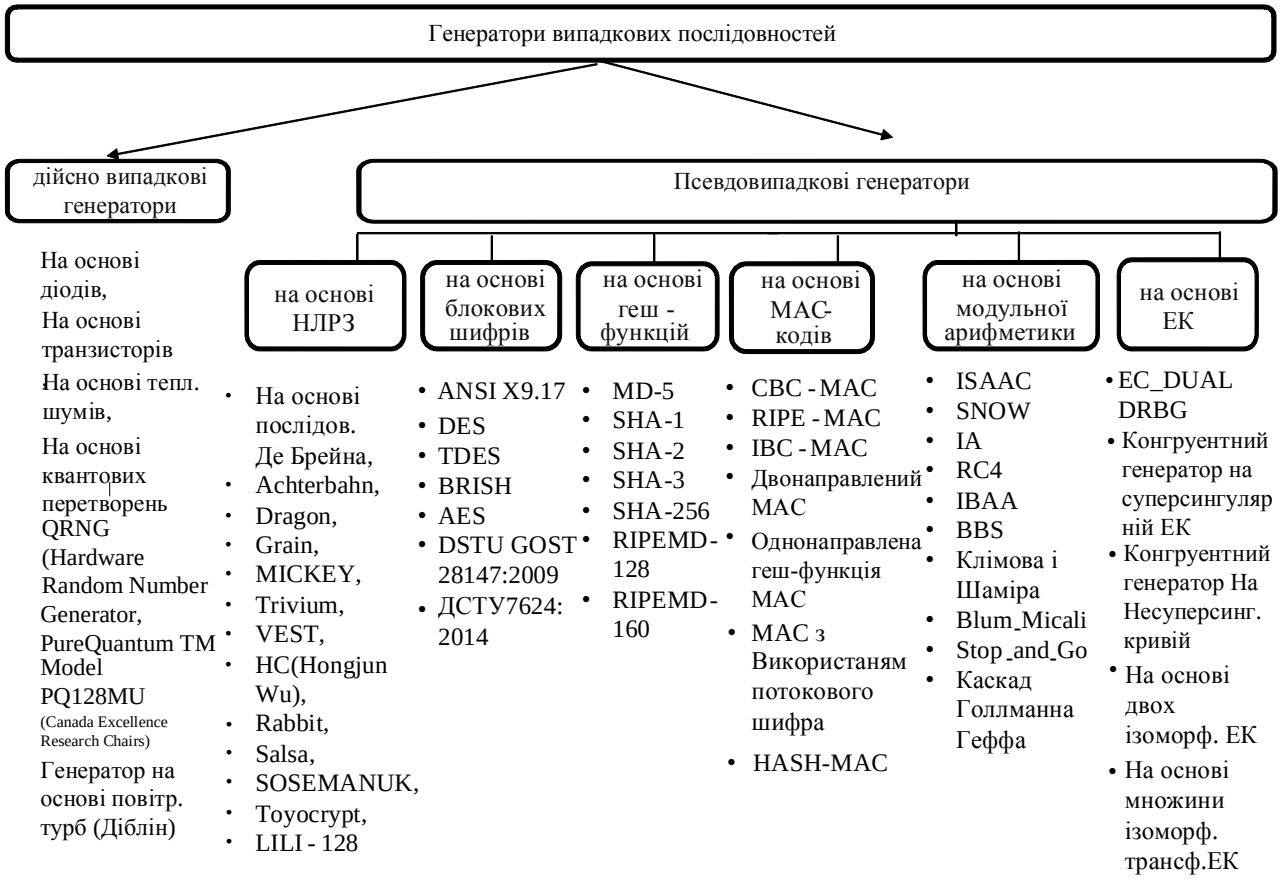

Рис. 1. Відомі схеми побудови генераторів випадкових послідовностей

Поряд з цим, поява перших квантових комп'ютерів, не дивлячись на їх величезну вартість, створила потенційну загрозу існуючим криптоалгоритмам [1, 2]. Отриманий Шором алгоритм [4], на відміну від відомих, таких як алгоритми ρ-Поларда, ρ-Поларда з модифікаціями Брента та Флойда, λ-Поларда, Поліга-Хелмана, MOV-алгоритм, створив потенційну загрозу таким криптографічними алгоритмам, як *RSA, DSA, ECRSA, ECDSA.*

За останніми результатами теоретичних досліджень стверджують, що складність рішення задачі дискретного логарифмування на майбутньому квантовому комп'ютері потужністю 2048 кубітів з реалізованим алгоритмом Шора складе $4{,}3 \cdot 10^9$ операцій, для цієї ж задачі з довжиною модуля 3072 біта складність буде $1{,}16 \cdot 10^{11}$ операцій, коли для класичного комп'ютера складність криптоаналізу еквівалентна $2{,}8 \cdot 10^{26}$ та $5 \cdot 10^{44}$ операцій відповідно. Для квантового комп'ютера, як можна побачити з наведених прикладів, передбачається лінійне зростання складності криптоаналізу в порівнянні з нелінійним зростанням класичного підходу [2].

Наприклад, для дискретного логарифмування в групі точок еліптичних кривих з порядком базової точки 160 бітів складність квантового криптоаналізу складе $1{,}5 \cdot 10^9$ у порівнянні зі складністю 10^{24} операцій класичного алгоритму. Для кривої з порядком базової

точки 256 біт складність квантового криптоаналізу буде $6 \cdot 10^9$, а для класичного алгоритму – $3 \cdot 10^{38}$ операцій. Для кривих з бітовою довжиною порядку базової точки 512 біт складність квантового криптоаналізу складе $4{,}8 \cdot 10^{10}$ операцій, а для класичного алгоритму – 10^{77} операцій.

Слід зауважити, що для такого криптоаналізу відповідні квантові комп'ютери повинні мати 1159, 1834 та 3630 кубітів відповідно. Вартість першого 2000-кубитного квантового комп'ютера *D-Wave 2000Q* склала 15 мільйонів доларів. Згідно прогнозів, висунутих на форумах з квантової криптографії „*Quantum-Safe Cryptography*" у 2013 році та „*Cybersecurity in a Post-Quantum World*" у 2015 році планується до 2030 року створити квантовий комп'ютер з можливістю здійснювати криптоаналіз алгоритмів *AES* (128), *EC* (160), *RSA* (2048) з бюджетом 1 млрд доларів [6].

В зв'язку з цим, за останні п'ять років істотно збільшилось кількість робіт та проектів з розробки нових квантовостійких[1] алгоритмів криптографічного захисту інформації. Одним з таких проектів є *PQCRYPTO* (*Post-quantum cryptography for long-term security*) [7]. За результатами останнього форуму з постквантової криптографії були визначені кандидати для подальших досліджень на стандарт квантовостійкого криптографічного алгоритму, до яких віднесли деякі перспективні алгоритми, які побудовані з використанням одного з наступних підходів:

криптографія на основі решіток (*Lattice-based cryptography*) – цей клас криптосистем лежить в основі повністю гомоморфного шифрування, методів формування кодових конструкцій, шифрування на основі атрибутів. Перевага таких алгоритмів в простоті, можливості розпаралелювання та ефективності реалізації [5];

криптографія на основі кодів (*Code-based cryptography*) – ця криптосистема була запропонована у 1978 році. Перевагою цього класу криптосистем є відсутність способів криптоаналізу. В ході розвитку були запропоновані різні варіанти, частина з яких мала надвеликі розміри ключів шифрування. Так, для алгоритму на основі криптосистеми *McEliece* – 262000/520047 біт, для алгоритму на основі криптосистеми *Niederreiter* – 32750 біт. Вибір цього класу алгоритмів призведе до необхідності переобладнання серверного обладнання, центрів сертифікації та розповсюдження ключів та багатьох протоколів криптографічного захисту інформації. Використання таких ключів в сучасній інфраструктурі відритих ключів суттєво збільшить витрати практично в усіх сферах бізнесу, державному секторі і так далі;

багатоваріантна поліноміальна криптографія (*Multivariate polynomial cryptography*) – ці схеми основані на складності рішення систем багатомірних многочленів над кінцевими полями. За останні десять років було запропоновано багато схем на основі багатоваріантних поліномів, але більшість з них була зламана [5]. За цей час більшу користь багатоваріантна поліноміальна криптографія показала для підписів [7];

підписи на основі геш-функцій (*Hash-based signatures*) – цей клас описує методи формування підписів на основі геш-функцій (наприклад підпис Меркля). Поки ще не відомі алгоритми для ефективного пошуку колізій з використанням квантових комп'ютерів. Недоліком цього класу алгоритмів є необхідність підписувачу вести суворий облік раніше підписаних повідомлень. Будь-яка помилка при цьому призведе до зниження стійкості підписів. Іншим недоліком є те, що підписувач може створювати лише обмежену кількість підписів. Збільшення кількості підписів призведе до збільшення довжини підпису [8]. Геш-алгоритми сьогодні вважаються достатньо стійкими до квантового криптоаналізу, які дозволяють забезпечити вимоги щодо квантової стійкості лише при збільшені довжини геш-коду в два рази з 256 до 512 бітів, що не суттєво впливає на зменшення швидкодії;

криптографія на основі ізогенії еліптичної кривої (*elliptic curve isogeny*) – ці криптоперетворення основані на ізогенії суперсингулярної еліптичної кривої. Перехід від

[1] квантовостійкий алгоритм – зазвичай називають криптографічний алгоритм потенційно стійкий до криптоаналітичних атак з використанням квантового комп'ютера, сьогодні це алгоритм Шора та Гровера.

задач на основі дискретного логарифмування у скінченному полі до задач на основі дискретного логарифмування в групі точок еліптичних кривих став черговим етапом розвитку теоретично стійких криптоалгоритмів.

Постановка завдання досліджень. На відміну від задачі дискретного логарифмування на еліптичній кривій, яка може бути ефективно вирішена алгоритмом Шора на квантовому комп'ютері, задача розв'язання проблеми ізогенії на суперсингулярних кривих, а також інших задач, які використовують множину ізоморфних перетворень еліптичної кривої, сьогодні вважаються перспективною для подальших досліджень [9]. Виникає необхідність порівняння складності задач дискретного логарифмування, аналізу можливостей використання множини ізоморфних трансформацій для підвищення стійкості перетворень в класичних стандартизованих алгоритмах генерації ПВП на еліптичних кривих. Для обґрунтування стійкості на оцінки властивостей ПВП для перспективного класу генераторів доцільно використовувати аналітичні оцінки, отримані в роботі [10], які вказують на розмір множини ізоморфних трансформацій еліптичної кривої приблизно рівний порядку p скінченного поля. Це забезпечить достатній запас для забезпечення квантової стійкості.

2. Визначення структури та вимог до квантовостійкого алгоритму генерації криптографічної псевдовипадкової послідовності

Розглянемо сутність підходів до побудови генераторів псевдовипадкових послідовностей не основі еліптичних кривих.

Відповідно сучасним стандартам з криптографічного захисту інформації використовують рівні безпеки, що відповідають довжині ентропійного значення 128, 192, 256 біт відповідно [8]. Наприклад, рівень безпеки з довжиною ентропійного значення 256 біт забезпечує складність зламу криптографічного алгоритму 10^{77} операцій. Цей рівень для криптосистем на основі дискретного логарифмування в групі точок еліптичної кривої потребує використання довжини ключа не менше 512 бітів, а для криптосистем на основі дискретного логарифмування в простому полі не менше 15360 біт.

З відомих класів криптосистем, а саме – безумовно стійкі або теоретично недешифровані, обчислювально стійкі та імовірно (теоретично) стійкі найбільш безпечними є безумовно стійкі криптосистеми, які забезпечують умову $t_б \to \infty$, тобто безпечний час криптосистеми необмежений. Однак складність реалізації такої криптосистеми не дозволяє їх використовувати на практиці. В зв'язку з цим, на практиці використовують імовірно стійкі та обчислювально стійкі шифри, які забезпечують умову $t_б >> t_{ці}$, де $t_{ці}$ – час, який інформація представляє цінність.

Усі блокові алгоритми шифрування, гешування та інші подібні алгоритми прийнято вважати обчислювально стійкими. На відміну від обчислювально стійких криптосистем для теоретично стійких оцінка криптографічної стійкості основана на зведенні задачі зламу криптосистеми до рішення відомої усім математичної задачі. Згідно з гіпотезою вважається, що певна функція є односпрямованою. Наведемо визначення.

Визначення 1. Односпрямована функція – це ефективно обчислювальна функція, для знаходження вхідного значення якої на основі вихідного значення функції не існує ефективних алгоритмів.

Визначення 2. Якщо існує поліноміальний алгоритм, який обчислює для кожного x свою $f(x)$, та якщо імовірністю визначення будь-якою поліноміальною імовірнісною машиною Т'юринга А значення x за відомим $f(x)$ можна знехтувати, тоді поліноміальна $f(x)$ функція називається односпрямованою [11].

Наприклад, гіпотеза існування класу NP-повних задач математики. Класифікація відомих теоретичних задач, які були використані різними вченими для побудови односпрямованих функцій, представлена на рис. 2.

В роботах [12 – 14] були обґрунтовані оцінки стійкості та якості криптографічних генераторів ПВП. Існує багато результатів щодо розробки нових методів та алгоритмів

генерації ПВП за останні десятиріччя. Особливе місце серед усіх генераторів ПВП сьогодні посіли генератори на еліптичних кривих. Тому оцінка криптографічної стійкості цього класу генераторів ПВП та збільшення їх стійкості стали основним етапом для подальшого розвитку й вибору нових математичних задач (рис. 2).

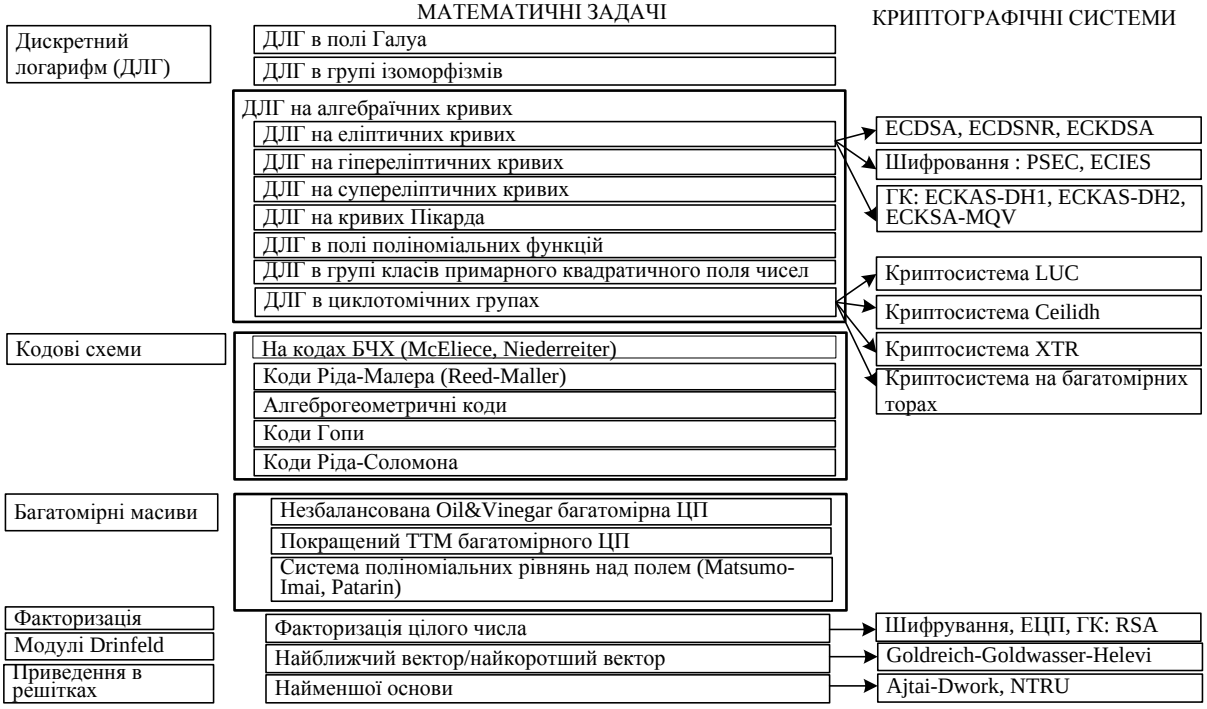

Рис. 2. Класифікація теоретико-складнісних задач математики

Для обґрунтування стійкості криптоперетворень над групою точок еліптичних кривих використовують метод ρ-Поларда, складність якого визначається виразом (1):

$$I_{EC} = \sqrt{\frac{\pi n}{4}}, \tag{1}$$

де n – порядок циклічної підгрупи точок еліптичної кривої.

Так, для вирішення задачі дискретного логарифмування у групі точок еліптичної кривої над двійковим полем з розширенням поля P-163 метод ρ-Поларда потребує $2^{81,5}$ операцій ($2{,}42*10^{24}$ *MIPS*[2]), для кривої P-192 – $2^{95,5}$ операцій ($5{,}6*10^{28}$ *MIPS*), для кривої B-256 – $2^{127,5}$ операцій ($2{,}41*10^{38}$ *MIPS*).

З появою квантового комп'ютера, а точніше з появою квантового алгоритму Шора для асиметричних криптосистем, складність криптоаналізу стали визначати виразом (2):

$$I_{Shor} = O(\log^2 N \log^3(\log N)), \tag{2}$$

де $N = 2^n$ число станів, які представлені як n-бітова строка, яке необхідно розкласти на співмножники, з використанням $O(\log N)$ логічних кубітів.

Так, час для рішення задачі *ECDLP* з використанням алгоритму Шора складає для P163 – $1{,}6*10^9$, для P256 – $6.0*10^9$, для P512 – $50*10^9$ сек.

Наведемо математичну модель генератора ПВП на еліптичних кривих.

Для побудови генератору використовується еліптична крива E_p затверджена стандартом [14]. Властивості генератора досліджені в роботі [13].

2 MIPS – одиниця виміру швидкодії, яка дорівнює одному мільйону інструкцій за секунду.

Нехай криптографічний генератор ПВП (*Dual_EC_DRBG*) створює послідовність внутрішніх станів генератора, яку можна представити еквівалентною послідовністю точок кривої. На кожній ітерації генератор *Dual_EC_DRBG* обчислює чергову точку кривої, а на виході генератора створюється блок b_i , який обчислюється за допомогою виразу (3):

$$b_i = extr\left[t_i * Q\right] = extr\left[(\psi(t_{i-1} * P) * Q)\right], \tag{3}$$

де $\psi(P) = X_P \bmod n$,

$t_0 = HDF(seed, nonce, ID)$,

n – порядок циклічної підгрупи точок.

Послідовність внутрішніх станів генератора $\{t_1, ..., t_{\upsilon-1}\}$ утворюється за правилом (4):

$$t_i = \psi(P_i) = \psi(\psi(t_{i-1} * P) * P), \tag{4}$$

де $i = (\overline{1, \upsilon})$, $\upsilon \le n$, P – базова точка кривої.

Вважається, що послідовність (4) є випадковою, тому що створена на основі випадкового (секретного) значення *seed*. Але, як показали дослідження [10], ця послідовність стає детермінованою після першого зациклення генератора.

Примітка. Число різних значень (координат точок кривої) на виході другого скалярного множення в виразі (3) дорівнює числу внутрішніх станів генератора. Послідовність виходів другого скалярного множення також залежить від послідовності $\{t_1, ..., t_{\upsilon-1}\}$ і не впливає на порядок слідування внутрішніх станів та їх число. В більшості сучасних робіт, стосовно побудови генераторів на еліптичних кривих, період такого генератора вважається близьким до кількості n його внутрішніх станів, тобто порядку циклічної підгрупи. Однак ця границя не є точною, у зв'язку з існуванням для цього типу перетворення зациклень з малим періодом, що було детально досліджено в роботі [15].

Існують різні бібліотеки реалізації операцій над скінченними полями, в групі точок еліптичних кривих, а також які реалізують повністю криптографічні алгоритми. Наприклад, бібліотека lib4145 (що реалізує ГОСТ 28147-89, ГОСТ 34.311-95, ДСТУ 4145-2002), бібліотека криптографічних функцій "Цезаріс-Крипто" (що реалізує ГОСТ 28147-89, ГОСТ 343.311-95, ГОСТ 34.310-95, ДСТУ 4145-2002, ДСТУ *ISO/IEC* 10118-3:2005, ISO/IEC 18033-3), бібліотека *Algebraic Abstractions Library* (*AAL*), бібліотека *Bee2* (що реалізує СТБ 34.101.31, 34.101.45, 34.101.47, 34.101.60, 34.101.66), бібліотеки *Crypto++*, *OpenSSL*, *CryptLib (Sleepycat)*, *MIRACLE*, *GNU Crypto*, *Botan*. Під час досліджень для реалізації операцій над точками еліптичних кривих використовувалась бібліотека програмних функцій *MIRACLE*, за причиною її відкритості, постійним оновленням та підтримкою розробниками актуальних криптоалгоритмів та нових криптографічних функцій. З використанням бібліотеки *MIRACLE* були реалізовані наведені відомі структури генераторів ПВП та досліджена їх статистична безпека.

3. Один з підходів до генерації квантовостійких ПВП

Для захисту від квантового криптоаналізу необхідно ввести додаткові ізоморфні перетворення для базового стандартизованого алгоритму генерації внутрішніх станів генератора (3). Для цього зафіксуємо наступні параметри.

Нехай, $RI \subset F_p$ – ціле число, де довжина характеристики поля $l_p = \{256, 384, 512\}$. Значення *RI* показує число секретних ізоморфних параметрів, які згідно запропонованого методу генерації створюються функцією *reseed*. Як було показано раніше, функція *HDF*, на основі якої працює *reseed*, побудована з використанням алгоритму *SHA256/512*. Алгоритм гешування *SHA256/512*, за прогнозами експертів для захисту від квантового криптоаналізу

потребує лише подвоєння довжини геш-кодів або криптографічних ключів у випадку використання блокових алгоритмів шифрування.

Нехай задані: базова еліптична крива E, точка $P(X_P, Y_P) \in E_{F_{2^m}}$ та початкові параметри ізоморфного перетворення (i_{fin}). На кожній ітерації точка P трансформується в ізоморфну точку $P_{\varphi i} = \varphi_{ui}(P)$. За допомогою скалярного множення на кожній ітерації отримується точка $P_i = t_i * P_{\varphi_i}$, де $t_i = f(t_{i-1})$, $t_0 = HDF(seed, Nonce, ID)$. Враховуючи ізоморфізм груп точок кривих, не має різниці яку спочатку операцію виконувати, скалярне множення або ізоморфну трансформацію. Після отримання координати $X_i = X[P_i] = X[t_i * P_{\phi_i}]$, на основі результату скалярного множення відокремлюється частина біт координати точки кривої, яка стає черговим блоком вихідним $b_i = extr(X(P_i))$. Алгоритм генерації ПВП можна навести наступними кроками:

Крок 1. Генерується секретний *seed.*

Крок 2. Генеруються початкові значення t_0, u_0.

Крок 3. Початок $for(i = 0, i < i_{fin}, i++)$.

Крок 3.1. Обчислюється $t_i = \psi(t_{i-1} * P)$.

Крок 3.2. Обчислюється $u_i = (u_{i-1} + \tilde{u}) \bmod p$.

Крок 3.3. Обчислюється точка ізоморфної кривої: $\varphi_{u_i}(P_i)$.

Крок 3.4. Обчислюється $s_i = \psi(\varphi_{u_i}(P_i))$.

Крок 3.5. Обчислюється $Q_i = s_i * Q$.

Крок 3.6. Обчислюється $r_i = \psi(Q_i)$.

Крок 3.7. Обчислюється $b_i = extr(r_i)$.

Крок 3.8. Вивід b_i.

Крок 3.9. Кінець циклу.

Крок 4. Видалення з оперативної пам’яті змінних.

Кінець.

Математична модель генератора можна представити виразом (5):

$$b_i = extr\left[\psi(\varphi(\psi(t_{i-1} * P))\right]. \qquad (5)$$

де P – точка еліптичної кривої над F_{2^m},

$$\varphi = \begin{cases} X_{P'} = X_P, \\ Y_{P'} = Y_P + kX_{P'}, k^2 + k + a_1 = a_2. \end{cases}$$

Нехай значення секретного параметру ізоморфного перетворення u_{01} створюється за допомогою функції *HDF* (*Nonce1*, *Entropy*, *ID*). Значення другого секретного параметру ізоморфного перетворення u_{02} створюється за допомогою функції *HDF* (*Nonce2*, *Entropy*, *ID*). Тоді існує два результати генерації внутрішнього стану: $\psi(\varphi_{u_{01}}(\psi(t_{i-1} * P))$ та $\psi(\varphi_{u_{02}}(\psi(t_{i-1} * P))$, які створюють дві послідовності координат точок від двох ізоморфних кривих. Вони пов’язані одна з одною через секретний параметр u, який розраховується через функцію *HDF*, побудовану на основі геш-функції.

Якщо для відтворення першої послідовності точок криптоаналітик може використовувати алгоритм Шора (один потік), то для відтворення другої послідовності значень він знову буде вимушений застосовувати алгоритм Шора (другий потік), або мати відповідну потужність для запуску двох паралельних процесів, які працюють за алгоритмом

Шора. Або використовувати додаткові алгоритми криптоаналізу для відтворення секретних параметрів ізоморфної трансформації. Використання декількох ізоморфних кривих дозволяє змінювати число *RI* параметрів ізоморфної трансформації u_{0RI} на основі функції *HDF* (*NonceRI, Entropy, ID*). Число *RI* можна змінювати в залежності від необхідного для певної системи рівня стійкості.

Порівняємо запропонований спосіб побудови генераторів ПВП з іншими. Наприклад, для криптосистемами *McEliece* необхідно використовувати ключ довжиною 262000 біт, а для криптосистеми *Niederreiter* 32750 біт. Для розробленого методу на основі секретних ізоморфних перетворень над скінченним полем з довжиною характеристики поля 512 біт можна використати значення *RI* довжиною 512 біт для генерації секретних ізоморфних трансформацій, отриманих різними функціями *HDF* (*NonceRI, Entropy, ID*). Це збільшить довжину ключа стандартизованого генератора в два рази, тобто дорівнюватиме 1024 біти, але при цьому зробить алгоритм стійким до квантових атак. Реалізація запропонованого алгоритму на основі бібліотеки *MIRACLE* потребує невеликого додаткового об'єму пам'яті для здійснення додаткових ізоморфних перетворень у порівнянні зі стандартизованим алгоритмом.

Висновки

Таким чином, при широкому розповсюдженні квантових комп'ютерів рішення задачі *ECDLP* буде можливо вирішено. Так, для дискретного логарифмування в групі точок еліптичних кривих з порядком базової точки 160 бітів складність квантового криптоаналізу складе $1{,}5 \cdot 10^9$ у порівнянні зі складністю 10^{24} операцій класичного алгоритму. Для кривої з порядком базової точки 256 біт складність квантового криптоаналізу складе $6 \cdot 10^9$, при цьому для класичного алгоритму – $3 \cdot 10^{38}$ операцій. Для кривих з бітовою довжиною базової точки 512 біт складність квантового криптоаналізу складе $4{,}8 \cdot 10^{10}$ операцій, а для класичного алгоритму – 10^{77} операцій. Це створює суттєву проблему використання криптографічних алгоритмів цього класу в майбутньому. З іншого боку, слід врахувати, що однією з проблем використання квантового комп'ютеру є проведення аналізу та вимірів різних квантових станів, що накладає суттєві обмеження на квантову криптоаналітичну систему. Але якщо це питання буде вирішено, сумнівів щодо появи реального квантового комп'ютеру, який вирішить задачу ECDLP не залишиться.

В зв'язку з цим, в результаті проведеної роботи були визначені перспективні шляхи подальшого розвитку криптографічних методів захисту інформації, в тому числі і методів генерації криптографічних ПВП. В результаті досліджень були визначені основні математичні конструкції, які стали основою для побудови алгоритмів – кандидатів на постквантовий алгоритм, а саме: кодові конструкції, алгебраїчні решітки, геш-функції. Практично усі з цих конструкцій мають переваги та суттєві недоліки. Було проведено пошук нових шляхів підвищення криптографічної стійкості існуючих та діючих на практиці криптографічних алгоритмів та систем. Аналіз відомих робіт та наукових результатів дозволили визначити перспективність використання ізоморфних трансформацій еліптичної кривої для побудови потенційно квантовостійких криптографічних алгоритмів. Слід зазначити, що прототип цих операцій ліг в основу одного з претендентів на постквантовий алгоритм, це конструкції на основі ізогенії еліптичної кривої.

В ході роботи було запропоновано використовувати ізоморфні перетворення еліптичної кривої з секретним параметром для побудови нових методів генерації ПВП. Це відкриває нові шляхи щодо розвитку квантовостійких алгоритмів за рахунок використання секретної генерації параметрів ізоморфної трансформації еліптичних кривих. Було показано можливість збільшити число внутрішніх станів стандартизованого генератора на еліптичних кривих у $1/2(p\text{-}1)$ разів за рахунок використання ізоморфних трансформацій кривої. Це дозволило підвищити стійкість генератора ПВП пропорційна характеристиці поля p. При фіксованому значенні числа внутрішніх станів стандартизованого генератора розроблений генератор дозволив скоротити бітову довжину характеристики p поля та підвищити його швидкодію. В подальшому, підхід до використання ізоморфних перетворень може бути

застосований для побудови алгоритмів генерації криптографічних ключів в легковагової криптографії, в криптографічних системах захисту інформації критичної інфраструктури.

В якості напрямків подальших досліджень необхідно визначити: аналіз криптографічної стійкості ізогенії еліптичної кривої, ізоморфних перетворень еліптичної кривої та інших перетворень, які були визначені як перспективні для побудови квантовостійких алгоритмів, програмна реалізація та дослідження запропонованих алгоритмів з урахуванням останніх результатів, таких як, розроблена у 2016 році компанією Microsoft бібліотека SIDH (Supersingular Isogeny Key Exchange) на мові C (Microsoft Visual Studio-Windows+LNU GCC+clang ОС Linux) з відкритим вихідним кодом. В цієї бібліотеці використовуються криві в формі Монтгомері, які захищені від атак за часом.

ЛІТЕРАТУРА

1. Thurimella R. Cryptography for Cyber Security and Defense: Information Encryption and Cyphering / R. Thurimella and L. C. Baird III // IGI Global, 2009, chapter title: „Network Security”.

2. Богданов А.Ю. Квантовые алгоритмы и их влияние на безопасность современных классических криптографических систем / Богданов А.Ю. Кижватов И.С // РГГУ ФЗИ (2005) – С. 18.

3. Shor P. W. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer / Shor P. W. // Foundations of Computer Science : Conference Publications. – 1997. – P. 1484 – 1509.

4. Barak B. On the (Im)possibility of obfuscating.programs / Barak B., Goldreich O., Impagliazzo R., Rudich S., Sahai A.,.Vedhan S., Yang K. // CRYPTO’01 – Advances in Cryptology, Lecture Notes in.Computer Science, v. 2139, 2001, p. 1 – 18.

5. Hoffstein J. NTRU: A ringbased public key cryptosystem / J. Hoffstein, J. Pipher, J. H. Silverman // In buhler, pp. 267 – 288.

6. http://www.etsi.org/images/files/ETSIWhitePapers/QuantumSafeWhitepaper.pdf.

7. https://www.iso.org/organization/5984715.html.

8. NIST SP 800-57 part 1. Recommendation for Key Management, Part 1. https://csrc.nist.gov/publications/detail/sp/800-57-part-1/revised/archive/2007-03-01.

9. Хопкрофт Д. Введение в теорию автоматов, языков и вичислений / Д. Хопкрофт, Р.Мотвани, Дж.Ульман // М.: „Вильямс”, 2002. – 528 с.

10. Чевардин В. Е. Изоморфные трансформации эллиптической кривой над конечным полем / Чевардин В. Е. // Международный научно-теоретический журнал „Кибернетика и системный анализ”. 2013. Том 49, № 3. С. 168 – 171.

11. Kaliski Jr. B. S. A pseudo-random bit generator based on elliptic logarithms / B. S. Kaliski Jr. // Advances in Cryptology: Proceedings of Crypto '86 (Lecture Notes in Computer Science, vol. 263), Springer-Verlag, New York, 1987, pp. 84 – 103.

12. Impagliazzo R. Pseudo-random generation from one-way functions / R. Impagliazzo, L. Levin, and M. Luby // Proceedings of the 21st Annual ACM Symposium on Theory of Computing, ACM, New York, 1989, pp. 12 – 24.

13. Gjøsteen K. Comments on Dual-EC-DRBG/NIST SP 800-90, Draft December 2005 / Kristian Gjøsteen // March 16, 2006.

14. NIST Special Publication 800-90A. Recommendation for Random Number Generation Using Deterministic Random Bit Generators / Elaine Barker, John Kelsey // Computer Security Division Information Technology Laboratory National Institute of Standards and Technology. – January 2012.

15. Чевардін В.Є. Аналітичні оцінки зациклень генераторів псевдовипадкових послідовностей на еліптичних кривих / Чевардін В.Є., Ковальчук Л. В. // Науково-технічний журнал „Радиотехника”. ХНУРЕ. Харків. 2015. №183. С. 150 – 160.