УДК 003.026:004.056 **DOI:10.30837/rt.2021.4.207.05**

О.Є. ПЕТРЕНКО, канд. техн. наук, О.С. ПЕТРЕНКО, канд. техн. наук,
О.В. СЄВЄРІНОВ, канд. техн. наук, О.І. ФЄДЮШИН, канд. техн. наук,
А.В. ЗУБРИЧ, Д.В. ЩЕРБИНА

АНАЛІЗ ШЛЯХІВ ПІДВИЩЕННЯ СТІЙКОСТІ КРИПТОАЛГОРИТМІВ НА АЛГЕБРАЇЧНИХ РЕШІТКАХ ЩОДО ЧАСОВИХ АТАК

Вступ

Запропонований у 1994 році алгоритм Шора довів можливість факторизації числа за допомогою квантового комп'ютера з достатньою кількістю кубітів за поліноміальний час. Вказаний факт ставить під сумнів можливість застосування асиметричних криптосистем, таких як RSA. Поширене використання алгоритму в багатьох криптографічних додатках обумовило необхідність пошуку альтернативних крипостійких алгоритмів. З 2016 року Національний інститут стандартизації та технологій об'явив конкурс на вибір алгоритмів стійких до атак в постквантовий період. Результати конкурсного відбору будуть представлені у 2022 році. В теперішній час розроблено алгоритми NTRUEncrypt, NTRUSign, Falcon [1, 2], стійкість яких обумовлена складністю розв'язання задачі пошуку короткого вектору алгебраїчної решітки. Проблемним питанням при застосуванні алгоритмів є той факт, що вони ще мало досліджені, використовують обмежене коло параметрів, для яких була доведена крипостійкість до відомих атак. Алгоритми Falcon, NTRUEncrypt увійшли у другий тур конкурсу NIST та знаходяться на стадії ретельного вивчення. Запропоноване коло параметрів придатних до застосування унеможливлює поширене використання вказаних алгоритмів та не може зробити їх універсальним для вирішення широкого кола завдань в порівнянні з алгоритмом RSA. Дане проблемне питання вимагає подальших досліджень алгоритмів, що застосовують алгебраїчні решітки NTRU з метою розширення кола безпечних до застосування параметрів. Метою статті є дослідження алгоритмів, стійкість яких базується на пошуку короткого вектору решітки, з визначенням параметрів стійких до часових атак.

1. Алгоритми NTRUENCRYPT, NTRUSIGN

NTRUEncrypt – криптосистема з відкритим ключем, також відома як NTRU алгоритм шифрування, він являється решіткою на основі альтернативи RSA і ECC (Elliptic – curve cryptography) і основана на розв'язанні задачі, що пов'язана з пошуком найкоротшого вектору в решітці.

Алгоритм оснований на передбачуваній складності факторизації деяких многочленів із усіченого кільця многочленів в приватні два многочлена з дуже малими коефіцієнтами. Криптоаналіз криптосистеми тісно пов'язаний з алгоритмічною проблемою редукції решітки в певному класі. Для забезпечення криптографічної стійкості необхідним є проведення дослідження, яке дозволяє здійснити ретельний вибір параметрів, стійких до існуючих атак.

Оскільки і шифрування, і дешифрування використовують тільки просте поліноміальне множення, ці операції дуже швидкі в порівнянні з іншими схемами асиметричного шифрування, такими як RSA, ElGamal і криптографія на основі еліптичних кривих. Однак NTRUEncrypt [1] та пов'язаний з ним алгоритм цифрового підпису NTRUSign [2] ще не пройшли такий же обсяг криптографічного аналізу в розгорнутій формі.

Алгоритм NTRU та побудована на його основі асиметрична криптосистема базуються на перетвореннях на алгебраїчних решітках. NTRUEncrypt є ймовірно стійкою системою, тобто для зашифрування повідомлень використовують випадковий елемент. За цієї умови кожне повідомлення має багато шифротекстів. Стійкість криптосистеми NTRUEncrypt визначена експериментальним шляхом та базується на факті складності знаходження короткого вектору алгебраїчної решітки. Перевагою даної системи є факт, що шифрування, розшифрування повідомлення та процес створення ключів є швидким і легким в реалізації.

Алгоритми NTRUEncrypt, NTRUSign залежить від параметрів, які є цілими числами та можуть бути представлені у поліноміальному вигляді. Для того щоб параметри не сприяли виникненню випадкових помилок, при дешифруванні необхідно включати контрольні біти у кожній блок повідомлення.

Для побудови математичної моделі алгоритму використовують наступні параметри:

– N – розмірність кільця поліномів, що використовують при шифруванні повідомлень;

– p – натуральне число, що приймає участь в шифруванні та дешифруванні повідомлення;

– q – натуральне число, що приймає участь в шифруванні, дешифруванні повідомлення та при визначенні відкритого ключа;

– k – таємний ключ від якого залежить стійкість від атак;

– d_i (i=1,2) – розподіли коефіцієнтів многочленів, які застосовуються при формуванні відкритого та таємного ключів.

При генерації ключів розглядають кільце зрізаних поліномів $R = Z[x]/\left(x^N - 1\right)$. Кожний елемент кільця може бути представлений в поліноміальному $f = \sum_{s=0}^{N-1} f_s x^s$ або векторному вигляді $(f_0, f_1, f_2, ..., f_{N-1})$. Усі коефіцієнти полінома є цілими числами. Зменшити складність обчислення операції множення поліномів в кільці зрізаних поліномів можливо за рахунок застосування операції "згортки" за правилом: нехай необхідно перемножити 2 полінома $f = \sum_{s=0}^{N-1} f_s x^s$ та $g = \sum_{s=0}^{N-1} g_s x^s$ в кільці зрізаних поліномів $R = Z[x]/\left(x^N - 1\right)$. Результатом множення $h = f \otimes g$ є поліном виду: $h = \sum_{s=0}^{N-1} h_s x^s$, коефіцієнти якого обчислюються за формулою: $h_s = \sum_{i=0}^{s} f_i g_{s-i} + \sum_{i=s+1}^{N-1} f_i g_{N+s-i}$.

Дане правило дозволяє зменшити обчислювальну складність множення поліномів в $R = Z[x]/\left(x^N - 1\right)$ шляхом відсутності необхідності приводити по $\mathrm{mod}\left(x^N - 1\right)$ доданки, ступінь яких більше ніж *N*.

Параметри *p* та *q* необов'язково повинні бути простими числами, але обов'язково вони повинні задовольняти умовам: НСД(p, q)=1, параметр p повинен бути значно меншим за *q*. Використовуючи значення *p* та *q* випадково обирають 2 полінома f та g. Поліном f належить кільцю зрізаних поліномів $R = Z[x]/\left(x^N - 1\right)$ з розподілом коефіцієнтів по закону розподілу з параметром d_1. Це означає, що в поліномі f міститься d_1 коефіцієнтів, які дорівнюють 1, d_1 – 1 коефіцієнтів, які дорівнюють -1 та всі інші коефіцієнти дорівнюють 0. Такий розподіл коефіцієнтів обумовлює наявність оберненого полінома до полінома f Поліном g належить кільцю зрізаних поліномів $R = Z[x]/\left(x^N - 1\right)$ з розподілом коефіцієнтів по закону розподілу з параметром d_2. Це означає, що в поліномі g міститься d_2 коефіцієнтів, які дорівнюють 1, d_2 – 1 коефіцієнтів, які дорівнюють -1 та всі інші коефіцієнти дорівнюють 0. Застосовуючи коефіцієнти полінома f будують поліноми $f_p \equiv f(\mathrm{mod}\, p)$, $f_q \equiv f(\mathrm{mod}\, q)$. Отримані поліноми мають обернені поліноми в кільці зрізаних поліномів $R_p = Z_p[x]/\left(x^N - 1\right)$ та $R_q = Z_q[x]/\left(x^N - 1\right)$. Щодо поліномів, які отримані редукцією полінома g по модулю *p* та *q*, то вони не мають обернених поліномів в кільці зрізаних поліномів $R_p = Z_p[x]/\left(x^N - 1\right)$ та $R_q = Z_q[x]/\left(x^N - 1\right)$.

Відкритий ключ обчислюють за правилом: $h \equiv pf_q^{-1} \otimes g (\mathrm{mod}\, q)$. Слід зазначити, що поліном h та числа p та q – є відкритими параметрами, а поліном f та f_q^{-1} – таємними. Для зашифрування повідомлень випадковим чином обирають поліном r, який має розподіл коефіцієнтів d_3 в кільці зрізаних поліномів $R = Z[x]/(x^N - 1)$ та відкритий ключ h. Це означає, що в поліномі h міститься d_3 коефіцієнтів, які дорівнюють 1, d_3 коефіцієнтів, які дорівнюють -1 та всі інші коефіцієнти дорівнюють 0. Повідомлення m шифрується наступним чином: $c \equiv r \otimes h + m (\mathrm{mod}\, q)$. Розшифрування повідомлення здійснюють в два етапи.

Спочатку обчислюють поліном з цілими коефіцієнтами з проміжку $\left(\frac{-q}{2}, \frac{q}{2}\right)$ за формулою $a \equiv f \otimes c (\mathrm{mod}\, q)$. Далі обчислюють $f_q^{-1} \otimes a$.

Вказаний алгоритм шифрування має недолік, який пов'язаний з появою параметрів, що сприяють появі помилок, тому для кожного блоку повідомлення необхідно включати контрольні біти. Причина появи таких помилок полягає в невірному центруванні повідомлення. Позбутися її можливо шляхом обчислення полінома $a \equiv f \otimes c (\mathrm{mod}\, q)$ з цілими коефіцієнтами в проміжку $\left(\frac{-q}{2} + x, \frac{q}{2} + x\right)$ для невеликого значення x від'ємного чи додатного. Якщо даний алгоритм не спрацює, тоді повторюють процедуру шифрування.

Із процедури розшифрування можна дійти до висновку, що криптосистема NTRU являється вірогідною, тому зі зашифрованого тексту відкритий текст не завжди відновлюється правильно. Коректний вибір многочленів f, g, r дозволяє понизити вірогідність такої помилки до 2^{-100}.

2. Аналіз параметрів алгоритмів NTRUENCRYPT, NTRUSIGN.

Криптосистема NTRU володіє декількома перевагами, а саме: велика швидкість роботи і збільшення стійкості при фактично тієї самої довжині ключа, що і в RSA. Із мінусів поки що один – необхідність застосовувати тільки рекомендовані параметри. Саме ця вимога визивала загальну незадоволеність свого часу, коли виникла необхідність перехода на елептичні криві і сприяла усіяким підозрам про наявність лазійок, які полегшували у подальшому конструкторам шифру криптоаналіз. В табл. 1 представлено параметри для алгоритму NTRU, що рекомендовані до використання [3]. Рівномірний розподіл, який застосовується для вибору поліномів f, g ключової пари алгоритму, дозволяє обмежити норму короткого вектору решітки довжиною $2n$. Застосування рівномірного розподілу з точки зору атаки "грубої сили" дає непоганий результат та дозволяє для параметра $n = 503$ обрати коефіцієнти поліному f з 10^{235} варіантів, що в свою чергу зводить імовірність отримати коефіцієнти повним перебором до величини 2^{-705}.

Таблиця 1

Рекомендовані параметри для NTRU

	n	p	q	кількість одиниць в многочленах		
				f	g	r
NTRU 167:3	167	3	128	61	20	18
NTRU 251:3	251	3	128	50	24	16
NTRU 503:3	503	3	256	216	72	55
	n	p	q	кількість одиниць в многочленах		
				f	g	r
NTRU 167:2	167	2	127	45	35	18
NTRU 251:2	251	2	127	35	35	22
NTRU 503:2	503	2	253	155	100	65

Однак алгоритм NTRU має обмежене число параметрів, придатних до застосування в криптоперетвореннях, що повязано з вразливістю даного алгоритму до часових атак [4]. Згідно з вимогами конкурсу, який був оголошений Національним інститутом стандартизації та технологій США (NIST), на кращі асиметричні алгоритми шифрування та генерації цифрових підписів, було запропоновано розробити криптоалгоритми, які будуть стійкими крім стандартного набору атак до атак по бічних каналах та часових атак. При прийнятті рішень щодо стандартизації алгоритмів Національний інститут стандартизації та технологій спирається на доказ стійкості запропонованих параметрів, а також розробку та тестування контрзаходів для розширених атак по бічних каналах та часових атак. Алгоритм NTRU пройшов до другого туру конкурсу та все ще розглядається як альтернативний варіант для стандартизації. Одним з проблемних питань алгоритму NTRU є питання, що обумовлені обмеженим числом стійких до криптоаналізу параметрів та нестійкістю алгоритму до часових атак. Її сутність полягає в тому, що зловмисник може посилати довільно зашифровані тексти $c(x)$ одержувачу, такі що коефіцієнти $a(x)$ повністю залежить від секретного ключа $f(x)$. Витік в такому випадку відбувається до того, як буде перевірено дійсність $c(x)$. Тому, час виконання кроку дешифрування залежить від цих коефіцієнтів. Зловмисник може використати це, ретельно вимірявши, скільки часу займає операція дешифрування, і зробивши висновок з цього про значення коефіцієнтів секретного ключа.

Для усіх криптографічних конструкцій, які використовують алгебраїчні решітки, необхідним є генерація стійкого відкритого базису випадкової решітки. У таких криптографічних конструкціях можливо використати функцію з потаємним входом. Покращити криптографічну стійкість алгоритму до часових атак та атак по бічних каналах можливо шляхом використання для алгоритму NTRU дискретного нормального (Гаусівського) розподілу для генерації поліномів f, g, де в якості потаємного входу виступає середнє квадратичне відхилення нормального (Гаусівського) закону розподілу. Вибір середнєквадратичного відхилення σ при використанні функції з потаємним входом є важливим параметром, який необхідно встановити для забезпечення стійкості алгоритму. Достатньою умовою для рівня безпеки, встановлених Національним інститутом стандартизації та технологій, є умова прийняти значення параметра $\sigma \leq 1.312\,||B||_{GS}$, де $||B||_{GS}$ – це норма Грамма – Шмідта, яка дорівнює максимальному значенню Евклідової норми серед векторів, що отримано в процесі ортогоналізації Грамма – Шмідта. Вектори для обчислення норми Грамма – Шмідта обирають серед

базисних векторів, які задають решітку. У даному випадку $\sigma \leq 1.55\sqrt{q}$, де число q є простим числом, яке обчислюється за формулою: $q = k \cdot 2^n + 1$. Для забезпечення рівнів безпеки, згідно з вимогами Національного інституту стандартизації та технологій, покращити запропоновані параметри, які наведено в табл. 1, можливо, прийнявши $q = k \cdot 2^n + 1 = \mathrm{q} = 3 \cdot 4 \cdot 1024 + 1 = 3 \cdot 2^{12} + 1 = 12289$. Тоді при формуванні поліномів f, g використовується дискретний нормальний розподіл, який називають вибіркою Гауса з стандартним квадратичним відхиленням $\sigma = 1{,}17\sqrt{\frac{q}{2n}}$ та математичним сподіванням, яке дорівнює 0. Знаходиться вибірка за допомогою функції щільності імовірностей нормального (Гаусівського) закону розподілу, яка має вигляд $f_{\sigma,a}(x) = e^{\frac{-\pi\|x-a\|^2}{\sigma^2}}$. Для створення нормального (Гаусівського) розподілу необхідно висунути ряд умов. По-перше, необхідно запропонувати дискретний Гаусівський розподіл над цілими числами з усіма властивостями, які очікуються від вибірки для широкого застосування. Дискретний нормальний (Гаусівський) розподіл має бути простим і модульним, що дозволить спростити аналіз отриманих результатів. Необхідно довести безпечність вказаного дискретного розподілу відносно часових атак.

Простота та модульність є першим аспектом, який слід прийняти до уваги. На високому рівні структура потребує лише два компоненти (базовий компонент та компонент відхилення) та поєднує їх простим способом за допомогою "чорного ящика".

Універсальність алгоритму є другим його аспектом. Алгоритм вибірки Гауса за допомогою дискретного нормального (Гаусівського) розподілу працює з довільним математичним сподіванням та стандартним квадратичним відхиленням. Крім того, не передбачено застосування попереднього обчислення: враховуючи фіксовану базову вибірку параметра (Z_n) max, структура дозволяє здійснювати вибірку з множини алгебраїчних решіток DZ для будь-якого (Z_n) max.

Для досягнення постійного часу перетворень застосовується вибірка Гауса за допомогою дискретного нормального (Гаусівського) розподілу, на основі якого створюють вибірку з відхиленням. Вибірка Гауса відрізняється від нормального розподілу та обирає для побудови дискретного розподілу значення z, використовуючи функцію $D_{S,\sigma,a}(z) = f_{\sigma,a}(z) / f_{\sigma,a}(S)$, де z приймає лише цілі додатні значення. Якщо математичне сподівання дорівнює нулю значення $f_{\sigma,a}(S) = \sigma\sqrt{2\pi}$. Для створення дискретної вибірки застосовується таблиця, доступ до якої здійснюється за постійний час. З огляду на те, що запропонована вибірка використовує лише цілі значення та працює як дискретний набір випадкових послідовностей, виникає питання щодо відповідності характеристик отриманого дискретного розподілу до характеристик нормального розподілу. Вирішити дане питання можливо шляхом перевірки отриманих випадкових значень на відповідність до нормального розподілу. Здійснюють дану перевірку на основі різних статистичних тестів та критеріїв. Одним з таких критеріїв є критерій Пірсона, який дозволяє перевірити відповідає вибірки з генеральної сукупності властивостям генеральної сукупності.

Набір тестів SAGA [5] дозволяє перевірити, чи дійсно вибірка Гауса, яка отримана за допомогою дискретного нормального розподілу, має властивості, притаманні нормальному закону розподілу. Використовуються стандартні статистичні інструменти, які дозволяють перевірити роботу алгоритму, що реалізує дискретну вибірку Гауса з точки зору коректності отримання середнього значення, стандартного відхилення, асиметрії і ексцеса. Крім того, вказаний інструмент перевіряє нормально розподілені вихідні дані алгоритму чи ні. Вказана перевірка здійснюється на основі критерія Пірсона. Асиметрія і ексцес нормального розподілу вимірюють відповідно симетрію і плосковершинність або гостровершинність щільності ймовірності розподілу. Повний статистичний аналіз цих тестів було реалізовано за допомогою Python клас Univariate Samples, який приймає в якості аргументів ініціалізації очікуване середнє значення (mu), очікуване стандартне відхилення (sigma) і список спостережуваних одновимірних Гаусових вибірок (data). Крім одновимірного застосування, вказаний набір тестів SAGA, можливо застосувати і для багатовимірного випадку. Дана властивість дозволяє використати тести для багатовимірних випадків, а саме для побудови дискретного нормального багатовимірного (Гаусівського) розподілу для генерації базисів алгебраїчних решіток.

Багатомірні тести на перевірку вихідних даних вибірки Гауса також спрямовані на перевірку отримання нормального розподілу при заданих вхідних параметрах. Вказані тести дозволяють виявити випадки, коли при реалізації алгоритму вибірки Гауса з цілими числами високорівнева схема (наприклад, схема підписів) використовує її неправильно і призводить до некоректного значення багатомірної вибірки Гауса.

Крім того, тести SAGA розроблені для роботи в загальному вигляді, незалежно від техніки, вимагаючи при цьому лише введення або список одномірних або багатомірних вибірок Гауса. SAGA може застосовуватись до будь-якої криптографічної схеми на основі решітки, що вимагає застосування вибірки Гауса. Пошук нових наборів параметрів алгоритмів NTRU, які є стійкими до часових атак, здійснено з застосовуванням Гаусівської дискретної вибірки замість рівномірного розподілу для побудови ключів. Для запуску роботи тестів на першому

кроці обирають прийнятні з точки зору криптостійкості значення середньоквадратичного відхилення. Враховуючи той факт, що значення середньоквадратичного відхилення пов'язане з нормою короткого вектору алгебраїчної решітки, прийнятними значеннями для середньоквадратичного відхилення. В ході дослідження реалізовано тести SAGA для перевірки відповідності властивостей вибірок Гауса нормальному розподілу. Реалізація тестів SAGA для деяких значень середньоквадратичного відхилення та математичного сподівання з можливого діапазону та прийнятних для застосування в криптоперетвореннях на алгебраїчних решітках довжинах поліномів з перевіркою отриманих вибірок Гауса на відповідність нормальному розподілу наведено в табл. 2 – 5.

Відповідно до результатів, наведених в табл. 2 – 5, вибірки Гауса, які створені за допомогою дискретного нормального (Гаусівського) розподілу, мають такі ж самі властивості що й для нормального розподілу.

Таблиця 2

Перевірка тестів SAGA для параметрів алгоритму NTRU для ступеня полінома 509

Довжина поліному	509		
Середнє значення	0.00197	0.06680	0.01965
Середньоквадратичне відхилення	0.81690	0.82177	0.82424
Коефіцієнт асиметрії	-0.00362	-0.12402	-0.03644
Ексцес	-1.50146	-1.50876	-1.52716
Хі-2 статистичний	472.782	528.205	491.059
Хі-2 р-значення (повинне бути більше 0.001)	$5.67*10^{-98}$	$6.89*10^{-110}$	$6.70*10^{-102}$
Чи поліном дійсний?	Так	Так	Так

Таблиця 3

Перевірка тестів SAGA для параметрів алгоритму NTRU для ступеня полінома 677

Довжина поліному	677		
Середнє значення	-0.00739	-0.00739	-0.00739
Середньоквадратичне відхилення	0.81253	0.81253	0.81253
Коефіцієнт асиметрії	0.01350	0.01350	0.01350
Ексцес	-1.48521	-1.48521	-1.48521
Хі-2 статистичний	612.838	612.838	612.838
Хі-2 р-значення (повинне бути більше 0.001)	$4.06*10^{-127}$	$4.06*10^{-127}$	$4.06*10^{-127}$
Чи поліном дійсний?	Так	Так	Так

Таблиця 4

Перевірка тестів SAGA для параметрів алгоритму NTRU для ступеня полінома 701

Довжина поліному	701		
Середнє значення	0.00999	0.00999	0.00999
Середньоквадратичне відхилення	0.80026	0.80026	0.80026
Коефіцієнт асиметрії	-0.01795	-0.01795	-0.01795
Ексцес	-1.43830	-1.43830	-1.43830
Хі-2 статистичний	645.538	645.538	645.538
Хі-2 р-значення (повинне бути більше 0.001)	$3.76*10^{-134}$	$3.76*10^{-134}$	$3.76*10^{-134}$
Чи поліном дійсний?	Так	Так	Так

Таблиця 5

Перевірка тестів SAGA для параметрів алгоритму NTRU для ступеня полінома 821

Довжина поліному	821		
Середнє значення	-0.01340	-0.01340	-0.01340
Середньоквадратичне відхилення	0.81165	0.81165	0.81165
Коефіцієнт асиметрії	0.02447	0.02447	0.02447
Ексцес	-1.48163	-1.48163	-1.48163
Xi-2 статистичний	739.597	739.597	739.597
Xi-2 p-значення (повинне бути більше 0.001)	$2.12*10^{-154}$	$2.12*10^{-154}$	$2.12*10^{-154}$
Чи поліном дійсний?	Так	Так	Так

З огляду на це, дискретні вибірки Гауса можна застосувати для покращення стійкості алгоритму NTRU до часових атак.

Застосовуючи статистичні тести SAGA над поліномами криптографічних перетворень NTRU, було зроблено висновок, що дискретна Гаусівська вибірка дозволяє генерувати стійкі до часових атак параметри, використовуючи в якості середньоквадратичного відхилення норму або довжину короткого базису (вектору) решітки.

Список літератури:

1. Hoffstein J., Lieman D., Pipjer J., Silverman J. NTRU: A public key cryptosystem // Conference International Algorithmic Number Theory Symposium Springer, Berlin, Heidelberg Pages 267-288 Publication date 1998/6/21.
2. Alagic G., Alperin-Sheriff J., Apon D., Cooper D., Dang Q., Miller C., Moody D., Peralta R., Perlner R., Robinson A., Smith-Tone D. and Y.-K. Liu. Status Report on the First Round of the NIST Post-Quantum Cryptography Standardization Process. National Institute of Standards and Technology, Interagency/Internal Report 8240, 2019.
3. IEEE Standard Specification for Public Key Cryptographic Techniques Based on Hard Problems over Lattices', Institute of Electrical and Electronics Engineers, IEEE Standard 1363.1-2008, 2009.
4. Kocher P. C. Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems // Advances in Cryptology – CRYPTO'96, in Lecture Notes in Computer Science, vol. 1109, Springer, Berlin, Heidelberg, 1996. P. 104–113.
5. Isochronous Gaussian Sampling: From Inception to Implementation. With James Howe and Thomas Prest and Thomas Ricosset. In the proceedings of PQ-Crypto 2020.

Надійшла до редколегії 08.11.2021

Відомості про авторів:

Петренко Ольга Євгенівна – канд. техн. наук, доцент, Харківський національний університет радіоелектроніки, доцент кафедри безпеки інформаційних технологій, факультет комп'ютерної інженерії та управління; Україна; email: olha.petrenko@nure.ua; ORCID: https://orcid.org/0000-0002-7862-5399

Петренко Олексій Сергійович – канд. техн. наук, Харківський національний університет Повітряних Сил, заступник начальника науково-дослідного відділу наукового центру Повітряних Сил; Україна; email: alexwgs78@gmail.com; ORCID: https://orcid.org/0000-0001-9903-7388

Сєвєрінов Олександр Васильович – канд. техн. наук, доцент, Харківський національний університет радіоелектроніки, доцент кафедри безпеки інформаційних технологій, факультет комп'ютерної інженерії та управління; Україна; email: oleksandr.sievierinov@nure.ua; ORCID: https://orcid.org/0000-0002-6327-6405

Федюшин Олександр Іванович – канд. техн. наук, доцент, Харківський національний університет радіоелектроніки, доцент кафедри безпеки інформаційних технологій, факультет комп'ютерної інженерії та управління; Україна; email: oleksandr.fediushyn@nure.ua; ORCID: http://orcid.org/0000-0002-3600-405X

Зубрич Артем Віталійович – Харківський національний університет радіоелектроніки, студент кафедри безпеки інформаційних технологій, факультет комп'ютерної інженерії та управління; Україна; email: artem.zubrych@nure.ua

Щербина Денис Вадимович – Харківський національний університет радіоелектроніки, магістрант кафедри безпеки інформаційних технологій, факультет комп'ютерної інженерії та управління; Україна; email: denys.shcherbyna@nure.ua