УДК 004.056.55

Рой Євген Олександрович,

студент І курсу Харківського національного університету радіоелектроніки

Доленко Олексій Дмитрович

студент І курсу Харківського національного університету радіоелектроніки

Петренко Ольга Євгенівна,

к.т.н., доцент кафедри безпеки інформаційних технологій Харківського національного університету радіоелектроніки

ПЕРСПЕКТИВИ ВПРОВАДЖЕННЯ АЛГОРИТМУ NTRU ДЛЯ КРИПТОГРАФІЧНОГО ЗАХИСТУ МОБІЛЬНИХ МЕСЕНДЖЕРІВ

Анотація: стрімкий розвиток квантових обчислень створює серйозну загрозу безпеці сучасних мобільних месенджерів з наскрізним шифруванням, які спираються на класичні криптосистеми з відкритим ключем, такі як RSA та ECC. У роботі проведено

багатокритеріальний порівняльний аналіз алгоритмів RSA, ECC та постквантового алгоритму NTRU за показниками безпеки, енергоефективності і продуктивності. В ході проведеного аналізу з'ясовано, що алгоритм RSA поступається в продуктивності алгоритмам ECC та NTRU. Алгоритм ECC відповідає сучасним вимогам забезпечення безпеки та продуктивності, але не спроможний забезпечити надійний захист в постквантовий період. Алгоритм NTRU є перспективним для застосування завдяки його енергоефективності, швидкодії та забезпечення рівня безпеки в постквантовий період.

Ключові слова: месенджери, алгоритми наскрізного шифрування, продуктивність, забезпечення безпеки, енергоефективність.

Стрімкий розвиток мобільних технологій та бездротового зв'язку зумовив поширене використання мобільних месенджерів як для особистої, так і для корпоративної комунікації. Для забезпечення конфіденційності інформації сучасні застосунки реалізують наскрізне шифрування (E2EE), де ключі генеруються та зберігаються виключно на пристроях користувачів. Традиційно аутентифікація та узгодження сеансових ключів спираються на асиметричні алгоритми RSA та еліптичні криві (ECC). Проте прогрес у галузі квантових обчислень, що спостерігається останнім часом, та практична реалізація алгоритму Шора загрожують безпеці класичних криптосистем, тому що дозволяють за поліноміальний час розв'язати задачі цілочисельної факторизації (IFP) та дискретного логарифмування (ECDLP). Водночас мобільні пристрої функціонують в умовах суворих обмежень щодо обчислювальної потужності, оперативної пам'яті та енергоефективності. Це створює нагальну потребу в виборі алгоритмів криптографічного захисту для розробки месенджерів, що побудовані на їх основі, спроможних забезпечити надійний захист повідомлень в постквантовий період з одного боку та мати прийнятну продуктивність та енергоефективність з другого.

Мета роботи: обґрунтувати вибір асиметричного криптографічного алгоритму для створення захищених мобільних месенджерів шляхом порівняльного аналізу традиційних (RSA, ECC) та постквантових (NTRU) алгоритмів за показниками, що забезпечують продуктивність та енергоефективність.

Стійкість алгоритмів RSA, ECC та NTRU базується на розв'язання

задачі факторизації, дискретного логарифму та пошуку короткого вектора рещітки. Враховуючи необхідність створення месенджера спроможного забезпечити захищеність повідомлень не лише в сучасних умовах, а і в майбутньому, здійснено порівняльний аналіз алгоритмів RSA, ECC та NTRU. Для порівняння вказаних алгоритмів, з точки зору їх використання в месенджерах введено умовні критерії порівняння, а саме прийнятну для застосування довжину ключів, швидкодію алгоритмів, масштабованість, квантову стійкість. В таблиці 1.1 наведені основні параметри алгоритмів RSA, ECC та NTRU, які відповідають введеним умовним критеріям.

Таблиця 1.1 - Порівняльний аналіз криптографічних алгоритмів за рівнем безпеки 128, 192,256 біт

Алгоритм / Рівень стійкості	RSA	ECC	NTRU
	Розмір ключа, біт		
Стандартний 128	3072	256	3501
Високий 192	7680	384	5193
Надвисокий 256	15360	521	7690
	Швидкодія, секунди		
Стандартний 128	118,0258	0,0006	8,4831
Високий 192	1371,5620	0,0010	21,3666
Надвисокий 256	13894,3672	0,002	34,0984
	масштабованість		
Стандартний 128	експоненційне зростання	Лінійне зростання	помірне зростання
Високий 192			
Надвисокий 256			
	квантова стійкість		
Стандартний 128	ні	ні	ні
Високий 192	ні	ні	так
Надвисокий 256	ні	ні	так

Сучасні месенджери повинні бути ефективними під час використання інформаційних, апаратних і програмних ресурсів, з одного боку та мати високу швидкодію в процесі обміну повідомленнями з другого. В результаті виникає питання вибору алгоритму шифрування, який дозволить забезпечити захист повідомлень, які надсилаються, і мінімізувати навантаження на процесор та пам'ять. Згідно проведеного аналізу даних в таблиці 1.1 зроблено висновок, що використання алгоритму RSA не є

доцільним, бо він поступається як алгоритму ЕЕС так і алгоритму NTRU по довжинам ключів, що застосовуються, маштабованості та швидкодії. Щодо останніх двох алгоритмів виникає питання їх застосування для створення сучасних месенджерів. На основі проведеного у роботі аналізу з'ясовано, що в теперішній час алгоритм ECC дозволяє забезпечити ефективність та продуктивність месенджерів. Завдяки забезпеченню надійного захисту при невеликих довжинах ключів та високої швидкодії він покладений в основу роботи таких месенджерів як: WhatsApp і Signal. Популярність цих месенджерів та їх поширене використання привертає увагу зловмисників, які знаходячи їх уразливості реалізують загрози, кількість яких постійно зростає. Крім того, алгоритми на еліптичних кривих уразливі до алгоритму Шора, що унеможливлює їх застосування в постквантовий період. Алгоритм NTRU, поступається алгоритму ECC по критеріям швидкодія, маштабованість та розмір ключа, але його використання в месенджерах є прийнятним. Слід зазначити, що інкапсуляція в NTRU виконується достатньо швидко, що робить його чудовим вибором для застосунків, критичних до вимоги продуктивності Так набір параметрів, що забезпечує 128-бітний рівень безпеки, має відкриті ключі та шифротексти розміром 930 байтів, завдяки чому він ідеально підходить для середовищ із обмеженими ресурсами. Вибір алгоритму NTRU також обумовлений високою швидкістю обчислень та невеликим розміром ключів, в порівнянні з іншими постквантовими алгоритмами. Крім того, як і алгоритми на ECC, алгоритм NTRU витримав випробування часом, протягом якого пройшов ретельну перевірку. Перевага NTRU полягає в тому, що його реалізацію можливо оптимізувати для різних потреб та широкого кола завдань. Застосування різних рівнів безпеки, розмірів ключів дозволяє отримати прийнятну обчислювальну складність, продуктивність та енергоефективність, що так необхідно для роботи месенджерів.

Отже, за результатами багатокритеріального аналізу обґрунтовано, що алгоритм RSA стає непридатним для мобільних месенджерів завдяки

зростанню обчислювальних витрат, зниженню продуктивності та енергоефективності при забезпеченні необхідних рівнів безпеки. Алгоритм ECC в сучасних умовах є вибором для застосування у доквантовий період завдяки мінімальному розміру ключа (256 біт) та економії трафіку. Проте постквантовий алгоритм NTRU визнано найперспективнішим алгоритмом для використання завдяки його швидкості обчислень, яка з надлишком компенсує розмір відкритого ключа, забезпечуючи високу продуктивність та надійний захист мобільних месенджерів у постквантовий період.

Список використаних джерел

1. Аналіз методів захисту інформації, що знаходять використання у сучасних месенджерах / О. О. Білокуров, М. А. Майба, О. К. Шлома, М. О. Дробяз // Проблеми електромагнітної сумісності перспективних безпроводових мереж зв'язку (ЕМС-2022) : матеріали восьмої Міжнародної науково-технічної конференції, 24–25 листопада 2022 р. – Харків, ХНУРЕ, 2022. – С. 71-73. URL*:* https://openarchive.nure.ua/handle/document/21190 (date of access: 22.10.2026).
2. Ramanjaneyulu.S, Rakesh Nayak, "Secure Mobile System Using NTRU Encrypt," *International Journal of Computer Trends and Technology (IJCTT)*, Vol. 4, no. 2, P. 172-176, 2013. URL*:* https://doi.org/10.14445/22312803/IJCTT-V4I2P124 (date of access: 22.10.2026).
3. Гнатюк С. О., Кінзерявий В. М., Поліщук Ю. Я., Нечипорук О. П., Горбаха Б. М. (2022). Аналіз методів забезпечення конфіденційності даних, які передаються з БПЛА. *Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка»*, *1*(17), 167–186. URL: https://doi.org/10.28925/2663-4023.2022.17.167186 (дата звернення: 22.10.2026).
4. Comparative analysis of RSA and NTRU algorithms and implementation in the cloud / B. Harjito et al. *International journal of advanced computer science and applications*. 2022. Vol. 13, no. 3. URL: https://doi.org/10.14569/ijacsa.2022.0130321 (date of access: 22.10.2026).
5. Loriya H., Kulshreshta A., Keraliya D. Security analysis of various public key cryptosystems for authentication and key agreement in wireless communication network. *International journal of advanced research in computer and communication engineering*. 2017. Vol. 6, no. 2. P. 267–274. URL: https://ijarcce.com/wp-content/uploads/2017/february-17/IJARCCE%2062.pdf (date of access: 22.10.2026).