УДК 004.056.55

ДО ПИТАННЯ ПОБУДОВИ КАСКАДНИХ СИСТЕМ ПОТОКОВИХ ШИФРІВ

Главчев М.І., к.е.н., доц.[1]; Панченко В.І.[2].; Баленко О.І., к.т.н, доц.[3]
[1,2,3]Національний технічний університет «Харківський політехнічний інститут»
[1,2,3]Україна, Харків
[1]ORCID 0000-0001-9670-9118; [2]ORCID 0000-0003-3364-3398; [3]ORCID 0000-0002-2314-0984

Анотація. *У тезах систематизовано принципи побудови надійних каскадних систем на основі потокових шифрів. Проаналізовано три ключові архітектурні моделі: лінійну, паралельну та лінійну зі зворотним зв'язком. Проведено їх якісний та кількісний порівняльний аналіз за критеріями продуктивності, теоретичної безпеки та складності реалізації. Сформульовано вимоги до вибору криптографічних примітивів на основі принципу структурної різноманітності та розглянуто перспективи застосування каскадування для створення гібридних пост-квантових систем.*

Ключові слова: *каскадне шифрування; потокові шифри; управління ключами; KDF; криптографічна стійкість; архітектурні моделі; пост-квантова криптографія.*

Вступна частина. Актуальність даного дослідження обумовлена необхідністю підвищення криптографічної стійкості систем передачі даних. В умовах зростання обчислювальних потужностей та появи нових криптоаналітичних методів, включно з квантовими загрозами, застосування одного криптоалгоритму може не забезпечувати достатнього рівня довгострокової безпеки. Каскадне шифрування, як варіант комбінованих шифрів[1], що передбачає композицію кількох перетворень, є визнаним підходом для побудови відмовостійких криптосистем. Ця робота є логічним продовженням дослідження методів управління ключами, де було запропоновано методику генерації криптографічного матеріалу з секретів з низькою ентропією за допомогою пам'ять-вимогливих функцій.

Метою дослідження є формулювання та систематизація принципів побудови надійних каскадних систем на основі потокових шифрів.

Основна частина. Проектування каскадних систем базується на трьох основних архітектурних моделях. Для всіх моделей єдиним джерелом ключової інформації слугує функція виведення ключів (KDF), що перетворює майстер-ключ на набір сесійних ключів та векторів ініціалізації [2]. Загальна модель описується як:

$$\{k_i, IV_i\}^n_{i=1} = KDF\{MK, Salt)$$

Ця формула показує, як з одного майстер-ключа *MK* та випадкової "солі" *(Salt)* за допомогою функції виведення ключів *KDF* створюється весь набір криптографічного матеріалу. На виході отримуємо набір *{...}*, що складається з унікального ключа k_i та вектора ініціалізації IV_i для кожного з n шифрів у каскаді.

1. Лінійна модель:

$$C = E_{kn}(...E_{k2}(E_{k1}(P))...)$$

Це модель послідовного шифрування. Відкритий текст (P) спочатку шифрується першим шифром з ключем k_1. Результат цього шифрування подається на вхід другого шифру з ключем k_2, і так далі *n* разів. *C* — це фінальний шифротекст. Згідно з теоремою Маурера-Мессі, криптостійкість такого каскаду не нижча за стійкість найсильнішого компонента [3]

2. Паралельна модель:

$$C = P \text{ xor } \bigoplus_{i=1}^{n} G_i(k_i, IV_i)$$

У цій моделі n генераторів ключового потоку G_i працюють незалежно та одночасно, кожен зі своїм ключем k_i та вектором ініціалізації IV_i. Всі згенеровані ними потоки складаються між собою через операцію *XOR* (символ $\oplus$). Отриманий сумарний потік потім "накладається" на відкритий текст P також через *XOR*, щоб отримати шифротекст C.

3. Лінійна модель зі зворотним зв'язком

Це система з двох формул, що працюють на кожному кроці:

(Модифікація ключа): $k'_i = F(k_i, C_{i-1})$

Ключ для поточного i-го етапу k'_i не береться напряму. Він створюється шляхом комбінування початкового ключа для цього етапу k_i з результатом шифрування попереднього етапу C_{i-1} за допомогою функції F (наприклад, гешування).

(Шифрування): $C_i = E_{ki}(C_{i-1})$

Шифрування на поточному етапі відбувається з використанням вже модифікованого ключа k'_i.

Вибір конкретної архітектури є компромісом між продуктивністю, безпекою та складністю. У таблиці 1 наведено порівняльний аналіз трьох розглянутих моделей.

Таблиця 1 – Порівняння архітектурних моделей каскадування

Критерій	Лінійна модель	Паралельна модель	Лінійна модель зі зворотним зв'язком
Продуктивність	Середня. Обчислення суворо послідовні.	Висока. Можливість повного розпаралелювання генерації ключів.	Низька. Послідовні обчислення з додатковими операціями.
Теоретична безпека	Висока. Стійкість не нижча за найсильніший компонент.	Висока. Стійкість забезпечується, якщо хоча б один генератор надійний.	Дуже висока. Сильна дифузія та ускладнення для криптоаналізу.
Складність реалізації	Середня. Проста логіка послідовного виклику.	Низька. Незалежні потоки, які легко реалізувати та відлагодити.	Висока. Потребує реалізації функції F та управління залежностями.
Розпаралелювання	Неможливе.	Повне. Ідеально підходить для багатоядерних систем та GPU.	Неможливе.
Поширення помилок	Високе. Помилка на одному етапі впливає на всі наступні.	Відсутнє. Помилка в одному потоці не впливає на інші.	Дуже високе. Помилка впливає на дані та генерацію наступних ключів.
Найкраще застосування	Системи зберігання даних, де надійність важливіша за швидкість.	Системи реального часу, потокове відео, VPN-канали.	Системи з максимальними вимогами до безпеки (військові, урядові).

Для більш наочного порівняння, оцінимо моделі у відсотках, прийнявши за 100% показники лінійної моделі (табл.2). Розрахунки є умовними і базуються на припущенні про

каскад з трьох (n=3) шифрів з приблизно однаковою продуктивністю, що виконуються на багатоядерній системі.

Таблиця 2 – Кількісне порівняння моделей (відносно лінійної)

Критерій	Лінійна модель	Паралельна модель	Лінійна модель зі зворотним зв'язком	Примітки
Час виконання	100% (База)	~35-40%	~110-120%	Паралельна модель майже втричі швидша завдяки розпаралелюванню. Модель зі зворотним зв'язком повільніша через додаткові обчислення.
Відносна надійність	100% (База)	~100%	>100%	Надійність лінійної та паралельної моделей експоненційно вища за надійність одного шифру. Модель зі зворотним зв'язком додає ще один рівень складності для аналізу.
Стійкість до помилок	~0%	100%	~0%	У лінійних моделях помилка на одному етапі повністю руйнує кінцевий результат. У паралельній моделі помилка в одному потоці зіпсує дані, але не вплине на роботу інших.

З таблиці видно, що паралельна модель пропонує найкращий баланс, забезпечуючи величезний приріст у швидкості (~60-65%) при збереженні експоненційного рівня надійності, властивого каскадуванню.

Ефективність каскаду безпосередньо залежить від правильного вибору його компонентів. Ключовою вимогою є принцип структурної різноманітності (Design Diversity), що мінімізує ризик одночасної компрометації всіх шифрів через фундаментальний криптоаналітичний прорив.

Основні критерії сумісності алгоритмів:

- Різноманітність математичних підходів: Поєднання шифрів, що базуються на різних принципах, наприклад, ARX-шифри (Add-Rotate-XOR, як ChaCha20) [4] та шифри на основі таблиць заміни (S-box, як AES в режимі CTR).

- Алгебраїчна незалежність: Компоненти каскаду не повинні мати спільних алгебраїчних властивостей, які могли б бути використані в атаках вищого порядку.

- Відсутність відомих слабкостей: Кожен примітив повинен бути стандартизованим та не мати відомих практичних вразливостей.

Критичним аспектом безпеки потокових шифрів є управління векторами ініціалізації (nonces). Повторне використання пари (ключ, nonce) для шифрування різних повідомлень призводить до компрометації конфіденційності та є катастрофічною помилкою реалізації [5]. Тому система повинна гарантувати унікальність nonce для кожного повідомлення. Централізована генерація всього криптографічного матеріалу на етапі KDF дозволяє детерміновано виділяти унікальні nonce для кожного компонента каскаду, що мінімізує ризик колізій.

На відміну від блочних шифрів, потокові шифри не мають вимог до вирівнювання даних (padding), що спрощує їх поєднання в лінійній моделі. У паралельній моделі необхідно

забезпечити генерацію ключових потоків однакової довжини, що дорівнює довжині повідомлення.

Каскадування є ефективною стратегією для побудови гібридних криптосистем, що поєднують класичні та пост-квантові алгоритми. Така архітектура реалізує принцип криптографічної агільності та "подвійної впевненості": система залишається стійкою, якщо хоча б один з її компонентів зберігає криптографічну стійкість до відповідного класу атак (класичних чи квантових). Прикладом може слугувати каскад AES-256-CTR та одного з потокових шифрів, стандартизованих NIST в межах конкурсу пост-квантової криптографії [6].

Висновки. Побудова надійних каскадних систем потокового шифрування є комплексною науково-технічною задачею, що виходить за рамки простого поєднання стійких алгоритмів. Ефективність та безпека таких систем визначаються трьома ключовими факторами: надійною процедурою генерації та розподілу ключів, свідомим вибором архітектурної моделі відповідно до системних вимог, та дотриманням принципу структурної різноманітності при виборі криптографічних примітивів.

Запропоновані принципи та моделі дозволяють системно підходити до проектування каскадів, мінімізуючи ризики, пов'язані як з помилками реалізації, так і з фундаментальними проривами в криптоаналізі. Врахування пост-квантових загроз на етапі проектування робить такий підхід основою для створення перспективних гібридних криптосистем з довготривалим життєвим циклом.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

[1] Глачев, М.І., & Новикова, А.В. (2012). *Загальний підхід до комбінованих шифрів*. У матеріалах Міжнародної наукової конференції MicroCAD: Секція №21 - Інформатика і моделювання (с. 12). Національний технічний університет «Харківський політехнічний інститут». https://repository.kpi.kharkov.ua/server/api/core/bitstreams/c2363a6a-9c41-4f46-aa26-530dd3282e27/content?trackerId=2eb224b318a58d0e

[2] Krawczyk, H., & Eronen, P. (2010). *HMAC-based extract-and-expand key derivation function (HKDF)* (RFC 5869). Internet Engineering Task Force. https://doi.org/10.17487/RFC5869

[3] Maurer, U. M., & Massey, J. L. (1993). Cascade ciphers: The importance of being first. *Journal of Cryptology, 6*(1), 55–61. https://doi.org/10.1007/BF00192095

[4] Nir, Y., & Langley, A. (2018). *ChaCha20 and Poly1305 for IETF protocols* (RFC 8439). Internet Engineering Task Force. https://doi.org/10.17487/RFC8439

[5] Ferguson, N., Schneier, B., & Kohno, T. (2010). *Cryptography engineering: Design principles and practical applications*. Wiley Publishing, Inc.

[6] Chen, L., Jordan, S., Liu, Y.-K., Moody, D., Peralta, R., Perlner, R., & Smith-Tone, D. (2016). *Report on post-quantum cryptography* (NISTIR 8105). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.IR.8105

Glavchev M.I. Panchenko V.I., Balenko O.I.

ON THE ISSUE OF CONSTRUCTING CASCADE STREAM CIPER SYSTEMS

Abstract. *The theses systematize the principles for constructing reliable cascaded systems based on stream ciphers. Three key architectural models are analyzed: linear, parallel, and linear with feedback. A qualitative and quantitative comparative analysis of these models is conducted based on criteria of performance, theoretical security, and implementation complexity. Requirements for the selection of cryptographic primitives based on the principle of design diversity are formulated, and the prospects of using cascading to create hybrid post-quantum systems are considered.*

Keywords: *cascaded encryption; stream ciphers; key management; KDF; cryptographic strength; architectural model; post-quantum cryptography.*