Про нові постквантові потокові алгоритми шифрування, визначені в термінах темпоральних алгебраїчних графів

Василь Устименко[1,2] (доповідач), Олександр Пустовіт[2] і Тимофій Свириденко[2]
[1] Роял Холоввей Університет, Лондон, Велика Британія.
[2] Інститут телекомунікацій і глобального інформаційного простору НАН України, Київ
e-mails: Vasyl.Ustimenko@rhul.ac.uk, sanyk_set@ukr. net, ipz23-t.svyrydenko@nubip.edu.ua

Графи *D(n, q)* були визначені 33 роки тому. Їхні зв'язні компоненти є апроксимаціями нескінченного *q*-регулярного дерева *T(q)*. Цей факт використовувався в різних застосуваннях до інформатики. Разом з графами *D(n, q)* часто використовувалися інші гомоморфні образи *A(m, q)* дерева *T(q)*.

Ми коротко оглянемо використання цих сімейств графів та їх узагальнення у розробці алгебраїчних потокових шифрів та LDPC-кодів. Ми пропонуємо загальний метод обфускації криптосистем на основі *D(m, q)* або *A(n, q)* за допомогою методів штучного інтелекту або квантових обчислень.

Ми пропонуємо новий потоковий шифратор на основі цих графів з небієктивною функцією шифрування, що є поліноміальним перетворенням від багатьох змінних ступеня, який не обмежений незалежною сталою.

Стандартна форма цього відображення визначає обфускацію відомого публічного ключа криптографії від багатьох змінних (див. [1], [2]). Швидкість виконання становить *O(n)*, різні активні паролі створюють різні шифрограми. Комп'ютерне моделювання демонструє хороші властивості змішування шифратора.

У доповіді ми визначимо модифікацію цього алгоритму через його перетворення у криптосистему квантової криптографії або криптосистеми вживанням інструментів штучного інтелекту. Модифікація визначається через заміну графів *D(n, q)* та *A(n, q)* та їх темпоральні аналоги.

Огляд результатів застосування Штучного Інтелекту для ускладнення потокових алгоритмів шифрування Криптографії у термінах Теорії Графів буде подано у доповіді В. Устименка на міжнародній конференції «Artificial Intelligence & Mathematical Sciences», AIMS 2026, Université Paris-Est Créteil (UPEC), Paris, France, July 7-8, 2026 (див. [3]).

Література

1. V. Ustimenko, On new multivariate cryptosystems based on hidden Eulerian equations, Dopov. Nath Acad of Sci, Ukraine, 2017. № 5, pp 17-24.
2. V. Ustimenko, On new multivariate cryptosystems based on hidden Eulerian equations over finite fields, Cryptology ePrint Archive, 093, 2017.
3. https://sites.google.com/risat.org/home/conf/aims-conf/aims-26/aims-26-talks