Свойства произведения Адамара констациклических линейных кодов и их применение в криптоанализе

Линь Пэйфэн

Студент

Факультет ВМК МГУ имени М. В. Ломоносова, Москва, Россия

E-mail: lin__pf@163.com

Научный руководитель *— Чижов Иван Владимирович*

В рамках конкурса [1] постквантовой криптографии, проводимого Национальным институтом стандартов и технологий (NIST) США, оригинальная криптосистема Мак-Элиса достигла четвёртого раунда. Однако, несмотря на этот успех, данная криптосистема столкнулась с проблемой значительных размеров ключей, в отличие от более распространенных решёточных шифров. В связи с этим, принято решение заменить коды, используемые в оригинальной системе, на более простые, такие как коды Рида-Маллера. Однако, при этой замене было выявлено, что некоторые из предложенных мер снижают безопасность системы, как указано в [2]. В данной работе проведен анализ криптосистемы Мак-Элиса, основанный на констациклических кодах с целью устранения обнаруженных недостатков.

Открытый ключ криптосистемы Мак-Элиса представляет собой пару матриц (G, G'), где G — $(k \times n)$ порождающая матрица кода C, на котором криптосистема строится, и G' — $(k \times n)$ порождающая матрица кода C^σ. Основной этап восстановления секретного ключа по открытому ключу (G, G') включает поиск перестановки σ' такой, что $\sigma \cdot \sigma' \in \mathrm{Aut}(C)$, где $\mathrm{Aut}(C)$ — группа перестановочных автоморфизмов кода C.

В работе предложена атака на криптосистему Мак-Элиса, построенную на основе констациклических линейных кодов на основе изучения свойств произведения Адамара констациклических линейных кодов из статьей [3,4] и описания их группы автоморфизмов. Атака возможно оказывается эффективной, если некоторая степень Адамара основного кода порождается многочленом вида $p(x) = \sum_{i=0}^{\frac{n}{v}-1} \alpha^i x^{v \cdot i}$. В этом случае если порядок ℓ_α элемента α больше чем n/v и v настолько мала, что $v!$ в некоторых случаях является полиномом от длины входа, то структурная атака выполняется за полиномиальное время.

В рамках данной работы далее ещё указан метод предотвращения вышеупомянутой атаки - построение криптосистемы на основе

констациклических линейных кодов над полем с небольшим числом элементов, например $GF(2)$, чтобы обеспечить невыполнение условия $\ell_\alpha > n/v$. Важно отметить, что это сопровождается уменьшением пространства ключей.

Литература

1. Страница конкурса NIST `https://csrc.nist.gov/projects/post-quantum-cryptography`
2. Бородин М. А., Чижов И. В. Эффективная атака на криптосистему Мак-Элиса, построенную на основе кодов Рида–Маллера // Дискретная математика. 2014. Т. 26, № 1. С. 10–20.
3. H. Randriambololona. "On products and powers of linear codes under componentwise multiplication,"Contemporary Mathematics. 637, 3-78, (2015).
4. B. H. Falk, N. Heninger, M. Rudow. "Properties of constacyclic codes under the Schur product,"Designs, Codes and Cryptography. 88, 993-1021, (2020).