УДК 51-74

ОБЗОР МЕТОДОВ МОДИФИКАЦИИ КРИПТОСИСТЕМЫ МАКЭЛИСА

Носков И.К. (Университет ИТМО)
Научный руководитель – доцент, доктор технических наук Беззатеев С.В.
(Университет ИТМО)

Введение. Криптосистема МакЭлиса [1] была предложена Робертом Мак-Элисом в 1978 году, а аналогичная криптосистема – криптосистема Нидеррайтера [2] – была предложена в 1986 году. Данные схемы во многом схожи, их главным отличием является открытый ключ: в криптосистеме МакЭлиса – порождающая матрица линейного кода, в криптосистеме Нидеррайтера – проверочная матрица линейного кода. Несмотря на то, что данные криптосистемы не получили широкого применения в период их создания из-за размеров открытого ключа, возможность создания квантовых компьютеров привела к поиску и созданию новых методов построения криптосистем. Поэтому в настоящее время данные схемы модифицируются, а модификация криптосистемы МакЭлиса [3] является претендентом на стандарт постквантовой криптографии, так как данная система устойчива к атаке по информационной совокупности. Несмотря на это, главными проблемами представленного алгоритма остаются размер открытого ключа (проверочная матрица линейного кода, урезанная по методу Гаусса) и сложность вычислений, так как с ростом защиты системы возрастает размерность поля, в котором эти вычисления производятся, что приводит к росту времени создания ключей.

Основная часть. В настоящее время существует два основных подхода к решению проблем, связанных с размерами открытого ключа и сложностью вычислений. Первое направление повышение эффективности системы шифрования связано с поиском возможностей для снижения вычислительной сложности алгоритмов построения проверочной матрицы в качестве открытого ключа системы и декодирования кодов Гоппы [4]. Чтобы уменьшить сложность вычислений предлагается использовать вместо кодов Гоппы обобщенные (L, G)-коды [5] с нумераторами различных степеней. Например, при использовании нумераторов второй степени размерность поля 2^{2m} уменьшается до размерности 2^{m+1}. Данный метод усложняет процесс получения множества нумераторов кода, а также усложняет возможность использования процедуры Ченя при декодировании. Вторым направлением является решение достаточно традиционной задачи – уменьшения размера открытого ключа. Для решения этой проблемы можно использовать квазициклические обобщенные (L, G)-коды [6]. При использовании данных кодов появляется возможность не использовать всю проверочную матрицу в качестве открытого ключа, так как всю проверочную матрицу кода можно представить как циклические сдвиги строк некоторой начальной проверочной подматрицы квазициклического обобщенного (L, G)-кода. Основная проблема такого подхода заключается с одной стороны в поиске множества таких квазициклических кодов, а с другой в существенном уменьшении безопасности системы вследствие наличия определенной циклической структуры такого квазициклического кода.

Выводы. Проведен аналитический обзор методов построения модифицированного варианта криптосистемы МакЭлиса, которые позволяют уменьшить сложность вычислений и размер открытого ключа.

Список использованных источников:

1. McEliece R.J. A public-key cryptosystem based on algebraic coding theory. Technical report: NASA, 1978.

2. Niederreiter H. Knapsack-type cryptosystems and algebraic coding theory // Problems of Control and Information Theory. 1986. V. 15. N 2. P. 159–166.

3.Bernstein D., Chou T., Lange T., Maurich I., Misoczki R., Niederhagen R., Persichetti E., Peters C, Schwabe P., Sendrier N., Szefer J., Wang W. Classic McEliece: conservative code-based cryptography. Проектная документация [Электронный ресурс]. Режим доступа: https://classic.mceliece.org/nist/mceliece-20190331.pdf

4. Гоппа В.Д. Новый класс линейных корректирующих кодов // Проблемы передачи информации. 1970. Т. 6. № 3. С. 24–30.

5. Bezzateev S.V, Shekhunova N.A. One generalization of Goppa codes// Proceedings of ISIT-97, Ulm, Germany, 1997. P.299

6. Bezzateev S.V., Shekhunova N.A ,Quasi-cyclic Goppa codes, IEEE International Symposium on Information Theory, Canada, 1995, p.499

Носков И.К. (автор) Подпись

Беззатеев С.В. (научный руководитель) Подпись