А. В. Жаткин

ПРИМЕНЕНИЕ СИСТЕМ КВАДРАТНЫХ УРАВНЕНИЙ МНОГИХ ПЕРЕМЕННЫХ В АСИММЕТРИЧНОЙ КРИПТОГРАФИИ

Сегодня криптографические примитивы с открытым ключом стали неотъемлемой частью множества сетевых протоколов, нашли применение в RFID-метках и являются основой схем аутентификации и алгоритмов цифровой подписи. Криптографические системы с открытым ключом широко известны по всему миру. Однако, несмотря на повсеместное использование, их разнообразие довольно ограничено. В основе лежат всего несколько задач, которые, как считается, имеют высокую вычислительную сложность, в частности задача факторизации больших чисел и задача дискретного логарифмирования.

Ограниченность набора базовых математических принципов ведет к уязвимости множества существующих криптосистем в случае получения эффективного алгоритма решения рассматриваемых задач. На данный момент уже известны эффективные квантовые алгоритмы факторизации чисел и вычисления дискретных логарифмов, представленные П. Шором [1]. Это означает, что создание эффективного и масштабируемого квантового компьютера приведет к уязвимости всех асимметричных криптосистем, стойкость которых основана на трудоемкости этих задач. Кроме того, даже классические компьютеры, объединенные в большие кластеры, способны решать эти задачи для достаточно больших длин ключей. Так, в 2009 г. был успешно разложен на множители модуль для RSA-768 (число из 768 бит, являющееся произведением пары простых) [2], а в 2012 г. был вычислен дискретный логарифм над конечным полем размерностью в 1175 бит [3].

В связи с потенциальной уязвимостью классических асимметричных криптосистем исследователями во всем мире ведутся активные поиски альтернативных подходов к построению криптографических примитивов с открытым ключом. Так, рассматриваются группы кос, решетки, а также системы нелинейных алгебраических уравнений. Представленный доклад посвящен применению систем квадратных алгебраических уравнений для построения базового криптографического примитива — однонаправленной функции с секретом. Как известно, решение системы нелинейных уравнений в общем случае является NP-полной задачей и имеет экспоненциальную сложность [4]. Кроме того, пока не известно и эффективных квантовых алгоритмов для решения этой задачи. Поэтому системы алгебраических уравнений представляют интерес в качестве возможной основы для новых асимметричных алгоритмов.

На данный момент широко известны два вида асимметричных криптосистем, основанных на системах квадратных уравнений многих переменных: семейство MQ-систем [5] и MQQ-система, представленная Д. Глигороски и др. [6]. Вначале рассмотрим общую структуру однонаправленной функции с секретом на основе систем квадратных алгебраических уравнений и обоснование ее единственности: открытым ключом является некоторая система квадратных уравнений P (т. е. вектор коэффициентов ее уравнений). Секретом функции является тройка (S, P', Q), где первый и последний компоненты являются аффинными преобразованиями, а P' — система квадратных уравнений. Скрытая система P' строится таким образом, чтобы ее обращение (т. е. решение системы для произвольного вектора значений ее уравнений) было сравнительно простым. В то же время обращение открытой системы P в общем случае является NP-полной задачей и имеет экспоненциальную сложность. Данная схема устройства однонаправленной функции с секретом является единственно возможной, поскольку «скрывающие» преобразования S и Q не могут иметь степень выше или равную внутреннему преобразованию, которое осуществляет система квадратных уравнений P', а поскольку аффинные преобразования образуют группу, то увеличение их количества не влияет на стойкость криптосистемы.

Исторически первыми криптосистемами, использовавшими системы квадратных алгебраических уравнений, были схема Матсумото — Имаи, схема UOV (unbalanced oil and vinegar),

схема HFE (hidden field equations) и схема STS (stepwise triangular systems). Все они оказались уязвимы к атакам с помощью алгебраического анализа, в частности базисов Грёбнера [5]. Лишь схема UOV при правильном подборе параметров оказалась достаточно стойкой, однако она является сравнительно неэффективной за счет трехкратного увеличения длины сообщения, а также невозможности использования в качестве основы для алгоритма шифрования.

Криптосистема MQQ была представлена в 2008 г. Д. Глигороски и др. Она сразу была оформлена в виде готового асимметричного алгоритма шифрования с единственным параметром (длина открытого ключа). Основой конструкции стали квазигруппы над системами квадратных уравнений многих переменных, построение которых позволяет легко обращать скрытое преобразование P'. Второй частью схемы является биекция Доббертина, представленная им в [7] и используемая для сокрытия линейной части преобразования с помощью MQQ. Полученный в итоге алгоритм продемонстрировал высокое быстродействие, сравнимое с симметричными системами.

К сожалению, рассмотренные в 2010 г. методы атаки на криптосистему MQQ не позволили ей стать серьезным конкурентом распространенных криптосистем, таких как RSA. Полученные в [8] результаты показали совершенно неудовлетворительную стойкость схемы MQQ по отношению к атаке с помощью базисов Грёбнера или современных алгоритмов решения систем, таких как Mutant XL. Однако в той же работе было продемонстрировано, что сами по себе MQQ могут представлять интерес для дальнейшего изучения, поскольку рост меры нелинейности в общей схеме, по-видимому, ограничивается именно преобразованием Доббертина. Следовательно, целесообразно провести исследование для нахождения иного преобразования, которое смогло бы эффективно скрывать линейную часть на выходе MQQ и одновременно не снижало бы общую меру нелинейности криптосистемы. В случае успеха станет возможным построение достаточно надежной однонаправленной функции с секретом, обладающей высокой вычислительной эффективностью.

СПИСОК ЛИТЕРАТУРЫ:

1. *Shor P. W.* Algorithms for quantum computation: Discrete logarithms and factoring // Symposium on Foundations of Computer Science, IEEE Computer Society Press, 1994. P. 124–134

2. *Thorsten K., Kazumaro A., Jens F., Lenstra A. K., et al.* Factorization of a 768-bit RSA modulus // Proceedings of the 30th annual conference on Advances in cryptology, Springer-Verlag Berlin, Heidelberg, 2010. P. 333–350.

3. *Joux A.* Faster index calculus for the medium prime case. Application to 1175-bit and 1425-bit finite fields. // Cryptology ePrint Archive: Report 2012/720, 2012.

4. *Wolf C.* Hidden Field Equations (HFE) — variations and attacks. UniversitДat Ulm, 2002. — 87 p.

5. *Wolf C., Preneel B.* Taxonomy of Public Key Schemes based on the problem of Multivariate Quadratic equations. IACR Eprint archive, 2005. — 64 p.

6. *Gligoroski D., Markovski S., Knapskog S. J.* Multivariate quadratic trapdoor functions based on multivariate quadratic quasigroups // MATH'08: Proceedings of the American Conference on Applied Mathematics. Stevens Point, Wisconsin, USA, 2008. P. 44–49.

7. *Dobbertin H.* One-to-one highly nonlinearpower functions on GF(2^n) // Applied Algebra Eng. Commun. Comput. T. 9. 1998. P. 139–152.

8. *Faugere J.-C., Ш degard R. S., Perret L., Gligoroski D.* Analysis of the MQQ Public Key Cryptosystem // 9th International Conference. CANS 2010. Lecture Notes in Computer Science. Vol. 6467, Springer Berlin, Heidelberg, 2010. P. 169–183.