XXX Юбилейная Неделя науки СПбГТУ. Материалы межвузовской научной конференции. Ч. VII: С159, 2002.

УДК 681.3.053

П.В. Трифонов (5 курс, каф. РВКС), Е.А. Крук, д.т.н., проф.

ДВУХМАТРИЧНЫЕ КРИПТОСИСТЕМЫ

Ввиду широкого распространения компьютерных сетей в настоящее время остро стоит проблема обеспечения безопасности связи. Проблема может быть частично решена путем использования систем симметричного шифрования, но в этом случае для обмена ключами шифрования необходимо создание отдельных систем. В настоящее время для этих целей используются криптосистемы с открытым ключом. Наибольшее распространение получили теоретико-числовые конструкции (RSA, протокол Диффи-Хеллмана, системы на эллиптических кривых и др.). Их основным достоинством является небольшой размер ключа. Вместе с тем, для всех этих систем практически ничего не известно о сложности математических задач, положенных в их основу. Обратная ситуация имеет место в случае кодовых криптосистем Мак-Элиса и Нидеррайтера. Несмотря на то, что в их основе лежит NP-полная задача декодирования линейного кода, были найдены достаточно эффективные алгоритмы ее решения, что привело к необходимости использования чрезвычайно больших публичных ключей. В данной работе представлены некоторые возможные методы решения этой проблемы, а также исследована их криптостойкость.

В работе рассматриваются криптосистемы, в которых шифрование сообщения x осуществляется как $y=xK_1+eK_2$, где K_i – публичные ключи, e – случайный вектор ошибки ограниченного веса. Такие криптосистемы являются реализацией общего подхода, предложенного в [1]. Для всех подобных криптосистем выделены следующие классы атак:

Умножение зашифрованного сообщения на матрицу K_2^{-1} (при ее существовании). В этом случае криптосистема сводится к случаю криптосистемы Мак-Элиса [2]. Для обеспечения безопасности криптосистемы необходимо убедиться в том, что минимальное расстояние кода с порождающей матрицей $K_1K_2^{-1}$ не позволяет однозначно декодировать сообщение.

Умножение зашифрованного сообщения на матрицу $H_1^T : K_1H_1^T = 0$. Тогда криптосистема сводится конструкции Нидеррайтера [3]. Для обеспечения безопасности криптосистемы необходимо убедиться в том, что минимальное расстояние кода с проверочной матрицей $K_2H_1^T$ не позволяет однозначно декодировать вектор e.

Умножение зашифрованного сообщения на матрицу $H_2^T : K_2H_2^T = 0$. Такое преобразование позволяет уничтожить вектор ошибки. Для обеспечения безопасности криптосистемы необходимо убедиться в том, что матрица $K_1H_2^T$ имеет достаточно малый ранг.

В работе также исследованы возможности применения нелинейных функций для обеспечения невозможности раздельного нахождения векторов x и e.

ЛИТЕРАТУРА:

1. E. Krouk and U. Sorger. A public key cryptosystem based on total decoding of linear codes. In Proceedings on Sixth International Workshop ”Algebraic and Combinatorial Coding Theory”’, Pskov, Russia, pages 158–160, 1998.
2. R. J. McEliece. A public-key cryptosystem based on algebraic coding theory. DSN Progress Report, 42-44:114–116, 1978.
3. H. Niederreiter Kanpsack-type cryptosystems and algebraic coding theory, Problems of Control and Information Theory, 1986.