О ПРОГРАММНОЙ РЕАЛИЗАЦИИ КРИПТОСИСТЕМЫ МАК-ЭЛИСА– СИДЕЛЬНИКОВА

В.А. ЛИПНИЦКИЙ, А.В. КОСТЕЛЕЦКИЙ

В 1978 году Мак-Элис (McEliece) предложил криптосистему с открытым ключом, основанную на сложности ряда задач теории кодирования. Суть её заключается в следующем. Имеется G — порождающая матрица линейного двоичного $[n, k]$-кода, исправляющего t ошибок и имеющего быстрый алгоритм декодирования. Абонент случайно, равновероятно и независимо выбирает невырожденную матрицу H (размерности $k \times k$) и перестановочную матрицу Γ (размерности $n \times n$). Эта пара матриц — секретный ключ абонента. Матрица $E=HG\Gamma$ — открытый ключ (общедоступный).

Мак-Элис предлагал взять за основу коды Гоппы, затем, по предложению Сидельникова В.М., стали использоваться коды Рида-Маллера, имеющие быстрые алгоритмы кодирования и декодирования.

Коды Рида-Маллера — низкоскоростные, но исправляющие большое число ошибок. Эти коды используется в космических исследованиях (передачи с Марса, связь с “Вояджером” и прочее). Кроме того, криптосистемы, основанные на этом коде, обладают высокой стойкостью к нападению.

Сидельников В.М. предложил модификацию рассматриваемой системы с целью увеличения криптографической стойкости. Абонент случайно, равновероятно и независимо выбирает набор $H=(H_1, H_2, \ldots H_u)$, состоящий из u невырожденных матриц размерности $k \times k$, и перестановочную матрицу Γ размера $un \times un$. Затем образуется набор матриц $E_1=H_1G$, $E_2=H_2G$, …, $E_u=H_uG$, и матрица $\boldsymbol{E=(E_1 \angle E_2 \angle \ldots \angle E_u \angle)\Gamma}$. Матрица E — открытый ключ, пара (H, Γ) — секретный ключ абонента. Также Сидель- ников разработал алгоритмы декодирования, которые могут исправлять значительно больше чем t ошибок.

Одним из основных препятствий в применении криптосистем с открытым ключом является сложность реализации некоторых этапов (обычно медленное декодирование, как, например, в криптосистеме RSA). В этом плане криптосистема Мак-Элиса – Сидельникова находится в стадии теоретической разработки. В докладе идёт речь об опыте программной реализации этой криптосистемы. В частности, с помощью пакета Mathematica 4.2, разработана программа задания кода Рида-Маллера с заданными параметрами (формирование порождающей и проверочной матриц, получение кодовых слов), программа формирования секретных и открытых ключей в модифицированной криптосистеме Сидельникова. И программа коррекции ошибок в криптосистемах с большим кодовым расстоянием.