ОЦЕНКА МОЩНОСТИ ОТКРЫТЫХ КЛЮЧЕЙ В КРИПТОСИСТЕМЕ МАК-ЭЛИСА-СИДЕЛЬНИКОВА

В.А. ГОТОВКО, В.А. ЛИПНИЦКИЙ

Берлекэмп, Мак-Элис и Тилборг [1] установили NP-полноту ряда задач помехоустойчивого кодирования. На этой основе в 1978 г. Мак-Элис предложил криптосистему с открытым ключом [2], построенную на основе помехоустойчивого кодирования. Суть криптосистемы в следующем. Берется линейный (n, k)-код C над конечным полем F_q, исправляющий t ошибок (сам Мак-Элис за основу брал коды Гоппы). Как известно, такой код однозначно задается своей порождающей матрицей G порядка $k \times n$ над полем F_q. Абонент A с помощью секретного ключа — пары матриц H, Γ (H — произвольная невырожденная матрица над F_q, Γ — перестановочная), создает открытый ключ $E=H \cdot G \cdot \Gamma$, который рассылает заинтересо-

ванным лицам или делает его общедоступным. Абонент B передает абоненту A конфиденциальную информацию $\overline{m}$ - k - мерный вектор над F_q. Он зашифровывает сообщение в виде вектора $\overline{c} = \overline{m} \cdot E + \overline{z}$, где $\overline{z}$ вектор ошибок, корректируемый кодом C. Получатель, используя закрытый ключ и декодирующие алгоритмы, восстанавливает информацию. Мак-Элис предполагал, что атака на шифр возможна только перебором закрытых ключей (NP-полная задача). Позднее было замечено, что E является матрицей кода C', эквивалентному коду C. На этом основании в [3] В.М. Сидельниковым и С.О. Шестаковым установлено, что криптосистема Мак-Элиса на основе кодов Гоппы может быть вскрыта за полиномиальное время. Тем не менее, В.М. Сидельников [4] модифицирует криптосистему: а) предлагает за основу взять коды Рида-Маллера (длиной N), имеющие быстрые алгоритмы декодирования [5]; б) увеличивает секретный ключ, взяв в качестве такого $(\widetilde{H}, \widetilde{\Gamma})$, где $\widetilde{H} = (H_1, ..., H_u)$, H_1 — невырожденная $k \times k$ матрица, $\widetilde{\Gamma}$ — $uN \times uN$ перестановочная. Такая система имеет высокую скорость передачи и криптографическую стойкость. Это подтверждено, в частности, работой [6], где установлено точное значение мощности ключей $(\widetilde{H}, \widetilde{\Gamma})$ при u=2.

В докладе приводится и обосновывается значение мощности открытых ключей при $u = 3$, приводится оценка этой мощности для произвольного u.

Литература

1. Berlekamp E.R., McEliece R.J., van Tilborg H.C.A. On the Inherent Intractability of Certain Coding Problem. //IEEE Trans. Inf. Theory, 1978. V. 29. №3. - P. 384 – 386.
2. McEliece R.J. Public-key cryptosystem based on algebraic coding theory. //DSN Prog. Rep., Jet Prog. Lab., California Inst. Technol., Pasadena, 1978. - P. 114 – 116
3. Сидельников В.М., Шестаков С.О. О системе шифрования, построенной на осно-ве обобщенных кодов Рида-Соломона. //Дискр. матем., 1992. Т. 4, №3. - С. 57 – 63.
4. Сидельников В.М. Открытое шифрование на основе двоичных кодов Рида-Маллера. //Дискр. матем., 1994. Т. 6, №2. - С. 3 – 20.
5. Сидельников В.М., Першаков А.С. Декодирование кодов Рида-Маллера при боль-шом числе ошибок. //Пробл. передачи информации, 1992. Т. 28, №3. – С. 80 – 94.
6. Карпунин Г.А. О ключевом пространстве криптосистемы Мак-Элиса на основе двоичных кодов Рида-Маллера. //Дискр. матем., 2004. Т. 16, №2. – С. 79 – 84.