ЛИТЕРАТУРА

1. *Courtois N., Bard G., and Jefferson C.* Efficient Methods for Conversion and Solution of Sparse Systems of Low-Degree Multivariate Polynomials over GF(2) via SAT-Solvers. Cryptology ePrint Archive, Report 2007/024, 2007. http://eprint.iacr.org/2007/024
2. *Soos M., Nohl K., and Castelluccia C.* Extending SAT solvers to cryptographic problems // Proc. 12th Intern. Conf. Theory and Applications of Satisfiability Testing. 2009. P. 244–257.
3. *Charfi A.* SAT-Solving in Algebraic Cryptanalysis. Bachelor Thesis, 2014. https://www.cdc.informatik.tu-darmstadt.de/reports/reports/Ahmed_Charfi.bachelor.pdf
4. *Courtois N., Gawinecki J., and Song G.* Contradiction immunity and guess-then-determine attack on GOST // Tatra Mt. Math. Publ. 2012. V. 53. P. 65–79. https://www.sav.sk/journals/uploads/0114113604CuGaSo.pdf
5. *Kazymyrov O., Oliynykov R., and Raddum H.* Influence of addition modulo 2^n on algebraic attacks // Cryptography and Communications. 2016. V. 8. Iss. 2. P. 277–289.
6. *Dinur I., Dunkelman O., and Shamir A.* Improved attacks on full GOST // LNCS. 2012. V. 7549. P. 9–28. https://eprint.iacr.org/2011/558.pdf
7. *Nakahara J., Sepehrdad P., Zhang B., and Wang M.* Linear (hull) and algebraic cryptanalysis of the block cipher PRESENT // 8th Intern. Conf. Cryptology and Network Security CANS'09. N.Y., 2009. P. 58–75.
8. *Lacko-Bartosov L.* Algebraic cryptanalysis of PRESENT based on the method of syllogism // Tatra Mt. Math. Publ. 2012. V. 53. P. 201–212. https://www.sav.sk/journals/uploads/0114111812lackob.pdf
9. The Sage Developers. SageMath, the Sage Mathematics Software System (Version 7.4), 2016. http://www.sagemath.org
10. Sage Reference Manual: Cryptography Release 7.5. http://doc.sagemath.org/pdf/en/reference/cryptography/cryptography.pdf
11. *Бабенко Л. К., Ищукова Е. А.* Анализ алгоритма ГОСТ 28147-89: поиск слабых блоков // Известия ЮФУ. Технические науки. Информационная безопасность. 2014. №2 (151). С. 129–138.

УДК 519.725 DOI 10.17223/2226308X/10/27

КРИПТОГРАФИЧЕСКИЙ АНАЛИЗ ОБОБЩЁННОГО ПРОТОКОЛА ЭЛЬ-ГАМАЛЯ НАД ГРУППОЙ $\mathbf{GL}(8, \mathbb{F}_{251})$[1]

Д. Д. Болотов, Е. А. Магдин

Приводится криптографический анализ обобщённого протокола Эль-Гамаля над группой $\mathrm{GL}(8, \mathbb{F}_{251})$, описанного в работе Педро Хехта. Показано, что существует алгоритм, который эффективно вычисляет формируемый в протоколе ключ. Схема формирования общего ключа в обобщённом протоколе Эль-Гамаля является частным случаем схемы Шпильрайна — Ушакова. Анализ показывает, что рассматриваемый протокол является теоретически и практически нестойким.

Ключевые слова: *криптографический анализ, протокол Эль-Гамаля, протокол Шпильрайна — Ушакова.*

Введение

В работе рассматривается опубликованный в 2017 г. обобщённый протокол Эль-Гамаля [1], который в общем случае строится на группе матриц над конечным полем.

[1]Исследование выполнено при поддержке Российского научного фонда (проект №16-11-10002).

Автор [1] предлагает использовать конкретную группу матриц размера 8×8 над простым конечным полем $\mathbb{F}_{251}$. Схема формирования ключа в протоколе Хехта является частным случаем схемы из протокола Шпильрайна — Ушакова [2].

В [3] показано, что если протокол Шпильрайна — Ушакова (соответственно — протокол Хехта) построен на линейной группе, то существует эффективная процедура, вычисляющая формируемый общий ключ без знания и без вычисления секретных параметров протокола. Другими словами, показана криптографическая нестойкость протокола при указанном условии. В работе приводится конкретная реализация этой процедуры, которая в данном случае существенно упрощается.

1. Протокол формирования общего секретного ключа Хехта

Приведём описание протокола формирования общего секретного ключа из [1]. Предположим, что два корреспондента — Алиса и Боб — договорились о выборе линейной группы $\mathrm{GL}(8, \mathbb{F}_{251})$ и двух матриц G и P из $\mathrm{GL}(8, \mathbb{F}_{251})$.

В процессе получения открытого ключа Алиса выбирает натуральные числа $k_1, k_2 \in \mathbb{N}$ и диагональную матрицу $D_A = \mathrm{diag}(\lambda_1, \ldots, \lambda_8)$, $\lambda_i \in \mathbb{F}^*_{251}$. Затем она вычисляет матрицы $A = PD_AP^{-1}$ и $A' = A^{k_1}GA^{k_2}$. Открытым ключом Алисы является матрица A'.

Аналогичным образом Боб выбирает диагональную матрицу $D_B = \mathrm{diag}(\mu_1, \ldots, \mu_8)$, $\mu_i \in \mathbb{F}^*_{251}$, вычисляет матрицу $B = PD_BP^{-1}$, выбирает натуральные числа $r_1, r_2 \in \mathbb{N}$ и вычисляет матрицу $B' = B^{r_1}GB^{r_2}$. Открытым ключом Боба является матрица B'. Затем Алиса и Боб обмениваются ключами A' и B'.

После обмена ключами Алиса вычисляет сформированный ключ $K = A^{k_1}B'A^{k_2}$, а Боб вычисляет $K' = B^{r_1}A'B^{r_2}$. Несложно проверить, что ключи, полученные Алисой и Бобом, одинаковы:

$$K = A^{k_1}B'A^{k_2} = A^{k_1}(B^{r_1}GB^{r_2})A^{k_2} = B^{r_1}(A^{k_1}GA^{k_2})B^{r_2} = B^{r_1}A'B^{r_2} = K'.$$

2. Криптографический анализ протокола Хехта

Предположим, что Джон перехватывает все сообщения, которые отправляют между собой Алиса и Боб, знает протокол, с помощью которого Алиса и Боб обмениваются сообщениями, и следующие элементы протокола: $P, G, A', B' \in \mathrm{GL}(8, \mathbb{F}_{251})$.

Матрицы A' и B' Джон может представить следующим образом:

$$A' = A^{k_1}GA^{k_2} = (PD_AP^{-1})^{k_1}G(PD_AP^{-1})^{k_2} = (PD_A^{k_1}P^{-1})G(PD_A^{k_2}P^{-1}),$$
$$B' = B^{r_1}GB^{r_2} = (PD_BP^{-1})^{r_1}G(PD_BP^{-1})^{r_2} = (PD_B^{r_1}P^{-1})G(PD_B^{r_2}P^{-1}).$$

Любую диагональную матрицу $D \in \mathrm{GL}(8, \mathbb{F}_{251})$ можно представить как $D = \sum\limits_{k=1}^{8} \lambda_k E_k$, где $\lambda_k \in \mathbb{F}_{251}$; E_k — матрица, в которой k-й элемент на диагонали равен 1 ($e_{kk} = 1$), а все остальные равны 0. При разложениях $D_A^{k_1} = \sum\limits_{i=1}^{8} \alpha_i E_i$ и $D_A^{k_2} = \sum\limits_{j=1}^{8} \beta_j E_j$ матрица A' имеет вид

$$A' = (P\sum_{i=1}^{8} \alpha_i E_i P^{-1})G(P\sum_{j=1}^{8} \beta_j E_j P^{-1}) = \sum_{i,j=1}^{8} (P\alpha_i E_i P^{-1})G(P\beta_j E_j P^{-1}) =$$
$$= \sum_{i,j=1}^{8} \alpha_i\beta_j (PE_iP^{-1})G(PE_jP^{-1}) = \sum_{i,j=1}^{8} \delta_{ij}(PE_iP^{-1})G(PE_jP^{-1}), \text{ где } \delta_{ij} = \alpha_i\beta_j.$$

Значения δ_{ij} можно найти как решение соответствующей системы линейных уравнений, например методом Гаусса. После этого, подставив в правую часть вместо матрицы G матрицу B', Джон получит сформированный ключ K и сможет читать все сообщения, которые отправляют Алиса и Боб между собой:

$$\sum_{i,j=1}^{8} \delta_{ij}(PE_iP^{-1})B'(PE_jP^{-1}) = \sum_{i,j=1}^{8} \delta_{ij}(PE_iP^{-1})(PD_B^{r_1}P^{-1})G(PD_B^{r_2}P^{-1})(PE_jP^{-1}) =$$

$$= \sum_{i,j=1}^{8} (PD_B^{r_1}P^{-1}) \left(\delta_{ij}(PE_iP^{-1})G(PE_jP^{-1})\right) (PD_B^{r_2}P^{-1}) =$$

$$= (PD_B^{r_1}P^{-1}) \left(\sum_{i,j=1}^{8} \delta_{ij}(PE_iP^{-1})G(PE_jP^{-1}) \right) (PD_B^{r_2}P^{-1}) =$$

$$= B^{r_1} \left(\sum_{i,j=1}^{8} \delta_{ij}(PE_iP^{-1})G(PE_jP^{-1}) \right) B^{r_2} = B^{r_1}A'B^{r_2} = K.$$

Заключение

Данная атака основана на методе линейной разложимости [3]. Для её осуществления достаточно, чтобы протокол строился на линейной группе. Необходимые вычисления выполняются методом Гаусса, который квадратичен по числу уравнений и линеен по числу неизвестных. Заметим, что достаточно найти любое частное решение соответствующей системы линейных уравнений. Уравнений в данном случае 64 (число элементов в матрице), неизвестных 64 (коэффициенты в разложении). При атаке «грубой силой» пришлось бы подбирать параметры k_1, k_2, r_1 и r_2. Этот перебор может быть ограничен, но ограничение не может быть меньше, чем порядок мультипликативной группы поля для каждого из этих параметров. Кроме того, пришлось бы подбирать ненулевые элементы поля $\alpha_1, \ldots, \alpha_8, \beta_1, \ldots, \beta_8$. Размер этого ключевого пространства 250^{16}. Атака методом линейного разложения на рассматриваемый протокол является не только эффективной, но и практически реализуемой. От общей схемы атаки методом линейного разложения на протокол Шпильрайна — Ушакова [3] рассматриваемая атака отличается тем, что для неё нет необходимости строить базисы линейных подпространств, без чего не обойтись в общем случае.

ЛИТЕРАТУРА

1. *Hecht P.* Post-Quantum Cryptography (PQC): Generalized ElGamal Cipher over GF(251^8). arXiv:1702.03587v1 [cs.CR], 12 Feb 2017. 6 p.
2. *Shpilrain V. and Ushakov A.* Thompson's group and public key cryptography // LNCS. 2005. V. 3531. P. 151–164.
3. *Романьков В. А.* Алгебраическая криптография. Омск : Изд-во Ом. ун-та, 2013. 135 с.

УДК 003.26, 519.725 DOI 10.17223/2226308X/10/28

КВАДРАТ КОДА РИДА — МАЛЛЕРА И КЛАССЫ ЭКВИВАЛЕНТНОСТИ СЕКРЕТНЫХ КЛЮЧЕЙ КРИПТОСИСТЕМЫ МАК-ЭЛИСА — СИДЕЛЬНИКОВА

В. В. Высоцкая

Исследован вид классов эквивалентности секретных ключей криптосистемы Мак-Элиса — Сидельникова. Найден вид этих классов в случае, когда квадрат кода