Исследование стойкости задачи Диффи-Хеллмана в группе точек эллиптической кривой над конечным полем с помощью обращения спариваний

Герасимов Илья Юрьевич

Студент

Факультет ВМК МГУ имени М. В. Ломоносова, Москва, Россия

E-mail: ilia_gerassimov@mail.ru

Научный руководитель *— Черепнёв Михаил Алексеевич*

Задача Диффи-Хеллмана является значимым механизмом для криптосистем с открытым ключом и используется в протоколах согласования ключа [1]. По причине её широкого использования, а также наличия связи со сложностью задачи дискретного логарифмирования [2] актуален вопрос о стойкости задачи. Одним из подходов является анализ сложности задачи обращения спаривания, к которой задача Диффи-Хеллмана полиномиально сводится [3, 4]. В статье [5] был представлен алгоритм решения задачи обращения спаривания, имеющий полиномиальную сложность для некоторых эллиптических кривых с малой степенью расширения.

Однако для построенного спаривания размер области определения невелик, в результате чего вероятность получения решения по выполнению алгоритма мала. Для решения проблемы в работе предлагается построить достаточно большие собственные подпространства автоморфизма Фробениуса, для элементов которых процедура понижения степени рациональной функции спаривания выполняется. В результате была доказана следующая теорема.

Теорема 1. *Пусть задана эллиптическая кривая $E(\mathbb{F}_r)$ над простым полем $\mathbb{F}_r$ из $r \geq 3$ элементов фиксированного порядка $\#E(\mathbb{F}_r)$ с малой степенью расширения $k \leq C = \text{const}$. Пусть p —простой делитель $\#E(\mathbb{F}_r)$, отличный от r, Σ — универсальная экспонента группы точек эллиптической кривой над расширением поля $E(\mathbb{F}_{r^k})$. Тогда для любого r существует $\epsilon : 0 < \epsilon < 1$, что вероятность существования достаточно большого подпространства автоморфизма Фробениуса оценивается снизу как:*

$$Pr\left[\text{существует } X : \#\ker(\pi - [X]) \cap E(\mathbb{F}_{r^k}) \geq \frac{\#E(\mathbb{F}_{r^k})}{p}\right] \geq$$

$$\geq \left(1 - e^{-2\ln 2 + \frac{c_1}{\ln^2 2}}\right) \frac{1}{2^{(1+\epsilon)\ln(C \ln r)}},$$

где $c_1 = \text{const}, c_1 < 2\ln^3(2)$, *при условии, что в зависимости от значения* $\gamma_2(\Sigma)$ *— степени вхождения числа* 2 *в разложение* Σ *на простые множители, выполняется следующее:*

- *при* $\gamma_2(\Sigma) = 1$ *выполнено* $\#E(\mathbb{F}_r) \equiv 0 (\mathrm{mod}\, 2)$,
- *при* $\gamma_2(\Sigma) = 2$ *выполнено:*

$$\begin{cases} \#E(\mathbb{F}_r) \equiv 0 (\mathrm{mod}\, 4) \\ r \equiv 1 (\mathrm{mod}\, 4) \end{cases} \quad \textit{либо} \quad \begin{cases} \#E(\mathbb{F}_r) \equiv 2 (\mathrm{mod}\, 4) \\ r \equiv 3 (\mathrm{mod}\, 4) \end{cases},$$

- *при* $\gamma_2(\Sigma) \geq 3$ *выполнено* $\#E(\mathbb{F}_r) \equiv 0 (\mathrm{mod}\, 8)$ *и:*

$$r \equiv 3 (\mathrm{mod}\, 8) \textit{ либо } r \equiv 7 (\mathrm{mod}\, 8).$$

В качестве ограничения на степень расширения k можно рассматривать $C = 32$, так как в стандарте ГОСТ 34.10-2018 [6] требуется, чтобы $k \geq 31$.

Литература

1. Diffie W., Hellman M. New directions in cryptography // IEEE transactions on Information Theory. — 1976. — Т. 22. — № 6. — P. 644-654.
2. Черепнев М. А. О связи сложностей задач дискретного логарифмирования и Диффи–Хеллмана // Дискретная математика. — 1996. — Т. 8. — № 3. — С. 22-30.
3. Galbraith S., Hess F., Vercauteren F. Aspects of pairing inversion // IEEE Transactions on Information Theory. — 2008. — Т. 54. – № 12. – P. 5719-5728.
4. Черепнев М. А. Обращение спариваний для решения задачи дискретного логарифмирования // Фундаментальная и прикладная математика. — 2013. — Т. 18. — № 4. — С. 185-195.
5. Черепнёв М. А., Грачева С. С. Решение задачи Диффи-Хеллмэна на некоторых эллиптических кривых, удовлетворяющих ГОСТ 34.10-2018 // Информационные технологии. — 2020. — Т. 26. — № 3. — С. 159-168.
6. ГОСТ 34.10-2018 Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи. — 2019. — С. 20