О КРИПТОГРАФИЧЕСКОЙ ВЕРИФИКАЦИИ ПОЛИНОМИАЛЬНОГО ДЕЛЕНИЯ

М.М. Васьковский, Г.В. Матвеев

Белгосуниверситет, факультет прикладной математики и информатики, Минск, Беларусь
vaskovskii@bsu.by, matveev@bsu.by

Схемы разделения секрета лежат в основе многих криптографических протоколов в распределенных системах. Разделение секрета применяется для совместных конфиденциальных вычислений, шифрования на основе атрибутов и электронного защищенного голосования. Важной задачей в разделении секрета является построение таких схем, где пользователи могут проверить корректность секрета и тем самым не допустить обман со стороны остальных участников и дилера. Такие схемы строятся на основе протоколов с нулевым разглашением. В схемах верифицируемого разделения секрета дилер распределяет информацию о секретном значении среди участников таким образом, что для честных пользователей гарантируется получение ими значения секрета, а для нечестных — невозможность восстановить секрет.

Полиномиальное деление лежит в основе модулярного разделения секрета в кольцах от одной переменной над конечным полем. При этом секрет $S(x) \in \mathbb{F}_p[x]$ преобразуется в частичный секрет $s(x)$ путем деления $S(x)$ на открытый ключ участника $m(x) \in \mathbb{F}_p[x]$. Многочлен $m(x)$ выбирается неприводимым, а его старший коэффициент равен 1.

Таким образом, $S(x) = m(x)q(x) + s(x)$.

Разделение секрета в полиномиальных кольцах было предложено в работе [1]. Позднее оно было запатентовано в США [2], а недавно оно легло в основу стандарта РБ [3].

Целью верификации является подтверждение корректности вычисления многочлена $s(x)$, осуществляемого дилером. При этом участник не должен получать существенной информации о ключе $S(x)$.

В работе [4] получено частичное решение этой задачи. Предполагается, что поле $\mathbb{F}_p$ достаточно большое. Сейчас мы предлагаем решение задачи в общем случае. Предлагаемый протокол основан на следующих утверждениях.

Теорема 1. *Существует инъективное отображение поля разложения многочлена* $(S(x) - s(x))m(x)$ *в кольцо* $\mathbb{Z}$, *при котором условие делимости разности* $S(x) - s(x)$ *на многочлен* $m(x)$ *сохраняется.*

Теорема 2. *Для любого* $\alpha > 0$ *существует эффективно вычислимая постоянная* $c(\alpha)$ *такая, что для любых многочленов* $f(x)$, $g(x) \in \mathbb{Z}[x]$, *для которых высоты* $H(f)$, $H(g)$ *не превосходят* α *и старший коэффициент многочлена* $g(x)$ *равен* 1, *и любой целой постоянной* $c \geqslant c(\alpha)$ *делимость* $g(c) \mid f(c)$ *влечет делимость* $g(x) \mid f(x)$.

Литература

1. Galibus T. V., Matveev G. V. *Generalized Mignotte's sequences over polynomial rings* // ENTCS. 2007. V. 186. P. 43–48.

2. Schneider J. P. *Sharing a secret using polynomial division over gf(q).* US20100046739A1.

3. СТБ 34.101.60-2011 «*Информационные технологии и безопасность. Алгоритмы разделения секрета*», введен в действие с 01.07.2011 www.belgiss.org.by.

4. Галибус Т. В., Матвеев Г. В. *Верификация параметров модулярного разделения секрета* // Вестн. БГУ. Сер. 1. 2015. № 1. С. 76–79.