УДК 681.3.06

И.Д. ГОРБЕНКО, К.А. ПОГРЕБНЯК

Харьковский Национальный университет радиоэлектроники, Украина

КЛАССЫ СЛОЖНОСТЕЙ АЛГОРИТМОВ НА ОСНОВЕ БИЛИНЕЙНЫХ ОТОБРАЖЕНИЙ

В работе рассматривается взаимосвязи между проблемами дискретного логарифма, Диффи-Хелмана и билинейными проблемами Диффи-Хелмана. Мы рассматриваем известные отношения между вариациями проблем Диффи-Хелмана и предлагаем некоторую классификацию

билинейное отображение Вейля, билинейное отображение Тейта, билинейная проблема Диффи-Хелмана

Введение

В последнее время значительный интерес проявляется к ассиметричной криптографии, которая основана на билинейных отображениях [1]. Находят применение спаривания Вейля и Тейта, вернее их модификации [2]. Предложенные на основе спаривания точек эллиптических кривых протоколы дают ряд преимуществ. Представляют значительный интерес задачи оценки перспектив и дальнейшего развития подобных систем, а также их внедрения в существующие инфраструктуры.

Несмотря на гибкость протоколов, в основе которых лежат билинейные отображения, открытым остается вопрос повышения скорости вычислений. Требует особого внимания выбор эллиптических кривых пригодных для криптопреобразований, а также исследование свойств преобразований.

Немаловажным остается вопрос стойкости криптосистем на базе спариваний Вейля и Тейта. Считается, что в таких системах стойкость базируется на сложности решения проблем дискретного логарифма и проблем Диффи-Хелмана [3].

Допустим, что задано билинейное отображение $e: G \times G \to H$, где G, H – аддитивная и мультипликативная группы. Для заданных (g, ag, bg, cg) билинейная проблема Диффи-Хелмана (BDH) заключается в нахождении $e(g,g)^{abc}$ [4]. Хотя большинство протоколов основываются на проблеме BDH, тем не менее, ее сложность и связь с известными классами сложности до сих пор полностью не изучены. Известно, что проблема Диффи-Хелмана на G и H порождают проблему BDH [3]. Причем проблема Диффи-Хелмана на H связана с проблемой Диффи-Хелмана на G, если порядок группы G удовлетворяет определенным условиям, которые считаются справедливыми почти для всех простых порядков.

Для того чтобы говорить о связях в обратную сторону, необходимо чтобы билинейное отображение было обратимо. Поскольку билинейное отображение является функцией двух переменных, обратимость можно определить несколькими способами. Говорят, что билинейное отображение слабообратимо, если можно вычислить прообраз (g_1, g_2) элемента h, такой что $e(g_1, g_2) = h$ для произвольного $h \in H$. Пользуясь этим определением можно показать, что проблема Диффи-Хелмана на H и проблема Диффи-Хелмана на G, при определенных предположениях, эквивалентны BDH.

Рассмотрим более строгое определение. Пусть существует $g \in G$ такое, что можно с полиномиальной сложностью вычислить прообраз элемента h, а именно $e(g_1, g) = h$ для $h \in H$. В этом случае

проблема DH на G легко разрешима, а следовательно, и легко разрешима BDH проблема. Более общо, если задано билинейное отображение $e: G \times G \to H$, и существует инъективный гомоморфизм $f: H \to G$, тогда проблема DH на G эффективно разрешима. Как следствие, эффективно вычислимое невырожденное билинейное отображение $e_s: G \times G \to G$ не существует на группе G, если проблема DH, определенная на этой группе, трудно разрешима. Такой же результат в группах XTR представлен в работе [5].

Хотя BDH считается эквивалентной проблеме Диффи-Хелмана в определенных группах, но на сегодняшний день не существует доказательства этого предположения. Более того, сложная структура, делающая эллиптические кривые пригодными для билинейной криптографии, обеспечивает криптоаналитиков дополнительной информацией. Поскольку конструктивное использование спариваний является недавним открытием, поэтому еще не в достаточной мере изучены классы сложности и их связи.

Также необходимо отметить, что с появлением протоколов, основанных на билинейных спариваниях, наметилась тенденция использования значительного количества классов сложности. Эти классы, как правило, зависят от структуры протокола, поэтому сложно определить характер связей между этими проблемами. Не совсем ясны и связи с известными вычислительными проблемами в конечном поле и в группе точек эллиптической кривой. Потому, на сегодняшний день билинейная криптография в основном основывается на предположениях, вытекающих из эмпирического опыта.

Определение и характеристик и классов сложностей

Дадим основной перечень проблем, появляющихся в протоколах (табл. 1).

Пусть задана конечная мультипликативная группа H порядка n с образующим элементом h. Не ограничивая общности, предположим, что порядок группы простое число. Следовательно, H – циклическая и имеет единственный образующий элемент.

Таблица1

Классификация классов сложностей

<table>
<tr><th></th><th>Классические классы сложностей</th><th>Билинейные классы сложностей</th><th>Частные классы сложностей</th></tr>
<tr><td>Проблемы дискретного логарифма</td><td>Проблема дисктетного логарифма</td><td>Билинейная проблема дискретного логарифма</td><td></td></tr>
<tr><td rowspan="6">Проблемы Диффи-Хелмана</td><td rowspan="2">Вычислительная проблема Диффи-Хелмана</td><td rowspan="3">Билинейная проблема Диффи-Хелмана</td><td>Слабая DH проблема</td></tr>
<tr><td>Обратная DH проблема</td></tr>
<tr><td rowspan="2">Проблема принятия решения Диффи-Хелмана</td><td>(k+1)-экспоненциальная проблема</td></tr>
<tr><td rowspan="3">Промежуточная проблема Диффи-Хел-мана</td><td rowspan="3">Билинейная проблема принятия решения Диффи-Хелмана</td><td>k-обратная DH проблема</td></tr>
<tr><td>k-сильная DH проблема</td></tr>
<tr><td>Collusion Attack Algorithm with k-traitors</td></tr>
</table>

Проблема дискретного логарифма (DL). Пусть задан элемент $h_1 \in H$, такой что $h_1 = h^x$, $\forall x \in Z_n^*$. Под проблемой дискретного логарифма подразумевают нахождение элемента x при заданных h_1 и h. Обычно используется обозначение $DL_h(h_1) = x$.

Вычислительная проблема Диффи-Хелмана (CDH или DH). Пусть $a, b \in Z_n^*$. Для данных

h, $h_1 = h^a$, $h_2 = h^b$, вычислительная проблема Диффи-Хелмана задается нахождением элемента $h_3 \in H$, такого что $h_3 = g^{ab}$. Обозначается она как $CDH_h(h_1, h_2) = h_3$.

Проблема принятия решения Диффи-Хелмана (DDH). Пусть $a, b, c \in Z_n^*$.

При заданных h, $h_1 = h^a$, $h_2 = h^b$, $h_3 = h^c$ проблема принятия решения Диффи-Хелмана заключается в проверке выполняется ли сравнение вида $h_3 = h^{ab} (\mathrm{mod}\, n)$. Формализовано будем записывать

$$\begin{cases} DDH_h(h_1, h_2, h_3) = 1, & \text{если } CDH_h(h_1, h_2) = h_3; \\ DDH_h(h_1, h_2, h_3) = 0, & \text{в остальных случаях.} \end{cases}$$

Промежуточная проблема Диффи-Хелмана (GDH). Пусть $a, b \in Z_n^*$. Промежуточная проблема Диффи-Хелмана представляет собой решение $CDH_h(h^a, h^b)$ с возможностью эффективного разрешения проблемы принятия решения Диффи-Хелмана .

Пусть G аддитивная циклическая группа порядка n, H мультипликативная циклическая группа такого же порядка. Отображение $e: G \times G \to H$ называется симметрическим спариванием, если оно удовлетворяет следующим свойствам:

1) билинейность:

$$e(g_1 + g_2, g_3) = e(g_1, g_3) e(g_2, g_3)$$

и $e(g_1, g_2 + g_3) = e(g_1, g_2) e(g_1, g_3)$ для произвольных $g_1, g_2, g_3 \in G$;

2) строго невырождено: $e(g, g) \neq 1$;

3) вычислимо за полиномиальное время.

Пусть $e: G \times G \to H$ – симметрическое спаривание. Определим для него билинейную проблему Диффи-Хелмана таким образом

Билинейнаяная проблема Диффи-Хелмана (BDH). Пусть $a, b, c \in Z_n^*$. При заданных g, ag, bg, cg, билинейная проблема Диффи-Хелмана задается вычислением $e(g, g)^{abc}$. Обозначается она как $BDHg(ag, bg, cg) = e(g, g)^{abc}$.

Очевидно, что BDH не сложнее, чем CDH в группе G. Действительно, зная решение $Q = CDH_g(ag, bg)$, легко вычисляется $e(Q, cg) = e(g, g)^{abc}$. Аналогично вычисления проводятся и для случаев $Q = CDH_g(ag, cg)$ и $Q = CDH_g(bg, cg)$. Далее, BDH также зависит от сложности в группе H. Если задано $e(g, ag) = h^a$ и $e(bg, cg) = h^{bc}$, то вычислительная проблема Диффи-Хелмана заключается в нахождении элемента $h^{abc} = CDH_h(h^a, h^{bc}) = e(g, g)^{abc}$, что в точности является решением билинейной проблемы Диффи-Хелмана.

Билинейная проблема дискретного логарифма (BDL). Для произвольного элемента $g \in G$ BDL_g при заданных g, ag, bg определяется в виде процедуры вычисления такого t, что $e(ag, bg) = e(g, g)^t$. Обозначение $BDL_g(g, ag, bg) = ab$.

Билинейная проблема принятия решения Диффи-Хелмана (DBDH). Для произвольного элемента $g \in G$ $DBDH_g$ определяется следующим образом при заданных g, ag, bg, cg, h^w, где $h = e(g, g)$, определить выполнено ли сравнение $abc = w \bmod n$. Формализовано обозначим как

$$\begin{cases} DBDH_g(g, ag, bg, cg, h^w) = 1, & \text{если } abc = w; \\ DBDH_g(g, ag, g, cg, h^w) = 0, & \text{в остальных случаях.} \end{cases}$$

Слабая проблема Диффи-Хелмана (WDH). При заданных g_1, g_2, sg_1, где $g_1, g_2 \in G$, $s \in Z_n^*$, вычислить sg_2.

Обращение CDH проблемы (RCDH). При заданных g, ag, rg, где $a, r \in Z_n^*$, вычислить bQ, где $b \in Z_n^*$ и $a = rb \bmod n$.

(k+1)-экспоненциальная проблема. При заданных $g, yg, y^2 g, ..., y^k g$, где $y \in Z_g^*$, вычислить $y^{k+1} g$.

k-обратная проблема Диффи-Хелмана. При заданных $g, yg, y^2 g, ..., y^k g$, где $y \in Z_n^*$, вычислить $\frac{1}{y} g$.

k-сильная проблема Диффи-Хелмана. При заданных $g, yg, y^2 g, ..., y^k g$, где $y \in Z_n^*$, вычислить $c, \frac{1}{y+c} g$, где $c \in Z_n^*$.

Collusion Attack Algorithm with k-traitors. При заданных $g, yg, h_1, ..., h_k \in Z_n^*, \frac{1}{h_1 + y} g, ..., \frac{1}{h_k + y} g$, где $y \in Z_n^*$, вычислить $\frac{1}{h+y} g$, где $h \notin \{h_1, ..., h_k\}$.

Заключение

1. Проблемы дискретного логарифма и Диффи-Хелмана могут быть определены и взаимосвязаны через классические, билинейные и частные классы сложности.

2. Проблема BDH эквивалентна DH проблеме на *H*, когда билинейное отображение слабообратимо. Не известно, может ли условие слабообратимости быть ослаблено. Необходимо изучить, как свойство слабообратимости билинейного отображения влияет на сложность DH проблемы или BDH проблемы.

3. Появление новых протоколов порождает классы сложности, которые являются модификациями существующих классов. Необходима систематизация появившихся проблем и построение общей абстрактной модели.

4. Известно сведение более слабых классов к более сильным при определенных условиях, но остается открытым вопросом необходимые и достаточные условия

5. Необходимо построение общей модели оценки систем на базе билинейных отображений.

Литература

1. Boneh D., Franklin M. Identety Based Encryption from the Weil Pairing // Advances in Cryptology. – Crypto 2001, LNCS 2139, Springer-Verlag, – 2001. – P.213-229.

2. Sakai R., Ohgishi K., Kasahara M. Cryptosystems based on pairing // Proceedings of the 2000 Symposium on Cryptography and Information Security, Okinawa, Japan. – January 2000.

3. Cheon J.H., Lee D.H. Diffie-Hellman Problems and Bilinear Maps. Cryptology ePrint Archive, Report 2002/117.

4. Yacobi Y. A Note on the Bilinear Diffie-Hellman Assumption. Cryptology ePrint Archive, Report 2002/113 5.

5. Verhuel E. Evidence that XTR Is More Secure than Supersingular Elliptic Curve Cryptosystems // Advances in Cryptology. – ASIACRYPT 2001, LNCS 2248, Springer-Verlag, 2001. – P.533-551.

Поступила в редакцию 16.01.2007

Рецензент: д-р техн. наук, проф. В.И. Долгов, Харьковский национальный университет радиоэлектроники, Харьков.