УДК 681.322.067

Д.О. Косолапов, Е.А. Харин, С.М. Гончаров, П.Н. Корнюшин

Мультилинейные криптосистемы в асимметричной криптографии

Описаны три криптосистемы с использованием мультилинейных отображений. Внедрение мультилинейных криптосистем позволит значительно снизить связную сложность групповых криптопротоколов.

Асимметричные криптосистемы (криптосистемы с открытым ключом) были предложены в 1976 г. У. Диффи и М. Хеллманом. Их суть состоит в том, что каждым участником схемы генерируются два ключа, связанные между собой по определенному правилу. Один ключ является открытым и доступен всем участникам, а другой объявляется закрытым и сохраняется в тайне. Немного позднее были разработаны криптосистема RSA и семейство протоколов Эль-Гамаля.

Безопасность асимметричных криптосистем основана на сложности решения некоторых общеизвестных математических задач, таких как, например, задача факторизации целого числа и задача нахождения дискретного логарифма в конечном поле. Алгоритмы решения данных задач имеют субэкспоненциальную сложность, поэтому при определенных размерах ключей их решение полагают невозможным на современном этапе развития вычислительной техники.

В 90-х годах XX в. получили распространение асимметричные криптосистемы на эллиптических кривых, использующие в качестве базовой алгебраической структуры группу точек эллиптической кривой, заданной над конечным полем. Эллиптические криптосистемы получаются небольшим преобразованием схемы Эль-Гамаля, основаны на сложности решения задачи дискретного логарифма и обеспечивают аналогичный уровень безопасности при меньших длинах ключей.

В 2000 г. [1] была предложена первая билинейная криптосистема – криптосистема на основе билинейных спариваний в группе точек эллиптической кривой. Билинейное спаривание представляет собой отображение (функцию) $e : G_1 \times G_2 \to G_3$, для которого выполняется свойство билинейности $e(aP, bP) = e(P, P)^{ab}$, где G_1 и G_2 – торсионные подгруппы группы точек эллиптической кривой, заданной над конечным полем; G_3 – подгруппа мультипликативной группы конечного поля. Безопасность билинейных криптосистем основана на сложности получения одного из (или обоих) аргументов функции по известному значению функции и другого аргумента [2].

Билинейные спаривания позволили упростить некоторые криптосистемы, а также решить специфические задачи в криптографии. Например, с использованием билинейных спариваний легко реализуется схема шифрования на основе идентификационных данных (IBE) [3], в которой открытый ключ пользователя получается явным образом из его идентификатора, а закрытый генерируется и выдается Центром генерации закрытых ключей (далее – Центр).

Боне и Сильверберг [4] предложили обобщение билинейного спаривания и ввели понятие мультилинейной формы – отображения вида $\mu : \underbrace{G_1 \times G_1 \times \ldots \times G_1}_{n} \to G_2$, обладающего свойством мультилинейности, т.е. $\mu(a_1 P, a_2 P, \ldots, a_n P) = \mu(P, \ldots, P)^{\prod_{i=1}^{n} a_i}$. Использование мультилинейных форм позволит упростить большинство современных n-сторонних криптопротоколов. Однако вопрос построения конкретных мультилинейных отображений до сих пор остается открытым.

Мультилинейные криптосистемы могут быть построены путем обобщения некоторых билинейных криптосистем. Приведем описание трех мультилинейных схем.

Мультилинейная схема шифрования на основе идентификационных данных [3].

Данная схема является стойкой к атаке на основе выбранного шифртекста в модели со случайным оракулом при предположении сложности решения мультилинейной проблемы Диффи–Хеллмана. Пусть имеется n абонентов с идентификаторами $ID_1, \ldots, ID_n$, которым должно быть отправлено зашифрованное сообщение, при этом число и состав абонентов могут изменяться. Протокол состоит из алгоритмов инициализации, получения секретного ключа, шифрования и расшифрования. Пусть k – принимаемый протоколом на этапе инициализации параметр безопасности.

Инициализация

1. На основе k Центр генерирует простой порядок q групп G_1 и G_2, $2n$-мультилинейную форму $\mu : \underbrace{G_1 \times G_1 \times \ldots \times G_1}_{2n} \to G_2$ и произвольный образующий элемент группы $P \in G_1$.

2. Центр случайным образом выбирает $s_1, \ldots, s_n \in Z_q^*$ и вычисляет $P_{pub_1} = s_1 P, \ldots, P_{pub_n} = s_n P$.

3. Центр выбирает криптографические хеш-функции $H_1 : \{0,1\}^* \to G_1^*$, $H_2 : G_2 \to \{0,1\}^l$ для некоторого l, $H_3 : \{0,1\}^l \times \{0,1\}^l \to Z_q^*$ и $H_4 : \{0,1\}^l \to \{0,1\}^l$.

Пространством сообщений и шифртекстов являются множества $\mu = \{0,1\}^l$ и $C = G_1^* \times \{0,1\}^l$. $s_1,\ldots,s_n \in Z_q^*$ называются мастер-ключами абонентов. Системными параметрами является набор $\langle G_1, G_2, \mu, l, P, P_{pub_1},\ldots,P_{pub_n}, H_1, H_2, H_3, H_4\rangle$.

Получение секретного ключа

Для $ID_1,\ldots,ID_n \in \{0,1\}^*$:

1. Центр вычисляет $Q_{ID_1} = H_1(ID_1) \in G_1^*,\ldots,Q_{ID_n} = H_1(ID_n) \in G_1^*$.
2. Центр вычисляет закрытые ключи $d_{ID_1} = s_1 Q_{ID_1},\ldots,d_{ID_n} = s_n Q_{ID_n}$, где $s_1,\ldots,s_n$ — мастер-ключи.

Шифрование

Для шифрования сообщения M открытыми ключами $ID_1,\ldots,ID_n$ абонент выполняет следующие операции:

1. Вычисляет $Q_{ID_1} = H_1(ID_1) \in G_1^*,\ldots,Q_{ID_n} = H_1(ID_n) \in G_1^*$.
2. Выбирает случайное $\sigma \in \{0,1\}^l$.
3. Устанавливает $r = H_3(\sigma, M)$.
4. Вычисляет шифртекст $C = \langle rP, \sigma \oplus H_2(g^r), M \oplus H_4(\sigma)\rangle$,

где $g = \mu(Q_{ID_1},\ldots,Q_{ID_n} P_{pub_1},\ldots,P_{pub_n}) \in G_2^*$.

Расшифрование

1. Пусть $C = \langle U, V, W\rangle$ — шифртекст, полученный абонентом с идентификатором ID_i. Для расшифрования C абонент получает у Центра секретный ключ $d_{ID_i} \in G_1^*$ и вычисляет:

$$V \oplus H_2(\mu(Q_{ID_1},\ldots,Q_{ID_{i-1}}, d_{ID_i}, Q_{ID_{i+1}},\ldots,Q_{ID_n}, P_{pub_1},\ldots,P_{pub_{i-1}}, U, P_{pub_{i+1}},\ldots,P_{pub_n})) = \sigma.$$

2. Абонент вычисляет $W \oplus H_4(\sigma) = M$.
3. Далее вычисляет $r = H_3(\sigma, M)$ и проверяет $U = rP$. Если равенство ложно, то он не принимает шифртекст, в противном случае полагает, что M — открытый текст.

Корректность схемы подтверждается следующим выражением:

$$\mu(Q_{ID_1},\ldots,Q_{ID_{i-1}}, d_{ID_i}, Q_{ID_{i+1}},\ldots,Q_{ID_n}, P_{pub_1},\ldots,P_{pub_{i-1}}, U, P_{pub_{i+1}},\ldots,P_{pub_n}) =$$
$$= \mu(Q_{ID_1},\ldots,Q_{ID_n}, P_{pub_1},\ldots,P,\ldots,P_{pub_n})^{sr} = \mu(Q_{ID_1},\ldots,Q_{ID_n}, P_{pub_1},\ldots,P_{pub_n})^r = g^r.$$

Мультилинейный протокол подписи Боне, Линна и Шахема [5].

Пусть имеется n абонентов, которым необходимо совместно подписать сообщение m, при этом каждому из абонентов необходимо проверить подпись всех предыдущих (например, схема согласования служебной записки в компании). Условием реализации протокола является существование $2,3,\ldots,n,n+1$-мультилинейных форм $\mu_2,\mu_3,\ldots,\mu_n,\mu_{n+1}$.

Генерация ключа

Пусть $H_1 : \{0,1\}^* \to G_1^*$ — криптографическая хеш-функция. Закрытыми ключами является набор $x_1,\ldots,x_n \in Z_q^*$, открытыми ключами — набор $P_{pub_1} = x_1 P,\ldots,P_{pub_n} = x_n P$.

Подпись

По данному секретному ключу x_1 и сообщению $m \in \{0,1\}^*$ 1-й подписывающий вычисляет подпись $s = x_1 H_1(m)$ и отправляет ее второму абоненту, который осуществляет проверку подлинности подписи по предложенной ниже схеме. Затем вычисляет свою подпись $s = x_2 s$ и отправляет следующему абоненту. После подписи n абонентами сообщение m и подпись $s = x_1 \ldots x_n H_1(m)$ отправляются получателю.

Проверка подписи

По открытым ключам $P_{pub_1} = x_1 P,\ldots,P_{pub_n} = x_n P$, сообщению m и подписи s получатель проверяет равенство $\mu_{n+1}(P,\ldots,P,s) = \mu_{n+1}(P_{pub_1},\ldots,P_{pub_n}, H_1(m))$.

Данная схема основана на предположении существования GDH групп (CDH сложна в G_1). Подпись защищена от подделки при атаке на основе выбранных текстов в модели со случайным оракулом.

Мультилинейный протокол подписи Занг, Сафави-Наини и Сусило [6].

Данный протокол использует предположение о сложности проблемы $(k+1)$-й степени.

Аналогично предыдущему протоколу пусть имеется n абонентов, которым необходимо совместно подписать сообщение m, при этом каждому из абонентов необходимо проверить подпись всех преды-

дущих. Условием реализации протокола является существование $2,3,\ldots,n,n+1$-мультилинейных форм $\mu_2,\mu_3,\ldots,\mu_n,\mu_{n+1}$..

Генерация ключа

Открытыми параметрами схемы является набор $< G_1, G_2, q, n, \mu_2, \mu_3, \ldots, \mu_n, \mu_{n+1}, P, H >$. Закрытыми ключами является набор $x_1,\ldots,x_n \in Z_q^*$, открытыми ключами – набор $P_{pub_1} = x_1 P,\ldots,P_{pub_n} = x_n P$.

Подпись

По данному закрытому ключу x_1 и сообщению m первый абонент вычисляет подпись $S = \frac{1}{H(m)+x_1} P$ и отправляет ее второму абоненту, который осуществляет проверку подлинности подписи по предложенной ниже схеме. Затем второй абонент вычисляет свою подпись $S = \frac{1}{(H(m)+x_2)} S$ и отправляет следующему. После подписи n абонентами сообщение m и подпись $S = \frac{1}{(H(m)+x_1)(H(m)+x_2)\ldots(H(m)+x_n)} P$ отправляются получателю.

Проверка подписи

По набору открытых ключей $P_{pub_1},\ldots,P_{pub_n}$, сообщению m и подписи S получатель проверяет равенство

$$\mu_{n+1}(H(m)P + P_{pub_1}, H(m)P + P_{pub_2},\ldots,H(m)P + P_{pub_n}, S) = \mu_{n+1}(P,P,\ldots,P).$$

Данная криптосистема является стойкой к атакам на основе выбранных сообщений в модели со случайным оракулом.

Предложенные мультилинейные криптосистемы основаны на предположении сложности решения мультилинейной проблемы Диффи–Хеллмана, а именно вычислении $\mu(g,\ldots,g)^{a_1\ldots a_{n+1}}$ в группе G_2 по заданным значениям $g, g^{a_1},\ldots,g^{a_{n+1}}$ в группе G_1. Использование мультилинейных криптографических отображений позволит значительно уменьшить связную сложность рассматриваемых протоколов, сократив объем передаваемой информации, и потенциально может снизить вычислительную сложность алгоритмов. До настоящего времени не удалось построить криптографические мультилинейные отображения со степенью мультилинейности выше 2. Ведутся исследования по разработке таких отображений.

Литература

1. Joux A. A One Round Protocol for Tripartite Diffie-Hellman. Proceedings of ANTS 4, LNCS 1838. – 2000. P. 385–394.

2. Galbraith S., Hess F. and Vercauteren F. Aspects of Pairing Inversion. University of London, Technische Universirat Berlin, University of Leuven, 2007.

3. Boneh D. and Franklin M. Identity-based encryption from the Weil pairing, Crypto'2001, Lecture Notes in Computer Science, Springer–Verlag, 2001.

4. Boneh D. and Silverberg A. Applications of Multilinear Forms to Cryptography, 2002.

5. Boneh D., Lynn B., Shacham H. Short Signatures from the Weil Pairing. In proceedins of Asiacrypt, 2001.

6. Zhang F., Safavi-Naini R. and Susilo W. An Efficient Signature Scheme from Bilinear Pairings and it's Applications. PKC, 2004.

7. Sakai R., Ogishi K. and Kasahara M. Cryptosystems Based on Pairing. SCIS 2000-c20. – Okinawa, Japan. 2000. – January.

Косолапов Дмитрий Олегович
Дальневосточный государственный университет, аспирант

Харин Евгений Алексеевич
Дальневосточный государственный университет, аспирант

Гончаров Сергей Михайлович
Дальневосточный государственный университет, к.ф.-м.н., доцент

Корнюшин Павел Николаевич
Дальневосточный государственный университет
Директор ДВРУНЦ по проблемам информационной безопасности, д.ф.-м.н., профессор
Эл. почта: korn@ifit.phys.dvgu.ru.

S.M. Goncharov, P.N. Korniushin, D.O. Kosolapov, E.A. Kharin
This article describes three multilinear based cryptosystems

Implementation of multilinear cryptosystems lets us decrease group difficulty of multiparty cryptosystems.