УДК 621.391

МЕТОД КЛЮЧЕВОГО ХЕШИРОВАНИЯ НА ОСНОВЕ АРИФМЕТИКИ В ГРУППЕ ТОЧЕК ЭЛЛИПТИЧЕСКОЙ КРИВОЙ

к.т.н. А.А. Кузнецов, В.Е. Чевардин, к.т.н. В.Н. Лысенко
(представил д.т.н., проф. Ю.В. Стасев)

Рассматриваются методы ключевого хеширования для обеспечения целостности и доступности данных. Предлагается метод ключевого хеширования информации на основе арифметики в группе точек эллиптической кривой.

Постановка проблемы в общем виде, анализ литературы. Важным требованием безопасности информационных ресурсов в АСУ являются целостность и доступность, которые характеризуют способность системы противостоять несанкционированному изменению обрабатываемых и передаваемых данных. Эффективным механизмом обеспечения целостности и доступности является ключевое хеширование [1 – 6].

Суть хеширования состоит в формировании на основе односторонней криптографической функции сжатого образа сообщения, т.н. хеш-кода. На приемной стороне уполномоченный пользователь, знающий секретный ключ, проверяет соответствие хеш-кода принятому сообщению и принимает решение об его подлинности.

Большинство известных механизмов ключевого хеширования используют в качестве односторонней криптографической функции блочный симметричный криптоалгоритм [2]. Этот подход позволяет эффективно, с точки зрения производительности, реализовать процедуру хеширования информации.

Особое место в общей классификации занимают механизмы хеширования, основанные на использовании несимметричных криптоалгоритмов, например, на модульной арифметике [4 – 6]. Это позволяет, с одной стороны, построить гибкий механизм хеширования, стойкость которого базируется на некоторой теоретико-сложностной проблеме. С другой стороны, применение несимметричного криптоалгоритма позволяет отказаться от дорогостоящей рассылки секретных ключей по закрытым каналам связи и использовать протокол обмена открытыми ключами. В тоже время,

© к.т.н. А.А. Кузнецов, В.Е. Чевардин, к.т.н. В.Н. Лысенко, 2004

существенным недостатком такого подхода является низкая производительность несимметричных криптоалгоритмов [7].

Таким образом, актуальным представляется разработка и исследование методов ключевого хеширования, основанных на использовании несимметричных криптоалгоритмов и обладающих при этом высокими показателями производительности.

1. Несимметричные криптоалгоритмы и применение в хешировании. Несимметричные криптосистемы основаны на использовании некоторой теоретико-сложностной проблемы, общая классификация приведена на рис. 1. На рисунке приведены так же некоторые стандарты криптографического преобразования данных, которые основаны на соответствующей теоретико-сложностной проблеме.

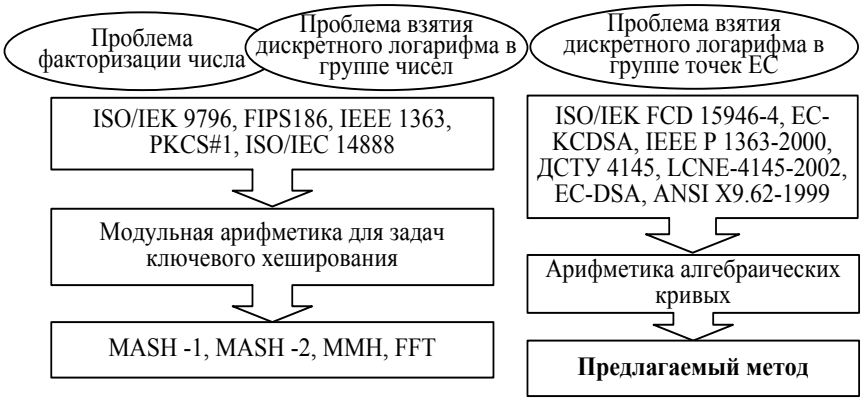

Рис. 1. Теоретико-сложностные проблемы, получившие применение в криптографии

Наибольшую популярность получили теоретико-сложностные проблемы факторизации числа и решения дискретного логарифма. В целях ключевого хеширования применение нашли криптоалгоритмы, основанные на проблеме факторизации числа. Это такие функции ключевого хеширования как MASH1 и MASH2 [4], MMH [5], FFT [6], отличающиеся как по производительности, так и по обеспечиваемой стойкости.

В тоже время, как показано в [8 – 9], использование дискретного логарифма в группе точек эллиптической кривой позволяет построить несимметричный криптоалгоритм, эффективность которого (по соотношению производительность/обеспечиваемая стойкость) существенно превосходит соответствующий показатель для криптосистем на модульной арифметике. Этот факт является веским основанием для разработки

ключевых функций хеширования, основанных на арифметике эллиптических кривых.

2. Предлагаемый метод ключевого хеширования. Воспользуемся понятием дискретного логарифма, введенного в [7].

Определение 1. Пусть H – конечная группа, g и y – элементы этой группы. Любое целое k, такое, что $g^k = y$ называется *дискретным логарифмом* y по основанию g. Каждый элемент $y \in H$ имеет дискретный логарифм по основанию g тогда и только тогда, когда H является циклической группой с образующей g. В общем случае известные алгоритмы вычисления дискретных логарифмов в группах порядка m имеют приблизительно одинаковую сложность с алгоритмами факторизации m [7 – 8].

Применительно к группе точек эллиптической кривой введем следующее понятие дискретного логарифма.

Определение 2. Пусть H_{EC} – конечная группа точек эллиптической кривой, P_i и P_j – элементы этой группы. Любое целое k, такое, что $kP_i = P_j$ называется *дискретным логарифмом на эллиптической кривой.* Криптостойкость алгоритмов, построенных на эллиптических кривых основана на трудности взятия дискретного логарифма и состоит в определении k по известным P_i и P_j.

Рассмотрим возможность применения теоретико-сложностной проблемы взятия дискретного логарифма в группе точек эллиптической кривой в целях ключевого хеширования.

Суть итерационной процедуры хеширования состоит в последовательной обработке поступающих данных. Последовательность входных данных *x* различной длины разбивается на конечное число блоков M_i и последовательно обрабатывается цикловой функцией f. Результатом работы такой хеш-функции является хеш-код h(x) – сжатый образ поступившего сообщения x. Общая схема цикловой хеш-функций представлена на рис. 2.

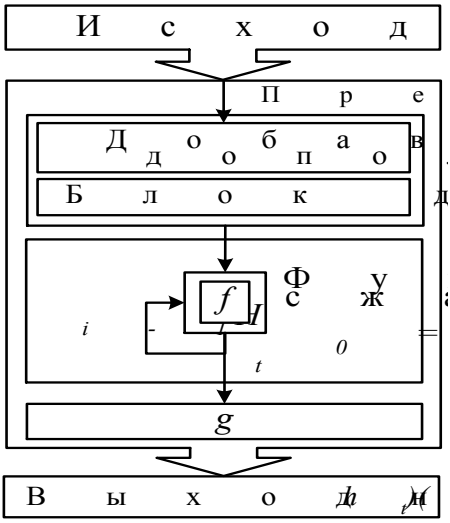

Рис. 2. Общая схема цикловой хеш-функции

Ядром цикловой хеш-функции, как видно из рис. 2, является цикловая функция f. Предлага-

ется два способа ключевого хеширования, основанных на проблеме взятия дискретного логарифма.

Способ 1. В качестве секретного параметра выступает скаляр k. Поступающие на вход блоки данных отождествляются точками кривой $M_i \rightarrow P_i$. Каждая точка, поступившая на вход цикловой функции, скалярно умножается на k. Цикловая функция осуществляет суммирование точек кривой, умноженных на соответствующий скаляр:

$$P_i = kP_i + kP_{i-1}.$$

После обработки последнего блока данных полученная точка P_t кривой отождествляется числом (координатой X), которое принимается за сжатый хеш-образ и поступает на выход в виде хеш-кода h(x). Начальное значение (первая точка в цикловой обработке) – точка импликации O, причем $O + P_i = P_i$, для любого i. Общая схема формирования хеш-кода представлена на рис. 3.

На рис. 4 приведен алгоритм формирования хеш-кода по способу 1.

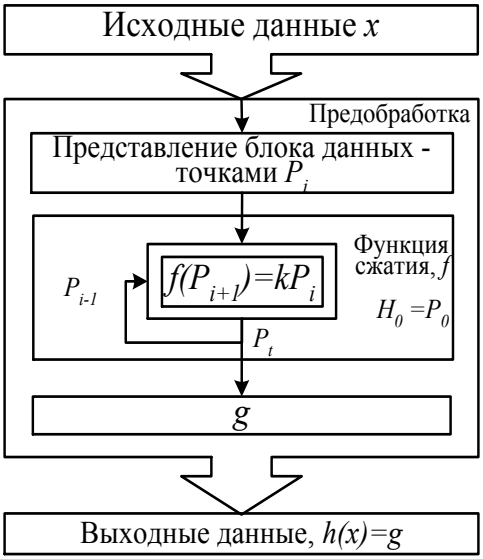

Рис. 3. Схема формирования хеш-кода (способ 1)

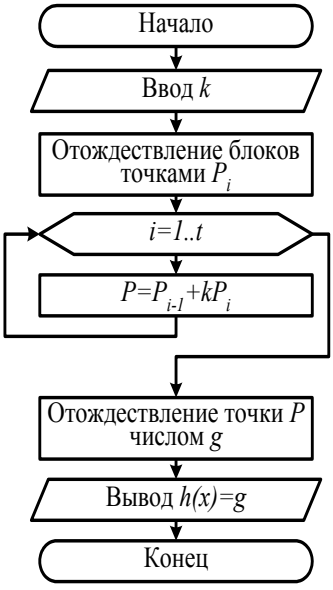

Рис. 4. Алгоритм формирования хеш-кода (способ 1)

Вычислительная сложность предлагаемого алгоритма определяется выражением:

$$I_1 = t \cdot I_a + t \cdot I_m. \qquad (1)$$

где t – количество блоков данных; I_a – сложность скалярного сложения; I_m – сложность скалярного умножения в группе точек эллиптической кривой.

Следует отметить, что использование групповых свойств точек эллиптической кривой позволяет значительно снизить сложность формирования хеш-кода в выражении (1). Справедливо утверждение.

Утверждение 1. Основную операцию цикловой функции $P_i = kP_i + kP_{i-1}$ можно заменить на итеративное сложение точек кривой с последующим умножением результирующей точки на скаляр k.

Доказательство. Действительно, в результате формирования хеш-кода цикловая функция последовательно выполняет операции умножения точек на скаляр k с их последующим суммированием, т.е. можно записать:

$$P_t = \sum_i kP_i$$

для всех i, как номеров поступающих на вход хеш-функции блоков данных M_i.

Групповые операции над точками эллиптической кривой ассоциативны, дистрибутивны, коммутативны [8 – 9]. Следовательно, запишем, что

$$P_t = k\sum_i P_i .$$

Очевидно, что хеш-образ, соответствующий точке P_t можно сформировать в результате итеративного сложения точек P_i кривой с последующим умножением на скаляр k, что завершает доказательство.

С учетом утверждения 1 выражение 1 перепишем в виде:

$$I_1 = t \cdot I_a + I_m. \qquad (2)$$

Для формирования хеш-кода в этом случае необходимо изменить алгоритм, приведенный на рис. 4 – умножение на скаляр производится один раз, на последнем цикле.

Рассмотрим другой способ формирования хеш-кода, так же основанный на использовании арифметики эллиптической кривой.

Способ 2. В качестве секретного параметра выступает базовая точка кривой Q. Поступающие на вход блоки данных отождествляются скалярами $M_i \rightarrow k_i$. Базовая точка умножается на соответствующий скаляр $k_i \cdot Q$. Цикловая функция осуществляет суммирование точек кривой, умноженных на соответствующий скаляр:

$$P_i = k_i \cdot Q + k_{i-1} \cdot Q.$$

После обработки последнего блока данных полученная точка P_t кривой отождествляется числом (координатой X), которое принимается за сжатый хеш-образ и поступает на выход в виде хеш-кода h(x).

Начальное значение (первый скаляр в цикловой обработке) – $k_1 = 1$, так, что $k_1 \cdot Q = Q$. Общая схема цикловой хеш-функций представлена на рис. 5.

На рис. 6 приведен алгоритм формирования хеш-кода по способу 1. Вычислительная сложность предлагаемого алгоритма определяется следующим выражением:

$$I_2 = I_1 = t \cdot I_a + t \cdot I_m. \quad (3)$$

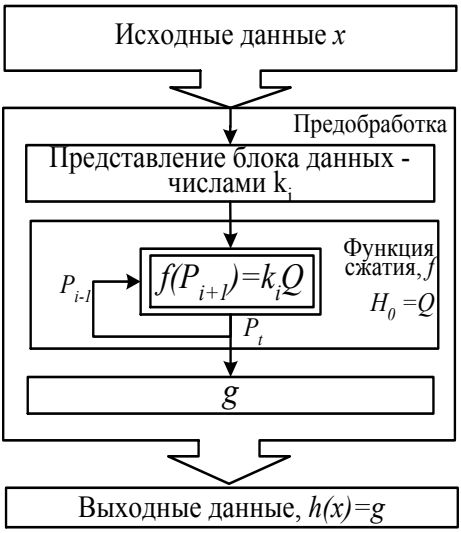

Рис. 5. Схема формирования хеш-кода по способу 2

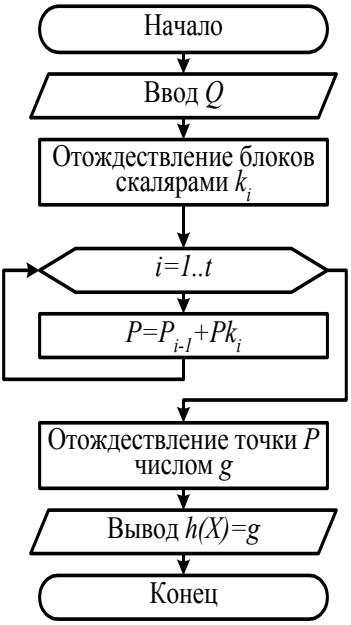

Рис. 6. Алгоритм формирования хеш-кода по способу 2

Воспользуемся групповыми свойствами точек эллиптической кривой. Справедливо следующее утверждение.

Утверждение 2. Основную операцию цикловой функции $P_i = k_i \cdot Q + k_{i-1} \cdot Q$ можно заменить на итеративное сложение скаляров k_i с последующим умножением результирующего скаляра на базовую точку Q.

Доказательство очевидно. По аналогии с утверждением 1 воспользовавшись свойствами ассоциативности, дистрибутивности и коммутативности группы точек эллиптической кривой следует перегруппировать сумму скаляров и умножения результата на точку Q.

Очевидно, что способ 2 по сложности реализации аналогичен способу 1.

Выводы. В результате проведенных исследований, разработан метод ключевого хеширования на основе арифметики эллиптических кривых. Стойкость ключевой хеш-функции основана на теоретико-сложностной проблеме взятия дискретного логарифма в группе точек эллиптической кривой. Предложено два способа формирования сжатого хеш-образа сообщения, которые отличаются видом цикловой функции и позволяют эффективно использовать групповые свойства точек эллиптической кривой в целях ключевого хеширования.

Перспективным направлением дальнейших исследований является исследование криптографических свойств предложенного метода ключевого хеширования на основе арифметики эллиптических кривых.

ЛИТЕРАТУРА

1. *ISO/IEC 10118-1. Information technology. Security techniques. Hash-functions. Part 1: General.*
2. *ISO/IEC 10118-2. Information technology. Security techniques. Hash-functions. Part 2: Hash-functions using an n-bit block cipher.*
3. *ISO/IEC 10118-3. Information technology. Security technique. Hash-functions. Part 3: Dedicated hash-functions.*
4. *ISO/IEC 10118-4. Information technology. Security techniques. Hash-function. Part 4: Hash-functions using modular arithmetic.*
5. *MMH: Software Message Authentication in the Gbit/second Rates / S. Halevi, H. Krawczuk. Extended Abstract, March, 1997. – 222 p.*
6. *FFT-Hash-II is not yet Collision-free. S.VAUDENAY. Liens-92-17, 1992.*
7. *Саломаа А. Криптография с открытым ключом: Пер. с англ. – М.: Мир, 1995. – 318 с.*
8. *Алгоритмические основы эллиптической криптографии / А.А. Болотов, С.Б. Гашков, А.Б. Фролов, А.А. Часовских. – М.: Мэи, 2000. – 240 с.*
9. *Silverman J., The Arifmetic of Ellipic Curves. – B.: Springer-Verlag, 1986. – 440 с.*

Поступила 20.10.2004

***КУЗНЕЦОВ Александр Александрович**, канд. техн. наук, старший научн. сотр., нач. НИЛ Харьковского университета Воздушных Сил. В 1996 году окончил Харьковский военный университет. Область научных интересов – криптографическое преобразование информации, алгебраическая теория кодов и их применение в системах передачи данных.*

***ЧЕВАРДИН Владислав Евгеньевич**, адъюнкт Полтавского военного института связи. В 2001 году окончил Харьковский военный университет. Область научных интересов – криптографическое преобразование информации.*

***ЛЫСЕНКО Валерий Николаевич**, начальник отдела научного центра ракетных войск и артиллерии Сумского военного института артиллерии. В 1985 году окончил ХВВКИУРВ. Область научных интересов – криптографическое преобразование информации.*