УДК 519.7

А.М. Иванцов, С.М. Рацеев

О ПРИМЕНЕНИИ ЭЛЛИПТИЧЕСКИХ КРИВЫХ В НЕКОТОРЫХ ПРОТОКОЛАХ АУТЕНТИФИКАЦИИ И РАСПРЕДЕЛЕНИЯ КЛЮЧЕЙ

Иванцов Андрей Михайлович, *кандидат технических наук, доцент, окончил Ленинградское высшее военное инженерное училище связи, Военную академию связи, очную адъюнктуру ВАС. Доцент кафедры «Информационная безопасность и теория управления» Ульяновского государственного университета. Имеет статьи, учебные пособия в области защиты информации. [e-mail: iwanzow@mail.ru].*

Рацеев Сергей Михайлович, *доктор физико-математических наук, доцент, окончил механико-математический факультет УлГУ. Профессор кафедры «Информационная безопасность и теория управления» УлГУ. Имеет статьи, учебные пособия в области криптографических методов защиты информации, PI-алгебр. [e-mail: ratseevsm@mail.ru].*

Аннотация

В работе рассматриваются криптографические протоколы аутентификации с нулевым разглашением знания и протоколы обмена ключами. Криптографические протоколы аутентификации, основанные на доказательстве знания с нулевым разглашением, позволяют проверить подлинность сторон без утечки секретной информации в течение информационного обмена. Протоколы обмена ключами позволяют формировать общие секретные ключи участников криптосистем. В работе предложены модификации некоторых криптографических протоколов открытого распределения ключей и криптографических протоколов аутентификации с нулевым разглашением знания: семейства протоколов MTI, трехпроходного протокола аутентификации Шнорра и протокола аутентификации на основе алгоритма Диффи-Хеллмана. Данные протоколы приводятся на основе эллиптических кривых, применение которых позволяет значительно уменьшить размеры параметров протоколов и увеличить их криптографическую стойкость. Стойкость приводимых протоколов основана на трудной задаче дискретного логарифмирования в группе точек эллиптической кривой.

Ключевые слова: криптографический протокол, протокол аутентификации, протокол распределения ключей, протокол Шнорра, эллиптическая кривая.

ON APPLICATION OF ELLIPTIC CURVES IN SOME AUTHENTICATION AND KEY DISTRIBUTION PROTOCOLS

Andrei Mikhailovich Ivantsov, *Candidate of Engineering; graduated from the Leningrad Higher Military Engineering School of Communications, the Military Academy of Communications; finished his postgraduate studies at the Military Academy of Communications; Associate Professor at the Department of Information Security and Control Theory of Ulyanovsk State University; an author of articles and textbooks in the field of information security. e-mail: iwanzow@mail.ru.*

Sergei Mikhailovich Ratseev, *Doctor of Physics and Mathematics, Associate Professor; graduated from the Faculty of Mechanics and Mathematics of Ulyanovsk State University; Professor at the Department of Information Security and Control Theory of Ulyanovsk State University; an author of articles and textbooks in the field of cryptographic methods of information security, PI-algebras. e-mail: ratseevsm@mail.ru.*

Abstract

Cryptographic authentication protocols with zero disclosure of knowledge and key exchange protocols are considered in the article. The cryptographic authentication protocols based on the proof of knowledge with zero disclosure allow to verify authenticity of the sides without leakage of the classified information during information exchange. Key exchange protocols allow to create the general secret keys of participants of cryptosystems. Modifications of some cryptographic protocols of open distribution of keys and such cryptographic authentication protocols with zero disclosure of knowledge as families of the MTI protocols, Shnor's triple-pass authentication protocol and authentication protocol on the basis of the Diffie-Hellman algorithm are offered. These protocols are provided on the basis of elliptic curves, which application allows to reduce considerably the sizes of protocols parameters and to increase their cryptography firmness. Firmness of the provided protocols is based on the difficult task of the discrete logarithmation in group of points of an elliptic curve.

Key words: cryptographic protocol, authentication protocol, key exchange protocol, Shnor's protocol, elliptic curve.

Введение

Одной из самых сложных задач управления ключами, возникающих в криптографии, является формирование общих секретных ключей участников криптосистем. *Протокол распределения ключей* — протокол получения пользователями ключей, необходимых для функционирования криптографической системы.

Протокол аутентификации – протокол установления подлинности сторон, участвующих во взаимодействии, но не доверяющих друг другу. Одной из основных целей протоколов аутентификации является обеспечение контроля доступа к определенным ресурсам, таким как банковские счета, базы данных с информацией ограниченного доступа, здания, сооружения и т. д.

Протоколы аутентификации разделяют на следующие классы: протоколы, основанные на паролях (слабая аутентификация); протоколы, использующие технику «запрос-ответ» (сильная аутентификация); протоколы, основанные на технике доказательства знания; протоколы доказательства знания с нулевым разглашением.

В парольных схемах злоумышленник может запомнить передаваемые сообщения и в следующий раз использовать эту информацию. В протоколах типа «запрос-ответ» злоумышленник, контролируя канал связи, может навязывать специально подобранные запросы и, анализируя ответы, получить информацию о секрете. Чтобы избежать этого, применяют протоколы доказательства знания (некоторой секретной информации), которые обладают дополнительным свойством нулевого разглашения секрета.

В данной работе рассматриваются протоколы открытого распределения ключей MTI и приводится их модификация на эллиптических кривых. Также приводится модифицированный трехпроходный протокол аутентификации Шнорра с нулевым разглашением и протокол аутентификации на основе алгоритма Диффи-Хеллмана. Данные протоколы приводятся на основе эллиптических кривых.

Сам принцип функционирования криптосистем на эллиптических кривых подробно изложен в [1]. Безопасность криптосистем на эллиптических кривых ECC (Elliptic Curve Cryptography), как правило, основана на трудности решения задачи дискретного логарифмирования в группе точек эллиптической кривой [1] (в отличие от совершенных криптосистем, которые не зависят от вычислительных мощностей криптоаналитиков [2, 3]).

Исследования показывают, что в классе криптосистем с открытым ключом криптосистемы на эллиптических кривых превосходят классические криптосистемы на основе модулярной арифметики, как минимум, по двум важным параметрам: степени защищенности в расчете на каждый бит ключа и быстродействию при аппаратной и программной реализациях. Наглядно это демонстрирует следующая таблица (размер ключей для ECC и RSA согласно NIST [4]):

Таблица 1

Размеры ключей для ECC и RSA согласно NIST

Ключ для ECC (длина в битах)	Ключ для RSA (длина в битах)	Отношение длин
163	1024	1:6
256	3072	1:12
384	7680	1:20
512	15360	1:30

Основное преимущество эллиптической криптографии заключается в том, что на данный момент неизвестно ни одного субэкспоненциального алгоритма решения задачи дискретного логарифмирования в группе точек эллиптической кривой. Поэтому криптостойкость приводимых ниже протоколов на эллитических кривых основана на данном факте и таблице 1.

Семейство протоколов MTI

Протоколы MTI были предложены Т. Мацумото, И. Такашима и Х. Имаи для защиты протокола Диффи-Хеллмана от атаки «противник в середине». Они предложили серию протоколов, предполагающих наличие у пользователей

открытых ключей и использующих модификации процедуры выработки общего ключа.

Пусть p – достаточно большое простое число, пользователи A и B имеют соответствующие секретные ключи $x_A (1 \le x_A \le p-2)$ и $x_B (1 \le x_B \le p-2)$ и публикуют свои открытые ключи $y_A = g^{x_A} (mod\ p)$, $y_B = g^{x_B} (mod\ p)$. В некоторых из представленных ниже протоколах используются x_A^{-1}, x_B^{-1}. В этом случае должны выполняться условия $НОД(x_A, p-1) = НОД(x_B, p-1) = 1$, $x_A^{-1}, x_B^{-1} \in \mathbf{Z}_{p-1}$. Кроме того, пользователи A и B должны сгенерировать соответствующие случайные числа $\alpha\ (1 \le \alpha \le p-2)$ и $\beta\ (1 \le \beta \le p-2)$.

В семействе протоколов MTI в общем случае для выработки общего секретного ключа k пользователи A и B обмениваются следующими сообщениями:

$A \to B$: $m_1 (mod\ p)$;

$A \leftarrow B$: $m_2 (mod\ p)$.

Затем участники A и B вычисляют соответствующие значения $k_A (mod\ p)$ и $k_B (mod\ p)$, причем общим секретным ключом становится значение $k_{AB} = k_A = k_B$ Протоколы MTI отличаются значениями m_1, m_2, k_A и k_B следующим образом:

Протокол	m_1	m_2	k_A	k_B	k_{AB}
MTI/A(0)	g^{α}	g^{β}	$\left(g^{\beta}\right)^{x_A} y_B^{\alpha}$	$\left(g^{\alpha}\right)^{x_B} y_A^{\beta}$	$g^{\alpha x_B + \beta x_A}$
MTI/B(0)	y_B^{α}	y_A^{β}	$\left(y_A^{\beta}\right)^{x_A^{-1}} g^{\alpha}$	$\left(y_B^{\alpha}\right)^{x_B^{-1}} g^{\beta}$	$g^{\alpha+\beta}$
MTI/C(0)	y_B^{α}	y_A^{β}	$\left(y_A^{\beta}\right)^{x_A^{-1}\alpha}$	$\left(y_B^{\alpha}\right)^{x_B^{-1}\beta}$	$g^{\alpha\beta}$
MTI/A(s)	$g^{\alpha x_A^s}$	$g^{\beta x_B^s}$	$\left(g^{\beta x_B^s}\right)^{x_A} y_B^{\alpha x_A^s}$	$\left(g^{\alpha x_A^s}\right)^{x_B} y_A^{\beta x_B^s}$	$g^{\beta x_A x_B^s + \alpha x_B x_A^s}$
MTI/B(s)	$y_B^{\alpha x_A^s}$	$y_A^{\beta x_B^s}$	$\left(y_A^{\beta x_B^s}\right)^{x_A^{-1}} g^{\alpha x_A^s}$	$\left(y_B^{\alpha x_A^s}\right)^{x_B^{-1}} g^{\beta x_B^s}$	$g^{\alpha x_A^s + \beta x_B^s}$
MTI/C(s)	$y_B^{\alpha x_A^s}$	$y_A^{\beta x_B^s}$	$\left(y_A^{\beta x_B^s}\right)^{x_A^{-1}\alpha x_A^s}$	$\left(y_B^{\alpha x_A^s}\right)^{x_B^{-1}\beta x_B^s}$	$g^{\alpha\beta x_A^s x_B^s}$

Любая подмена сообщений в данных протоколах приведет к тому, что все стороны получат различные значения ключа, что приведет к невозможности работы криптографической системы.

Ниже приводятся криптографические протоколы на эллиптических кривых, которые позволяют значительно уменьшить размер параметров протокола и увеличить криптографическую стойкость.

Модифицированное семейство протоколов MTI на эллиптических кривых

Любая криптосистема, основанная на дискретном логарифмировании может быть перенесена на эллиптические кривые. В этом случае операция $y = g^x (mod\ p)$ заменяется на $Y = [x]G$, где $[k]G = [k-1]G + G$. Пусть q – некоторый (достаточно большой) простой делитель числа $|E_p(a, b)|$, где $E_p(a, b)$ – эллиптическая кривая над полем $\mathbf{Z}_p$ вида

$$E_p(a,b): y^2 = x^3 + ax + b \pmod p.$$

Пусть некоторая точка $G \in E_p(a, b)$ имеет порядок q, т. е. образует циклическую подгруппу порядка q в аддитивной абелевой группе $(E_p(a, b), +)$:

$<G> = \{G, [2]\ G, ..., [q]G = \circ\}$.

Общедоступные параметры системы: $p, q, G, E_p(a, b)$. Абоненты A и B выбирают соответствующие секретные (положительные) ключи x_A и x_B, не превосходящие числа $q-1$. По каждому секретному ключу вычисляется открытый ключ:

A: $Y_A = [x_A]G$,

B: $Y_B = [x_B]G$.

В некоторых из представленных ниже протоколах используются x_A^{-1}, x_B^{-1}. В этом случае должно выполняться условие $x_A^{-1}, x_B^{-1} \in \mathbf{Z}_q$. Также пользователи A и B должны сгенерировать соответствующие случайные числа $\alpha\ (1 \le \alpha \le q-1)$ и $\beta\ (1 \le \beta \le q-1)$.

Модификация протокола MTI/A0. Для выработки общего секретного ключа k пользователи A и B обмениваются следующими сообщениями:

$A \to B$: $[\alpha]G$;

$A \leftarrow B$: $[\beta]G$.

Затем участники вычисляют следующие точки эллиптической кривой $E_p(a, b)$:

$$A: Z_A = [x_A]([\beta]G) + [\alpha]Y_B = [\beta x_A + \alpha x_B]G,$$

$$B: Z_B = [x_B]([\alpha]G) + [\beta]Y_A = [\alpha x_B + \beta x_A]G.$$

При этом $Z_A = Z_B$ Теперь абоненты A и B могут использовать, например абсциссу точки Z_A в качестве ключа k для секретной переписки.

Модификация протокола MTI/A(s). Для выработки общего секретного ключа k пользователи A и B обмениваются следующими сообщениями:

$$A \to B: \quad \left[\alpha x_A^s\right]G;$$

$$A \leftarrow B: \quad \left[\beta x_B^s\right]G.$$

Затем участники вычисляют следующие точки эллиптической кривой $E_p(a, b)$: