К. Г. Когос, С. Н. Кяжин, А. В. Юзбашев

О КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЕ ИНФОРМАЦИИ В ОБЛАЧНЫХ ИНФРАСТРУКТУРАХ: МЕТОДЫ PKI И IBE[1]

Введение

Согласно прогнозам экспертов, использование облачной архитектуры в России в ближайшие годы будет расти экспоненциально и к 2015 г. российский рынок облачных сервисов достигнет колоссального объема [1]. С точки зрения информационной безопасности требования обеспечения конфиденциальности, целостности и доступности информации остаются неизменными и для облачных сервисов. Тем не менее при организации защиты облачной инфраструктуры возникает ряд специфических задач, которые могут быть решены с использованием криптографических методов.

Для организации доверенного взаимодействия сторон по незащищенному каналу связи необходимо решать задачу согласования общего секретного ключа сессии. Существует большое количество схем выработки общего ключа [2]. Также среди факторов, затрудняющих защиту в облачных средах, можно отметить необходимость обеспечения корректного взаимодействия клиентов и серверов, находящихся в облачной инфраструктуре, иными словами, задачу аутентификации участников информационного обмена.

Криптосистема, в основе которой лежит технология аутентификации с помощью открытых ключей, подразумевает, что каждый пользователь имеет свой собственный закрытый ключ и связанный с ним открытый ключ [3]. Удостоверяющий центр публикует открытый ключ пользователя и выпускает сертификат, в котором указываются, в частности, идентификационные данные пользователя и его открытый ключ. Таким образом, криптосистемам, использующим PKI (Public Key Infrastructure), необходима система управления цифровыми сертификатами, которая, как правило, слишком сложна в обслуживании и функционировании [4].

А. Шамир первым ввел понятие криптографии на основе идентификационных данных [5], которая во многом могла бы уменьшить сложность, присущую традиционным асимметричным криптосистемам, из-за наличия системы управления цифровыми сертификатами. Лишь через 17 лет (в 2001 г.) удалось реализовать идею А. Шамира: использование технологии IBE (Identity Based Encryption) стало возможным благодаря отображениям «спаривания» [6], [7].

Спариванием называется невырожденное билинейное отображение e: $G_1 \times G_1 \rightarrow G_2$. Если для вычисления спаривания известен полиномиальный алгоритм, то его можно применять для создания криптосистем. Стойкость таких криптосистем основана на труднорешаемости билинейной проблемы Диффи — Хеллмана. Среди бесконечного множества спариваний выделяют 2 класса спариваний, часто используемых в эллиптической криптографии, — спаривание Вейля и спаривание Тейта.

Пусть $E(F_{q^k})$ — эллиптическая кривая над полем F_{q^k}, где k — характеристика поля, q^k — порядок поля, (0) — бесконечная точка. Для любой точки P: $P + (0) = (0) + P = P$. Если $P = (x,y)$, то $-P = (x, -y)$. Точка P кривой $E(F_{q^k})$ называется точкой r-кручения, если $[r]P = (0)$. Пусть $E[r]$ — множество точек r-кручения.

Спариванием Вейля называется отображение e_r: $E[r] \times E[r] \rightarrow F_{q^k}$, удовлетворяющее условиям:

1) билинейность: $e_r(P_1 + P_2,Q) = e_r(P_1,Q)\ e_r(P_2,Q)$, $e_r(P,Q_1 + Q_2) = e_r(P,Q_1)e_r(P, Q_2)$;

2) невырожденность: для любой конечной точки $P \in E[r]$ существует точка $Q \in E[r]$, такая, что $e_r(P,Q) \neq 1$;

3) альтернированность: $e_r(P,P) = 1$.

[1] Работа выполнена при поддержке «ИнфоТеКС Академия 2012».

Спариванием Тейта называется отображение $<x,x>: E(F_q)[r] \times E[r] \rightarrow F_{q^k}$, удовлетворяющее тем же условиям 1–3, что и спаривание Вейля.

Известна связь между спариваниями Тейта и Вейля [4]:

$$e_r(P,Q) = \frac{<P,Q>_r}{<Q,P>_r}.$$

Согласно этому соотношению считается, что для вычисления спаривания Вейля необходимо вычислить 2 спаривания Тейта. Заметим, что это соотношение верно только для данных классов спариваний.

В криптографии на основе идентификационных данных закрытый ключ генерируется и выпускается доверенным источником. Этот закрытый ключ соответствует открытому ключу пользователя, который генерируется из некоторых определенных строк (это может быть адрес электронной почты, мобильный телефон, имя пользователя и пр.), и подтверждает подлинность пользователя, не требуя при этом наличия его сертификата.

IBE-криптосистемы вполне могут заменить криптосистемы, использующие PKI, когда требуются эффективное управление ключами и умеренная защита. Стойкость таких систем базируется на предположениях о сложности решения различных проблем Диффи – Хеллмана. Однако, несмотря на очевидные преимущества идентификационной криптографии, имеются также и некоторые нерешенные задачи. Математический аппарат таких криптосистем непрерывно совершенствуется и основан на билинейном отображении, называемом «спаривание», которое с прикладной точки зрения представляет трудности из-за высокой трудоемкости вычисления.

1. Криптографические протоколы, которые возможно применить для защиты информации при облачных вычислениях

В контексте данной работы рассмотрены две различные схемы генерации общего ключа: протокол, основанный на спаривании, и протокол MQV. Для аутентификации данных, передаваемых по телекоммуникационным каналам, активно применяется технология электронной подписи. Создание и проверка электронных подписей – аспект криптографии, имеющий место как в криптосистемах, использующих PKI, так и в IBE-криптосистемах. Среди большого количества существующих схем электронной подписи рассмотрены две IBE-схемы – схема короткой подписи и схема ID-подписи, а также классическая схема цифровой подписи на эллиптической кривой ГОСТ Р 34.10-2012.

Протокол согласования ключа, основанный на спаривании Вейля [7]

Пусть l – порядок группы G точек эллиптической кривой, H – функция, переводящая открытые данные пользователя в число, $e(S,T)$ – отображение спаривания.

Настройка системы:

1. Центр генерации ключей выбирает $s \in \{1, ..., l-1\}$.

2. Центр генерации ключей выбирает случайную точку $P \in G$. Осуществляется вычисление $P_{KGS} = [s]P$.

3. Центр генерации ключей публикует (P_{KGS}, P).

4. Пользователь с определенным ID получает свой открытый ключ $Q_{ID} = H(ID)$.

5. Центр генерации ключей получает связанный с открытым ключом закрытый ключ $S_{ID} = [s]Q_{ID}$.

Выработка общего ключа:

Пусть два пользователя A и B хотят выработать общий ключ. Обозначим секретные ключи, полученные пользователями от центра генерации ключей, как $S_A=[s]Q_A$ и $S_B=[s]Q_B$.

1. Пользователи генерируют кратковременные закрытые ключи, назовем их a и b.

2. Обмен данными, соответствующими этим ключам: $T_A=[a]P$ и $T_b=[b]P$.

3. Пользователь A вычисляет общий секретный ключ $K_A = e([a]Q_B, P_{KGS})e(S_A, T_B)$.

4. Пользователь B вычисляет общий секретный ключ $K_B = e([b]Q_A, P_{KGS})e(S_B, T_A)$; тогда $K_A = e([a]Q_B, P_{KGS})e(S_A, T_B) = e(Q_B, P)^{as}e(Q_A, P)^{bs} = e(S_B, T_A)e([b]Q_A, P_{KGS}) = K_B$.

Протокол согласования ключа MQV [8]

Пусть E — эллиптическая кривая над F_q — конечное поле простой характеристики ρ. Осуществим проверку параметров домена $(q, a, b, P = (x_\rho, x_y), n, h)$, (0) — бесконечная точка, $\overline{R_A}$, $\overline{R_B}$ — константы протокола, (w_A, W_A) и (w_B, W_B) — пары закрытых и открытых ключей пользователей соответственно.

Проверка параметров:

1. Проверка, что $q = \rho^m$, где m — целое.

2. Проверка, что a, b, x_ρ, x_y принадлежат полю F_q.

3. Проверка, что P удовлетворяет уравнению кривой.

4. Проверка, что n простое, $n > 2^{160}$, n делит порядок кривой.

5. Проверка, что $[n]P = (0)$.

Вычисление $h' = \lfloor(\sqrt{q} + 1)/n\rfloor$ и проверка $h = h'$.

Выработка общего ключа:

1. A генерирует случайное число r_a, $1 < r_a < n - 1$, вычисляет точку $R_A = [r_a]P$ и отправляет B.

2. B генерирует случайное число r_b, $1 < r_b < n - 1$, вычисляет точку $R_B = [r_b]P$ и отправляет A.

3. A проверяет, принадлежит ли R_B группе точек и на равенство нулю; если проверка не пройдена, то протокол прерывается.

4. A вычисляет $s_A = (r_a + \overline{R_A}w_A) \bmod n$, вычисляется $K = [hs_A](R_B + \overline{R_B}W_B)$. Если $K = (0)$, то A прерывает протокол.

5. B проверяет, принадлежит ли R_A группе точек и на равенство нулю; если проверка не пройдена, протокол прерывается.

6. B вычисляет $s_B = (r_b + \overline{R_B}w_B) \bmod n$, вычисляется $K = [hs_B](R_A + \overline{R_A}W_A)$. Если $K = (0)$, то B прерывает протокол.

7. Точка K — общий секретный ключ.

Схема короткой подписи (Short Signature) [9]

Генерация ключей:

$H:\{0,1\}^* \to G_1$ — хэш-функция, G_1 — группа точек эллиптической кривой, $e(S,T)$ — отображение спаривания, $P \in G_1$ — точка порядка q. Закрытый ключ x — случайное число из Z_q^*, открытый ключ $P_{pub} = [x]P$.

Подпись:

Для ключа x и текста m вычисление подписи: $\sigma = [x]H(m)$.

Проверка:

Для данного открытого ключа $P_{pub} = [x]P$, текста m и подписи σ проверяем $e(P,\sigma) = e(P_{pub}, H(m))$.

Схема ID-подписи (ID based signature from Pairing) [10]

Установка:

Пусть $H_1:\{0,1\}^* \to G_1$, $H:\{0,1\}^* \times G_2 \to Z_q^*$ — хэш-функции, G_1 — группа точек эллиптической кривой, G_2 — мультипликативная группа, $e(S,T)$ — отображение спаривания. Выбираем закрытый ключ s из Z_q^* случайным образом и вычисляем открытый ключ $P_{pub} = [s]P$, где P — точка порядка q.

Генерация ключей:

Для идентификатора ID $\in \{0,1\}^*$ вычисляем открытый ключ $Q_{ID} = H_1(ID)$ и закрытый ключ $S_{ID} = [s]Q_{ID}$.

Подпись:

Для закрытого ключа S_{ID} и сообщения $m \in \{0,1\}^*$ подписывающий выбирает случайную точку $P_1 \in G_1$ и случайное $k \in Z_q^*$ и вычисляет

1. $r = e(P_1,P)^k$.
2. $v = H(m,r)$.
3. $u = [v]S_{ID} + [k]P_1$.

Подпись — это пара $(u,v) \in G_1 \times Z_q^*$.

Проверка:

Для открытого ключа Q_{ID}, сообщения m и подписи (u,v) проверка происходит следующим образом:

1. $r = e(u,P)e(Q_{ID}, -P_{pub})^v$.
2. Подпись корректна, если $v = H(m,r)$.

Схема цифровой подписи на эллиптической кривой ГОСТ Р 34.10-2012 [11]

Подпись:

Исходными данными этого процесса являются ключ подписи d и подписываемое сообщение M.

1. $h = H(M)$, $H:\{0,1\}^* \to \{0,1\}^n$.
2. $E = \alpha(\mathrm{mod}\ q)$, α— число, для которого двоичным представлением является вектор h; если $e = 0$ положить $e = 1$.
3. Генерация случайного числа k: $0 < k < q$, где q — порядок группы точек одной из эллиптических кривых, описанных в стандарте.
4. Вычислить точку $C = [k]P$, $r = x_c(\mathrm{mod}\ q)$, где P — точка порядка q.
5. Вычислить значение $s = (rd + ke)(\mathrm{mod}\ q)$, d — ключ подписи.
6. Вычислить двоичные векторы $r`$ и $s`$, соответствующие числам r и s. Подписью является конкатенация $r`$ и $s`$ $(r`\|s`)$.

Проверка:

Исходными данными этого процесса являются подписанное сообщение M, цифровая подпись и ключ проверки подписи Q.

1. Вычислить числа r и s, если $0 < r < q$ и $0 < s < q$, то перейти к следующему шагу, иначе прекратить проверку.
2. Вычислить значение $h = H(M)$.
3. Вычислить значение $e = \alpha(\mathrm{mod}q)$, α — число, для которого двоичным представлением является вектор h; если $e = 0$ положить $e = 1$.
4. Вычислить значение $v = e^{-1}(\mathrm{mod}\ q)$.
5. Вычислить значение $z_1 = sv(\mathrm{mod}\ q)$, $z_2 = -rv(\mathrm{mod}\ q)$.
6. Вычислить точку эллиптической кривой $C = [z_1]P + [z_2]Q$, $R = x_c(\mathrm{mod}\ q)$.
7. Если $R = r$, то подпись верна.

Заметим, что существуют также протоколы аутентификации, основанные на спаривании и специальным образом спроектированные для использования в облачных инфраструктурах. Описание их реализации, затрат на коммуникации и вычислительных затрат содержится, например, в работе [10].

2. Труднорешаемые математические проблемы, на которых основана стойкость исследуемых криптографических протоколов

Исследуем математические проблемы, обеспечивающие криптографические качества рассматриваемых протоколов.

1. Стойкость *протокола согласования ключа MQV* и *цифровой подписи на эллиптической кривой ГОСТ Р 34.10-2012* основана на проблеме дискретного логарифмирования (DLP). Даны P, Q; необходимо найти такое a, что $[a]P = Q$.

2. Стойкость *схемы короткой подписи* основана на вычислительной проблеме Диффи – Хеллмана (CDH). Даны $\langle P,[a]P,[b]P\rangle$, где $a,b \in Z_q^*$. Необходимо вычислить $[ab]P$.

Утверждение 1. Если DLP легко решаема, то CDH легко решаема.

Доказательство. Если DLP легко решаема, то по известным P, $[a]P$ можно найти a. Тогда из данных $P,[a]P,[b]P$ находятся a,b, вычисляется ab и затем $[ab]P$.

3. Стойкость *протокола согласования ключа на спаривании Вейля* основана на билинейной проблеме Диффи – Хеллмана (BDH). Даны $\langle P,[a]P,[b]P,[c]P\rangle$ для некоторых $a,b,c \in Z_q^*$. Необходимо вычислить спаривание, заданное на группах G_1 и G_2, $e(P,P)^{abc}$.

Утверждение 2. Пусть существует билинейное спаривание на (G_1,G_2). Тогда если CDH легко решаема в G_1 или G_2, то BDH также легко решаема.

Доказательство. Если CDH легко решаема в G_1, то можно вычислить $[ab]P$ с помощью $[a]P$ и $[b]P$, тогда $e(P,P)^{abc} = e([ab]P,[c]P)$. Если CDH легко решаема в G_2, то можно вычислить элементы $g = e(P,P)$, $g^{ab} = e([a]P,[b]P)$ и $g^c = e(P,[c]P)$, затем еще раз решить CDH в G_2 и получить g^{abc}.

4. Стойкость *схемы ID-подписи* основана на слабой проблеме Диффи – Хеллмана (WDH). Она заключается в следующем: даны $P,Q,[a]P$. Необходимо найти $[a]Q$.

Утверждение 3 [12]. Если CDH легко решаема, то WDH легко решаема.

Стоит отметить, что также существуют и иные математические проблемы, которые могут быть использованы для обоснования стойкости протоколов, применяемых при защите информации в облачных вычислениях [12–14].

Проведенные исследования показывают, что стойкость классических криптосистем с открытым ключом сводится к труднорешаемости проблем DLP, CDH. Стойкость криптосистем на основе идентификационных данных базируется на труднорешаемости проблемы BDH. В работе выявлена взаимосвязь данных проблем и показано, что при правильном выборе групп, над которыми осуществляется спаривание, сложность решения BDH не ниже сложности решения DLP, CDH в группах, над которыми осуществляется спаривание. Таким образом, на сегодняшний день не найдено доказательств того, что спаривание ослабляет криптографические качества групп, над которыми оно осуществляется.

Единственным фактором, ограничивающим применение IBE-криптографии, остается высокая трудоемкость вычисления спаривания. Рассмотрим вычисления, необходимые для применения исследуемых протоколов.

3. Трудоемкость применения исследуемых криптографических протоколов

1. Вычислительные затраты на применение схемы короткой подписи.

Подпись: одно вычисление значения хэш-функции, одно возведение в степень в группе точек эллиптической кривой.

Проверка: одно возведение в степень в группе точек эллиптической кривой, два вычисления преобразования спаривания.

2. Вычислительные затраты на применение схемы ID-подписи.

Подпись: одно вычисление преобразования спаривания, одно возведение в степень в G_2, одно вычисление значения хэш-функции, три возведения в степень в группе точек эллиптической кривой.

Проверка: два вычисления преобразования спаривания, одно возведение в степень в G_2, одно вычисление значения хэш-функции.

3. Вычислительные затраты на применение схемы цифровой подписи ГОСТ Р 34.10-2012.

Подпись: одно вычисление значения хэш-функции, три приведения по модулю, два умножения, одно нахождение обратного элемента, одно возведение в степень в группе точек эллиптической кривой.

Проверка: одно вычисление значения хэш-функции, пять приведений по модулю, одно нахождение обратного элемента, два умножения, два возведения в степень в группе точек эллиптической кривой.

4. Вычислительные затраты на применение протокола, основанного на спаривании Вейля.

Каждой стороне необходимо произвести возведение в степень в группе точек эллиптической кривой, одно умножение в G_2, два вычисления преобразования спаривания.

5. Вычислительные затраты на применение протокола MQV.

Каждой стороне требуется произвести ряд вычислений, а именно пять операций умножения и три операции сложения.

Отсюда следует, что актуальной является задача понижения трудоемкости вычисления спаривания. В частности, авторами исследуется возможность понижения трудоемкости вычисления спаривания путем распараллеливания итераций алгоритма Миллера [7], который используется для вычисления спаривания Тейта.

СПИСОК ЛИТЕРАТУРЫ:

1. Безопасность облачных сред / PCWeek [Электронный ресурс]. URL: http://www.pcweek.ru/security/article/detail.php?ID=139185 (дата обращения: 10.04.2014).
2. *Шнайер Б.* Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. Новгород: Триумф, 2002. — 860 с.
3. *Menezes A., Van Oorschot P., Vanstone S.* Handbook of Applied Cryptography. Boca Raton: CRC Press, 1996. — 780 с.
4. *Gentry C.* Certificate-based encryption and the certificate revocation problem. International Conference on the Theory and Applications of Cryptographic Techniques, Warsaw, Poland, 2003. С. 272—293.
5. *Shamir A.* Identity-based cryptosystems and signature schemes. Proceedings of CRYPTO 84. The Weizmann Institute of Science, Rehovot, 1985. С. 47—53.
6. *Boneh D., Franklin M. K.* Identity-Based Encryption from the Weil Pairing Advances in Cryptology. CRYPTO 2001. Santa Barbara, California, USA, 2001. С. 586—615.
7. *Болотов А. А., Гашков С. Б., Фролов А. Б., Часовских А. А.* Элементарное введение в эллиптическую криптографию. М:.КомКнига, 2006. — 356 с.
8. *Гончаров С.М.* О перспективах развития асимметричных криптосистем с упрощенной инфраструктурой. Научная сессия МИФИ-2006. XIII Всероссийская научная конференция. Проблемы информационной безопасности в системе высшей школы. С. 43—44.
9. *Boneh D., Lynn B., Shacham H.* Short signatures from the Weil pairing. Asiacrypt 2001. J. of Cryptology, Vol. 17, No. 4, 2001. С. 297—319.
10. *Li H., Dai1 Y., Tian L., Yang H.* Identity-based authentication for cloud computing. First International Conference, CloudCom 2009, Beijing, China, 2009. С. 157—166.
11. ГОСТ Р 34.10-2012. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи.
12. *Dutta R., Barua R., Sarkar P.* Pairing-based cryptographic protocol: a survey. Kolkata, India, 2004. — 45 с.
13. *Diffie W., Hellman M. E.* New directions in cryptography. Information Theory, IEEE Transactions, 1976. С. 644—654.
14. *Boneh D.* The decision Diffie-Hellman problem. Lecture notes in computer science. Third Algorithmic Number Theory Symposium, Lecture Notes in Computer Science, Vol. 1423, Springer-Verlag, 1998. С. 48—63.

REFERENCES:

1. Bezopasnost oblachnyih sred / PCWeek. URL: http://www.pcweek.ru/security/article/detail.php?ID=139185 (Date of access: 10.04.2014).

2. *Schneier B*. Applied Cryptography. New-York: John Wiley & Sons, Inc. 1995. — 810 p.
3. *Menezes A., Van Oorschot P., Vanstone S*. Handbook of Applied Cryptography. Boca Raton: CRC Press, 1996. — 780 p.
4. *Gentry C*. Certificate-based encryption and the certificate revocation problem. International Conference on the Theory and Applications of Cryptographic Techniques, Warsaw, Poland, 2003. P. 272—293.
5. *Shamir A*. Identity-based cryptosystems and signature schemes. Proceedings of CRYPTO 84. The Weizmann Institute of Science, Rehovot, 1985. P. 47—53.
6. *Boneh D., Franklin M. K*. Identity-Based Encryption from the Weil Pairing Advances in Cryptology. CRYPTO 2001. Santa Barbara, California, USA, 2001. P. 586—615 .
7. *Bolotov A. A., Gashkov S. B., Frolov A. B., Chasovskih A. A*. Elementarnoe vvedenie v ellipticheskuyu kriptografiyu.M:. ComKniga, 2006. — 356 p.
8. *Goncharov S. M*. O perspektivah razvitiya asimmetrichnyih kriptosistem s uproschennoy infrastrukturoy. Problemi informacionoi bezopasnosti v sisteme vishei shkoli. Moscow: Mephi 2006.
9. *Boneh D., Lynn B., Shacham H*. Short signatures from the Weil pairing. Asiacrypt 2001. J. of Cryptology, Vol. 17, No. 4, 2001. P. 297—319.
10. *Li H., Dai1 Y., Tian L., Yang H*. Identity-based authentication for cloud computing. First International Conference, CloudCom 2009, Beijing, China, 2009. P. 157—166.
11. GOST R 34.10-2012. Informatsionnaya tehnologiya. Kriptograficheskaya zaschita informatsii. Protsessyi formirovaniya i proverki elektronnoy tsifrovoy podpisi.
12. *Dutta R., Barua R., Sarkar P*. Pairing-based cryptographic protocol: a survey. Kolkata, India, 2004 — 45 p.
13. *Diffie W., Hellman M. E*. New directions in cryptography. Information Theory, IEEE Transactions, 1976. P. 644—654.
14. *Boneh D*. The decision Diffie-Hellman problem. Lecture notes in computer science. Third Algorithmic Number Theory Symposium, Lecture Notes in Computer Science, Vol. 1423, Springer-Verlag, 1998. P. 48—63.