УДК 681.3.06

СРАВНИТЕЛЬНЫЙ АНАЛИЗ ПРОТОКОЛОВ СОГЛАСОВАНИЯ ОБЩЕГО КЛЮЧА НА ОСНОВЕ ИДЕНТИФИКАЦИОННЫХ ДАННЫХ

Кравченко П.А., аспирант, **Макутонина Л.В.**, магистр
(Харьковский национальный университет радиоэлектроники)

Проведен краткий обзор протоколов согласования ключа. Приведены результаты сравнительного анализа данных протоколов и анализ свойств безопасности протокола, предложенного Баруа, Даттой и Саркаром

Введение. Посредством использования криптографических систем на идентификаторах стало возможным построение многосторонних протоколов согласования общего ключа, то есть построение безопасного канала взаимодействия между пользователями системы [1]. Схема формирования общего ключа, позволяющая двум участникам установить общий секретный ключ, была впервые предложена Диффи-Хелманом. Однако этот протокол оказался незащищенный от атаки типа «человек-по-середине». Для защиты от этой атаки позже было предложено большое количество протоколов аутентификации. Но большинство из них использует инфраструктуру открытых ключей (PKI), поддержка которой является довольно трудоемкой задачей. Первый протокол согласования общего ключа с аутентификацией на идентификаторах, использующий билинейные спаривания, был предложен Смартом. Этот протокол базировался на идее Боне-Франклина и на идее трехстороннего протокола Жу. Однако в дальнейшем была показана его уязвимость. В дальнейшем было предложено большое количество подобных протоколов, но большинство из них обладает теми или иными уязвимости. На сегодняшний день существуют теоретические модели построения групповых протоколов на идентификаторах, с возможностью динамического выхода или присоединении пользователей к доверенным групп [2]. Целью данной работы является анализ многосторонних протоколов согласования общего ключа, на основе идентификационных данных, с последующими рекомендациями относительно их применения и усовершенствования.

1. Обзор протоколов согласования ключа на идентификаторах

1) Протокол согласования ключа Смарта (Smart, 2002). В данной схеме требуется, что бы все пользователи, которые участвуют в согласовании ключа, были клиентами одного PKG (генератора секретных ключей). Смарт также предложил модификацию данного протокола согласования ключа с подтверждением аутентификации ключа. Далее Шим в своей работе теоритически доказал, что протокол Смарта не имеет совершенной частичной опережающей скрытности и предложил модифицированную схему, которая, в свою очередь, оказалась небезопасной против атаки Сана и Се типа «человек-по-середине». Протокол можно представить в следующем виде (рис. 1):

– пользователь А вычисляет: $K_A = e(aQ_B, P_{pub})e(S_A, T_B)$, где $S_A = sQ_A$;

– пользователь B вычисляет: $K_B = e(bQ_A, P_{pub})e(S_B, T_A)$, где $S_B = sQ_B$;

– согласованный ключ: $K_{AB} = K_A = K_B = e(aQ_B + bQ_A, P_{pub})$.

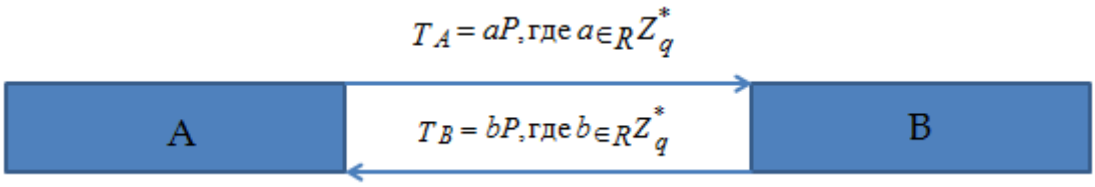

Рис. 1. Протокол согласования ключа Смарта.

Налла и Редди расширили этот протокол к протоколу с несколькими участниками, путем использования структуры бинарного дерева и теоритически доказали, что их модификация данного протокола обеспечивает некоторые желательные атрибуты безопасности.

2) Протокол согласования ключа Скотта (Scott, 2002). Скотт предложил схему, в которой каждый пользователь выбирает ПИН-код и PKG для каждого пользователя ассоциирует результирующий секретный ключ данного пользователя с его идентификатором. Значение, вычисленное, из секретного ключа и ПИН-кода храниться внутри аппаратного токена. Индивидуальный секрет может быть восстановлен, из ранее сохраненных значений ПИН-кода, идентификатора и токена. Протокол можно представить в следующем виде (рис. 2):

– пользователь A вычисляет: $K_A = T_B^a$;

– пользователь B вычисляет: $K_B = T_A^b$;

– согласованный ключ: $K_{AB} = K_A = K_B = e(Q_A, Q_B)^{sab}$.

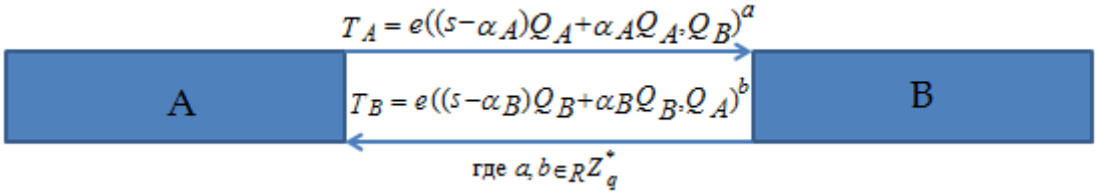

Рис. 2. Протокол согласования ключа Скотта.

3) Протокол согласования ключа Чена и Кудлы (Chen, Kudla, 2002). Протокол можно представить в следующем виде (рис. 3):

– пользователь A вычисляет: $K_A = e(S_A, T_B + aQ_B)$;

– пользователь B вычисляет: $K_B = e(S_B, T_A + bQ_A)$;

– согласованный ключ: $K_{AB} = K_A = K_B = e(Q_A, Q_B)^{s(a+b)}$.

–

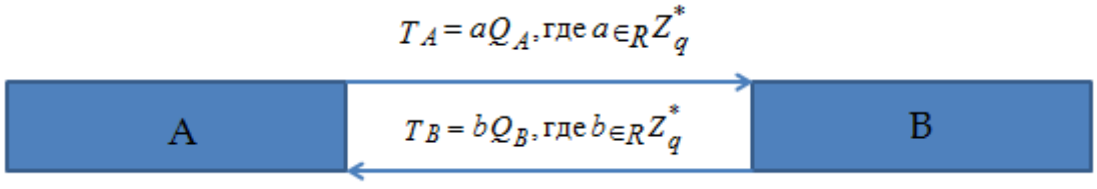

Рис. 3. Протокол согласования ключа Чена и Кудлы.

Данный протокол является более эффективным, чем протокол Смарта. Чен и Кудла также предложили механизм передачи хранения ключа третей доверенной стороне (ТДС), применимый и к протоколу Смарта (данная модификация дает возможность пользователям через ТДС сохранить конфиденциальность даже с PKG). Они также предложили другую модификацию, которая позволяет пользователям, принадлежащим разным PKG, согласовывать ключи. Авторы доказали безопасность своего протокола в модели случайного оракула.

4) Протокол согласования ключа Маккала и Баррето (McCullagh, Barreto, 2004). Данный протокол может быть использован как в режимах обычной и свободной передачи хранения третей стороне, так и в схемах согласования ключа между пользователей разных PKG. Предполагается, что данный протокол обладает заданными свойствами безопасности в модели случайного оракула. Протокол можно представить в следующем виде (рис. 4):

– пользователь А вычисляет: $K_A = e(T_B, S_A)^{xa}$;

– пользователь В вычисляет: $K_B = e(T_A, S_B)^{xb}$;

– согласованный ключ: $K_{AB} = K_A = K_B = e(P,P)^{x_a x_b}$.

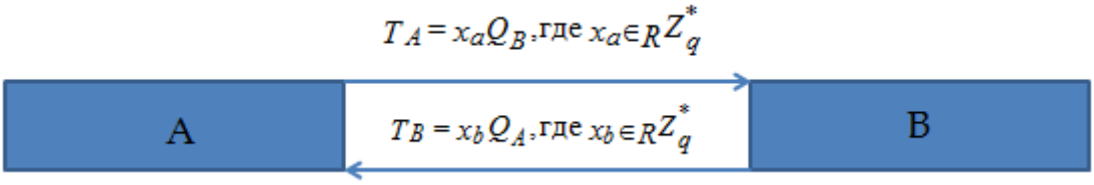

Рис. 4. Протокол согласования ключа Маккала и Баррето.

Позже, Се доказал, что злоумышленник может успешно реализовать атаку компрометации ключа, и устранил этот недостаток, предложив модификацию протокола. Кван и Чю показали, что обе схемы и их модифицированные варианты не безопасны, если злоумышленник имеет возможность выявить участников, повторно использующих сеансовый ключ.

5) Трехсторонний протокол согласования ключа Чжана, Лю и Кима (Zhang, Liu, Kim, 2002). Данный протокол использует подпись Гесса, основанную на идентификаторах. В данном протоколе каждый из трех участников выполняет одну передачу, пять скалярных умножений, пять спариваний, два отображения в точку ЭК, два умножения и две операции хеширования.

Протокол можно представить в следующем виде (рис. 5):

– (1) пользователь А вычисляет:

$T_A = H(P_A)S_A + aP$, и отправляет (P_A, T_A) к В и С;

– (2) пользователь В вычисляет:

$T_B = H(P_B)S_B + bP$, и отправляет (P_B, T_B) к А и С;

– (3) пользователь С вычисляет:

$T_C = H(P_C)S_C + cP$, и отправляет (P_C, T_C) к А и В.

– Пользователь А проверяет:

$$e(T_B + T_C, P) \stackrel{?}{=} e(H(P_B)Q_B + H(P_C)Q_C, P_{pub})e(P_B, P_B)e(P_C, P_C);$$

и если проверка прошла успешно, вычисляет: $K_A = e(P_B, P_C)^a$.

– Пользователь B проверяет:

$$e(T_A + T_C, P) \stackrel{?}{=} e(H(P_A)Q_A + H(P_C)Q_C, P_{pub})e(P_A, P_A)e(P_C, P_C);$$ и если проверка прошла успешно, вычисляет: $K_B = e(P_A, P_C)^b$.

– Пользователь C проверяет:

$$e(T_A + T_B, P) \stackrel{?}{=} e(H(P_A)Q_A + H(P_B)Q_B, P_{pub})e(P_A, P_A)e(P_B, P_B);$$ и если проверка прошла успешно, вычисляет: $K_C = e(P_A, P_B)^c$.

– Согласованный ключ: $K_{ABC} = K_A = K_B = K_C = e(P,P)^{abc}$.

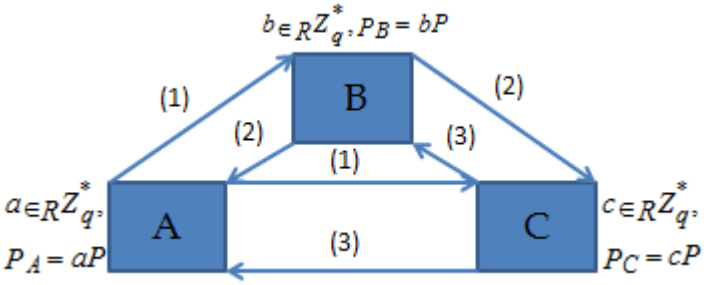

Рис. 5. Протокол согласования ключа Чжана, Лю и Кима.

2. Сравнительный анализ протоколов согласования ключа на идентификаторах. Основные свойства безопасности и эффективности данных протоколов были сведены в сравнительные табл. 1 и табл. 2 соответственно.

Таблица 1

Сравнительная таблица свойств безопасности, рассмотренных протоколов согласования ключа на идентификаторах

Свойства безопасности	Протокол согласования ключа				
	1	2	3	4	5
Задача, на которой основан протокол	DLP, CDH	DLP, CDH	BDH	BDHI	BDH, Weak-DH
Аутентификация ключа	+/неявная	-	-	-	+/-
Безопасность ключа	заданная	-	-	заданная	заданная
Опережающая скрытность	+/-	-	+/-	+	+/-
Защита от атак типа «Маскарад»	только ключа	+	только ключа	-	только ключа
Защита от неизвестных частей ключа	+	-	+	-	+
Управление ключом	+/-	-	+/-	+	-

где «+/-» - означает частичное обеспечение рассматриваемого свойства.

Таким образом, можно увидеть, что ни один из рассмотренных протоколов не обеспечивает всех рассматриваемых свойств безопасности. Максималь-

ное количество участников в данных протоколах равно трем (протокол Чжана, Лю и Кима).

Таблица 2

Сравнительная таблица эффективности рассмотренных протоколов

Протокол согласования ключа	Количество операций выполняемых пользователем/сервером PKG						
	скалярное умножение	спаривание	умножение	отображение в точку ЭК	возведение в степень	вычитание	операции хеширования
1	1/2	2/-	1/-	1/1	-	-	-
2	1/2	1/-	-	1/1	2/-	1/-	-
3	2/2	1/-	-	2/1	2/-	-	-
4	1/2	1/-	-	-/1	1	-	1
5	5/2	5/-	2/-	2/1	-	-	2

Анализ подтвердил, что самым защищенным из данных протоколов является трехсторонний протокол согласования ключа Чжана, Лю и Кима. Дутта и Брау предложили модифицировать данный протокол, и предложили на его базе трех групповой протокол согласования ключа [3,4], который будет рассмотрен в следующем разделе данной статьи. На базе его можно построить сеть, в которой неограниченной число пользователей может защищено взаимодействовать между собой. Ими же была доказана безопасность данного протокола против пассивного злоумышленника. Далее, эту модификацию предложили усовершенствовать в динамический протокол, в котором пользователи могли бы свободно перемещаться из группы в группу.

3. Анализ многостороннего протокола согласования общего ключа на идентификаторах, предложенного Баруа, Даттой и Саркаром. В данном разделе проанализирован *n*-сторонний протокол согласования ключа [5], на идентификаторах, использующий рекурсивный алгоритм, вызывающий две процедуры – Combine Three и Combine Two.

Для процедуры Combine Three согласованным общим ключом является $H(e(P,P)^{s_1 s_2 s_3})$, для трех групп пользователей U_1, U_2, U_3, с соответствующими секретными сеансовыми ключами s_1, s_2, s_3. Аналогично выполняется процедура Combine Two. Если количество пользователей в каждой группе, при выполнении процедур CombineThree, и Combine Two равно одному, тогда данные процедуры принимают вид трехстороннего протокола согласования общего ключа Zhang, Lin, Kim и двухстороннего протокола Диффи-Хеллмана, соответственно.

Алгоритм имеет несколько уровней, на каждом уровне согласовывается общий ключ. Для n пользователей, пусть уровни будут пронумерованы от нуля до $R(n)$. На уровне i, пусть число групп будет n_i. Таким образом, $n_0 = n$, и $n_k = 1$, где $k=R(n)$. Представим некоторые системы обозначений для удобства анализа алгоритма:

$U_j^{(i)}, 1 \le j \le n_i$ – j-тая группа пользователей, на уровне i;

$s_j^{(i)}$ – общий секретный ключ, для группы пользователей $U_j^{(i)}$;

$P_j^{(i)} = s_j^{(i)} P$ – i-тый уровень j-того открытого ключа.

Пусть общее количество пользователей равно n, делим его на три группы $U_1^{(k-1)}, U_2^{(k-1)}, U_3^{(k-1)}$, и если остаток от деления равен двум, то к двум последним группам прибавляем по одному пользователю, если одному – то к последней группе одного. Применяем рекурсивную процедуру, для каждого набора пользователей $U_j^{(i)}$, разбивая ее на три подгруппы пользователей, в зависимости от n, каждая такая подгруппа делиться от одной до трех. Процедура Combine Three вызывается при количестве раундов ≥ 2, а процедура CombineTwo, при количестве раундов < 2.

Пусть *Rep(U)* – текущее состояние группы пользователей U, тогда процедуры Combine Three и Combine Two, можно представить в виде алгоритмов:

procedure
CombineThree(U[l,2,3], s[l, 2,3])
i=1 to 3 do {
Rep(U_i) computes $P_i = s_i P$
and $T_{\mathrm{Re}\,p(U_i)} = \hat{H}(P_i) S_{\mathrm{Re}\,p(U_i)} + s_i P_i$;
Let $\{j,k\} = \{1,2,3\} \backslash \{i\}$;
Rep(U_i) sends P_i, $T_{\mathrm{Re}\,p(U_i)}$}
to all members of both U_j, U_k.
i=1 to 3 do {
Let $\{j,k\} = \{1,2,3\} \backslash \{i\}$;
each members of U_i
verifies:
$e(T_{\mathrm{Re}\,p(U_j)} + T_{\mathrm{Re}\,p(U_k)}, P) =$
$= e(\hat{H}(P_i) Q_{\mathrm{Re}\,p(U_j)} +$
$+ \hat{H}(P_k) Q_{\mathrm{Re}\,p(U_k)}, P_{pub}) e(P_j, P_j) e(P_k, P_k)$
and computes $H(e(P_j, P_k)^{s_i})$}
end CombineThree

procedure
CombineTwo(U[l,2], s[l, 2])
i=1 to 2 do {
Rep(U_i) computes $P_i = s_i P$
and $T_{\mathrm{Re}\,p(U_i)} = \hat{H}(P_i) S_{\mathrm{Re}\,p(U_i)} + s_i P_i$ }
Rep(U_1) generates $\bar{s} \in_R Z_q^*$
and sends $\bar{s}P$,
$\bar{T}_{\mathrm{Re}\,p(U_1)} = \hat{H}(\bar{s}P) S_{\mathrm{Re}\,p(U_1)} + \bar{s}^2 P$
to the rest of the users;
each member of U_1, U_2
except *Rep*(U_1) verifies:
$e(\bar{T}_{\mathrm{Re}\,p(U_1)}, P) =$
$= e(\hat{H}(\bar{s}P) Q_{\mathrm{Re}\,p(U_1)}, P_{pub}) e(\bar{s}P, \bar{s}P)$;
Rep(U_1) sends P_1, $T_{\mathrm{Re}\,p(U_1)}$
to all members of U_2;
Rep(U_2) sends P_2, $T_{\mathrm{Re}\,p(U_2)}$
to all members of U_1;
each members of U_1
verifies : $e(T_{\mathrm{Re}\,p(U_2)}, P) =$
$= e(\hat{H}(P_2) Q_{\mathrm{Re}\,p(U_2)}, P_{pub}) e(P_2, P_2)$
and computes $H(e(P_2, \bar{s}P)^{s_1})$;
each members of U_2
verifies : $e(T_{\mathrm{Re}\,p(U_1)}, P) =$
$= e(\hat{H}(P_1) Q_{\mathrm{Re}\,p(U_1)}, P_{pub}) e(P_1, P_1)$
and computes $H(e(P_1, \bar{s}P)^{s_2})$;
end CombineTwo

Данный протокол обеспечивает защиту против активного злоумышленника путем применения специальной схемы подписи, и обеспечивает следующие свойства безопасности:

1) *Неявная аутентификация ключа (Implicit Key Authentication)* – только пользователи, с которыми А хочет согласовать общий ключ, имеют возможность вычислить значение данного ключа.

2) *Безопасность с известным сеансовым ключом (Known Session Key Security)* – злоумышленник, имея некоторые предыдущие сеансовые ключи, не может вычислить текущий сеансовый ключ.

3) *Идеальная или опережающая скрытность (Forward (Perfect) Secrecy)* – компрометация долгосрочного секретного ключа одного или нескольких (всех в идеальном случае) пользователей не влияет на безопасность предыдущих сеансовых ключей.

4) *Олицетворение без компрометации ключа (No Key-compromise Impersonation)* – компрометация секретного долгосрочного ключа одного пользователя, не влияет на секретные ключи других пользователей. Злоумышленник может выдать себя только за пользователя, чей ключ он скомпрометировал.

5) *Отсутствие неизвестных частей ключа (No Unknown Key-share)* – злоумышленник не в состоянии убедить группу пользователей в том, что они разделили ключ со злоумышленником, а не с легальными пользователями.

6) *Отсутствие контроля ключа (No Key Control)* – не возможно контролировать / предсказать значение сеансового ключа любым участником (или злоумышленником).

Выводы. Согласование ключа является одним из фундаментальных криптографических примитивов после шифрования и цифровой подписи. Основной целью механизмов согласования ключей является построение защищенного канала, для последующего безопасного взаимодействия пользователей. Также, механизмы согласования ключа служат основой для построения защищенных, комплексных, высокоуровневых протоколов.

Проведен краткий обзор и анализ основных криптографических протоколов на идентификаторах позволил сделать вывод о том, что криптографические протоколы на идентификаторах, являются перспективной и активно развивающейся отраслью современной криптографии и могут быть задействованы при построении инфраструктуры открытых ключей. Такие преобразования является единственной альтернативой существующей системы ЕЦП. Также был проанализирован протокол согласования общего ключа на идентификаторах, использующий билинейные отображения точек на эллиптической кривой. Протокол является стойким против пассивного и активного злоумышленника, и основывается на решении проблемы DHBDH (Decisional Hash Bilinear Diffie-Hellman). Данный протокол обеспечивает безопасный канал передачи данных между пользователями.

Криптографические протоколы на идентификаторах, являются перспективной и активно развивающейся отраслью современной криптографии и могут быть задействованы при построении инфраструктуры открытых ключей на идентифи-

каторах. Данное направление нуждается в дальнейшем глубоком исследовании и развитии как в теоретическом, так и в практическом смысле.

Список литературы

1. Chen, L., Cheng, Z., Smart, N.P.: Identity-based Key Agreement Protocols from Pairings. International Journal of Information Security 6(4), 213–241 (2007).
2. R. Barua, R. Dutta, P. Sarkar. Extending Joux Protocol to Multi Party Key Agreement., LNCS 2904, pp. 205-217, Springer-Verlag, 2003.
3. .R. Dutta, R. Barua and P. Sarkar. Provably Secure Authenticated Tree Based Group Key Agreement., LNCS 3269, pp. 92-104, Springer-Verlag, 2004.
4. R. Dutta and R. Barua. Dynamic Group Key Agreement in Tree-based Setting., LNCS 3574, pp. 101-112, Springer-Verlag, 2005.
5. R. Barua, R. Dutta, P. Sarkar. Extending Joux Protocol to Multi Party Key Agreement., LNCS 2904, pp. 205-217, Springer-Verlag, 2003.

Анотація

Порівняльний аналіз протоколів узгодження спільного ключа на основі ідентифікаційних даних

Проведено короткий огляд протоколів узгодження ключа. Наведено результати порівняльного аналізу даних протоколів і аналіз властивостей безпеки протоколу, запропонованого Баруа, Датою і Саркаром.

Abstract

Comparative analysis of common key agreement protocol based on identity

Held a brief overview of the key agreement protocol. The results of comparative analysis of protocols and analysis of security properties of the protocol proposed by Barua, Dutta and Sarkar.