2 Актуальні питання криптографії і технічного захисту інформації. Метрологічне забезпечення

УДК 681.3.06:519.248.681

ОБОСНОВАНИЕ ПЕРЕЧНЯ И ФУНКЦИОНАЛЬНЫХ ТРЕБОВАНИЙ К КРИПТОГРАФИЧЕСКИМ ПРОТОКОЛАМ В ГРУППАХ ТОЧЕК ЭЛЛИПТИЧЕСКИХ КРИВЫХ

Леонид Скрыпник*, Иван Горбенко, Станислав Збитнев, Андрей Поляков**
**ДСТСЗИ СБУ, ХНУРЭ, **АО "ИИТ"*

Анотація: **Розглядаються і формуються функціональні вимоги до протоколів узгодження та транспортування ключів. Наводиться перелік протоколів та обгрунтовується їх використання з описом виконуваних гарантій об'єктів. Проводиться аналіз криптографічних методів, таких як Діффі-Хелмана та MQV.**
Summary: **Considered and are formed functional requirements to protocols of agreement and transportations of keys. Happens To a list of protocols and proof of their use with the description of executable object warranties. Consider cryptographic methods, such as Diffie-Hellman and MQV.**
Ключові слова: **Криптографические протоколы согласования ключей, транспортировка ключей, алгоритмы симметричного шифрования, стойкость протоколов, аутентификация ключей.**

В защищенных информационных технологиях определяющей процедурой является процедура выработки общего ключа (секрета). Для решения этой задачи разработаны и применяются различной степени сложности состоятельные протоколы, прежде всего Диффи-Хелмана, реализованные на основе преобразований в полях Галуа [2]. Однако развитие методов и средств криптоанализа таких криптосистем и криптопротоколов вынуждает увеличивать размеры общесистемных параметров и ключей, вследствие чего увеличивается сложность выполнения базовых операций в полях, в ряде случаев до недопустимых величин. Разрешение этого противоречия может быть достигнуто за счет выработки общего секрета в группах точек эллиптических кривых (ЭК) над полем Галуа $GF(q)$

I Алгоритмы выработки общего секрета

В основе протоколов управления ключами лежат два математических алгоритма вычисления общего секретного значения – это простой алгоритм Диффи-Хелмана (ДХ) и сложный алгоритм (MQV). Причем алгоритм ДХ обеспечивает выработку общего секрета на основе одного личного ключа d, используемого, как правило, многократно.

В алгоритме MQV один из ключей, например d_2, является сеансовым. Функция $avf(Q)$ определяет преобразованное (связанное) значение точки P. Несмотря на повышенную по сравнению с алгоритмом ДХ вычислительную сложность алгоритм MQV в большинстве случаев является более предпочтительным, так как на каждый сеанс или файл позволяет вырабатывать сеансовый ключ, а следовательно обеспечивается защита от компрометации ключей и криптографических атак. В табл. 1 приведено описание алгоритмов ДХ и MQV.

Таблица 1 – Алгоритмы выработки общего секрета.

Алгоритм Диффи-Хелмана	**Алгоритм MQV**
• d_A – личный ключ объекта A; • Q_B – открытый ключ объекта B.	• Две пары ключей, долговременный $(d_{1,A},Q_{1,A})$ и сеансовый $(d_{2,A},Q_{2,A})$, принадлежащих объекту A. • Два открытых ключа $Q_{1,B}$ и $Q_{2,B}$, принадлежащих объекту B.
1. Вычислить точку $P=(x,y)=d_A \cdot Q_B$. 2. Проверить $P \neq O$, где O – ноль аддитивной группы (точка бесконечности). Если $P=O$, то вывести "недостоверный" и остановка. 3. Установить $Z=x_P$, где x_P – x-координата	1. Вычислить целое число: $r = d_{2,A}+(avf(Q_{2,A})\times d_{1,A}) \pmod n$, где n – порядок базовой точки на ЭК. 2. Вычислить точку на эллиптической кривой: $P = h \times r \times (Q2,B+(avf(Q2,B)\times Q1,B))$, где h коэффициент связи порядка ЭК u и порядка базовой точки n.

Продолжение таблицы 1

	3 Проверить $P \neq O$. Если $P=O$, то вывести "недостоверный" и остановка. 4. Установить $Z=x_P$, где x_P – x-координата точки P.

Из предварительного анализа приведенных алгоритмов видно, что вычислительно более сложным является алгоритм *MQV*. При выполнении алгоритма *MQV* должно выполняться как минимум две вычислительно сложных операции – определение значения r и вычисление точки P с использованием операции скалярного умножения. В алгоритме Диффи-Хелмана выполняется только скалярное умножение.

II Криптопротоколы, характеристика и требования к ним

Под криптопротоколами в нашем случае понимается распределенный алгоритм, который представляет собой совокупность алгоритмов совместного решения этих задач для каждого объекта (участника), спецификации форматов информации (данных), пересылаемых между участниками, спецификаций по осуществлению синхронизации действий, описания действий при сбоях и т. п.

Проведенный анализ показал [1], что протоколы управления ключами можно разделить на два класса:

- *протоколы согласования ключей*, задачей которых является выработка общего секрета (секретного ключа) на основе известных открытых ключей объектов;
- *протоколы транспортировки ключей*, задачей которых является доставка, ввод в действие и использование ключей с обеспечением их целостности, подлинности и при необходимости, конфиденциальности.

Названные протоколы по своему функциональному предназначению очень похожи, поэтому на них как правило накладываются одни и те же функциональные требования. Вместе с тем существуют различия в методах и, как следствие, средствах их реализации.

В практическом аспекте основным требованием к рассматриваемым протоколам является требование их состоятельности в смысле обеспечения целостности, подлинности, конфиденциальности, доступности и наблюдаемости ключей на всех этапах их жизненного цикла. В теоретическом смысле каждый из протоколов должен обладать свойствами полноты, корректности, а также в некоторых случаях свойством нулевого разглашения знаний.

Представляет интерес рассмотрение протоколов, реализуемых в группах точек эллиптических кривых с позиции их состоятельности, целостности, подлинности ключей и параметров, что может обеспечиваться за счет включения в протокол и выполнения при каждом обращении к ключам и параметрам дополнительных алгоритмов проверки, которые строятся на основе математических свойств ключей и параметров. Такие дополнительные проверки позволяют защититься от ряда угроз, прежде всего:

- *подмены параметров эллиптической кривой*;
- *преднамеренного или вынужденного использования слабых кривых*;
- *несоответствия и несогласованности общественного ключа с параметрами эллиптической кривой*.

Проведенный анализ показал, что в существующих протоколах управления ключами выработка конкретного значения секретного ключа производится из общего секрета посредством использования специальных функций, обозначаемых как *kdf*.

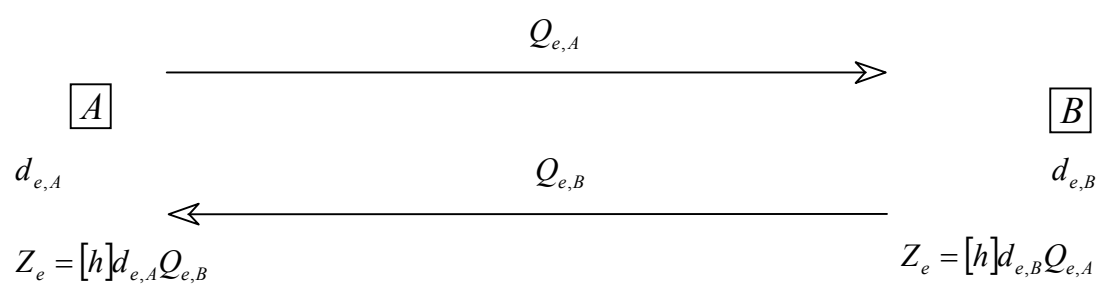
Поэтому важным является определение требований к таким функциям и выполнение этих требований.

III Стандартные протоколы согласования ключей

Рассмотрим основные стандартные протоколы согласования ключей с целью их классификации и анализа. При этом выделим два объекта, один из которых является инициатором, а другой – ответчиком (приемником). В таком протоколе ключи состоят из пары сеансовых (временных) ключей.

Протокол 1. *Сеансовый протокол согласования ключей.*

Секретными являются ключи $d_{e,A}$ и $d_{e,B}$, открытые $Q_{e,A}$ и $Q_{e,B}$.



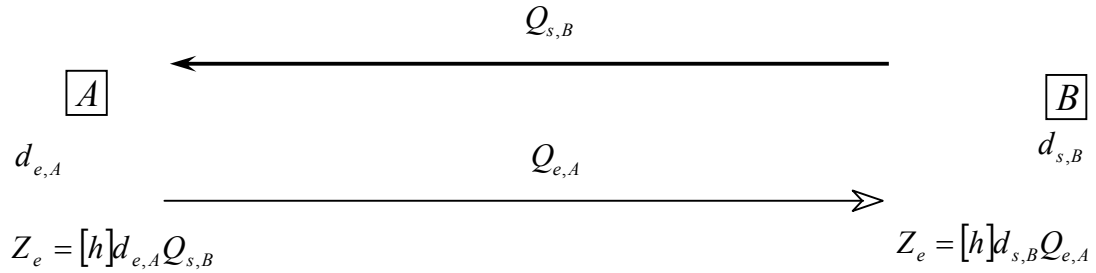
Общим секретом является Z_e, вырабатываемый пользователями A и B, где h – кофактор. Конкретное секретное значение вырабатывается как

$$ключ = kdf(Z_e)$$

Таким образом, протокол реализует выработку сеансовых пар ключей и производит обмен открытыми сеансовыми ключами, на основании которых вырабатывается общее секретное значение.

Протокол 2. *Однопроходной протокол Диффи-Хелмана.*

В протоколе используются две пары ключей $\{d_{e,A}, Q_{e,A}\}$ и $\{d_{s,B}, Q_{s,B}\}$, одна из которых является сеансовой, другая главной. Открытый главный ключ $Q_{s,B}$ передается заранее. Жирными линиями выделены те передачи ключей, которые не участвуют в протоколе, они были произведены заранее. Их иллюстрация является информативной.

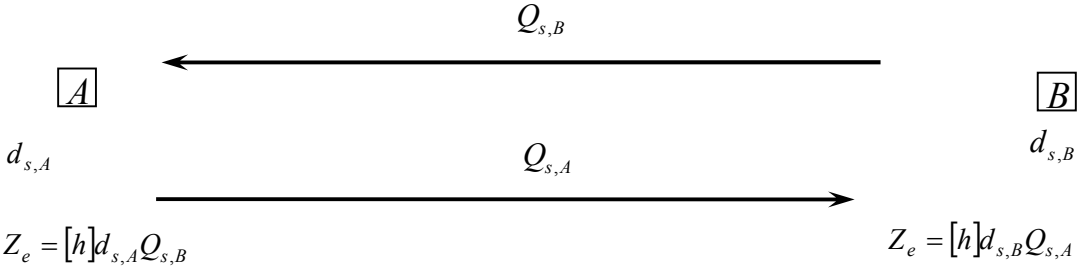


В протоколе выполняется только одна передача сеансового ключа $Q_{e,A}$. Значение секретного ключа вырабатывается как

$$ключ = kdf(Z_e).$$

Протокол 3. *Протокол на главных ключах.*

В протоколе используются только главные пары ключей $\{d_{s,A}, Q_{s,A}\}$ и $\{d_{s,B}, Q_{s,B}\}$.

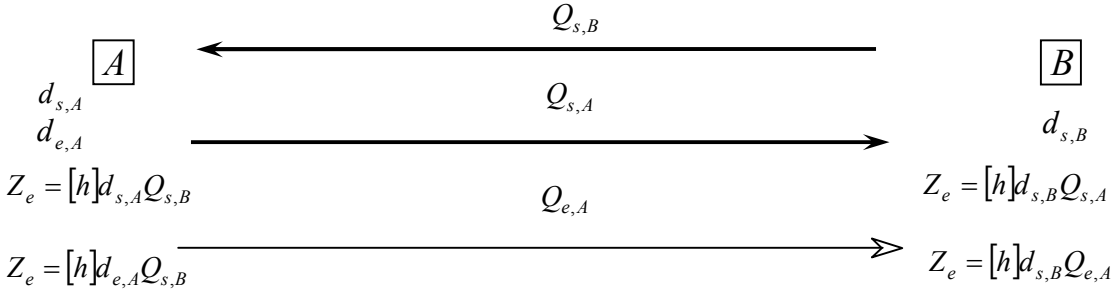


Протокол выполняет вычисление общего секрета, основываясь только на главных ключах, что позволяет не производить передачи открытых ключей во время выполнения протокола. Секретный ключ вычисляется с использованием следующей функции

$$ключ = kdf(Z_e).$$

Протокол 4. *Однопроходной протокол с использованием главных ключей.*

Ключевой материал, использующийся в протоколе, состоит из двух пар главных ключей $\{d_{s,A}, Q_{s,A}\}$, $\{d_{s,B}, Q_{s,B}\}$ и одной пары сеансовых ключей $\{d_{e,A}, Q_{e,A}\}$.

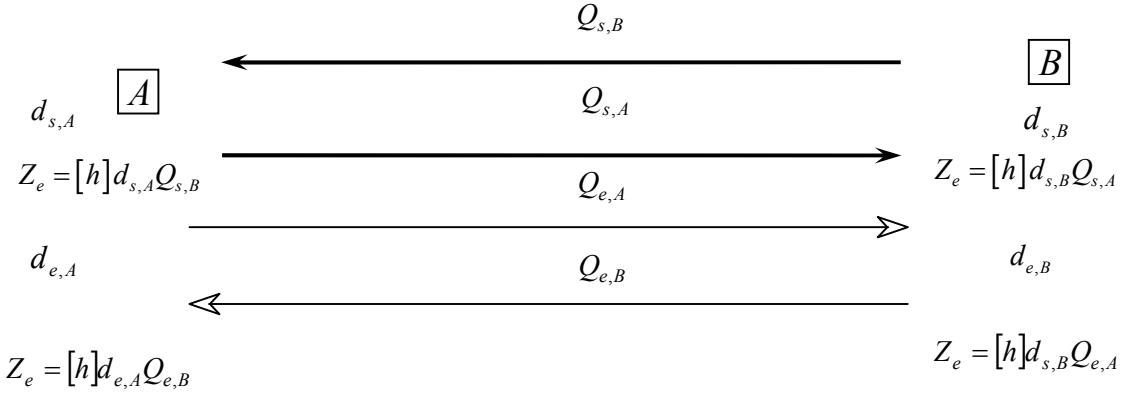


Протокол является усиленной версией однопроходного протокола ДХ. В протоколе выполняется одна передача открытого сеансового ключа. На основании используемого ключевого материала вычисляется два общих секретных значения, Z_s и Z_e. Вычисление секретного ключа осуществляется на основании этих значений – необходимо вначале выполнить операцию конкатенации (операция объединения) над значениями Z_s и Z_e, а затем вычислить секретный ключ:

$$ключ = kdf\left(Z_s \parallel Z_e\right).$$

Протокол 5. *Полный протокол согласования ключей.*

Данный протокол является полным протоколом согласования ключей. Ключевой материал состоит из двух пар главных ключей $\left\{d_{s,A}, Q_{s,A}\right\}$, $\left\{d_{s,B}, Q_{s,B}\right\}$ и двух пар сеансовых ключей $\left\{d_{e,A}, Q_{e,A}\right\}$, $\left\{d_{e,B}, Q_{e,B}\right\}$.



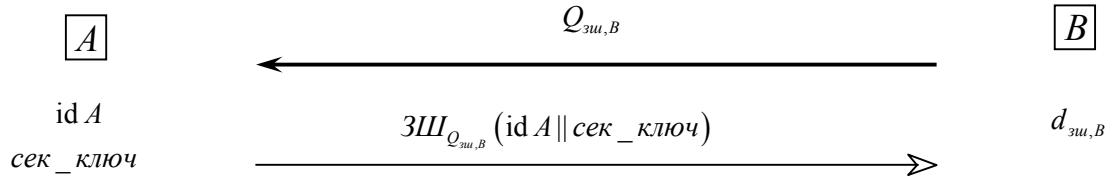
В данном протоколе выполняется две передачи сеансовых открытых ключей. С использованием ключей, личных и открытых материалов формируются общие секретные значения, Z_s и Z_e. Вычисление секретного ключа производится по формуле

$$ключ = kdf\left(Z_s \parallel Z_e\right)$$

IV Протокол транспортировки ключей

Протокол 6. *Однопроходной протокол транспортировки ключей.*

Протокол реализует защищенную передачу секретного ключа симметричного криптоалгоритма от одного объекта другому объекту. Инициатором протокола является тот, кто желает передать секретный ключ другому объекту (получателю). В данном протоколе передача ключа осуществляется в зашифрованном виде, для этого используется протокол направленного зашифрования на ЭК (ЗШ), для расшифрования



используется алгоритм (РШ). В протоколе используются главная пара ключей $\left\{d_{зш,B}, Q_{зш,B}\right\}$, идентификаторы объектов $\mathrm{id}\,A$ и передаваемый секретный ключ *сек_ключ*.

В протоколе выполняется только одна передача, содержащая в себе зашифрованный ключ. Идентификатор $\mathrm{id}\,A$ известен, поэтому в протоколе не передается. После получения зашифрованного сообщения получатель выполняет расшифровку и выделяет секретный ключ

$$\mathrm{id}\,A \parallel сек\_ключ = РШ_{d_{зш,B}}\left(ЗШ_{Q_{зш,B}}\left(\mathrm{id}\,A \parallel сек\_ключ\right)\right).$$

Этот протокол является состоятельным и обеспечивает реализацию функции причастности. Перед началом выполнения протокола необходимо, чтобы объекты произвели согласования по использованию криптографических алгоритмов, хеш-функции, функции выработки ключа и алгоритма симметричного шифрования.

V Функциональные требования к протоколам

Приведенные выше протоколы позволяют построить сложные состоятельные протоколы управления ключами. Проведенный анализ показал, что они должны удовлетворять ряду функциональных требований.

Основной функцией любых из приведенных криптопротоколов установления ключей есть распределение ключевых данных. В идеальном случае ключевые данные должны порождаться случайно, равномерно, независимо и однородно. Они должны быть случайно распределены и ни один несанкционированный объект не должен ничего знать о ключевых данных каждого из объектов.

Асимметричные схемы установления ключей дают больше функциональных преимуществ, чем симметричные. Ни одна асимметричная схема не может обеспечить безусловную защиту в информационно-теоретическом смысле. Это означает, что злоумышленник с неограниченной вычислительной мощностью несомненно может восстановить ключевые данные. На практике такая задача представляется сложно реализуемой, так как разумно предположить, что реально злоумышленник обладает ограниченными вычислительными ресурсами.

Поэтому протоколы установления ключей, основанные на асимметричной криптографии, должны иметь высокую степень стойкости и обладать теми же требованиями, что и симметричные ключи. Таким образом, протоколы установления ключей должны удовлетворять следующим специальным требованиям:

- неявной и явной аутентификации;
- конфиденциальности, что дает гарантии того, что секретный ключ не будет скомпрометирован в результате компрометации главного секретного ключа;
- защиты ключей в смысле обеспечения целостности и конфиденциальности ключей симметричных криптоалгоритмов.

По сути это требования, которыми обладают симметричные криптоалгоритмы. Некоторые из требований, такие как аутентификация явных ключей, считаются важными почти во всех протоколах. Другие требования, такие как прямая конфиденциальность и защита ключей, считаются важными в зависимости от среды применения [1].

Полный набор протоколов приведен в проекте стандарта согласования и транспортировки ключей. Все схемы являются эффективными для конкретной среды применения.

VI Требования к длине ключа

Задача схем установления ключей состоит в установлении секретных ключевых данных, разделяемых двумя объектами. Сложность атаки схемы (протоколы) установления ключей должна быть не меньше сложности атаки полного перебора ключей. То есть, когда кто-нибудь устанавливает симметричные ключи, он хочет иметь гарантию, что схема установления ключей будет иметь ту же криптоаналитическую сложность, что и симметричного алгоритма.

Такое основное условие должно быть выполнено при выборе размера параметров ЭК. Это требование связано с тем, что условие $n > 2^{160}$ в настоящее время является достаточным для обеспечения защиты, но не дает требуемого уровня защиты для 256-битного ключа симметричного шифрования.

В практически применяемых системах обеспечивается вычислительная сложность. Так в [3] определены требования к длине ключей криптопреобразований для симметричных криптоалгоритмов. Они заключаются в том, что для первого класса сложности в симметричных криптоалгоритмах длина ключа должна быть не менее 256 бит, 2-го – 128 бит и 3-го – 128 бит.

При решении данной проблемы необходимо знать сложность наилучшей криптоаналитической атаки на эллиптические кривые. Наилучшей атакой на ЭК в настоящее время считается алгоритм ρ-Полларда [2]. Его сложность можно оценить количеством операций сложения на эллиптической кривой

$$I_{ЭК} = \sqrt{\frac{\pi \cdot n}{4}} .$$

В таблице 2 приведены длины модулей преобразований в группах точек эллиптической кривой, при которых обеспечивается такая же стойкость ключа, как и в симметричных криптоалгоритмах.

Таблица 2.

Название симметричного криптоалгоритма	Длина ключа симметричного криптоалгоритма	Длина модуля преобразования ЭК
DEA	56	112
2-ключевой 3-DES	112	224

Продолжение таблицы 2

RIJNDAL	128	256
3-ключевой 3-DES	168	336
RIJNDAL	192	384
RIJNDAL	256	512

Выводы

Использование протоколов установления и выработки ключей в группах точек эллиптической кривой позволяет согласованно выработать ключи и обеспечить функцию причастности. Использование преобразований в группах точек ЭК по сравнению с преобразованиями в кольцах и полях [3] позволяет в 4 – 6 и более раз сократить длины открытых ключей и общесистемных параметров, или при тех же параметрах существенно повысить стойкость.

Используемые на практике состоятельные протоколы, реализуемые за счет преобразований в кольцах и полях, являются состоятельными и при использовании в группах точек эллиптических кривых.

Следует ожидать, что в ближайшие годы при реализации состоятельных протоколов будут использоваться алгоритмы направленного шифрования, цифровой подписи и выработки ключей, построенные на основе преобразований в группах точек эллиптической кривой.

Литература: 1. X9.42 Public Key Cryptography for the Financial Services Industry: Agreement of Symmetric Algorithm Keys Using Diffie-Hellman, 1996. Working Draft. 2. X9.63 Public Key Cryptograph For The Financial Services Industry: Key Agreement and Key Transport Using Elliptic Curve Cryptography. 1999. 207 с. 3. Криптографические преобразования в группах точек эллиптических кривых методом Полларда / И. Д. Горбенко, С. И. Збитнев, А. А. Поляков // Радиотехника: Всеукр. межвед. науч.-тех. сб. 2001. Вып. 119. с. 43 –50. 3. http://crypto.nessie.org

УДК 681.3

СРАВНИТЕЛЬНЫЙ ОБЗОР АНТИВИРУСНЫХ ПРОДУКТОВ ДЛЯ РАБОЧИХ СТАНЦИЙ НА БАЗЕ ОС WINDOWS

Олег Сыч
ООО "Украинский Антивирусный Центр"

Аннотация: **Дан анализ технических характеристик ведущих антивирусных продуктов, обеспечивающих возможность комплексной антивирусной защиты локальной сети.**
Summary: **The analysis of characteristics of conducting anti-virus products ensuring an opportunity of complex anti-virus protection of a local network.**
Ключевые слова: **Информационная безопасность, антивирусная безопасность.**

На сегодняшний день рынок антивирусных продуктов представлен наиболее крупными и известными продуктами: Norton Antivirus [1], McAfee, KAV [2] (ранее AVP) и DrWeb. Кроме того, стоит отметить также продукт отечественной разработки UNA. Каждый из продуктов обладает своими достоинствами и недостатками. Как правило, для комплексной защиты локальной сети и серверов рекомендуется применять несколько различных антивирусных продуктов, но при этом на одном компьютере должно стоять не более одного антивируса.

При выборе антивирусных продуктов, как правило, руководствуются следующими параметрами:

1. Вирусная база продукта.
2. Известность продукта и компании разработчика.
3. Стабильность работы и удобство пользования.
4. Стоимость продукта.
5. Качество технической поддержки.
6. Страна происхождения.

С точки зрения национальной безопасности важное значение имеет происхождение антивирусного продукта, особенно в сетях, где информация содержит государственную, банковскую или коммерческую тайну, в частности в государственных органах, а также после ряда громких скандалов, вызванных