3. https://github.com/rurban/smhasher.
4. Хэш-функция t1ha. https://github.com/PositiveTechnologies/t1ha.

УДК 004.056.55 DOI 10.17223/2226308X/14/17

ПОРОГОВАЯ СХЕМА ПРОТОКОЛА ДИФФИ — ХЕЛЛМАНА

Д. Н. Колегов, Ю. Р. Халниязова

Предлагается пороговая схема протокола Диффи — Хеллмана на эллиптических кривых, которая позволяет создавать и хранить закрытый ключ участника протокола распределённым образом без необходимости восстановления ключа для выполнения криптографических операций на этом ключе.

Ключевые слова: *пороговая криптография, протокол Диффи — Хеллмана, эллиптические кривые.*

Пусть sk — закрытый ключ участника протокола Диффи — Хеллмана. Будем называть *функцией Диффи — Хеллмана* функцию $DH(sk, Q)$, которая принимает на вход закрытый ключ sk (скаляр) и точку Q на эллиптической кривой и возвращает точку $sk \cdot Q$. Под протоколом Диффи — Хеллмана обычно понимают следующую последовательность вычислений (G — образующий элемент подгруппы простого порядка q группы точек эллиптической кривой E над конечным полем):

1) Алиса генерирует случайное число $a \in \mathbb{Z}_q$, вычисляет значение $A = DH(a, G)$ и отправляет его Бобу;
2) Боб генерирует случайное число $b \in \mathbb{Z}_q$, вычисляет значение $B = DH(b, G)$ и отправляет его Алисе;
3) Алиса вычисляет общий секрет как $K = DH(a, B)$, а Боб — как $K = DH(b, A)$.

Идея пороговой схемы Диффи — Хеллмана заключается в том, чтобы сгенерировать закрытый ключ участника протокола x с помощью распределённого алгоритма некоторыми сущностями, а затем делегировать им вычисление значения функции $DH(x, Q)$, используя методы пороговой криптографии. Будем называть таких сущностей *агентами*, а *участником* протокола Диффи — Хеллмана будем называть группу агентов, которая представляет одну из сторон протокола Диффи — Хеллмана и выполняет установленные протоколом шаги.

Если в классическом протоколе Диффи — Хеллмана участником является атомарная сущность (человек, процесс и т. д.), то теперь участник протокола — это группа сущностей — агентов (людей, процессов, ...), которые взаимодействуют между собой посредством разработанных протоколов так, что для внешних сущностей (другого участника протокола, сторонних наблюдателей и т. д.) группа агентов неотличима от обычного участника протокола Диффи — Хеллмана. При этом по результатам выполнения этих протоколов любой из агентов знает открытый ключ группы и может представлять группу при взаимодействии с другим участником протокола. Так как группа агентов неотличима для внешних сущностей от обычного участника, то для простоты изложения далее будем считать, что только один из участников протокола Диффи — Хеллмана представлен группой агентов. При этом неважно, какой именно из участников протокола состоит из агентов, так как вычисления, выполняемые участниками, симметричны.

Первым этапом предлагаемой схемы является генерация долей закрытого ключа, а также вычисление открытого ключа соответствующего участника протокола Диффи — Хеллмана. Вычисленный открытый ключ известен каждому агенту из группы,

а соответствующий закрытый ключ неизвестен никому и существует только в виде сгенерированных долей. Этот этап описывается *протоколом генерации ключей.*

Протокол генерации ключей основан на идее распределенной генерации ключей, которая строится с использованием проверяемой схемы разделения секрета Фельдмана [1]. Каждому агенту P_j ставится в соответствие индекс, который определяет получаемую им долю в схеме Фельдмана. Для простоты будем считать, что индексом агента P_j является значение j (в качестве индексов могут быть использованы любые значения, на которых определены многочлены схемы Фельдмана, если эти значения различны для всех агентов; они устанавливаются на фазе подготовки, не являются секретными и должны быть известны всем агентам). Тогда во всякой схеме Фельдмана агент P_j получает долю $f(j)$, где f — многочлен схемы Фельдмана. При этом генерация итоговых долей на агентах происходит без участия дилера, в результате чего секретная доля закрытого ключа каждого агента известна только ему самому. Это достигается за счёт того, что каждый агент по очереди выступает в роли дилера в схеме Фельдмана, разделяя некоторое случайное значение u_i, а затем благодаря свойству схемы Фельдмана (сумма долей a_i и b_i от значений a и b соответственно является долей от значения $a + b$) агенты, складывая полученные значения, получают новые доли от значения $x = \sum\limits_i u_i$, которое не было разделено явным образом.

В ходе протоколов агенты обмениваются открытыми значениями друг с другом, используя схемы обязательств для фиксации передаваемых значений. Обозначения, использованные для описания протоколов, взяты из [2]:

1) Каждый агент P_i выбирает случайное значение $u_i \in_{\mathrm{R}} \mathbb{Z}_q$ и вычисляет $[KGC_i, KGD_i] = Com(y_i)$, где $y_i = u_i \cdot G$; Com — алгоритм схемы обязательства; KGC_i — вычисленное с помощью алгоритма обязательство; KGD_i — строка, позволяющая его раскрыть. Затем агент отправляет KGC_i всем агентам.
2) Каждый агент P_i отправляет KGD_i всем агентам, а затем разделяет значение u_i между всеми агентами, используя (t, n)-схему Фельдмана. Открытый ключ соответствующего участника протокола Диффи — Хеллмана равен $y = \sum\limits_i y_i = \sum\limits_i u_i \cdot G$.
3) Каждый агент складывает доли, полученные в схемах Фельдмана, для вычисления своей закрытой доли x_i. Итоговое значение закрытой доли агента x_i является долей от закрытого ключа $x = \sum\limits_i u_i$ в (t, n)-схеме Шамира. При этом закрытый ключ x не восстанавливается ни в какой момент выполнения протокола и существует только в форме долей.

Для вычисления общего секрета предлагается *протокол выработки общего секрета.* Получая на вход открытый ключ Y другого участника протокола Диффи — Хеллмана, агенты вычисляют общий секрет $S = x * Y$, используя свои доли закрытого ключа, при этом не раскрывая их в ходе протокола:

1) Каждый агент P_i вычисляет коэффициент Лагранжа λ_i и значение $w_i = \lambda_i x_i$, которое является долей данного агента в аддитивной $(t-1, t)$-схеме разделения секрета от значения x. Здесь λ_i — значение i-го базисного многочлена в схеме интерполяции Лагранжа в точке 0.
2) Агент вычисляет значения $S_i = w_i \cdot Y$, $[EXC_i, EXD_i] = Com(S_i)$, где Com — это алгоритм схемы обязательства, EXC_i — вычисленное с помощью алгоритма обязательство и EXD_i — строка, позволяющая его раскрыть. Затем агент отправляет EXC_i другим участникам.

3) Агенты отправляют друг другу значения EXD_i. Общий секрет равен $S = \sum_i S_i$.

Пороговая схема позволяет расширить число сценариев применения протокола Диффи — Хеллмана, в том числе представляет возможность улучшения свойств безопасности закрытых ключей участников протокола Диффи — Хеллмана: если в классической схеме злоумышленнику достаточно получить доступ к узлу сети, который хранит соответствующий закрытый ключ, то теперь необходимое количество узлов зависит от порога и всегда больше единицы.

Предложенная схема реализована для протоколов Диффи — Хеллмана на кривых Curve25519 и NIST P-256.

Препринт статьи доступен на arxiv.org [3].

ЛИТЕРАТУРА

1. *Feldman P.* A Practical Scheme for Non-interactive Verifiable Secret Sharing. `http://www.cs.umd.edu/~gasarch/TOPICS/secretsharing/feldmanVSS.pdf`.
2. *Gennaro R. and Goldfeder S.* Fast Multiparty Threshold ECDSA with Fast Trustless Setup. `https://eprint.iacr.org/2019/114`.
3. *Kolegov D., Khalniyazova Yu., and Varlakov D.* Towards Threshold Key Exchange Protocols. `https://arxiv.org/abs/2101.00084`.

УДК 003.26 + 004.056 DOI 10.17223/2226308X/14/18

ИСПОЛЬЗОВАНИЕ РОССИЙСКИХ КРИПТОГРАФИЧЕСКИХ АЛГОРИТМОВ В ПРОТОКОЛЕ БЕЗОПАСНОСТИ СЕТЕВОГО УРОВНЯ WireGuard[1]

Д. Н. Колегов, Ю. Р. Халниязова

Рассматривается криптографический протокол WireGuard, предназначенный для обеспечения защищённости сетевого уровня TCP/IP и построенный с использованием российских криптографических алгоритмов. Необходимость разработки такого протокола вызвана потребностью в применении WireGuard в отечественных перспективных распределённых и облачных технологиях, построенных с применением средств криптографической защиты информации. Описывается решение данной задачи: выбор примитивов, их внедрение, альтернативные подходы, аспекты программной реализации и тестирования, основные текущие результаты работы, а также актуальные направления исследования. Разработанная спецификация и референсная реализация могут быть использованы в качестве отправной точки для разработки рекомендаций по стандартизации протокола WireGuard с российскими криптографическими алгоритмами.

Ключевые слова: *WireGuard, GOST, VPN.*

В настоящее время в области защищённых сетевых технологий активно исследуются, разрабатываются и применяются протоколы семейства Noise Protocol Framework. Основным протоколом здесь является WireGuard, с недавнего времени также поддерживаемый в ядре Linux.

WireGuard — это свободно распространяемое программное обеспечение с открытым исходным кодом, предназначенное для замены устаревшего протокола IPsec и его реализаций. Несомненными достоинствами WireGuard по сравнению со схожими

[1]Работа выполнена ООО «Безопасная информационная зона» и НПО «Криптонит» в рамках совместного исследовательского проекта.