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.

по назначению программными средствами с открытым исходным кодом, такими, как OpenVPN, Strongswan, Libreswan, Linux XFRM и другими системами с закрытым исходным кодом, реализующими технологии VPN на базе IPsec, являются:

— небольшой размер исходного кода (примерно 3800 LoC на июнь 2020);
— простота дизайна протокола и его конечно-автоматной модели и, как следствие, достижимость простоты программной реализации на практике;
— наличие встроенных в протокол средств защиты от DoS-атак, сетевого сканирования и фаззинга;
— относительная простота верификации как протокола, так и его программной реализации;
— соответствие современным криптографическим требованиям;
— формальная верификация свойств безопасности протокола (считается, что протокол WireGuard в текущей версии, использующей Curve25519, верифицирован);
— высокая производительность.

В настоящее время в зарубежной программной разработке, связанной с сетевыми криптографическими протоколами, повсеместно внедряются реализации и адаптации протоколов семейства Noise в целом и WireGuard в частности. Драйверами этих процессов являются разработка протоколов с постквантовыми криптографическими примитивами, а также развитие технологий SDN/SD-WAN, Service Mesh и MPC.

Кратко перечислим лишь самые основные из них:

— протокол nQUIC, созданный компанией Cloudflare и используемый вместо TLS для протокола QUIC, разрабатываемого в качестве замены TCP;
— постквантовая версия протокола WireGuard, использующая постквантовые криптографические алгоритмы и, несмотря на это, показавшая бóльшую производительность, чем IPsec на базе Curve25519 или OpenVPN;
— VPN Flannel;
— применение WireGuard для защиты транспорта в Kubernetes;
— оверлейная сеть Nebula компании Slack;
— фрэймворк libp2p.

В связи с вышесказанным представляется логичным разработать российскую версию протокола WireGuard, использующую отечественные криптографические алгоритмы.

В 2019 г. в ТК26 было направлено предложение по началу работ для стандартизации Noise/WireGuard. На тот момент этот вопрос никого в Комитете не заинтересовал и поддержки не получил. Несмотря на это, исследовательским подразделением компании BI.ZONE был проведён ряд исследовательских работ по возможности применения криптографических протоколов семейства Noise в облачных и сетевых технологиях:

— исследована и обоснована возможность применения пост-квантовых алгоритмов в протоколе QUIC;
— разработан прототип протокола управления WireGuard с использованием пороговой криптографии;
— исследована возможность построения пороговой версии WireGuard на произвольных эллиптических кривых.

Поводом к исследованиям по пороговой версии WireGuard стала публикация в 2019 г. множества работ, выявивших уязвимости в технологиях HSM, TPM и Intel SGX (например, plundervault). Это свидетельствует о том, что использование технологий HSM, TPM, TEE само по себе не говорит о защищённости системы. Дан-

ные системы сложны в управлении, а их пользователи не имеют полного контроля над ними. В настоящее время альтернативным методом получения подобных функциональных свойств считается применение технологий Multi-Party Computation и Threshold Cryptography в протоколах распределения ключей (key agreement in a threshold setting). Так как BI.ZONE активно исследует возможность применения протоколов Noise в своих сервисах, нас заинтересовала возможность построения пороговой версии протокола, что позволило бы решать задачу обеспечения главных ключей не стандартными способами с помощью HSM и TPM, а с использованием криптографических алгоритмов. С удивлением было обнаружено, что данным вопросом в мире не интересуются, несмотря на то, что уже разработаны и активно исследуются пороговые схемы алгоритмов криптографической подписи ECDSA, построенные на том же математическом аппарате.

Причина этого в том, что основным источником таких задач выступают технологии криптовалюты и блокчейн, а не сетевые и облачные технологии. Разработка пороговой схемы WireGuard позволяет обеспечить безопасность закрытого статического ключа WireGuard для клиента и/или сервера, но не с помощью аппаратных методов защиты, применяемых в HSM, TPM и TEE, а с помощью пороговой криптографии.

В таблице приведены алгоритмы, определённые в предлагаемой спецификации. Все алгоритмы используют 256-битные значения входных и выходных параметров. Более подробно начальные предложения по замене криптографических алгоритмов представлены в [1, 2]. Референсная реализация протокола Ru-WireGuard доступна в репозитории [3].

Тип алгоритма	Замена
Алгоритм согласования ключа	ГОСТ Р 34.10-2012 VKO или DH
Эллиптическая кривая	ГОСТ Р 34.10-2012 GC256A
Хэш-функция	ГОСТ Р 34.11-2012
HMAC	ГОСТ Р 34.11-2012
KDF	ГОСТ Р 34.11-2012 KDFTREE или HKDF
AEAD	ГОСТ Р 34.12–2015 Кузнечик в режиме MGM

Для проверки корректности спецификации и программной реализации разработаны три независимых прототипа: два на языке Go и один на языке C. Проведено тестирование возможности работы друг с другом всех прототипов, получены контрольные векторы для основных криптографических значений протокола.

Разработка высокопроизводительной версии протокола не была целью, но, несмотря на это, мы провели базовое тестирование производительности. Ru-WireGuard в настоящее время значительно медленнее wireguard-go. Связано это, во-первых, с тем, что сами по себе криптоалгоритмы оригинального протокола WireGuard быстрее выбранных алгоритмов ГОСТ, а во-вторых, они реализованы на Go Assembler.

Результаты данной работы:

— представлена эталонная реализация протокола Ru-WireGuard;
— исследована производительность полученной референсной реализации в сравнении с оригинальной реализацией wireguard-go;
— проведено тестирование на ошибки спецификации;
— представлены контрольные векторы.

ЛИТЕРАТУРА

1. BI.ZONE. Проект протокола Ru-WireGuard. `https://github.com/bi-zone/ruwireguard-spec`.

2. Ru-WireGuard: Использование российских криптографических алгоритмов в протоколе безопасности сетевого уровня WireGuard. https://bit.ly/3mChAdq.
3. Reference implementation of the Ru-WireGuard protocol in Go. https://github.com/bi-zone/ruwireguard-go.

УДК 519.7 DOI 10.17223/2226308X/14/19

АЛГЕБРАИЧЕСКИЙ КРИПТОАНАЛИЗ НИЗКОРЕСУРСНЫХ ШИФРОВ SIMON И SPECK[1]

А. В. Куценко, Н. Д. Атутова, Д. А. Зюбина, Е. А. Маро, С. Д. Филиппов

Представлены алгебраические атаки на шифры Simon и Speck — два семейства низкоресурсных блочных шифров, имеющих LRX- и ARX-структуры соответственно. Они были представлены Агентством национальной безопасности США в 2013 г., а затем стандартизированы ISO как часть стандарта радиоинтерфейса RFID. Шифры алгебраически кодируются и получаемые системы булевых уравнений решаются с помощью различных SAT-решателей, а также методов, основанных на линеаризации. Впервые к этим шифрам применяются подходы, использующие разреженность систем булевых уравнений. Оценены параметры линеаризации в системах уравнений для обоих шифров. Приведено сравнение эффективности используемых методов.

Ключевые слова: *алгебраический криптоанализ, блочный шифр, низкоресурсный шифр,* Simon, Speck.

Низкоресурсная криптография — направление исследований, представляющее интерес в настоящее время. Это связано с тем, что влияние и использование RFID-меток, ПЛИС, смарт-карт, мобильных телефонов, сенсорных сетей и других криптографических алгоритмов для устройств с ограничениями на используемые ресурсы постоянно растёт и приобретает всё большую важность. Низкоресурсные криптографические примитивы предназначены для обеспечения эффективности и безопасности при ограниченном объёме ресурсов. В этом случае возникает проблема поиска компромисса между безопасностью и эффективностью. В 2013 г. Агентство национальной безопасности США представило семейства Simon и Speck низкоресурсных блочных шифров. Шифр Simon был оптимизирован для производительности на аппаратных устройствах, а Speck — для производительности в программном обеспечении. Но было подчеркнуто, что оба семейства работают исключительно хорошо как в аппаратном, так и в программном обеспечении, обеспечивая гибкость платформы, требуемую будущими приложениями. По состоянию на октябрь 2018 г. шифры Simon и Speck были стандартизированы Международной организацией по стандартизации (ISO) в рамках стандарта радиоинтерфейса RFID (радиочастотной идентификации). Эти шифры являются представителями LRX- и ARX-структур блочных шифров, основой которых является явное использование нелинейных алгебраических операций вместо S-блоков. Это обуславливает интерес к алгебраическому анализу данных шифров. Алгебраический анализ Simon проведён в [1], комбинация алгебраического и усечённого дифференциального криптоанализа шифра Simon от малого числа раундов рассмотрена в [2]. Алгебраические атаки представлены SAT-решателем и алгоритмом ElimLin.

[1]Работа выполнена в рамках госзадания ИМ СО РАН (проект № 0314-2019-0017) при поддержке лаборатории криптографии JetBrains Research; работа первого автора выполнена при поддержке РФФИ (проект № 20-31-70043).