С. В. Гребнев, Е. В. Лазарева, П. А. Лебедев, А. Ю. Нестеренко, А. М. Семенов, Интеграция отечественных протоколов выработки общего ключа в протокол TLS 1.3, *ПДМ. Приложение*, 2018, выпуск 11, 62–65

DOI: 10.17223/2226308X/11/19

УДК 004.056.55 DOI 10.17223/2226308X/11/19

ИНТЕГРАЦИЯ ОТЕЧЕСТВЕННЫХ ПРОТОКОЛОВ ВЫРАБОТКИ ОБЩЕГО КЛЮЧА В ПРОТОКОЛ TLS 1.3

С. В. Гребнев, Е. В. Лазарева, П. А. Лебедев, А. Ю. Нестеренко, А. М. Семенов

Рассматривается актуализация протокола TLS 1.3 с учётом опыта отечественных исследователей и разработчиков, последующая модификация данного протокола, исправляющая ряд недостатков и удовлетворяющая требованиям по безопасности информации, действующим в Российской Федерации. Изменения касаются логики взаимодействия участников протокола при установлении соединения в различных режимах, используемых криптографических примитивов и шифронаборов, а также ключевой системы протокола.

Ключевые слова: *криптографический протокол, выработка общего ключа, TLS.*

Разработка протокола TLS 1.3 началась в 2014 г. В марте 2018 г. проект спецификации данного протокола получил статус стандарта [1]. Новая версия протокола разрабатывалась с целью сделать более быстрый, за счёт сокращения времени на установление соединения, более защищённый и более скрытный, за счёт использования шифрования в процессе установления соединения, вариант протокола. Протокол TLS 1.3 нацелен на использование алгоритмов блочного шифрования в режиме AEAD.

Независимо от TLS 1.3, начиная с 2011 г. в Российской Федерации проводились исследования по созданию новых протоколов выработки общего ключа, первым из которых был Лимонник-3 (L-3) [2]. К данному семейству «цветочных» протоколов относятся протокол Crocus [3], представленный на конференции RusCrypto'12, и протоколы Эхинацея-2 (E-2) и Эхинацея-3 (E-3) [4], представленные на конференции RusCrypto'14.

Итогом проведённых исследований стало создание в 2017 г. рекомендаций по стандартизации Р 1323565.1.004-2017 [5], описывающих схемы выработки общего ключа на основе аутентификации. В состав рекомендаций вошли схемы E-2, E-3 и L-3.

С учётом опыта разработки отечественных решений и особенностей эксплуатации СКЗИ на территории Российской Федерации для использования протокола TLS 1.3 в РФ необходимо внести ряд модификаций, которые позволили бы удовлетворить основным положениям [6].

Отметим ряд положительных качеств протокола TLS 1.3:

— По сравнению с предшествующими версиями установление соединения по протоколу TLS 1.3 является более быстрым за счёт сокращения числа пересылок.
— При установлении соединения по протоколу TLS 1.3 участники стараются как можно быстрее перейти к использованию шифрования. Быстрый переход к обмену зашифрованными сообщениями позволяет обеспечить защиту от утечки метаинформации об участниках протокола и позволяет обеспечить выполнение свойства анонимности на стороне клиента.
— При установлении соединения по протоколу TLS 1.3 осуществляется привязка ключей, полученных в рамках установления соединения данного сеанса связи, к контексту установления соединения.
— Протокол TLS 1.3 обеспечивает возможность создания предварительно распределённого ключа PSK и привязки его к конкретному сеансу связи.

— Протокол TLS 1.3 нацелен на использование режимов шифрования, позволяющих обеспечить имитозащиту всех передаваемых сообщений. Это защищает от большого класса атак, нацеленных на предыдущие версии протокола TLS.

Основываясь на опыте разработки отечественных решений, можно выделить ряд негативных сторон протокола TLS 1.3:

— Согласно спецификации протокола TLS 1.3 [1], в случае использования предварительно распределённого ключа PSK генерация общей точки эллиптической кривой по протоколу Диффи — Хеллмана в процессе установления соединения может являться опциональным параметром, что может привести к нарушению свойства PFS (Perfect Forward Security).
— Использование при генерации ключей третьего уровня (application traffic secret) неполного контекста сеанса установления соединения, зависящего только от первой и второй пересылок, нарушает принцип зависимости сеансовых ключей от всего контекста установления соединения.
— Процесс установления соединения по протоколу TLS 1.3 в случае проведения взаимной аутентификации оставляет возможность отправки сервером данных не аутентифицированному клиенту в рамках второй пересылки.
— TLS 1.3 нацелен на использование режима шифрования AEAD. В этом случае для шифрования и выработки имитовставки используется один ключ. Использование двух ключей — одного для шифрования и другого для имитозащиты — позволяет обеспечить более высокий уровень защиты, что регламентируется принятым в Российской Федерации стандартом ГОСТ Р 34.13-2015 [7] и рекомендациями по стантартизации Р 1323565.1.012-2017 [6].
— При генерации случайных значений в процессе установления соединения по протоколу TLS 1.3 может использоваться один и тот же датчик случайных чисел (ДСЧ) для генерации как секретных, так и открытых случайных значений. Это потенциально может привести к определению секретных значений в случае использования слабых ДСЧ.
— Протокол TLS 1.3 позволяет для реализации протокола Диффи — Хеллмана использовать мультипликативную группу конечного простого поля, что может не обеспечивать необходимый уровень защиты [8]. Данный подход не применяется в Российской Федерации с 2001 г.
— Спецификация протокола TLS 1.3 не предусматривает возможность использования национальных наборов криптографических преобразований и алгоритмов.
— Протокол TLS 1.3 допускает использование режима установления соединения 0-RTT, который является менее стойким по сравнению с другими режимами установления соединения.

Данная работа посвящена описанию способа интеграции схем протоколов E-2 и E-3, в случае односторонней и взаимной аутентификации, в различные режимы установления соединения по протоколу TLS 1.3. Рассматриваемый протокол носит название RuTLS и представляет собой модифицированный вариант протокола TLS 1.3.

Проведённый анализ предлагаемого варианта протокола RuTLS позволяет утверждать, что он является стойким, удовлетворяет набору свойств безопасности, описанных в [9], и обеспечивает более высокий уровень защиты по сравнению с исходным вариантом протокола TLS 1.3.

При внесении модификаций в логику работы протокола установления соединения и ключевую систему использовался опыт отечественных исследований, полученный при

разработке схем Лиммонник-3 [2], Крокус [3] и Эхинацея-2(3) [4]. Данный протокол разрабатывался с учётом дальнейшего его использования на территории Российской Федерации, основываясь на [6]. Отметим ряд наиболее важных отличий протокола RuTLS от TLS 1.3:

— Использование режимов установления соединения в протоколе RuTLS нацелено в первую очередь на обеспечение защиты передаваемой информации, а не на ускорение работы протокола.
— RuTLS не поддерживает менее стойкий, по сравнению с другими, режим установления соединения 0-RTT.
— Отправка данных приложения допускается только после завершения процесса аутентификации.
— Для аутентификации могут использоваться только сертификаты открытых ключей, использование RawKeys не поддерживается.
— Вариант протокола RuTLS предполагает использование минимум двух различных ДСЧ для генерации секретных и открытых случайных значений.
— Исходная ключевая система протокола TLS 1.3 упрощена и переработана с учётом [6].
— При генерации ключей используются идентификаторы участников протокола, извлекаемые из сертификатов, как предложено при разработке схем Эхинацея-2(3) [4].
— При генерации ключей осуществляется привязка ключей, выработанных в рамках установления соединения данного сеанса связи, к контексту установления соединения. Подобный подход использовался при проектировании схемы отечественного протокола Крокус [3].
— Предлагаемый вариант ключевой системы позволяет формировать и использовать различные ключи для шифрования и имитозащиты.
— При установлении соединения в обязательном порядке формируется общая точка эллиптической кривой по протоколу Диффи — Хеллмана (ECDH).
— Ключевая система подразумевает использование только группы точек эллиптической кривой.
— Переработанная ключевая система, логика взаимодействия участников и порядок формирования ключей позволяют разгрузить сервер от проведения лишних вычислений, что может быть полезно при защите от DoS-атак.

ЛИТЕРАТУРА

1. The Transport Layer Security (TLS) Protocol Version 1.3. 2018. `https://tlswg.github.io/tls13-spec/draft-ietf-tls-tls13.html` (дата обращения: 28.03.2018)
2. *Матюхин Д. В.* О некоторых свойствах схем выработки общего ключа, использующих инфраструктуру открытых, в контексте разработки стандартизированных криптографических решений. 2011. `http://www.ruscrypto.ru/resource/summary/rc2011/02_matyukhin.pdf` (дата обращения: 09.01.2018)
3. *Нестеренко А. Ю.* Об одном подходе к построению защищенных соединений // Математические вопросы криптографии. 2013. № 6. С. 170–176.
4. *Гребнев С. В.* О возможности стандартизации протоколов выработки общего ключа. 2018. `http://www.ruscrypto.ru/resource/summary/rc2014/03_grebnev.pdf` (дата обращения: 09.01.2018)

5. Р 1323565.1.004-2017. Информационная технология. Криптографическая защита информации. Схемы выработки общего ключа с аутентификацией на основе открытого ключа. М.: Стандартформ, 2017.
6. Р 1323565.1.012-2017. Информационная технология. Криптографическая защита информации. Принципы разработки и модернизации шифровальных (криптографических) средств защиты информации. М.: Стандартформ, 2017.
7. ГОС Р 34.13–2015. Информационная технология. Криптографическая защита информации. Режимы работы блочных шифров. М.: Стандартформ, 2015.
8. *Kleinjung T.* Discrete logarithms in GF(p) — 768 bits. June 16, 2016. `https://listserv.nodak.edu/cgi-bin/wa.exe?A2=NMBRTHRY;a0c66b63.1606` (дата обращения: 09.01.2018)
9. Automated Validation of Internet Security Protocols and Applications. Properties (Goals). `http://www.avispa-project.org/delivs/6.1/d6-1/node3.html` (дата обращения: 28.03.2018)

УДК 519.17 DOI 10.17223/2226308X/11/20

О ПЕРЕМЕШИВАЮЩИХ И НЕЛИНЕЙНЫХ СВОЙСТВАХ МОДИФИЦИРОВАННЫХ АДДИТИВНЫХ ГЕНЕРАТОРОВ

А. М. Коренева

Исследованы локальные характеристики подстановок множества состояний модифицированных аддитивных генераторов (МАГ), построенных на основе регистров сдвига длины 8 над множеством двоичных 32-мерных векторов, для трёх вариантов множества точек съёма (обратной связи) и двух вариантов модифицирующего преобразования. К исследованным характеристикам подстановок относятся: а) локальный $(0, 256)$-экспонент перемешивающей матрицы M порядка 256, то есть наименьшее натуральное число γ_0, такое, что при любом натуральном $t \geqslant \gamma_0$ положительны все столбцы матрицы M^t с номерами $0, 1, \ldots, 31$; б) показатель 0-совершенности, то есть наименьшее число тактов работы генератора, после которых каждая координатная функция 0-го блока зависит существенно от всех битов начального состояния; в) показатель 0-сильной нелинейности, то есть наименьшее число тактов работы генератора, после которых каждая координатная функция 0-го блока является нелинейной. Вычисленные значения характеристик варьируются от 8 до 29. Полученные результаты могут быть использованы при построении криптографических алгоритмов на основе МАГ, в частности алгоритмов ключевого расписания блочных шифров, обеспечивающих сложную нелинейную взаимосвязь битов основного и раундовых ключей.

Ключевые слова: *модифицированный аддитивный генератор, нелинейные функции, перемешивающие свойства, регистр сдвига, существенная переменная.*

Введение

В основе принципа перемешивания, важного для многих криптографических алгоритмов, лежит существенная нелинейная зависимость выходных данных от элементов входа. Эти свойства важны для оценки эффективности атак на системы защиты информации, таких, например, как последовательное опробование частей секретного параметра системы. Исследованы криптографические свойства степеней преобразования модифицированного аддитивного генератора для двух модификаций аддитивного генератора и трёх вариантов множества точек съёма. С помощью матрично-графово-