

УДК 004.056.5

Внедрение постквантовой криптографии в инфраструктуру сети Интернет

Венедюхин Александр Анатольевич^{1(*)}

vened@indata.org.ru

Проклашкина Софья Антоновна²

proklashkinasa@student.bmstu.ru

Якубов Павел Дмитриевич²

yakubovpd@student.bmstu.ru

¹ Фонд развития сетевых технологий «ИнДата», Москва, Россия² МГТУ им. Н.Э. Баумана, Москва, Россия

Аннотация. Работа посвящена анализу возможностей и последствий внедрения в инфраструктуру сети Интернет постквантовых алгоритмов, в частности, ML-DSA-65. Разработаны программные утилиты, использующие ML-DSA-65 для создания электронных подписей файлов и цифровых сертификатов. Проведено сравнение скорости работы ML-DSA с традиционными алгоритмами цифровой подписи — RSA, ECDSA. Рассмотрены технологии, которые массовое внедрение ML-DSA затронет в первую очередь — в связи с их широким использованием.

Ключевые слова: постквантовый алгоритм, алгоритм Шора, ML-DSA, ML-DSA-65, TLS

Введение. Постквантовые алгоритмы (квантово-устойчивые алгоритмы) — это криптографические алгоритмы, которые, в отличие от широко используемых алгоритмов традиционной криптографии, имеют теоретическую стойкость к атакам квантовых компьютеров, проводимых с помощью алгоритма Шора [1]. Актуальность работы обусловлена возможным появлением квантовых компьютеров и необходимостью своевременной защиты данных и каналов связи от атак.

Методы и материалы; результаты. Для многих распространенных языков программирования, таких как Go, C, Python, Java и других, существуют библиотеки с открытым исходным кодом, позволяющие использовать реализацию постквантовых алгоритмов в любых целях. Разработанные с их помощью на языке программирования Go утилиты продемонстрировали работоспособность и высокую скорость алгоритмов семейства ML-DSA. Из таблицы видно, что ML-DSA по скорости не уступает традиционным алгоритмам цифровой подписи.

С помощью утилиты для создания сертификатов были созданы TLS-сертификаты с постквантовой схемой цифровой подписи, успешно распознающиеся широко распространенной утилитой «openssl». Основной недостаток цифровых подписей типа ML-DSA — их размер, превышающий обычный размер подписей в десятки раз. При массовом внедрении ML-DSA, он окажет сильное влияние на TLS и DPI из-за превышения размера TLS-записи, а также на DNSSEC. Хотя ML-DSA был стандартизован относительно недавно и его распространение по сети Интернет только началось [2], успешный при-

мер внедрения постквантового алгоритма уже есть — алгоритм обмена ключами ML-KEM уже используется современными браузерами по умолчанию и занимает большую долю в мировом трафике.

Сравнение скорости работы различных алгоритмов цифровой подписи

Алгоритм	Генерация ключа, мкс	Подпись данных, мкс	Проверка подписи, мкс
ML-DSA-44	84	212	36
ML-DSA-65	150	339	50
ML-DSA-87	220	373	72
ECDSA-P384	108	171	499
RSA-3072	156256	909	31

Заключение. Выполненный анализ позволил оценить: как постквантовые алгоритмы используются в инфраструктуре сети Интернет; чем они отличаются от традиционных и какое влияние на сеть Интернет вызовет широкое внедрение ML-DSA-65. Дальнейшее развитие данной работы состоит в разработке и практическом применении утилит, использующих постквантовые алгоритмы и анализе их работы.

Список источников

- [1] Наседкин П.Н., Сверкунов В.А. Криптографические алгоритмы на пути к постквантовой криптографии. *Информационные технологии и математическое моделирование в управлении сложными системами*, 2022, № 4 (16), с. 67–73.
[https://doi.org/10.26731/2658-3704.2022.4\(16\).67-73](https://doi.org/10.26731/2658-3704.2022.4(16).67-73)
- [2] Артюхин А.А., Евсеев А.В., Коваленко Т.А. Постквантовая криптография 2025 года: стандарты Fips 203-205 и алгоритм HQC в контексте ресурсно ограниченных систем. *Парадигма*, 2025, № 5–2, с. 343–347.