Параметрический выбор криптопримитивов для блокчейн-платформ

100 стр. | PDF | 2022 г.

В настоящее время в технологически развитых странах мира, главным образом в США, Китае, России и странах Евросоюза, запланирован переход к постквантовой криптографии. Актуальность упомянутого перехода подтверждается требованиями национальной программы *«Цифровая экономика Российской Федерации»*, утвержденной распоряжением Правительства Российской Федерации от 28 июня 2017 г. № 1632-р. В этой программе «обеспечение устойчивости и безопасности функционирования информационной инфраструктуры и сервисов передачи, обработки и хранения больших объемов данных», в том числе национальных блокчейн-экосистем и платформ, является одной из пяти ключевых целей Проекта «Информационная безопасность». При этом акцент делается именно на устойчивости к новым атакам злоумышленников с использованием так называемого релевантного или значимого квантового компьютера (*Cryptographically Relevant Quantum Computer*, CRQC).

В настоящем учебно-методическом пособии рассмотрено возможное решение задачи параметрического выбора постквантовых криптопритивов на основе целочисленных решеток (*lattice-based cryptography*), кодов, исправляющих ошибки (*code-based cryptography*), многочленов от многих переменных (*multivariate cryptography*), криптографических хеш-функций (*hash-based cryptography*), изогений суперсингулярных эллиптических кривых (*supersingular isogeny-based cryptography*) и пр. Приведены соответствующие примеры и выработан ряд полезных рекомендаций.

Пособие представляет определенный теоретический и практический интерес для специалистов в области информационных технологий и киберустойчивости Цифровой экономики Российской Федерации.