Кудін Антон Михайлович

Атаки за побічними каналами на постквантові криптосистеми: відкриті проблеми та нові напрями досліджень

Захист постквантових криптосистем від атак за побічними каналами (side-channel cryptanalysis (SCA)) є одним із актуальних напрямів досліджень в сучасній криптології, оскільки надає альтернативний шлях послаблення стійкості постквантової криптосистеми, який не залежить від прогресу створення промислових квантових обчислювачів. Алгоритми, які стали переможцями в конкурсах на нові стандарти посквантових криптосистем (ML-KEM (раніше CRYSTALS-Kyber) — стандарт FIPS 203 та ML-DSA (раніше CRYSTALS-Dilithium) — стандарт FIPS 204) на основі модульних решіток, використовують специфічні математичні операції (наприклад, NTT) та традиційні методи захисту від SCA для AES чи RSA криптосистем тут часто виявляються неефективними або занадто ресурсомісткими. До цієї проблеми додається необхідність реалізації нових криптосистем для сучасних обчислювальних платформ – таких як розподілені та блокчейн платформи, оптимізація програмних реалізацій нових стандартів за критерієм «безпека/продуктивність» для забезпечення достатнього рівня SCA-захисту для пристроїв з обмеженими ресурсами (IoT, смарт-карти, тощо). В доповіді аналізуються нові постановки задач SCA та сучасні методи захисту від них. Аналізуються нові методи побудови безпечних криптографічних модулів для розподілених/блокчейн систем, запропонованих автором на основі підходу Шеннона побудови надійних систем з ненадійних елементів. Аналізується можливість застосування теорії загальних оптимальних алгоритмів як метрики SCA захисту.