Назва:
За межами постквантової криптографії або криптосистеми, стійкі в певних моделях обчислень

Короткий опис:
Проблема оцінки стійкості криптографічних перетворень в сучасній криптографії як правило реалізується за допомогою аксіоматичного або «доказового» підходу. Він полягає в зведенні стійкості криптографічних алгоритмів до стійкості криптографічних примітивів з відомою стійкістю або до вирішення певних обчислювальних задач, складність яких добре вивчена. Оскільки квантова модель обчислень змінює складність певних обчислювальних задач (наприклад, задачі факторизації цілих чисел), в криптографії вивчаються класи алгоритмів, які будуть залишатись стійкими в квантовій моделі обчислень – так звані постквантові криптографічні алгоритми. Узагальненням цієї постановки задачі є вивчення моделей обчислень, в яких існують криптографічні алгоритми, найкращий алгоритм криптоаналізу яких має експоненційну складність або наближається до такої. Ідеї зв'язку криптоаналізу та моделей обчислень вперше була запропонована в 80-х роках 20 сторіччя Брасардом і отримала назву «релятівістської криптографії». В доповіді розглядаються сучасний стан досліджень в цій галузі, розглядається існування реальних моделей обчислень, в яких деякі сучасні криптоалгоритми є нестійкими та пропонуються підходи до побудови криптографічних перетворень, стійких в перспективних моделях обчислень.

Відомості про доповідача:
науковий ступінь – д.т.н.
організація – Національний банк України, Навчально-науковий Фізико-технічний інститут КПІ ім. Ігоря Сікорського