Назва: Про нові цифрові підписи криптографії від багатьох змінних

Короткий опис:

Криптографія від багатьох змінних (КБЗ) є одним із п'яти основних напрямків постквантової криптографії. Цей напрямок особливо важливий для створення швидких процедур цифрових підписів. Незважаючи на те, що в даний час оголошені Інститутом національних стандартів інформаційних технологій (NIST, США) стандарти постквантової криптографії будуються в рамках альтернативних до КБЗ підходів, тривають інтенсивні дослідження нових криптосистем від багатьох змінних.

Що стосується цифрових підписів, NIST оголосивдва стандарти. Перший називається алгоритмом .цифрового підпису на основі модульної решітки (скорочено ML-DSA) і визначає загальний алгоритм цифрового підпису.

Другий називається алгоритмом цифрового підпису на основі хешування без збереження стану (скорочено SLH-DSA). Це алгоритм цифрового підпису, заснований на техніці хешування.

Значно коротші підписи можна отримувати за допомогу побудованоі методами БГЗ криптосистеми «TUOV: Triangular Unbalanced Oil and Vinegar» . Вона була нещодавно представлена в NIST (див. https://csrc.nist.gov/csrc/media/Projects/pqc-dig-sig/documents/round-1/spec -files/TUOV-spec-web.pdf , головний заявник – відомий Jintaj Ding з Китаю.

Пропонована доповідь представляє розроблені автором цифрові підписи криптографії від багатьох змінених.

Деякі з них відомі ще з 2015 року, кританаліз для них досі не знайдено. Запропоновані методи дозволяють побудувати значне укладання довільно вибраної криптосистеми від багатьох змінних такої, як згадана вище TUOV, стара система Matsumoto-Imai, різні варіанти системи олії та оцету.

Крім того, новий метод дає можливість створювати алгебраїчні криптосистеми над скінченими комутативними кільцями відмінними від полів, такими як арифметичні або булеві кільця. Запропоновані алгоритми вже зараз можна використовувати для захисту інформаційних систем.

Відомості про доповідача:

Устименко Василь Олександрович

науковий ступінь – доктор фізико -математичних наук

вчене звання – професор

посада – Visiting Professor of Royal Holloway University of London, Principal Investigator of the

project of British Academy LTRSF\100333.