МЕТОД ШИФРУВАННЯ НА ОСНОВІ БАГАТОПАРАМЕТРИЧНИХ ГРУП

Гвоздьов Р. Ю., Сєвєрінов О. В.
Харківський національний університет радіоелектроніки, Харків, Україна

В роботі розглянуто методи шифрування на основі багатопараметричних груп.

Об'єктом дослідження є алгоритми шифрування та електронного підпису на основі криптосистеми MST3.

Предмет дослідження – процес аналізу стійкості математичних перетворень на базі багатопараметричних груп.

Зі стрімким розвитком квантових технологій, квантових комп'ютерів, що базуються на цьому явищі, виникла необхідність у нових криптоалгоритмах, що будуть стійкими до квантового криптоаналізу.

Стійкість криптографічних систем на багатопараметричних групах базується на задачі розкладання елемента такої групи по набору елементів логарифмічною підпису. До теперішнього часу відома тільки одна реалізація криптосистеми MST3, побудованої за Абелевим центром групи Судзукі [1].

Проблема побудови багатопараметричних груп на практиці полягає в розробці ефективного алгоритму для відображень числа на групу і зворотного відображення з обчислювально простою груповою операцією.

В роботі розглядаються алгоритми побудови та використання криптосистеми MST3 для шифрування та електронного підпису [2, 3]. В роботі був виміряний час генерації ключових даних, виконання шифрування та розшифрування у порівнянні з криптосистемою RSA. Також наводиться час генерації ключових даних, створення та перевірки електронного підпису. Здійснюється аналіз щодо можливої стійкості проти квантовий алгоритму Шора – розв'язку дискретного логарифму в скінченному полі [4].

Список літератури

1. Khalimov G. et al. Encryption Scheme Based on the Automorphism Group of the Suzuki Function Field //2020 IEEE International Conference on Problems of Infocommunications. Science and Technology (PIC S&T). – IEEE, 2020. – С. 383-387.

2. Haibo Hong, Jing Li, Licheng Wang, Yixian Yang, and Xinxin Niu. A Digital Signature Scheme Based on MST3 Cryptosystems. – 2014.

3. Khalimov G. et al. Towards three-parameter group encryption scheme for MST3 cryptosystem improvement //2021 Fifth World Conference on Smart Trends in Systems Security and Sustainability (WorldS4). – IEEE, 2021. – С. 204-211.

4. Marrtin Ekera Quantum algorithms for computing general discrete logarithms and orders with tradeoffs. – 2020.