МЕТОДИ ЕЛЕКТРОННОГО ПІДПИСУ НА ОСНОВІ НЕКОМУТАТИВНИХ ГРУП

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

З розвитком технологій квантових обчислень та побудовою дослідних образків квантових комп'ютерів відбувається модернізація криптографічних алгоритмів та протоколів на предмет підвищення їх стійкості.

Наявність квантових алгоритмів розкладання цілих чисел і дискретних логарифмів ставить під загрозу можливість використання криптографії доквантового періоду.

Особливо це чіпає алгоритми асиметричних перетворень, таких як асиметричне шифрування та електронний підпис. В даний момент відбувається перехід до пост-квантових алгоритмів які будуть стійкі до нових атак з використанням квантових обчислень.

Одним із перспективних напрямків є використання алгоритмів на основі некомутативних груп.

Метою доповіді є розгляд та аналіз моделей електронного підпису на основі некомутативних груп, таких як криптосистеми на основі груп Судзукі, Томпсона.

Здійснюється огляд різних груп з різною кількістю параметрів та некомутативних операцій, що використовуються для створення криптоалгоритмів. Проводиться аналіз існуючих протоколів автентифікації, розподілу ключів, електронного підпису, асиметричного шифрування та оцінка їх можливості потенційного та практичного використання.

Розглядаються методи оптимізації швидкодії алгоритмів та можливості їх використання при побудові нової та модернізації існуючої інфраструктури відкритих ключів.

Список літератури

1. G.Khalimov, Y.Kotukh, S.Khalimova, O.Sievierinov, A.Vlasov. "Towards advance encryption based on a Generalized Suzuki 2-groups". International Conference on Electrical, Computer, Communications and Mechatronics Engineering (ICECCME) 2021.

2. G.Khalimov, Y.Kotukh, I.Didmanidze, O.Sievierinov. "Towards three-parameter group encryption scheme for MST3 cryptosystem improvement". Fifth World Conference on Smart Trends in Systems Security and Sustainability (WorldS4) 2021.

3. Gautam Kumar and Hemraj Saini "Novel Noncommutative Cryptography Scheme Using Extra Special Group" Department of Computer Science & Engineering, Jaypee University of Information Technology, Solan 173234, India.

4. I. Anshel, M. Anshel, D. Goldfeld, An algebraic method for public-key cryptography, Math. Res. Lett. 6 (1999), 287–291.