ПІДПИС НА ОСНОВІ КРИПТОСИСТЕМ З ЛОГАРИФМІЧНИМ ПІДПИСОМ

Хівренко Г.О., Фроленко В.О.
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.

У кінці 1970-х років Спірос Магліверас розпочав вивчення використання спеціальних факторизацій для неабелевих груп з відомими властивостями, що називаються логарифмічними підписами. Пізніше були опубліковані роботи, що описують створені ним криптосистеми MST1, які ґрунтуються на логарифмічних підписах, та MST2, що базуються на іншому типі множин, відомих як [s,r]-осередки [1]. Нещодавно була розроблена нова криптосистема з відкритими ключами, яка поєднує дві попередні криптосистеми та працює на основі логарифмічних підписів та випадкових покриттів неабелевих груп. Для реалізації цієї системи були введені Судзукі 2-групи

Метою доповіді є розгляд алгоритмів побудови цифрового підпису на основі криптосистем MST3. Розглянута побудова цифрового підпису на основі криптосистеми MST3, яка відносяться до класу квантово-стійкої. MST3 криптосистема будується на основі логарифмічних підписів, а також на Судзукі 2 групі [2, 3]. Актуальним є розвиток криптосистем схожого типу на багатопараметричні групи, що дозволяє зменшити складність обчислень без втрати секретності. Досліджувана область має великий потенціал, оскільки вона відноситься до області, яку називають "післяквантовою криптографією". Серед актуальних завдань у цій галузі можна виділити розробку нових підходів до створення логарифмічних підписів, досягнення більшої продуктивності криптосистем і створення надійних схем захисту даних.

Виконано попередній квантовий криптоаналіз на основі використання алгоритму Гровера, який показує, що складність квантового комп'ютера буде пропорційна кореню квадратному з K, де K - розмір множини ключів. Квантовий алгоритм запропоновано для моделі переборної атаки на ключі.

Список літератури

1. Svaba, Pavol. (2011). Covers and Logarithmic Signatures of Finite Groups in Cryptography.

2. Hong, Haibo & Li, Jing & Wang, Licheng & Yang, Yixian & Niu, Xinxin. (2014). A Digital Signature Scheme Based on MST3 Cryptosystems. Mathematical Problems in Engineering. 2014. 10.1155/2014/630421.

3. Khalimov G., Kotukh Y., Didmanidze I., Sievierinov O., Khalimova S., Vlasov A. (2021, July). Towards three-parameter group encryption scheme for MST3 cryptosystem improvement. In *2021 Fifth World Conference on Smart Trends in Systems Security and Sustainability (WorldS4)* (pp. 204-211). IEEE.