КРИПТОСИСТЕМИ НА ОСНОВІ ЛОГАРИФМІЧНОГО ПІДПИСУ

Колесніков М.Є., Халімов Г.З.
Харківський національний університет радіоелектроніки, Харків, Україна

Після того, як Вітфілд Діффі та Мартін Геллман представили ідею відкритих ключів шифрування, асиметрична криптографія різко стрибнула вперед. Існує багато криптосистем з відкритим ключем, але більшість з них вже зламано, а такі, що витримали перевірку часом, ґрунтуються на складності вирішення певних математичних задач.

Наприкінці 1970-х років Спірос Магліверас почав досліджувати використання в криптографії спеціальних факторизацій для кінцевих неабелевих груп, відомих як логарифмічні підписи [1]. Пізніше були опубліковані роботи, які описують розроблені ним криптосистеми - MST1, що базується на логарифмічних підписах, та MST2 на основі іншого типу накриття множин - так званих [s, r]-осередках.

Втім, на сьогодні нема відомих реалізацій MST1 або MST2. Нещодавно була розроблена нова криптосистема на відкритих ключах – MST3, що поєднує дві попередні та працює на основі логарифмічних підписів та випадкових накриттів кінцевих неабелевих груп. Для реалізації цієї системи були запропоновані 2-групи Судзукі [2].

Метою доповіді є розгляд алгоритму MST3, що базуватиметься на поєднанні 2-груп Судзукі та логарифмічних підписів, а також у доведенні того, що в практичній криптографії можна використовувати логарифмічні підписи та накриття для кінцевих груп.

В доповіді увага буде зосереджена на накриттях та методах їхнього ефективного генерування для великих кінцевих груп. Досліджуватиметься реалізація криптосистеми MST3 з відкритим ключем з 2-групами Судзукі. Завдяки їхній простій структурі, вони дозволяють вивчити безпеку системи та забезпечити ефективну реалізацію.

Буде представлено дослідження її безпеки. Використовуючи властивості групової операції у 2-групах Судзукі, а також властивості самих логарифмічних підписів, буде розроблена та застосована атака, що показує непридатність канонічних підписів в цій реалізації.

Список літератури

1. S. S. Magliveras. A Cryptosystem from Logarithmic Signatures of Finite Groups / Magliveras S. S. // Тези доповідей XXIX Середньозахідного симпозіуму з електронних мікросхем та систем. – Амстердам : видавничий дім «Elsevier», 1986 – С. 972—975. DOI: https://doi.org/10.1007/s10623-010-9369-9

2. G. Higman. Suzuki 2-groups / Higman G. // Ілінойський математичний журнал. – Дарем : видавничий дім «Duke University Press», 1963. Т. 7, №1. С. 79–96. DOI: https://doi.org/10.1215/ijm/1255637483.