Фауре Еміль Віталійович
д.т.н., проф., професор кафедри інформаційної безпеки та комп'ютерної інженерії, Черкаський державний технологічний університет, м. Черкаси, Україна
Махинько Микола Вікторович
GoodLabs Studio Inc., Торонто, Канада

АЛГОРИТМ ФОРМУВАННЯ АНСАМБЛЮ КОДОВИХ СЛІВ – ПЕРЕСТАНОВОК З ЗАДАНИМИ ВЛАСТИВОСТЯМИ

Підхід до побудови трьохетапного криптографічного протоколу [1] базується на представленні інформаційного повідомлення у вигляді перестановки чисел заданої довжини M.

Використання трьохетапного протоколу на основі перестановок [1], на відміну від інших трьохетапних протоколів, відзначається тим, що на кожному етапі передавання даних учасники інформаційної взаємодії мають отримувати перестановки. В умовах високої зашумленості каналу зв'язку така особливість призводить до необхідності використання підходів до завадостійкого передавання перестановок.

У випадку, коли для передавання інформації має бути використаний ансамбль повідомлень з потужністю, значно меншою за $M!$, довільний вибір перестановок не є максимально ефективним з точки зору забезпечення завадостійкості їх передавання.

Метою цієї роботи є побудова алгоритму формування ансамблю кодових слів – перестановок з необхідними потужністю та показниками достовірності.

Формування такого ансамблю кодових слів досягається застосуванням афінної загальної лінійної групи $AGL(1,M)$ та проективної загальної лінійної групи $PGL(2,M)$ [2, 3]. Показано, що такий підхід, окрім забезпечення кодової відстані $M-1$ для ансамблю перестановок, дозволяє формувати мережні та сеансові ключі під час обміну даними.

Розроблений алгоритм формування ансамблю кодових слів – перестановок, окрім трьохетапного криптографічного протоколу може також бути ефективно застосованим для нероздільного факторіального кодування даних, наприклад, під час забезпечення інформаційної взаємодії машинного типу з динамічно змінюваною структурою об'єктів взаємодії.

Список літератури

1. Shcherba A., Faure E., Lavdanska O. Three-Pass Cryptographic Protocol Based on Permutations // *2020 IEEE 2nd International Conference on Advanced Trends in Information Theory (ATIT)*, Kyiv, Ukraine, Nov. 2020. P. 281–284. doi: https://doi.org/10.1109/ATIT50783.2020.9349343

2. Huppert B. Endliche Gruppen I. Berlin, Heidelberg: Springer Berlin Heidelberg, 1967. 796 p. doi: https://doi.org/10.1007/978-3-642-64981-3

3. Mojica de la Vega L. G. Permutation Arrays with Large Hamming Distance : PhD dissertation.The University of Texas at Dallas, 2017. 108 p.