ВДОСКОНАЛЕННЯ ТЕХНОЛОГІЇ ПОБУДОВИ НЕКОМУТАТИВНИХ СЕТ-ОПЕРАЦІЙ

Рудницький В.М., Лада Н.В.
Державний науково-дослідний інститут випробувань і сертифікації озброєння та військової техніки, Україна
Короткий Т.К.
Черкаський державний технологічний університет, Черкаси, Україна

Одним із перспективних шляхів розвитку малоресурсної криптографії є СЕТ-шифрування, яке реалізується на основі генерації псевдовипадкових наборів СЕТ-операцій. СЕТ-операції представляють собою дискретні моделі таблиць підстановки [1]. Серед СЕТ-операцій особливе місце займають СЕТ-операції які допускають перестановку операндів. Особливість даних операцій полягає в тому що після перестановки операндів змінюється дискретна модель операції і змінюються таблиці підстановки, що забезпечує збільшення до двох разів кількості таблиць підстановки в криптоалгоритмі [1]. На жаль синтез даних операцій проводиться лише за результатами обчислювального експерименту [2] за відсутності теоретичних методів побудови.

Метою доповіді є вдосконалення технології побудови некомутативних СЕТ-операцій на основі об'єднання одноопераднних операцій.

Синтез симетричних двохоперандних СЕТ-операцій які допускають перестановку операндів можна реалізувати на основі дублювання одноопераднних операцій. Дублювання одноопераднних СЕТ-операцій по своїй сутності представляє повтор СЕТ-операцій з різними аргументами. Можна допустити, що об'єднання одноопераднних СЕТ-операцій з різними аргументами забезпечить синтез як симетричних так і несиметричних двохоперандних СЕТ-операцій які допускають перестановку операндів. За результатами дослідження вдалося синтезувати всі 576 двохрозрядні двохоперандні СЕТ-операції які допускають перестановку операндів.

Отримані результати дозволили удосконалити технологію синтезу комутативних і некомутативних двохоперандних СЕТ-операцій для побудови мало ресурсних систем потокового шифрування.

Список літератури

4. V. Rudnytskyi, N. Lada, V. Babenko, H. Kuchuk, D. Pidlasyi, D. Kamak and Ye. Ivashchenko Modeling of groups of dual-cycle non-commutative two-operand CET-operations. Journal of Xidian University Volume 18 – Issue 10 – October 2024 Page No: 916-958. Doi.10.37896/jxu18.10/069

5. Рудницький В.М., Лада Н.В., Геращенко М., Короткий Т.К. Стабецька Т.А. Modeling relationships in non-commutative two-operand two-bit cet-operations of a double cycle when permuting the operands Технічний аудит і резерви виробництва. №3/2 (77), 2024. с.30-35. https://doi.org/10.15587/2706-5448.2024.306980