МЕТОДИКА МАСШТАБУВАННЯ БЛОЧНИХ СИМЕТРИЧНИХ ШИФРІВ

Шпак Д.М.
Научный руководитель – к.т.н., доц. Олійников Р.В.
Харківський національний університет радіоелектроніки
(61166, Харків, пр. Леніна,14, каф. Безпеки інформаційних технологій)

The given work is devoted to the methods of the scaling block symmetrical chippers. The Offered method consists of five stages. The Method allows valuing the structured similarity of scaled and scalable cipher.

Статистичні дослідження є значною частиною аналізу блочних симетричних шифрів. Існує ряд досліджень, виконання яких є неможливим по причині їх надвеликих обчислювальної складності та затрат пам'яті. Можливим вирішенням цієї проблеми є створення масштабованих моделей алгоритмів, що досліджуються, та визначення властивостей шифру виходячи з результатів дослідження моделей. Обов'язковою умовою для масштабованих моделей є щонайбільша структурна схожість. У теперішній час поняття та методи оцінки структурної схожості не є чітко визначені. Методика створення масштабованих моделей не є повністю вивченою. Сформована та закінчена методика масштабування може поліпшити вивчення БСШ, формувати масштабовані моделі для різних шифрів за єдиним принципом, а також визначати, яка з моделей шифру має найбільшу структурну схожість з масштабуємим алгоритмом.

Запропонована методика масштабування містить ряд етапів.

На першому етапі визначається об'єкт та мета масштабування. На другому етапі виходячи з цілей масштабування встановлюються вимоги до моделі алгоритми та формуються критерії відповідності до вимог. На третьому етапі проводиться вивчення алгоритму, що масштабується визначається ефективність перетворень та матриця співвідношень. На четвертому етапі на основі отриманих даних та відповідно вимогам до моделі створюється проект моделі масштабованого алгоритму. Для нього обчислюється ефективність перетворень та матриця співвідношень. Відбувається реалізація масштабованого алгоритму. На п'ятому етапі отримана масштабована модель блочного симетричного шифру тестується на відповідність критеріям масштабування. Проводиться оцінка структурної схожості моделі та масштабуємого алгоритму. Та робиться висновок щодо відповідності отриманої масштабованої моделі вимогам масштабування.

У подальшому ця методика може бути використана для мастабування інших алгоритмів.

Актуальним є подальше поглиблення методики масштабування для підвищення її ефективності.