УДК 004.056.055

РЕКОМЕНДАЦІЇ ЩОДО ПОБУДОВИ СИМЕТРИЧНИХ БЛОКОВИХ ШИФРІВ (СБШ) ПІДВИЩЕНОЇ ШВИДКОСТІ

А. В. Остапенко, аспірант
Вінницький національний технічний університет
asja87@gmail.com

Потреба вирішення проблеми захисту електронної інформації обумовлює актуальність розробки шифрів, як одного із видів криптографічних перетворень, що використовують для захисту інформації в комп'ютерних системах та мережах. Недоліки алгоритмічної реалізації перетворень СБШ можуть призводити до зменшення їх криптографічної стійкості та зменшення швидкості процедур зашифрування, розшифрування.

Як правило, алгоритми зашифрування та розшифрування СБШ є ітераційними і складаються з послідовності перетворень (раундів). Ці перетворення описуються однією і тією ж функцією, але в якості аргументів використовуються результати попереднього перетворення і раундовий ключ, який отримується як результат процедури розгортання секретного ключа.

Проведений аналіз відомих СБШ дозволяє сформулювати рекомендації для вибору перетворень, що забезпечать підвищення швидкості шифрування.

Використання великої кількості табличних замін збільшує вимоги шифру до енергонезалежної пам'яті. Тому, необхідно передбачити можливість реалізації табличної заміни як таблиці або як послідовність операцій, для вибору у конкретній системі.

Масове використання операцій орієнтованих на певний вид платформ суттєво зменшує швидкість шифрування СБШ на інших платформах, що обмежує можливості їх використання.

Використання складних процедур розгортання секретного ключа значно зменшують швидкість шифрування СБШ. Отже, процедура розгортання секретного ключа повинна бути реалізована максимально просто з можливістю розпаралелення обчислень в багатопроцесорних системах.

В багатьох СБШ збільшення рівня криптографічної стійкості досягається шляхом збільшення кількості раундів шифрування, що значно зменшує швидкість шифрування цих шифрів. Тому, стійкість шифру не повинна досягатись лише виключно збільшенням кількості ітерацій перетворення.

Використання складних перетворень з великою кількістю операцій, впливає на швидкість шифрування СБШ, ускладнює можливість аналізу стійкості та унеможливлює доведення відсутності вразливостей. Тому, структура перетворень СБШ повинна бути максимально зрозумілою та прозорою для її аналізу та дослідження.

Використання однорідних структур перетворень може призвести до того, що закономірність одного раунду може бути розповсюджена на весь ланцюжок перетворень, полегшуючи тим самим криптоаналіз СБШ. Тому, деякі автори криптоалгоритмів використовують неоднорідну структуру, в якості основи для СБШ. При цьому різні раунди шифрування можуть мати вразливості різних типів, але в сукупності забезпечувати високу стійкість перетворення в цілому.