УДК 004.056

Миронець І.В., Миронюк Т.В., Сисоєнко С.В.
Черкаський державний технологічний університет

Апаратна реалізації базової групи операцій перестановок керованих інформацією

Серед усього спектру методів захисту даних від несанкціонованого доступу особливе місце займають криптографічні методи. На відміну від інших методів, вони спираються лише на властивості самої інформації і не використовують властивості її матеріальних носіїв, особливості вузлів її обробки, передачі та зберігання.

Широке застосування комп'ютерних технологій та постійне збільшення обсягу інформаційних потоків викликає постійне зростання інтересу до криптографії. Останнім часом збільшується роль програмних засобів захисту інформації, які не потребують великих фінансових витрат в порівнянні з апаратними криптосистемами. Сучасні методи шифрування гарантують практично абсолютний захист даних, але завжди залишається проблема надійності їх реалізації [1].

Протягом багатьох років криптографія слугувала виключно військовим цілям. Сьогодні звичайні користувачі отримали можливість звертатися до засобів, які дозволяють їм захистити себе від несанкціонованого доступу до конфіденційної інформації, застосовуючи методи комп’ютерної криптографії.

Захист інформації в автоматизованих системах та комунікаційних мережах здійснюється впровадженням необхідних правових, організаційних та технічних заходів, розробкою відповідного математичного, програмного та апаратного забезпечення. Серед цих складових, вагоме місце належить криптографічним методам, які забезпечують особливі перетворення інформації шляхом залучення спеціального математичного апарату. Наукові дослідження багатьох вчених зумовили появу вагомих математичних результатів у цій сфері, надійність і перспективність застосування яких набуло визнання.

Процес криптографічного закриття даних може здійснюватися як програмно, так і апаратно. Апаратна реалізація відрізняється суттєво більшою вартістю, однак їй властиві й переваги: висока продуктивність, простота, захищеність і т.д.. Програмна реалізація більш практична, допускає відому гнучкість у використанні.

В публікації [2] була доведена коректність застосування отриманих внаслідок обчислювального експерименту базових груп операцій криптографічного перетворення, побудованих на основі визначених восьми базових операцій, які є придатними для криптографічного перетворення інформації в системах інформаційної безпеки.

В результаті представлення групи базових операцій у вигляді дискретних моделей було визначено залежності для основних елементів операцій. А в ході аналізу одержаних результатів було виявлено, що базову групу операцій криптографічного перетворення можуть утворювати лише ті операції криптографічного перетворення, в яких значення основних елементів по діагоналі дорівнює 2^3 варіантів [2].

Дослідивши побудовані структурні схеми, які відображають реалізацію дискретних моделей базових операцій, що входять до

визначеної базової групи операцій перестановок, керованих інформацією, створимо загальну функціональну схему реалізації базових операцій перестановок керованих інформацією для систем криптозахисту та представимо її у вигляді функціональної схеми зображеної на рис. 1.

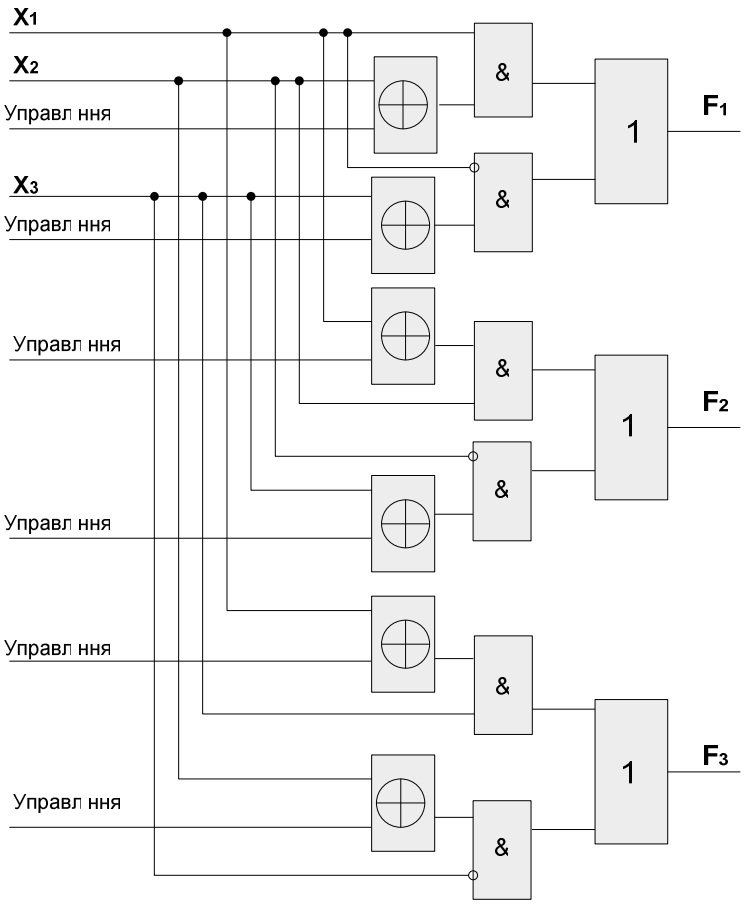

Рис. 1. Загальна функціональна схема реалізації базової групи операцій перестановок керованих інформацією

Створений пристрій реалізує повний набір базових груп елементарних операцій перестановок керованих інформацією для криптографічного перетворення.

Отже, в результаті проведеного дослідження проаналізовано базові операції, що входять до базової групи операцій перестановок, керованих інформацією, реалізацію їх дискретних моделей, а також отримано загальну функціональну схему апаратної реалізації базової групи операцій перестановок керованих інформацією для систем криптозахисту, що дає можливість підвищити стійкість та ефективність криптоалгоримів, а саме - збільшення їх варіативності та стійкості до лінійного криптоаналізу.

Список використаних джерел

1. *Миронець І.В. Зменшення складності пристроїв криптографічного перетворення інформації на основі введення інформаційної надлишковості. / І.В. Миронець // Системи обробки інформації: збірник наукових праць. – Х.: Харківський університет Повітряних Сил імені Івана Кожедуба, 2015. – Вип. 11 (136). – 232 с. - С.9-11.*
2. *Миронюк Т.В. Визначення елементарних операцій базової групи перестановок, керованих інформацією / Т.В. Миронюк // Вісник Черкаського державного технологічного університету, № 2, Черкаси, 2016. – С. 100-105.*