УДК 004.056

Ю. В. Баришев

АПАРАТНІ ЗАСОБИ ДЛЯ ПСЕВДОНЕДЕТЕРМІНОВАНИХ КРИПТОГРАФІЧНИХ ПЕРЕТВОРЕНЬ

Вінницький національний технічний університет

Анотація

В роботі представлено автомати, що реалізують псевдонедетерміновані криптографічні перетворення. На основі цих автоматів синтезовано структуру апаратних засобів. Реалізовано комп'ютерне моделювання роботи цих засобів та проведено їх швидкодії з деякими відомими апаратними засобами.

Ключові слова: криптографія, псевдонедетермінованість, автомат, спеціалізований процесор, операційний пристрій.

Abstract

Automatons, which implement pseudonondeterministic cryptographic transformations, are presented at the work. The structure of hardware tools was synthesized basing of these automatons. Computer modeling of these devices and their rapidity estimation comparatively to known ones were performed.

Key words: cryptography, pseudonondeterministic, automaton, specialized processor, operating device.

Вступ

Відкриття криптографічних перетворень для громадськості дозволяє користувачам переконуватись в їх коректності та стійкості. Водночас така відкритість криптографії дозволила криптоаналітикам розробити низку атак, що передбачають можливість попередньої підготовки до їх реалізації [1, 2]. Причому ця підготовка можлива ще до створення повідомлення, яке захищатиметься такими криптографічними засобами. Основною небезпекою цих атак є те, що при лінійному зростанні кількості ресурсів, що витрачаються на попередню підготовку, ймовірність успішного проведення цієї атаки зростає експоненційно [2]. Саме тому актуально розробити методи та засоби псевдонедетермінованої криптографії, які ускладнюватимуть зловмисникам реалізацію атак, зокрема таких, що передбачають можливість попередньої підготовки [1, 3, 4].

Метою даного дослідження є підвищення швидкості реалізації псевдонедетермінованих криптографічних перетворень за рахунок розробки операційних пристроїв спеціалізованих процесорів.

Для досягнення мети необхідно розв'язати такі задачі:

- формалізувати у вигляді автомата спеціалізований процесор для псевдонедетермінованих криптографічних перетворень;
- розробити структуру операційного пристрою спеціалізованого процесора;
- реалізувати дану структуру та провести комп'ютерне моделювання його роботи.

Операційні пристрої для псевдонедетермінованих криптографічних перетворень

Особливістю концепції псевдонедетермінованої криптографії є те, що методи криптографічних перетворень виглядають для зловмисника як такі, що виконуються за допомогою недетермінованого автомата [3]. Такого ефекту пропонується досягати за рахунок включення до моделі процесу криптографічного перетворення додаткового параметру, що залежить від ключа, а відтак невідомого зловмисникові. Для псевдонедетермінованого шифрування такий автомат формалізується так $\{\mathbf{D}, \mathbf{A}, \mathbf{F}, k, d_l, \mathbf{V}\}$, де $\mathbf{D}$ – множина шифротекстів, $\mathbf{A}$ – алфавіт автомата (для потокового шифрування зазвичай $\mathbf{A} = \{0; 1\}$), $\mathbf{F}$ – множина функцій, що реалізують криптографічне перетворення, $\mathbf{F} = \{f_{v_i}(\cdot)\}$; k – ключ (початковий стан генератора гами), d_l – останній блок шифротексту; $\mathbf{V}$ – множина векторів керування, що визначають вибір функції, що реалізує криптографічне перетворення. Аналогічним чином описується псевдонедетерміноване гешування $\{\mathbf{H}, \mathbf{M}, \mathbf{F}, k, h_l, \mathbf{V}\}$, де $\mathbf{H}$ – множина можливих проміжних геш-значень, $\mathbf{M}$ – множзина можливих блоків даних, h_l – проміжне геш-значення, отримане після обробки всіх вхідних даних (для більшості конструкцій – результат гешування) [3].

З аналізу наведеного вище опису автоматів випливає, що ключовим елементом для реалізації апаратних засобів псевдонедетермінованих криптографічних перетворень є операційний пристрій, що повинен бути здатним адаптуватися до виконання різних перетворень над різними наборами вхідних

даних.

Для реалізації описаних вище автоматів пропонується низка операційних пристроїв, узагальнена структура яких наведена на рис. 1.

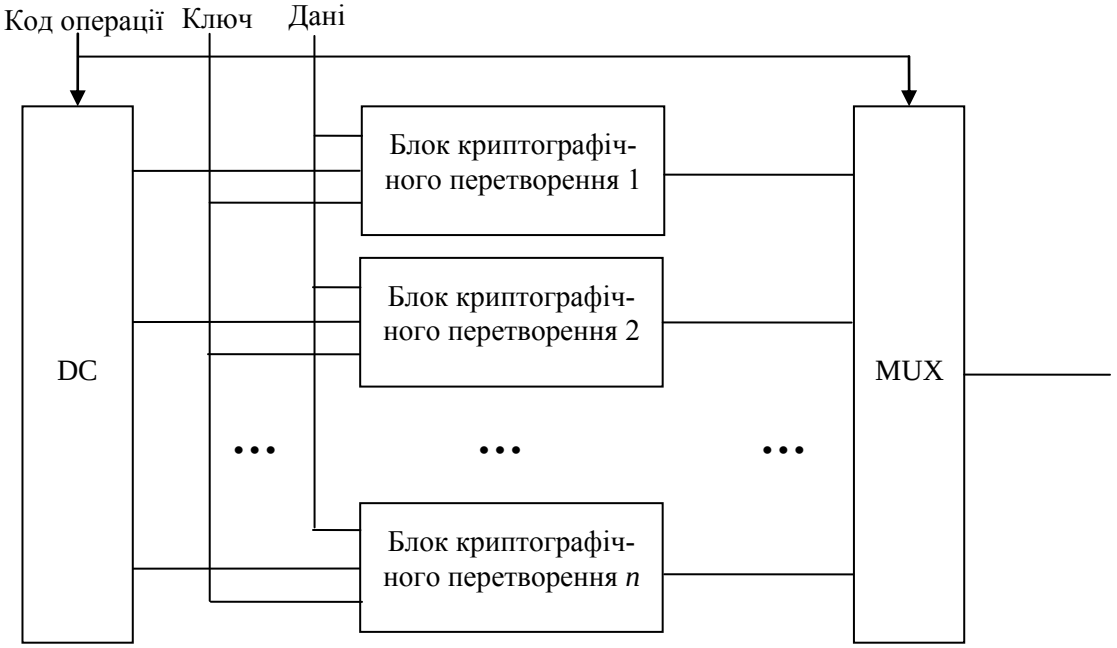

Рис. 1. Узагальнена структура операційного пристрою

Як видно з рис. 1 завдяки дешифратору та мультиплексору досягається керування виконуваною функцією $f_{v_i}(\cdot)$, обраної з множини **F**, що виконується за допомогою v_i-го блоку криптографічного перетворення.

Структури таких операційних пристроїв для псевдонедетермінованого гешування та потокового шифрування описано за допомогою мови VHDL та симульовано їх роботу за допомогою середовища ModelSim. З аналізу отриманих результатів моделювання випливає, що додаткові операції, пов'язані з генеруванням керуючих сигналів для дешифратора та мультиплексора, істотно не впливають на швидкодію пристрою порівняно з операційним пристроєм, що реалізує лише одне криптографічне перетворення [1, 6]. Це досягається завдяки розпаралеленню виконуваних операцій. Проте операційні пристрої псевдонедетермінованих криптографічних перетворень порівняно з такими операційними пристроями мають вищу апаратну складність. Однак при цьому досягається вища криптографічна стійкість перетворення.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Баришев Ю. В. Методи та засоби швидкого багатоканального гешування даних в комп'ютерних системах : монографія / Ю. В. Баришев, В. А. Лужецький; за заг. ред. В. А. Лужецького – Вінниця : ВНТУ, 2016. – 144с
2. Kelsey J. Herding hash functions and the Nostradamus attack / John Kelsey, Tadayoshi Kohno. – 2005. – 18 с. – Режим доступу до статті: http://archives.scovetta.com/pub/crypto/Nostradamus%20Attack.pdf
3. Luzhetsky V. The Generalized Construction of pseudonondeterministic hashing / Volodymyr Luzhetsky, Yurii Baryshev// Computing, – 2012 – Vol. 11. Issue 3 – P. 302-308.
4. Баришев Ю. Структури операційних пристроїв для реалізації псевдонедетермінованих криптографічних перетворень / Юрій Баришев // Матеріали Міжнародної науково-практичної конференції "Інформаційні технології та комп'ютерне моделювання", м. Івано-Франківськ, 23-28 травня 2016 року. – Івано-Франківськ: Супрун В. П., 2016 – С. 109-110.
5. Глушков В. М. Синтез цифровых автоматов / Виктор Михайлович Глушков. – М. : Физматгиз, 1962. – 476 с.
6. Криптографическое кодирование: методы и средства реализации : монография / [В. Н. Рудницкий и др]. – Тольятти: Тольят. гос. ун-т, 2013. – 196 с.

Юрій Володимирович Баришев – канд. техн. наук, доцент кафедри захисту інформації, Вінницький національний технічний університет, Вінниця

Yurii Baryshev – Cand. Sc. (Eng), Associate Professor of Information Protection Department, Vinnytsia National Technical University, Vinnytsia