Структури операційних пристроїв для реалізації псевдонедетермінованих криптографічних перетворень

Ю. В. Баришев
кафедра захисту інформації
Вінницький національний технічний університет
Вінниця, Україна
yuriy.baryshev@gmail.com

Operating Devices Structures for Pseudonondeterministic Cryptographic Transformations Implementation

Y. Baryshev
Department of Information Protection
Vinnytsia National Technical University
Vinnytsia, Ukraine
yuriy.baryshev@gmail.com

***Анотація*— Проаналізовано відомі підходи до розробки апаратних засобів криптографічного перетворення. Виділено ті з них, які можуть використовуватись як базові для реалізації псевдонедетермінованих криптографічних перетворень та наведено приклад такої реалізації.**

***Abstract*—Known cryptographic transformations hardware design approaches were analyzed. Those of them, which could be used as basic ones for the pseudonondeterministic cryptographic transformations implementation, were pointed out and an instance of the implementation was presented.**

Ключові слова—псевдонедетерміноване перетворення; операційний пристрій; керовані перетворення

Keywords—pseudonondeterministic transformation; operatind device; driven transformations

I. Вступ

Концепція відкритості криптографічних алгоритмів при закритих параметрах криптографічних перетворень (ключів) дозволяє дослідити науковій громаді досліджувати їх стійкість. Останнє сприяє науковим дискусіям, а відтак швидкості розвитку криптографії. Водночас, попри цю низку переваг така відкритість криптографічних перетворень дозволяє криптоаналітикам реалізовувати атаки, обумовлені власне такою відкритістю алгоритмів [1-3]. Таким чином постала проблема розробки криптографічних перетворень, які при збережені відкритості до досліджень закривали б від зловмисників спосіб криптографічних перетворень, які відбуваються над даними, що захищаються [4, 5], актуальність якої обумовлюється вищевикладеними суперечливими тенденціями. Рішенню цієї проблеми присвячені, зокрема, дані дослідження.

Метою даного дослідження є підвищення стійкості криптографічних перетворень до аналізу зловмисників шляхом реалізації псевдонедетермінованих криптографічних перетворень.

На шляху до досягнення даної мети необхідно розв’язати низку задач. Однією з цих задач є розробка спеціалізованих криптографічних апаратних засобів. Розв’язанню якої присвячено дану роботу.

II. Структури операційних пристроїв

Відома низка робіт присвячених розробці апаратних засобів для реалізації криптографічних перетворень, що створюють для зловмисника невизначеність в параметрах операцій, що виконуються [6-9].

В роботі [6] пропонується структура уніфікованого пристрою криптографічних перетворень, який реалізує

низку перетворень, вибір яких залежить від вектора керування. Таким чином, для зловмисника, якому невідомий вектор керування, утворюється невизначеність у виконуваному перетворені. У роботі [7] наводяться спеціалізовані пристрої для керованих криптографічних перетворень на основі керованих перестановок.

Апаратні засоби та структура спеціалізованого процесора для багатоканального керованого гешування, розглянуті в роботах [8, 9], базуються на логічних функціях, аналогічних використаним у SHA-2, та керовані зсуви аргументів цих функцій. На рис. 1 наведено приклад такої структури.

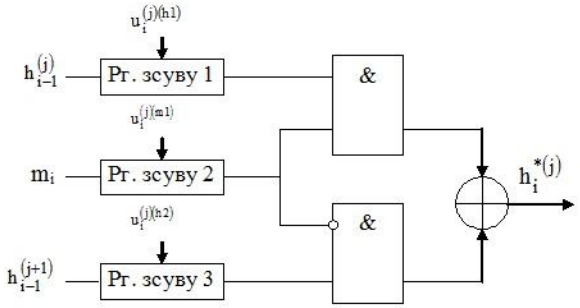

Рис. 1. Структура операційного пристрою на основі логічної функції та регістрів зсуву

Загальним недоліком даних засобів та підходів, що лежать в їх основі є те, що попри певну невизначеність у виконуваних перетвореннях, зловмиснику залишаються відомими кількість та черговість цих перетворень, а також дані, над якими ці перетворення виконувались. У роботі [4] запропоновано моделі псевдонедетермінованих криптографічних перетворень, які дозволяють усунути зазначені недоліки.

Для реалізації моделей псевдонедетермінованих перетворень пропонується удосконалити підхід, використаний в роботах [8, 9] з урахуванням утворення невизначеності зловмисника у даних, що обробляються на певній ітерації. На рис. 2 наведено структуру такого операційного пристрою. Його перевагою над структурою, зображено на рис. 1 є можливість адаптуватися до вхідних даних різної розмірності. Блок комутації й ущільнення в операційному пристрої дозволяє ущільнити дані до допустимих в логічних блоках, з'єднані з його виходами.

Висновки

В даній роботі визначено актуальність реалізації псевдонедетермінованих криптографічних примітивів. На основі відомих структур криптографічних пристроїв запропоновано структуру операційного пристрою, який може використовуватись в структурі спеціалізованого процесора.

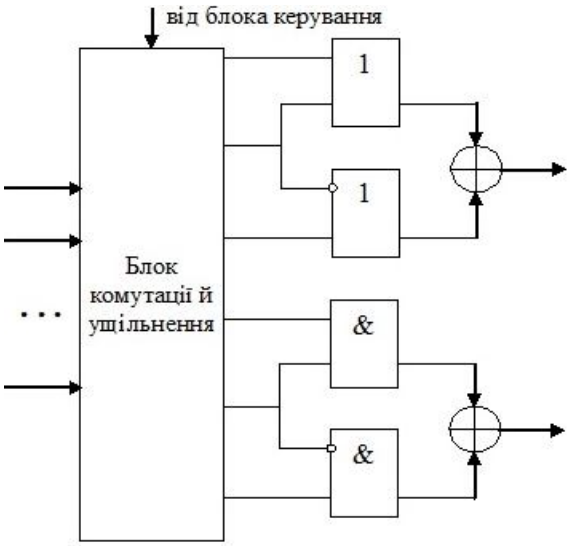

Рис. 2. Приклад структури операційного пристрою для псевдонедетермінованого перетворення

Недоліком запропонованої структури є її апаратна надлишковість порівняно з аналогами. Проте даний недолік компенсується за рахунок можливості його використання для реалізації декількох різних криптографічних перетворень, наприклад симетричного блокового шифрування та гешування.

Література References

[1] C. Blondeau, G. Leander, K. Nyberg. Differential-Linear Cryptanalysis Revisited, 2014, p. 20, http://users.ics.aalto.fi/~blondeau/PDF/FSE2014.pdf

[2] J.Kelsey, T. Kohno. Herding hash functions and the Nostradamus attack, 2005, p. 18. http://archives.scovetta.com/pub/crypto/Nostradamus%20Attack.pdf

[3] J. J.Hoch, A. Shamir Breaking the ICE – Finding Multicollisions in Iterative Concatenated and Expanded (ICE) Hash Functions, 2006, p. 13. http://www.wisdom.weizmann.ac.il/~yaakovh/papers/hashpaper_submission.pdf

[4] Ю. В. Баришев. Моделі псевдонедетермінованих криптографічних перетворень. "Інформаційні технологій та комп'ютерна інженерія"; матеріали статей п'ятої міжнародної науково-практичної конференції, м. Івано-Франківськ, 27-29 травня 2015 року, Івано-Франківськ: Супрун В. П., 2015, С.189-191.

[5] В. А. Лужецький, Ю. В. Баришев. Концепція псевдонедетермінованого гешування. Системи управління, навігації та зв'язку, 3, 2010, С. 94-98.

[6] В. М. Рудницький, В. Г. Бабенко. Модель уніфікованого пристрою криптографічного перетворення інформації Системи обробки інформації, 3, 2009, С. 91-95.

[7] Н.А. Молдовян, А.А. Молдовян, М.А. Еремеев. Криптография: от примитивов к синтезу алгоритмов, СПб.: Питер, 2004, 448 с.

[8] В. А. Лужецький, Ю. В. Баришев Апаратні засоби для реалізації багатоканального керованого хешування. Системи обробки інформації, 3, 2011, С. 130-133.

[9] Ю. В. Баришев. Структура спеціалізованого криптографічного процесора для керованого хешування. Сучасні проблеми радіоелектроніки, телекомунікацій та приладобудування (СПРТП-2011): матеріали V Міжнародної науково-технічної конференції, м. Вінниця, 19-21 травня 2011 р., Вінниця: ВНТУ, 2011 С. 169-170.