УДК 004.056.55

В. Р. Караван

МЕТОД ПСЕВДОНЕДЕТЕРМІНОВАНОГО ШИФРУВАННЯ

Вінницький національний технічний університет

Анотація

Проаналізовано відомі потокові шифри, щодо можливості їх використання в малоресурсній криптографії. Запропоновано метод потокового шифрування, алгоритм якого відкритий для користувачів, але його конкретна реалізація буде захищена від зламу зловмисником.

Ключові слова: шифрування, потокові шифри, псевдовипадковий, криптографія, алгоритм, генератор.

Abstract

The analysis of known stream ciphers was performed for the possibility of their usage at the field of minimum hardware cryptography. The method of stream ciphering algorithm which is open for users, but is certain implementation would be infeasible for intruder breaking.

Keywords: ciphering, stream ciphers, pseudorandom, cryptography, algorithm, generator.

Вступ

Більшість сучасних потокових шифрів так чи інакше були розкриті зловмисниками. На початку розвитку потокових шифрів їх алгоритми були закриті для дослідження, що в свою чергу забезпечувало певний захист [1, 2]. Але обставини ринкової економіки породили необхідність у розкритті алгоритмів. При цьому стійкість шифру визначається складністю підбору ключа. Тому актуально розробити такий шифр, алгоритм якого буде відкритий для користувачів задля доведення його стійкості, але його конкретна реалізація буде захищена від зламу зловмисником.

Метою дослідження є підвищення стійкості потокових шифрів.

Для її досягнення необхідно:

- проаналізувати відомі потокові шифри;
- розробити підхід до реалізації ідеї;
- розробити структуру пристрою, що реалізує підхід.

Аналіз потокових шифрів

Найбільш відомими потоковими шифрами є A5, ORYX, PIKE, RC4 та SEAL [1, 2]. Шифр A5 використовується в системі мобільного цифрового зв'язку GSM для забезпечення конфіденційності даних між телефоном і базовою станцією. Шифр заснований на побітовому додаванні за модулем два, що генерується псевдовипадковою послідовністю. У A5 псевдовипадкова послідовність генерується на основі трьох лінійних регістрів зсуву зі зворотним зв'язком. Регістри мають довжини 19, 22 і 23 біти відповідно [3]. Зсувами керує спеціальна схема, яка організовує на кожному кроці зміщення як мінімум двох регістрів, що призводить до їх нерівномірного руху. У склад генератора ORYX входять три 32-розрядні LFSR, а також 8-розрядний S-блок з фіксованою таблицею замін розмірністю 8 x 256. Ключем є початкове заповнення трьох регістрів LFSR. Іноді застосовується алгоритм розгортання ключа, що скорочує ключовий простір до розміру, який легко перевіряється при пошуку ключа повним перебором. PIKE – це модифікація зламаного шифру FISH. Алгоритм використовує три адитивних генератора. Керування синхронізацією здійснюється на основі аналізу бітів переносу cro_1, cro_2, cro_3 на виходах суматорів. RC4 – потоковий шифр зі змінним розміром ключа. В алгоритмі використовується два 8-розрядних лічильника Q_1 та Q_2 і 8-розрядний блок заміни (S-блок). Таблиця замін має розмірність 8 x 256 і є перестановкою двійкових чисел від 0 до 255. SEAL – це симетричний потоковий алгоритм шифрування даних, що оптимізований для програмної реалізації. Для роботи йому потрібно кеш-пам'ять на кілька кілобайт і вісім 32-бітових регістрів. Швидкість шифрування – приблизно 4 машинних такти на байт тексту [1].

Як видно з результатів аналізу, всі відомі потокові шифри мають відкритий алгоритм. Така відкритість дозволяє проводити зловмиснику криптоаналіз цих шифрів. Відповідно актуально розробити новий шифр, який усуне вищезазначений недолік.

Метод та засіб псевдонедетермінованого потокового шифрування

Ідея шифру полягає у реалізації концепції псевдонедетермінованої криптографії в процесі розробки потокового шифру [4, 5]. Зокрема це втілиться у використанні різних операцій для накладання гами для кожного біта вхідних даних. Запропонований метод реалізований на базі п'яти регістрів зсуву з лінійним зворотнім зв'язком. Виходи РЗЛЗЗ 1 і 2 є входами РЗЛЗЗ 3 і 4, перша пара задає кількість зсувів, а інша – формує можливі гами. РЗЛЗЗ 5 керує входами мультиплексора MUX 1, на які надходять виходи РЗЛЗЗ 3 та 4. За допомогою демультиплексора DMUX відбувається накладання обраної гами з даними, використовуючи операційні пристрої, де ОП 1 – це XOR, а ОП 2 – інверсний XOR. Після цього інформація потрапляє до мультиплексора MUX 2, виходом якого є послідовність зашифрованих бітів. Структуру пристрою, що реалізує даний підхід наведено на рисунку 1.

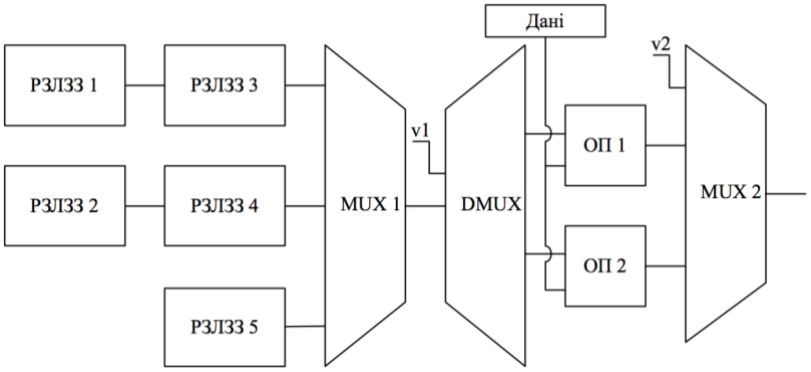

Рисунок 1 – Схема пристрою

Стійкість запропонованого методу полягає у тому, що зловмисник не може дослідити характер гами, а також не знає, яка з вбудованих операцій була виконана.

Висновки

Алгоритми відомих потокових шифрів були закритими для дослідження, що забезпечувало стійкість перед зловмисниками, але після їх розкриття задача зламу суттєво спростилася. Для збільшення стійкості при збереженні відкритості алгоритму пропонується використовувати псевдонедетермінований підхід. Але зі збільшенням стійкості зростає також і апаратна складність реалізації алгоритму, в порівнянні з вже відомими рішеннями. Модифікація схеми Геффа відповідно до цього підходу показала його перспективність. В подальших дослідженнях планується розробка шифрів на основі інших генераторів гами та їх порівняльний аналіз.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Петров А.А. Компьютерная безопасность / Петров А.А. – Москва: Лайт Лтд., 2000 – 448 с.

2. Шнайер Брюс. Прикладная криптография. Протоколы, алгоритмы и исходные тексты на языке С. 2-е издание. / Брюс Шнайер – М.: Дело, 2003 – 610 с.

3. Поточные шифры / [Мирский А.А. и др.] – Москва: Кудиц-Образ, 2003 – 330 с.

4. Luzhetsky V. The Generalized Construction of pseudonondeterministic hashing / Volodymyr Luzhetsky, Yurii Baryshev // Computing. – Vol. 11 (Issue 3). – 2012. – p. 302-308.

5. Лужецький В. А. Концепція псевдонедетермінованого хешування / В. А. Лужецький, Ю. В. Баришев // Системи управління, навігації та зв'язку. – №3. – 2010. – С. 94-98.

Караван Владислав Русланович — студент, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця, email: vlad30.96.12@gmail.com

Науковий керівник: ***Баришев Юрій Володимирович*** — к. т. н., доцент кафедри захисту інформації, Вінницький національний технічний університет, email: yuriy.baryshev@gmail.com

Karavan Vladislav — student, Faculty of Information Technology and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, email: vlad30.96.12@gmail.com

Supervisor: ***Baryshev Yurii*** — Cand. Sc. (Eng), Associated Professor of Information Protection Chair, Vinnytsia National Technical University, Khmelnytske shosse 95, Vinnytsia, Ukraine, yuriy.baryshev@gmail.com