УДК 621.326

Дмитро Іваненко, к.т.н., доцент, Аліна Андрушкевич
Харківський національний університет радіоелектроніки

МАТЕМАТИЧНІ МОДЕЛІ СУЧАСНИХ ПОТОЧНИХ ШИФРІВ

Дана робота присвячена аналізу сучасних потокових шифрів, а також методиці оцінювання поточних шифрів за наступними критеріями: шифрування довгих повідомлень, шифрування коротких повідомлень, ініціалізація / генерація ключових параметрів.
Ключові слова: криптографія, потоковий шифр, швидкісні показники, тестування

Dmytro Ivanenko, Alina Andrushkevych

THE MATHEMATICAL MODELS OF MODERNSTREAM CIPHERS

This paper devoted to the analysis of modern stream ciphers and methods of evaluation of stream ciphers on the following criteria: encrypting long messages, encrypting short messages, initialization / key generation parameters.
Key words: cryptography, stream cipher, high-speed performance, testing

Невід'ємною частиною сучасних телекомунікаційних систем є нескінчений потік, послідовність яка гіпотетично може бути нескінченої довжини. Важливою вимогою подібних систем є висока швидкість шифрування, яка може бути забезпечена тільки при застосуванні поточних шифрів.

На сьогодні поточний шифр європейського стандарту повинен відповідати досить високим показникам – сотні Мбіт/с та навіть декілька Гбіт/с, якщо дивитись у майбутнє та робити запас на декілька десятиліть. Ефективне рішення, крім високої продуктивності, повинно мати обґрунтованість, доказану надійність, простоту та масштабованість, завершеність та ясність алгоритму, забезпечувати конфіденційність у каналах передачі інформації.

Розглянемо всесвітньовідомі криптоалгоритми, які стандартизовані на міжнародному або національному рівні, які на сьогоднішній день мають найбільшу довіру та розповсюдження. Розглянемо методику дослідження характеристик поточних шифрів.

Потоковий симетричний шифр «SNOW 2.0» є генератором ключових потоків, який використовує як вхідні дані 128 або 256-бітовий секретний ключ K_i 128-бітовий вектор ініціалізації *IV*. Шифр є слово-орієнтованим. Алгоритм було стандартизовано у ISO/IEC 18033-4 [1]. Максимально рекомендована кількість біт ключового потоку, виробленого на одній парі (*K, IV*) дорівнює $23*2^{50}$ біт. Це обмеження виправдане з точки зору забезпечення стійкості алгоритму проти криптоаналітичних атак.

Потоковий шифр «Струмок» [2] являє собою класичну схема підсумовуючого генератора. Криптоалгоритм орієнтований на 64-розрядні обчислювальні системи, і, відповідно, розмір слова в шифрі визначено рівним 64 бітам. В якості вхідних даних використовується 512 (або 1024)-бітний секретний ключ *K* та 512-бітний вектор ініціалізації *IV*. Шифр за своєю структурою подібний до алгоритму «SNOW 2.0».

Потоковий симетричний шифр «Sosemanuk» – це синхронний програмно-орієнтований потоковий шифр, який відповідає першому профілю конкурсу eECRYPT [3]. Його довжина ключа може бути обрана між 128 і 256 бітами. Шифр працює з 128 бітовим початковим значенням, при цьому, як стверджується розробниками алгоритму, будь-яка довжина ключа досягає 128-бітного захисту.

Алгоритм Sosemanuk використовує деякі основні принципи потокового шифру «SNOW 2.0» і деякі перетворення, отримані з блокового шифру SERPENT.

Потоковий симетричний шифр «Trivium» – це симетричний апаратно-орієнтований паралельний потоковий шифр проекту eSTREAM (другий профіль) [3], що призначений для генерації 2^{64} біт ключового потоку з 80 біт секретного ключа і 80 біт вектору ініціалізації. Шифр є біт-орієнтованим.

Потоковий симетричний шифр «Enocoro» –апаратно-орієнтований криптоалгорим [4] (також має і ефективну програмну реалізацію), що є байт-орієнтований шифром із довжиною ключа 128 біти та вектору ініціалізації 64 біти.

Потоковий симетричний шифр «HC-256» – простий, безпечний, програмно-орієнтований шифр [3] з ефективною реалізацією і може вільно використовуватися. Для ініціалізації використовується 256-бітний ключ та вектор ініціалізації довжиною 256 біт. Рекомендована максимальна довжина ключової послідовності – 2^{128}.

Потоковий симетричний шифр «Grain» – симетричний алгоритм синхронного поточного шифрування [3], який орієнтований на використання на обчислювальних машинах з обмеженою кількістю вентилів (gate), невеликими потужністю та обсягом пам'яті. В залежності від апаратної реалізації шифр Grain може бути біт-орієнтованим або слово-орієнтованим. В Grain v1 на вхід подається ключ довжиною 80 біт та вектор ініціалізації довжиною 64 біти. В основі конструкції алгоритму лежать 2 регістри зсуву – з лінійним та нелінійним зворотним зв'язком та вихідна функція. Рекомендована довжина ключового потоку, який може бути вироблено на одній парі ключ/вектор – 2^{44} біт.

Потоковий симетричний шифр «Mickey» – апаратно-орієнтований шифр [3]. Для ініціалізації початкового стану використовуються ключ довжиною 80 біт та вектор ініціалізації довжиною до 80 біт. Максимально можлива довжина ключового потоку дорівнює 2^{40} біт на одному ключі, але з використанням різних векторів ініціалізації одної довжини. Завдяки використанню нерегулярного руху регістрів зсуву, а також нових методів, забезпечується висока стійкість до певних криптоаналітичних атак.

Потоковий симетричний шифр «MUGI» – генератор ключових потоків, який було стандартизовано у ISO/IEC 18033-4 [1]. Шифр MUGI э слово-орієнтованим.У якості початкових даних MUGI використовує 128-бітовий секретний ключ, 128-бітовий вектор ініціалізації. MUGI використовує нелінійні блоки підстановки та лінійні трансформації з використанням MDS матриці алгоритму AES. Основні конструкції шифру подібні до конструкцій шифру Panama.

Потоковий симетричний шифр «Rabbit» – програмно-орієнтовний алгоритм, що був представлений на конкурсі eSTREAM [3]. Алгоритм використовує 128-бітний ключ і 64-бітний вектор ініціалізації. На одній парі ключ/вектор може бути вироблено до 2^{67} бітів ключового потоку.

Потоковий симетричний шифр «Salsa 20» [3] – програмно-орієнтовний алгоритм, що був переможцем на конкурсі eSTREAM в першому профілі. Для ініціалізації внутрішнього стану використовується ключ довжиною 256 біт, 64-бітний nonce та 64-бітна позиція блоку ключового потоку. Максимальна довжина псевдовипадкової ключової послідовності дорівнює 2^{70} біт.

Блоковий симетричний шифр «AES», який стандартизовано уа міжнародному рівні стандартизовано у ISO/IEC 18033-3 [5]. Використовує ключ довжиною 128, 192 або 256 біт. В залежності від довжини ключа відбувається 10, 12 або 14 раундів шифрування. AES базується на принципі, відомому як мережа замін-перестановок та, завдяки цьому, має швидку апаратну та програмну реалізацію. У режимі зворотного зв'язку за виходом цей шифр можна використовувати як потоковий.

Критерієм вибору поточного шифру є зазвичай показники швидкості зашифрування довгих послідовностей та часу ініціалізації/генерації ключових параметрів. У цій роботі була розглянута методика з міжнародного конкурсу eSTREAM. За цією методикою поточні шифри порівнюються за наступними критеріями:

– Критерій зашифрування довгих потоків, поточні шифри мають найбільш потенційну перевагу над блочними шифрами при зашифруванні довгих потоків. Тому цей показник є важливим критерієм оцінки. У досліджені вимірювався час зашифрування 1Гб даних.

– Критерій зашифрування коротких потоків, цей показник відображає швидкість зашифрування пакетів різної довжини. Кожен виклик функції включає до себе окрему установку вектору ініціалізації (IV), довжина пакетів (40, 576, и 1500 байт) були обрана так, щоб були репрезентивними для телекомунікаційного трафіку. У досліджені вимірювався час зашифрування пакету, швидкість зашифрування байт на мікросекунду та швидкість зашифрування пакетів на мікросекунду.

– Критерій ініціалізації/генерація ключових параметрів. Окремо відображає ефективність встановлення ключа та вектору ініціалізації. Ці два параметра найменш критичні для відображення швидкості зашифрування пакетів так як зневажливо малі порівнюючи з процесом створення та відновлення ключа. . При дослідження поточних шифрів були взяті наступні дані: для ключа – 7000 ключових установок (10 ключів на 700 установок на ключ), для вектору ініціалізації – 500 ключових установок (10 ключів на 50 установок); для цих параметрів було зафіксовано загальний час виконання операцій, скільки затрачено циклів на установку та скільки можливо зробити установок за секунду.

Література

1. ISO/IEC 18033-4:2011. Information technology – Security techniques – Encryption algorithms – Part 4: Stream ciphers. [Електронний ресурс]. – Режим доступу: http://www.iso.org/iso/home/store/catalogue_ics/catalogue_detail_ics. htm?csnumber=54532

2. Кузнецов О.О., Іваненко Д.В., Белозерцев І.М., Андрушкевич А.В. Алгоритм потокового криптоперетворення «Струмок» // Труды научно-технической конференции с международным участием «Компьютерное моделирование в наукоемких технологиях», 26-31 мая 2016 г. – Х.: ХНУ имени В.Н. Каразина – 2016. – С. 187-190.

3. The eSTREAM Project - eSTREAM: the ECRYPT Stream Cipher Project. [Електронний ресурс]. – Режим доступу: http://www.ecrypt.eu.org/stream/

4. ISO/IEC 29192-3:2012. Information technology – Security techniques – Lightweight cryptography – Part 3: Stream ciphers. [Електронний ресурс]. – Режим доступу: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail. htm?csnumber=56426

5. Information technology – Security techniques – Encryption algorithms, Part 3: Block ciphers (ISO/IEC 18033-3) - 80 p.