АНАЛИЗ НА ХАРАКТЕРИСТИКИТЕ НА СЪВРЕМЕННИ ПОТОЧНИ ШИФРИ

ANALYSIS OF THE CHARACTERISTICS OF CONTEMPORARY STREAM CIPHERS

Антония Ташева, Огнян Наков
Технически Университет – София, България

Abstract

The restrictions in development of new stream ciphers during the project eSTREAM and the published finalists with software realization are examined. A comparison analysis of their characteristics is made and conclusions for the contemporary trends of designing new fast, secure and effective stream ciphers are drawn.

Keywords: Stream Ciphers; Cryptography; Cryptoanalysis; LFSR; NLFSR; eSTREAM.

ВЪВЕДЕНИЕ

Шифрирането на информация се е превърнало в необходимост и неизменна част от съвременната комуникация. Въпреки това в последните години поточните шифри остават незаслужено на заден план.

Поточните шифри имат неоспорими предимства в определени ситуации и именно това е причината през 2004 година да се даде старт на програмата „ECRYPT Framework VI Network of Excellence“, финансирана от Европейския съюз, която има своето продължение в „ECRYPT II“ през 2008 година [1, 6]. Тя цели създаване и сертифициране на нови поточни шифри, както с научна цел, така и за директно приложение в бизнеса и индустрията.

По проекта са предадени множество предложения, като само 16 от тях са определени за финалисти [1]. Поставените критерии за избор описват съвременните изисквания за сигурност, устойчивост и бързодействие на поточните шифри. Именно те ще бъдат разгледани в настоящия доклад, за да бъдат направени изводи за актуалните спецификации и нужди в дадената проблемна област.

Статията е структурирана по следния начин. Първо са представени условията при разработка на нови поточни шифри в проекта eSTREAM и публикуваните софтуерни финалисти. Следва сравнителен анализ на техните характеристики, в резултат на който са направени изводи за съвременните тенденции при проектирането на бързи, сигурни и ефективни поточни шифри.

ПРОЕКТЪТ ESTREAM

Два са основните клонове за реализация на поточните шифри - софтуерен и хардуерен. Неоспоримо предимство за поточното криптиране спрямо блоковото такова и в двата клона съответно е възможността за изграждане на високопроизводителни системи в софтуера и хардуерни модули с изключително ограничени ресурси.

eSTREAM специфицира два основни профила на поточните шифри [6]:

- Профил 1: Поточни шифри със софтуерно приложение с високо бързодействие.
- Профил 2: Поточни шифри с хардуерно приложение за работа с ограничени ресурси.

Всеки от тях може да съществува и във вариант с асоцииран метод за автентификация (Профил 1A и Профил 2A).

В таблица 1 са дадени изискванията за дължината на ключа Key и на инициализиращия вектор IV (Initial Vector). Целта е предложените алгоритми да постигнат 128 битова сигурност на криптиране при софтуерната си реализация.

Таблица 1. *Изисквания за изходни параметри на шифъра* [1]

	Key, bits	**IV, bits**
Профил 1	128	64 или 128
Профил 1A	128	64 или 128
Профил 2	80	32 или 64
Профил 2A	80	32 или 64

Критериите за оценка поставени от проекта eSTREAM са следните [6]:

- сигурност;
- производителност спрямо AES (Advanced Encryption Standard);
- производителност спрямо другите шифри;
- обосновка и съпътстващ анализ;
- простота и гъвкавост;
- завършеност и яснота.

Тези критерии могат да служат като отправна точка при конструирането на нови поточни шифри, защото горните изисквания са поставени като необходим минимум за нуждите на европейската общност.

След няколко годишно изследване и развитие от предложените 34 алгоритъма са избрани по 6 финалиста във всеки от двата профила. Имената им са изброени в таблица 2.

Таблица 2. *Финалисти в eSTREAM*

Профил 1	**Профил 2**
CryptMT v3	DECIM v2
DRAGON	Edon-80
HC-128	F-FCSR-H
LEX	Grain v1
NLS v2	MICKEY v2
Rabbit	MOUSTIQUE
Salsa20	POMARANCH v3
SOSEMANUK	Trivium

ШИФРИ СЪС СОФТУЕРНА РЕАЛИЗАЦИЯ

В статията е направен сравнителен анализ на избраните за финалисти софтуерни поточни шифри, въз основа на което могат да се систематизират предложените по-долу тенденции и характеристики на съвременните поточни шифри със софтуерна реализация.

Размерност на шифрите

Всички финалисти предоставят алгоритъм, приемащ като изходни параметри ключ и инициализиращ вектор с дължина, зададена в предварителните изисквания, като само някои от тях залагат на променливата им дължина (CryptMT v3 [11], DRAGON [4] и SOSEMANUK [5]) и постигането на по-универсален и разширяем алгоритъм. В таблица 3 са систематизирани входно-изходните количествени характеристики на шифрите от Профил 1.

Таблица 3. *Входно-изходни характеристики*

Шифър	**Key, bit**	**IV, bit**	**Изх. блок**
CryptMT v3	от 128 до 2048	от 128 до 2048	32
DRAGON	128 или 256	128 или 256	64
HC-128	128	128	32
LEX	128	128	4 x 32
NLS v2	128		32
Rabbit	128	64	128
Salsa20	256	64	512
SOSEMA-NUK	128 или 256	128	32

Всеки един от предложените алгоритми представлява цикъл от операции, след или по време на който на изхода се извежда блок от битове. В зависимост от спецификата на алгоритъма той варира по големина от 32 до 512 бита.

Големината на тези изходни блокове е тясно свързана с характерните особености на архитектурата на съвременните компютри, като не случайно се цели съответствие с големината на техните регистри и аритметично логическо

устройство за постигане на по-голямо бързодействие, което е и основната цел на шифрите от Профил 1.

Архитектура на шифрите

При изследване на структурата на предложените поточни шифри се забелязва тенденцията за широкото приложение на линейните LFSR (Linear Feedback Shift Register) и нелинейните NLFSR (Non Linear Feedback Shift Register) преместващи регистри с обратни връзки. Те са се доказали като отлични генератори на псевдослучайни числа и са в основата на четири от финалните осем шифъра (CryptMT v3, DRAGON, NLS v2 [1] и SOSEMANUK). Всеки един от тях използва в една или друга форма преместващ регистър с обратни връзки и филтър с памет. Паметта е необходима, за да се реализира нелинейна функционална зависимост между вътрешното състояние на регистъра и изхода на шифъра. Това цели постигане на устойчивост на някои видове атаки, които ще бъдат описани в следващата точка.

Известен недостатък на използването на LFSR в поточните шифри е наличието на повторяемост на изхода. Във връзка с това периодите на четирите шифъра са показани в таблица 4. По тази характеристика шифърът CryptMT v3 има очевидно превъзходство, но и останалите са намерили решение, чрез периодична смяна на ключа и/или на инициализиращия вектор.

Таблица 4. *Период на шифри с LFSR и NLFSR*

Шифър	Период
CryptMT v3	$\geq 2^{19937} - 1$
DRAGON	2^{576} думи
NLS v2	$\geq 2^{80}$
SOSEMANUK	максимум $2^{320} - 1$

От останалите финалисти два от алгоритмите ползват единствено циклично обновяваща се памет. Шифърът HC-128 [7] използва 2 секретни таблици, всяка с по 512 32 битови елемента, общо 4 KB памет, в която периодично обновява и извежда елементи чрез нелинейни функции. Другият алгоритъм – Rabbit използва 513 бита памет, разделена между 8 променливи, 8 брояча и един бит за пренос. Алгоритмът извършва редица от операции и преобразувания и аналогично част от вътрешното състояние се извежда на изхода.

При тези два шифъра също се наблюдава повторяемост на изходния поток, като при Rabbit [3] цикъл се получава при $2^{256} - 1$, а при HC-128 неговата дължина е средно над 2^{256}.

Интересно решение е предложено от авторите на семейството шифри Salsa20 [10], които използват единствено дълга поредица от три прости операции, събиране по модул 2^{32}, XOR на 32-битови числа и ротация. Шифърът съществува във варианти с различен брой етапи в алгоритъма. Колкото повече са те – толкова по-бавен става алгоритъма, но пък увеличава своята сигурност. Така например за шифрите от това семейство с 5 и 6 етапа Salsa20/5 и Salsa20/6 са разбити.

Последният от финалистите LEX [2] дава интересна интерпретация на блоковия шифър AES като поточен. Предложеният алгоритъм се състои от 4 AES кръга, при всеки от които се извеждат 4 байта от междинното състояние. Тук се наблюдава цикъл на изходния поток при 2^{128}.

КРИПТОАНАЛИЗ

За да се определи един алгоритъм като успешен шифър, той трябва да е устойчив на всички видове атаки срещу секретните ключовете и потока данни. Съществуват множество видове познати и общо приложими атаки, както и индивидуални, които се съставят в зависимост от спецификата на конкретния шифър.

Предложените осем поточни шифъра са изследвани спрямо редица атаки и въз основа на това могат да се определят различни подходи за преодоляването на тези евентуални дупки в сигурността. За неприложима се счита една атака, когато сложността ѝ е по голяма от тази на пълното изчерпване.

Всеки един от алгоритмите се подлага на *статистически анализ*, където посредством стандартизирани инструменти

на NIST [8] и DIEHARD [9] се изследват различни характеристики на изходния поток.

Алгебричната атака (Algebraic Attack) е избегната като при седем от осемте шифъра се избира нелинейна функция за обновяване на състоянията. Това осигурява голям брой неизвестни и невъзможност за бързо решаване на системата от уравнения за определяне на ключа и вътрешното състояние. При шифъра LEX, който по своята същност коренно се различава от останалите, алгебричната атака се избягва чрез смяна на ключа на всеки 500 шифъра.

Поточните шифри с LFSR в състава си могат да бъдат подложени на успешна *корелационна атака* (Correlation Attack). Тя цели намирането на зависимости между входните и изходните битове на шифъра. Аналогично на алгебричната, корелационната атака може да бъде избегната чрез правилен избор на нелинейна функция за обновяване на състоянието, както при HC-128, Rabbit и CryptMT v3.

Друга атака, за която е необходимо да се изследват шифрите, е т.нар. *атака чрез различаване* (Distinguishing Attack). Тя се състои в това шифрираният поток да бъде сравнен и разграничен от случаен такъв. Тази атака не е успешна за нито един от финалистите в eSTREAM, като за CryptMT v3 тя е със сложност $O(2^{19937x2})$. При DRAGON тя е по-голяма от тази на пълното изчерпване. При HC-128 са необходими поне 2^{128} изхода. За NLS v1 е установено, че е неустойчив на тази атака, което налага допълнителна промяна в една променлива и в следващия си вариант NLS v2 атаката чрез различаване има сложност $O(2^{74})$. Шифърът SOSEMANUK е устойчив на тази атака благодарение на избора на Serpent1 в своя алгоритъм.

Съществуват и *атаки със съпоставка на време, памет и данни* (Time-Memory-Data Tradeoff Attacks). Те изследват взаимовръзката между необходимото време, памет и обем данни за разбиване на един шифър. Атаката се счита за успешна, когато се намери вариант, при който и трите гореспоменати параметъра имат стойности в рамките на разумното и постижимото.

Например при шифъра DRAGON е възможно предварително да бъдат изчислени изходите при различни ключове и състояния, които след това да бъдат запаметени в таблица. Така за шифъра Dragon-256 за време $T = 2^{256}$ и ограничение на максималната дължина на потока от 2^{64} бита, се определя долна граница на необходимата памет от 2^{896} бита. Установената сложност на CryptMT v3 за тази атака пък е $O(2^{10048})$. Три от изброените шифри (HC-128, LEX, SOSEMANUK) преодоляват атаката благодарение на големия обем на вътрешното си състояние.

Друг вид атаки, които са приложими към поточните шифри, са от типа *атака „предположи и определи“* (Guess and Determine Attack). За шифрите NLS v2 и SOSEMANUK те са изчислени съответно на 2^{256} и 2^{226}. При DRAGON и Rabbit те се определят като по-бавни от метода на грубата сила и съответно неприложими.

ЗАКЛЮЧЕНИЕ

Разгледаните поточни шифри за софтуерно приложение дават ясна представа за нуждите в съвременната криптография. Търсената минимална 128 битова сигурност би била полезна при необходимост от проектиране на бързи и ефективни софтуерни решения. Други две допълнителни изисквания, които се предявяват към съвременните бързи поточни шифри, са: необходимостта да имат добри статистически характеристики и да са устойчиви на всички видове познати атаки.

От направения сравнителен анализ може да се направи изводът, че основна тенденция в развитието на съвременните поточни шифри е реализирането им на базата на LFSR в комбинация с нелинеен филтър или функция за обновяване на състоянията. Това позволява да се постигне простота, икономичност и бързодействие на реализацията, от една страна, а от друга – необходимата сигурност на приложението.

ЛИТЕРАТУРА

[1] Babbage St., The eSTREAM Portfolio, April 15, 2008, http://www.ecrypt.eu.org/stream/portfolio.pdf.

[2] Biryukov Al., The Design of a Stream Cipher LEX, Selected Areas in Cryptography, Selected Areas in Cryptography, Lecture Notes in Computer Science, SpringerLink 2007, Volume 4356/2007, 67-75.

[3] Boesgaard M., Mette Vesterager and Erik Zenner, The Rabbit Stream Cipher, New Stream Cipher Designs, Lecture Notes in Computer Science, 2008, Volume 4986/2008, 69-83.

[4] Chen K. et al, Dragon: A Fast Word Based Stream Cipher, Information Security and Cryptology – ICISC 2004, Lecture Notes in Computer Science, SpringerLink 2005, Volume 3506/2005, 105-143.

[5] Cho J. Y. and Miia Hermelin, Improved Linear Cryptanalysis of SOSEMANUK, Information, Security and Cryptology – ICISC 2009, Lecture Notes in Computer Science, 2010, Volume 5984/2010, 101-117.

[6] ECRYPT. The eSTREAM project, http://www.ecrypt.eu.org/stream/

[7] Maitra S. et al, Some observations on HC-128, Designs, Codes and Cryptography, Volume 59, SpringerLink 2011, 231-245.

[8] National Institute of Standards and Technology, Computer Security Devision, http://csrc.nist.gov/groups/ST/toolkit/rng/documentation_software.html

[9] Soto J., Statistical Testing of Random Number Generators, http://csrc.nist.gov/groups/ST/toolkit/rng/documents/nissc-paper.pdf

[10] Tsunoo Y. et al, Differential Cryptanalysis of Salsa20/8, https://www.cosic.esat.kuleuven.be/ecrypt/stream/papersdir/2007/010.pdf

[11] Zhang H., and Wang X., On the Security of Stream Cipher CryptMT v3, http://eprint.iacr.org/2009/110.pdf