СРАВНИТЕЛЬНЫЙ АНАЛИЗ ПОТОЧНЫХ СИММЕТРИЧНЫХ ШИФРОВ ПРОЕКТА eSTREAM

Нейванов А.В.[1,2], Головашич С.А.[2], Горбенко И.Д.[1]
Харьковский национальный университет радиоэлектроники[1]
ООО «Криптомаш»[2]
61057, Харьков, ул. Чернышевского, 4, Центр сертификации ключей ООО «Криптомаш»,
тел. +380 (57) 706-20-54, E-mail: Andrey.Neyvanov@cryptomach.com,
факс: +380 (57) 706-20-87

The given work is devoted to the modern developments in the field of stream symmetrical ciphers. We regard the winners of eSTREAM project and conduct a comparative analysis with a goal to selecting perspective algorithm.

После более чем трех лет проект eSTREAM подошел к концу [1]. На электронном ресурсе проекта появился финальное Собрание работ, которое содержит наиболее успешные поточные симметричные шифры и некоторые аспекты открытых расчетов.

Основной целью проекта eSTREAM была стимуляция работы в области поточных симметричных шифров. И в этом организаторы добились успеха. Они не ставили перед собой цели организовать конкурс как AES или предстоящий SHA-3 на лучший алгоритм. Организаторы также не использовали слово «победители» и не выбирали один (максимум два) шифра. Они составили перечень из поточных симметричных шифров прошедших через три этапа конкурса. Самых стойких, по мнению криптографов, которые в последствии могут быть рассмотрены как стандарты.

Поточные симметричные шифры проекта eSTREAM составляют два профиля [1]. В Профиль 1 входят шифры ориентированные на программную реализацию, а в Профиль 2 – шифры ориентированные на аппаратную реализацию. В алфавитном порядке Собрание работ выглядит так:

Таблица 1 – Собрание работ, содержащее лучшие алгоритмы проекта eSTREAM

Профиль 1	Профиль 2
HC-128	F-FCSR-H v2
Rabbit	Grain v1
Salsa20/12	MICKEY v2
Sosemanuk	Trivium

На третий этап попали гораздо больше шифров. Помимо приведенных выше в Профиль 1 вошли поточные симметричные шифры NLS v2, LEX v2, CryptMT v3, Dragon, а в Профиль 2 – Decim v2, Edon80, Pomaranch v3 и Moustique соответственно. Не вошли в Собрание работ они в связи с малым количеством балов на последнем голосовании.

Таблица 2 – Результаты заключительного голосования проекта eSTREAM

Профиль 1		Профиль 2	
Rabbit	2.80	Trivium	4.35
Salsa20	2.80	Grain v1	3.50
Sosemanuk	1.20	F-FCSR-H v2	0.52
HC-128	0.60	MICKEY v2	0.17
NLS v2	-0.60	Decim v2	-1.38
LEX v2	-1.20	Edon80	-1.72
CryptMT v3	-1.40	Pomaranch v3	-2.24
Dragon	-1.60	Moustique	-2.50

Как уже говорилось выше, в Профиль 1 вошли поточные симметричные шифры с хорошей программной реализацией. На столько хорошей, что должны были

превосходить по скоростным показателям блочный симметричный алгоритм шифрования AES в режимах генерации гаммы. Основным требованием к Профилю 1 было обеспечение уровня безопасности в 128 бит. Некоторые из представленных поточных симметричных шифров вошедших в Профиль 1 позволяют обеспечить уровень безопасности в 256 бит.

Почему же в Профиль 1 Собрания работ вошли не все поточные симметричные шифры, прошедшие третий этап? Начнем с алгоритма NLS v2. В третьем этапе конкурса рассматривалась только 2 версия алгоритма NLS. Предыдущие версии были отброшены. Данный алгоритм имел хорошую устойчивость к криптоаналитическим атакам и большой запас прочности. Однако по скоростным показателям он был сравним с алгоритмом AES в режимах генерации гаммы, что противоречило основному условию конкурса, и сильно отставал от оппонентов вошедших в Собрание работ.

Также не вошел в Профиль 1 Собрания работ алгоритм LEX v2. Разработанный в проекте AES алгоритм LEX был одним из аналитических ноу-хау. Самым элегантным и «провокационным». Однако был подвержен криптоанализу. В связи с чем и не вошел в финальное Собрание работ.

Ещё один интересный алгоритм прошедший третий этап, но не вошедший в Профиль 1 Собрания работ – CryptMT v3. Алгоритм CryptMT имел очень необычную конструкцию. Считался стойким алгоритмом до тех пор, пока на последнем этапе не были получены успешные результаты криптоанализа. Криптографическое сообщество надеялось, что данные уязвимости будут устранены в последующих версиях шифра. Однако на данный момент ожидания не оправдались, и поточный симметричный шифр CryptMT v3 не вошел в Профиль 1 Собрания работ.

Шифр Dragon также не вошел в Профиль 1 Собрания работ проекта eSTREAM. Изначально предполагалось, что он будет сильным шифром. Он противостоял всем атакам реализованным в проекте. Dragon также прошел этап сравнения с шифром AES в режиме счётчика (изначальная цель проекта eSTREAM). Негативом послужило то, что хорошего сравнения с AES оказалось недостаточно, чтобы преодолеть требования выдвинутые на финальной фазе проекта eSTREAM.

Профиль 2 Собрания работ проекта eSTREAM формировали поточные симметричные шифры с хорошей аппаратной реализацией. Они должны были быть пригодными к развертыванию на пассивных радиочастотных идентификаторах или на дешёвых устройствах, которые могли бы быть использованы в сенсорных сетях. Поточные симметричные шифры, представленные в Профиль 2 Собрания работ, также должны были обеспечить уровень безопасности в 80 бит. Некоторые алгоритмы помимо 80 битного уровня безопасности поддерживали и 128 битный уровень.

В Профиль 2 Собрания работ проекта eSTREAM также не вошли некоторые поточные симметричные шифры прошедшие третий этап. Это шифры Decim v2, Edon80, Pomaranch v3 и Moustique.

Начнем с шифра Decim v2. На первую версию шифра был найден эффективный метод криптоанализа. Вторая версия была устойчива ко всем атакам. Однако на заключительном голосовании жури посчитали, что хотя и шифр состоит из интересных элементов, он все же не может быть занесён в Профиль 2 Собрания работ.

С точки зрения жюри проекта eSTREAM шифр Edon80 представляет очень большой интерес. Они отметили инженеров-проектировщиков за отдельные элементы конструкции поточного симметричного шифра. Однако к нему была применима криптоаналитическая атака по восстановлению ключа. Что в свою очередь не позволило включить шифр в финальное Собрание работ, так как он перестал являться претендентом, обеспечивающим высокий уровень безопасности. И всё же тот факт, что шифр прошел 3 этапа проекта позволяет говорить, что его аппаратная реализация эффективнее чем алгоритм AES. Также жюри побаиваются, что данный поточный симметричный шифр может быть более эффективен, чем шифры представленные в финальном Собрании работ.

Подобно шифру Edon80 был отмечен поточный симметричный шифр Pomaranch v3 за отдельные элементы конструкции. Однако существование двух базовых атак на шифр как ключевой генератор не позволило его также включить в финальное Собрание работ.

Как только в проекте eSTREAM появились поточные симметричные шифры самосинхронизации, сразу был замечен алгоритм Moustique. На протяжении 3 этапов проекта он удовлетворял всем требованиям безопасности. Однако на последнем этапе была найдена атака, основанная на корреляции ключевых потоков. И этот факт в свою очередь привел к тому, что данный алгоритм также не вошел в финальное Собрание работ.

Далее рассмотрим шифры, вошедшие в финальное Собрание работ. Начнём с Профиля 1, ПСШ адаптированных под программную реализацию. В данный профиль, как видно из изложенного выше материала, вошли шифры HC-128, Rabbit, Salsa20/12 и Sosemanuk. Начнём по порядку с шифра HC-128.

Поточный симметричный шифр HC-128 является вариантом первоначального шифра HC-256. Он соответствует всем требованиям проекта eSTREAM. Имеет хорошую скорость в программных реализациях. За все три этапа конкурса на него не было найдено эффективных методов криптоанализа, позволяющих уменьшить его уровень защиты. К недостаткам шифра можно отнести большие временные затраты на повторную инициализацию. Данный недостаток существенно заметен в первоначальной реализации шифра HC-256.

Rabbit является одной из старейших конструкций проекта eSTREAM. Данный поточный симметричный шифр не был подвержен каким-либо модификациям или дополнениям. Его спецификация оставалась неизменной с 2003 года и по данный момент. Шифр пережил все три этапа проекта и не на одном из них не был подвержен криптоаналитическим атакам. Кроме всего прочего данный алгоритм очень хорошо реализуется на новых процессорах семейства Intel. Как недостатки можно заметить тот факт, что шифр Rabbit обеспечивает уровень безопасности только в 128 бит. Однако это и было основным условием проекта eSTREAM. Большего уровня безопасности организаторы конкурса не требовали.

Поточный симметричный шифр Salsa20/12 использует простые, чистые и масштабируемые конструкции. Также шифр позволяет работать с ключами длиной 128 и 256 бит. Простота и масштабируемость алгоритма позволили привлечь большое внимание криптоаналитиков. Однако Salsa20/12 прошел все 3 этапа проекта и так и не был успешно атакован. Для Собрания работ жюри выбрали версию поточного симметричного шифра Salsa20 состоящую из двенадцати раундов. Также на проекте были рассмотрены версии из восьми и двадцати раундов. В соотношении производительность/надёжность оптимальным был всё же выбран вариант из двенадцати раундов.

О шифре Sosemanuk известно, что он имеет очень большой запас надёжности. Он использует компоненты предшествующих ему блочных симметричных шифров. И соответственно данный факт позволил ему выдержать все три этапа конкурса. По мнению жюри проекта eSTREAM поточный симметричный шифр Sosemanuk представляет собой большой исследовательский интерес.

Профиль 2 Собрания работ, как было сказано выше, состоит из поточных симметричных шифров ориентированных на аппаратную реализацию. В данный профиль, как видно из изложенного выше материала, вошли шифры F-FCSR-H v2, Grain v1, MICKEY v2, Trivium. Начнём по порядку с шифра F-FCSR-H v2.

Поточный симметричный шифр F-FCSR-H v2 является очень простым и, тем не менее, эффективным. Хотя он и не является таким универсальным как Grain v1 или Trivium, но отсутствие на него эффективных методов криптоанализа позволило включить данный алгоритм в финальное Собрание работ.

Grain v1 является очень хорошим шифром для аппаратной реализации. Запас надёжности у данного шифра очень велик, что позволило ему выдержать все три этапа проекта. Жюри проекта eSTREAM также возлагают надежду на то, что разработчиками будут проанализированы все самые последние методы криптоаналитических атак на поточные симметричные шифры и выйдет новая более сильная версия шифра.

Поточный симметричный шифр MICKEY v2 по показателям эффективности не уступает шифрам Grain v1 и Trivium. Как недостаток можно отметить отсутствие гибкости в алгоритме. Инженеры-проектировщики данного шифра выбрали консервативный подход в проектировании, что могло привести к довольно-таки сложной и громоздкой конструкции. Однако этого не случилось. Также позитивно отразился тот факт, что на шифр не было осуществлено ни одного эффективного метода криптоанализа, что позволило поточному симметричному шифру MICKEY v2 войти в финальное Собрание работ.

Алгоритм Trivium является лидером Профиля 2 Собрания работ. Он довольно таки простой и прозрачный по конструкции. Именно прозрачность данного поточного симметричного шифра вдохновляла многих на реализацию атак. Тем не менее, на данный момент не существует ни одного эффективного метода криптоанализа. Также данный поточный симметричный шифр имеет хорошие показатели по производительности при аппаратных реализациях. Что позволило ему занять почётное первое место в финальном Собрании работ.

В целом проект eSTREAM видится весьма успешным. В результате совместной деятельности на мировом уровне были не только разработаны новые стойкие криптографические примитивы и поточные симметричные шифры, но и изобретены новые подходы к анализу безопасности схем поточного шифрования. Алгоритмы, представленные в Собрании работ, приведенном выше, рекомендуются к рассмотрению на стандарты шифрования и широкому использованию в информационных сетях и каналах связи.

Литература

1. The eSTREAM Portfolio, Steve Babbage, Christophe De Canni`ere, Anne Canteaut4, Carlos Cid, Henri Gilbert, Thomas Johansson, Matthew Parker, Bart Prenee, Vincent Rijmen, and Matthew Robshaw. April 15, 2008

2. ДСТУ Проект ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ. КРИПТОГРАФІЧНИЙ ЗАХИСТ ІНФОРМАЦІЇ. ТЕРМІНИ ТА ВИЗНАЧЕННЯ.