

УДК 519.713

СРАВНИТЕЛЬНЫЙ АНАЛИЗ АППАРАТНЫХ ПОТОЧНЫХ СИММЕТРИЧНЫХ ШИФРОВ ПОБЕДИТЕЛЕЙ ПРОЕКТА eSTREAM

Андрей Нейванов, Иван Горбенко

Харьковский национальный университет радиоэлектроники

Аннотация: В этом тезисе описывается подход к сравнительному анализу аппаратных алгоритмов поточного симметричного шифрования проекта eSTREAM.

Summary: This summary describes the approach to the comparative analysis of hardware algorithms for symmetric stream encryption of project eSTREAM.

Ключевые слова: Аппаратные поточные симметричные шифры, информационная безопасность.

После более чем трёх лет проект eSTREAM подошел к концу. На электронном ресурсе проекта появилось финальное Собрание работ, которое состоит из наиболее успешных поточных симметричных шифров и некоторых аспектов открытых расчетов. Основной целью проекта eSTREAM была стимуляция работы в области поточных симметричных шифров. И в этом организаторы добились успеха. Они составили перечень из поточных симметричных шифров, которые выдержали три этапа конкурса. Самых стойких, по мнению криптографов, которые в последствии могут быть рассмотрены как стандарты, рекомендованные к испытанию и использованию. Целью этого тезиса является описание подхода к отбору лучших аппаратных алгоритмов ПСШ и анализу их свойств.

Для проведения сравнительного анализа предложена методика принятия решений на множестве альтернативных вариантов. Как одна из методик хорошо себя зарекомендовавших и позволяющих провести комплексную оценку по ряду критериев оцениваемых объектов.

Оценка претендентов будет проводиться в два этапа. На первом этапе алгоритмы-кандидаты будут проверяться на соответствие безусловным критериям. Поскольку безусловные критерии допускают выбор только стойких алгоритмов, то каждый алгоритм, который соответствует безусловным критериям, потенциально может использоваться.

К безусловным критериям отнесено те критерии (показатели), выполнение которых является обязательным для шифра.

Поточный симметричный шифр должен безусловно владеть следующими свойствами (удовлетворять безусловному критерию):

1. Защищённость от всех известных и потенциально возможных криптоаналитических атак.
2. Статистическая безопасность алгоритма шифрования.
3. Надежность математической базы.
4. Практическая защищённость алгоритма шифрования от силовых атак.
5. Отсутствие слабых начальных ключей и подозрений на существование ключей.
6. Сложность прямого и обратного преобразования не превышают допустимой величины, кроме того, сложность генерации ключевого потока не превышает заданной.

Помимо безусловных критериев поточные симметричные шифры на втором этапе будут сравниваться по условным критериям. Из условных критериев мы выделяем следующие:

1. Возможность и условия свободного распространения алгоритма в Украине с учётом национального и международного законодательства.
2. Уровень доверия к шифру.
3. Перспективность применения алгоритма шифрования.
4. Сложность аппаратной реализации.
5. Гибкость алгоритма шифрования.

Таким образом, предложенная методика и выбранные критерии позволяют осуществить сравнительный анализ перспективных алгоритмов шифрования.

Анализ данных значений безусловного и условного критерия оценки алгоритмов шифрования позволяет сделать вывод, о наилучшем алгоритме и алгоритмах стоящих внимания. К тому же можно сделать вывод о том, какой аппаратный алгоритм поточного симметричного шифрования целесообразно рекомендовать к использованию в Украине для решения задач обеспечения конфиденциальности информации сегодня.