УДК 681.3.06

АНАЛИЗ УСОВЕРШЕНСТВОВАНИЙ ШИФРА RIJNDAEL

Ирина Лисицкая, Александр Казимиров, Евгений Мельничук, Алексей Широков, Алексей Обухов

Харьковский национальный университет радиоэлектроники

Анотація: **Наводиться аналіз рішень, що маються у літературі, присвячених вдосконаленню шифру Rijndael.**

Аннотация: **Приводятся анализ имеющихся в литературе решений, являющихся усовершенствованиями шифра Rijndael.**

Сегодня уже можно назвать не одно решение по построению усовершенствованных версий шифра Rijndael (шифров, строящихся на основе идей, использованных при построении шифра Rijndael). В их числе шифры Anubis и GrandCru представленные на Европейском конкурсе, а также шифры Калина и ADE, заявленные на украинский конкурс по выбору и принятию национального стандарта.

Основными направлениями усовершенствований является дальнейшее наращивание стойкости за счет дополнительного перекрытия потенциальных слабостей, выявленных в процессе экспертизы конструкции Rijndael специалистами. При разработке версии Anubis была также поставлена задача повышения показателей производительности.

Во всех модифицированных решениях вместо S-блоков, имеющих явно выраженную алгебраическую структуру (реализующих идеи построения S-блоков, предложенные К. Нюберг), использованы S-блоки случайного типа. В шифрах GrandCru и ADE, в дополнение к отмеченному, задача дальнейшего наращивания стойкости решается путем введения в цикловую функцию ключезависимых преобразований. В ADE все цикловые преобразования сделаны зависимыми от ключа, а в GrandCru введено два дополнительных ключезависисмых преобразования, и сама цикловая функция дополнительно усложнена. Дополнительно стоить отметить, что в модифицированных версиях использованы различные схемы разворачивания ключей.

Напомним, что шифры Anubis и GrandCru были сняты с рассмотрения на конкурсе Nessie. Хотя Anubis и имел преимущества перед шифром Rijndael по производительности, эксперты посчитали, что его отличия от Rijndael не столь существенны, чтобы их воспринимать как новое прогрессивное решение. Шифр GrandCru был воспринят как слишком усложненный и трудный для понимания, а, самое главное, он в значительно проиграл шифру Rijndael по производительности.

Что касается украинских предложений, то предпочтение на сегодняшний день отдано шифру Калина. Можно здесь заметить, что авторы и сегодня продолжают совершенствовать предложенную конструкцию (не меняя основных решений) в направлении дальнейшего повышения производительности.

В первой части работы представляются результаты сравнительного анализа S-блоков шифров Rijndael и конструкций, предложенных в модифицированных решениях. Сравнение осуществляется на основе анализа криптографических свойств булевых функций. Примененные в модифицированных шифрах случайные подстановки, как и S-блоки шифра Rijndael, не удовлетворяют таким криптографическим показателям как: критерий распространения, корреляционная иммунность и др. (этим критериям не удовлетворяет большая часть булевых функций рассмотренных S-блоков).

Во второй части работы приводятся данные по оценке показателей стойкости уменьшенных моделей рассмотренных шифров к атакам линейного и дифференциального криптоанализа. Для решения этих задач разработаны соответствующие уменьшенные модели и в соответствии с разработанной методикой проведены статистические эксперименты по определению полных дифференциалов и линейных корпусов.

Общий вывод этой части работы состоит в том, что все предложенные модификации шифра Rijndael в целом по показателям стойкости к атакам дифференциального и линейного криптоанализа не уступают оригиналу.

Дальнейшее исследование связано с поиском подстановок, применение которых в шифрах без изменения структуры, заявленной разработчиками, позволяет добиться наращивания показателей стойкости. В частности, уже имеющиеся результаты экспериментов свидетельствуют, что использование случайных S-блоков нового типа позволяет не только исключить потенциально существующую угрозу в виде возможной уязвимости шифра Rijndael к алгебраическим атакам, но существенно улучшить динамические показатели шифра в части уменьшения минимального значения числа циклов, при котором шифр достигает установившегося (асимптотического) значения полного дифференциала и соответствующего асимптотического значения линейного корпуса.