УДК 621.3.06

ОЛЕЙНИКОВ Р.В., КАЗИМИРОВ А.В.

Харьковский национальный университет радиоэлектроники

# СРАВНЕНИЕ ФУНКЦИЙ РАЗВОРАЧИВАНИЯ КЛЮЧА СИММЕТРИЧНЫХ БЛОЧНЫХ ШИФРОВ

Симметричные блочные шифры являются одним из наиболее распространённых криптографических примитивов. Помимо обеспечения конфиденциальности при шифровании сообщений, эти алгоритмы применяются как конструктивные элементы хэш-функций, генераторов псевдослучайных последовательностей, протоколов аутентификации и др. Современные блочные шифры проектировались с учетом необходимости увеличения производительности и в этих областях [1], что привело к минимизации сложности шифрующего преобразования и, особенно, функций разворачивания ключа (ФРК). Тенденция упрощения ФРК привела к тому, что в новых работах [2] были продемонстрированы методы, позволяющие в достаточно специфических условиях получить ключ шифрования ГОСТ 28147-89 и AES-192/256 со сложностью, значительно меньшей, чем полный перебор ключей.

В связи с этим актуальной становится задача сравнения функций разворачивания ключей существующих алгоритмов шифрования. Предлагаемая классификация ориентирована на оценку сложности восстановления криптоаналитиком ключа шифрования (мастер-ключа) при наличии одного или нескольких подключей (полученных в результате дифференциального анализа сбоев, алгебраического криптоанализа или других атак). После рассмотрения функций разворачивания ключей симметричных блочных шифров (Blowfish, DES, CAST-128, SHACAL1, SHACAL2, MISTY1, Camellia, Калина, Лабиринт, ГОСТ 28147, Rijndael и др.) предлагается разделить все ФРК на 3 класса:

класс 1 – знание подключа позволяет вычислить другой подключ, мастер-ключ или их части;

класс 2 – знание подключа позволяет вычислить другой подключ или его часть, но не даёт информации о мастер-ключе;

класс 3 – знание подключа не даёт явной информации о других подключах или мастер-ключе.

Учитывая особенности проведения криптоанализа современных ФРК, предложенные классы целесообразно разделить на подклассы в соответствии с таблицей 1.

Таблица 1 – Классификация ФРК

| | |
|---|---|
| 1А | Каждый последующий подключ формируется путём линейных операций из предыдущего подключа или мастер-ключа. |
| 1Б | Каждый последующий подключ формируется путём нелинейных и линейных операций из предыдущего подключа или мастер-ключа. |
| 2А | Известен простой алгоритм, позволяющий гарантированно найти мастер-ключи, которые дают хотя бы один одинаковый цикловой подключ. |
| 2Б | Существует верхняя граница вероятности (меньшая 1) нахождения мастер-ключей, которые дают хотя бы один одинаковый цикловой подключ. |
| 3А | Неизвестен алгоритм, позволяющий сформировать мастер-ключи, которые дают хотя бы один одинаковый цикловой подключ. |
| 3Б | Все подключи, для каждого из циклов, формируются независимо и длина мастер-ключа равна сумме длин подключей. |

Классификация ФРК рассмотренных шифров приведёна в таблице 2.

Таблица 2 –классификация функций разворачивания ключа

| 1А | 1Б | 2Б | 3А | 3Б |
|---|---|---|---|---|
| ГОСТ 28147, DES | Rijndael, SHACAL2, Camellia, MISTY1, Лабиринт | Калина | Blowfish, SEED | DESI |

ФРК, относящиеся к классу 1, потенциально уязвимы к атакам на связанных ключах, но при этом обеспечивают высокую производительность и простоту реализации. С другой стороны, алгоритмы, имеющие ФРК класса 3, имеют очень высокий уровень защищённости от криптографических атак, однако значительно проигрывают в быстродействии. Оставшийся класс 2 наиболее сбалансирован с точки зрения стойкости и производительности, но в большинстве случаев требует строгого обоснования выбранного решения.

**Оценка быстродействия функций разворачивания ключа**

Учитывая, что в большинстве случаев современные криптографические примитивы имеют программную реализацию (для архитектуры общего назначения или специализированных микроконтроллеров), оценку быстродействия и сложности реализации целесообразно выполнять с учетом именно этой особенности.

Количество операций для наименьшей длины ключа функций разворачивания ключа рассмотренных шифров приведено в таблице 3.

Таблица 3 – число операций для рассмотренных ФРК

| Название алгоритма | Размер подключей, биты | Сдвиги | XOR | AND | OR | NOT | Сложение по модулю | Выборка из памяти | Всего операций |
|---|---|---|---|---|---|---|---|---|---|
| ГОСТ 28147 | 1024 | – | – | – | – | – | – | 24 | 24 |
| MISTY1 | 1024 | – | 40 | 8 | 16 | – | – | 24 | 88 |
| Rijndael | 1408 | 10 | 50 | – | – | – | – | 40 | 100 |
| Лабиринт | 512 | 1 | 57 | – | – | – | 6 | 48 | 112 |
| Camellia | 1664 | 32 | 148 | 24 | – | 9 | 9 | – | 222 |
| Калина | 1536 | 9 | 168 | – | – | 2 | 12 | 96 | 287 |
| SHAC-2 | 2048 | 228 | 192 | – | – | – | 144 | – | 564 |
| DES | 768 | 686 | 21 | 311 | 256 | – | – | 128 | 1402 |

Скорость работы ФРК рассмотренных шифров на универсальной программной платформе (Intel Core 2 Duo E8200/2.66 ГГц/Windows 7/VS C++ 2008 SP1) приведена в таблице 4. В правой колонке таблицы указан показатель KA (key agility) [3], выражающий отношение производительности ФРК к скорости шифрования. Если KA < 1, то быстродействие систем, где необходимо вырабатывать ключи на каждый блок, будет напрямую зависеть от скорости ФРК. Как видно из таблицы 4, наибольшую скорость функции разворачивания ключей имеют алгоритмы ГОСТ, Rijndael, MISTY1 и Лабиринт. Тем не менее, простота конструкции ведет к возможности реализации эффективных криптоаналитических атак на ФРК. Алгоритмы с более медленными ФРК имеют лучший уровень защищенности, что необходимо учитывать при выборе шифра для конкретного применения.

**Выводы**

Предложенная классификация функций разворачивания ключей позволяет оценить частные показатели эффективности существующих алгоритмов шифрования и оптимизировать проектируемые.

Таблица 4 – скорость работы рассмотренных ФРК на универсальной платформе

| Название алгоритма | Размер подключей, биты | ФРК, ключей/с | ФРК, Мбит/с | Шифрование, блоков/с | Шифрование, Мбит/с | $K_A$ |
|---|---|---|---|---|---|---|
| ГОСТ-28147 | 1024 | 64516129,03 | 63004,03 | 6410256,41 | 391,25 | 10,06 |
| MISTY1 | 1024 | 21276595,74 | 20777,93 | 5571030,64 | 350,03 | 3,82 |
| Лабиринт | 512 | 11695906,43 | 5710,89 | 2785515,32 | 340,23 | 4,20 |
| Rijndael | 1408 | 10695187,17 | 14361,21 | 6756756,76 | 824,80 | 1,58 |
| Camellia | 1664 | 7117437,72 | 11294,76 | 4140786,75 | 505,47 | 1,72 |
| SHACAL-2 | 2048 | 7117437,72 | 13901,25 | 2564102,56 | 626,00 | 2,78 |
| Калина | 1536 | 6410256,41 | 9390,02 | 3466204,51 | 423,12 | 1,85 |
| DES | 768 | 4750593,82 | 3479,44 | 6410256,41 | 391,25 | 0,74 |

Алгоритмы, имеющие высокие показатели скорости разворачивания подключей, как правило, уязвимы для атак специального вида, поэтому необходимы дополнительные исследования перед использованием AES/Rijndael, ГОСТ 28147-89 в хэш-функциях, ГПСЧ и др.

Шифры, представленные на открытый криптографический конкурс в Украине (Калина, Лабиринт) имеют достаточно высокие показатели криптографической стойкости ФРК при среднем уровне быстродействия.

**Литература**

1. *Biryukov A. Related-key cryptoanalysis of the full AES-192 and AES-256 [Electronic resource] / A. Biryukov, D. Khovratovich. Mode of access : WWW.URL: https://cryptolux.org/mediawiki/uploads/1/1a/Aes-192-256.pdf*

2. *Preneel B. Final report of European project number IST-1999-12324, named New European Shames for Signatures, Integrity, and Encryption [Electronic resource] / B. Preneel, A. Biryuov, C. De Canniere, etc. Mode of access : WWW.URL: https://www.cosic.esat.kuleuven.be/nessie/Bookv015.pdf*

3. *Whiting D. AES Key Agility Issues in Hight-Speed IPsec Implementations [Electronic resource] / D. Whiting, B. Schneier, S. Bellovin. Mode of access : WWW.URL: www.securiteinfo.com/ebooks/palm/AES-KeyAgile.pdf*