

ДВА МЕТОДА ПОСТРОЕНИЯ ЛИНЕЙНЫХ БАЗИСОВ ВЕКТОРНЫХ ПРОСТРАНСТВ НА $GF(2)$

Головашич С.А.

Процедуру блочного шифрования можно рассматривать как управляемое секретным ключом биективное отображение блоков данных фиксированной длины. В то же время процедуру блочного симметричного шифрования удобно рассматривать как композицию некоторого множества элементарных шифрующих преобразований коротких блоков данных.

В силу простоты реализации на широком спектре аппаратных средств, наибольшее распространение, среди управляемых ключом отображений, получили простые аффинные операции: сложение подблока фиксированной длины n с подключом той же длины, по некоторому модулю равному 2 либо 2^n .

Указанные преобразования обладают свойством транспортирования дифференциальных и линейных характеристик. На этой особенности построены наиболее эффективные на сегодняшний день атаки соответственно дифференциального и линейного криптоанализа. Основным средством защиты от атак этого типа является применение высоко нелинейных преобразований, в качестве альтернативного (либо дополнительного) средства защиты некоторые разработчики предлагают использовать управляемый циклический сдвиг подблоков. Развитием этого принципа является применение переменного аффинного преобразования (циклический сдвиг является частным случаем перестановки битов, которая является частным случаем аффинного (линейного) отображения пространства V_n на $GF(2)$). Подобные преобразования могут быть эффективно реализованы программно и особенно аппаратно.

В докладе рассматриваются способы построения линейных базисов векторных пространств V_n на $GF(2)$, которые могут использоваться для определения биективных линейных отображений на указанном пространстве.

Предложенные алгоритмы позволяют решить задачу построения линейных базисов для различных приложений. В зависимости от области применения, может использоваться либо ресурсоёмкий алгоритм «матричного разложения», обеспечивающий выбор базиса из полного множества, либо высокоскоростной алгоритм выбора базиса из некоторого ограниченного множества.

Первый, из предложенных алгоритмов, ориентирован на статическое (предварительное) формирование базиса, в то время как областью применения двух других алгоритмов являются приложения динамического (в реальном масштабе времени) формирования базисов.