ШИФРОВАНИЕ НА ОСНОВЕ МНОГОМЕРНОГО ПРЕДСТАВЛЕНИЯ ВИРТУАЛЬНЫХ ВЫБОРОЧНЫХ ПРОСТРАНСТВ АНСАМБЛЕЙ КЛЮЧА

Котенко В.В., Румянцев К.Е,
Поликарпов С.В., Левендян И.Б.
Таганрогский Государственный Радиотехнический Университет, Таганрог

Реализация стратегии виртуализации выборочных пространств ансамблей ключа [1] на основе многомерного представления выборочных пространств занимает особое место среди возможных вариантов реализации данной стратегии. В первую очередь, это объясняется открывающейся возможностью применения принципиально отличного математического аппарата. В данном случае под многомерным понимается представление в виде совокупности процедур виртуализации $VIR_j(K_{nd}(i))$, каждая из которых рассматривается как отдельное измерение. С этих позиций процесс формирования виртуального ключа $K_V^M(t)$ может быть представлен как виртуализация исходного ключа в некотором М-мерном пространстве одновременно по всем его измерениям с последующей унификацией результатов виртуализации в некоторую функцию этого пространства, которая будет представлять собой виртуальный ключ:

$$K_V^M(t) = UNIF(K_V^j(t)), \quad (1)$$

$$K_V^j(t) = VIR_j(K_{nd}(i)), \quad (2)$$

где UNIF (.) – процедура унификации;

VIR_j (.) – процедура виртуализации, определяющая j-е измерение;

$K_{nd}(i)$ - исходный ключ, формируемый на основании заданных ключевых данных K_d;

$K_V^j(t)$ - проекция виртуального ключа на j-е измерение;

Развернутый ключ формируется путем девиртуализации полученного виртуального ключа:

$$K_r^M(i) = DVIR_M(K_V^M(t)). \quad (3)$$

Выражения (1)-(3) определяют общий алгоритм формирования развернутого ключа при многомерном представлении виртуальных выборочных пространств ансамблей ключа. Конкретизация данного алгоритма осуществляется путем задания процедуры унификации. Варианты такой конкретизации представлены выражениями (4) и (5)

$$K_r^M(i) = DVIR_M\left(\sum_{j=1}^{M}(K_V^j(t))\right), \quad (4)$$

$$K_r^M(i) = DVIR_M\left(\prod_{j=1}^{M}K_V^j(t)\right). \quad (5)$$

Программная реализация алгоритмов, заданных в выражениях (4), (5) позволила создать программный комплекс шифрования, открывающий возможность обеспечения абсолютной недешифруемости. Проводимые в настоящее время экспериментальные исследования данного комплекса подтверждают его значительные потенциальные возможности. Приведенные результаты получены в ходе исследований при поддержке гранта Министерства образования РФ Т02-03.1-816.

Список литературы

1. Котенко В.В., Поликарпов С.В. Стратегия формирования виртуальных выборочных пространств ансамблей ключа при решении задач защиты информации // Вопросы защиты информации. 2002. №2. С.47 − 52.

ШИФРОВАНИЕ С ПАРАЛЛЕЛЬНЫМ УСЛОЖНЕНИЕМ ВИРТУАЛЬНЫХ ВЫБОРОЧНЫХ ПРОСТРАНСТВ АНСАМБЛЕЙ КЛЮЧА

Котенко В.В., Румянцев К.Е,
Поликарпов С.В., Левендян И.Б.
Таганрогский Государственный Радиотехнический Университет, Таганрог

Возможность обеспечения абсолютной недешифруемости, которую открывает стратегия виртуализации выборочных пространств ансамблей ключа [1] определяет актуальность дальнейших исследований в данном направлении. Полученные в настоящее время результаты данных исследований показывают, что одним из вариантов реализации данной стратегии является параллельное усложнение виртуальных выборочных пространств. Под параллельным усложнением в данном случае понимается формирование виртуального ключа и его девиртуализация одновременно по М независимым каналам. При этом развернутый ключ формируется путем объединения (унификации) результатов девиртуализации используемых каналов. Таким образом, алгоритм формирования рабочего ключа может быть представлен в виде

$$K_V^j(t) = VIR_j(K_{nd}(i)) \quad (1)$$

$$K_V^j(t) = VIR_j(K_{nd}(i)) \quad (2)$$

где

UNIF (.) – процедура объединения (унификации).

VIR_j (.) – процедура виртуализации j-го канала;

$DVIR_j$ (.) – процедура девиртуализации j-го канала;

$K_V^j(t)$ – виртуальный ключ j-го канала;

$K_{nd}(i)$ – исходный ключ, формируемый на основании заданных ключевых данных K_d

Порядок усложнения виртуального выборочного пространства в данном случае определяется числом параллельно используемых каналов j. Приведенный алгоритм является общим. Его конкретизация производится путем выбора процедуры унификации. Необ-

ходимо подчеркнуть, что здесь для исследователя открывается широкое поле деятельности. Например, в качестве этой процедуры могут быть использованы суммирование и произведение результатов девиртуализации каналов. В первом случае алгоритм формирования развернутого ключа принимает вид, представленный выражением (3), во втором – выражением (4)

$$K_r^M(i) = \prod_{j=1}^{M} DVIR_j(K_V^j(t)) : \quad (3)$$

$$K_r^M(i) = \sum_{j=1}^{M} DVIR_j(K_V^j(t)) \quad (4)$$

Реализация приведенных алгоритмов позволила создать программный комплекс шифрования, открывающий возможность обеспечения абсолютной недешифруемости. Исследования, проводимые в направлении совершенствования данного комплекса дают обнадеживающие результаты, представляющий научный и практический интерес. Приведенные результаты получены в ходе исследований при поддержке гранта Министерства образования РФ Т02-03.1-816.

Список литературы

1. Котенко В.В., Поликарпов С.В. Стратегия формирования виртуальных выборочных пространств ансамблей ключа при решении задач защиты информации // Вопросы защиты информации. 2002. №2. С.47 − 52.

ШИФРОВАНИЕ С ПОСЛЕДОВАТЕЛЬНЫМ УСЛОЖНЕНИЕМ ВИРТУАЛЬНЫХ ВЫБОРОЧНЫХ ПРОСТРАНСТВ АНСАМБЛЕЙ КЛЮЧА

Котенко В.В., Румянцев К.Е, Поликарпов С.В., Левендян И.Б.
Таганрогский Государственный Радиотехнический Университет, Таганрог

Актуальность решения проблемы обеспечения абсолютной недешифруемости в современных условиях определяется неуклонным возрастанием роли информационных технологий. В последнее время в этом направлении наметился определенный прогресс. Так, в [1] была предложена стратегия решении данной проблемы на основе виртуализации выборочных пространств ансамблей ключа. Последующие исследования позволили получить ряд вариантов реализации данной стратегии. Одним из таких вариантов является шифрование, основанное на последовательном усложнении виртуальных выборочных пространств ансамблей ключа. Его основу составляет рекуррентный алгоритм (1) формирования виртуального ключа:

$$K_V^j(t) = VIR_j(DVIR_{j-1}(K_V^{j-1}(t))), j = 1...N, \quad (1)$$

где

$VIR_j(\,.\,)$ – процедура виртуализации;

$DVIR_j(\,.\,)$ – процедура девиртуализации;

j – порядок уровня усложнения.

Полученный алгоритм предполагает многократную последовательную виртуализацию и девиртуализацию ансамбля ключа. При этом на каждом шаге виртуализации в качестве исходного ключа выступает результат девиртуализации виртуального ключа, полученного на предыдущем шаге. Начальным условием $DVIR_0(K_V^0(t))$ функционирования данного алгоритма является исходный ключ $K_{nd}(i)$, формируемый на основании заданных ключевых данных K_d:

$$DVIR_0(K_V^0(t)) = K_{nd}(i). \quad (2)$$

Развернутый ключ $K_n^N(i)$ формируется путем девиртуализации виртуального ключа, полученного на конечном N-ом шаге усложнения:

$$K_n^N(i) = DVIR_N(K_V^N(t)) \quad (3)$$

На основании приведенного подхода было получено семейство способов шифрования с последовательным усложнением виртуального ключа, открывающих возможность обеспечения абсолютной недешифруемости. Реализация данных способов позволила создать программный комплекс шифрования, обладающий уникальными возможностями. Экспериментальные исследования показали высокую надежность и эффективность данного комплекса.

Приведенные результаты получены в ходе исследований при поддержке гранта Министерства образования РФ Т02-03.1-816.

Список литературы

1. Котенко В.В., Поликарпов С.В. Стратегия формирования виртуальных выборочных пространств ансамблей ключа при решении задач защиты информации // Вопросы защиты информации. 2002. №2. С.47 − 52.

ЭЛЕКТРОХИМИЧЕСКАЯ РАЗМЕРНАЯ ОБРАБОТКА ПОЛИГОНАЛЬНЫМ КАТОДОМ

Котляр Л.М., Миназетдинов Н.М., Хайруллин А.Х.
Камский государственный политехнический институт, Набережные Челны

Электрохимическая размерная обработка металлов – один из современных методов изготовления деталей из металлов и сплавов с заданной формой, размерами и качеством поверхности. Метод основан на принципе локального растворения анода – обрабатываемой заготовки в проточном электролите. Роль катода – обрабатывающего инструмента выполняет электрод с заданной геометрической формой поверхности. Протекание электрохимических процессов обеспечивается прокачкой раствора электролита через межэлектродный промежуток (МЭП) с целью выноса из зоны обработки продуктов реакции (газа, шлама) и выделившегося тепла