УДК 004.056.55 (004.421.5)

А.В. ГАПЕЕНКО*, *Л.В. ДЕРБУНОВИЧ, докт. техн. наук, профессор

Использование сдвиговых регистров с нелинейными обратными связями в генераторах ключевых последовательностей

Все более широкое применение электронных средств передачи данных, в сочетании с ростом использования компьютерной техники приводит к необходимости расширения ассортимента и повышения качества методов защиты информации.

Криптография является одним из наиболее часто используемых практических методов защиты информации, передаваемой по незащищенному каналу. Для защиты больших объемов данных, а также данных, передаваемых на высоких скоростях, очевидным выбором является симметричный способ шифрования. К симметричным методам криптографической защиты данных относятся специализированные блочные и поточные алгоритмы шифрования. Однако им обоим характерен один существенный недостаток: необходимость обеспечения надёжных средств и процедур по созданию, распространению и хранению ключей шифрования. Для создания качественных с криптографической точки зрения ключевых последовательностей используются генераторы случайных и псевдослучайных чисел [1]. Такие генераторы позволяют получать непредсказуемые или труднопредсказуемые последовательности битов, которые могут быть интерпретированы как случайные или псевдослучайные числа или в криптографических средствах – как ключи шифрования.

Основной причиной использования непредсказуемых случайных битовых последовательностей (СБП) в криптографии является невозможность по короткому фрагменту такой последовательности при наличии необходимых вычислительных ресурсов определить все биты этой последовательности.

Для получения СБП широко используются специализированные генераторы псевдослучайных битов (ГПБ). Для того чтобы битовая последовательность была случайной, её период должен быть достаточно большим и различные модели заданной длины должны быть равномерно распределены по последовательности.

Наиболее простым и распространённым методом генерации СБП является использование сдвиговых регистров с обратной связью, которые служат основным функциональным элементом в большом разнообразии схем генераторов псевдослучайных чисел [2].

Простейшим и наиболее популярным видом сдвигового регистра с обратной связью является сдвиговый регистр с линейной обратной связью (СРЛОС). Обратная связь в этом устройстве реализуется просто как сумма по модулю 2 всех (или некоторых) выходов запоминающих ячеек регистра. Биты, которые участвуют в обратной связи, образуют отводную последовательность. СРЛОС имеют многочисленные области применения, в

том числе выявление и исправление ошибок, сжатие данных, тестирование и криптография.

Помимо СРЛОС существуют сдвиговые регистры, обратная связь которых представляет собой некоторую нелинейную булеву функцию. Такие регистры называются сдвиговыми регистрами с нелинейными обратными связями или СРНОС. Случайные последовательности, получаемые с помощью сдвиговых регистров этого типа, обладают очень хорошими статистическими свойствами, которые по некоторым параметрам оказываются значительно лучше, чем у последовательностей, получаемых с помощью СРЛОС. Однако для СРНОС отсутствует пока решение для ряда фундаментальных теоретических проблем, важнейшей из которых является отсутствие формализованной систематической процедуры построения схемы для получения последовательности с гарантированно максимальным периодом.

Исследованию принципов построения СРНОС и поиска описанной выше процедуры посвящено множество работ [3−5] и в этой области наблюдается определённый прогресс. Возникает задача разработки новых схем генерации псевдослучайных последовательностей на СРНОС или адаптация уже существующих на базе СРЛОС.

В качестве цели работы был поставлен анализ возможностей и поиск способов применения СРНОС в схемах генераторов псевдослучайных битовых последовательностей, основанных на использовании СРЛОС. Применение СРНОС в качестве основного функционального элемента в этих генераторах может привести к существенному улучшению статистических качественных характеристик генерируемой последовательности при незначительном увеличении аппаратных затрат.

Как показывает практика реализации схем СРНОС, перестройка функциональной составляющей схем СРЛОС для реализации нелинейных функций приводит к незначительному увеличению затрат аппаратных средств вследствие увеличения функционального логического базиса и возникновения необходимости в введении дополнительных связей между элементами схемы.

Таким образом, технически возможно в типовых схемах заменить СРЛОС на СРНОС при условии всестороннего изучения статистических характеристик и критериев криптографической стойкости и подтверждение того, что они не ухудшатся. Принципиальных различий в реализации между ними нет.

Список литературы:

1. Шнайер. Б. Прикладная криптография (Applied Cryptography), 2-е издание. – 1994.

2. Kencheng Zeng. "Pseudorandom Bit Generators in Stream-Cipher Cryptography," / Kencheng Zeng, Chung-Huang Yang, Dah-Yea Wei, T.R.N. Rao // Computer, vol. 24, no. 2, -- 1991. -- pp. 8-17,

3. Annexstein F.S. Generating de Bruijn sequences: An efficient Implementation // IEEE Trans. On. Computers. – 1997. – Vol. C-46, №2. – p.198 – 200.

4. Дербунович Л. В. Генераторы тестов для дискретных ДУ с самотестированием / Дербунович Л.В., Татаренко Д.А., Темников И.Н. // Информационно – управляющие системы на железнодорожном транспорте. – 2004. – № 1. – с. 40 – 45.

5. Темников И. Н. Генератор нелинейной псевдослучайной тестовой последовательности // Вестник ХГПУ. – Харьков: ХГПУ. – 2000. – Вып. 112. – с. 130 –134.