– AES-256 блочный шифр, криптографические стандарты открытого ключа RSA, ISO 9796-2 система подписи, SHA-1 систему хэширования и RC4 шифрование потока. В ooVoo аутентификация пользователей осуществляется по защищенному каналу TLS (RSA-RC4-128-MD5), аудио и видео трафик передается в открытом виде. Таким образом, Microsoft Lync Server 2010 и Skype используют схожие технологии информационной безопасности и предоставляют более защищенные сервисы по отношению к ooVoo.

КРИПТОГРАФИЧЕСКИЙ АНАЛИЗ АЛГЕБРО-ГЕОМЕТРИЧЕСКИХ КОДОВ НА СООТВЕТСТВИЕ ТРЕБОВАНИЯМ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ

С.Б. САЛОМАТИН, В.В. ПАНЬКОВА

Кодовые структуры, обладающие стойкостью к раскрытию, используют как компоненты систем защиты информации. Одним из эффективных средств защиты от ошибок и преднамеренных воздействий является комплексная кодовая зашита. Объектом исследования являлись алгебро-геометрические коды Эрмита, мощность которых превосходит аналогичный показатель кодов эллиптических кривых.

Основными критериями, предъявляемыми к разработке и исследованию эффективности криптоалгоритмов, являются такие показатели, как нелинейность преобразований, сбалансированность криптографической функции, линейная сложность шифрующей последовательности. Автокорреляционная функция (АКФ) предоставляет возможность описания критериев безопасности через оценку вероятностных параметров.

Криптографический анализ проведён на примере алгебро-геометрического кода (32, 64), заданного кривой Эрмита в поле GF(16). Оценка АКФ указывает на близость исследуемых последовательностей к случайным. Значения компонент спектра Уолша-Адамара эквивалентных сопряжённых последовательностей кодированных векторов отражают уровень нелинейности (от 106 до 104 при верхней границе 120), что указывает на высокую степень удалённости последовательностей от линейных, а значит, высокую степень устойчивости к линейному криптоанализу. Значения нулевых компонент спектров имеют отклонения от нуля, что указывает на определенную несбалансированность структуры кода. Уровень линейной сложности шифрующих последовательностей оценён с помощью алгоритма Берлекемпа-Месси и составляет от 120 до 124, т.е. криптосистемы, использующие подобные последовательности, устойчивы к вскрытию, и криптоаналитик не может предсказать ни следующий, ни предыдущий бит последовательности.

МОНИТОРИНГ СИСТЕМЫ БЕЗОПАСНОСТИ СЕТИ 2G/3G (UMTS)

Д.Н. ПИСКУН

Системы связи UMTS требуют осуществления глобального роуминга, высокой скорости передачи информации и оказания электронных услуг различного вида. Все эти функции должны быть поддержаны системой защиты информации, одной из опций которой является анализ состояний мобильных станций и сетевой структуры.

Целью данной работы является разработка моделей и алгоритмов анализа состояния системы связи в режиме мониторинга зон покрытия, а также написание программного обеспечения системы защиты информации.

Библиотека БГУИР

Архитектура системы безопасности сетей связи 3G (UMTS) представляет собой многоуровневую структуру. Одной из неотъемлемых функций архитектуры является поддержка требований по наблюдаемости и конфигурируемости системы защиты информации на основе анализа состояний мобильный станций, оконечных мобильных устройств, каналов передачи, сетевой инфраструктуры. Априорное знание этих состояний, в сочетании с точными географическими параметрами (широта, высота, долгота), позволяют оценить степень конфиденциальности и произвести оценку целостности всей инфраструктуры сети. Перспективным инструментом анализа в этом отношении являются методы основанные на фрактальных вейвлетных моделях.

В данной работе предполагается использование программно-аппаратного комплекса базирующегося на высокотехнологичном радиоизмерительном оборудовании — модульной измерительной системе компании National Instruments, основанной на открытом промышленном стандарте PXI. для использования своих модульных измерительных систем, компания National Instruments предлагает использовать среду графического программирования NI LabVIEW. в состав NI LabVIEW входят специализированные модули для имитации и записи реального сигнала UMTS и измерения различных технических параметров сигнала.

КОДОВАЯ КОРРЕКЦИЯ СМЕЩЕНИЯ В ГЕНЕРАТОРАХ СЛУЧАЙНЫХ ЧИСЕЛ

С.Б. САЛОМАТИН, Т.А. АНДРИАНОВА

Основными элементами в инфраструктуре формирования ключевого пространства является генераторы случайных чисел. Одним из недостатков генераторов такого рода является возможность появления постоянного смещения e в распределениях случайных последовательностей чисел.

Для предотвращения появления смещения можно использовать метод кодовой коррекции работы генератора случайных чисел. Суть метода состоит в дополнительном кодировании данных, формируемых генератором случайных чисел.

Кодовые корректоры смещения можно разделить на два вида: линейные и нелинейные.

Линейный кодовый корректор отображает n бит входных данных в m бит выхода с величиной смещения $e/2$. Смещение любой ненулевой комбинации выходных бит будет не больше $e^d/2$, где d — минимальное кодовое расстояние линейного кода, задаваемого порождающей матрицей G.

Действие линейного корректора удобно описать с помощью (n, m, t)-устойчивой функции. Под (n, m, t)-устойчивой функцией будем понимать функцию, отображающую n битов входа в m битов выхода таким образом, что если t входных битов имеют фиксированные значения, то не происходит никаких изменений на выходе.

Нелинейный корректор отображает n бит в m бит. При этом ненулевая линейная комбинация выхода определяется как вектор булевой функции. Величина смещения может быть вычислена с помощью таблицы истинности. Используя преобразования Уолша, можно оценить смещение с помощью функции веса кода.

В качестве примера рассматривается применение кода БЧХ с параметрами (256, 21, 111) и дуального кода (256, 234, 6) с порождающим полиномом $h(x)$, имеющего степень 21 Вектор из 255 символов представляется в полиномиальном виде $m(x)$. Далее выполняется кодирование $m(x)$ mod $h(x)$. При этом происходит

Библиотека БГУИР