– 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.