ЗАЩИТА ИНФОРМАЦИИ НА ОСНОВЕ КОДИРОВАНИЯ УРОВНЕЙ ГИПЕРПОВЕРХНОСТИ ДУАЛЬНОЙ РЕШЕТКИ

С.Б. Саломатин, Т.А. Андриянова

Решетка L определяется как дискретная, имеющая базис, абелева подгруппа действительных или комплексных n-мерных векторных пространств V и базисом v. Каждая решетка имеет свою дуальную решетку с инверсным по отношению к v базисом u.

Вычислительные задачи теории решеток связаны:

– с нахождением наиболее короткого ненулевого вектора s в L (ShortestVectorProblem (SVP));

– нахождением вектора в решетки, наиболее близко расположенным к точке вне решетки (ClosestVectorProblem (CVP));

– нахождением аппроксимирующих векторов задач apprSVP и apprCVP.

Вектор s позволяет формировать различные уровни дуальной решетки, образовывая, так называемые, скрытые гиперповерхности H. Например, определяя дуальную решетку как множество y, скрытая гиперповерхность k-го уровня формируется как множество векторов y, удовлетворяющих равенству ys = k.

Алгоритм кодирования. Логический ноль кодируется случайной точкой, располагающейся между уровнями гиперповерхностей. Логическая единица кодируется случайной точкой в узле уровня дуальной решетки.

Алгоритм декодирования. Принятый вектор декодируется как логический ноль, если его проекция достаточно далека от решетки гиперповерхности. Принятый вектор декодируется как логическая единица, если его проекция распложена вблизи от гиперповерхности.

При неизвестном случайном k задача раскрытия системы становится трудно выполнимой, что позволяет классифицировать предлагаемую схему как вариант криптографической системы с открытым ключом — структурой решетки. Закрытым ключом может служить величина уровня k.

ОЦЕНКА ВНУТРИСИСТЕМНОЙ ЭМС В СЕТЯХ СОТОВОЙ СВЯЗИ СТАНДАРТА GSM ВНУТРИ ЗДАНИЙ

А.С. Свистунов

В связи с постоянным ростом территориальной плотности базовых станций (БС) сотовой связи, а также использованием завышенных уровней электромагнитных излучений БС большой интерес представляет вопрос о состоянии внутрисистемной электромагнитной совместимости (ЭМС) сотовых радиосетей и о связи уровня внутрисистемных помех в этих сетях с их безопасностью для населения.

Оценки внутрисистемной ЭМС выполнены на основе имитационного моделирования фрагмента сети сотовой связи стандарта GSM с использованием модели городской застройки при размещении абонентских станций (АС) внутри зданий на разных этажах и многолучевой модели распространения радиоволн. Принято, что уровень внутрисистемной ЭМС определяется значением отношения «сигнал/(помеха+шум)» (*SNIR*) на входе приемника АС. Использованы сценарии, в которых реализована трехсекторная структура сайтов сети при различной размерности *N* кластера частотного планирования.

При частотно-территориальном планировании сотовой сети с размерностью кластера $N = 4$, и высотах подвеса антенн БС, соизмеримых с высотой городской застройки, относительное количество АС, для которых условия внутрисистемной ЭМС неудовлетворительны ($SNIR \le 9$ дБ), достигает 10…25%. При увеличении размерности кластера до $N = 7$ данное относительное количество АС снижается до 2…4%. Снижение эквивалентной изотропной излучаемой мощности БС с 53 дБм до 43 дБм не приводит к существенному росту данного относительного количества АС. Изменение высот подвеса антенн БС неоднозначно влияет на внутрисистемную ЭМС: увеличение высот подвеса антенн БС улучшает внутрисистемную ЭМС нижних этажах зданий, но сопровождается ее очевидным ухудшением на верхних этажах. Поэтому высоты подвеса антенн БС являются параметром, подлежащим оптимизации в конкретных условиях.

Таким образом, можно утверждать, что качество связи определяется только уровнем внутрисистемной ЭМС, фактически определяемым уровнем внутрисетевых помех и распределением значений *SNIR* на входе множества АС сети, а также за счет оптимизации сети, динамического перераспределения радиочастотного ресурса между БС в различное время суток и т.п. На территории городской застройки использование уровней ЭИИМ БС выше 43–45 дБм нецелесообразно, поскольку

данная мера не приводит к заметному улучшению качества связи, но может быть причиной повышенной интенсивности электромагнитного фона в местах с высокой плотностью населения, что является небезопасным с точки зрения электромагнитной безопасности.

ПОРОГОВАЯ СХЕМА ЦИФРОВОЙ ПОДПИСИ НА ЭЛЛИПТИЧЕСКИХ КРИВЫХ С РАЗДЕЛЕННЫМ СЕКРЕТОМ

О.А. Селеня, С.Б. Саломатин

Защита с помощью использования пороговой электронно-цифровой подписи с разделенным секретом включает в себя задачи разделения доступа, подтверждения авторства, контроль целостности, конфиденциальность, обеспечение юридической значимости электронного документа.

Существует большое количество схем ЭЦП на основе разделения секрета, одна из них приведена в [1]. В ходе анализа этой схемы было выявлено, что возникают проблемы при использовании описанного алгоритма для нечетного числа участников так как количество долей в ключевом наборе является четным, а следовательно при собирании общей подписи одной доли либо будет недоставать, либо она будет дублироваться, что приведет к неправильному значению общей подписи. Наборы, отсылаемые одному участнику, содержат все разделенные доли секрета, что снижает надежность алгоритма. Кроме того, по этой схеме генерируются и отсылаются каждому участнику наборы для каждого порога, что увеличивает размер хранимой информации на стороне клиентов и сервера. В модифицированном алгоритме эти недостатки устраняются путем генерации количества наборов равного количеству участников. При этом для работы с порогами выше минимального не требуется вычислять свои наборы, достаточно сгенерированных наборов для минимального порога.

Литература

1. *Джунковский П.О., Дитенкова А.С.* Пороговая схема цифровой подписи с разделенным секретом на базе ГОСТ Р 34.10-2001. Журнал «Безопасность информационных технологий». Выпуск №3, 2010.

ОБ ИСПОЛЬЗОВАНИИ ХАОТИЧЕСКИХ ОТОБРАЖЕНИЙ ПРИ ФОРМИРОВАНИИ ХРУПКИХ ЦИФРОВЫХ ВОДЯНЫХ ЗНАКОВ

А.В. Сидоренко, И.В. Шакинко

Значительные достижения в области мультимедиа и веб-технологий за последнее время привели к широкому распространению изображений в цифровом виде. При этом возникает необходимость в решении задач, связанных с аутентификацией цифровых изображений [1]. Для решения данных задач применяется метод, связанный с хрупкими цифровыми водяными знаками. Хрупкие цифровые водяные знаки используются для выявления изменений в изображении при его передаче [2].

В данной работе при формировании хрупких цифровых водяных знаков применяются хаотические отображения. На каждой итерации значения интенсивности элементов передаваемого изображения добавляются к значениям параметров с учетом переменных выбранного отображения. При этом через некоторое количество итераций выявляются существенные отличия в значениях переменных отображения.

Нами предложена схема встраивания хрупких цифровых водяных знаков в изображения. Проведенное тестирование этой схемы подтверждает способность выявления искажений, возникающих при передаче по каналу связи. Полученные данные свидетельствуют о возможности использования предлагаемой схемы встраивания хрупких цифровых водяных знаков при решении задач, связанных с аутентификацией.

Литература

1. Sidiropoulos P. Invertible chaotic fragile watermarking for robust image authentication / P. Sidiropoulos, N. Nikolaidis, I. Pitas // Chaos, Solitons and Fractals. 2009. Vol. 42. P. 2667–2674.

2. Vartak R. Survey of Digital Image Authentication Techniques / R. Vartak, S. Deshmukh // International Journal of Research in Advent Technology. 2014. Vol. 2, № 7. P. 176–179.