УДК 519.688

Самохина М.А [1]

[1] Московский физико-технический институт

Использование модифицированной криптосистемы Нидеррайтера при передачи и для защиты меняющихся изображений

На сегодняшний день существует большое количество программного обеспечения и интегрированных систем, обеспечивающих организацию видеоконференций между двумя и более абонентами по сети передачи данных. Передача потока звука и видео по сети передачи данных обеспечивается путем кодирования/декодирования аудио и видео потока с использованием стандартизованных аудио- и видео-кодеков. Одной из основных задач таких систем является помехоустойчивое кодирование. Зачастую при организации видеоконференций возникает также необходимость защиты передаваемых данных.

Для защиты передаваемого потока звука и видео предлагается использовать новую модификацию криптосистемы Нидеррайтера основанную на ранговых кодах [1]. Новая криптосистема строится по принципу системы Нидеррайтера [2] со следующими изменениями. Во-первых, зашумляется проверочная матрица кода, для этого вводится скрывающая матрицы. В качестве скрывающей матрицы может быть выбрана матрица единичного ранга [3]. Но более стойкой система будет при использовании скрывающей матрицы ранга, значительно большего единицы [4]. Во-вторых, используются различные метрик, отличных от классической хэммингова метрики. Заключительным этапом является построение кодов с набором специфических свойств.

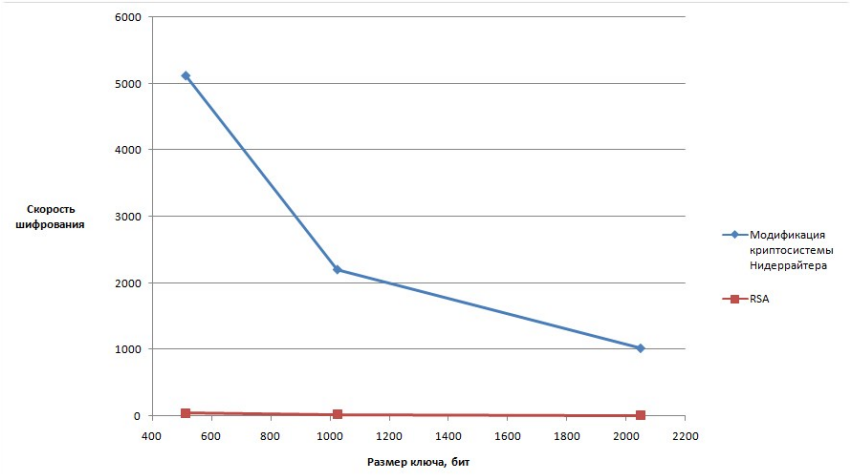

Рис. 1. Зависимость скорости шифрования от размера ключа криптосистемы для модифицированной системы Нидеррайтера.

На рисунке 1 приведена зависимость скорости шифрования от размера ключа криптосистемы для предлагаемой модифиции системы Нидеррайтера, основанной на матрице Фробениуса. Также на графике представлены данные для криптосистемы RSA для нешумящего канала. Из графика видно, что предлагаемая криптосистемы оказывается быстрее, чем криптосистема RSA. Также данное сравнение не корректно для случая шумящего канала, так как для использования RSA в шумящем канале необходимо производить кодирование с вероятностью ошибки в бите не более 10^{-8}.

К предлогаемой новой модификации криптосистемы Нидеррайтера применимы два основных вида атак: прямые и структурные атаки. Под прямыми атаками понимаются перебор по искусственным ошибкам, перебор по сообщениям, декодирование опубликованного кода как случайного. Среди структурных атак стоит выделить различные модификации атаки Гибсона, адаптированные к модификациям криптосистемы, а также варианты атаки Сидельникова-Шестакова [5]. Опираясь на результаты криптоанализа проведенного в [6], можно выделить основные условия для параметров криптосистемы, основанной на матрице Фробениуса, так, чтобы она могла считаться стойкой. При выборе (48, 24)-кода над полем $GF(2^{16})$, размер открытого ключа будет составлять 1 Kb, а вычислительная сложность приведенной атаки составит порядка 2^{140}. При различных параметрах криптосистемы стойкость криптосистемы будет варьироваться в зависимости от частоты передаваемых изображений. На рисунке 2 приведен график зависимости стойкости от поддерживаемой частоты смены кадров при размере кадров соответствующих возможностям сотового телефона SonyEricsson W900.

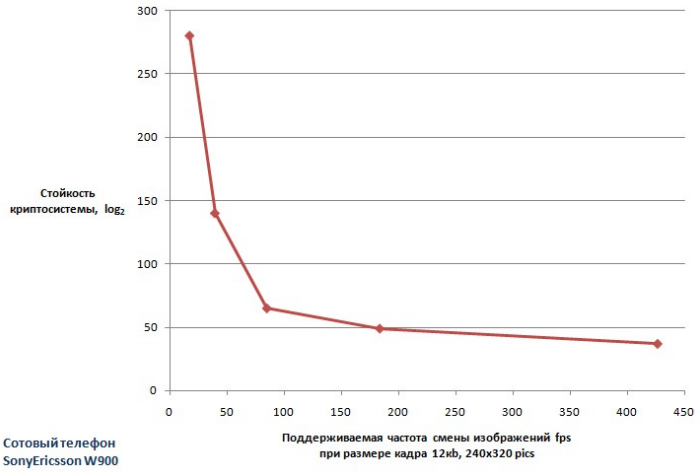

Рис. 2. Зависимость стойкости от поддерживаемой частоты смены кадров (для SonyEricsson W900)

Применение данной модификации криптосистемы Нидеррайтера также позволяет не только защищать данные от несанкционированного доступа, но и обеспечивать помехоустойчивое кодирование. Чтобы гарантировать коррекцию ошибок канала,

необходимо наложить дополнительные ограничения на выбор матриц в модуле инициализации (подробнее в [7]). Недостаток интегрированной системы заключается в том, что исправление ошибок канала вносит дополнительные ограничения на выбор параметров, что приводит к снижению криптостойкости части системы, отвечающей за шифрование. В этом случае, для повышения стойкости к атакам следует выбирать бОльшие размерности, а это в свою очередь влечет к снижению скорости интегрированной системы и увеличению ключей криптосистемы. Что касается снижения скорости, то оно не очень существенно и намного меньше уменьшения скорости при использовании двух различных систем.

СПИСОК ЛИТЕРАТУРЫ

1. *Чурусова М.А., Габидулин Э.М*. Модификация криптосистемы Нидеррайтера, основанная на новой метрике. — Научный вестник Московского государственного института радиотехники, электроники и автоматики, Москва, Январь, 2005, Стр. 27-29.
2. *Niederreiter H.* Knapsack-Type Cryptosystem and Algebraic Coding Theory. — Probl. Control and Inform. Theory, 1986. . — Vol. 15 . — P. 19-34.
3. *Gabidulin E., Ourivski A., Pavlouchkov V*. On the modified Niederreiter cryptosystem. — Proc. Information Theory and Networking Workshop. — Metsovo - Greece, 1999. - P. 50.
4. *Габидулин Э.М., Обернихин В.А*. Коды в F-метрике Вандермонда и их применение. — Proc. Eighth Int. Workshop on Algebraic and Combinatorial Coding Theory. — Tsarskoe Selo - M. 2002. - P. 124-127.
5. *Сидельников В.М. Шестаков С.О*. О системе шифрования, основанной на обощенных кодах Рида-Соломона. — Москва: Дискретная математика. 1992. - Т. 3. Вып. 3.
6. *Самохина М.А*. Криптоанализ систем, основанных на линейных кодах. — Проблемы информационной безопасности. Компьютерные системы. Ежеквартальный журнал издательства СПбГПУ под редакцией проф. Зегжды П.Д. — Санкт-Петербург 2008. – Стр. 94-103.
7. *Самохина М.А*. Применение модификаций криптосистем Нидеррайтера в системах исправления ошибок и защиты от несанкционированного доступа. — Моделирование и обработка информации. Сборник научных трудов . — Москва 2008. - Стр.127-136.