УДК 519.688

М.А. Самохина
Московский физико-технический институт (государственный университет)

Модификации криптосистемы Нидеррайтера, их стойкость и практические применения

В работе рассмотрены различные подходы к модификации классической криптосистемы Нидеррайтера. Проанализированы наиболее успешные варианты атаки на такого рода системы. Представлены результаты практического использования модификации криптосистемы Нидеррайтера, основанной на матрице фробениусовского вида.

Ключевые слова: криптография, криптология, криптоанализ, криптосистемы с открытым ключом, криптосистема Нидеррайтера, криптосистемы, основанные на линейных кодах, помехоустойчивое кодирование, системы исправления ошибок, моделирование.

В теории криптосистем с открытым ключом известны два основных типа систем, основанных на линейных кодах. Это система Мак Элиса (McElice) [1] и система Нидеррайтера [2]. Эта статья посвящена системе Нидеррайтера и её модификациям.

Идея системы Нидеррайтера состоит в следующем. В качестве секретных ключей выбираются:

— проверочная матрица $H = [z_j x_j^i]$, где $i = 0, 1, ..., r-1$; $\quad j = 1, 2, ..., n$, некоторого обобщённого кода Рида–Соломона над полем $GF(q)$;

— случайно выбранная невырожденная скремблирующая матрица S порядка r над полем $GF(q)$. Эта матрица вводится для того, чтобы скрыть от криптоаналитика видимые закономерности, разрушая структуру проверочной матрицы.

Открытым ключом в данном случае будет скремблированная проверочная матрица $H_{cr} = SH$.

Сообщениями являются все n-векторы с координатами из поля $GF(q)$ с весом, не превосходящим $\frac{r}{2}$. Здесь сообщения не являются кодовыми словами выбранного кода Рида–Соломона, а представляют собой всевозможные ошибки, которые этот код в состоянии исправлять.

Шифртекст, соответствующий сообщению m, является r-вектором и вычисляется следующим образом:

$$c = mH_{cr}^T = mH^T S^T.$$

Законный пользователь после приёма шифртекста c умножает его справа на матрицу $(S^T)^{-1}$, а затем применяет известный лишь ему алгоритм быстрого декодирования и получает переданное сообщение m.

Описанная криптосистема оказалась нестойкой и была взломана Сидельниковым и Шестаковым. Авторам удалось угадать структуру закрытого ключа по открытому ключу и подобрать такие матрицы $\tilde{H}$ и $\tilde{S}$, что $H_{cr} = \tilde{S}\tilde{H}$ [3].

В последующие годы неоднократно предпринимались попытки модифицировать классическую криптосистему Нидеррайтера так, чтобы повысить её криптостойкость. На сегодняшний день существует несколько модификаций криптосистемы, среди которых можно выделить три основных подхода. Во-первых, зашумляется проверочная матрица кода при помощи введения скрывающей матрицы. Например, в работе [4] в качестве скрывающей матрицы была предложена матрица единичного ранга. В работе [5] использовались скрывающие матрицы ранга, значительно большего единицы. Во-вторых, используются различные метрики, отличные от классической хэмминговой метрики. Примером такой метрики может служить ранговая [6] метрика. В-третьих, строятся коды с набором специфических свойств.

Довольно успешным является сочетание сразу двух или более из описанных выше способов модификаций. Комбинация описанных способов модификаций бы-

ла предложена авторами [7]. В данном случае построена метрика на основе матрицы Фробениуса, а шифртекст имеет вид: $mH_{pub} = mS(F + G^T U)P$. Основная идея модификации заключается в скрытии структуры закрытого ключа. Это делается для того, чтобы избежать структурных атак, подобных атакам Сидельникова–Шестакова. Структура закрытого ключа усложняется так, чтобы синдром родительского кода выступал в роли искусственно созданной ошибки нового кода в новой метрике. При этом структура шифртекста представляет собой сумму векторов $g + e$, умноженную на шумовую матрицу. Для расшифрования легальному пользователю необходимо сначала найти вектор ошибки, применив алгоритм быстрого декодирования некоего нового кода, который является синдромом родительского кода. А затем уже применить алгоритм быстрого декодирования в родительском коде, получая в результате открытый текст.

Рассмотрим подробнее криптосистему, использующую метрику, основанную на матрице Фробениуса. Модификация заключается в ведении новой метрики, дополнительном зашумлении открытого ключа и использовании ранговых кодов. Для построения новой метрики выбирается матрица F размером $N \times n$ с элементами из поля $GF(q^N)$ такая, что $n < N$ и ранг матрицы F меньше n. Элементы матрицы выбираются из поля $GF(q^N)$ и должны быть линейно независимыми над базовым полем, а сама матрица F имеет следующий вид:

$$F = \begin{pmatrix} h_1 & h_1^q & \dots & h_1^{q^{n-1}} \\ h_2 & h_2^q & \dots & h_2^{q^{n-1}} \\ \vdots & \vdots & \dots & \vdots \\ h_{N_1} & h_{N_1}^q & \dots & h_{N_1}^{q^{n-1}} \end{pmatrix}.$$

Обозначим h_1, h_2, ..., h_N строки матрицы F. Для любого ненулевого вектора x из пространства $GF(q^N)^n$ его норма определяется как минимальное число ненулевых коэффициентов a_i в разложении:

$$x = \sum_{i=1}^{n} a_i h_i.$$

Построение криптосистемы начинается с выбора матрицы рангового кода F. Эта матрица задает новую метрику. Затем выбирается порождающая матрица G_k таким образом, чтобы код, порожденный матрицей G_k, являлся оптимальным кодом и мог исправлять ошибки в новой метрике:

$$G_k = \begin{pmatrix} g_1 & g_1^q & \dots & g_1^{q^{n-1}} \\ g_2 & g_2^q & \dots & g_2^{q^{n-1}} \\ \vdots & \vdots & \dots & \vdots \\ g_k & g_k^q & \dots & g_k^{q^{n-1}} \end{pmatrix}.$$

Для построенного таким способом кода существует алгоритм быстрого декодирования. Заключительным этапом является выбор невырожденной скремблирующей матрицы S с элементами из $GF(q^N)$ и невырожденной матрицы P с элементами из базового поля.

Секретный ключ модифицированной криптосистемы представляет собой набор матриц $(\ F \quad G_k \quad S \quad P\ )$.

Открытый ключ представляет собой матрицу $H_{pub} = P(F + UG_k)S$, где U — некоторая случайная матрица. Кодовыми векторами являются строки матрицы UG_k. Матрица U не нужна при расшифровании, но для криптоаналитика она должна быть недоступной.

Текст сообщения представляет собой N_1-мерный вектор $m = (\ m_1 \quad m_2 \quad \dots \quad m_{N_1}\ )$ такой, что $d_H(m) = t_{\min} = \min(\ t_k \quad t_p\ )$, где t_k — корректирующая способность кода, задаваемого матрицей G_k в пространстве с новой метрикой, t_p — корректирующая способность родительского кода. Число сообщений равно.

Шифртекст вычисляется как синдром:

$$s = mH_{pub} =$$
$$= mP(F + UG_k)S = \tilde{m}(F + UG_k)S,$$
$$s = (m_1(F_1 + G_{k_1}) + m_2(F_2 + G_{k_2}) + \dots +$$
$$+ \dots + m_{N_1}(F_{N_1} + G_{k_{N1}}))S = (g + e)S,$$

где $\tilde{m} = mP$, F_i и G_i — строки матриц $F \cup G$ соответственно.

Расшифрование: легальный пользователь умножает полученный шифртекст $(g + e)S$ на S^{-1}. Затем применяет алгоритм быстрого декодирования в новой метрике. В результате пользователь получит векторы g и e. После применения алгоритма быстрого декодирования родительского кода легальный пользователь получит вектор $\tilde{m}$. После умножения $\tilde{m}$ на матрицу P^{-1} получим открытый текст m.

К предлагаемой новой модификации криптосистемы Нидеррайтера применимы два основных вида атак: прямые и структурные. 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 [3]. При оценке трудоёмкости каждой из атак необходимо учитывать размер открытого ключа. Как правило, размер ключа выбирается с учётом требований, предъявляющихся сегодня на практике к ассиметричным криптосистемам.

Криптоанализ рассматриваемого класса криптосистем сводится к двум основным этапам. Во-первых, нахождение вектора-ошибки, который необходим для исправления ошибки в новой метрике. Во-вторых, вычисление открытого текста по синдрому.

Что касается первого пункта, то для него необходимо выполнить ряд трудоемких операций. Второй этап менее ресурсоемкий и частично реализован на примере атаки Сидельникова–Шестакова, тем не менее вторая часть атаки бессмысленна без прохождения первого этапа.

Задача нахождения вектор-ошибки e сводится к декодированию некоторого линейного (n,k,d)-кода C над полем $GF(q^N)$ наименьшей нормы d_F в построенной метрике. Поставленную задачу можно переформулировать следующим образом: по заданной порождающей матрице G кода C и с помощью вектора c длины n найти k — вектор m такой, что вектор-ошибка $e = c - mG$ имеет наименьшую возможную норму в ассоциированной метрике.

Декодирование кода C в пределах его корректирующей способности может быть сведено к поиску вектора, имеющего минимальную норму в некотором другом коде, включающем C как подкод. Процедура в конечном счете сводится к решению параметрической системы линейных уравнений. Подробное описание такого способа приведено в [8].

Общая сложность наиболее трудоемкой части процесса декодирования составляет порядка $O\left((Nr)^3 q^{(r-1)(k+1)+2}\right)$. Количество неизвестных в решаемой системе составляет: $(k+m+1)+N(r-1)$. Значит, для разрешимости системы необходимо, чтобы $(k+m+1)+N(r-1) \leqslant mN$. Например, для (24,12)-кода над полем $GF(2^{12})$, который может исправлять ошибки ранга вплоть до 3, сложность декодирования составит 2^{52}.

Опираясь на результаты проведённого криптоанализа, 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 приведённой атаки составит порядка 2^{140}. Из описанного примера видно, что для ключа в 1 Kb (на сегодняшний день такой размер ключа используется во многих стандартных асимметричных) количество операций рассматриваемой структурной атаки велико.

Таким образом, для использования в случае, когда необходима высокая криптостойкость, можно рекомендовать выбирать параметры так, чтобы размер открытого ключа был порядка 1024 бит.

Одной из положительных особенностей данной криптосистемы является возможность её использования в качестве системы исправления ошибок канала. Криптосистема основана на ранговых кодах, успешно применяющихся при помехоустойчивом кодировании, свойства которых можно использовать при возникновении ошибок в канале при передаче сообщений.

При постановке задачи создания интегрированной системы исправления ошибок канала с системой защиты информации от несанкционированного доступа рассматриваемая модификация криптосистемы Нидеррайтера подходит как нельзя лучше.

Предположим, что при передаче зашифрованного сообщения в криптосистеме возникают различного рода помехи, это приводит к искажению кодового слова. В случае, когда присутствует ошибка канала $\tilde{e}$, совпадающая с одним из базисных векторов, она имеет в новой метрике норму, равную 1. Если искусственная ошибка e имеет норму $t = (d-3)/2$, тогда система может исправлять также и ошибки канала.

Чтобы гарантировать коррекцию ошибок канала, необходимо наложить дополнительные ограничения на выбор матриц в модуле инициализации. Для исправления ошибок канала в любом случае мы должны иметь представление о характере ошибок. Следует собрать статистику и, предварительно проанализировав ее, сделать вывод о характере ошибок и модификации криптосистемы с целью их исправления. В базовом поле шифртекст представляет собой матрицу с элементами из $GF(q)$:

$$C = \begin{pmatrix} c_{11} & \dots & c_{1n} \\ \vdots & \ddots & \vdots \\ c_{N1} & \dots & c_{Nn} \end{pmatrix}.$$

Элементы матрицы C имеют вид

$$c_{ij} = [s_{ij}\,(g_1 u_{1i} + \dots + g_k u_{ki} + h_i) + \dots +$$

$$+ \dots + s_{jj}(g_1^{q^{j-1}} u_{1i} + \dots + g_k^{q^{j-1}} u_{ki} + h_i^{q^{j-1}})]m_j.$$

Пусть приёмник получил шифртекст, искажённый ошибкой, в виде: $g + e + \tilde{e}$. Не стоит забывать, что в таких случаях для того, чтобы гарантировать коррекцию ошибок канала, необходимо наложить дополнительные ограничения на выбор матрицы из Q. В работе [9] рассматриваются различные виды ошибок и способы их исправления в предлагаемой системе.

Для исправления любой ошибки вида $(e + \tilde{e})$ требуется, чтобы норма искусственной ошибки удовлетворяла условию

$$t \leqslant \frac{d - 2n - 1}{2}.$$

В свою очередь последнее условие накладывает ограничение на количество матриц Q, что со своей стороны может привести к ухудшению криптосистемы с точки зрения криптостойкости. Поэтому для определения параметров криптосистемы сначала необходимо точно определить характеристики канала.

Применение такой интегрированной системы оправдано в случае передачи видеоизображения. Например, при видеоконференциях зачастую требуется не только система, обеспечивающая помехоустойчивое кодирование, но и криптосистема для защиты видеопотока от несанкционированного доступа.

В традиционном плёночном кинематографе используется частота 24 кадра в секунду. Системы телевидения PAL и SECAM используют 25 кадров в секунду, а система NTSC использует 29,97 кадров в секунду. Оцифрованные видеоматериалы хорошего качества, как правило, используют частоту 30 кадров в секунду. Верхняя пороговая частота мелькания, воспринимаемая человеческим мозгом, в среднем составляет 39–42 Гц и индивидуальна для каждого человека. Некоторые современные профессиональные камеры могут снимать с частотой до 120 кадров в секунду. А специальные камеры для сверхбыстрой съёмки снимают с частотой до 1000 кадров в секунду и выше, что необходимо, например, для детального изучения траектории полёта пули или структуры взрыва. Все же наибольшее распространение на сегодняшний день получила частота 25 кадров в секунду.

На рис. 1 приведён график зависимости стойкости криптосистемы от поддерживаемой частоты смены кадров, соответствующих возможностям сотового телефона SonyEricsson W900.

В случае передачи видеоизображения повышенного качества HDTV, кадр размером 1920×1080 пикселей, частота смены изображений поддерживаемой системой сокращается, тем не менее она намного превышает возможную скорость при использовании в случае канала без шума криптосистемы RSA. Из графика (рис. 2) видно, что предлагаемая криптосистема оказывается быстрее и в случае передачи изображений повышенного качества HDTV.

Данное сравнение не совсем корректно для шумящего канала, так как для использования RSA в шумящем канале необходимо производить кодирование с вероятностью ошибки в бите не более 10^{-8}. Таким образом, получаем дополнительное ограничение на использование криптосистемы RSA, и использование стандартной реализации алгоритма становится невозможным. Это приводит к дополнительным трудностям, для решения которых необходимы слишком ресурсоёмкие затраты. В результате кроме превосходства по скоростям использование новой предлагаемой модификации криптосистемы Нидеррайтера не требует дополнительных затрат как со стороны разработки ПО, так и в плане увеличения вычислительных мощностей используемого аппаратного комплекса.

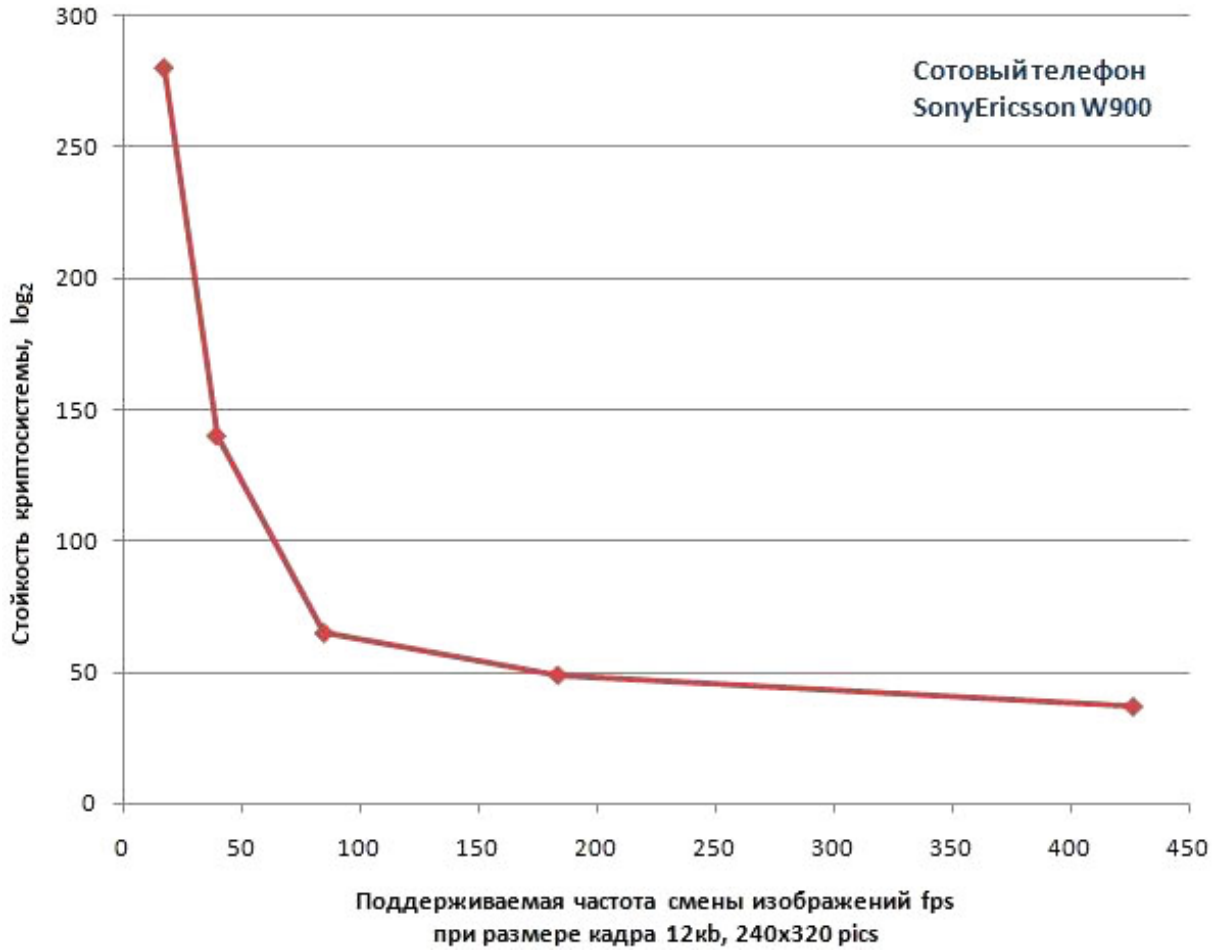


Рис. 1. Зависимость стойкости криптосистемы Нидеррайтера от поддерживаемой частоты смены кадров, соответствующих возможностям сотового телефона SonyEricsson W900

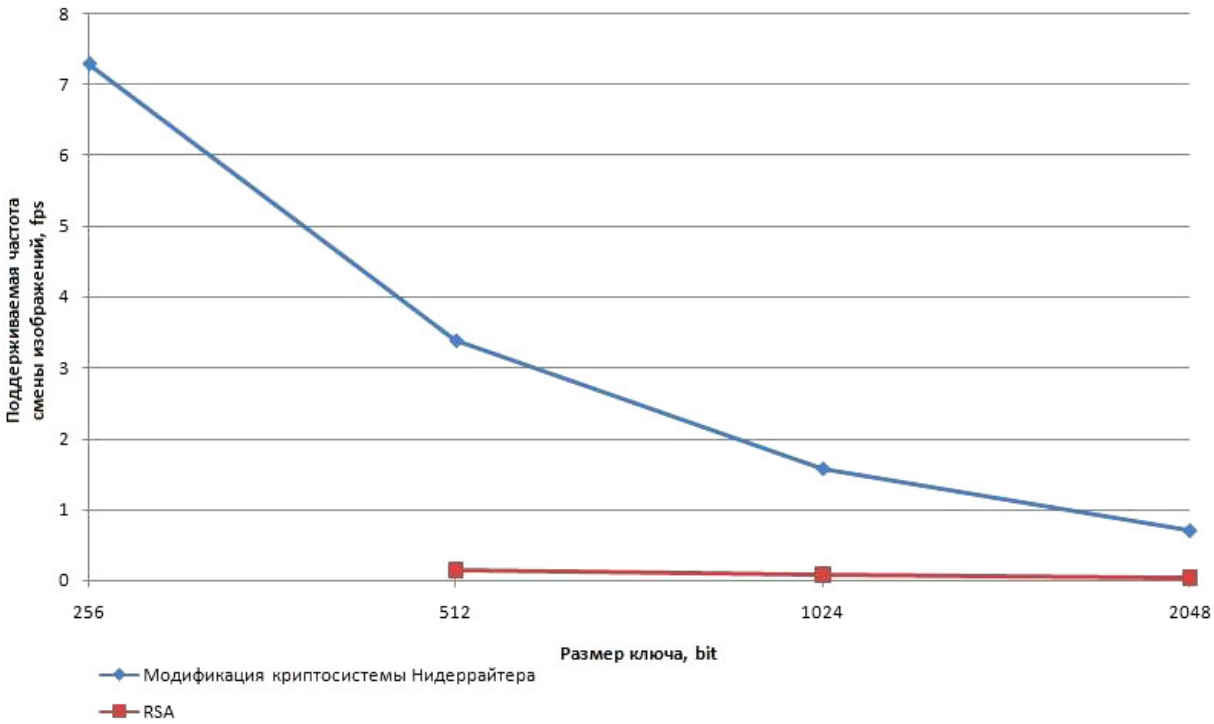
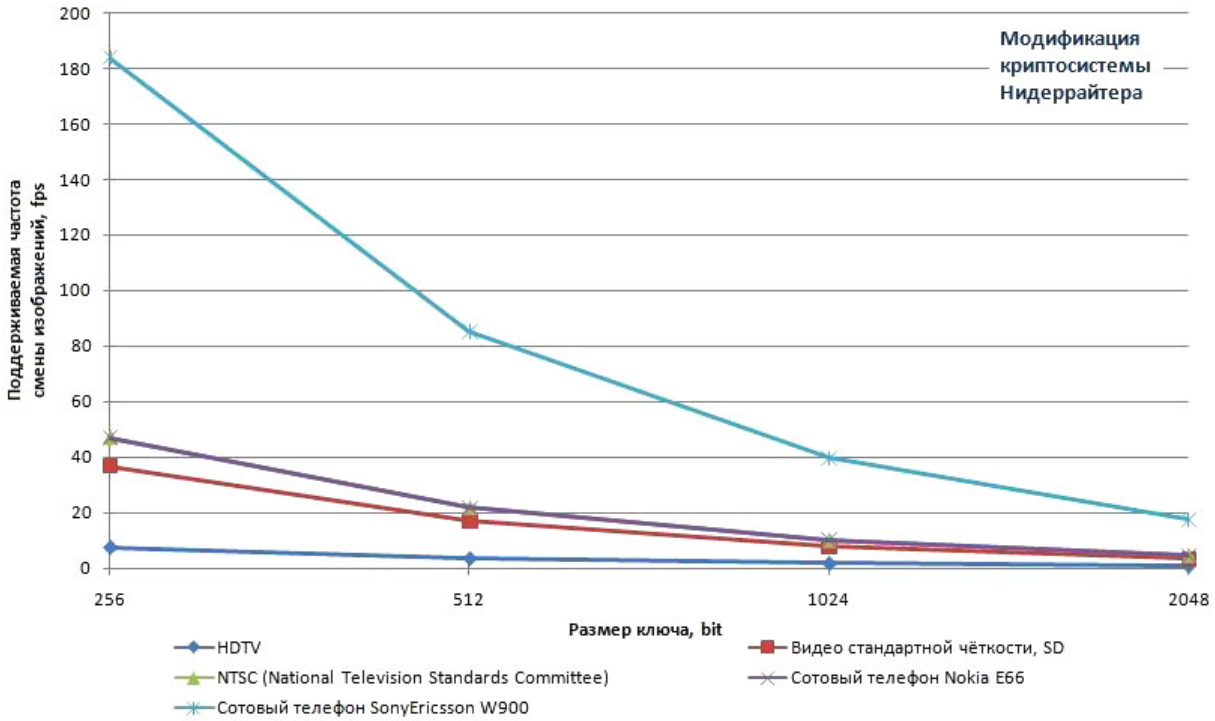


Рис. 2. Сравнение использования криптосистем для нешумящего канала в случае передачи изображений повышенного качества HDTV

На рис. 3 приведена серия графиков зависимости поддерживаемой частоты смены кадров от размера ключа при размере кадров, соответствующих различным качествам передаваемого изображения.



Стандарты	Размер кадра, pics
HDTV	1920×1080
Видео стандартной чёткости, SD	720x576
NTSC (National Television Standards Committee)	648×486
Сотовый телефон Nokia E66	640 x 480
Сотовый телефон SonyEricsson W900	240x320

Рис. 3. Зависимость поддерживаемой частоты смены кадров от размера ключа

Рассмотрим теперь объединение систем, которые решают задачи исправления ошибок и шифрования по отдельности. При передаче информации по любому физическому каналу возникают ошибки передачи независимо от того, передаются открытые или зашифрованные данные. Практически в любом случае возникает потребность в использовании систем, исправляющих ошибки канала. На практике наиболее часто применяют две различные системы: одну для исправления ошибок, другую — для защиты информации от несанкционированного доступа. При этом возникает много дополнительных проблем, которые нужно решать. Одной из них является согласование типов данных, с которыми оперируют каждая из систем. Необходимо заново реализовывать уже существующие системы криптозащиты и систему исправления ошибок или же включать дополнительные модули, обеспечивающие согласование передаваемых данных. В обоих случаях требуются дополнительные затраты на разработку модулей системы. Работоспособность полученной системы будет также зависеть от сред, где разрабатывались модули системы. Существует большое количество систем, комбинация которых практически невозможна из-за особенностей, связанных с их архитектурой.

Другой проблемой является согласование обработки нештатных ситуаций, возникающих при исправлении ошибок. В этом случае криптосистема не должна получать в качестве шифртекста искажённое сообщение, в противном случае результат расшифрования заведомо будет не совпадать с открытым текстом. В случае, когда система исправления ошибок сработала некорректно, возможны следующие варианты:

1) ошибка была исправлена неверно;

2) ошибка не была обнаружена;

3) система выдала отказ при обработке и т. п.

Во всех случаях при несогласованных взаимодействиях модулей системы будут происходить потери производительности или даже отказы системы.

В случае использования интегрированной системы исправления ошибок и защиты от нелегального доступа такого рода проблем не возникнет. Это является одним из преимуществ рассматриваемой интегрированной системы по сравнению с традиционным подходом использования раздельно помехо- и криптозащиты.

Указанное преимущество интегрированной системы достигается потерей некоторой качественной характеристики: исправление ошибок канала вносит дополнительные ограничения на выбор параметров, что приводит к снижению криптостойкости части системы, отвечающей за шифрование. В таком случае для повышения стойкости к атакам следует выбирать большие размерности, а это в свою очередь влечет к снижению скорости и увеличению размера ключей. Что касается снижения скорости, то оно не очень существенно: намного меньше уменьшения скорости при использовании стандартных криптосистем с открытым ключом.

Литература

1. *McElice R.J.* A Public Key Cryptosystem Based on Algebraic Coding Theory // DSN Progress Report 42–44. — Pasadena, CA: Jet Propulsion Lab, 1978. — P. 114–116.

2. *Niederreiter H.* Knapsack-Type Cryptosystem and Algebraic Coding Theory // Probl. Control and Inform. Theory. — 1986. — V. 15. — P. 19–34.

3. *Сидельников В.М., Шестаков С.О.* О системе шифрования, основанной на обощенных кодах Рида–Соломона // Дискретная математика. — 1992. — Т. 3, вып. 3.

4. *Gabidulin E., Ourivski A., Pavlouchkov V.* On the modified Niederreiter cryptosystem // Proc. Information Theory and Networking Workshop. — Metsovo, Greece, 1999. — P. 50.

5. *Габидулин Э.М., Обернихин В.А.* Коды в F-метрике Вандермонда и их применение. — Долгопрудный: МФТИ, 2005.

6. *Габидулин Э.М.* Теория кодов с максимальным ранговым расстоянием // Проблемы передачи информации. — 1985. — Т. XXI, № 1.

7. *Чурусова М.А., Габидулин Э.М.* Модификация криптосистемы Нидеррайтера, основанная на новой метрике // Теоретические вопросы вычислительной техники, программного обеспечения и информационных технологий в муниципальном хозяйстве. Межвузовский сборник научных трудов. — М.: МИРЭА, 2005. — С. 21–25.

8. *Самохина М.А.* Криптоанализ систем, основанных на линейных кодах // Проблемы информационной безопасности. Компьютерные системы. — СПб., 2008. — С. 94–103.

9. *Самохина М.А.* Применение модификаций криптосистем Нидеррайтера в системах исправления ошибок и защиты от несанкционированного доступа // Моделирование и обработка информации. Сборник научных трудов. — М., 2008. — С. 127–136.

Поступила в редакцию 13.10.2008.