- возможность обработки сообщений произвольной длины;
- использование одного ключа шифрования.

Большинство известных альтернативных схем используют 2 или 3 ключа шифрования, что является существенным недостатком.

Из известных режимов один ключ используется в OMAC, при этом обеспечивается защита механизма дополнения сообщения, чья длина не кратна размеру блока.

Лучшая атака на OMAC является атакой с выбранными открытыми текстами, когда криптоаналитик выполняет статистический поиск коллизии ($2^{n/2}$ шифрований, где n – размер блока), т.е. фактически теоретический максимум стойкости.

Схема является стойкой, имеет низкую вычислительную сложность, простая в реализации и удобная в использовании.

Таким образом, при использовании предложенных подходов перспективный алгоритм шифрования будет иметь высокий уровень криптографической стойкости и статистической безопасности, обладать высоким уровнем производительности, вместе с тем обеспечивая простоту программной и аппаратной реализации. Полученные показатели стойкости и производительности перспективного шифра позволяют рекомендовать его в качестве замены действующему стандарту ГОСТ 28147-89 [14].

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. NESSIE Call for Cryptographic Primitives, Version 2.2, 8th March 2000: http://cryptonessie.org.

2. AES discussion forum: http://aes.nist.gov.

3. New European Schemes for Signatures, Integrity, and Encryption NESSIE: http://cryptonessie.org.

4. Final report of European project number IST-1999-12324, named New European Schemes for Signatures, Integrity, and Encryption. Springer-Verlag, Berlin Heidelberg NewYork, etc. 2004, 5. NESSIE public report D20. NESSIE Security Report. http://cryptonessie.org.

6. http://cryptrec.org/ Cryptography Research and Evaluation Committees.

7. *Daemen, J. Rijmen V.* «AES Proposal: Rijndael», AES Round 1 Technical Evaluation CD-1: Documentation, National Institute of Standards and Technology, Aug 1998. http://www.nist.gov/aes.

8. Camelli http://info.isl.ntt.co.jp /crypt /camellia /index.html.

9. National Institute of Standards and Technology, FIPS–197: "Advanced Encryption Standard." Nov. 2001. http://www.nist.gov/aes.

10. *Daemen J. and Rijmen V.*, "AES proposal: Rijndael".http://www.nist.gov/aes.

11. *Courtois N.T., Pieprzyk J.*, Cryptanalysis of block ciphers with overdefined systems of equations. Proceedings of Asiacrypt'02, LNCS. Springer-Verlag, 2002.

12. *Nakahara J. Jr.* Key-Shedule Analysis of AES Candidates //Katholieke Universiteit Leuven, 1999.– P. 143.

13. FIPS 81. DES modes of operation. Federal Information Processing Standards Publication 81, U.S. Department of Commerce / National Bureau of Standards, National Technical Information Service, Springfield, Virginia, 1980.

14. ГОСТ 28147-89. Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования. – М.: Госстандарт СССР, 1989.

М.Д. Скубилин*, А.В. Письменов*, Ф.Д. Касимов**
Россия, г. Таганрог*, Технологический институт ЮФУ
Азербайджан, г. Баку, Национальная Академия Авиации**

О КРИПТОСТОЙКОСТИ ГРАФИЧЕСКОЙ ИНФОРМАЦИИ

Известные алгоритмы кодирования и декодирования графической информации, передаваемой по открытым каналам связи, недостаточно надежно обеспечивают её конфиденциальность на разумный отрезок времени.

Цель работы – синтез алгоритмов защиты графической и текстовой информации от несанкционированных пользователей.

При адаптации для этих целей компьютерных алгоритмов защиты и восстановления информации широкое применение в оптической обработке информации находит безопорная голография. Известно [1], что процесс восстановления изображения из безопорной голограммы (**RLH**) можно интерпретировать как ассоциативный, при этом главные аспекты безопорного искажения и реконструкции оптического сигнала следующие:

– в физическом смысле **RLH** является когерентной фотографией, исходя из чего получение информации о фазе исходного сигнала невозможно из прямого анализа безопорной голограммы;

– изображение, реконструируемое из **RLH**, восстанавливается лишь в том случае, когда для этого используется часть начального поля, записанного на **RLH**, эта часть начального поля может быть интерпретирована как некоторый «ключ» для декодирования безопорной голограммы.

Из рассмотрения фурье-случая формирования и восстановления **RLH** вытекает, что свойства фурье-преобразования позволяют построить системы обработки, имеющие определенные преимущества по сравнению с ранее известными экспериментальными схемами. К таким преимуществам, прежде всего, следует отнести пространственную инвариантность фурье-системы, которая обеспечивает эффективную работу системы независимо от локализации сигнала во входной плоскости.

Представив поле $\mathbf{U(y, x)}$ во входной плоскости как сумму двух полей вида

$$\mathbf{U(x, y)=U_{0(}\, y, x)+U_{key}}, \tag{1}$$

поле в фурье-плоскости $\mathbf{V(w,v)}$ описывается как

$$\mathbf{V(w, v)=V_0(w, v)+V_{key}}, \tag{2}$$

где $\mathbf{V=I\{U\}}$ – фурье-образ начального поля.

Распределение интенсивности в плоскости **w, v** допустимо записать на фоточувствительный материал, что представляет собой безопорная голограмма, описываемая по

$$\mathbf{RLH\approx I(w, v)=\ldots V_0V^*_{key}+....} \tag{3}$$

При восстановлении безопорной голограммы закрывают непрозрачным экраном часть поля $\mathbf{U_0}$ графической информации, а само поле $\mathbf{U_{key}}$ заменяют на $\mathbf{U^i_{key}}$ его **RLH**, тогда после преобразования поле описывается по

$$\mathbf{V_i=V^i_{key}\times RLH= \ldots +V_0V^*_{key}V^i_{key}+ \ldots.} \tag{4}$$

В выходной плоскости поле соответственно описывается выражением

$$\mathbf{U_i(x_i,y_i)=I^{-1}\{V_i\}=\ldots+U_0\otimes I^{-i}\{V^*_{key}V^i_{key}\}+ \ldots,} \tag{5}$$

где $\mathbf{I^{-i}\{V^*_{key}V^i_{key}\}=U_{key}\times U^i_{key}=\varphi(x_i, y_i)}$ – корреляционная функция и

$$\begin{aligned}&\mathbf{\varphi(x_i, y_i)\rightarrow\delta(x_i, y_i)} \text{ при } \mathbf{U_{key}=U^i_{key}} \text{ и}\\ &\mathbf{\varphi(x_i, y_i)\rightarrow 0} \quad\quad \text{при } \mathbf{U_{key}\neq U^i_{key}}.\end{aligned} \tag{6}$$

Из (5) и (6) следует, что выходное поле стремится к $\mathbf{U_0}$, если выполняется первое условие, и стремится к **0**, т. е.

$$\mathbf{U^i(x_i, y_i) \rightarrow U_0(x_i, y_i)} \text{ и } \mathbf{U^i(x_i, y_i) \rightarrow 0.} \quad (7)$$

Таким образом, часть $\mathbf{U_{key}}$ начального поля, формируемая при записи **RLH**, может быть использована как некоторый ключ для восстановления поля $\mathbf{U_0}$. Но такая реконструкция успешна только в случае, когда $\mathbf{U^i_{key}=U_{key}}$.

Алгоритм искажения и восстановления графического сообщения предполагает его представление совокупностью "**0**" и "**1**" ("бинарным" файлом), но тогда каждая "**1**" может быть интерпретирована как некоторый точечный источник с единичной интенсивностью и координатою, определяемой местом этой "**1**" в файле. Дополнительно каждому точечному источнику может быть присвоена случайная фаза (в пределах 0,2 $\boldsymbol{\pi}$). Таким образом, такой трансформированный ("image" файл) может рассматриваться как некоторое скалярное поле – аналог поля $\mathbf{U_0}$.

Естественно, что ключевой файл также может быть сформирован как аналог поля $\boldsymbol{U_{key}}$, т. е. квадрат модуля амплитуды Фурье-образа описывается по

$$\mathbf{RHL(w, v)=|I\{U_0(x, y)+U_{key}\}|^2} \quad (8)$$

и является компьютерным аналогом **RLH**. **RLH**-файл передается по каналу связи. Фурье-образ поля $\mathbf{V_{key}}$, или номер ключевого файла (если санкционированный получатель сообщения имеет набор ключевых файлов), передается по каналу связи.

Процедура восстановления начального сообщения начинается с того, что санкционированный получатель множит поэлементно данные файлов **RLH** и $\mathbf{V_{key}}$ ключевого файла. После обратного преобразования Фурье результата умножения полученное поле $\mathbf{U_r(x_i, y_i)}$ стремится к полю $\mathbf{U_0(x_i, y_i)}$, если $\mathbf{V^i_{key}=V_{key}}$.

Для наглядности в качестве тест-файла, передаваемого по каналу связи, допустимо использовать графический файл в формате "**bmp**" "Распределение интенсивности в частотной плоскости" – графическое представление переданного сообщения (**RLH**), но тогда передаваемое сообщение формируется как файл со случайными данными, а наличие "регулярной" структуры в виде креста объясняется тем, что случайная фазовая модуляция вводилась только в ключевой файл. В [2] показано, что и в этом случае восстановление начального изображения невозможно из прямого анализа **RHL**-файла. Разработано программное обеспечение, оптимизированное под оболочку типа «WINDOWS».

И хотя предлагаемый алгоритм обеспечивает высокую помехозащищенность графического сообщения, что обусловлено ассоциативным характером процесса восстановления исходного изображения, его применение для текстовой информации нецелесообразно в силу значительных временных затрат на защиту информации и её восстановление, а для графической информации, в дополнение к выше сказанному, еще не исключается и потеря части информации на принимающей стороне**.**

Текстовую конфиденциальную информацию с целью упрощения процесса её подготовки к передаче по открытому каналу связи, не заботясь о помехоустойчивости канала, оказывается возможным и целесообразным осуществлять программными средствами с привлечением уже повсеместно эксплуатируемых промышленных средств вычислительной техники.

Если информационное сообщение (текст, файл) диверсифицировать, то его репликация тем более затруднена, чем больше объём исходного информационного сообщения. Исходя из этого, допустимо, не усложняя процесс искажения, на

передающей стороне осуществлять преобразования исходного информационного сообщения, при которых исходный файл информации разбивается на блоки варьируемой длины и в каждом блоке осуществлять варьируемый сдвиг по кольцу **ASII**-кода каждого символа в блоке. Искаженный таким образом файл можно оперативно восстановить (расшифровать) путем обратного сдвига символов блоков файла.

Алгоритм и программа реализации искажения и/или восстановления информации, например на языке программирования "**Borlad C**", предполагает наличие конфиденциальной информации, подлежащей содержанию в конфиденциальном состоянии и передаче по каналу электронной коммуникации, например в файле "**proba.txt**", и запускающего модуля – в файле "**kod.exe**". При этом осуществляется ввод с командной строки **KOD proba.txt** $\mathbf{K_iR_j}$, $\mathbf{K_iL_j}$, …, "**Enter**" или **KOD proba.txt** $\mathbf{U_iR_j}$, $\mathbf{U_iL_j}$, …, "**Enter**" (для кодирования и декодирования соответственно), где **K** – кодировать, **U** – декодировать, **i** (**i**=1, **m**) – число символов в данном блоке, **R** – сдвиг вправо, **L** – сдвиг влево, **j** (**j**=1, **n**) – число позиций сдвига символов в данном блоке [3–8].

Описанный в последнем случае алгоритм кодирования и/или декодирования текстовой информации реализован на аппаратном и программном уровнях. Использование предлагаемого способа защиты информации от несанкционированного доступа обеспечивает идентичность технических средств на передающей и принимающей сторонах каналов связи, оперативную, доли секунды, диверсификацию и/или репликацию информации санкционированным адресатом, и невозможность за разумное время её репликации несанкционированным адресатом, т. к. содержит значительное число более $\mathbf{10^{10}}$ вариантов кодирования и декодирования информации. Его использование допустимо в оборонных, правоохранительных, коммерческих и других целях, требующих соблюдения конфиденциальности сообщений.

Но сказанное для текстовой информации применимо и для отсканированной графической информации, что обеспечивает описанному выше алгоритму применимость для произвольной информации, электронная версия которой может передаваться по произвольному каналу коммуникации.

Дальнейшее повышение криптостойкости электронной версии конфиденциальной информации видится в повторной диверсификации файла на передающей стороне и обратной его репликации на принимающей санкционированным пользователем стороне, но ключи диверсификации и репликации на каждом этапе её обработки подлежат замене. Такое решение приводит к повышению криптостойкости по крайней мере на 2–3 порядка, а временные затраты возрастают незначительно.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Collier R.J., Pennington K.S.* Ghost imaging by holograms formed in the field. //Appl. Phys. Letters. 1966. № 8, – p. 44–46.

2. *Мохунь И.И., Росляков С.Н., Яценко В.В.* Восстановление фазовой и амплитудной составляющих дифракционного поля, рассеянного мелкоструктурным объектом, из голограммы без опорного пучка //Известия РАН, серия физическая. –56, № 4. – М.: АН РФ, 1992, – С. 205–211.

3. *Божич В.И., Скубилин М.Д., Спиридонов О.Б.* Способ и устройство защиты информации от несанкционированного доступа //Патент RU 2130641, G06F 13/00, G09C 1/00, H04L 9/00, 1999.05.20.

4. *Скубилин М.Д., Письменов А.В., Письменов Д.А., Спиридонов О.Б.* Программа диверсификации/репликации информации //Свидетельство (об официальной регистрации программы для ЭВМ) RU 2000610440. Роспатент: – М.: 2000.05.29.

5. *Скубілін М.Д. Спірідонов О.Б., Чєрєдничєнко Д.І.* Спосіб утримування інформації у недоступному для невизначеного кола осіб стані. Патент UA 33278, G06F 13/00, G09C 1/00, H04L 9/00, 2001.02.15.

6. *Skubilin M.D., Pismenov A.V.* Teghekatzrrlthlan kgvoghviknan edavnak. Патент AM 973, G01F 13/00, G09C 1/00, H04L 9/00, б. 2, 2001.06.10.

7. *Skubilin M.D., Kasimov F.C., Spiridonov O.B., Regimov R.M.* Melumatin programli kodlaşdirma – dekodlaşdirma űsulu. Patent AZ 20010140, G06F 13/00, G09C 1/00, H04L 9/00, 2001.10.02.

8. *Скубилин М.Д., Божич В.И., Спиридонов О.Б.* Способ защиты информации от несанкционированного доступа и устройство для его осуществления //Патэнт BY 5605, G06F 13/00, G09C 1/00, 2003.12.30.

Р. Г. Бияшев, С. Е. Нысанбаева
Казахстан, г. Алматы, Институт проблем информатики и управления

МОДЕЛИРОВАНИЕ ГЕНЕРАЦИИ КЛЮЧЕЙ В НЕПОЗИЦИОННОЙ ПОЛИНОМИАЛЬНОЙ СИСТЕМЕ СЧИСЛЕНИЯ

Использование непозиционных полиномиальных систем счисления (систем счисления в остаточных классах с полиномиальными основаниями или модулярной арифметики) при создании симметричных криптосистем позволяет существенно повысить их надежность, критерием которой является криптостойкость самого алгоритма шифрования. В непозиционной полиномиальной системе счисления (НПСС) основаниями служат неприводимые многочлены над полем $GF(2)$. В этой системе существенно повышается также криптостойкость алгоритма формирования электронной цифровой подписи (ЭЦП), при этом возможно значительное сокращение длины хэш-значения и подписи [1-3].

В работе представлена модель процедуры генерации ключевых последовательностей для алгоритмов зашифрования и расшифрования электронного сообщения заданной длины *N* бит (далее – сообщения) при хранении и передаче электронной информации и формирования ЭЦП в НПСС на базе нетрадиционного криптографического метода шифрования [4].

В связи с тем, что построение нетрадиционных алгоритмов и методов шифрования и формирования ЭЦП основано на выборе системы полиномиальных оснований, была создана база данных неприводимых многочленов, содержащая их общее число для каждой из степеней от 1 до 22. Пополнение базы данных неприводимыми многочленами последующих степеней производится по мере необходимости в полиномах более высокой степени.

Алгоритм шифрования начинается с формирования системы полиномиальных оснований. Пусть основаниями выбраны неприводимые многочлены с двоичными коэффициентами $p_1(x), p_2(x),..., p_S(x)$ соответственно степени $m_1, m_2,..., m_S$, называемые также рабочими основаниями. Многочлен $P(x) = p_1(x)p_2(x)...p_S(x)$ степени $m = \sum_{i=1}^{S} m_i$ является основным рабочим диапазоном НПСС. В этой системе любой многочлен, степени меньшей *m*, имеет единственное представление в виде его вычетов по модулям рабочих оснований соответственно. Все основания системы должны быть различными: соблюдение этого необходимо для выполнения китайской теоремы об остатках, даже если основания выбираются из неприводимых многочленов одной степени.