УДК 002.5:681.3

В.А. Михеев, М.М. Репин

РАЗРАБОТКА АЛГОРИТМА КОМПЛЕКСНОЙ ЗАЩИТЫ СТЕГАНОГРАФИЧЕСКИХ СООБЩЕНИЙ

Представлена проблема неэффективности современных стеганографических систем защиты информации как проблема зависимости надёжности системы стеганографической защиты информации от объёма встраиваемых данных в файл-контейнер. На основе рассмотренного математического аппарата и проведенных исследований разработан алгоритм, повышающий степень надёжности сокрытия информации и обеспечивающий контроль целостности стеганографического сообщения.

Современные стеганографические системы; файл-контейнер; множественная инкапсуляция.

V.A. Mikheev, M.M. Repin

DEVELOPMENT OF STEGANOGRAPHIC MESAGGES INTEGRATED PROTECTION ALGORITHM

The article presents the problem of inefficiency of modern steganographic security system as a problem depending on the reliability of steganographic security information on the amount of embedded data in the container file. On the basis of the considered mathematical apparatus and the conducted researches the algorithm that enhances reliability of concealment of the information and provides control of the integrity of steganographic message was developed.

Modern steganography system; the container file; multiple encapsulation.

Используя методы современной стеганографии, пользователи стеганосистем сталкиваются с проблемами качественного сокрытия информации, так как зачастую объёмы скрываемой информации велики и не позволяют незаметно скрыть сообщение в контейнере. Как правило, объём самого файла-контейнера (контейнера) меньше, чем объём информации, который необходимо в нём скрыть.

Умение пользоваться методами стеганографического анализа со знанием заполненного контейнера (известного видеоролика, популярной музыкальной композиции, фотографии и прочего) и со знанием, к примеру, контейнера оригинала дают реальные шансы злоумышленнику получить доступ к скрываемой информации. Как показывает практика, для повышения надёжности сокрытия информации лучше использовать не вызывающий подозрения простой контейнер, существование общедоступной копии которого мало вероятно, или она вообще не существует [1].

Каждая из задач, решаемых с помощью стеганографии, будь то защита от копирования, скрытая аннотация документов, аутентификация, скрытая связь или просто скрытое хранение какой-либо информации требует определённого соотношения между устойчивостью встроенного сообщения к внешним влияниям и размером встроенного сообщения.

Для большинства современных методов, которые используются для скрытия сообщений в файлах цифрового формата, имеет место характерная зависимость надёжности системы от объёма встраиваемых данных, представленная на рис. 1 [2].

Острой проблемой задач стеганографии является соблюдение определенного уровня устойчивости стеганосистем [2, 3]. Из рис. 1 видно, что увеличение объёма встраиваемых данных значительно снижает надежность системы.

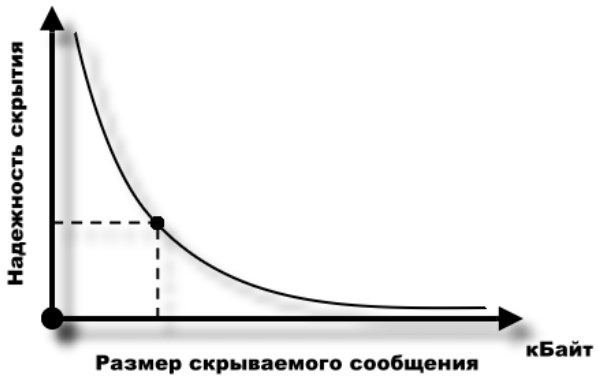

Рис. 1. Взаимосвязь между устойчивостью стеганосистемы и объемом скрываемого сообщения при неизменном размере контейнера

Данная зависимость приводит к необходимости принятия рационального решения при выборе между количеством (объёмом) скрываемых данных и степенью устойчивости (скрытости) к возможной модификации (анализу) сигнала-контейнера. Путём ограничения степени ухудшения качеств контейнера, которые способен воспринимать человек, при стеганографической обработке контейнера можно достичь или высокого уровня (объёма) встраиваемых данных, или высокой устойчивости к модификации (анализу), но никоим образом не обоих этих показателей одновременно, поскольку рост одного из них неизбежно приводит к уменьшению другого. Несмотря на то, что данное утверждение математически может быть продемонстрировано только для некоторых методов стеганографии (например, для скрытия путём расширения спектра), очевидно, что оно является справедливым и для других методов скрытия данных.

При использовании любого метода, благодаря избыточности информации, существует возможность повысить степень надёжности скрытия, снижая при этом пропускную способностью (объём скрываемых данных). Объём встроенных данных и степень модификации контейнера могут изменяться от метода к методу. Также очевиден и тот факт, что в зависимости от целей, для которых используется скрытие данных, различными являются и требования относительно уровня устойчивости системы к модификации контейнера. Как следствие этого, для разных целей оптимальными являются разные методы стеганографии.

Помимо того, что стеганосистема должна обладать определённой стойкостью, она должна иметь приемлемую вычислительную сложность реализации (под вычислительной сложностью понимается количество шагов или арифметико-логических операций, необходимых для решения вычислительной проблемы, в данном случае – процесса встраивания/извлечения информации в/из сигнала контейнерах [4]).

Следовательно, необходим алгоритм, повышающий степень надёжности сокрытия информации и предполагающий расширение пропускной способности (объема встраиваемых данных). Так же при передаче стеганографических сообщений важным остается контроль целостности. При перехвате передаваемого сообщения противником есть вероятность, что оно будет модифицировано и использовано для дезинформации. Данную проблему можно решить, применяя алгоритмы электронной цифровой подписи. Используя результаты работ [1, 5, 8], приведем алгоритм, удовлетворяющий сформулированным ранее требованиям.

Базовая модель стеганографической системы.

Рассмотрим математическую модель стеганосистемы. Процесс тривиально стеганографического преобразования описывается зависимостями [2]:

Ψ – процесс скрытия информации;

D – процесс извлечения скрытой информации;

$$\Psi: C \times M \to S; \quad (1)$$

$$D: S \to M, \quad (2)$$

где $S = \{(c_1, m_1), (c_2, m_2), \dots, (c_n, m_n), \dots, (c_q, m_q)\} = \{s_1, s_2, \dots, s_q\}$ – множество контейнеров-результатов (стегонограмм). Необходимые условия: 1. Отсутствие "пересечения", то есть, если $m_a \neq m_b$, причем $m_a, m_b \in M$, а $(c_a, m_a), (c_b, m_b) \in S$, то $E(c_a, m_a) \cap E(c_b, m_b) = \emptyset$.

$$|C| \geq |M|. \quad (3)$$

Стороны должны знать алгоритмы прямого (Ψ) и обратного (D) стенографического преобразования.

На основании этого, под стеганосистемой будем понимать совокупность $\sum = (C, M, S, \Psi, D)$ контейнеров, сообщений и преобразований, которые их связывают.

Для оценки надежности стеганосистемы введем функцию подобия на множестве C.

Определение 1.

Пусть C – непустое множество, тогда функция $sim(C) \to (-\infty, 1]$ является функцией подобия на множестве C, если для каких-либо x,y $x, y \in C$ справедливо, что $sim(x, y)$=1 в случае $x = y$ и $sim(x, y) < 1$ при $x \neq y$. Стеганосистема может считаться надежной, если $sim[c, E(c, m)] \approx 1$ для всех $m \in M$ и $c \in C$, причем в качестве контейнера c должен избираться ранее не использованный.

Теперь рассмотрим понятие абсолютно надежной стеганосистемы. Её идея базируется на случайности избирания контейнера c из множества C с вероятностью P_c. Встраивание сообщения в контейнер можно описать функцией, определенной на множестве C. Пусть P_c – вероятность формирования стеганосистемы $\Psi(c, m, k)$ на множестве S всех возможных стеганограмм, полученных с помощью стеганосистемы. $P_s(c)$ =0, если контейнер c никогда не используется для получения стеганограмм. Учтя распределение вероятностей на множестве ключей K и множестве сообщений M, можно вычислить вероятность P_s. Определим на множестве Q такое соотношение для относительной энтропии, с помощью которого можно измерить неэффективность принятия неверной гипотезы о распределении P_1 в случае истинного распределения P_0:

$$D(P_0||P_1) = \sum_{q \in Q} P_0(q) \cdot log_2 \left(\frac{P_0(q)}{P_1(q)}\right), \quad (4)$$

где выражение log_2 является алгоритмическим отношением правдоподобия.

Определение 2.

Пусть $\sum$ – стеганографическая система; P_s – распределение вероятностей передачи каналом связи стеганограмм; P_c – распределение вероятностей передачи каналом связи пустых контейнеров. Система $\sum$ называется $\rho -$ надежной к пассивным атакам, если $D(P_c||P_s) \leq \rho$, и является абсолютно надежной, если $\rho = 0$. Следовательно стеганостистема $\sum$ теоретически абсолютно надежна, если процесс встраивания секретного сообщения в контейнер не изменяет распределение P_c.

Теорема.

Пусть $\sum$ – стеганографическая система, которая является ρ надежной против пассивных атак. Тогда вероятность β того, что нарушитель не обнаружит скрытое

сообщение, и вероятность α того, что он ошибочно обнаружит несуществующее скрытое сообщение, удовлетворяют соотношению $d(\alpha,\beta) \le \rho$, где $d(\alpha,\beta)$ – относительная двоичная энтропия, которая определяется как

$$d(\alpha,\beta) = \alpha \cdot log_2 \frac{\alpha}{1-\beta} + (1-\alpha) \cdot log_2 \frac{1-\alpha}{\beta}. \quad (5)$$

В частности, если $\alpha = 0$, то $\beta \ge 2^{-\rho}$.

Используя рассмотренный математический аппарат, можно предложить следующий алгоритм, в основе которого лежит цель сведения вероятности обнаружения наличия скрытых сообщений к минимуму. Основой алгоритма является создание большой избыточности контейнеров, которая позволит отвлечь внимание от скрытой информации, так как изменение распределения P_c при встраивании сообщений будет минимально.

Для реализации необходимо разбить исходное сообщение на несколько блоков минимально возможного размера. Например можно применить архиватор. Для повышения стойкости рекомендуется параллельно использовать криптоалгоритмы, шифруя блоки сообщения.

На вход поступает соотношение Q. Введем функцию $\Omega(Q) = S_1, S_2 \dots S_n$, которая осуществляет разбиение Q и зашифровывание получившихся блоков. В стеганокодере осуществляется распределение шифроблоков по контейнерам, причем в различных файлах должно использоваться их одинаковое число. Для повышения надежности при передаче можно использовать инверсию функции Ω к сообщению Q. $\overline{\Omega}(Q) = S_n \dots S_2, S_1$. (6)

На выходе стеганокодера получаем контейнеры с дублированием, что повышает вероятность успешного декодирования. Такой способ допустим только при небольших размерах исходного сообщения, так как в этом случае избыточность не критична.

Повышение скорости работы алгоритма даст отказ от шифрования на этапе встраивания блоков в пустые контейнеры.

Для зашифровывания при разбиении целесообразно использовать алгоритмы с открытым ключом [6]. В этом случае может быть несколько участников тайного информационного обмена.

Множественная инкапсуляция

Для создания многоступенчатой системы защиты используем предложенную в [1] множественную инкапсуляцию.

Пусть ω – глубина инкапсуляции, Q – сообщение, подлежащее зашифровыванию, $\Omega(Q) = S_1, S_2, \dots, S_n$ – функция, осуществляющая разбиение Q и зашифровывание получившихся блоков, $\overline{\Omega}(Q) = S_1, S_2, \dots, S_n$ – инверсия функции Z к сообщению Q, $F_1, F_2, \dots, F_\omega$ – псевдосообщения для инкапсуляции.

Алгоритм множественной инкапсуляции

ВХОД: Исходное сообщение Q.

ВЫХОД: Набор стеганоконтейнеров.

Шаг 1. Разбиение исходного сообщения и зашифровывание получившихся блоков $\Omega(Q) = S_1, S_2, \dots, S_n$.

Шаг 2. Разбиение псевдосообщений $\Omega(F) = S'_1, S'_2, \dots, S'_n$.

Шаг 3. Процесс инкапсуляции $\Omega(Q) \to \Omega(F)$.

Алгоритм множественной инкапсуляции представлен на рис. 2.

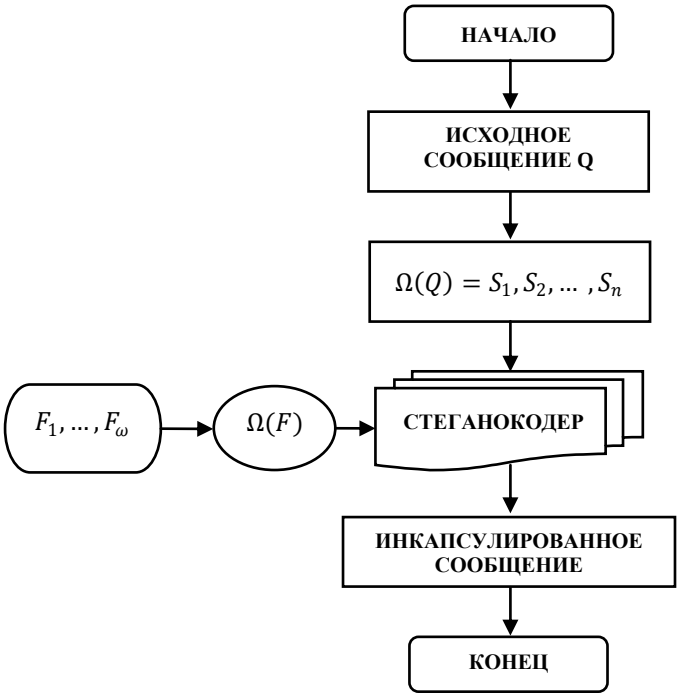

Рис. 2. Алгоритм процесса зашифровывания с инкапсуляцией в псевдосообщения

Применение множественной инкапсуляции позволит скрыть от злоумышленника сам факт наличия стеганосообщения в контейнере, так как глубина инкапсуляции не известна, а взлом контейнеров верхнего уровня дает набор неструктурированной и бессмысленной информации.

Защита от модификации стеганосообщения. Для предотвращения модификации стеганосообщения в рассмотренном алгоритме можно использовать российский стандарт электронно-цифровой подписи (ЭЦП) ГОСТ Р 34.10-2001 [7]. Стойкость алгоритма базируется на сложности дискретного логарифмирования в группе точек эллиптической кривой.

В [7] сформулированы следующие параметры ЭЦП:

- простое число p – модуль эллиптической кривой, удовлетворяющее неравенству $p > 2^{255}$;
- эллиптическая кривая E, задаваемая своим инвариантом $J(E)$ или коэффициентами $a, b \in F_p$, где F_p – конечное поле из p элементов. $J(E)$ связан с коэффициентами a и b следующим образом:

$$J(E) = 1728 \cdot \frac{4a^3}{4a^3+27b^2} (mod\ p), \text{ причем } 4a^3 + 27b^2 \not\equiv 0\ (mod\ p); \qquad (7)$$

- целое число m – порядок группы точек эллиптической кривой E, $m \neq p$;
- простое число q – порядок циклической подгруппы группы точек эллиптической кривой E, для которого выполнены следующие условия:

$$\begin{cases} m = nq, \ \ n \in Z, n \geq 1 \\ 2^{254} < q < 2^{256} \end{cases}; \qquad (8)$$

- точка $P \neq O$ эллиптической кривой E, с координатами (x_p, y_p), удовлетворяющая равенству $qP = O$, где O – нулевая точка;
- хеш-функция $h(\cdot): V_\infty \to V_{256}$, отображающая сообщения, представленные в виде двоичных векторов произвольной конечной длины, в двоичные вектора длины 256 бит. Хэш-функция определена в [8].

Анализ рассмотренных параметров показал, что генерация открытого ключа для криптосистемы сводится к выбору эллиптической кривой с циклической группой большого простого порядка m, при наличии следующих требований:

$$m \neq p; \tag{9}$$

m взаимно просто с

$$p - 1, p^2 - 1, \dots, p^k - 1. \tag{10}$$

На основе анализа, проведенного в [9], для выбора эллиптической кривой будем использовать алгоритм Newton AGM.

Алгоритм Newton AGM. Возьмем простое число p, такое, что $p \in \mathbb{N}^*$, $q = p^n$ и E данная эллиптическая кривая. Проблема подсчета числа точек эллиптической кривой эквивалентна вычислению следа морфизма Фробениуса Fr_q как $\#E(F_q) = 1 + q - Tr(Fr_q)$.

Условные обозначения и сложность гипотез. Будем считать, что произведение двух целых чисел длинной n бит занимает $O(n^\mu)$ битовых операций. Классически, с алгоритмом умножения целых чисел с БПФ, $\mu = 1 + \epsilon$. Пусть p постоянное малое простое число, $q = p^n$ и $\mathbb{F}_q$ – конечное поле с q элементами. Обозначим через $\mathbb{Z}_q$ кольцо нормирования неразветвленного расширения степени n из $\mathbb{Q}_p$, σ будет обозначать перестановки Фробениуса над полем рациональных чисел $\mathbb{Z}_q$, что рассматривается как расширение $\mathbb{Q}_p$ и неархимедову оценку $\mathbb{Z}_q$ обозначим как υ. Для каждого $m \in \mathbb{N}^*$, мы имеем каноническую проекцию $\pi_m: \mathbb{Z}_q \to \mathbb{Z}_q/p^m\mathbb{Z}_q$ и установим $\pi = \pi_1$ для проекции на конечное поле $\mathbb{F}_q$.

Многие математические объекты, использованные в описании алгоритмов, можно рассматривать как список элементов $\mathbb{Z}_q$. Формально говоря, отображения в π_m этих элементов из $\mathbb{Z}_p$ будут называться в этих алгоритмах математическими объектами, вычисленными “с точностью m ” или “с погрешностью m” или “по модулю p^m ”.

Будем обозначать $T_{m,n}$ сложность перемножения двух элементов из $\mathbb{Z}_{p^n}$ с точностью m. Далее, пусть $S_{m,n}$ будет временной сложностью вычисления с точностью m отображения элемента из $\mathbb{Z}_q$ с помощью перестановок Фробениуса. Если E эллиптическая кривая над $\mathbb{F}_q$, то j(E) будет j −инвариантой и $E^\uparrow$ – канонический подъем E. Предположим, что $j(E) \in \mathbb{F}_q \backslash \mathbb{F}_{p^2}$. Точка, бесконечно удаленная от эллиптической кривой, будет обозначаться $\mathcal{O}$.

Вычисление корней обобщенных уравнений Артина-Шрейера (Artin-Schreier’s).

Если $\mathbb{F}_q$ является полем характеристики p, то уравнение Артина-Шрейера имеет вид $x^p - x + \beta = 0$ с $\beta \in \mathbb{F}_q$. Будем говорить, что уравнение является обобщенным уравнением Артина-Шрейера, если оно может быть записано в виде

$$\sigma(x) + ax + b = 0, c\ a, b \in \mathbb{Z}_q. \tag{11}$$

В частности, π примененное к этому уравнению дает все классические уравнения Артина-Шрейера. На рис. 3 приведен алгоритм поиска корней такого уравнения.

Алгоритм решения обобщенного уравнения Артина-Шрейера (ArtinScheierRoot)

ВХОД: a и b в $\frac{\mathbb{Z}_q}{p^m\mathbb{Z}_q}$, m и ν в $\mathbb{N}$.

ВЫХОД: A и B такие, что решение $\sigma(x) = ax + b \bmod p^m$ удовлетворяет $\sigma^\nu(x) = \sigma^\nu(A)x + \sigma^\nu(B) \bmod p^m$.

Шаг 1. Если $\nu = 1$, тогда возвращает $\sigma^{n-1}(a) \bmod p^m, \sigma^{n-1}(b) \bmod p^m$.

Шаг 2. $A, B := \mathrm{ArtinSchreierRoot}(a, b, m, \lfloor\frac{\nu}{2}\rfloor)$.

Шаг 3. Вычисляем $A, B := A\sigma^{n-\lfloor\frac{\nu}{2}\rfloor}(A) \bmod p^m, A\sigma^{n-\lfloor\frac{\nu}{2}\rfloor}(B) + B \bmod p^m$.

Шаг 4. Если $\nu \bmod 2 = 1$, тогда $A, B := A\sigma^{n-\nu}(a) \bmod p^m, A\sigma^{n-\nu}(b) + B \bmod p^m$.

Шаг 5. Возвращает A, B.

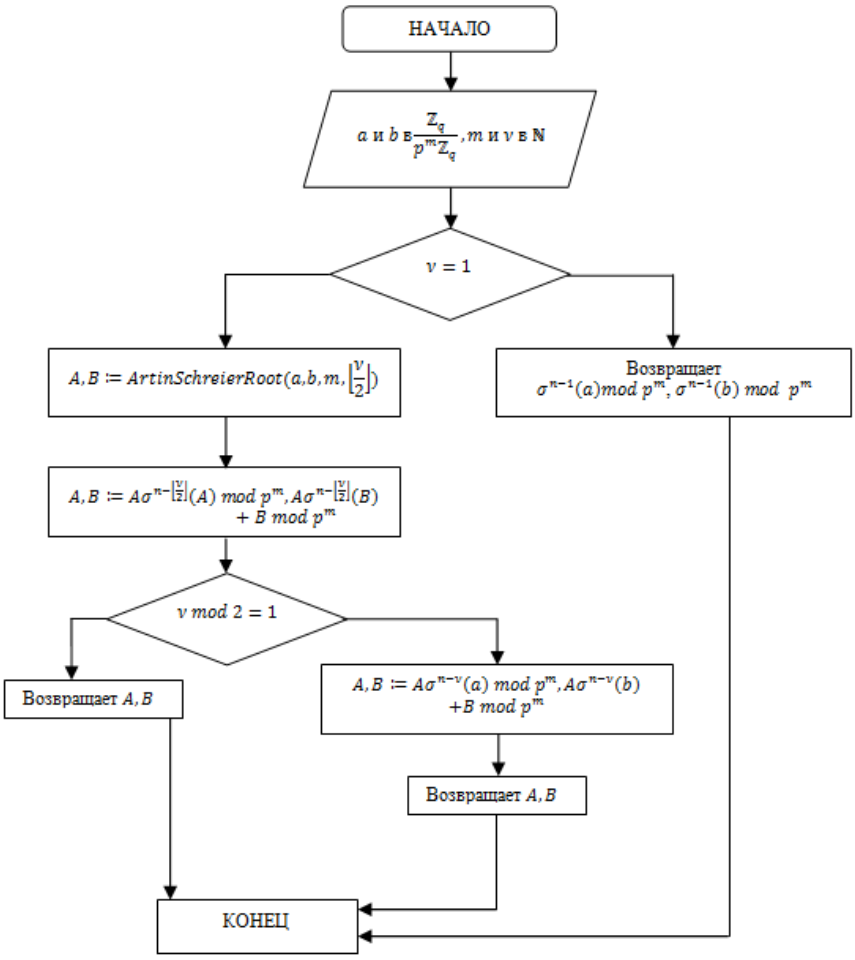

Рис. 3. Алгоритм решения обобщенного уравнения Артина-Шрейера

Улучшенный алгоритм подъема. Опишем алгоритм, предложенный Рейнальдом Лесьером (Reynald Lercier) и Давидом Любицом (David Lubicz) для подсчета количества точек эллиптической кривой, определенной над конечным полем [10].

Для решения основной проблемы, содержащейся в алгоритмах подсчета точек, которая заключается в поиске корней в $\mathbb{Z}_q$ с точностью m, при фиксированном $m \in \mathbb{N}$, уравнения вида $\phi(x, \sum(x)) = 0$, с полиномиальными коэффициентами ϕ в $\mathbb{Z}_q$, когда решение x_0 при низкой точности такого уравнения уже известно, Лесьером и Любицом был предложен расширенный алгоритм Ньютона. Основная идея этого алгоритма заключается в небольшой модификации хорошо известного алгоритма для вычисления корней одномерных полиномов над $\mathbb{Z}_q$ с целью восстановления квадратичной сходимости.

В частности, пусть $\phi \in \mathbb{Z}_p[x, y]$ двумерный полином с коэффициентами в $\mathbb{Z}_q$. Пусть $x_0 \in \mathbb{Z}_q$ нулевой элемент уравнения $\phi(x, \sum(x)) = 0 \; mod \; p^{\omega}, \omega \in \mathbb{N}$. Кроме того, предположим, что

$$\upsilon\left(\frac{\delta\phi}{\delta x}(x_0, \sum(x_0))\right) \geq \upsilon\left(\frac{\delta\phi}{\delta y}(x_0, \sum(x_0))\right) \quad (12)$$

и

$$\upsilon\left(\phi(x_0, \sum(x_0))\right) > \upsilon\left(\left(\frac{\delta\phi}{\delta y}\right)^2(x_0, \sum(x_0))\right). \quad (13)$$

Единственная сложность в случае одномерного полинома, это композиция с Σ. Но так как такие морфизмы сохраняют оценки, доказательство результата в этом случае очень близко к доказательству для классической сходимости Ньютона [11. С. 493-494]. Опустим данное доказательство и приведем непосредственно алгоритм.

Алгоритм NewtonLift

Алгоритм вычисляет корни $\phi(x, \sum(x)) mod \; p^m$, при известном решении x_0 по модулю p^{2k+1},
где

$$k = \upsilon\left(\frac{\delta\phi}{\delta y}(x_0, \sum(x_0))\right). \quad (14)$$

ВХОД: $x_0 \in \frac{\mathbb{Z}_q}{p^{2k+1}\mathbb{Z}_q}, m \in \mathbb{N}$.

ВЫХОД : x −решение $\phi(x, \sum(x)) mod \; p^m$.

Шаг 1. Если $m \leq 2k + 1$ тогда возвращаем x_0.

Шаг 2. $\omega := \left\lceil \frac{m}{2} \right\rceil + k$.

Шаг 3. $x := \mathbf{NewtonLift}(x_0, \omega)$.

Шаг 4. Подъем x к $\frac{\mathbb{Z}_q}{p^m\mathbb{Z}_q}$; $y := \sum(x) mod \; p^m$.

Шаг 5. $\Delta_x := \delta_x\phi(x, y) mod \; p^{\omega-k}$;.

$$\Delta_y := \delta_y\phi(x, y) mod \; p^{\omega-k}.$$

Шаг 6. $V := \phi(x, y) mod \; p^m$

Шаг 7. $a, b :=$**ArtinSchreierRoot** $\left(-\frac{V}{p^{\omega-k}\Delta_y}\right), -\frac{\Delta_x}{\Delta_y}, \omega - k, n)$.

Шаг 8. Возвращает $x + p^{\omega-k}(1 - a)^{-1}b$.

В [12] Местре описывает очень эффективный алгоритм вычисления точек на эллиптических кривых, определенных над $\mathbb{F}_{2^n}$. В нем используется алгебраическо-геометрическое среднее (AGM).

Опишем сначала версию данного алгоритма, которая обычно используется на практике. Пусть E – эллиптическая кривая, определенная над полем $\mathbb{F}_{2^n}$ уравнением $y^2 + xy = x^3 + a_6$. Мы можем рассмотреть последовательность элементов $\mathbb{Z}_{2^n}$, определенную как

$$\alpha_{n+1} = (1+\alpha_n)/2\sqrt{\alpha_n} \tag{15}$$

с первым элементом, равным $\alpha_0 = 1 + 8\alpha_6 \in \mathbb{Z}_{2^n}$. Квадратный корень уравнения выбран так, что $\sqrt{1+8t} = 1+4t'$ с $t, t' \in \mathbb{Z}_{2^n}$. Тогда получается, что

$$Tr(Fr_q) = N_{\frac{\mathbb{Z}_{2^n}}{\mathbb{Z}_2}}\left(\frac{2\alpha_{\lceil \frac{n}{2} \rceil+3}}{1+\alpha_{\lceil \frac{n}{2} \rceil+3}}\right), \tag{16}$$

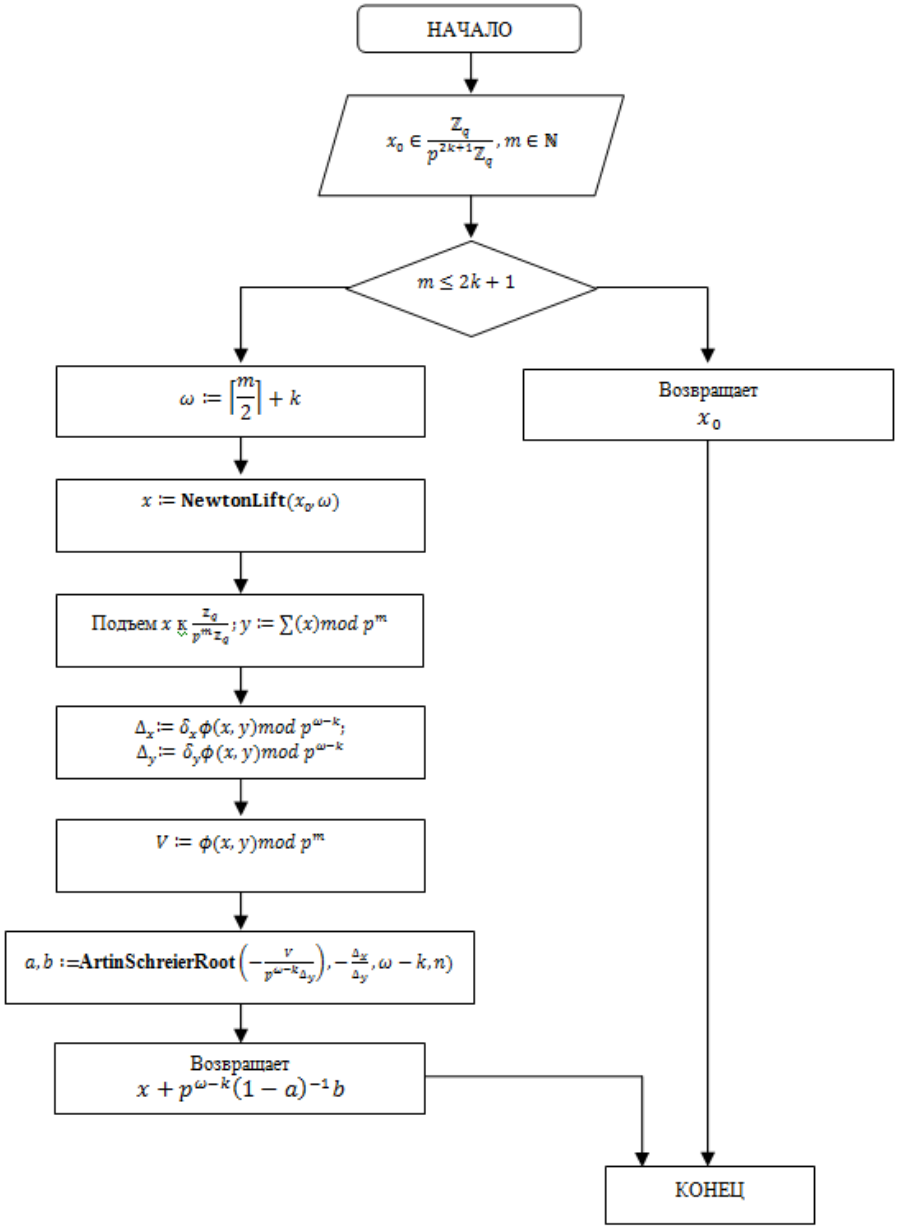

Рис. 4. Алгоритм NewtonLift

Другой важный факт, это $\alpha_{n+1} \simeq \sigma(\alpha_n) mod 2^{n+3}$. Поэтому, как и алгоритм Сатоша, метод AGM можно четко разделить на две части. В первой части содержится вычисление корней $4x\sigma(x)^2 = (1+x)^2$ в точности до $\left\lceil \frac{n}{2} \right\rceil + 3$. Вторая часть дает след Фробениуса с нормой вычисления. Первая часть может быть улучшена путем применения процедуры NewtonLift к

$$\phi(x, y) = 4xy^2 - (1+x)^2,$$

поскольку

$$\upsilon\left(\frac{\delta\phi}{\delta x}(\alpha_0, \sigma(\alpha_0))\right) \geq \upsilon\left(\frac{\delta\phi}{\delta y}(\alpha_0, \sigma(\alpha_0))\right). \quad (17)$$

В данном алгоритме временная сложность тривиально та же, как и в алгоритме NewtonLift.

Использование приведенного алгоритма при формировании параметров ЭЦП исключит ситуацию выбора слабых эллиптических кривых, а также сократит временные и ресурсные затраты на проведение расчетов.

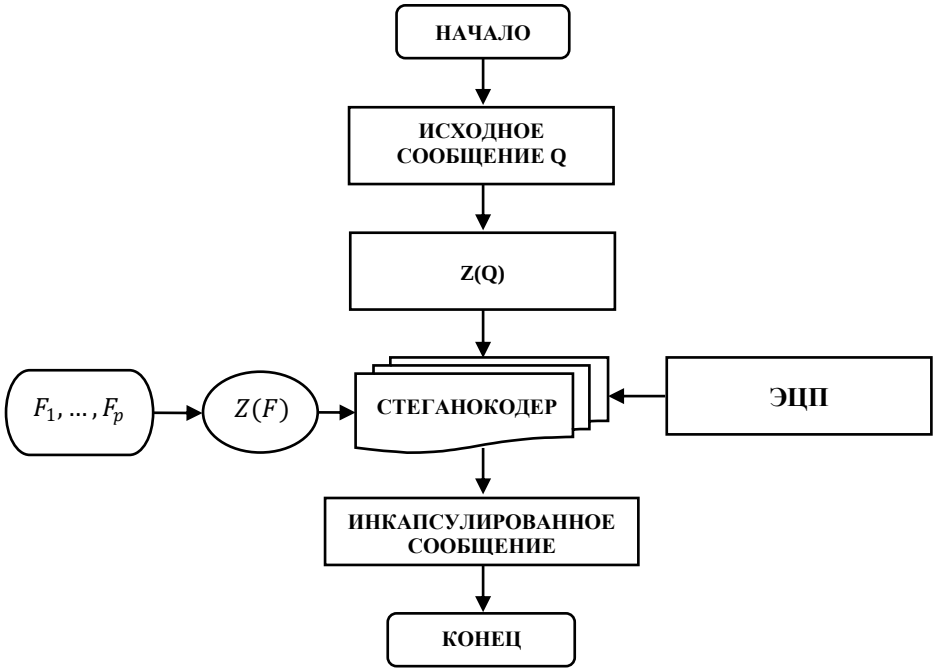

Рис. 5. Применение ЭЦП при формировании стеганосообщения

Таким образом, был разработан алгоритм, повышающий степень надёжности сокрытия информации и создающий возможность расширения пропускной способности (объёма встраиваемых данных). Оптимальный выбор количества частей разбиения исходного сообщения позволит наиболее эффективно скрыть сам факт наличия конфиденциальной информации в контейнере. Использование ЭЦП позволит: предотвратить модификацию информации в стеганосообщении, определить, какие части сообщения были подвержены атаке и исключить возможность дезинформации.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Михеев В.А. Репин М.М.* Способ многоконтейнерной стеганографической защиты информации с разделением исходного сообщения на части и множественной инкапсуляцией // Материалы XXI Международной научно-практической конференции «Информационная безопасность-2010» (Часть I). – Таганрог: Изд-во ТРТУ, 2010. – С. 88-90.
2. *Конахович Г.Ф.* Пузыренко А.Ю. Компьютерная стеганография, теория и практика. – Киев: МК-Пресс, 2006.
3. *Christian Cachin.* An Information-Theoretic Model for Steganography, In Proceeding of 2nd Workshop on Information Hiding (D. Aucsmith, ed.), Lecture Notes in Computer Science, Springer, 1998. – P. 306-318.
4. *Грибунин В.Г., Оков И.Н., Туринцев И.В.* Цифровая Стеганография. – М.: Солон-Пресс, 2002. – 272 с.
5. *Михеев В. А., Николаев А. В., Репин М. М.* Способ многоконтейнерной стеганографической защиты информации с разделением исходного сообщения на части // Вопросы защиты информации. – М.: ВИМИ, 2009. – № 4 (87). – С. 32-35.
6. *Саломаа А.* Криптография с открытым ключом: Пер. с англ. – М.: Мир, 1995. – 318 с.
7. ГОСТ Р 34.10-2001. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи. – М.: ГОССТАНДАРТ РОССИИ, 2001.
8. ГОСТ Р 34.11-94 Информационная технология. Криптографическая защита информации. Функция хэширования. – М.: ГОССТАНДАРТ РОССИИ, 1994.
9. *Михеев В.А., Репин М.М.* Анализ алгоритмов подсчета числа рациональных точек эллиптической кривой // Материалы XXI Международной научно-практической конференции «Информационная безопасность-2010» (Часть I). – Таганрог: Изд-во ТРТУ, 2010. – С. 91-92.
10. *Reynald Lercier, David Lubicz.* Counting Points on Elliptic Curves over Finite Fields of Small Characteristicin Quasi Quadratic Time. – 2005.
11. *Serge Lang.* Algebra (3rd revised edition), volume 211 of Graduate Texts in Mathematics. Springer-Verlag, 2002.
12. *Jean-Francois Mestre.* Lettre a Gaudry et Harley. Available at http://www.math.jussieu.fr/~mestre, 2001.

Михеев Вячеслав Алексеевич
Открытое акционерное общество «Концерн радиостроения «Вега»».
E-mail: mikheev@vega.su.
121170, г. Москва, Кутузовский проспект, 34.
Тел.: 84992490585; факс: 84959331563.

Репин Максим Михайлович
E-mail: bmstu.iu8@gmail.com.
Тел.: 84992494429; факс: 84959331563.

Mikheev Viatcheslav Alexeevich
Joint-Stock Company «Radio Engineering Corporation «VEGA»».
E-mail: mikheev@vega.su.
34, Kutuzov avenue, Moscow, 121170. Russia.
Phone: +74992490585; fax: +74959331563.

Repin Maxim Mixajlovich
E-mail: bmstu.iu8@gmail.com.
Phone: +74992494429; fax: +74959331563.