УДК 621.391

С.П. Евсеев[1], Б.П. Томашевский[2], В.В. Огурцов[1], Т.А. Свердло[1]

[1] *Харьковский национальный экономический университет имени Семена Кузнеца, Харьков*
[2] *Национальная Академия Сухопутных войск имени Петра Сагайдачного, Львов*

ПОСТРОЕНИЕ СХЕМЫ ДВУХФАКТОРНОЙ АУТЕНТИФИКАЦИИ НА ОСНОВЕ ИСПОЛЬЗОВАНИЯ КРИПТО-КОДОВЫХ СХЕМ

Рассматриваются основные принципы построения крипто-кодовых схем Мак-Элиса и Нидеррайтера. Проводится анализ различных систем двухфакторной аутентификации, их противостояние различным видам атак. Предлагается схема двухфакторной аутентификации на основе использования крипто-кодовых схем Мак-Элиса и Нидеррайтера с целью повышения криптостойкости формируемого аутентификатора в схеме двухфакторной аутентификации.

Ключевые слова: *двухфакторная аутентификация, крипто-кодовые схемы Мак-Элиса и Нидеррайтера.*

Вступление

Развитие современных вычислительных технологий существенно влияет на безопасность информации, циркулирующей в коммуникационных системах и сетях. Стандартные услуги и специальные механизмы обеспечения безопасности в соответствии с международными стандартами ISO 7498, ISO/IEC 10181, как правило, используют криптографические методы преобразования информации. Особое место среди коммуникационных систем занимают критические системы, примером которых могут быть банковские внутриплатежные системы – нарушение любой подсистемы или элемента таких систем приводит к их полному разрушению. Для пользователей банковскими услугами особое место в системе безопасности играют механизмы обеспечения аутентификации, позволяющие идентифицировать личность пользователя банковскими счетами.

Существующие системы аутентификации базируются на предъявлении пользователем компьютеру статической пары идентификатор/пароль. Однако в таком случае пары могут быть скомпрометированы из-за халатности пользователей или возможности подбора паролей злоумышленником [1 – 4]. Значительные интервалы времени, в течение которых пароль и идентификатор остаются неизменными, позволяют применить различные методы их перехвата и подбора. Для повышения защищенности компьютерной системы администраторы ограничивают срок действия паролей, но в типичном случае этот срок составляет недели и месяцы, что вполне достаточно для злоумышленника. Радикальным решением является применение двухфакторной аутентификации, когда система просит пользователя предоставить ей «то, что ты знаешь» (имя и, возможно, некий PIN-код), и «то, что у тебя есть» – какой-либо аппаратный идентификатор, ассоциирующийся с этим пользователем [1; 2].

Целью статьи является проведение сравнительного анализа различных систем двухфакторной аутентификации, их противостояние различным видам атак, исследование основных принципов построения крипто-кодовых схем Мак-Элиса и Нидеррайтера, рассмотрение предлагаемой схемы двухфакторной аутентификации на основе использования крипто-кодовых схем Мак-Элиса и Нидеррайтера с целью повышения криптостойкости формируемого аутентификатора в схеме двухфакторной аутентификации.

Основная часть

Сравнительный анализ различных систем двухфакторной аутентификации

Методы строгой (двухфакторной) аутентификации чаще всего используются в финансовой сфере, но в принципе могут применяться практически в любой другой области. Основные способы построения систем двухфакторной аутентификации приведены на рис. 1 и подразделяются [3]:

1. *ПО для идентификации конкретного ПК.* В компьютер инсталлируется специальная программа, устанавливающая в нем криптографический маркер. Тогда в процесс аутентификации будут вовлечены два фактора: пароль и маркер, встроенный в ПК. Так как маркер постоянно находится на данном компьютере, пользователю для входа в систему нужно будет лишь ввести логин и пароль.

2. *Биометрия*. Использование биометрии в качестве вторичного фактора идентификации осуществляется путем идентификации физических характеристик человека (отпечаток пальца/ладони, радужная оболочка глаза и т.п.).

3. *Одноразовый e-mail- или sms-пароль*. Использование в качестве вторичного фактора идентификации такого пароля возможно путем отправки второго одноразового пароля на зарегистрированный адрес электронной почты или на мобильный телефон.

© С.П. Евсеев, Б.П. Томашевский, В.В. Огурцов, Т.А. Свердло

4. *Токен с одноразовым паролем*. Пользователю выдается устройство, которое генерирует постоянно изменяющиеся пароли. Именно эти пароли и вводятся пользователем в дополнение к обычным паролям при аутентификации.

5. *Контроль извне*. Этот метод предполагает звонок из банка на предварительно зарегистрированный телефонный номер. Пользователь должен ввести пароль по телефону, и только после этого он получит доступ к системе.

6. *Идентификация с использованием гаджетов*. Такого рода идентификация осуществляется путем помещения криптографической метки на какое-нибудь устройство пользователя (например, на USB-накопитель, iPad, карту памяти и т.п.). При регистрации пользователь должен подсоединить данное устройство к ПК.

7. *Карточка с соскабливаемым слоем*. Пользователю выдается карточка с PIN-кодом, который используется лишь однажды.

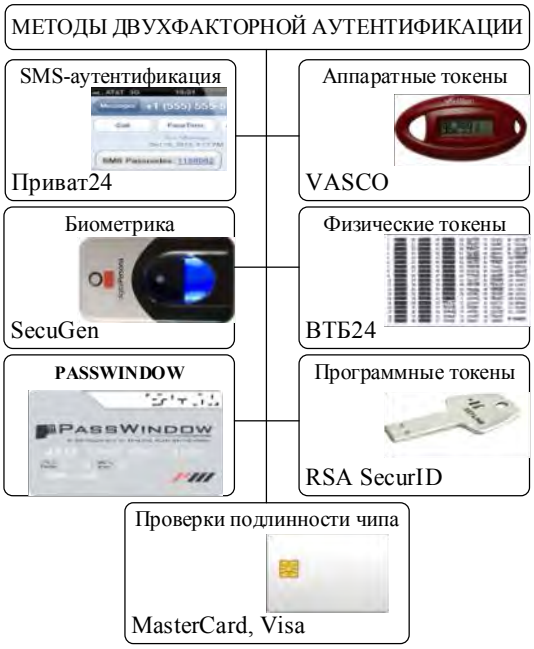

Рис. 1. Основные системы двухфакторной аутентификации

Проведенный анализ показал, что в банковских системах, как правило, применяются системы двухфакторной аутентификации, основанные на одноразовых sms-паролях. Пользователям услуг нет необходимости иметь при себе дополнительные программно-аппаратные средства и различные типы токенов или биометрические карты с целью формирования аутентификатора транзакции.

Сегодня несколько компаний предлагают системы двухфакторной аутентификации, основанные на генерации одноразовых паролей (One-Time Password – OTP), в числе которых RSA Security, VASCO Data Security и ActivIdentity. Для ее реализации используются различные виды генераторов OTP. Генератор OTP представляет собой автономный портативный электронный прибор, способный генерировать и отображать на встроенном ЖК-дисплее цифровые коды. Для семейства устройств Digipass компании VASCO механизм генерации одноразовых паролей основан на криптографическом TripleDES-преобразовании набора данных, состоящего из 40 бит текущего времени и 24-битового вектора данных, уникальных для каждого идентификатора доступа. Полученный результат преобразования виден на дисплее в виде шести или восьми десятичных цифр, визуально считывается пользователем и вручную вводится как пароль в ответ на запрос прикладных программ об аутентификации. Периодичность смены паролей при этом составляет 36 с., таким образом, пользователь получает действительно одноразовый пароль для входа в систему [4].

На серверной части компьютерной системы этот пароль сравнивается с паролем, сгенерированным самим сервером по такому же алгоритму с использованием показаний текущего времени часов сервера и уникальных данных устройства, которые хранятся в специальной БД. При совпадении паролей разрешается доступ пользователя в систему. Принцип работы системы двухфакторной аутентификации фирмы VASCO представлен на рис. 2.

Рис. 2. Принцип работы системы двухфакторной аутентификации фирмы VASCO

Оценка безопасности систем двухфакторной аутентификации. Анализ современных систем аутентификации показал, что их безопасность измеряется путем деления разности между стоимостью атак и выгоды для атакующего на стоимости защиты от них. Таким образом, дорогие, хотя и более безопасные методы, такие как криптографические PKI-устройства с собственными защищенными каналами связи, экранов и клавиатур оцениваются так низко по шкале безопасности, в то время как банковские системы все еще преимущественно опираются на самый дешевый и, казалось бы, наименее защищенных способ использования PIN-кодов и паролей. Общая стоимость и сложность развертывания таких устройств часто перевешивает пользу от их сверхвысокой безопасности.

Угрозы безопасности в сети можно разделить на сетевые атаки (информация, поступающая с уда-

ленного агента) и локальные атаки, которые происходят от вредоносных программ, уже установленных на системе клиента, например, троянов, руткитов, и так далее. Часто оценки безопасности аутентификации сосредоточены главным образом на сетевых атаках, предполагая, что пользовательский терминал (т.е. настольный компьютер, ноутбук или мобильное устройство) является защищенной платформой [1 – 4]. Тем не менее, часто злоумышленник получает полный доступ к ПК жертвы через скрытые процессы связи, которые остались от вредоносных программ, использующие неисправленные дыры в безопасности лицензионного программного обеспечения. Системы двухфакторной аутентификации, основанные на одноразовых sms-паролях, используют два канала передачи, что существенно затрудняет злоумышленнику перехват обеих частей аутентификатора. Однако рост нежелательного программного обеспечения для мобильных устройств теперь позволяет злоумышленнику получить доступ к кодам аутентификации, отправленным через SMS не только с помощью традиционного перехвата с помощью вредоносного ПО, но и путем перехвата и дешифрования данных, передаваемых через сеть GSM-телекоммуникаций. Атаки аутентификации мобильных устройств успешно проводятся и без таких технологий. Вместо этого злоумышленник просто выдает себя за пользователя устройства и запрашивает, чтобы все SMS сообщения направлялись на другой номер телефона в течение всей атаки [5].

Исследование основных принципов построения крипто-кодовых схем Мак-Элиса и Нидеррайтера

Перспективным направлением в развитии криптографических средств защиты информации доказуемой стойкости являются крипто-кодовые механизмы, построение которых основано на сведении задачи взлома ключевых данных к решению теоретико-числовой задачи декодирования случайного кода [7 – 10]. Данные системы позволяют интегрировано обеспечивать доказуемую криптостойкость и достоверность передаваемой информации, а также манипулировать этими критериями в зависимости от ТТХ используемых каналов передачи информации, что существенно при использовании их в банковских системах в пиковые нагрузки на системы. Сложность их реализации сопоставима с симметричными криптоалгоритмами (блочно-симметричными шифрами (БСШ)).

В табл. 1 приведены результаты сравнительных исследований эффективности криптографических методов защиты информации при фиксированном уровне стойкости.

Таблица 1

Результаты сравнительных исследований эффективности криптографических методов защиты информации при фиксированном уровне стойкости

Методы криптографического преобразования	Модель безопасности	Длина ключевых данных, бит	Скорость криптопреобразования, бит/с	Дополнительные функции
Блочные симметричные шифры	Практическая	128, 256, 512	$10^6 – 10^9$	–
Поточные симметричные шифры	Практическая	128, 256, 512	$10^7 – 10^{10}$	–
Несимметричные RSA-подобные криптоалгоритмы	Доказуемая	3248 (128), 15424 (256)	$10^2 – 10^3$	–
Несимметричные криптоалгоритмы на эллиптических кривых	Доказуемая	283 (128), 571 (256)	$10^3 – 10^4$	–
Несимметричные криптоалгоритмы с использованием кодовых конструкций	Доказуемая	$0{,}5 \cdot 10^6$ (128), $2 \cdot 10^6$ (256)	$10^6 – 10^8$	Контроль ошибок

Таким образом, несимметричные криптосистемы с использованием крипто-кодовых схем позволяют реализовать криптографическую защиту информации по технологии открытых ключей, обеспечить скорость крипто-кодового преобразования информации со скоростью шифрования блочно-симметричных шифров, и повысить достоверность передаваемых данных на основе канального кодирования. Общая классификация известных методов построения теоретико-кодовых схем приведена на рис. 3.

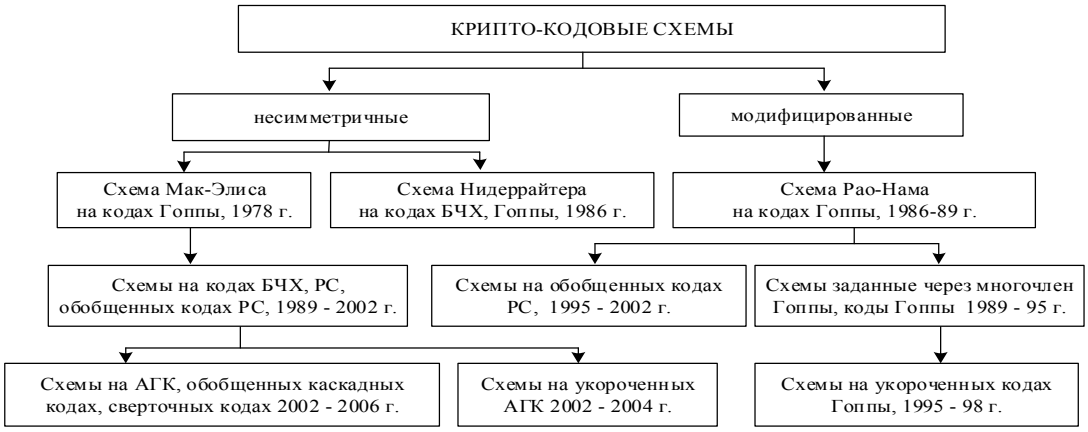

Рис. 3. Общая классификация крипто-кодовых схем

Общая конструкция крипто-кодовых схем

Рассмотрим общую конструкцию крипто-кодовых схем. Зафиксируем конечное поле GF(q). Рассмотрим векторное пространство $GF^n(q)$ как множество n-последовательностей элементов из GF(q) с покомпонентным сложением и умножением на скаляр. Линейный (n, k, d) код C есть подпространство в $GF^n(q)$, т.е. непустое множество n-последовательностей (кодовых слов) над GF(q), k – размерность линейного подпространства, d – минимальное кодовое расстояние (минимальный вес ненулевого кодового слова).

Основной целью кодирования информации является контроль (обнаружение и исправление) ошибок, произошедших при передаче сообщения по каналу с шумами. Для контроля ошибок кодирующее устройство вносит избыточность (проверочную часть длины r, r = n – k) в передаваемые данные. На приемной стороне, анализируя свойства проверочной части и ее соответствие передаваемым данным, декодер уменьшает влияние ошибок, возникших при передаче.

Задача раскодирования может быть эффективно решена (с полиномиальной сложностью) для узкого класса кодов, например, кодов БЧХ и кодов Рида-Соломона. Одним из наиболее эффективных алгоритмов алгебраического декодирования кодов БЧХ является алгоритм Берлекемпа-Месси и его модификации (улучшения). Известно, что алгоритм Берлекемпа-Месси содержит число реализации умножений, порядка t^2, или, формально, сложность алгоритма $O(t^2)$, где t – исправляющая способность кода, $t = \lfloor (d-1)/2 \rfloor$. Для большого t используют ускоренный алгоритм Берлекемпа-Месси, позволяющий уменьшить вычислительную сложность алгоритма. Еще более эффективным, с точки зрения вычислительной сложности, является рекуррентный алгоритм Берлекемпа-Месси. Асимптотическая сложность декодирования кодов Рида-Соломона в этом случае не превосходит величины $O(n\log^2 n)$, причем очень близка к величине O(nlogn).

Декодирование произвольного линейного кода (кода общего положения) является весьма сложной вычислительной задачей, сложность ее решения растет экспоненциально. Так, для корреляционного декодирования произвольного (n, k, d) кода над GF(q) необходимо, в общем случае, сравнить принятую последовательность со всеми q^k кодовыми словами и выбрать ближайшее (в метрике Хемминга). Даже для небольших n, k, d и q задача корреляционного декодирования весьма трудоемка. Это положение лежит в основе всех криптосистем на алгебраических блоковых кодах. Маскируя код с быстрым алгоритмом декодирования (полиномиальной сложности) под произвольный (случайный) линейный код можно представить задачу декодирования для постороннего наблюдателя (возможного злоумышленника) как вычислительно сложную задачу (экспоненциальной сложности). Для уполномоченного пользователя криптосистемы (имеющего секретный ключ) декодирование – полиноминально разрешимая задача.

Принципы построения крипто-кодовых схем на эллиптических кодах

Одним из перспективных направлений в развитии алгебраической теории кодов являются методы алгеброгеометрического кодирования. Недвоичные алгебраические блоковые коды, построенные по алгебраическим кривым (алгеброгеометрические коды) обладают хорошими асимптотическими свойствами. Доказано, что при большой длине эти коды лежат выше границы Варшамова-Гилберта [6].

Зафиксируем конечное поле GF(q). Пусть X – гладкая проективная алгебраическая кривая в проективном пространстве P^n над GF(q), g = g(X) – род кривой, X(GF(q)) – множество ее точек над конечным полем, N = X(GF(q)) – их число. Пусть C – класс дивизоров на X степени $\alpha > g - 1$. Тогда C определяет отображение $\varphi: X \to P^{k-1}$, где $k \ge \alpha - g + 1$. Набор $y_i = \varphi(x_i)$ задает код. Число точек в пересечении $\varphi(X)$ с гиперплоскостью равно α, т.е. $n - d \le \alpha$. Эта конструкция позволяет строить коды с параметрами $k + d \ge n - g + 1$, длина n которых меньше либо равна числу точек на кривой X. При $2g < \alpha \le n$ алгеброгеометрический код имеет параметры $(n, \alpha - g + 1, d)$, $d \ge n - \alpha$. Двойственный к нему код также является алгеброгеометрическим и имеет параметры $(n, n - \alpha + g - 1, d^{\perp})$, $d^{\perp} \ge \alpha - 2g + 2$. Дадим следующее определение алгеброгеометрического кода.

Определение 1. Пусть X – гладкая проективная алгебраическая кривая в проективном пространстве P^n, т. е. совокупность решений однородного неприводимого алгебраического уравнения степени degX с коэффициентами из GF(q). Рассмотрим многообразия, соответствующие проективным гиперповерхностям, заданным P^n уравнениями F = 0, где F – однородные одночлены степени degF. Пусть $I(i_1, i_2, \ldots, i_n)$ – информационная последовательность. Алгеброгеометрический код по кривой X над GF(q) – это линейный код длины $n \le N$, кодовые слова $C(c_1, c_2, \ldots, c_n)$ которого задаются равенством

$$\sum_{i=0}^{k-1} i_j F_j(P_i) = c_i ,$$

где $P_i(X_i, Y_i, Z_i)$ – проективные точки кривой X, т.е. (X_i, Y_i, Z_i) – решения однородного алгебраического уравнения, задающие кривую X, $i = \overline{1, n}$; $F_j(P_i)$ – значения генераторных функций в точках кривой.

Это определение равносильно матричному представлению алгеброгеометрического кода:

$$G\,(i_0, i_1, ..., i_{k-1})^T = (c_0, c_1, ..., c_{n-1}),$$

где G – порождающая матрица размерности k×n, k = α - g+1, α=degX·degF.

$$G = \begin{pmatrix} F_0(P_0) & F_0(P_1) & ... & F_0(P_{n-1}) \\ F_1(P_0) & F_1(P_1) & ... & F_1(P_{n-1}) \\ ... & ... & ... & ... \\ F_{k-1}(P_0) & F_{k-1}(P_1) & ... & F_{k-1}(P_{n-1}) \end{pmatrix} = \left\| F_j(P_i) \right\|_{n,k}.$$

Определение 2 [7; 8]. *Эллиптической кривой (EC)* в аффинном пространстве A^2 над полем GF(q) называется гладкая кривая, заданная уравнением

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

или в P^2 заданная однородным уравнением

$$y^2z + a_1xyz + a_3yz^2 = x^3 + a_2x^2z + a_4xz + a_6z^3,$$

$a_i \in GF(q)$, род кривой g = 1.

Утверждение 1 [7; 8]. Алгеброгеометрический (n, k, d) код по эллиптической кривой (эллиптический код) над GF(q) построенный через отображение вида $\varphi: EC \to P^{k-1}$ связан характеристиками k + d ≥ n, причем:

$n \le 2\sqrt{q} + q + 1$, k ≥ α, d ≥ n – α, α = 3 · degF.

Определение 3. Пусть X – гладкая проективная алгебраическая кривая в P^n, т.е. совокупность решений однородного неприводимого алгебраического уравнения степени degX с коэффициентами из GF(q), F – однородные одночлены степени degF. Алгеброгеометрический код по кривой X над GF(q) – это линейный код, состоящий из всех слов (c_1, c_2, …, c_n) длины n ≤ N, для которых выполняется равенство d + g – 1 уравнений

$$\sum_{i=0}^{n-1} c_i F_j(P_i) = 0,$$

где $c_i \in GF(q)$, d ≥ α – 2g + 2, α = degX · degF.

Это определение равносильно матричному представлению алгеброгеометрического кода:

$$H\,(c_0, c_1, ..., c_{n-1})^T = 0,$$

где H – проверочная матрица кода размерности r × n, r = n – k = d + g – 2.

$$H = \begin{pmatrix} F_0(P_0) & F_0(P_1) & ... & F_0(P_{n-1}) \\ F_1(P_0) & F_1(P_1) & ... & F_1(P_{n-1}) \\ ... & ... & ... & ... \\ F_{r-1}(P_0) & F_{r-1}(P_1) & ... & F_{r-1}(P_{n-1}) \end{pmatrix} = \left\| F_j(P_i) \right\|_{n,r}.$$

Утверждение 2 [7; 8]. Эллиптический (n, k, d) код над GF(q), построенный через отображение вида: $EC \to P^{r-1}$ связан характеристиками k + d ≥ n, причем: $n \le 2\sqrt{q} + q + 1$, k ≥ n – α, d ≥ α, α = 3 · degF.

Определения 1-2 и результат утверждения 1 позволяют задать теоретико-кодовую схему Мак-Эллиса на основе эллиптических кодов следующим образом. Пусть G^{EC} – порождающая матрица эллиптического (n, k, d) кода над GF(q) вида

$$G^{EC} = \begin{pmatrix} F_0(P_0) & F_0(P_1) & ... & F_0(P_{n-1}) \\ F_1(P_0) & F_1(P_1) & ... & F_1(P_{n-1}) \\ ... & ... & ... & ... \\ F_{k-1}(P_0) & F_{k-1}(P_1) & ... & F_{k-1}(P_{n-1}) \end{pmatrix} = \left\| F_j(P_i) \right\|_{n,k}$$

и размерности k×n, k = α, α=3·degF.

Пусть X – невырожденная k × k-матрица над GF(q), D – диагональная матрица с ненулевыми на диагонали элементами, P – перестановочная матрица размера n × n.

Определим несимметричную схему Мак-Эллиса с эллиптическим кодом:

– открытый ключ – матрица

$$G_X^{EC} = X \cdot G^{EC} \cdot P \cdot D,$$

– секретный (закрытый) ключ – матрицы X, P, D.

Закрытая информация (кодограмма) представляет собой вектор длины n и вычисляется по правилу

$$c_X^* = i \cdot G_X^{EC} + e,$$

где вектор $c_X = i \cdot G_X^{EC}$ принадлежит эллиптическому (n, k, d) коду с порождающей матрицей G_X^{EC}, i – k-разрядный информационный вектор, вектор e – секретный вектор ошибок веса ≤ t.

Чтобы задать *несимметричную схему Нидеррайтера на эллиптических кодах* воспользуемся другим определением алгеброгеометрического кода.

Определение 3 [7; 8]. Пусть X – гладкая проективная алгебраическая кривая в P^n, т.е. совокупность решений однородного неприводимого алгебраического уравнения степени degX с коэффициентами из GF(q), F – однородные одночлены степени degF. *Алгеброгеометрический код по кривой X* над *GF(q)* – это линейный код, состоящий из всех слов (c_1, c_2, …, c_n) длины n ≤ N, для которых выполняется равенство d + g – 1 уравнений

$$\sum_{i=0}^{n-1} c_i F_j(P_i) = 0,$$

где $c_i \in GF(q)$, d ≥ α – 2g + 2, α = degX · degF.

Это определение равносильно матричному представлению алгеброгеометрического кода:

$$H\,(c_0, c_1, ..., c_{n-1})^T = 0,$$

где H – проверочная матрица кода размерности r × n, r = n – k = d + g – 2

$$H = \begin{pmatrix} F_0(P_0) & F_0(P_1) & ... & F_0(P_{n-1}) \\ F_1(P_0) & F_1(P_1) & ... & F_1(P_{n-1}) \\ ... & ... & ... & ... \\ F_{r-1}(P_0) & F_{r-1}(P_1) & ... & F_{r-1}(P_{n-1}) \end{pmatrix} = \left\| F_j(P_i) \right\|_{n,r}.$$

Определение 3 и результат утверждения 2 позволяют определить теоретико-кодовую схему Нидеррайтера на основе эллиптических кодов следую-

щим образом. Пусть H^{EC} – проверочная матрица эллиптического (n, k, d) кода над GF(q) вида

$$H^{EC} = \begin{pmatrix} F_0(P_0) & F_0(P_1) & ... & F_0(P_{n-1}) \\ F_1(P_0) & F_1(P_1) & ... & F_1(P_{n-1}) \\ ... & ... & ... & ... \\ F_{r-1}(P_0) & F_{r-1}(P_1) & ... & F_{r-1}(P_{n-1}) \end{pmatrix} = \left\| F_j(P_i) \right\|_{n,r}$$

и размерности r×n, r = α, α=3·degF.

Пусть X – невырожденная k × k-матрица над GF(q), D – диагональная матрица с ненулевыми на диагонали элементами, P – перестановочная матрица размера n × n. Определим несимметричную *схему Нидеррайтера с эллиптическим кодом*:

– открытый ключ – матрица

$$H_X^{EC} = X \cdot H^{EC} \cdot P \cdot D,$$

– секретный (закрытый) ключ – матрицы X, P, D.

Закрытая информация (кодограмма) представляет собой вектор длины n и вычисляется по правилу

$$S_X = e \cdot \left(H_X^{EC} \right)^T,$$

где вектор e – вектор длины n и веса ≤ t, который несет конфиденциальную информацию (информационное сообщение, подлежащее закрытию).

Доказанные утверждения 1–2 и предложенные теоретико-кодовые схемы с эллиптическими кодами позволяют формировать кодограммы по несимметричному алгоритму, т.е. использовать открытый ключ для обмена закрытой информации.

Данные крипто-кодовые схемы позволяют интегрировано обеспечивать достоверность и доказуемую безопасность передаваемых данных. При этом схема Мак-Элиса, использующая при формировании кодового слова вектор ошибки, позволяет изменять данные критерии в зависимости от требований увеличения показателя достоверности или безопасности. Вес вектора ошибки $w(e)$ лежит в пределах исправляющей способности кода и является определяющей величиной при оценке достигаемого уровня безопасности и достоверности передачи данных. Задача криптоанализа крипто-кодовых средств защиты информации эквивалентна решению задачи декодирования алгебраического блокового (n, k, d) кода над $GF(q)$, замаскированного для неуполномоченного пользователя (злоумышленника) под случайный код (код общего положения), т.е. для решения задачи криптоанализа следует решить задачу декодирования кодового слова (n, k, d) кода с внесенными $w(e)$ ошибками. Таким образом, можем записать:

$$S_Б = f\left(\frac{w(e)}{t} \right), \; t = \left\lfloor \frac{d-1}{2} \right\rfloor,$$

где $f(x)$ – неубывающая функция относительно x;

$\frac{w(e)}{t}$ – нормированный относительно исправляющей способности (n, k, d) кода вес вектора e, причем:

1) если $w(e) = t = \left\lfloor \frac{d-1}{2} \right\rfloor$, тогда крипто-кодовая система защиты информации обеспечивает максимально возможный при использовании применяемого (n, k, d) кода уровень безопасности передачи данных;

2) если $w(e) = 0$, тогда крипто-кодовая система защиты информации функционирует как система помехоустойчивого кодирования, безопасность передачи данных не обеспечивается;

3) если $w(e)$ лежит в интервале $0 < w(e) < t$, тогда уровень обеспечиваемой крипто-кодовой системой защиты информации определяется величиной $w(e)$.

Достигаемый уровень достоверности передачи данных при использовании крипто-кодовых средств защиты информации также зависит от веса $w(e)$:

$$S_Д = f^*\left(\frac{t - w(e)}{t} \right), \; t = \left\lfloor \frac{d-1}{2} \right\rfloor,$$

где $f^*(x)$ – неубывающая функция относительно x;

$\frac{t - w(e)}{t}$ – нормированная относительно исправляющей способности кода величина, обратная весу вектора e относительно t, причем:

1) если $w(e) = t = \left\lfloor \frac{d-1}{2} \right\rfloor$, тогда крипто-кодовая система защиты информации не позволяет исправлять возникающих при передаче данных ошибок, достоверность не обеспечивается;

2) если $w(e) = 0$, тогда крипто-кодовая система защиты информации позволяет исправлять $w(e) \le t = \left\lfloor \frac{d-1}{2} \right\rfloor$ возникающих при передаче данных ошибок, обеспечивается максимально возможная при использовании применяемого (n, k, d) кода достоверность;

3) если $w(e)$ лежит в интервале $0 < w(e) < t$, тогда крипто-кодовая система защиты информации позволяет исправлять $t - w(e)$ возникающих при передаче данных ошибок, обеспечиваемая достоверность определяется величиной $t - w(e)$. Таким образом, адаптивное изменение веса $w(e)$ последовательностей сеансовых ключей $e = (e_0, e_1, ..., e_{n-1})$ в зависимости от условий применения крипто-

кодовой защиты информации позволяет интегрировано обеспечивать требуемые показатели безопасности и достоверности передачи данных.

Для повышения оперативности обработки данных крипто-кодовой системе Нидеррайтера в работах [9; 10] предлагается использовать метод недвоичного равновесного кодирования на основе обобщенного биномиально-позиционного представления, который позволяет обобщить рассмотренный выше подход на недвоичный случай и практически реализовать вычислительные алгоритмы формирования недвоичных последовательностей фиксированного веса. Процесс формирования равновесной недвоичной последовательности представим в четыре этапа.

1. Представление числа A в виде чисел $A_Б$ и

$$A_П:\ A_Б = \left\lfloor \frac{A}{(q-1)^w} \right\rfloor,\ A_П = (A) \bmod \left((q-1)^w\right),$$

где $\lfloor y \rfloor$ – целая часть числа y.

Однозначность представления числа A в виде чисел $A_Б$ и $A_П$ обосновывается китайской теоремой об остатках.

Число $A_Б$ лежит в пределах

$$0 \le A_Б < \frac{M}{(q-1)^w}$$

и может, таким образом, быть представлено в биномиальной системе счисления с кодовыми ограничениями:

$$\begin{cases} \forall j: w(c_j) = \text{const} = w; \\ 0 \le A_Б < \dfrac{n!}{w!(n-w)!}; \\ 0 \le w \le n. \end{cases}$$

Число $A_П$ лежит в пределах $0 \le A_П < (q-1)^w$ и, соответственно, может быть представлено в позиционной системе счисления по основанию $h = q-1$.

2. Представление числа $A_Б$ в биномиальной системе счисления:

$$A_Б = \sum_{i=0}^{n-1} a_{Бi} b_i,\ b_i = \binom{n-i-1}{w-1}.$$

3. Представление числа $A_П$ в позиционной системе счисления:

$$A_П = \sum_{l=0}^{w-1} (a_l - 1) h^l,\ h = q-1.$$

4. Формирование последовательности

$$C_A = \left(C_{A_0}\ \ C_{A_1}\ \ \ldots\ \ C_{A_{n-1}}\right) \in C:$$

$$C_{A_i} = a_l a_{Бi},\ i = 0,1,\ldots,n-1,\ l = 0,1,\ldots,w-1,$$

т.е., если для некоторого $i = 0,1,\ldots,n-1$ в представлении $A_Б$ имеем $a_{Бi} = 0$, тогда получим $C_{A_i} = 0$; если $a_{Бi} = 1$, тогда получим $C_{A_i} = a_l$, т.е. искомый элемент равен соответствующему ненулевому элементу в представлении $A_П$.

Таким образом, формирование криптограмм в крипто-кодовой схеме Нидеррайтера осуществляется посредством выполнения процедур и функций равновесного и неравновесного алгебраического кодирования, методов маскирования соответствующих кодов под случайную последовательность и функциональных операций над конечными полями.

Алгоритм формирования криптограмм в предложенных крипто-кодовых средствах защиты информации представим следующим образом.

Шаг 1. Ввод информационного сообщения $M_i = (I_0, I_1, \ldots, I_{k-1})$, $\forall I_j \in GF(q)$, ключевых данных и общесистемных параметров. Под общесистемными параметрами понимаются порождающая и проверочная матрицы, задающие алгебраический блоковый код, совокупность формализованных данных, задающих правило равновесного кодирования недвоичными последовательностями.

Шаг 2. Равновесное кодирование введенного информационного сообщения, т.е. преобразование вектора $M_i = (I_0, I_1, ..., I_{m-1})$ в вектор

$$\varepsilon_i = (e_0, e_1, ..., e_{n-1}),\ \forall e_j \in GF(q).$$

Шаг 3. Разворачивание ключевых данных и формирование проверочной матрицы H_X^j замаскированного алгебраического блокового (n, k, d) кода над GF(q).

Шаг 4. Формирование синдромной последовательности (криптограммы):

$$E_i = (S_{X_0}, S_{X_1}, ..., S_{X_{n-k-1}}),\ \forall S_{X_j} \in GF(q),$$

посредством умножения равновесной последовательности $\varepsilon_i = (e_0, e_1, ..., e_{n-1})$ на транспонированную матрицу $\left(H_X^j\right)^T$.

Шаг 5. Вывод сформированной криптограммы

$$E_i = (S_{X_0}, S_{X_1}, ..., S_{X_{n-k-1}}).$$

Проведенные исследования на основе программной реализации рассмотренных крипто-кодовых схем Мак-Элиса и Нидеррайтера показали, что требуемые показатели криптостойкости (10^{21} – 10^{25} групповых операций) и достоверности передаваемой информации ($P_{ош} = 10^{-9} – 10^{-12}$) обеспечиваются при их построении над расширенным полем GF (2^5), что с ростом вычислительных технологий может быть недостаточно [7; 8]. Однако увеличение мощности поля приводит к значительному снижению вычислительной мощности. В табл. 2 приведены результаты исследований зависимости количества вызовов функций, реализующих элементарные операции при программной реализации в зависимости от увеличения информационной последовательности (увеличения мощности расширенного поля Галуа).

Таблица 2

Анализ производительности при кодового слова в ККС от длины информационной посылки

	Крипто-кодовые схемы					
	Niderveter			MacElis		
K, бит	10	100	1000	10	100	1000
Количество вызовов функций, реализующих элементарные операции	1 734 132	3 691 362	23 263 662	16 516 381	46 125 790	120 639 896

Результат, представленный в табл. 2, показывает значительное увеличение запросов процессора при реализации функции формирования кодового слова, при этом затраты с использованием схемы Мак-Элиса на порядок выше, чем схемы Нидеррайтера.

Схема двухфакторной аутентификации на основе использования крипто-кодовых схем Мак-Элиса и Нидеррайтера

Проведенный анализ Интернет-атак на схемы двухфакторной аутентификации с использованием sms-сообщений и достоинства крипто-кодовых схем позволяют усовершенствовать схему двухфакторной аутентификации с целью повышения уровня криптостойкости и достоверности формируемого аутентификатора.

Для этого банковская карточка (БК), должна хранить следующие элементы данных:

(1) *Индекс открытого ключа центра сертификации* – так как терминал может работать с несколькими центрами сертификации, эта величина специфицирует, какой из ключей необходимо использовать терминалу при работе с данной картой.

(2) *Сертификат открытого ключа эмитента* – подписывается соответствующим центром сертификации.

(3) *Сертификат открытого ключа БК* – подписывается эмитентом и формируется на основе схемы Мак-Элиса.

(4) Модуль и экспоненту открытого ключа эмитента.

(5) Модуль и экспоненту открытого ключа БК.

(6) Секретный ключ БК.

Терминал, поддерживающий схему двухфакторной аутентификации, должен хранить открытые ключи всех центров сертификации и ассоциированную информацию, относящуюся к каждому из ключей.

Терминал должен также уметь выбирать соответствующие ключи на основе индекса (1) и некоторой специальной идентификационной информации.

Для поддержки двухфакторной аутентификации банковская карточка (БК) пользователя должна иметь свою собственную ключевую пару (открытый и секретный ключи аутентификатора). Открытый ключ БК хранится на БК в сертификате её открытого ключа. Каждый открытый ключ БК сертифицируется её эмитентом, а доверенный центр сертификации сертифицирует открытый ключ эмитента. Это означает, что для проверки аутентификатора карты терминалу вначале необходимо проверить два сертификата для того, чтобы восстановить и аутентифицировать открытый ключ БК, который затем применяется при проверке аутентификатора БК.

Процесс предлагаемой аутентификации состоит из четырех этапов:

(1) *Восстановление терминалом открытого ключа центра сертификации*. Терминал считывает индекс (1), идентифицирует и извлекает хранящиеся в нём модуль и экспоненту открытого ключа центра сертификации, и ассоциированную информацию, выбирает соответствующие алгоритмы.

(2) *Получение секретных мест в векторе ошибки от банка эмитента*. Формирование вектора ошибки путем введения пользователем кратности.

(3) *Формирование аутентификатора на основе использования схемы Мак-Элиса*. Получение кодового слова (аутентификатора) на основе использования крипто-кодовой схемы.

(4) *Проверка подлинности аутентификатора.* Нахождение кратности вектора ошибки и сравнение с полученным. Структура предлагаемого метода двухфакторной аутентификации на основе криптокодовых схем Мак-Элиса и Нидеррайтера представлена на рис. 4.

Существенным достоинством, на взгляд авторов, использования данной двухфакторной схемы аутентификации является обеспечение требуемых показателей криптостойкости передаваемых транзакций, использование сеансового ключа при каждой транзакции и упрощенный алгоритм является раскодирования (в алгоритме Берлекемпа-Месси нет необходимости выполнять задачу локализации по процедуре Месси), возможность передачи по различным каналам связи (от воздушных до цифровых), масштабируемость программного модуля путем изменения использования ККС Мак-Элиса и Нидеррайтера.

Выводы

Проведенный анализ методов двухфакторной аутентификации показал, что практически все системы в своей основе используют криптографические алгоритмы (таблицы) и подвержены как традиционным атакам на криптографические процедуры, так и атакам, на основе социальной инженерии, и не в полном объеме обеспечивают безопасность их использования в банковских системах. Предложенная схема аутентификации на крипто-кодовых схемах Мак-Элиса и Нидеррайтера позволит обеспечить доказуемую стойкость и достоверность передаваемой информации.

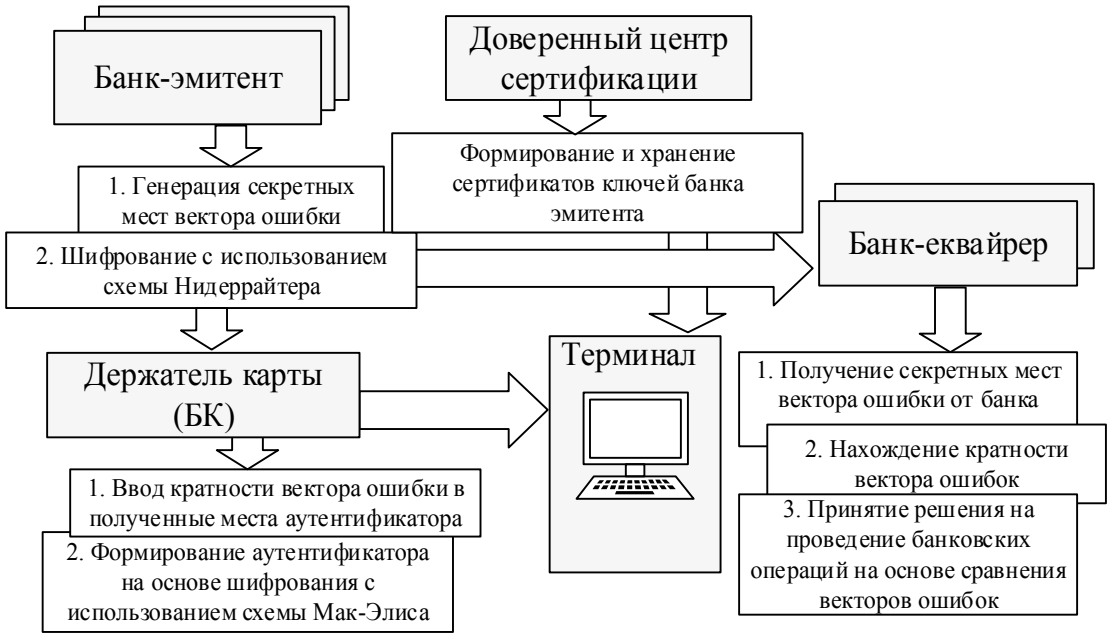

Рис. 4. Структура предлагаемого метода двухфакторной аутентификации на основе крипто-кодовых схем Мак-Элиса и Нидеррайтера

Перспективным направлением дальнейших исследований является формирование процедур протокола аутентификации на основе крипто-кодовых схем.

Список литературы

1. Двухфакторная Аутентификация [Электронный ресурс]. – Режим доступа к ресурсу: http://www.aladdin-rd.ru/solutions/authentication/.

2. Настройка двухфакторной аутентификации [Электронный ресурс]. – Режим доступа к ресурсу: http://support.citrix.com/proddocs/topic/web-interface-impington/nl/ru/wi-configure-two-factor-authentication-gransden.html?locale=ru.

3. Семь методов двухфакторной аутентификации [Электронный ресурс]. – Режим доступа к ресурсу: http://www.infosecurityrussia.ru/news/29947.

4. Двухфакторная аутентификация при удаленном доступе [Электронный ресурс]. – Режим доступа к ресурсу: http://itc.ua/articles/dvuhfaktornaya_autentifikaciya_pri_udalennom_dostupe_23166/.

5. Евсеев С.П. Исследование методов двухфакторной аутентификации / С.П. Евсеев, О.Г. Король // Системи обробки інформації. – 2014. – Вип. 2(118). – С. 81-87.

6. Блейхут Р. Теория и практика кодов, контролирующих ошибки: Пер. с англ. / Р. Блейхут. – М.: Мир, 1986. – 576 с.

7. Евсеев С.П. Несимметричный алгоритм шифрования с использованием эллиптических кодов / С.П. Евсеев // Збірник наукових праць ХПІ. – Х.: ХПІ, 2004. – Вип. 46. – С. 175-180.

8. Кузнецов А.А. Разработка теоретико-кодовых схем с использованием эллиптических кодов / А.А. Кузнецов, С.П. Евсеев // Системи обробки інформації. – Х.: ХВУ, 2004. – Вип. 5. – С. 127-132.

9. Дудикевич В.Б. Метод недвійкового рівноважного кодування / В.Б. Дудикевич, О.О. Кузнецов, Б.П. Томашевський // Сучасний захист інформації. – 2010. – №3. – С. 57-68.

10. Дудикевич В.Б. Крипто-кодовий захист інформації з недвійковим рівноваговим кодуванням / В.Б. Дудикевич, О.О. Кузнецов, Б.П. Томашевський // Сучасний захист інформації. – 2010. – №2. – С. 14-23.

Поступила в редколлегию 18.02.2015

Рецензент: д-р техн. наук, проф. В.А. Хорошко, Национальный авиационный университет, Киев.

ПОБУДОВА СХЕМИ ДВОФАКТОРНОЇ АВТЕНТИФІКАЦІЇ НА ОСНОВІ ВИКОРИСТАННЯ КРИПТО-КОДОВИХ СХЕМ

С.П. Євсеєв, Ю.П. Томашевський, В.В. Огурцов, Т.О. Свердло

Розглядаються основні принципи побудови крипто-кодових схем Мак-Еліса і Нідеррайтера. Проводиться аналіз різних систем двофакторної автентифікації, їх протистояння різних видів атак. Пропонується схема двофакторної автентифікації на основі використання крипто-кодових схем Мак-Еліса і Нідеррайтера з метою підвищення криптостійкості формованого автентифікатора у схемі двофакторної автентифікації.

Ключові слова: *двофакторна автентифікація, крипто-кодові схеми Мак-Еліса і Нідеррайтера.*

CONSTRUCTION OF TWO-FACTOR AUTHENTICATION SCHEME BASED ON CRYPTO-CODING SCHEMES USAGE

S.P. Yevseiev, B.P. Tomashevskyy, V.V. Ohurtsov, T.A. Sverdlo

The basic principles of the crypto-code schemes McEliece and Niederreiter. The analysis of the various systems of two-factor authentication, their opposition to various types of attacks. The scheme of two-factor authentication using crypto-code schemes McEliece and Niederreiter in order to increase the reliability of the authenticator generated in the two-factor authentication scheme.

Keywords: *two-factor authentication, crypto-code scheme McEliece and Niederreiter.*