Anderson, editor, Fast Software Encryption – Cambridge Security Workshop, pp. 179–184, Springer-Verlag, Berlin, 1994.

УДК 621.391, 519.7

АЛГЕБРАИЧЕСКИЕ МОДЕЛИ КРИПТОГРАФИЧЕСКИХ СИСТЕМ С ОТКРЫТЫМ КЛЮЧОМ

Антон Алексейчук, Сергей Пришлин, Александр Романов
Военный институт телекоммуникации и информатизации НТУУ "КПИ"

Анотація: **Запропоновані загальні алгебраїчні моделі систем відкритого шифрування інформації та систем цифрового підпису, які є багатоосновними універсальними алгебрами. В межах розроблених моделей стисло охарактерізовані основні задачі аналізу стійкості систем з відкритим ключем, розглянуті взаємозв'язки між системами цифрового підпису і відкритого шифрування, а також приклади застосування алгебраїчних моделей цих систем.**
Summary: **There were proposed the general algebraic models of the open encryption systems and digital signature that are the multybase universal algebras. Within a framework of the designed models the general problems of the analysis of the security of the public-key systems were briefly characterized, the connections between the systems of public-key encryption and digital signature were considered. The examples of practical using of these algebraic models were given.**
Ключові слова: **Система відкритого шифрування, система цифрового підпису, багатоосновна алгебра.**

I Введение

После выхода в свет в 1976 году известной работы У. Диффи и М. Хеллмана [1], в которой впервые были изложены принципы построения систем открытого шифрования и открытого распределения ключей, появилось большое число различных вариантов таких систем, многие из которых послужили источниками новых математических задач. В 1994 году В. А. Артамонов и В. В. Ященко [2] предложили единую алгебраическую модель процедуры выработки общего ключа (так называемую public key- или pk-алгебру), включающую в себя почти все известные ранее системы открытого распределения ключей.

В последнее время наблюдается повышенный интерес исследователей к изучению математических моделей систем обработки и хранения дискретной информации (в том числе криптографических систем), представляющих собой алгебраические структуры – многоосновные универсальные алгебры (см., например, [2 – 6]). Отметим, что общая алгебраическая модель шифра по существу была предложена еще К. Шенноном [7]. Моделирование работы реальных устройств (алгоритмов) преобразования информации с помощью алгебраических структур дает возможность приблизиться к более глубокому пониманию принципов их построения и функционирования и позволяет на абстрактом уровне решать различные теоретические задачи анализа и синтеза таких устройств.

II Постановка задачи

Разнообразие известных в настоящее время систем открытого шифрования и цифровой подписи обусловливает актуальность задачи построения абстрактых алгебраических моделей указанных систем с целью анализа и осмысления с единых общих позиций их криптографических свойств, а также уточнения специфических особенностей, присущих конкретным криптосистемам открытого шифрования и цифоровой подписи. В отличие от известной модели системы открытого распределения ключей (pk-алгебры [2]), авторам не удалось найти в общедоступной литературе описание аналогичных моделей систем открытого шифрования и цифровой подписи, представленных в виде многоосновных универсальных алгебр.

III Основная часть

Как известно, существенной особенностью несимметричных криптосистем является использование различных ключей для зашифрования и расшифрования информации. При этом указанные ключи связаны определенной функциональной зависимостью таким образом, что вычислить по одному из них (открытому) второй (секретный) практически невозможно. Именно наличие такой зависимости позволяет организовать обмен шифрованными сообщениями с использованием только открытых каналов связи, то есть отказаться от секретных каналов для преварительного обмена ключами.

Один из возможных общих подходов к формальному определению системы открытого шифрования состоит в следующем. Рассмотрим многоосновную алгебру

$$\mathfrak{I} = (X, K, Y, U, L, \theta, f, g), \quad (1)$$

где X, K, Y, U, L – непустые конечные множества, θ: $K \to U$, f: $X \times U \times L \to Y$ и g: $Y \times K \to X$ – отображения, удовлетворяющие следующим условиям:

а) θ – сюръекция;

б) для любых $k \in K$, $x \in X$, $l \in L$ справедливо равенство

$$g(f(x, \theta(k), l), k) = x. \quad (2)$$

Назовем алгебру $\mathfrak{I}$ *системой открытого шифрования* (или *несимметричной криптосистемой*) *с множеством открытых текстов* (*сообщений*) X, *множеством шифрованных текстов* Y, *множеством секретных ключей* K, *множеством открытых ключей* U, *множеством параметров* L и *функциями зашифрования и расшифрования* f *и* g *соответственно*. Будем говорить, что открытый ключ $u \in U$ соответствует секретному ключу $k \in K$ криптосистемы $\mathfrak{I}$, если выполняется равенство $u = \theta(k)$.

Практическое использование криптосистемы $\mathfrak{I}$ для обмена зашифрованной информацией между группой абонентов (пользователей телекоммуникационной системы) осуществляется следующим образом.

Каждый из абонентов вырабатывает (известный только ему) секретный ключ $k \in K$ и вычисляет соответствующий k открытый ключ $u = \theta(k)$. Пусть некоторому абоненту A требуется передать (с сохранением конфиденциальности) открытое сообщение $x \in X$ другому абоненту B. Для этого A фиксирует элемент $l \in L$ (который хранит в секрете), зашифровывает сообщение x на открытом ключе $u = u_B$ абонента B с помощью функции f и посылает B шифрованный текст $y = f(x, u_B, l)$. Абонент B, в свою очередь, расшифровывает y на собственном секретном ключе $k = k_B$ с помощью функции g, то есть вычисляет значение $g(y, k_B)$, которое в силу равенства $\theta(k_B) = u_B$ и тождества (2) совпадает с исходным открытым сообщением x.

Как правило, вспомогательные параметры (элементы множества L) используются при зашифровании с целью повышения стойкости криптосистемы $\mathfrak{I}$. Последняя определяется вычислительной сложностью задачи нахождения открытого текста $x \in X$ по известным открытому ключу u_B и шифрованному тексту $y = f(x, u_B, l)$. В силу равенства (2) один из возможных путей решения этой задачи состоит в том, чтобы найти произвольный элемент $k \in K$, удовлетворяющий уравнению

$$\theta(k) = u_B \quad (3)$$

(например, определить секретный ключ k_B абонента B), а затем вычислить x по формуле $x = g(y, k)$. Таким образом, необходимым (но, очевидно, не достаточным) условием стойкости криптосистемы $\mathfrak{I}$ является высокая вычислительная сложность задачи решения уравнения (3). В подавляющем большинстве практических случаев указанная задача представляет собой известную сложную (в вычислительном плане) математическую проблему.

Пример 1. (*Система открытого шифрования RSA*).

Пусть p и q – различные простые числа, $n = pq$. Положим $X = Y = \boldsymbol{Z}_n = \{0, 1, \ldots, n-1\}$, $K = U = (\boldsymbol{Z}/\phi(n))^*$, где $\phi(n) = (p-1)(q-1)$, $(\boldsymbol{Z}/\phi(n))^*$ – множество обратимых элементов кольца $\boldsymbol{Z}/\phi(n)$.

Определим отображения θ: $K \to U$, f: $X \times U \to Y$ и g: $Y \times K \to X$ следующим образом:

$$\theta(k) = k^{-1} \pmod{\phi(n)}, \quad (4)$$

$$f(x, k) = g(x, k) \underset{\text{def}}{=} x^k \pmod{n},\ k \in (\boldsymbol{Z}/\phi(n))^*,\ x \in \boldsymbol{Z}_n. \quad (5)$$

Нетрудно убедиться в том, что в алгебре $\mathfrak{R}_{p,q} = (X, K, Y, U, \theta, f, g)$ выполняется тождество (2) и, следовательно, эта алгебра является системой открытого шифрования (с одноэлементым множеством параметров L). Назовем алгебру $\mathfrak{R}_{p,q}$ *криптосистемой RSA*. Далее, следуя сложившейся традиции, будем обозначать секретный ключ $k \in K = (\boldsymbol{Z}/\phi(n))^*$ символом d, а соответствующий ему открытый ключ $u = \theta(k) \in (\boldsymbol{Z}/\phi(n))^*$ – символом e.

Для обмена шифрованной информацией с абонентом A абонент B выбирает пару (p, q) различных простых чисел, задавая (фиксируя) тем самым вполне определенную алгебру $\mathfrak{R}_{p,q}$, которая (в отличие от самих чисел p и q) является общедоступной. Стойкость криптосистемы $\mathfrak{R}_{p,q}$ определяется вычислительной сложностью задачи нахождения открытого сообщения $x \in \boldsymbol{Z}_n$ по известным шифртексту

$$y = x^e \pmod{n}, \quad (6)$$

открытому ключу e и числу $n = pq$. Хорошо известно [4], что для решения указанной задачи достаточно найти p и q, то есть разложить число n на простые сомножители.

Пример 2. (*Система открытого шифрования Эль-Гамаля*).

Пусть p – простое число, a – примитивный элемент поля $\boldsymbol{GF}(p) = \{0, 1, \ldots, p-1\}$. Положим в равенстве (1)

$$X = \boldsymbol{GF}(p),\ K = U = \boldsymbol{GF}(p)^*,\ L = (\boldsymbol{Z}_{p-1})^*,\ Y = \boldsymbol{GF}(p)^* \times \boldsymbol{GF}(p),$$

$$\theta(k) = a^k,\ f(x, u, l) = (a^l, u^l x),\ g((y_1, y_2), k) = y_2 (y_1)^{-k}, \quad (7)$$

где $k \in K$, $x \in X$, $l \in L$, $(y_1, y_2) = y \in Y$ (операции умножения и возведения в степень в выражениях (7) выполняются

по модулю p). Нетрудно видеть, что многоосновная алгебра $\wp \overset{\text{def}}{=} (X, K, Y, U, L, \theta, f, g)$ удовлетворяет условиям а) и б) определения системы открытого шифрования. Действительно, условие а) (сюръективность отображения θ) выполняется в силу примитивности элемента $a \in \boldsymbol{GF}(p)$, а справедливость условия б) следует из (7) и равенств $g(f(x, \theta(k), l), k) = g((a^l, a^{kl} x), k) = a^{kl} x\,(a^l)^{-k} = x$.

Назовем построенную криптосистему $\wp$ *системой открытого шифрования* (или *криптосистемой) Эль-Гамаля* [8].

В соответствии с общим принципом, изложенным выше, практическая стойкость криптосистемы $\wp$ определяется вычислительной сложностью решения уравнения вида (3), то есть основывается на трудоемкости вычисления дискретного логарифма в поле $\boldsymbol{GF}(p)$ (см. (7)).

Особенностью криптосистемы $\wp$ является использование при зашифровании вспомогательного параметра $l \in L = (\boldsymbol{Z}_{p-1})^*$. На практике реализуются случайная генерация чисел l большого размера и их уничтожение после формирования шифрованных сообщений. Повторное использование данного значения l приводит к снижению стойкости шифрования [4].

Построим общую алгебраическую модель системы цифровой подписи.

Пусть X, K, Y, U, L – непустые конечные множества, называемые соответственно *множеством* (*подписываемых*) *сообщений*, *множеством секретных ключей*, *множеством подписей*, *множеством открытых ключей* и *множеством параметров*. Пусть далее $\theta: K \to U$, $f: X \times K \times L \to Y$ и $\delta: X \times Y \times U \to \{0, 1\}$ – отображения, удовлетворяющие условиям

а) θ – сюръекция;

б) для любых $x \in X$, $k \in K$, $l \in L$ имеет место равенство

$$\delta(x, f(x, k, l), \theta(k)) = 1. \tag{8}$$

Назовем алгебраическую структуру

$$\Lambda = (X, K, Y, U, L, \theta, f, \delta) \tag{9}$$

системой цифровой подписи. Отображение f назовем *функцией подписывания*, а отображение δ – *функцией проверки подписи*. Элемент $y = f(x, k, l)$ называется (*цифровой*) *подписью сообщения* $x \in X$ *на секретном ключе* $k \in K$ *при значении параметра* $l \in L$.

Рассмотрим схему обмена информацией между абонентами A и B с подверждением подлинности отправителя сообщений на основе системы цифровой подписи Λ вида (9). Вначале абонент A вычисляет по известному только ему секретному ключу $k \in K$ открытый ключ $u = \theta(k)$. Для передачи абоненту B сообщения $x \in X$ A фиксирует тем или иным способом значение параметра $l \in L$ (которое хранит в секрете) и вычисляет цифровую подпись $y = f(x, k, l)$ сообщения $x \in X$ на секретном ключе $k \in K$. Получив *подписанное сообщение* (x, y) абонент B осуществляет проверку подписи, то есть вычисляет значение $\delta(x, y, u)$. Если указанное значение равно 1, то сообщение x признается подписанным абонентом, который предоставил ранее открытый ключ u (то есть абонентом A). В противном случае (см. условие б) определения системы цифровой подписи) становится ясно, что сообщение x подписано кем-то другим или искажено до того, как попало к B.

Предположим, что противник, желая послать абоненту B сообщение $x' \in X$ от имени абонента A, подделывает его подпись, формируя подписанное сообщение (x', y'), где y' – некоторый элемент множества Y. Очевидно, что проверка подписи не вызовет у B подозрений (в том, что автором сообщения x' является именно A) тогда и только тогда, когда элемент y' удовлетворяет уравнению

$$\delta(x', y', u) = 1, \tag{10}$$

где

$$u = \theta(k) \tag{11}$$

– открытый ключ A. Следовательно, стойкость системы цифровой подписи Λ (относительно возможной подделки (фальсификации) подписей сообщений) определяется вычислительной сложностью задачи решения относительно $y' \in Y$ уравнения (10) при известных значениях $x' \in X$ и $u \in U$. Зная секретный ключ k абонента A, легко найти решение этого уравнения, вычисляя его по формуле $y' = f(x', k, l)$, где l может быть любым элементом множества L. Таким образом, как и в случае систем открытого шифрования, стойкость системы цифровой подписи Λ зависит, прежде всего, от вычислительной сложности восстановления секретного ключа k по известному открытому ключу u (трудоемкости алгоритмов решения уравнения (11)).

Известно, что в ряде случаев для построения систем цифровой подписи можно использовать системы открытого шифрования. Основная идея (предложенная У. Диффи и М. Хеллманом [1]) создания таких систем цифровой подписи заключается в том, чтобы поменять местами роли секретного и открытого ключей в несимметричной криптосистеме: сделать открытый ключ шифрования k' секретным ключом подписывания, а соответствующий ему секретный ключ расшифрования u' – открытым ключом проверки подписи. В

результате зашифрования сообщения x на ключе k' получим цифровую подпись y данного сообщения. Проверка подписи осуществляется путем сравнения x с сообщением, получаемым при расшифровании подписи y на ключе u'.

Дадим формальное определение *системы цифровой подписи*, *построенной на основе системы открытого шифрования*. Пусть $\mathfrak{I} = (X, K, Y, U, L, \theta, f, g)$ – несимметричная криптосистема вида (1), где θ: $K \to U$, f: $X \times U \times L \to Y$, g: $Y \times K \to X$, удовлетворяющая условию

$$|K| = |U|. \tag{12}$$

Обозначим θ^{-1}: $K \to U$ обратное к θ отображение, положим $K' = U$, $U' = K$ и определим функцию δ: $X \times Y \times U' \to \{0, 1\}$, полагая для любых $x \in X$, $y \in Y$, $u' \in U'$ $\delta(x, y, u') = 1$ в том и только том случае, когда $g(y, u') = x$. Нетрудно видеть, что алгебра $\Lambda_{\mathfrak{I}} \overset{\text{def}}{=} (X, K', Y, U', L, \theta^{-1}, f, \delta)$ представляет собой систему цифровой подписи (с множеством секретных ключей $K' = U$ и множеством открытых ключей $U' = K$). Действительно, в силу равенства (2) и определения отображения δ для любых $x \in X$, $k' = \theta(k) \in K'$, $l \in L$ имеют место соотношения

$$g(f(x, \theta(k), l), k) = x \Leftrightarrow g(f(x, k', l), \theta^{-1}(k')) = x \Leftrightarrow \delta(x, f(x, k', l), \theta^{-1}(k')) = 1,$$

из которых следует справедливость тождества (10) в алгебре $\Lambda_{\mathfrak{I}}$.

Итак, каждой несимметричной криптосистеме $\mathfrak{I}$, удовлетворяющей равенству (12), соответствует вполне определенная система цифровой подписи $\Lambda_{\mathfrak{I}}$. Стойкость последней (относительно фальсификации) определяется, как и в общем случае, трудоемкостью алгоритмов решения уравнений (10), (11), которые, согласно определению системы $\Lambda_{\mathfrak{I}}$, могут быть записаны в виде

$$g(y', u') = x', \tag{13}$$

$$u' = \theta^{-1}(k') \tag{14}$$

соответственно. Здесь $x' \in X$, $u' \in U'$ и $y' \in Y$, $k' \in K'$ обозначают, соответственно, известные открытое сообщение и секретный ключ и неизвестные шифрованное сообщение и открытый ключ системы открытого шифрования $\mathfrak{I}$. (Напомним, что множество секретных (открытых) ключей криптосистемы $\mathfrak{I}$ совпадает с множеством открытых (секретных) ключей системы цифровоvй подписи $\Lambda_{\mathfrak{I}}$).

Таким образом, стойкость системы цифровой подписи, построенной на основе несимметричной криптосистемы $\mathfrak{I}$, определяется вычислительной сложностью следующих задач:

1) нахождение из уравнения (13) шифрованного сообщения y' по известным секретному ключу u' и открытому сообщению x' криптосистемы $\mathfrak{I}$;

2) нахождение из уравнения (14) открытого ключа k' криптосистемы $\mathfrak{I}$ по известному секретному ключу u' и (в общем случае) частично известному отображению θ. (Очевидно, что для решения первой из указанных задач достаточно решить вторую. При этом отображение θ^{-1} в уравнении (14) может зависеть от неизвестных криптоаналитику параметров, таких как, например, числа p и q в криптосистеме RSA $\mathfrak{R}_{p,q}$; см. соотношения (4), (5)).

Ясно, что не каждой системе открытого шифрования $\mathfrak{I}$, стойкой относительно атаки на основе известного шифрованного сообщения, соответствует стойкая относительно фальсификации система цифровой подписи $\Lambda_{\mathfrak{I}}$. Например, в системе цифровой подписи $\Lambda_{\wp}$, построенной на основе криптосистемы Эль-Гамаля $\wp$ (см. пример 2), легко подделать подпись любого открытого сообщения x', если известен ключ u' проверки подписи. Тем не менее, хорошо известно, что в определенных случаях исходная система открытого шифрования $\mathfrak{I}$ и построенная на ее основе система цифровой подписи $\Lambda_{\mathfrak{I}}$ имеют одинаковую вычислительную стойкость.

Пример 3. (*Система цифровой подписи RSA*).

Обозначим $\Lambda_{p,q}$ систему цифровой подписи, построенную на основе криптосистемы RSA $\mathfrak{R}_{p,q}$ (см. пример 1). Из определений алгебр $\mathfrak{R}_{p,q}$ и $\Lambda_{p,q}$ следует, что цифровая подпись $y = x^d \pmod n$ сообщения $x \in \boldsymbol{Z}_n$ представляет собой результат зашифрования данного сообщения на ключе $k' = d \in (\boldsymbol{Z}/\phi(n))^*$ (секретном ключе подписывания) абонента A. Получаемые абонентом B сообщение x и подпись y признаются правильными в том и только том случае, когда выполняется условие $x = y^e \pmod n$, где $e = u'$ – открытый ключ (проверки подписи), соответствующий секретному ключу d.

Как известно, использование в качестве цифровой подписи результата шифрования не является общим методом, а скорее служит иллюстрацией перехода от способа подтверждения подлинности, основанного на наличии у абонентов телекоммуникационной системы одинаковых секретных ключей, к системам с двумя различными ключами (секретным и открытым). Среди методов формирования цифровой подписи, не использующих открытое шифрование, широкую известность получил метод, предложенный Эль-Гамалем [8].

Пример 4. (Система цифровой подписи Эль-Гамаля).

С формальной точки зрения *система цифровой подписи Эль-Гамаля* является алгеброй $\Gamma \overset{\text{def}}{=} (X, K, Y, U, L,$

θ, *f*, δ) вида (9), определяемой для данных простого числа *p* и примитивного элемент *a* поля ***GF***(*p*) с помощью следующих соотношений:

$$X = \mathbf{GF}(p),\ K = U = \mathbf{GF}(p)^*,\ L = (\mathbf{Z}_{p-1})^*,\ Y = \mathbf{GF}(p)^* \times \mathbf{Z}_{p-1},$$

$$\theta: K \to U,\ f: X \times K \times L \to Y,\ \delta: X \times Y \times U \to \{0, 1\},$$

$$\theta(k) = a^k \pmod p,\ f(x, u, l) = (y_1, y_2),$$

$$y_1 = a^l \pmod p,\ y_2 = (x - k\,y_1)\,l^{-1} \bmod (p-1), \qquad (15)$$

$$\delta(x, (y_1, y_2), u) = 1 \Leftrightarrow u^{y_1} y_1^{y_2} \equiv a^x \pmod p,$$

где $k \in K$, $x \in X$, $l \in L$, $(y_1, y_2) = y \in Y$. Следует обратить внимание на определенное сходство систем Эль-Гамаля $\wp$ (открытого шифрования) и Γ (цифровой подписи). Так, множества *X*, *K*, *U* и *L* соответственно подписываемых сообщений, секретных ключей, открытых ключей и параметров системы Γ совпадают с аналогичными множествами криптосистемы $\wp$ (см. пример 2). Кроме того, в обеих системах используются одинаковые алгоритмы вычисления открытых ключей по секретным (совпадают отображения θ). Также равны первые координаты y_1 значений функций шифрования и подписывания соответственно. Наиболее существенное различие между системами открытого шифрования и цифровой подписи Эль-Гамаля заключается в способе формирования координаты y_2 подписи и соответственно шифрованного сообщения (см. соотношения (15) и (7)).

IV Выводы

Предложенный подход к формализации понятий системы открытого шифрования и системы цифровой подписи, очевидно, не является единственно возможным. Вместе с тем, построенные выше алгебраические модели несимметричных криптосистем составляют формальную теоретическую основу исследований общих критографических свойств различных систем с открытым ключом. Основная задача в области анализа несимметричных криптосистем, представленных в виде многоосновных универсальных алгебр, состоит в конструктивном описании таких алгебр, допускающих простую реализацию и обеспечивающих приемлемую вычислительную стойкость шифрования (цифровой подписи). Важной задачей дальнейших исследований является также определение условий эквивалентности (в том или ином смысле) несимметричных криптосистем или сводимости их друг к другу.

Литература: 1. Diffie W., Hellman M. E. New directions in cryptography // IEEE Trans. on Inf. Theory. – 1976. – IT-22. – P. 644-654. 2. Артамонов В. А., Ященко В. В. Многоосновные алгебры в системах открытого шифрования // Успехи матем. наук. – 1994. – Т. 49. – С. 149-150. 3. Сидельников В. М., Черепнев М. А., Ященко В. В. Системы открытого распределения ключей на основе некоммутативных полугрупп // Доклады РАН. – 1993. – Т. 332. – № 5. – С. 566-567. 4. Schneier B. Applied Cryptography. – John Wille & Sons, Inc. – N-Y. – 1996. 5. Горчинский Ю. Н. О гомоморфизмах многоосновных универсальных алгебр в связи с криптографическими применениями // Труды по дискретной математике – 1997. – Т. 1. – С. 43-66. 6. Шапошников И. Г. О конгруэнциях конечных многоосновных универсальных алгебр // Дискретная математика. – 1999. – Т. 11. – В. 3. – С. 48-62. 7. Шеннон К. Теория связи в секретных системах // Работы по теории информации и кибернетике. – М.: Изд-во иностр. литературы, 1963. – С. 333- 402. 8. El Gamal T. A public-key cryptosystem and signature scheme based on discrete logarithms // IEEE Trans. on Inf. Theory. – 1985. – IT-31. – № 4.

УДК 681.3.06: 519.248.681

СТОЙКОСТЬ ГОСТ 28147-89 ПРИ ИСПОЛЬЗОВАНИИ ТАБЛИЦЫ ПОДСТАНОВОК ИЗ ГОСТ 34.311-95

Роман Олейников

Харьковский Национальный Университет Радиоэлектроники

Анотація: **Розглядається стійкість ГОСТ 28147-89 при використанні довгострокового ключа, що наведений у стандарті хешування ГОСТ 34.311-95. Наводяться приклади побудови диференційних характеристик та доводиться неможливість диференційної та лінійної атаки на ГОСТ 28147-89 з**