Системы распределения ключей на основе "экспоненциального" представления линейной группы $GL_n(\mathbf{F}_p)$

В. М. Сидельников

Первая система распределения ключей (key distribution system) была предложена Диффи и Хеллманом в [1] (см. также [2]). В работе [3] (см. также § 1 этой работы) был предложен новый способ построения систем распределения ключей с помощью некоммутативной группы G. В настоящей работе изучается один частный случай этой системы, в котором объединяются идеи работ [1], [2]. А именно, рассматриваются системы, построенные на основе группы $GL_n(\mathbf{F}_p)$, которая "представлена" с помощью вспомогательной циклической группы U порядка p. В качестве группы U может, например, выступать группа $\mathbf{F}_q$-рациональных точек эллиптической кривой и т. п.

Подробно рассмотрен случай $U = \langle\eta\rangle$ — подгруппа порядка p мультипликативной группы вспомогательного поля $\mathbf{F}_q$, $p \mid q-1$, а G — группа аффинных преобразований поля $\mathbf{F}_p$, $G < GL_2(\mathbf{F}_p)$. В этом случае задача определения общего ключа $\mathbf{u}_{XY}$ абонентов X и Y вычислительно эквивалентна задаче: вычислить элемент $\eta^{xy/z}$ при известных элементах η^x, η^y, η^z. Последняя задача предположительно не сводится к нескольким задачам Диффи — Хеллмана: вычислить элемент $f = \eta^{xy}$ при известных элементах η^x, η^y.

В системе, построенной с помощью группы $G = GL_2(\mathbf{F}_p)$ возникает несколько новых параметров, которые отсутствуют в системах типа Диффи и Хеллмана. В частности, появляется новый секретный ключ всей системы, без знания которого предположительно невозможно определить ключ $\mathbf{u}_{XY}$.

В § 4 представлен новый способ вычисления цифровой подписи сообщений.

1. Введение

Коротко опишем частный случай системы открытого распределения ключей, предложенной в работе [3]. Пусть G — произвольная, вообще говоря, некоммутативная группа и H и R — ее коммутативные подгруппы. Эти объекты будут далее использованы для построения системы распределения ключей. Каждая пара абонентов X и Y системы с помощью обмена информацией по открытому каналу связи может выработать общий секретный элемент $\mathrm{g} = \mathrm{g}_{XY}$ из G, называемый общим ключом этих абонентов. Ключ g_{XY}, например, можно использовать в качестве ключа шифратора для связи абонентов X и Y.

Обычно в качестве такого общедоступного канала выступает справочник, в котором помещается определенная информация каждого абонента системы. Эта информация называется открытым ключом (public key) соответствующего абонента. В нашем случае открытый ключ является элементом g_X группы G и справочник является списком таких элементов. Кроме открытого ключа каждый абонент X имеет и секретную информацию (private key), которую он никому не сообщает, но использует при построении секретного ключа g_{XY}.

Алгоритм выработки элемента g_X — открытого ключа абонента X – - состоит в следующем. В каждой из подгрупп H и R выбирается по одному элементу $h_X \in H$ и $r_X \in R$. Открытый ключ g_X имеет вид $\mathrm{g}_X = h_X \cdot k \cdot r_X$, где знак $\cdot$ обозначает групповую операцию в G; k — некоторый фиксированный элемент группы G, одинаковый для всех абонентов сети, который может быть и дополнительным секретным ключом всей ключевой структуры. Пара $(h_X,\ r_X)$ является секретным ключом (private key) абонента X. Аналогично и независимо от X строится открытый ключ $\mathrm{g}_Y = h_Y \cdot k \cdot r_Y$ абонента Y.

В качестве общего секретного ключа g_{XY} абонентов X и Y выступает элемент $\mathrm{g} = \mathrm{g}_{XY} = h_X \cdot h_Y \cdot k \cdot r_Y \cdot r_X$. Абонент X вычисляет элемент g с помощью своего секретного ключа $(h_X,\ r_X)$ в виде $\mathrm{g} = h_X \cdot \mathrm{g}_Y \cdot r_X$, а Y — в виде $\mathrm{g} = h_Y \cdot \mathrm{g}_X \cdot r_Y$. В силу коммутативности групп H и R последние два элемента совпадают.

Основное требование к системе состоит в том, что нападающей стороне, которая обладает всей информацией, пересылаемой абонентами друг другу или помещенных ими в общедоступном справочнике, для вычисления элемента g_{XY} необходимо затратить неприемлемо большое число операций.

Как было отмечено в работе [3], стойкость к нападению описанной системы распределения ключей определяется сложностью решения следующей математической задачи.

Задача (A). По известным элементам g_X и g_Y из G, допускающим представление $\mathrm{g}_X = h_X \cdot k \cdot r_X$ и $\mathrm{g}_Y = h_Y \cdot k \cdot r_Y$, найти неизвестный элемент $\mathrm{g} = h_X \cdot h_Y \cdot k \cdot r_Y \cdot r_X$.

Вместе с задачей (A) будет рассматриваться

Задача (B). По известным группам H и R и известному элементу g, допускающему представление $\mathrm{g} = h \cdot k \cdot r$, найти какие-либо h' и r' из групп H' и R', для которых справедливо $\mathrm{g} = h' \cdot k \cdot r'$, где $H',\ R'$ — коммутативные расширения в группе G групп H и R.

Очевидно, что решение задачи (B) позволяет решить и задачу (A). Обратное, вообще говоря, не верно. Отметим, что в системе Диффи и Хеллмана логарифмирование является задачей (B), а задача Диффи и Хеллмана (определение см. в аннотации) — задачей (A). Автору известны безуспешные попытки доказать или опровергнуть вычислительную эквивалентность этих задач.

Следует отметить, что для многих групп, представленных в их естественном виде, сложность решения задачи (B) невысока, если предполагать известным элемент k. В частности, для группы $G = GL_n(\mathbf{F}_p)$ квадратных невырожденных матриц порядка n над конечным полем $\mathbf{F}_p$ эта сложность, как показано в [3], не выше $O(n^3)$ элементарных алгебраических операций в поле $\mathbf{F}_p$. Таким образом, использовать эту группу с известным элементом k в ее естественном представлении (в виде матриц над $\mathbf{F}_p$ с обычным законом умножения) для построения системы распределения ключей не следует из-за малой сложности решения задачи (B).

Как будет показано ниже, группу $GL_n(\mathbf{F}_p)$, а вместе с ней и систему распределения ключей, можно реализовать и несколько иным, отличным от традиционного, способом с помощью вспомогательной циклической группы U порядка p. Это представление, названное U-представлением группы $GL_n(\mathbf{F}_p)$, принципиально усиливает стойкость системы распределения ключей к нападению. Переходим к его описанию.

Пусть U — произвольная циклическая группа порядка p с мультипликативной записью ее групповой операции, и υ — ее порождающий элемент, т.е. $U = \langle \upsilon \rangle = \{\upsilon^i;\ i = 0, \ldots, p-1\}$.

Будем считать, что элементами поля $\mathbf{F}_p$ являются классы вычетов mod p. Пусть x — представитель одного из таких классов. Очевидно, элемент υ^x группы U определяется только классом, к которому принадлежит x, и не зависит от выбора представителя в этом классе. Поэтому поле $\mathbf{F}_p$ можно представлять себе как множество элементов U, в котором сложение выполняется как умножение двух элементов в U, а умножение элементов a и b в поле $\mathbf{F}_p$ как возведение элемента a в степень, равную индексу (логарифму) элемента b по основанию υ.

Таким образом, получаем изоморфный образ поля $\mathbf{F}_p$ в виде множества элементов U, на котором действуют две операции. Рассмотренное представление поля $\mathbf{F}_p$ с помощью группы U порядка p будем называть (экспоненциальным) U-представлением поля $\mathbf{F}_p$.

Достаточно очевидно, что, используя прямое произведение $U \times \ldots \times U$ — k экземпляров группы U, можно аналогичным и достаточно очевидным образом определить $U-$ представление поля $\mathbf{F}_{p^k}$. В данной работе останавливаться на этом не будем.

С помощью U-представления поля $\mathbf{F}_p$ может быть реализована и линейная группа $GL_n(\mathbf{F}_p)$. Опишем эту реализацию подробнее.

Каждой матрице $\mathbf{h} = \|h_{ij}\|$ из $GL_n(\mathbf{F}_p)$ сопоставим матрицу $\upsilon^{\mathbf{h}} = \|\upsilon^{h_{ij}}\| = \|\chi_{ij}\|$ с элементами из группы U. Произведение $\upsilon^{\mathbf{t}}$ двух матриц $\upsilon^{\mathbf{h}}$ и $\upsilon^{\mathbf{r}}$, где $\mathbf{t} = \mathbf{hr}$ в поле $\mathbf{F}_p$, вычисляется следующим образом:

$$\upsilon^{\mathbf{t}} = (\upsilon^{\mathbf{h}})^{\mathbf{r}} = {}^{\mathbf{h}}(\upsilon^{\mathbf{r}}) = \|\tau_{ij}\|,\ \tau_{ij} = \prod_{k=1}^{n} (\upsilon^{h_{ik}})^{r_{kj}} = \prod_{k=1}^{n} (\chi_{ik})^{r_{kj}}. \qquad (1)$$

Отметим, что для вычисления произведения матриц $\upsilon^{\mathbf{h}}$ и $\upsilon^{\mathbf{r}}$ необходимо знать либо матрицу $\|r_{kj}\|$, образованную индексами (логарифмами) элементов матрицы $\upsilon^{\mathbf{r}}$, либо матрицу $\|h_{kj}\|$, состоящую из логарифмов элементов матрицы $\upsilon^{\mathbf{h}}$.

В работе предлагается вместо открытых ключей $\mathbf{g}_X = \mathbf{h}_X \cdot \mathbf{k} \cdot \mathbf{r}_X$ из группы $GL_n(\mathbf{F}_p)$ использовать их U-представление, а именно, элементы $\mathbf{u}_X = \upsilon^{\mathbf{g}_X}$. Сами элементы $\mathbf{h}_X$ и $\mathbf{r}_X$ являются секретными ключами (private key) и хранятся абонентом X в обычном виде, т.е. в виде матриц над $\mathbf{F}_p$.

Ключ $\mathbf{u} = \mathbf{u}_{XY} = \upsilon^{\mathbf{h}_X \cdot \mathbf{h}_Y \cdot \mathbf{k} \cdot \mathbf{r}_Y \cdot \mathbf{r}_X}$ для связи абонентов X и Y так же, как открытый ключ $\mathbf{u}_X$, представляет собой матрицу размера $n \times n$ с элементами из группы U. Элемент $\mathbf{u}$ вычисляется абонентом X при известных ему элементе $\upsilon^{\mathbf{g}_Y}$ и элементах $\mathbf{h}_X, \mathbf{r}_X$ из $GL_n(\mathbf{F}_p)$ с помощью соотношения (1). Совершенно аналогично элемент $\mathbf{u}$ вычисляет абонент Y.

Отметим, что элемент $\mathbf{k}$ всюду выступает только в "экспоненциальном" виде $\upsilon^{\mathbf{k}}$. Его знание необходимо устроителю системы однажды, а именно только при первом вычислении элемента $\kappa = \upsilon^{\mathbf{k}}$.

Поэтому элемент $\mathbf{k}$ также можно считать секретным ключом всей системы, который отсутствует в системе Диффи-Хеллмана.

Возможно, в некоторых случаях можно случайно выбирать матрицу κ сразу из множества всех матриц с коэффициентами из U, не вычисляя при этом матрицу $\mathbf{k}$. Правда, здесь возникает, возможно, мнимая опасность: что будет, если для κ не найдется матрицы $\mathbf{k}$ из $GL_n(\mathbf{F}_p)$, для которой $\kappa = \upsilon^{\mathbf{k}}$?

Очевидно, отображение $\phi : \mathbf{g} \to \mathbf{u} = \upsilon^{\mathbf{g}}$ элементов группы $GL_n(\mathbf{F}_p)$ в множество матриц с коэффициентами из группы U является взаимно однозначным, но для рассматриваемых ниже примеров группы U сложность вычисления $\phi(\mathbf{g}) = \upsilon^{\mathbf{g}}$ является полиномиальной от длины записи $\mathbf{g}$, в то время как сложность вычисления $\phi^{-1}(\mathbf{u})$ сводится к предположительно "сложной" задаче логарифмирования в группе U. Вместе с тем следует отметить, что из упомянутого выше результата работы [3] о невысокой сложности решения задачи (A) для группы $GL_n(\mathbf{F}_p)$ в ее естественном представлении вытекает, что при известной матрице $\mathbf{k}$ стойкость рассматриваемой системы не выше сложности логарифмирования в группе U.

Перечислим отличия рассматриваемой матричной системы от системы Диффи и Хеллмана (DH-системы).

Во-первых, в матричной системе появляются новые параметры: группы H и R и элемент $\mathbf{k}$. В DH-системе эти параметры отсутствуют, ибо в циклической группе, например, в $\mathbf{F}_q^*$, всего одна-две подходящие подгруппы, которые по одному ее элементу могут быть однозначно определены. Иначе обстоит дело в группе $GL_n(\mathbf{F}_p)$, $n \geq 2$: подходящих подгрупп H и R в $GL_n(\mathbf{F}_p)$ очень много, и многие из них не определяются одним своим элементом. Выбор этих подгрупп в некоторых случаях можно сделать секретным и они станут дополнительными секретными ключами системы, не известными не только нападающей стороне, но и абонентам системы.

Во-вторых, как уже было отмечено, элемент $\mathbf{k}$, используется абонентами только в форме U-представления, а именно в виде $\upsilon^{\mathbf{k}}$. Поэтому, если не оговорено противное, элемент $\mathbf{k}$ будем далее считать "глобальным" секретным ключом всей системы распределения ключей. "Локальными" ключами являются ключи $\mathbf{h}_X, \mathbf{r}_X$. Отметим, что если даже нападающая сторона узнает все "локальные" ключи $\mathbf{h}_X, \mathbf{r}_X$, то "глобальный" ключ $\mathbf{k}$ ей все равно будет недоступен без логарифмирования в группе U.

В дальнейшем изложении G — некоторая подгруппа матриц второго порядка над полем $\mathbf{F}_p (n = 2)$. В качестве группы U будет рассматриваться подгруппа порядка p мультипликативной группы вспомогательного поля $\mathbf{F}_q$, $p \mid q-1$. Кроме того, в качестве группы U может быть использована подгруппа группы $E(\mathbf{F}_q)$ — группы $\mathbf{F}_q-$ рациональных точек эллиптической кривой, заданной уравнением с коэффициентами из некоторого вспомогательного поля $\mathbf{F}_q$ (см. [4],[5]).

Предварительно рассмотрим частный случай: G — полупрямое произведение циклических групп порядков t и p, $t < p$, $t \mid p-1$ [6]. Эта группа изоморфна подгруппе аффинной группы преобразований поля $\mathbf{F}_p$. Будем полагать, что $\mathbf{k}$ — единичный элемент группы G. Этот случай, с одной стороны, имеет принципиальные отличия от DH-системы, а с другой — его можно до конца разобрать, в частности, выписать в обозримом виде элементы $\mathbf{u}_X, \mathbf{u}_Y$ и $\mathbf{u}_{XY}$.

2. G — подгруппа аффинной группы преобразований поля $\mathbf{F}_p$

В рассматриваемом случае G изоморфна группе $\mathfrak{A}$ матриц вида $\mathcal{A} = \left\| \begin{matrix} u & v \\ 0 & 1 \end{matrix} \right\| = (u, v)$ над $\mathbf{F}_p$, где $u^t = 1$, и содержит pt элементов. Изоморфизм между группой аффинных преобразований $\psi(x) = ux + v (u^t = 1, v \in \mathbf{F}_p)$ поля $\mathbf{F}_p$ и группой $\mathfrak{A}$ очевиден: функции $\psi(x)$ соответствует линейное преобразование $\mathcal{A} \cdot (x, 1)^{\mathrm{T}}$.

Пусть Π_t — циклическая подгруппа порядка t мультипликативной группы поля $\mathbf{F}_p$,Θ_p — подгруппа порядка p мультипликативной группы поля $\mathbf{F}_q$, $p \mid q-1$, и ξ, η — порождающие элементы групп Π_t и $\Theta_p (\xi \in \mathbf{F}_p, \eta \in \mathbf{F}_q)$. Каждому элементу $\mathcal{A} = (u, v)$ группы $\mathfrak{A}$ сопоставим пару $\gamma = (a, b)$, где $a = \eta^u$ и $b = \eta^v$. Групповая операция между элементами $\gamma = (a, b)$ и $\delta = (c, d)$, $c = \eta^w$, $d = \eta^k$, соответствующая групповой операции в группе $\mathfrak{A}$, очевидно, определяется соотношением

$$(\eta^u, b) \cdot (c, d) = (a, b) \cdot (\eta^w, \eta^k) = (c^u, b \cdot d^u) = (a^w, b \cdot a^k) \tag{2}$$

Группу, образованную парами γ с групповой операцией (2), будем обозначать через $\Gamma_{p,t}$.

Отметим, что при умножении слева элемента (a, b) на (c, d) в группе $\Gamma_{p,t}$ необходимо знать только индекс u одного элемента a; индексы остальных элементов c, b, d знать не надо. В то время как при

умножении справа элемента (c,d) на элемент (a,b) необходимо знать индексы двух элементов — c и d. Это замечание будет использовано ниже.

Как легко убедиться, в группе $\mathfrak{A}$ содержатся следующие циклические подгруппы: одна подгруппа Δ_p порядка p, порожденная элементом $(1,v)$,$v \neq 0$, и p подгрупп $\Delta_t(v),\ v \in \mathbf{F}_p$, порядка t, которые состоят из элементов вида $(\xi^i, v(\xi^i-1)),\ i=0,\dots,t-1$. Заметим, что из определения группы $\mathfrak{A}$ и из соотношения (2) вытекает соотношение

$$(\xi^i, v(\xi^i-1))\cdot(\xi^j, v(\xi^j-1)) = (\xi^{i+j}, v(\xi^{i+j}-1)). \tag{3}$$

Отметим, что подгруппы $\Delta_t(v)$ и $\Delta_t(s)$ сопряжены, и $\Delta_t(v)\cap\Delta_t(s)=(1,0)$, если $s\neq v$, где (1,0) — единица группы $\mathfrak{A}$. Если t — простое число, то других нетривиальных коммутативных подгрупп в группе $\mathfrak{A}$ нет.

Подгруппы в $\Gamma_{p,t}$, соответствующие Δ_p и $\Delta_t(z)$, будем обозначать через $\widetilde{\Delta}_p$ и $\widetilde{\Delta}_t(\alpha)$, где $\alpha=\eta^z, \alpha\in\Theta_p$. Подгруппа $\widetilde{\Delta}_p$ порождается элементом $(\eta,b),\ b\in\Theta_p,\ b\neq 1$, а подгруппа $\widetilde{\Delta}_t(\alpha)$ состоит из элементов вида (η^u,α^{u-1}), где u пробегает элементы группы Π_t. Умножение в $\widetilde{\Delta}_t(\alpha)$, как вытекает из (3), производится по правилу

$$(\eta^u,\alpha^{u-1})\cdot(\eta^w,\alpha^{w-1}) = (\eta^{uw},\alpha^{uw-1}),\ u,w\in\Pi_t. \tag{4}$$

В качестве подгрупп H и R группы $\Gamma_{p,t}$ при построении системы открытого распределения ключей берутся разные подгруппы $\widetilde{\Delta}_t(\alpha)$ и $\widetilde{\Delta}_t(\beta)$ "общего положения", т.е. подгруппы со случайно выбранными α и β из $\Theta_p\backslash\{1\}$ с условием $\alpha\neq\beta$.

Таким образом, в рассматриваемой системе открытого распределения ключей открытым ключом абонента является элемент $(a,b)\cdot(c,d)$, где $(a,b)=(\eta^u,\alpha^{u-1})$,$(c,d)=(\eta^w,\beta^{w-1})$,$\alpha=\eta^z$, $\beta=\eta^s$, при этом элементы u,w случайно и независимо выбраны в группе Π_t.

Как было замечено, для того чтобы умножить слева произвольный элемент группы $\Gamma_{p,t}$ на элемент (a,b), достаточно знать индекс только элемента a. Поэтому далее будем полагать, что секретным ключом абонента X является пара $\mathbf{U}_X=((u,b),(w,s(w-1)))$, где $b=\eta^{z(u-1)}\in\mathbf{F}_q, u,w\in\Pi_t, s\in\mathbf{F}_p^*$. Выбор в качестве секретного ключа пары $\mathbf{U}_X$, а не $((u,z(u-1)),(w,s(w-1))$, усиливает стойкость системы к нападению, ибо при этом от нападающей стороны скрывается элемент z.

Будем предполагать, что нападающей стороне известен по меньшей мере один секретный ключ $\mathbf{U}_Z$. Из этого предположения вытекает, что нападающей стороне, во-первых, известен и элемент $b_1=\eta^z$, который она может легко вычислить, и, во-вторых, ей известен элемент s, который определяет подгруппу R.

Элемент

$$\mathbf{u}_X=(\eta^u,\alpha^{u-1})\cdot(\eta^w,\beta^{w-1})=(\eta^{uw},\eta^{su(w-1)+z(u-1)}) \tag{5}$$

является открытым ключом абонента X.

Как легко установить, множество $\Delta_t(z)\cdot\Delta_t(s)=\{\mathcal{A}_1\cdot\mathcal{A}_2;\ \mathcal{A}_1\in\Delta_t(z),\ \mathcal{A}_2\in\Delta_t(s)\}$, $z\neq s$, содержит t^2 элементов. Поэтому при $t=p-1$ почти все элементы группы $\mathfrak{A}$ могут выступать в качестве открытых ключей $\mathbf{u}_X$.

Общий ключ $\mathbf{u}=\mathbf{u}_{XY}$ для связи абонентов X и Y имеет вид

$$\mathbf{u}=(\eta^u,\alpha^{u-1})g_Y(\eta^w,\beta^{w-1})=(\eta^{un},\alpha^{un-1})\cdot(\eta^{wm},\beta^{wm-1})=(\eta^{uwnm},\eta^{suwnm+(z-s)un-z}),$$

где $\mathbf{u}_Y=(\eta^n,\alpha^{n-1})\cdot(\eta^m,\beta^{m-1})$ — открытый ключ абонента Y. Если теперь положить $x_1=uw$,$x_2=nm$,$y_1=u$,$y_2=n$, то, как нетрудно проверить, ключ $\mathbf{u}$ можно представить в виде $\mathbf{u}=(\eta^{x_1x_2},\ \eta^{s(x_1x_2-y_1y_2)+z(y_1y_2-1)})$, а известные элементы (открытые ключи абонентов) — в виде $\mathbf{u}_X=(\eta^{x_1},\ \eta^{s(x_1-y_1)+z(y_1-1)}$, $\mathbf{u}_Y=(\eta^{x_2},\ \eta^{s(x_2-y_2)+z(y_2-1)})$ и $b_1=\eta^z$ (см. (5)).

Таким образом, задача (А) (см. §1) определения ключа $\mathbf{u}$ эквивалентна решению двух задач: задаче $DH(\eta)$ — вычислению элемента $f=\eta^{x_1x_2}$ при известных элементах η^{x_1},η^{x_2} (задаче Диффи-Хеллмана) и задаче $P(\eta)$ — вычислению элемента $\eta^{s(x_1x_2-y_1y_2)+z(y_1y_2-1)}$ при известных элементах η, η^z, s, $\mathbf{u}_X$, $\mathbf{u}_Y$.

В свою очередь, задача $P(\eta)$ эквивалентна решению следующих двух задач: задачи $DH(\eta^s)$ и задачи $T(\eta)$: вычислить элемент $\eta^{y_1y_2(z-s)}$ при известных элементах $\eta^{y_1(z-s)}$, $\eta^{y_2(z-s)}$, η, η^z и s.

Если ввести новые переменные $x=y_1(z-s)$,$y=y_2(z-s)$,$z'=z-s$, то задачу $T(\eta)$ можно записать в виде: вычислить элемент $\eta^{xy/z'}$ при известных элементах η^x, η^y, $\eta^{z'}$.

Как представляется автору, задача $P(\eta)$ не сводится к нескольким задачам $DH(\eta)$ и достаточно существенно отличается от задачи $DH(\eta)$. В целом, можно утверждать, что рассматриваемая система распределения ключей даже в рассмотренном простейшем случае отличается от системы Диффи-Хеллмана.

Отметим, что задача (B) (см. §1) может быть, как следует из (5), сведена к определению значений неизвестных u, w из системы трех показательных уравнений

$$a = \eta^{uw},\ b = \eta^{z},\ c = \eta^{zu}$$

с известными левыми частями.

Необходимо сказать, что приведенные выше результаты о сложности решения задач (A) и (B) получены в предположении о знании нападающей стороной секретного ключа по крайней мере одного абонента системы.

3. U — подгруппа группы $\mathbf{F}_q^*$ и $\mathbf{G} = \mathbf{GL_2(F_p)}$

В этом параграфе будем предполагать, что группы H и R известны нападающей стороне, а элемент $\mathbf{k}$ является дополнительным глобальным секретным ключом системы.

Пусть $A \in GL_2(\mathbf{F}_p)$. Предположим, что характеристический многочлен $f_A(x) = |xE - A|$ матрицы A неприводим над $\mathbf{F}_p$. Будем рассматривать в качестве коммутативных подгрупп подгруппы $H(A)$ вида $H(A) = \{xA + yE \,|\, (x,y) \in (\mathbf{F}_p)^2,\ (x,y) \neq (0,0)\}$.

Очевидно, что умножение матриц из $H(A)$ является коммутативным и множество $H(A)$ замкнуто относительно умножения его элементов. Многочлен $f_A(x)$ — неприводим, поэтому, как легко показать, каждая матрица из $H(A)$ является невырожденной. Отсюда вытекает, что $H(A)$ действительно является коммутативной группой и содержит $p^2 - 1$ элементов.

Сначала рассмотрим случай $H = H(A), R = H(B), B \notin H(A), G$ — подгруппа группы $GL_2(\mathbf{F}_p)$, состоящая из всевозможных произведений элементов из множества HR, и $\mathbf{k} = E$.

Лемма 1. *Множество HR состоит из $(p^2-1)(p+1)$ элементов.*

Доказательство. Пусть $\mathbf{h} = xA + yE, \mathbf{r} = zB + uE$. Покажем, что равенство $\mathbf{hr} = E$ выполнено только тогда, когда $x = z = 0$ и $u = y^{-1}$. Действительно, из того, что $\mathbf{hr} = E$, вытекает $xA + yE = x'B + y'E = \mathbf{r}^{-1}$. Из этого соотношения и условия $B \notin H(A)$ следует требуемое.

Равенство $\mathbf{hr} = \mathbf{h}_1\mathbf{r}_1$ выполнено только тогда, когда $(\mathbf{h}_1)^{-1}\mathbf{hr}(\mathbf{r}_1)^{-1} = E$. Отсюда и из доказанного выше вытекает, что равенство $\mathbf{hr} = \mathbf{h}_1\mathbf{r}_1$ имеет место тогда и только тогда, когда $\mathbf{h} = y\mathbf{h}_1$ и $\mathbf{r} = y^{-1}\mathbf{r}_1, y \in \mathbf{F}_p^*$. Это доказывает лемму, ибо число элементов у групп $H(A)$ и $H(B)$ равно $p^2 - 1$.

Следствие 1. *Если $\mathbf{k}B\mathbf{k}^{-1} \notin H(A)$, то множество состоит из $(p^2-1)(p+1)$ элементов.*

В условиях следствия 1 множество $H\mathbf{k}R$ порождается элементами $\mathbf{h}$ из $H(A)$, которые определяются двумя параметрами x и y, и представителями $\mathbf{r}$ различных смежных классов в $H(B)$ по подгруппе скалярных матриц $xE,\ x \in \mathbf{F}_p^*$. В качестве представителей естественно взять следующие элементы из $H(B) : zB + E,\ B$ и $z \in \mathbf{F}_p$, определяемые одним параметром z. Таким образом, при $\mathbf{k} = E$ в качестве открытого ключа $\mathbf{hr}$ абонента будут выступать элементы группы $GL_2(\mathbf{F}_p)$ вида $xzAB + yzB + xA + yE$ и матрицы вида $xAB + yB$, определяемые тремя параметрами x, y, z.

Будем изучать два случая: a) группы H и R сопряжены в группе $GL_2(\mathbf{F}_p)$ и b) группы H и R не сопряжены в $GL_2(\mathbf{F}_p)$.

Случай a). В этом случае $B = CAC^{-1}, C \in GL_2(\mathbf{F}_p)$. Пусть $\mathbf{u}_X = \eta^{\mathbf{hkr}}, \mathbf{u}_Y = \eta^{\mathbf{fkt}}$ — открытые ключи абонентов X и Y, где $\mathbf{h}, \mathbf{f} \in H,\ \mathbf{r}, \mathbf{t} \in R,\ \mathbf{k} \in GL_2(\mathbf{F}_p)$.

Ключи $\mathbf{u}_X, \mathbf{u}_Y$ и $\mathbf{u} = \mathbf{u}_{XY} = \eta^{\mathbf{hfkrt}}$ можно преобразовать к виду $\mathbf{u}'_X = (\mathbf{u}_X)^C = \eta^{\mathbf{hk'h'}}$ и $\mathbf{u}' = \mathbf{u}^C = \eta^{\mathbf{fhk'h'f'}}$, где $\mathbf{f}$, $\mathbf{f}'$, $\mathbf{h}$, $\mathbf{h}' \in H,\ \mathbf{k}' = \mathbf{k}C$. Таким образом, этот случай при известной матрице C можно свести к случаю $H = R$ при некотором $\mathbf{k}$.

В виду того, что каждая матрица из $GL_2(\mathbf{F}_p)$ сопряжена с некоторой сопровождающей матрицей, мы далее ограничимся только случаем A, B — сопровождающие матрицы.

Случай b). Пусть $A = \begin{Vmatrix} 0 & a \\ 1 & b \end{Vmatrix}, B = \begin{Vmatrix} 0 & c \\ 1 & d \end{Vmatrix}$ — сопровождающие не сопряженные матрицы, $H = H(A),\ R = H(B)$ и $\mathbf{k} = \begin{Vmatrix} 1 & 0 \\ 0 & 1 \end{Vmatrix} = E$. Открытые ключи $\mathbf{u}_X = \eta^{\mathbf{hr}}, \mathbf{u}_Y = \eta^{\mathbf{h'r'}}$ в этом случае определяются матрицами $\mathbf{x} = \mathbf{hr} = (xA + yE)(B + zE)$ и $\mathbf{x}' = \mathbf{h'r'} = (x'A + y'E)(B + z'E)$, если предполагать, что ни $\mathbf{r}$, ни $\mathbf{r}'$ не являются диагональными матрицами. Ключ $\mathbf{u} = \mathbf{u}_{XY} = \eta^{\mathbf{h'hrr'}},\ \mathbf{h}, \mathbf{h}' \in H,\ \mathbf{r}, \mathbf{r}' \in R$, в этом случае определяется матрицей $\mathbf{y} = \mathbf{sv}$, где $\mathbf{s} = \mathbf{hh}' = (xy' + x'y + \omega xx')A + (yy' +$

$\sigma xx')E = h_A A + h_E E, \mathbf{v} = \mathbf{rr}' = (z + z' + \omega')B + (zz' + \sigma')E = r_B B + r_E E$ и $f_A(x) = x^2 - \omega x - \sigma, f_B(x) = x^2 - \omega' x - \sigma'$ — минимальные многочлены матриц A и B. Очевидно, $\mathbf{x} = xAB + yB + xzA + yzE, \mathbf{x}' = x'AB + y'B + x'z'A + y'z'E$ и $\mathbf{y} = h_A r_B AB + r_B h_E B + h_A r_E A + r_E h_E E = \|y_{ij}\|$. Например, $y_{11} = y_{11}(x, y, z, x', y', z') = a(xy' + x'y + \omega xx')(z + z' + \omega') + (yy' + \sigma xx')(zz' + \sigma')$.

Задача (A) в рассматриваемом случае $\mathbf{k} = E$ сводится к задаче: вычислить все элементы матрицы $\eta^{\mathbf{y}}$ при известных элементах матриц $\eta^{\mathbf{x}}$, $\eta^{\mathbf{x}'}$. В частности, необходимо вычислить элемент $\eta^{y_{11}}$ поля $\mathbf{F}_q$, зная восемь элементов матриц $\eta^{\mathbf{x}} = \|\eta^{x_{ij}}\|$ и $\eta^{\mathbf{x}'} = \|\eta^{x'_{ij}}\|$, $i, j = 1, 2$, где y_{11}— выписанная функция четвертого порядка нелинейности от переменных x, y, z, x', y', z', а $x_{ij}(x'_{ij})$ — функции второго порядка от переменных x, y, $z(x', y', z')$.

4. Цифровая подпись

Пусть $\mathbf{a}, \mathbf{x}, \mathbf{y} \in G < GL_n(\mathbf{F}_p)$,$\mathbf{p} = \eta^{\mathbf{y}}$,$\mathbf{u}_X = \eta^{\mathbf{hkr}} = \eta^{\mathbf{t}}$ — открытый ключ абонента X. Будем полагать, что $\mathbf{a}$ — сообщение, которое необходимо "подписать" абоненту X, а $(\mathbf{p}, \mathbf{x})$ — цифровая подпись сообщения $\mathbf{a}$, которая связана с $\mathbf{a}$ соотношением

$$\eta^{\chi_1(\mathbf{p})\mathbf{t}\chi_2(\mathbf{a})} = {}^{\chi_1(\mathbf{p})}(\mathbf{u}_X)^{\chi_2(\mathbf{a})} = \mathbf{p}^{\mathbf{x}}\eta^{\mathbf{a}} = \eta^{\mathbf{yx}+\mathbf{a}}, \tag{6}$$

где $\chi_1(\mathbf{p})$ — некоторая общеизвестная хеш-функция, отображающая матрицу $\mathbf{p}$ из $GL_n(\mathbf{F}_q)$ в подмножество множества $GL_n(\mathbf{F}_p)$ всех матриц с коэффициентами из $\mathbf{F}_p$,$\chi_2(\mathbf{a})$ — хеш-функция, отображающая элементы подгруппы G в $GL_n(\mathbf{F}_p)$, и $\mathbf{p}^{\mathbf{x}}\eta^{\mathbf{a}}$ — поэлементное умножение матриц $\mathbf{p}^{\mathbf{x}}$ и $\eta^{\mathbf{a}}$.

В качестве $\chi_1(\mathbf{p})$ можно, например, использовать функцию $\chi(\mathbf{p}) = \psi(\eta^{\psi(\mathbf{p})})$, где $\psi(\mathbf{p})$ — матрица из $GL_n(\mathbf{F}_p)$, полученная из $\mathbf{p} \in GL_n(\mathbf{F}_q)$ с помощью некоторого отображения $\psi(\cdot)$ ее элементов в поле $\mathbf{F}_p$. Если q — простое число, то можно положить $\psi(x) = x \bmod p$, где $x \in \mathbf{F}_q$ представлено как неотрицательное число, меньшее q, и под $x \bmod p$ понимается неотрицательный вычет числа x, который трактуется как элемент поля $\mathbf{F}_p$. В качестве $\chi_2(\mathbf{a})$ можно использовать функцию $\psi(\eta^{\mathbf{a}})$. Возможно, что можно обойтись и одной хеш-функцией, положив, например, $\chi_2(\mathbf{a}) = const$.

Секретную матрицу $\mathbf{y}$ естественно выбирать случайно в $GL_n(\mathbf{F}_p)$ или в некоторой ее подгруппе, а матрицу $\mathbf{x}$ вычислять как функцию от $\mathbf{a}$ и $\mathbf{y}$. Любой абонент может проверить выполнение соотношения (6).

Только абонент X знает матрицы $\mathbf{t}$ и $\mathbf{y}$. Поэтому он может вычислить матрицу $\mathbf{x} = \mathbf{y}^{-1}(\chi_1(\mathbf{p})\mathbf{t}\chi_2(\mathbf{a}) - \mathbf{a})$. Предположительно без логарифмирования в поле $\mathbf{F}_q$ никто другой этого сделать не сможет.

Можно предложить и другой вариант соотношения (6): $(\mathbf{u}_X)^{\chi(\mathbf{a},\mathbf{p})} = \mathbf{p}^{\mathbf{x}}$, где $\chi(\mathbf{a}, \mathbf{p})$ — хеш-функция, отображающая прямое произведение $GL_n(\mathbf{F}_p) \times GL_n(\mathbf{F}_q)$ в подмножество множества $GL_n(\mathbf{F}_p)$.

Цифровая подпись этого параграфа является дальнейшим развитием цифровой подписи Эль Гамаля (см. [7];[2], стр.154).

5. Дальнейшие замечания

Без принципиальных изменений вместо группы $GL_n(\mathbf{F}_p)$ можно взять группу $GL_n(\mathbf{R})$, образованную невырожденными матрицами над кольцом $\mathbf{R}$. В частности, можно положить $\mathbf{R} = \mathbf{Z}/m\mathbf{Z}$ — кольцо вычетов по mod m. В качестве группы U — произвольную циклическую группу порядка m, например, группу рассмотренную в работах [6],[7].

Порядок M некоторых групп вычислить не просто. Это, например, относится к упомянутой выше группе $E(\mathbf{F}_q)$, которая часто рассматривается в качестве варианта для реализации системы распределения ключей, подобной системе Диффи и Хеллмана (см. [8],[9]). Отметим, что, в принципе, в качестве группы U возможно использовать циклическую группу со сложной задачей логарифмирования. Возможно, точное знание порядка M такой группы не обязательно: достаточно знать лишь оценку M снизу.

Например, при $n = 2$ в обозначениях §3 в качестве полугрупп H и R группы $GL_n(\mathbf{Z}/m\mathbf{Z})$ можно использовать подмножества $H'(A) = \{xA + yE\,;\, 0 \le x, y \le N\}$,$H'(B) = \{xB + yE\,;\, 0 \le x, y \le N\}$, $N < M$, подгрупп $H(A)$, $H(B)$. Произведение $\mathbf{hkr}$, $\mathbf{h} \in H$, $\mathbf{r} \in R$, можно вычислять в кольце целых чисел, ибо приведение по mod m автоматически осуществится при его отображении в группу U.

Выражаю признательность Н. П. Варновскому за ценные советы, которые позволили улучшить статью.

Литература

[1] Diffie W., Hellman M. New Direction in Cryptography // IEEE Trans. Inform. Theory. 1976, V. 22. P. 472–492.

[2] Cryptology and Computational Number Theory. Proc. of Symp. in App. Math. V. 42, Edited by C. Pomerance. 1989.

[3] В.М. Сидельников, М.А. Черепнев, В.В. Ященко, Системы открытого распределения ключей на основе некоммутативных полугрупп // Докл. РАН. 1993. Т. 332. N5.

[4] Miller V.S. Use of Elleptic Curves in Cryptography, Adv. in Cryptology (Proc. of Crypto 85) Lecture Notes in Computer Science. N.Y., V. 218. P. 417–426. 1986.

[5] Koblitz N. Elliptic curve cryptosystems // Math. Comp. 1987. V. 48, P. 203–209.

[6] О.В. Мельников и др. Общая алгебра, т. 1. М.: Наука, 1990.

[7] T. ElGamal, A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms // IEEE Trans. Inform. Theory. 1985. V. 31. P. 469–472.

[8] Nobauer R. Key Distribution Cryptosystem Based on Polinomial Function and on Redei-Functions // Probl. Control and Inform. Theory. 1986. V. 15. N 1. P. 91–100.

[9] Niederreiter H. A Public Key Cryptosystem Based on Shift Register Sequences, Lecture Notes in Computer Shience, V. 219, P. 35–39.