Криптография с открытым ключом и нечисловые алгебраические системы

А.Е. Жуков

Московский Государственный Технический Университет им. Н.Э. Баумана
Россия, Москва, 2-я Бауманская ул., д.5

Введение

За время своего существования криптография с открытым ключом из новой концепции превратилась в общепризнанную опору криптографической технологии, при этом потребность в ней продолжает расти. Однако, на сегодняшний день известно сравнительно небольшое число криптосистем с открытым ключом, причём к ним зачастую предъявляются претензии, как ввиду их малой скорости работы, так и по поводу плохого обоснования их стойкости. Вплоть до самого последнего времени «технологическая база» криптографии с открытым ключом продолжала оставаться чрезвычайно бедной. В основании стойкости таких систем обычно лежит вычислительная трудность решения некоторой задачи для какой-то алгебраической системы, чаще всего – алгебраической системы с элементами числовой природы. В подавляющем большинстве случаев это или задача факторизации больших чисел или задача дискретного логарифмирования в поле вычетов по большому простому модулю. Учитывая тот факт, что числа, как наиболее древние математические объекты, давно изучаются, неудивительны большие достижения в разработке алгоритмов для решения этих задач. В случае очередного успеха в этой области, системы, стойкость которых основана на задачах факторизации и вычисления дискретных логарифмов, могут стать значительно более уязвимыми или даже совершенно нестойкими. Поиск же других алгебраических систем, применимых в криптографии с открытым ключом, является трудной задачей и требует вовлечения в криптографический обиход новых математических объектов. Именно в этом направлении в последние годы и ведутся основные теоретические исследования.

Классические криптосистемы с открытым ключом

Как уже говорилось, стойкость подавляющего большинства криптосистем с открытым ключом основывается либо на трудности решения задачи факторизации либо на трудности задачи дискретного логарифмирования.

Задача факторизации больших чисел лежит в основании самой известной и общепризнанной системы RSA и множестве её вариантов (матричных и др.), системы Rabin-Williams, , системы LUC, предложенной Smith, Lennon (1993), систем, использующих эллиптические кривые над кольцами вычетов и т.д.

Отметим, что задача факторизации больших чисел эквивалентна задаче нахождения значения функции Эйлера $\varphi(n)$ для данного $n = pq$ при условии, что разложение числа n на множители не известно. Очевидно, что решение любой из этих задач ведет к раскрытию системы RSA. В то же время не известно, эквивалентна ли задача раскрытия системы RSA этим задачам.

Задача дискретного логарифмирования – DLP (**D**iscrete **L**ogarithm **P**roblem) в конечном поле вычетов по большому простому модулю – лежит в основании таких

наиболее известных криптоалгоритмов, как схема ключевого обмена Диффи-Хелмана и алгоритм шифрования Эль Гамаля. Аналогично ситуации с предыдущей задачей, решение DLP ведет к раскрытию схемы Диффи-Хеллмана, в то же время не известно, эквивалентна ли задача раскрытия схемы Диффи-Хеллмана (DHP – **D**iffie-**H**ellman **P**roblem) задаче DLP.

Первоначально возникнув, как теоретико-числовая проблема вычисления индекса, проблема дискретного логарифма (DLP) довольно быстро была осознана как теоретико-групповая проблема, что послужило толчком для создания *криптосистем на эллиптических кривых*. Для логарифмирования в группах, соответствующих этим кривым, в настоящее время неизвестно субэкспоненциальных алгоритмов, в отличии от мультипликативных групп полей вычетов и их расширений.

В этом же направлении находятся исследования Lenstra, Verheul и др. по *криптосистеме XTR.* Обычно схема DH, работающая с мультипликативной группой поля $\mathbf{F}_q^*$, требует от каждой стороны передачи $\sim \log_2 q$ бит информации. В работе […] предложен эффективный и компактный метод представления элементов подгруппы $G \subset \mathbf{F}_{p^6}^*$ порядка $|G| = p^2 - p + 1$. Элементы этой группы, не являющейся подгруппой мультипликативных групп подполей $\mathbf{F}_{p^2}$, $\mathbf{F}_{p^3}$, являются элементами поля $\mathbf{F}_{p^6}$, но могут быть выражены через элементы поля $\mathbf{F}_{p^2}$, т.е. для их представления требуется не $\sim 6\log_2 p$ бит , а $\sim 2\log_2 p$ бит. При этом для логарифмирования в XTR-группах применимы либо ρ-метод Полларда (квадратичной сложности), либо дискретное логарифмирование в мультипликативной группе $\mathbf{F}_{p^6}^*$ (субэкспоненциальный алгоритм). В любом случае, выбрав $p \sim \frac{1024}{6} \sim 170$ бит, получаем криптосистему по стойкости не уступающую системам, основанным на мультипликативной группе поля $\mathbf{F}_{1024}$, но элементы которой имеют представление, требующее не 1024 бита, а ~340 бит. Скорость?

Другие системы с открытым ключом

Надо отметить, что практически начиная с момента открытия двухключевой криптографии велись поиски систем с открытым ключом, стойкость которых не базируется на этих теоретико-числовых задачах. Отметим наиболее существенные направления этих исследований.

1. *Системы ранцевого типа.* Первой была система Меркля-Хеллмана (1978), основанная на классической задаче о ранце. До ее раскрытия в 1983 г. появилось огромное количество вариантов на эту тему, многие из которых теперь приводятся в учебниках как примеры успешного криптоанализа. Несмотря на это и в самое последнее время преложено несколько систем ранцевого типа, например …….
2. *Системы на корректирующих кодах.* Прежде всего, это криптосистема МакЭлайса (1978), основанная на использовании кода, исправляющего ошибки (код Гоппы), и целый ряд вариаций в этом направлении различных авторов.
3. *Решетчатые системы.* В 1997 г. Goldreih, Goldwasser, Halevi на конференции Crypto-97 предложили новую однонаправленную функцию с лазейкой, основанную

на вычислительной трудности задач на решетках, в частности на трудности нахождения точки решетки, ближайшей к заданной точке *n*-мерного действительного пространства. Под решеткой понимается множество точек *n*-мерного действительного пространства, являющихся целочисленными линейными комбинациями базисных векторов. Предложенная схема вычисляет эффективнее, чем алгоритмы RSA и El-Gamal, но требует более длинных ключей. Так, если k – параметр стойкости, то длина ключа у решетчатой системы и RSA соответственно равны $O(k^2)$ и $O(k)$, а объем вычислений, соответственно, $O(k^2)$ и $O(k^3)$.

4. К предыдущему направлению иногда относят систему *NTRU*. Предложенная в 1996 г. Hoffstein, Pipher, Silverman (США), система NTRU работает с многочленами из кольца $\mathbf{Z}[x]/(x^N - 1)$, при этом вычисления с этими многочленами проводятся по двум различным модулям p и q. За 5 лет, прошедших с момента опубликования этой системы, появилась довольно большая серия работ, посвященных ее анализу ……., а также многочисленные исследования, размещенные на сайте NTRU …… Стойкость этой системы базируется на сложности анализа операций с многочленами по различным модулям. В то же время в ряде работ показано, что стойкость ее базируется также и на сложности решения задач на решетке.

Алгебраическая формализация схемы RSA

Для описания систем, основывающихся на трудности факторизации, введём понятие кольца с лазейкой. Кольцо R называется кольцом с лазейкой […], если существует такое натуральное $n>1$, что для всех элементов $x \in R$ выполняется равенство $x^n = x$. Число n с таким свойством (такое число не обязательно единственно) является секретной информацией. Тогда операции шифрования/расшифрования можно задавать как операции возведения в степень элемента кольца R, соответствующего открытому тексту или шифртексту: $c = x^e$, $x = c^d = (x^e)^d = x^{ed} = x^n$, при условии, что $ed=n$. При этом значение e является открытым ключом, а d – секретным.

В работе […] (Varadharajan, 1986) доказано, что любое конечное кольцо с лазейкой является прямой суммой конечных полей. По сути дела этот результат показывает, что переход к кольцам с лазейкой не дает принципиально новых криптосистем, отличных от RSA. Другие возможные алгебраические структуры, для которых выполняется аналогичное соотношение – полугруппы и группы. Так в случае группы в качестве n можно выбрать число $n = k|G| + 1$, где $|G|$ – порядок этой группы.

Однако известные примеры таких групп дают криптосистемы, стойкость которых по-прежнему основана на сложности задачи факторизации. Так для $\mathrm{GL}(m, \mathbf{Z}_n)$ – группы невырожденных $(m \times m)$-матриц над кольцом $\mathbf{Z}_n$ – выражение для порядка $|\mathrm{GL}(m, \mathbf{Z}_n)|$ можно получить, если известно разложение числа n на простые множители. Если это разложение неизвестно, задача раскрытия сходна с задачей нахождения функции Эйлера $\varphi(n)$ при неизвестном разложении числа n на множители. Другую достаточно перспективную возможность дает рассмотрение группы обратимых матриц над кольцом многочленов по составному модулю.

Формализация схем DH и ElGamal

Попытаемся сформулировать наиболее общие условия, т.е. условия, не использующие понятие дискретного логарифма, при которых схема Диффи-Хеллмана (DH) и алгоритм Эль Гамаля будут работать:

Классический алгоритм Диффи-Хеллмана	Формальная схема Диффи-Хеллмана:
A: $y_1 = x^a \pmod p \mapsto$ B B: $y_2 = x^b \pmod p \mapsto$ A A: $K = (y_2)^a = (x^b)^a = x^{ab} \pmod p$ B: $K = (y_1)^b = (x^a)^b = x^{ab} \pmod p$	$\forall a \in A, \quad \forall b \in B:$ $\{E_a(x), b\} \Rightarrow E_{ab}(x); \quad \{E_b(x), a\} \Rightarrow E_{ab}(x)$ $\{E_a(x), E_b(x)\} \Rightarrow E_{ab}(x)$
Классический алгоритм шифрования Эль Гамаля:	Формальная схема Эль Гамаля:
открытый ключ: (g, g^a) *открытый текст*: m *зашифрованное сообщение*: $(g^{ab} \cdot m, g^b)$ *или* $(g^{ab} \oplus m, g^b)$	$\forall a \in A, \quad \forall b \in B:$ $\{E_a, b\} \Rightarrow E_{ab}^{-1}; \quad \{E_b, a\} \Rightarrow E_{ab}^{-1}$ $\{E_a, E_b\} \Rightarrow E_{ab}^{-1}$

Трудные задачи в теории групп

В последнее время возобновились попытки построения криптосистем с открытым ключом, использующих однонаправленные функции, базирующиеся на трудных или неразрешимых задачах теории групп или полугрупп.

Так, например, как доказано Новиковым (1955), проблема слов в общем случае, неразрешима. Для конечных групп эта проблема разрешима всегда, однако это может оказаться вычислительно трудной задачей. Проблема слов, применительно к криптографии можно было бы использовать следующим образом: выбираем два неэквивалентных слова w_1 и w_2. Одно из них преобразуется случайными преобразованиями из конечного множества образующих соотношений. Например, в группе G с образующими $\sigma_1,...,\sigma_{n-1}$ и определяющими соотношениями $\sigma_i\sigma_j\sigma_i = \sigma_j\sigma_i\sigma_j$, для $|i-j|=1$ и $\sigma_i\sigma_j = \sigma_j\sigma_i$, для $|i-j| \geq 2$, следующие слова эквивалентны:

$$\sigma_1\sigma_2\sigma_3\underline{\sigma_1\sigma_2\sigma_1} \sim \sigma_1\underline{\sigma_2\sigma_3\sigma_2}\sigma_1\sigma_2 \sim \underline{\sigma_1\sigma_3}\sigma_2\underline{\sigma_3\sigma_1}\sigma_2 \sim$$

$$\sim \sigma_3\underline{\sigma_1\sigma_2\sigma_1}\sigma_3\sigma_2 \sim \sigma_3\sigma_2\sigma_1\underline{\sigma_2\sigma_3\sigma_2} \sim \sigma_3\sigma_2\sigma_1\sigma_3\sigma_2\sigma_3.$$

Видно, что даже в этом весьма простом случае установить эквивалентность первого и последнего слова в приведенной цепочке равенств весьма не просто. Один бит шифруется следующим образом: выбирается одно из двух неэквивалентных слов w_0 или w_1, после

чего данное слово преобразуется в эквивалентное ему с помощью случайно выбранных эквивалентных преобразований. Для расшифрования требуется определить, какому из двух слов w_0 или w_1 эквивалентно полученное слово. Кодирование *n* битов делается аналогично после выбора одного из 2^n неэквивалентных слов.

Введение лазейки в проблему слов:

Пусть группа $G = \langle x_1, x_2, ..., x_n \mid r_1 = r_2 = ... = r_m = e \rangle$, где $x_1, x_2, ..., x_n$ – образующие, а $r_1 = r_2 = ... = r_m = e$ – определяющие соотношения. Добавим несколько новых соотношений, в результате получится группа

$$G' = \langle x_1, x_2, ..., x_n \mid r_1 = r_2 = ... = r_m = s_1 = ... = s_p = e \rangle,$$

тогда $G' = G / N$, где $N = \langle s_1 = ... = s_p \rangle$, обозначим через φ естественный гомоморфизм: $\varphi : G \to G'$. Если $x \sim y$ в группе G, то $\varphi(x) \sim \varphi(y)$ в группе G', и обратно: если $\varphi(x) \nsim \varphi(y)$ в группе G', то $x \nsim y$ в группе G. Чтобы лазейка работала, в группе G необходимо выбрать слова w_i таким образом, чтобы для любой пары различных слов w_i, w_j их образы $\varphi(w_i) \nsim \varphi(w_j)$, и при этом в группе G' проблема эквивалентных слов была бы легко разрешима. Тогда в группе G' надо найти слово $\varphi(w_i)$, которое эквивалентно слову $\varphi(y)$.

Для того, чтобы построить такую лазейку, необходимо выбрать дополнительные соотношения $s_1 = s_2 = ... = s_p = e$ т.о., чтобы соотношения $r_1 = r_2 = ... = r_m = e$ стали тривиальными. Слова $\{r_i\}$, определяющие исходные соотношения, подбираются т.о., чтобы это было легко осуществимо.

Так как для алгебраических объектов теоретико-числовой природы разработаны сравнительно хорошие алгоритмы, для построения новых систем с открытым ключом можно попробовать уход в алгебраические системы с элементами нечисловой природы, например, в неабелевые группы – группы заведомо нечисловой природы. При использовании таких групп в криптосистеме с открытым ключом прежде всего возникают следующие вопросы:

- Как представить сообщение в виде элемента группы *G*;
- Существует ли единственное представление для элементов группы *G*. Если элементы представляются не единственным образом, открытый текст и расшифрованный могут не совпасть как выражения.
- Возможно ли эффективное вычисление такого представления.

Существуют группы, для которых знаменитая теоретико-групповая проблема – проблема равенство слов – разрешима в полиномиальное время, и в то же время для которых неизвестны алгоритмы полиномиальной сложности, разрешающие проблему сопряженности. Пример – группы кос.

Трудно решаемые проблемы для некоммутативных групп

1. ***Проблема сопряженности:***
   Дано: $x, y \in G$
   Определить: $x \sim y$?

2. ***Проблема поиска сопрягающего элемента:***
   Дано: $x, y \in G, \quad x \sim y$
   Определить: $a \in G : \; axa^{-1} = y$

3. ***Обобщенная проблема поиска сопрягающего элемента:***

   Дано: $x, y \in G, \quad y = bxb^{-1}, \quad b \in H \subset G, \quad b - неизвестен$

   Определить: $a \in H: \; axa^{-1} = y$

4. ***Проблема сопряженной разрешимости:***

   Дано: $x, y \in G, \quad y = bxb^{-1}, \quad b \in H \subset G$

   Определить: $a_1, a_2 \in G: \; a_1 x a_2 = y$

5. ***Проблема извлечения корня:***

   Дано: $y \in G, \quad y = x^p, \quad x - неизвестен$

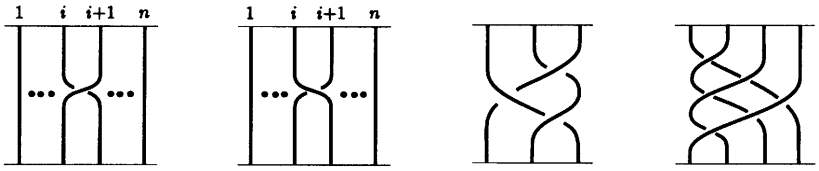
   Определить: $z \in G: \; y = z^p$

Группы кос (Braid groups)

В 2000 году на конференции Crypto-2000 группа южнокорейских ученых (Ko и другие) предложили новую криптосистему с открытым ключом, основанную на трудности решения проблемы сопряженности в группах кос – бесконечных неабелевых группах. Группа кос может быть формально задана как

$$B_n = \left\langle \sigma_1, \ldots, \sigma_{n-1} \;\middle|\; \begin{array}{ll} \sigma_i \sigma_j \sigma_i = \sigma_j \sigma_i \sigma_j, & |i-j| = 1 \\ \sigma_i \sigma_j = \sigma_j \sigma_i, & |i-j| \geq 2 \end{array} \right\rangle.$$

Элементы группы B_n действуют на множестве занумерованных нитей, называемых косой. Образующий элемент σ_i переплетает нити i и i+1 косы таким образом, что нить i+1 лежит сверху. Число n нитей в косе называется индексом косы. Умножение двух кос a и b получается, если косу a расположить раньше косы b. Нейтральный элемент e образован n прямыми нитями, обратный элемент σ_i^{-1} переплетает нити i и i+1 косы таким образом, что нить i+1 лежит снизу.



(a) σ_i (b) σ_i^{-1} (c) $\sigma_2\sigma_1^{-1}\sigma_2$ (d) Δ_4

Заметим, что если к имеющимся соотношениям (*) добавить соотношения $\left\{\sigma_i^2 = e\right\}$, то получим представление симметрической группы S_n, для системы образующих транспозиций $\left\{\sigma_i = (i, i+1)\right\}$. Таким образом, существует единственный эпиморфизм $\rho: B_n \to S_n$.

Элементы группы B_n допускают неоднозначное представление через образующие:

$$\Delta_4 = \sigma_1\sigma_2\sigma_3\underline{\sigma_1\sigma_2\sigma_1} = \sigma_1\underline{\sigma_2\sigma_3\sigma_2}\sigma_1\sigma_2 = \underline{\sigma_1\sigma_3}\sigma_2\underline{\sigma_3\sigma_1}\sigma_2 =$$

$$= \sigma_3\underline{\sigma_1\sigma_2\sigma_1}\sigma_3\sigma_2 = \sigma_3\sigma_2\sigma_1\underline{\sigma_2\sigma_3\sigma_2} = \sigma_3\sigma_2\sigma_1\sigma_3\sigma_2\sigma_3$$

Однако существует единственным образом определенное представление кос через некоторые косы Δ_n, называемые фундаментальными, и подставки из S_n. Считаем, что группа B_n содержит группу B_m, $m < n$, в качестве подгруппы. В работе «New Public-Key Cryptosystem Using Braid Group» Ko, Lee, Cheon, Han, Kang, Park (Корея, США) на Crypto-2000

предложено использовать сложность обобщенной проблемы поиска сопрягающего элемента.

Однонаправленная функция:

$B_{l+r} \supset B_l, B_r$ – подгруппы, соответствующие l левым и r правым нитям: $B_{l+r} = \langle \sigma_1,...,\sigma_{l+r-1} \rangle$, $B_l = \langle \sigma_1,...,\sigma_{l-1} \rangle$, $B_r = \langle \sigma_{l+1},...,\sigma_{l+r-1} \rangle$. Элементы $a \in B_l$ и $b \in B_r$ коммутируют: $ab = ba$.

Однонаправленная функция:

$$f : B_l \times B_{l+r} \to B_{l+r} \times B_{l+r}$$
$$f(a,x) = (axa^{-1}, x)$$

Функция *f* однонаправлена, так как по данным элементам (*a*,*x*) можно легко найти axa^{-1}, но по известным (axa^{-1}, x) найти элемент *a* можно, насколько это известно, лишь за экспоненциальное время.

Протокол выработки секретного ключа (вариант протокола DH для группы кос): Открытая информация: группа B_{l+r} и достаточно сложный элемент $x \in B_{l+r}$.

1. A выбирает секретный элемент $a \in B_l$ и посылает B элемент $y_1 = axa^{-1}$.
2. B выбирает секретный элемент $b \in B_r$ и посылает A элемент $y_2 = bxb^{-1}$.
3. A вычисляет $K = ay_2a^{-1} = abxb^{-1}a^{-1}$.
4. B вычисляет $K = by_1b^{-1} = baxa^{-1}b^{-1} = abxb^{-1}a^{-1}$.

Криптосистема с открытым ключом – типа El Gamal. Пусть $H : B_{l+r} \to \{0,1\}^k$ – хорошая хэш-функция. Выбирается группа B_{l+r} и достаточно сложный элемент $x \in B_{l+r}$. Кроме того выбирается элемент $a \in B_l$.

Открытый ключ: $(x, y = axa^{-1})$. Секретный ключ: *a*.

Шифрование: Открытый текст $m \in \{0,1\}^k$. Выбирается случайное $b \in B_r$.

Посылается пара (*c*,*d*), где $d = bxb^{-1}$, $c = m \oplus H(byb^{-1})$.

Расшифрование: Вычисляется $ada^{-1} = abxb^{-1}a^{-1} = baxa^{-1}b^{-1} = byb^{-1}$, а тогда $m = c \oplus H(byb^{-1})$

В работе Pseudorandomness from Braid Groups Lee, Lee, Hahn (Корея) доказано, что на основе криптосхем, использующих группы кос, можно получить доказуемо секретные псевдослучайные генераторы случайных последовательностей.

Новая криптосистема с открытым ключом, построеная на базе конечных неабелевых групп.

Была представлена на конференции Crypto-2001 южнокорейскими учеными Paeng, Ha, Kim, Chee, Park (New Public Cryptosystem Using Finite Non Abelian Groups).

Сложные задачи для неабелевых групп:

1) *Проблема сопряженности*: для сопряженных элементов $x, y \in G$ найти $u \in G$, такой, что $uxu^{-1} = y$.

2) *Специальная проблема сопряженности*: для данного автоморфизма Inn_g (но неизвестного элемента g) найти $g_1 \in G$, такой, что $Inn_{g_1} = Inn_g$.

Для неабелевой группы *G* со сложной проблемой сопряженности можно построить следующую криптосистему.

Пусть группа $G = \langle \delta_i \rangle$, т.е. $\{\delta_i\}$ – ее образующие, а элемент $g \in G$.

Открытый ключ: $\{\varepsilon_i = g\delta_i g^{-1}\}$. Секретный ключ: $g \in G$, точнее Inn_g.

Если $m \in G$ – открытый текст, $c \in G$ – шифртекст, то

$$c = m^g = gmg^{-1} = Inn_g(m), \quad m = c^{g^{-1}} = g^{-1}mg = Inn_{g^{-1}}(m).$$

Для шифрования нужно, чтобы $m \in G$ можно было легко выразить через образующие $\{\delta_i\}$, а затем в полученном выражении заменить δ_i на ε_i. Однако, если любой элемент группы *G* легко выражается через $\{\varepsilon_i\}$, дешифрование (взлом) происходит так же легко, как и шифрование.

Стойкость системы основана на сложности нахождения $g_1 \in G$, такого, что $Inn_{g_1} = Inn_g$. К сожалению, для многих неабелевых групп, например, для $\mathrm{SL}(2, \mathbf{Z}_p)$, проблема сопряженности легко разрешима (для группы $\mathrm{SL}(2, \mathbf{Z}_p)$ она сводится к решению системы линейных уравнений над $\mathbf{Z}_p$).

Новая криптосистема:

Пусть выбрана большая неабелева группа *G*, *Z*(*G*) – ее нетривиальный центр большого порядка, а элемент $g \in G$. Пусть $\{\gamma_i\}$ – множество образующих элементов группы *G*, т.е. $G = \langle \delta_i \rangle$. Внутренний автоморфизм Inn_g будем задавать набором соответствующих образов образующих элементов:

$$\{Inn_g(\gamma_1), ..., Inn_g(\gamma_i), ...\} = \{\gamma_1^g, ..., \gamma_i^g, ...\} = \{\varepsilon_1, ..., \varepsilon_i, ...\}.$$

Для системы с открытым ключом: $\begin{cases} \text{отрытый ключ: } (Inn_g, \ Inn_{g^a}) \\ \text{секретный ключ: число } a \end{cases}$

Шифрование:

1) Выразить открытый текст $m \in G$ как произведение образующих элементов
2) Выбрать число *b* и вычислить $Inn_{(g^a)^b}$, задаваемый как набор

$$\{Inn_{g^{ab}}(\gamma_1), ..., Inn_{g^{ab}}(\gamma_i), ...\}$$

3) Вычислить шифртекст $c = Inn_{g^{ab}}(m)$

4) Вычислить $\varphi = Inn_{g^b}$, т.е. набор $\{Inn_{g^b}(\gamma_1), ..., Inn_{g^b}(\gamma_i), ...\}$

5) Послать сообщение: (c, φ)

Расшифрование:

1) Выразить шифртекст c через образующие $\{\gamma_i\}$

2) Вычислить $\varphi^{-a} = Inn_{g^{-ab}}$

3) Открытый текст $m = \varphi^{-a}(c)$

1) Для практической реализации этой схемы необходимо, чтобы Inn_{g^a} выражалось небольшим количеством бит. Далее, необходимо иметь эффективное выражение элементов группы G через образующие $\{\gamma_i\}$.

2) Если в схеме шифрования Эль-Гамаля зашифровать два сообщения на одном и том же b, то имеет место соотношение $c_1^{-1}c_2 = (m_1 g^{ab})^{-1}(m_2 g^{ab}) = m_1^{-1}m_2$. В нашей схеме, зная $c_1 = Inn_{g^{ab}}(m_1)$ и $c_2 = Inn_{g^{ab}}(m_2)$, получить информацию о $m_1^{-1}m_2$ по-видимому трудно.

Задача нахождения секретного ключа a по известному ключу $(Inn_g,\ \ Inn_{g^a})$.

1) Если решать DLP в группе $\langle Inn_g \rangle_N$ непосредственно – в силу представления ее же элементов – ничего лучше $O\sqrt{N}$, где N – ее порядок.

2) Если решать DLP в группе $\langle g \rangle \subset G$ и предположить, что для группы G легко решается специальная проблема сопряженности, т.е. по Inn_{g^a} легко находиться такой g_0, что $Inn_{g_0} = Inn_{g^a}$, тогда получаем: $g_0 = g^a z,\ \ z \in Z(G)$, где $z \in Z(G)$ – центр группы G. Если порядок $|Z(G)|$ большой, то трудно определить принадлежность $g^a z \in \langle g \rangle$.

Выбор открытого текста m и элемента $g \in G$ надо делать осторожно: если m и g коммутируют, то $c = g^{ab} m g^{-ab} = m$. В частности, $m, g \in Z(G)$.

Выбор группы G.

Группы матриц и полупрямое произведение абелевых групп являются такими неабелевыми группами, для которых существует каноническое представление элементов, т.е. дающее для любого элемента группы единственное выражение. В работе […] предлагается новая криптосистема с открытым ключом, основанная на использовании конечной неабелевой группы G. Ее стойкость базируется на DLP для группы внутренних автоморфизмов группы G:

$$\mathrm{Aut}G \supseteq \mathrm{Inn}G = \left\{ f_g \in \mathrm{Aut}G \,\middle|\, f_g(x) = gxg^{-1} \quad \forall x \in G \right\}.$$

Конструкция полупрямого произведения групп. Пусть G и H – группы, θ – гомоморфизм группы H в группу автоморфизмов группы G: $H \xrightarrow{\theta} \mathrm{Aut}G$, $\mathrm{Aut}G = \{ f \mid f : G \cong G \}$. Пусть $h \xrightarrow{\theta} f_h$. Будем обозначать действие автоморфизма f_h на элементе $g \in G$ как $f_h(g) = (g)^h$. Тогда полупрямым произведением групп G и H относительно гомоморфизма θ называется множество $G \times_\theta H = \{ (g,h) \mid g \in G, h \in H \}$ с заданной на нем бинарной операцией $(g_1,h_1)(g_2,h_2) = \left(g_1 \cdot (g_2)^{h_1}, h_1 \cdot h_2\right)$ относительно которой $G \times_\theta H$ является группой. Заметим, что $(g,h)^{-1} = \left((g^{-1})^{h^{-1}}, h^{-1}\right)$ и тогда

$$(1_G,h_1)\cdot(g_2,1_H)\cdot(1_G,h_1)^{-1} = \left(1_G (g_2)^{h_1}, h_1\right)\cdot\left(1_G^{h_1^{-1}}, h_1^{-1}\right) = \left(g_2^{h_1}, 1_H\right).$$

Таким образом, G является нормальной подгруппой группы $G \times_\theta H$. Если $\theta(H) \neq \{Id\} \subset \mathrm{Aut}G$, то $G \times_\theta H$ – неабелева, даже если G и H – абелевы группы.

Пример.

Рассмотрим группу автоморфизмов группы вычетов по модулю 3:

$$\mathrm{Aut}\,\mathbf{Z}_3 \cong \mathbf{Z}_2 \Rightarrow \begin{cases} f_0: & f_1: \\ 0 \to 0 & 0 \to 0 \\ 1 \to 1 & 1 \to 2 \\ 2 \to 2 & 2 \to 1 \end{cases}$$

Группа $\mathbf{Z}_3 \times_\theta \mathbf{Z}_2$ – неабелева: $\begin{cases} (2,0)\cdot(1,1) = (2 + f_0(1), 0+1) = (0,1) \\ (1,1)\cdot(2,0) = (1 + f_1(2), 1+0) = (2,1) \end{cases}$

Пример.

Рассмотрим неабелеву группу G, тогда существует гомоморфизм $Inn : G \to \mathrm{Aut}G$, определяемый формулой $g \to Inn_g$, $Inn_g x = gxg^{-1} = x^g$ для которого $\mathrm{Ker}Inn = Z(G) = \{z \in G \,|\, zx = xz, \forall x \in G\}$ – центр группы G. Если группа G – абелева, то $G \times_{Inn} G = G \times G$ – прямое произведение.

Рассмотрим группу $\mathrm{SL}(2,\mathbf{Z}_p)$, элемент $\alpha = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in \mathrm{SL}(2,\mathbf{Z}_p)$ имеет порядок $o(\alpha) = p$. Пусть $\mathbf{Z}_p \xrightarrow{\theta} \mathrm{Aut}\,SL(2,\mathbf{Z}_p)$ является композицией изоморфизма θ_1 и гомоморфизма Inn: $\mathbf{Z}_p \xrightarrow{\theta_1} \langle a \rangle \xrightarrow{Inn} \mathrm{Aut}\,SL(2,\mathbf{Z}_p)$. Рассмотрим группу $G = SL(2,\mathbf{Z}_p) \times_\theta \mathbf{Z}_p$. Порядок ее центра $|Z(G)| = 2p$. Нетрудно заметить, что $(x,y)\cdot(a,b)\cdot(x,y)^{-1} = \left(x\cdot(a)^y \cdot (x^{-1})^b, b\right)$, таким образом, открытый текст $m \in \mathrm{SL}(2,\mathbf{Z}_p)$ т.к. вторая компонента при транспозиции не меняется.

В группе $\mathrm{SL}(2,\mathbf{Z}_p)$ выделяются две образующие:

$$SL(2,\mathbf{Z}_p) = \langle T, S \rangle, \quad T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \quad S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}.$$

Любой элемент $m \in \mathrm{SL}(2,\mathbf{Z}_p)$ с $m_{12} \neq 0$ единственным образом представляется в виде $m = T^{j_1} S T^{j_2} S T^{j_3}$. Тогда для группы G множество образующих имеет вид: $G = \langle (T,0), (S,0), (E,1) \rangle$.

Заметим, что вероятность выбрать m из центра группы G оценивается как $\mathrm{P}\{m \in Z(G)\} \approx \frac{2}{p^2} \xrightarrow[p\to\infty]{} 0$. Аналогично, $\mathrm{P}\{g \in Z(G)\} \approx \frac{2}{p^3} \xrightarrow[p\to\infty]{} 0$ и $\mathrm{P}\{m \in Z(g)\} \approx \frac{2}{p} \xrightarrow[p\to\infty]{} 0$.

Задача DLP в группе $\langle g \rangle_N$, где $N = o(g)$, оценивается как $\mathrm{O}(\sqrt{q})$, где q – максимальный простой делитель числа N.

Можно выбрать g: $p \,|\, N$.

Если специальная проблема сопряженности легко разрешима, то для нахождения $g_0 = g^a$, $g_0 \in \langle g \rangle$ понадобится ~O(N) попыток – даже хуже, чем для DLP.

Если выбрать $p \sim 2^{160}$, стойкость нашей системы сопоставима со стойкостью RSA-1024 (сложность DLP для нас и задача разложения для RSA-1024 оцениваются, соответственно, как 2^{87} и 2^{80}).

По скорости: шифрует в 30 раз быстрее RSA с открытым ключом в 32 бита, расшифровывает в 200 раз быстрее RSA с открытым ключом в 32 бита.

В 40 раз быстрее ECC-170 бит.

Рассматриваются другие возможные конструкции для неабелевой группы G.

Преимущества:

- Криптосистема с группой G может применяться, даже если DLP и проблема сопряженности для самой группы G не являются сложными задачами.
- Хотя в принципе используется схема шифрования Эль-Гамаля: g^a – открытый ключ, m – открытый текст, $(g^{ab}m, g^b)$ – шифртекст, в нашем случае, в отличии от классического алгоритма Эль-Гамаля, можно зафиксировать значение b и не вычислять его для каждого открытого текста заново. Тем самым повышается скорость шифрования и расшифрования. Так, по сравнению со схемой RSA с аналогичными параметрами, скорость шифрования возрастает в 30 раз, а расшифрования – в 200.
- На основе предложенной криптосхемы легко построить схему выработки цифровой подписи. В общем случае при использовании неабелевых групп, например, групп кос – это сделать достаточно сложно.

Литература.

Jae Choon Cha, Ki Hyoung Ko, Sang Jin Lee, Jae Woo Han, and Jung Hee Cheon. ***An Efficient Implementation of Braid Groups***: C. Boyd (Ed.): Advances in Cryptology - ASIACRYPT 2001 7th International Conference on the Theory and Application of Cryptology and Information Security, Gold Coast, Australia, December 9-13, 2001. Proceedings, LNCS 2248, p. 144 ff.

Seong-Hun Paeng, Kil-Chan Ha, Jae Heon Kim, Seongtaek Chee, and Choonsik Park. ***New Public Key Cryptosystem Using Finite Non Abelian Groups***: J. Kilian (Ed.): Advances in Cryptology CRYPTO 2001, 21st Annual International Cryptology Conference, Santa Barbara, California, USA, August 19-23, 2001, Proceedings, LNCS 2139, p. 470 ff.

Jeffrey Hoffstein, Jill Pipher, and Joseph H. Silverman. ***NSS: An NTRU Lattice-Based Signature Scheme***: B. Pfitzmann (Ed.): Advances in Cryptology - EUROCRYPT 2001, Second Symposium, PADO 2001, Aarhus, Denmark, May 21-23, 2001, Proceedings, LNCS 2045, p. 211 ff.