УДК 681.3

А. А. Григорьев, П. В. Дудкин

Московский физико-технический институт (государственный университет)

Криптографические примитивы на полупрямых произведениях групп

Исследуется новый класс криптографических примитивов, опирающихся на операцию возведения в степень в некоммутативных группах. Широкий класс некоммутативных групп дает известная конструкция полупрямого произведения. Анализ этой конструкции выявляет специфику структуры степени элемента в полупрямом произведении групп. Эта специфика приводит к схеме генерации секретных ключей, подобной известной схеме Диффи–Хеллмана. Предложено два конкретных протокола генерации ключей. В одном из них используется расширение мультипликативной группы простого поля Z_p посредством некоторой циклической подгруппы ее группы автоморфизмов. Во втором – конструкция некоммутативной группы порядка p^3 как полупрямого произведения циклических групп порядков p^2 and p. Обсуждается сложность атак на предложенные схемы генерации ключей.

Ключевые слова: криптография, генерация ключей, полупрямое произведение.

A. A. Grigoriev, P. V. Dudkin

Moscow Institute of Physics and Technology (State University)

Cryptographic primitives based on semidirect group products

A new class of cryptographic primitive constructions based on exponentiation in noncommutative groups is discussed. A wide class of noncommutative groups is given by the classical construction of semidirect group product. Discussing semidirect products we reveal the form of an expression for a group element power. This form leads to key generation procedure analogues to the Diffie-Hellman scheme. Two concrete key generation protocols are given. One of them is based on an extension of the multiplicative group of the simple field Z_p by some cyclic subgroup of its automorphism group. The other use is the construction of the noncommutative p^3-group as a semidirect product of cyclic groups of orders p^2 and p. The complexity of attacks on a proposed key generation procedures is given.

Key words: cryptography, key generation, semidirect product.

1. Схема генерации ключей Диффи–Хеллмана

Пусть две стороны A и B, соединенные каналом связи, хотят стать обладателями секретного ключа K, недоступного какой-либо третьей стороне. Для этого они предварительно выбирают и публикуют большое простое число p и некоторый элемент ξ из мультипликативной группы Z_p^* поля Z_p чисел по модулю p.

Сторона A случайно выбирает большое натуральное l, вычисляет число $L = \xi^l$ и передает его стороне B. Сторона B выбирает случайное r и передает стороне A число $R = \xi^r$. По завершении обмена $L \leftrightarrows R$ стороны получают возможность вычислить общий ключ K:

$$R^l = (\xi^r)^l = K = (\xi^l)^r = L^r.$$

Для того чтобы третья сторона, перехватившая сообщения $L = \xi^l$ и $R = \xi^r$, смогла вычислить ключ K, она должна найти хотя бы один из случайных показателей l, r, то есть решить задачу вычисления дискретного логарифма $l = \log_\xi L$ или $r = \log_\xi R$.

2. Полупрямые произведения

Пусть даны две группы N и H и пусть $H \to Aut(N)$ – гомоморфизм группы H в группу автоморфизмов группы N. Иными словами, пусть каждому элементу $h \in H$ поставлен с соответствие автоморфизм $\varphi_h(n) : N \to N$, так что $\varphi_{h_1}(\varphi_{h_2}(n)) = \varphi_{h_1 h_2}(n)$. Нейтральному элементу $e \in H$ отвечает при этом тривиальный автоморфизм группы N: $\varphi_e(n) = n$.

Полупрямое произведение $G = N \times_\varphi H$, [3], вводится как множество пар (n, h), $n \in N, h \in H$, с групповой операцией

$$(n_1, h_1)(n_2, h_2) = (n_1 \varphi_{h_1}(n_2), h_1 h_2).$$

Ассоциативность так введенного умножения легко проверяется. Нейтральным элементом группы $G = N \times_\varphi H$ является пара (e, e) нейтральных элементов N и H. Обратным к (n, h) является элемент $(\varphi_{h^{-1}}(n^{-1}), h^{-1})$. Наборы (n, e), $n \in N$ и (e, h), $h \in H$, образуют подгруппы, изоморфные N и H. Пересечение этих подгрупп состоит из единственного нейтрального элемента (e, e). Легко показать, что $(\mathrm{e}, h)(n, e)(e, h)^{-1} = (\varphi_h(n), e)$, так что подгруппа N нормальна в G (инварианта относительно внутренних автоморфизмов), а действие на N внутреннего автоморфизма, отвечающего элементу (e, h), совпадает с действием φ_h.

Если гомоморфизм $H \to Aut(N)$ тривиален – ставит в соответствие всем элементам H тривиальный автоморфизм группы N, полупрямое произведение сводится к декартову произведению $G = N \times H$ с операцией

$$(n_1, h_1)(n_2, h_2) = (n_1 n_2, h_1 h_2).$$

В противном случае в G существует нетривиальный внутренний автоморфизм, так что эта группа заведомо некоммутативна.

Группу $G = N \times_\varphi H$ называют расширением N посредством группы H. Расширению отвечает точная последовательность морфизмов

$$e \to N \to G \to H \to e,$$

где левый морфизм – это вложение группы N, образом которого является нормальная подгруппа группы G, а правый морфизм отображает фактор-группу по этой нормальной подгруппе на группу H. В конструкции расширения участвуют три группы (сами группы N, H и группа $Aut(N)$ автоморфизмов N) и один гомоморфизм $H \to Aut(N)$, который отображает H на некоторую подгруппу $Aut(N)$. Конструкция становится более прозрачной, если в качестве H выбрана непосредственно некоторая подгруппа $Aut(N)$, в частности, вся эта группа: $H = Aut(N)$. Тогда в конструкции оказываются задействованными только N и $H \subseteq Aut(N)$.

В любом случае построение полупрямого произведения требует знания группы $Aut(N)$ автоморфизмов группы N, избранной для расширения. Проблема описания структуры групп автоморфизмов до конца решена для конечных коммутативных групп. Всякая такая группа является декартовым произведением циклических групп, а описание группы автоморфизмов циклической группы сводится к характеризации набора ее примитивных элементов: всякий автоморфизм переводит примитивный элемент в примитивный, и наоборот, всякое отображение примитивного элемента на примитивный продолжается до автоморфизма порождаемой ими группы.

Изучим структуру операции возведения в степень в полупрямом произведении групп: $(n, h)^s$, $(n, h) \in N \times_\varphi H$. Имеем

$$(n, h)^2 = (n, h)(n, h) = (n\varphi_h(n), h^2),$$

$$(n, h)^3 = (n\varphi_h(n), h^2)(n, h) = (n\varphi_h(n)\varphi_{h^2}(n), h^3),$$

и так далее до

$$(n, h)^s = (n\varphi_h(n)\varphi_{h^2}(n) \dots \varphi_{h^{(s-1)}}(n), h^s) = (n^{(s)}, h^s),$$

где

$$n^{(s)} = n\varphi_h(n)\varphi_{h^2}(n)\dots\varphi_{h^{(s-1)}}(n).$$

Видно, что при возведении в степень элемента $(n,h) \in N \times_\varphi H$ его компоненты $n \in N$ и $h \in H$ преобразуются по-разному. Компонент h просто возводится с степень s, как и в кольце Z_n. А вот степень $n^{(s)}$ компонента n вычисляется как произведение элементов группы N, входящих в орбиту элемента n относительно последовательного действия отображения $\varphi_h(n)$. Число элементов в этой орбите в общем случае равно периоду элемента φ_h в группе $Aut(N)$. Если этот период велик, то степень $y = n^{(s)}$ оказывается произведением s различных элементов группы N, так что задача вычисления дискретного логарифма $s = \log_n(y)$ существенно усложняется. Это и дает основание предполагать, что адекватный выбор структуры полупрямого произведения позволит предложить односторонние функции, более стойкие по сравнению с обычным дискретным логарифмом в модульном кольце.

3. Генерация ключей на полупрямых произведениях

Пусть в публичном доступе находится элемент (n,h) полупрямого произведения $G = N \times_\varphi H$. Как и ранее, сторона A выбирает случайное l и вычисляет $(n,h)^l = (n^{(l)}, h^l) = (L, h^l)$, где

$$L = n^{(l)} = n\varphi_h(n)\varphi_{h^2}(n)\dots\varphi_{h^{(l-1)}}(n).$$

Элемент L передается стороне B. Сторона B выбирает случайное r, вычисляет $(n,h)^r = (n^{(r)}, h^r) = (R, h^r)$,

$$R = n^{(r)} = n\varphi_h(n)\varphi_{h^2}(n)\dots\varphi_{h^{(r-1)}}(n)$$

и передает R стороне A. Теперь стороны A и B оказываются в состоянии вычислить общий ключ K. На стороне A вычисление проводится по схеме

$$(n,h)^{l+r} = (n,h)^l(n,h)^r = (L,h^l)(R,\dots) = (L\varphi_{h^l}(R),\dots) = (K,\dots),$$

а на стороне B несколько иначе:

$$(n,h)^{r+l} = (n,h)^r(n,h)^l = (R,h^r)(L,\dots) = (R\varphi_{h^r}(L),\dots) = (K,\dots).$$

Существенно, что недостающие на сторонах элементы h^r, h^l в вычислениях не используются. Общим для двух сторон ключом становится элемент $K = L\varphi_{h^l}(R) = R\varphi_{h^r}(L)$.

Чтобы вычислить ключ K по результатам перехвата L, R, необходимо знать хотя бы один из показателей l, r, а их нахождение по известным $n^{(l)}, n^{(r)}$ эквивалентно вычислению дискретного логарифма в полупрямом произведении.

4. Простой пример

Выберем в качестве N циклическую мультипликативную группу Z_p^* поля Z_p и пусть ξ – ее примитивный элемент с периодом $p-1$. Набор примитивных элементов Z_p^* исчерпывается степенями ξ^k с показателями k, взаимно простыми с $(p-1)$. Каждому такому k отвечает автоморфизм $\varphi_k(x) = x^k$, который переводит элемент ξ в ξ^k. В качестве H возьмем циклическую подгруппу $Aut(Z_p^*)$, порожденную автоморфизмом $\varphi_k(x)$. Степень $(n,k)^s$ элемента (n,k), $n \in Z_p^*, \varphi_k \in Aut(Z_p^*)$ имеет вид: $(n^{(s)}, \varphi_{k^s})$, где

$$y = n^{(s)} = nn^k n^{k^2}\dots n^{k^{(s-1)}} = n^{\frac{k^s-1}{k-1}}.$$

Видно, что для вычисления дискретного логарифма $s = \log_n(y)$ требуется не только найти показатель m, такой что $y = n^m$, но и найти затем число s, такое что $m = \frac{k^s-1}{k-1}$. А это эквивалентно двукратному решению задачи вычисления дискретного логарифма.

5. Некоммутативная группа порядка p^3

Существуют в точности две некоммутативные группы порядка p^3 [3]. Одна из них является полупрямым произведением циклической группы $N = C_{p^2}$ порядка p^2 на циклическую группу $H = C_p$ порядка p. Вторая получается как полупрямое произведение группы $N = C_p \times C_p$ – декартова произведения двух групп C_p на ту же группу $H = C_p$. Более предпочтительной с позиций криптографии представляется первая группа, содержащая элементы периода p^2. Периоды всех элементов второй группы составляют p.

Группа автоморфизмов C_{p^2} изоморфна декартову произведению $C_p \times C_{p-1}$ и содержит подгруппу, изоморфную C_p. Так что вложение группы $H = C_p$ в группу автоморфизмов группы $N = C_{p^2}$ конструируется естественным образом.

Циклическую группу C_{p^2} можно реализовать как подгруппу мультипликативной группы $Z^*_{p^3}$ кольца Z_{p^3}. Группа $Z^*_{p^3}$ циклическая порядка $p^2(p-1)$. В ней существует подгруппа порядка p^2, порожденная степенями некоторого элемента $\xi \in Z_{p^3}$ порядка p^2. Итак, пусть

$$N = \{1 = \xi^0, \xi^1, \xi^2, \dots \xi^{p^2-1}, \xi^{p^2} = \xi^0 = 1\}, \quad \xi \in Z_{p^3},\ \xi^{p^2} = 1.$$

В этом представлении отображение аддитивной группы $H = C_p$ в группу автоморфизмов группы $N = C_{p^2}$ строится элементарно: элементу $h \in C_p$ поставим в соответствие автоморфизм $\varphi_h(\xi^n) = \xi^{n(1+ph)}$. Это соответствие действительно является гомоморфизмом, поскольку

$$\varphi_{h_2}(\varphi_{h_1}(\xi^n)) = \xi^{n(1+ph_1)(1+ph_2)} = \xi^{n(1+p(h_1+h_2))} = \varphi_{h_1+h_2}(\xi_n).$$

Степень s элемента (ξ, n) в $G = C_{p^2} \times_\varphi C_p$ вычисляется как

$$(\xi, h)^s = (\xi\xi^{1+hp}\xi^{1+2hp} \dots \xi^{1+h(s-1)p}, sn) = (\xi^{s+hp\frac{s(s-1)}{2}}, ns) = (\xi^{(s)}, ns).$$

Результатом становится следующая схема генерации ключей: публикуемые данные – простое p, элемент $\xi \in Z_{p^3}$ порядка p^2, число $n \in Z_p$.

Сторона A выбирает случайное l, вычисляет $L = \xi^{(l)}$ и передает L на сторону B. Сторона B выбирает случайное r, вычисляет $R = \xi^{(r)}$ и передает R на сторону A.

Стороны вычисляют общий секретный ключ по схеме

$$K = LR^{(1+npl)} = RL^{(1+npr)}.$$

Для нахождения секретного ключа K по перехваченным L, R злоумышленнику придется решить уравнение

$$\mathrm{y} = \xi^{(s)} = \xi^{s+hp\frac{s(s-1)}{2}}$$

относительно показателя s в кольце Z_{p^3}. Для этого требуется вначале решить задачу вычисления дискретного логарифма $m = \log_\xi(y)$ в кольце Z_{p^3}, а затем решить уравнение $m = s + hp\frac{s(s-1)}{2}$ по модулю p^2 относительно показателя s. Сложность создает здесь как добавление второго этапа, так и то, что вычисление дискретного логарифма производится в подгруппе порядка p^2 группы $Z^*_{p^3}$.

6. Заключение

Анализ полученных результатов показывает, что даже в случае рассмотренных здесь элементарных реализаций схема генерации ключей на полупрямых произведениях групп обеспечивает более высокую стойкость по отношению к атакам по сравнению со схемой Диффи–Хеллмана. Становится понятными также и слабое место предложенного подхода. Оно состоит в том, что при вычислении степени

$$n^{(s)} = n\varphi_h(n)\varphi_{h^2}(n) \dots \varphi_{h^{(s-1)}}(n)$$

на самом деле используется лишь циклическая подгруппа группы $Aut(N)$, порожденная степенями $\varphi_{h^k} = \varphi_h^k$ базового автоморфизма φ_h, а сам этот автоморфизм в обоих примерах обладает простой структурой, что позволяет привести выражение для степени $n^{(s)}$ к форме $n^{F(s)}$ с относительно простой функцией $F(s)$. Это усложняет атаку вычислением показателя s ровно на сложность обращения функции $F(s)$. Такое усложнение вряд ли достаточно радикально, чтобы мотивировать решительный отказ от простой классической схемы.

Достижения большей стойкости требует усложнения структуры формулы степени $n^{(s)}$. В этой связи интерес представляют расширения групп N, обладающих мощными группами автоморфизмов $Aut(N)$, содержащими нетривиально вычисляемые отображения φ_h, произведение степеней которых не удается привести к компактному виду.

Альтернативный путь может дать переход от вычисления степени $(n, h)^s$ к вычислению произведения $(n, h_1)(n, h_2)\dots(n, h_s)$ с s различными элементами группы H. При этом в формуле для $n^{(s)}$ окажутся задействованными автоморфизмы, не являющиеся степенями базового. Возможность получения простой формулы для $F(s)$ этим практически исключается, а вычисление общего ключа по схеме $K = L\varphi_{h^l}(R) = R\varphi_{h^r}(L)$ знания последовательности элементов, использованных удаленной стороной, не требует.

Литература

1. *Габидулин Э.М., Кшевецкий А.С., Колыбельников А.И.* Защита информации. М.: МФТИ, 2011.
2. *Diffie W., Hellman M.E.*, New Directions in Cryptography // IEEE Transactions on Information Theory 1976, IT-22, P. 644.
3. *Milne J.S.* Group theory. 2011. www.jminline.org/matn
4. *Hankerson D., Menezes A., Vanstone S.A.* Guide to Elliptic Curve Cryptography. Springer-Verlag, 2004.
5. *Kahrobaei D., Koupparis C., Shpilrain V.* Public key exchange using matrices over group rings // Groups, Complexity, Cryptology. 2013. V. 5. P. 97.

References

1. *Gabidulun E.M., Kshevetcky A.C., Kolybelnikov A.I.* Protection of Information. M.: MIPT. 2011.
2. *Diffie W., Hellman M.E.*, New Directions in Cryptography. IEEE Transactions on Information Theory 1976, IT-22, P. 644.
3. *Milne J.S.* Group theory. 2011. www.jminline.org/matn
4. *Hankerson D., Menezes A., Vanstone S.A.* Guide to Elliptic Curve Cryptography. Springer-Verlag. 2004.
5. *Kahrobaei D., Koupparis C., Shpilrain V.* Public key exchange using matrices over group rings. Groups, Complexity. Cryptology. 2013. V. 5. P. 97.

Поступила в редакцию 18.11.2016