Исследование принципов применения неассоциативных алгебраических структур при синтезе асимметричных криптографических механизмов

Глухов М.М., Карюк Н.А., Катышев С.Ю.

Петрозаводск, 4 июня 2024 г.

Содержание

Алгоритм Диффи-Хеллмана (1976)

Пусть $(G, \cdot)$ – конечная группа, $g \in G$ – элемент большого порядка

1. Абонент A выбирает секретный ключ k_A и направляет абоненту B:

$$g^{k_A}.$$

2. Абонент B выбирает секретный ключ k_B и направляет абоненту A:

$$g^{k_B}.$$

3. Абоненты устанавливают общий секретный ключ из равенства:

$$(g^{k_A})^{k_B} = (g^{k_B})^{k_A}.$$

Стойкость основана на *проблеме дискретного логарифмирования*:

$$g^x = h.$$

Проблема дискретного логарифмирования

$$g^x = h.$$

1. Алгоритм Сильвера-Полига-Хеллмана для произвольной группы – «экспоненциальная трудоемкость».

Проблема дискретного логарифмирования

$$g^x = h.$$

1. Алгоритм Сильвера-Полига-Хеллмана для произвольной группы – «экспоненциальная трудоемкость».
2. Методы решета для мультипликативной группы конечного поля – «субэкспоненциальная трудоемкость».

Проблема дискретного логарифмирования

$$g^x = h.$$

1. Алгоритм Сильвера-Полига-Хеллмана для произвольной группы – «экспоненциальная трудоемкость».
2. Методы решета для мультипликативной группы конечного поля – «субэкспоненциальная трудоемкость».
3. MOV-атака для некоторых групп точек эллиптической кривой – «субэкспоненциальная трудоемкость».

Проблема дискретного логарифмирования

$$g^x = h.$$

1. Алгоритм Сильвера-Полига-Хеллмана для произвольной группы – «экспоненциальная трудоемкость».
2. Методы решета для мультипликативной группы конечного поля – «субэкспоненциальная трудоемкость».
3. MOV-атака для некоторых групп точек эллиптической кривой – «субэкспоненциальная трудоемкость».
4. Алгоритм Шора (использование квантового вычислителя) для произвольной абелевой группы – «полиномиальная трудоемкость».

Обобщенная схема выработки общего ключа

Пусть $(G, *)$ – конечный группоид, $\mathcal{L}_A$, $\mathcal{L}_B$ – некоторые поэлементно перестановочные подмножества его эндоморфизмов (преобразований), $g \in G$.

1. Абонент A выбирает секретный ключ $\rho_A \in \mathcal{L}_A$ и направляет B:

$$g^{\rho_A}.$$

2. Абонент B выбирает секретный ключ $\rho_B \in \mathcal{L}_B$ и направляет A:

$$g^{\rho_B}.$$

3. Абоненты устанавливают общий секретный ключ из равенства:

$$(g^{\rho_A})^{\rho_B} = (g^{\rho_B})^{\rho_A}.$$

Общая схема алгоритма шифрования с открытым ключом

Пусть $(G, *)$ – конечный группоид, $\mathcal{L}_A$, $\mathcal{L}_B$ – некоторые поэлементно перестановочные подмножества его эндоморфизмов, $g \in G$ – обратимый.

1. Абонент A выбирает секретный ключ $\rho_A \in \mathcal{L}_A$ и формирует:

$$k_A = g^{\rho_A}.$$

2. Для зашифрования $m \in G$ абонент B выбирает $\rho_B \in \mathcal{L}_B$ и вычисляет:

$$c = (c_1, c_2) = ((g)^{\rho_B}, m * (k_A)^{\rho_B}).$$

3. Для расшифрования c абонент A вычисляет:

$$m = c_2/(c_1)^{\rho_A}.$$

Некоторые другие механизмы

Пусть $(G, *)$ – конечный группоид, $\mathcal{L}_A$, $\mathcal{L}_B$ – некоторые поэлементно перестановочные подмножества его эндоморфизмов, $g \in G$ – обратимый.

Хеш-функция

Вычислим для секретного $\rho \in \mathcal{L}_A$ элемент $h = g^\rho$. Пусть каждому элементу x кольца вычетов соответствует эндоморфизм ρ_x из $\mathcal{L}_B$, тогда:

$$h(x_1, x_2) = g^{\rho_{x_1}} * h^{\rho_{x_2}}.$$

Другие механизмы

Защищенная передача ключа, Выработка общего секретного ключа между несколькими пользователями, Схема цифровой подписи типа Эль-Гамаля...

Требования к группоиду и множествам эндоморфизмов

1. Существование достаточно больших классов поэлементно перестановочных подмножеств эндоморфизмов $\mathcal{L}_A$, $\mathcal{L}_B$ группоида G, таких что:

$$|\mathcal{L}_A(g)| \approx |\mathcal{L}_B(g)| \approx |G|.$$

2. Эффективность вычисления значения эндоморфизма $\rho \in \mathcal{L}_A$ ($\rho \in \mathcal{L}_B$) на элементе g:

$$g \to g^\rho.$$

3. Трудноразрешимость «задачи дискретного логарифмирования», или нахождения неизвестного $\rho \in \mathcal{L}_A$ ($\rho \in \mathcal{L}_B$) для некоторых $g, h \in G$ из уравнения:

$$g^\rho = h.$$

4. Некоторые другие требования для реализации цифровой подписи.

Выбор алгебраической структуры

Внимание на следующие аспекты:

1. выбор алгоритмически трудноразрешимой задачи, на которой будет основываться стойкость протокола;
2. выбор алгебраической структуры, обеспечивающей необходимый размер задачи, а также требуемые криптографические свойства;
3. выбор способа представления алгебраической структуры, обеспечивающей с одной стороны эффективную реализацию протокола, а с другой не приводящей к снижению его трудоемкости.

Содержание

Поиск подходящих группоидов. Некоммутативные группы

1. Сопряжение:
$$g^{\rho_x} = x^{-1}gx.$$

Поиск подходящих группоидов. Некоммутативные группы

1. Сопряжение:

$$g^{\rho_x} = x^{-1}gx.$$

Ko K., Lee S., Cheo J. и другие
Группы кос Артина

Поиск подходящих группоидов. Некоммутативные группы

1. Сопряжение:
$$g^{\rho_x} = x^{-1}gx.$$
2. Двухстороннее домножение:
$$g^{\rho_{x_1,x_2}} = x_1 g x_2.$$

Поиск подходящих группоидов. Некоммутативные группы

1. Сопряжение:
$$g^{\rho_x} = x^{-1}gx.$$
2. Двухстороннее домножение:
$$g^{\rho_{x_1,x_2}} = x_1 g x_2.$$

Джинджихадзе М., Мегрелишвили Р., Сидельников В., Черепнев М., Ященко В., Alvarez R., Eftekhari M., Hurley T., Kahrobaei D., Myasnikov A., Shpilrain V., Romanczuk U. and Ustimenko V., Ushakov A., Stickel E., ...

Группа Томпсона, группа кос Артина, матрицы над полем, арифметические пространства, матрицы над некоммутативными кольцами, матрицы над групповыми кольцами...

Поиск подходящих группоидов. Некоммутативные группы

1. Сопряжение:
$$g^{\rho_x} = x^{-1}gx.$$
2. Двухстороннее домножение:
$$g^{\rho_{x_1,x_2}} = x_1 g x_2.$$
3. Композиция сопряжения и возведения в степень:
$$g^{\rho_{x,k}} = x^{-1}g^k x.$$

Поиск подходящих группоидов. Некоммутативные группы

1. Сопряжение:
$$g^{\rho_x} = x^{-1}gx.$$
2. Двухстороннее домножение:
$$g^{\rho_{x_1,x_2}} = x_1 g x_2.$$
3. Композиция сопряжения и возведения в степень:
$$g^{\rho_{x,k}} = x^{-1}g^k x.$$

Kahrobaei D. and Khan B., Lee S., Cheon J., Han J., Kang J., Koo K., Park C., Yamamura A., Молдовян Н., Молдовян Д., Молдовян А., ...
Группа кос Артина, матричные группы

Поиск подходящих группоидов. Некоммутативные группы

1. Сопряжение:
$$g^{\rho_x} = x^{-1}gx.$$
2. Двухстороннее домножение:
$$g^{\rho_{x_1,x_2}} = x_1 g x_2.$$
3. Композиция сопряжения и возведения в степень:
$$g^{\rho_{x,k}} = x^{-1}g^k x.$$
4. Применение внутренних автоморфизмов:
$$g^{\rho_k} = \rho_k(g).$$

Поиск подходящих группоидов. Некоммутативные группы

1. Сопряжение:
$$g^{\rho_x} = x^{-1}gx.$$
2. Двухстороннее домножение:
$$g^{\rho_{x_1,x_2}} = x_1 g x_2.$$
3. Композиция сопряжения и возведения в степень:
$$g^{\rho_{x,k}} = x^{-1}g^k x.$$
4. Применение внутренних автоморфизмов:
$$g^{\rho_k} = \rho_k(g).$$

Grigoriev D., Shpilrain V., Mahalanobis A., Paeng S., Ha K., Rososhek S., Ерофеев С., Романьков В., Молдовяны Н. и Д., ...

Группы движения, некоммутативные нильпотентные группы, полупрямые произведения групп преобразований

Поиск подходящих группоидов. Некоммутативные группы

1. Сопряжение:
$$g^{\rho_x} = x^{-1}gx.$$
2. Двухстороннее домножение:
$$g^{\rho_{x_1,x_2}} = x_1 g x_2.$$
3. Композиция сопряжения и возведения в степень:
$$g^{\rho_{x,k}} = x^{-1}g^k x.$$
4. Применение внутренних автоморфизмов:
$$g^{\rho_k} = \rho_k(g).$$

Результаты по анализу – Глухов М., Нечаев А., Tobias C. , Романьков В., Tsaban B., Shpilrain V., Ushakov A. и др.

Поиск подходящих группоидов. Участники NIST PQ

HK-17

Pedro Hecht and Jorge Alejandro Kamlofsky представили схему выработки общего секретного ключа на кватернионах (октанионах), основанную на двустороннем умножении.

WalnutDSA

Iris Anshel, Derek Atkins, Dorian Goldfeld, and Paul E. Gunnells представили схему цифровой подписи на группе кос Артина, основанную на двустороннем умножении.

Ни одна из схем не прошла во второй этап.

Поиск подходящих группоидов. Полукольца и полуполя

Полукольцом называют алгебраическую структуру $(A, +, \cdot)$, если
– $(A, +)$ – коммутативная полугруппа с нулем,
– $(A, \cdot)$ – полугруппа с единицей,
– выполнены левая и правая дистрибутивность.

Durcheva M., Grigoriev D., Shpilrain V., Huang H.,...
Двухстороннее домножение в полукольце матриц над полукольцом:

$$g^{\rho_{x_1,x_2}} = x_1 g x_2.$$

Результаты по анализу – Браун, Коблиц и др.

Содержание

Поиск подходящих группоидов. Квазигруппы

Квазигруппой называют группоид $(G, *)$, в котором каждое из уравнений

$$x * a = b, \qquad a * x = b,$$

имеет единственное решение.

❶ Возведение в правую (принципиальную) степень:

$$g^{[n]} = (\dots((g * g) * g) * \dots) * g.$$

❷ Двухстороннее возведение в степень:

$${}^{[k]}(g^{[n]}) = g^{[n]} * (\cdots * (g^{[n]} * (g^{[n]} * g^{[n]})) * \dots).$$

❸ Возведение в произвольную степень (скобки произвольно):

$$g^A = g^{A(n)} = g * g * \cdots * g.$$

Квазигруппы. Задача дискретного логарифмирования

Стойкость механизмов будет основываться на следующих проблемах.

Задача правого дискретного логарифмирования

$$g^{[x]} = h.$$

Задача лево-правого дискретного логарифмирования

$$^{[x]}g^{[y]} = h.$$

Задача обобщенного дискретного логарифмирования

$$g^{X} = h.$$

В условиях, что решения существуют.

Поиск подходящих группоидов. Медиальные квазигруппы

Необходимое условие – перестановочность степеней:

$$(g^{[n]})^{[k]} = (g^{[k]})^{[n]}, \quad (g^A)^B = (g^B)^A.$$

Теорема (Murdoch, 1939)

Если квазигруппа $(G, *)$ *обладает тождеством медиальности*

$$(x * u) * (v * y) = (x * v) * (u * y),$$

то для любых $g, h \in G$ *и обобщенных степеней* A, B *выполнено*

$$(g * h)^A = g^A * h^A, \qquad (g^A)^B = (g^B)^A.$$

Позднее независимо от Мердоча частные случаи этого результата получены в работах Барышникова, Нечаева, Катышева, Кахробая, Шпилрайна.

Медиальные квазигруппы. Использование

Теорема (Toyoda, 1941)

Если квазигруппа $(G, *)$ *обладает тождеством медиальности, то:*

$$\forall g, h \in G: \ g * h = g^{\sigma} \cdot h^{\tau} \cdot c,$$

где $(G, \cdot)$ *– абелева группа,* σ, τ *– перестанов. автоморфизмы* $(G, \cdot)$, $c \in G$.

Использование при построении схем распределение ключей

- В. Марков, А. Нечаев, 2006, при $h = e$, σ, τ – степени;
- С. Катышев, В. Марков, А. Нечаев, 2011, при $h = e$;
- M. Habeeb, D. Kahrobaei and V. Shpilrain, 2013, при $h = e$, $\tau = \varepsilon$;
- А. Барышников, С. Катышев, 2017, общий случай;
- D. Gligoroski, 2021, общий случай.

Медиальные квазигруппы. Алгебраические носители

Рассматривались (локально-) медиальные квазигруппы построенные на следующих структурах:

1. Циклические группы
   (В. Марков, А. Нечаев, 2006)
2. Матрицы над групповыми кольцами
   (M. Habeeb, D. Kahrobaei and V. Shpilrain, 2013);
3. Суперсингулярные эллиптические кривые
   (С. Катышев, В. Марков, А. Нечаев, 2014)
4. Гиперэллиптические кривые
   (А. Барышников, С. Катышев, 2017)
5. Прямое произведение групп
   (D. Gligoroski, 2021)

Медиальные квазигруппы. Дискретное логарифмирование

$$g^{[x]} = h.$$

1. Алгоритмы согласования и сведения к примарным квазигруппам – «экспоненциальная трудоемкость».
2. Модификация алгоритма Шора (квантовый вычислитель) – «полиномиальная трудоемкость».

$$g^{X} = h.$$

1. Получены оценки трудоемкости применения метода Хеллмана – «экспоненциальная трудоемкость».
2. Построены алгоритмы решения в частных случаях – «субэкспоненциальная трудоемкость».
3. Обоснована необходимость большего числа квантовых элементов, в т.ч. для медиальных квазигрупп на гиперэллиптических кривых.

Медиальные квазигруппы. Стойкость механизмов

Теорема (Lorenz Panny, 2021)

Для произвольной степени A элемента g в медиальном группоиде $(Q, *)$ $\exists \gamma \in \mathbb{Z}[\sigma, \tau]$:

$$g^A = g \cdot (g^{\sigma+\tau-\varepsilon} \cdot c)^\gamma.$$

Причем, если равенство выполнено для некоторого $x = g \in Q$, то оно выполнено и при любом $x \in < g >_*$.

1. Получено и опубликовано в частных случаях до 2021 г.
2. С использованием теоремы показано, что стойкость механизмов не превышает трудоемкости нахождения γ. На этом построен метод имитирующего отображения.
3. Позволяет свести всех механизмов к логарифмированию в группе (квантовый вычислитель) – «полиномиальная трудоемкость».

Содержание

Обобщенная схема выработки общего ключа

Пусть $(G, *)$ – конечный группоид, $\mathcal{L}_A$, $\mathcal{L}_B$ – некоторые поэлементно перестановочные подмножества его преобразований. $g \in G$.

1. Абонент A выбирает секрет $\rho_A \in \mathcal{L}_A$ и направляет абоненту B:

$$g^{\rho_A}.$$

2. Абонент B выбирает секрет $\rho_B \in \mathcal{L}_B$ и направляет абоненту A:

$$g^{\rho_B}.$$

3. Абоненты устанавливают общий секретный ключ из равенства:

$$(g^{\rho_B})^{\rho_A} = (g^{\rho_A})^{\rho_B}.$$

Новый подход к выработке общего ключа

Пусть $(G, *)$ – конечный группоид, $\mathcal{L}_A$, $\mathcal{L}_B$ – некоторые подмножества его преобразований.

1. Абонент A выбирает секрет $\rho_A \in \mathcal{L}_A$ и направляет абоненту B:

$$g^{\rho_A}.$$

2. Абонент B выбирает секрет $\rho_B \in \mathcal{L}_B$ и направляет абоненту A:

$$g^{\rho_B}.$$

3. Абоненты устанавливают общий секретный ключ из равенства:

$$(g^{\rho_B})^{\rho_A} = (g^{\rho_A})^{\overline{\rho_B}}.$$

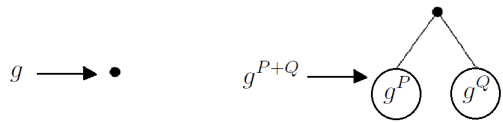
Степени элементов квазигруппы

Правая (принципиальная) степень:

$$g^1 = g, \quad g^n = g^{n-1} * g,$$

Произвольная обобщенная степень:

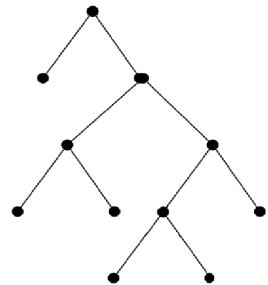
$$g^{P+Q} = g^P * g^Q, \quad g^{P \cdot n} = \left(g^P\right)^n.$$



Высота листа – расстояние до корня.
Высота дерева – максимум высот листов.

$A(n,h)$ – степень высоты h и n листами.

$g^{A(6,4)} = g^{1+(2+3)} = g * ((g * g) * ((g * g) * g))$.

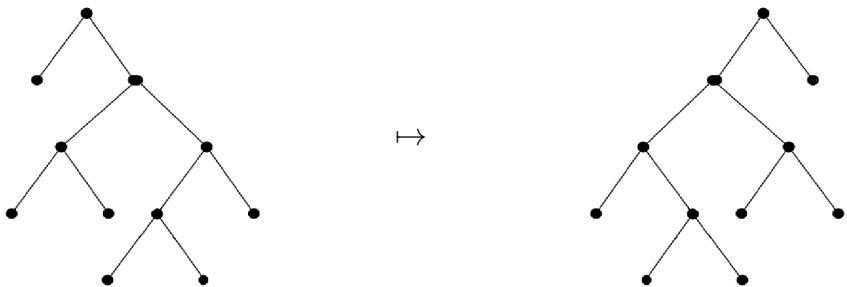


Симметричные степени элемента

Степень $g^{\overline{P}}$ элемента g *симметричную к степени* g^P определим:

$$g^1 = g, \quad g^{\overline{n}} = g * g^{\overline{n-1}}, \quad g^{\overline{P+Q}} = g^{\overline{Q}} * g^{\overline{P}}, \quad g^{\overline{P \cdot n}} = \left(g^{\overline{P}}\right)^{\overline{n}}$$

Например, тогда $g^{\overline{1+(2+3)}} = g^{(\overline{3}+\overline{2})+\overline{1}} = ((g * (g * g)) * (g * g)) * g.$



Свойство почти гомоморфности возведения в степень

Теорема

Если квазигруппа $(G, *)$ *обладает тождеством парамедиальности*

$$(x * u) * (v * y) = (y * u) * (v * x),$$

то для любых элементов $g, h \in G$ *и обобщенной степени* $A = A(n, k)$, *такой что все листы дерева степеней* $A(n, k)$ *имеют высоту одной четности, верно:*

$$(g * h)^{A(n,k)} = \begin{cases} h^{\overline{A(n,k)}} * g^{\overline{A(n,k)}}, & \text{если } k \text{ – нечетно}, \\ g^{\overline{A(n,k)}} * h^{\overline{A(n,k)}}, & \text{если } k \text{ – четно}. \end{cases}$$

Свойство почти перестановочности степеней

Теорема

Если квазигруппа $(G, *)$ *обладает тождеством парамедиальности*

$$(x * u) * (v * y) = (y * u) * (v * x),$$

то для любого элемента $g \in G$ *и любых степеней* $A(n,k)$ *и* $B(m,l)$*, таких что все их листы имею высоту одной четности, выполнено:*

$$\left(g^{A(n,k)}\right)^{B(m,l)} = \begin{cases} \left(g^{B(m,l)}\right)^{A(n,k)}, & \text{если } k \text{ и } l \text{ – четно,} \\ \left(g^{B(m,l)}\right)^{\overline{A(n,k)}}, & \text{если } k \text{ – четно и } l \text{ – нечетно,} \\ \left(g^{\overline{B(m,l)}}\right)^{A(n,k)}, & \text{если } k \text{ – нечетно и } l \text{ – четно,} \\ \left(g^{\overline{B(m,l)}}\right)^{\overline{A(n,k)}}, & \text{если } k, l \text{ – нечетно.} \end{cases}$$

Схема выработки общего секретного ключа

Пусть $(G, *)$ – парамедиальная квазигруппа.

1. Абонент A выбирает секрет $A(n, 2k+1)$ и направляет абоненту B:

$$g^{A(n,2k+1)}.$$

2. Абонент B выбирает секрет $B(m, 2l)$ и направляет абоненту A:

$$g^{B(m,2l)}.$$

3. Абоненты устанавливают общий секретный ключ из равенства:

$$(g^{B(m,2l)})^{A(n,2k+1)} = (g^{A(n,2k+1)})^{\overline{B(m,2l)}}.$$

Трудоемкость, стойкость, доля степеней, удовлетворяющих условию...

Линейные квазигруппы

Теорема (Kepka-Nemec, 1971)

Операция в любой парамедиальной квазигруппе может быть представлена в виде линейной квазигруппы:

$$\forall a, b \in G: \ a * b = a^{\sigma} \cdot b^{\tau} \cdot c,$$

где $(G, \cdot)$ *– абелева группа,* σ, τ *– автоморфизмы группы* $(G, \cdot)$.

Теорема (Обобщение результата Panny)

Для степени A *элемента в линейной квазигруппе* $(Q, *)$ $\exists \gamma \in \mathbb{Z}[\sigma, \tau]$:

$$g^A = g \cdot (g^{\sigma+\tau-\varepsilon} \cdot c)^{\gamma}.$$

Причем, если равенство выполнено для некоторого $x = g \in Q$, *то оно выполнено и при любом* $x \in < g >_*$.

Линейные квазигруппы. Стойкость механизмов

Теорема (Обобщение результата Panny)

Для степени A элемента в линейной квазигруппе $(Q, *)$ $\exists \gamma \in \mathbb{Z}[\sigma, \tau]$:

$$g^A = g \cdot (g^{\sigma+\tau-\varepsilon} \cdot c)^\gamma.$$

Причем, если равенство выполнено для некоторого $x = g \in Q$, то оно выполнено и при любом $x \in < g >_*$.

1. Стойкость механизмов не превышает трудоемкости нахождения γ.
2. Позволяет свести всех механизмов к логарифмированию в полугруппе (квантовый вычислитель) – «полиномиальная трудоемкость».
3. Позволяет свести всех механизмов к логарифмированию в полугруппе, но большего размера!