Построение криптосистемы в кольце эндоморфизмов бинарных последовательностей

Е.И. Коновалова[a], А.М. Саяпин[a]

[a] *Самарский национальный исследовательский университет им. академика С.П.Королева, 443086, Московское шоссе, 34 , Россия*

Аннотация

В работе изучается граф, вершинами которого являются бинарные последовательности (последовательности, состоящие из 0 и 1). На множестве бинарных последовательностей вводятся две структуры – структура графа и структура аддитивной группы с операцией сложения по модулю 2 (XOR). Рассматривая действие разностного оператора на бинарные последовательности, был построен алгоритм асимметричного шифрования, который является альтернативой существующим алгоритмам.

Ключевые слова: криптосистема; алгоритм асимметричного шифрования; кольцо эндоморфизмов; бинарные последовательности; граф бинарных последовательностей

1. Введение

В настоящее время широко распространены криптосистемы с открытым ключом, одной из которых является криптосистема Эль-Гамаля. Для построения криптосистемы Эль-Гамаля выбирается большое простое число p, выбирается целое число g, являющиеся первообразным корнем числа p, и выбирается случайное целое число x, $1 < x < p$. Далее вычисляется $y = g^x \bmod p$. Тогда открытым ключом системы является набор (y, g, p), а закрытым ключом – степень x. Стойкость криптосистемы держится на отсутствии эффективных полиномиальных алгоритмов нахождения x.

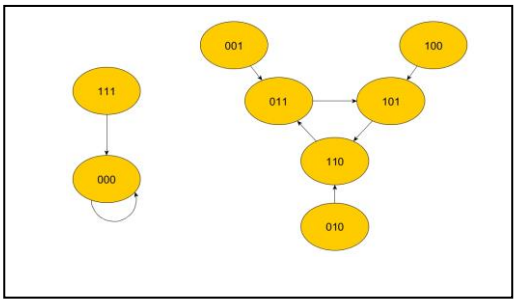
Эта задача внешне похожа на задачу нахождения эндоморфизма в некотором кольце K. Пусть φ - некоторый эндоморфизм кольца K, и пусть известно только его действие на множестве элементов $x_1, x_2 ... x_s$ кольца K. То есть предполагаем, что известно множество пар $(x_i, \varphi(x_i)), i = 1...s$. Требуется найти эндоморфизм φ' такой, что выполняются равенства $\varphi'(x_i) = \varphi(x_i), \forall i = 1...s$. Заметим, что эта задача является вычислительно сложной, поскольку в общем случае требует полного перебора всех эндоморфизмов кольца K.

С.К Росошеком в работе [3] была предложена базовая схема криптосистемы на произвольном групповом кольце. В настоящей работе некоторые идеи работы [3] были применены для построения криптосистемы на графе бинарных последовательностей.

2. Граф бинарных последовательностей

Рассмотрим множество последовательностей длины n, состоящих из 0 и 1: $x = (x_1, x_2, ... x_n)$, $x_i = (0,1)$. Множество S всех таких последовательностей конечно, его мощность равна 2^n. Определим оператор взятия разности $A: S \to S$, $Ax = y$, где x, y - бинарные последовательности длины n, по следующему правилу: $A(x_1, x_2, ..., x_n) = (|x_2 - x_1|, ..., |x_n - x_1|)$.

В 2005 году В.И. Арнольдом ([1]) было предложено представление всех бинарных последовательностей длины n в виде ориентированного графа, вершины которого есть все 2^n элементов множества S. При этом существует



единственная дуга из последовательности x в y если и только если $Ax = y$.

Рис. 1. Граф бинарных последовательностей.

На рис. 1 показан пример графа бинарных последовательностей для n=3, граф имеет 2^n=8 вершин, направление стрелок показывает действие оператора A. Данный граф имеет две компоненты связности, один цикл длины 3. В общем случае, для различных n существует произвольное число компонент связности, в каждой из которых есть единственный цикл. К каждому элементу цикла подвешено бинарное дерево размера $2^{g(n)}$, где функция $g(n)$ возвращает

максимальную степень числа 2, входящую в разложение *g(n)*. Все бинарные деревья между собой изоморфны. В краткой форме это можно записать $\Sigma_i \alpha_i(O_i * T_s)$, где t — число различных циклов, T_s - бинарное дерево размера s, O_{li} цикл длины li, α_i - число циклов равных li. Количество компонент связности $\Sigma_i \alpha_i$. Например, структура графа для n = 3 $(O_3 * T_2) + (O_1 * T_2)$.

Структура графа бинарных последовательностей подробно описана в работах А.И. Гарбера[5] и О.Н.Кропенкова [6]. В работе Э.Ю.Лернера[7] приведена таблица, в которой содержится структура графа при $n \le 300$. В работе А.М.Саяпина[4] был сформулирован и доказан критерий принадлежности последовательности циклу. Изучение структуры графа бинарных последовательностей является самостоятельным направлением исследования (в общем случае структура графа до сих пор не описана), однако авторов заинтересовала возможность использования этого графа в практических задачах. В работе [2] был предложен алгоритм асимметричного шифрования, основанный на графе бинарных последовательностей.

Авторы заметили, что предложенный подход имеет ряд общих черт с алгоритмом, рассмотренным С.К. Росошеком в работе [3]. При построении криптографических систем предлагается использовать структуру группового кольца KG, где K – кольцо, G - группа. Идея использования группового кольца заключается в том, что даже при небольших порядках группы и кольца, порядок группового кольца очень велик. Если порядок группы равен n, а порядок кольца равен k, то порядок группового кольца равен k^n.

Основная сложность реализации криптосистемы, предложенной С.К.Росошеком, заключается в отсутствии эффективных алгоритмов умножения в групповом кольце.

Применив подход С.К.Росошека к множеству бинарных последовательностей, авторы предлагают использовать следующий алгоритм шифрования.

3. Алгоритм асимметричного шифрования

Пусть S – множество бинарных последовательностей длины n. Множество S с операцией XOR (сложение по модулю два) образует коммутативную группу. Рассмотрим множество эндоморфизмов множества S: $\varphi : S \to S,\ \varphi(xXORy) = \varphi(x) XOR \varphi(y)$. Заметим, что оператор взятия разностей A, на основе которого был построен граф бинарных последовательностей, является эндоморфизмом.

Пусть φ - некоторый эндоморфизм группы бинарных последовательностей S, и пусть известно только его действие на множестве последовательностей $x_1, x_2 \ldots x_k$. То есть предполагаем, что известно множество пар $(x_i, \varphi(x_i)),\ i = 1 \ldots k$. Требуется найти эндоморфизм φ' такой, что выполняются равенства $\varphi'(x_i) = \varphi(x_i), \forall i = 1 \ldots k$. Заметим, что эта задача является вычислительно сложной, поскольку в общем случае требует полного перебора всех эндоморфизмов кольца K.

Определение. Множество всех эндоморфизмов, коммутирующих с оператором A, будем называть централизатором A: $C(A) = \{\varphi : \varphi A = A\varphi\}$.

Утверждение. Порядок централизатора оператора A равен 2^n: $|C(A)|=2^n$.

Доказательство.

Представим оператор A в виде матрицы, в которой первая строка имеет вид (1,1,0…0), все остальные строки получены последовательными циклическими перестановками первой строки.

Тогда задача о поиске коммутирующего оператора становится задачей о решении матричного уравнения $\varphi A - A\varphi = 0$, что равносильно решению системы n линейных однородных уравнений с n^2 неизвестными. Легко заметить, что эта система имеет n линейно независимых решений $\varphi_1, \varphi_2 \ldots \varphi_n$, тогда произвольное решение системы представлено в виде суммы: $\varphi = \Sigma c_i \varphi_i$, где коэффициенты c_i принимают значения 0 или 1. Таким образом, количество всех решений равно 2^n . Итак, порядок централизатора оператора A: $|C(A)|=2^n$. □

Заметим, что задача поиска эндормофизма, коммутирующего с оператором A, является вычислительно сложной. На решении этой задачи основан следующий алгоритм шифрования.

Пусть A и B - участники сеанса связи по открытому каналу.

1 этап. Создание открытого и закрытого ключа.

1 Выбирается длина последовательности n.

2 Выбираются k бинарных последовательностей длины n: $a_1, a_2, \ldots a_k$.

3 Выбираются эндоморфизмы $\varphi_1, \varphi_2, ... \varphi_k \in C(A)$, принадлежащие централизатору оператора A ($C(A)$).

4 Вычисляется значение $y = \varphi_1(a_1) XOR \varphi_2(a_2) XOR ... XOR \varphi_k(a_k)$.

5 Открытым ключом будет последовательность образующих $a_1, a_2, ..., a_k$ и контрольная сумма y, закрытым ключом набор эндоморфизмов $\varphi_1, \varphi_2, ... \varphi_k$.

2 этап. Шифрование сообщения участником B.

Участник B, чтобы отправить A сообщение M, поступает следующим образом. Сообщение M преобразуется в бинарную последовательность любым стандартном способом (например с использованием ASCII таблиц) в бинарную последовать. Полученная последовательность m дополняется незначащими нулями до достижения длины n.

1. Преобразует сообщение M в бинарную последовательность m, используя алгоритм, описанный выше.
2. Выбирает эндоморфизм $\psi \in C(A)$, принадлежащий централизатору оператора A.
3. Вычисляет $m XOR \psi(y)$ и $\psi(a_1^{-1})$, $\psi(a_2^{-1}), \ldots \psi(a_k^{-1})$.
4. Отправляет участнику A криптограмму: $c = (m XOR \psi(y), \psi(a_1^{-1}), ... \psi(a_k^{-1}))$.

3 этап. Дешифрование сообщения участником A.

Участник A вычисляет значение:

$$m = m XOR \psi(y) XOR \varphi_1\psi(a_1^{-1}) XOR \varphi_2\psi(a_2^{-1}) XOR ... XOR \varphi_k\psi(a_k^{-1})$$

В силу коммутативности операторов, это выражение равно m.

4. Возможные атаки

Так как передача данных происходит по открытому каналу, то необходимо рассмотреть возможные атаки злоумышленника:

1. Атака на участника A.
   Злоумышленник может попробовать на основе открытого ключа подобрать эндоморфизмы $\varphi_1, \varphi_2, ... \varphi_k \in C(A)$
   Отметим, что в таком случае злоумышленнику придется решать уравнение с неизвестными, $y = x_1 XOR\, x_2 XOR ... XOR\, x_k$ в общем случае которое имеет 2^n решений, что является вычислительной сложной задачей.]]
2. **Атака на участника B.**
   Злоумышленник может атаковать участника B в тот момент, когда участник B передает криптограмму c.
   Рассмотрим два вида атаки:
   a) Атака на $m XOR \psi(y)$:
      Чтобы расшифровать сообщение m в последовательности $m XOR \psi(y)$ злоумышленнику достаточно применить операцию XOR с последовательностью равной $\psi(y)$. Без дополнительных знаний об эндоморфизме ψ это означает полный перебор последовательностей длины n, что означает перебор всевозможных вариантов (2^n решений).
   b) Атака на $\psi(a_1^{-1}), ... \psi(a_k^{-1})$:
      Злоумышленник может попробовать решить уравнение $\psi(a) = b$ и по известным a и b.
      Заметим, что количество решений зависит от положения вершины a на бинарном дереве. Максимальное количество решений относительно ψ уравнение $\psi(a) = b$ имеет в случае, когда последовательность a принадлежит циклу, единственное решение в том случае, когда a является листом дерева. Количество решений для последовательностей на цикле в точности равно высоте бинарного дерева.

5. Выбор параметров алгоритма

Исходя из возможности атак, авторами рекомендуются следующие параметры:

1. Для параметра k, рекомендуемое значение $1 < k < 10$.
2. Параметр n зависит от длины сообщения m, поэтому, в общем случае, нельзя указать явное значение для n. Отметим, что для алгоритма важен размер бинарных деревьев, чем больше размер дерева, тем лучше криптостойкость. Согласно этому, нужно максимизировать функцию $g(n)$. Хорошими значениями будут n = 192, 384, 768 и т.п.

3. Выбор эндоморфизмов происходит исходя из соображений сложности взлома. В общем случае нельзя указать конкретные эндоморфизмы, поэтому существуют простые правил для их выбора:
    a) Любые выбранные эндоморфизмы не должны переводить последовательность *a* в нулевую.
    b) Участнику А необходимо выбирать разные эндоморфизмы.

6. Заключение

В ходе исследования были получены следующие результаты:

1. проанализирована структура оператора А и его матричного представления;
2. получен способ построения эндоморфизмов, коммутирующих с оператором А и приведена точная оценка их количества;
3. разработан алгоритм построения криптосистемы в кольце эндоморфизмов, действующих на множестве бинарных последовательностей.

Литература

[1] Арнольд, В.И. Экспериментальное наблюдение математических фактов / В.И. Арнольд – М.:МЦНМО, -2006. – 120 с.

[2] Коновалова, Е.И. Алгоритм асимметричного шифрования на основе бинарных последовательностей / Е.И.Коновалова, А.М.Саяпин // Информационные технологии и нанотехнологии Материалы Международной конференции и молодежной школы. Федеральное государственное автономное образовательное учреждение высшего образования «Самарский государственный аэрокосмический университет имени академика С.П. Королева (Национальный исследовательский университет)».- 2015.- С. 263-265.

[3] Росошек, С.К. Криптосистемы в группах автоморфизмов групповых колец абелевых групп / С.К.Росошек // Фундамент. и прикл. матем.- 2007. Т 13, № 3.-С. 157–164.

[4] Саяпин, А.М. Сложность бинарных последовательностей/ А.М.Саяпин // Вестник СМУиС – 2013.-Т 2, №1.- С62-65.

[5] Garber, A.I. Graphs of difference operators for p-ary sequences/ A.I.Garber // Funct. Anal. and Other Math.- 2006.- Vol.1(2).- P. 179-195.

[6] Karpenkov, O.N. On examples of difference operators for {0,1}- valued functions over finite sets/ O.N.Karpenkov // Funct. Anal. and Other Math.- 2006.- Vol.1(2).- P. 175–180.

[7] Lerner, E.Yu. Tables of graphs of binary and ternary sequences differentiation.[Electronic resource].- Access mode: http://arxiv.org/abs/0704.2947v1.