Анализ параметров динамической схемы распределения ключей Блома

Сейед Пурья Захраи

***Аннотация*—В работе рассматриваются матричные схемы предварительного распределения ключей, построены на основе схемы Блома. Такие схемы используются, в частности, в беспроводных сенсорных сетях и позволяют эффективно менять секретные ключевые параметры доверенного центра (ДЦ) при компрометации ключей отдельных участников протокола.**

В работе представлена модернизированная матричная схема Блома. Предполагается, что ДЦ выбирает матрицу P размера N × N над конечным полем GF(q), где N-размер сети и q>N. Затем в зависимости от значения параметра безопасности t в качестве открытой матрицы берутся первые t+1 строк матрицы P. Матрица P является публичной, и предполагается, что любая система из t+1 столбцов этой матрице линейно независима. Кроме того предполагается, что ДЦ генерирует случайную (t+1)×(t+1) симметричную секретную матрицу S над GF(q), $S = X * X^T$, X - случайная матрица размера (t+1) × (t+1), и вычисляет матрицу $A = (S.P)^T$.

Если узлам i и j нужно устанавливать общий ключ, они сначала обмениваются столбцами из матрицы P и затем вычисляют K_{ij} и K_{ji}, соответственно, используя секретные строки матрицы A.

Подсчитана вероятность совпадения ключей у разных пар участников.

На основе программной реализации представлены результаты вычислительных экспериментов. В частности, экспериментально установлена зависимость вероятности совпадения ключей двух участников от параметров протокола (размер поля и число участников). Для q=1009 получено число совпадений ключей для разных значений N. Также получены результаты для значений N в предположении, что максимум совпадений должно быть равно 5.

***Ключевые слова*— схема Блома, доверенный центр (ДЦ), модель Блома, модифицированная схема Блома, атака, вероятность совпадения ключей.**

I. Введение

Большинство криптографических протоколов требуют проведения предварительного распределения секретных ключей. Для предварительного распределения стороны могут обменяться ключами при личной встрече, либо поручить доставку ключей специально назначенному доверенному курьеру, либо использовать для передачи некоторый выделенный защищенный канал. В зависимости от назначения криптографической системы иногда оказывается удобным распределять не сами ключи, а некоторые вспомогательные ключевые материалы, на основании которых каждый участник или группа участников могут самостоятельно вычислить необходимый ключ, используя для этого некоторую установленную заранее процедуру.

Если число участников сети засекреченной связи невелико, то и число распределяемых ключей также невелико. Для больших же сетей распределение ключей становится очень серьезной проблемой. Она заключается в том, что для сети, в которой работают n участников, необходимо выработать заранее и хранить в дальнейшем n(n-1)/2 ключей. Кроме того, каждому участнику сети необходимо передать ключи для связи с остальными (n-1) участниками, которые участник должен постоянно хранить. Например, для сети со 100 участниками нужно сгенерировать и хранить почти 5000 ключей, причем каждый участник при этом должен хранить у себя 99 ключей.

Для уменьшения объема хранимой ключевой информации применяются различные схемы предварительного распределения ключей в сети связи. Их суть заключается в том, что в действительности вначале происходит распределение не самих ключей, а некоторых вспомогательных ключевых материалов, занимающих меньшие объемы. На основании этих материалов каждый участник может самостоятельно вычислить по некоторому алгоритму необходимый для связи ключ. Такой подход позволяет уменьшить объемы как хранимой, так и распределяемой секретной информации.

Впервые эта проблема рассмотрена в работе Блома [4].

Модифицированные схемы Блома рассматривались в работах [1], [2].

II. Модель Блома

Классическая схема Блома.

Выберем поле F, имеющее конечное, но достаточно большое число элементов, и зафиксируем n различных элементов $r_1, \dots, r_N \in F$, отличных от нуля. Каждый элемент r_i припишем i-му участнику сети, i=1,...,N. Эти элементы не являются секретными и могут храниться на общедоступном сервере сети. Выберем симметрический

Статья получена 27 апреля 2018.
Сейед Пурья Захраи Московский Государственный Университет имени М.В. Ломоносова (zpouria@gmail.com)

$a_{ij} = a_{ji} = q - 1 = -1 (mod\ q)$ $a_{ij} = a_{ji} = 0$

многочлен над полем F степени 2t, $1 \le t < N$, вида

$$f(x,y) = \sum_{i=0}^{t} \sum_{j=0}^{t} a_{ij}\, x^i y^j$$

где $a_{ij} = a_{ji}, i \ne j,\ i,j = 0,\dots,t$. Его коэффициенты являются секретными и должны храниться только в центре распределения ключей. Коэффициенты многочлена $f(x,y)$ задают секретную матрицу S. Каждый участник A_i получает в качестве ключевых материалов набор $(a_{0_i}, a_{1_i}, \dots, a_{t_i})$, состоящий из коэффициентов многочленов

$$g_i(x) = f(x, r_i) = a_{0_i} + a_{1_i} x + \dots + a_{t_i} x^t$$

Для связи между участниками A_i и A_j теперь можно использовать общий ключ k_{ij} :

$$k_{ij} = k_{ji} = f(r_i, r_j) = g_j(r_i) = g_i(r_j)$$

который могут легко вычислить оба участника.

При использовании данной схемы каждый участник должен хранить t+1 секретных значений вместо N-1, общее же число секретных коэффициентов многочлена f равно t(t+1)/2.

В [4] доказано, что если злоумышленнику известны секретные ключи m участников ($m \le t$), то он не сможет определить секретные ключи любого другого из оставшихся участников протокола. Параметр t называется параметром безопасности, $t \ll N$.

Эта безопасность достигает за счет того, что любые t+1 столбцов матрицы P:

$$P = \begin{bmatrix} 1 & 1 & 1 & \cdots & 1 \\ r_1 & r_2 & r_3 & \cdots & r_N \\ r_1^2 & r_2^2 & r_3^2 & \cdots & r_N^2 \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ r_1^t & r_2^t & r_3^t & \cdots & r_N^t \end{bmatrix}$$

линейно независимы, при условии $r_i \ne r_j, i \ne j$.

Эти столбцы образуют матрицу Вандермонда.

III. Модифицированная схема Блома

Теперь рассмотрим некоторые модифицированные схемы Блома.

Как было сказано ранее, схема Блома использует матрицу Вандермонда, которая является публичной матрицей, и эта матрица отвечает за все вычисления при генерировании ключей. Все элементы этой матрицы должны быть выбраны так, чтобы любые (t + 1) столбцы P (публичная матрица) были линейно независимы, чтобы генерировать уникальные ключи. Но когда значение t увеличивается до больших значений, количество строк публичной матрицы увеличивается, и это потребует значительного увеличения памяти (для хранения ключей и секретной матрицы) и энергопотребления.

A. Для ускорения вычисления и уменьшения памяти в схеме Блома вместо “матрицы Вандермонда” (P) можно использовать матрицу смежности в качестве публичной матрицы. Матрица смежности представляет собой квадратную (1,0) матрицу, и это уменьшает сложность вычисления ключей участников (узлов) протокола.

Матрица a_{ij} смежности по модулю q (q простое, q > N) формируется следующим образом:

Если узлы i и j связаны, то $a_{ij} = a_{ji} = 1$; в противном случае (либо)

Процедура вычисления ключей

1. Формирование матрицы P.
   - 1.1. Выбираем поле $\mathbb{Z}_q$, $q > N$ (N- число узлов сети).
   - 1.2. Формируется матрица смежности Q размера $N \times N$ как описано выше.
   - 1.3. Матрица P состоит из первых $(t+1)$ строк матрицы Q. Столбец P_i матрицы – это открытый ключ для i-ого узла.
2. Формирование ключевого пространства.
   - 2.1. Доверенный центр (ДЦ) генерирует m случайных симметрических матриц $S_1,\dots,S_m$ размера $(t+1) \times (t+1)$.
   - 2.2. Если $S_i = S$ (матрица S_i заменяется матрицей S_j при компрометации сети), то вычисляется секретная матрица $A = (S.P)^T = P^T.S^T = P^T.S$, где T – операция транспонирования матрицы. Матрица A состоит из N строк и (t+1) столбцов.
     Строка A_i матрицы A – это секретный ключ i-ого узла.
   - 2.3. Вычисление секретного ключа k_{ij} из 2.1 и 2.2 следует, что
     $K_{ij} = K_{ji} = (A_i.P_j) = (A_j.P_i)$
     Ключ $K_{ij}(K_{ji})$ — это скалярное произведение вектор-строк A_i и P_j (A_j и P_i).

B. Теперь рассмотрим другую модифицированную схему Блома.

Процедура вычисления общего ключа:

1. ДЦ выбирает секретную матрицу P размера $(t+1) \times (t+1)$. Эта матрица является публичной.
2. ДЦ генерирует секретную симметричную матрицу S размера $(t+1) \times (t+1)$.
   Матрицу S можно генерировать в виде $X.X^T$, где X-секретная случайная матрица. Очевидно, что $S^T = S$.
3. Матрица $A = (S.P)^T = P^T.S$
4. Вычисление общего секретного ключа так же, как в пункте A.

C. Назначение уникального идентификатора.

ДЦ присваивает идентификатор для каждого узла сети, который является общедоступным для всей сети, до вычисления публичных и секретных матриц. Как только узел получает свой уникальный идентификатор, он информирует ДЦ.

Возникает проблема, что, если злоумышленник уже находится в сети до того, как ему будет присвоен идентификатор, то его уже будет невозможно отличить от доверяемого узла.

По этой причине предполагается, что каждый узел проходит проверку подлинности для данной сети, прежде чем он будет добавлен в эту сеть. Аутентификация проходит следующем образом.

1. ДЦ запрашивает идентификатор сети и идентификатор узла, выданные ДЦ.
2. Узел посылает ДЦ значение идентификатора.
3. ДЦ проверяет идентификатор и аутентифицирует узел.
4. ДЦ выдает новый идентификатор узлу и снова запрашивает старый идентификатор сети.
5. Узел отправляет ДЦ идентификатор сети.

6. ДЦ проверяет, что узел не скомпрометирован, и на этом процесс завершается.

Теперь предположим, что два узла хотят общаться друг с другом. Требуется получить секретный ключ от ДЦ, чтобы вычислить общий ключ. Для того чтобы получить ключ, после выполнения аутентификации выполняется следующая процедура:

1. Узел запрашивает секретный ключ.
2. ДЦ подтверждает запрос, запрашивая присвоенный новый идентификатор.
3. Узел отправляет ДЦ свой идентификатор.
4. ДЦ проверяет идентификатор узла и отправляет секретный ключ (по закрытому каналу).
5. Узел отправляет идентификатор.
6. ДЦ проверяет идентификатор, и процесс завершается.

ДЦ поддерживает следующие таблицы заражения для вредоносных узлов. Например:

ID (вредоносных узлов)	число вторжений
ВУ1	1
ВУ2	2

В любом из вышеперечисленных шагов, если ДЦ обнаружит какой-либо узел как нелегальный, он обновляет значения уникального идентификатора узла, и увеличивает число вторжении на 1, блокирует все сообщения в этом конкретном пути и рассылает его всем узлам в сети.

D. Динамические Секретные Матрицы:

Центр динамически обновляет секретную матрицу в каждом из следующих случаев:

- С каждым увеличением количества вторжений в таблице заражения.
- Предположим, что узел i хочет общаться с узлом j (i и j легальные узлы). Когда центр дает секретный ключ для обоих узлов, он обновляет секретную матрицу S для следующего запроса от узлов.

Центр выполняет через регулярные интервалы времени следующую процедуру аутентификации с целью выявления вредоносных узлов.

1. ДЦ запрашивает у узла идентификатор.
2. Узел подтверждает запрос, отправляя присвоенный идентификатор.
3. ДЦ проверяет соответствует ли полученный идентификатор данному узлу.
4. ДЦ обновляет идентификатор, отправляет узлу и запрашивает старый идентификатор.
5. Узел отправляет старый идентификатор, и ДЦ проверяет, что новый идентификатор отправил легальному узлу и процесс завершается.

После того, как ключ был установлен между узлами, узлы, прежде чем начать общаться друг с другом, проводят взаимную аутентификацию между узлами и центром.

Например рассмотрим вариант, когда узел U хочет общаться с узлом V:

1. U и V отправляют ДЦ свои ключи и идентификаторы.
2. ДЦ проверяет, чтобы значения ключей, отправленных от обеих сторон, были равны.
3. ДЦ снова запрашивает значение ключей U и V и после их получения от каждого узла проверяет, что они не скомпрометированы, и процесс завершается.

IV. АТАКИ

Предполагаем, что система состоит из узлов, принадлежащих одному ДЦ. Предполагается, что ДЦ имеет доступ к криптографическому безопасному генератору случайных чисел. Секретные ключи считаются защищенными. При необходимости их можно удалить после создания всех возможных наборов открытых и секретных ключей. Узлы имеют доступ к стойким криптографическим алгоритмам.

Будем считать, что злоумышленник обладает достаточными вычислительными ресурсами. Он может контролировать передачи, сообщения в сети и передавать свои секретные сообщения. Он также способен физически захватывать узлы и извлекать все материалы для ключей, включая идентификаторы открытых ключей, наборы секретных ключей и параметры ключей из памяти ROM и RAM.

Схема считается нарушенной, если злоумышленник способен:

- получить попарные ключи любых других пар нескомпрометированных узлов;
- создавать новые открытые и секретные ключи;
- вычислить секретные ключи ДЦ.

Атака Sybil

В этой атаке злоумышленник будет создавать новые открытые и секретные ключи с помощью скомпрометированных ключей и использовать их для маскировки легитимных узлов. Предположим, что известны открытые и секретные ключи n узлов. Злоумышленник может изготовить новый открытый ключ P_x с помощью линейной комбинации захваченных открытых ключей следующим образом:

$$P_x = \alpha_1 P_1 + \cdots + \alpha_n P_n (mod\ q)$$

Соответствующий секретный ключ K_x также будет аналогичной линейной комбинацией скомпрометированных секретных ключей

$$K_x = P_x^T A = (\alpha_1 P_1^T + \cdots + \alpha_n P_n^T)A$$
$$= \alpha_1 P_1^T A + \cdots + \alpha_n P_n^T A$$
$$= \alpha_1 K_1 + \cdots + \alpha_n K_n (mod\ q)$$

Выбирая различные комбинации $\alpha_1, \ldots \alpha_n$, злоумышленник может изготовить любой открытый ключ и соответствующий секретный ключ.

Для противодействия этой атаке необходимо выполнить три условия:

- открытые ключи должны соответствовать предписанной структуре;
- открытые ключи линейно независимы;
- скомпрометировано не более t узлов т. е. n <t + 1.

Первое условие гарантирует, что ключ, сформированный из произвольных линейных комбинаций захваченных ключей, не будет принят. Если все открытые ключи имеют предписанную структуру, например, в столбце матрицы Вандермонда, то произвольные открытые ключи просто отбрасываются.

Предположим, что t узлов были скомпрометированы, и все открытые ключи линейно независимы. Злоумышленнику известны $P_1, \ldots, P_t$ ключи t узлов. Злоумышленник сможет построить систему от t линейных уравнений для каждого секретного ключа, используя отношение $K_i = P_i^T A$, которое после

транспонирования может быть записано как $A^T P_i = K_i^T$, где $A^T = A$ и вычислить:

$$A[P_1\ P_2 \dots P_t] = [K_1^T\ K_2^T \dots K_t^T]$$

$$\text{т.е } AP = K$$

$$\text{если } P \text{ обратимый, то } A = KP^{-1}$$

Если $\det P \neq 0$, то P – обратимая матрица. Следовательно, вектор-столбцы матрицы P должны быть линейно независимы. Элементы секретного ключа можно получить, например, с помощью метода исключения Гаусса.

V. Исследование модернизированной схемы

В отличие от схемы, рассмотренной в пункте В, будем предполагать, что ДЦ выбирает матрицу P размера N × N над конечным полем GF(q), где N-размер сети и q>N. Затем в зависимости от значения t (параметр безопасности) в качестве открытой матрицы берутся первые t + 1 строк матрицы P. Матрица P является публичной, и предполагается, что любая система из t + 1 столбцов этой матрице линейно независима. Кроме того, в отличие от схемы, рассмотренной в пункте А, будем предполагать, что ДЦ генерирует случайную (t+1) × (t+1) симметричную матрицу S (секретная матрица) над GF(q), $S = X * X^T$, X- случайная матрица размера (t+1) × (t+1), и вычисляет матрицу $A = (S.P)^T$,где $(S.P)^T$- Матрица S должна храниться в тайне. Так как S симметричная, то легко видеть, что $A.P = (S.P)^T.P = P^T.S^T.P = P^T.S.P = (A.P)^T$ то есть A·P является симметрической матрицей. Если мы положим K = A·P, то $K_{ij} = K_{ji}$, и будем использовать K_{ij} (или K_{ji}) как попарный секретный ключ между узлом i и узлом j. Рисунок 1 иллюстрирует, как вычисляются ключи $K_{ij} = K_{ji}$.

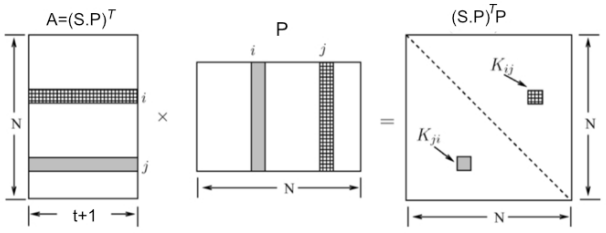

Рис. 1. Вычисление ключей

Если узлам i и j нужно устанавливать общий ключ, они сначала обмениваются столбцами из матрицы P и затем вычисляют K_{ij} и K_{ji}, соответственно, используя секретные строки матрицы A. Поскольку P является общедоступной, ее столбцы могут быть переданы по открытому каналу. В [4] показано, что вышеуказанная схема t-безопасная, если любые t + 1 столбцы P линейно независимы.

Пример:

Рассмотрим сеть с 5 узлами и следующими параметрами:

- Параметр безопасности t=3, q=31, означает, что если не более 3 узлов в сети взломаны, то невозможно найти ключи других пользователей.
- В качестве публичной матрицы выбирается случайная матрица P порядка (t+1) * (N) доверенным центром. В качестве P может быть взята любая случайная (3+1) * (5+1) матрица, например:

$$P = \begin{pmatrix} 29 & 4 & 0 & 18 & 21 & 5 \\ 25 & 10 & 30 & 17 & 8 & 28 \\ 8 & 27 & 10 & 9 & 19 & 21 \\ 19 & 17 & 8 & 20 & 5 & 17 \end{pmatrix}$$

- Секретная симметрическая матрица может быть получена следующим образом:

  Возьмем случайную матрицу,

$$X = \begin{pmatrix} 21 & 8 & 22 & 12 \\ 0 & 14 & 15 & 26 \\ 28 & 10 & 7 & 7 \\ 19 & 25 & 8 & 22 \end{pmatrix}$$

  Получаем секретную матрицу S как произведение матриц X и X^T,

$$S = \begin{pmatrix} 17 & 10 & 7 & 16 \\ 10 & 12 & 24 & 19 \\ 7 & 24 & 21 & 0 \\ 16 & 19 & 0 & 15 \end{pmatrix}$$

- Вычисляем матрицу A, используя соотношение:

  A =$(S.P)^T$mod (31)

$$A = \begin{pmatrix} 18 & 27 & 10 & 15 \\ 9 & 15 & 29 & 13 \\ 2 & 8 & 0 & 8 \\ 22 & 19 & 10 & 12 \\ 30 & 20 & 25 & 5 \\ 9 & 4 & 1 & 30 \end{pmatrix}$$

- Вычисляем ключи,

K[1,2]=$A_1 * P_2$=$\begin{pmatrix}18 & 27 & 10 & 15\end{pmatrix}\begin{pmatrix}4\\10\\27\\17\end{pmatrix}$= 30

K[2,1]=$A_2 * P_1$=$\begin{pmatrix}9 & 15 & 29 & 13\end{pmatrix}\begin{pmatrix}29\\25\\8\\19\end{pmatrix}$= 30

K [1,3]= K [3,1]=7
K [1,4]= K [4,1]=26
K [1,5]= K [5,1]=22
K [1,6]= K [6,1]=9
K [2,3]= K [3,2]=7
K [2,4]= K [4,2]=8
K [2,5]= K [5,2]=26
K [2,6]= K [6,2]=24
K [3,4]= K [4,3]=22
K [3,5]= K [5,3]=22
K [3,6]= K [6,3]=29
K [4,5]= K [5,4]=27
K [4,6]= K [6,4]=2
K [5,6]= K [6,5]=18

Заметим, что K [1,5] = K [3,4] = K [3,5].

VI. Проблема совпадения ключей

Оценим вероятность совпадения хотя бы двух секретных ключей при равномерном распределении f на множестве симметрических функций.

Пусть F - конечное поле, например $F = \mathbb{Z}_q \ni x, y$. Обозначим

$$f_1(x,y) = x.y\ ; f_2(x,y) = x + y$$

$$x_1y_1 + \cdots x_Ny_N$$

$$\varphi(x,y) = f_2(\dots f_2(f_1(x_1,x_1), f_1(x_2,x_2)), \dots, f_1(x_N,x_N))$$

$$M_q = \{f: F \times F \to \phi | f(x,y) = f(y,x)\}$$

Оценим вероятность того, что все парные секретные ключи для N участников различны, при равномерном распределении функции f на M_q. Пусть также случайный набор $r = (r_{1,\dots,}r_N)$ равномерно распределен на $X_{q,N} = \{(r_{1,\dots,}r_N)|r_i, r_j \in F, r_i \neq r_j, i \neq j\}$, причем f и r независимы. Заметим, что $|M_q| = q^{q(q+1)/2}$ и $|X_{q,N}| = \frac{q!}{(q-N)!}$. очевидно, что $q > N(N-1)/2$.

Для каждой пары индексов $(i,j): 1 \leq i \leq j \leq N$ рассмотрим случайную величину $\xi_{ij} = f(r_i, r_j)$. Зафиксируем некоторое подмножество $\{e_{ij}|1 \leq i \leq j \leq N\} \subset F$ элементов из $N(N-1)/2$ элементов. Вычислим

$$P\{\forall i,j: 1 \leq i < j \leq N\ \xi_{ij} = e_{ij}\} = \sum_{x=(x_1,\dots,x_N)\in X_{q,N}} P\{r = x, \forall i,j: 1 \leq i < j \leq N\ f(x_i,x_j) = e_{ij}\} = \sum_{x\in X_{q,N}} P\{r = x\}.P\{\forall i,j: 1 \leq i < j \leq N\ f(x_i,x_j) = e_{ij}\} = \sum_{x\in X_{q,N}} \frac{1}{|X_{q,N}|}\cdot\frac{1}{q^{N(N-1)/2}} = \frac{1}{q^{N(N-1)/2}}$$

Тогда вероятность того, что все ξ_{ij} различны, равна 1

$$P\{|\{\xi_{ij}|1 \leq i < j \leq N\}| = N(N-1)/2\} = \sum_{x=(x_1,\dots,x_{N(N-1)/2})\in X_{q,N(N-1)/2}} P\{\forall i,j: 1 \leq i < j \leq N\ \xi_{ij} = x_{i+(j-2)(j-1)/2}\} = \sum_{x\in X_{q,N(N-1)/2}} P\{\forall i,j: 1 \leq i < j \leq N\ \xi_{ij} = e_{ij}\} = \frac{q!}{(q-N(N-1)/2)!}.P\{\forall i,j: 1 \leq i < j \leq N\ \xi_{ij} = e_{ij}\}$$

$$= \frac{q(q-1).\cdots.(q-\frac{N(N-1)}{2}+1)}{q^{N(N-1)/2}} = 1 - \left(\sum_{k=1}^{\frac{N(N-1)}{2}-1} k\right).\frac{1}{q} + O\left(\frac{1}{q^2}\right) = 1 - \frac{\frac{N(N-1)}{2}\left(\frac{N(N-1)}{2}-1\right)}{2}.\frac{1}{q} + O\left(\frac{1}{q^2}\right), \text{при } q \to \infty.$$

таким образом справедливо утверждение:

Утверждение 1. Для модернизированной схемы Блома вероятность совпадения двух секретных ключей удовлетворяет соотношению:

$$P\{|\{\xi_{ij}|1 \leq i < j \leq N\}| = N(N-1)/2\} = 1 - \frac{\frac{N(N-1)}{2}\left(\frac{N(N-1)}{2}-1\right)}{2}.\frac{1}{q} + O\left(\frac{1}{q^2}\right), \text{при } q \to \infty.$$

Статистические эксперименты.

Подсчитаем вероятность совпадения ключей при различных параметрах: N - размер матрицы (N - число участников), q - мощность поля, P - вероятность совпадения ключей.

Для проведения экспериментов была программно реализована модернизированная схема Блома.

1) Здесь мы будем использовать то, что отображение

$\sigma: \{(i,j)|1 \leq i \leq j \leq n\} \to \left\{1,\dots,\frac{n(n-1)}{2}\right\}, \sigma(i,j) = i + (j-2)(j-1)/2$

является биекцией.

Результаты экспериментов для различных параметров N и q приведены в таблице 1.

Таблица 1. Результаты экспериментов

N	6	8	10	12
q	1009	1559	2003	2503
P	10.4%	24.24%	49.42%	85.69%

На рисунке 2 для q=1009 получено число совпадений ключей для разных значений N. Чтобы вычислить число совпадений ключей, применим алгоритм 1000 раз и подсчитаем сколько совпадений при каждом вычислении. Как видно на рисунке, число совпадений зависит от размера матрицы и поля. При увеличении размера матрицы, если мы возьмём фиксированное поле, число совпадении сильно увеличивается.

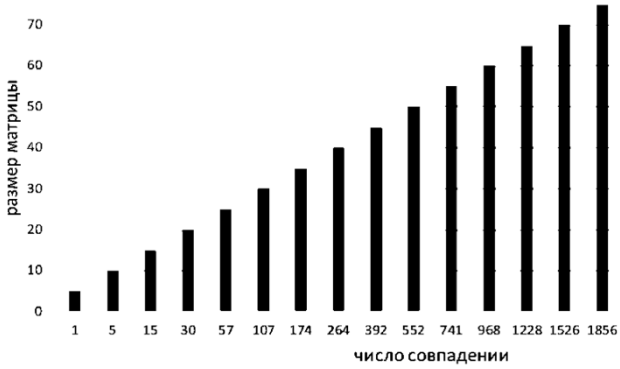

Рис 2. Число совпадений ключей для разных значений N

В следующем эксперименте мы предполагали, что у нас максимум совпадений равно 5. Результаты экспериментов показаны на рисунке 3.

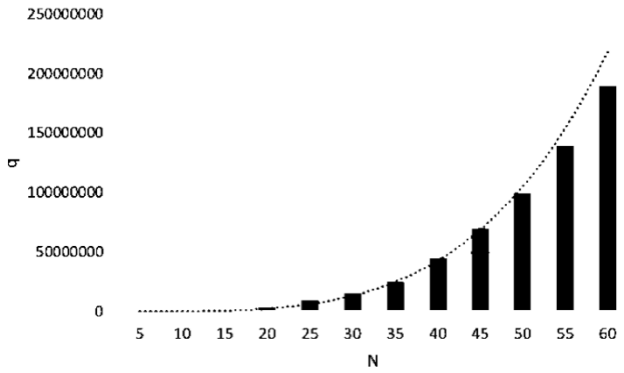

Рис 3. Значение N при максимуме 5 совпадений

На основе этих экспериментов оказалось, что параметры протокола q и N связаны следующим соотношением.

$$q = 16.039N^{4.0126}$$

VII. Заключение

В работе рассматриваются современные методы синтеза и анализа схем предварительного распределения секретных ключей для сенсорных сетей.

Предложена модернизированная схема Блома, и для этой схемы получена аналитическая оценка вероятности совпадения ключей.

Проведены эксперименты подсчета вероятности совпадения ключей для различных значений параметров схемы.

Библиография

[1]. Divya Harika Nagabhyrava, EFFICIENT KEY GENERATION FOR DYNAMIC BLOM'S SCHEME https://arxiv.org/pdf/1410.7340.pdf

[2]. S.Sukumar Computational Analysis of Modified Blom's Scheme.

[3]. А. П. АЛФЕРОВ, А. Ю, ЗУБОВ, А. С. КУЗЬМИН, А. В. ЧЕРЕМУШКИН. Основы Криптографии. М. 2005. С. 390-394.

[4]. R. Blom, An Optimal Class Of Symmetric Key Generation Systems. Ericsson Radio Systems, Stockholm, Sweden, 1985.

[5]. A.Parakh and S. Kak, Efficient key management in sensor networks. Proceedings IEEE GLOBECOM workshops (GC workshops). pp. 1539–1544, 2010.

[6]. A.Parakh and S. Kak, Matrix based key agreement algorithms for sensor networks. Proceedings IEEE 5th International Conference on Advanced Networks and Telecommunication Systems (ANTS), pp. 1–3, 2011.

[7]. W. Du, J. Deng, Y S. Han, P. Varshney, J. Katz, and A. Khalili. A pairwise key pre- distribution scheme for wireless sensor networks. ACM Transactions on Information and System Security (TISSEC), 2005.

[8]. D. Liu, P. Ning, and R. Li. Establishing pairwise keys in distributed sensor networks. ACM Trans. Inf Syst. Secur., 8:41-77, Oct 2005.

[9]. A. Parakh and S. Kak, Online data storage using implicit security. Information Sciences, vol. 179, pp. 3323-3331, 2009.

[10]. A. Parakh and S. Kak, Space efficient secret sharing for implicit data security. Information Sciences, vol. 181, pp. 335-341, 2011.

[11]. G. J. Pottie and W. J. Kaiser. Wireless Integrated Network Sensors. Communications of the ACM, 43(5):51-58, 2000.

[12]. R.S. Reddy, "Key management in wireless sensor networks using a modified Blom scheme", arXiv: 1103.5712.

[13]. Mee Loong Yang, Adnan Al-Anbuky and William Liu, An Authenticated Key Agreement Scheme for Wireless Sensor Networks

Parameter analysis of Blom's key distribution dynamic scheme

Seyed Pouria Zahraei

***Abstract*—Matrix schemes of preliminary key distribution are considered in the paper, they are constructed on the basis of the Blom scheme. Such schemes are used, in particular, in wireless sensor networks and allow effectively changing secret key parameters of a trusted center (TC) when the keys of certain protocol participants are compromised.**

The paper presents a modernized Blom matrix scheme. It is assumed that the TC selects an N × N matrix P over a finite field GF (q), where N is the size of the network and q> N. Then, depending on the value of the security parameter t, the first t + 1 rows of the matrix P are taken as an open matrix. The matrix P is public, and it is assumed that any system of t + 1 columns to this matrix is linearly independent. In addition, it is assumed that the TC generates a random (t + 1) × (t + 1) symmetric secret matrix S over GF (q), $S = X * X^T$, X is a random matrix of size (t + 1) × (t +1), and computes the matrix $A = (S.P)^T$.

If nodes i and j need to set a common key, they first exchange columns from the matrix P and then compute K_{ij} and K_{ji}, respectively, using the secret rows of the matrix A.

The probability of coincidence of keys for different pairs of participants is calculated.

Based on the program implementation, the results of computational experiments are presented. In particular, the dependence of the probability of coincidence of the keys of two participants on the protocol parameters (the size of the field and the number of participants) was established experimentally. For q = 1009, the number of key matches for different N values was obtained. Also, the results for the value of N were obtained on the assumption that the maximum of coincidences should be equal to 5.

***Keywords* — Blom's scheme, trusted center (TC), Blom model, modified Blom's scheme, attack, probability of key matching.**