# Кольцевые подписи и их приложения

From CryptoWiki

**Кольцевая подпись (ring signature)** - такая электронная подпись (http://cryptowiki.net/index.php?title=%D0%AD%D0%BB%D0%B5%D0%BA%D1%82%D1%80%D0%BE%D0%BD%D0%BD%D0%B0%D1%8F_%D0%BF%D0%BE%D0%B4%D0%BF%D0%, которая позволяет одному из участников группы (называемой **кольцом**) выполнить подписание некоторого сообщения от имени всей группы, при этом не будет доподлинно известно, кто из участников группы выполнил подписание.

## Contents



## Постановка задачи защиты информации

В отличие от схемы групповой подписи (group signature), схема кольцевой подписи не требует наличия обслуживающих участников (именно поэтому выбрано название "кольцевая" - кольцо представляет из себя геометрическую фигуру без центра [RST01]). В схеме кольцевой подписи нет заранее подготовленной группы участников, не требуется проведение каких-либо подготовительных процедур для создания или изменения такой группы. Также отсутствует механизм отзыва анонимности подписывающего. Главное требование - каждый из участников должен быть ассоциирован с парой ключей какой-либо схемы открытого шифрования. Это позволяет подписывающему выбрать произвольное множество возможных подписывающих (в которое он включает самого себя) и самостоятельно вычислить подпись, используя открытые ключи других участников из множества возможных и свой секретный ключ (Рисунок 1).

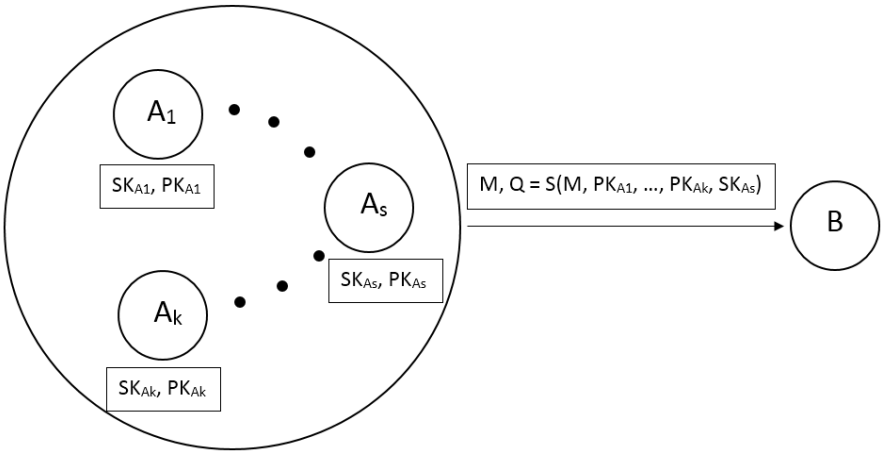


Рисунок 1 - Схема выработки кольцевой подписи участником As с использованием открытый ключей других участников

Таким образом, схема кольцевой подписи может быть использована в случае, если требуется обеспечить анонимность подписывающего, а также его независимость от остальных участников, и при этом обеспечить целостность и подлинность подписываемого сообщения (получатель будет уверен, что сообщение поступило от участника некоторой группы и не от кого-либо вне это группы).

## Теоретические основы решения задачи

### Определения

Под **кольцом** будем понимать группу участников, состоящую из возможных подписантов и подписывающего. **Подписывающим** будем называть участника, желающего подписать некий документ с помощью кольцевой подписи. Каждый из возможных подписантов (об. **X**) ассоциирован со своим публичным ключом **PKx** и соответствующим ему ключом **SKx**. В общем виде не требуется, чтобы индивидуальные схемы подписи каждого из участников обладали какими-либо конкретными свойствами, однако в работе [RST01] приводится пример построения схемы кольцевой подписи с использованием односторонних функций с секретом (например, из схемы RSA). Кольцевая подпись определяется двумя процедурами:

- **RingSign**(M, PK1, PK2,...,PKr, s, SKs) - процедура вычисления кольцевой подписи **Q** - принимает на вход сообщение **M**, которое нужно подписать открытые, ключи участников кольца и секретный ключ **SKs** подписывающего с идентификатором **s**;

- **RingVerify**(M, Q) - процедура проверки кольцевой подписи **Q** - принимает на вход сообщение **M** и кольцевую подпись **Q**, вычисленную на его основе; возвращает значение 1, если подпись верна, и 0 в противном случае.

### Требования

Схема кольцевой подписи не нуждается в проведении подготовительных процедур. Подписывающему не нужно согласие остальных участников кольца. Они даже могут не знать о том, что участвовали в формировании подписи. Подписывающий лишь должен знать открытые ключи всех участников кольца для успешного вычисления кольцевой подписи. Проверка подписи должна удовлетворять условиям полноты и корректности, но также требуется, чтобы имела место **неоднозначность подписывающего** в том смысле, что проверяющий должен быть неспособен определить подписывающего с вероятностью большей, чем **1/r** (**r** - количество участников в кольце).

## Криптографические конструкции

Предположим, участник **As** хочет подписать сообщение **M** кольцевой подписью с **r**участниками **A1**, ..., **Ar**.

### Однонаправленная функция с секретом

Каждый участник Ai имеет свой открытый ключ PKi = (ni, ei), который определяет однонаправленную функцию с секретом: $f_i(x) = x^{e_i} \pmod{n_i}$.

Предполагается, что только участник Ai может эффективно вычислить $f_i^{-1}$, поскольку ему известен закрытый ключ **SKi**.

В работе RST предлагается использование расширенной однонаправленной функции с секретом для каждой функции **fi**. Функция принимает на вход b-битовое значение **m**, для которого определяются числа **qi** и **ri** следующим образом: $m = q_i n_i + r_i, 0 \le r_i < n_i$. Расширенная однонаправленная функция с секретом **gi** определяется следующим образом:

$$g_i(m) = \begin{cases} q_i n_i + f_i(r_i) & \text{if } (q_i+1)n_i \le 2^b \\ m & \text{else.} \end{cases}$$

Очевидно, что для каждого участника будет определена собственная расширенная однонаправленная функция с секретом. При этом эффективно вычислить обратное значение функции **gi** можно лишь зная закрытый ключ **SKi**.

### Симметричное шифрование

Пусть **E** - симметричный алгоритм шифрования строк длиной **b** бит. **Ek** - обратимое криптографическое преобразование, использующее ключ **k**.

### Хеш-функция

Пусть **h** - устойчивая к коллизиям хеш-функция, которая преобразует свой вход в строку, используемую в качестве ключа для **Ek** и обратного ему преобразования.

### Комбинационная функция

Под комбинационной функцией будем понимать функцию вида $C_{k,v}(y_1, y_2, \ldots, y_r)$, где **k** - ключ схемы симметричного шифрования, **v** - случайное значение длиной **b** бит, используемое в качестве инициализирующего, **yi** - входные значения длиной **b** бит. Требуется RST, чтобы комбинационная функция удовлетворяла следующим свойствам:

- Для любого входного значения при фиксированных остальных комбинационная функция является взаимно однозначным отображением нефиксированного входного значения к выходному;
- Можно эффективно найти любое неизвестное входное значение при известных остальных и известном выходном значении;
- Невозможно найти входные значения при известном выходном значении и известных параметрах **k** и **v**.

В работе [RST01] предлагается следующая комбинационная функция:

$$C_{k,v}(y_1, y_2, \ldots, y_r) = E_k(y_r \oplus E_k(y_{r-1} \oplus E_k(y_{r-2} \oplus E_k(\ldots \oplus E_k(y_1 \oplus v)\ldots)))).$$

Если принять, что $y_i = g_i(x_i)$, то комбинационную функцию можно изобразить следующим образом:

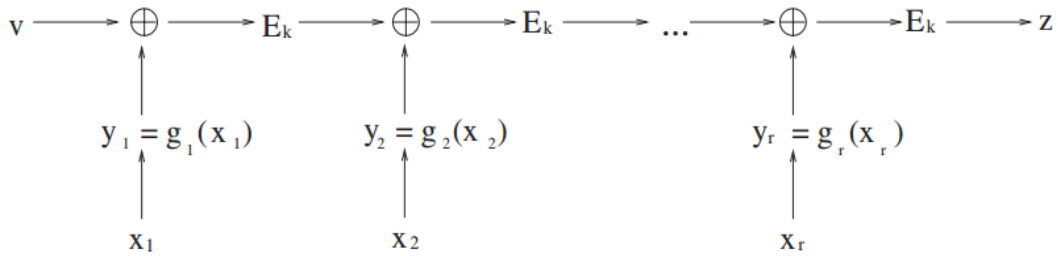


Рисунок 2 - Предложенная комбинационная функция

Данная функция может быть использована для создания кольцевой подписи и ее проверки.

### Создание подписи

Имея сообщение **m**, свой закрытый ключ **SKs** и последовательность открытых ключей участников кольца, подписывающий **As** создает кольцевую подпись следующим образом:

- Вычисляет ключ **k** следующим образом: $k = h(m)$
- Выбирает случайное значение **v**

- Выбирает случайные значения **xi** кроме значения, соответствующего собственному номеру **s**, и вычисляет значения $y_i = g_i(x_i)$
- Находит **ys**, решая уравнение $C_{k,v}(y_1, y_2, \ldots, y_r) = v$
- Находит **xs** с помощью знания **SKs**: $x_s = g_s^{-1}(y_s)$
- Предоставляет вычисленную кольцевую подпись в виде $v; x_1, x_2, \ldots, x_r$

### Проверка подписи

Имея кольцевую подпись сообщения **m**, само сообщение и набор открытых ключей участников кольца, проверяющий может проверить подпись следующим образом:

- Для каждого значения **xi** вычисляет $y_i = g_i(x_i)$
- Вычисляет ключ **k** следующим образом: $k = h(m)$
- Проверяет верность уравнения $C_{k,v}(y_1, y_2, \ldots, y_r) = v$ для значений **yi**
- Если уравнение верно, подпись считается верной, в противной случае считается неверной

## Приложения кольцевой подписи

### Криптовалюты

Кольцевая подпись используется в некоторых криптовалютах (Основанных на протоколе CryptoNote) для сокрытия отправителя. В таких системах в качестве адреса получателя используются одноразовые адреса. Кольцевые подписи подтверждают право пользоваться одним из возможных адресов в цепочке, но каким именно - неизвестно.Транзакции, подписанные кольцевой подписью, ссылаются на несколько других транзакций в цепочке блоков. С точки зрения наблюдателя, такая транзакция с равной вероятностью может использовать в качестве входа любую из транзакций, на которые она ссылается. Чем большее количество ссылок на предыдущие транзакции включено в кольцевую подпись, тем больше неопределённость и тем больше размер самой подписи.

### Анонимные источники информации

Кольцевая подпись может быть использована [AJR05] в следующем случае: некий чиновник желает разгласить некую информацию, при этом подписав ее от имени нескольких чиновников. Таким образом, прочие лица смогут ссылаться на эту информацию и быть уверены в том, что источник действительно является чиновником. При этом сам чиновник останется анонимным.

### Доказательство права доступа к ресурсу

Кольцевая подпись может позволить [AJR05] принять доказательство того, что некий член группы пользователей имеет доступ к некоторому ресурсу, в то же время не разглашая личность этого пользователя.

### Электронная почта

Кольцевая подпись с кольцом размера 2 может быть использована в электронной почте [AJR05] для того, чтобы один из пользователей мог отправить другому подписанное сообщение, но при этом другой пользователь не мог в последствии доказать, кто является отправителем.

## Глоссарий

- Симметричное шифрование
- Ассиметричная криптография
- RSA
- XOR
- Хеширование
- Криптовалюты на основе блокчейна

## Список литературы

Перейти к Список литературы к разделу "Кольцевые подписи и их приложения"

*Резвухин Р.А, 2016*