Протокола одноразовой кольцевой подписи (One-Time Ring Signature)

СТУДЕНТ: ЛЕ КУАНГ ХОАЙ

ГРУППА: С21-762

1. Введение:

- Кольцевая подпись (ring signature) позволяет участнику группы подписывать сообщения от имени всей группы (указывая для проверки вместо своего открытого ключа ключи всех участников группы). Проверяющий уверен, что использован один из секретных ключей, но чей именно — он не знает. В то же время кольцевая подпись обеспечивает большую гибкость: отсутствие менеджера группы, отсутствие специальной настройки и динамика выбора группы. Однако в некоторых приложениях кольцевая подпись уязвима для злонамеренных или безответственных подписывающих лиц из-за своей анонимности.
- Тег(tag): состоящую из списка участников группы и проблемы, относящейся, например, к общественному делу или выборам. Участник кольца может высказать любое подписанное, но анонимное мнение по проблеме, но только один раз (для каждого тега).
- Одноразовой кольцевой подписи (One-time ring signature)— это вариант кольцевых подписей, который ограничивает гарантии анонимности, гарантируя, что участник может подписать анонимно не более одного сообщения на тег.
- Такое свойство востребовано во многих областях: электронные выборы (каждый участник может проголосовать только один раз), цифровые деньги (электронные монеты можно потратить лишь единожды) и т. д. Продемонстрируем применение алгоритма в сфере открытых электронных транзакций на примере децентрализованной p2p-валюты Bitcoin. Это решение позволяет участнику совершать полностью неотслеживаемый платёж (что на данный момент невозможно в Bitcoin), открыто публикуя детали операций по переводу и получению средств.

2. Одноразовая кольцевая подпись Fujisaki-Suzuki

- тег L = (issue, pkN), где pkN — это набор открытых ключей участников кольца и проблема относятся.
- Участник кольца может подписать сообщение, используя свой собственный секретный ключ, а проверяющий может проверить подпись сообщения относительно тега L, но не может знать, кто сгенерировал подпись среди всех возможных участников кольца в L.
- Если подписавший подписал другие сообщении с тем же тегом, то анонимность подписавшего отозван
- Но если он подписал то же самое снова сообщение с тем же тегом, каждый только может видеть, что две подписи связаны (tag-linkability)
- Дефект: злоумышленник, который просто хочет нарушить работу системы, может организовать простую атаку типа «отказ в обслуживании», непрерывно отправляя несколько подписей одного и того же сообщения.

3. Одноразовая кольцевая подпись Scafuro-Zhang

В любом случае, если подписавший подписал с тем же тегом несколько раз, его анонимность будет раскрыта.

Идея основана на двусмысленности схемы фиксации битов Наора:

λ - параметр безопасности

1. R - случайная строка 3λ-битов

2. обязательство c рассчитывается следующим

$c := G(s) \oplus (b \cdot R)$

b — бит фиксации

PRG $G: \{0,1\}^{\lambda} \rightarrow \{0,1\}^{3\lambda}$

Чтобы открыть обязательство c (вычисленное по строке R), отправитель просто отправляет начальное значение PRG s (которое использовалось для вычисления c).

На основе начального числа s получатель может сделать вывод, был ли бит, зафиксированный в c, равен 0 или 1, просто попытавшись перечислить c либо как $G(s)$ ($b = 0$), либо как $G(s) \oplus R$ ($b = 1$).

3. Одноразовая кольцевая подпись Scafuro-Zhang

Trapdoor:

Если R двусмысленный:

$R = G(s0) \oplus G(s1)$

s0, s1 random seeds

Обязательство c = G(s0) может быть открыто как 0 или 1.

Если b=0: $s=s0 \rightarrow G(s) \oplus (b \cdot R)=G(s0) \oplus (0 \cdot R)=G(s0)=c$

Если b=1: $s=s1 \rightarrow G(s) \oplus (b \cdot R)=G(s1) \oplus G(s0) \oplus G(s1)=G(s0)=c$

Чтобы двусмысленно зафиксировать λ-битную строку, просто нужно λ строк (R1,..., Rλ), вычисленных в «двусмысленном режиме».

4. Схема Scafuro-Zhang

Key Generation: (pki , ski) ← GenKey(1^λ)

Signing Algorithm: (R, σ, m) ← RSign(R, m, sk_l)

R = (pk_1, pk_2,…, pk_N) - кольцо

sk_l – открытый ключ отправителя

m - сообщение

σ – подпись на m

Verification Algorithm: {0, 1} ← RVer(R, m, σ)

Выход 1 если подпись подтверждает, иначе 0

Trace: Trace(R, m1, σ1, m2, σ2)

Выход “pk_l” если подписи σ1, σ2 того же участника l, иначе “indep”

5. Key Generation

PRG G: $\{0,1\}^{\lambda} \rightarrow \{0,1\}^{3\lambda}$

Хеш-функция H: $\{0,1\}^{*} \rightarrow \{0,1\}^{\lambda}$

Участник i присоединяется к системе следующим образом:

1. Выбор 2λ seed: $s_{i,j}^{0} \leftarrow \{0,1\}^{\lambda}$, $s_{i,j}^{1} \leftarrow \{0,1\}^{\lambda}$, $j = 1,\ldots\lambda$
2. Вычислить $pk_{i,j} = G(s_{i,j}^{0}) \oplus G(s_{i,j}^{1})$ и $sk_{i,j} = (s_{i,j}^{0}, s_{i,j}^{1})$
3. Открытый ключ $pk_i = (pk_{i,1}, pk_{i,2}, \ldots, pk_{i,\lambda})$
   Секретный ключ $sk_i = (sk_{i,1}, sk_{i,2}, \ldots, sk_{i,\lambda})$

6. Signing Algorithm

Участник I подписывает сообщение следующим образом.

1. $R = (pk_1, pk_2, \ldots, pk_N)$, $sk_I=(s_{I,1}^{0}, s_{I,1}^{1}, \ldots, s_{I,\lambda}^{0}, s_{I,\lambda}^{1})$
2. $\forall i \neq I$:

   Применить случайную строку $x_i \in \{0, 1\}^{\lambda}$

   a. Для j-го бита строки x_i, выбирать $r_{i,j} \leftarrow \{0, 1\}^{\lambda}$ и вычислить $c_{i,j}=G(r_{i,j}) \oplus (x_i[j].pk_{i,j})$

   b. $c_i=(c_{i,1},c_{i,2},\ldots,c_{i,\lambda})$
3. $c_I=[G(s_{I,1}^{0}), G(s_{I,2}^{0}), \ldots, G(s_{I,\lambda}^{0})]$
4. $z=H(R,m,c_1,c_2,\ldots,c_N)$
5. Вычислить $x_I^{*}= \bigoplus_i x_i \oplus z$, $i \neq I$
6. $c_{I,j} = G(s_{I,j}^{0})$ может быть открыто как 0 или 1 на $x_I^{*}[j]$: $r_{I,j}=s_{I,j}^{0}$ если $x_I^{*}[j]=0$, $r_{I,j}=s_{I,j}^{1}$ если $x_I^{*}[j]=1$
7. Подпись $\sigma =(x, r)$

7. Verification Algorithm

1. Вычислить $c_{i,j}=G(r_{i,j}) \oplus (x_i[j].pk_{i,j})$ $i=1,...n$, $j=1,..., \lambda$
2. Вычислить $z'=H(R,m,c_1,c_2,...,c_N)$
3. Если $z'=x1 \oplus x2 \oplus ... \oplus xN$ => вывод 1 (подпись подтверждена) иначе вывод 0

8. Trace (R, m1, σ1, m2, σ2)

Заметьте, что если σ1, σ2 того же участники i, то $r_{i,j}^{(1)}$ и $r_{i,j}^{(2)}$ имеют значении либо $s_{i,j}^{0}$ либо $s_{i,j}^{1}$ для любого $j=1,\ldots,\lambda$
Если λ достаточно большое, то вероятность $x_i^{(1)}=x_i^{(2)}$ очень мала
Тогда это казалось в любой момент, что $\exists j: x_i^{(1)}[j] \neq x_i^{(2)}[j] \rightarrow r_{i,j}^{(1)} \neq r_{i,j}^{(2)} \rightarrow G(r_{i,j}^{(1)}) \oplus G(r_{i,j}^{(2)})=G(s_{i,j}^{0}) \oplus G(s_{i,j}^{0})=pk_i[j]$

Поэтому если ∃pki и $\exists j: G(r_{i,j}^{(1)}) \oplus G(r_{i,j}^{(2)})= pk_i[j]$
то σ1 и σ2 — подписи одного и того же человека i → вывод pki
Иначе вывод “indep”

9. Заключение

- Одноразовая кольцевая подпись — это криптографический метод, который позволяет подписавшему защитить свою личность, создавая подпись так, как если бы она была создана любым членом группы, без раскрытия точного подписавшего если он подписал только один раз.
- В этом отчете я исследовал и проанализировал метод одноразовой кольцевой подписи, предложенный Скафуро и Чжаном.
- Методика Скафуро и Чжана предлагает значительные улучшения по сравнению с предыдущими методами, особенно в аспектах безопасности и эффективности. В любом случае, если подписавший подписал с тем же тегом несколько раз, его анонимность будет раскрыта.

Литература

[1] One-time Traceable Ring Signaturesю. Alessandra Scafuro and Bihan Zhang.North Carolina State University
[2] Eiichiro Fujisaki and Koutarou Suzuki. Traceable ring signature. In Public Key Cryptography - PKC 2007, pages 181–200, 2007.