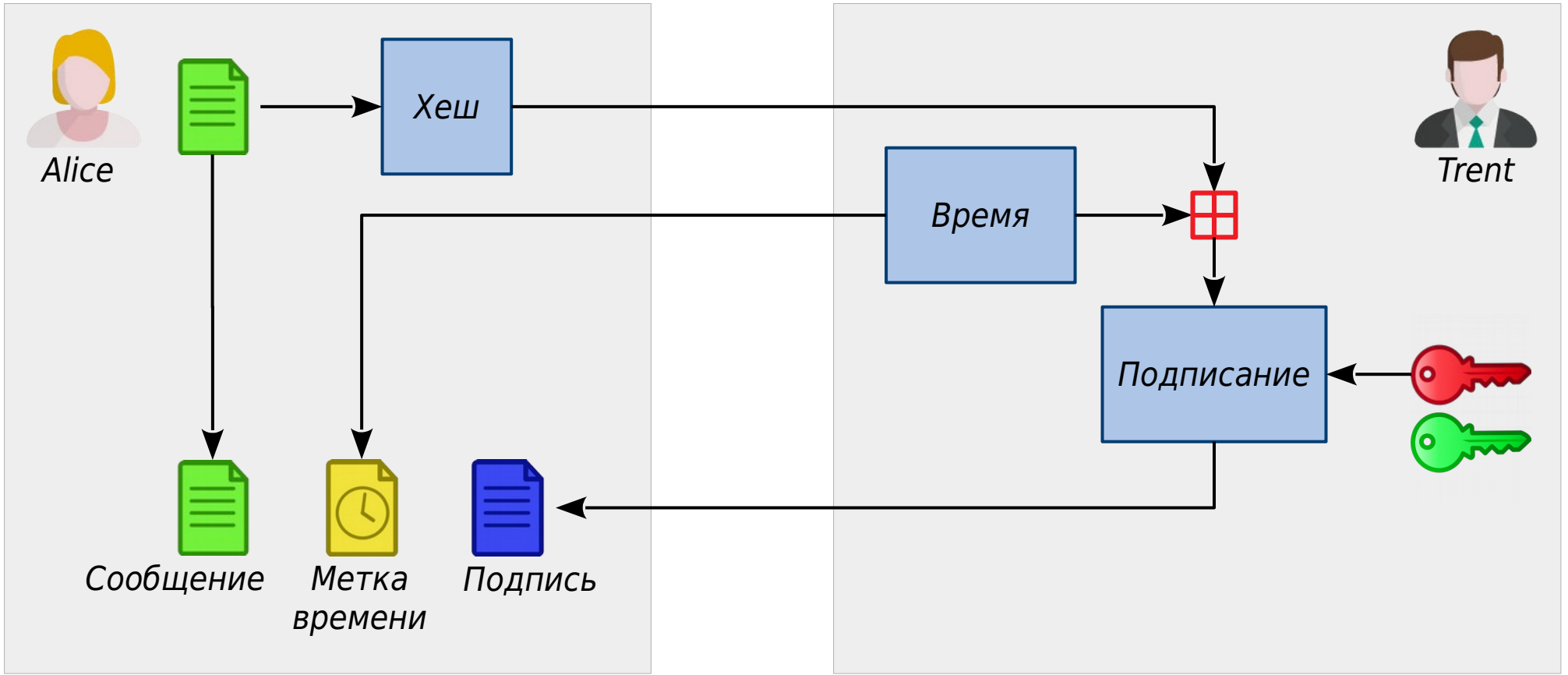
Криптография

Лекция 5. Специальные цифровые подписи.

Дмитрий Яхонтов *“Кочерга”, 2018*

Метки времени
(TimeStamps)



Неотрицаемая подпись

Более удачным было бы название
“Непередаваемая подпись” или *“Некопируемая подпись”*

- Подписант может доказать корректность подписи лично получателю
- Получатель не может передать это доказательство кому-либо другому
- Кроме протокола подтверждения, существует протокол отрицания, который позволяет подписанту доказать некорректность подписи, если это действительно так
- Подписант не может ложно отрицать свою настоящую подпись

Протокол подтверждения

Alice

Bob

открытые простые **p**, **g** ⟶ **p, g**

закрытый ключ: **X**

открытый ключ:

$g^x \bmod p = \mathbf{Y}$ ⟶ **Y**

подписание:

$m^x \bmod p = \mathbf{Z}$ ⟶ **Z**

проверка:

a, **b** < p — *случайные*

C ⟵ $\mathbf{C} = m^a g^b \bmod p$

случайное **q** < p

$Cg^q \bmod p = \mathbf{S1}$ ⟶ **S1**, **S2**

$(Cg^q)^x \bmod p = \mathbf{S2}$

a, **b** ⟵ **a**, **b**

проверяет C

$\mathbf{S1} = Cg^q \bmod p$

q ⟶ **q**

$\mathbf{S2} = Z^a Y^{(b+q)} \bmod p$

Невозможность передачи подписи

Примерно вот так:

a, **b** < p

C = $m^a g^b \bmod p$

Bob

S1 = $Cg^q \bmod p$

S2 = $Z^a Y^{(b+q)} \bmod p$

Протокол отрицания

Alice

Bob

случайные **a**, **s**
V1 = m^s g^a mod p
V2 = Z^s Y^a mod p = $V1^x$

V1, **V2** ←

$V1^x$ mod p
$V1^x$ $V2^{-1}$ = $(m^s g^a)^x (Z^s g^{xa})^{-1}$ = $(m^x Z^{-1})^s$
$m^x Z^{-1}$ = 1 *если* Z = m^x mod p

подсчитывает $(m^x Z^{-1})^i$ *для всех* **i**
и находит i = s.
Это возможно только если
подпись некорректна

случайное **r**
Hash (r, i) →

Hash (r, i)

← **a**

a

проверяет V1, V2

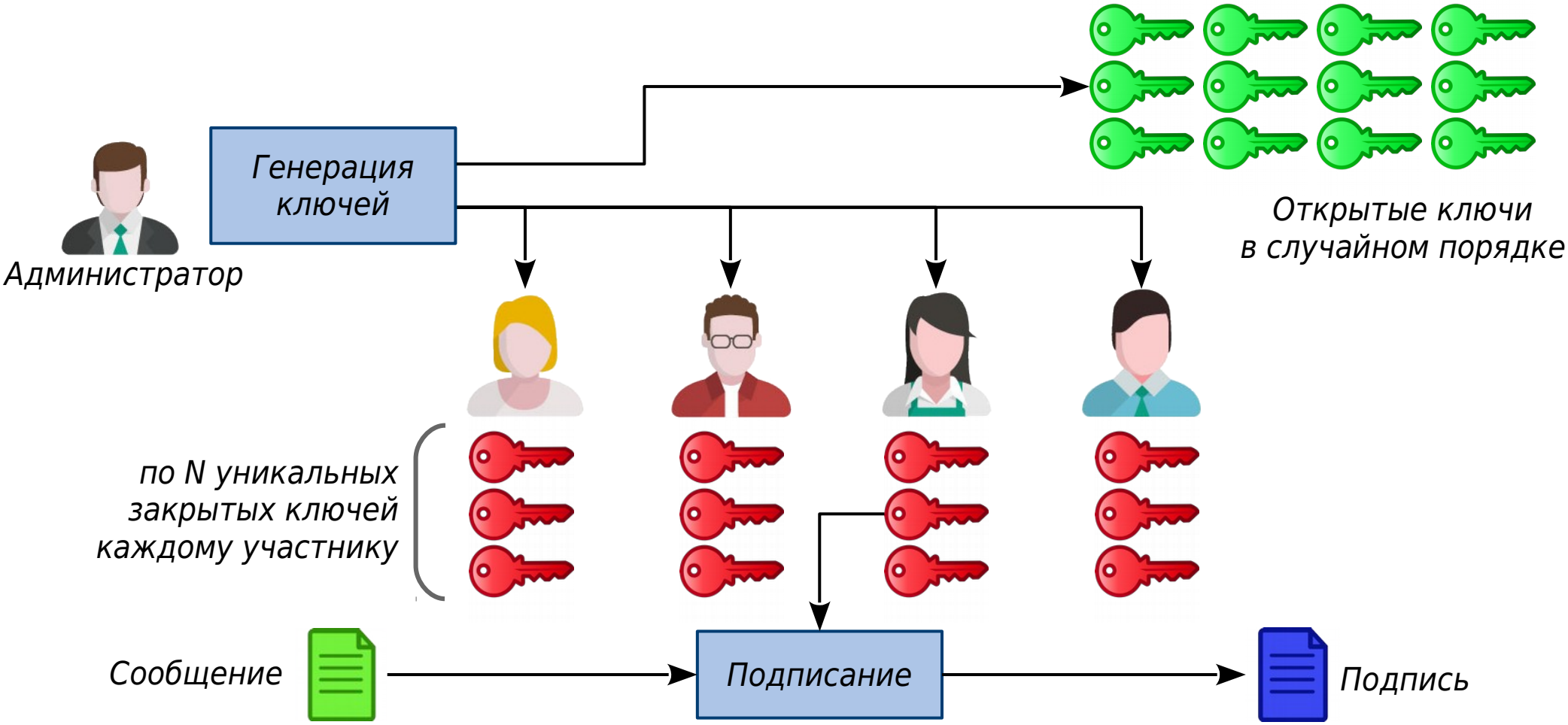
r →

проверяет Hash (r, i) = Hash (r, s)

Групповая подпись

- Участник группы анонимно подписывает сообщение от имени группы
- Подписи двух одинаковых сообщений не дают информации о том, один подписант их сгенерировал или разные
- Несколько участников, сговорившись, не могут подделать подпись другого участника, не входящего в их круг
- При необходимости администратор группы может раскрыть личность подписанта
- Администратор не может ложно объявить подписантом не автора подписи

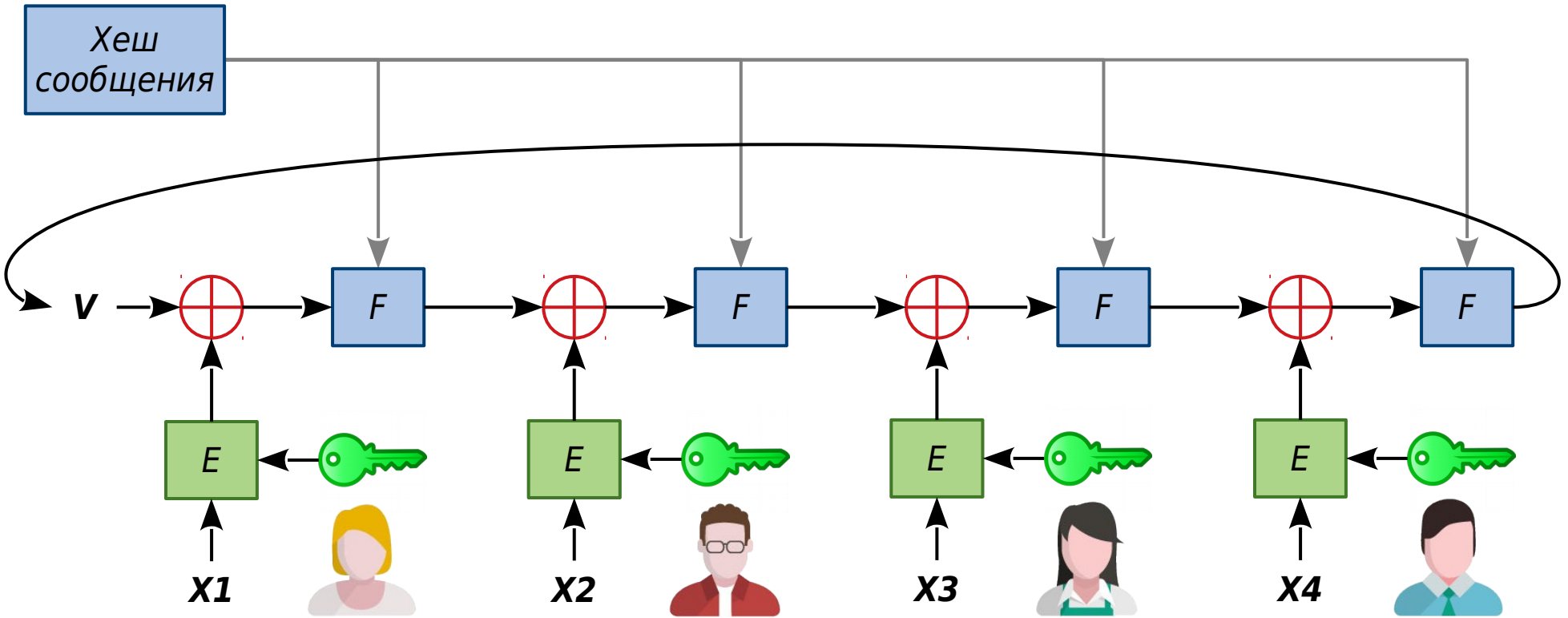
Групповая подпись



Кольцевая подпись

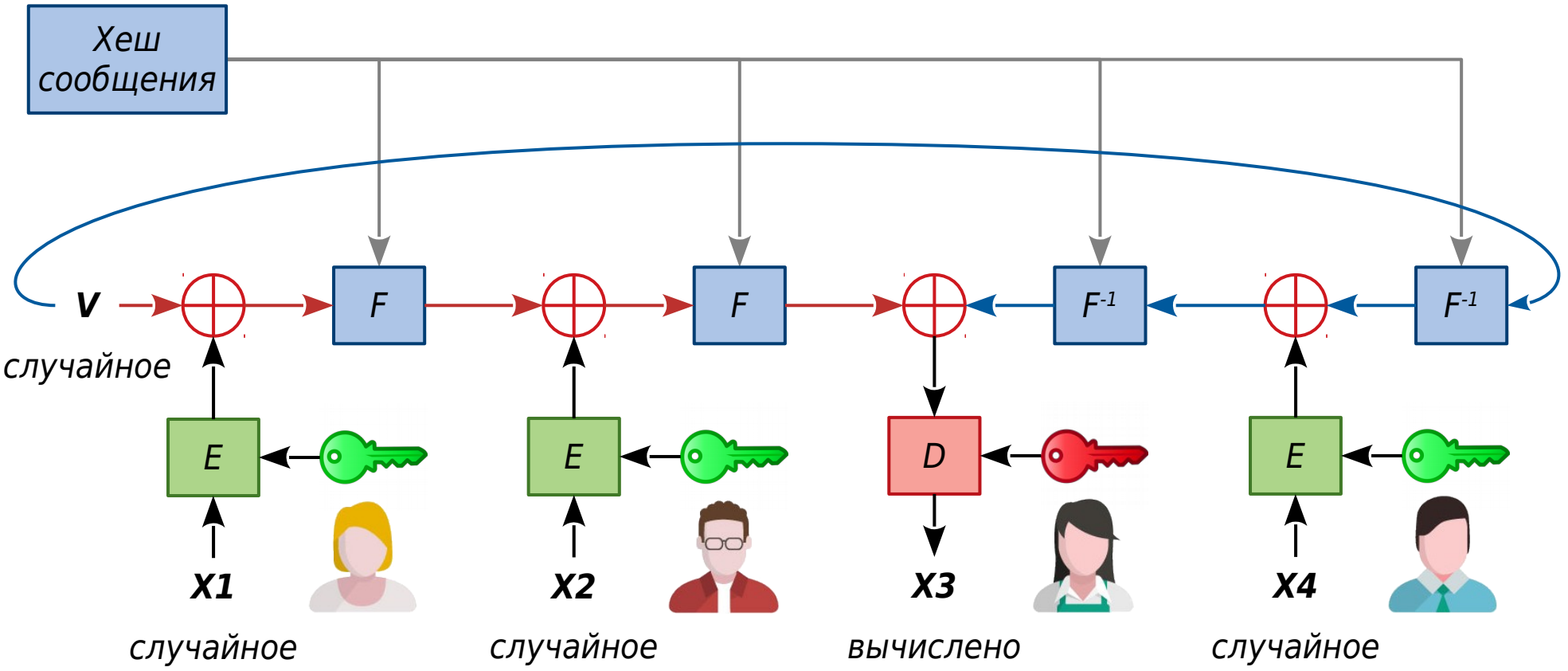
- Участник группы анонимно подписывает сообщение от имени группы
- Подпись гарантирует, что её сгенерировал один из участников, но кто именно — определить невозможно
- У группы нет администратора
- Подписант сам определяет состав группы
- Подписанту не требуется содействие остальных участников (только их открытые ключи)

Проверка кольцевой подписи



Подпись: V, X1, X2, X3, X4

Формирование кольцевой подписи



Слепая подпись

- Подпись корректна и обладает всеми свойствами цифровых подписей (достоверность, неизменность, неотделимость от документа, невозможность отречения от подписи)
- Невозможно связать подписанный документ с конкретным актом подписания. Даже сам подписант не может этого сделать.

1. Алиса применяет к документу *маскирующее преобразование*
2. Боб подписывает замаскированный документ
3. Алиса применяет преобразование, обратное маскирующему, и получает документ, подписанный Бобом

Слепая подпись на основе RSA

Alice

Bob

p, **q** — *секретные простые*

n ← **n** = pq

открытый ключ:

e ← **e** *взаимно простое с* (p-1)(q-1)

сообщение **m**

случайный множитель **k**

закрытый ключ:

d = e^{-1} mod ((p-1)(q-1))

маскирование:

T = mk^e mod n →

подписание:

T

U ← **U** = T^d mod n = $(mk^e)^d$ mod n

демаскирование:

S = U / k mod n = m^d mod n

Задачи

1. Модифицируйте протокол кольцевой подписи так, чтобы подпись могли сформировать только N участников совместно.
   Естественно, требование анонимности сохраняется.
   Никто, кроме подписантов, не должен иметь возможности узнать, кто именно оставил подпись.

2. Алиса — секретный агент. Для успешной работы на вражеской территории ей нужна дипломатическая неприкосновенность, которую может дать министр Боб. Но Алиса — *очень* секретный агент, и имя, под которым она будет работать, не должен знать даже Боб.

   Алиса предлагает Бобу поставить слепую подпись под документом об её неприкосновенности. Боб опасается, что Алиса отдаст ему на подпись, например, приказ выплатить ей миллион долларов.

   Предложите протокол, не позволяющий Алисе обмануть Боба, но и не позволяющий Бобу узнать агентурное имя Алисы.

Ссылки

- Обратная связь:
  - android.ruberoid@gmail.com
  - lesswrongru.slack.com @android_ruberoid
- Анонсы:
  - facebook.com/kocherga.club
  - vk.com/kocherga_club
  - vk.com/kocherga_prog
- Материалы лекций:
  - github.com/notOcelot/Kocherga_crypto
- Видео:
  - youtube.com/channel/UCeLSDFOndl4eKFutg3oowHg