# Специальные схемы цифровой подписи

## Многократные (коллективные, групповые) подписи

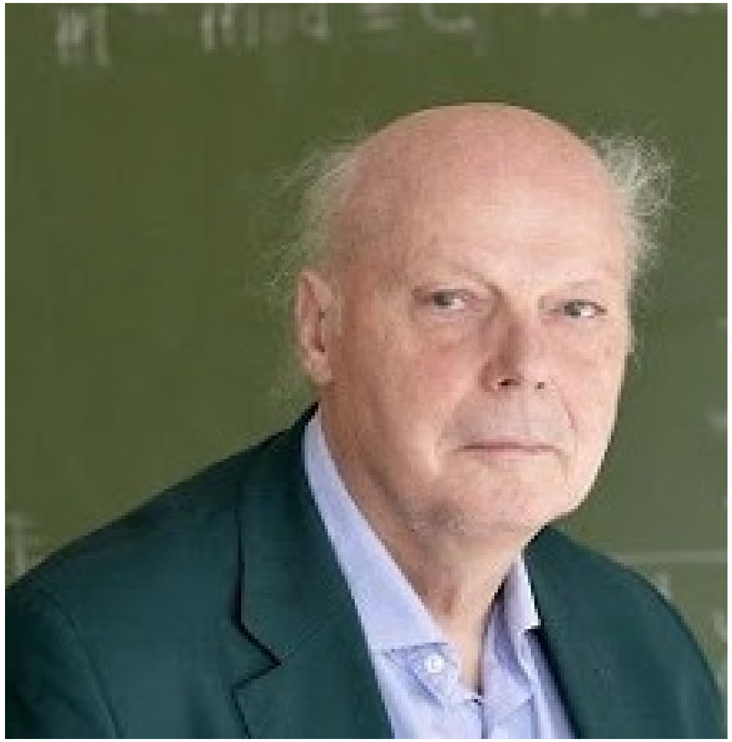
Несколько человек подписывают один и тот же документ. Они легко и просто могут подписать его независимо друг от друга. Однако, прилагаемые таким образом подписи могут значительно увеличить объём пересылаемой информации, связанной с исходным документом. Следующая схема подписи заметно оптимизирует эту задачу.

# Специальные схемы цифровой подписи

## Многократные (коллективные, групповые) подписи

## Многократная подпись Гиллу-Кискате

**Луи Гилу**
(Louis Claude Guillou, 1947 г. Франция)



**Жан-Жак Кискатер**
(Jean-Jacques Quisquater, 1945 г. Бельгия)

# Специальные схемы цифровой подписи

## Многократные (коллективные, групповые) подписи

## Многократная подпись Гиллу-Кискате

Алиса ($A$) и Боб ($B$) подписывают сообщение $m$, с тем, чтобы в дальнейшем Кэрол ($C$) могла проверить их совместную подпись.

**Генерация общих параметров**.

Доверенный центр $T$ (Трент) выбирает большое число $n = p \cdot q$, где $p$, $q$ — большие различные простые числа, которые держатся в секрете. $T$ выбирает целое число $e$ ($1 < e < \varphi(n)$), взаимно простое с $\varphi(n)$, где $\varphi(n) = (p - 1)(q - 1)$ — функция Эйлера. Параметры $\{n, e\}$ объявляются открытыми и общими для подписантов.

**Генерация индивидуальных параметров**.

$T$ вычисляет $s = e^{-1} (\mathrm{mod}\, \varphi(n))$. Затем $T$ вычисляет закрытый ключ Алисы $x_A = J_A^{-s} (\mathrm{mod}\, n)$, где $J_A$ — открытый ключ Алисы (битовая строка личной информации о пользователе $A$ с условием $(J_A, n) = 1$), и закрытый ключ Баба $x_B = J_B^{-s} (\mathrm{mod}\, n)$, где $J_B$ — открытый ключ Боба (битовая строка личной информации о пользователе $B$ с условием $(J_B, n) = 1$). Индивидуальными параметрами соответственно являются $\{J_A, x_A\}$ и $\{J_B, x_B\}$.

# Специальные схемы цифровой подписи

## Многократные (коллективные, групповые) подписи

## Многократная подпись Гиллу-Кискате

**Генерация подписи**.

1. $A \to B$: $\{a_A\}$, где $a_A = r_A{}^e \bmod n$ и $r_A$ — случайное число Алисы, $1 \le r_A \le n - 1$;
2. $B \to A$: $\{a_B\}$, где $a_B = r_B{}^e \bmod n$ и $r_B$ — случайное число Боба, $1 \le r_B \le n - 1$;
3. $A, B$: $\{a\}$, где $a = a_A \cdot a_B \bmod n$ (Алиса и Боб вычисляют $a$);
4. $A, B$: $\{d\}$, где $d = h(m \| a) \bmod e$;
5. $A \to B$: $\{z_A\}$, где $z_A = r_A \cdot x_A{}^d \bmod n$;
6. $B \to A$: $\{z_B\}$, где $z_B = r_B \cdot x_B{}^d \bmod n$;
7. $A, B$: $\{z\}$, где $z = z_A \cdot z_B \bmod n$;
8. $A, B \to C$: $\{m, d, z, J_A, J_B\}$.

**Проверка подписи**.

9. $C$ : $\{J\}$, где $J = J_A \cdot J_B \bmod n$;
10. $C$ : $\{a^*\}$, где $a^* = z^e \cdot J^d \bmod n$;
11. $C$ : $\{d^*\}$, где $d^* = h(m \| a^*) \bmod e$;
12. $C$ : проверяет, что $d^* = d$.

# Специальные схемы цифровой подписи

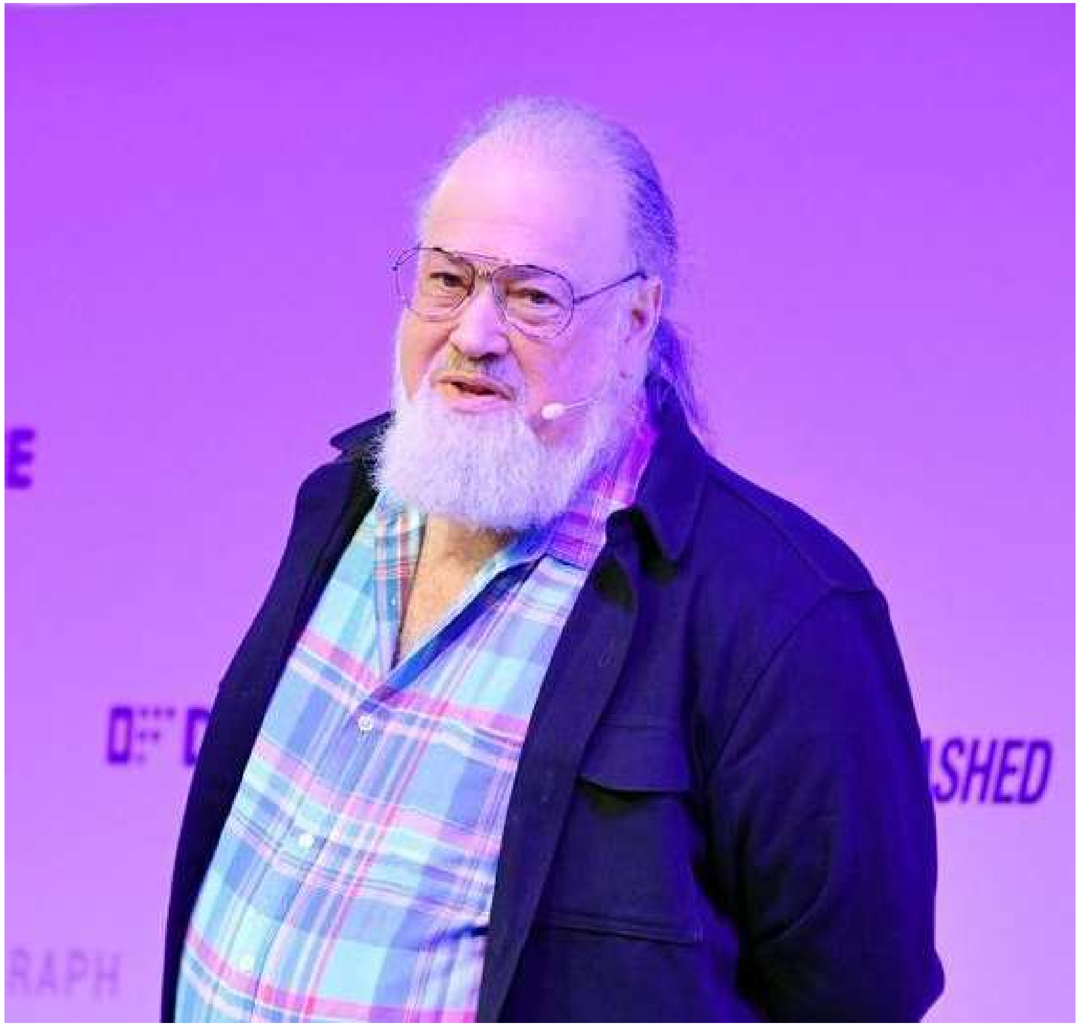
## Неоспоримые подписи

Протокол неоспоримой подписи имеет такое название в силу того, что его записи не могут убедить третью сторону в подлинности подписи без того, чтобы третья сторона не провела весь протокол самостоятельно. Особенностью этих протоколов является тот факт, что проверка подписи осуществляется в интерактивном режиме и требует несколько проходов для участников протокола.

# Специальные схемы цифровой подписи

## Неоспоримые подписи

## Неоспоримая подпись Дэвида Чаума



# Специальные схемы цифровой подписи
## Неоспоримые подписи
## Неоспоримая подпись Дэвида Чаума

Алиса подписывает сообщение $m$, Боб проверяет подпись.

**Генерация общих параметров**. Генерируются: $p$ — большое простое число; $g$ — примитивный корень по модулю $p$.

**Генерация индивидуальных параметров**. Генерируются: $x$ — случайное число Алисы с условием $(x, p - 1) = 1$; $y = g^x \bmod p$. Элементы $\{p, g, y\}$ объявляется открытым ключом, элемент $\{x\}$ — закрытым ключом Алисы.

**Генерация подписи**.

1. $A$: $\{z\}$, Алиса вычисляет подпись $z = m^x \bmod p$.
2. $A \to B$: $\{m, z\}$.

**Проверка подписи**.

3. $B \to A$: $\{c\}$, где $c = z^a y^b \bmod p$, $a, b$ — случайные числа Боба, $1 < a, b < p$;
4. $A \to B$: $\{d\}$, где $d = c^t \bmod p$, $t = x^{-1} \bmod (p - 1)$;
5. $B$ : проверяет, что $d \equiv m^a g^b \bmod p$.

# Специальные схемы цифровой подписи

## Неоспоримые подписи

## Неоспоримая подпись Дэвида Чаума

Покажем, что этот протокол действительно нельзя оспорить. Допустим, Дейв перехватил $m$, $z$ и хочет показать в рамках данного протокола, что на самом деле подпись $z$ принадлежит Еве, а не Алисе. Для этого:

3. $D \to E$: $\{c'\}$, где $c' = z^u y^v \bmod p$, $u, v$ — случайные числа Дейва, $1 < u, v < p$.

Затем Дейв вычисляет $d' \equiv m^u g^v \bmod p$ и отправляет это значение Еве по их совместному тайному каналу, с тем, чтобы она вернула ему это значение, будто бы она его вычислила как $d' = c'^t \bmod p$, $t = x^{-1} \bmod (p-1)$. После чего Ева возвращает это значение Дейву по открытому каналу:

4. $E \to D$: $\{d'\}$;
5. $D$ : проверяет, что $d' \equiv m^u g^v \bmod p$.

Кэрол, имеет две записи этого протокола, от Боба и от Дейва.

| $p, g, y, m, z.$ | |
|---|---|
| $a, b, c = z^a y^b \bmod p, d,$<br>проверка $d \equiv m^a g^b \bmod p.$ | $u, v, c' = z^u y^v \bmod p, d',$<br>проверка $d' \equiv m^u g^v \bmod p.$ |

И Кэрол не может определить авторство подписи, поскольку эти записи выглядят совершенно равносильными.

# Специальные схемы цифровой подписи
## Неоспоримые подписи
## Неоспоримая подпись Дэвида Чаума

Следующий способ проверки этой же подписи позволяет как подтвердить, так и опровергнуть подпись.

**Проверка подписи**.

3. $B \to A$: $\{c\}$, где $c = m^a g^b \bmod p$, $a, b$ — случайные числа Боба, $1 < a, b < p$;
4. $A \to B$: $\{s_1, s_2\}$, где $s_1 = c\, g^q \bmod p$, $s_2 = (c\, g^q)^x \bmod p$, $q$ — случайное число Алисы, $1 < q < p$;
5. $B \to A$: $\{a, b\}$, чтобы Алиса могла убедиться, что Боб не мошенничал на проходе 3;
6. $A \to B$: $\{q\}$, чтобы Боб мог воспользоваться $z = m^x \bmod p$ и восстановить $s_1$ и $s_2$;
7. $B$ : проверяет, что $s_1 \equiv c\, g^q \bmod p$ и $s_2 \equiv (g^x)^{b+q} z^a \bmod p$.

# Специальные схемы цифровой подписи
## Преобразуемые неоспоримые подписи

Преобразуемыми такие подписи названы в силу того обстоятельства, что опубликование дополнительного параметра этой неоспоримой подписи превращает её в обычную цифровую подпись, т.е. в подпись, проверка которой не требует ни одного интерактивного прохода. Преобразуемые неоспоримые подписи основаны на алгоритме цифровых подписей Эль-Гамаля. Рассмотрим сначала этот алгоритм.

Доктор Тахер Эль -Гамаль (араб. طاهر الجمل; род. 18 августа 1955, Каир, Египет) — американский криптограф родом из Египта.
В 1985 году он опубликовал статью под названием «Криптосистема с открытым ключом и схема цифровой подписи на основе дискретных логарифмов», в котором представил свои разработки по созданию систем асимметричного шифрования и цифровой подписи, эксплуатирующих сложность проблемы дискретного логарифмирования. Предложенная им схема ЭЦП стала основой для алгоритма DSA, принятого Национальным институтом стандартов и технологий США (NIST) в качестве стандарта цифровой подписи. Учёный также участвовал в создании протокола оплаты по кредитной карте SET, а также ряда схем интернет-платежей.

# Специальные схемы цифровой подписи

## Преобразуемые неоспоримые подписи

## Схема ELGamal

Эту схему можно использовать как для цифровых подписей, так и для шифрования. Её безопасность основана на трудности вычисления дискретного логарифма в конечном поле. Схема была предложена Тахером Эль-Гамалем в 1985 году.

Алиса подписывает сообщение $m$, Боб проверяет подпись.

**Генерация общих параметров**. Генерируются: $p$ — большое простое число, с условием $m < p$, в качестве $m$ может выступать не само сообщение, а его хэш-значение; $g$ — примитивный корень по модулю $p$.

**Генерация индивидуальных параметров**. Генерируются: $x$ — случайное число Алисы, $1 < x < p$, с условием $(x, p - 1) = 1$; $y = g^x \bmod p$. Элементы $\{p, g, y\}$ объявляется открытым ключом, элемент $\{x\}$ — закрытым ключом Алисы.

**Генерация подписи**.

1. $A$: $\{k\}$, где $k$ — случайное число Алисы, с условием $(k, p - 1) = 1$, $1 < k < p - 1$;
2. $A$: $\{a\}$, где $a = g^k \bmod p$;
3. $A$: $\{b\}$, где $b = k^{-1}(m - xa) \bmod (p - 1)$ [в случае шифрования $b = y^k m \bmod p$];
4. $A \rightarrow B$: $\{m, a, b\}$ [в случае шифрования $\{a, b\}$].

**Проверка подписи**.

5. $B$ : проверяет, что $y^a a^b \bmod p = g^m \bmod p$
   [в случае шифрования $m = b{\cdot}(a^x)^{-1} = b{\cdot}a^{(p-1)-x} \bmod p$].

# Специальные схемы цифровой подписи
## Преобразуемые неоспоримые подписи
## Преобразуемая неоспоримая подпись ELGamal

Алиса подписывает сообщение $m$, Боб проверяет подпись.

**Генерация общих параметров**. Генерируются: $q$ — большое простое число, $p$ — большое простое число вида $p = 2^n \cdot q + 1$ (т.е. $p - 1 = 2^n \cdot q$). Далее следующим образом генерируется число $g$. Выбирается случайное число $h$ ($1 < h < p - 1$) и вычисляется $g = h^{(p-1)/q} \bmod p$. Если $g \neq 1$, то используется полученное значение $g$.

**Генерация индивидуальных параметров**. Генерируются: $x$ и $z$ — различные случайные числа Алисы, $1 < x, z < q$; вычисляются $y = g^x \bmod p$ и $u = g^z \bmod p$. Элементы $\{p, q, g, y, u\}$ объявляется открытым ключом, элементы $\{x, z\}$ — закрытым ключом Алисы.

# Специальные схемы цифровой подписи
## Преобразуемые неоспоримые подписи
## Преобразуемая неоспоримая подпись ELGamal

**Генерация подписи**.

1. $A$: $\{t\}$, где $t$ — случайное число Алисы, $1 < t < q$;
2. $A$: $\{T\}$, где $T = g^{t} \bmod p$;
3. $A$: $\{m'\}$, где $m' = Ttzm \bmod q$;

Теперь вычисляется обычная подпись Эль-Гамаля для $m'$ в следующих обозначениях:

4. $A$: $\{R\}$, где $R$ — случайное число Алисы, с условием $(R, p-1) = 1$, $1 < R < p-1$;
5. $A$: $\{r\}$, где $r = g^{R} \bmod p$;
6. $A$: $\{s\}$, где $s = R^{-1}(m' - rx) \bmod q$;
7. $A \to B$: $\{m, r, s, T\}$.

# Специальные схемы цифровой подписи
## Преобразуемые неоспоримые подписи
## Преобразуемая неоспоримая подпись ELGamal

**Проверка подписи**.

8. $B \to A$: $\{c\}$, где $c = T^{Tma} \cdot g^{b} \bmod p$ и $a, b$ — случайные числа Боба, $1 < a, b < p$;
9. $A \to B$: $\{h_1, h_2\}$, где $h_1 = c \cdot g^{k} \bmod p$, $h_2 = h_1^{z} \bmod p$ и $k$ — случайное число Алисы, $1 < k < p$;
10. $B \to A$: $\{a, b\}$;
11. $A$: проверяет, что $c$, полученное на проходе 8, удовлетворяет условию $c = T^{Tma} \cdot g^{b} \bmod p$, после чего
12. $A \to B$: $\{k\}$;
13. $B$: проверяет, что $h_1 = T^{Tma} \cdot g^{b+k} \bmod p$, и $h_2 = y^{ra} \cdot r^{sa} \cdot u^{b+k} \bmod p$;

Опубликовав значение $z$, Алиса может преобразовать все свои неоспоримые подписи в обычные. Теперь любой сможет проверить подпись Алисы без ее помощи.

# Специальные схемы цифровой подписи
## Подписи «вслепую»

Суть подписи «вслепую» заключается в том, чтобы подписант не имел возможности ознакомиться с содержанием документа, который он подписывает. Понятие слепой подписи было предложено Дэвидом Чаумом в 1982 г., он же предложил и первую реализацию подобной подписи. Она использует алгоритм RSA и обеспечивается его стойкостью. У Боба есть открытый ключ $e$, закрытый ключ $d$ и открытый модуль $n$. Алиса хочет, чтобы Боб вслепую, не читая, подписал сообщение $m$.

**Генерация подписи**.

1. $A \to B$: $\{t\}$, где $t = m \cdot k^e \bmod n$, и $k$ — случайное число Алисы, с условием $1 < k < n$ (Алиса маскирует сообщение $m$);
2. $B \to A$: $\{b\}$, где $b = t^d \bmod n$ (Боб подписывает сообщение $t$);
3. $A$: $\{s\}$, где $s = b \cdot k^{-1} \bmod n$ (Алиса снимает маскировку и получает подпись Боб $s = m^d \bmod n$).
4. $A \to D$: $\{m, s\}$.

**Проверка подписи**.

1. $D$ : проверяет, что $m = s^e \bmod n$.

# Специальные схемы цифровой подписи
## Подписи, подтверждаемые доверенным лицом

Идея этой подписи состоит в возможности Алисе подписать сообщение и Бобу проверить её подпись так, чтобы Кэрол (доверенное лицо Алисы) немного позже могла доказать Дэйву (третьему лицу) правильность подписи Алисы.

Алиса подписывает сообщение $m$, Боб проверяет подпись.

**Генерация общих параметров**. $p$ — большое простое число; $g$ — примитивный корень по модулю $p$; $n$ — произведению двух различных больших простых чисел, отличных от $p$.

**Генерация индивидуальных параметров**. $x$ — случайное число Алисы, её закрытый ключ; $a = g^x \bmod p$ — открытый ключ Алисы; $z$ — случайное число Кэрол, её закрытый ключ; $h = g^z \bmod p$ — открытый ключ Кэрол;

**Генерация подписи**.

1. $A \to B$: $\{m, a, b, j\}$, где $a = g^x \bmod p$, $b = h^x \bmod p$, $x$ — случайное число Алисы ($1 < x < n$), $H(m)$ — хэш-значение от $m$, $H(a, b)$ — хэш-значение от конкатенации $a$ и $b$, и $j = (H(m) \oplus H(a, b))^3 \bmod n$;

# Специальные схемы цифровой подписи

## Подписи, подтверждаемые доверенным лицом

**Проверка подписи Бобом**.

2. $B \to A$: $\{c\}$, где $c = g^s \cdot h^t \bmod p$ и $s, t$ — случайные числа Боба, $1 < s, t < p$;
3. $A \to B$: $\{d, e\}$, где $d = g^q \bmod p$, $e = (cd)^x \bmod p$ и $q$ — случайное число Алисы, $1 < q < p$;
4. $B \to A$: $\{s, t\}$;
5. $A$: проверяет, что $g^s h^t = c \bmod p$, после чего
6. $A \to B$: $\{q\}$;
7. $B$: проверяет, что $d \equiv g^q \bmod p$, $ea^{-q} \equiv a^s b^t \bmod p$ и $(H(m) \oplus H(a, b))^3 \equiv j \bmod n$. Если все три тождества подтверждаются, то подпись считается действительной.

# Специальные схемы цифровой подписи
## Подписи, подтверждаемые доверенным лицом

Боб не может использовать запись этого доказательства для убеждения Дэйва в истинности подписи, но Дэйв может выполнить протокол с доверенным лицом Алисы Кэрол, которая уполномочена подтверждать ее подпись. Вот как Кэрол убеждает Дэйва в том, что $a$ и $b$ образуют правильную подпись.

**Проверка подписи Дэйвом с помощью Кэрол**.

1. $D \to C$: $\{k\}$, где $k = g^{u} \cdot a^{v} \bmod p$ и $u, v$ — случайные числа Дэйва, $1 < u, v < p$;
2. $C \to D$: $\{l, y\}$, где $l = g^{w} \bmod p$, $y = (kl)^{z} \bmod p$ и $w$ — случайное число Кэрол, $1 < w < p$;
3. $D \to C$: $\{u, v\}$;
4. $C$: проверяет, что $g^{u}a^{v} = k \bmod p$, после чего
5. $C \to D$: $\{w\}$;
6. $D$: проверяет, что $l \equiv g^{w} \bmod p$, $yh^{-w} \equiv h^{u}b^{v} \bmod p$. Если оба тождества подтверждаются, то подпись считается действительной.

# Специальные схемы цифровой подписи

**Задание 1**. Алиса может отрицать подпись $z$ под сообщением $m$ в схеме неоспоримой подписи. Описать подробно действия этого отрицания.
**Задание 2**. Проверить корректность схемы ELGamal.
**Задание 3**. Каждая подпись или шифрование ELGamal требует нового значения $k$, и это значение должно быть выбрано случайным образом. Если когда-нибудь Ева раскроет $k$, используемое Алисой, она сможет раскрыть закрытый ключ Алисы $x$. Если Ева когда-нибудь сможет получить два сообщения, подписанные или зашифрованные с помощью одного и того же $k$, то она сможет раскрыть $x$, даже не зная значения $k$. Подробно раскрыть эти способы вскрытия схемы ELGamal.
**Задание 4**. Проверить корректность процедуры проверки преобразуемой неоспоримой подписи ELGamal.
**Задание 5**. В конце протокола преобразуемой неоспоримой подписи записано «Опубликовав значение $z$, Алиса может преобразовать все свои неоспоримые подписи в обычные». Показать, как в этом случае будет осуществляться проверка подписи.