Алгоритм пороговой электронной цифровой прокси подписи без раскрытия секретного ключа

Толюпа Евгений

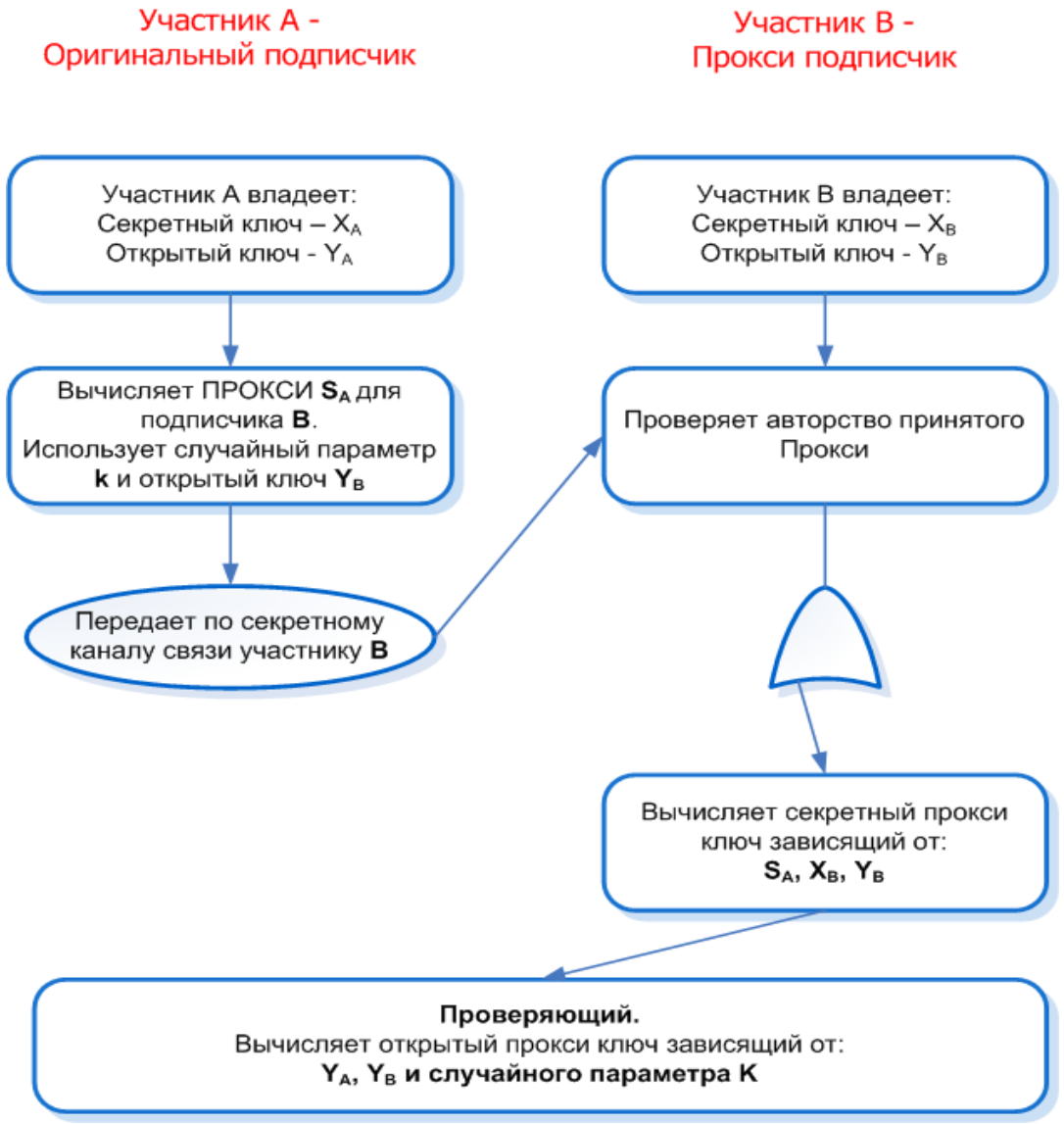
ЯрГУ им. П.Г. Демидова

Г. Ярославль

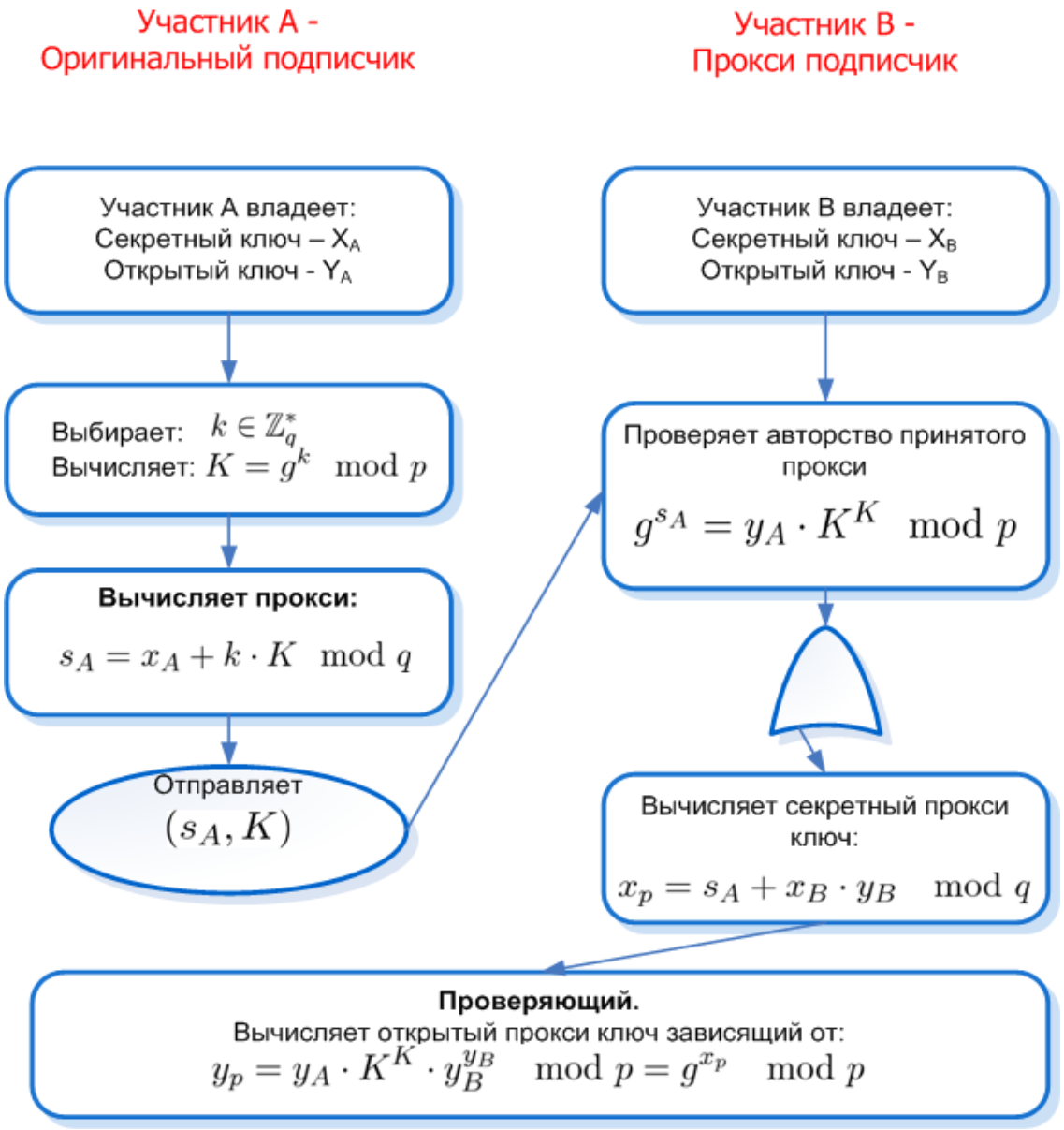
Определения

- **Оригинальный подписчик** – владелец ЭЦП, который передает свои полномочия доверительному подписчику
- **Прокси** – информация, которую вырабатывает оригинальный подписчик для последующей генерации прокси ключа доверительным подписчиком
- **Прокси подписчик** – участник ЭДО, который ставит подпись под документом от лица оригинального подписчика
- **Электронная цифровая прокси подпись** (прокси подпись) – подпись, поставленная прокси подписчиком, под сообщением M от лица оригинального подписчика
- **Прокси ключи** – ключи, которые были выработаны для вычисления прокси подписи.

Общая схема


Участник А -
Оригинальный подписчик
Участник В -
Прокси подписчик
Участник А владеет:
Секретный ключ – X_A
Открытый ключ - Y_A
Участник В владеет:
Секретный ключ – X_B
Открытый ключ - Y_B
Вычисляет ПРОКСИ S_A для подписчика **B**.
Использует случайный параметр **k** и открытый ключ Y_B
Передает по секретному каналу связи участнику **B**
Проверяет авторство принятого Прокси
Вычисляет секретный прокси ключ зависящий от:
S_A, X_B, Y_B
Проверяющий.
Вычисляет открытый прокси ключ зависящий от:
Y_A, Y_B **и случайного параметра K**

Алгоритм Mambo & al



Постановка задачи

- Прокси подписи не позволяют контролировать какие документы будут подписываться прокси подписчиками.
  - Вариант решения: использование пороговых алгоритмов распределения ключевой информации.
- Прокси подпись может быть поставлена только в том случае, если определенное число участников будут согласны подписаться.

Требования

Предъявляемые требования:

- Многоразовое использование прокси
- Невозможность восстановить секретный прокси ключ
- Открытый прокси ключ не зависит от состава группы, восстановившей секрет

Алгоритм Педерсена

За основу взят алгоритм Педерсена, который позволяет:

- Выработать пару ключей (x,y) группе из n участников
- Группа публикует открытый ключ до восстановления секретного ключа
- Группа из t-участников располагает достаточной информацией для восстановления секретного ключа

- Минус – группа из t-человек узнает, секретный ключ и уже любой участник группы может им пользоваться единолично

Оригинальный подписчик

Участник А -
Оригинальный подписчик

1. Генерирует случайное число: $r \in \mathbb{Z}_q^*$
2. Вычисляет: $R = g^r \mod p$
3. Вычисляет прокси:
$$s_A = x_A + r \cdot R \mod q$$

Генерирует многочлен:

$$f_A(x) = s_A + a_1 \cdot x + a_2 \cdot x^2 + \cdots + a_{k-1} \cdot x^{k-1} + a_n \cdot x^n;$$

$$f_A(0) = s_A$$

Каждому участнику группы $\mathcal{P}$ передает значение, соответствующее его порядковому номеру:

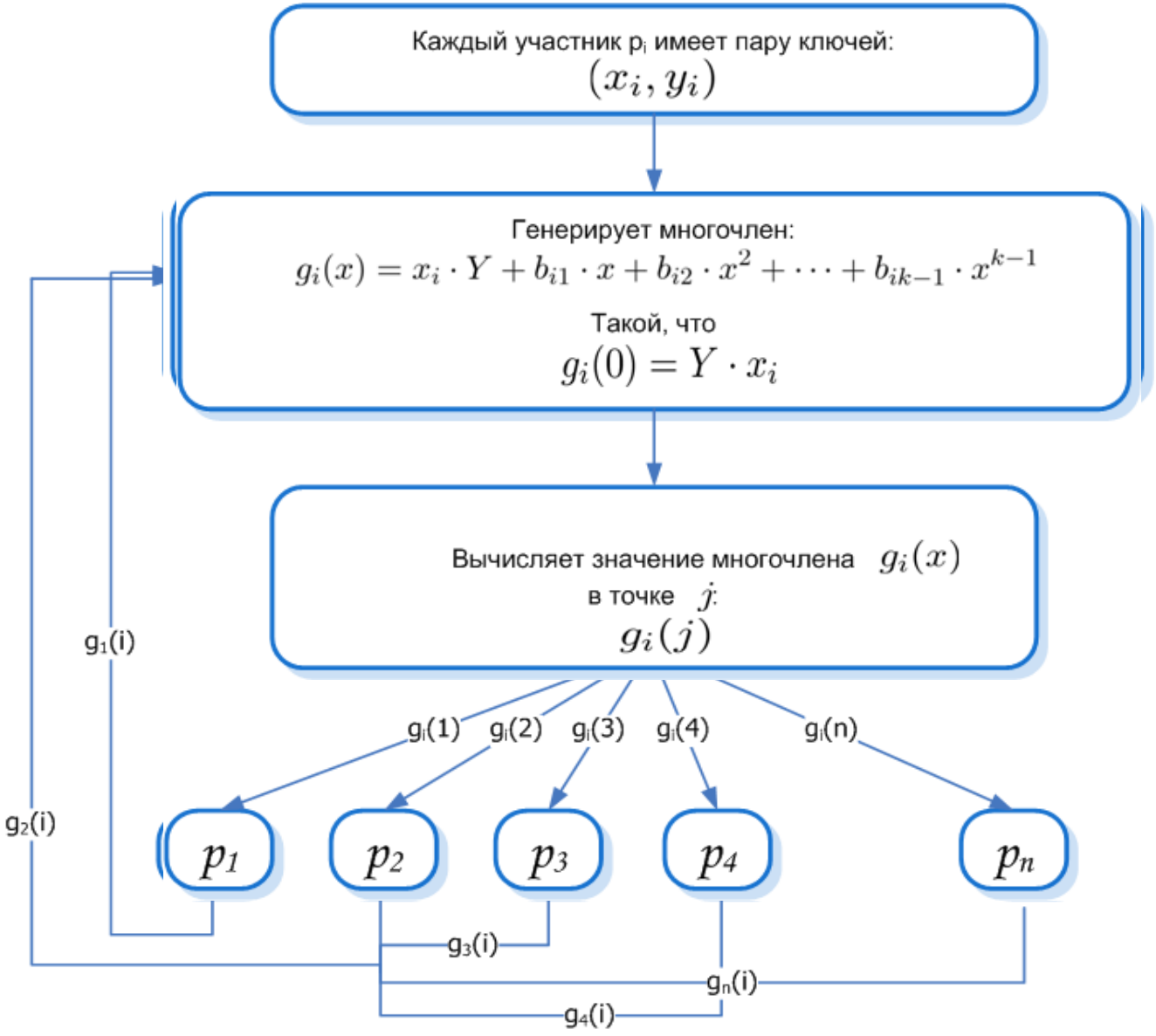
$$f_A(i)$$

Полученное значение передает i-ому участнику по секретному каналу связи

Передает ***Арбитру*** по секретному каналу связи значение старшего коэффициента

$$f_A(x)$$

Действия группы



Результат подготовки

Пусть $G(x) = f_A(x) + \sum_{i=1}^{n} g_i(x)$

Сумма многочлена оригинального подписчика и многочлена каждого участника группы

Каждый i-ый участник группы знает значение многочлена G(x) в точке i:

$$G(i) = f_A(i) + \sum_{l=1}^{n} g_l(i).$$

Секретный прокси ключ это

$$G(0) = s_A + Y \sum_{l=1}^{n} x_l$$

Подписание

- В качестве алгоритма формирования ЭЦП будем использовать алгоритм Шнорра
- Пусть k участников решили подписать сообщение. Обозначим группу **PS**
- Участники будут подписывать сообщение M
- Каждый участник группы вычисляет значение хэш-функции H(M||Y)

Подпись документа

Каждый участник p_i использует в качестве секретного ключа:

$$G(i)$$

Вырабатывает случайное число $\mathbf{k_i}$ и вычисляет:

$$S_i = k_i \cdot \prod_{j=1_{(j \neq i)}}^{k} \frac{i-j}{0-j} + G(i) \cdot H(M||Y)$$

S_i – часть подписи i-ого участника

Такой операцией каждый участник группы PS
Умножил свободный член G(x) на $H(M||Y)$ и прибавил k_i
Коэффициент при старшем члене увеличился на

$$k_i \prod_{j=1_{(j \neq i)}}^{k} \frac{1}{-j}$$

Используя алгоритм Педерсена вырабатывают общее значение K = k_1+….+k_t

Действия Арбитра

Арбитр получает от каждого участника значение

$$S_i$$

Понижает степень многочлена G(x).
Была степень n станет степень k-1

$$S_i - (a_n + K) \cdot i^n$$

Полученный многочлен обозначим G'(x)

Зная значения t-точек многочлена, Арбитр восстанавливает Значение многочлена G'(x).

G'(0) = G(0)H(M||Y)+K

Полученное значение G'(0) возвращается участникам группы, как подпись

Выводы

- Не позволяет злоупотреблять полномочиями прокси подписчику
- Проверяющий идентифицирует оригинального подписчика и исходную группу прокси подписчиков по открытому ключу:

$$Y_v = y_A \cdot R^K Y^Y$$

- Оригинальный подписчику для делегации полномочий нет необходимости создавать новые пары ключей. Таким образом разгружается Удостоверяющий центр.

Благодарю за внимание