# Диссертационная работа на тему:

## ПРОТОКОЛЫ КОЛЛЕКТИВНОЙ ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ НАД ЭЛЛИПТИЧЕСКИМИ КРИВЫМИ

**Специальность:**
05.13.01 – Системный анализ, управление и обработка информации

**Автор:** Доронин Станислав Евгеньевич
аспирант кафедры АСОИУ, ФКТИ

**Научный руководитель:**
доктор технических наук, профессор
Молдовян Николай Андреевич

Санкт-Петербургский государственный электротехнический университет
”ЛЭТИ” им. В.И.Ульянова (Ленина)

# Диссертационная работа на тему:

## ПРОТОКОЛЫ КОЛЛЕКТИВНОЙ ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ НАД ЭЛЛИПТИЧЕСКИМИ КРИВЫМИ

**Цели:**

- анализ и разработка механизмов противодействия специфическим атакам на коллективную ЭЦП
- построение схем коллективной ЭЦП с использованием эллиптических кривых
- разработка схем для защиты бумажных носителей от подделки;
- разработка подходов осуществления потенциальных атак на схемы коллективной ЭЦП и оценка стойкости разработанных схем коллективной ЭЦП;
- реализация протоколов эллиптической криптографии с использованием полей, заданных в явной векторной форме;

# Диссертационная работа на тему:

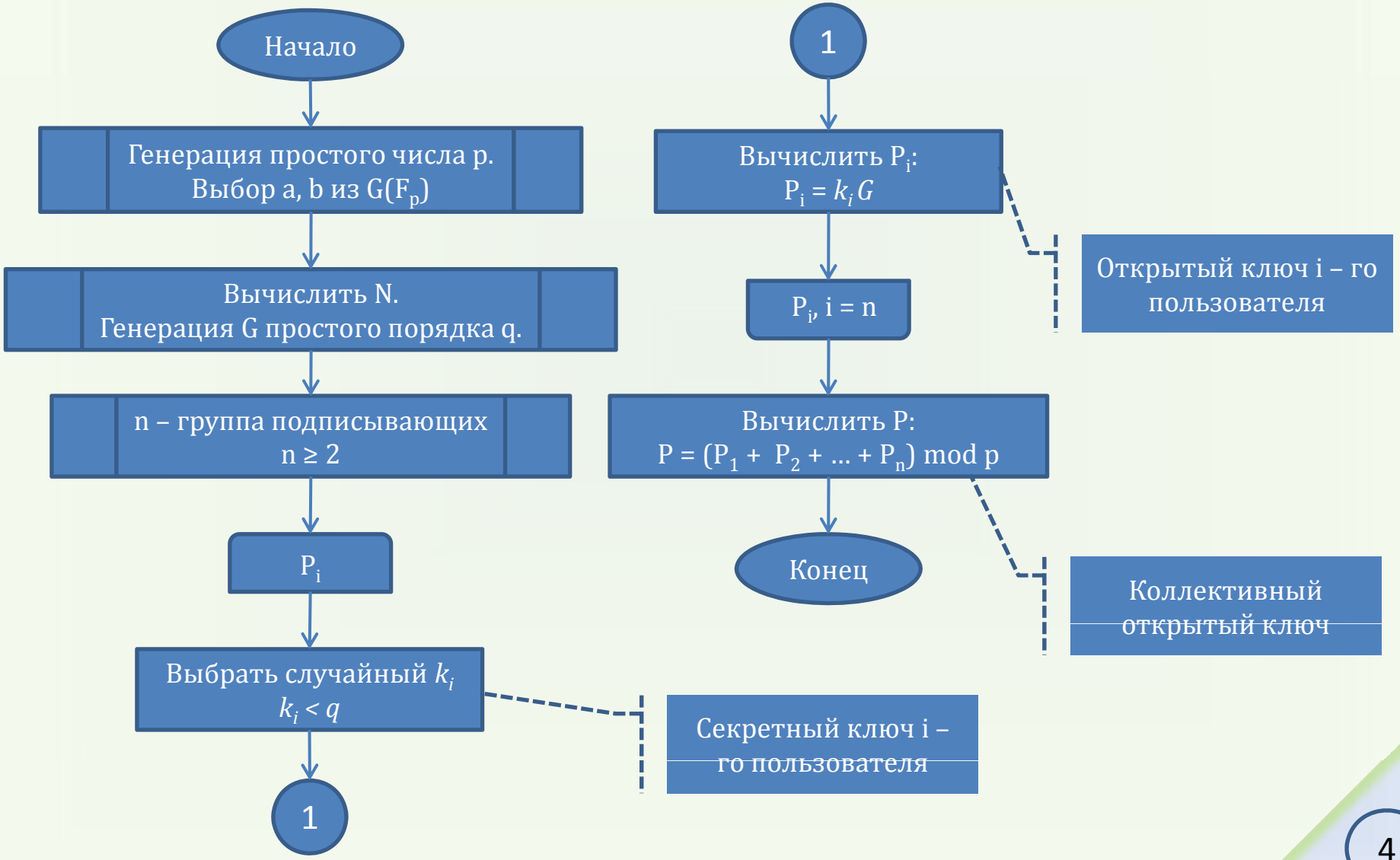
## ПРОТОКОЛЫ КОЛЛЕКТИВНОЙ ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ НАД ЭЛЛИПТИЧЕСКИМИ КРИВЫМИ

**Положения выносимые на защиту:**

- способ формирования коллективной ЭЦП, отличающийся обеспечением ее внутренней целостности
- протокол коллективной ЭЦП, отличающийся сокращением вычислительной сложности процедур ее проверки и формирования
- протокол композиционной ЭЦП, сокращающий ее размер для использования на бумажных носителях
- алгоритм построения ЭЦП, отличающийся использованием эллиптических кривых, заданных над конечными полями в явной векторной форме

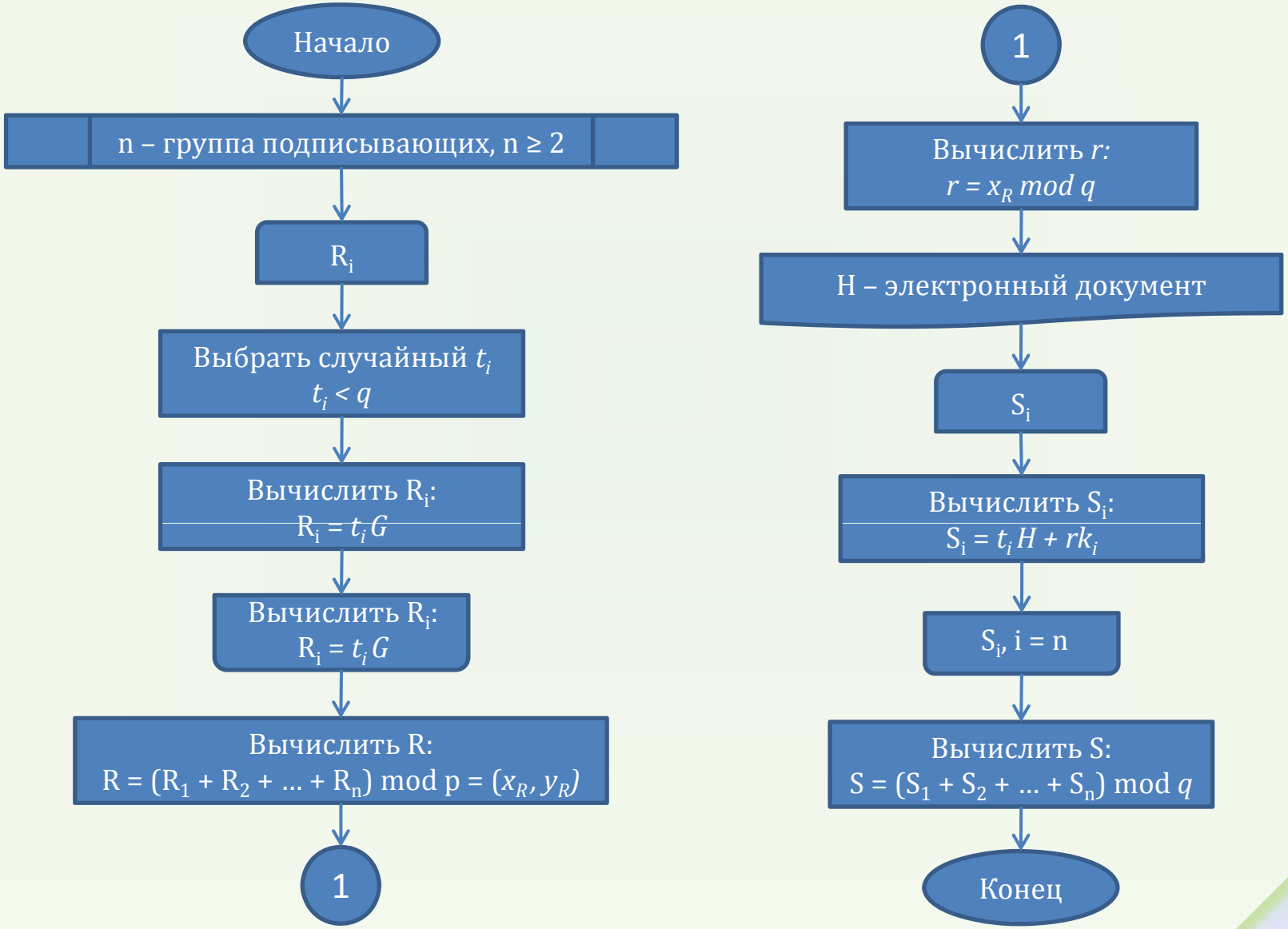
# Базовая схема КЭЦП на ЭК

## генерация ключей и системных параметров



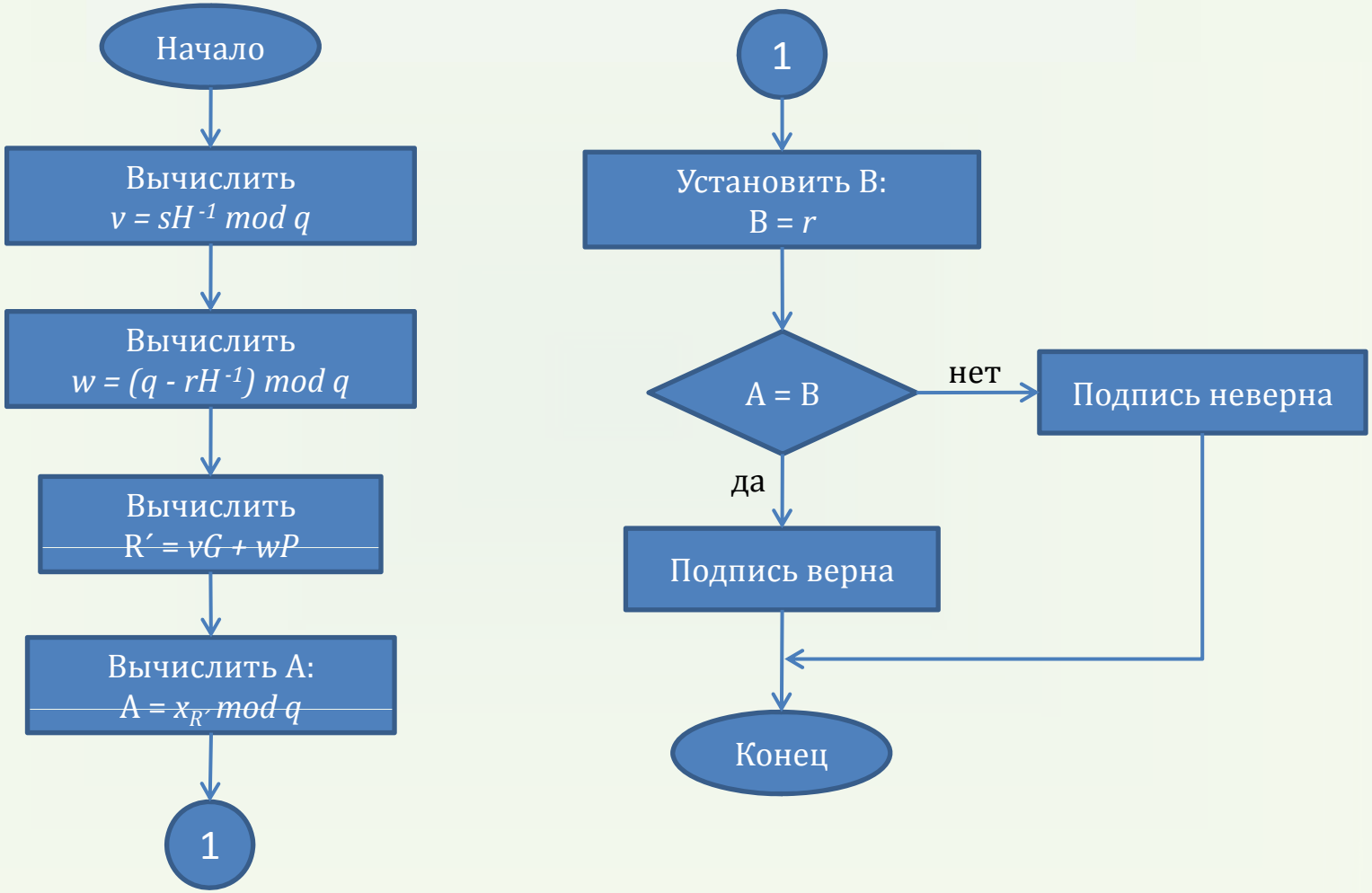
# Базовая схема КЭЦП на ЭК

подпись документа



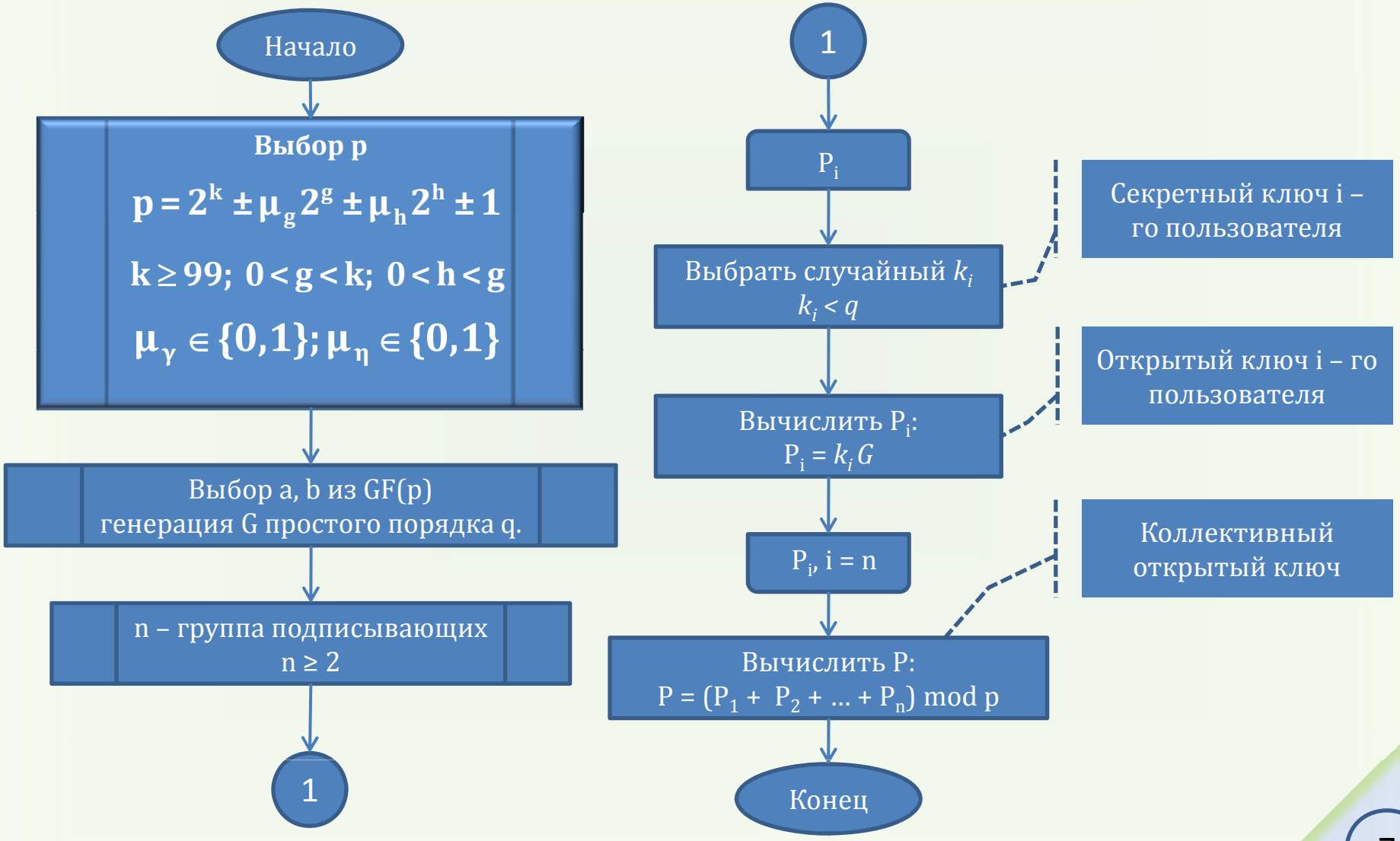
# Базовая схема КЭЦП на ЭК

## проверка подписи



# Модификация схемы КЭЦП на ЭК

## генерация ключей и системных параметров



# Модификация схемы КЭЦП на ЭК

## уменьшение временной сложности операции умножения по модулю *p*

$u_1, u_2, u_3, u_4: \quad c = ab = u_1 \| u_2 \| u_3 \| u_4$

разрядность $u_1$ не превышает значение $k + 1$ $u_2$ – $(k - g)$-разрядное число, $u_3$ – $(g - h)$-разрядное число и $u_4$ – $h$-разрядное число

$$c = u_1 \| u_2 \| u_3 \| u_4 = u_1 \cdot 2^k + u_2 \cdot 2^g + u_3 \cdot 2^h + u_4 =$$
$$= u_1 \cdot 2^k \pm u_1 \cdot 2^g \pm u_1 \cdot 2^h \pm u_1 \mp u_1 \cdot 2^g \mp u_1 \cdot 2^h \mp u_1 +$$
$$+ u_2 \cdot 2^g + u_3 \cdot 2^h + u_4 =$$
$$= u_1\left(2^k \pm 2^g \pm 2^h \pm 1\right) + \left(u_2 \mp u_1\right) \cdot 2^g + \left(u_3 \mp u_1\right) \cdot 2^h + u_4 \mp u_1.$$

$$p = 2^k \pm \mu_g 2^g \pm \mu_h 2^h \pm 1$$

$k \geq 99; \quad 0 < g < k; \quad 0 < h < g$

$\mu_g \in \{0,1\}; \mu_h \in \{0,1\}$

a, b – k-разрядные числа

$c' = u_1' \| u_2' \| u_3' \| u_4' \equiv c \bmod p$ $(g + k + 1)$-разрядное значение

разрядность $u'_1$ не превышает значение $g + 1$ $u'_2$ – $(k - g)$-разрядное число, $u'_3$ – $(g - h)$-разрядное число и $u'_4$ – $h$-разрядное число

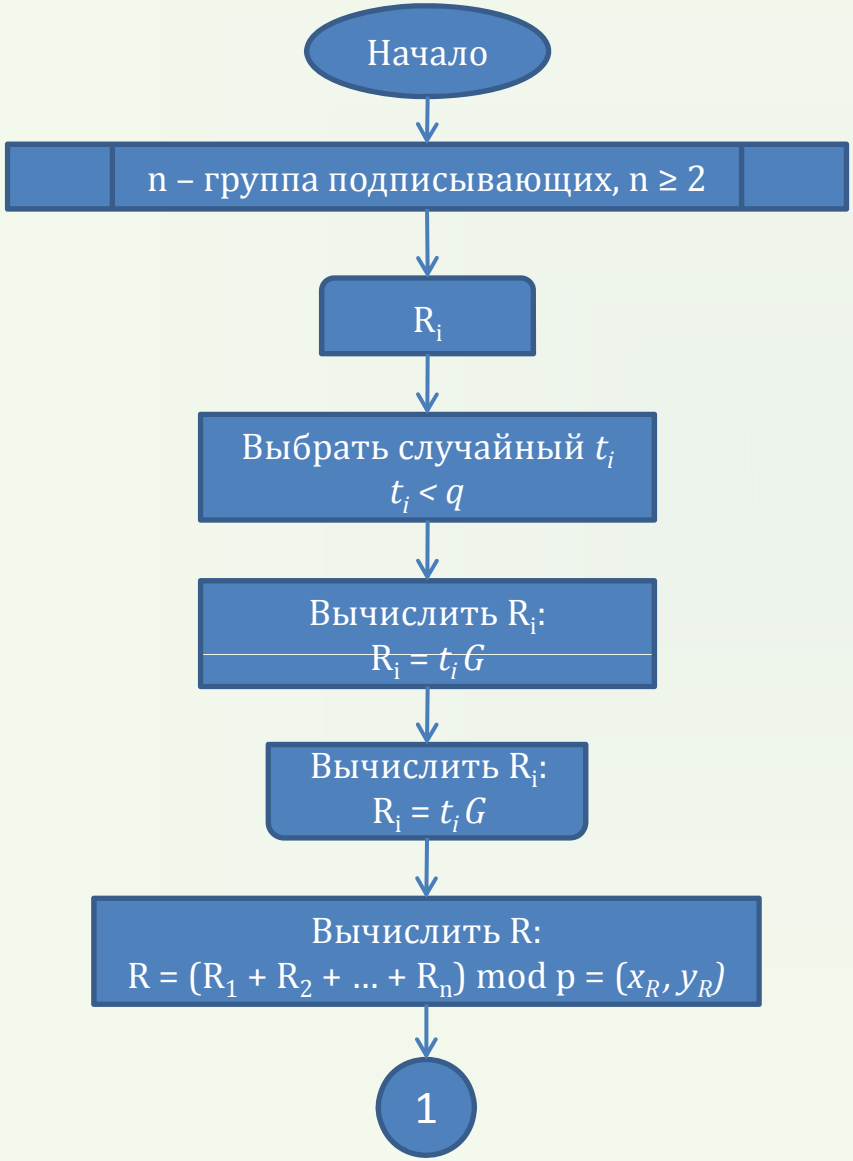
$$c' = u_1' \| u_2' \| u_3' \| u_4' = u_1' \cdot 2^k + u_2' \cdot 2^g + u_3' \cdot 2^h + u_4' =$$
$$= u_1' \cdot 2^k \pm u_1' \cdot 2^g \pm u_1' \cdot 2^h \pm u_1' \mp u_1' \cdot 2^g \mp u_1' \cdot 2^h \mp u_1' +$$
$$+ u_2' \cdot 2^g + u_3' \cdot 2^h + u_4 =$$
$$= u_1'\left(2^k \pm 2^g \pm 2^h \pm 1\right) + \left(u_2' \mp u_1'\right) \cdot 2^g + \left(u_3' \mp u_1'\right) \cdot 2^h + u_4' \mp u_1'.$$

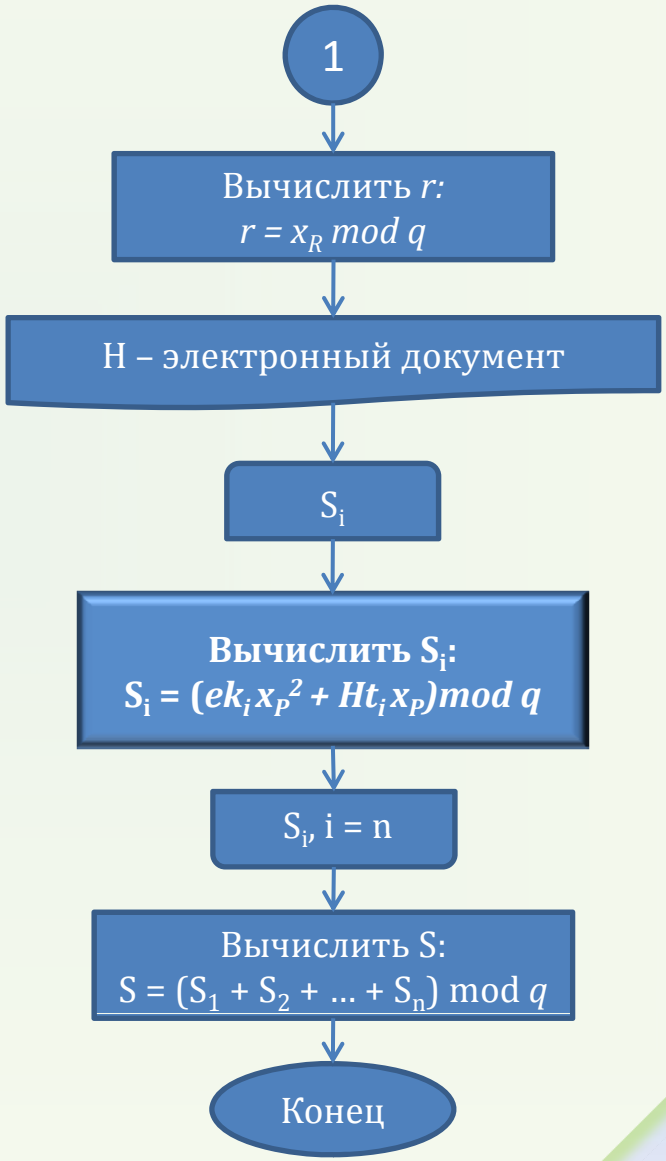
$c^*$ - $(2g + 1)$-разрядное значение, при g < k/2

$c^* = ab \bmod p$

# Модификация схемы КЭЦП на ЭК

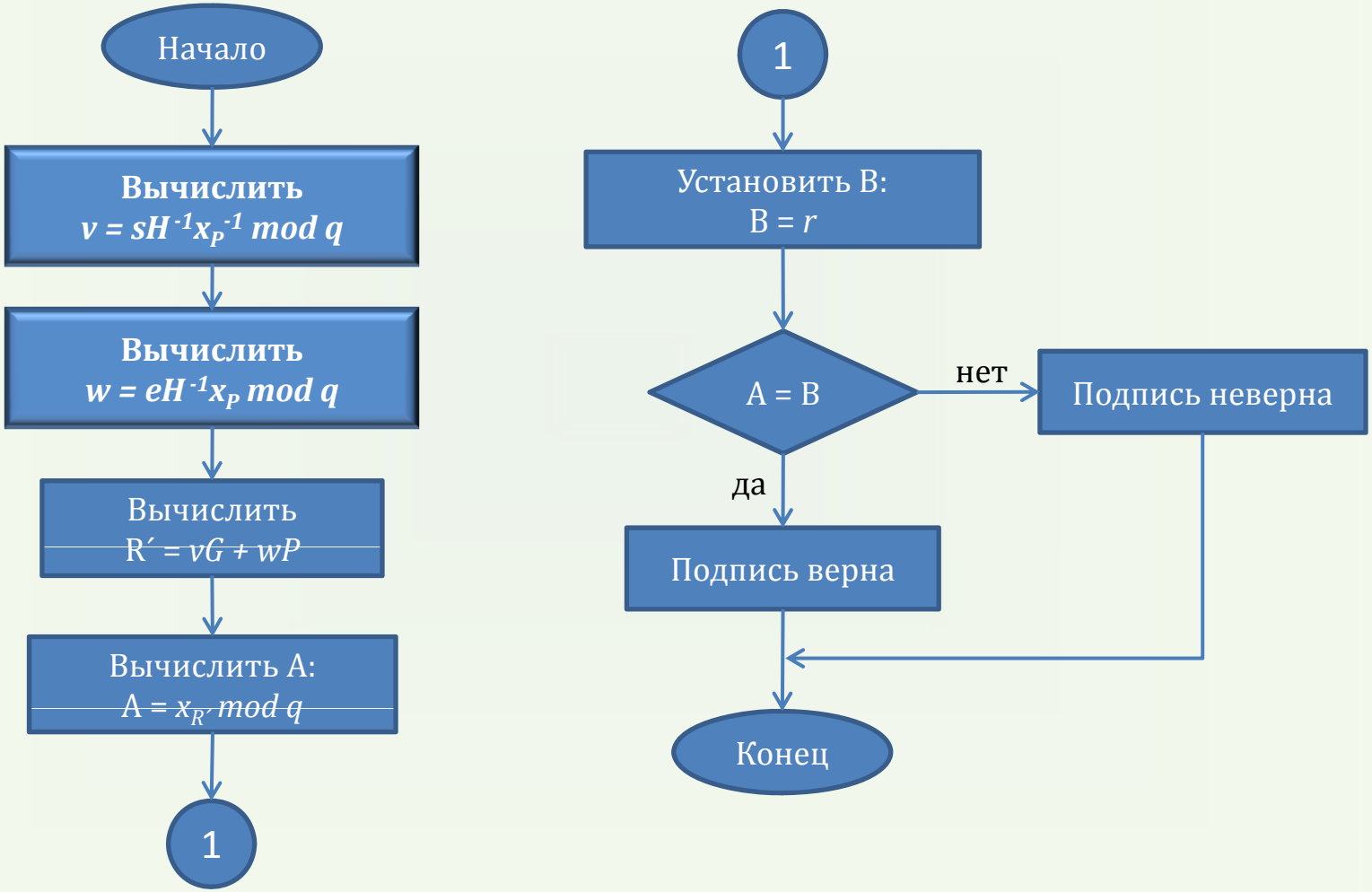
## схема коллективной ЭЦП зависимой от открытого ключа



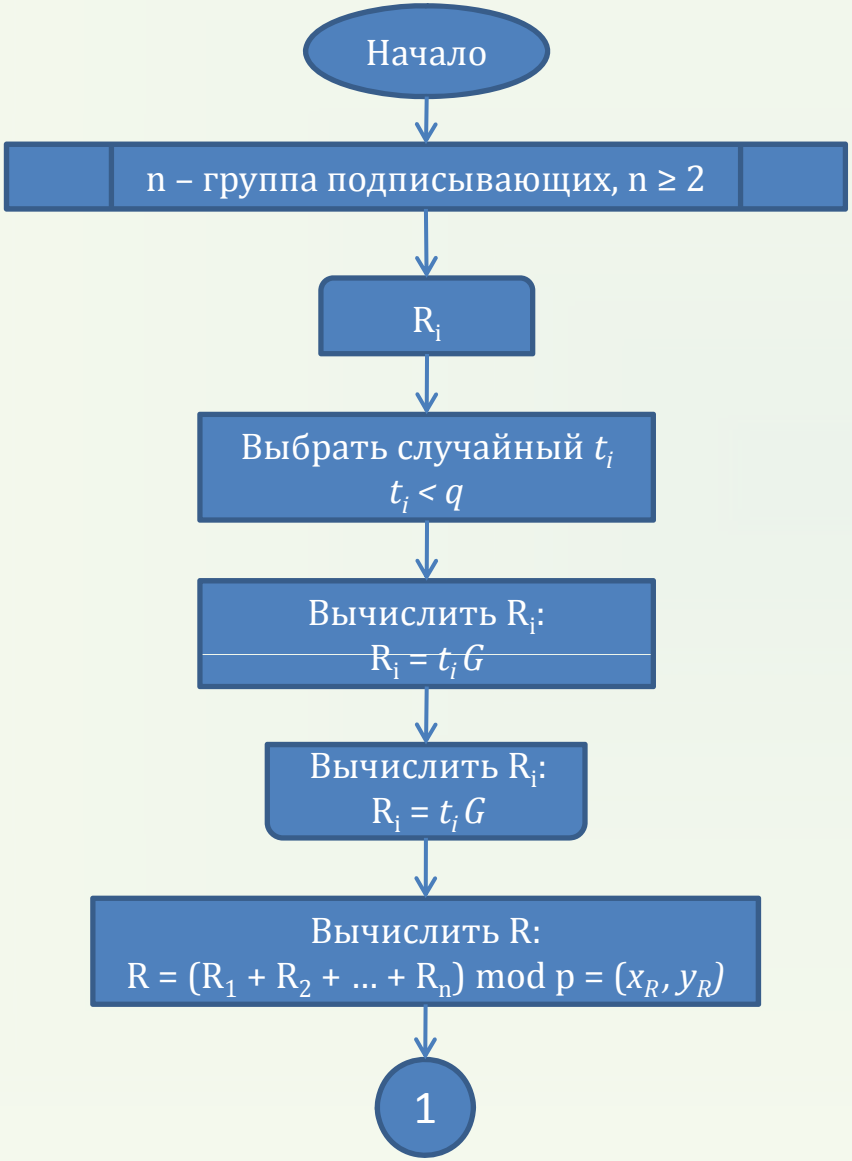
# Модификация схемы КЭЦП на ЭК

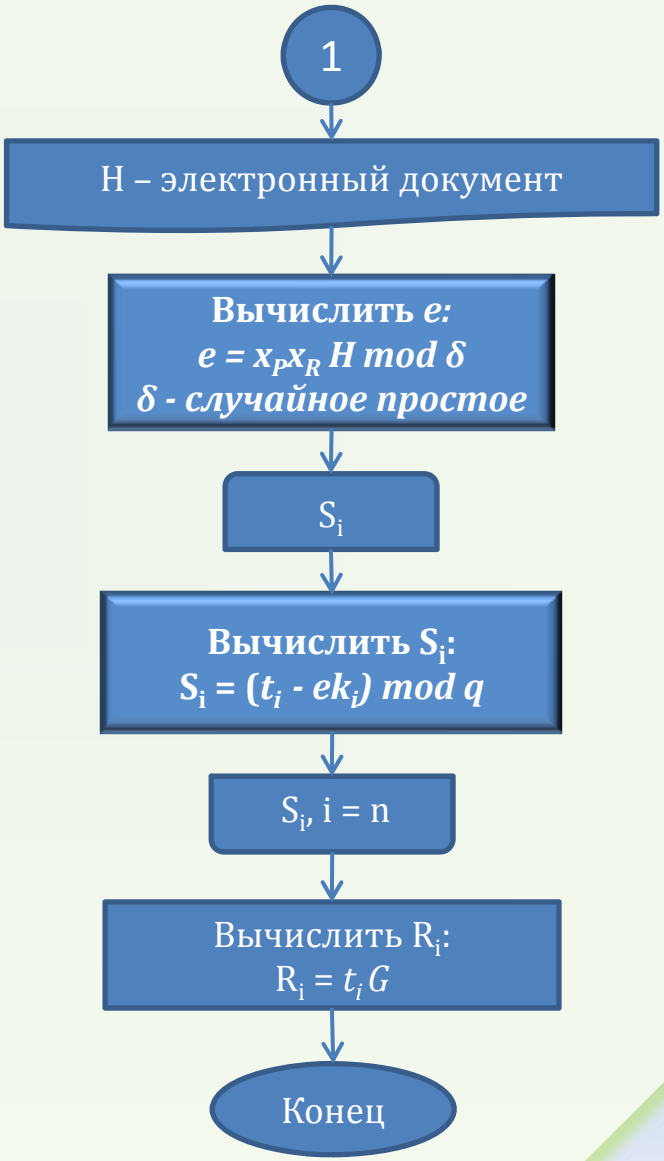
## схема коллективной ЭЦП зависимой от открытого ключа



# Модификация схемы КЭЦП на ЭК

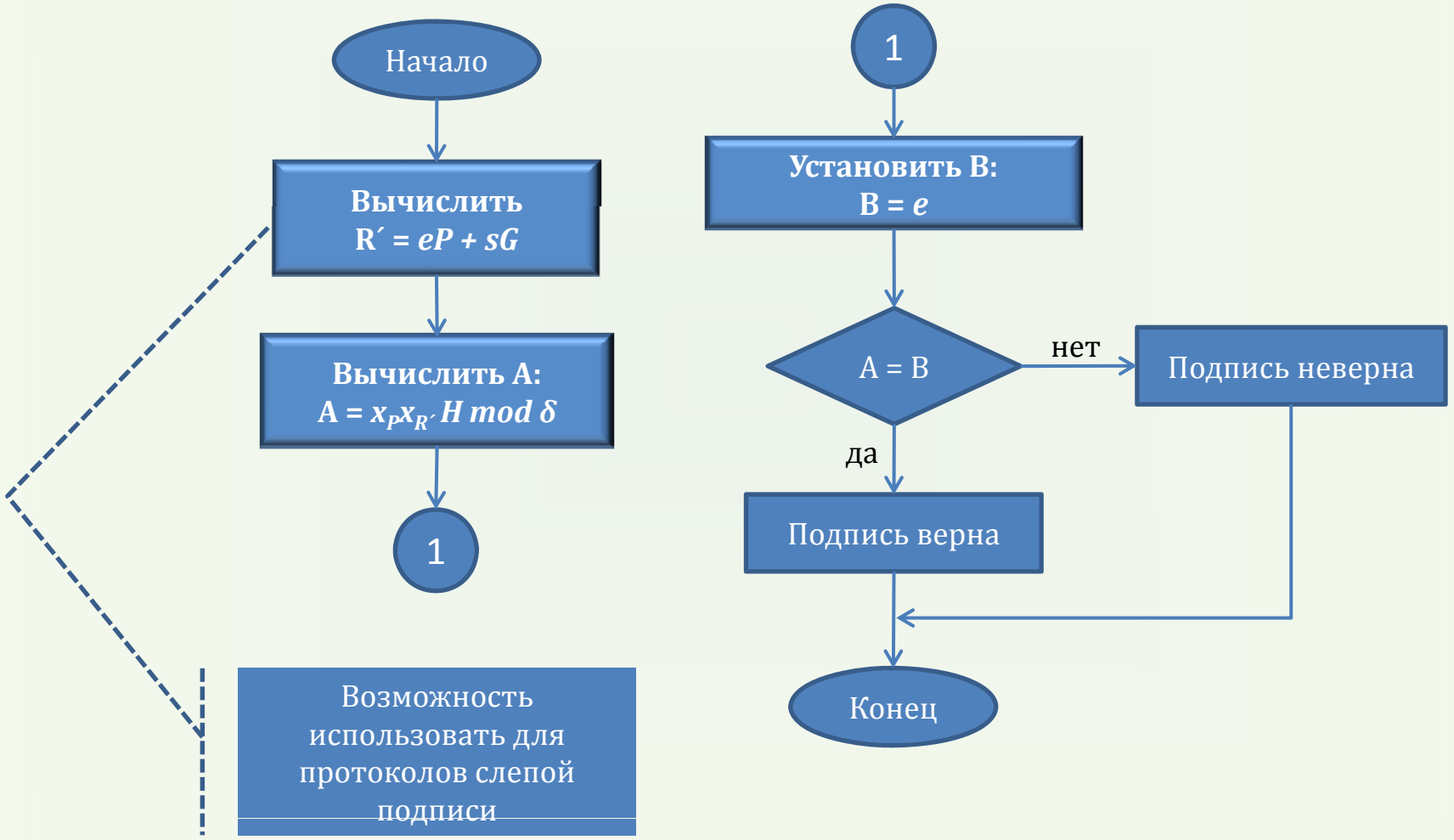
## схема коллективной ЭЦП зависимой от открытого ключа



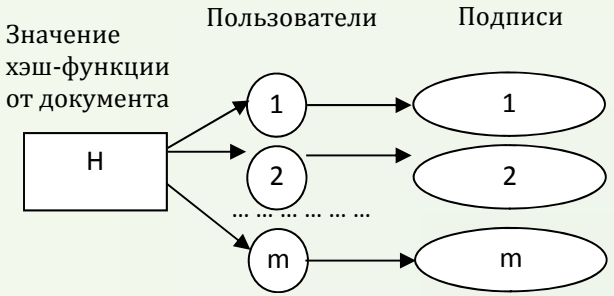



# Модификация схемы КЭЦП на ЭК

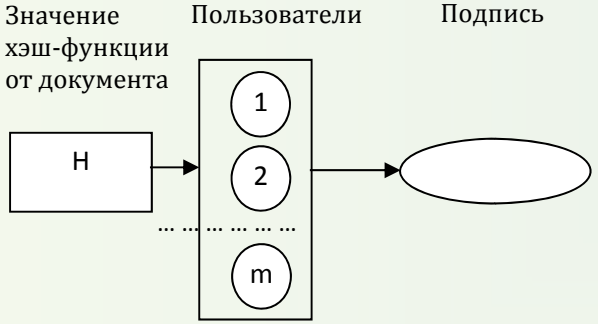
## схема коллективной ЭЦП зависимой от открытого ключа



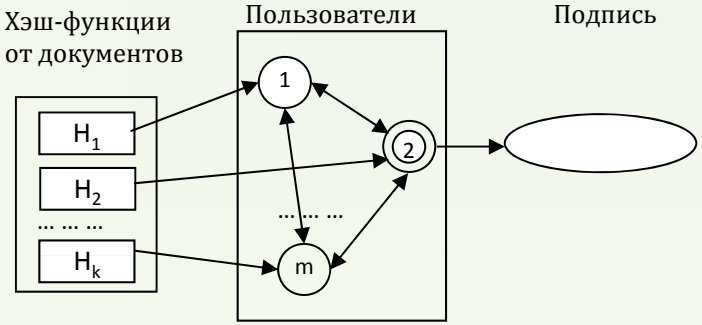
# Композиционная подпись




Заверение документа коллективом субъектов с использованием обычной схемы ЭЦП



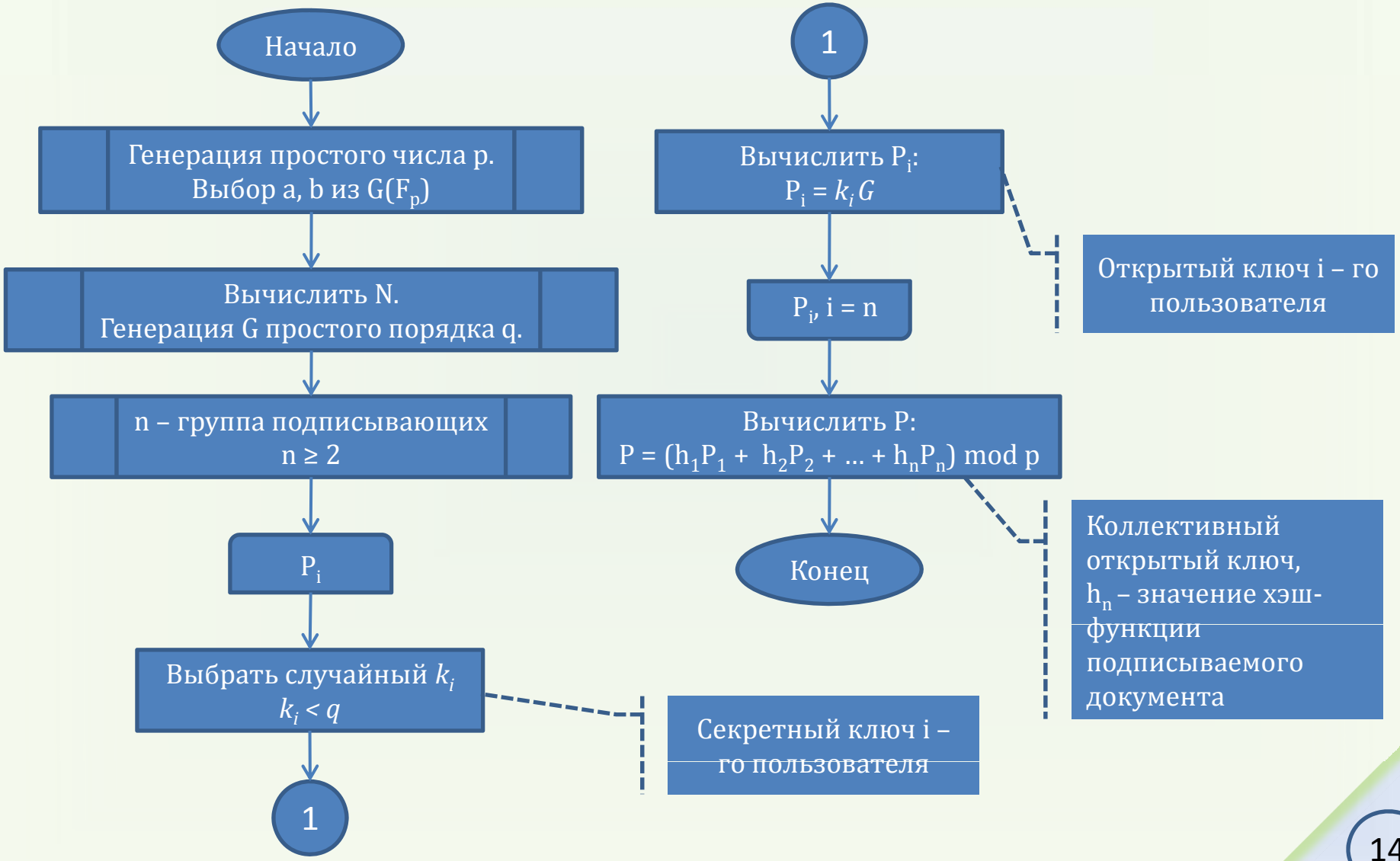

Заверение документа коллективом субъектов с использованием коллективной подписи




Заверение документа коллективом субъектов с использованием композиционной подписи

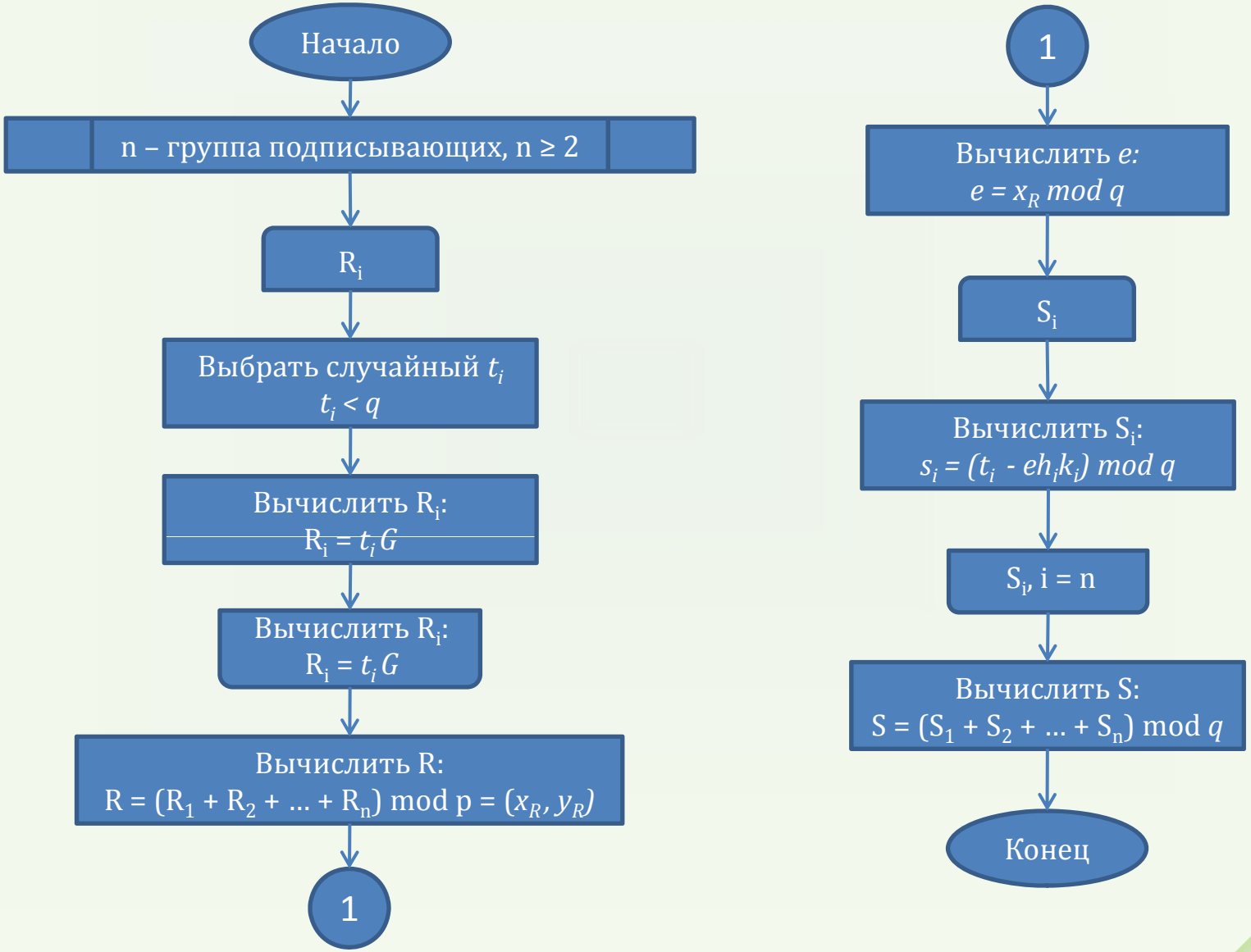
# Схема композиционной подписи на ЭК

## генерация ключей и системных параметров



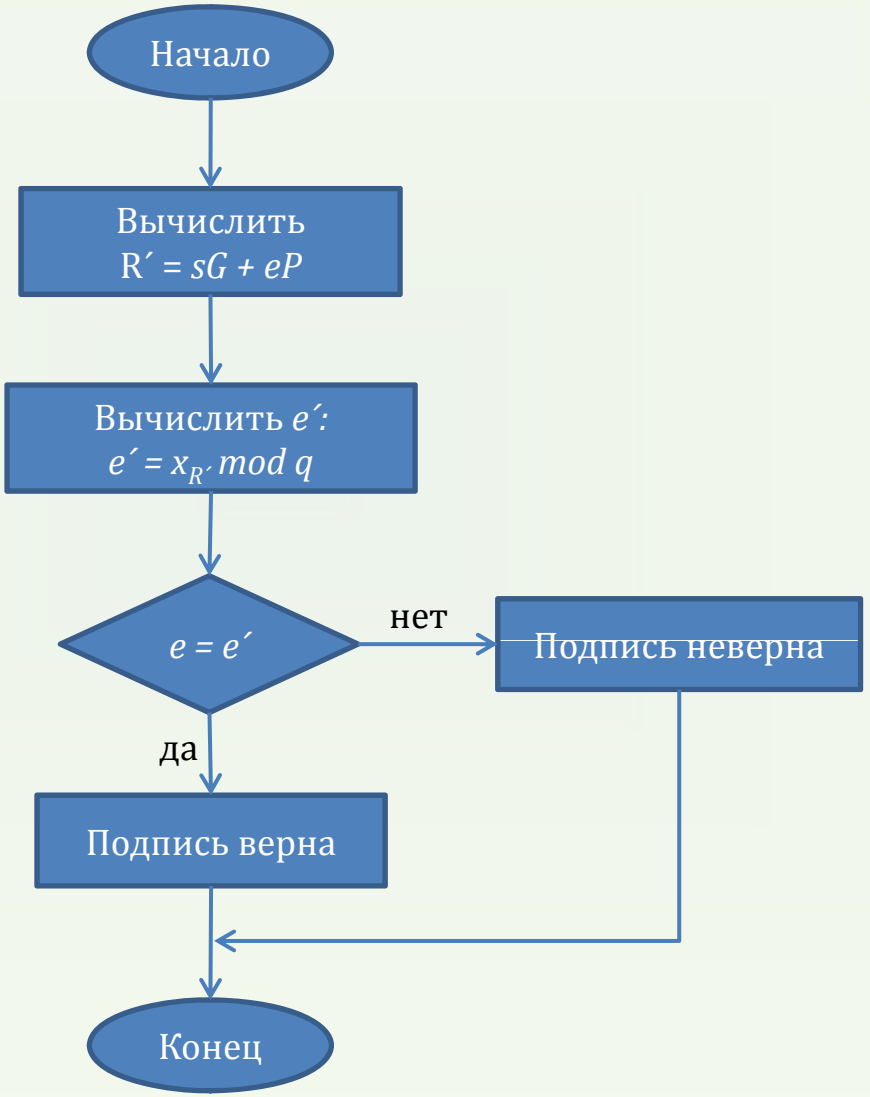
# Схема композиционной подписи на ЭК

подпись документа



# Схема композиционной подписи на ЭК

## проверка подписи



# Атаки на электронную цифровую подпись стойкость коллективной ЭЦП

**Стойкость КЭЦП**

- лобовая атака
- слабость хэш – функции
- подделка ЭЦП

m – пользователей, m - 1 нарушителей $Q_1, Q_2, \ldots, Q_m$

$$Q_{\text{кол}} = Q_m + Q' \qquad Q' = \sum_{i=1}^{m-1} Q_i \qquad R = x_C \bmod q$$

$$C = ((Se^{-1}) \bmod q)G + ((q - R)e^{-1} \bmod q)(Q' + Q_m)$$

$$(R^*, S^*) \quad Q^* = Q' + Q'_m \qquad Q'_m = Q_m - Q'$$

$$C^* = ((S^* e^{-1}) \bmod q)G + ((q - R^*)e^{-1} \bmod q)Q^* =$$

$$= ((S^* e^{-1}) \bmod q)G + ((q - R^*)e^{-1} \bmod q)(Q' + Q'_m) \Rightarrow$$

$$\Rightarrow C^* = ((S^* e^{-1}) \bmod q)G + ((q - R^*)e^{-1} \bmod q)Q_m$$

$(R^*, S^*)$ - подлинная индивидуальная подпись $m$-ого пользователя

# Атаки на электронную цифровую подпись
## подделка коллективной ЭЦП

m – пользователей $Q_1, Q_2, \ldots, Q_m$

$$R = x_C \bmod q$$

$$Q_i = (Rd_i + k_i e) \bmod q$$

$$Q_x = (Rd_x + k_x e) \bmod q$$

$$Q^* = Q_x - \sum_{i=1}^{m-1} Q_i$$

$$Q = \sum_{i=1}^{m} Q_i = Q^* + \sum_{i=1}^{m-1} Q_i = Q_x - \sum_{i=1}^{m-1} Q_i + \sum_{i=1}^{m-1} Q_i = Q^*$$

# Конечные расширенные поля векторов над полем $GF(p)$

$a\cdot\mathbf{e} + b\cdot\mathbf{i} + \ldots + c\cdot\mathbf{j}$ **e**, **i**, … **j** -- базисные вектора, представленные в виде набора координат $(a,b,\ldots,c)$, являющихся элементами конечного поля $GF(p)$

Операция сложения: $(a,b,\ldots,c) + (x,y,\ldots,z) = (a + x, b + y, \ldots, c + z)$

Операция умножения: $(a\cdot\mathbf{e} + b\cdot\mathbf{i} + \ldots + c\cdot\mathbf{j})(x\cdot\mathbf{e} + y\cdot\mathbf{i} + \ldots + z\cdot\mathbf{j}) = ax\cdot\mathbf{ee} + ay\cdot\mathbf{ei} + \ldots$
$+ az\cdot\mathbf{ej} + \quad + bx\cdot\mathbf{ie} + by\cdot\mathbf{ii} + \ldots + bz\cdot\mathbf{ij} + \ldots + cx\cdot\mathbf{je} + cy\cdot\mathbf{ji} + \ldots + cz\cdot\mathbf{jj}$ , где **ee**, **ei**, **ej**, **ie**, **ii**, …**ij**, …**je**, **ji**, …**jj** – заменяются на $\varepsilon\mathbf{v}$, где $\varepsilon$ - структурный коэффициент из поля GF(p), **v** – табличный вектор

Сравним сложность умножения в $GF(p^m)$ и $\boldsymbol{Z}_{p'}$, где $|p'| = m|p|$,$|p|$ - битовая длина числа $p$

$GF(p^m)$ включает $m^2$ операций умножения в поле $GF(p)$, сложность пропорциональна $|p|^2$ и приблизительно равна сложности в $\boldsymbol{Z}_{p'}$

$m^2$ операций арифметического умножения и
$m$ операций деления чисел на модуль $p$

Рассмотрим сложность умножения в поле $GF(p^m)$, заданном в виде конечного кольца многочленов степени $m - 1$

$m^2$ операций арифметического умножения $|p|$-битовых чисел и
$m$ операций деления $2|p|$-битовых чисел на модуль $p$

# Таблицы умножения базисных векторов

| × | *e* | *i* | *j* | *k* |
|---|---|---|---|---|
| ***e*** | **e** | **i** | **j** | **k** |
| ***i*** | **i** | ε·**j** | ε·**k** | ε·**e** |
| ***j*** | **j** | ε·**k** | ε·**e** | **i** |
| ***k*** | **k** | ε·**e** | **i** | ε·**j** |

m = 4; ε, μ ∈ $GF(p)$

| × | *e* | *i* | *j* | *k* | *v* | *w* |
|---|---|---|---|---|---|---|
| ***e*** | **e** | **i** | **j** | **k** | **u** | **v** |
| ***i*** | **i** | ε·**j** | ε·**k** | **u** | ε·**v** | ε·**e** |
| ***j*** | **j** | ε·**k** | μ·**u** | **v** | ε·**e** | μ·**i** |
| ***k*** | **k** | **u** | **v** | **e** | **i** | **j** |
| ***u*** | **u** | ε·**v** | ε·**e** | **i** | ε·**j** | ε·**k** |
| ***v*** | **v** | ε·**e** | μ·**i** | **j** | ε·**k** | μ·**u** |

m = 6; ε, μ ∈ $GF(p)$

| × | *e* | *i* | *j* | *k* | *u* |
|---|---|---|---|---|---|
| ***e*** | **e** | **i** | **j** | **k** | **u** |
| ***i*** | **i** | ε·**j** | ε·**k** | ε·**u** | ε·**e** |
| ***j*** | **j** | ε·**k** | ε·**u** | ε·**e** | μ·**i** |
| ***k*** | **k** | ε·**u** | ε·**e** | **i** | **J** |
| ***u*** | **u** | ε·**e** | μ·**i** | **j** | μ·**k** |

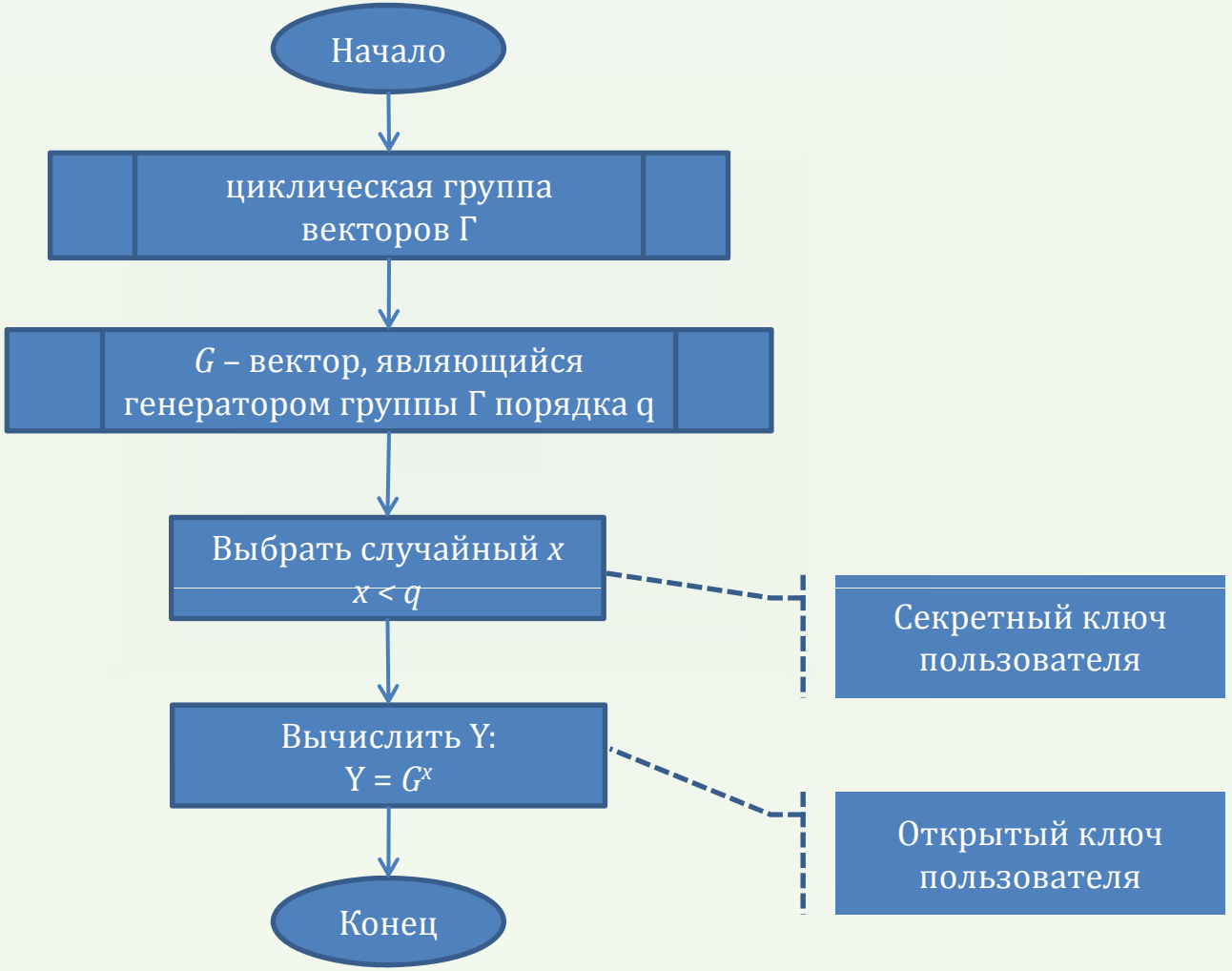
m = 5; ε, μ ∈ $GF(p)$

| × | *e* | *i* | *j* | *k* | *u* | *v* | *w* |
|---|---|---|---|---|---|---|---|
| ***e*** | **e** | **i** | **j** | **k** | **u** | **v** | **w** |
| ***i*** | **i** | ε·μ·**k** | ε·μ·**v** | μ·τ·**u** | ε·μ·**w** | ε·μ·τ·**e** | μ·τ·**j** |
| ***j*** | **j** | ε·μ·**v** | ε·**u** | ε·μ·τ·**e** | ε·**i** | ε·**w** | ε·**k** |
| ***k*** | **k** | μ·τ·**u** | ε·μ·τ·**e** | μ·τ·**w** | μ·τ·**j** | τ·**i** | μ·τ·**v** |
| ***u*** | **u** | ε·μ·**w** | ε·**i** | μ·τ·**j** | ε·μ·**v** | ε·**k** | ε·μ·τ·**e** |
| ***v*** | **v** | ε·μ·τ·**e** | ε·**w** | τ·**i** | ε·**k** | τ·**j** | τ·**u** |
| ***w*** | **w** | μ·τ·**j** | ε·**k** | μ·τ·**v** | ε·μ·τ·**e** | τ·**u** | τ·**v** |

m = 7; ε, μ ∈ $GF(p)$

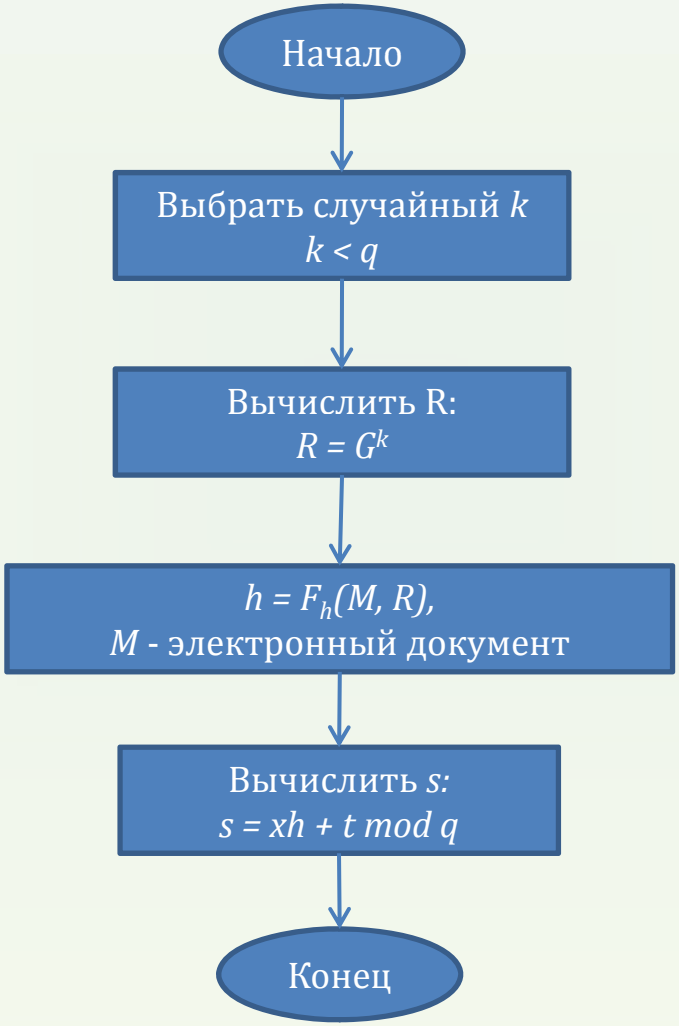
# Схема подписи над векторными полями

## генерация ключей и системных параметров



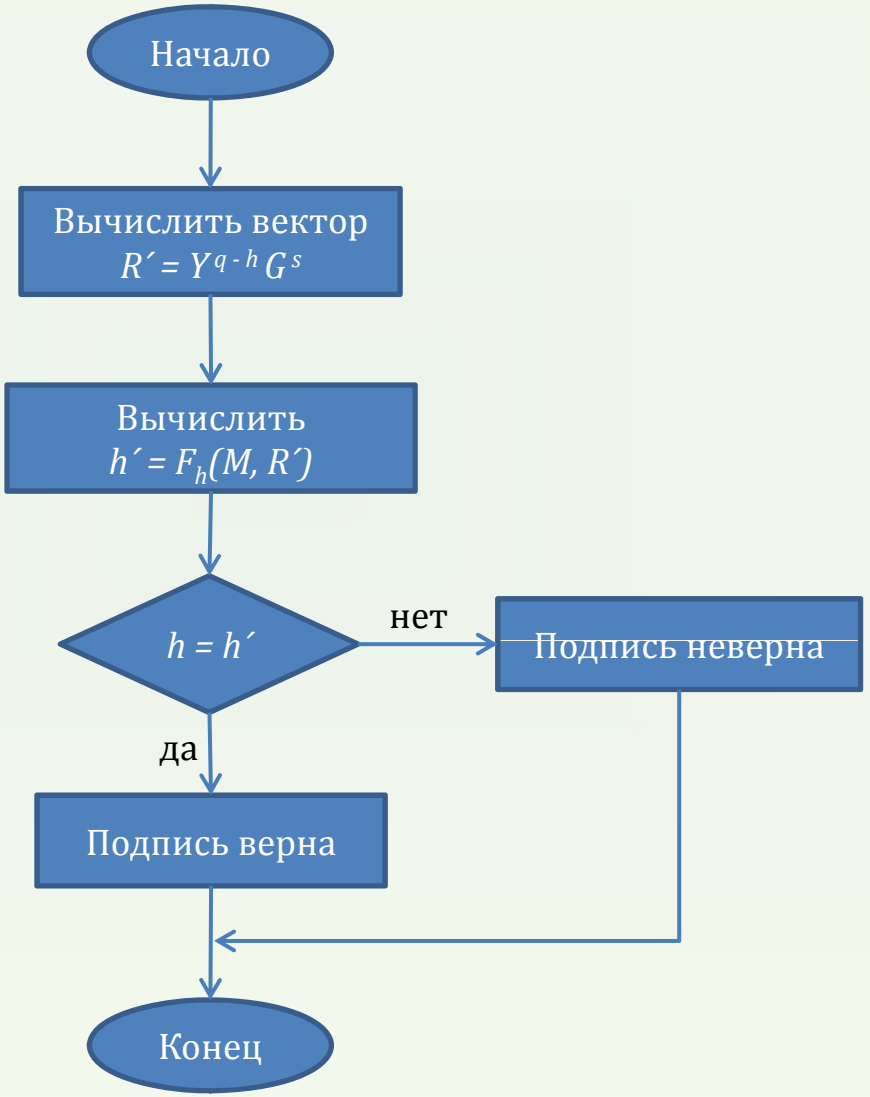
# Схема подписи над векторными полями

подпись документа



# Схема подписи над векторными полями

## проверка подписи



# Диссертационная работа на тему:
## ПРОТОКОЛЫ КОЛЛЕКТИВНОЙ ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ НАД ЭЛЛИПТИЧЕСКИМИ КРИВЫМИ

**Основные результаты:**

- протоколы коллективной ЭЦП, в которых задается зависимость подписи от открытого ключа, сформированного подписывающим коллективом, что позволяет обеспечить внутреннюю целостность используемой коллективной ЭЦП;
- механизмы формирования схем коллективной ЭЦП, используя модуль особого вида, позволяющий снизить временную сложность процедур проверки и формирования подписи;
- протокол композиционной ЭЦП, базирующийся на сложности задачи дискретного логарифмирования в группе точек эллиптической кривой, для обеспечения криптографической защиты бумажных документов;

# Диссертационная работа на тему:
## ПРОТОКОЛЫ КОЛЛЕКТИВНОЙ ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ НАД ЭЛЛИПТИЧЕСКИМИ КРИВЫМИ

**Основные результаты:**

- алгоритмы модификации криптографических процедур для противодействия атакам на протоколы коллективной ЭЦП, а так же была формально доказана криптографическая стойкость применяемых схем ЭЦП, сводимая к стойкости базовых методов положенных в их основу;
- обоснована перспективность использования конечных векторных полей для построения схем ЭЦП на эллиптических кривых, для ускорения механизмов проверки и формирования подписи за счет распараллеливания ресурсоемких операций;

# Диссертационная работа на тему:
## ПРОТОКОЛЫ КОЛЛЕКТИВНОЙ ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ НАД ЭЛЛИПТИЧЕСКИМИ КРИВЫМИ

**Апробация результатов работы:**

- V Санкт-Петербургская межрегиональная конференция «Информационная безопасность регионов России (ИБРР-2007)». С-Петербург, 23-25 октября 2007 г.
- Инновационная деятельность в Вооруженных силах Российской Федерации: Труды всеармейской научно-практической конференции, 22-23 ноября 2007 г.
- XI Санкт-Петербургская международная конференция Региональная информатика-2008 (РИ-2008) СПб, 22-24 октября 2008 г.
- VI Санкт-Петербургской межрегиональной конференции «Информационная безопасность регионов России (ИБРР-2009)». С-Петербург, 28-30 октября.
- XV Санкт-Петербургская Ассамблея молодых учёных и специалистов и Международная научно-практическая конференция XXXIX НЕДЕЛЯ НАУКИ СПбГПУ. 7 декабря 2010 г.

# Диссертационная работа на тему:
## ПРОТОКОЛЫ КОЛЛЕКТИВНОЙ ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ НАД ЭЛЛИПТИЧЕСКИМИ КРИВЫМИ

**Публикации:**


• Доронин С.Е., Молдовяну П.А., Синев В.Е. Векторные конечные поля: задание умножения векторов большой четной размерности // Вопросы защиты информации. 2008. № 4(83). С.2-7.

• Доронин С.Е., Молдовян Н.А., Синев В.Е. Конечные расширенные поля для алгоритмов электронной цифровой подписи // Информационно-управляющие системы. 2009. № 1. С. 33-40.

• Молдовян Н.А., Морозова Е.В., Костин А.А., Доронин С.Е. Системы композиционной электронной цифровой подписи // Программные продукты и системы. 2008. № 4. С. 161-164.

• Галанов А.И., Доронин С.Е., Костин А.А., Молдовян У.А. Протокол слепой коллективной подписи на основе сложности задачи дискретного логарифмирования // Инновационная деятельность в Вооруженных силах Российской Федерации: Труды всеармейской научно-практ. конференции, 10-11 декабря 2009, г. С-Петербург. СПб.: ВАС, 2009. С. 163-168

• Доронин С.Е., Еремеев М.А., Молдовян А.А. реализация коллективной подписи на основе задач дискретного логарифмирования в мультипликативной группе и на эллиптической кривой // V С-Петербургская межрегиональная конференция «Информационная безопасность регионов России (ИБРР-2007)». С-Петербург, 23-25 октября 2007 г. / Труды конф. СПб, 2008. с.177-180.

• Доронин С.Е., Молдовян Н.А., Молдовяну П.А.. Схемы коллективной подписи на основе задач дискретного логарифмирования // Инновационная деятельность в Вооруженных силах Российской Федерации: Труды всеармейской научно-практ. конф. 22-23 ноября 2007 г., С-Петербург. СПб.: ВАС, 2007. С.242-246.