

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

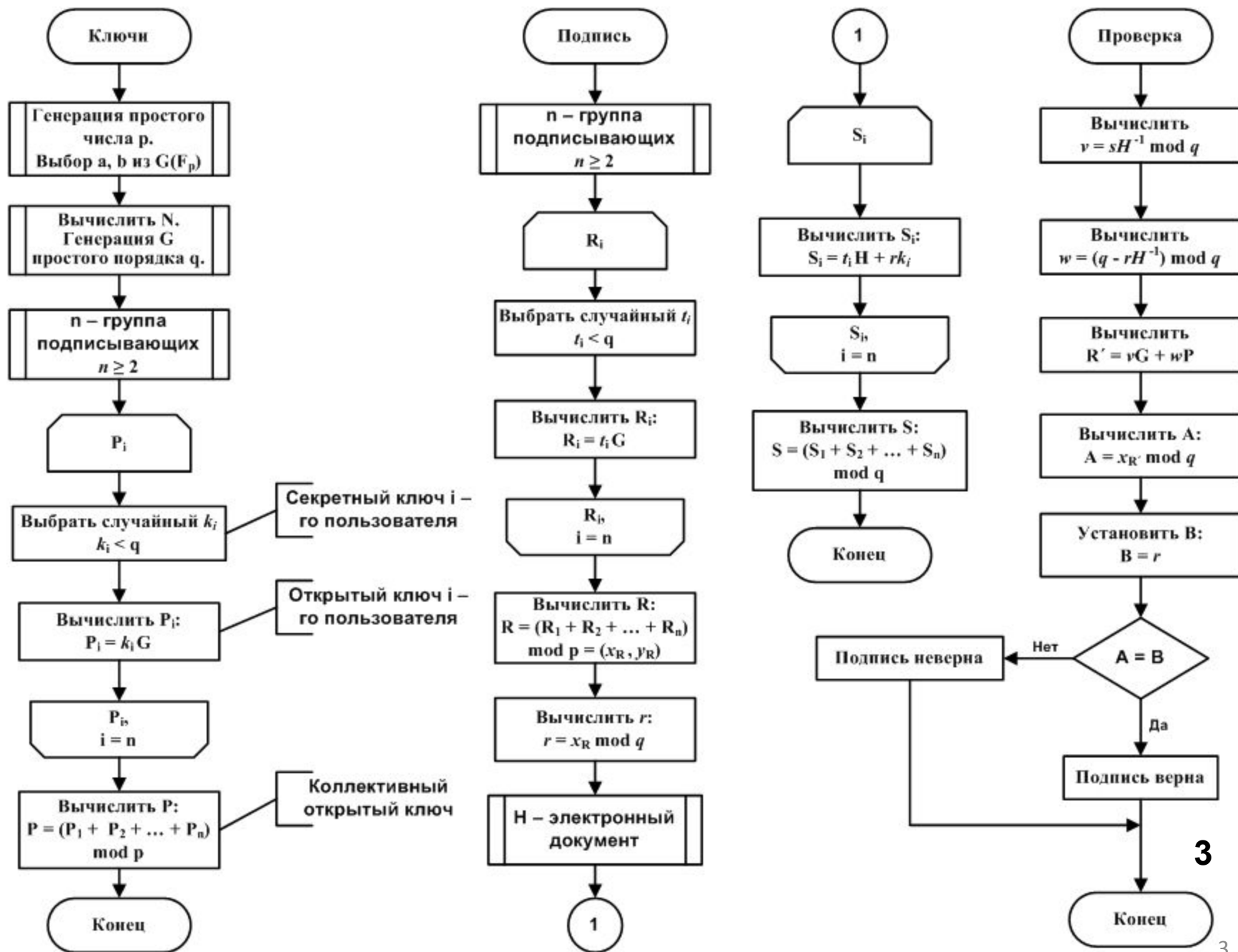
Цели:

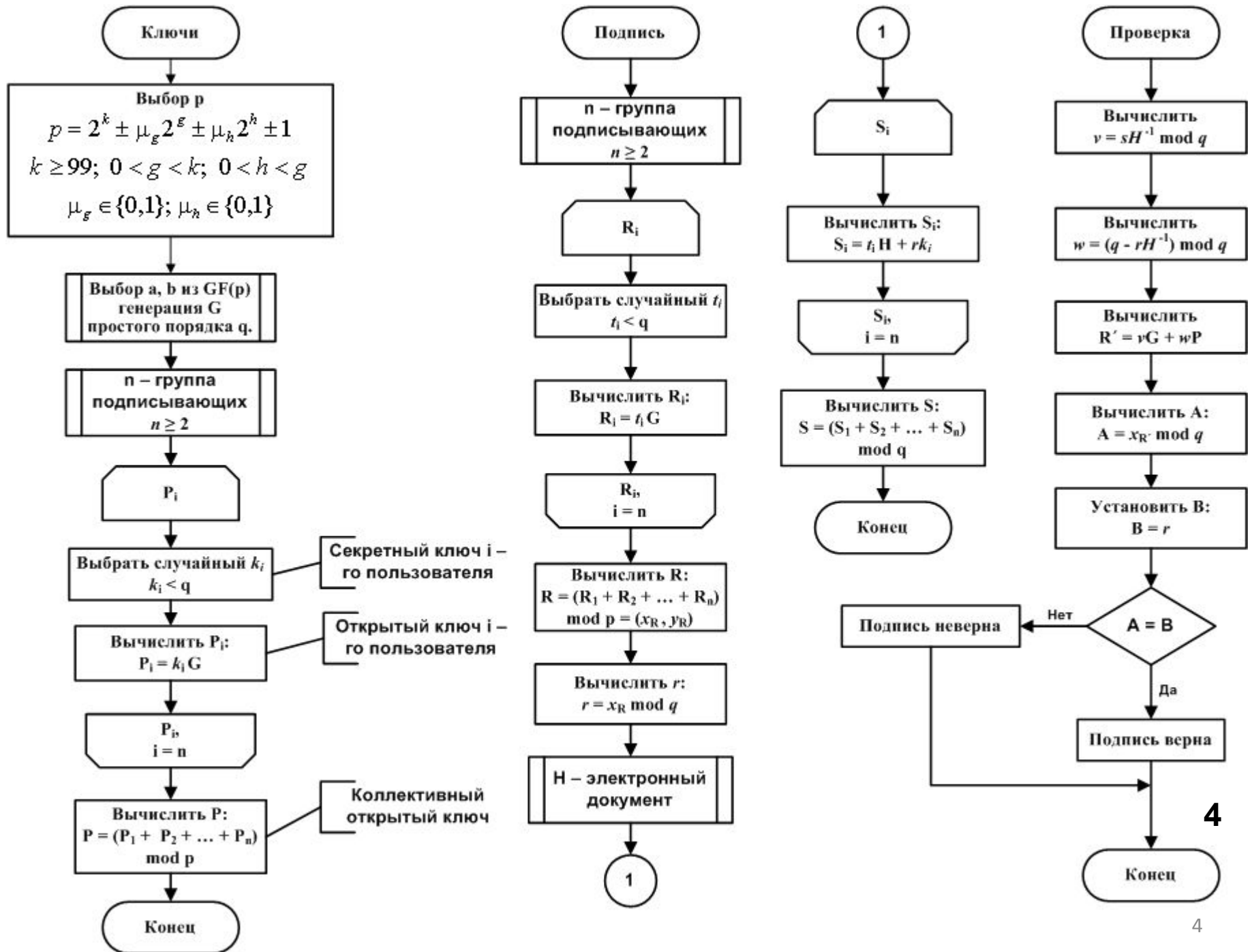
- анализ и разработка механизмов противодействия специфическим атакам на коллективную ЭЦП
- построение схем коллективной ЭЦП с использованием эллиптических кривых
- разработка схем потенциальных атак на разработанные схемы коллективной ЭЦП и оценка стойкости разработанных схем коллективной ЭЦП
- реализация протоколов эллиптической криптографии с использованием полей, заданных в явной векторной форме

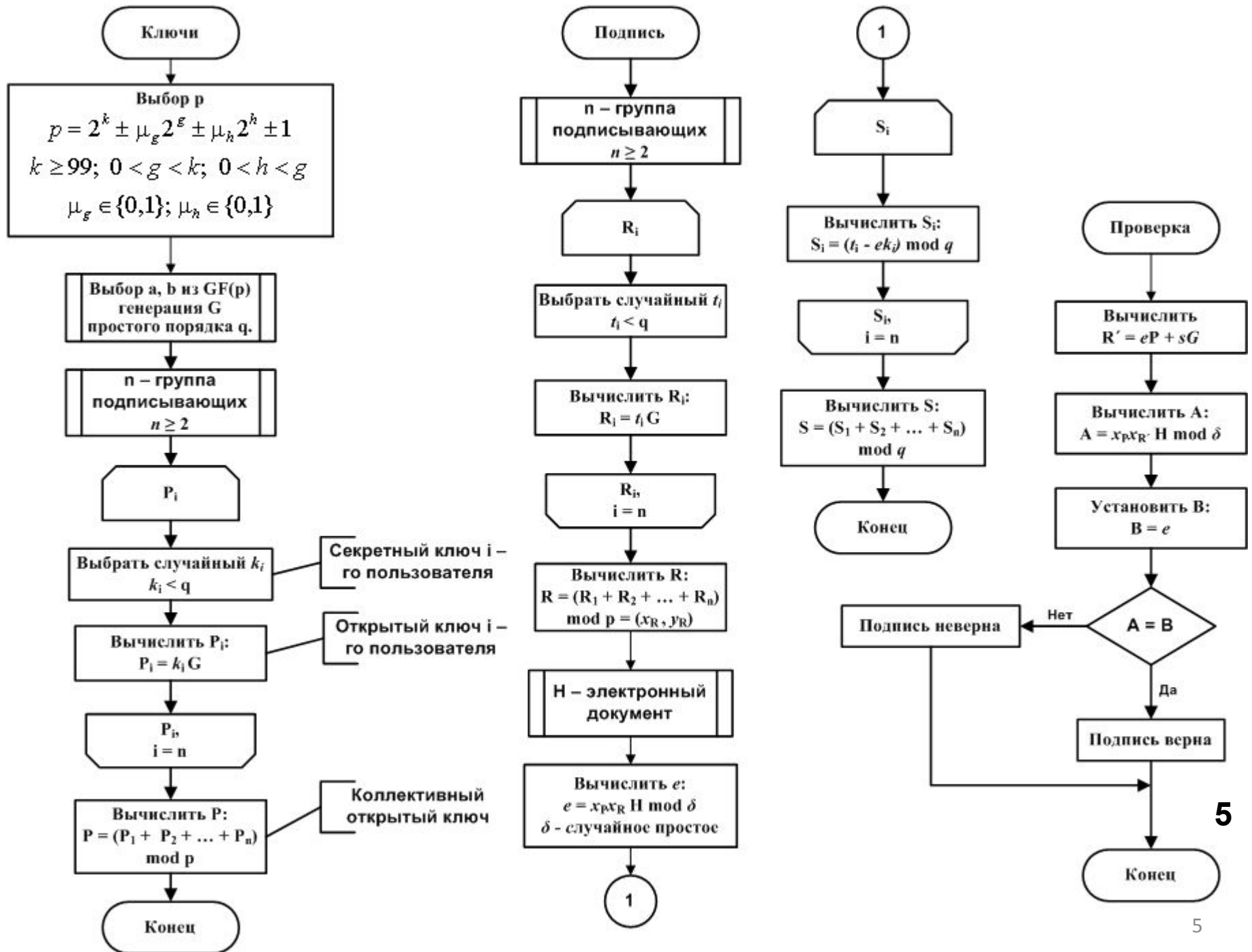
Диссертационная работа на тему: ПРОТОКОЛЫ КОЛЛЕКТИВНОЙ ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ НАД ЭЛЛИПТИЧЕСКИМИ КРИВЫМИ

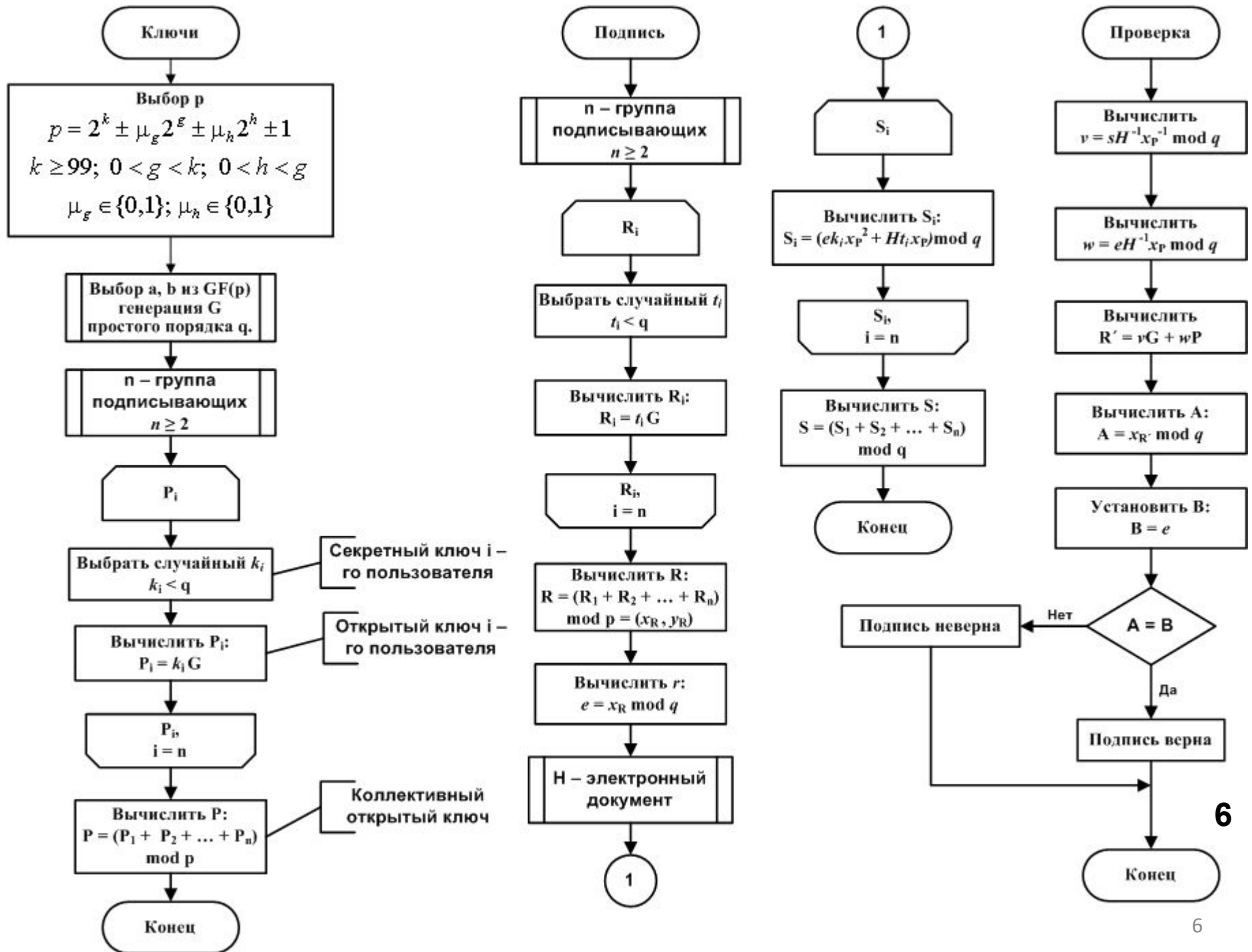
Положения выносимые на защиту:

- 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 конечных векторных полей

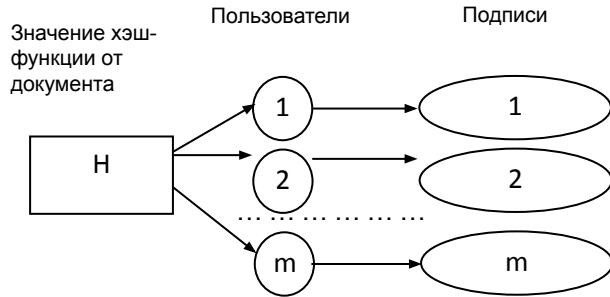




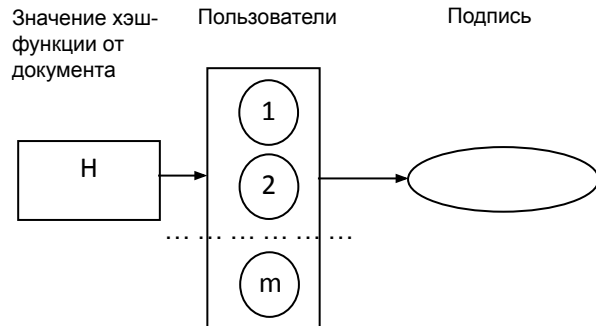




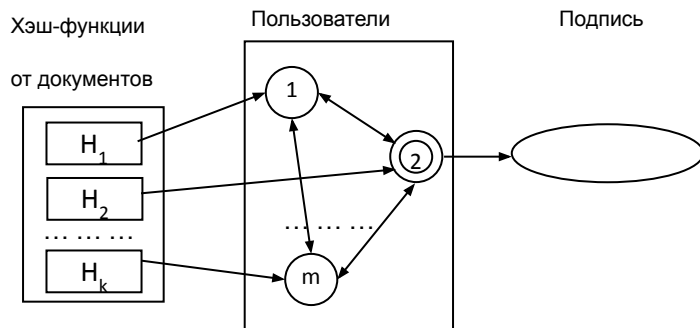
Композиционная подпись



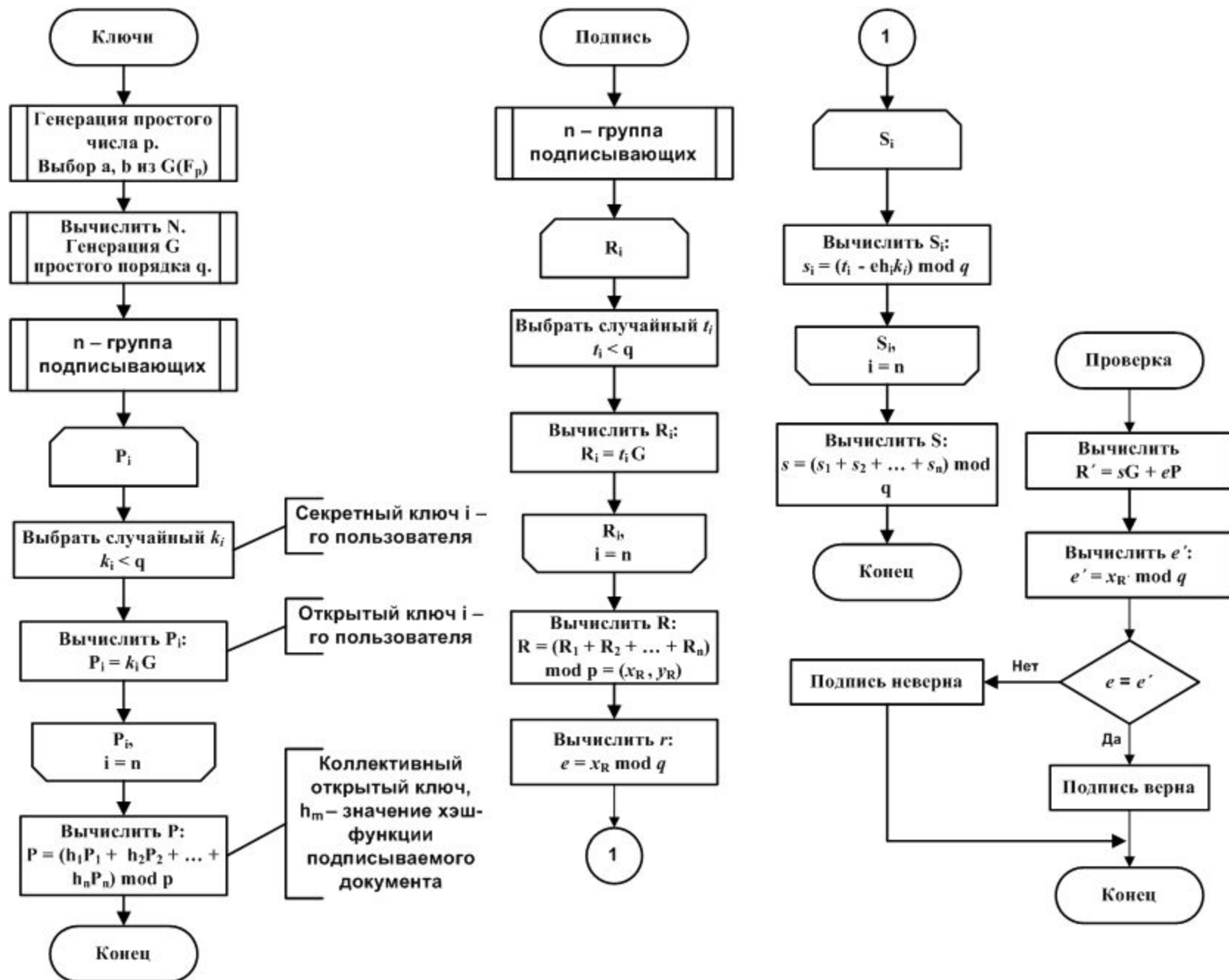
Заверение документа коллективом субъектов с использованием обычной схемы ЭЦП



Заверение документа коллективом субъектов с использованием коллективной подписи



Заверение документа коллективом субъектов с использованием композиционной подписи



Стойкость КЭЦП

m – пользователей, $m - 1$ нарушителей

Q_1, Q_2, \dots, Q_m

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

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

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

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

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

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

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

- лобовая атака
- слабость хэш – функции
- подделка ЭЦП

Подделка коллективной электронной цифровой подписи

$$m - \text{пользователей} \quad R = x_C \bmod q$$
$$Q_1, Q_2, \dots, Q_m$$

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

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

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

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

Конечные расширенные поля векторов над полем

$GF(p)$

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

Операция сложения:

$$(a, b, \dots, c) + (x, y, \dots, z) = (a + x, b + y, \dots, c + z)$$

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

Сравним сложность умножения в $GF(p^m)$ и \mathbb{Z}_p , где $|p'| = m|p|, |p|$ - битовая длина числа $GF(p^m)$ включает m^2 операций умножения в поле $GF(p)$, сложность пропорциональна $|p|^2$

и приблизительно равна сложности в \mathbb{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

Конечные группы и поля в пространстве многомерных векторов

\times	e	i	j	k
e	e	i	j	k
i	i	$\varepsilon \mu \cdot j$	$\varepsilon \cdot k$	$\varepsilon \mu \cdot e$
j	j	$\varepsilon \cdot k$	$\varepsilon \cdot e$	i
k	k	$\varepsilon \mu \cdot e$	i	$\mu \cdot j$

$m = 4;$

$\varepsilon, \mu \in GF(p)$

\times	e	i	j	k	u
e	e	i	j	k	u
i	i	$\varepsilon \cdot j$	$\varepsilon \mu \cdot k$	$\varepsilon \cdot u$	$\varepsilon \mu \cdot e$
j	j	$\varepsilon \mu \cdot k$	$\varepsilon \mu \cdot u$	$\varepsilon \mu \cdot e$	$\mu \cdot i$
k	k	$\varepsilon \cdot u$	$\varepsilon \mu \cdot e$	i	j
u	u	$\varepsilon \mu \cdot e$	$\mu \cdot i$	j	$\mu \cdot k$

$m = 5;$

$\varepsilon, \mu \in GF(p)$

\times	e	i	j	k	v	w
e	e	i	j	k	u	v
i	i	$\varepsilon \cdot j$	$\varepsilon \mu \cdot k$	u	$\varepsilon \cdot v$	$\varepsilon \mu \cdot e$
j	j	$\varepsilon \mu \cdot k$	$\mu \cdot u$	v	$\varepsilon \mu \cdot e$	$\mu \cdot i$
k	k	u	v	e	i	j
u	u	$\varepsilon \cdot v$	$\varepsilon \mu \cdot e$	i	$\varepsilon \mu \cdot j$	$\varepsilon \mu \cdot k$
v	v	$\varepsilon \mu \cdot e$	$\mu \cdot i$	j	$\varepsilon \mu \cdot k$	$\mu \cdot u$

$m = 6;$

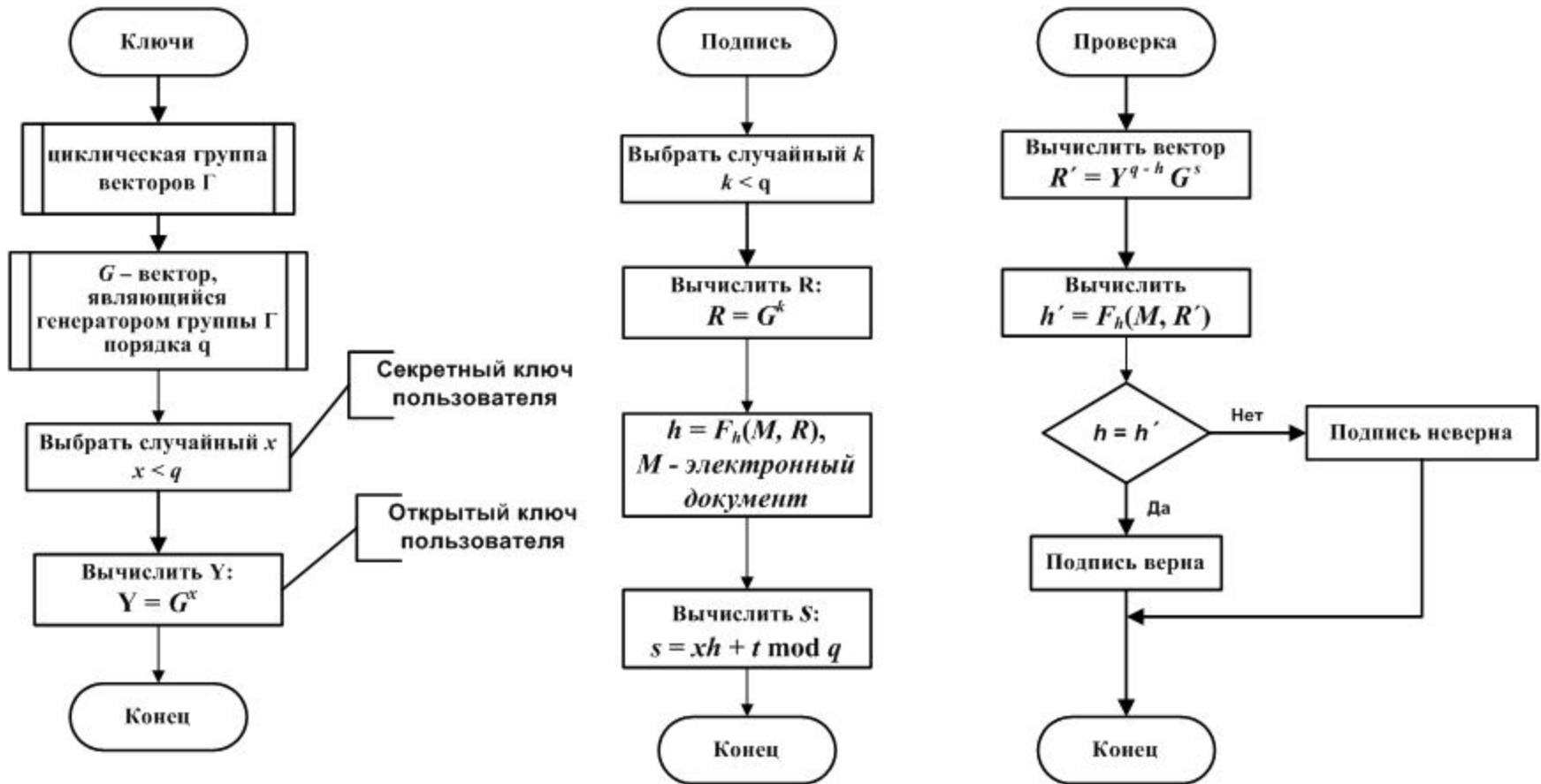
$\varepsilon, \mu \in GF(p)$

\times	e	j	k	u	v	w	
e	e	i	k	u	v	w	
i	i	$\varepsilon \mu \cdot k$	$\varepsilon \mu \cdot v$	$\mu \tau \cdot u$	$\varepsilon \mu \cdot w$	$\varepsilon \mu \tau \cdot e$	$\mu \tau \cdot j$
j	j	$\varepsilon \mu \cdot v$	$\varepsilon \cdot u$	$\varepsilon \mu \tau \cdot e$	$\varepsilon \cdot i$	$\varepsilon \cdot w$	$\varepsilon \cdot k$
k	k	$\mu \tau \cdot u$	$\varepsilon \mu \tau \cdot e$	$\mu \tau \cdot w$	$\mu \tau \cdot j$	$\tau \cdot i$	$\mu \tau \cdot v$
u	u	$\varepsilon \mu \cdot w$	$\varepsilon \cdot i$	$\mu \tau \cdot j$	$\varepsilon \mu \cdot v$	$\varepsilon \cdot k$	$\varepsilon \mu \tau \cdot e$
v	v	$\varepsilon \mu \tau \cdot e$	$\varepsilon \cdot w$	$\tau \cdot i$	$\varepsilon \cdot k$	$\tau \cdot j$	$\tau \cdot u$
w	w	$\mu \tau \cdot j$	$\varepsilon \cdot k$	$\mu \tau \cdot v$	$\varepsilon \mu \tau \cdot e$	$\tau \cdot u$	$\tau \cdot v$

$m = 7;$

$\varepsilon, \mu \in GF(p)$

Алгоритмы ЭЦП с использованием конечных расширенных полей, заданных в новой форме



$$|P| \geq \frac{160 - |m|}{m-1} \approx \frac{160}{m-1}$$

$$m \in \{3, 5, 7, 11, 13, 17, 19, 23\}$$

$$|\Omega'| \geq 1024$$