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

Цели:

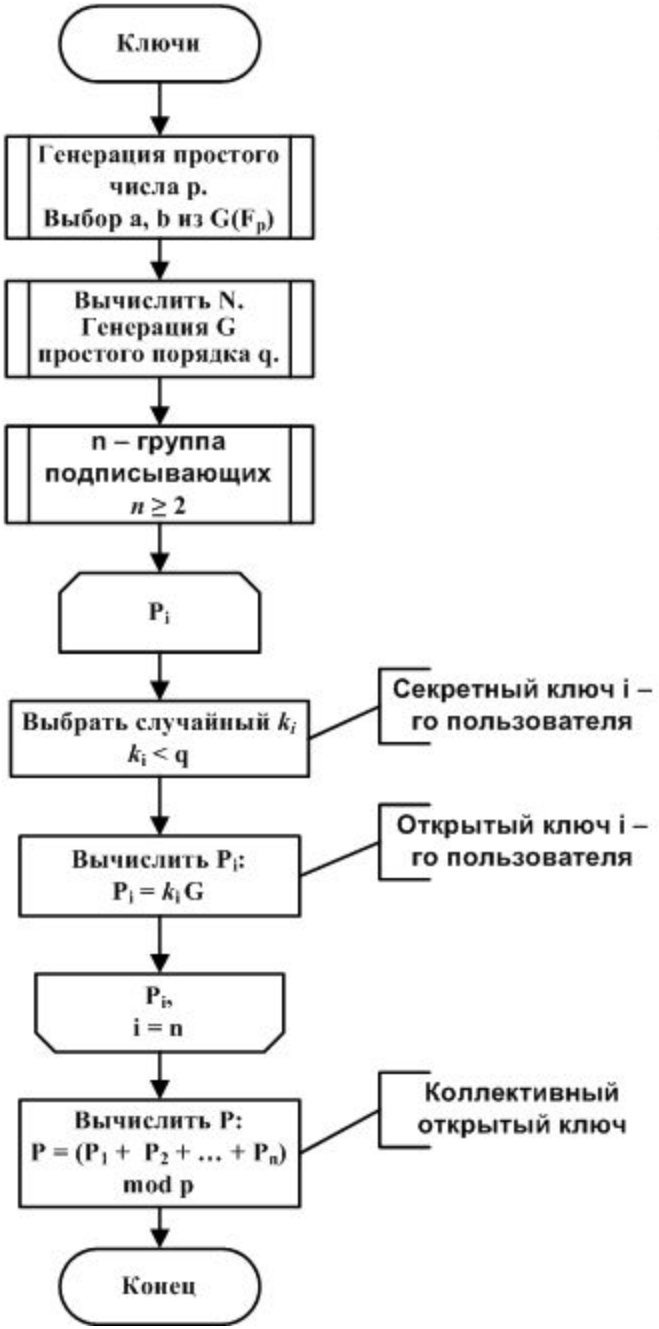
- анализ и разработка механизмов противодействия специфическим атакам на коллективную ЭЦП
- построение схем коллективной ЭЦП с использованием эллиптических кривых
- разработка схем потенциальных атак на разработанные схемы коллективной ЭЦП и оценка стойкости разработанных схем коллективной ЭЦП
- реализация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

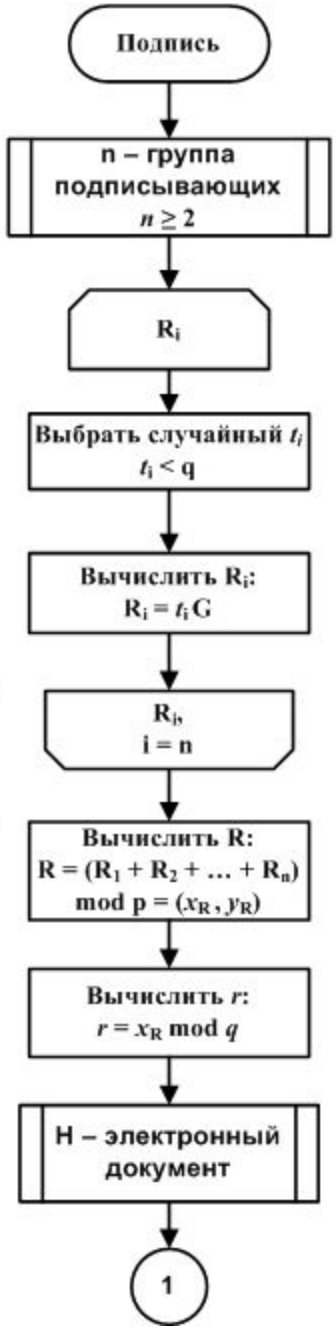
Диссертационная работа на тему:
ПРОТОКОЛЫ КОЛЛЕКТИВНОЙ ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ НАД ЭЛЛИПТИЧЕСКИМИ КРИВЫМИ

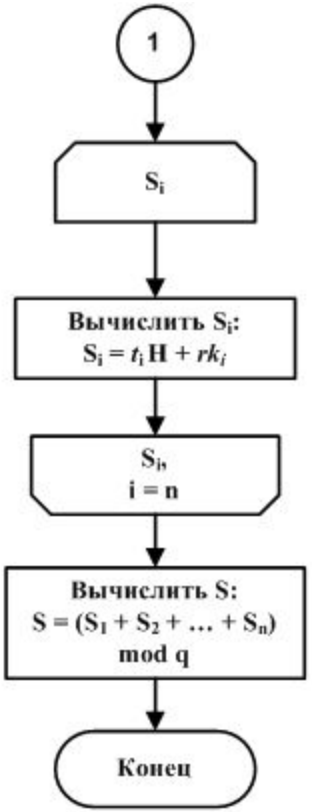
Положения выносимые на защиту:

- 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

2

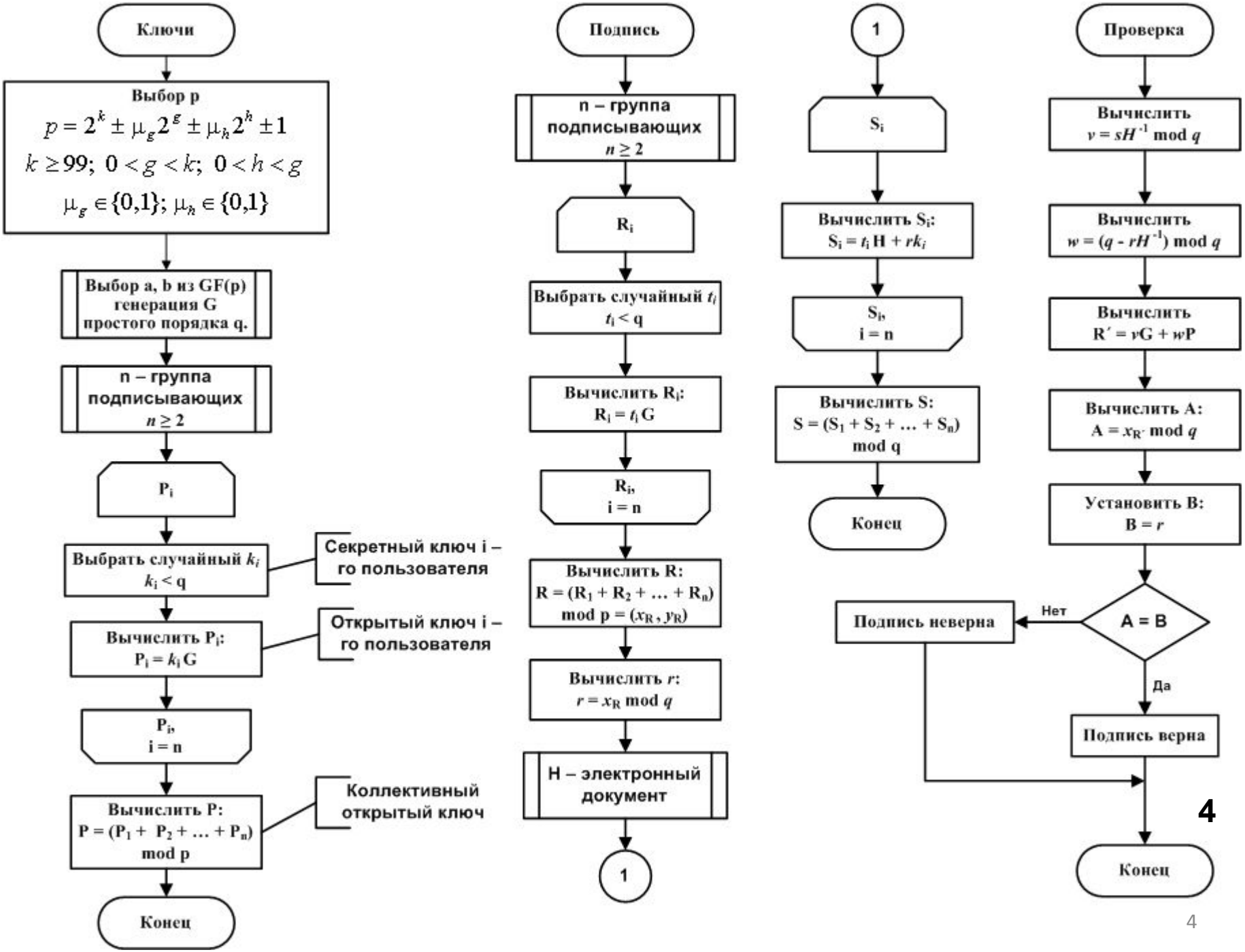

Ключи
Генерация простого числа p. Выбор a, b из G(F_p)
Вычислить N. Генерация G простого порядка q.
n – группа подписывающих n ≥ 2
P_i
Выбрать случайный k_i k_i < q
Секретный ключ i – го пользователя
Вычислить P_i: P_i = k_i G
Открытый ключ i – го пользователя
P_i, i = n
Вычислить P: P = (P_1 + P_2 + … + P_n) mod p
Коллективный открытый ключ
Конец


Подпись
n – группа подписывающих n ≥ 2
R_i
Выбрать случайный t_i t_i < q
Вычислить R_i: R_i = t_i G
R_i, i = n
Вычислить R: R = (R_1 + R_2 + … + R_n) mod p = (x_R , y_R)
Вычислить r: r = x_R mod q
H – электронный документ
1

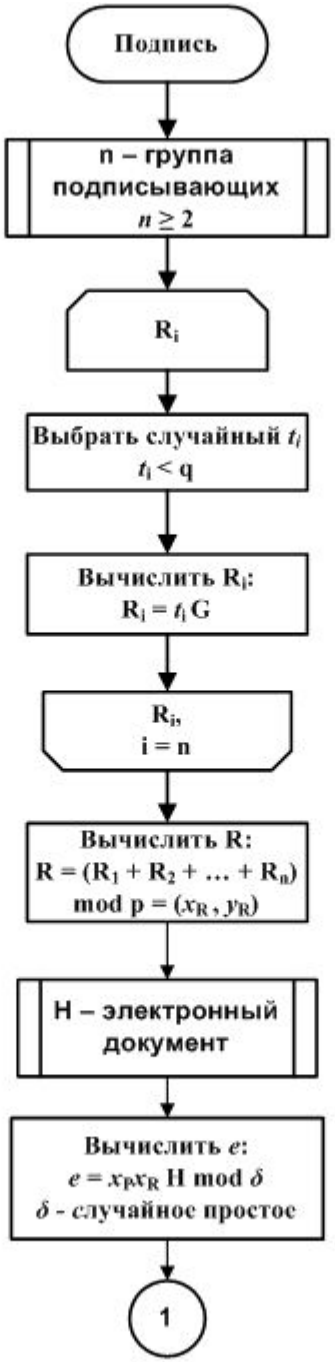

1
S_i
Вычислить S_i: S_i = t_i H + rk_i
S_i, i = n
Вычислить S: S = (S_1 + S_2 + … + S_n) mod q
Конец

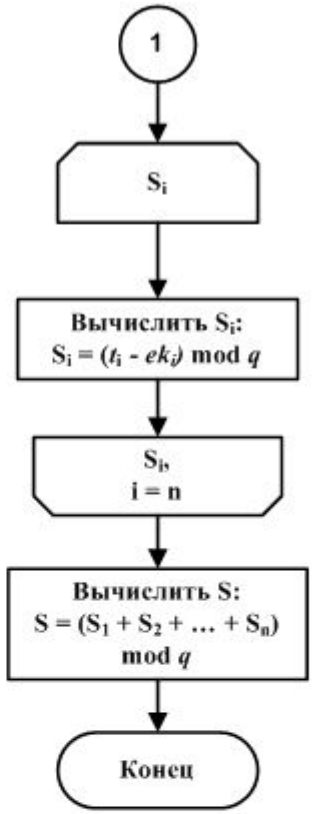
Проверка
Вычислить v = sH^-1 mod q
Вычислить w = (q - rH^-1) mod q
Вычислить R′ = vG + wP
Вычислить A: A = x_R′ mod q
Установить B: B = r
A = B
Нет
Подпись неверна
Да
Подпись верна
Конец

3


Ключи
Выбор p
$p = 2^k \pm \mu_g 2^g \pm \mu_h 2^h \pm 1$
$k \geq 99;\ 0 < g < k;\ 0 < h < g$
$\mu_g \in \{0,1\};\ \mu_h \in \{0,1\}$
Выбор a, b из GF(p) генерация G простого порядка q.
n – группа подписывающих $n \geq 2$
P_i
Выбрать случайный k_i $k_i < q$
Секретный ключ i – го пользователя
Вычислить P_i: $P_i = k_i G$
Открытый ключ i – го пользователя
P_i, i = n
Вычислить P: $P = (P_1 + P_2 + \ldots + P_n) \bmod p$
Коллективный открытый ключ
Конец
Подпись
n – группа подписывающих $n \geq 2$
R_i
Выбрать случайный t_i $t_i < q$
Вычислить R_i: $R_i = t_i G$
R_i, i = n
Вычислить R: $R = (R_1 + R_2 + \ldots + R_n) \bmod p = (x_R, y_R)$
Вычислить r: $r = x_R \bmod q$
H – электронный документ
1
1
S_i
Вычислить S_i: $S_i = t_i H + r k_i$
S_i, i = n
Вычислить S: $S = (S_1 + S_2 + \ldots + S_n) \bmod q$
Конец
Проверка
Вычислить $v = sH^{-1} \bmod q$
Вычислить $w = (q - rH^{-1}) \bmod q$
Вычислить $R' = vG + wP$
Вычислить A: $A = x_{R'} \bmod q$
Установить B: B = r
A = B
Нет
Подпись неверна
Да
Подпись верна
Конец
4

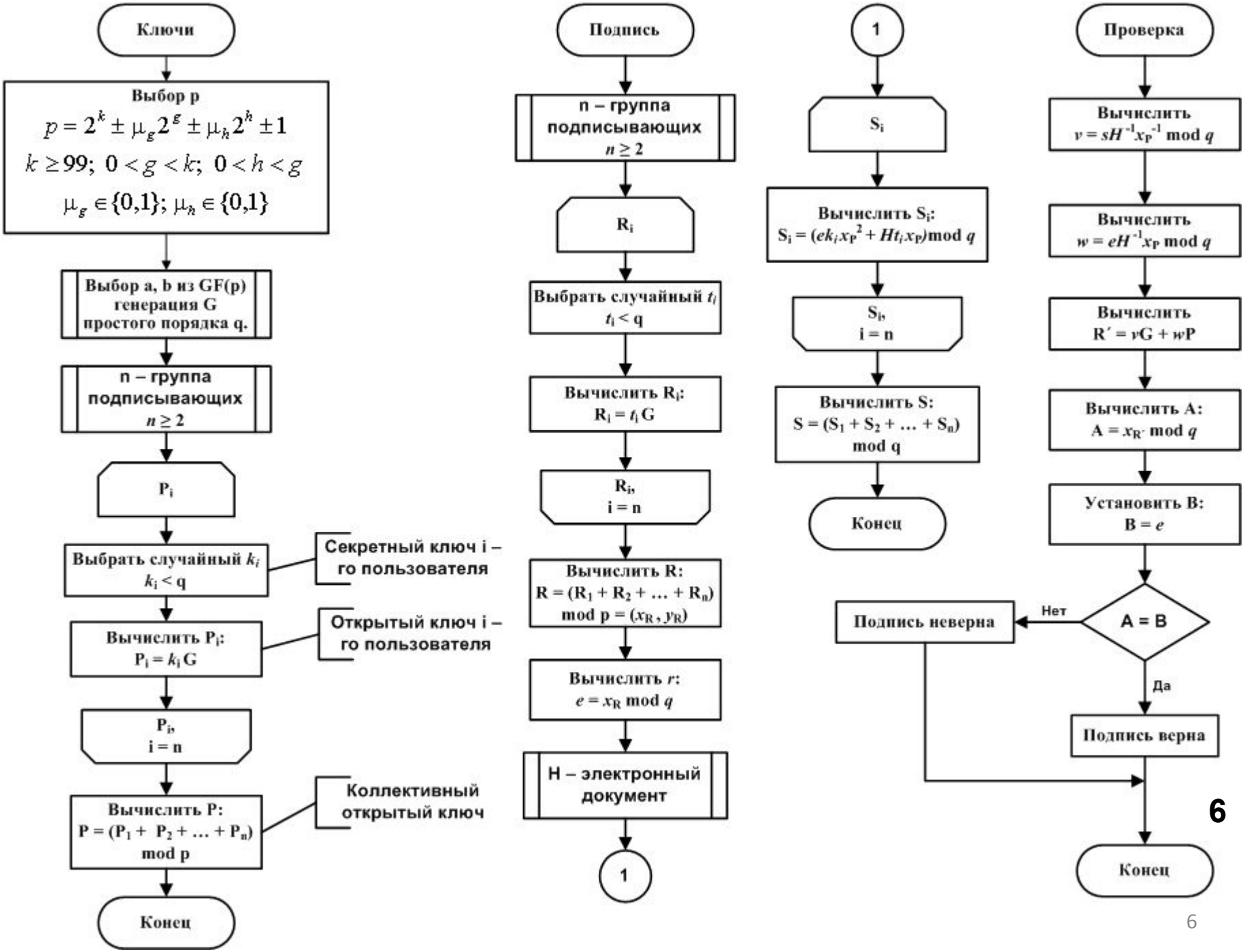

Ключи
Выбор p
$p = 2^k \pm \mu_g 2^g \pm \mu_h 2^h \pm 1$
$k \geq 99;\ 0 < g < k;\ 0 < h < g$
$\mu_g \in \{0,1\};\ \mu_h \in \{0,1\}$
Выбор a, b из GF(p) генерация G простого порядка q.
n – группа подписывающих $n \geq 2$
P_i
Выбрать случайный k_i $k_i < q$
Секретный ключ i – го пользователя
Вычислить P_i: $P_i = k_i G$
Открытый ключ i – го пользователя
P_i, i = n
Вычислить P: $P = (P_1 + P_2 + \ldots + P_n) \bmod p$
Коллективный открытый ключ
Конец


Подпись
n – группа подписывающих $n \geq 2$
R_i
Выбрать случайный t_i $t_i < q$
Вычислить R_i: $R_i = t_i G$
R_i, i = n
Вычислить R: $R = (R_1 + R_2 + \ldots + R_n) \bmod p = (x_R, y_R)$
H – электронный документ
Вычислить e: $e = x_R x_R H \bmod \delta$
δ - случайное простое
1


1
S_i
Вычислить S_i: $S_i = (t_i - ek_i) \bmod q$
S_i, i = n
Вычислить S: $S = (S_1 + S_2 + \ldots + S_n) \bmod q$
Конец

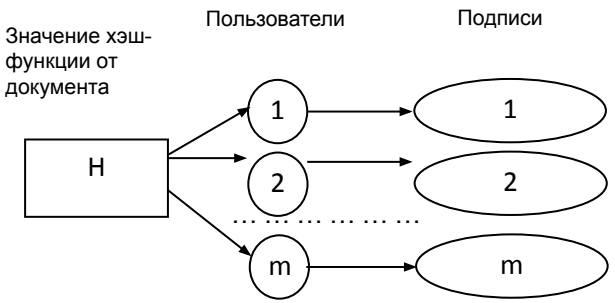

Проверка
Вычислить $R' = eP + sG$
Вычислить A: $A = x_R x_{R'} H \bmod \delta$
Установить B: $B = e$
A = B
Нет
Подпись неверна
Да
Подпись верна
Конец

5

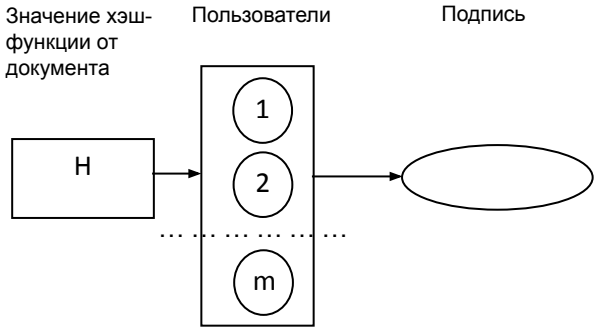

Ключи
Выбор p
$p = 2^k \pm \mu_g 2^g \pm \mu_h 2^h \pm 1$
$k \geq 99;\ 0 < g < k;\ 0 < h < g$
$\mu_g \in \{0,1\};\ \mu_h \in \{0,1\}$
Выбор a, b из GF(p) генерация G простого порядка q.
n – группа подписывающих $n \geq 2$
P_i
Выбрать случайный k_i $k_i < q$
Секретный ключ i – го пользователя
Вычислить P_i: $P_i = k_i G$
Открытый ключ i – го пользователя
P_i, i = n
Вычислить P: $P = (P_1 + P_2 + \ldots + P_n) \bmod p$
Коллективный открытый ключ
Конец
Подпись
n – группа подписывающих $n \geq 2$
R_i
Выбрать случайный t_i $t_i < q$
Вычислить R_i: $R_i = t_i G$
R_i, i = n
Вычислить R: $R = (R_1 + R_2 + \ldots + R_n) \bmod p = (x_R, y_R)$
Вычислить r: $e = x_R \bmod q$
H – электронный документ
1
1
S_i
Вычислить S_i: $S_i = (ek_i x_P^2 + Ht_i x_P) \bmod q$
S_i, i = n
Вычислить S: $S = (S_1 + S_2 + \ldots + S_n) \bmod q$
Конец
Проверка
Вычислить $v = sH^{-1}x_P^{-1} \bmod q$
Вычислить $w = eH^{-1}x_P \bmod q$
Вычислить $R' = vG + wP$
Вычислить A: $A = x_{R'} \bmod q$
Установить B: $B = e$
A = B
Нет
Подпись неверна
Да
Подпись верна
Конец

6

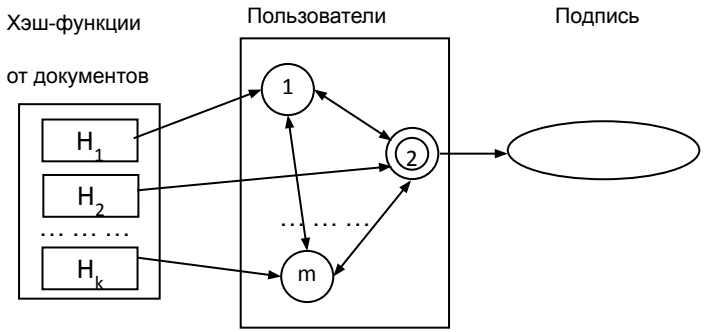
Композиционная подпись



Заверение документа коллективом субъектов с использованием обычной схемы ЭЦП

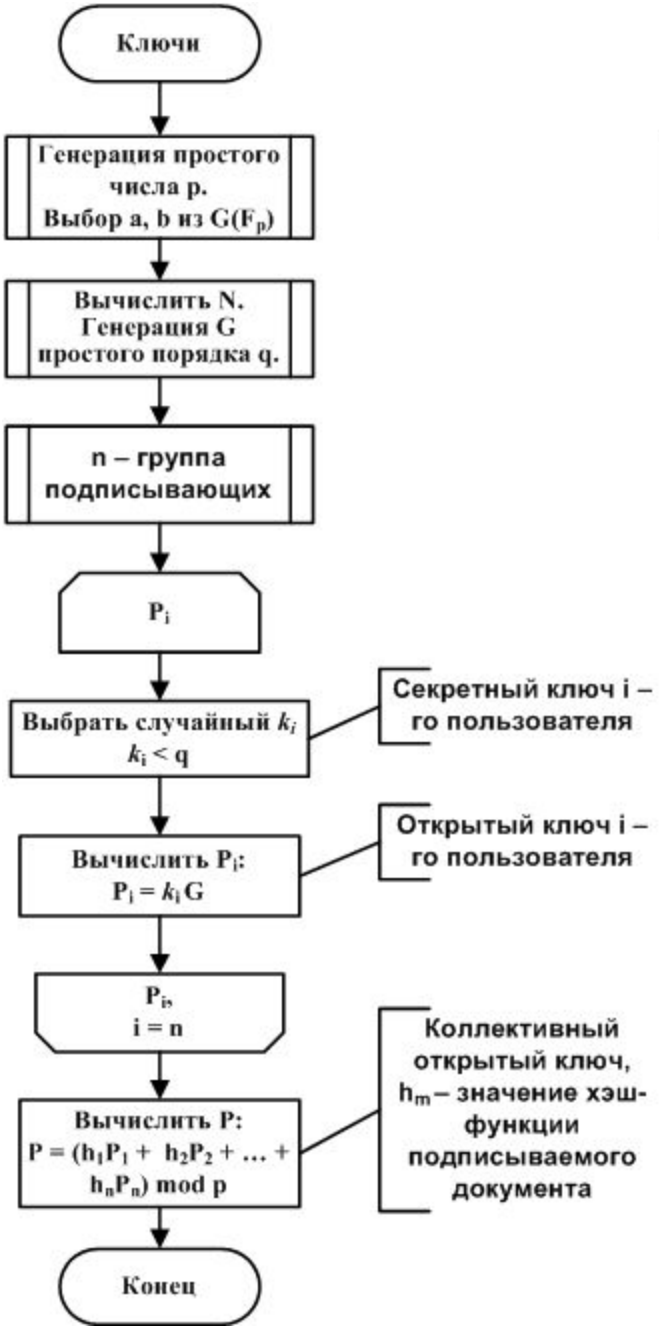


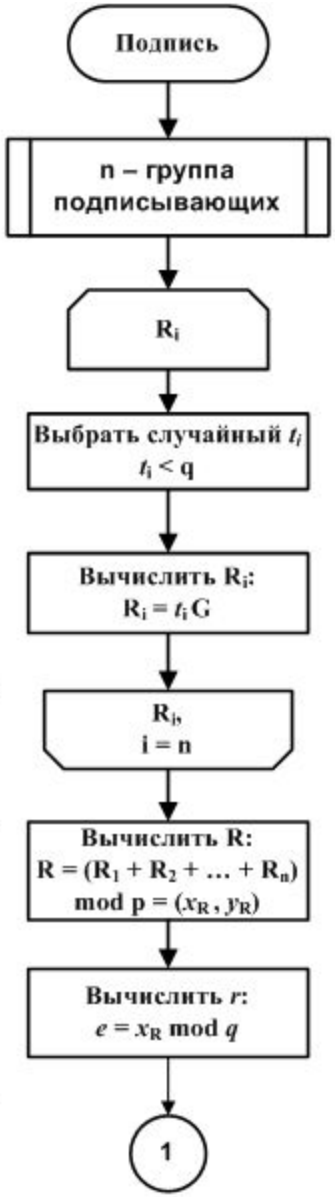
Заверение документа коллективом субъектов с использованием коллективной подписи

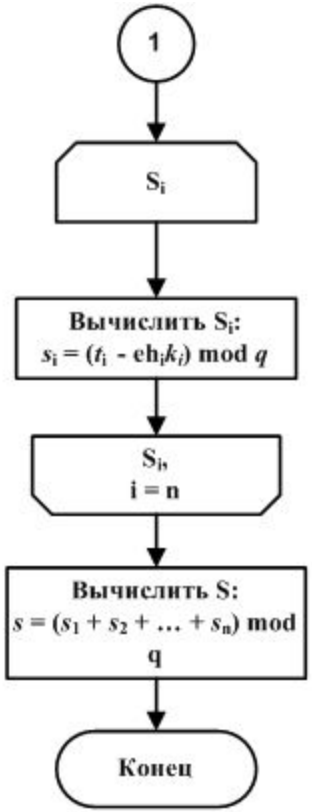


Заверение документа коллективом субъектов с использованием композиционной подписи

7


Ключи
Генерация простого числа p. Выбор a, b из $G(F_p)$
Вычислить N. Генерация G простого порядка q.
n – группа подписывающих
P_i
Выбрать случайный k_i $k_i < q$
Секретный ключ i – го пользователя
Вычислить P_i: $P_i = k_i G$
Открытый ключ i – го пользователя
P_i, i = n
Вычислить P: $P = (h_1P_1 + h_2P_2 + \ldots + h_nP_n) \bmod p$
Коллективный открытый ключ, h_m – значение хэш-функции подписываемого документа
Конец


Подпись
n – группа подписывающих
R_i
Выбрать случайный t_i $t_i < q$
Вычислить R_i: $R_i = t_i G$
R_i, i = n
Вычислить R: $R = (R_1 + R_2 + \ldots + R_n) \bmod p = (x_R, y_R)$
Вычислить r: $e = x_R \bmod q$
1


1
S_i
Вычислить S_i: $s_i = (t_i - eh_ik_i) \bmod q$
S_i, i = n
Вычислить S: $s = (s_1 + s_2 + \ldots + s_n) \bmod q$
Конец


Проверка
Вычислить $R' = sG + eP$
Вычислить e': $e' = x_R \bmod q$
$e = e'$
Нет
Подпись неверна
Да
Подпись верна
Конец

8

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

9

Подделка коллективной электронной цифровой подписи

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

$$R = x_C \bmod q$$

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

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

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

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

10

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: $(a \cdot \mathbf{e} + b \cdot \mathbf{i} + \ldots + c \cdot \mathbf{j})(x \cdot \mathbf{e} + y \cdot \mathbf{i} + \ldots + z \cdot \mathbf{j}) = ax \cdot \mathbf{ee} + ay \cdot \mathbf{ei} + \ldots + az \cdot \mathbf{ej} + \ldots + bx \cdot \mathbf{ie}$
, где **ee**, **ei**, **ej**, **ie**, **ii**, …**ij**, …**je**, **ji**, …**jj** – заменяются на ε**v**, где ε - 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

11

Конечные группы и поля в пространстве многомерных векторов

×	*e*	*i*	*j*	*k*
e	**e**	**i**	**j**	**k**
i	**i**	εμ·**j**	ε·**k**	εμ·**e**
j	**j**	ε·**k**	ε·**e**	**i**
k	**k**	εμ·**e**	**i**	μ·**j**

m = 4;

ε, μ ∈ *GF*(*p*)

×	*e*	*i*	*j*	*k*	*u*
e	**e**	**i**	**j**	**k**	**u**
i	**i**	ε·**j**	εμ·**k**	ε·**u**	εμ·**e**
j	**j**	εμ·**k**	εμ·**u**	εμ·**e**	μ·**i**
k	**k**	ε·**u**	εμ·**e**	**i**	**J**
u	**u**	εμ·**e**	μ·**i**	**j**	μ·**k**

m = 5;

ε, μ ∈ *GF*(*p*)

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

m = 6;

ε, μ ∈ *GF*(*p*)

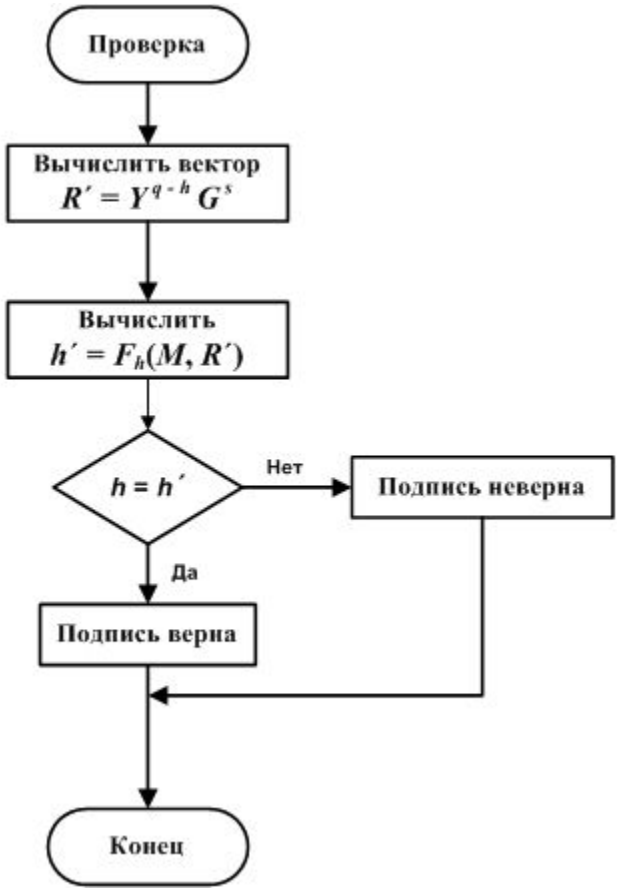
×	*e*	*i*	*j*	*k*	*u*	*v*	*w*
e	**e**	**i**	**j**	**k**	**u**	**v**	**w**
i	**i**	εμ·**k**	εμ·**v**	μτ·**u**	εμ·**w**	εμτ·**e**	μτ·**j**
j	**j**	εμ·**v**	ε·**u**	εμτ·**e**	ε·**i**	ε·**w**	ε·**k**
k	**k**	μτ·**u**	εμτ·**e**	μτ·**w**	μτ·**j**	τ·**i**	μτ·**v**
u	**u**	εμ·**w**	ε·**i**	μτ·**j**	εμ·**v**	ε·**k**	εμτ·**e**
v	**v**	εμτ·**e**	ε·**w**	τ·**i**	ε·**k**	τ·**j**	τ·**u**
w	**w**	μτ·**j**	ε·**k**	μτ·**v**	εμτ·**e**	τ·**u**	τ·**v**

m = 7;

ε, μ ∈ *GF*(*p*)

12

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



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

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

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

13