ҚАЗАҚСТАН РЕСПУБЛИКАСЫНЫҢ ҰЛТТЫҚ СТАНДАРТЫ

Ақпараттық технология
Ақпаратты криптографиялық қорғау

ЭЛЕКТРОНДЫ САНДЫҚ ҚОЛТАҢБАНЫ ҚАЛЫПТАСТЫРУ ЖӘНЕ ТЕКСЕРУ ПРОЦЕСТЕРІ

ҚР СТ ГОСТ Р 34.10-2015

(*ГОСТ Р 34.10-2012 Ақпараттық технология. Ақпаратты криптологиялық қорғау. Электронды цифрлық қолтаңбаны қалыптастыру және тексеру процестері,* IDT)

Ресми басылым

Қазақстан Республикасы Инвестициялар және даму министрлігінің
Техникалық реттеу және метрология комитеті
(Мемстандарт)

Астана

Алғысөз

1 «М. Тынышпаев атындағы Қазақ көлік және коммуникациялар академиясы» акционерлік қоғамы **ӘЗІРЛЕП ЕНГІЗДІ.**

2 Қазақстан Республикасы Инвестициялар және даму министрлігі Техникалық реттеу және метрология комитетіт Төрағасының 2015 жылғы 18 қарашадағы № 262-од бұйрығымен **БЕКІТІЛІП ҚОЛДАНЫСҚА ЕНГІЗІЛДІ.**

3 Осы стандарт ГОСТ Р 34. 10 - 2012 Ақпараттық технология. Ақпаратты криптографиялық қорғау. Электрондық сандық қолтаңбаны қалыптастыру және тексеру процестері халықаралық стандарты талаптарына сай.

Осы стандарттың негізі болған шет мемлекет стандарттардың ресми даналары нормативтік техникалық құжаттардың Бірыңғай мемлекеттік қорында бар.

Ресми нұсқасы мемлекеттік және орыс тілдерінде.

Сәйкестік дәрежесі - бірдей (IDT).

4 Осы стандартта «Техникалық реттеу туралы» Қазақстан Республикасының 2004 жылғы 9 қарашадағы № 603–II заңының; «Қазақстан Республикасының тілдер туралы» 1997 ж. 11 шілдедегі № 152 және «Ақпараттандыру туралы» Қазақстан Республикасының 2007 жылғы 11 қаңтардағы № 217-III (29.12.2014 өзгертулер мен қосымшаларымен) заңдарының нормалары жүзеге асырылды.

5 БІРІНШІ ТЕКСЕРУ МЕРЗІМІ **2022 жыл**
ТЕКСЕРУ КЕЗЕҢДІЛІГІ **5 жыл**

6 АЛҒАШ РЕТ ЕНГІЗІЛДІ

Осы стандартқа енгізілген өзгертулер туралы ақпарат жыл сайын басылып шығарылатын «Стандарттау жөніндегі нормативтік құжаттар» сілтемесінде, ал өзгертулер мен түзетулер мәтіні - ай сайын басылып шығарылатын «Ұлттық стандарттар» ақпараттық сілтемелерінде жарияланады. Осы стандарт қайта қаралған (өзгертілген) немесе жойылған жағдайда, тиісті хабарлама ай сайын басылып шығарылатын «Ұлттық стандарттар» ақпараттық сілтемесінде жарияланады.

Мазмұны

ҚАЗАҚСТАН РЕСПУБЛИКАСЫНЫҢ ҰЛТТЫҚ СТАНДАРТЫ

Ақпараттық технологиялар
Ақпаратты криптографиялық қорғау

ЭЛЕКТРОНДЫҚ САНДЫҚ ҚОЛТАҢБАНЫ ҚАЛЫПТАСТЫРУ ЖӘНЕ ТЕКСЕРУ ПРОЦЕСТЕРІ

Енгізілген күні 2017-01-01

1 Қолданылу саласы

Осы стандарт электрондық сандық қолтаңба (ЭСҚ) (бұдан әрі – сандық қолтаңба) схемасын, түрлі мақсаттағы ақпараттарды өңдеу жүйелеріндегі жалпы қолданыстағы қорғалмаған телекоммуникациялық желілер арқылы берілетін хабардың (құжаттың) төменгі жағындағы сандық қолтаңбаны қалыптастыру мен тексеру процестерін анықтайды.

Сандық қолтаңбаны осы стандарт негізінде енгізу берілетін хабарлардың жасандылық пен бұрмалаулардан қорғалу деңгейін бұрынғы қолданыстағы сандық қолтаңба схемасымен салыстырғанда жоғарылатады.

Осы стандарт түрлі мақсаттағы ақпараттарды өңдеу жүйелерін жасау, пайдалану және жетілдіру барысында қолдануға ұсынылады.

2 Нормативтік сілтемелер

Осы стандартты қолдану үшін мынадай сілтемелік нормативті құжаттар қажет. Сілтемелік нормативті құжаттың басылымы тек даталанған сілтемелері үшін қолданылады, даталанбаған сілтемелері үшін сілтемелік құжаттың соңғы басылымы (олардың барлық өзгерістерін қоса) қолданылады.

ГОСТ Р 34. 11-2012 Ақпараттық технология. Ақпаратты криптографиялық қорғау. Хэштеу қызметі.

3 Терминдер, анықтамалар және белгілер

Осы стандартта мынадай терминдермен анықтамалар және шартты белгілер қолданылады:

3.1 Терминдер мен анықтамалар

3.1.2

Қолтаңба кілті (signaturekey): субъектіге тән және сандық қолтаңбаны қалыптастыру процесінде тек осы субъект қана пайдаланатын құпия деректер элементі.

(ISO/IEC 14888-1:2008 [4])

3.1.3

Қолтаңбаны тексеру кілті (verification key): қолтаңба кілтімен математикалық байланысты және сандық қолтаңбаны тексеру барысында тексеруші тарап пайдаланатын деректер элементі.

(ISO/IEC 14888-1:2008 [4])

3.1.4

ЭСҚ схемасының параметрі (domain parameter): сандық қолтаңба схемасының барлық субъектілері үшін ортақ, осы субъектілердің барлығына мәлім немесе қолжетімді деректер элементі.

(ISO/IEC 14888-1:2008 [4])

3.1.5

Қол қойылған хабар (signed message): хабардан және хабардың бөлшегі болып табылатын толықтырудан тұратын деректер элементтерінің жиынтығы..

(ISO/IEC 14888-1:2008 [4])

3.1.6

Жалған кездейсоқ сандар тізбегі(pseudo-random number sequence): әлдебір арифметикалық (есептеу) процесті орындау нәтижесінде алынатын, нақты жағдайда кездейсоқ сандар тізбегі орнына пайдаланылатын сандар тізбегі.

3.1.7

Кездейсоқ сандар тізбегі (random number sequence): әрбірі оның алдындағы осы тізбек сандарын білу негізінде ғана алдын ала айтыла алмайтын (есептеп шығарылмайтын) сандар тізбегі.

3.1.8

Қолтаңбаны тексеру процесі (verification process): бастапқы деректер ретінде қол қойылған хабар, қолтаңбаны тексеру кілті және ЭСҚ схемасының параметрі пайдаланылатын процесс, оның нәтижесі сандық қолтаңбаның дұрыстығы немесе қате екендігі туралы қорытынды болып табылады.

(ISO/IEC 14888-1:2008 [4])

3.1.9

Қолтаңбаны қалыптастыру процесі (signature process): бастапқы деректер ретінде хабар, қолтаңба кілті және ЭСҚ схемасының параметрі пайдаланылатын процесс, оның нәтижесінде сандық қолтаңба қалыптастырылады. (ISO/IEC 14888-1:2008 [4])

3.1.10

Куәлік (witness): тексеруші тарапқа қолтаңба ақиқаттығының (ақиқат еместігінің) тиісті дәлелдерін көрсететін деректер элементі.

3.1.11

Кездейсоқ сан (random number): белгілі бір сандар жиынтығынан берілген жиынтықтағы әрбір сан бірдей ықтималдықпен таңдап алына алатындай таңдап алынған сан.

3.1.12

Хабар (message): еркін шеткі ұзындық биттар қатары.
(ISO/IEC 14888-1:2008 [4])

3.1.13

Хэш-код (hash-code): хэш-функцияның шығатын нәтижесі болып табылатын биттар қатары.
(ISO/IEC 14888-1:2008 [4])

3.1.14

Хэш-функция (collision-resistanthash-function): биттар қатарын бекітілген ұзындық биттары қатарында бейнелейтін және мынандай қасиеттерді қанағаттандыратын функция:

1) функцияның берілген мәні бойынша осы мәнді бейнелейтін бастапқы деректерді есептеп шығу күрделі;

2) берілген бастапқы деректер үшін функцияның дәл сол мәнін бейнелейтін басқа бастапқы деректерді есептеп шығу күрделі;

3) бір мәнді бейнелейтін қандай да бір бастапқы деректер жұбын есептеп шығу күрделі.

(ISO/IEC 14888-1:2008 [4]

Ескертпелер

1 Электрондық сандық қолтаңба саласына сәйкес санап шығу қасиеті

1) белгілі электрондық сандық қолтаңба бойынша бастапқы хабарды қайта қалпына келтіру мүмкін емес деп түсіндіріледі, санап шығу қасиеті;

2) берілген қол қойылған хабар үшін дәл сондай электрондық қолтаңбасы бар, басқа (бұрмаланған) хабар таңдап алу қиын деп түсіндіріледі, санап шығу қасиеті;

3) бір қолтаңбаға ие қандай да бір хабарлар жұбын таңдап алу қиын деп түсіндіріледі.

2 Осы стандартта қолданыстағы отандық нормативтік құжаттармен және жарияланған ғылыми-техникалық басылымдармен терминологиялық сабақтастықты сақтау мақсатында «хэш-функция», «криптографиялық хэш-функция», «хэштілеу функциясы» және «криптографиялық хэштілеу функциясы» терминдері синонимдер болып табылатыны белгіленген.

3.1.15

Электрондық сандық қолтаңба (signature); ЭСҚ: Қолтаңбаны қалыптастыру процесі нәтижесінде алынған биттар қатары.
(ISO/IEC 14888-1:2008 [4])

Ескертпелер

1 Қолтаңба болып табылатын биттар қатарының қолтаңбаны қалыптастыратын нақты бір механизмге тәуелді ішкі құрылымы болуы мүмкін.

2. Бұл стандартта қолданыстағы отандық нормативтік құжаттармен және жарияланған ғылыми-техникалық басылымдармен терминологиялық сабақтастықты сақтау мақсатында «электрондық қолтаңба», «сандық қолтаңба», және «электрондық сандық қолтаңба» терминдері синонимдер болып табылатыны белгіленген.

3.2 Белгілер

Бұл стандартта мынадай белгілер қолданылған:

V_l -l бит ұзындықты барлық екілік векторлардың көптігі;

V^* _ барлық еркін шеткі ұзындық екілік векторлардың көптігі;

Z - барлық бүтін сандардың көптігі;

p -қарапайым сан, $p>3$,

F_p - p бүтін сандардан $\{0,1,...,p-1\}$ тұратын көптік түріндегі шеткі қарапайым өріс;

$b(\mathrm{mod}p)$ –p модулі бойынша b салыстырылатынминималды теріс емес сан;

M - қолданушының хабары, $M \in V^*$;

$(\overline{h_1}||\overline{h_2})$ - екі екілік вектордың конкатенациясы (бірігуі);

a, b- эллиптикалық қисық коэффициенттері;

m - эллиптикалық қисық нүктелері топтарының реті;

q- эллиптикалық қисық нүктелері топтары шағын тобының реті;

O - эллиптикалық қисықтың нөлдік нүктесі;

P- q реттегі эллиптикалық қисық нүктесі;

d- бүтін сан – қолтаңба кілті;

Q- эллиптикалық қисық нүктесі – қолтаңбаны тексеру кілті;

ζ- M хабардың төменгі жағындағы сандық қолтаңба.

4 Жалпы ережелер

Сандық қолтаңбаның жалпы танылған схемасы (моделі) (қара: ISO/IEC 14888-1 [4]) мынадай процестерді қамтиды:

- кілттерді (қолтаңбаны және қолтаңбаны тексерулерді) генерациялау;
- қолтаңбаны қалыптастыру;
- қолтаңбаны тексеру.

Бұл стандартта кілттерді (қолтаңбаны және қолтаңбаны тексерулерді) генерациялау процесі қарастырылмаған. Бұл процестің сипаттамалары мен жүзеге асырылу әдістерін оған тартылған субъектілер анықтайды, олар өзара келісе отырып тиісті параметрлерді белгілейді.

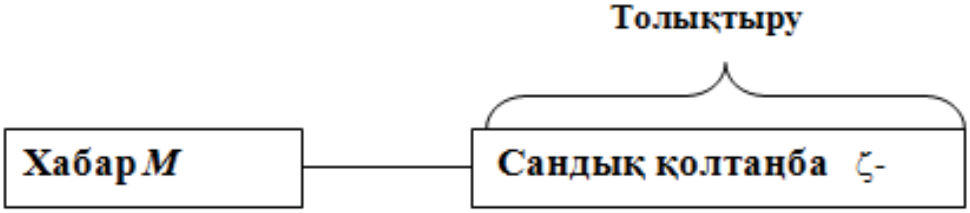
Сандық қолтаңба механизмі негізгі екі процесті жүзеге асыру арқылы анықталады (қара: 6-тарау):

- қолтаңбаны қалыптастыру (қара: 6.1);
- қолтаңбаны тексеру (қара: 6.2).

Сандық қолтаңба электрондық хабарға қол қойған адамды аутентификациялауға арналған. Мұнан өзге, ЭСҚ пайдалану қол қойылған жүйеде беру кезінде мынадай қасиеттерді қамтамасыз ету мүмкіндігін береді:

- берілетін қол қойылған хабардың тұтастығын бақылауды жүзеге асыру,
- хабарға қол қойған адамның авторлығын растау дәлелі,
- хабарды қолдан жасау мүмкіндігінен қорғау.

Қол қойылған хабардың схемалық көрінісі 1-суретте көрсетілген.



Сурет 1– Қол қойылған хабардың схемасы

Бұл суретте көрсетілген «Мәтін» өрісі мен «Сандық қолтаңба» толықтырма өрісі, мысалы, хабарға қол қойған субъектінің идентификаторларына және / немесе уақыт белгісіне ие бола алады.

Осы стандартта орнатылған сандық қолтаңба схемасы шеткі қарапайым өрістің үстінде анықталған эллиптикалық қисықтың нүктелер тобы операцияларын, сондай хэш-функцияларды пайдаланып жүзеге асырылуы тиіс.

Сандық қолтаңбаның берілген схемасының криптографиялық беріктігі эллиптикалық қисықтың нүктелер тобындағы дискреттік логарифимдеу міндеттерін шешу күрделілігіне, сондай-ақ пайдаланылатын хэш-функция беріктігіне негізделеді. Хэш-функцияны есептеп шығу алгоритмі ГОСТ Р 34.11-2012 белгіленген.

Сандық қолтаңбаның оны қалыптастыруға және тексеруге қажет параметрлерінің схемасы 5.2-де анықталған. Осы стандартта параметрлерге қойылатын талаптардың екі вариантының бірін таңдау мүмкіндігі алдын ала көзделген.

Бұл стандарт сандық қолтаңба схемасы параметрлерін генерациялау процесін анықтамайды. Бұл процесті жүзеге асырудың нақты алгоритмін (әдісін) сандық қолтаңба схемасының субъектілері электрондық құжат айналымын жүзеге асырушы аппараттық-бағдарламалық құралдарға қойылатын талаптарға сүйене отырып анықтайды.

l бит ұзындықты 512 немесе 1024 бит екілік вектор түрінде көрсетілген сандық қолтаңба 6.1-де баяндалған белгілі бір ережелер жиынтығының көмегімен есептеп шығарылады.

Алынған хабардың төменгі жағындағы қолтаңбаны қабылдауға немесе қабыл алмауға мүмкіндік беретін ережелер жиынтығы 6.2-де белгіленген.

5 Математикалық нысандар

Сандық қолтаңба схемаларының анықтамалары үшін оны қалыптастыру және тексеру процестерінде пайдаланылатын базалық математикалық нысандарды сипаттау қажет. Бұл тарауда сандық қолтаңба схемасының параметрлеріне қойылатын негізгі математикалық анықтамалар мен талаптар белгіленген.

5.1 Математикалық анықтамалар

F_p шеткі қарапайым өріс үстінде анықталған (бұл жерде p >3 – қарапайым сан) E эллиптикалық қисығы (x, y), x, $y \in F_p$ сандары жұптарының көптігі деп аталады, олар

$$y^2 \equiv x^3 + ax + b (mod\ p) \quad (1)$$

теңдеуіне сәйкес, бұл жерде a, $b \in F_p$ және $4a^3 + 27b^2$ p модулі бойынша нөлмен салыстырмалы емес.

$J(E)$ шамасы эллиптикалық қисық инварианты деп аталады, ол

$$J(E) \equiv 1728 \frac{4a^3}{4a^3 + 27b^2} (mod\ p) \quad (2)$$

тепе-теңдігіне сәйкес.

x,y– F_p өрісінің элементтері болып табылатын, (1) теңдеуіне сәйкес келетін (x,y) жұптары «E эллиптикалық қисығының нүктелері» деп аталады; x және y - сәйкесінше x- және y – нүкте координаталары деп аталады.

Нүкте қисық эллиптиялық Q (x, y) тең болады, егер олардың тиісті x-и y-координаты қисық екі нүктесі белгіленеді немесе жай ғой. эллиптиялық тең.

Е арналған барлық нүктелерінің тиер эллиптиялық таңбаланушы "+" белгісімен, қисық қосу әрекеті айқындалды. $Q_1(x_1,y_1)$ және $Q_2(x_2,y_2)$ үшін кез келген екі нүкте (x1, y1) қисық эллиптиялық Е бірнеше жағдайлары қарайды.

Координаталары $x_1 \neq x_2$ шартына сәйкес Q_1 және Q_2 нүктелері үшін олардың қосындысы $Q_3(x_3, y_3)$ нүктесі деп аталады, оның координаталары

$$\begin{cases} x_3 \equiv \lambda^2 - x_1 - x_2 (mod\ p), \\ y_3 \equiv \lambda(x_1 - x_3) - y_1 (mod\ p), \end{cases} \quad (3)$$

теңдеулерімен анықталады, бұл жерде $\boldsymbol{\lambda} \equiv \frac{y_2 - y_1}{x_2 - x_1} (mod\ p)$.

Егер $x_1 = x_2$ және $y_1 = y_2 \neq 0$ теңдіктері орындалса, онда Q_3 нүктесінің координаталары мынандай жолмен анықталады:

$$\begin{cases} x_3 \equiv \lambda^2 - 2x_1 (mod\ p), \\ y_3 \equiv \lambda(x_1 - x_3) - y_1 (mod\ p), \end{cases} \quad (4)$$

бұл жерде $\boldsymbol{\lambda} \equiv \frac{3x_1^2 + a}{2y_1} (mod\ p)$.

Егер $x_1 = x_2$ және $y_1 = -y_2 (\text{mod } p)$ шарттары орындалса, онда Q_1 және Q_2 нүктелерінің қосындысы оның *x*- және *y*- координаталарының анықтамасынсыз *O* нөлдік нүктесі деп аталады. Бұл жағдайда Q_2 нүктесі Q_1 нүктесінің терістеуі деп аталады. *O* нөлдік нүктесі үшін

$$Q+O=O+Q=Q, \quad (5)$$

теңдіктері орындалған, бұл жерде*Q* - *E* эллиптикалық қисығының еркін нүктесі.

Енгізілген қосу операциясына қатысты *E* эллиптикалық қисығының барлық нүктелерінің көптігі нөлдік нүктесімен бірге *m*ретіндегі абелев (коммутативтік) шеткі тобын құрайды,ол үшін теңсіздігі орындалған.

$$p + 1 - 2\sqrt{p} \leq m \leq p + 1 + 2\sqrt{p} \quad (6)$$

Егер әлдебір *P* нүктесі үшін теңдігі орындалса, *Q* нүктесі «*k* еселік нүктесі» деп немесе жай «*E* эллиптикалық қисығының еселік нүктесі» деп аталады.

$$Q = \underbrace{P + \ldots + P}_{k} = kP \quad (7)$$

5.2 Сандық қолтаңба параметрлері

Сандық қолтаңба схемасының параметрлері:

- *p* қарапайым саны – эллиптикалық қисықтың модулі;
- *E* эллиптикалық қисығы, өзінің *J(E)* инвариантымен немесе $a, b \in F_p$ коэффициенттерімен беріледі;
- *m* бүтін саны- *E* эллиптикалық қисығы нүктелер тобының реті;
- *q* бүтін саны - *E* эллиптикалық қисығы нүктелер тобы циклдік шағын тобының реті, ол үшін мынадай шарттар орындалған:

$$\begin{cases} m = nq, \ \ n \in Z, \ \ n \geq 1 \\ 2^{254} < q < 2^{256} \textit{ немесе } 2^{508} < q < 2^{512}; \end{cases} \quad (8)$$

- координаталары (x_p,y_p), $qP=O$ теңдігіне сәйкес *E* эллиптикалық қисығының $P \neq O$ нүктесі.

- $V^* \to V_1$ хэш-функциясы еркін шеткі ұзындықтардың екілік векторлар түріндегі l бит ұзындықты екілік векторларға хабарларды көрсетеді. Хэш-функция ҚР СТ ГОСТ Р 34.11-2012 анықталған. Егер $2^{254}<q<2^{256}$ болса, онда l =256. Егер $2^{508}<q<2512$ болса,онда l=512.

Сандық қолтаңба схемасының әрбір қолданушысының мынандай жеке кілттері болуы тиіс:

- қолтаңба кілті - $0 <d<q$ теңсіздігіне сәйкес келетін d бүтін саны;

- қолтаңбаны тексеру кілті - $dP = Q$ теңдігіне сәйкес келетін координаталары (x_q,y_q) Q_c эллиптикалық қисық нүктесі.

Сандық қолтаңба схемасының жоғарыда келтірілген параметрлеріне мынандай талаптар қойылады:

- барлық t=1,2,...,B бүтіндері үшін $p^t \neq 1 \pmod q$ шарты орындалуы тиіс, егер $2^{254}<q<2^{256}$ және B= 131 болса, егер $2^{508}<q<2^{512}$болса,бұл жерде B =31;

- $m \neq p$ теңсіздігі орындалуы тиіс;

- қисықтың инварианты $J(E)\neq 0$, және $J(E)\neq 1728$ шартына сәйкес болуы тиіс.

5.3 Екілік векторлар

Сандық қолтаңбаны қалыптастыру және тексеру процестерін анықтау үшін бүтін сандар мен l бит ұзындықты екілік векторлар арасында сәйкестік орнату қажет.

l бит ұзындықты мынадай екілік векторды қарастырайық, бұл жерде кіші биттар - оң жақта, ал үлкен биттар сол жақта орналасқан:

$$\bar{h} = (\alpha_{l-1}, \dots, \alpha_0), \bar{h} \in V_l \tag{9}$$

бұл жерде α_i,i=0,..,l-1 1-ге немесе 0-ге тең.

Егер

$$\alpha = \sum_{i=0}^{l-1} \alpha_i 2^i \tag{10}$$

теңдігі орындалса, $\alpha \in Z$ саны $\bar{h}$ *екілік векторына сәйкес*.

α және β бүтін сандарына сәйкес келетін

$$\overline{h_1} = (\alpha_{l-1,} \dots, \alpha_0),$$

$$\overline{h_2} = (\beta_{l-1,} \dots, \beta_0) \tag{11}$$

екі екілік векторлары үшін конкатенация (бірігу) операциясы былайша анықталады:

$$\overline{h_1}\|\overline{h_2} = (\alpha_{l-1}, \dots, \alpha_0, \beta_{l-1}, \dots, \beta_0) \quad (12)$$

Бірігу $\overline{h_1}$. *және* $\overline{h_2}$. векторларының коэффициенттерінен құралған 2*l* бит ұзындықты екілік вектор болып табылады. (11) және (12) формулалары 2*l* бит ұзындықты $\overline{h_1}.\|\overline{h_2}$. екілік векторын осылардың конкатенациясы болып табылатын *l* бит ұзындықты екі екілік векторына бөлу тәсілін анықтайды.

6 Негізгі процестер

Бұл тарауда қолданушы хабарыныңтөменгі жағындағы сандық қолтаңбаны қалыптастыру және тексеру процестері анықталған. Бұл процестерді жүзеге асыру үшін сандық қолтаңба схемасының 5.2 талаптарына сәйкес параметрлері барлық қолданушыларға белгілі болуы тиіс. Мұнан өзге, әрбір қолданушының *d* қолтаңба кілті мен $Q(x_q, y_q)$ қолтаңбаны тексеру кілті болуы тиіс, олар да 5.2 талаптарыны сәйкес келуі тиіс.

6.1 Сандық қолтаңбаны қалыптастыру

M ∈*V** хабарының төменгі жағындағы сандық қолтаңбаны алу үшін I алгоритм бойынша мынадай амалдарды (қадамдарды) орындау қажет:

1-қадам - *M* хабарының хэш-кодын есептеп шығу*:*

$$\bar{h}=h(M) \quad (13)$$

2 − қадам h *векторы екілік көрінісі болып табылатын* α *бүтін санын есептеп шығу жәнанықтау*.

$$e \equiv \alpha (mod\ q) \quad (14)$$

Егер *e* = 0 болса, онда *e* = 1 анықтау.

3-қадам - теңсіздігіне сәйкес келетін кездейсоқ (жалған кездейсоқ) *k* бүтін санын генерациялау.

$$0<k<q \quad (15)$$

4-қадам - *C* = *kP* эллиптикалық қисықтың нүктесін есептеп шығу және анықтау,

$$r \equiv x_c (mod\ q), \tag{16}$$

бұл жерде x_c-x – C нүктесінің координатасы.

Егер r = 0 болса, онда 3-қадамға қайтып оралу керек.

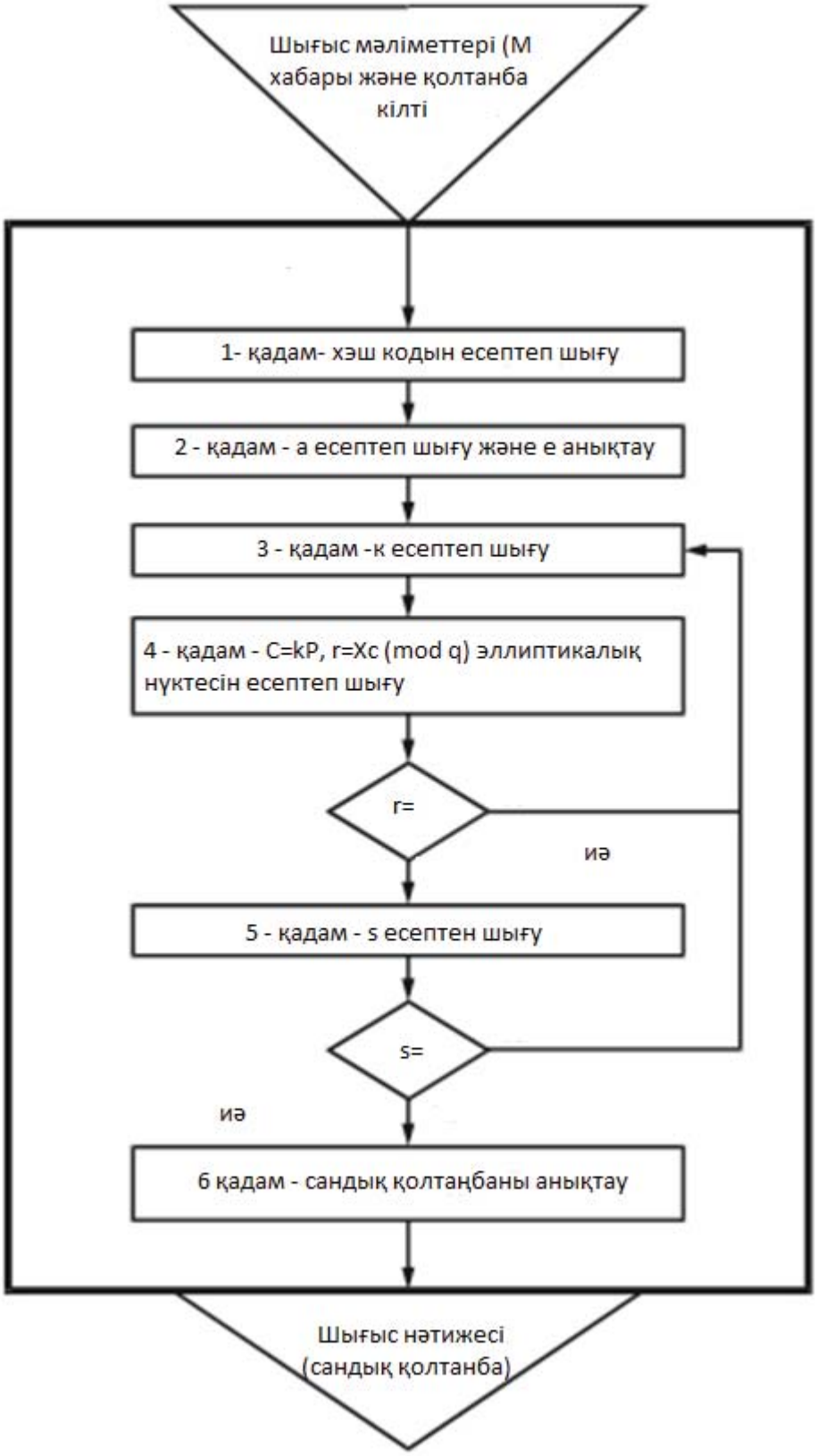
5-қадам - мәнін есептеп шығу.

$$s \equiv (rd + ke)(mod\ q). \tag{17}$$

Егер s = 0 болса, онда 3-қадамға қайтып оралу керек.

6-қадам - r және s *сәйкес келетін* $\bar{r}$ *және* $\bar{s}$ *және* x екілік векторларын есептеп шығу және екі екілік векторының конкатенациясы ζ=$\bar{r}||\bar{s}$ сандық қолтаңбасын анықтау.

Бұл процестің бастапқы деректері қолтаңба кілті d мен қол қойылатын M хабары, ал шығатын нәтижесі - ζ сандық қолтаңбасы болып табылады. Сандық қолтаңбаны қалыптастыру процесінің схемасы 2-суретте келтірілген.



Сурет 2 – Сандық қолтаңбаны қалыптастыру процесінің схемасы

6.2 Сандық қолтаңбаны тексеру

Алынған M хабарының төменгі жағындағы ζ сандық қолтаңбасын тексеру үшін II алгоритм бойынша мынадай амалдарды (қадамдарды) орындау қажет:

1-қадам – алынған ζ қолтаңбасы бойынша r және s бүтін сандарын есептеп шығу. Егер$0<r<q$, $0<s<q$ теңсіздігі орындалса, онда мынадай қадамға көшу керек. Олай болмаған күнде қолтаңба қате деген сөз.

2-қадам - алынған M хабарының хэш-кодын есептеп шығу:

$$\bar{h} = h(M) \tag{18}$$

3-қадам - $\bar{h}$ векторы екілік көрінісі *болып табылатын* α *бүтін санын есептеп шығу және*

$$e \equiv \alpha(mod\ q) \tag{19}$$

анықтау.

Егерe = 0 болса, онда e = 1 екенін анықтау керек.

4-қадам -$v \equiv e^{-1}(mod\ q)$ мәнін есептеп шығу (20)

5-қадам - мәндерін есептеп шығу

$$z_1 \equiv sv(mod\ q), z_2 \equiv -rv(mod\ q) \tag{21}$$

6-қадам - $C=z_1P+z_2Q$ эллиптикалық қисықтың нүктесін есептеп шығу және

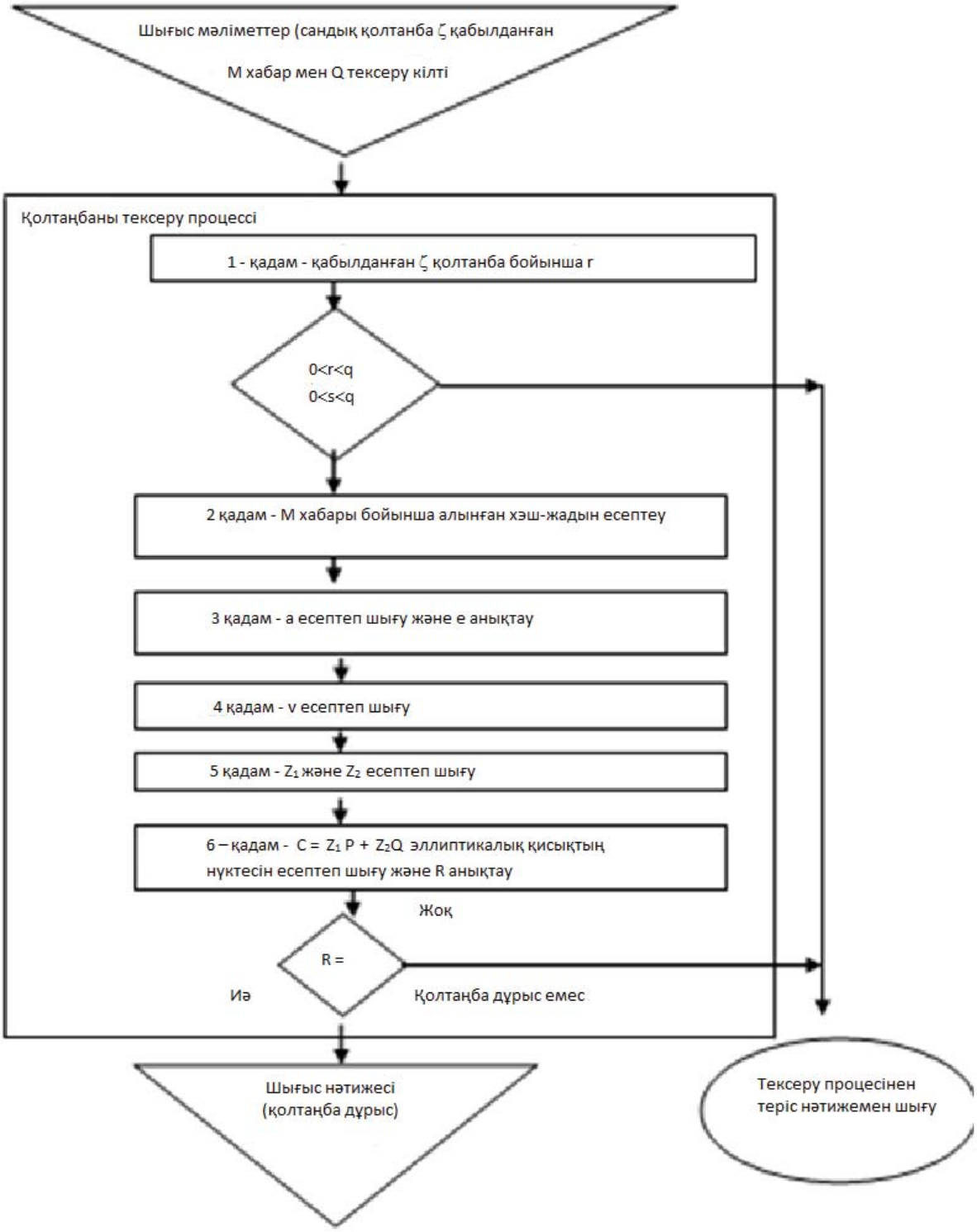
$$R \equiv x_c(mod\ q) \tag{22}$$

анықтау, бұл жерде x_c–x- C нүктесінің координатасы.

7-қадам – егер $R = r$ теңдігі орындалса, онда қолтаңба қабылданады. Олай болмаған күнде қолтаңба қате деген сөз.

Бұл процестің бастапқы деректері қол қойылған M хабары, ζ сандық қолтаңбасы және қолтаңбаны тексеру кілті Q, ал шығатын нәтижесі – осы қолтаңбаның ақиқаттығының немесе қате екендігінің дәлелі болып табылады.

Сандық қолтаңбаны тексеру процесінің схемасы 3-суретте келтірілген.



Сурет 3– Сандық қолтаңбаны тексеру процесінің схемасы

А қосымшасы
(ақпараттық)

Бақылау мысалдары

Төменде келтірілген *p, a, b, m, q, P* параметрлерінің, сондай-ақ *d* және *Q* қолтаңба кілттері мен қолтаңбаны тексеру мәндерін осы стандартта сипатталған алгоритмдерді нақты жүзеге асыруды түзету жұмыстарына ғана пайдалануға кеңес беріледі.

Барлық сандық мәндер ондық және он алтылық жазбада келтірілген. Сандар жазбасындағы төменгі индекс есептеу жүйесінің негізін білдіреді. «\\» белгісі сандардың жаңа жолға тасымалдануын білдіреді. Мысалы,

$12345\backslash\backslash$

67890_{10}

$499602D2_{16}$

жазбасы 1234567890 бүтін санын сәйкесінше ондық және он алтылық есептеу жүйелерінде көрсетеді.

А.1 1-мысал

А.1.1 Сандық қолтаңба схемасының параметрлері

Сандық қолтаңбаны қалыптастыру және тексеру үшін мынадай параметрлер пайдаланылуы тиіс (қара 5.2).

А.1.1.1. Эллиптикалық қисықтың модулі

Бұл мысалда *p* параметріне мынадай мән берілген:

p= 57896044618658097711785492504343953926\\
$6349923328202820197287920039565648210 41_{10}$

p=8000000000000000000000000000000000000000000000000000000000000431$_{16}$.

А.1.1.2 Эллиптикалық қисықтың коэффициенттері

Бұл мысалда *a* және *b* параметрлері мынадай мәндерге ие болады:

$a = 7_{10}$,

$a = 7_{16}$,

b = 4330887654676727690576590459565093199 5\\
$9421117944510395832529688420338495804 14_{10}$,

b=5FBFF498AA938CE739B8E022FBAFEF40563F6E6A3472FC2A514C0CE9DAE23B7E$_{16}$.

А.1.1.3 Эллиптикалық қисық нүктелері тобының реті

Бұл мысалда *m* параметрі мынадай мәнге ие болады:

m = 57896044618658097711785492504343953 92\\
$7082934583725450622380973592137631069 619_{10}$,

m=8000000000000000000000000000000150FE8A1892976154C59CFC193ACCF5B3$_{16}$

А.1.1.4 Эллиптикалық қисық нүктелері тобы циклдік шағын тобының реті

Бұл мысалда q параметрі мынадай мәнге ие болады:

q = 57896044618658097711785492504343953927082934583725450622380973592137631069619$_{10}$,

q=8000000000000000000000000000000150FE8A1892976154C59CFC193ACCF5B3$_{16}$

А.1.1.5 Эллиптикалық қисық нүктесінің коэффициенті

Бұл мысалда P нүктесінің координаталары мынадай мәндерге ие болады:

x_p= 2$_{10}$,

x_p= 2$_{16}$,

y_p= 40189740565390375033354494229370597756357393899055450806909793652134315662801$_{0}$,

y_p= 8E2A8A0E65147D4BD6316030E16D19C85C97F0A9CA267122B96ABBCEA7E8FC8$_{16}$.

А.1.1.6 Қолтаңба кілті

Бұл мысалда қолданушы d қолтаңбасының мынадай кілтіне ие деп саналады

d = 55441196065363246126355624130324183196576709222340016572108097750006097525544$_{10}$,

d = 7A929ADE789BB9BE10ED359DD39A72C11B60961F49397EEE1D19CE9891EC3B28$_{16}$

А.1.1.7 Қолтаңбаны тексеру кілті

Бұл мысалда қолданушы координаталары мынадай мәндерге ие Q қолтаңбаны тексеру кілтіне ие деп саналады:

x_q= 57520216126176808443631405023338071176630104906313632182896741342206604859403$_{10}$,

x_q= 7F2B49E270DB6D90D8595BEC458B50C58585BA1D4E9B788F6689DBD8E56FD80B$_{16}$,

y_q= 17614944419213781543809391949654080319426620453636392607098478594382867639940$_{10}$,

y_q= 26F1B489D6701DD185C8413A977B3CBBAF64D1C593D26627DFFB101A87FF77DA$_{16}$.

А.1.2 Сандық қолтаңбаны қалыптастыру процесі (I алгоритм)

I алгоритм бойынша 1 – 3 қадамдар орындалған соң (қара. 6.1) мынадай сандық мәндер алынған болсын:

a = 20798893674476452017134061561508270130637142515379653289952617252661468872421$_{10}$,

a = 2DFBC1B372D89A1188C09C52E0EEC61FCE52032AB1022E8E67ECE6672B043EE5$_{16}$,

k = 53854137677348463731403841147996619241504003434302020712960838528893196233395$_{10}$,

k = 77105C9B20BCD3122823C8CF6FCC

$7B956DE33814E95B7FE64FED924594DCEAB3_{16}$.

Бұл жерде $C = k\,P$ еселік нүктесі мынандай координаталарға ие:

x_c= 29700980915817952874371204983938256 9\\
$90422752107994319651632687982059210933395_{10}$,

x_c= 41AA28D2F1AB148280CD9ED56FED\\
$A41974053554A42767B83AD043FD39DC0493_{16}$,

y_c= 32842535278684663477094665322517084 5\\
$06804721032454543268132854556539274060910_{10}$,

y_c= 489C375A9941A3049E33B34361DD\\
$204172AD98C3E5916DE27695D22A61FAE46E_{16}$.

$r = x_c \ (mod\ q)$ параметрі мынандай мәнге ие болады:

r = 29700980915817952874371204983938256 9\\
$90422752107994319651632687982059210933395_{10}$,

r = 41AA28D2F1AB148280CD9ED56FED\\
$A41974053554A42767B83AD043FD39DC0493_{16}$.

$s = (rd + ke)\ (\mathrm{mod}\ q)$ параметрі мынандай мәнге ие болады:

s = 57497340027008465417892531001914703\\
$84552270426490985639337189991755158395 52_{10}$,

s=1456C64BA4642A1653C235A98A60249BCD6D

А.1.3 Сандық қолтаңбаны тексеру процессі (II алгоритм)

II алгоритм бойынша 1 – 3 қадамдар орындалған соң (қара 6.2) мынадай сандық мәндер алынған болсын:

e= 20798893674476452017134061561508270 13\\
$06371425153796532899526172526614688724 21_{10}$.

e= 2DFBC1B372D89A1188C09C52E0EE\\
$C61FCE52032AB1022E8E67ECE6672B043EE5_{16}$.

Бұл жерде $v = e^{-1}\,(mod\ q)$ параметрі мынадай мәнге ие болады:

v = 17686683605934468677301713824900268 5\\
$62746883080675496715288036572431145718978_{10}$,

v = 271A4EE429F84EBC423E388964555BB\\
$29D3BA53C7BF945E5FAC8F381706354C2_{16}$.

$z_1 \equiv sv\,(mod\ q)$ және $z_2 \equiv -\,rv\,(\mathrm{mod}\ q)$ параметрлері мынадай мәнге ие болады:

z_1 = 37699167500901938556841057293512656 1\\
$08841345190491942619304532412743720999759_{10}$,

z_1 = 5358F8FFB38F7C09ABC782A2DF2A\\
$3927DA4077D07205F763682F3A76C9019B4F_{16}$,

z_2 = 14171998427343472112515917969500765 7\\
$69246655838972862114499932653333671092 21_{10}$,

z_2 = 3221B4FBBF6D101074EC14AFAC2D4F7\\
$EFAC4CF9FEC1ED11BAE336D27D527665_{16}$.

$C = z_1P + z_2Q$ нүктесі мына координаталарға ие:

x_c= 29700980915817952874371204983938256 99\\
$04227521079943196516326879820592109333 95_{10}$,

x_c= 41AA28D2F1AB148280CD9ED56FED\\
$A41974053554A42767B83AD043FD39DC0493_{16}$,

y_c = 32842535278684663477094665322517084 50\\

$$68047210324545432681328545565392740609\,10_{10},$$

$$y_c = 489C375A9941A3049E33B34361DD\backslash\backslash$$
$$204172AD98C3E5916DE27695D22A61FAE46E_{16}.$$

Сонда $R = x_c (mod\ q)$ параметрі мына мәнге ие болады:

$$R = 297009809158179528743712049839382569\,9\backslash\backslash$$
$$042275210799431965163268798205921093339\,5_{10},$$

$$R = 41AA28D2F1AB148280CD9ED56FED\backslash\backslash$$
$$A41974053554A42767B83AD043FD39DC0493_{16}.$$

$R=r$ теңдігі орындалғандықтан, сандық қолтаңба қабылданады.

А.2 2-мысал

А.2.1 Сандық қолтаңба схемасының параметрлері

Сандық қолтаңбаны қалыптастыру және тексеру үшін мынадай параметрлер пайдаланылуы тиіс (қара 5.2).

А.2.1.1 Эллиптикалық қисықтың модулі

Бұл мысалда p параметріне мынадай мән берілген:

$$p = 36239861022290036359077887536838743060213209255346786050\backslash\backslash$$
$$86546150450856166624002482588482022271496854025090823603\,05\backslash\backslash$$
$$87351637342638223719649872285829073724\,03_{10},$$

$$p = 4531ACD1FE0023C7550D267B6B2FEE80922B14B2FFB90F04D4EB7C09B5D2D15D\backslash\backslash$$
$$F1D852741AF4704A0458047E80E4546D35B8336FAC224DD81664BBF528BE6373_{16}.$$

А.2.1.2 Эллиптикалық қисықтың коэффициенті

Бұл мысалда a және b параметрлері мынадай мәндерге ие болады:

$$a = 7_{10},$$

$$a = 7_{16},$$

$$b = 151865506921082853450895003471404315492874752774020643\,6\backslash\backslash$$
$$19401882335280998244379373282975691478597467486604160539788367\,75\backslash\backslash$$
$$96626326413990136959047435811826396_{10},$$

$$b = 1CFF0806A31116DA29D8CFA54E57EB748BC5F377E49400FDD788B649ECA1AC4\backslash\backslash$$
$$361834013B2AD7322480A89CA58E0CF74BC9E540C2ADD6897FAD0A3084F302ADC_{16}.$$

А.2.1.3 Эллиптикалық қисық нүктелері тобының реті

Бұл мысалда m параметрі мынадай мәнге ие болады:

$$m = 362398610222900363590778875368387430602132092553467860508654\,61\backslash\backslash$$
$$504508561666239691648983050328630684999614040794379365854558651922\,12\backslash$$
$$97073480881261812061974\,3_{10},$$

$$m = 4531ACD1FE0023C7550D267B6B2FEE80922B14B2FFB90F04D4EB7C09B5D2D15D\backslash\backslash$$
$$A82F2D7ECB1DBAC719905C5EECC423F1D86E25EDBE23C595D644AAF187E6E6DF_{16}.$$

А.2.1.4 Эллиптикалық қисық нүктелері тобы циклдік шағын тобының реті

Бұл мысалда qпараметрі мынадай мәнге ие болады:

$$q = 362398610222900363590778875368387430602132092553467860508654\,61\backslash\backslash$$
$$504508561666239691648983050328630684999614040794379365854558651922\,12\backslash\backslash$$

$$970734808812618120619743_{10},$$

q=4531ACD1FE0023C7550D267B6B2FEE80922B14B2FFB90F04D4EB7C09B5D2D15D\\
A82F2D7ECB1DBAC719905C5EECC423F1D86E25EDBE23C595D644AAF187E6E6DF$_{16}$.

А.2.1.5 Эллиптикалық қисық нүктесінің коэффициенттері

Бұл мысалда P нүктесінің координаталары мынадай мәндерге ие болады:

x_p=19283569440670228493993094012431375989977866354595079743570754913077665\\
92685835441065557681003184874819658004903212332884252335830250729527632 38\\
$$3493573274_{10},$$

x_p=24D19CC64572EE30F396BF6EBBFD7A6C5213B3B3D7057CC825F91093A68CD762\\
FD60611262CD838DC6B60AA7EEE804E28BC849977FAC33B4B530F1B120248A9A$_{16}$,

y_p=22887286933719728599700121555294784163535623273295061803\\
14497425931102860301572814141997072271708807066593850650334152381 8\\
$$57347798885864807605098724013854_{10},$$

y_p= 2BB312A43BD2CE6E0D020613C857ACDDCFBF061E91E5F2C3F32447C259F39B2\\
C83AB156D77F1496BF7EB3351E1EE4E43DC1A18B91B24640B6DBB92CB1ADD371E$_{16}$.

А.2.1.6 Қолтаңба кілті

Бұл мысалда қолданушы d қолтаңбасының мынадай кілтіне ие деп саналады:

d=61008180413637309821953815323984758300684551906953156298238 8135\\
35489060630178225538360839342337237905766552759511682730702504645883\\
$$744076612118046687586 0_{10},$$

d=BA6048AADAE241BA40936D47756D7C93091A0E8514669700EE7508E508B102072\\
E8123B2200A0563322DAD2827E2714A2636B7BFD18AADFC62967821FA18DD4$_{16}$.

А.2.1.7 Қолтаңбаны тексеру кілті

Бұл мысалда қолданушы координаталары мынадай мәндерге ие Q қолтаңбаны тексеру кілтіне ие деп саналады:

x_q=90954685300253659655669076866983031000692927254655628159 63\\
72965370312498563182320436892870052842808608262832456858223580\\
$$7137802907179868558634334311505 61_{10},$$

x_q=115DC5BC96760C7B48598D8AB9E740D4C4A85A65BE33C1815B5C320C854621D\\
D5A515856D13314AF69BC5B924C8B4DDFF75C45415C1D9DD9DD33612CD530EFE1$_{16}$.

y_q= 29214572033744256206324497342484154556407008235594887051648958\\
37509539134297327397380287741428246088626609329139441895016863758\\
$$9841063266005724768223720 76_{10},$$

y_q= 37C7C90CD40B0F5621DC3AC1B751CFA0E2634FA0503B3D52639F5D7FB72AFD6\\
1EA199441D943FFE7F0C70A2759A3CDB84C114E1F9339FDF27F35ECA93677BEEC$_{16}$.

А.2.2 Сандық қолтаңбаны қалыптастыру процесі (I алгоритм)

I алгоритм бойынша 1 – 3 қадамдар орындалған соң (қара. 6.1) мынадай сандық мәндер алынған болсын:

e=28979638816828685755628272785538650491737451978718251995629 47\\
41904138895097053666110955349995424873308871974884453896464128165 44\\
$$6351329697382770627204596 4_{10},$$

e=3754F3CFACC9E0615C4F4A7C4D8DAB531B09B6F9C170C533A71D147035B0C591\\

7184EE536593F4414339976C647C5D5A407ADEDB1D560C4FC6777D2972075B8C$_{16}$,

k=1755163560258504995406282799211252803334510317477377916502\\
0814424318205707503444610298675096250890922723586612687247351680781055417\\
47529710309879958632945$_{10}$,

k=359E7F4B1410FEACC570456C6801496946312120B39D019D455986E364F3\\
65886748ED7A44B3E794434006011842286212273A6D14CF70EA3AF71BB1AE679F1$_{16}$.

Бұл жерде C = k P еселік нүктесі мына координаталарға ие

x_c=248920447703134926507286464303214775366745131928213144402749863 73\\
576110928102217951018714129288237168059598287083302842436534530853\\
22004442442534151761462$_{10}$,

x_c=2F86FA60A081091A23DD795E1E3C689EE512A3C82EE0DCC2643C78EEA8FCAC\\
D35492558486B20F1C9EC197C90699850260C93BCBCD9C5C3317E19344E173AE36$_{16}$,

y_c=770173889928991836047844798780960441682062631876096137673946801 50\\
24422293532765176528442837832456936422662546513702148162933079517\\
0843005015210864150831 0$_{10}$,

y_c=EB488140F7E2F4E35CF220BDBC75AE44F26F9C7DF52E82436BDE80A91831DA27\\
C8100DAA876F9ADC0D28A82DD3826D4DC7F92E471DA23E55E0EBB3927C85BD6$_{16}$.

$r = x_c(mod\ q)$ параметрімына мәнге ие болады

r=248920447703134926507286464303214775366745131928213144402749863 73\\
576110928102217951018714129288237168059598287083302842436534530853\\
22004442442534151761462$_{10}$,

r=2F86FA60A081091A23DD795E1E3C689EE512A3C82EE0DCC2643C78EEA8FCAC\\
D35492558486B20F1C9EC197C90699850260C93BCBCD9C5C3317E19344E173AE36$_{16}$.

$s = (rd + ке)$ ($mod\ q$) параметрімына мәнге ие болады

s =864523221707669519038849297382936917075023735848431579919598 7\\
993133851805647488771956396724601794217607708932780309568076901 15\\
82270990385368283183515937 0$_{10}$,

s=1081B394696FFE8E6585E7A9362D26B6325F56778AADBC081C0BFBE933D52FF58\\
23CE288E8C4F362526080DF7F70CE406A6EEB1F56919CB92A9853BDE73E5B4A$_{16}$.

А.2.3 Сандық қолтаңбаны тексеру процесі (II алгоритм)

II алгоритм бойынша 1 – 3 қадамдар орындалған соң (қара. 6.2) мынадай сандық мәндер алынған болсын:

e=289796388168286857556282727855386504917374519787182519956 2947\\
419041388950970536661109553499954248733088719748844538964641281 6544\\
63513296973827706272045964$_{10}$,

e=3754F3CFACC9E0615C4F4A7C4D8DAB531B09B6F9C170C533A71D147035B0C591\\
7184EE536593F4414339976C647C5D5A407ADEDB1D560C4FC6777D2972075B8C$_{16}$.

Бұл жерде $v = e^{-1}(mod\ q)$ параметрімынадай мәнге ие болады

v=255694215394605222266074084316408615387769223440078319114692849\\
356194345732344708924001925205698280688153534004145821243990606136\\
70722381859348159602526 71$_{10}$,

v=30D212A9E25D1A80A0F238532CADF3E64D7EF4E782B6AD140AAF8BBD9BB4729\\
84595EEC87B2F3448A1999D5F0A6DE0E14A55AD875721EC8CFD504000B3A840FF$_{16}$.

z_1= sv(mod q) және z_2 =-rv(mod q) параметрлері мынадай мәндерге ие болады:

z_1=320647082733676862968690710187347525034330644808903031121 4484\\

$$38587274320504518034520882655290100349673294104978035779354194205 5\backslash\backslash$$
$$60008495619817370719790257 5_{10},$$
$$z_1=3D38E7262D69BB2AD24DD81EEA2F92E6348D619FA45007B175837CF13B026079\backslash\backslash$$
$$051A48A1A379188F37BA46CE12F7207F2A8345459FF960E1EBD5B4F2A34A6EEF_{16},$$
$$z_2=13667709118340031081429778480218475973204553475356412734827\backslash\backslash$$
$$32082047028342168006031261814273230879203690726448631222679743757 5\backslash\backslash$$
$$61637266958056805859603008203_{10},$$
$$z_2=1A18A31602E6EAC0A9888C01941082AEFE296F840453D2603414C2A16EB6FC529\backslash\backslash$$
$$D8D8372E50DC49D6C612CE1FF65BD58E1D2029F22690438CC36A76DDA444ACB_{16}.$$

$C = z_1P + z_2Q$ нүктесі мынадай координаталарға ие:

$$x_c= 24892044770313492650728646430321477536674513192821314440274986 37\backslash\backslash$$
$$35761109281022179510187141292882371680595982870833028424365345308 53\backslash\backslash$$
$$22004442442534151761462_{10},$$
$$x_c=2F86FA60A081091A23DD795E1E3C689EE512A3C82EE0DCC2643C78EEA8FCAC\backslash\backslash$$
$$D35492558486B20F1C9EC197C90699850260C93BCBCD9C5C3317E19344E173AE36_{16},$$
$$y_c=77017388992899183604784479878096044168206263187609613767394680 15\backslash\backslash$$
$$02442229353276517652844283783245693642266254651370214816293307951 70\backslash\backslash$$
$$8430050152108641508310_{10},$$
$$y_c=EB488140F7E2F4E35CF220BDBC75AE44F26F9C7DF52E82436BDE80A91831DA27\backslash\backslash$$
$$C8100DAA876F9ADC0D28A82DD3826D4DC7F92E471DA23E55E0EBB3927C85BD 6_{16}$$

Онда $R= x_c(mod\ q)$ параметрі мынадай мәнге ие болады

$$R=24892044770313492650728646430321477536674513192821314440274986\backslash\backslash$$
$$37357611092810221795101871412928823716805959828708330284243653453085\backslash\backslash$$
$$32200444244253415176146 2_{10},$$
$$R=2F86FA60A081091A23DD795E1E3C689EE512A3C82EE0DCC2643C78EEA8FCAC\backslash\backslash$$
$$D35492558486B20F1C9EC197C90699850260C93BCBCD9C5C3317E19344E173AE36_{16}.$$

$R=r$ теңдігі орындалғандықтан, сандық қолтаңба қабылданады.

Библиография

[1] ISO 2382-2:1976 (ISO 2382-2:1976) Ақпарат жүйесін өңдеу. Сөздік. 2. Бөлім. Арифметикалық және логикалық операциялар (Data processing — Vocabulary — Part 2: Arithmetic and logic operations)

[2] ISO/IEC 9796-2:2010 (ISO/IEC 9796-2:2010) Ақпараттық технология. Қауіпсіздікті қамтамасыз ету әдістері. Хабарламаны қалпына келтіруді қамтамасыз ететін сандық қолтаңба сызбасы. 2.бөлім. Бүтін сандық факторизациялау негізіндегі механизмдер (Information technology —Security techniques — Digital signatures with appendix — Part 2: Integer factorization based mechanisms)

[3] ISO/IEC 9796-3:2006 (ISO/IEC 9796-3:2006) Ақпараттық технология. Қауіпсіздікті қамтамасыз ету әдістері. Хабарламаны қалпына келтіруді қамтамасыз ететін сандық қолтаңба сызбасы. 3.бөлім. Дискреттік логарифм негізіндегі механизмдер (Information technology — Security techniques — Digital signature schemes giVing message recoVery — Part 3: Discrete logarithm based mechanisms)

[4] ISO/IEC 14888-1:2008 (ISO/IEC 14888-1:2008) Ақпараттық технология. Қорғаныс әдістері. Қосымшасымен сандық қолтаңба. 1. Бөлім. Жалпы ережелер (Information technology — Security techniques — Digital signatures with appendix — Part 1: General)

[5] ISO/IEC 14888-2:2008 (ISO/IEC 14888-2:2008) Ақпараттық технология. Қорғаныс әдістері. Сандық қолтаңба қосымшасымен. 2. Бөлім. Жалпы ережелер. Көбейткішті жіктеуге арналған негізіндегі механизмдер (Information technology — Security techniques — Digital signatures with appendix — Part 2: Integer factorization based mechanisms)

[6] ISO/IEC 14888-3:2006 (ISO/IEC 14888-3:2006) Ақпараттық технология. Қорғаныс әдістері. Қосымшасымен сандық қолтаңба. 3. Бөлім. Дискреттік логарифм негізіндегі механизм (Information technology — Security techniques — Digital signatures with appendix — Part 3: Discrete logarithm based mechanisms)

[7] ISO/IEC 14888-3:2006/Өзгеру.1:2010 (ISO/IEC 14888-3:2006/ Amd1:2010) Ақпараттық технология. Қорғаныс әдістері. Сандық қолтаңба қосымшасымен. 3-бөлім. Дискреттік логарифм негізіндегі механизм. Өзгеріс 1. Эллиптикалық қисықтағы орсы сандық қолтаңбасының алгоритмі, Шнорр сандық қолтаңбасының алгоритмі, эллиптикалық қисық үшін Шнорр сандық қолтаңбасының алгоритмі жәнеэллиптикалық қисық үшін Шнорр сандық қолтаңбасының толық (Informationtechnology — Securitytechniques — Digital signatures with appendix — Part 3: Discrete logarithm based mechanisms. Amendment 1. Elliptic CurVe Russian Digital Signature Algorithm, Schnorr Digital Signature Algorithm, Elliptic CurVeSchnorr Digital Signature Algorithm, and Elliptic CurVe Full Schnorr Digital Signature Algorithm)

[8] ISO/IEC 10118-1:2000 (ISO/IEC 10118-1:2000) Ақпараттық технология. Ақпараттарды қорғау әдістері. Хэш-қызмет. 1-бөлім Жалпы ережелер. (Information technology — Security techniques — Hash-functions — Part 1: General)

[9] ISO/IEC 10118-2:2010 (ISO/IEC 10118-2:2010) Ақпараттық технология. Ақпараттарды қорғау әдістері. Хэш-қызметі. 2 -бөлім. *n*-битті блокты алгоритмдік шифрлауды пайдалананатын хэш-қызметі (Information technology — Security techniques — Hash-functions — Part 2: Hash-functions using an *n*-bitblock cipher)

[10] ISO/IEC 10118-3:2004 (ISO/IEC 10118-3:2004) Ақпараттық технология. Ақпараттарды қорғау әдістері. Хэш-қызметі. 3-бөлім. Бөлінген хэш-қызметтер (Information technology — Security techniques — Hash-functions — Part 3: Dedicated hash-functions)

[11] ISO/IEC 10118-4:1998 (ISO/IEC 10118-4:1998) Ақпараттық технология. Ақпараттарды қорғау әдістері. Хэш-қызметі. 4-бөлім. Қалдық класстарда арифметиканы пайдаланатын хэш-қызметі (Information technology — Security techniques — Hash-functions — Part 4: Hash function susing modular arithmetic)

ӘОЖ 681.3.06:006.354 **МСЖ 35.040**

Түйінді сөздер: деректерді өңдеу, деректерді беру, ақпарат алмасу, хабарлар, сандық қолтаңбалар, ақпаратты қорғау, сандық қолтаңбаны қалыптастыру, сандық қолтаңбаны тексеру.

НАЦИОНАЛЬНЫЙ СТАНДАРТ РЕСПУБЛИКИ КАЗАХСТАН

Информационная технология
Криптографическая защита информации

ПРОЦЕССЫ ФОРМИРОВАНИЯ И ПРОВЕРКИ ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ

СТ РК ГОСТ Р 34.10-2015

(ГОСТ Р 34.10-2012 Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи, IDT)

Издание официальное

Комитет технического регулирования и метрологии
Министерства по инвестициям и развитиюРеспублики Казахстан
(Госстандарт)

Астана

Предисловие

1 ПОДГОТОВЛЕН И ВНЕСЕН Акционерное общество «Казахская академия транспорта и коммуникаций им. М.Тынышпаева».

2 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Председателя Комитета технического регулирования и метрологии Министерства по инвестициям и развитию Республики Казахстан от 18 декабря 2015 года № 262-од

3 Настоящий стандарт идентичен ГОСТ Р 34.10-2012 «Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи»

Официальный экземпляр стандарта иностранного государства, на основе которого разработан настоящий стандарт, и на которые даны ссылки, имеются в Едином Государственном фонде нормативных технических документов.

Официальной версией является текст на государственном и русском языках.

Степень соответствия – идентичная (IDT).

4 В настоящем стандарте реализованы Закон Республики Казахстан «О техническом регулировании» № 603 от 9 ноября 2004 года, Закона Республики Казахстан «О языках в Республике Казахстан» № 151 от 11 июля 1997 года и Закона Республики Казахстан «О информатизации» от 11 января 2007 года № 217–III (с изменениями и дополнению по состоянию на 29.12.2014).

5 СРОК ПЕРВОЙ ПРОВЕРКИ **2022 год**
ПЕРИОДИЧНОСТЬ ПРОВЕРКИ **5 лет**

6 ВВЕДЕН ВПЕРВЫЕ

Информация об изменениях к настоящему стандарту публикуется в ежегодно издаваемом информационном указателе «Нормативные документы по стандартизации», а текст изменений и поправок – в ежемесячно издаваемых информационных указателях «Национальные стандарты». В случае пересмотра (замены) или отмены настоящего стандарта соответствующее уведомление будет опубликовано в ежемесячно издаваемом информационном указателе «Национальные стандарты».

Содержание

НАЦИОНАЛЬНЫЙ СТАНДАРТ РЕСПУБЛИКИ КАЗАХСТАН

Информационная технология
Криптографическая защита информации

ПРОЦЕССЫ ФОРМИРОВАНИЯ И ПРОВЕРКИ ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ

Дата введения 2017-01-01

1 Область применения

Настоящий стандарт устанавливает схему электронной цифровой подписи (ЭЦП) (далее - цифровая подпись), процессы формирования и проверки цифровой подписи под заданным сообщением (документом), передаваемым по незащищенным телекоммуникационным каналам общего пользования в системах обработки информации различного назначения. Настоящий стандарт устанавливает и повышает, по сравнению с ранее действовавшей схемой цифровой подписи, уровень защищенности передаваемых сообщений от подделок и искажений.

Настоящий стандарт устанавливает применение при разработке, эксплуатации и модернизации систем обработки информации различного назначения.

2 Нормативные ссылки

Для применения настоящего стандарта необходимы следующие ссылочные нормативные документы. Для недатированных ссылок применяют последнее издание ссылочного документа (включая любые поправки).

ГОСТ Р 34.11-2012 Информационная технология. Криптографическая защита информации. Функция хэширования

3 Термины, определения и обозначения

3.1 Термины и определения

В настоящем стандарте применяются следующие термины с соответствующими определениями:

3.1.1

Дополнение (appendix): Двоичная последовательность, формируемая из цифровой подписи и произвольного текстового поля.

(ISO/МЭК 14888-1:2008 [4])

3.1.2

Ключ подписи (signature key): Элемент секретных данных, специфичный для субъекта и используемый только данным субъектом в процессе формирования цифровой подписи.

(ISO/МЭК 14888-1:2008 [4])

3.1.3

Ключ проверки подписи (verification key): Элемент данных, математически связанный с ключом подписи и используемый проверяющей стороной в процессе проверки цифровой подписи.

(ISO/МЭК 14888-1:2008 [4])

3.1.4

Параметр схемы ЭЦП (domain parameter): Элемент данных, общий для всех субъектов схемы цифровой подписи, известный или доступный всем этим субъектам.

(ISO/МЭК 14888-1:2008 [4])

3.1.5

Подписанное сообщение (signed message): Набор элементов данных, состоящий из сообщения и дополнения, являющегося частью сообщения.

(ISO/МЭК 14888-1:2008 [4])

3.1.6

Последовательность псевдослучайных чисел (pseudo-random number sequence): Последовательность чисел, полученная в результате выполнения некоторого арифметического (вычислительного) процесса, используемая в конкретном случае вместо последовательности случайных чисел.

3.1.7

Последовательность случайных чисел (random number sequence): Последовательность чисел, каждое из которых не может быть предсказано (вычислено) только на основе знания предшествующих ему чисел данной последовательности.

3.1.8

Процесс проверки подписи (verification process): Процесс, в качестве исходных данных которого используются подписанное сообщение, ключ проверки подписи и параметры схемы ЭЦП, результатом которого является заключение о правильности или ошибочности цифровой подписи.

(ISO/МЭК 14888-1:2008 [4])

3.1.9

Процесс формирования подписи (signature process): Процесс, в качестве исходных данных которого используются сообщение, ключ подписи и параметры схемы ЭЦП, а в результате формируется цифровая подпись.

(ISO/МЭК 14888-1:2008 [4])

3.1.10

Свидетельство (witness): Элемент данных, представляющий соответствующее доказательство достоверности (недостоверности) подписи проверяющей стороне.

3.1.11

Случайное число (random number): Число, выбранное из определенного набора чисел таким образом, что каждое число из данного набора может быть выбрано с одинаковой вероятностью.

3.1.12

Сообщение (message): Строка бит произвольной конечной длины.
(ISO/МЭК 14888-1:2008 [4])

3.1.13

Хэш-код (hash-code): Строка бит, являющаяся выходным результатом хэш-функции.
(ISO/МЭК 14888-1:2008 [4])

3.1.14

Хэш-функция (collision-resistant hash-function): Функция, отображающая строки бит в строки бит фиксированной длины и удовлетворяющая следующим свойствам:

1) по данному значению функции сложно вычислить исходные данные, отображаемые в это значение;

2) для заданных исходных данных сложно вычислить другие исходные данные, отображаемые в то же значение функции;

3) сложно вычислить какую-либо пару исходных данных, отображаемых в одно и то же значение.

(ISO/МЭК 14888-1:2008 [4])

Примечание

1 Применительно к области электронной цифровой подписи свойство по перечислению

1) подразумевает, что по известной электронной цифровой подписью невозможно восстановить исходное сообщение; свойство по перечислению

2) подразумевает, что для заданного подписанного сообщения трудно подобрать другое (фальсифицированное) сообщение, имеющее ту же электронную цифровую подпись; свойство по перечислению

3) подразумевает, что трудно подобрать какую-либо пару сообщений, имеющих одну и ту же подпись.

2 В настоящем стандарте в целях сохранения терминологической преемственности с действующими отечественными нормативными документами и опубликованными научно-техническими изданиями установлено, что термины «хэш-функция», «криптографическая хэш-функция», «функция хэширования» и «криптографическая функция хэширования» являются синонимами.

3.1.15

Электронная цифровая подпись (signature); ЭЦП: Строка бит, полученная в результате процесса формирования подписи.

(ISO/МЭК 14888-1:2008 [4])

Примечание

1. Строка бит, являющаяся подписью, может иметь внутреннюю структуру, зависящую от конкретного механизма формирования подписи.

2. В настоящем стандарте в целях сохранения терминологической преемственности с действующими отечественными нормативными документами и опубликованными научно-техническими изданиями установлено, что термины «электронная подпись», «цифровая подпись» и «электронная цифровая подпись» являются синонимами.

3.2 Обозначения

В настоящем стандарте используются следующие обозначения и сокращения:

V_l-множество всех двоичных векторов длиной l бит;

V*-множество всех двоичных векторов произвольной конечной длины;

Z-множество всех целых чисел;

p- простое число, $p>3$,

F_p- конечное простое поле, представляемое как множество из p целых чисел $\{0,1,...,p-1\}$;

$b(\mathrm{mod}p)$- минимальное неотрицательное число, сравнимое с bпо модулю p;

M-сообщение пользователя, $M \in V^*$;

$(\overline{h_1}||\overline{h_2})$- конкатенация (объединение) двух двоичных векторов;

a, b- коэффициенты эллиптической кривой;

m- порядок группы точек эллиптической кривой;

q- порядок подгруппы группы точек эллиптической кривой;

O- нулевая точка эллиптической кривой;

P- точка эллиптической кривой порядка q;

D- целое число - ключ подписи;

Q- точка эллиптической кривой - ключ проверки подписи;

ζ- цифровая подпись под сообщением M.

4 Общие положения

Общепризнанная схема (модель) цифровой подписи (см. ISO/МЭК 14888-1 [4]) охватывает следующие процессы:

- генерация ключей (подписи и проверки подписи);
- формирование подписи;
- проверка подписи.

В настоящем стандарте процесс генерации ключей (подписи и проверки подписи) не рассмотрен. Характеристики и способы реализации данного процесса определяются вовлеченными в него субъектами, которые устанавливают соответствующие параметры по взаимному согласованию.

Механизм цифровой подписи определяется посредством реализации двух основных процессов (см. раздел 6):

-формирование подписи (см. 6.1);

- проверка подписи (см. 6.2).

Цифровая подпись предназначена для аутентификации лица, подписавшего электронное сообщение. Кроме того, использование ЭЦП предоставляет возможность обеспечить следующие свойства при передаче в системе подписанного сообщения:

- осуществление контроля целостности передаваемого подписанного сообщения,

- доказательное подтверждение авторства лица, подписавшего сообщение,

- защита сообщения от возможной подделки.

Схематическое представление подписанного сообщения показано на рисунке 1.

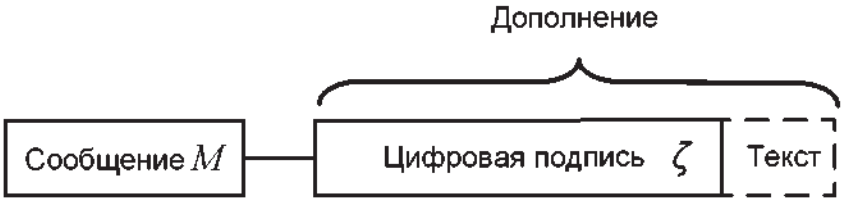


Рисунок 1 – Схема подписанного сообщения

Поле «Текст», показанное на данном рисунке и дополняющее поле «Цифровая подпись», может, например, содержать идентификаторы субъекта, подписавшего сообщение, и/или метку времени.

Установленная в настоящем стандарте схема цифровой подписи должна быть реализована с использованием операций группы точек эллиптической кривой, определённой над конечным простым полем, а также хэш-функции.

Криптографическая стойкость данной схемы цифровой подписи основывается на сложности решения задачи дискретного логарифмирования в группе точек эллиптической кривой, а также на стойкости используемой хэш-функции. Алгоритмы вычисления хэш-функции установлены в ГОСТ Р 34.11-2012.

Параметры схемы цифровой подписи, необходимые для ее формирования и проверки, определены в 5.2. В настоящем стандарте предусмотрена возможность выбора одного из двух вариантов требований к параметрам.

Настоящий стандарт не определяет процесс генерации параметров схемы цифровой подписи. Конкретный алгоритм (способ) реализации данного процесса определяется субъектами схемы цифровой подписи исходя из требований к аппаратно-программным средствам, реализующим электронный документооборот.

Цифровая подпись, представленная в виде двоичного вектора длиной 512 или 1024 бита, должна вычисляться с помощью определенного набора правил, изложенных в 6.1.

Набор правил, позволяющих принять либо отвергнуть цифровую подпись под полученным сообщением, установлен в 6.2.

5 Математические объекты

Для определения схемы цифровой подписи необходимо описать базовые математические объекты, используемые в процессах ее формирования и проверки. В данном разделе установлены основные математические определения и требования, предъявляемые к параметрам схемы цифровой подписи.

5.1 Математические определения

Эллиптической кривой *E,* определенной над конечным простым полем F_p(где p>3 - простое число), называется множество пар чисел (x, y), x, $y \in F_p$, удовлетворяющих уравнению

$$y^2 \equiv x^3 + ax + b (mod p) \quad (1)$$

где a, $b \in F_p$ и $4a^3 + 27b^2$ не сравнимо с нулем по модулю р.

Инвариантом эллиптической кривой называется величина $J(E)$, удовлетворяющая тождеству

$$J(E) \equiv 1728 \frac{4a^3}{4a^3+27b^2} (mod\ p) \quad (2)$$

Пары *(x,y),* где x,y– элементы поля F_p, удовлетворяющие уравнению (1), называются «точками эллиптической кривой *E»; x* и *y* - соответственно *x*- и *y* - координатами точки.

Точка эллиптической кривой обозначается *Q(x, y)* или просто *Q*. Две точки эллиптической кривой равны, если равны их соответствующие *x*-и *y*-координаты.

На множестве всех точек эллиптической кривой *E* определена операция сложения, обозначаемая знаком «+». Для двух произвольных точек $Q_1(x_1,y_1)$ и $Q_2(x_2,y_2)$ эллиптической кривой *E* рассматривают несколько случаев.

Для точек Q_1и Q_2, координаты которых удовлетворяют условию $x_1 \neq x_2$, их суммой называется точка $Q_3(x_3, y_3)$координаты которой определяются сравнениями

$$\begin{cases} x_3 \equiv \lambda^2 - x_1 - x_2 (mod p), \\ y_3 \equiv \lambda(x_1 - x_3) - y_1 (mod p), \end{cases} \quad (3)$$

где $\boldsymbol{\lambda} \equiv \frac{y_2 - y_1}{x_2 - x_1} (mod\ p)$.

Если выполнены равенства $x_1 = x_2$и $y_1 = y_2 \neq 0$, то координаты точки Q_3определяются следующим образом:

$$\begin{cases} x_3 \equiv \lambda^2 - 2x_1 (mod p), \\ y_3 \equiv \lambda(x_1 - x_3) - y_1 (mod p), \end{cases} \quad (4)$$

где $\boldsymbol{\lambda} \equiv \frac{3x_1^2 + a}{2y_1} (mod\ p)$.

Если выполнены условия $x_1 = x_2$и $y_1 = -y_2 (\mathrm{mod} p)$, то сумма точек Q_1 и Q_2называется нулевой точкой Oбез определения ее x-и y- координат. В этом случае точка Q_2 называется отрицанием точки Q_1. Для нулевой точки Oвыполнены равенства

$$Q + O = O + Q = Q, \quad (5)$$

где Q - произвольная точка эллиптической кривой E.

Относительно введенной операции сложения множество всех точек эллиптической кривой E, вместе с нулевой точкой, образуют конечную абелеву (коммутативную) группу порядка m, для которого выполнено неравенство

$$p + 1 - 2\sqrt{p} \leq m \leq p + 1 + 2\sqrt{p} \quad (6)$$

Точка Qназывается «точкой кратности k», или просто «кратной точкой эллиптической кривой E», если для некоторой точки Pвыполнено равенство

$$Q = \underbrace{P + \ldots + P}_{k} = kP \quad (7)$$

5.2 Параметры цифровой подписи

Параметрами схемы цифровой подписи являются:
- простое число p - модуль эллиптической кривой;

- эллиптическая кривая E, задаваемая своим инвариантом $J(E)$ или коэффициентами $a, b \in F_p$;

- целое число m- порядок группы точек эллиптической кривой E;

-простое число q - порядок циклической подгруппы группы точек эллиптической кривой E, для которого выполнены следующие условия:

$$\begin{cases} m = nq, \ n \in Z, \ n \geq 1 \\ 2^{254} < q < 2^{256} \text{ или } 2^{508} < q < 2^{512}; \end{cases} \quad (8)$$

-точка $P \neq O$ эллиптической кривой E, с координатами (x_p, y_p), удовлетворяющая равенству $qP=O$.

- хэш-функция $V^* \to V_1$,отображающая сообщения, представленные ввиде двоичных векторов произвольной конечной длины, в двоичные вектора длины lбит. Хэш-функция определена в ГОСТ Р 34.11-2012. Если $2^{254}<q<2^{256}$, то l =256.Если$2^{508}<q<2^{512}$,тоl=512.

Каждый пользователь схемы цифровой подписи должен обладать личными ключами:

-ключом подписи - целым числом d, удовлетворяющим неравенству $0<d<q$;

-ключом проверки подписи - точкой эллиптической кривой Qс координатами(x_q,y_q), удовлетворяющей равенству $dP = Q$.

К приведенным выше параметрам схемы цифровой подписи предъявляют следующие требования:

- должно быть выполнено условие $p^t \neq 1 \pmod q$, для всех целых t=1,2,...,B,гдеB=31,если $2^{254}<q<2^{256}$, и B= 131, если $2^{508}<q<2^{512}$;

- должно быть выполнено неравенство $m \neq p$;

- инвариант кривой должен удовлетворять условию $J(E) \neq 0$,и $J(E) \neq 1728$.

5.3 Двоичные векторы

Для определения процессов формирования и проверки цифровой подписи необходимо установить соответствие между целыми числами и двоичными векторами длины l бит.

Рассмотрим следующий двоичный вектор длиной l бит, в котором младшие биты расположены справа, а старшие - слева:

$$\bar{h} = (\alpha_{l-1}, \dots, \alpha_0), \bar{h} \in V_l \quad (9)$$

где α_i,i=0,..,l-1 равно либо 1, либо 0.

Число $\alpha \in Z$ соответствует двоичному вектору $\bar{h}$, если выполнено равенство

$$\alpha = \sum_{i=0}^{l-1} \alpha_i 2^i \qquad (10)$$

Для двух двоичных векторов

$$\overline{h_1} = (\alpha_{l-1,} \dots, \alpha_0),$$

$$\overline{h_2} = (\beta_{l-1,} \dots, \beta_0), \qquad (11)$$

соответствующих целым числам αи β, операция конкатенации (объединения) определяется следующим образом:

$$\overline{h_1} \| \overline{h_2} = (\alpha_{l-1}, \dots, \alpha_0, \beta_{l-1}, \dots, \beta_0) \qquad (12)$$

Объединение представляет собой двоичный вектор длиной 2*l*бит, составленный из коэффициентов векторов $\overline{h_1}$.и $\overline{h_2}$. Формулы (11) и (12) определяют способ разбиения двоичного вектора $\overline{h_1}.\|\overline{h_2}$. длиной 2*l*бит на два двоичных вектора длиной *l* бит, конкатенацией которых он является.

6 Основные процессы

В данном разделе определены процессы формирования и проверки цифровой подписи под сообщением пользователя. Для реализации данных процессов необходимо, чтобы всем пользователям были известны параметры схемы цифровой подписи, соответствующие требованиям 5.2. Кроме того, каждый пользователь должен иметь ключ подписи *d* и ключ проверки подписи *Q* (x_q, y_q), которые также должны соответствовать требованиям 5.2.

6.1 Формирование цифровой подписи

Для получения цифровой подписи под сообщением *M* $\in V^*$ необходимо выполнить следующие действия (шаги) по алгоритму I:

Шаг 1 - вычислить хэш-код сообщения

$$M: \bar{h} = h(M) \qquad (13)$$

Шаг 2 - вычислить целое число α, двоичным представлением которого является вектор $\bar{h}$, и определить

$$e \equiv \alpha (mod\ q) \qquad (14)$$

Если $e = 0$, то определить $e = 1$.

Шаг 3 - сгенерировать случайное (псевдослучайное) целое число k, удовлетворяющее неравенству

$$0<k<q \tag{15}$$

Шаг 4 - вычислить точку эллиптической кривой $C = kP$ и определить

$$r \equiv x_c(modq), \tag{16}$$

где x_c-x-координата точки C.

Если r = 0, то вернуться к шагу 3.

Шаг 5 - вычислить значение

$$s \equiv (rd + ke)(modq). \tag{17}$$

Если $s = 0$, то вернуться к шагу 3.

Шаг 6 - вычислить двоичные векторы $\bar{r}$ и $\bar{s}$ их, соответствующие r и s, и определить цифровую подпись $\zeta=\bar{r}||\bar{s}$ как конкатенацию двух двоичных векторов.

Исходными данными этого процесса являются ключ подписи dи подписываемое сообщение M, а выходным результатом - цифровая подпись ζ. Схема процесса формирования цифровой подписи приведена на рисунке 2.

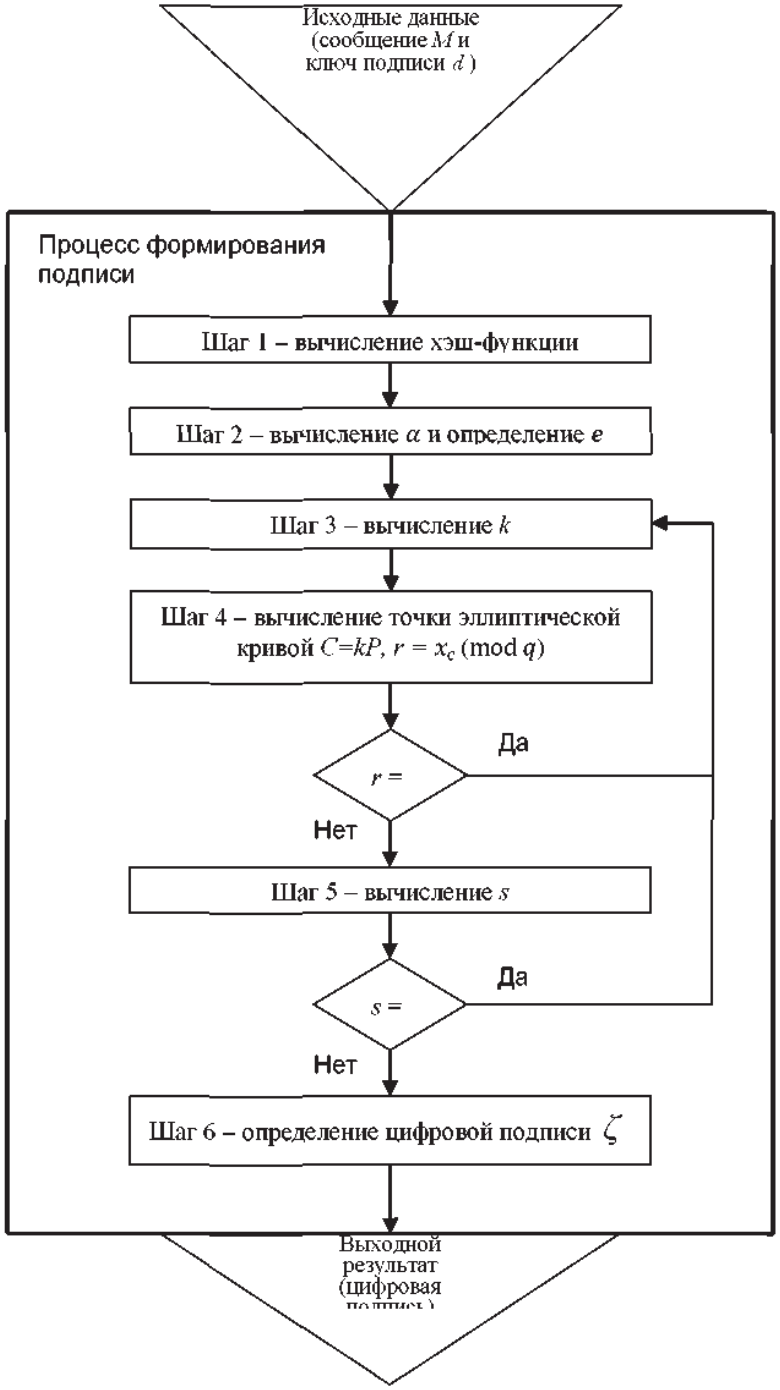


Рисунок 2 - Схема процесса формирования цифровой подписи

6.2 Проверка цифровой подписи

Для проверки цифровой подписи ζ под полученным сообщением M необходимо выполнить следующие действия (шаги) по алгоритму II:

Шаг 1 - по полученной подписи ζ вычислить целые числа r и s. Если выполнены неравенства $0<r<q$, $0<s<q$, то перейти к следующему шагу. В противном случае подпись неверна.

Шаг 2 - вычислить хэш-код полученного сообщения M:

$$\bar{h} = h(M) \quad (18)$$

Шаг 3 - вычислить целое число α, двоичным представлением которого является вектор $\bar{h}$ и определить

$$e \equiv \alpha(mod\ q) \quad (19)$$

Если $e = 0$, то определить $e = 1$.

Шаг 4 - вычислить значение$v \equiv e^{-1}(mod\ q)$ (20)

Шаг 5 - вычислить значения

$$z_1 \equiv sv(modq), z_2 \equiv -rv(modq) \quad (21)$$

Шаг 6 - вычислить точку эллиптической кривой $C=z_1P+z_2Q$и определить

$$R \equiv x_c(mod\ q) \quad (22)$$

где x_c - x-координата точки C.

Шаг 7 - если выполнено равенство $R = r$, то подпись принимается, в противном случае - подпись неверна.

Исходными данными этого процесса являются подписанное сообщение M, цифровая подпись ζ, и ключ проверки подписи Q, а выходным результатом -свидетельство о достоверности или ошибочности данной подписи.

Схема процесса проверки цифровой подписи приведена на рисунке 3.

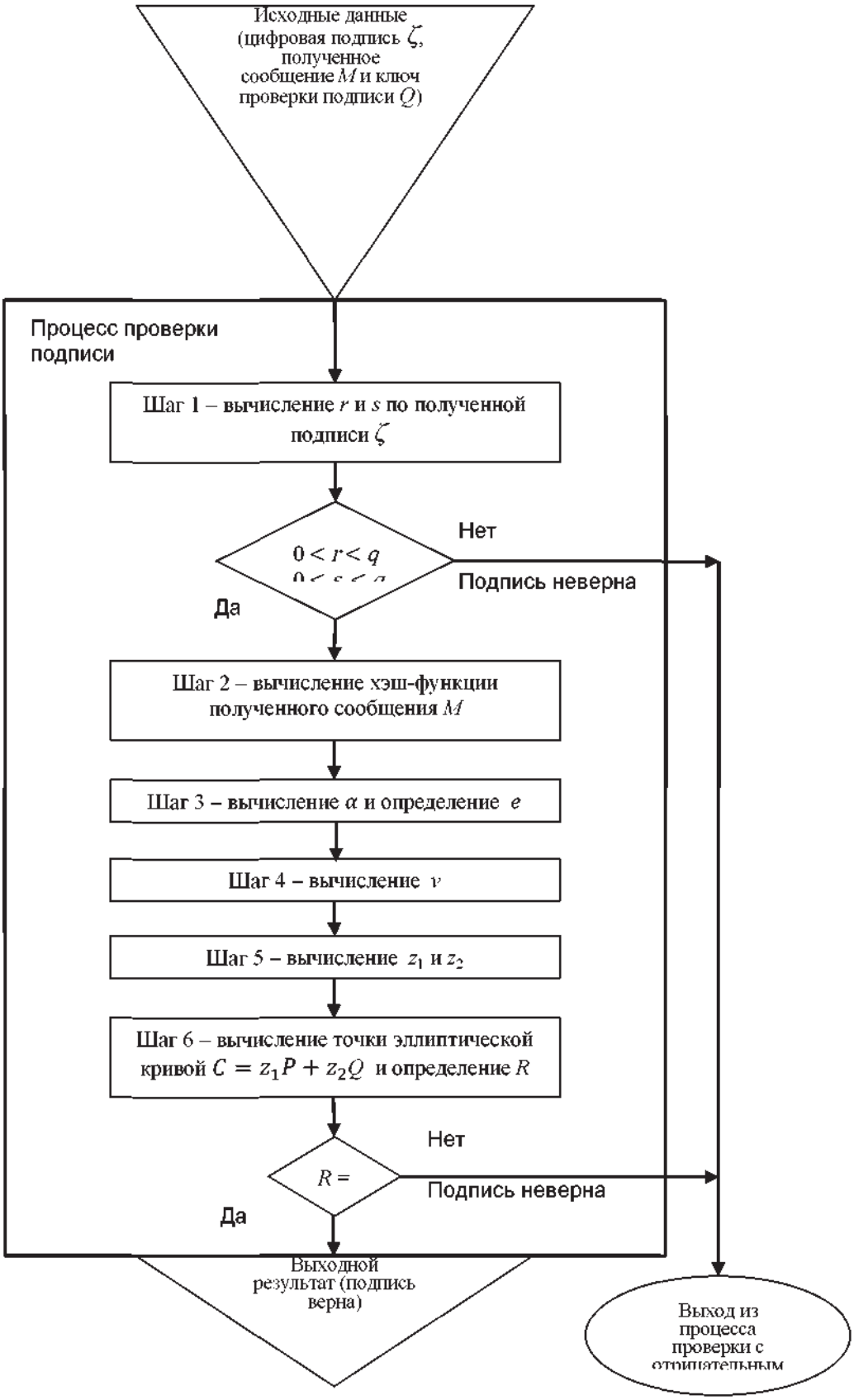


Рисунок 3 - Схема процесса проверки цифровой подписи

Приложение А
(информационное)

Контрольные примеры

Приводимые ниже значения параметров *p*, *a*, *b, m, q*, *P*, а также значения ключей подписи и проверки подписи *d* и *Q* рекомендуется использовать только для проверки корректной работы конкретной реализации алгоритмов, описанных в настоящем стандарте.

Все числовые значения приведены в десятичной и шестнадцатеричной записи. Нижний индекс в записи числа обозначает основание системы счисления. Символ «\\» обозначает перенос числа на новую строку. Например, запись

12345\\
67890_{10}
$499602D2_{16}$

представляет целое число 1234567890 в десятичной и шестнадцатеричной системах счисления соответственно.

А.1 Пример 1

А.1.1 Параметры схемы цифровой подписи

Для формирования и проверки цифровой подписи должны быть использованы следующие параметры (см. 5.2).

А.1.1.1 Модуль эллиптической кривой

В данном примере параметр*p* присвоено следующее значение:

p= 57896044618658097711785492504343953926\\
$6349923328202820197287920039565648210 41_{10}$
$p=8000000000000000000000000000000000000000000000000000000000000431_{16}$.

А.1.1.2 Коэффициенты эллиптической кривой

В данном примере параметры *a* и *b*принимают следующие значения:

$a = 7_{10}$,
$a = 7_{16}$,
b = 43308876546767276905765904595650931995\\
$942111794451039583252968842033849580414_{10}$,
$b=5FBFF498AA938CE739B8E022FBAFEF40563F6E6A3472FC2A514C0CE9DAE23B7E_{16}$.

А.1.1.3 Порядок группы точек эллиптической кривой

В данном примере параметр *m* принимает следующее значение:

m = 57896044618658097711785492504343953927\\
$708293458372545062238097359213763106961 9_{10}$,
$m = 8000000000000000000000000000000150FE8A1892976154C59CFC193ACCF5B3_{16}$

А.1.1.4 Порядок циклической подгруппы группы точек эллиптической кривой

В данном примере параметр *q*принимает следующее значение:

q = 57896044618658097711785492504343953\\
7082934583725450622380973592137631069619$_{10}$,
q = 8000000000000000000000000000000150FE8A1892976154C59CFC193ACCF5B3$_{16}$

А.1.1.5 Коэффициенты точки эллиптической кривой

В данном примере координаты точки *P* принимают следующие значения:

xp= 2$_{10}$,
xp= 2$_{16}$,
yp= 4018974056539037503335449422937059\\
7563573938990554508069097936521343156628$0_{10}$,
yp= 8E2A8A0E65147D4BD6316030E16D19\\
C85C97F0A9CA267122B96ABBCEA7E8FC8$_{16}$.

А.1.1.6 Ключ подписи

В данном примере считается, что пользователь обладает следующим ключом подписи *d*

d = 5544119606536324612635562413032418\\
3196576709222340016572108097750006097525544$_{10}$,
d = 7A929ADE789BB9BE10ED359DD39A72C\\
11B60961F49397EEE1D19CE9891EC3B28$_{16}$

А.1.1.7 Ключ проверки подписи

В данном примере считается, что пользователь обладает ключом проверки подписи *Q*, координаты которого имеют следующие значения:

xq= 5752021612617680844363140502333807\\
1766301049063136321828967413422066048594$03_{10}$,
xq= 7F2B49E270DB6D90D8595BEC458B5\\
0C58585BA1D4E9B788F6689DBD8E56FD80B$_{16}$,
yq= 1761494441921378154380939194965408\\
0319426620453636392607098478594382867639$94_{10}$,
yq= 26F1B489D6701DD185C8413A977B3\\
CBBAF64D1C593D26627DFFB101A87FF77DA$_{16}$.

А.1.2 Процесс формирования цифровой подписи (алгоритм I)

Пусть после выполнения шагов 1 — 3 по алгоритму I (см. 6.1) были получены следующие числовые значения:

a = 2079889367447645201713406156150827013\\
0637142515379653289952617252661468872421$_{10}$,
a = 2DFBC1B372D89A1188C09C52E0EE\\
C61FCE52032AB1022E8E67ECE6672B043EE5$_{16}$,
k = 5385413767734846373140384114799661\\
9215040034343020207129608385288931962333$95_{10}$,
k = 77105C9B20BCD3122823C8CF6FCC\\

$7B956DE33814E95B7FE64FED924594DCEAB3_{16}$.

При этом кратная точка $C = kP$ имеет координаты:

xc= 29700980915817952874371204983938256 9\\
$90422752107994319651632687982059210933395_{10}$,

xc= 41AA28D2F1AB148280CD9ED56FED\\
$A41974053554A42767B83AD043FD39DC0493_{16}$,

yc= 32842535278684663477094665322517084 5\\
$06804721032454543268132854556539274060910_{10}$,

yc= 489C375A9941A3049E33B34361DD\\
$204172AD98C3E5916DE27695D22A61FAE46E_{16}$.

Параметр $r = x_c$ *(modq)* принимает значение:

r= 29700980915817952874371204983938256 9\\
$90422752107994319651632687982059210933395_{10}$,

r= 41AA28D2F1AB148280CD9ED56FED\\
$A41974053554A42767B83AD043FD39DC0493_{16}$.

Параметр s = (rd + ке) (modq) принимает значение:

s = 57497340027008465417892531001914703\\
$84552270426490985639337189991755158395 52_{10}$,

s=1456C64BA4642A1653C235A98A60249BCD6D.

А.1.3 Процесс проверки цифровой подписи (алгоритм II)

Пусть после выполнения шагов 1 — 3 по алгоритму II (см. 6.2) были получены следующие числовые значения:

e= 20798893674476452017134061561508270 13\\
$06371425153796532899526172526614688724 21_{10}$.

e= 2DFBC1B372D89A1188C09C52E0EE\\
$C61FCE52032AB1022E8E67ECE6672B043EE5_{16}$.

При этом параметр v =e-1(modq) принимает значение:

v = 17686683605934468677301713824900268 5\\
$62746883080675496715288036572431145718978_{10}$,

v = 271A4EE429F84EBC423E388964555BB\\
$29D3BA53C7BF945E5FAC8F381706354C2_{16}$.

Параметры z1≡sv(modq) и z2≡ — rv(modq) принимают значения:

z1 = 37699167500901938556841057293512656 1\\
$08841345190491942619304532412743720999759_{10}$,

z1 = 5358F8FFB38F7C09ABC782A2DF2A\\
$3927DA4077D07205F763682F3A76C9019B4F_{16}$,

z2 = 14171998427343472112515917969500765 7\\
$69246655838972862114499932653333671092 21_{10}$,

z2 = 3221B4FBBF6D101074EC14AFAC2D4F7\\
$EFAC4CF9FEC1ED11BAE336D27D527665_{16}$.

Точка C = z1P + z2Q имеет координаты:

xc= 29700980915817952874371204983938256 99\\
$04227521079943196516326879820592109333 95_{10}$,

xc= 41AA28D2F1AB148280CD9ED56FED\\
$A41974053554A42767B83AD043FD39DC0493_{16}$,

yc = 32842535278684663477094665322517084 50\\
$68047210324545432681328545565392740609 10_{10}$,

yc = 489C375A9941A3049E33B34361DD\\

204172AD98C3E5916DE27695D22A61FAE46E$_{16}$.

Тогда параметр R = xc(modq) принимает значение:

R= 297009809158179528743712049839382569 9\\
042275210799431965163268798205921093339 5$_{10}$,

R= 41AA28D2F1AB148280CD9ED56FED\\
A41974053554A42767B83AD043FD39DC0493$_{16}$.

Поскольку выполнено равенство *R=r,* то цифровая подпись принимается.

А.2 Пример 2

А.2.1 Параметры схемы цифровой подписи

Для формирования и проверки цифровой подписи должны быть использованы следующие параметры (см. 5.2).

А.2.1.1 Модуль эллиптической кривой

В данном примере параметру *p* присвоено следующее значение:

p= 362398610222900363590778875368387430602132092553467860 50\\
865461504508561666240024825884820222714968540250908236030 5\\
873516373426382237196498722858290737240 3$_{10}$,

p= 4531ACD1FE0023C7550D267B6B2FEE80922B14B2FFB90F04D4EB7C09B5D2D15D\\
F1D852741AF4704A0458047E80E4546D35B8336FAC224DD81664BBF528BE6373$_{16}$.

А.2.1.2 Коэффициенты эллиптической кривой

В данном примере параметры *a* и *b* принимают следующие значения:

a = 7$_{10}$,

a = 7$_{16}$,

b = 151865506921082853450895003471404315492874752774020643 6\\
194018823352809982443793732829756914785974674866041605397883 6775\\
966263264139901369590474358118263 96$_{10}$,

b = 1CFF0806A31116DA29D8CFA54E57EB748BC5F377E49400FDD788B649ECA1AC4\\
361834013B2AD7322480A89CA58E0CF74BC9E540C2ADD6897FAD0A3084F302ADC$_{16}$.

А.2.1.3 Порядок группы точек эллиптической кривой

В данном примере параметр *m* принимает следующее значение:

m= 362398610222900363590778875368387430602132092553467860508654 61\\
504508561666239691648983050328630684999614040794379365854558651 92212\\
970734808812618120619743$_{10}$,

m= 4531ACD1FE0023C7550D267B6B2FEE80922B14B2FFB90F04D4EB7C09B5D2D15D\\
A82F2D7ECB1DBAC719905C5EECC423F1D86E25EDBE23C595D644AAF187E6E6DF$_{16}$.

А.2.1.4 Порядок циклической подгруппы группы точек эллиптической кривой

В данном примере параметр *q*принимает следующее значение:

q= 362398610222900363590778875368387430602132092553467860508654 61\\
504508561666239691648983050328630684999614040794379365854558651 92212\\
970734808812618120619743$_{10}$,

q=4531ACD1FE0023C7550D267B6B2FEE80922B14B2FFB90F04D4EB7C09B5D2D15D\\
A82F2D7ECB1DBAC719905C5EECC423F1D86E25EDBE23C595D644AAF187E6E6DF$_{16}$.

А.2.1.5 Коэффициенты точки эллиптической кривой

В данном примере координаты точки *P* принимают следующие значения:

x_p=19283569440670228493993094012431375989977866354595079743570754913077665\\
92685835441065557681003184874819658004903212332884252335830250729527632 38\\
3493573274$_{10}$,

x_p=24D19CC64572EE30F396BF6EBBFD7A6C5213B3B3D7057CC825F91093A68CD762\\
FD60611262CD838DC6B60AA7EEE804E28BC849977FAC33B4B530F1B120248A9A$_{16}$,

y_p= 22887286933719728599700121555294784163535623273295061803\\
14497425931102860301572814141997072271708807066593850650334152381 8\\
5734779888586480760509872401385 4$_{10}$,

yp= 2BB312A43BD2CE6E0D020613C857ACDDCFBF061E91E5F2C3F32447C259F39B2\\
C83AB156D77F1496BF7EB3351E1EE4E43DC1A18B91B24640B6DBB92CB1ADD371E$_{16}$.

А.2.1.6 Ключ подписи

В данном примере считается, что пользователь обладает следующим ключом подписи *d:*

d=6100818041363730982195381532398475830068455190695315629823881 35\\
3548906063017822553836083934233723790576655275951168273070250464 5883\\
7440766121180466875860$_{10}$,

d=BA6048AADAE241BA40936D47756D7C93091A0E8514669700EE7508E508B102072\\
E8123B2200A0563322DAD2827E2714A2636B7BFD18AADFC62967821FA18DD4$_{16}$.

А.2.1.7 Ключ проверки подписи

В данном примере считается, что пользователь обладает ключом проверки подписи *Q*, координаты которого имеют следующие значения:

xq=90954685300253659655669076866983031000692927254655628159 63\\
7296537031249856318232043689287005284280860826283245685822 3580\\
7137802907179868558634334311505 61$_{10}$,

xq=115DC5BC96760C7B48598D8AB9E740D4C4A85A65BE33C1815B5C320C854621D\\
D5A515856D13314AF69BC5B924C8B4DDFF75C45415C1D9DD9DD33612CD530EFE1$_{16}$.

yq= 29214572033744256206324497342484154556407008235594887051648958\\
37509539134297327397380287741428246088626609329139441895016863758\\
9841063266005724768223720 76$_{10}$,

yq= 37C7C90CD40B0F5621DC3AC1B751CFA0E2634FA0503B3D52639F5D7FB72AFD6\\
1EA199441D943FFE7F0C70A2759A3CDB84C114E1F9339FDF27F35ECA93677BEEC$_{16}$.

А.2.2 Процесс формирования цифровой подписи (алгоритм I)

Пусть после выполнения шагов 1 — 3 по алгоритму I (см. 6.1) были получены следующие числовые значения:

e=28979638816828685755628272785538650491737451978718251995629 47\\
4190413889509705366611095534999542487330887197488445389646412 816544\\
6351329697382770627204596 4$_{10}$,

e=3754F3CFACC9E0615C4F4A7C4D8DAB531B09B6F9C170C533A71D147035B0C591\\
7184EE536593F4414339976C647C5D5A407ADEDB1D560C4FC6777D2972075B8C$_{16}$,

k=17551635602585049954062827992112528033345103174773779165 02\\

0814424318205707503444610298675096250890922723586612687247351680781054l7\\
$475297103098799586329451_{10}$,
k=359E7F4B1410FEACC570456C6801496946312120B39D019D455986E364F3\\
65886748ED7A44B3E7944340060118422862122 73A6D14CF70EA3AF71BB1AE679F1$_{16}$.

При этом кратная точка C = kP имеет координаты

xc=2489204477031349265072864643032147753667451319282131444027498637 3\\
5761109281022179510187141292882371680595982870833028424365345308 53\\
$22004442442534151761462_{10}$,
xc=2F86FA60A081091A23DD795E1E3C689EE512A3C82EE0DCC2643C78EEA8FCAC\\
D35492558486B20F1C9EC197C90699850260C93BCBCD9C5C3317E19344E173AE36$_{16}$,
yc=770173889928991836047844798780960441682062631876096137673946801 50\\
2442229353276517652844283783245693642266254651370214816293307951 7\\
$0843005015210864150831 0_{10}$,
yc=EB488140F7E2F4E35CF220BDBC75AE44F26F9C7DF52E82436BDE80A91831DA27\\
C8100DAA876F9ADC0D28A82DD3826D4DC7F92E471DA23E55E0EBB3927C85BD6$_{16}$.

Параметр r = xc(modq) принимает значение

r=2489204477031349265072864643032147753667451319282131444027498637 3\\
5761109281022179510187141292882371680595982870833028424365345308 53\\
$22004442442534151761462_{10}$,
r=2F86FA60A081091A23DD795E1E3C689EE512A3C82EE0DCC2643C78EEA8FCAC\\
D35492558486B20F1C9EC197C90699850260C93BCBCD9C5C3317E19344E173AE36$_{16}$.

Параметрs = (rd + ке) (modq) принимает значение

s=8645232217076695190388492973829369170750237358484315799195987\\
9931338518056474887719563967246017942176077089327803095680769011 5\\
$8227099038536828318351593 70_{10}$,
s=1081B394696FFE8E6585E7A9362D26B6325F56778AADBC081C0BFBE933D52FF58\\
23CE288E8C4F362526080DF7F70CE406A6EEB1F56919CB92A9853BDE73E5B4A16.

А.2.3 Процесс проверки цифровой подписи (алгоритм II)

Пусть после выполнения шагов 1 — 3 по алгоритму II (см. 6.2) были получено следующее числовое значение:

e=2897963881682868575562827278553865049173745197871825199562947\\
4190413889509705366611095534999542487330887197488445389646412816544\\
$6351329697382770627204596 4_{10}$,
e=3754F3CFACC9E0615C4F4A7C4D8DAB531B09B6F9C170C533A71D147035B0C591\\
7184EE536593F4414339976C647C5D5A407ADEDB1D560C4FC6777D2972075B8C$_{16}$.

При этом параметрv = e-1(modq) принимает значение

v =2556942153946052222660740843164086153877692234400783191146928 49\\
3561943457323447089240019252056982806881535340041458212439906061 36\\
$70722381859348159602526 71_{10}$,
v =30D212A9E25D1A80A0F238532CADF3E64D7EF4E782B6AD140AAF8BBD9BB4729\\
84595EEC87B2F3448A1999D5F0A6DE0E14A55AD875721EC8CFD504000B3A840FF$_{16}$.

Параметры z1= sv(modq) и z2 =-rv(modq) принимают значения:

z1=3206470827336768629686907101873475250343306448089030311214484\\
3858727432050451803452088265529010034967329410497803577935419420 55\\
$60008495619817370719790257 5_{10}$,
z1=3D38E7262D69BB2AD24DD81EEA2F92E6348D619FA45007B175837CF13B026079\\
051A48A1A379188F37BA46CE12F7207F2A8345459FF960E1EBD5B4F2A34A6EEF$_{16}$,
z2=1366770911834003108142977848021847597320455347535641273482 7\\

32082047028342168006031261814273230879203690726448631222679743757 5\\
$6163726695805680585960300820 3_{10}$,
z2=1A18A31602E6EAC0A9888C01941082AEFE296F840453D2603414C2A16EB6FC529\\
D8D8372E50DC49D6C612CE1FF65BD58E1D2029F22690438CC36A76DDA444ACB$_{16}$.

Точка C = z1P + z2Q имеет координаты:

xc= 24892044770313492650728646430321477536674513192821314440274976 37\\
35761109281022179510187141292882371680595982870833028424365345308 53\\
$22004442442534151761462_{10}$,
xc=2F86FA60A081091A23DD795E1E3C689EE512A3C82EE0DCC2643C78EEA8FCAC\\
D35492558486B20F1C9EC197C90699850260C93BCBCD9C5C3317E19344E173AE36$_{16}$,
yc=77017388992899183604784479878096044168206263187609613767394680 15\\
02442229353276517652844283783245693642266254651370214816293307951 70\\
$8430050152108641508310_{10}$,
yc=EB488140F7E2F4E35CF220BDBC75AE44F26F9C7DF52E82436BDE80A91831DA27\\
C8100DAA876F9ADC0D28A82DD3826D4DC7F92E471DA23E55E0EBB3927C85BD6$_{16}$

Тогда параметр R= xc(modq) принимает значение

R=24892044770313492650728646430321477536674513192821314440274986\\
37357611092810221795101871412928823716805959828708330284243653453085\\
$32200444244253415176146 2_{10}$,
R=2F86FA60A081091A23DD795E1E3C689EE512A3C82EE0DCC2643C78EEA8FCAC\\
D35492558486B20F1C9EC197C90699850260C93BCBCD9C5C3317E19344E173AE36$_{16}$.

Поскольку выполнено равенство R=r, то цифровая подпись принимается.

Библиография

[1] ISO 2382-2:1976 (ISO 2382-2:1976) Системы обработки информации. Словарь. Часть 2. Арифметические и логические операции (Data processing - Vocabulary - Part 2: Arithmetic and logic operations)

[2] ISO/IEC 9796-2:2010 (ISO/IEC 9796-2:2010) Информационные технологии. Методы обеспечения безопасности. Схемы цифровой подписи, обеспечивающие восстановление сообщений. Часть 2. Механизмы на основе целочисленной факторизации (Information technology - Security techniques - Digital signatures with appendix - Part 2: Integer factorization based mechanisms)

[3] ISO/IEC 9796-3:2006 (ISO/IEC 9796-3:2006) Информационные технологии. Методы обеспечения безопасности. Схемы цифровой подписи, обеспечивающие восстановление сообщений. Часть 3. Механизмы на основе дискретного логарифма (Information technology. Security techniques. Digital signatures chemes giving message recovery. Part 3: Discrete logarithm based mechanisms)

[4] ISO/IEC 14888-1:2008 (ISO/IEC 14888-1:2008) Информационные технологии. Методы защиты. Цифровые подписи с приложением. Часть 1. Общие положения (Information technology. Security techniques.Digital signatures with appendix. Part 1: General)

[5] ISO/IEC 14888-2:2008 (ISO/IEC 14888-2:2008) Информационные технологии. Методы защиты. Цифровые подписи с приложением. Часть 2. Механизмы, основанные на разложении на множители (Information technology. Security techniques. Digital signatures with appendix. Part 2: Integer factorization based mechanisms)

[6] ISO/IEC 14888-3:2006(ISO/IEC 14888-3:2006) Информационные технологии. Методы защиты. Цифровые подписи с приложением. Часть 3. Механизмы на основе дискретного логарифма (Information technology. Security techniques. Digital signatures with appendix. Part 3: Discrete logarithm based mechanisms)

[7] ISO/IEC 14888-3:2006/Изм1:2010(ISO/IEC 14888-3:2006/Amd1:2010Информационныетехнологии. Методы защиты. Цифровые подписи с приложением. Часть 3. Механизмы на основе дискретного логарифма. Изменение 1. Алгоритм русской цифровой подписи эллиптической кривой, алгоритм цифровой подписи Шнора, алгоритм цифровой подписи Шнораэллиптической кривой, и полный алгоритм цифровой подписи Шнора для эллиптической кривой (Information technology. Security techniques. Digital signatures with appendix. Part 3: Discrete logarithm based mechanisms. Ammendment 1. Elliptic Curve Russian Digital Signature Algorithm, Schnorr Digital Signature Algorithm, Elliptic Curve Schnorr Digital Signature Algorithm, and Elliptic Curve Full SchnorrDigital Signature Algorithm)

[8] ISO/IEC 10118-1:2000 (ISO/IEC 10118-1:2000) Информационные технологии. Методы защиты информации. Хэш – функции. Часть 1. Общие положения (Information technology.Security techniques.Hash-functions. Part 1: General)

[9] ISO/IEC 10118-2:2010 (ISO/IEC 10118-2:2010) Информационные технологии. Методы защиты информации. Хэш – функции. Часть 2. Хэш функции с использованием алгоритма *n* – битными блоками (Information technology. Security techniques. Hash-functions. Part 2:Hash-functions using ann-bit block cipher)

[10] ISO/IEC 10118-3:2004 (ISO/IEC 10118-3:2004) Информационные технологии. Методы защиты информации. Хэш – функции. Часть 3. Выделение хэш-функции (Information technology. Security techniques. Hash-functions. Part 3:Dedicatedhash-functions)

[11] ISO/IEC 10118-4:1998(ISO/IEC 10118-4:1998) Информационные технологии. Методы защиты информации. Хэш – функции. Часть 4. Хэш–функции с применением арифметики в остаточных классах (Information technology. Security techniques. Hash-functions. Part 4: Hash-functions using modular arithmetic)

УДК 681.3.06:006.354 **МКС 35.040**

Ключевые слова: обработка данных, передача данных, обмен информацией, сообщения, цифровые подписи, защита информации, формирование цифровой подписи, проверка цифровой подписи.

Басуға _____ ж. қол қойылды Пішімі 60х84 1/16
Қағазы офсеттік. Қаріп түрі «KZ Times New Roman»,
«Times New Roman»
Шартты баспа табағы 1,86. Таралымы ____ дана. Тапсырыс ____

«Қазақстан стандарттау және сертификаттау институты»
республикалық мемлекеттік кәсіпорны
010000, Астана қаласы, Орынбор көшесі, 11 үй,
«Эталон орталығы» ғимараты
Тел.: 8 (7172) 79 33 24