Параметрли эллиптик эгри чизиқларга асосланган электрон рақамли имзо алгоритми

т.ф.н. Х.П. Хасанов, т.ф.н. О.П. Ахмедова,
ф.-м.ф.н. М.Х. Назарова (“UNICON.UZ” ДУК)

Мазкур мақолада эллиптик эгри чизиқларга асосланган электрон рақамли имзо алгоритмининг математик асослари ва жараёнлари баён этилган.

В данной статье изложены математические основы и процессы алгоритма электронной цифровой подписи на базе эллиптических кривых с параметром.

This article describes the mathematical foundations and processes of digital signature algorithm based on elliptic curves with parameter.

Эллиптик эгри чизиқ (ЭЭЧ) назариясини яратишда сўнгги қадимий грек математиги Диофантдан бошлаб ўтмишнинг кўпгина энг йирик олимлари қатнашган. ЭЭЧ алгебраик структурасини машҳур француз математиги Анри Пуанкаре таклиф этган бўлиб, йиллар давомида ЭЭЧ соф математика соҳаси бўлиб келган. Ўтган асрнинг 80 йилларида ЭЭЧ катта сонларни факторлаш алгоритмларини тузиш соҳасида қўлланила бошлади ва бу қўлланишлар криптографиянинг носимметрик тизимлар ва псевдотасодифий сонларни генерациялаш йўналишларида яққол намоён бўлди. Эллиптик криптографияда ҳақиқий бурилиш 1985 йилда Н.Коблиц ва В.Миллер илмий ишлари чоп этилгандан сўнг юз берди. Шу дамдан бошлаб машҳур жаҳон криптологлари эллиптик криптография билан шуғуллана бошладилар [1].

XXI асрнинг бошидан бошлаб, носимметрик криптографиянинг анъанага айланиб қолган криптотизимлардан бардошлилиги ЭЭЧ алгебраик структурасида дискрет логарифмлаш муаммосининг мураккаблигига асосланган тизимларга ўтиш бошланган. Чунки ЭЭЧ алгебраик структурасида нисбатан қисқа калит узунлиги асосида криптотизимлар ишлаб чиқариш имконияти мавжуд. Бундай имконият АҚШ ва Россия Федерациясида амалдаги стандартларни эллиптик криптографияга оид стандартлар билан алмаштиришга олиб келди. Ҳозирги кунда ЭЭЧларга асосланган алгоритмлар кўплаб халқаро, миллий ва соҳага оид стандартлар қаторидан ўрин олган [2]. Ўзбекистон Республикасида ҳам бу йўналишдаги илмий-тадқиқот ишлари амалга оширилиши натижасида ўзбек олимлари томонидан таклиф этилган параметрли алгебра эллиптик криптографияга тадбиқ этилди ва Ўзбекистон Республикасининг давлат стандарти ишлаб чиқилди.

O‘z DSt 2826:2014 “Ахборот технологияси. Ахборотнинг криптографик муҳофазаси. Эллиптик эгри чизиқларга асосланган электрон рақамли имзони шакллантириш ва текшириш жараёнлари” давлат стандарти “Ўзстандарт” агентлигининг 2014 йил 30 майдаги 05-546-сон қарори билан тасдиқланди ва жорий этилди [3]. Ушбу стандарт умумий фойдаланишдаги муҳофазаланмаган телекоммуникация каналлари орқали узатиладиган, электрон ҳужжат остига қўйилган ЭЭЧларга асосланган электрон рақамли имзо (ЭРИ) ни шакллантириш ва унинг ҳақиқийлигини тасдиқлаш жараёнларини белгилайди.

Стандарт ЭРИни шакллантириш ва унинг ҳақиқийлигини тасдиқлашда турли мақсадлар учун мўлжалланган ахборотни қайта ишлаш тизимларида қўллаш учун мўлжалланган.

ЭРИнинг умумий тан олинган схемаси учта жараённи ўз ичига олади:

- ЭРИ калитларини генерациялаш;
- ЭРИни шакллантириш;
- ЭРИни ҳақиқийлигини тасдиқлаш.

Узатилган хабарни қабул қилиш давомида қабул қилувчи ЭРИ алгоритмига оид воситалар билан узатма бутунлиги ва жўнатувчининг ҳақиқийлигини тасдиқлашни амалга ошириши мумкин.

ЭРИ ёзма имзонинг электрон аналоги ҳисобланади ва шунинг учун ЭРИни қабул қилувчи ёки учинчи томон хабарга ҳақиқатан жўнатувчи имзо қўйганини тасдиқлаш учун ундан фойдаланиши мумкин. Маълумотлар ва дастурларни сақлаш учун исталган вақтда уларнинг бутунлигини текшириш мумкин бўлиши учун ҳам ЭРИ шакллантирилиши мумкин.

ЭРИ алгоритмларини аниқлаш учун ЭРИни шакллантириш ва ҳақиқийлигини тасдиқлаш жараёнида қўлланиладиган асосий математик объектларни тавсифлаш зарур. Қуйида ЭРИ алгоритмларининг объектларига қўйиладиган асосий математик таърифлар ва талаблар белгиланган.

p>3 туб сони берилган бўлсин. У ҳолда, F_p чекли туб майдонда аниқланган *E* эллиптик эгри чизиқ деб,

$$y_0^2 \equiv x_0^3 + ax_0 + b \ (\mathrm{mod}\ p), \qquad (1)$$

айниятни қаноатлантирувчи (x_0, y_0), $x_0, y_0 \in F_p$, сонлар жуфтликлари тўпламига айтилади, бу ерда $a, b \in F_p$ ва $4a^3 + 27b^2$ ифода *p* модуль бўйича нолдан фарқли [4].

R параметрни киритиш, ўзгарувчилар ва коэффициентларнинг алмаштирилиши асосида (1) қуйидаги модулли шаклга келтирилади:

$$y'^2 \equiv x'^3 + ax + B \ (mod\ p), \qquad (2)$$

бунда: $B \equiv (a+b)\ R^{-1} (mod\ p);$
$y'^2 \equiv (y_0^2 - 1)\ R^{-1} (mod\ p);$
$y \equiv (y_0 - 1)\ R^{-1} (mod\ p);$
$y \equiv (x'^3 + ax + B)'^{0.5} (mod\ p);$
$y^- \equiv -(y + 2R^{-1})\ (mod\ p);$
$x'^3 \equiv (x_0^3 - 1)\ R^{-1} (mod\ p);$
$x \equiv (x_0 - 1)\ R^{-1}\ (mod\ p);$
y_0, x_0, y, y^-, x – ўзгарувчилар;
a, B – бутун сон қийматли коэффициентлар;
R – параметр, $0<R<p$, $(R; p)=1$ шартни қаноатлантиради.

Ошкора шаклдаги ЭЭЧнинг тенгламаси (1) га қўшимча махфийлик *R* ни киритиш уни ошкора бўлмаган шаклдаги ЭЭЧ тенгламаси (2)га айлантиради.

Агар $PE(F_p)$={параметрли ЭЭЧнинг барча нуқталари тўплами} U 0_E, *R* параметр, бунда $0 < R \in F_p$ ва $+'$ - $PE(F_p)$ устида параметрли қўшиш амали бўлса, у ҳолда $(PE(F_p); +')$ жуфтлик параметрли ЭЭЧ нуқталарининг чекли коммутатив группаси дейилади.

Параметрли ЭЭЧнинг инварианти деб қуйидаги айниятни қаноатлантирувчи *J(PE)* катталикка айтилади:

$$J(PE) = 1728 \frac{4a^3}{4a^3 + 27(BR - a)^2} (\mathrm{mod}\ p), \qquad (3)$$

бунда: $a, B \in PE(F_p)$ ва $4a^3 + 27(BR - a)^2 \neq 0 \bmod p$ шартни қаноатлантиради.

PE параметрли ЭЭЧнинг *a*, *B* коэффициентлари *J*(P*E*) инвариант бўйича қуйидагича аниқланади:

$$\begin{cases} a \equiv 3 \cdot k (\mathrm{mod}\ p), \\ B \equiv 5 \cdot k \cdot R^{-1} (\mathrm{mod}\ p), \end{cases} \quad (4)$$

бу ерда, $k \equiv \dfrac{J(PE)}{1728 - J(PE)} (\mathrm{mod}\ p)$ *J(PE) ≠ 0* ёки 1728.

(2) айниятни қаноатлантирувчи (*x, y*) жуфтликлар *PE* параметрли ЭЭЧнинг нуқталари деб аталади, *x* ва *y* – мос равишда нуқтанинг *x* ва *y* координаталари ҳисобланади.

ЭЭЧнинг нуқталарини *T(x, y)* ёки *T* деб белгилаймиз. ЭЭЧнинг иккита нуқтаси тенг бўлади, агар уларнинг мос *x* ва *y* координатлари тенг бўлса.

PE(F_p) ЭЭЧнинг барча нуқталари тўпламида қўшиш амалини киритиб, уни «$+^{\backslash}$» деб белгилаймиз. *PE*(F_p) ЭЭЧнинг ихтиёрий иккита $T_1(x_1, y_1)$ ва $T_2(x_2, y_2)$ нуқталари учун бир нечта вариантларни кўриб чиқамиз.

Фараз қилинсинки, T_1 ва T_2 нуқталар координаталари учун $x_1 \neq x_2$ шарт қаноатлантирилсин. У ҳолда, бу нуқталарнинг йиғиндиси деб, координаталари қуйидаги таққослашлар билан аниқланувчи $T_3(x_3, y_3)$ нуқтага айтилади:

$$\begin{cases} x_3 \equiv (L^2 - 3)R^{-1} - x_1 - x_2 (\mathrm{mod}\ p), \\ y_3 \equiv L(x_1 - x_3) + y_1^{-} (\mathrm{mod}\ p), \end{cases} \quad (5)$$

бу ерда, $L \equiv (y_2 - y_1)(x_2 - x_1)^{-1} (mod p)$.

Агар $x_1 = x_2$ ва $y_1 = y_2 \neq 0$ тенглик бажарилса, у ҳолда T_3 нуқтанинг координаталари қуйидагича аниқланади:

$$\begin{cases} x_3 \equiv (L^2 - 3)R^{-1} - 2x_1 (\mathrm{mod}\ p), \\ y_3 \equiv L(x_1 - x_3) + y_1^{-} (\mathrm{mod}\ p), \end{cases} \quad (6)$$

бу ерда: $L \equiv (3(R x_1^{\backslash 2} + 1) + a)(2(R y_1 + 1))^{-1} (mod p)$.

$x_1 = x_2$ ва $y_1 = -y_2$ (mod *p*) шарти бажарилган ҳолда, T_1 ва T_2 нуқталар йиғиндисини, унинг *x* ва *y* координаталарини аниқламасдан 0_E ноль нуқта деб атаймиз. Ушбу ҳолатда T_2 нуқта T_1 нуқтанинг қарама-қарши нуқтаси деб аталади. 0_E ноль нуқта учун қуйидаги тенглик бажарилади:

$$T +^{\backslash} 0_E = 0_E +^{\backslash} T = T \quad (7)$$

бу ерда, *T* - *PE*(F_p) параметрли ЭЭЧнинг ихтиёрий нуқтаси.

Киритилган қўшиш амалига нисбатан барча *PE*(F_p) параметрли ЭЭЧнинг нуқталари тўплами ноль нуқта билан биргаликда *w* тартибли (коммутатив) чекли абел группасини ташкил қилиб, *w* учун қуйидаги тенгсизлик бажарилади:

$$p + 1 - 2\sqrt{p} \leq w \leq p + 1 + 2\sqrt{p}\ . \quad (8)$$

Агар ЭЭЧга тегишли бирор ***N*** нуқта учун қуйидаги тенглик бажарилса, *T* нуқта *k* га каррали ёки оддийгина қилиб, *PE*(F_p) параметрли ЭЭЧнинг каррали нуқтаси деб аталади:

$$T = \underbrace{N +^{\backslash} \ldots +^{\backslash} N}_{k} = [k] \cdot^{\backslash} N . \qquad (9)$$

ЭРИ алгоритми махсус криптографик модулларга нисбатан ошкора бўлмаган ЭЭЧ параметри муаммосининг мураккаблигига асосланган. Агар ошкора бўлмаган ЭЭЧ нуқталари группаси *(PE(F$_p$);+$^{\backslash}$)*да (ёпиқ параметрлар учлиги *(R, a, B)* билан) нуқталар группаси қисм группасининг тартиби *q*, базавий нуқта *G=(x$_1$,y$_1$)* ва *Y=[d]·$^{\backslash}$G* тенгликни қаноатлантирувчи очиқ калит *Y=(x$_2$,y$_2$)* (ёки *x* нинг координатаси *x$_2$*) берилган бўлса, унда *d* ва параметрлар учлиги *(R, a, B)* топилсин; бунда параметрли ЭЭЧ тенгламаси *y$^{\backslash 2}$≡x$^{\backslash 3}$+ax+B (modp)* кўринишга эга.

ЭРИ алгоритми қуйидаги параметрлардан фойдаланади:

a) *p – p > 2^{255}* тенгсизликни қаноатлантирувчи туб сон. Ушбу соннинг юқори чегаралари ЭРИни муайян амалга ошириш жараёнида белгиланиши керак;

b) *PE(F$_p$)* параметрли ЭЭЧ ўзининг *J(PE)* инварианти ёки *4a^3+27(B·R-a)^2(modp)≠0* шартни қаноатлантирувчи *a,B∈PE(F$_p$)* коэффициентлар билан берилган;

c) *R – PE(F$_p$)* параметрли ЭЭЧ параметри, бунда $2^{160} < R < 2^{255}$ шарт бажарилади;

d) бутун сон *w=# PE(F$_p$) - PE(F$_p$)* параметрли ЭЭЧ нуқталари группасининг тартиби;

e) *q* туб сон - қуйидаги шартлар бажарилган *PE(F$_p$)* параметрли ЭЭЧ нуқталари группаси циклик қисм группасининг тартиби:

$$\begin{cases} w = lq, \quad l \in Z, \quad 1 \le l \le 4 \\ \quad 2^{254} < q < 2^{256} \end{cases}, \qquad (10)$$

бу ерда: *l* – кофактор, *l=# PE(F$_p$)/q;*

f) *G=(x$_3$, y$_3$) – R* параметрли *PE(F$_p$)* ЭЭЧларнинг *q·$^{\backslash}$G=0$_E$* шартни қаноатлантирувчи базавий нуқтаси, бунда *0$_E$* - параметрли ЭЭЧнинг нол нуқтаси,*·$^{\backslash}$– R* параметрли кўпайтириш амали символи;

g) *H* – хэш-функция*;*

h) *S* – бошланғич қиймат, параметрли ЭЭЧлар «тасодифий танлаш» стратегияси бўйича генерация қилинганда, тизим параметрлари таркибига киритилади.

Юқорида келтирилган ЭРИ параметрларига қуйидаги талаблар қўйилади:

- барча бутун $t = 1,2,\ldots,C$ сонлар учун $p^t \neq 1 (\mathrm{mod}\, q)$ шарт бажарилиши керак, бу ерда, *C* сон *C ≥ 31* тенгсизликни қаноатлантиради;

- *w ≠ p* тенгсизлик бажарилиши керак;

- эгри чизиқ инварианти $J(PE) \neq 0$ ёки 1728 шартларини қаноатлантириши керак.

ЭРИ алгоритмининг ҳар бир фойдаланувчиси қуйидаги шахсий калитларга эга бўлиши керак:

a) *d$_i$ – i*-фойдаланувчининг ЭРИ ёпиқ калити, бу ерда *2^{160}≤d$_i$<q-2^{160};*

b) *Y$_i$ =(x, y) - i*-фойдаланувчининг ЭРИ очиқ калити.

Қуйида фойдаланувчи хабари остига қўйиладиган ЭРИни шакллантириш ва унинг ҳақиқийлигини тасдиқлаш жараёнлари келтирилган.

Электрон рақамли имзони шакллантириш жараёни

M хабар остига қўйиладиган ЭРИни яратиш учун алгоритм бўйича қуйидаги қадамларни бажариш зарур:

1-қадам: *M* хабар, учлик параметрлар *R, a* ва *B* конкатенациясининг хэш-функцияси *h=H(M||R||a||B)* ҳисобланади;

2-қадам: *e≡h(mod q)* ҳисобланади. Агар *e=0* бўлса, у ҳолда *e=1* деб қабул қилинади;

3-қадам: ушбу $2^{160}<k_i<q-2^{160}$ тенгсизликни қаноатлантирувчи тасодифий k_i сон генерация қилинади;

4-қадам: тасодифий k_A сонга кўра параметрли эллиптик эгри чизиқнинг $[k_i]\cdot^{\backslash}G=(x_1, y_1)$ нуқтаси ҳисобланади;

5-қадам: $r_i \equiv x_1 \ (mod\ q)$ ҳисобланади, агар $r=0$ бўлса, у ҳолда 3-қадамга қайтилади;

6-қадам: $s_i \equiv (r_i d_i + k_i e)(mod\ q)$ ҳисобланади, агар $s=0$ бўлса, у ҳолда 3-қадамга қайтилади;

7-қадам: дастурий криптографик модуль чиқишида (r_i, s_i) ЭРИ ҳосил қилинади.

Ушбу жараён учун дастлабки маълумотлар бўлиб d_i - ёпиқ калит ва имзоланувчи хабар, чиқиш натижаси бўлиб эса, (r_i, s_i) ЭРИ ҳисобланади.

Электрон рақамли имзонинг ҳақиқийлигини тасдиқлаш жараёни

Олинган M хабар остига қўйилган ЭРИ ҳақиқийлигини тасдиқлаш учун алгоритм бўйича қуйидаги қадамларни бажариш зарур:

1-қадам: $0<r_i,\ s_i<q$ шарт бажарилиши текширилади, агар шарт бажарилса, навбатдаги қадамга ўтилади, акс ҳолда, дастурий криптографик модулнинг чиқишида «ЭРИ ҳақиқий эмас» хабари пайдо бўлади;

2-қадам: M хабар, учлик параметрлар R, a ва B конкатенациясининг хэш-функцияси $h=H(M||R||a||B)$ ҳисобланади;

3-қадам: $e \equiv h(mod\ q)$ ҳисобланади. Агар $e=0$ бўлса, у ҳолда $e=1$ деб қабул қилинади;

4-қадам: $v \equiv e^{-1}(mod\ q)$ ифоданинг қиймати ҳисобланади;

5-қадам: $z_1 \equiv s_i v(mod\ q)$ ва $z_2 \equiv -r_i v(mod\ q)$ ифодалар қийматлари ҳисобланади;

6-қадам: агар очиқ калит x кўринишида киритилган бўлса, у ҳолда x_i бўйича $y_i^{\backslash 2} \equiv x_i^{\backslash 3}+ax_i+B(mod\ p)$ ва $y_i \equiv (x_i^{\backslash 3}+ax_i+B)^{\backslash 0.5}(mod\ p)$ ҳисобланиб, параметрли эллиптик эгри чизиқнинг $Y_i=(x_i, y_i)$ нуқтаси ҳосил қилинади;

7-қадам: параметрли эллиптик эгри чизиқнинг $C=[z_1]\cdot^{\backslash}G+^{\backslash}[z_2]\cdot^{\backslash}Y_i$ нуқтаси ҳисобланади ва $X \equiv x_c \ (mod\ q)$ деб қабул қилинади, бунда x_c – C нуқтанинг x координатаси;

8-қадам: $X=r_i$ тенглик текширилади, агар тенглик бажарилса, у ҳолда чиқишда «ЭРИ ҳақиқий» хабари, акс ҳолда – «ЭРИ ҳақиқий эмас» хабари пайдо бўлади.

Ушбу стандарт махсус аппарат криптографик модулида амалга оширилувчи, ЭРИни шакллантириш ҳамда ЭРИнинг ҳақиқийлигини тасдиқлаш алгоритмини тавсифлайди.

Ишлаб чиқилган ЭРИ алгоритмининг криптографик бардошлилиги махсус криптографик модулларга нисбатан ошкора бўлмаган эллиптик эгри чизиқ параметри муаммосини ҳал қилиш мураккаблигига, шунингдек O‘z DSt 1106 бўйича фойдаланилаётган хэш-функция бардошлилигига асосланади.

Фойдаланилган адабиётлар

1. Коблиц Н. Введение в эллиптические кривые и модулярные формы // Пер с англ. – Москва: Мир, 1988.
2. X9.62 – 1999 Public Key Cryptography For The Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA).
3. O‘z DSt 2826:2014 “Ахборот технологияси. Ахборотнинг криптографик муҳофазаси. Эллиптик эгри чизиқларга асосланган электрон рақамли имзони шакллантириш ва текшириш жараёнлари”.
4. Элементарное введение в эллиптическую криптографию: алгебраические и алгоритмические основы / Болотов А.А., Гашков С.Б., Фролов А.В., Часовских А.А. – Москва МЭИ, 2006.