Такомиллаштирилган “кўр-кўрона” электрон рақамли имзо алгоритми

Ахмедова О.П., Назарова М.Х., Нуриддинов О.Ж. («UNICON.UZ» ДУК)

Ушбу мақолада электрон тўлов тизимларида ахборот хавфсизлигини таъминлаш учун хизмат қилувчи параметрли алгебра асосида такомиллаштирилган “кўр-кўрона” электрон рақамли имзо алгоритми баён этилган.

В данной статье изложен усовершенствованный алгоритм “слепой” электронной цифровой подписи на основе алгебры с параметром, который служит для обеспечения информационной безопасности электронных платёжных систем.

This article describes an improved algorithm "blind" digital signature based on algebra with a parameter that is used to ensure information security of electronic payment systems.

Ҳозирги кунда электрон тижоратнинг асосларидан бири бўлган электрон тўлов тизимларида ахборот хавфсизлигини таъминлаш усулларини ишлаб чиқиш масаласи муҳим аҳамият касб этмоқда. Электрон тўлов тизимларини бир неча синфларга ажратиш мумкин. Масалан, реал вақтда ишлайдиган аноним бўлмаган электрон тўлов тизимлари ва аноним бўлмаган автоном электрон тўлов тизимлари шулар жумласидандир [1]. Реал вақтда ишлайдиган аноним бўлмаган электрон тўлов тизимлари энг содда синфга тааллуқли тизим ҳисобланади. Ахборот хавфсизлиги нуқтаи назаридан қараганда, бундай тизимлар эътиборни унча тортмайди. Баъзи электрон тўлов тизимлари умуман криптографик усуллардан фойдаланмайди, баъзиларида эса ҳимояланган каналнинг мавжудлиги талаб этилади.

Аноним бўлмаган автоном электрон тўлов тизимларида бузишнинг олдини олувчи фойдаланувчи қурилмасидан фойдаланилади. Қурилма ўзига хос “чўнтак банки” бўлиб, битта электрон ҳисоб олиб боради ва ҳисобдан фақат рухсат этилган амалиётлар бажарилишини таъминлайди. Аммо бундай ёндашувнинг камчилиги истеъмолчи учун бу қурилманинг

муҳофазаланганлик даражаси номаълумлигидадир. Яна бир муаммо шундаки, иккита турли томон банк ҳам ва мижоз ҳам ўша битта қурилмага ишониши лозим бўлиб, бунда банк қурилма тузилишининг юқори даражада махфийлаштирилишидан манфаатдор бўлса, мижоз унинг эълон қилинганлигига ва очиқ текширила олишидан манфаатдор бўлади [1]. Аноним бўлмаган автоном электрон тўлов тизимларини икки турга ажратиш мумкин:

- электрон рақамли имзо (ЭРИ)га асосланган тизимлар;
- симметрик аутентификацияга асосланган тизимлар [2].

Амалиётда ЭРИга асосланган аноним бўлмаган автоном электрон тўлов тизимлари кенг оммалашмаган. Бунинг ўрнига симметрик криптотизимларнинг қўлланилишига асосланган тизимлар қўлланилади. Бу эса, симметрик тизимлардаги махфий калитларни тақсимлаш билан боғлиқ техник муаммоларни келтириб чиқаради.

Электрон тўлов тизими тўловчи ва қабул қилувчининг анонимлигини таъминлагани билан, ундаги анонимлик даражаси жуда паст. Тизимнинг пул маблағларини йўқотиб қўйишга бардошлилиги муаммоси минимал тарзда ечилган: яъни, агар иштирокчилардан бирортаси ўзининг махфий калитини йўқотиб қўйса, у ҳисобига кириш ҳуқуқидан айрилади, чунки унга ҳисобнинг тегишлилигини исботловчи (агар махсус чоралар кўрилмаган бўлса) бошқа усуллар мавжуд эмас.

“Кўр-кўрона” ЭРИга асосланган электрон тўлов тизимлари маълум бўлган аноним тўлов тизимларидан энг яхшиси ҳисобланади. Ушбу электрон тўлов тизимларининг асосий криптографик хусусияти уларда қўлланилган “кўр-кўрона” ЭРИ ғоясидир. Бу ғоя биринчи марта Дэвид Шаум ишларида таклиф этилган [3]. “Кўр-кўрона” ЭРИнинг асосий моҳияти қуйидагича. **А** юборувчи ҳужжатни **В** томонга юборади. **В** томон эса ҳужжатни имзолайди ва қайта **А** томонга юборади. **А** томон қабул қилган имзосидан фойдаланиб **В** томоннинг имзосини ҳисоблаб топиши ва уни ўзи учун муҳим бўлган ҳужжатни имзолашда ишлатиши мумкин. Бу протоколнинг бажарилиш якунида **В** томон махфий хабар ҳақида ҳам ва унинг тагидаги имзо ҳақида ҳам ҳеч нарсани билмайди.

Бу схемани ичига ҳужжат ва нусха кўчирувчи қоғоз жойланган конверт билан таққослаш мумкин. Агар конверт имзоланса, имзо ҳужжатга ҳам кўчиб қолади, бунда конверт очилганда ҳужжат имзоланган бўлади. Бунда “кўр-кўрона” имзодан мақсад имзоловчи шахс **В** нинг **А** томон хабари остига имзосини қўйиш асносида, **В** нинг ушбу хабар билан танишишга тўсқинлик қилишдан иборат.

“Кўр-кўрона” имзо протоколлари рақамли пул соҳасида кенг қўлланилади. Масалан, банк омонатчи алдамаслиги учун қуйидаги протоколдан фойдаланиши мумкин: омонатчи бир хил купюра номиналини 100 та турли рақамли ҳужжатларга ёзади ва банкда шифрланган ҳолда депозитга қўяди. Банк тасодифий равишда 99 тасини танлайди ва барчасида $10 ўрнига $1000 ёзилмаганлигини текшириш учун очишни талаб қилади. Сўнгра очилмай қолган конвертдаги купюрани кўрмасдан имзолайди.

“Кўр-кўрона” имзо алгоритмини қуйидагича ифодалаш мумкин:

1. **B** ҳар бирида қандайдир уникал сўз ёзилган n та ҳужжат тайёрлайди.
2. Ҳар бир ҳужжатни **B** бирор бир тасодифий сонга кўпайтиради, яъни уни уникал ниқобловчи (маскаловчи) кўпайтувчи билан ниқоблайди ва ҳосил бўлган ҳужжатларни **A** га юборади.
3. **A** барча ҳужжатларни қабул қилади ва тасодифий ҳолда улардан $n-1$ тасини танлайди.
4. **A** томон **B** дан танланган ҳужжатлар учун ниқобловчи кўпайтувчиларни юборишини сўрайди.
5. **B** юборади.
6. **A** $n-1$ та ҳужжатни очади ва уларнинг ҳақиқийлигига ишонч ҳосил қилади.
7. **A** қолган ҳужжатларни имзолайди ва **B** га юборади.
8. Энди **B** да **A** томонидан имзоланган уникал сўзли ҳужжат бор бўлиб, буни **A** билмайди.

“Кўр-кўрона” ЭРИ биринчи марта Давид Чаум томонидан RSA [4] криптотизими ёрдамида амалга оширилган:

Параметрларни генерация қилиш босқичи:

1. Махфий тутиладиган ҳамда етарли катта бўлган иккита ихтиёрий туб p ва q сонлар танланади (масалан, ҳар бири 1024 битли);
2. Уларнинг кўпайтмаси $n = pq$ ҳисобланиб, модул сифатида қабул қилинади.
3. Эйлер функциясининг қиймати $\varphi(n)=(p-1)\cdot(q-1)$ ҳисобланади.
4. Бу $\varphi(n)$ - функция билан ўзаро туб ва $(1<e<\varphi(n))$ шартни қанотлантирувчи бутун e сон танланади.
5. Сўнгра e сонига $\varphi(n)$ модул бўйича мультипликатив тескари бўлган d сони ҳисобланади ва d - махфий калит деб эълон қилинади.

B да ошкора калит e, махфий калит d, очиқ модул n бор. **A** томон **B** ни m хабарни ўқимасдан, яъни кўр-кўрона имзолашини хоҳлайди.

m хабар учун “кўр-кўрона” ЭРИ генерация қилиш босқичи:

1. **A** томон 1 дан n гача бўлган диапазондан n билан ўзаро туб бўлган тасодифий k сонни танлайди. Сўнгра у m хабарни қуйидагича ҳисоблаб ниқоблайди: $t=m\cdot k^e \bmod n$.

2. **B** томон қуйидагича имзолайди t: $t^d=(m\cdot k^e)^d \bmod n$.

3. **A** томон t^d даги ниқобни қуйидаги ҳисоблаш ёрдамида олиб ташлайди: $s=t^d/k \bmod n$.

4. Натижада $s=m^d \bmod n$ ҳосил бўлади.

1-мисол

Иккита туб сон танланади: $p=19,\ q=23$.

Модул ҳисобланади: $n=p\cdot q=19\cdot 23=437$.

Эйлер функцияси ҳисобланади : $\varphi(n)=(p-1)\cdot(q-1)=18\cdot 22=396$.

Ошкора калит танланади: $e=5$.

Махфий калит ҳисобланади: $5d \equiv 1 \bmod 437\ d=317$.

Ошкора калит жуфтлиги $(e, n)=(5,437)$ эълон қилинади.

Махфий калит $(d, \varphi(n))=(317,396)$ сақлаб қўйилади.

A томон **B** ни $m=43$ хабарни ўқимасдан, яъни кўр-кўрона имзолашини хоҳлайди.

A томон 1 дан 437 гача бўлган диапазондан 437 билан ўзаро туб бўлган тасодифий $k=29$ сонни танлайди.

$m=43$ хабарни қуйидагича ҳисоблаб ниқоблайди:

$t=m\cdot k^e \bmod n = 43\cdot 29^5 \bmod 437=224$.

B томон қуйидагича имзолайди t:

$t^d=(m\cdot k^e)^d \bmod n=(224)^{317} \bmod 437=421$.

A томон t^d даги ниқобни қуйидаги ҳисоблаш ёрдамида олиб ташлайди: $s=t^d/k \bmod n=421\cdot 29^{-1} \bmod 437=120$.

RSA протоколига асосланган такомиллашган “кўр-кўрона” ЭРИ алгоритмини параметрли группа асосида ишлаб чиқилди.

Параметрли группа қуйидагича таърифланади [5].

Таъриф. F_n – чекли, яъни, n та элементдан иборат бутун сонлар тўплами, ® – F_n устида $a®b \equiv a + b + a\cdot R\cdot b \ (mod\ n)$ кўринишида аниқланган алгебраик амал бўлса, $(F_n; Ω)$ – жуфтлик параметрли мультипликатив группа деб аталади; бу ерда $a, b, R \in F_n$, параметр $R>0$,+, · – бутун сонлар устида қўшиш, кўпайтириш амалларининг ва ® – параметрли кўпайтириш амалининг белгилари.

Параметр $R>0$ бўлса, *параметрли коммутатив группа мультипликатив*, $R=0$ бўлса, *параметрли коммутатив группа аддитивдир*.

Параметрли кўпайтириш амали ўз моҳияти бўйича тернар амалдир.

Нолдан фарқли тўплам элементи a учун тескари элемент $a^{\backslash -1}$ ва қарама-қарши элемент n-a мавжуд. $a^{\backslash -1}$ параметрли тескари элемент деб аталади ва

$a \circledR a^{\backslash -1} \equiv 0 \ (mod\ n)$ шартини қаноатлантиради. Бу ерда 0 – параметрли бирлик элементи бўлиб, $a \circledR 0 \equiv a$ аксиомани қаноатлантиради.

Параметрли тескари элемент қуйидагича ҳисобланади:

$$a^{\backslash -1} \equiv -a(1+aR)^{-1} \ (mod\ n).$$

Бу ерда $^{-1}$ - n модул бўйича тескарилаш амалининг белгисидир.

Таъриф. Модул арифметикасида параметр $R \geq 1$ билан даражага ошириш функцияси параметрли функция деб аталади.

Модул n бўйича асос a ни R параметрли x даражага ошириш натижаси $a^{\backslash x} (mod\ n)$ шаклида ифодаланади, бу ерда $^{\backslash}$ – R параметрли даражага ошириш белгисидир**.**

R параметр билан дискрет даражага ошириш худди анъанавий дискрет даражага ошириш жараёни каби рекурсив тарзда ҳисоблашлар орқали амалга оширилади, масалан, a нинг $e=37$ R параметрли даражасини қуйидагича ҳисобланади:

$$a^{\backslash 37} (mod\ p) \equiv a^{\backslash (32+4+1)} (mod\ p) \equiv (((((a^{\backslash 2})^{\backslash 2})^{\backslash 2})^{\backslash 2}) \circledR ((a^{\backslash 2})^{\backslash 2}) \circledR a \ (mod\ p),$$

бунда: $a^{\backslash 2} (mod\ p) \equiv a \cdot (2+R \cdot a) \ (mod\ p)$.

Параметрли функция чекли майдон ва ҳалқада дискрет даражага ошириш функциясининг хоссаларига ўхшаш хоссаларга эга.

Ушбу келтирилган параметрли алгебра ва параметрли функцияни қўллаб, RSA протоколига асосланган “кўр-кўрона” ЭРИ алгоритмини такомиллаштирамиз. RSA протоколига асосланган такомиллашган “кўр-кўрона” ЭРИ алгоритми қуйида келтирилади.

Параметрларни генерация қилиш босқичи:

1. Махфий тутиладиган ҳамда етарли катта бўлган иккита ихтиёрий туб p ва q сонлар танланади (масалан, ҳар бири 1024 битли);
2. Уларнинг кўпайтмаси $n = pq$ ҳисобланиб, модул сифатида қабул қилинади.
3. R – параметр, $R < q$ шартни қаноатлантирувчи натурал сон бўлиб, фойдаланувчиларнинг чекланган гуруҳи учун очиқ.
4. Эйлер функциясининг қиймати $\varphi(n)=(p-1)\cdot(q-1)$ ҳисобланади.
5. Бу $\varphi(n)$ - функция билан ўзаро туб ва $(1<e<\varphi(n))$ шартни қанотлантирувчи бутун e сон танланади.
6. Сўнгра e сонига $\varphi(n)$ модул бўйича мультипликатив тескари бўлган d сони ҳисобланади ва d -махфий калит деб эълон қилинади.

B томонда ошкора калит e, махфий калит d, очиқ модул n ва R параметр бор. **A** томон **B** ни m хабарни ўқимасдан, яъни кўр-кўрона имзолашини хоҳлайди.

1. **A** томон *1* дан *n* гача бўлган диапазондан *n* билан ўзаро туб бўлган тасодифий *k* сонни танлайди. Сўнгра у *m* хабарни қуйидагича ҳисоблаб ниқоблайди: $t=m®k^{\backslash e} \bmod n$.

2. **B** томон қуйидагича имзолайди *t*: $t^{\backslash d}=(m®k^{\backslash e})^{\backslash d} \bmod n$.

3. **A** томон $t^{\backslash d}$ даги ниқобни қуйидаги ҳисоблаш ёрдамида олиб ташлайди: $s=t^{\backslash d} ® k^{\backslash -1} \bmod n$.

4. Натижада $s=m^{\backslash d} \bmod n$ ҳосил бўлади.

2-мисол

Иккита туб сон танланади: $p=19, q=23$.

Модулни ҳисобланади: $n=p\cdot q=19\cdot 23=437$.

Эйлер функцияси ҳисобланади : $\varphi(n)=(p-1)\cdot(q-1)=18\cdot 22=396$.

Ошкора калит танланади: $e=5$.

Махфий калит ҳисобланади: $5d \equiv 1 \bmod 437\ d=317$.

Ошкора калит жуфтлиги $(e, n)=(5,437)$ эълон қилинади.

Махфий калит $(d, \varphi(n))=(317,396)$ сақлаб қўйилади.

A томон **B** ни $m=43$ хабарни ўқимасдан, яъни кўр-кўрона имзолашини хоҳлайди.

A томон 1 дан 437 гача бўлган диапазондан 437 билан ўзаро туб бўлган тасодифий $k=29$ сонни танлайди.

$m=43$ хабарни қуйидагича ҳисоблаб ниқоблайди:

$t=m®k^{\backslash e} \bmod n =43®29^{\backslash 5} \bmod 437=43®251=244$.

B томон қуйидагича имзолайди *t*:

$t^{\backslash d}=(m®k^{\backslash e})^{\backslash d} \bmod n =(224)^{\backslash 317} \bmod 437=301$.

A томон t^d даги ниқобни қуйидаги ҳисоблаш ёрдамида олиб ташлайди: $s=t^d/k \bmod n=301\cdot 29^{-1} \bmod 437=147$.

Ушбу мақолада юқорида келтирилган параметрли алгебра асосида такомиллашган “кўр-кўрона” ЭРИ алгоритмининг дастур ойналари келтирилган.

Факторлаш муаммосига асосланган такомиллашган “кўр-кўрона” ЭРИ алгоритми асосида ишлаб чиқилган дастурнинг ишлаши қуйида келтирилган.

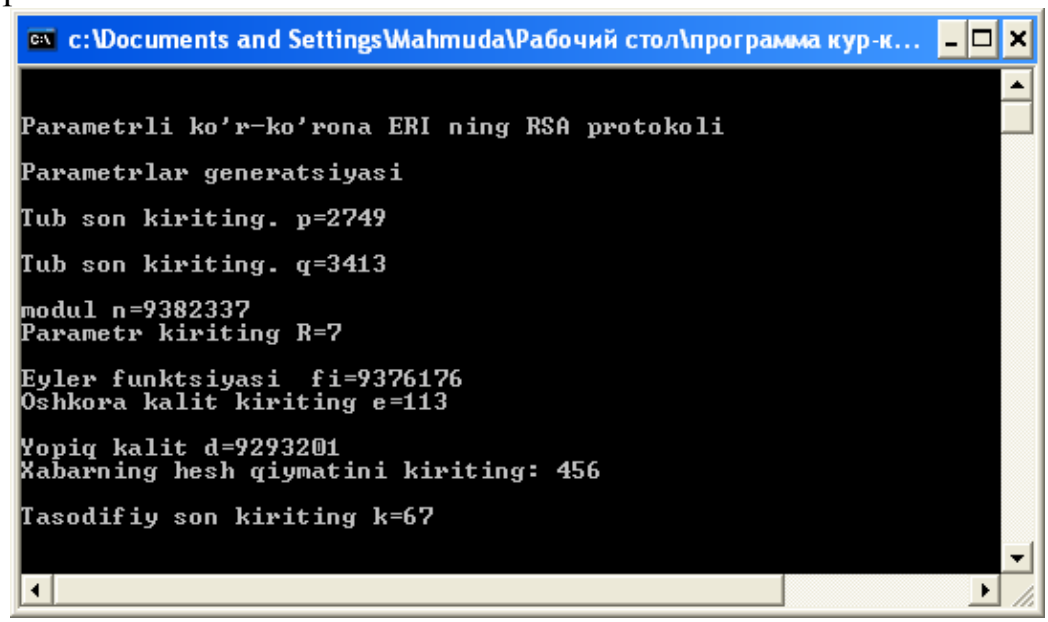
“Кўр-кўрона” ЭРИнинг параметрли алгебра асосида такомиллаштирилган RSA протоколи алгоритмининг дастури:

1-босқич ташкилий босқичдан иборат бўлиб, бу босқичда *RSA* протоколи параметрлари генерация қилинади:

- иккита туб сон, бу икки туб сонлар асосида протокол модули ва Эйлер функцияси;
- ошкора ва махфий калитлар;
- *R* параметр;
- хабарнинг хэш-қиймати;

- тасодифий сон.

Қуйидаги 1-расмда *ташкилий босқичнинг дастур ойнаси кўриниши* келтирилган.

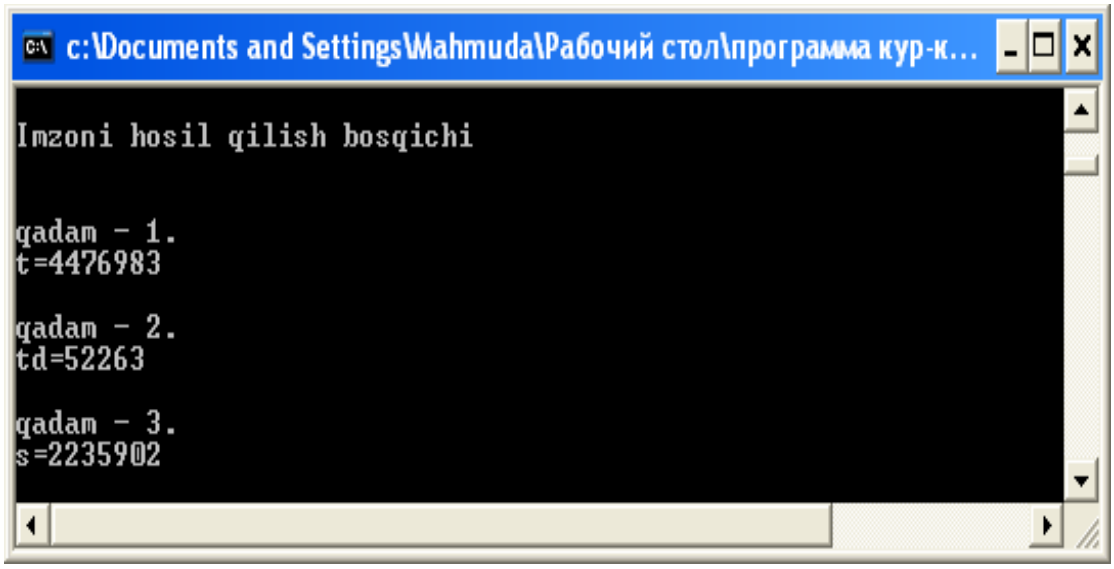


1-расм. Ташкилий босқич дастур ойнаси

B да ошкора калит *e*, махфий калит *d*, очиқ модул *n* ва *R* параметр бор. **A** томон **B** ни *m* хабарни ўқимасдан, яъни кўр-кўрона имзолашини хоҳлайди.

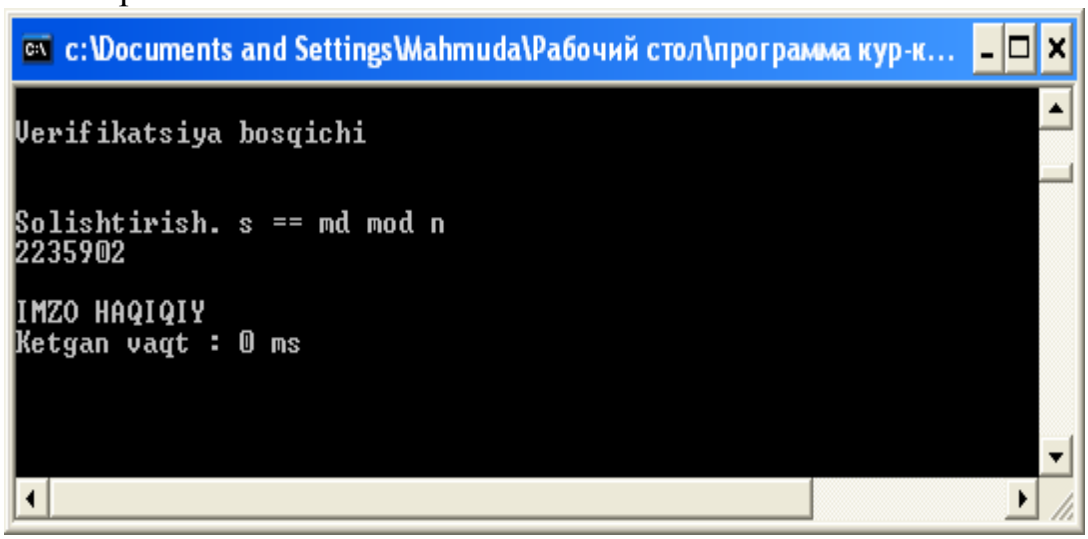
- **A** томон *m* хабарни қуйидагича ниқоблайди: $t=m \circledR k^{\backslash e} \bmod n$.
- **B** қуйидагича имзолайди *t*: $t^{\backslash d}=(m \circledR k^{\backslash e})^{\backslash d} \bmod n$.
- **A** ниқобни қуйидаги олиб ташлайди: $s=t^{\backslash d} \circledR k^{\backslash -1} \bmod n$.

Қуйидаги 2-расмда *ушбу босқичнинг дастур ойнаси* келтирилган.



2-расм. *RSA* протоколига асосланган такомиллашган "кўр-кўрона" ЭРИ ҳосил қилиш босқичи

Имзони текшириш босқичида **B** $s=m^{\backslash d}$ *mod n* ни ҳисоблайди, бунда ҳосил бўлган *s* матинни ЭРИ қиймати билан тенг, демак имзо ҳақиқий бўлади. Қуйидаги 3-расмда “кўр-кўрона” *ЭРИ текшириш босқичнинг дастур ойнаси* келтирилган.



3-расм. *RSA* протоколига асосланган такомиллашган “кўр-кўрона” ЭРИ текшириш босқичи

“Кўр-кўрона” ЭРИнинг параметрли алгебра асосида такомиллаштирилган RSA алгоритмининг дастури қуйидаги конфигурацияли компьютерда ишлаб чиқилди:

Операцион тизим: Windows 7.

Тезкор хотира: 4.00 ГБ.

Тизим тури: 64 разрядли ОТ.

Процессор: Intel (R) Pentium (R) CPU G2020, 2.90 GHz.

Мазкур мақолада келтирилган такомиллашган алгоритмда қўшимча махфийлик сифатида *R* параметри киритилиши ҳисобига ҳисоблаш мураккаблиги ортган. Бу эса ишлаб чиқилган алгоритмнинг бардошлилиги юқорилигидан далолат беради. Ишлаб чиқилган криптографик алгоритм ва унинг дастурий таъминотидан ҳозирги кунда Республикамизда жорий этила бошланган миллий электрон тўлов тизимларида ахборот хавфсизлигини таъминлаш учун фойдаланиш тавсия этилади.

ФОЙДАЛАНИЛГАН АДАБИЁТЛАР РЎЙХАТИ

1. «Анонимные денежные переводы через Интернет» Игорь Ананченко, "Мир Internet", №3 март 2002 г.

2. *С.Запечников. Криптографические протоколы* и их применение в финансовой и коммерческой деятельности , Москва Горячая линия - Телеком 2007.

3. Chaum D. Bilind Signatures for untraceable payments // Advances in Cryptology – Proc. of CRYPTO’82.

4. Chaum: Blind signature systems, Advances in Cryptology, Crypto' 83, Plenum, p.153.
Хасанов Х.П. Такомиллашган диаматрицалар алгебралари ва параметрли алгебра асосида криптотизимлар яратиш усуллари ва алгоритмлари. Тошкент, ФТМТМ, 2008.