Параметрли алгебра асосида такомиллаштирилган RSA “кўр-кўрона” электрон рақамли имзо алгоритми

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

Ушбу мақолада муаллифлар томонидан ишлаб чиқилган электрон тўлов тизимларида ахборот хавфсизлигини юқори даражада муҳофазаланганлигини таъминлаш учун хизмат қилиши мумкин бўлган ахборотни криптографик муҳофазалаш алгоритми ёритилган.

В данной статье описан алгоритм криптографической защиты информации, способной обеспечить высокую степень информационной безопасности в электронных платежных системах, разработанный авторами.

This article describes an algorithm for cryptographic protection of information that can provide a high degree of information security in electronic payment systems, developed by the authors.

Ҳозирги кунга келиб Республикамизда тижоратнинг янги йўналишларидан бири бўлган «электрон тижорат» жадаллик билан ривожланиб бормоқда ва айни кунда тижоратнинг электрон турлари оммалашиб бормоқда. Электрон тижоратнинг асосларидан бири бўлган электрон тўлов тизимларида ахборот хавфсизлигини таъминлаш усулларини ишлаб чиқиш масаласи муҳим аҳамият касб этади. Ушбу мақолада муаллифлар томонидан ишлаб чиқилган электрон тўлов тизимларида ахборот хавфсизлигини юқори даражада муҳофазаланганлигини таъминлаш учун хизмат қилиши мумкин бўлган ахборотни криптографик муҳофазалаш алгоритми ёритилган.

Замонавий электрон тўлов тизимларида “кўр-кўрона” ёки қоронғилаштирилган электрон рақамли имзо ғоясидан фойдаланилади. Чунки “кўр-кўрона” имзога асосланган электрон тўлов тизимлари бугунги кунда маълум бўлган аноним тўлов тизимларидан энг яхшиси ҳисобланади. “Кўр-кўрона” электрон рақамли имзо (ЭРИ) деганда қандайдир шифрланган рақамли хабарга мос келадиган тўғри ЭРИни шакллантириш имконини берадиган имзо тушунилади [1]. “Кўр-кўрона” ЭРИ протоколлари рақамли пул соҳасида кенг қўлланилади. “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.

“Кўр-кўрона” ЭРИ биринчи марта 1983 йилда Давид Чаум томонидан RSA [2-3] 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 $\varphi(n)=(p-1)(q-1)$ ҳисобланади.

4. Бу $\varphi(n)$-функция билан ўзаро туб ва $(1<e<\varphi(n))$ шартни қанотлантирувчи бутун *e* сони танланади.

5. Сўнгра *e* сонига $\varphi(n)$ модул бўйича мультипликатив тескари бўлган d сони ҳисобланади ва d - махфий калит деб эълон қилинади.

Бобда ошкора калити *e*, махфий калити *d*, очиқ модул *n* бор. Алиса Бобни *m* хабарни ўқимасдан, яъни кўр-кўрона имзолашини хоҳлайди.

m хабар учун "кўр-кўрона" ЭРИ генерация қилиш босқичи:

1. Алиса 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. Боб қуйидагича имзолайди *t*: $t^d=(m\cdot k^e)^d \bmod n$.

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

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

Келтирилган алгоритмнинг бажарилишини қуйидаги 1-мисолда кўриб чиқамиз.

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: $5\cdot d \equiv 1 \bmod 437$ $d=317$.

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

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

Алиса Бобни $m=43$ хабарни ўқимасдан, яъни кўр-кўрона имзолашини хоҳлайди.

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

$m=43$ хабарни қуйидагича ҳисоблаб ниқоблайди:

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

Боб қуйидагича имзолайди *t*:

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

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

Параметрли группа қуйидагича таърифланади [4].

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.

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 ҳисобланди.
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.

Бобда ошкора калит *e*, махфий калит *d*, очиқ модул *п* ва *R* параметр бор. Алиса Бобни *m* хабарни ўқимасдан, яъни кўр-кўрона имзолашини хоҳлайди.

1. Алиса 1 дан *п* гача бўлган диапазондан *п* билан ўзаро туб бўлган тасодифий *k* сонни танлайди. Сўнгра у *m* хабарни қуйидагича ҳисоблаб ниқоблайди: $t=m \circledR k^{\backslash e} \ mod\ n.$
2. Боб қуйидагича имзолайди *t*: $t^{\backslash d}=(m \circledR k^{\backslash e})^{\backslash d} \ mod\ n.$
3. Алиса $t^{\backslash d}$ даги ниқобни қуйидаги ҳисоблаш ёрдамида олиб ташлайди: $s=t^{\backslash d} \circledR k^{\backslash -1} \ mod\ n.$
4. Натижада $s=m^{\backslash d} \ mod\ n$ ҳосил бўлади.

Юқорида келтирилган алгоритмнинг бажарилишини қуйидаги 2-мисолда кўриб чиқамиз.

2-мисол.

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

Модулни ҳисобланади: *n=p·q=19·23=437.*

Эйлер функцияси ҳисобланади : $\varphi(n)=(p-1)\cdot(q-1)=18\cdot22=396.$

Ошкора калит танланади: *e=5.*

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

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

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

Алиса Бобни *m=43* хабарни ўқимасдан, яъни кўр-кўрона имзолашини хоҳлайди.

Алиса 1 дан *437* гача бўлган диапазондан *437* билан ўзаро туб бўлган тасодифий *k=29* сонни танлайди.

m=43 хабарни қуйидагича ҳисоблаб ниқоблайди:

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

Боб қуйидагича имзолайди *t*:

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

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

Юорида келтирилган “кўр-кўрона” ЭРИ алгоритмларида криптобардошликнинг ортиши бир томонлама параметрли функция ифодасида қатнашадиган даражага ошириш параметри *R* ни ноқонуний фойдаланувчилардан сир сақланиши ҳисобига эришилади. Яъни бунда махсус аппаратли ва унга мос криптомодулларда амалга оширилган “кўр-кўрона” ЭРИ алгоритмлари учун модул танлашда уларнинг узунликларини ҳисоблаш қурилмаларининг тезликлари ортиб боришига мос тарзда йилдан-йилга ошириб бориш шарт эмас. Чунки зарурий бардошликка даража параметри *R* ҳисобига эришилади.

Фойдаланилган адабиётлар

1. O’z DSt 1109:2013 «Ахборот технологияси. Ахборотнинг криптографик муҳофазаси. Атама ва таърифлар».

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

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

4. Хасанов Х.П. Такомиллашган диаматрицалар алгебралари ва параметрли алгебра асосида криптотизимлар яратиш усуллари ва алгоритмлари. – Тошкент, 2008. - 208 б.