ISSN (o): 3030-3362



№ 4(26)
27.04.2025
IF 2024 11.7

RTADQIQ VA TATBIQ
Research and implementation
scientific-methodical journal

SCIENCES
Exact, Natural, Political, Social, Economic, Technical, Medical, Pedagogical

zenodo
Google scholar
OpenAIRE
ISSN INTERNATIONAL STANDARD SERIAL NUMBER INTERNATIONAL CENTRE
CERTIFICATE № 078777
ral-journal.uz
@ferteach_uz

Editor in Chief:
F.M.Mukhtarov
PhD, associate prof

Executive editor
S.I.Zokirov
PhD, associate prof

Languages:
Uzbek, Russian, English and Karakalpak

Registered in the Agency of Information and Mass Communications under the Administration of the President of the Republic of Uzbekistan on May 3, 2023 under number 078777.

IF-2024: 11.7

@ferteach_uz
+99893-343-13-14
https://rai-journal.uz

SCAN ME

Editorial Board:

B.R.Ismailov *– Dr. Tech. Sc., Prof., M.Avezov South Kaz. Univ., Shymkent, Kazakhstan*
I.Bjorn *- Ph.D., Imeritus, Technical University of Denmark, Copenhagen, Denmark*
A.Rasulov *– Dr. Phys.-Math. Sc., Prof., TUIT Fergana Branch, Fergana, Uzbekistan*
L.K.Mamadaliyeva *– Dr. Tech. Sc. (DSc), Prof., FerPI, Fergana, Uzbekistan*
M.E.Yunusaliyev *– Dr. Tech. Sc. (DSc), Prof., FerPI, Fergana, Uzbekistan*
X.B.Ismailov *– Can. Tech. Sc., Assoc. Prof., M.Avezov South Kaz. Univ., Shymkent, Kazakhstan*
J.T.Moldaliyev *– Can. Bio. Sc., Assoc. Prof.. OshSU, Osh, Kyrgyzstan*
O.S.Nazarmatov *– DSc in Econ., TUIT Fergana Branch, Fergana, Uzbekistan*
G.K.Obidova *- DSc in Ped., TUIT Fergana Branch, Fergana, Uzbekistan*
T.M.Abdullayev *- Ph.D. in Tech. Sc., TUIT Fergana Branch, Fergana, Uzbekistan.*
N.I.Ibrokhimov *- Ph.D. in Phys.-Math., TUIT Fergana Branch, Fergana, Uzbekistan.*
A.R.Nurmatov *- Ph.D. in History, NamSU, Fergana, Uzbekistan.*
T.Yu.Bakirov *- PhD in Ped. Sc., FarSU, Fergana, Uzbekistan*
D.F.Tukhtasinov *- Ph.D. in Ped. Sc., TUIT Fergana branch, Fergana, Uzbekistan.*
S.B.Atajonova *- Ph.D in Ped. Sc., AndMI, Andijan Uzbekistan*
Sh.A.Umarov *- Ph.D. in Phys.-Math. Sc., TUIT Fergana branch, Fergana, Uzbekistan.*
I.A.Rustamov *- Ph.D. in Phil. Sc., TUIT Fergana branch, Fergana, Uzbekistan.*
B.Kh.Tolipov *- Ph.D. in Phil. Sc., TUIT Fergana branch, Fergana, Uzbekistan.*
O.Kh.Otakulov *- Can. Tech. Sc., Assoc. Prof.. TUIT Fergana branch, Uzbekistan*
O.S.Raimjonova *- Ph.D in Tech. Sc., Assoc. Prof., TUIT Fergana branch, Uzbekistan*
R.A.Nurdinova *- Ph.D in Tech. Sc., Assoc. Prof., TUIT Fergana branch, Uzbekistan*
M.I.Ismoilov *- Ph.D in Tech. Sc., Assoc. Prof., TUIT Fergana branch, Uzbekistan*
I.T.Tojiboyev *- Can. Tech. Sc., Assoc. Prof., Fergana State University, Uzbekistan*
Sh.J.Kholmatov *- PhD., TUIT Fergana branch, Fergana, Uzbekistan*
Z.N.Khatamova *- PhD. in Tech. Sc., TUIT Fergana branch, Fergana, Uzbekistan*
Q.Kh. Akhunov *- Can. Tech. Sc., Assoc. Prof., Fergana Polytechnic Institute, Uzbekistan*
M.Kh. Okhunov *- Can. Tech. Sc., Assoc. Prof., Fergana Polytechnic Institute, Uzbekistan*
A.Q. Khomidov *- Can. Tech. Sc., Assoc. Prof., Fergana Polytechnic Institute, Uzbekistan*
Sh.Sh. Akramov *- PhD, TUIT Fergana Branch, Fergana, Uzbekistan*
A.A. Salimov *- PhD in Econ., Fergana Polytechnic Institute, Uzbekistan*
Z.G'. Ubaydullayev *– Can. Econ., TUIT Qarchi Branch, Qarchi, Uzbekistan*
S.S. Ibragimov *- Ph.D in Tech. Sc., AndMI, Andijan Uzbekistan*
Sh.J. Kholmatov *- Ph.D. in Phil., TUIT Fergana Branch, Fergana, Uzbekistan*
G.D. Kuchkarova *- Ph.D. in Phil., TUIT Fergana Branch, Fergana, Uzbekistan*
I.R.Teshabayeva *- Ph.D. in Tech. Sc., TUIT Fergana Branch, Fergana, Uzbekistan*
A.L.Meliquziyev *- Ph.D. in Phil. Sc., TUIT Fergana Branch, Fergana, Uzbekistan*
O.U.Kholmatova *- Ph.D. in Phil. Sc., TUIT Fergana Branch, Fergana, Uzbekistan*
N.N.Radjabov *- Ph.D. in Phil. Sc., Assoc. Prof., Oriental University, Tashkent, Uzbekistan*
Sh.A.Yuldashov *- Ph.D. in Tech. Sc., Fergana State University, Fergana, Uzbekistan*
A.A.Yuldashev *- Ph.D. in Tech. Sc., Fergana State University, Fergana, Uzbekistan*
M.Israilov *- Can. Tech. Sc., Armed Forces of the Republic of Uzbekistan Academy of Forces*
N.S.Abdullaeva *- PhD in Ped. Sc., NamDU, Namangan, Uzbekistan*
A.G.Turgunboyeva *- PhD in Ped. Sc., NamDPI, Namangan, Uzbekistan*
M.A.Abdullaeva *- Prof., NamDU, Namangan, Uzbekistan*
I.O.Ergashev *- PhD in Econ., Fiscal Institute, Tashkent, Uzbekistan*
N.T.Mamatxanova *- PhD in Ped. Sc., NamDPI, Namangan, Uzbekistan*
U.Yu.Akhundzhanov *- PhD in Tech. Sc., TUIT Fergana Branch, Fergana, Uzbekistan*
O.M.Ergashev *- PhD in Tech. Sc., TUIT Fergana Branch, Fergana, Uzbekistan*
N.R.Khallieva *- PhD in Econ., Bukhara MTI, Bukhara, Uzbekistan*
F.K.Achilova *– Can. Econ. Sc., TUIT Qarchi Branch, Qarchi, Uzbekistan*
A.K.Samyayev *- PhD in Geog., Sam. Reg. Ped. Skills Center, Samarkand, Uzbekistan*
J.S.Abdullayev *- Can. Phys.-Math. Sc., Assoc. Prof.. TUIT Fergana branch, Uzbekistan*
N.D.Botirova *–PhD in Ped, TUIT Fergana Branch, Fergana, Uzbekistan*

Bosh muharrir:

Tahrir hay'ati:

F.M.Mukhtarov
PhD, dotsent

Ijrochi muharrir:
S.I.Zokirov
PhD, dotsent

Nashr tillari:
O‘zbek, Rus, Inzliz va Qoraqalpoq

O‘zbekiston Respublikasi Prezidenti Administratsiyasi huzuridagi Axborot va ommaviy kommunikatsiyalar agentligi tomonidan 2023-yil 3-mayda 078777 raqami bilan ro‘yxatga olingan..

IF-2024: 11.7

@ferteach_uz
+99893-343-13-14
https://rai-journal.uz

B.R.Ismailov *– t.f.d., prof. M.Avezov Jan. Qoz. Univ-ti., Chimkent, Qozog‘iston*
I.Byorno - *Ph.D., Imeritus, Daniya Texnika Universiteti, Kopengagen, Daniya*
A.Rasulov *– f.-m..f.d., prof.TATU Farg‘ona filiali, Farg‘ona, O‘zbekiston*
L.K.Mamadaliyeva – *t.f.d. (DSc), prof. FarPI, Farg‘ona, O‘zbekiston*
M.E.Yunusaliyev – *t.f.d. (DSc), prof. FarPI, Farg‘ona, O‘zbekiston*
X.B.Ismailov- *t.f.n., dot., M.Avezov Jan. Qoz. Univ-ti., Chimkent, Qozog‘iston*
J.T.Moldaliyev *- bio. f. n., dotsent. OshDU, Osh, Qirg‘iziston*
O.S.Nazarmatov *- iqt.f.d. DSc, TATU Farg‘ona filiali, Farg‘ona, O‘zbekiston*
G.K.Obidova *- ped.f.d. DSc, TATU Farg‘ona filiali, Farg‘ona, O‘zbekiston*
T.M.Abdullayev *– t.f.b. Ph.D., TATU Farg‘ona filiali, Farg‘ona, O‘zbekiston.*
N.I.Ibrokhimov *– f.-m.f.b. Ph.D., TATU Farg‘ona filiali, Farg‘ona, O‘zbekiston.*
A.R.Nurmatov *– tarix f.b. Ph.D., NamDU, Farg‘ona, O‘zbekiston.*
T.Yu.Bakirov *- ped. f.b. PhD, FarDU, Farg'ona, O‘zbekiston*
D.F.To‘xtasinov *- ped.f.b. Ph.D., TATU Farg‘ona filiali, Farg‘ona, O‘zbekiston.*
S.B.Atajonova *- ped.f.b. Ph.D, AndMI, Andijon O‘zbekiston*
Sh.A.Umarov *- f.-m.f.b. Ph.D., TATU Farg‘ona filiali, Farg‘ona, O‘zbekiston.*
I.A.Rustamov *- fal.f.b. Ph.D., TATU Farg‘ona filiali, Farg‘ona, O‘zbekiston.*
B.X.Tolipov *- f.f.b. Ph.D., TATU Farg‘ona filiali, Farg‘ona, O‘zbekiston.*
O.X.Otaqulov *– t.f.n., dotsent. TATU Farg‘ona filiali, O‘zbekiston*
O.S.Raimjonova *– t.f.b. Ph.D, dotsent, TATU Farg‘ona filiali, O‘zbekiston*
R.A.Nurdinova *– t.f.b. Ph.D, dotsent, TATU Farg‘ona filiali, O‘zbekiston*
M.I.Ismoilov – *t.f.b. Ph.D, dotsent, TATU Farg‘ona filiali, O‘zbekiston*
I.T.Tojiboyev *– t.f.n., dotsent, Farg‘ona davlat universiteti, O‘zbekiston*
Sh.J.Kholmatov *- i.i.f.b. PhD., TATU Farg‘ona filiali, Farg‘ona, O‘zbekiston*
Z.N.Khatamova *- t.f.b. PhD., TATU Farg‘ona filiali, Farg‘ona, O‘zbekiston*
Q.X. Axunov *- t.f.n., dotsent, Farg‘ona politexnika instituti, O‘zbekiston*
M.X. Oxunov *- t.f.n., dotsent, Farg‘ona politexnika instituti, O‘zbekiston*
A.Q.Xomidov *- t.f.n., dotsent, Farg‘ona politexnika instituti, O‘zbekiston*
Sh.Sh.Akramov *– q.x.f.b. PhD, TATU Farg‘ona filiali, Farg‘ona, O‘zbekiston*
A.A.Salimov *- iqt.f.b. PhD, Farg‘ona politexnika instituti, O‘zbekiston*
Z.G‘.Ubaydullayev *- iqt.f.n., TATU Qarchi filiali, Qarchi, O‘zbekiston*
S.S.Ibragimov *- t.f.b. Ph.D, AndMI, Andijon O‘zbekiston*
Sh.J.Xolmatov *- fal.f.b. Ph.D., TATU Farg‘ona filiali, Farg‘ona, O‘zbekiston*
G.D.Kuchkarova *- fal.f.b. Ph.D., TATU Farg‘ona filiali, Farg‘ona, O‘zbekiston*
I.R.Teshabayeva *- t.f.b. Ph.D., TATU Farg‘ona filiali, Farg‘ona, O‘zbekiston*
A.L.Meliquziyev *- fil.f.b. Ph.D., TATU Farg‘ona filiali, Farg‘ona, O‘zbekiston*
O.U.Xolmatova *- fil.f.b. Ph.D., TATU Farg‘ona filiali, Farg‘ona, O‘zbekiston*
N.N.Radjabov *- fil.f.b. Ph.D., dotsent, Oriental University, Toshkent, O‘zbekiston*
Sh.A.Yuldashov *- t.f.b. Ph.D., Farg‘ona davlat universiteti, Farg‘ona, O‘zbekiston*
A.A.Yuldashev *- t.f.b. Ph.D., Farg‘ona davlat universiteti, Farg‘ona, O‘zbekiston*
M.Israilov *- t.f.n., O‘zbekiston Respublikasi Qurolli Kuchlar Akademiyasi*
N.S.Abdullayeva *- p.f.b. PhD, NamDU, Namangan, O‘zbekiston*
A.G.Turg‘unboyeva *- p.f.b. PhD, NamDPI, Namangan, O‘zbekiston*
M.A.Abdullayeva *- professor, NamDU, Namangan, O‘zbekiston*
I.O.Ergashev *– iqt.f.b. PhD, Fiskal instituri, Toshkent, O‘zbekiston*
N.T.Mamatxanova *- p.f.b. PhD, NamDPI, Namangan, O‘zbekiston*
U.Yu.Axundjanov *- t.f.b. PhD, TATU Farg‘ona filiali, Farg‘ona, O‘zbekiston*
O.M.Ergashev *- t.f.b. PhD, TATU Farg‘ona filiali, Farg‘ona, O‘zbekiston*
N.R.Xallieva *- iqt.f.b. PhD, Buxoro MTI, Buxoro, O‘zbekiston*
F.K.Achilova *- iqt.f.n., TATU Qarchi filiali, Qarchi, O‘zbekiston*
A.K.Samyayev *- g.f.b. PhD, Sam. vil. ped. mah. mar, Samarqand, O‘zbekiston*
J.S.Abdullayev *- f.-m.f.n., TATU Farg‘ona filiali, Farg‘ona, O‘zbekiston.*
N.D.Botirova *– ped.f.b. PhD, TATU Farg‘ona filiali, Farg‘ona, O‘zbekiston*

Маълумотлар алмашинувини электрон рақамли имзо орқали амалга ошириш йўллари

Турдиматов Мамиржон Мирзаевич, Араббоев Алишер Авазбек ўғли

Фарғона давлат техника университети

Copyright: © 2025 by the author.
Licensee: This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (https:// creativecommons.org/licenses/by/ 4.0/).

Аннотация. Ушбу мақолада электрон рақамли имзо алгоритмлари ёрдамида маълумотлар алмашинувини амалга ошириш усуллари ва Шнор схемаси асосида электрон рақамли имзо алгоритмининг моҳияти таснифи ва уларнинг қиёсий таҳлили келтирилган, хамда мураккаблиги бўйича синфланган. Шунингдек, Эл-Гамалнинг рақамли имзо схемаси билан боғлиқ муаммолар ўрганилган.

Таянч иборалар: электрон рақамли имзо, рақамли имзо схемаси, симметрик, асимметрик, параметрли алгебра, ЭЭЧ, дискрет логарифмлаш, электрон хужжат, очиқ калит, ёпиқ калит.

Способы реализации обмена информацией посредством электронной цифровой подписи

Турдиматов Мамирджон Мирзаевич, Араббоев Алишер Авазбек оглы

Ферганский государственный технический университет

Аннотация. В данной статье представлены методы реализации обмена данными с использованием алгоритмов электронной цифровой подписи и дана классификация сущности алгоритма электронной цифровой подписи на основе схемы Шнорра, а также проведен их сравнительный анализ, а также дана классификация по сложности. Также были изучены проблемы со схемой цифровой подписи Эль-Гамаля.

Ключевые слова: электронная цифровая подпись, схема цифровой подписи, симметричный, асимметричный, параметрическая алгебра, ЭЭЧ, дискретный логарифм, электронный документ, открытый ключ, закрытый ключ.

Ways to implement information exchange through electronic digital signature

Turdimatov Mamirjon Mirzaevich, Arabboyev Alisher Avazbek ogli

Fergana State Technical University

Abstract. This article presents methods for implementing data exchange using electronic digital signature algorithms and a classification of the essence of the electronic digital signature algorithm based on the Schnorr scheme and their comparative analysis, as well as classification by complexity. Also, problems associated with El-Gamal's digital signature scheme are studied.

Key terms: electronic digital signature, digital signature scheme, symmetric, asymmetric, parametric algebra, EDS, discrete logarithmization, electronic document, public key, private key.

Ҳозирги кунга келиб жамиятнинг барча соҳаларида замонавий ахборот технологияларини жорий этиш, ҳамда улардан фойдаланиш, фуқароларнинг ахборотга бўлган эҳтиёжларини янада тўлароқ қондириш, жаҳон ахборот тизимига кириш ҳамда унинг ресурсларидан фойдаланишни кенгайтириш учун қулай шарт – шароитлар яратилиб келинмоқда. Шуларни инобатга олган холда “Электрон ҳужжат”, “Электрон рақамли имзо(ЭРИ)” тушунчалари тизимнинг ҳар бир соҳасига кириб бормоқда.

Электрон ҳужжат техника воситаларидан ва ахборот тизимлари хизматларидан ҳамда ахборот технологияларидан фойдаланилган ҳолда яратилади, ишлов берилади ва сақланади. Электрон шаклда қайд этилган, ЭРИ билан тасдиқланган ва электрон ҳужжатнинг уни идентификация қилиш имкониятини берадиган бошқа реквизитларига эга бўлган ахборот электрон ҳужжатдир [1].

Агар биз ЭРИ тарихига назар ташласак у 1976 йилда Уитфилд Диффи ва Мартин Хелман биринчи марта "Электрон рақамли имзо" тушунчасини таклиф қилишди, гарчи улар фақат рақамли имзо схемалари мавжуд бўлиши мумкинлигини тахмин қилишган.

1977 йилда Роналд Ривест , Ади Шамир ва Леонард Адлеман RSA ишлаб чиқдилар, ундан бошқа ўзгартиришларсиз ибтидоий рақамли имзоларни яратиш учун фойдаланиш мумкин. Шунингдек, 1984 йилда Шафи Голдwассер , Силвио Мисали ва Роналд Ривест биринчи бўлиб рақамли имзо алгоритмлари учун хавфсизлик талабларини қатъий белгиладилар. Улар рақамли имзо алгоритмларига ҳужумлар моделларини тасвирлаб беришди, тавсифланган талабларга жавоб берадиган GMP Электрон хужжатларни алмашиниш

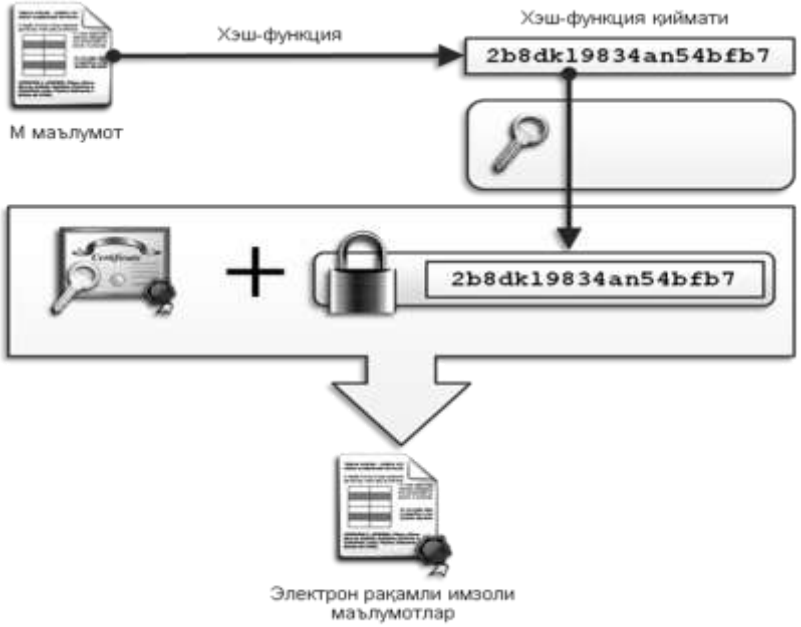
жараёнларидаги ахборот хавфсизлигини таъминлаш муаммосини ҳал этишда муҳим ўрин эгаллаган криптографик восита Шнор схемасига асосланган электрон рақамли имзо алгоритми хисобланади.

Эл-Гамалнинг рақамли имзо схемаси билан боғлиқ муаммо шундаки,

дискрет логарифмини қийинлаштириши учун жуда катта бўлиши керак. Узунлиги камида 1024 бит бўлиши тавсия этилади. Сиз 2048 бит ҳажмида имзо қўйишингиз мумкин. Имзо ҳажмини камайтириш учун Шнорр Эл-Гамал схемасига асосланган, аммо қисқартирилган имзо ҳажмига эга янги схемани таклиф қилди. Қуйидаги расмда Шнорнинг рақамли имзо схемаси ҳақида умумий тушунча берилган.[1]

Шнорр рақамли имзо схемасининг умумий ғояси Имзоланиш жараёнида иккита функция иккита имзо ҳосил қилади. Текшириш жараёнида битта функциянинг чиқиши текшириш учун биринчи имзо билан таққосланади.

Шунингдек, ЭРИ корхона ва савдо-сотиққа оид ташкилотларда ҳисоботларни электрон кўринишда топширишда, электрон ҳужжатга юридик мақомини беришда катта аҳамиятга эга.



1-расм. ЭРИни шакллантириш жараёни.

ЭРИнинг умумий тан олинган схемаси (модели) учта жараённи ўз ичига олади:

ЭРИ калитларини генерациялаш;

ЭРИни шакллантириш;

ЭРИни текшириш (ҳақиқийлигини тасдиқлаш) [4].

Электрон ҳужжатни ЭРИ билан шакллантириш жараёни 1-расмда келтирилган бўлиб, аввал юборилувчи маълумотнинг хэш-функция қиймати ҳисобланади. Сўнгра электрон рақамли имзо алгоритмига кўра жўнатувчи томон ёпиқ калити орқали маълумот имзоланади.

ЭРИни текширишда жўнатувчи томон очиқ калити орқали ҳисобланган хэш-функция қиймати ва маълумот хэш-функция қийматлари солиштирилади. Қуйидаги 2-расмда. ЭРИни текшириш жараёни келтирилган.

Турли ЭРИ алгоритмларини шакллантириш ва унинг ҳақиқийлигини текшириш амаллари уларнинг математик функциялари орқали фарқланади.

Ушбу мақолада мавжуд ЭРИ алгоритмларининг математик функциялари муаммолар мураккаблигига кўра синфланган (1-жадвал):

- Факторлаш муаммосининг мураккаблигига асосланган ЭРИ алгоритмлари;
- Дискрет логарифм муаммосининг мураккаблигига асосланган ЭРИ алгоритмлари;
- Эллиптик эгри чизиқли дискрет логарифм муаммосининг мураккаблигига асосланган ЭРИ алгоритмлари;
- Параметрлар алгебрасига асосланган ЭРИ алгоритмлари;
- Турли муаммоларга (масалан. квадратик чегирма, n модули бўйича квадрат илдизга) асосланган ЭРИ алгоритмлари. Қуйида ЭРИ алгоритмлари муаммолар мураккаблиги бўйича синфланган.



2-расм. ЭРИни текшириш жараёни

ESIGN схемаси 1985 йил Япония олимлари томонидан таклиф қилинган. Бу электрон рақамли имзонинг асосий хусусияти унинг тезкорлигидир. RSA ёки Эл-Гамал алгоритмларига солиштирилганда, ESIGN алгоритми ёрдамида ҳужжатни имзолаш ва имзони текшириш жараёни бир неча марта тезлик билан амалга оширилади.

Имзо параметрларига қуйидагилар киради: ESIGN алгоритмида махфий калит сифатида катта туб p ва q сонлар жуфтлигидан фойдаланилади ва улар бўйича n = p2*q ифода билан аниқланади. Ошкора калит сифатида (n, k) жуфтлиги олинади. Бу ерда k – хавфсизлик параметридир.

ESIGN алгоритми бўйича ЭРИ шакллантириш ва уни узатиш қуйидаги қадамлар кетма-кетлигини ўз ичига олади (3-расм):

1. M ахборот учун m = H(M) хэш-функция ҳисобланади, 0<m<n-1.

2. x сон генерацияланади, p*q<x.

3. w □ ((m - x k) (mod n))/p*q.

4. S электрон рақамли имзо шакллантирилади:

S □ x+((w/kx k-1 (mod p))p*q.

Қабул қилувчи томон олинган ахборот M ва электрон рақали имзо S дан фойдаланиб қуйидаги қадамлар кетма-кетлигини амалга оширади:

1. хэш-функция m = H(M) ҳисобланади;

2. ошкора калит (n, к) дан фойдаланиб S учун Sk (mod n) ҳисобланади;

3. n битлар сонининг иккиланганини 3 га бўлганига тенг ёки катта бўлган, бутундан анча кичик a сони ва 2a ҳисобланади;

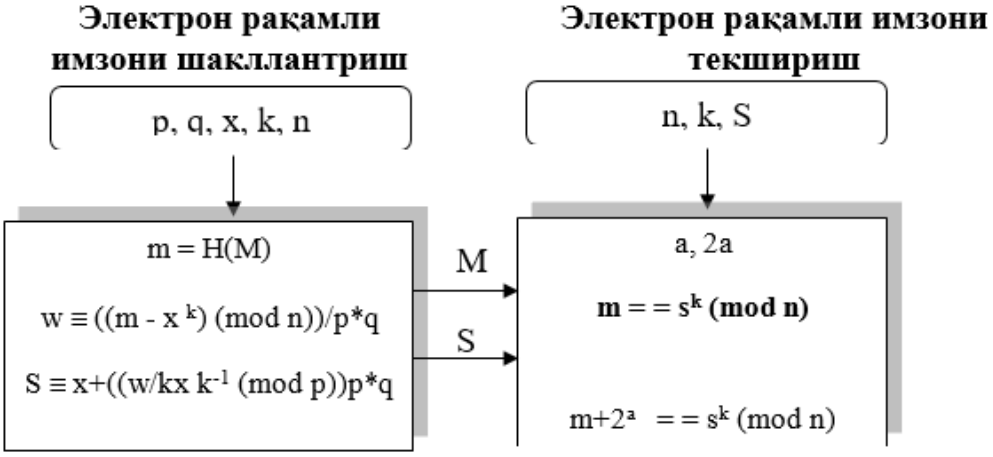
4. m ва m+2a билан Sk (mod n) таққосланади:

m = = sk (mod n);

m+2a = = sk (mod n).

Агар Sk (mod n) m га тенг ёки ундан катта бўлса ва sk (mod n) m+2a дан кичик бўлса, ЭРИ ҳақиқий, акс ҳолда ҳақиқий эмас деб топилади. Бу алгоритмда x ва k билан боғлиқ ҳисоблашларни олдиндан бажариб қўйиш имконияти мавжудлиги ЭРИ шакллантириш жараёнини тезлаштиришга имконият яратади.

Дискрет логарифмлаш муаммосига асосланган Шнорр электрон рақамли имзосини шакллантиришда асосий модул асосида ҳисобланадиган ва ундан анча кичик иккинчи туб модулдан фойдаланилади. Шнорр электрон рақамли имзоси калитларни генерация қилиш учун аввало иккита туб p ва q сон шундай танланадики, q сони p-1 нинг кўпайтувчиси бўлсин. Кейин aq □ 1 (mod p) бўлганда 1 дан катта a танланади. p, q ва a эркин ҳолда эълон қилиниши ҳамда фойдаланувчилар гуруҳи учун қўлланилиши мумкин [5].



3-расм. ESIGN алгоритмини шакллантириш ва текшириш жараёнлари.

Калитлар жуфтлигини генерация қилиш учун q дан кичик тасодифий сон танланади. У махфий калит s бўлиб, унинг ёрдамида ошкора калит □ □ a-s (mod p) ҳисобланади.

Шнорр электрон рақамли имзо схемасининг асосий камчилиги шундаки, душман криптотизим асосига олинган дискрет логарифм муаммосини етарлича аниқ қўя олганда ва унинг бу муаммони ҳал қилишга ресурслари етарлича бўлганда қабул қилувчига келиб тушган электрон рақамли имзо сохта бўлса, имзоловчи шахсда имзони сохталигини исботловчи далиллар ва маълумотларнинг йўқлигидир.

Хавфсизлик поғонаси бир хил бўлганда Шнорр схемаси учун электрон рақамли имзо узунлиги RSA ва Эл-Гамал электрон рақамли имзо схемалариникидан анча қисқароқдир. Миллий стандартдаги O'zDSt 1092:2009 стандартида ҳам Шнорр алгоритмига асосланган p ва q модулларидан фойдаланилади.

Ҳозирги вақтда энг мураккаб ҳисобланган эллиптик эгри чизиқли дискрет логарифм муаммосига асосланган ЭРИ алгоритмларидан кенг фойдаланилмоқда. Эллиптик криптографиянинг афзаллик тарафи шундаки, айни пайтда эллиптик эгри чизиқлар нуқталари гурухида дискрет логарифмлаш масалалари ечимлари учун субэкспоненциал алгоритмлар мавжуд эмас.

Бу муаммога асосланган алгоритмларнинг энг машхурлари ГОСТ 34.10-2001, ECDSA ЭРИ алгоритмларидир. ECDSA алгоритмида калит ўлчамини ошириш билан имзо шакллантириш сезиларли даражада тезроқ амалга оширилади, имзо ҳақиқийлигини тасдиқлаш эса анча секинроқ бўлади.

Қуйидаги 1-жадвалда эллиптик эгри чизиқли дискрет логарифм муаммосига асосланган ECDSA алгоритмининг факторлаш муаммосига

асосланган RSA алгоритмига нисбатан қисқа калитларда тезкорлиги кўрсатилган [5].

1-жадвал

RSA ва ECDSA алгоритмлари асосида ЭРИ яратиш ва уни текшириш

Алгоритмлар	Имзо яратиш	Имзони текшириш
RSA (2048 бит)	120 ms	5 ms
ECDSA (216 бит)	68 ms	70 ms

Мазкур жадвалдан кўриниб турибдики, 216 бит узунликда ECDSA алгоритми билан ЭРИ яратиш учун кетган вақт 2048 бит узунликда RSA алгоритми билан ЭРИ яратиш учун кетган вақтдан тахминан 2 баровар кам сарфланади.

Ҳозирги кундаги мураккаблик даражаси юқори бўлган криптографик муаммолардан бири бу параметрлар алгебрасидир. Ўзбекистонлик олимлар томонидан ишлаб чиқилган O‘zDSt 1092:2009 стандарти шу муаммога асосланади[4]. Унда модул арифметикасининг яшириш йўлли янги бир томонлама функцияси қўлланилади. O‘zDSt 1092:2009да электрон рақамли имзони шакллантириш жараёнига электрон рақамли имзонинг ҳақиқийлигини тасдиқлаш жараёнида қўлланиладиган сеанс калити тартиботини киритиш билан электрон рақамли имзонинг сохталигини аниқлаш назарда тутилади.

ЭРИ ахборот-коммуникация тармоғида электрон ҳужжат алмашинуви жараёнида қуйидаги учта масалани ечиш имконини беради:

- электрон ҳужжат манбасининг ҳақиқийлигини аниқлаш;
- электрон ҳужжат яхлитлигини (ўзгармаганлигини) текшириш;
- электрон ҳужжатга рақамли имзо қўйган субъектни муаллифликдан бош тортмаслигини таъминлаш.

Электрон рақамли имзонинг умумий тан олинган схемаси учта жараённи ўз ичига олади:

-электрон рақамли имзо калитларини генерациялаш;

-электрон рақамли имзони шакллантириш;

- электрон рақамли имзони ҳақиқийлигини тасдиқлаш.

Имзо қўйиш муаллиф томонидан, фақат унга маълум бўлган шахсий калит билан амалга оширилади. Имзонинг ҳақиқийлигини текшириш эса исталган шахс томонидан, имзо муаллифининг очиқ калити билан амалга оширилиши мумкин.[3] Электрон рақамли имзо алгоритмларини шакллантириш ҳам ҳозирги кунда дастурий, аппарат ва аппарат дастурий воситалардан фойдаланилмоқда.

Хулоса.

Хулоса қилиб шуни айтиш мумкинки, эллиптик эгри чизиқли дискрет логарифм муаммосининг мураккаблигига асосланган ЭРИ алгоритмларининг афзаллик томонлари қисқа калитлар қўлланиланилиши ҳисобига уларнинг тезкорлигида бўлса, параметрли алгебрага асосланган ЭРИ алгоритмларининг афзаллиги-янги бир томонлама функцияни қўллаш ҳисобига криптобардошликнинг юқори бўлишидир. Параметрли алгебрага асосланган ЭРИни қалбакилаштирилганда уни аниқлаш механизмини аниқлаш имкони мавжудлиги натижасида қалбакилаштирилган ҳужжатнинг қўлланилишига чек қўйилади.

Электрон рақамли имзо қоғозли ҳужжат алмашинувидаги анъанавий шахсий имзо хусусиятларидан фарқли бўлиб, иккилик саноқ тизими хусусиятлари билан белгиланадиган хотира регистрлари битларига боғлиқ. Хотира битларининг маълум бир кетма-кетлигидан иборат бўлган электрон имзони кўчириб бирор жойга қўйиш ёки ўзгартириш компьютерлар асосидаги алоқа тизимларида мураккаблик туғдирмайди[5].

Бугунги юқори даражада ривожланган бутун дунё цивилизациясида ҳужжатлар, жумладан махфий ҳужжатларнинг ҳам, электрон кўринишда ишлатилиши ва алоқа тизимларида узатилиши кенг қўлланилиб борилаётганлиги электрон ҳужжатлар ва электрон имзоларнинг ҳақиқийлигини аниқлаш масалалари ечимларининг муҳимлигини келтириб чиқармоқда[6,7].

Рақамли имзонинг самарадорлиги унинг асосини ташкил этувчи криптографик алгоритмнинг тезкорлиги, бардошлилиги ва ҳисоблаш машиналарига мослашувчанлигига боғлиқ.

Ушбу мақолада электрон хужжатларни алмашиниш жараёнларидаги ахборот хавфсизлигини таъминлаш муаммосини ҳал этишда муҳим ўрин эгаллаган криптографик восита Шнор схемасига асосланган электрон рақамли имзо алгоритмининг моҳияти тавсия этилади. Эл-Гамалнинг рақамли имзо схемаси билан боғлиқ муаммо шундаки, дискрет логарифмини қийинлаштириши учун жуда катта бўлиши керак, узунлиги камида 1024 бит бўлиши тавсия этилади. Сиз 2048 бит ҳажмида имзо қўйишингиз мумкин, аммо имзо ҳажмини камайтириш учун Шнорр Эл-Гамаль схемасига асосланиб яратиш мақсадга мувофиқ деб хисоблаш мумкин.

Адабиётлар

1. “Электрон ҳужжат айланиши тўғрисида”ги Ўзбекистон Республикаси Қонуни. 11.12.2003 й.
2. “Электрон рақамли имзо тўғрисида”ги Ўзбекистон Республикаси Қонуни. 29.04.2003й.
3. O‘z DSt 1092:2009 «Ахборот технологияси. Ахборотнинг криптографик муҳофазаси. Электрон рақамли имзони шакллантириш ва текшириш жараёнлари».

4. Брюс Шнайер. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке СИ – Москва: ТРИУМФ, 2002.
5. Хасанов Х.П. Такомиллашган диаматрицалар алгебралари ва параметрли алгебра асосида криптотизимлар яратиш усуллари ва алгоритмлари. – Тошкент, 2008. 208 б.
6. Xudoynazarov, U., & Meliquziyev, A. (2023). OCHIQ KALITLI RSA SHIFRLASH ALGORITMINI PARAMETRLI ALGEBRA ASOSIDA TAKOMILLASHTIRISH. Research and implementation.
7. Акбаров Д., Хасанов П., Хасанов Х., Ахмедова О. Криптографиянинг математик асослари. Ўқув қўлланма.– Тошкент, 2010 – 210 б.
8. Акбаров Д.Е. Ахборот хавфсизлигини таъминлашнинг криптографик усуллари ва уларнинг қўлланишлари. Тошкент. ”Ўзбекистон маркаси “, 2009. – 432 б.

Scientific-methodical journal “Research and implementation”

Address:
150100, Fergana region, Fergana, Solim street, 23/4, apt. 26

E-mail:
chief_editor@rai-journal.uz

Our website:
https://rai-journal.uz/

The Scientific-methodical journal “Research and implementation” was founded by LLC Fer-Teach and supports by the Fergana branch of the Tashkent University of Information Technologies named after Muhammad al-Khorezmi.
This journal was registered by the Agency of Information and Mass Communications under the Administration of the President of the Republic of Uzbekistan on May 3, 2023 (No 078777).
ISSN 3030-3362.

"Research and implementation" is a specialized journal in the field of technology and covers all major areas of research and development in various fields of technical sciences: physics, mathematics, information technology. The journal also publishes scientific articles on linguistics, teaching methods and the history of the development of technical sciences.

Languages: Uzbek, Russian, English, Karakalpak

ВНИМАНИЕ!

При использовании материалов журнала необходимо указывать источник
Авторы статей несут ответственность за содержание статей и за сам факт их публикации.
Редакция не всегда разделяет мнения авторов и не несет ответственности за недостоверность публикуемых данных.
Редакция журнала не несет никакой ответственности перед авторами и/или третьими лицами и организациями за возможный ущерб, вызванный публикацией статьи.

ATTENTION!

When using journal materials, you must indicate the source.
The authors of the articles are responsible for the content of the articles and for the very fact of their publication.
The editors do not always share the opinions of the authors and are not responsible for the unreliability of the published data.
The editorial board of the journal does not bear any responsibility to the authors and / or third parties and organizations for possible damage caused by the publication of the article

DIQQAT!

Jurnal materiallaridan foydalanganda manbani ko‘rsatish kerak.
Maqola mualliflari maqolalar mazmuni va ularning nashr etilishi fakti uchun javobgardirlar.
Har doim ham mualliflarning fikrlari tahririyat nuqtai nazarini ifodalamaydi va nashr etilgan ma’lumotlarning haqiqiyligi uchun javobgar emas.
Jurnal tahririyati mualliflar va/yoki uchinchi shaxslar va tashkilotlarga maqolaning e’lon qilinishi natijasida yetkazilishi mumkin bo‘lgan zarar uchun javobgar emas.