АХБОРОТ ХАВФСИЗЛИГИ
ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Жамоавий электрон рақамли имзо бардошлигини ошириш усулини асослаш

Хасанов Х.П., Ахмедова О.П., Назарова М.Х., Нуриддинов О.Ж.

Мақолада жамоавий электрон рақамли имзо бардошлигини ошириш усуллари таҳлил этилди ва унинг бардошлигини оширишнинг параметрли эллиптик эгри чизиқларга асосланган янги усули асосланди.

В статье проанализированы методы повышения стойкости коллективной электронной цифровой подписи и обоснован новый метод повышения её стойкости на базе эллиптических кривых с параметром.

Methods of increasing the stability of collective digital signature were analyzed and method of increasing the stability on the base of elliptic curve with parameters was proofed in the paper.

Электрон рақамли имзо шакллантириш имкониятини юзага келтирган ошкора криптографик алгоритмларнинг бардошлиги бир томонлама махфий йўлли функцияни тескарилашнинг мураккаблигига боғлиқ бўлиб, ҳозирги кунда фойдаланилаётган криптографик алгоритмлар катта тоқ сонлар кўпайтмасини факторлаш, чекли майдонларда дискрет логарифмлаш ва эллиптик эгри чизиқларда дискрет логарифмлаш муаммоларининг мураккаблигига асосланган [1].

Ҳозирги кунда Ўзбекистон Республикасида жамоавий электрон рақамли имзо бўйича давлат стандарти ишлаб чиқилмаганлиги туфайли бардошлиги оширилган жамоавий электрон рақамли имзо алгоритмларини ишлаб чиқиш долзарб масаладир.

Криптографик бардошлик - криптографик алгоритмнинг мумкин бўлган ҳужумларга қарши тура олиш имкониятидир. Ҳужумни амалга оширувчи субъект (масалан, хакер) криптотаҳлил усулларидан фойдаланади. Алгоритм муваффақиятли бўлиши мумкин бўлган ҳужумларга қарши туриб бера олиши учун ҳужумкорнинг ҳисоблаш ресурслари етарли бўлмаса, очиқ матн ва шифрланган маълумотлар ҳажми камлик қилса ёки криптотаҳлилни амалга ошириш учун зарур бўлган вақт сарфи тугагунча ахборот ўз долзарблигини йўқотса, бундай алгоритм **криптобардошли ҳисобланади.** Бардошликни тасдиқламоқ мумкин эмас, уни бузиш орқалигина рад этиш мумкин холос.

Мавжуд жамоавий электрон рақамли имзо (ЖЭРИ) алгоритмларининг бардошлигини ошириш асосида қуйидаги муаммоларга тегишли шахсий калитни топиш мураккаблиги ётади:

- дискрет логарифм муаммосининг мураккаблиги;
- факторлаш муаммосининг мураккаблиги;
- эллиптик эгри чизиқда дискрет логарифм муаммосининг мураккаблиги;
- даража параметри муаммосининг мураккаблиги [2-3].

Бинобарин, шахсий калит асосан **модуль узунлиги** билан аниқланиши туфайли мавжуд ЖЭРИ

алгоритмларининг бардошлигини ошириш асосида **модуль бинар узунлигини ошириш** ётади.

ЖЭРИ алгоритмларининг бардошлигини ошириш учун ЭЭЧ нуқталари циклик қисм группасининг **(базавий нуқталарининг) тартибини ошириш лозим.** Олиб борилган тадқиқотлар шуни кўрсатадики, РФнинг ГОСТ Р 34.10-94 ва ГОСТ Р 34.10-2001 асос этиб олинган O'z DSt 1092:2009, Украинаннг ДСТУ 4145-2002 ва Белорусиянинг 1176.2-99 давлат стандартлари асосида ЖЭРИ шакллантириш имконияти мавжуддир. Бироқ, АҚШнинг давлат стандартлари DSA ва ECDSA асосида эса ЖЭРИ шакллантириш мумкин эмаслиги [4]да кўрсатилган.

ЭЭЧга асосланган кўпчилик криптографик алгоритмларнинг бардошлиги ЭЭЧда дискрет логарифмлаш масаласини ечиш мураккаблиги (ECDLP) билан белгиланади.

Бугунги кунда ECDLP масаласини, яъни ЭЭЧда дискрет логарифмлаш масаласини ечишнинг маълум усулларидан энг машҳури Поллардннг ρ- ва λ- усулларидир [5-6]. ЭЭЧ нуқталарини қўшиш билан аниқланувчи Поллардннг ρ-усули мураккаблигини қуйидаги ифода орқали баҳолаш мумкин:

$$Ip=\sqrt{\pi q/2},$$

бу ерда q – ЭЭЧ базавий нуқталари тартиби.

[7] да Поллард ρ-усули тезлигини $\sqrt{2}$ мартага ошириш мумкинлиги кўрсатилган. У ҳолда усул мураккаблиги $I_p=\sqrt{\pi q/4}$ билан баҳоланади.

Поллард ρ-усулининг афзаллик томонларидан бири криптотаҳлил жараёнини мустақил бир нечта параллел жараёнларга ажратишдир. Бу ҳолда ҳар бир жараённи амалга ошириш мураккаблиги $I_p=\sqrt{\pi q/2r^2}$ ва $I_p=\sqrt{\pi q/4\ r^2}$ билан баҳоланади.

Поллард λ-усули мураккаблиги $I_\lambda=2\sqrt{q}$ билан ва параллеллашда $I_\lambda=2\bar{}^{1}\sqrt{q}$ билан баҳоланади.

Поллардннг иккала усулининг қиёсий таҳлили Поллард λ-усули Поллард ρ-усулига нисбатан мураккаброқлигини кўрсатади.

2004 йилда Поллард параллелланган алгоритми асосида "бузилган" ЭЭЧ калитининг энг катта узунлиги *109* битни ташкил этди [8].

ЭЭЧда дискрет логарифмлаш масаласини Поллард ρ-усулидан фойдаланиб, ечиш мураккаблигига тааллуқли келтирилган маълумотлар шуни кўрсатадики, ЭРИ алгоритмларида базавий нуқтаси $q\geq 2^{256}$ тартибли ЭЭЧ қўлланилиши ЭЭЧ базасидаги ЭРИ зарур бардошлигининг келажакдаги истиқболини таъминлайди. Бу ГОСТ Р 34.10-2001нинг 10 йил давомида муваффақиятли эксплуатацияси ва калитни очиш мураккаблиги $3*10^{38}$ арифметик амалдан иборатлиги билан ҳам асосланади.

Калит узунлиги d бит (l_q) криптотаҳлилчи қўпол ҳужумни амалга ошириши мумкин. Шу туфайли энг кўп кутилган калит узунлиги l_q. Унда агар G маълум бўлса l_1 марта d ни танлаш оқибатида шахсий калитни, сўнгра Q ни топиш мумкин. Криптотаҳлил мураккаблиги $I_1 \sim (l_q - 1)$ бўлади. Қуйидаги жадвалда бу ҳол учун усуллар мураккабликлари [7] да келтирилган.

I бўйича таққослама таҳлил шуни кўрсатадики, қўшимча базавий нуқта G ни билмаслик ҳужумни амалга ошириш имкониятини мураккаблаштиради ва q га нисбатан квадратик боғланишга эга бўлади. Оқибатда криптотаҳлил масаласини ҳал этиш мураккаблиги симметрик алгоритмга қўпол ҳужумга нисбатан янада мураккаброқ бўлади. Бу ҳолларда фиксирланган q да ЖЭРИ бардошлиги анча юқори бўлиши таъминланади.

Криптотаҳлил мураккаблиги усуллари

Жадвал

Базавий нуқталари тартиби q	ρ- Поллард усули мураккаблиги I_ρ	Оптималь Поллард ρ-усули мураккаблиги $I_{\rho\text{-оп}}$	Поллард λ-усули мураккаблиги I_λ	Q конфиденциаль калит мураккаблиги I_1
2^{128}	$2^{64,72}$	$2^{64,22}$	$2^{65,39}$	2^{127}
2^{160}	$2^{80,17}$	$2^{79,68}$	$2^{80,85}$	2^{159}
2^{256}	$2^{128,31}$	$2^{127,83}$	$2^{82,49}$	2^{255}
2^{512}	$2^{256,30}$	$2^{255,82}$	$2^{256,99}$	2^{511}
2^{1024}	$2^{512,26}$	$2^{511,78}$	$2^{512,94}$	2^{1023}

Шундай қилиб, юқорида келтирилган ЖЭРИ бардошлигини ошириш усуллари орасида энг унумлиси ЭЭЧ **базавий нуқталари тартиби *q* ни ошириш усулидир.**

Жамоавий электрон рақамли имзо бардошлигини оширишнинг яна бир усули параметрли функциялар билан боғлиқ янги **муаммолар мураккаблиги билан асосланади**. [2-3] да келтирилган параметрли функция хоссалари орасида асосан даража параметри R нинг махфийлиги криптографик тизим криптобардошлигини оширишга хизмат қилади. Шунингдек, параметрли ЭЭЧ группасида даража параметри R билан бир қаторда a, B коэффициентларнинг ва ЭЭЧ нуқтасининг иккинчи координатаси махфийлиги криптотизим криптобардошлигини оширишга хизмат қилади. Бундай имконият бардошлиги факторлаш, дискрет логарифмлаш ва ЭЭЧ группасида дискрет логарифмлаш муаммоларининг мураккаблигига асосланган алгоритмлар учун асосан махсус аппаратли криптомодуллардан фойдаланилганда тўла юзага чиқади. Чунки, махсус аппаратли криптомодулларда ваколатли субъект томонидан ўрнатиладиган махфий даража параметри R билан бир қаторда махфий калитли хэш-функциядан фойдаланилади. Агар ЖЭРИни ишлаб чиқишда дастурий криптомодуллардан фойдаланилса ҳам, унда ваколатли субъект хизматларидан фойдаланган ҳолда мазкур махфий катталикларни дастурий криптомодулга ҳам ўрнатиш мумкин. Шу зайлда амалга оширилган криптомодулларни махсус аппаратли криптомодулга мос дастурий криптомодуль деб атаймиз.

ЖЭРИда модуль сифатида туб ёки таркибли сондан фойдаланилган. ЖЭРИ криптобардошлигининг ортиши бир томонлама параметрли функция ифодасида қатнашадиган даражага ошириш параметри (қисқача, даража параметри) R ноқонуний фойдаланувчилардан сир сақланишига асосланади. Криптографияга оид нашрларда бунга ўхшаш муаммо келтирилмаган.

Даража параметри муаммоси учта мураккаблик поғонаси билан фарқланиб, унинг таърифлари [2-3]да келтирилган. Мазкур муаммоларнинг юзага чиқиши бир томонлама параметрли функциянинг қуйидаги хоссаси билан боғлиқ:

$$a^{\backslash e} \equiv a^* \sum_{i=0}^{i=e-1} F^i \ (mod\ n),$$

бу ерда $F=1+R^*a$, $n \in \{p, p_1^*p_2\}$.

Ҳозирги кунга қадар бу муаммони эффектив ечиш усули маълум эмас.

Даража параметри муаммосига берилган 3 та таърифларда номаълумлар сонини эътиборга олсак, муаммони ҳал этиш мураккаблиги ўзаро мос тарзда учинчи, иккинчи ва биринчи поғонага оид деб ҳисоблаш ўринлидир.

Параметр *R* берилганда қонуний фойдаланувчилар учун даража параметри муаммоси қуйидагича таърифланади:

Таъриф. Агар параметрли алгебра $(F_p; ®)$ да ташувчи F_p нинг элементлари *y* ва *R* берилган бўлса, унда даража кўрсаткичи *e* ва элемент *a* топилсин**,** бу ерда F_p **-** *n* та бутун сонлардан тузилган чекли тўплам, $y \equiv a^{\backslash e} (mod\ p)$, $^{\backslash e}$ - *a* ни параметр *R* билан *e*-даражаси рамзи, элемент *a* $a^{\backslash \omega} \ (mod\ n) \equiv 0$ шартини фақат ω=*q* бўлгандагина қаноатлантиради**,** *q* - *φ(n)* нинг бутун сонли бўлувчиси, *φ(n)* - *Эйлер пи-функцияси*.

Ушбу таърифга тааллуқли даража параметри муаммосини n=p бўлганда, унинг дискрет логарифм муаммосига осонгина келтиришини эътиборга олиб, дискрет диалогарифм муаммоси деб аташ мумкин ва уни ечиш мураккаблиги, параметр берилгани сабабли, нолинчи даражага тегишли десак хато бўлмайди.

Даража параметри муаммосининг юзага келиши тамойилли янгича ёндашувга асосланган ЖЭРИлар яратишга имконият туғдиради.

Криптобардошлиги даража параметри муаммосини ҳал этишнинг биринчи мураккаблик поғонасига асосланган ЖЭРИ тизимларида модуль $n \geq 2^{256}$, даража кўрсаткичи туб сон бўлиб, $e \geq 2^{160}$ шартларига жавоб бериши лозимлиги тавсия этилади. Шу билан бир қаторда, махфий параметр $2^{256} > R$, $R^{-1} \geq 2^{160}$ шартини қондириши зарур.

Криптобардошлиги даража параметри муаммосини ҳал этишнинг биринчи мураккаблик поғонасига асосланган ЖЭРИ тизимларида модуль $p \geq 2^{160}$, даража кўрсаткичи туб сон бўлиб, $e \geq 2^{150}$ шартларига жавоб бериши лозимлиги тавсия этилади. Шу билан бир қаторда, махфий параметр $2^{160} > R$, $R^{-1} \geq 2^{150}$ шартини қондириши зарур.

Даража параметри муаммосининг мураккаблигини ошириш бардошлиги дискрет логарифмлаш муаммосининг мураккаблиги билан белгиланадиган ЖЭРИ яратилишига олиб келади. Маълумки, мураккаблик турлари қанчалик кам бўлса, криптотизим бардошлиги шунчалик юқори бўлади, чунки муаммонинг кўпайгани билан ҳар доим ҳам бардошлик ошавермайди. Шу сабабдан ЖЭРИни лойиҳалашда оптималь криптотизим ягона муаммонинг мураккаблигига асосланган криптотизим бўлишига эътибор бериш лозим.

ЖЭРИ хавфсизлиги қуйидаги тахминларга асосланади:

1) дискрет логарифмлаш муаммоси мураккаблигига;

2) тасодифий сонлар генератори энтропияси калит генератори энтропиясидан кам бўлмаслигига;

3) калитдан фойдаланиш давомида икки тасодифий сон такрорланиши эҳтимоллигини ҳисобга олмаслик даражасида камлигига;

4) хэш-функциянинг қайтмаслигига;

5) хэш-функция коллизиясини ҳисоблаб топиш мураккаблигига.

Бинобарин, ЖЭРИ бардошлиги параметр *R* ни топиш, дискрет логарифмлаш, фойдаланилаётган тасодифий сон, хэш-функцияни тескарилаш, хэш-функция коллизиясини топиш мураккабликларининг энг кичик қийматидан кам бўлмайди.

Ишлаб чиқиладиган махсус аппаратли криптомодулларда ЖЭРИ алгоритмларида туб модуль узунлиги $p > 2^{255}$ бит бўлганда ёпиқ хэшлаш калити *м*, параметр *R* ва асос *а* ни бардошликлари мос тарзда қуйидаги ифодалар бўйича аниқланади:

$q_m=2^{255}$, $q_R=2^{254}$, $q_a=2^{160}$ ва бардошлик баҳоси қуйидаги кўринишга эга:

$$l=q_m\, q_R\, q_a=2^{669}.$$

Бардошликнинг бундай юқори бўлиши ҳозирги кунгача даража параметри муаммосининг ҳал этилмаганлиги билан бегиланади, уни ҳал этиш учун майдон элементлари устида 2^{669} та амал бажариш керак бўлади, ҳозирги кунгача бундай ҳисоблаш ресурсларига эга бўлган қурилмалар яратилмаган.

Шу туфайли барча маълум бўлган ҳужум турлари - универсал сохталаштириш, тўла очиб ташлаш, маълум ошкора калит асосида ҳужум, имзоланган маълумотга асосланган ҳужум, имзони ошкора калитни билмаган ҳолда сохталаштириш, селектив сохталаштириш, экзенциаль сохталаштириш каби ҳужумлар самара бермайди.

Факторлаш муаммоси асос қилиб олинган RSA алгоритмларидан фойдаланишга асосланган ишлаб чиқиладиган махсус аппаратли ёки унга мос дастурий криптомодуллардаги ЖЭРИ алгоритмларида мураккаб модуль узунлиги $n\geq 2^{2^*255}$ бит бўлганда ёпиқ хэшлаш калити *м* ва параметр *R* ни бардошликлари мос тарзда қуйидаги ифодалар бўйича аниқланади:

$q_m=2^{510}$, $q_R=2^{508}$ ва бардошлик баҳоси қуйидаги кўринишга эга:

$$l=q_m\, q_R\, =2^{1018}.$$

Бардошликнинг бундай юқори бўлиши ҳозирги кунгача даража параметри муаммосиниг ҳал этилмаганлиги билан бегиланиб, уни ҳал этиш учун майдон элементлари устида 2^{1018} та амал бажариш керак бўлади, ҳозирги кунгача бундай ҳисоблаш ресурсларига эга бўлган қурилмалар яратилмаган.

Юқорида келтирилганлардан шу нарса маълум бўлдики**,** махсус аппаратли ва унга мос криптомодулларда қурилган ЖЭРИ алгоритмлари учун туб модуль ва мураккаб модуль танлашда уларнинг узунликларини ҳисоблаш қурилмаларининг тезликлари ортиб боришига мос тарзда йилдан-йилга ошириб бориш шарт эмас. Чунки зарурий бардошликка даража параметри *R* ва махфий хэшлаш калити *м* ҳисобига эришилади.

Маълумки, анъанавий криптотизимларда фойдаланиладиган ЭЭЧлар тенгламаларининг коэффициентлари очиқ (ошкора) бўлади ва уларни ёпиқ (ошкормас) қилиш криптобардошликни оширишга сезиларли ҳисса қўшмайди. Чунки, очиқ калит сифатида эълон этилган ЭЭЧ нуқталари сони ёпиқ коэффициентлар сонига етгач, уларни ҳисоблаб топиш қийин эмас.

Параметрли ЭЭЧ нуқталари группаси $(PE(F_p);\ +^{\backslash})$ дан фойдаланилганда қўшимча махфий параметр *R* туфайли ЭЭЧлар тенгламаларининг коэффициентларини ёпиқ қилиш криптотизим криптобардошлигини оширишга олиб келади [9].

Бундай ЭЭЧни параметрли ошкора бўлмаган ЭЭЧ деб атаймиз. Мазкур муаммонинг ечими ҳозирча маълум эмас, уни анъанавий ЭЭЧларга оид мураккаблик поғонасидан юқори деб ҳисоблаш ўринли.

Шунинг учун ҳам параметрли ЭЭЧлардан фойдаланишга асосланган ЖЭРИ схемаларида на

туб модуль *p* ни, на ошкора бўлмаган ЭЭЧ базавий нуқталари группаси тартиби *q* ни ошириш лозим эмас. Эллиптик эгри чизиқ тенгламаси асосан унга параметр *R* киритилиши туфайли ошкора бўлмаган эллиптик эгри чизиққа айланади.

ЖЭРИ хавфсизлиги ЭЭЧларда дискрет логарифмлаш муаммоси мураккаблигига, тасодифий сонлар генератори энтропияси, икки тасодифий сон такрорланиши, хэш-функциянинг қайтмаслиги ва коллизиясини ҳисоблаб топиш мураккаблигига оид мулоҳазаларга асосланади.

Бинобарин, ЖЭРИ бардошлиги ЭЭЧларда дискрет логарифмлаш, фойдаланилаётган тасодифий сон, хэш-функцияни тескарилаш, хэш-функция коллизиясини топиш мураккабликларининг энг кичик қийматидан кам бўлмайди.

Ишлаб чиқиладиган махсус аппаратли криптомодулларда ошкора бўлмаган ЭЭЧдан фойдаланишга асосланган ЖЭРИ алгоритмларида ёпиқ параметрлар *R, a, B,* мос тарзда, қуйидаги ифодалар бўйича аниқланади:

$$2^{p-2} < q_m < 2^p,\ 2^{160} < q_R < 2^{255},$$

$$q_a = q_B = 2^{160}.$$

Бу ерда $p > 2^{255}$ ва бардошлик баҳоси қуйидаги кўринишга эга:

$$l = l\ q_m q_R q_a\ q_B.$$

Бу ерда $l \in [1; 4]$.

$l=1$ учун, $q_m = 2^{255}$, $q_R = 2^{254}$ ва бардошлик баҳоси қуйидаги кўринишга эга:

$$l = q_m q_R q_a\ q_B = 2^{829}.$$

Бардошликнинг бундай юқори бўлиши ҳозирги кунгача ошкора бўлмаган ЭЭЧ параметри муаммосиниг ҳал этилмаганлиги билан бегиланади. Шу туфайли барча маълум бўлган ҳужум турлари - универсал сохталаштириш, тўла очиб ташлаш, маълум ошкора калит асосида ҳужум, имзоланган маълумотга асосланган ҳужум, имзони ошкора калитни билмаган ҳолда сохталаштириш, селектив сохталаштириш, экзенциаль сохталаштириш каби ҳужумлар самара бермайди.

Ҳар қандай ҳужумни амалга ошириш учун ошкора бўлмаган ЭЭЧ параметри муаммосини ҳал этиш зарур, бу эса ЭЭЧ нуқталари устида 2^{829} та қўшиш амалларини бажаришни талаб этади, ҳозирги кунгача бундай ҳисоблаш ресурсларига эга бўлган қурилмалар яратилмаган.

Асосий хулосалар

Мазкур мақолада жамоавий электрон рақамли имзо бардошлигини ошириш усулларининг тадқиқи ва қиёсий таҳлили келтирилди. Тадқиқ ва таҳлил натижалари шуни кўрсатадики, мавжуд жамоавий электрон рақамли имзо бардошлиги асосан дискрет логарифмлаш усулига тегишли модуль узунлигини ошириш, факторлаш усулига тегишли модуль узунлигини ошириш ва эллиптик эгри чизиқ базавий нуқталари тартибини оширишга асосланган.

Жамоавий электрон рақамли имзо бардошлигини ошириш усули параметрли функциялар билан боғлиқ янги муаммолар мураккаблиги билан асосланади.

Бардошлиги факторлаш, дискрет логарифмлаш ва ЭЭЧ группасида дискрет логарифмлаш муаммоларининг мураккаблигига асосланган ЖЭРИ алгоритмлари асосан махсус аппаратли криптомодулларда амалга оширилса, бардошлик энг юқори чегарада бўлади. Чунки, махсус аппаратли криптомодулларда ваколатли субъект томонидан ўрнатиладиган махфий даража параметри *R* билан бир қаторда махфий калитли хэш-функция дастури ўрнатилган бўлади.

Агар ЖЭРИни ишлаб чиқишда дастурий криптомодуллардан фойдаланилса ҳам унда ваколатли субъект хизматларидан фойдаланган ҳолда мазкур махфий катталикларни дастурий криптомодулга ўрнатиш ва юқори бардошликка эришиш мумкин.

Махсус аппаратли ва унга мос криптомодулларда қурилган ЖЭРИ алгоритмлари учун туб модуль ва мураккаб модуль танлашда уларнинг узунликларини ҳисоблаш қурилмаларининг тезликлари ортиб боришига мос тарзда йилдан-йилга ошириб бориш шарт эмас. Чунки таклиф этилаётган усуллар ёрдамида зарурий бардошликка даража параметри *R* ва махфий хэшлаш калити *м* ҳисобига эришилади.

Мазкур мақолада таклиф этилаётган муаммоларнинг юзага келиши бардошлиги юқори бўлган ЖЭРИ тизимларини янгича ёндашувлар асосида яратиш имкониятини туғдиради.

Адабиётлар

1. Венбо Мао. Современная криптография. Теория и практика. – Москва, «Вильямс», 2005. – 768 с.

2. Хасанов П.Ф., Хасанов Х.П. Стойкость Государственного стандарта ЭЦП Республики Узбекистан // «Сервисы удостоверяющих центров. Новые области применения PKI»: Тез. докл. международной научно – практической конференции PKI Forum- 2006, Санкт-Петербург, 7-10 ноября 2006.

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

4. Протоколы слепой коллективной подписи на основе стандартов цифровой подписи / Фахрутдинов Р. Ш., Костин А. А., Молдовян Н. А. / Вопросы защиты информации. — 2010. — № 1. — С. 14–23.

5. Menezes, Y. Wu, R. Zuccherato. An Elementary Introduction to Hyperelliptic Curves – Springer-Verlag, Berlin (Germany), 1998. – 31 p.

6. Кобец А.М. Подмена подписанного документа в новом американском стандарте ЭЦП ECDSA// http: www.bugtrag/ru.

7. Горбенко И.Д., Збитнев С.И., Поляков А.А. Криптоанализ криптографических преобразований в группах точек эллиптических кривых методом Поларда // Радиотехника: Всеукр. межвед. науч.-техн. сб. 2001. Вып. 119. С.43-50.

8. Стандарт ЦП Украины на эллиптической кривой. Опубликовано: domarev , On: Nov-19-2004 http://www.security.ukrnet.net

9. Хасанов Х.П. Криптографические системы на базе эллиптических кривых с параметром. Ахборотқоммуникациялар: Тармоқлар – Технологиялар – Ечимлар. – Т.: №4, 2008. — С. 42–46.