Т АХБОРОТ ТЕХНОЛОГИЯЛАРИ УНИВЕРСИТЕТИ
ҲУЗУРИДАГИ ИЛМИЙ ДАРАЖАЛАР БЕРУВЧИ
7.06.2017.T.07.01 РАҚАМЛИ ИЛМИЙ КЕНГАШ

ТОШКЕНТ АХБОРОТ ТЕХНОЛОГИЯЛАРИ УНИВЕРСИТЕТИ

**ХУДОЙҚУЛОВ ЗАРИФ ТЎРАҚУЛОВИЧ**

# САМАРАЛИ КРИПТОГРАФИК КАЛИТЛАРНИ ГЕНЕРАЦИЯЛАШ УСУЛЛАРИ ВА АЛГОРИТМЛАРИ

05.01.05 – Ахборотларни ҳимоялаш усуллари ва тизимлари. Ахборот хавфсизлиги

**ТЕХНИКА ФАНЛАРИ БЎЙИЧА ФАЛСАФА ДОКТОРИ (PhD) ДИССЕРТАЦИЯСИ АВТОРЕФЕРАТИ**

**Тошкент-2018**

УДК: 004.056.55

**Техника фанлари бўйича фалсафа доктори (PhD) диссертацияси авторефератн мундарижаси**

**Оглавление автореф... ертации**
**доктора ... ским наукам**



**...f philosophy (PhD)**



...ш усуллари ва ..... 3

...ографических ..... 21

ation ..... 39

..... 43

**ТОШКЕНТ АХБОРОТ ТЕХНОЛОГИЯЛАРИ УНИВЕРСИТЕТИ ҲУЗУРИДАГИ ИЛМИЙ ДАРАЖАЛАР БЕРУВЧИ DSc.27.06.2017.T.07.01 РАҚАМЛИ ИЛМИЙ КЕНГАШ**

**ТОШКЕНТ АХБОРОТ ТЕХНОЛОГИЯЛАРИ УНИВЕРСИТЕТИ**

**ХУДОЙҚУЛОВ ЗАРИФ ТЎРАҚУЛОВИЧ**

# САМАРАЛИ КРИПТОГРАФИК КАЛИТЛАРНИ ГЕНЕРАЦИЯЛАШ УСУЛЛАРИ ВА АЛГОРИТМЛАРИ

05.01.05 – Ахборотларни ҳимоялаш усуллари ва тизимлари. Ахборот хавфсизлиги

**ТЕХНИКА ФАНЛАРИ БЎЙИЧА ФАЛСАФА ДОКТОРИ (PhD) ДИССЕРТАЦИЯСИ АВТОРЕФЕРАТИ**

**Тошкент-2018**

**Техника фанлари бўйича фалсафа доктори (PhD) диссертацияси мавзуси Ўзбекистон Республикаси Вазирлар Маҳкамаси хузуридаги Олий аттестация комиссиясида B2017.3.PhD/T353 рақам билан рўйхатга олинган.**

Диссертация Тошкент ахборот технологиялари университетида бажарилган.

Диссертация автореферати уч тилда (ўзбек, рус, инглиз (резюме)) Илмий кенгаш веб-саҳифасида (www.tuit.uz) ва «Ziyonet» Ахборот таълим порталида (www.ziyonet.uz) жойлаштирилган.

| | |
|---|---|
| **Илмий раҳбар:** | **Ганиев Салим Каримович**<br>техника фанлари доктори, профессор |
| **Расмий оппонентлар:** | **Алоев Рахматилло Жураевич**<br>физика-математика фанлари доктори, профессор |
| | **Туйчиев Гулом Нумонович**<br>физика-математика фанлари доктори |
| **Етакчи ташкилот:** | **«UNICON.UZ» – фан-техника ва маркетинг тадқиқотлари маркази** |

Диссертация ҳимояси Тошкент ахборот технологиялари университети ҳузуридаги DSc.27.06.2017.T.07.01 Илмий кенгашнинг 2018 йил «21» декабр соат 14 00 даги мажлисида бўлиб ўтади. (Манзил: 100202, Тошкент шаҳри, Амир Темур кўчаси, 108-уй. Тел.: (99871) 238-64-43, факс: (99871) 238-65-52, e-mail: tuit@tuit.uz).

Диссертация билан Тошкент ахборот технологиялари университети Ахборот-ресурс марказида танишиш мумкин ( 2 ГБ/ рақам билан рўйхатга олинган.). (Манзил: 100202, Тошкент шаҳри, Амир Темур кўчаси, 108-уй. Тел.: (99871) 238-65-44).

Диссертация автореферати 2018 йил «17» декабр да тарқатилди.
(2018 йил «16» ноябр даги 14 рақамли реестр баённомаси.)

**Р.Х. Хамдамов**
Илмий даражалар берувчи илмий кенгаш раиси, т.ф.д., профессор

**Ф.М. Нуралиев**
Илмий даражалар берувчи илмий кенгаш илмий котиби, т.ф.д., доцент

**Р.Ж. Алоев**
Илмий даражалар берувчи илмий кенгаш қошидаги илмий семинар раиси, ф-м.ф.д., профессор

## КИРИШ (фалсафа доктори (PhD) диссертациясининг аннотацияси)

**Диссертация мавзусининг долзарблиги ва зарурати.** Жаҳонда ахборотнинг криптографик ҳимоя тизимларини ишлаб чиқишга ва уларни самарадорлигини оширишга алоҳида эътибор қаратилмоқда. Ахборот-коммуникация тизимлари ривожининг ҳозирги замон босқичида ахборотнинг конфиденциаллиги ва бутунлигини таъминлаш муҳим ҳисобланади. «Accenture компанияси маълумотига кўра, 2018 йил учун кибер ҳужумларнинг энг қиммат компоненти маълумотни сирқиб чиқиши бўлиб, умумий келтириладиган зарарнинг 43%ни ташкил этади»[1]. Бу йўналишда ривожланган мамлакатларда, жумладан, АҚШ, Россия Федерацияси, Япония, Хитой ва бошқа давлатларда ҳисоблаш тармоқларида узатилаётган ахборот яхлитлиги ва конфиденциаллигини таъминлаш имкониятини берувчи криптографик воситалар ишлаб чиқиш муҳим аҳамият касб этмоқда.

Жаҳонда бардошли калитларни генерациялаш имконини берувчи, қурилмага ёки операцион тизим ресурсларига асосланган калит генераторларини яратишга йўналтирилган илмий-тадқиқот ишлари олиб борилмоқда. Бу борада, жумладан ҳосил қилинаётган калитларнинг тасодифийлик даражасини аниқ ҳисоблаш, ҳодиса манбаларидан келаётган қийматларни хавфсиз тўплаш ва тасодифий қиймат асосида старлича узунликдаги псевдотасодифий кетма-кетликларни тезкорлик билан шакллантириш усулларини ишлаб чиқиш муҳим вазифалардан бири ҳисобланмоқда. Шу билан бирга криптографик калитларни хавфсиз бошқариш, эсда сақлашни ва олиб юришни талаб этмайдиган калитлардан фойдаланиш имконини берувчи жараёнларни такомиллаштиришни илмий асослаш зарур бўлмоқда.

Республикамизда давлат ва хўжалик бошқарув органларида электрон ҳужжат алмашинув тизимларини татбиқ этишда ва электрон ҳукумат тизимини шакллантиришда маълумотлар хавфсизлигини таъминлашга қаратилган кенг қамровли чора-тадбирлар амалга оширилмоқда. 2017-2021 йилларда Ўзбекистон Республикасини янада ривожлантириш бўйича Ҳаракатлар стратегиясида, жумладан «...ахборот хавфсизлигини таъминлаш ва ахборотни ҳимоялаш тизимини такомиллаштириш, ахборот соҳасидаги таҳдидларга қарши ўз вақтида ва муносиб қаршилик кўрсатиш»[2] вазифалари белгиланган. Мазкур вазифаларни бажаришда ахборотнинг криптографик ҳимоя воситалари, хусусан турли ҳодиса манбаларидан келаётган тасодифий қийматлар асосида самарали криптографик калитларни генерациялаш усуллари ва воситаларини ишлаб чиқиш муҳим вазифалардан бири ҳисобланади.

Ўзбекистон Республикаси Президентининг 2017 йил 7 февралдаги ПФ-4947-сон «Ўзбекистон Республикасини янада ривожлантириш бўйича

[1] https://blog.varonis.com/cybersecurity-statistics/

[2] Ўзбекистон Республикаси Президенти 2017 йил 7 февралдаги ПФ-4947-сон «Ўзбекистон Республикасини янада ривожлантириш бўйича Ҳаракатлар стратегияси тўғрисида» ги Фармони

Ҳаракатлар стратегияси тўғрисида»ги, 2018 йил 14 мартдаги ПФ-5379-сон «Ўзбекистон Республикасининг давлат хавфсизлиги тизимини такомиллаштириш чора-тадбирлари тўғрисида»ги ва 2018 йил 19 февралдаги ПФ-5349-сон «Ахборот технологиялари ва коммуникациялари соҳасини янада такомиллаштириш чора-тадбирлари тўғрисида»ги Фармонлари, 2007 йил 3 апрелдаги ПҚ-614-сон «Ўзбекистон Республикасида ахборотни криптографик муҳофаза қилишни ташкил этиш чора-тадбирлари тўғрисида»ги Қарори ҳамда мазкур фаолиятга тегишли бошқа меъёрий-ҳуқуқий ҳужжатларда белгиланган вазифаларни амалга оширишга мазкур диссертация тадқиқоти маълум даражада хизмат қилади.

**Тадқиқотнинг республика фан ва технологиялари ривожланишининг устувор йўналишларига мослиги.** Мазкур тадқиқот республика фан ва технологиялар ривожланишининг IV. «Ахборотлаштириш ва ахборот-коммуникация технологияларини ривожлантириш» устувор йўналиши доирасида бажарилган.

**Муаммонинг ўрганилганлик даражаси.** Криптографик тизимлар учун самарали калитларни генерациялаш хусусан, псевдотасодифий кетма-кетликларни ҳосил қилиш, биометрик параметрларга асосланган калитларни генерациялаш усулларини ишлаб чиқиш ва уларнинг хавфсизлик хусусиятларини таҳлил қилиш бўйича B.Schneier, J.Viega, Y.Dodis, J.Kelsey, L.Ballard, A.Juels, A.Smith, A.Shamir, M.Al Tarawneh, N.Ferguson, О.В.Куликова ва бошқа чет эллик олимлар томонидан инженерлик-тадқиқот ишлари олиб борилмоқда.

Ўзбекистонда С.К.Ганиев, М.М.Каримов, П.Ф.Хасанов, Д.Е.Акбаров, А.И.Мусаевлар бошчилигидаги илмий жамоалар томонидан ахборотнинг криптографик ҳимоя усуллари хусусан, криптографик тизимлар учун тасодифий калитларни генерациялаш, оқимли шифрлаш, симметрик блокли шифрлаш, очиқ калитли шифрлаш, хэш-функция ва электрон рақамли имзо усуллари ўрганиб чиқилган.

Шунинг билан бирга калитнинг тасодифийлик даражасига аниқ баҳо берувчи энтропияни ҳисоблаш усуллари, тезкорлик ва юқори псевдотасодифийлик даражасига эга бўлган криптографик сонлар генераторларини яратиш ва амалда қўлланилувчи биометрик параметрларга асосланган самарали криптографик калитларни генерациялаш усуллари етарли даражада ўрганилмаган.

**Диссертация тадқиқотининг диссертация бажарилган олий таълим муассасасининг илмий-тадқиқот ишлари режалари билан боғлиқлиги.** Диссертация тадқиқоти Тошкент ахборот технологиялари университетининг илмий-тадқиқот ишлари режасининг №Ф706-17 – «Ахборот тизимларида биометрик – криптографик технологиялар қўлланилишининг тадқиқи» (2017-2018) мавзусидаги лойиҳа доирасида бажарилган.

**Тадқиқотнинг мақсади** тасодифийлик даражаси юқори аниқликка эга самарали криптографик калитларни генерациялаш имкониятини берувчи

ҳамда уларни эсда сақлашни ва олиб юришни талаб этмайдиган усул ва алгоритмларни ишлаб чиқишдан иборат.

**Тадқиқотнинг вазифалари:**

таҳдид моделини ва унинг асосида энтропияни юқори аниқликда ҳисоблаш усулини ишлаб чиқиш;

тасодифийлик даражаси юқори бўлган қийматларни ҳосил қилувчи псевдотасодифий сонларни генерациялаш усули ва алгоритмини ишлаб чиқиш;

бармоқ изи тасвиридан ишончли муҳим нуқталарни ажратиш усулини такомиллаштириш;

калитларни сақлашни ва хавфсиз олиб юришни талаб этмайдиган бармоқ изи параметрларига асосланган самарали калитларни генерациялаш усули ва алгоритмини ишлаб чиқиш.

**Тадқиқотнинг объекти** сифатида криптографик тизимларда қўлланилувчи криптобардошли калитларни генерациялаш олинган.

**Тадқиқотнинг предметини** биометрик параметрларга асосланган тасодифийлик даражаси юқори аниқликга эга калитларни генерациялаш усуллари ва алгоритмлари ташкил этади.

**Тадқиқотнинг усуллари.** Тадқиқот жараёнида ахборотни криптографик ҳимоялаш тизимлари назарияси, эҳтимоллик назарияси, сонлар назарияси, математик мантиқ, моделлаш ва объектга йўналтирилган дастурлаш усулларидан фойдаланилган.

**Тадқиқотнинг илмий янгилиги** қуйидагилардан иборат:

таҳдид модели ва унинг асосида тасодифий сонлар генератори томонидан генерацияланган кетма-кетликлар энтропиясини аниқ ҳисобловчи усул ишлаб чиқилган;

ҳодисалар манбаларини мантиқий гуруҳларга ажратиш асосида тасодифий сонлар генераторидан келаётган қийматларни «пул»ларда тўплаш усули такомиллаштирилган;

симметрик блокли шифрлаш ва калитли хэш-функция алгоритмларини санагич режимида фойдаланиш орқали псевдотасодифий сонларни генерациялаш усули ва алгоритми ишлаб чиқилган;

бармоқ изи тасвиридаги муҳим нуқталар орасидан қалбакиларини аниқлаш орқали криптографик калит учун керакли ахборотни ажратиш усули такомиллаштирилган;

бармоқ изи ёрдамида калитларни эсда сақлашни ва хавфсиз олиб юришни талаб этмайдиган самарали криптографик калитларни генерациялаш усули ва алгоритми ишлаб чиқилган.

**Тадқиқотнинг амалий натижаси** қуйидагилардан иборат:

юқори аниқликдаги энтропияга эга тасодифий кетма-кетликлар асосида криптобардошли калитларни генерациялашнинг дастурий воситаси ишлаб чиқилган;

бармоқ изига асосланган калитларни генерациялаш имконини берувчи дастурий восита ишлаб чиқилган;

генерацияланган кетма-кетликларни тасодифийлик даражасини текширувчи ва таҳдид модели асосида энтропия қийматларини ҳисобловчи дастурий воситалар ишлаб чиқилган.

**Тадқиқот натижаларининг ишончлилиги.** Тадқиқот натижаларининг ишончлилиги криптографик тизимларда зарур бўлган бардошли калитларни ҳосил қилиш мақсадида ишлаб чиқилган таҳдид модели ва унга асосланган энтропияни ҳисоблаш, тасодифий ва псевдотасодифий калитларни генерациялаш алгоритмларидан олинган реал ва тажрибавий таҳлиллар билан изоҳланади.

**Тадқиқот натижаларининг илмий ва амалий аҳамияти.** Тадқиқот натижаларининг илмий аҳамияти таклиф этилган таҳдид модели асосида тасодифий сонлар генератори учун энтропия қийматини аниқ ҳисоблаш ва биометрик параметрларга асосланган самарали калитларни генерациялаш алгоритмларини ва дастурларини ишлаб чиқиш билан изоҳланади.

Тадқиқот натижаларининг амалий аҳамияти криптографик тизимларга бўладиган калитга боғлиқ таҳдидларни минималлаштириш, калитларни хавфсиз сақлашни ва олиб юришни талаб этмайдиган криптографик калитларни бошқариш имконияти билан изоҳланади.

**Тадқиқот натижаларининг жорий қилиниши.** Ишлаб чиқилган таҳдид модели ва унга асосланган энтропияни ҳисоблаш усули орқали самарали криптографик калитларни генерациялаш усуллари, алгоритмлари ҳамда дастурий воситалари бўйича олинган илмий натижалар асосида:

самарали криптографик калитларни генерациялаш бўйича «BIO KEY BINDING SYSTEM», «Trusted (Pseudo) random number generators» ва «WIN RNG» дастурий воситаларига «UNICON.UZ» ДУК томонидан фойдаланиш мумкинлиги тўғрисида хулоса берилган («UNICON.UZ» ДУКнинг 2018 йил 7 ноябрдаги хулосаси). Натижада мавжуд ҳодисалар манбаларидан ҳосил бўлган қийматлар энтропиясини ўлчаш асосида тасодифий калитларни, улар асосида бардошли псевдотасодифий калитларни генерациялаш ва калитларни самарали бошқариш имкониятлари яратилган;

ҳодисалар манбаидан келаётган ахборот энтропиясини аниқ ҳисоблаш асосида мантиқий ажратилган «пул»ларда сақлаш орқали шакллантирилган тасодифий қийматга кўра калитларни генерациялаш имкониятини берувчи дастурий восита «UNICON.UZ» ДУКнинг амалий фаолиятига жорий қилинган (Ахборот технологиялари ва коммуникацияларини ривожлантириш вазирлигининг 2018 йил 5 октябрдаги 33-8/7438-сон маълумотномаси). Илмий тадқиқот натижасида маълумотларни тўпловчи махсус қурилма маълумотларни шифрлашда зарур ишончли тасодифий калитлар билан таъминланиб, уларни доимий янгилаш имконини берган;

симметрик блокли шифрлардан ва калитли хэш-функциялардан санагич режимида фойдаланиш асосида криптографик инфратузилмалар, симметрик, очиқ калитли ва аутентификация тизимлари учун турли тасодифий қийматларни ва калитларни генерациялаш имконини берувчи дастурий восита «AlpCrypto» МЧЖга жорий қилинган (Ахборот технологиялари ва

коммуникацияларини ривожлантириш вазирлигининг 2018 йил 5 октябрдаги 33-8/7438-сон маълумотномаси). Илмий тадқиқот натижасида ишлаб чиқилган дастурий восита NIST Special Publication 800-22 тестлар тўплами доирасида 95,3% тасодифийлик даражасига эга кетма-кетликларни генерациялаш имконини берган;

бармоқ изи асосида калитларни сақлашни ва олиб юришни талаб этмайдиган криптографик калитларни генерациялаш усулининг дастурий воситаси «MironSoft» корхонасига жорий этилган (Ахборот технологиялари ва коммуникацияларини ривожлантириш вазирлигининг 2018 йил 5 октябрдаги 33-8/7438-сон маълумотномаси). Илмий тадқиқот натижасида бармоқ изи асосида 128 ва 256 битли калитларни генерацияловчи дастурий восита калитларни генерациялаш самарадорлигини 78%гача ошириш имконини берган.

**Тадқиқот натижаларининг апробацияси.** Мазкур тадқиқот натижалари 5 та халқаро ва 5 та республика илмий-амалий анжуманларида муҳокамадан ўтказилган.

**Тадқиқот натижаларининг эълон қилинганлиги.** Диссертациянинг мавзуси бўйича жами 21 та илмий иш чоп этилган, жумладан, Ўзбекистон Республикаси Олий аттестация комиссиясининг диссертацияларнинг асосий илмий натижаларини чоп этиш тавсия этилган илмий нашрларида 8 та мақола, 2 таси хорижий ва 6 таси республика журналларида нашр этилган ҳамда 3 та ЭҲМ учун яратилган дастурий воситаларни қайд қилиш гувоҳномалари олинган.

**Диссертациянинг тузилиши ва ҳажми.** Диссертация таркиби кириш, тўртта боб, хулоса, фойдаланилган адабиётлар рўйхати ва иловалардан иборат. Диссертация ҳажми 119 бетни ташкил этади.

## ДИССЕРТАЦИЯНИНГ АСОСИЙ МАЗМУНИ

**Кириш** қисмида диссертация мавзусининг долзарблиги ва зарурияти асосланган, тадқиқотнинг Ўзбекистон Республика фан ва технологиялари ривожланишининг устувор йўналишларига мослиги кўрсатилган, мақсад ва вазифалари белгилаб олинган ҳамда тадқиқот объекти ва предмети аниқланган, олинган натижаларнинг ишончлилиги асослаб берилган, уларнинг назарий ва амалий аҳамияти, тадқиқот натижаларини амалда жорий қилиш ҳолати, нашр этилган ишлар ва диссертациянинг тузилиши бўйича маълумотлар келтирилган.

Диссертациянинг **«Криптографик калитларни бошқариш муаммолари»** деб номланган биринчи боби криптографик калитлар ва уларни бошқаришда қўйиладиган талаблар, калитларни бошқариш жараёнида мавжуд таҳдидлар ва криптографик калитларни генерациялаш усулларининг тадқиқига бағишланган.

Тасодифий кетма-кетликларни генерациялаш усуллари 3 та туркумга: хавфсиз бўлмаган тасодифий сонлар генератори, криптографик псевдотасодифий сонлар генератори ва энтропия тўпловчиларига ажратилади.

Мазкур туркумларга тегишли мавжуд калит генераторларидаги хавфсизлик муаммолари 1-жадвалда келтирилган. Биринчи туркумга тегишли алгоритмлар тезкор саналсада, такрорланиш даври кичик. Иккинчи туркумга тегишли генераторлар киришда фиксирланган тасодифий қийматни қабул қилиб, чиқишда катта узунликдаги кетма-кетликларни ҳосил қилади. Энтропия тўпловчилар турли ҳодисалар манбаидан чиқаётган қийматларни тўплаб боради ва маълум вақтда фиксирланган узунликда тасодифий калитни генерациялайди. Бу калит криптографик псевдотасодифий сонлар генератори учун кириш қиймати сифатида фойдаланилади.

**1-жадвал**

**Тасодифий сонларни генерациялаш усуллари**

| № | Тасодифий сонларни генерациялаш усули | Мавжуд камчилик |
|---|---|---|
| 1. | Хавфсиз бўлмаган тасодифий сонлар генератори (турли дастурлаш тилларидаги rand() ёки random() функцияси) | - Хавфсиз эмас;<br>- Такрорланиш даври кичик; |
| 2. | Криптографик псевдотасодифий сонлар генератори (ANSI X9.17, BBS, ISAAC ва ҳ.) | - Тезкорлиги паст;<br>- Бардошли бўлмаган алгоритмдан фойдаланилган (масалан, MD5, SHA1 ва ҳ.) |
| 3. | Энтропия тўпловчилар (/dev/random, Fortuna, Yarrow ва ҳ.) | - Энтропияни ҳисоблашда турли исботланмаган эвристик тенгликлардан, фаразлардан фойдаланилган ёки ҳисоблашдан қочилган; |

Таъкидлаш лозимки, криптографик калитларни генерациялашнинг мавжуд усуллари тасодифий қиймат энтропиясини аниқ ҳисоблай олмайди ва хавфсиз бўлмаган криптографик алгоритмлардан фойдаланилиб ишлаб чиқилган псевдотасодифий сонлар генераторлари тезкор саналмайди ҳамда фойдаланувчидан калитларни хавфсиз сақлаш зуруриятини талаб этгани боис калитга қаратилган таҳдидларнинг ошишига сабаб бўлади.

Диссертациянинг **«Криптобардошли калитларни генерациялаш усуллари»** деб номланган иккинчи бобида таҳдид модели ва унга асосланган энтропияни ҳисоблаш усули таклиф этилган. Операцион тизимдаги тасодифий қийматларни «пул»ларга асосланган ҳолда тўплаш усули такомиллаштирилиб, хавфсиз ва тезкор бўлган Blake2b хэш-функциясидан фойдаланилиб қийматлар бир томонлама ўзгартиришлар асосида «пул»ларда сақланган. Бундан ташқари, калитли хэш-функцияларни ва блокли симметрик шифрларни санагич режимида фойдаланишга асосланган псевдотасодифий сонлар генератори таклиф этилган.

Таклиф этилган таҳдид модели учун икки турдаги таҳдидчилар: локаль тармоқ сегментини бошқариш (масофадан) имкониятига эга ва тармоқдан

фойдаланувчи, бироқ ҳодим компьютеридан фойдаланиш имтиёзига эга бўлмаган таҳдидчилар олинди. Ушбу таҳдидчиларга маълум даражадаги имкониятлар берилиб, ҳар бир таҳдидчи учун профессионал бўлмаган, мутахассис ва профессионал кўринишидаги малака даражаси олинди. Биринчи турдаги таҳдидчининг малакасига мос хавф даражалари $\mu = \{0,16; 0,26; 0,34\}$ га тенг деб олинган бўлса, иккинчи таҳдидчи учун ушбу қийматлар $\mu = \{0,28; 0,34; 0,45\}$ га тенг бўлди.

Таклиф этилган таҳдид моделига асосан тасодифий сонлар генераторига таҳдидчилар томонидан келтириши мумкин бўлган зарар даражалари юқори, ўрта ва паст тоифаларга ажратилиб, уларни мос равишда сонли миқдори $\sigma = \{1; 0,5; 0,1\}$ га тенг деб олинди. Бўлиши мумкин бўлган таҳдидлар STRIDE (*Spoofing* - қалбакилаштириш, *Tampering* - ўзгартириш, *Repudiation* - рад этиш, *Information disclosure* - ахборотни ошкор бўлиши, *Denial of service* - хизматдан воз кечишга ундаш, *Elevation of privilege* - имтиёзнинг ортиши) методологиясига кўра олиниб, уларнинг умумий улуши 2-жадвалда акс эттирилган.

**2 - жадвал**

**Тасодифий сонлар генераторига бўлиши мумкин бўлган таҳдидларнинг STRIDE методологияси бўйича улуши**

| STRIDE омили | S | T | R | I | D | E |
|---|---|---|---|---|---|---|
| Улуши, ρ | 1/11 | 1/11 | 0 | 1/11 | 3/11 | 5/11 |
| Таъсир коэффиценти, σ | 1 | 1 | 0,5 | 1 | 0,1 | 0,5 |
| Таҳдид улушининг тасодифий калит генераторига таъсири, $\tau = \rho * \sigma$; | 1/11 | 1/11 | 0 | 1/11 | 3/110 | 25/110 |

Умумий ҳолда STRIDE методологиясига кўра якуний таҳдид улушларининг йиғиндиси қуйидагига тенг:

$$\tau_{умум} = \sum_{i=1}^{k} \rho_i * \sigma_i$$

Таклиф этилган таҳдид модели асосида манбаларга бўладиган хавф эҳтимоли ω, таҳдидчи малакасига боғлиқ ҳолда қуйидаги тенглик билан ифодаланади:

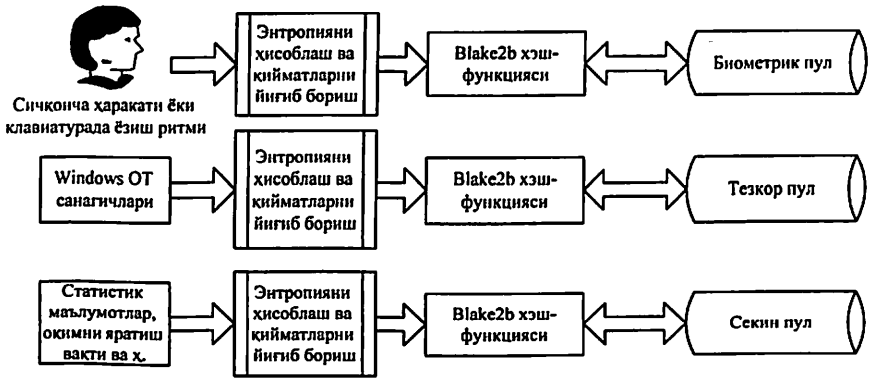
$$\omega = \mu * \tau$$

Энтропияни статистик қийматини ҳисоблашда NIST SP 800-90B нашрида тасодифий қийматни генерациялаш манбаларининг энтропиясини ҳисоблаш учун таклиф этилган минимал-энтропия (min-Entropy, $H_{min}$) дан фойдаланилди. Ушбу усулга асосан танлаб олинган таҳдид модели учун якуний энтропияни ҳисоблаш тенглигини қуйидагича ифодалаш мумкин:

$$H_{якуний,i} = (1 - \omega_i) * H_{min,i}$$

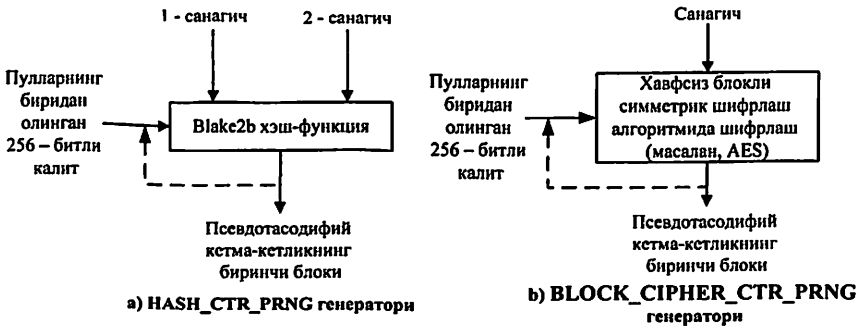
Тасодифий қийматларни «пул»ларга йиғиш усулини такомиллаштириш мақсадида, мавжуд тасодифий ҳодисалар манбалари алоҳида мантиқий

гуруҳларга ажратилди ва улардан келаётган қийматлар энтропиясини ҳисоблаш орқали Blake2b хэш-функцияси ёрдамида фиксирланган кўринишда сақланди (1-расм).




**1-расм. Энтропияни ҳисоблаб тасодифий қийматларни ажратилган «пул»ларга ёзиш**

«Пул»ларда йиғилган криптобардошли кетма-кетликларни генерацияловчи, калитли Blake2b хэш-функция ва блокли симметрик шифрлаш алгоритмларига асосланган псевдотасодифий сонлар генераторининг (ПТСГ) умумий кўриниши 2-расмда келтирилган.




**2-расм. Таклиф этилган псевдотасодифий сонлар генераторларининг умумий кўриниши**

Таклиф этилган псевдотасодифий сонлар генераторларида «пул»лардан олинган битта калит $2^{16}$ та кетма-кетликлар блокини ҳосил қилишда фойдаланилди ва ҳар бир талаб этилган кетма-кетликдан сўнг калитни янгилаш учун қўшимча кетма-кетлик блоклари генерацияланди. Бу ҳолда $2^{16}$ та блок ичида коллизиянинг вужудга келиш эҳтимоллиги $2^{-97}$ га тенг бўлади.

Псевдотасодифий сонлар генераторига мурожаат бўлганидан сўнг, дастлаб генераторнинг жорий ҳолати аникланади. Агар талаб қилинган

тасодифий байтларни генерация қилишга генераторнинг жорий ҳолати тўғри келмаса, тезкор «пул» асосида генераторнинг ички ҳолати янгиланади ва санагич нол ҳолатига ўрнатилади. Агар генератор ишлаётган шахсий компьютер энди юкланган бўлса, биометрик «пул» асосида генератор ҳолати янгиланади. Агар тезкор «пул» «ифлосланган» бўлса ёки калит узоқ муддатли фойдаланилганида секин «пул»да тўпланган энтропия асосида генератор ҳолати янгиланади.

Диссертация ишининг **«Самарали калитларни генерациялаш усуллари ва алгоритмлари»** номли учинчи бобида бармоқ изига асосланган, калитларни эсда сақлашни ва олиб юришни талаб этмайдиган, криптографик калитларни генерациялашнинг самарали усули ва алгоритми таклиф этилган. Таклиф этилган усулда бармоқ изидаги муҳим нуқталарнинг, қалбакиларидан ажратиб олиш усули такомиллаштирилган.

Биометрик параметрларга асосланган калитларни генерациялаш усуллари ўзида паролга ва токенга асосланган калитларни генерациялаш усулларида мавжуд бўлган эсда сақлашни ва олиб юришни талаб этмаслиги билан ажралиб туради.

Биометрик параметрларга асосланган калитларни генерациялашда мос биометрик хусусиятни танлаш муҳим аҳамиятга эга. Шу сабабли, бармоқ изи, юз тасвири, кўз қорачиғи, қўлнинг геометрик шакли ва овоз параметрлари универсаллик, такрорланмаслик, ўзгармаслик, тўпланувчанлик, амалга оширишлик, мувофиқлик, алданувчанлик ва жараён учун зарур бўлган қурилма ҳамда унинг нархи кесимида таҳлил қилинди (бунда ҳар бир омилни биометрик параметрларда мавжудлиги юқори = 100, ўртача = 75 ва паст = 50 даражада бўлиши мумкин). Таҳлил натижасига асосан бармоқ изи ва кўз қорачиғи энг юқори 89,3% натижани қайд этган бўлсада, бармоқ изи кўз қорачиғига қараганда арзон сканер қурилмасини талаб этади. Бундан ташқари, биометрик параметрларда калит учун етарли ахборотни мавжудлиги текширилганда, бармоқ изи ва кўз қорачиғи учун калит соҳаси мос ҳолда $2^{14}$ ва $2^{20}$ битга тенг бўлди. Ишлаб чиқиладиган биометрик параметрларга асосланган калит генератори учун таҳлил натижаларига асосан ва фойдаланувчиларга қулай бўлиши инобатга олиниб, бармоқ изи параметри танланди.

Таклиф этилган бармоқ изига асосланган калитларни генерациялаш усулида калитлар тасвирдаги муҳим нуқталар асосида ҳосил қилинади. Бармоқ изи тасвиридан ҳақиқий муҳим нуқталар билан бирга қалбаки муҳим нуқталар ҳам олиниши мумкин (3-расм).

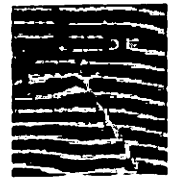
Мазкур ҳолда қалбаки муҳим нуқталар орасидан ҳақиқийларини ажратиб олиш учун бармоқ изи тасвирига ишлов бериш босқичлари сўнгги ишлов бериш усули асосида такомиллаштирилди.

Натижада $alfa = |p_i(\alpha) - p_j(\alpha)|$ ва $d = \sqrt{(x_i - x_j)^2 + (y_i - y_j)^2}$ қийматлар ҳисобланади. Бу ерда: *alfa* – иккита муҳим нуқта орасидаги бурчак, $d$ – иккита муҳим нуқта орасидаги Евклид масофаси.

Қалбаки уланмаган чизиқларни аниқлаш учун қуйидаги иккита шарт бажарилиши лозим: $alfa = 180$ ва $d \geq 10$. Агар ушбу шарт бажарилса, иккита муҳим нуқта текширишдан ўтган саналади.

Тасвирнинг четки қисмларида юзага келадиган қалбаки муҳим нуқталарни аниқлаш учун, олинган муҳим нуқтадан мос томонга қараб $r = 10$ пиксел доирасида қора нуқталарнинг мавжуд эмаслиги текширилади.

**a) ажратилган барча муҳим нуқталар**



**b) қалбаки уланмаган чизиқлар**

**c) юқори чап томондаги қалбаки тугалланган қирликлар**

**3-расм. Бармоқ изи тасвиридаги қалбаки муҳим нуқталар**

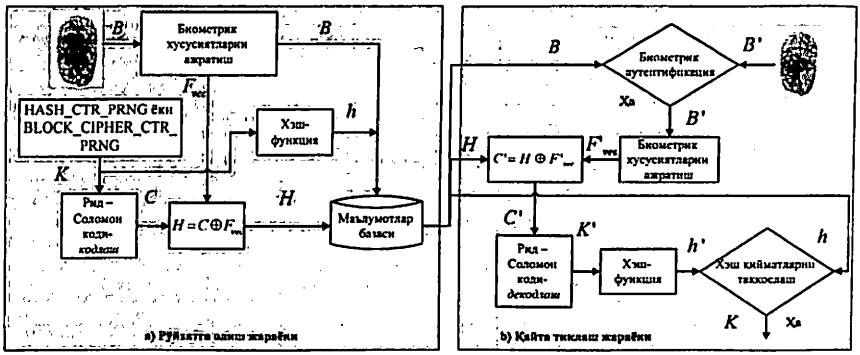
Юқорида келтирилган шартлар асосида муҳим нуқталар орасидан кераклиги ажратилиб олинди. Ажратиб олинган муҳим нуқталар асосида криптографик калитларни генерациялашда калитларни «озод этиш», калитларни боғлаш ва калитларни генерациялаш схемаларидан кенг фойдаланилди. Калитларни боғлаш схемаси қолганларига нисбатан янгилаш имкониятига эга ва юқори энтропия қийматли калитларни генерациялаш қобилияти билан ажралиб туради.

Таклиф этилган калитларни боғлаш схемаси асосида криптографик калитларни генерациялаш усулининг функционал схемаси 4-расмда келтирилган.

Таклиф этилган усулга асосан бармоқ изи тасвирларидан ажратиладиган умумий муҳим нуқталар сони $n$ нинг қийматига кўра 128 ($15 \leq n < 21$) ёки *256 ($n \geq 21$)* битли калитларни генерациялаш имконияти мавжуд. Акс ҳолда бармоқ изи тасвиридан калитни генерациялашнинг имкони бўлмайди.

Биометрик параметрлар норавшан турдаги ахборот саналганлиги боис, бир фойдаланувчига тегишли иккита биометрик намуналар орасида ҳам фарқ мавжуд. Маълум даражада фарқни бартараф этиш учун хатоликларни тузатишнинг Рид-Соломон кодидан фойдаланилди. Таклиф этилган усулга асосан хатоликни тузатиш коди бармоқ изидаги 3 та муҳим нуқтага тегишли

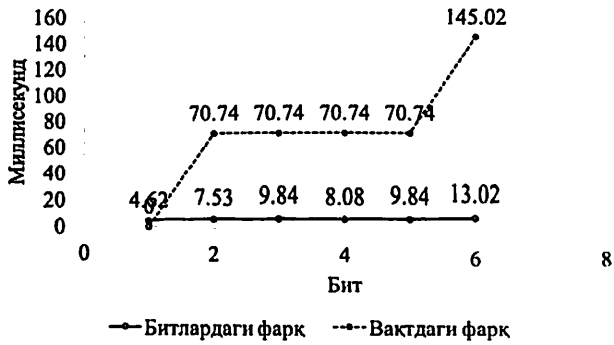
ахборотни тиклай олади. Бу эса 128 битли калитда мос келган муҳим нуқталар сонининг камида 12 та бўлишини талаб этади.



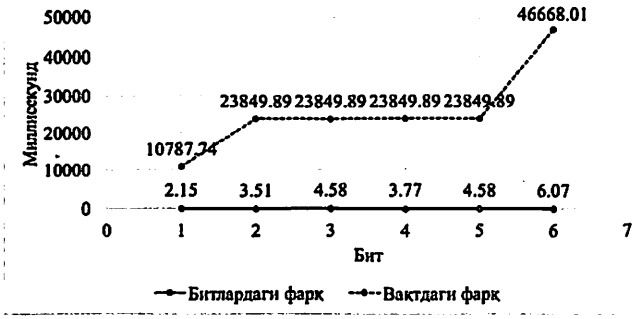

**4-расм. Криптографик калитларни боғлаш усулининг функционал схемаси**

Диссертациянинг «**Криптографик калит генераторларининг самарадорлигини баҳолаш**» номли тўртинчи бобида таклиф этилган таҳдид модели асосида тасодифий сонлар генератори қийматини ҳисоблаш усулининг, псевдотасодифий сонлар генераторининг ва бармоқ изига асосланган калит генераторининг самарадорликлари баҳоланган. Ҳар бир таклиф этилган усул асосида дастурий воситалар ишлаб чиқилган ва уларни амалда қўллаш натижалари таҳлилланган.

Мавжуд усул ва таҳдид моделига асосланган энтропияни ҳисоблашда битлар сони фарқининг вақтга боғлиқлиги 5-расмда келтирилган. Тезкор ва секин «пул»лар учун энг катта битлар фарқи иккинчи турдаги таҳдидчининг профессионал даражасига тегишли ва уларда 256 бит энтропияни тўплаш учун сарфланган вақтнинг мавжудидан фарқи мос равишда 145,02 мс ва 46668,01 мс га тенг бўлган.



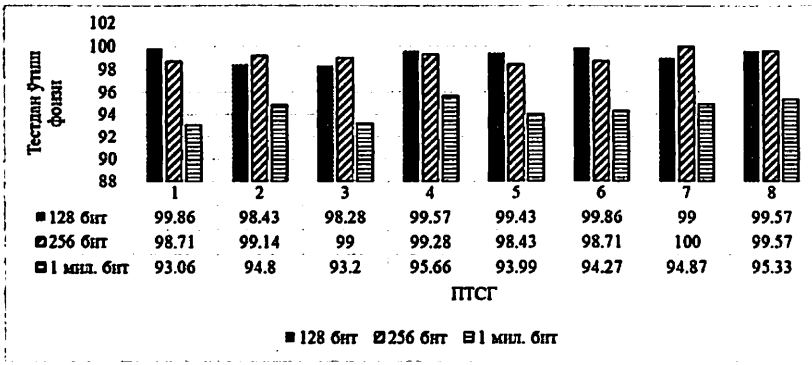

**а) тезкор «пул» учун**



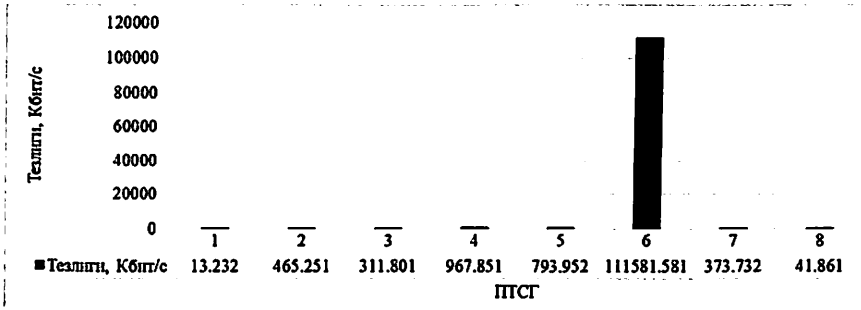

**b) секин «пул» учун**

**5-расм. Мавжуд усул ва таҳдид моделига асосланган энтропияни ҳисоблашда битлар сони фарқининг вақтга боғлиқлиги**

Таклиф этилган псевдотасодифий сонлар генераторини мавжудлари билан таққослаш қатор алгоритмлар асосида ва тасодифийлик даражаларини қиёслаш NIST Special Publication 800-22 тестлар тўплами ёрдамида амалга оширилди. Бундан ташқари, уларнинг тезлик хусусиятлари таққосланиб, қиёсий таҳлил натижалари 6-расмда келтирилган. Тасодифийлик даражасига кўра HMAC CTR ПТСГ ва BLOCK CIPHER CTR ПТСГлари томонидан 256 битли калитни генерациялашда энг юқори натижалар (100% ва 99,57%) қайд этилган. Қолган узунликдаги калитларни генерациялашда ҳам таклиф этилган ПТСГларининг натижалари юқорилигини кўриш мумкин. HMAC CTR ПТСГ ва BLOCK CIPHER CTR ПТСГлар бир турга тегишли мавжуд ПТСГ (RSAREF ПТСГ ва ANSI X9.17 ПТСГ) га нисбатан юқори тезкорликни қайд этди.




**a) тасодифийлик даражаси бўйича**




**b) тезкорлиги бўйича**

1 - ANSI X9.17 ПТСГ
2 - DSA ПТСГ
3 - RSAREF ПТСГ
4 - OPENSLL ПТСГ
5 - DEV/URANDOM ПТСГ
6 - CRYPTGEN - RANDOM ПТСГ
7 - HMAC CTR ПТСГ
8 - BLOCK CIPHER CTR ПТСГ

**6-расм. Таклиф этилган псевдотасодифий сонлар генераторларининг мавжудлари билан қиёсий таҳлили**

Таклиф этилган бармоқ изига асосланган калит генераторини тестлашда уч турдаги бармоқ изи базалари олиниб, умумий натижалар 3-жадвалда келтирилган (False rejection rate, FRR – ёлғондан рад этиш даражаси, False acceptance rate, FAR – ёлғондан тасдиқлаш даражаси).

**3-жадвал**

**Бармоқ изи базалари асосида олинган таҳлил натижалари**

| Омиллар | Cross Match Verifier 300 Classic | Digitalpersona U.are.U 4000 Scanner | Futronic FS88H |
|---|---|---|---|
| Субъектлар сони | 51 | 65 | 40 |
| Олинган бармоқ изи тасвирлари сони | 8 | 8 | 10 |
| Рўйхатга олиш ва калитни тиклашда фойдаланилган намуналар сони | 4/4 | 4/4 | 4/6 |
| Рўйхатга олиш жараёнидаги хатолик | 8/51 | 34/65 | 5/40 |
| Ажратилган MP (Minutiae points) лар сони | 15 MP – 8 та; 21 MP – 35 та. | 15 MP – 18 та; 21 MP – 13 та. | 15 MP – 6 та; 21 MP – 29 та. |
| FRR хатолиги (%) | 12,209 | 19,354 | 22,00 |
| Ўртача MP нуқталар фарқи | 1,633 | 1,991 | 2,071 |
| FAR хатолиги (%) | 0 | 0 | 0 |

Олинган натижаларга кўра энг юқори FRR хатолиги Futronic FS88H базасига тегишли бўлиб, ушбу ҳолда икки бармоқ изи тасвирдаги муҳим нуқталар сонининг фарқи 2,271 га тенг бўлди. Бу эса 3 та муҳим нуқта ахборотини тузатишга созланган Рид-Соломон кодидан фойдаланиб, ўртача ҳар тўртта уринишда 3 тасига тўғри калитни генерациялаш имконияти мавжудлигини билдиради. Калитларни генерациялашдан олдин аутентификация жараёнини амалга ошириш орқали FAR хатолиги нолга тенглаштирилди.

Таклиф этилган бармоқ изига асосланган калитни генерациялаш усулининг 3.2 - бўлимда келтирилган таҳдидларга қарши тура олиш қобилияти 4-жадвалда келтирилган.

**4-жадвал**

**Бармоқ изига асосланган калит генераторининг хавфсизлик таҳлили**

| Ҳужум тури | Таҳлил натижаси |
|---|---|
| Қўпол куч ҳужуми | - 128 ва 256 – битли калитларни генерациялайди ва бу калит узунликлари ушбу ҳужумга бардошли. |
| FAR хатолигига асосланган ҳужумлар | - олинган таҳлил натижаларига кўра FAR хатолиги 0 га тенг бўлди ва бу ҳужумга бардошли. |
| Хатоликларни тузатиш кодларига қаратилган ҳужумлар | - Рид-Соломон коди бармоқ изи тасвиридаги мос келмаган 3 та муҳим нуқталар ҳақидаги ахборотни қайта тиклашга мўлжалланган. |
| Биометрик хусусиятларни ўзгарувчанлиги | - FRR хатолиги 22,00% га тенг бўлганлиги учун ҳақиқий фойдаланувчи томонидан муваффақиятсиз уринишларнинг улуши ўртача 1/4 га тенг бўлди. |
| Калит учун етарли ахборотни мавжуд эмаслиги | - 128 битли ва 256 битли калитларни норавшан қайдлаш (fuzzy commitment) схемаси асосида генерациялаш амалга оширилди. |
| Биометрик параметрларнинг хавфсиз эмаслиги | - калитни тўғри генерациялаш учун талаб этилаётган муҳим нуқталар сони камида 12 (128 битли калит учун) қилиб олинди;<br>- бармоқни тирикликга текшириш имкониятига эга сканерлардан фойдаланилди. |

Ишлаб чиқилган бармоқ изига асосланган калит генератори 128 ва 256 битли калитларнинг норавшан қайдлаш схемасига асосан ҳосил қилиниши, FAR хатолигини нолга тенг бўлиши, калитни муваффақиятли генерациялаш учун муҳим нуқталар сонини камида 12 га тенг бўлиши, тўғри созланган Рид-Соломон кодидан ва сифатли бармоқ изи сканеридан фойдаланилганлиги мавжуд ҳужумларга қарши тура олиш имконини беради.

## ХУЛОСА

«Самарали криптографик калитларни генерациялаш усуллари ва алгоритмлари» мавзусидаги диссертация иши бўйича олиб борилган тадқиқотлар натижасида қуйидаги хулосалар тақдим этилди:

1. Тасодифий сонлар генераторидан чиқаётган қийматларнинг энтропиясини ҳисоблаш учун таҳдид модели ва унга асосланган усул ишлаб чиқилди. Ишлаб чиқилган энтропияни ҳисоблаш усули тасодифийлик даражасини аниқ ҳисоблаш ва сарфланган вақтни минималлаштириш имконини берди.

2. Энтропия манбаидан келаётган қийматларни йиғишда кенг ишлатиладиган «пул»ларга асосланган усул такомиллаштирилди. Такомиллаштирилган қийматларни йиғиш усули хавфсиз ва узоқ вақт фойдаланилувчи калитларни генерациялаш ҳамда тасодифий ҳодисалар манбалари «ифлосланган» тақдирда ҳам янги тасодифий қийматларни ҳосил қилиш имконини берди.

3. Тасодифий кириш қийматидан бардошли калитларни ҳосил қилувчи криптографик псевдотасодифий сонларни генерациялаш усуллари ишлаб чиқилди. Ишлаб чиқилган усуллар генератор ички ҳолатини янгилаш ва кириш қийматларини давомий алмаштириш орқали қисқа вақт ичида даражаси юқори тасодифий қийматларни ҳосил қилишга имкон берди.

4. Псевдотасодифий кетма-кетликларни генерациялаш усуллари 256 битли калитларни ҳосил қилишда NIST Special Publication 800-22 статистик тестлар доирасида мавжудларига нисбатан юқори тасодифийлик даражасини (HMAC CTR ПТСГ учун 100% ва BLOCK CIPHER CTR ПТСГ учун 99,57%) қайд этиб, мавжуд таҳдидларга қарши тура олиш имкониятини берди.

5. Бармоқ изи тасвирларидан муҳим нуқталарни ажратиш усули такомиллаштирилди. Такомиллаштирилган усул ажратилган муҳим нуқталар орасидан ҳақиқийларини аниқлаш ва улар асосида калитларни генерациялаш самарадорлигини оширишга хизмат қилди.

6. Бармоқ изи тасвиридаги муҳим нуқталар асосида самарали калитларни генерациялаш усули ва алгоритми ишлаб чиқилди. Ишлаб чиқилган усулда калитларни генерациялашда фойдаланувчининг

муваффақиятли уринишлари улуши етарли даражага тенг бўлганлиги калитларнинг мавжуд тахдидларга қарши тура олиш имкониятини оширди.

**НАУЧНЫЙ СОВЕТ DSc.27.06.2017.T.07.01
ПО ПРИСУЖДЕНИЮ УЧЕНЫХ СТЕПЕНЕЙ ПРИ ТАШКЕНТСКОМ УНИВЕРСИТЕТЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ**

**ТАШКЕНТСКИЙ УНИВЕРСИТЕТ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ**

**ХУДОЙКУЛОВ ЗАРИФ ТУРАКУЛОВИЧ**

# МЕТОДЫ И АЛГОРИТМЫ ГЕНЕРАЦИИ ЭФФЕКТИВНЫХ КРИПТОГРАФИЧЕСКИХ КЛЮЧЕЙ

05.01.05 – Методы и системы защиты информации. Информационная безопасность

**АВТОРЕФЕРАТ ДИССЕРТАЦИИ
ДОКТОРА ФИЛОСОФИИ (PhD) ПО ТЕХНИЧЕСКИМ НАУКАМ**

**Ташкент-2018**

**Тема диссертации доктора философии (PhD) по техническим наукам зарегистрирована в Высшей аттестационной комиссии при Кабинете Министров Республики Узбекистан за № B2017.3.PhD/T353.**

Диссертация выполнена в Ташкентском университете информационных технологий.

Автореферат диссертации на трех языках (узбекский, русский, английский (резюме)) размещен на веб-странице научного совета (www.tuit.uz) и на Информационно-образовательном портале «ZiyoNet» (www.ziyonet.uz).

| | |
|---|---|
| **Научный руководитель:** | **Ганиев Салим Каримович**<br>доктор технических наук, профессор |
| **Официальные оппоненты:** | **Алоев Рахматилло Жураевич**<br>доктор физико-математических наук, профессор |
| | **Туйчиев Гулом Нумонович**<br>доктор физико-математических наук |
| **Ведущая организация:** | **«UNICON.UZ» – центр научно-технических и маркетинговых исследований** |

Защита диссертации состоится «21» декабря 2018 года в 14[00] часов на заседании Научного совета DSc.27.06.2017.T.07.01 при Ташкентский университет информационных технологий. (Адрес: 100202, г. Ташкент, ул. Амира Темура, 108. Тел.: (99871) 238-64-43; факс: (99871) 238-65-52; e-mail: tuit@tuit.uz).

С диссертацией можно ознакомиться в Информационно-ресурсном центре Ташкентского университета информационных технологий (регистрационный номер №16). (Адрес: 100202, г. Ташкент, ул. Амира Темура, 108. Тел.: (99871) 238-65-44).

Автореферат диссертации разослан «07» декабря 2018 года.
(протокол рассылки №14 от «16» ноября 2018 года.)

**Р.Х. Хамдамов**
Председатель научного совета по присуждению ученых степеней, д.т.н., профессор

**Ф.М. Нуралиев**
Ученый секретарь научного совета по присуждению ученых степеней, д.т.н., доцент

**Р.Ж. Алоев**
Председатель научного семинара при научном совете по присуждению ученых степеней, д.ф-м.н. профессор

## ВВЕДЕНИЕ (аннотация диссертации доктора философии (PhD))

**Актуальность и востребованность темы диссертации.** В мире особое внимание уделяется разработке криптографических систем защиты информации и повышению их эффективности. В данном этапе развития информационных и коммуникационных систем важным является обеспечение конфиденциальности и целостности информации. «По данным компании Accenture, в 2018 году среди общего количества кибератак самым атакуемым компонентом явилась утечка данных, что составило 43% от общего количества принесенного ущерба»[1]. По данному направлению в развитых странах, таких как США, Российская Федерация, Япония, Китай и других странах важную роль играет разработка криптографических средств, позволяющие обеспечить целостность и конфиденциальность передаваемой информации в вычислительных системах.

В мире ведутся научные исследования, направленные на разработку генераторов ключей на основе устройства или ресурсов операционной системы, позволяющие создавать ключи с повышенной стойкостью. В этом направлении является одним из важных задач, разработка методов корректного вычисления уровня случайности создаваемых ключей, безопасное накопление значений, приходящие из источников событий, быстрое формирование псевдослучайных последовательностей с достаточной длиной на основе случайных значений. На ряду с этим остается необходимым научное обоснование усовершенствования процессов, которые позволяют безопасно управлять криптографическими ключами, использовать их без необходимости запоминания или безопасного хранения.

В нашей республике предпринимаются масштабные меры по обеспечению безопасности информационной безопасности при внедрении систем электронного документооборота и формированию системы электронного правительства в органах государственного и экономического управления. В Стратегии действий по дальнейшему развитию Республики Узбекистан в 2017-2021 гг. отмечены задачи, в том числе «...совершенствование системы обеспечения информационной безопасности и защиты информации, своевременное и адекватное противодействие угрозам в информационной сфере»[2]. Для выполнения поставленных задач этого направления одной из наиболее важных является разработка средств криптографической защиты информации, в частности, методов и средств для генерации криптографических ключей на основе случайных значений, поступающих из разных источников информации.

Данное диссертационное исследование, в определенной степени вносит вклад в выполнении задач, предусмотренных Указами Президента Республики Узбекистан №УП-4947 от 7 февраля 2017 года «О Стратегии действий по

[1] https://blog.varonis.com/cybersecurity-statistics/

[2] Указ Президента Республики Узбекистан №УП-4947 от 7 февраля 2017 г. «О Стратегии действий по дальнейшему развитию Республики Узбекистан»

дальнейшему развитию Республики Узбекистан», №УП-5379 от 14 марта 2018 года «О Мерах по совершенствованию системы государственной безопасности Республики Узбекистан», №УП-5349 от 19 февраля 2018 года «О мерах по дальнейшему совершенствованию сферы информационных технологий и коммуникаций» и Постановлением Президента Республики Узбекистан №ПП-614 от 03 апреля 2007 года «О мерах организации криптографической защиты информации в Республике Узбекистан» а также и других нормативно-правовых документов, принятых в данной сфере.

**Соответствие исследования приоритетным направлениям развития науки и технологий республики.** Данное исследование выполнено в соответствие с приоритетным направлением развития науки и технологий Республики IV. «Информатизация и развитие информационно-коммуникационных технологий».

**Степень изученности проблемы.** Для криптографических систем по генерированию эффективных ключей, в частности, по созданию псевдослучайных последовательностей, разработке методов генерации ключей на основе биометрических параметров и анализу характеристик безопасности со стороны B.Schneier, J.Viega, Y.Dodis, J.Kelsey, L.Ballard, A.Juels, A.Smith, A.Shamir, M.Al Tarawneh, Н.Фергусон, О.В.Куликова и других зарубежных ученых проводятся инженерно-исследовательские работы.

В Узбекистане научные коллективы под руководством С.К.Ганиева, М.М.Каримова, П.Ф.Хасанова, Д.Е.Акбарова, А.И.Мусаева изучены криптографические методы информации, в частности, для криптографических систем генерация случайных ключей, поточное шифрование, симметричное блочное шифрование, шифрование с открытым ключом, хэш-функция и электронно-цифровая подпись.

Вместе с тем, недостаточно изучены методы вычисления энтропии, дающие конкретную оценку уровня случайности ключа, методы создания генераторов криптографических чисел, обладающий такими свойствами, как быстродействие и высокий уровень псевдослучайности, а также методы генерации эффективных криптографических ключей, основанных на применяемых на практике, биометрических параметрах.

**Связь диссертационного исследования с планами научно-исследовательских работ высшего образовательного учреждения, где выполнена диссертация.** Диссертационное исследование выполнено в рамках научного проекта согласно плану научно-исследовательских работ Ташкентского университета информационных технологий №Ф706-17 - «Исследование применения биометрико – криптографических технологий в информационных системах» (2017-2018).

**Цель исследования** состоит в разработке методов и алгоритмов, позволяющих генерировать эффективные криптографические ключи,

имеющие высокую точность уровня случайности и не требующих их запоминания и хранения.

**Задачи исследования:**

разработать модель угроз и на её основе разработать метод вычисления энтропии с высокой точностью;

разработать метод и алгоритм генерации псевдослучайных чисел, создающие значения с высоким уровнем случайности;

усовершенствовать метод выделения важных и надежных точек из изображения отпечатки пальца;

разработать метод и алгоритм генерации эффективных ключей, позволяющие исключить необходимость их запоминания или безопасного хранения, основанных на параметрах отпечатков пальцев.

**Объектом исследования** является генерация криптостойких ключей, применяемая в криптографических системах.

**Предмет исследования** составляют методы и алгоритмы генерации ключей, основанные на биометрических параметрах и имеющие высокий уровень случайности.

**Методы исследования.** В процессе исследования использованы теория систем криптографической защиты информации, теория вероятности, теория чисел, математическая логика, моделирование и методы объектно-ориентированного программирования.

**Научная новизна исследования** заключается в следующем:

разработаны модель угрозы и на ее основе метод корректного вычисления энтропии созданных последовательностей со стороны генератора случайных чисел;

усовершенствован метод собирания в «пулах» значений, поступающих из генератора случайных чисел, основанный на выделении логических групп источников событий;

разработаны метод и алгоритм генерации псевдослучайных чисел на основе использования блочного шифрования и хэш-функций с ключом в режиме счетчика;

усовершенствован метод выделения информации, которая является необходимым для криптографического ключа, путем определения фальшивых среди важных точек в изображении отпечатка пальца;

разработаны метод и алгоритм генерации эффективных криптографических ключей, основанные на отпечатков пальцев, позволяющие исключить необходимость их запоминания и безопасного хранения.

**Практические результаты исследования** заключаются в следующем:

разработано программное средство генерирования криптостойких ключей на основе случайных последовательностей, которое позволяет вычислять энтропию с высокой точностью;

разработано программное средство, позволяющее генерировать ключи на основе отпечатков пальцев;

разработано программное средство, измеряющее значения энтропии на основе модели угрозы и проверяющее степень случайности сгенерированных последовательностей.

**Достоверность результатов исследования.** Достоверность результатов исследования подтверждаются результатами реальных и экспериментальных данных, полученных на основе разработанной модели угрозы и алгоритма вычисления энтропии, а также работой алгоритма генерации случайных и псевдослучайных ключей, разработанного с целью создания стойких ключей, используемых в криптографических системах.

**Научная и практическая значимость результатов исследования.** Научная значимость полученных результатов исследований заключается в том, что разработанные модели, методы и алгоритмы, позволяют генераторам случайных чисел корректно вычислять значения энтропии и генерировать на основе биометрических параметров эффективные ключи.

Практическая значимость полученных результатов исследования заключается в том, что за счет исключения необходимости запоминания или безопасного хранения ключей, минимизируется угроза по отношению к их раскрытию, в результате чего предоставляется легкое и удобное управление ими.

**Внедрение результатов исследования.** На основе полученных научных результатов, по методам, алгоритмам и программным средствам генерации криптографических ключей путем применения разработанной модели угрозы и метода вычисления энтропии, основанный на модели угроз:

по программным средствам генерации эффективных криптографических ключей «BIO KEY BINDING SYSTEM», «Trusted (Pseudo) random number generators» и «WIN RNG» дано заключение о возможности применения со стороны ГУП «UNICON.UZ» (заключение ГУП «UNICON.UZ» от 7 ноября 2018 года). В результате стала возможной генерация случайных ключей на основе измерения энтропии полученных от источников событий и на ее основе – генерация псевдослучайных стойких ключей, а также эффективное управление ключами;

программное средство, позволяющее генерировать ключи с учетом случайных значений, сформированных путем их сохранения в логически выделенных «пулах» на основе корректного вычисления энтропии информации, поступающие из источников событий, внедрено в практическую деятельность ГУП «UNICON.UZ» (справка Министерства по развитию информационных технологий и коммуникаций от 5 октября 2018 года №33-8/7438). В результате научного исследования получена возможность постоянного обновления необходимых и надежных случайных ключей, которое обеспечивается при шифровании данных в специальном устройстве собирания данных;

программное средство, позволяющее генерировать различные случайные числа и ключи для криптографических инфраструктур, таких как симметричное шифрование, асимметричное шифрование и аутентификации -

внедрен в деятельность ООО «AlpCrypto» (справка Министерства по развитию информационных технологий и коммуникаций от 5 октября 2018 года №33-8/7438). В результате научного исследования разработанное программное средство в рамках набора тестов NIST Special Publication 800-22 позволило генерировать последовательности, имеющие 95,3% уровень случайности.

программное средство метода генерации криптографических ключей на основе отпечатки пальца, исключающее необходимость их запоминания и безопасного хранения, внедрено в деятельности предприятия «MironSoft» (справка Министерства по развитию информационных технологий и коммуникаций от 5 октября 2018 года №33-8/7438). В результате научного исследования программное средство, генерирующее 128 и 256-битные ключи с использованием отпечатков пальцев, позволило повысить эффективность генерирования ключей до 78%.

**Апробация результатов исследования.** Результаты данного исследования были обсуждены на 5 международных и 5 республиканских научно-практических конференциях.

**Публикация результатов исследования.** По теме исследования опубликованы всего: 21 научная работа, из них 8 статей в журнальных изданиях, рекомендованных Высшей аттестационной комиссией Республики Узбекистан, в том числе 2 - в иностранных и 6 - в республиканских журналах, а также получены 3 свидетельства о регистрации программных продуктов для ЭВМ.

**Структура и объем диссертации.** Диссертация состоит из введения, четырех глав, заключения, списка использованной литературы и приложения. Объем диссертации составляет 119 страниц.

## ОСНОВНОЕ СОДЕРЖАНИЕ ДИССЕРТАЦИИ

**Во введении** обосновываются актуальность и востребованность темы диссертации, показано соответствие с приоритетными направлениями развития науки и технологий Республики Узбекистан, формулируются цель и задачи, также объект и предмет исследования, изложены научная новизна и практические результаты исследования, обоснована достоверность полученных результатов, раскрыта их теоретическая и практическая значимость, приведен перечень внедрений в практику результатов исследования, сведения об опубликованных работах и структура диссертации.

Первая глава диссертации, озаглавленная как **«Проблемы управления криптографическими ключами»**, посвящена исследованию требований к криптографическим ключам и управления ими, анализ существующих угроз, возникающих в процессе управления ключами и существующих методов генерации криптографических ключей.

Методы генерации случайных последовательностей делятся на 3 класса: генераторы небезопасных случайных чисел, генераторы криптографических псевдослучайных чисел и накопители энтропии. В таблице 1 приведены

проблемы безопасности существующих генераторов ключей, относящийся к данным классам. Алгоритмы, относящие к первому классу, хотя они и считаются быстрыми, но у них цикл повторения является коротким. Алгоритмы, которые относят к второму классу принимают при входе фиксированных случайных чисел, на выходе создают последовательности с большой длиной. Накопители энтропии собирают значения из разных источников событий и в определенном моменте генерируют случайных ключей с фиксированной длиной. Этот ключ используется в качестве входного значения для генераторов криптографических псевдослучайных чисел.

**Таблица 1**

**Методы генерации случайных чисел**

| № | Метод генерации случайных чисел | Существующие недостатки |
|---|---|---|
| 1. | Генераторы небезопасных случайных чисел (функции rand() или random() в разных языках программирования) | - Небезопасно;<br>- Цикл повторения короткий; |
| 2. | Генератор криптографических псевдослучайных чисел (ANSI X9.17, BBS, ISAAC и др.) | - Низкая скорость;<br>- Использован алгоритм, который не считается стойким (например, MD5, SHA1 и др.) |
| 3. | Накопители энтропии (/dev/random, Fortuna, Yarrow и др.) | - Применен разные эвристические уравнения и гипотез, которые не доказаны или непроизведенные вычисления; |

Следует отметить, что существующие методы генерации криптографических ключей не могут вычислить конкретно энтропию случайной величины, а генераторы псевдослучайных чисел, разработанные на основе использования небезопасных криптографических алгоритмов не считаются наиболее быстрыми, к тому же они являются причиной увеличения угроз на ключи из-за требования необходимости безопасного хранения ключа пользователей.

Во второй главе диссертации **«Методы генерации криптостойких ключей»**, предложена модель угрозы и на ее основе разработан метод вычисления энтропии. Усовершенствован метод коррекции случайных значений операционных систем в «пулах», использующую безопасную и быструю хеш-функцию Blake2b, значения сохранены в «пулах» на основе одностороннего преобразования. Кроме того, предложен генератор псевдослучайных чисел, основанный на использования хэш-функций с ключом, генерирующий блочные симметричные шифры в режиме счетчика.

Для предложенной модели угрозы выбраны два типа злоумышленников: злоумышленник, который имеет возможность управлять (удаленно) сетевым сегментом и имеющий возможность пользоваться локальной сетью, но при

этом не имеет возможности пользоваться компьютером персонала. Для данных злоумышленников даны в определенной степени возможности и для каждого злоумышленника определены степень квалификации, такие как не профессионал, специалист и профессионал. Для квалификации злоумышленников первого типа уровень риска равен $\mu = \{0,16; 0,26; 0,34\}$, а для квалификации злоумышленников второго типа уровень риска равен $\mu = \{0,28; 0,34; 0,45\}$.

При этом выделены типы уровней влияния угроз, такие как высокий, средний и низкий. При этом вред, наносимый злоумышленником, вычисленный в соответствии с предложенной моделью угроз и генераторов случайных чисел соответственно равны $\sigma = \{1; 0,5; 0,1\}$. Типовые угрозы выбраны по методологии STRIDE (*Spoofing* - фальсификация, *Tampering* - изменение, *Repudiation* - отказ, *Information disclosure* – раскрытие информации, *Denial of service* – отказ в обслуживании, *Elevation of privilege* – несанкционированное получение прав). Их общая доля показана в таблице 2.

**Таблица 2**

**Доля типовых угроз на генераторов случайных чисел по методологии STRIDE**

| STRIDE фактор | S | T | R | I | D | E |
|---|---|---|---|---|---|---|
| Доля, ρ | 1/11 | 1/11 | 0 | 1/11 | 3/11 | 5/11 |
| Коэффициент воздействия, σ | 1 | 1 | 0,5 | 1 | 0,1 | 0,5 |
| Влияние степени угрозы на генератор случайных ключей, $\tau = \rho * \sigma$; | 1/11 | 1/11 | 0 | 1/11 | 3/110 | 25/110 |

В общем случае сумма долей угроз, рассчитанная по методологии STRIDE равна следующему:

$$\tau_{общ} = \sum_{i=1}^{k} \rho_i * \sigma_i$$

Риск ω на основе предложенной модели угроз на ресурсы с учетом квалификации злоумышленника описывается следующим уравнением:

$$\omega = \mu * \tau$$

При вычислении статистического числа энтропии использована минимал-энтропия (min-Entropy,$H_{min}$), которая предложена в издании NIST SP 800-90B для вычисления энтропии источников генерации случайных чисел. Для модели угроз, выбранной на основе данного метода вычисления суммарной энтропии можно описать следующим образом:

$$H_{итог,i} = (1 - \omega_i) * H_{min,i}$$

Для усовершенствования метода сбора в «пулы» случайных значений, существующие источники случайных ситуаций выделяются в отдельные логические группы и выходные значения с вычислением их энтропии с помощью хэш-функции Blake2b сохраняются в фиксированном виде (рис.1).

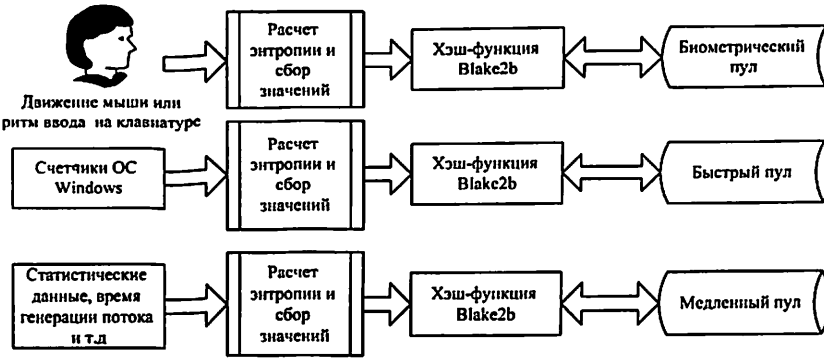



**Рис. 1. Запись случайных величин с вычислением энтропии на выделенные «пулы»**

На рисунке 2 приведен общий вид генератора псевдослучайных чисел, который создает криптостойкую последовательность, собранную в «пулы». Он основан на алгоритмах хэш-функции Blake2b с ключом и блочным симметричным шифрованием.

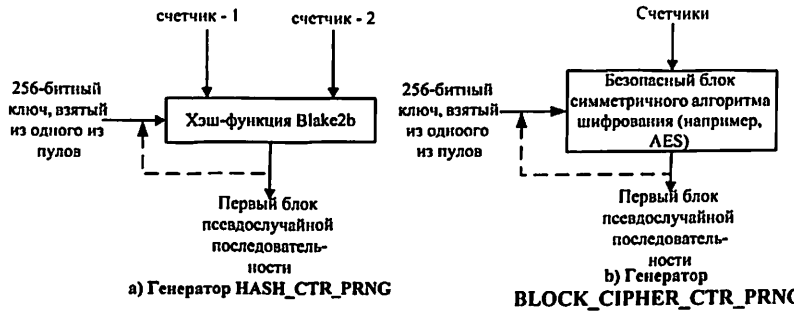



**Рис. 2. Общий вид предложенного генератора псевдослучайных чисел**

В предложенном генераторе псевдослучайных чисел вычисление одного ключа «пула» используется при создании $2^{16}$ блоков последовательностей, после каждой требуемой последовательности генерируется дополнительные блоки последовательностей для обновления ключа. В этом случае внутри $2^{16}$ блоков вероятность появления коллизии равна $2^{-97}$.

После обращения к генератору псевдослучайных чисел, изначально определяется текущее состояние генератора. Если текущее состояние генератора не соответствует к созданию требуемых случайных байтов, то генератор обновляется на основе быстрого «пула» и счетчик приведется к нулевом состоянию. Если персональный компьютер в котором работает генератор только что быль включен, то на основе биометрического «пула» состояние генератора обновляется. Если скоростной «пул» является в «загрязнённым» состоянии или требуется ключе для длительного

пользования, то состояние генератора обновляется на основе накопленной энтропии в медленном «пуле».

В третьей главе диссертации **«Методы и алгоритмы генерации эффективных ключей»** предложен эффективный метод и алгоритм генерации криптографических ключей на основе отпечатков пальцев, исключающий необходимость безопасного хранения ключей. В предложенном методе усовершенствован способ определения важных точек отпечатка пальца от фальсифицированных.

Методы генерации ключей, основанные на биометрических параметрах, отличаются от методов генерации ключей, основанных на паролях или токенах, при отсутствии требований безопасного хранения ключа.

Особо важным является при генерации ключей на основе биометрических параметров выбор соответствующих биометрических свойств. Поэтому, были проанализированы параметры отпечатка пальца, изображения лица, сетчатки глаза, геометрической формы руки и параметры голоса по критериям универсальности, уникальности, неизменности, собираемости, производительности, приемлемости, обход и необходимые устройства для процесса, а также их стоимость (при этом возможно существования каждого фактора на биометрическом параметре по следующим уровням высокий = 100, средний = 75 и низкий = 50). На основе полученных результатов анализа отпечатка пальца, и сетчатка глаза получили самый высокий 89,3% результат, но сканер отпечатка пальца, по сравнению со сканером сетчатки глаза, является более дешёвым. Кроме того, при проверке существование достаточной информации для ключа в биометрических параметрах для отпечатка пальца и сетчатки глаз диапазон ключа равен к $2^{14}$ и $2^{20}$, соответственно. Для разрабатываемого генератора ключа на основе биометрических данных выбран параметр отпечатка пальца на основе результатов анализа и с учетом удобности использования.

В предложенном методе генерации ключей, основанном на анализе отпечатка пальца, ключи создаются с использованием важных точек в изображении. Из изображения отпечатка пальца вместе с извлечением важных точек, отмечаются и фальсифицированные важные точки (рис 3).

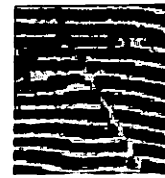
В результате для определения достоверных важных точек среди фальшивых этапов обработки изображения, процедура выявления фальсифицированных точек в отпечатке пальца усовершенствована на основе метода конечной обработки.

В результате вычисляются значения $alfa = |p_i(\alpha) - p_j(\alpha)|$ и $d = \sqrt{(x_i - x_j)^2 + (y_i - y_j)^2}$. Здесь: $alfa$ – угол между двумя важными точками, $d$ – Евклидово пространство между двумя важными точками.

Для определения фальшивых не соединенных линий должны быть выполнены следующие два условия: $alfa = 180$ и $d \geq 10$. Если данные условия выполняются, то считается, что две важные точки прошли проверку.

Для определения фальшивых важных точек, появляющихся в периферийных частях изображения, проверяется отсутствие черных точек в рамках $r = 10$ пикселя в соответствующую сторону от выбранной важной точки.

**a) извлеченные важные точки**



**b) фальшивые несвязанные линии**

**c) завершенные ложные гребни (линии) в верхней левой стороне**

**Рис. 3. Фальшивые важные точки в изображении отпечатка пальца**

На основе вышеприведенных условий среди важных точек выделяются необходимые точки. На основе выделенных важных точек при генерации криптографических ключей широко применяются схемы освобождения ключей, связывание ключей и генерация ключей. Схема связывания ключей по сравнению с другими, отличается возможностью обновления, а также генерации ключей с высоким значением энтропии.

Функциональная схема метода генерации криптографических ключей на основе предложенной схемы связывания ключей приведена на рисунке 4.

На основе предложенного метода по значению *n*, который является общим количеством важных точек, выделенных из изображения отпечатка пальца, возможно генерирование 128 ($15 \leq n < 21$) или 256 ($n \geq 21$) битные ключи. В обратной задаче невозможно генерировать ключи из изображений отпечатка пальца.

Так как биометрические параметры считаются нечеткими видами, существует отличия между двумя биометрическими образцами принадлежащие одному пользователю. При этом, для предотвращения ошибок на определенном уровне используется код Рида-Соломона, исправляющий такие ошибки. На основе предложенного метода, код исправления ошибок восстанавливает информацию о 3х важных точках отпечатка пальца. Для этого требуется минимум 12 соответствующих важных точек 128 битного ключа.

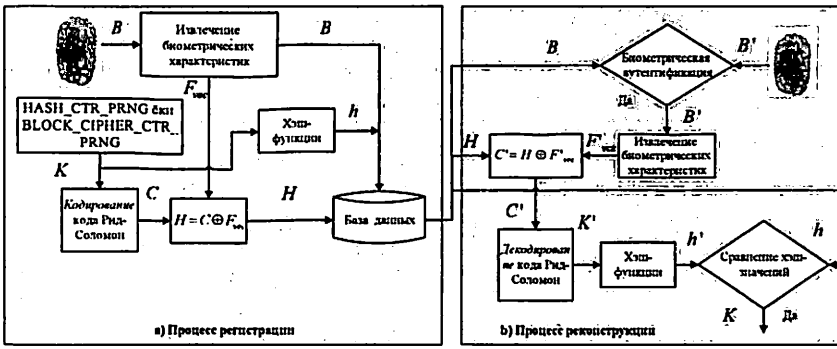
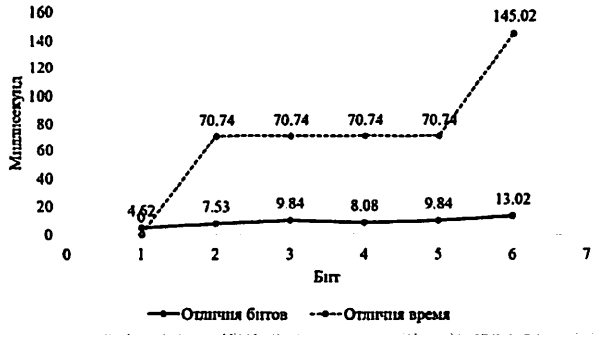


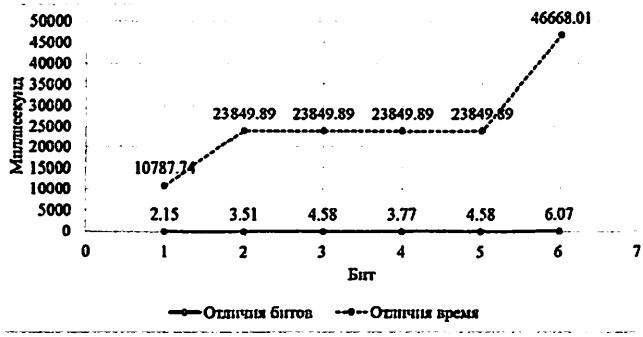

**Рис. 4. Функциональная схема метода связывания криптографических ключей**

В четвертой главе диссертации **«Оценка эффективности эффективных генераторов криптографических ключей»** оценена эффективность метода вычисления значений генератора случайных чисел, которая основана на предложенной модели угрозы, генератора псевдослучайных чисел и генератора ключа основанного на исследовании отпечатка пальца. На все предложенные в диссертации методы разработаны программные средства и проанализированы результаты, полученные при апробации в процессе их внедрения.

Зависимость различия количество битов от времени при вычислении энтропий на основе существующего метода и модели угроз приведены на рисунке 5. Разница самых больших битов для быстрого и медленного «пула» относится к профессиональному уровню второго вида злоумышленника, и разница потраченного времени на накопление энтропии с существующими составляет 145,02 мс и 46668,01 мс, соответственно.



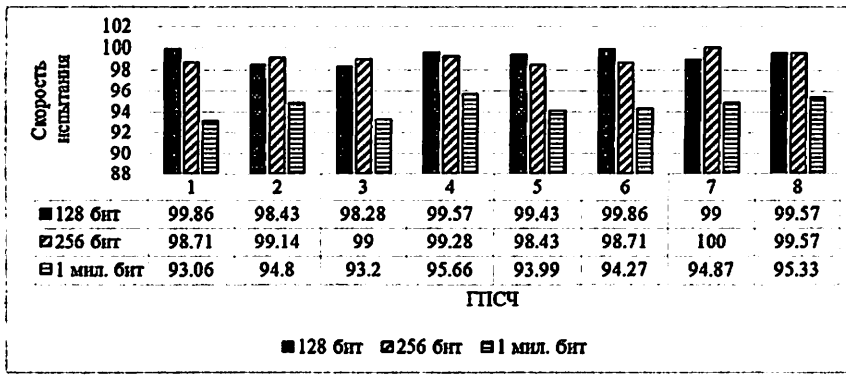

**а) для быстрого «пула»**




**b) для медленного «пула»**

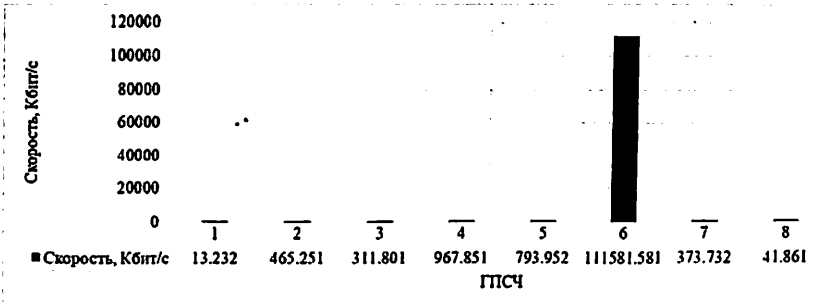
**Рис. 5. Зависимость различия количество битов от времени при вычислении энтропий на основе существующего метода и модели угроз**

Проведено сравнение предложенного генератора псевдослучайных чисел с существующими по нескольким алгоритмам, сопоставляющим уровни случайности, а также на основе набора тестов, опубликованного NIST Special Publication 800-22. Кроме того, сопоставлены свойства скорости и приведены сопоставительный анализ на рисунке 6. По уровню случайности для генерации 256 битных ключей получены самые высокие результаты (100% и 99,57%) с использованием генераторов HMAC CTR ГПСЧ и BLOCK CIPHER CTR ГПСЧ. Здесь можно увидеть высокие результаты, предложенные ГПСЧ и при генерации ключей с разными длинами. HMAC CTR ГПСЧ и BLOCK CIPHER CTR ГПСЧ показали более высокую скорость работы, по сравнению со существующими ГПСЧ (RSAREF ГПСЧ и ANSI X9.17 ГПСЧ), которые относятся к одному виду.




| | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
|---|---|---|---|---|---|---|---|---|
| 128 бит | 99.86 | 98.43 | 98.28 | 99.57 | 99.43 | 99.86 | 99 | 99.57 |
| 256 бит | 98.71 | 99.14 | 99 | 99.28 | 98.43 | 98.71 | 100 | 99.57 |
| 1 мил. бит | 93.06 | 94.8 | 93.2 | 95.66 | 93.99 | 94.27 | 94.87 | 95.33 |

**a) по уровню случайности**




**b) по быстродействию**

1 - ANSI X9.17 ГПСЧ
2 - DSA ГПСЧ
3 - RSAREF ГПСЧ
4 - OPENSLL ГПСЧ
5 - DEV/URANDOM ГПСЧ
6 - CRYPTGEN - RANDOM ГПСЧ
7 - HMAC CTR ГПСЧ
8 - BLOCK CIPHER CTR ГПСЧ

**Рис. 6. Сравнительный анализ предложенного генератора псевдослучайных чисел с существующими**

При тестировании предложенного генератора ключа основанного на исследовании отпечатка пальца, выбраны три вида баз отпечатков пальцев. В таблице 3 приведены общие результаты (False rejection rate, FRR – коэффициент ложного отказа в доступе, False acceptance rate, FAR – коэффициент ложного доступа).

**Таблица 3**

**Результаты анализа полученные на основе отпечатки пальцев**

| **Факторы** | **Cross Match Verifier 300 Classic** | **Digitalperso na U.are.U 4000 Scanner** | **Futronic FS88H** |
|---|---|---|---|
| Количество субъектов | 51 | 65 | 40 |
| Количество полученных изображений отпечатков пальца | 8 | 8 | 10 |
| Количество образцов, использованных для регистрации и восстановления ключа | 4/4 | 4/4 | 4/6 |
| Ошибки в процессе регистрации | 8/51 | 34/65 | 5/40 |
| Количество выделенных МР (Minutiae points) | 15 МР–8 шт.; 21 МР–35 шт.. | 15 МР–шт.; 21 МР–шт. | 15 МР–шт.; 21 МР–шт. |
| Ошибки FRR (%) | 12,209 | 19,354 | 22,00 |
| Среднее отличие точек МР | 1,633 | 1,991 | 2,271 |
| Ошибки FAR (%) | 0 | 0 | 0 |

По полученным результатам самая большая FRR ошибка относится к Futronic FS88H базе и в данном случае разница между числами важных точек из изображения отпечатков двух пальцев равна 2,271. А это означает, что использовав усовершенствованный код Рид-Соломона для исправления информации трех важных точек, существует возможность генерирования трех правильных ключей из четырех попыток. При этом прежде чем генерировать ключ, через реализации процесса аутентификации FAR ошибка приведена к нулю.

В таблице 4 приведены способности противостояния к угрозам предложенного метода генерирования ключа на основе отпечатка пальца, которые приведены в 3.2 разделе.

**Таблица 4**

**Анализ безопасности генераторов ключа основанные на отпечатка пальца**

| Вид атаки | Результат анализа |
|---|---|
| Атака грубой силы | - генерирует ключей с 128 и 256 битами и эти длины ключа является стойким к данной атаке. |
| Атаки, основанные на FAR ошибках | - по полученным результатам анализа FAR ошибка было равна к 0 и это означает стойкость к атаке. |
| Атаки направленные на коды исправления ошибок | - код Рид-Соломона предназначен на восстановление информации о не соответствующих трех важных точек из изображения отпечатки пальца. |
| Изменчивость биометрических свойств | - из-за ошибки FRR, который равен к 22,00%, доля не успешных попыток естественного пользователя равна среднем к 1/4. |
| Недостаточность информации для ключа | - реализована генерация на основе схемы нечеткого связывания (fuzzy commitment) 128 битных и 256 битных ключей. |
| Небезопасность биометрических параметров | - для правильной генерации ключа количества требуемых важных точек приравнен к 12 (для 128 битных ключей);<br>- использованы сканера которые проверяет живучесть пальцев. |

Создание 128 и 256 битных ключей на основе схемы нечеткого связывания, приравнивание к нулю ошибки FAR, существование минимум 12 важных точек для успешной генерации ключей, использование правильно настроенного кода Рид-Соломона и качественного сканера отпечатки пальца предоставляют возможность противостоять существующим атакам разработанного генератора ключа на основе отпечатка пальца.

## ЗАКЛЮЧЕНИЕ

Приведены следующие выводы в результате проведенных исследований по диссертационной работе на тему «Методы и алгоритмы генерации эффективных криптографических ключей»:

1. Разработаны модель угрозы и метод вычисления энтропии, основанный на модели для вычисления энтропии выходящих значений с генератора случайных чисел. Разработанный метод вычисления энтропии позволил корректно вычислить уровень случайности и минимизировать время, требуемое для вычисления.

2. Усовершенствован широко применяемый метод, основанный на «пулах» при сборе значений, приходящих из источников энтропии. Усовершенствованный метод сбора значений позволяет генерировать безопасные и длительно применяемые ключи, а также создавать новые случайные значения, даже если источники случайных чисел «загрязнены».

3. Разработан метод создания криптографических псевдослучайных чисел, генерирующий стойкие ключи на основе входящего случайного числа. Разработанный метод позволяет создавать случайные значения на высоком уровне за короткое время на основе обновления внутреннего состояния генератора и постоянного изменения входных значений.

4. Методы генерации псевдослучайных последовательностей при вычислении 256 битных ключей в рамках статистических тестов NIST Special Publication 800-22 показали более высокий уровень случайности, по сравнению с существующими (для HMAC CTR ГПСЧ 100% и для BLOCK CIPHER CTR ГПСЧ 99,57%) и дали возможность противостоять существующим угрозам.

5. Усовершенствован метод определения важных точек из изображения отпечатка пальца. Усовершенствованный метод позволил повысить эффективность генерации ключей на основе выделения настоящих точек среди фальшивых.

6. Разработаны метод и алгоритм генерации эффективных ключей на основе важных точек из изображения отпечатка пальца. Так как доля успешных попыток со стороны естественного пользователя является

достаточной при генерации стойких ключей, разработанный метод позволяет противостоять существующим угрозам.

SCIENTIFIC COUNCIL AWARDING SCIENTIFIC DEGREES
DSc.27.06.2017.T.07.01 AT TASHKENT UNIVERSITY OF
INFORMATION TECHNOLOGIES

TASHKENT UNIVERSITY OF INFORMATION TECHNOLOGIES

KHUDOYKULOV ZARIF TURAKULOVICH

# METHODS AND ALGORITHMS FOR EFFECTIVE CRYPTOGRAPHIC KEY GENERATION

05.01.05 – Methods and systems of information protection. Information security

DISSERTATION ABSTRACT OF THE DOCTOR OF PHILOSOPHY (PhD)
ON TECHNICAL SCIENCES

Tashkent-2018

**The theme of doctor of philosophy (PhD) on technical sciences was registered at the Supreme attestation commission at the Cabinet of Ministers of the Republic of Uzbekistan under number B2017.3.PhD/T353.**

The dissertation has been prepared at Tashkent University of Information Techologies.

The abstract of the dissertation is posted in three languages (Uzbek, Russian, English (resume)) on the website www.tuit.uz and on the website of «ZiyoNet» Information and educational portal www.ziyonet.uz.

| | |
|---|---|
| **Scientific adviser:** | **Ganiev Salim Karimovich**<br>doctor of technical sciences, professor |
| **Official opponents** | **Aloev Rakhmatillo Juraevich**<br>doctor of physical-mathematical sciences, professor |
| | **Tuychiev Gulom Numonovich**<br>doctor of physical-mathematical sciences |
| **Leading organization:** | **Scientific-Engineering and Marketing Researches Center «UNICON.UZ»** |

The defense will take place «21» december 2018 at 14 the meeting of Scientific council No. DSc.27.06.2017.T.07.01 at Tashkent University of Information Technologies (Address: 100202, Tashkent city, Amir Temur street, 108. Tel.: (+99871) 238-64-43, fax: (+99871) 238-65-52, e-mail: tuit@tuit.uz).

The dissertation can be reviewed at the Information Resourse Centre of the Tashkent University of Information Technologies (is registered under No256). (Address: 100202, Tashkent city, Amir Temur street, 108. Tel.: (+99871) 238-64-43, fax: (+99871) 238-65-52).

Abstract of dissertation sent out on «07» december 2018 y.
(mailing report No. 14 on «16» November 2018 y.).

**R.Kh. Khamdamov**
Chairman of the scientific council awarding scientific degrees, doctor of technical sciences, professor

**F.M. Nuraliev**
Scientific secretary of scientific council awarding scientific degrees, doctor of technical sciences, docent

**R.J. Aloev**
Chairman of the academic seminar under the scientific council awarding scientific degrees, doctor of physical-mathematical sciences, professor

## INTRODUCTION (abstract of PhD dissertation)

**The purpose of the research work** is to develop the methods and algorithms that give the possibility of effective cryptographic key generation with high accuracy randomness degree and do not require the need to remember and carry out.

**The object of the research work** is the generation of cryptographic keys used in cryptographic systems.

**The scientific novelty of the research work:**

a threat model was developed and, on its bases, a method allowing to correctly estimate the entropy of the generated sequences from the random number generator;

method of collecting in the pools values received by the random number generator, based on the allocation of logical groups of event sources was improved;

method and algorithm for pseudorandom number generator, based on the use of block encryption and hash functions with a key in the counter mode were proposed;

method of extracting information, which is important for the cryptographic key by identifying false among the minutiae points in the fingerprint image was improved;

method and algorithm for generating efficient cryptographic keys based on fingerprints, which allow to eliminate the need for their memorization and secure storage were worked out.

**Implementation of the research results.** On the basis of scientific results, using methods, algorithms and software for generating effective cryptographic keys by applying the developed threat model and entropy estimation method:

on the generation of effective cryptographic keys, «BIO KEY BINDING SYSTEM», «Trusted (Pseudo) random number generators» and «WIN RNG» software tools provided information on the applicability of SUE «UNICON.UZ» (Reference of SUE «UNICON.UZ» on November 7, 2018). As a result, it became possible to generate random keys based on entropy measurements obtained from event sources and, on its basis, to generate strong pseudorandom keys, as well as efficient key management;

software that allows you to generate keys based on random values generated by storing logically allocated pools based on the correct estimation of the entropy of information coming from event sources, implemented in the practical activities of SUE «UNICON.UZ» (Certificate No. 33-8/7438 as of October 5, 2018 the Ministry for Development of Information Technologies and Communications). As a result of scientific research, a special device that collects data, when encrypting data, is provided with necessary and reliable random keys and is given the opportunity to constantly update them;

software that allows you to generate various random numbers and keys for cryptographic infrastructures, such as symmetric encryption, asymmetric encryption and authentication implemented in the activities of LLC «AlpCrypto» (Certificate No. 33-8/7438 as of October 5, 2018 the Ministry for Development of Information Technologies and Communications). As a result of scientific research, the developed

software as part of the NIST Special Publication 800-22 test suite allowed us to generate sequences that have a 95,3% level of randomness;

software for generating cryptographic keys based on fingerprints, eliminating the need for their memorization and secure storage, was implemented in the activities of the enterprise «MironSoft» (Certificate No. 33-8/7438 as of October 5, 2018 the Ministry for Development of Information Technologies and Communications). As a result of scientific research, the software that generates 128 and 256-bit keys using fingerprints, allows you to increase the efficiency of key generation by up to 78%.

**The outline of the dissertation.** The dissertation consists of an Introduction, four Chapters, Conclusion, a list of References and Appendices. The volume of the dissertation is 119 pages.

## ЭЪЛОН ҚИЛИНГАН ИШЛАР РЎЙХАТИ
## СПИСОК ОПУБЛИКОВАННЫХ РАБОТ
## LIST OF PUBLISHED WORKS


1. Ganiev S.K., Khudoykulov Z.T., Islomov Sh.Z., Selection suitable biometrics for cryptographic key generators // TUIT BULLETIN. –Tashkent, 2016, №4 (40). – P. 80-92, (05.00.00; №10).

2. Ganiev S.K., Khudoykulov Z.T., Islomov Sh.Z., Current cryptographic key generation techniques analysis // TUIT BULLETIN. –Tashkent, 2016, №3 (39). – P. 79-88, (05.00.00; №10).

3. Ганиев С.К., Худойқулов З.Т., Кадиров М.М., Бармоқ изига асосланган биометрик – криптотизимларнинг таҳлили //ТошДТУ ХАБАРЛАРИ. –Тошкент, 2017, №4 – Б. 197-203, (05.00.00; №16).

4. Абдурахимов Б.Ф., Примкулов Б.Ш., Худойқулов З.Т., Алланов О.М., Симметрик блокли шифрлаш усулларининг таҳлили // ТошДТУ ХАБАРЛАРИ. –Тошкент, 2017, №2 – Б. 30-35, (05.00.00; №16).

5. Ganiev S.K., Khudoykulov Z.T., Islomov SH.Z., Fuzzy commitment for biometric template secrecy // TUIT BULLETIN. –Tashkent, 2015, №3 (35). – P. 172-179, (05.00.00; №10).

6. Khudoykulov Z.T., Islomov SH.Z., Khalmuratov O.U., Analysis and importance of error correcting codes for biometric template secrecy // TUIT BULLETIN. –Tashkent, 2015, №4 (36). – P. 111-117, (05.00.00; №10).

7. Ganiyev S.K., Khudoykulov Z.T., Halimtaeva I.U., Computer's source based (Pseudo) random number generation //2017 Information Science and Communications Technologies (ICISCT), -Tashkent, 2017. –P.1-6, (05.00.00; 31.10.2017 №243/3-сон раёсат қарори).

8. Khudoykulov Z.T., Islomov Sh.Z., Allanov O.M., Mardiyev U.R., A practical implementation of fingerprint based fuzzy commitment scheme // European Science Review, -Austria, Vienna, 2018, -№ (5-6) -P. 108-112 (05.00.00; №3).

9. Khudoykulov Z.T., Yusupov B.K., Comparative factors of key generation techniques //Information Science and Communications Technologies (ICISCT), International Conference on. – IEEE, Tashkent, 2016. – P. 1-3.

10. Ganiyev S.K., Khudoykulov Z.T., Biometric cryptosystems: Open issues and challenges //Information Science and Communications Technologies (ICISCT), International Conference on. – IEEE, Tashkent, 2016. – P. 1-3.

11. Xudoyqulov Z.T., Yusupov B.K., Cryptographic key generation based on biometrics: an overview // The International scientific conference «Perspectives for the development of information technologies ITPA 2015», - Tashkent, 2015, -P. 117-121.

12. Tashev K.A., Khudoykulov Z.T., Shazimov A.B., Comparative and analysis of biometric systems for cryptographic key generation // The International scientific

conference «Perspectives for the development of information technologies ITPA 2014», - Tashkent, 2014, -P. 104-108.

13. Karimov M.M., Tashev K.A., Islomov Sh.Z., Khudoykulov Z.T. Minimizing in Face Recognition Errors and Preprocessing Time // 4th International conference on application of information and communication technology and statistics in economy and education (ICAICTSEE – 2014). University of National and World Economy Sofia. – Bulgaria, October 24 – 25th 2014. – P. 212-216.

14. Xudoyqulov Z.T, Safarov A.R., Thinning algoritmlarining qiyosiy tahlili // «Муҳаммад Ал-Хоразмий издошлари» мавзусидаги Республика илмий-техникавий анжумани, Урганч, 2018. -Б. 272-275.

15. Худойқулов З.Т., Давронова Л.Ў., Биометрик криптотизимлар муаммолари // «Электрон ҳукумат тизимида ахборот хавфсизлиги муаммолари ва уларнинг ечимлари» мавзуси бўйича Республика семинари, Тошкент, 2017. -Б. 9-13.

16. Худойқулов З.Т., Назиров А.А., Криптографик калитларни бошқариш тизимларида мавжуд таҳдидлар // Республиканский семинар: «Информационная безопасность в сфере связи и информатизации. Проблемы и пути их решения», Ташкент, 2016, -С. 7-9.

17. Худойқулов З.Т., Назиров А.А., Криптографик калитларни бошқариш // Республиканский семинар: «Информационная безопасность в сфере связи и информатизации. Проблемы и пути их решения», Ташкент, 2016, -С. 10-11.

18. Ганиев С.К., Худойқулов З.Т., Биометрик криптотизимларнинг хавфсизлиги таҳлили // «Иқтисодиётнинг реал тармоқларини инновацион ривожланишида ахборот – коммуникацион технологияларининг аҳамияти» мавзусидаги Республика илмий – техник анжуман, Тошкент, 2017, - Б. 62-65.

19. Худойқулов З.Т.., Исломов Ш.З., Алланов О.М., Мардиев У.Р., Мавлонов О.Н. "Trusted (Pseudo) random number generators" // Дастурга гувоҳнома № DGU 04846, 27.10.2017.

20. Ганиев С.К., Худойқулов З.Т., Нормуминов Ф.Қ., Холимтоева И.У., Давронова Л.Ў., Имамалиев А.Т., Алланов О.М., Каримов А.А., Эшонқулов Н.Д. "WIN RNG" // Дастурга гувоҳнома № DGU 05402, 13.06.2018.

21. Ташев К.А., Иргашева Д.Я., Ахмедова О.П., Худойқулов З.Т., Исломов Ш.З., Мардиев У.Р., Алланов О.М., Остонов М.Б. "BIO KEY BINDING SYSTEM" // Дастурга гувоҳнома № DGU 05725, 24.10.2018.

Автореферат «Муҳаммад ал-Хоразмий авлодлари» илмий журнали таҳририятида таҳрирдан ўтказилди ва ўзбек, рус ва инглиз тилларидаги матнларини мослиги текширилди.

Бичими: 84x60 1/16. «Times New Roman» гарнитура рақамли босма усулда босилди.
Шартли босма табоғи: 2,5. Адади 100. Буюртма № 45.

«ЎзР Фанлар академияси Асосий кутубхонаси» босмахонасида чоп этилди.
100170, Тошкент, Зиёлилар кўчаси, 13-уй.