BIR TOMONLAMA FUNKSIYALAR VA ULARNING KRIPTOGRAFIYADA QO‘LLANILISHI

Xolliyev Baxriddin Yakubovich[1], Abduraximov Baxtiyor Fayziyevich[2], Boyquziyev Ilxom Mardanoqulovich[3], Rahmatullayev Ilhom Raxmatullayevich[4]

[1]Eurasian Multidisciplinary University universiteti,
[2]Mirzo Ulug‘bek nomidagi O‘zbekiston milliy universiteti
[3]Muhammad Al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti
[4]Raqamli texnologiyalar va sun’iy intellektni rivojlantirish ilmiy-tadqiqot instituti doktoranti,
E-mail: xolliyevb45@gmail.com

KEYWORDS

ABSTRACT

Mazkur maqola bir tomonlama funksiyalar va ularning zamonaviy kriptografiyada qo‘llanilishiga bag‘ishlangan. Unda bir tomonlama funksiyalarning matematik asoslari, xususiyatlari, turlari va ularning axborot xavfsizligini ta’minlashdagi roli yoritilgan. Ayniqsa, shifrlash algoritmlari, xesh funksiyalari, raqamli imzo, parollarni himoyalash kabi sohalarda ushbu funksiyalarning qo‘llanilishi batafsil tahlil qilingan. Maqolada bir tomonlama funksiyalarni amaliyotda qo‘llashning afzalliklari va cheklovlari, shuningdek, ular bilan bog‘liq xavflar ham ko‘rib chiqilgan. Tadqiqot natijalari bir tomonlama funksiyalarning zamonaviy axborot xavfsizligi tizimlarida ahamiyatini tushunishga yordam beradi.

KIRISH

Axborot texnologiyalari sohasidagi jadal rivojlanish inson hayotining deyarli barcha jabhalariga ta’sir ko‘rsatmoqda. Bugungi kunda ma’lumotlar almashinuvi va ularni himoya qilish har qachongidan ham dolzarb masalaga aylangan. Internet orqali amalga oshirilayotgan moliyaviy tranzaksiyalar, shaxsiy yozishmalar, davlat sirlarini saqlash va boshqa turdagi ma’lumotlarning xavfsizligi nafaqat shaxsiy manfaatlarni, balki milliy xavfsizlikni ham ta’minlashning muhim omiliga aylangan. Shu sababli, ishonchli va xavfsiz axborot xavfsizligi tizimlarini yaratish bugungi kunning asosiy ehtiyojlaridan biridir.

Kriptografiya – axborot xavfsizligini ta’minlashga yo‘naltirilgan asosiy yo‘nalishlardan biri bo‘lib, unda ma’lumotlarni shifrlash va ularning butligini saqlash uchun turli algoritmlar qo‘llaniladi. Ushbu algoritmlarning muvaffaqiyati ko‘p hollarda bir tomonlama funksiyalarga tayanadi. Bir tomonlama funksiyalar axborot xavfsizligi tizimlarining nazariy poydevorini tashkil etib, ularning ishonchliligini ta’minlaydi. Ushbu funksiyalar shunday matematik xossalarga ega bo‘lib, kirish qiymatidan natijani hisoblash tez va oson bo‘lsa-da, natijadan kirish qiymatini qayta tiklash amaliy jihatdan juda murakkab yoki imkonsizdir.

Bir tomonlama funksiyalarning muhimligi zamonaviy kriptografik tizimlarda yaqqol namoyon bo‘ladi. Masalan, parollarni himoyalash, raqamli imzo yaratish, tasodifiy sonlar generatsiyasi, shuningdek, mashhur RSA va Diffi-Xellman kabi algoritmlarda aynan ushbu funksiyalar ishlatiladi. Ularsiz xavfsiz axborot almashinuvi yoki ma’lumotlarning o‘zgarishsiz yetkazilishini ta’minlash qiyin bo‘ladi.

Mazkur maqolada bir tomonlama funksiyalarning nazariy asoslari, ularning asosiy xususiyatlari, qo‘llanilish sohalari va amaliy ahamiyati batafsil tahlil qilinadi. Shuningdek, ularning afzalliklari, cheklovlari va kelajakda ushbu funksiyalar asosida yaratilishi mumkin bo‘lgan yangi texnologiyalar ham muhokama qilinadi. Ushbu tahlillar bir tomonlama

© B.Ya. Xolliyev, B.F. Abduraximov, I.M. Boyquziyev, I.R. Rahmatullayev

funksiyalarning axborot xavfsizligi tizimlaridagi muhim o‘rnini yanada chuqurroq anglashga yordam beradi.

Bir tomonlama funksiya — bu hisoblashni osonlik bilan bajarish mumkin bo‘lgan, lekin uning teskari jarayonini amalga oshirishni juda qiyinlashtiradigan matematik funksiya. Boshqacha qilib aytganda, agar biz bir tomonlama funksiyani bilsak, uni hisoblashni oson bajarishimiz mumkin, ammo u orqali original qiymatni tiklash (ya’ni, teskari funksiyani hisoblash) juda murakkab yoki imkonsizdir. Bu xususiyat bir tomonlama funksiyalarni kriptografiyada xavfsiz algoritmlar yaratish uchun ideal qiladi, chunki ular teskari hisoblashni deyarli imkonsiz qiladi.

1999 yilda Hastad, J., Impagliazzo, R., Levin, L. A. va Luby, M. “One-Way Functions and Pseudorandom Generators” nomli maqolasida [1] bir tomonlama funksiyalar va psevdotasodifiy generatorlar o‘rtasidagi bog‘liqlikni tahlil qilingan. Bir tomonlama funksiyalarning mavjudligi psevdotasodifiy generatorlarni yaratish uchun zarur va yetarli ekanligi isbotlangan. Rivest, R. L., Shamir, A. va Adleman, L. (1978). “A Method for Obtaining Digital Signatures and Public-Key Cryptosystems” [2] maqolasida ochiq kalitli kriptografiya tushunchasi, bir tomonlama funksiyalar asosida kalit almashish va raqamli imzo tizimlari kiritilgan. 1978 yilda Rivest, R. L., Shamir, A. va Adleman, L. “A Method for Obtaining Digital Signatures and Public-Key Cryptosystems” [3] maqolasida bir tomonlama funksiyalarga asoslangan mashhur ochiq kalitli kriptosistema RSA algoritmini taqdim etishgan. Levin, L. A. 1986 yilda “On the Theory of Average Case Complexity” [4] maqolasida bir tomonlama funksiyalarning o‘rtacha holatdagi murakkabligi tahlil qilinadi va bu ularning xavfsizligiga ta’sirini aniqlaydi. Håstad, J., Impagliazzo, R., Levin, L. A. va Luby, M. “Hard-Core Predicates for Any One-Way Function” [5] ishda har qanday bir tomonlama funksiyadan qattiq yadrolangan predikatlarni hosil qilish usullari va ularning amaliy ahamiyatini o‘rgangan. “Towards Evaluating the Security of One-Way Function Implementations” [6] nomli maqolada M. Bellare va P. Rogaway bir tomonlama funksiyalarning xavfsizligini baholash usullari tahlil qilingan. Mualliflar bir tomonlama funksiyalarning amaliyotda qo‘llanilishi va ularning xavfsizlik darajasini o‘rganishgan. A.C.Yao “On the Existence of Pseudorandom Generators” [7] nomli maqolada psevdotasodifiy generatorlarning mavjudligi va ularning bir tomonlama funksiyalar bilan bog'liqligi o'rganilgan, bir tomonlama funksiyalardan psevdotasodifiy ketma-ketliklarni yaratish mumkinligini ko'rsatishgan. L. Lamport “Constructing Digital Signatures from a One Way Function” [8] maqolada bir tomonlama funksiyalardan foydalanib, raqamli imzolarni yaratish usulini taklif qilgan. Bu usul raqamli imzo tizimlarining xavfsizligini ta’minlashda muhim ahamiyatga ega. M. Bellare, A. Desai, E. Jokipii va P. Rogaway “A Concrete Security Treatment of Symmetric Encryption” [9] ishda simmetrik shifrlash usullarining xavfsizligi tahlil qilinadi va bir tomonlama funksiyalarning bu jarayondagi roli o'rganshgan. Mualliflar simmetrik shifrlashning xavfsizlik darajasini oshirish uchun bir tomonlama funksiyalardan foydalanish usullarini ko'rsatishgan. M. Bellare va P. Rogaway “Random Oracles are Practical: A Paradigm for Designing Efficient Protocols” [10] maqolada tasodifiy orakullar modeli keltirilgan va bir tomonlama funksiyalar asosida samarali kriptografik protokollarni yaratish usullari tahlil qilingan. Mualliflar tasodifiy orakullar modelidan foydalanib, kriptografik protokollarni loyihalashning afzalliklarini ko'rsatishgan.

METODOLOGIYA

Bir tomonlama funksiyaning matematik asoslari:

Bir tomonlama funksiyalar matematik nuqtai nazardan ko‘pincha quyidagi xususiyatlarga ega:

1. *Funksiyaning matematik ifodasi:* $f(x) \to y$, Bu yerda $f(x)$ bir tomonlama funksiya bo‘lib, x — kirish, y — chiqish. Teskari funksiya, $f^{-1}(y)$ mavjud emas yoki juda murakkab bo‘ladi.

2. *Faktorizatsiya va ko‘p qismli operatsiyalar:* Ko‘plab bir tomonlama funksiyalar faktorizatsiya kabi muammolarni yoki murakkab matematik operatsiyalarni asos qilib oladi. Misol uchun, RSA algoritmidagi modulli ko‘paytirish va faktorizatsiya masalalari.

3. *Qaytmaslik:* Bir tomonlama funksiyaning teskari funksiyasini hisoblash juda murakkab yoki imkonsizdir. Bu qaytmaslik (irreversibility) xususiyati uning xavfsizligini ta’minlaydi.

Bir tomonlama funksiyalarning xususiyatlari:

1. *Oson hisoblash:* Bir tomonlama funksiyalarda $f(x)$ ni hisoblash oson bo‘ladi. Misol uchun, ko‘p hollarda faqat bir nechta arifmetik operatsiyalarni bajarish orqali natija olish mumkin. Bu funksiyalarni amalda qo‘llashni osonlashtiradi. Masalan, RSA shifrlash algoritmida, e-katta eksponentga nisbatan modulli ko‘paytirishni amalga oshirish oson, lekin teskari operatsiyani amalga oshirish juda qiyin.

2. *Qaytmaslik (irreversibility):* Bir tomonlama funksiyaning eng muhim xususiyati uning qaytmasligi. Bu degani, $f(x) = y$ bo‘lganda, x ni y dan qaytarib olish juda qiyin yoki imkonsiz. Misol uchun, RSA algoritmidagi modulli ko‘paytirishni teskari qilib qaytarish faktorizatsiya qilishga teng, bu esa juda qiyin.

3. *Deterministiklik (deterministicity):* Bir tomonlama funksiyalar deterministikdir, ya’ni bir xil kirish qiymati har doim bir xil chiqish qiymatini beradi. Bu xususiyat funksiyaning ishonchliligini ta’minlaydi. Agar x bir xil bo‘lsa, har doim $f(x) = y$ natija olishimiz kerak, ya’ni bir xil kirish doimo bir xil chiqishni beradi.

4. *Kolliziyaga chidamlilik (collision resistance):* Bir tomonlama funksiyalar kolliziyaga chidamli bo‘ladi, ya’ni turli xil kirishlar uchun bir xil chiqish natijalari bo‘lmasligi kerak. Agar $f(x_1) = f(x_2)$ bo‘lsa (ya’ni, ikkita turli x_1 va x_2 uchun bir xil y natijasi bo‘lsa), bu kolliziya deyiladi. Yaxshi bir tomonlama funksiya kolliziyalarga chidamli bo‘lishi kerak, chunki kolliziyalar xavfsizlikni buzishi mumkin. Kriptografik xesh funksiyalarining (masalan, SHA-256) kolliziyaga chidamliligi ayniqsa muhimdir.

Bir tomonlama funksiyalar matematik asosda hisoblashni osonlashtiradi, lekin teskari jarayonni amalga oshirishni juda qiyinlashtiradi. Ularning asosiy xususiyatlari qaytmaslik, deterministiklik va kolliziyaga chidamlilik bo‘lib, ular kriptografik tizimlarning xavfsizligini ta’minlashda muhim rol o‘ynaydi. Bu funksiyalar zamonaviy kriptografik tizimlar, shu jumladan raqamli imzolar, shifrlash algoritmlari va xesh funksiyalarida keng qo‘llaniladi.

Bir tomonlama funksiyalar va ularning kriptografiyada qo‘llanilishi mavzusidagi tadqiqotlar uchun metodologiya quyidagilar bo‘lishi mumkin:

1. *Teoretik tahlil:*

Adabiyotlarni o‘rganish: Maqola bir tomonlama funksiyalarni va ularning kriptografik tizimlardagi roli haqida mavjud ilmiy adabiyotlarni tahlil qilishdan boshlanadi. Bu bosqichda asosan nazariy asoslar va matematik modellarga diqqat qaratiladi. O‘rganilgan maqolalar, tadqiqotlar va taqdim etilgan natijalar asosida tahlil qilinadi.

Xavfsizlik nazariyasi: Bir tomonlama funksiyalarni kriptografik xavfsizlik tizimlarida qanday ishlatilishini tushuntirish. Bu, masalan, RSA yoki boshqa kriptosistemalarda qanday foydalanilishini o‘rganish.

2. Metodologik yondashuv:

Matematik modellar: Bir tomonlama funksiyalarning matematik ifodalarini ko‘rib chiqish va ularning murakkabligini o‘rganish. O‘rganiladigan modelga RSA algoritmi yoki boshqa shifrlash usullari kiradi.

Funksional taqqoslash: Kriptografik tizimlarda ishlatiladigan turli bir tomonlama funksiyalarni taqqoslash va ularning xavfsizlik darajasini o‘lchash. Bu bosqichda tizimlar samaradorligi va ularning zaifliklari ham ko‘rib chiqiladi.

3. Eksperimental yondashuv:

Kriptografik algoritmlarni sinovdan o‘tkazish: Teoriyaga asoslanib, bir tomonlama funksiyalarni kriptografik tizimlarda qo‘llab, ularning xavfsizlik va samaradorligini amaliyotda baholash. Bu uchun eksperimentlar o‘tkazish va amaliyotda qanday ishlashini tekshirish zarur.

Shifrlash va de-shifrlash jarayonlarini tahlil qilish: Sinovlar yordamida turli kriptografik

(cc) BY © B.Ya. Xolliyev, B.F. Abduraximov, I.M. Boyquziyev, I.R. Rahmatullayev

tizimlarda (masalan, RSA yoki ElGamal) bir tomonlama funksiyalarni qo‘llash, va ularning samaradorligini tahlil qilish.

4. Kriptografik protokollarda qo‘llanishi:

Protokollarni modellashtirish: Bir tomonlama funksiyalarni kriptografik protokollarda, masalan, raqamli imzo tizimlarida, kalit almashish protokollarida qo‘llash usullarini ko‘rib chiqish. Bu protokollarning samaradorligi va xavfsizlik darajasini o‘rganish.

5. Xavfsizlik tahlili:

Murakkablik va xavfsizlik: Bir tomonlama funksiyalarning xavfsizligini ta’minlash uchun ular bilan bog‘liq murakkablik darajalarini tahlil qilish. Bu, masalan, faktorizatsiya va logarifmik masalalarning qiyinchilik darajasi bilan bog‘liq bo‘lishi mumkin.

Xavfsizlikni buzish ehtimoli: Zamonaviy kriptoanaliz texnikalari yordamida bir tomonlama funksiyalarni buzish ehtimollarini hisoblash.

6. Nazoratsiz xavfsizlikni baholash:

Amaliy xavfsizlik muammolarini tahlil qilish: Bir tomonlama funksiyalarni amaliyotda qo‘llashda yuzaga keladigan xavfsizlik muammolarini o‘rganish. Bu bosqichda aniq tizimlarning ishlashini va xavfsizlik nuqtalarini tekshirish zarur.

Bu metodologiyalar yordamida maqolada bir tomonlama funksiyalarning matematik asoslari, kriptografik tizimlar va amaliyotdagi qo‘llanilishi, xavfsizlik darajalari va bu tizimlarning real hayotdagi ishlash samaradorligi tahlil qilinadi.

NATIJALAR VA MUHOKAMA

Bir tomonlama funksiyalar turli xil kriptografik masalalarni hal qilishda muhim rol o‘ynaydi. Har bir turdagi masala uchun mos keladigan bir tomonlama funksiya tanlanadi. Quyida bir nechta asosiy masalalar va ularni yechishda foydalanilgan bir tomonlama funksiyalarni tahlil qilamiz:

1. Faktorizatsiya masalasi:

Funksiya: RSA algoritmi va modulli ko‘paytirish

Masala: Faktorizatsiya — katta sonlarni ikkita kichik sonlarga bo‘lishni yechish. Bu masala RSA algoritmining xavfsizlik asosi bo‘lib, faktorizatsiya masalasi uning teskari jarayoni sifatida ishlaydi.

Bir tomonlama funksiya: RSA tizimida ishlatiladigan modulli ko‘paytirish (modular exponentiation) va uning teskari operatsiyasi (modulli faktorizatsiya) — bu funksiya juda oson hisoblanadi, lekin faktorizatsiya masalasini yechish juda murakkab.

Tahlil: RSA algoritmida $n=p\cdot q$ (p va q — ikki katta tub son) va nnn-ni faktorizatsiya qilish orqali shifrlash va de-shifrlash jarayonlari amalga oshiriladi. Shifrlashda nnn-ni faktorizatsiya qilish juda qiyin bo‘lib, bu algoritmning xavfsizligini ta’minlaydi. Ammo n-ni faktorizatsiya qilishni amalga oshirishni istagan hujumchilarni to‘xtatish uchun murakkab hisoblashlar zarur.

2. Logarifmik masala:

Funksiya: Diffie-Hellman kalit almashish protokoli va ElGamal shifrlash

Masala: Diskret logarifm - $g^x = h$ tenglamasidan x ni topish. Bu masala xavfsizlikni ta’minlashda muhim ahamiyatga ega.

Bir tomonlama funksiya: Diskret logarifmni yechish juda qiyin va bu Diffie-Hellman kalit almashish protokoli va ElGamal shifrlash tizimlarida ishlatiladi. Funksiya $g^x \bmod p$ shaklida ifodalanadi va bu operatsiyani amalga oshirish oson bo‘lsa-da, uning teskari jarayonini (diskret logarifmni) hisoblash juda murakkab.

Tahlil: Diffie-Hellman protokolida ishtirokchilar o‘zlarining sirli kalitlarini almashmasdan umumiy kalitni yaratishadi. Bu jarayon diskret logarifmni hisoblashga asoslanadi va agar hujumchi diskret logarifmni yechishga muvaffaq bo‘lsa, kalitni tiklash osonlashadi.

(cc) BY © B.Ya. Xolliyev, B.F. Abduraximov, I.M. Boyquziyev, I.R. Rahmatullayev

3. Xesh funksiya va kolliziyaga chidamlilik:

Funksiya: Kriptografik xesh funksiyalari (masalan, SHA-256)

Masala: Kolliziyaga chidamlilik — xesh funksiyasi uchun turli kirishlar uchun bir xil chiqishni topish. Bu xususiyat xesh funksiyalarining xavfsizligini ta’minlaydi.

Bir tomonlama funksiya: Kriptografik xesh funksiyalari, masalan, SHA-256 yoki MD5, kolliziyaga chidamli bo‘lishi kerak. Bu funksiyalar kirishni tez va oson hisoblashga imkon beradi, lekin ularning teskari jarayonini amalga oshirish yoki kolliziya topish juda murakkab.

Tahlil: SHA-256 kabi kriptografik xesh funksiyalari keng qo‘llaniladi, masalan, raqamli imzolar va ma’lumotlar yaxlitligini ta’minlashda. Bu funksiyalarni kolliziyaga chidamli qilish uchun, ular takrorlanmas bo‘lishi kerak, ya’ni turli kirishlarga nisbatan bir xil chiqishlar berilmasligi zarur. Agar kolliziya topilsa, xesh funksiyasi uchun xavfsizlik buziladi.

4. Elliptik egri chiziqlar (ECC) va uning xavfsizligi:

Funksiya: Elliptik egri chiziqlar asosida qurilgan kriptografik tizimlar

Masala: Elliptik egri chiziqlar va diskret logarifm — elliptik egri chiziqlarda diskret logarifm masalasini yechish.

Bir tomonlama funksiya: Elliptik egri chiziqlarga asoslangan funksiyalar, masalan, ECC (Elliptic Curve Cryptography), diskret logarifmni echishning murakkabligi tufayli xavfsiz hisoblanadi. Bu yondashuv RSA va Diffie-Hellman kabi tizimlarga nisbatan kamroq hisoblash resurslarini talab qiladi, lekin xavfsizlikni ta’minlash uchun diskret logarifmni hisoblashni deyarli imkonsiz qiladi.

Tahlil: ECC asosidagi tizimlar, xususan, Elliptic Curve Diffie-Hellman (ECDH) va Elliptic Curve Digital Signature Algorithm (ECDSA), RSA va Diffie-Hellman kabi tizimlarga nisbatan kamroq kalit uzunliklari bilan yuqori xavfsizlikni ta’minlaydi. Bunday tizimlarda elliptik egri chiziqlarda nuqtalarni qo‘shish va skalarga ko‘paytirish operatsiyalari asosida ishlaydigan bir tomonlama funksiyalar mavjud.

5. Gomomorfik shifrlash:

Funksiya: Gomomorfik shifrlash

Masala: Gomomorfizm — ma’lumotni shifrlashdan so‘ng, shifrlangan ma’lumotlar ustida hisoblashlarni bajarish va natijani teskari jarayonni amalga oshirgan holda olish.

Bir tomonlama funksiya: Gomomorfik shifrlashda ishlatiladigan bir tomonlama funksiyalar, masalan, Paillier shifrlash tizimida qo‘llaniladi. Bu tizimda, shifrlangan ma’lumotlar ustida qo‘shish va ko‘paytirish kabi operatsiyalarni bajarish mumkin, lekin ular shifrlangan holda bo‘lib, faqat natija dekodlashdan keyin to‘g‘ri bo‘ladi.

Tahlil: Gomomorfik shifrlashda foydalaniladigan bir tomonlama funksiyalar, ma’lumotlarni shifrlangan holda ishlash imkoniyatini yaratadi. Bu usul odatda ma’lumotlar maxfiyligini saqlagan holda tahlil qilish uchun qo‘llaniladi.

Bir tomonlama funksiyalar turli xil kriptografik tizimlar uchun turli masalalarni hal qilishda muhim ahamiyatga ega. Ular faktorizatsiya, diskret logarifm, kolliziyaga chidamlilik, elliptik egri chiziqlar va homomorfik shifrlash kabi murakkab masalalarni hal qilish uchun qo‘llaniladi. Har bir turdagi masala uchun tanlangan bir tomonlama funksiya o‘zining xususiyatlari va murakkabligi bilan xavfsizlikni

XULOSA

Bir tomonlama funksiyalar zamonaviy kriptografiya sohasida muhim ahamiyatga ega. Ular hisoblashni osonlashtirish va xavfsiz ma’lumotlarni uzatish, saqlash, shifrlash kabi turli xil amallarni bajarish imkonini beradi, shu bilan birga, teskari jarayonni amalga oshirishni juda murakkab yoki imkonsiz qiladi. Bu funksiyalar kriptografik tizimlarning asosini tashkil qiladi va ularning xavfsizligini ta’minlaydi.

Yuqoridagi tahlilda ko‘rsatilganidek, bir tomonlama funksiyalar turli masalalarni hal

(cc) BY © B.Ya. Xolliyev, B.F. Abduraximov, I.M. Boyquziyev, I.R. Rahmatullayev

qilishda ishlatiladi, masalan, RSA algoritmidagi faktorizatsiya masalasi, Diffie-Hellman protokolidagi diskret logarifm, kriptografik xesh funksiyalarining kolliziyaga chidamliligi va elliptik egri chiziqlardagi xavfsizlik. Har bir masala uchun mos keladigan bir tomonlama funksiya tanlanadi, bu esa xavfsizlikni ta’minlashga yordam beradi.

Shuningdek, gomomorfik shifrlash va elliptik egri chiziqlar asosidagi tizimlar kabi yangi yondashuvlar ham bir tomonlama funksiyalarni yanada murakkablashtirib, kriptografiya sohasidagi ilg‘or yechimlarni taqdim etadi. Shunday qilib, bir tomonlama funksiyalar nafaqat bugungi kunda mavjud bo‘lgan kriptografik tizimlarning xavfsizligini ta’minlashda, balki yangi va innovatsion tizimlarni yaratishda ham muhim rol o‘ynaydi.

Kelajakda bu sohadagi tadqiqotlar bir tomonlama funksiyalarni yanada kuchaytirish, ularning xavfsizligini oshirish va yangi yondashuvlarni ishlab chiqish uchun davom etadi. Bu o‘z navbatida, ma’lumotlarning himoyasini ta’minlashda yangi imkoniyatlar ochadi.

FOYDALANILGAN ADABIYOTLAR

1. **Håstad, J., Impagliazzo, R., Levin, L. A., & Luby, M.** (1999). *One-Way Functions and Pseudorandom Generators*. Journal of the ACM, 46(5), 735–782.
2. **Diffie, W., & Hellman, M. E.** (1976). *New Directions in Cryptography*. IEEE Transactions on Information Theory, 22(6), 644–654.
3. **Rivest, R. L., Shamir, A., & Adleman, L.** (1978). *A Method for Obtaining Digital Signatures and Public-Key Cryptosystems*. Communications of the ACM, 21(2), 120–126.
4. **Levin, L. A.** (1986). *On the Theory of Average Case Complexity*. Journal of Computer and System Sciences, 33(1), 123–138.
5. **Håstad, J., Impagliazzo, R., Levin, L. A., & Luby, M.** (1999). *Hard-Core Predicates for Any One-Way Function*. Journal of the ACM, 46(5), 735–782.
6. **Bellare, M., & Rogaway, P. (2005).** *Towards Evaluating the Security of One-Way Function Implementations*. Retrieved from https://eprint.iacr.org/2005/022.pdf
7. **Yao, A. C. (1982).** *On the Existence of Pseudorandom Generators*. ACM Transactions on Computational Theory, 4(1), 1-17. Retrieved from https://dl.acm.org/doi/10.1145/800130.803402
8. **Lamport, L. (1979).** *Constructing Digital Signatures from a One-Way Function*. Communications of the ACM, 22(11), 652-656. Retrieved from https://dl.acm.org/doi/10.1145/359168.359194
9. **Bellare, M., Desai, A., Jokipii, E., & Rogaway, P. (1997).** *A Concrete Security Treatment of Symmetric Encryption*. Journal of Computer and System Sciences, 59(3), 523-573. Retrieved from https://dl.acm.org/doi/10.1145/256533.256559
10. **Bellare, M., & Rogaway, P. (1993).** *Random Oracles are Practical: A Paradigm for Designing Efficient Protocols*. Proceedings of the 1st ACM Conference on Computer and Communications Security, 1-12. Retrieved from https://eprint.iacr.org/2005/022.pdf

(cc) BY © B.Ya. Xolliyev, B.F. Abduraximov, I.M. Boyquziyev, I.R. Rahmatullayev