ISSN 3030-3346

OQIMLI SHIFRLASH ALGORITMLARI BARDOSHLILIGINI DIFFERENSIAL VA ALGEBRAIK KRIPTOTAHLIL USULLARI YORDAMIDA BAHOLASH

Rahmatullayev Ilhom Raxmatullayevich

Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti Samarqand filiali, E-mail: Ilhom9001@gmail.com

K E Y W O R D S

Kriptografik algoritmning bardoshliligi, entropiya, oqimli shifrlash, differensial kriptotahlil, algebraik kriptotahlil

A B S T R A C T

Mazkur maqolada shifrlash algoritmlari bardoshliligi masalalari, oqimli shifrlash nazariyasi va oqimli shifrlash algoritmlariga nisbatan qo'llaniladigan ayrim kriptotahlil usullari, xususan, differensial hamda algebraik kriptotahlil usullarining qo'llanilishi ikkita siljish registrlaridan iborat sodda oqimli shifrlash algoritmlari misolida yoritib berilgan.

Kirish

Kriptografik algoritmning bardoshliligi kriptotahlilchi maxfiy kalitni yoki shifrlangan ochiq matnni tiklash uchun bajarishi zarur bo'lgan hisob-kitoblar yoki talab qilinadigan resurslarning umumiy miqdorida ifodalanadi. Hisob-kitoblar ko'pincha shifrning hisoblash murakkabligi deb ataladi.

Mukammal himoyalangan shifrlash algoritmi uchun hisoblash murakkabligi kalit maydoni bilan bir xil bo'lib, ba'zan kalitning entropiyasi deb ataladi. Kalit maydoni barcha mumkin bo'lgan variantlar to'plamiga ishora qiladi va barcha maxfiy kalit bitlari yordamida kombinatsiyalarning umumiy sonini ifodalaydi. Kalitning o'lchami (kalit o'lchami) - bu to'liq kalit maydonining hajmini (2^n) ifodalaydigan n bitlar miqdori.

Maxfiy kalitni tiklashning eng sodda usuli bu barcha kombinatsiyalarni sinab ko'rishdir. Bunday metodologiya ko'pincha to'liq qidiruv yoki qo'pol kuch hujumi deb ataladi. Mazkur hujumda maxfiy kalitni aniqlash uchun deyarli 2^n ta variantni tanlash va hisoblash ishlarini bajarish zarur bo'ladi. Aniqroq qilib aytadigan bo'lsak, o'rtacha hisobda tahlilchi hisoblashlarning yarmida maxfiy kalitni aniqlashi mumkin, ammo bu oxirgi urinishlardan biri bo'lishi ham mumkin.

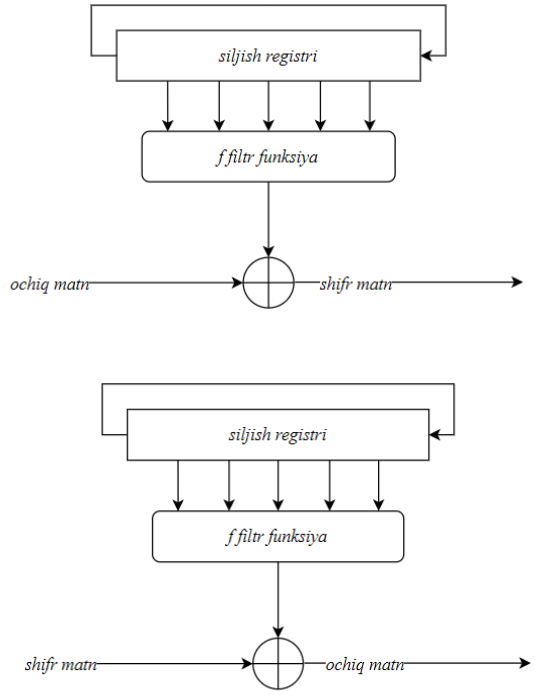
Mukammal xavfsiz bo'lgan shifrlash usuli xavfsiz kriptotizim uchun asos bo'lishi kerak. Amalda esa ko'pchilik shifrlash algoritmlari o'zlarining maxfiy kalitlarining to'liq entropiyasidan zaifroqdir. Hisob kitoblarni optimallashtirishlar yordamida ko'pincha haqiqiy entropiya talab qiladiganidan kamroq hisob-kitoblarni amalga oshirish orqali maxfiy kalitni topish mumkin. Bu shifrning haqiqiy hujum murakkabligi deb ataladi.

Oqim shifrlash bir martalik bloknot (OTP) shifrlash texnikasiga o'xshash shifrlashni amalga oshiradi. U maxfiy, tasodifiy ko'rinadigan ma'lumotlarning katta qismini ishlab chiqaradi va shifrlangan matnni yaratish uchun ularni ochiq matn bilan birlashtiradi. Ochiq matnni shifrlangan matndan ajratib bo'lmaydi. Tasodifiy ma'lumotlar maxfiy kalitdan olingan va odatda kalit oqimi deb ataladigan bitlar oqimini ifodalaydi. Oqimli shifrlash algoritmlarida maxfiy kalit tomonidan ishga tushiriladigan va har bir shifrlash bosqichidan so'ng keyingi holatga tarqaladigan ichki shifr holati deb nomlanadigan doimiy xotira mavjud. Bardoshli oqimli shifrlash algoritmlarining chiqishi Pseudo Random Number Generator (PRNG) tomonidan ishlab chiqarilgan bitlar oqimi bilan taqqoslanadi.

Oqimli shifrlash algoritmlarini ishlab chiqishda foydalaniladigan eng mashhur usullardan biri chiziqli bo'lmagan ikkilik ketma-ketliklarni

© *Rahmatullayev Ilhom Raxmatullayevich.*

ishlab chiquvchi generatorlardan foydalanishdir [1-5]. Ushbu generatorlar ikkilik kalitlar oqimini ishlab chiqaradi, bu juda katta maxfiy kalitni talab qilmasdan muntazam bir martalik shifrlash imkonini beradi. Chiziqli bo‘lmagan oqim shifriga asoslangan odatiy kriptotizimning umumiy ko‘rinishi 1-rasmda tasvirlangan. Ushbu turdagi shifrlarni kichik apparat ko‘rinishida amalga oshirish imkoniyati sababli juda mashhur hisoblanadi.



1-rasm. Oddiy chiziqsiz oqimli shifrlash tizimi sxemasi

1-rasmda ko‘rsatilgan kriptografik algoritm shifrning ichki holatini ifodalovchi aylanuvchi siljish registrini o‘z ichiga oladi. Kalitning har bir bitini hisoblashdan so‘ng, ichki funksiya ko‘proq entropiyani saqlab qolish maqsadida chiziqli funktsiya orqali ichki holatni yangilaydi. Chiqish komponenti keyingi kalit oqimi bitini hisoblash uchun chiziqli bo‘lmagan $f(\cdot)$ filtr funksiyasini qo‘llaydi. Kalit oqim bitlari XOR ($\oplus$) operatsiyasi bilan, jo‘natuvchi tomonidan ochiq matn bitlarini shifrlash uchun ishlatiladi (1a-rasm). Olingan shifrlangan matn xavfsiz bo‘lmagan kanal orqali uzatiladi. Qabul qiluvchi (1b-rasm) aynan bir xil hisob-kitoblarni amalga oshiradi va kalit oqimi bitlari bilan birgalikda shifrlangan matn bitlaridan ochiq matnni hosil qilish uchun XOR operatsiyasini qo‘llaydi. Shifrlangan matnga allaqachon kiritilgan kalit oqimi bitlari bekor qilinadi va qabul qiluvchida ko‘rinadi asl ochiq matn bitlari hosil bo‘ladi.

Adabiyotlarda kriptotahlil deb ataladigan oqimli shifrlash algoritmlariga nisbatan kriptografik hujumlarda qo‘llaniladigan ko‘plab ilg‘or va murakkab kriptografik hujum metodologiyalari va usullari taklif qilingan [6-14]. Mazkur maqolada oqimli shifrlash algoritmiga nisbatan kriptotahlil usullarining qo‘llanilish texnikalari yoritilgan.

Asosiy qism

1977 yilda joriy etilgan ma'lumotlarni shifrlash standarti (DES) ko‘p yillar davomida nazariy jihatdan xavfsiz deb hisoblangan. Bu ishonch 1991 yilgacha davom etdi, Biham va Shamir o‘zlarining [15] ishida DESga o‘xshash shifrga kriptografik hujum qilish mumkinligini ko‘rsatdi. Ular differensial kriptoanaliz sifatida joriy qilgan yangi hujum texnikasidan foydalanishgan.

DES ning dastlabki arxitekturasi uchun mas'ul bo‘lgan IBM kompaniyasi [16] ushbu maxsus hujum texnikasi bilan 15 yildan ko‘proq vaqt davomida tanish ekanliklarini da'vo qilishgan, bundan tashqari, ular DESda differensial kriptotahlilni imkon qadar oldini olish uchun o‘z bilimlaridan foydalanganliklarini ta’kidlashgan.

Oradan ikki yil o‘tgach, Biham va Shamir DES kriptografik algoritmiga nisbatan maxsus hujumni amalga oshirish bo‘yicha tadqiqot natijalarini [17] nashr etdilar. Hujum juda katta miqdordagi to‘plangan ma'lumotlarni talab qiladi va shuning uchun natijalar faqat nazariy hisoblangan. Lekin ularning ushbu tadqiqoti ko‘plab tadqiqotchilarni blokli shifrlar [18, 19, 20] va oqimli shifrlar [21, 22, 23] uchun differentsial hujum texnikasini yanada o‘rganish va optimallashtirishga ilhomlantirdi.

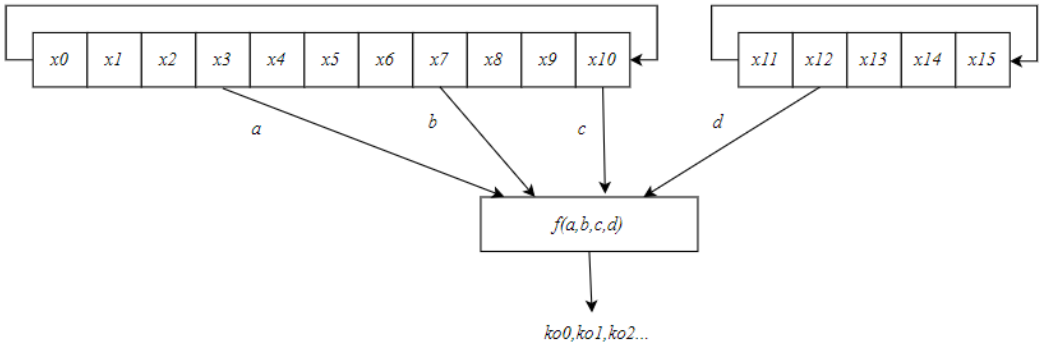
Differensial kriptotahlilning qo‘llanilishi ko‘p jihatdan ma'lum darajada farq qiladigan o‘xshash shifrlashlar to‘plamini yig‘ish imkoniyatiga bog‘liq. To‘g‘ridan-to‘g‘ri yondashuv shifrning ichki holatini to‘g‘ridan-to‘g‘ri ta'sir qiladigan va ozgina

(cc) BY © Rahmatullayev Ilhom Raxmatullayevich.

o‘zgartiradigan usulni topishdir. Bunday texnikani amaliyotda qo‘llash uchun ko‘pincha kriptotizimlarning qo‘shimcha komponentlari qasddan ichki holatda kerakli farqni hosil qilish uchun ishlatiladi. Bunday komponentlarga misol sifatida ichki holatni ishga tushirish tartibi, kalitlarni generatsiya qilish sxemalari va tasodifiy sonlar generatorlari kiradi. Ushbu komponentlarni nazorat qilish orqali tahlilchi ko‘pincha kerakli o‘zgarishlarni oldindan aytib berishi va oldindan hisoblashi mumkin.

Shifrni ishga tushirish protsedurasi tahlilchiga ma'lum bir pozitsiyada bitta ichki holat bitini o‘zgartirishga imkon berishi mumkin. Bunday kichik o‘zgarish to‘g‘ridan-to‘g‘ri boshqa chiqishga olib kelishi mumkin, bu o‘zgartirilgan bit filtr funktsiyasi uchun muhim kirish ekanligini ko‘rsatadi. Agar o‘zgarish mos keladigan kalit oqimi bitiga ta'sir qilmasa, bu bit filtrlash funktsiyasi uchun ahamiyatsiz kirish ekanligini ko‘rsatadi.

2-rasmda tasvirlangan chiziqli bo‘lmagan oqimli shifrlash algoritmi chiziqsiz filtr funksiyasidan foydalanadi.



2-rasm. Chiziqsiz oqimli shifrlash algoritmi

Chiziqsiz $f: F_4 \to F_2$ filtr funksiyasining ifodalanishi:

$$f(a,b,c,d) = (\bar{a} \wedge b) \oplus \bar{c} \oplus d$$

Ko‘pgina kriptotizimlar shifrlashga yangilik kiritish uchun tasodifiy qiyinchiliklardan foydalanadilar. Ushbu misolda muammolar 16-bitli tasodifiy qiymatdan iborat bo‘lib, u *nonce n* deb ataladi. Bundan tashqari, registrlarga *k* bitlari *nonce n* bilan XOR amali yordamida yuklanadi. Aniqroq aytganda, ishga tushirish $k_i \oplus n \to x_i$ $(i \in \{0, \ldots, 15\})$ifoda yordamida amalga oshiriladi.

Kriptotizimga nisbatan ikkita qo‘shimcha hujum vektori amalga oshiriladi. Tahlilchi n ustidan to‘liq nazoratga ega va u autentifikatsiyaga urinishdan istalgan vaqtda oddiy kalit oqimini chaqirishi va kuzatishi mumkin. Bu unga differensial kriptoanalizni quyidagi tarzda amalga oshirish imkonini beradi. Birinchidan, u $nonce\ n$ yordamida autentifikatsiya qiladi va birinchi hisoblangan kalit oqimi biti ko_0 ni aniqlaydi. Shundan so‘ng, tahlilchi $nonce\ n$ ning to‘rtinchi biti n_3 ni taxmin qiladi va muqobil n' ni aniqlashga harakat qiladi. Keyin, u n_3 bilan qayta autentifikatsiya qiladi va hisoblangan ko_0' bitini avval aniqlangan kalit oqimi biti ko_0 bilan solishtiradi.

Ikkita autentifikatsiyadan so‘ng, raqib x_3 ning haqiqiy qiymatini tiklay olmaydi. Biroq, u ikkita autentifikatsiya seansining ichki holati o‘rtasidagi farq x_3 bitini inkor qilish ekanligini aniqladi. Bundan tashqari, x_3 biti filtr funksiyasiga a kirishini ifodalaydi, bu esa o‘z navbatida ko_0 va ko_0' autentifikatsiyalari uchun birinchi kalit oqimi bitini hisoblash uchun ishlatiladi. E'tibor bering, x_3 bilan ifodalangan b kirish $n_7 = n_7'$ bo‘lganligi sababli $nonce$ tomonidan o‘zgartirilmagan. Xuddi shu narsa $nonce$ning to‘rtinchi biti o‘zgartirilganligi sababli c va d kirishlari uchun ham amal qiladi.

Filtr funksiyasining kirish-chiqish munosabati a kirish qiymati faqat b kiritish rost bo‘lgandagina muhimligini ko‘rsatadi. Birinchi kalit oqimi biti a

© Rahmatullayev Ilhom Raxmatullayevich.

kirish sifatida berilgan x_3 va b kirish sifatida esa x_3 bilan hisoblanadi. Shunday qilib, x_3 faqat $x_7 = 1$ bo'lganda ko_0 kalit oqimi bitiga ta'sir qiladi. Agar $ko_0 = ko_0'$ bo'lsa, tahlilchi $x_7 = 0$ degan xulosaga kelishi mumkin. Xuddi shunday, $ko_0 \neq ko_0'$ bo'lsa $x_7 = 1$ deb xulosa qilish mumkin.

Xulosa qilib aytganda, mazkur shifrga differensial hujum oddiygina to'rtinchi bitni taxmin qilib, qayta autentifikatsiya qilishda ishlatish orqali o'tkazilishi mumkin. Ikkala autentifikatsiyada birinchi hisoblangan kalit oqimi biti o'rtasidagi kuzatilgan farqlar x_7 qiymatini ochib beradi. n_7 va x_7 ni bilgan holda, maxfiy kalitning k_7 biti ni oddiygina $k_7 = x_7 \oplus n_7$ hisoblash orqali tiklash mumkin.

Ushbu maxsus misol faqat ikkita autentifikatsiyani amalga oshirish va ahamiyatsiz hisoblash murakkabligi bilan maxfiy kalitning bir bitini qanday tiklashni ko'rsatadi. Oqimli shifrlash jarayoni muntazam ravishda davom etganligi sababli, maxfiy kalitning ko'proq bitlarini tiklash uchun xuddi shu usuldan takroran foydalanish mumkin. n_4 bitini bir marta o'zgartirish va ko_0 dagi farqni kuzatish x_8 ni aniqlash mumkin.

Differensial kriptotahlil maxfiy kalitni qayta tiklashning samarali usullaridan hisoblanadi. Ehtiyotsiz ishlab chiqilgan ba'zi kriptotizimlar shu qadar zaifki, ularga differensial hujumni amaliy qiyinchiliklarsiz qo'llash ham mumkin. Masalan, [24,25] va [26-28] da taqdim etilgan MIFARE Classic va iClass shifrlash algoritmlari amaliy differensial hujumga amaliy hisoblashlar darajasida zaifdir. Ikkala algoritm ham kirishni hisoblangan chiqish maxfiy kalit haqidagi ma'lumotlarni sizdiradigan ko'rinishda manipulyatsiya qilishga imkon beradi.

Differensial hujum ko'pincha ma'lum kirish-chiqish farqlarini talab qiladi. Kriptotizimni ishga tushirish har doim ham raqibga ichki holatda bunday farqlarni qo'llashga imkon bermasligi mumkin. Shunga qaramay, har doim bog'liqliklarni aniqlash va oldindan belgilangan shartlarga javob beradiganlarni filtrlash imkoniyati mavjud. Bundan tashqari, tug'ilgan kun paradoksiga ko'ra [29], tahlilchi hujumni muvaffaqiyatli amalga oshirish uchun to'plashi zarur bo'lgan bog'liqliklar soni odatda his qilinadigan raqamlardan ancha kichikroq.

Bir qancha kriptotahlil usullarining metodologiyalari chiziqli bo'lmagan funksiyaga hujum qilish orqali oqimli shifrlash algoritmlarining hisoblash murakkabligini kamaytirishga qaratilgan. Biroq, ba'zi algoritmlari bir yoki bir nechta chiziqli komponentlardan iborat. Bunday shifrlash algoritmlari algebraik kriptotahlil hujumlariga nisbatan zaifdir. [30-33] ishlarda algebraik hujumlarga oid bir qancha dastlabki tadqiqotlar natijalari keltirilgan. So'nggi o'n yillikda hujumlarni umumlashtirish va optimallashtirishning bir nechta usullari taklif qilingan [34-42].

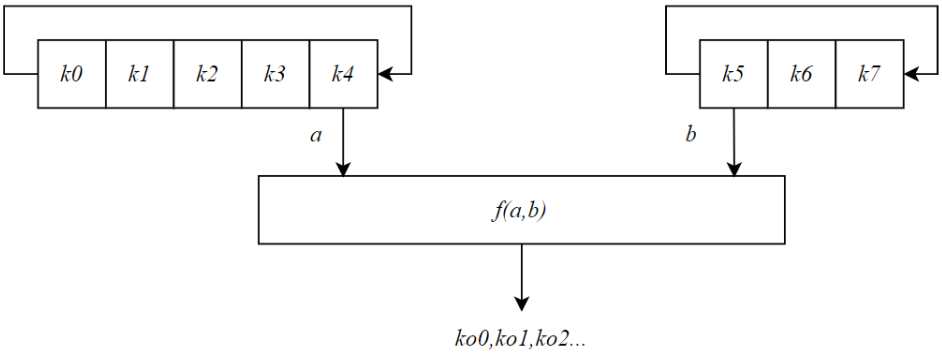
Chiziqli mantiqiy funksiyaning asosiy xususiyati baholashni kechiktirish imkoniyatidir. Kriptotahlil vaqtida rasmiylashtiriladigan hisoblash muammolarini mantiqiy tenglamalar tizimi sifatida tasvirlash mumkin [43]. Natijalarni to'g'ridan-to'g'ri hisoblash o'rniga, bu tenglamalarning kombinatsiyasini esa tenglamar sistemasini yechishning Gauss usuli kabi taniqli texnikalar yordamida yechish mumkin [44-45].

Mantiqiy algebraga ko'ra $f \in F_2$ funksiya o'z sohasidagi istalgan (x, y) juftlik elementlar uchun $f(x \oplus y) = f(x) \oplus f(y)$ tenglikni qanoatlantirsa chiziqli bo'ladi. Bundan tashqari, mantiqiy chiziqli funksiya kirish o'zgaruvchilari har doim yoki hech qachon chiqishga ta'sir qilmasligini belgilaydi. Shunday qilib, chiziqli funksiya tomonidan hisoblangan chiqish bitlarini kuzatish kirish bitlarining mos keladigan o'zgarishlari orasidagi chiziqli munosabatni ochib beradi. Ta'sir qilingan chiqish bitlarining ketma-ketligi kirish bitlari sonidan oshib ketganda, tenglamalar tizimini murakkab hisob-kitoblarni bajarmasdan hal qilish kifoya. Aksincha, chiziqli bo'lmagan funksiya teskari jarayonni qiyinlashtiradi, chunki alohida kirish bitlarining ta'siri ushbu bitlarning haqiqiy qiymatiga bog'liq. Chiziqli funksiyadan farqli o'laroq, har bir kirish uchun amal qiladigan chiziqli bo'lmagan funksiyalar uchun tenglamalarni umumlashtirish ancha qiyin hisoblanadi.

(cc) BY © Rahmatullayev Ilhom Raxmatullayevich.

ISSN 3030-3346

3-rasmda ko‘rsatilgan chiqish bitini chiziqli funksiya yordamida hisoblashga asoslangan shifrlash algoritmiga nisbatan algebraik kriptotahlil o‘tkazish jarayonini ko‘rib chiqamiz. U ikkita juda kichik bit bo‘yicha siljish registrlaridan iborat bo‘lib, ularning ikkalasi ham keyingi kalit oqimi bitini ishlab chiqarish uchun chiziqli filtr funktsiyasi $f(\cdot)$ ga bitta kirish bitini etkazib beradi.



3-rasm. Filtr funksiyasi chiziqli bo‘lgan oqimli shifrlash algoritmi

$f: F_4 \to F_2$ filtr funksiyasining ifodalanishi:

$$f(a,b) = a \oplus b$$

XOR operatori bitlar ustida amalga oshriladigan chiziqli amal bo‘lib, tahlilchiga tenglamalar tizimini tuzishga imkon beradi. Quyidagi $ko_0 ko_1 ko_2 ko_3 ko_4 ko_5 ko_6 ko_7 =$ *10110101* kalit oqimi bitlarini ko‘rib chiqamiz. 1-jadval to‘rtta ustundan iborat bo‘lib, ularning har biri baholash bosqichini ifodalaydi. Uch bosqichdan so‘ng, ko‘rib chiqilgan kalit oqimiga mos keladigan sakkizta tenglik hosil bo‘ladi. Ushbu tengliklar maxfiy kalit bitlarini ifodalaydigan tenglamalarda foydalaniladi.

1-jadval.

$ko_0 \dots ko_7 = 10110101$ chiqishga nisbatan algebraik tenglamalarni shakllantirish

$ko_0 = k_2 \oplus k_5$	$k_5 = k_2 \oplus ko_0$	$k_5 = k_2 \oplus 1$	$k_5 = \overline{k_2}$
$ko_1 = k_3 \oplus k_6$	$k_6 = k_3 \oplus ko_1$	$k_6 = k_3 \oplus 0$	$k_6 = k_3$
$ko_2 = k_4 \oplus k_7$	$k_7 = k_4 \oplus ko_2$	$k_7 = k_4 \oplus 1$	$k_7 = \overline{k_4}$
$ko_3 = k_0 \oplus k_5$	$k_5 = k_0 \oplus ko_3$	$k_5 = k_0 \oplus 1$	$k_5 = \overline{k_0}$
$ko_4 = k_1 \oplus k_6$	$k_6 = k_1 \oplus ko_4$	$k_6 = k_1 \oplus 0$	$k_6 = k_1$
$ko_5 = k_2 \oplus k_7$	$k_7 = k_2 \oplus ko_5$	$k_7 = k_2 \oplus 1$	$k_7 = \overline{k_2}$
$ko_6 = k_3 \oplus k_5$	$k_5 = k_3 \oplus ko_6$	$k_5 = k_3 \oplus 0$	$k_5 = k_3$
$ko_7 = k_4 \oplus k_6$	$k_6 = k_4 \oplus ko_7$	$k_6 = k_4 \oplus 1$	$k_6 = \overline{k_4}$

1-jadvalda ko‘rsatilgan tengliklardan quyida keltirilgan ikkita (1) va (2) tenglamalarni hosil mumkin.

$$k_6 = k_3 = k_1 = k_5 = k_7 \qquad (1)$$

$$\overline{k_6} = k_4 = k_2 = k_0 \qquad (2)$$

Ushbu tenglamalar maxfiy kalit bitlarining ikkita to‘plami mavjudligini ko‘rsatadi. Bitta to‘plamdagi barcha elementlar bir xil qiymatga ega (barchasi nol yoki barchasi bir). Biroq, har ikkala to‘plam bir-biriga qarama-qarshi qiymatni ifodalaydi, bu k_6 birinchi to‘plamning elementi va uning to‘ldiruvchisi $\overline{k_6}$ ikkinchi to‘plamning elementi ekanligi bilan tasdiqlanadi.

Tenglama (1) va (2) tenglamaga ko‘ra, faqat ikkita $k_0 k_1 \dots k_7 =$ *10101000* to‘plam yoki uning bitlari to‘ldiruvchilaridan iborat $k_0 k_1 \dots k_7 =$

(cc) BY © Rahmatullayev Ilhom Raxmatullayevich.

Recommended by: B.Mo'minov

01010111 to‘plam yechim bo‘lishi mumkin,. Tenglamalarni baholash uchun hisoblash murakkabligi ahamiyatsiz. Biroq, talab qilinadigan haqiqiy murakkablik, kalit oqimi bitlarini baholash, tengliklarni shakllantirish, keraksizlarini belgilash va yakuniy tenglamalarni shakllantirishni o‘z ichiga oladi. Bunday vazifalarni hisoblashning murakkabligi nuqtai nazaridan umumlashtirish ancha qiyin bo‘lsada bunday harakatlarni samarali optimallashtirish uchun bir nechta variantlar mavjud.

Xulosa

Mazkur maqolada shifrlash algoritmlari bardoshliligi masalalari, oqimli shifrlash nazariyasi va oqimli shifrlash algoritmlariga nisbatan qo‘llaniladigan ayrim kriptotahlil usullari, xususan, differensial hamda algebraik kriptotahlil usullarining qo‘llanilishi ikkita siljish registrlaridan iborat sodda oqimli shifrlash algoritmlari misolida yoritib berilgan. Keyingi tadqiqot ishlarida mazkur tahlil usullari yordamida murakkab oqimli shifrlash algoritmlarini baholash ko‘zda tutilgan.

Foydalanilgan adabiyotlar

1. Whitfield Diffie and Martin E Hellman. Privacy and authentication: An introduction to cryptography. Proceedings of the IEEE, 67(3):397–427, 1979.
2. S.W. Golomb. Shift Register Sequences. Holden-Day Series in Information Systems. Holden-Day, 1967.
3. El Groth. Generation of binary sequences with controllable complexity. IEEE Transactions on Information Theory, 17(3):288–296, 1971.
4. Edwin Key. An analysis of the structure and complexity of nonlinear binary sequence generators. IEEE Transactions on Information Theory, 22(6):732–736, 1976.
5. Vera S Pless. Encryption schemes for computer confidentiality. IEEE Transactions on Computers, 100(11):1133–1136, 1977.
6. Eli Biham and Adi Shamir. Differential fault analysis of secret key cryptosystems. In 17th International Cryptology Conference, Advances in Cryptology (CRYPTO 1997), volume 1294 of Lecture Notes in Computer Science, pages 513–525. Springer-Verlag, 1997.
7. Alex Biryukov and David Wagner. Slide attacks. In 6th International Workshop on Fast Software Encryption (FSE 1999), volume 1636 of Lecture Notes in Computer Science, pages 245–259. Springer-Verlag, 1999.
8. Andrey Bogdanov, Dmitry Khovratovich, and Christian Rechberger. Biclique cryptanalysis of the full AES. In 17th International Conference on the Theory and Application of Cryptology and Information Security, Advances in Cryptology (ASIACRYPT 2011), volume 7073 of Lecture Notes in Computer Science, pages 344–371. Springer-Verlag, 2011.
9. Dan Boneh, Richard A DeMillo, and Richard J Lipton. On the importance of checking cryptographic protocols for faults. In 16th International Conference on the Theory and Application of Cryptographic Techniques, Advances in Cryptology (EUROCRYPT 1997), volume 1233 of Lecture Notes in Computer Science, pages 37–51. Springer-Verlag, 1997.
10. Joan Daemen, Lars Knudsen, and Vincent Rijmen. The block cipher Square. In 4th International Workshop on Fast Software Encryption (FSE 1997), volume 1267 of Lecture Notes in Computer Science, pages 149–165. Springer-Verlag, 1997.
11. Donald Davies and Sean Murphy. Pairs and triplets of DES S-boxes. Journal of Cryptology, 8(1):1–25, 1995.
12. Itai Dinur and Adi Shamir. Cube attacks on tweakable black box polynomials. In 28th International Conference on the Theory and Application of Cryptographic Techniques, Advances in Cryptology (EUROCRYPT 2009), volume 5479 of Lecture Notes in Computer Science, pages 278–299. Springer-Verlag, 2009.
13. John Kelsey, Bruce Schneier, and David Wagner. Mod n cryptanalysis, with applications against RC5P and M6. In 6th International Workshop on Fast Software Encryption (FSE 1999), volume 1636 of Lecture Notes in Computer Science, pages 139–155. Springer-Verlag, 1999.

(cc) BY © Rahmatullayev Ilhom Raxmatullayevich.

14. David Wagner. The boomerang attack. In 6th International Workshop on Fast Software Encryption (FSE 1999), volume 1636 of Lecture Notes in Computer Science, pages 156–170. SpringerVerlag, 1999.
15. Eli Biham and Adi Shamir. Differential cryptanalysis of DES-like cryptosystems. Journal of Cryptology, 4(1):3–72, 1991.
16. Don Coppersmith. The data encryption standard (DES) and its strength against attacks. IBM journal of research and development, 38(3):243–250, 1994.
17. Eli Biham and Adi Shamir. Differential cryptanalysis of the Data Encryption Standard, volume 28. Springer-Verlag, 1993.
18. Martin Albrecht and Carlos Cid. Algebraic techniques in differential cryptanalysis. In Fast Software Encryption, pages 193–208. Springer-Verlag, 2009.
19. Florent Chabaud and Serge Vaudenay. Links between differential and linear cryptanalysis. In 13th International Conference on the Theory and Application of Cryptographic Techniques, Advances in Cryptology (EUROCRYPT 1994), volume 950 of Lecture Notes in Computer Science, pages 356–365. Springer-Verlag, 1995.
20. Xuejia Lai, James L Massey, and Sean Murphy. Markov ciphers and differential cryptanalysis. In 10th International Conference on the Theory and Application of Cryptographic Techniques, Advances in Cryptology (EUROCRYPT 1991), volume 547 of Lecture Notes in Computer Science, pages 17–38. Springer-Verlag, 1991.
21. Cunsheng Ding. The differential cryptanalysis and design of natural stream ciphers. In 1st International Workshop on Fast Software Encryption (FSE 1993), volume 809 of Lecture Notes in Computer Science, pages 101–115. Springer-Verlag, 1994.
22. Fr´ed´eric Muller. Differential attacks against the Helix stream cipher. In 11th International Workshop on Fast Software Encryption (FSE 2004), volume 3017 of Lecture Notes in Computer Science, pages 94–108. Springer-Verlag, 2004.
23. Hongjun Wu and Bart Preneel. Differential-linear attacks against the stream cipher Phelix. In 14th International Workshop on Fast Software Encryption (FSE 2007), volume 4593 of Lecture Notes in Computer Science, pages 87–100. Springer-Verlag, 2007.
24. Flavio D. Garcia, Peter van Rossum, Roel Verdult, and Ronny Wichers Schreur. Wirelessly pickpocketing a MIFARE Classic card. In 30th IEEE Symposium on Security and Privacy (S&P 2009), pages 3–15. IEEE Computer Society, 2009.
25. Carlo Meijer and Roel Verdult. Ciphertext-only cryptanalysis on hardened Mifare Classic cards. In 22nd ACM Conference on Computer and Communications Security (CCS 2015). ACM, 2015.
26. Flavio D. Garcia, Gerhard de Koning Gans, and Roel Verdult. Exposing iClass key diversification. In 5th USENIX Workshop on Offensive Technologies (WOOT 2011), pages 128–136. USENIX Association, 2011.
27. Flavio D. Garcia, Gerhard de Koning Gans, and Roel Verdult. Wirelessly lockpicking a smart card reader. International Journal of Information Security, 13(5):403–420, 2014.
28. Flavio D. Garcia, Gerhard de Koning Gans, Roel Verdult, and Milosch Meriac. Dismantling iClass and iClass Elite. In 17th European Symposium on Research in Computer Security (ESORICS 2012), volume 7459 of Lecture Notes in Computer Science, pages 697–715. SpringerVerlag, 2012.
29. William Simon. Mathematical magic. Courier Dover Publications, 1964
30. Lester S. Hill. Cryptography in an algebraic alphabet. American Mathematical Monthly, 36(6):306–312, 1929.
31. Lester S Hill. Concerning certain linear transformation apparatus of cryptography. American Mathematical Monthly, pages 135–154, 1931.
32. James Reeds. "Cracking" a random number generator. Cryptologia, 1(1):20–26, 1977.
33. Frank Rubin. Decrypting a stream cipher based on J-K flip-flops. IEEE Transactions on Computers, 100(7):483–487, 1979.

(cc) BY © *Rahmatullayev Ilhom Raxmatullayevich.*