ОҚИМЛИ ШИФРЛАШ АЛГОРИТМЛАРИ БАРДОШЛИЛИГИНИ БАҲОЛАШ УСУЛЛАРИ

Илхом Рахматуллаевич РАҲМАТУЛЛАЕВ
доцент
Техника фанлари бўйича (PhD) фалсафа доктори
Тошкент ахборот технологиялари университети Самарқанд филиали
Самарқанд, Ўзбекистон

Аннотация

Мазкур мақолада шифрлаш алгоритмлари бардошлилиги масалалари, оқимли шифрлаш назарияси ва оқимли шифрлаш алгоритмларига нисбатан қўлланиладиган айрим криптотаҳлил усуллари, хусусан, мослашувчанлик ва “бўлиб ташла ва эгалик қил” ҳужумлари содда мисоллар билан ёритиб берилган.

Таянч сўзлар: Криптографик алгоритмнинг бардошлилиги, энтропия, оқимли шифрлаш, мослашувчанлик ҳужуми, “бўлиб ташла ва эгалик қил” ҳужуми.

МЕТОДЫ ОЦЕНКИ УСТОЙЧИВОСТИ АЛГОРИТМОВ ПОТОКОВОГО ШИФРОВАНИЯ

Илхом Рахматуллаевич РАХМАТУЛЛАЕВ
доцент
доктор философии (PhD) по технических наукам
Самаркандский филиал Ташкентского университета информационных технологий
Самарканд, Узбекистан

Аннотация

В этой статье рассматриваются вопросы толерантности криптографических алгоритмов, теории потоковых шифров и некоторые методы криптоанализа, применяемые к алгоритмам потокового шифрования, в частности гибкость и атаки по принципу «разделяй и властвуй», с простыми примерами.

Ключевые слова: толерантность криптографических алгоритмов, энтропия, потоковое шифрование, атака гибкости, атака «разделяй и властвуй».

Криптографик алгоритмнинг бардошлилиги.

Криптографик алгоритмнинг бардошлилиги криптотаҳлилчи махфий калитни ёки шифрланган очиқ матнни тиклаш учун бажариши зарур бўлган ҳисоб-китоблар ёки талаб қилинадиган ресурсларнинг умумий миқдорида

ифодаланади. Ҳисоб-китоблар кўпинча шифрнинг ҳисоблаш мураккаблиги деб аталади.

Мукаммал ҳимояланган шифрлаш алгоритми учун ҳисоблаш мураккаблиги калит майдони билан бир хил бўлиб, баъзан калитнинг энтропияси деб аталади. Калит майдони барча мумкин бўлган вариантлар тўпламига ишора қилади ва барча махфий калит битлари ёрдамида комбинацияларнинг умумий сонини ифодалайди. Калитнинг ўлчами (калит ўлчами) - бу тўлиқ калит майдонининг

Махфий калитни тиклашнинг энг содда усули бу барча комбинацияларни синаб кўришдир. Бундай методология кўпинча тўлиқ қидирув ёки қўпол куч

м) ифодалайдиган битлар миқдори.

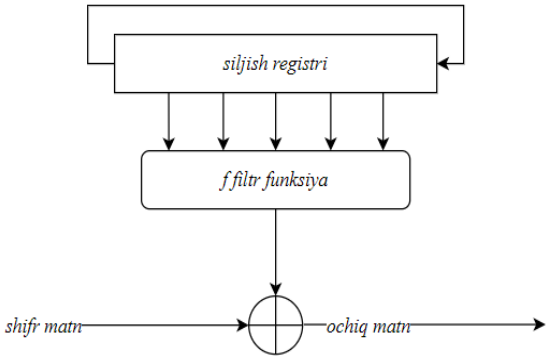
Мукаммал хавфсиз бўлмаган шифрлаш усули хавфсиз криптотизим учун асос бўлиши керак. Амалда эса кўпчилик шифрлаш алгоритмлари ўзларининг махфий калитларининг тўлиқ энтропиясидан заифроқдир. Ҳисоб китобларни оптималлаштириш ёрдамида кўпинча ҳақиқий энтропия талаб қиладиганидан камроқ ҳисоб-китобларни амалга ошириш орқали махфий калитни топиш мумкин. Бу шифрнинг ҳақиқий ҳужум мураккаблиги деб аталади.

Оқимли шифлаш алгоритмлари.

Оқим шифрлаш бир марталик блокнот (ОТП) шифрлаш техникасига ўхшаш шифрлашни амалга оширади. У махфий, тасодифий кўринадиган маълумотларнинг катта қисмини ишлаб чиқаради ва шифрланган матнни яратиш учун уларни очиқ матн билан бирлаштиради. Очиқ матнни шифрланган матндан ажратиб бўлмайди. Тасодифий маълумотлар махфий калитдан олинган ва одатда калит оқими деб аталадиган битлар оқимини ифодалайди. Оқимли шифрлаш алгоритмларида махфий калит томонидан ишга тушириладиган ва ҳар бир

шифрлаш босқичидан сўнг кейинги ҳолатга тарқаладиган ички шифр ҳолати деб номланадиган доимий хотира мавжуд. Бардошли оқимли шифрлаш алгоритмларининг чиқиши Pseudo Random Number Generator (PRNG) томонидан ишлаб чиқарилган битлар оқими билан таққосланади.

Оқимли шифрлаш алгоритмларини ишлаб чиқишда фойдаланиладиган энг машҳур усуллардан бири чизиқли бўлмаган иккилик кетма-кетликларни ишлаб чиқувчи генераторлардан фойдаланишдир [1-5]. Ушбу генераторлар иккилик калитлар оқимини ишлаб чиқаради, бу жуда катта махфий калитни талаб қилмасдан мунтазам бир марталик шифрлаш имконини беради. Чизиқли бўлмаган оқим шифрига асосланган одатий криптотизимнинг умумий кўриниши амалга ошириш имконияти сабабли жуда машҳур ҳисобланади.



расм. Оддий чизиқсиз оқимли шифрлаш тизими схемаси

расмда кўрсатилган криптографик алгоритм шифрнинг ички ҳолатини ифодаловчи айланувчи силжиш регистрини ўз ичига олади. Калитнинг ҳар бир битини ҳисоблашдан сўнг, ички фунция кўпроқ энтропияни сақлаб қолиш мақсадида чизиқли функция орқали ички ҳолатни янгилайди. Чиқиш компоненти кейинги калит оқими битини ҳисоблаш учун чизиқли бўлмаган

.

)

ф

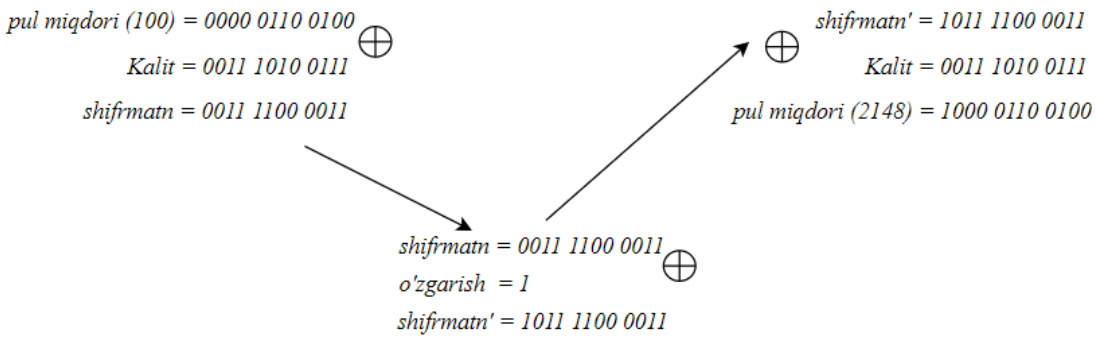
и

л

т

амалга оширади ва калит оқими битлари билан биргаликда шифрланган матн б
и
т
л Адабиётларда криптотаҳлил деб аталадиган оқимли шифрлаш алгоритмларига нисбатан криптографик ҳужумларда қўлланиладиган кўплаб р илғор ва мураккаб криптографик ҳужум методологиялари ва усуллари таклиф қилинган [6-14]. Мазкур мақолада оқимли шифрлаш алгоритмига нисбатан криптотаҳлил усулларининг қўлланилиш техникалари ёритилган.
а Криптографик ҳужум учун зарур бўлган ҳисоб-китобларни (қисман) олдиндан ҳисоблаш мумкин бўлган тарзда умумлаштириш мумкин. Бундай техника одатда Time-Memory Trade-Off (TMTO) деб аталади. Умумий ғоя криптографик ҳужумни икки босқичга, ҳисоблашдан олдинги босқичга (офф-лайне) ва фаол ҳужум босқичига (онлайн) бўлишдир. Ушбу техника бўйича батафсил маълумотларни [9-13] адабиётларда таклиф қилинган TMTO усуллари ва самарали қидирув усулларидан олиш мумкин.
а *Мослашувчанлик ҳужуми.*
т Чизиқли бўлмаган иккилик кетма-кетликни ҳосил қилувчи синхрон оқимли шифрида ишлаб чиқилган иккилик кетма-кетлик калит оқими сифатида хизмат қилади ва ХОР операторини қўллаш орқали очиқ матн билан бирлаштирилади. Бундай криптотизим, қоида тариқасида, маълумотларни узатишнинг махфийлигини ҳимоя қилувчи хавфсиз канални таъминлаши мумкин. Бироқ, қўшимча ҳимоясиз маълумотларнинг яхлитлиги кафолатланмайди. Хабар аутентификация коди (MAC) каби қўшимча қарши чоралар маълумотларнинг ҳақиқийлигини ҳимоя қилиши мумкин. Қўшимча криптографик усулларсиз оқимли шифрлаш тизими мослашувчанлик ҳужумига нисбатан бардошсиз ҳисобланади.
и
л
и
ш

Мослашувчанлик ҳужумининг мақсади махфий калитни тиклаш эмас. Махфий калит ҳақида ҳеч қандай маълумотга эга бўлмаган ҳолда криптотизимнинг хавфсизлигини бузишга ҳаракат қилишдир. 2-расмда мослашувчанлик ҳужуми учун заиф бўлган банк иловасининг маълумотлар узатиш тизимининг бузилиши кўрсатилган. Кичкина пул ўтказмасини ифодаловчи кетма-кетликдаги бир битни ўзгартирилади ва тўсатдан жуда катта пул ўтказмасини ифодалайди. Агар калит оқими ўта хавфсиз оқимли шифрда ишлаб чиқарилган бўлса ҳам, криптотизимнинг бошқа компонентлари ҳали ҳам заиф бўлиши мумкин. Бу ҳақиқий хавфсизликни белгилайдиган бутун криптотизимнинг бардошлилигидир.



2-расм. Мослашувчанлик ҳужумида пул ўтказмаси қийматини ўзгартириш жараёни

Мослашувчанлик ҳужуми самарали бўлиб туюлса-да, уни қўллаш унчалик осон эмас. Бузғунчи уни ўзгартиришга қодир бўлиши учун пулнинг қаерда ва қачон узатилишини аниқ билиши керак. Нотўғри позицияда битни ўзгартириш маъносиз ва узатишнинг бузилишига олиб келиши мумкин. Калитлар оқими ҳақидаги билимлар рақибга янада пухта ишлаб чиқилган бузғунчиликни тайёрлашга имкон беради. Бироқ, бу калит оқимидан қайта фойдаланишни ўз ичига олади. Таъкидлаб ўтилганидек, иккилик кетма-кетлик фақат бир марта ишлатилиши муҳим. Буни амалга ошириш учун оқимли шифрдан ҳар сафар фойдаланилганда ички ҳолат такрорланмас қиймат билан ишга туширилиши керак.

“Бўлиб ташла ва эгалик қил” ҳужуми.

Ҳисоблашнинг мураккаблигини камайтиришнинг энг самарали усулларидан бири катта муаммони иккита алоҳида кичик масалаларга бўлишдир, бу кўпинча *“бўлиб ташла ва эгалик қил”* деб аталади. Бу усул турли соҳаларида қийин ҳисоблаш масалаларини ечишни оптималлаштириш учун ишлатилади [12-

камайтириш учун ушбу услубни криптотизимларнинг айрим турларига ҳужум қ

и

л Аввал айтиб ўтилганидек, муҳим узунликдаги масалан, 80 бит, махфий

калитга эга криптографик ҳимояланган шифрни очиш учун жуда кўп вақт ва

ресурслар керак бўлади. Бундай криптотизим учун махфий калитни топиш учун

тўлиқ қидирувни бўлиш мураккабликни камайтирмайди. Бу рақибга фақат иккита

қидирувни параллеллаштиришга имкон беради, уларнинг ҳар бири асосий

муаммонинг аниқ ярим мураккаблиги 2^{79}. Бироқ, таҳлилчи катта муаммони

иккита кичикроқ масалага бўлиш йўлини топса, мураккаблик сезиларли даражада

камаяди.

д

расмда келтирилган шифрлаш схемаси учун мазкур ҳужумни қандай ўтказиш

м

у

м

к

и

и

н 3-расмда кўрсатилганидек оқимли шифрлаш алгоритмида саккизта

ячейкадан иборат силжиш регистри мавжуд. Ушбу регистрга ишга тушириш

вақтида махфий калитнинг бирлари ва ноллари юкланади. $f(\cdot)$ компоненти

чизиқли бўлмаган фунция бўлиб, у 4 та кириш битларидан фойдаланиб 1 чиқиш

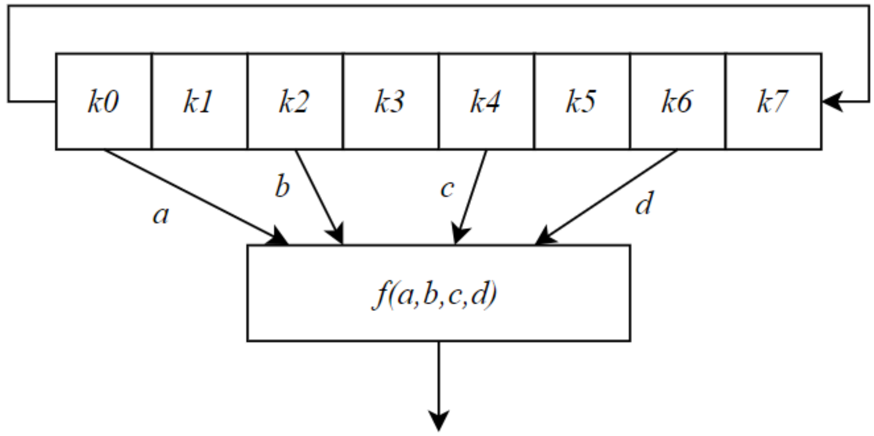
и

н

и

қ

битини ишлаб чиқаради, бу ишлаб чиқилган битлар кетма-кетлиги - калит оқими ko деб аталади. i – итератцияда ишлаб чиқилган бит эса ko_i билан белгиланади.

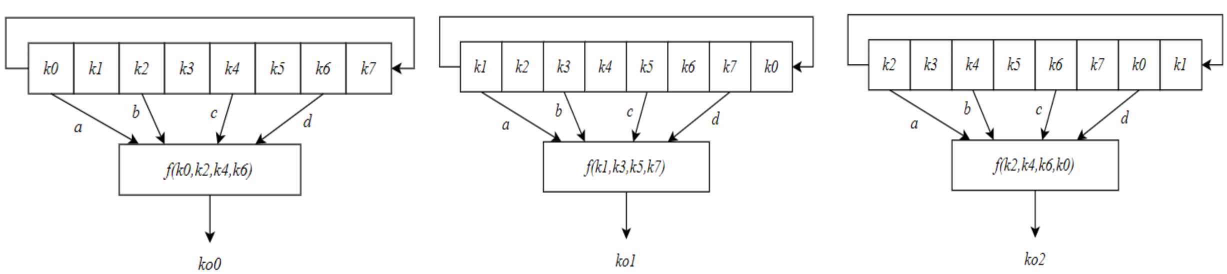


3-расм. “Бўлиб ташла ва эгалик қил” ҳужумини ифодалаш учун фойдаланиладиган алгоритм схемаси

4-расмда дастлабки учта шифрлаш итератцияси тасвирланган. ko_0, ko_1 ва ko_2 чиқиш битларини ишлаб чиқиш учун $f(\cdot)$ функциясига кириш битлари ҳам тасвирланган. Кўриш мумкинки, ko_0 ва ko_2 ни ишлаб чиқиш учун зарур бўлган махфий калит битлари бир хил бўлади, гарчи улар тартибда фарқ қилсалар ҳам.

Б

и



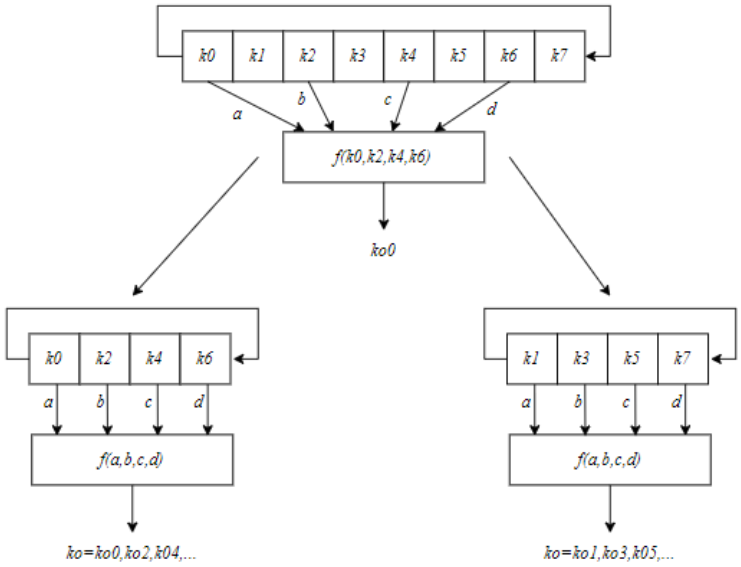
к

Чиқувчи калит оқимидаги тоқ ва жуфт тартибдаги ячейкалардан

р а с м Б и р и н ч и у ч т

а ф о й д а л и

расмдаги алгоритм битта катта алгоритм сифатида ишлаб чиқилган, аммо уни осонлик билан кичикроқ 2 та алгоритм бўлиш мумкин. 5-расмда алгоритмни қисмларга қандай ажратиш мумкинлиги кўрсатилган, уларнинг иккаласининг ҳам калит ўлчами асл шифрлаш алгоритмининг калит ўлачамининг ярмига тенг.



5-расм. “Бўлиб ташла ва эгалик қил” ҳужумини тоқ ва жуфт калит оқим битларига бўлиш орқали амалга ошириш жараёни

Ички шифр ҳолатининг атиги ярми билан тоқ ва жуфт шифр учун ҳисоблаш мураккаблиги 2^4 га тушади. Шундай қилиб, иккаласи учун умумий мураккаблик атиги $2\times2^4 = 2^5 = 32$ га камаяди, бу дастлабки мураккаблик 2^8=256 дан анча кам. Эътибор беринг, “бўлиб ташла ва эгалик қил” ҳужуми фақат асосий калит фазосининг энтропиясини икки баравар камайтирмайди. Бундай бўлиниш мураккабликни $\frac{2^8}{2} = 2^7 = 128$ га нисбатан анча кичик мураккабликгача камайтиришга олиб келади. Шифрни иккита мустақил махфий калитга таянадиган иккита кичик алгоритмга ажратиш анча самаралидир, бу ерда иккита калит асл махфий калитнинг иккала ярмини ифодалайди.

Мазкур мақолада шифрлаш алгоритмлари бардошлилиги масалалари, оқимли шифрлаш назарияси ва оқимли шифрлаш алгоритмларига нисбатан қўлланиладиган айрим криптотаҳлил усуллари, хусусан, мослашувчанлик ва “бўлиб ташла ва эгалик қил” ҳужумлари содда мисоллар билан ёритиб берилган.

Бу турдаги шифрлаш алгоритмларига нисбатан бошқа таҳлил усулларининг қўлланилиши кейинги тадқиқотларда ёритиш кўзда тутилган.

ФОЙДАЛАНИЛГАН АДАБИЁТЛАР:

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.

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. Hamid Reza Amirazizi and Martin E Hellman. Time-memory-processor trade-offs. IEEE Transactions on Information Theory, 34(3):505–512, 1988.