# СИММЕТРИК БЛОКЛИ ШИФРЛАШ АЛГОРИТМЛАРИНИНГ ЧИЗИҚЛИ ТАҲЛИЛИГА ДОИР

Жўраев Г.У., Шермухаммедов Ж.А.
*Мирзо Улуғбек номидаги Ўзбекистон Миллий университети, gjuraev@mail.ru*

Маълумки, ҳозирги вақтда катта миқдордаги шахсий, молиявий, тижорат ва технологик ахборотлар компьютер маълумотлар базаларида сақланмоқда ва компьютер тармоқлари бўйича узатилмоқда. Бундай ҳолатда ушбу ахборотлар ва маълумотларни ҳимоялаш, уларни конфеденциаллигини таъминлашда криптографик усул ва воситаларнинг ўрни биқиёс даражада каттадир. Симметрик блокли шифрлаш алгоритмлари юқори тезликка эга эканлиги сабабли шу мақсадда, яъни маълумотларни ҳимоялашда кенг қўлланилмоқда [1,4].

Симметрик блокли шифрлаш алгоритмларини яратишда қўйиладиган асосий талаблар ушбу алгоритмнинг компьютерда дастурий амалга оширишнинг тезлиги юқори бўлишлиги ҳамда асосий криптотаҳлил усулларига нисбатан криптобардошлигини таъминлашдан иборат. Чизиқли криптотаҳлил усули симметрик блокли шифрлаш алгоритмларининг асосий криптотаҳлил усулларидан биридир [1,2]. Агар блокли шифрлаш алгоритми чизиқли криптотаҳлил усули асосидаги ҳужумга нисбатан бардошли бўлса, у ҳолда ушбу алгоритм криптобардошли деб ҳисобланади ва махфий ахборотларни узатишда ҳеч иккиланмасдан ундан фойдаланиш мумкин.

Кўпчилик ҳолларда чизиқли криптотаҳлил усули тўлиқ саралаш усули билан биргаликда қўлланилади. Шифрлаш калитининг айрим битлари аввало чизиқли таҳлил усулида аниқланади, қолган битлари эса тўлиқ саралаш усулидан фойдаланиб, топилади.

Криптотаҳлилнинг чизиқли таҳлил усули очиқ матн ва унга мос келувчи шифрматн ўртасида чизиқли аппроксимацияни қуришга асосланган.

Ушбу усул шифр матнга мос келувчи очиқ матнни билишга асосланган бўлиб, унда шифрлаш қурилмасидан ёки алгоритмидан битларнинг конкрет наборини ўтишини таҳлил қилишдан фойдаланилади [1,3].

Чизиқли таҳлил усулини бирор бир шифрлаш алгоритмига қўллаш учун шифрлаш алгоритми структурасини билиш, шунингдек, бир неча очиқ матн ҳамда криптоаналитикка номаълум бўлган бир хил шифрлаш калити билан ҳосил қилинган, уларга мос келувчи шифрматнлар жуфтликлари статистикасига эга бўлиш талаб этилади.

Ушбу усулнинг моҳияти шифрни чизиқсиз алмаштириш кўринишида ифодаловчи мураккаб буль функцияларини содда чизиқли функция кўринишида ифодалашдан иборат. Бунинг натижасида ҳосил қилинган шифрни дастлабки шифрга нисбатан таҳлил қилиш соддалашади. Шу боис, айрим ҳолларда дастлабки шифрни криптотаҳлил қилиш масаласи унинг соддалаштирилган модификациясини етарлича аниқликда криптотаҳлил қилиш масаласига келтириш мумкин [1,4].

Чизиқли таҳлил усулини қўллашда асосий қийинчилик чизиқли яқинлашишни топишдан иборат. Таҳлил қилишда фойдаланиладиган очиқ матн–шифр матн жуфтликлари ҳажми топилган чизиқли функция қандай эҳтимоллик билан дастлабки шифрга яқинлашишига боғлиқ. Одатда, таҳлил қилишда фойдаланиладиган очиқ матн-шифр матн жуфтликлари ҳажми иложи борича минимал бўлиши талаб этилади.

Ушбу ишда битта чизиқли яқинлашишдан фойдаланиб, шифрлаш калитининг бир неча битларини аниқлаш имконини берувчи қуйидаги чизиқли таҳлил алгоритмидан фойдаланилган [1-3].

Оралиқ $C_1, C_{r-1}$ шифр матнлари ва шифрлаш калити битлари учун $1/2$ эҳтимолликдан юқори $p = 1/2 + \varepsilon'$ эҳтимоллик билан бажариладиган қуйидаги $L'$ чизиқли муносабат ўрнатилади ($\varepsilon'$ миқдор $L'$ *чизиқли муносабатнинг назарий салмоғи дейилади)*

$$\langle a, C_1 \rangle \oplus \langle b, C_{r-1} \rangle = \langle d, K \rangle .$$

Очиқ матнлар ва фиксирланган, номаълум $K$ шифрлаш калити асосидаги уларга мос келувчи шифр матнларнинг $N$ та жуфтликлари статистикаси тўпланади.

Маълум бўлган $P$ очиқ матн фойдаланиб, $\langle a, C_1 \rangle$ чизиқли муносабатни қийматини аниқлаш имконини берувчи $K$ шифрлаш калитининг минимал $K'$ қисми $K$ шифрлаш калитининг айнан қайси битларидан ташкил топганлигини аниқлаш учун шифрлашнинг биринчи раундини таҳлил қилиш етарли. Бунинг учун коэффициентлари нолдан фарқли $L'$ чизиқли муносабатда иштирок этувчи $C_1$ шифр матннинг битлари шифрлаш калитининг айнан қайси битларига сезиларли даражада боғлиқлигини аниқлаш лозим бўлади.

Худди шунингдек, маълум бўлган $C$ шифр матн фойдаланиб, $\langle b, C_{r-1} \rangle$ чизиқли муносабатни қийматини бир қийматли аниқлаш имконини берувчи $K$ шифрлаш калитининг минимал қисми $K''$ аниқланади.

Шифрлаш калитининг $K' \cup K''$ қисмга кирувчи битлари *фаол (айрим ҳолларда самарали) битлари дейилади.*

Шифрлаш калитининг $K' \cup K''$ қисми бўйича бўлиши мумкин бўлган вариантларини саралаш лозим. Ҳар бир фиксирланган $K' \cup K''$ қисм бўйича қуйидагиларни амалга ошириш лозим.

- $K'$, $K''$ қисмлардан фойдаланиб, ҳар бир $\left(P^{(i)}, C^{(i)}\right)$ очиқ-шифр матн жуфтлиги учун $\langle a, C_1 \rangle \oplus \langle b, C_{r-1} \rangle$ муносабатни қиймати ҳисобланади. Фараз қилайлик, очиқ матн ва шифр матнларнинг $N$ та жуфтликларидан $N_0$ та жуфтликлари учун ушбу қийматлар ноль, $N_1$ та жуфтликлари учун ушбу қийматлар бир бўлсин, яъни $N_0 + N_1 = N$.

- $1/2 + \bar{\varepsilon} = N_0 / N_1$ тенглик билан аниқланадиган чизиқли муносабатни *тажрибавий салмоғи* $\bar{\varepsilon}$ *нинг қиймати* ҳисобланади.

Кейинги қадамда чизиқли муносабатнинг тажрибавий салмоғи $\bar{\varepsilon}$ назарий салмоғи $\varepsilon'$дан кескин фарқ қилувчи шифрлаш калитининг $K' \cup K''$ қисми нотўғри қисмлар, шифрлаш калитининг қолган қисми тўғри қисмлар деб ҳисобланади ва массив кўринишида сақланади. Одатда, ушбу алгоритм билан ишлашда чизиқли муносабат салмоқларининг тафовутлари маълум бир $\delta$ аниқлик билан ҳисобланади. Агар $|\varepsilon' - \bar{\varepsilon}| \le \delta$ ўринли бўлса $K' \cup K''$ қисм $K$ шифрлаш калитининг тўғри, акс ҳолда нотўғри қисмлари деб ҳисобланади.

Кейинги ҳар қадамда $K$ шифрлаш калитининг ҳар бир тўғри қисмлари $K' \cup K''$ учун $K$ калитнинг қолган битларини саралаш йўли билан тиклаш лозим.

Ушбу алгоритмнинг асосий ютуғи шундаки, битта чизиқли муносабатдан фойдаланиб, $K$ шифрлаш калитининг битлар гуруҳини аниқлаш мумкин.

## Фойдаланилган адабиётлар


1. Бабенко Л.К., Ищукова Е.А. Современные алгоритмы блочного шифрования и методы их анализа. М.: Гелиос АРВ, 2006. – 376 с.

2. Панасенко С. П. Алгоритмы шифрования. Специальный справочник. СПб.: БХВ-Петербург, 2009. – 576 с.

3. Токарева Н. Н. Симметричная криптография. Новосибирский государственный университет. Новосибирск, 2012. – 234 с.

4. Шнайер Б. Прикладная криптография: Протоколы, алгоритмы, исходные тексты на языке Си. М.: Триумф. 2002. – 816 с.

## Муаллифлар ҳақида

Жўраев Гайрат Умарович – Мирзо Улуғбек номидаги ЎзМУ «Математик моделлаштириш ва криптоанализ» кафедраси доценти, физика-математика фанлари номзоди.

Шермухаммедов Жасурбек Абобакир ўғли – Мирзо Улуғбек номидаги ЎзМУ «Ахборот хавфсизлиги» мутахассислиги иккинчи босқич магистранти.