АППАРАТДА АМАЛГА ОШИРИЛАДИГАН ЯНГИ ОҚИМЛИ ШИФРЛАШ АЛГОРИТМИ

Илхом Рахматуллаевич РАҲМАТУЛЛАЕВ
Катта ўқитувчи
Тошкент Ахборот Технологиялари Университети
Самарқанд филиали
Самарқанд, Ўзбекистон

Аннотация

Мақолада умумий узунлиги 3 та силжитиш регистрларидан, 6 та AND ва 14 та XOR элементларидан иборат NHSA деб номланган оқимли шифрлаш алгоритмининг тавсифи келтирилган. Унинг ёрдамида ишлаб чиқилган кетма-кетликларнинг тасодифийлик даражаси бўйича баҳолаш натижалари ва айрим криптотаҳлил усулларига бардошлилиги бўйича хулосалар, шунингдек, алгоритмни аппаратда амалга ошириш учун зарур элементлар сони бўйича маълумотлар келтирилган.

Таянч сўзлар: NHSA, gate, Trevium, синхрон, алгебраик ҳужум, қайта синхронизация ҳужуми, LSFR, инициализация, генерация, NIST.

НОВЫЙ АППАРАТНО-РЕАЛИЗОВАННЫЙ АЛГОРИТМ ПОТОКОВОГО ШИФРОВАНИЯ

Илхом Рахматуллаевич РАХМАТУЛЛАЕВ
Старший преподаватель
Самаркандский филиал Ташкентский университет информационных
Самарканд, Узбекистан

Аннотация

В статье представлено описание алгоритма потокового шифрования под названием NHSA, состоящего из 3 сдвиговых регистров, 6 элементов AND и 14 элементов XOR. Представлены результаты оценки случайности последовательностей ячеек, разработанных с использованием указанного алгоритма, и выводы о переносимости некоторых методов криптоанализа, а также информация о количестве элементов, необходимых для реализации алгоритма на аппаратных средствах.

Ключевые слова: NHSA, gate, Trevium, синхронный, алгебраическая атака, LSFR, инициализация, генерация, NIST.

нинг бошланғич ҳолати умумий узунлиги 269 бит бўлган 3 та силжиш регистридир. Ҳар бир ҳолат ўнгга циклик силжиш регистрларидаги битларни чизиқсиз узатиш ва қайта алоқа комбинацияси орқали ўзгартирилади. Шифрни ишга тушириш учун 128 бит узунликка эга К калити ва инициализация вектори

алгоритм 4*269 = 1076 марта бажарилади, бу эса бошланғич ҳолатнинг ҳар бир бити калитнинг ва инициализация векторининг ҳар бир битига боғлиқлигини кафолатлайди.

Инициализация босқичидан ўтгандан сўнг, ҳар бир циклда чиқувчи калит оқимининг янги аъзоси ҳосил бўлади, у матннинг кейинги бити билан жараёни тескари тартибда амалга оширилади – шифрланган матннинг ҳар бир бити чиқувчи калит оқимининг ҳар бир бити билан ХОР амали ёрдамида қўшилади.

Инициализация. Инициализация жараёни Алгоритм 128 битли калит ва 128 битли инициализация векторини 269 (89+83+97) битли бошланғич ҳолат регистрларига юклаш орқали ишга туширилади. Инициализация жараёнини қуйидаги псевдокод ёрдамида тавсифлаш мумкин.

Регистр ячейкаларининг индекслари кетма-кетликда ифодаланган ҳолат учун:

$(K_0, K_1, \dots, K_{79}, 0, \dots, 0) \rightarrow (a_0, a_1, a_2, \dots, a_{88})$

$(I_0, I_1, \dots, I_{79}, 0,0,0) \rightarrow (a_{89}, a_{90}, a_{91}, \dots, a_{171})$

$(K_{80}, \dots, K_{127}, I_{80}, \dots, I_{127}, 0) \rightarrow (a_{172}, a_{173}, \dots, a_{268})$

$for\ i = 0\ to\ 1075\ do$

$a_{55} + a_{80} \cdot a_{81} + a_{82} + a_{72} \cdot a_{74} + a_{161} \rightarrow t_0$

$a_{151} + a_{164} \cdot a_{165} + a_{166} + a_{155} \cdot a_{157} + a_{259} \rightarrow t_1$

$a_{232} + a_{263} \cdot a_{264} + a_{265} + a_{242} \cdot a_{244} + a_{68} \rightarrow t_2$

$(t_2, a_0, \dots, a_{87}) \rightarrow (a_0, \dots, a_{88})$

$(t_1, a_{89}, \dots, a_{170}) \rightarrow (a_{89}, \dots, a_{171})$

$(t_0, a_{172}, \dots, a_{267}) \rightarrow (a_{172}, \dots, a_{268})$

$end\ for.$

Регистр ячейкаларининг индекслари ҳар бир регистр учун алоҳида тартибда ифодаланган ҳолат учун:

$(K_0, K_1, \dots, K_{79}, 0, \dots, 0) \rightarrow (a_0, a_1, a_2, \dots, a_{88})$

$(I_0, I_1, \dots, I_{79}, 0,0,0) \rightarrow (b_0, b_1, b_2, \dots, b_{82})$

$(K_{80}, \dots, K_{127}, I_{80}, \dots, I_{127}, 0) \to (c_0, c_1, \dots, a_{96})$

$for\ i = 0\ to\ 1075\ do$

$a_{55} + a_{80} \cdot a_{81} + a_{82} + a_{72} \cdot a_{74} + b_{72} \to t_0$

$b_{62} + b_{75} \cdot b_{76} + b_{77} + b_{66} \cdot b_{68} + c_{87} \to t_1$

$c_{60} + c_{91} \cdot c_{92} + c_{93} + c_{70} \cdot c_{72} + a_{59} \to t_2$

$(t_2, a_0, \dots, a_{87}) \to (a_0, \dots, a_{88})$

$(t_1, b_0, \dots, a_{81}) \to (b_0, \dots, b_{82})$

$(t_0, c_0, \dots, c_{95}) \to (c_0, \dots, c_{96})$

$end\ for.$

Генерация. Оқим генератори ҳолат регистрлари қийматининг 3 битини ўзгартириш ва калит оқимининг 1 битини ҳисоблаш учун 269 битли бошланғич ҳолат регистрларининг 21 битининг қийматларидан фойдаланади. Лекин 1076 итерациядан иборат инициализация жараёнидан кейин мазкур 21 битнинг қийматига калит ва инициалиацион векторнинг қийматлари тўлиқ таъсир қилиб бўлади. Шифрлаш учун зарур N $(N \leq 2^{64})$ бит калитни генерация қилиш жараёнини қуйидаги псевдокод ёрдамида ифодалаш мумкин.

Регистр ячейкаларининг индекслари кетма-кетликда ифодаланган ҳолат учун:

$for\ i = 0\ to\ N\ do$

$a_{55} + a_{82} \to t_0$

$a_{151} + a_{166} \to t_1$

$a_{232} + a_{264} \to t_2$

$t_0 + t_1 + t_2 \to chiqish_i$

$a_{55} + a_{80} \cdot a_{81} + a_{82} + a_{161} \to t_0$

$a_{151} + a_{164} \cdot a_{165} + a_{166} + a_{259} \to t_1$

$a_{232} + a_{263} \cdot a_{264} + a_{265} + a_{68} \to t_2$

$(t_2, a_0, \dots, a_{87}) \to (a_0, \dots, a_{88})$

$(t_1, a_{89}, \dots, a_{170}) \to (a_{89}, \dots, a_{171})$

$(t_0, a_{172}, \dots, a_{267}) \to (a_{172}, \dots, a_{268})$

$end\ for.$

Регистр ячейкаларининг индекслари ҳар бир регистр учун алоҳида тартибда ифодаланган ҳолат учун:

$for\ i = 0\ to\ N\ do$

$a_{55} + a_{82} \to t_0$

$b_{62} + b_{77} \to t_1$

$c_{60} + c_{93} \to t_2$

$t_0 + t_1 + t_2 \to chiqish_i$

$a_{55} + a_{80} \cdot a_{81} + a_{82} + a_{72} \cdot a_{74} + b_{72} \to t_0$

$b_{62} + b_{75} \cdot b_{76} + b_{77} + b_{66} \cdot b_{68} + c_{87} \to t_1$

$c_{60} + c_{91} \cdot c_{92} + c_{93} + c_{70} \cdot c_{72} + a_{59} \to t_2$

$(t_2, a_0, \dots, a_{87}) \to (a_0, \dots, a_{88})$

$(t_1, b_0, \dots, a_{81}) \to (b_0, \dots, b_{82})$

$(t_0, c_0, \dots, c_{95}) \to (c_0, \dots, c_{96})$

$end\ for.$

Юқорида келтирилган псевдокодларда қўшиш ва кўпайтириш амаллари 2 модул бўйича қўшиш ва кўпайтиришни амалга оширувчи XOP ва AND амаллари ҳисобланади.

Мазкур алгоритм ёрдамида битта калит ва инициализацион вектор ёрдамида 2^{64} бит узунликдаги калитларни генерация қилиш тавсия қилинади.

Алгоритм ёрдамида генерация қилиш жараёни тўғри ташкил қилиниши учун намуна қуйида келтирилган.

Кирувчи параметрлар:

Калит:00011100000001100011011000011001000010110001001001100000001000110011101100110101000100100101111100011110000111010000111000101111

*IV:*11110000111000001101000011000000101100001010000010010000100000000111000001100000010101000000001100000010000000010000000000000000

Инициализация жараёнидан аввал регистрларнинг қийматлари:

*a:*00011100000001100011011000011001000010110001001001100000001000110011101100110100000000

*б:*11110000111000001101000011000000101100001010000010010000100000000111000001100000000

*с:*00010010010111110001111000011101000011100010111101010100000000110000000100000000100000000000000000

Инициализация жараёнидан сўнг регистрларнинг қийматлари:

*а:*10110010010011010110101001101110110101100011110000010010111111100011101011011001011010000

*б:*01001110011100100110011000110100011010000011101000111010000110110101010011011110100

*с:*00000010000010101001101000100100111100100101111101001010001110101001001000100111111011010000000000

*чиқиш:*00100101110100111110111110111011010110110110000110001100101000010110101000001110…

NHSA – бу асосан аппаратга йўналтирилган мослаштирилган алгоритм. У гате (элемент)лар сони бўйича чекловлар бўлган муҳитларда ихчам бўлишга, чекланган қувват манбаларига эга платформаларда қувватни тежайдиган ва юқори тезликдаги шифрлашни талаб қиладиган иловаларда тезкорликни таъминлашга қаратилган.

Ихчам амалга ошириш талаби битга йўналтирилган ёндашувни таклиф қилади. Бундан ташқари, калит оқими генераторининг чиқишида ички ҳолат регистрларининг чизиқсиз боғлиқлилигини таъминлаш талаб қилинади. Энергияни самарали сарфлаш ва тезкор амалга оширишни таъминлаш имкони ҳам мавжуд бўлиши керак.

Келтирилган рақамларга асосланиб (яъни, ҳар бир Флип-флоп (суриш регистри элементи) учун 12 NAND шлюзи, XOP учун 2,5 пфеу ва AND учун 1,5 гате), аппаратда амалга ошириш учун зарур гателар сонини ҳисоблаш мумкин. EStream танловида қатнашган энг яхши оқимли шифрлаш алгоритмларидан бири бўлган Trevium алгоритми билан қиёсий таҳлил натижалари 1-жадвалда келтирилган.

1-жадвал.

NHSA ва Trevium алгоритмларининг аппарат татбиқи учун зарур гателар сони

Алгоритм	**Тревиум**	**HNHSA**
Калит узунлиги	80	128
IV узунлиги	80	128
Ички ҳолат регистри	288	269
AND gate	3	6
XOP gate	11	14
Жами gate лар сони	**3488**	**3272**

*Тасодифийлик тести натижалари***.** NHSA алгоритмида юқорида берилган калит ва IV ёрдамида генерация қилинган кетма-кетликлар NIST статистик тестлари ёрдамида тасодифийлик даражаси баҳоланади. Қуйида мазкур тест таркибидаги 15 та тест бўйича олинган натижалар келтирилган:

SUMMARY

monobit_test	0.3828976248514478 PASS
frequency_within_block_test	0.6354841415737159 PASS
runs_test	0.48512504500511644 PASS
longest_run_ones_in_a_block_test	0.4084594094693384 PASS
binary_matrix_rank_test	0.08050322562050827 PASS
dft_test	0.6543472577764083 PASS
non_overlapping_template_matching_test	1.00000828105159 PASS
overlapping_template_matching_test	0.03940335533694327 PASS
maurers_universal_test	0.9991531960785148 PASS
linear_complexity_test	0.6468061465110148 PASS
serial_test	0.16944057962301154 PASS
approximate_entropy_test	0.16901368121036756 PASS
cumulative_sums_test	0.16791543598886172 PASS
random_excursion_test	0.04385947941605159 PASS
random_excursion_variant_test	0.12339191184909339 PASS

Бу натижалардан кўриш мумкинки, NHSA алгоритми ёрдамида генерация қилинган кетма-кетликлар тасодифийлик шартлари бўйича хавфсизлик талабларига жавоб беради.

Алгоритмнинг даври. Алгоритмнинг ички ҳолати чизиқли бўлмаган тарзда ривожланиши сабабли унинг даврини аниқлаш қийин. Шунга қарамай, бир қатор кузатишлар орқали алгоритмнинг даврини тахмин қилиш мумкин. Биринчидан, агар AND эшикларисиз тўлиқ чизиқли схема олинса, ҳар қандай калит/IV жуфтлиги ёрдамида камида 2^{83-3}-1 даврига эга оқим ҳосил қилишини кўрсатиш мумкин. Бу NHSA учун бевосита таъсир қилмайди, лекин бунга регистрларнинг узунликлари тўғри танланганлигининг белгиси сифатида қаралиши мумкин.

Иккинчидан, NHSA ички ҳолати тескари тарзда янгиланади ва $(c_0, .., c_{96})$ регистрининг ишга туширилиши ҳолатнинг 96 итерациядан камроқ айланишининг олдини олади. Агар NHSA етарли миқдордаги итерациядан (бизнинг ҳолатда 269*4=1076 итерация) сўнг тасодифий алмаштириш сифатида ҳаракат қилади деб ҳисобланса, у ҳолда 2^{269} гача бўлган барча цикл узунликлари тенг эҳтимолга эга бўлади ва шунинг учун берилган калит/IV жуфтлигининг 2^{128} дан кичик циклни келтириб чиқариши эҳтимоли $2^{269-128}=2^{141}$ га тенг бўлади.

Шундай бўлса ҳам, юқорида генерация қилинган калитларнинг ишончлилигини максимал таъминланишини суғурталаш мақсадида бир калит/IV жуфтлиги ёрдамида 2^{64} бит калит генерация қилиш тавсияси келтирилди.

Корреляция ҳужуми. Синхрон оқим шифрининг хавфсизлигини таҳлил қилганда, криптоаналитик одатда икки хил турдаги корреляцияни кўриб чиқади. Биринчи тур калит оқими битлари ва ички ҳолат битларининг чизиқли бирикмалари ўртасидаги корреляция бўлиб, улар потенциал ҳолатда ҳолатнинг тўлиқ тикланишига олиб келиши мумкин. Корреляция ҳужумлари орқали ишлатиладиган иккинчи тур, калит оқим битларининг ўзлари ўртасидаги корреляциядир.

Шубҳасиз, калит оқим битлари ва ички ҳолат битлари ўртасидаги чизиқли корреляцияни топиш осон, чунки чиқиш бити оддийгина *chiqish i=a55+a82+b62+b77+c60+c93* га тенг деб белгиланган. Бироқ, бошқа LFSR асосидаги шифрлардан фарқли ўлароқ, NHSA нинг ички ҳолати чизиқли бўлмаган тарзда ўзгариб боради ва таҳлилчи ҳолатни самарали тиклаши учун ушбу тенгламаларни қандай бирлаштириш жараёни етарлича мураккаб муаммога айланади.

Иккинчи турдаги корреляцияларни топишнинг осон йўли шифр орқали чизиқли йўлларни кузатиб бориш ва барча дуч келган AND гателарининг чиқишларини 0 га яқинлаштиришдир. Бироқ NHSA-даги амалларнинг жойлашуви шундай танланганки, ҳар қандай йўл ушбу ўзига хос турдаги кузатувларда камида 144 та AND gate чиқишлари қийматини тўлиқ тахмин қилинишига олиб келади. Калит оқим битларининг корреляциясини аниқлашга қаратилган чизиқли бирикмасига мисол қуйида келтирилган:

Ушбу чизиқли бирикманинг корреляцияси ўзига хос кўриб чиқилган йўл билан тўлиқ ифодаланган деб фараз қилсак, мазкур тенглама 2^{-144} корреляция коэффициентига эга бўлади. Бундай корреляцияни аниқлаш учун камида 2^{288} бит калит оқими талаб қилинади, бу хавфсизлик талабидан ва калитни тўлиқ танлаш усули (2^{128}) дан анча юқори.

Алгебраик ҳужум. NHSA алгебраик ҳужум усули учун бир қарашда самарали қўлланилиши мумкин бўлган енгил алгоритм бўлиб туюлади. Тўлиқ схемани паст даражадаги жуда сийрак тенгламалар билан осонгина тасвирлаш имкони мавжуд. Бироқ, алгоритмнинг ички ҳолати чизиқли тарзда ўзгармаганлиги сабабли алгоритмдаги етарлича узун танланган LFSR регистрлари асосидаги схемалар учун яратилган тенгламалар тизимини ечиш учун ишлатиладиган самарали чизиқлилаштириш усулларини қўллаш етарлича қийин бўлади.

Қайта синхронизация ҳужумлари. Ҳужумларнинг яна бир тури – қайта синхронизация ҳужумлари бўлиб, бунда рақибга IV қийматини бошқаришга рухсат берилади ва тегишли калит оқимини текшириш орқали калит ҳақида

маълумот олишга ҳаракат қилинади. NHSA алгоритмида шифрлашда фойдаланиладиган калитни ишлаб чиқаришдан олдин инициализация жараёнида етарлича кўп бажариладиган итерациялар орқали ушбу турдаги ҳужумларнинг олдини олишга ҳаракат қилинган. Ҳар бир ҳолат бити иккита тўлиқ циклдан (яъни, 2 · 269 итерация) кейин ҳар бир калит ва IV битига чизиқли бўлмаган тарзда боғлиқлигини кўрсатиш мумкин. Шифрни қайта синхронизация ҳужумларидан ҳимоя қилиш учун яна иккита цикл етарли бўлишини таъкидлаш мумкин.

Шундай қилиб, NHSA оддий синхрон оқимли шифрлаш алгоритмидир, у мослашувчан аппарат татбиқини талаб қиладиган иловалар учун жуда мос келади. Алгоритмнинг ҳар бир итерациясида сийрак янгилаш функцияларидан қочиш кераклиги ҳақидаги умумий қоидага қарамай, ҳолатнинг фақат бир нечта битлари ишлатилади. Натижада, ҳужумларни тахмин қилиш ва аниқлаш, албатта, мураккаблик туғдиради. Тўғридан-тўғри ҳужум жами 128 бит махфий калитни (IV очиқ калит деб фараз қилинади) тахмин қилишдан иборат. Кейинчалик мураккаб ҳужумлар бу рақамни қай даражада камайтириши мумкинлигини аниқлаш учун қўшимча тадқиқотлар ўтказиш талаб этилади. Ўтказилган тадқиқотлар унинг хавфсизлик талабларига қанчалик мос эканлиги бўйича хулосалар беришда жуда муҳим ҳисобланади.

ФОЙДАЛАНИЛГАН АДАБИЁТЛАР:

1. Асосков А.В, Иванов М.А. Поточные шифры. – Москва: Кудиц-Образ, 2003. – 336 с.

2. Шеннон К. Теория связи в секретных системах // В кн. Работы по теории информации и кибернетике. – Москва: ИЛ, 1963.