



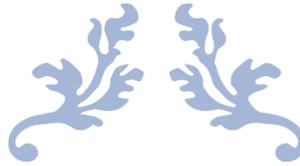
**RAQAMLI TEXNOLOGIYALARNING
YANGI O'ZBEKISTON
RIVOJIGA TA'SIRI**

Xalqaro ilmiy-amaliy
konferensiyasi to'plami

21 IYUN

2023





**RAQAMLI TEXNOLOGIYALARNING YANGI O'ZBEKISTON
RIVOJIGA TA'SIRI**

**ВЛИЯНИЕ ЦИФРОВЫХ ТЕХНОЛОГИЙ НА РАЗВИТИЕ
НОВОГО УЗБЕКИСТАНА**

**IMPACT OF DIGITAL TECHNOLOGIES ON THE DEVELOPMENT
OF NEW UZBEKISTAN**

Xalqaro ilmiy-amaliy konferensiyasi maqolalar to'plami



JUNE 21, 2023
KOKAND UNIVERSITY

"O'zbekiston Respublikasi Oliy ta'lim tizimini 2030 yilgacha rivojlantirish konsepsiyasini tasdiqlash to'g'risida" O'zbekiston Respublika Prezidentining 5847-sonli Farmonida ko'zda tutilgan vazifalardan biri – ilmiy izlanish yutuklarini amaliyotga joriy etish yo'li bilan fan sohalarini rivojlantirish, ya'ni xalqaro ilmiy hamjamiyatda e'tirof etilishiga xizmat qilishdir. Shu va boshqa tegishli farmonlarda va qarorlarda belgilangan vazifalarini amalga oshirish maqsadida 2023 yil 21-iyun kuni Qo'qon universiteti "Raqamli texnologiyalar va matematika" kafedrası "Raqamli texnologiyalarning Yangi O'zbekiston rivojiga ta'siri" mavzusidagi xalqaro miqyosida o'tkaziladigan ilmiy-amaliy konferensiyasi maqolalar to'plamini e'lon qiladi



MAS'UL MUHARRIR

Zahidov G'ofurjon Erkinovich – iqtisodiyot fanlari bo'yicha falsafa doktori, dotsent

TAHRIRIYAT HAY'ATI

G'ulomov Saidahrur Saidahmedovich – iqtisodiyot fanlari doktori, akademik;

Ahmedov Durbek Quدراتillayevich - iqtisodiyot fanlari doktori, professor;

Mahmudov Nosir Mahmudovich – iqtisodiyot fanlari doktori, professor;

Butaboyev Muhammadjon - iqtisodiyot fanlari doktori, professor;

Islamov Anvar Ashirkulovich - iqtisodiyot fanlari bo'yicha falsafa doktori, dotsent;

Ruziev Shohrusbek Ravshan o'g'li - iqtisodiyot fanlari bo'yicha falsafa doktori, dotsent

Mulaydinov Farxod Murotovich – Qo'qon universiteti, Raqamli texnologiyalar va matematika kafedrası mudiri

Texnik muharrir – Solidjonov Dilyorjon Zoirjon o'g'li



Ta'lim sifati yangi O'zbekiston taraqqiyotini yanada yuksaltirishning muhim omili / Raqamli texnologiyalarning Yangi O'zbekiston rivojiga ta'siri xalqaro ilmiy-amaliy konferensiyasi to'plami. Kokand university, 2023 yil 21 iyun, - «Innovatsion rivojlanish nashriyot-matbaa uyi» 2023.

© Matn. Mualliflar, 2023.

© Kokand university, 2023.

© «Innovatsion rivojlanish nashriyot-matbaa uyi», original maket, 2023.

38	INGLIZ TILI DARSLARIDA ONLINE PLATFORMALARDAN FOYDALANISH ORQALI QIZIQARLI DARS MUHITINI TASHKIL QILISH - Dilyorjon Solidjonov	156-158
3-SHO'BA. TIBBIYOTDA RAQAMLI TEXNOLOGIYALARDAN INSON SALAMATLIGI YO'LIDA FOYDALANISHNING ZAMONAVIY USUL VA VOSITALARI		
39	SHIFOKORLAR TOMONIDAN BEMORLARGA BERILADIGAN DORI RO'YHATINI RAQAMLASHTIRISH - Hakimova Dilnozaxon Sa'dulla qizi	160-163
40	AI IN THE MEDICAL FIELD: TRANSFORMING HEALTHCARE THROUGH INNOVATION - Erkinboev Sardorbek Ravshanbek o'g'li, Khasanov Akhmadjon Odiljon o'g'li, Erkinboyeva Madinabonu Afzaljon qizi	164-186
41	ИСПОЛЬЗОВАНИЕ АНАЛИТИКИ БОЛЬШИХ ДАННЫХ В ЗДРАВООХРАНЕНИИ - Имомназаров Хуршид Озодбаевич	187-190
42	ANORNING MEVASINING ZAMONAVIY XALQ TIBBIYOTIDA QO'LLANILISHI - Yusupova Moxidil Abdumutalibovna	191-194
43	DORIVOR XOM ASHYOSI PO'STLOQ XISOBLANGAN O'SIMLIKLARNI O'RGANISH VA ULARDAN OLINADIGAN PREPARATLARNI TIBBIYOTDA QO'LLANILISHI - M.A.Abdurahimova, SH.Z.Tursunaliyev	195-197
44	DORIVOR XOM ASHYOSI PO'STLOQ XISOBLANGAN O'SIMLIKLARNI O'RGANISH VA ULARDAN OLINADIGAN PREPARATLARNI TIBBIYOTDA QO'LLANILISHI - M. A. Abdurahimova	198-200
45	SOG'LIQNI SAQLASH VA XAVFSIZLIK XIZMATINING FUNKTSIONAL O'RGANISH VA TAHLIL QILISH - Xalmatov Misliddin Muxammatovich	201-203
46	TIBBIYOT TASVIRLARINI SEGMENTASIYA QILISH USULI - F.F. Meliyev	204-207
4-SHO'BA. ILMIY VA TEXNIK ISHLANMALAR SOHASIDA INNOVATSIYALARNI ISHLAB CHIQUISHDA RAQAMLI TEXNOLOGIYALARDAN FOYDALANISH		
47	FORECASTING GROSS DOMESTIC PRODUCT (GDP) AND GDP GROWTH: AN EXPLORATION OF IMPROVED PREDICTION USING MACHINE LEARNING ALGORITHMS - Azibaev Akhmadkhon Gulomjon ugli	209-214
48	ПОТОЧНЫЕ АЛГОРИТМЫ ШИФРОВАНИЯ С МАЛЫМ РАЗМЕРОМ ПАМЯТИ - Жураев Г.У., Икрамов А.А., Мухаммадиев Ф.Р.	215-217
49	АППАРАТНО-ОРИЕНТИРОВАННЫЕ ПОТОКОВЫЕ ШИФРЫ - Алаев Р.Х., Абдуллаев Т.Р., Бозоров О.Н., Фармонов Б.Д.	218-219
50	XARM 5ROBOTIDA INDUKTIV DATCHIK VA BO'G'INLAR SINXRON ISHLASH TIZIMINI LOYIHALASHAVTOMATLASHTIRISH - Abbosxon Qobiljonov Anvar o'g'li, Mirzayev Oybek Mahmudjon o'g'li	220-225
51	ТЕХНОЛОГИИ БОЛЬШИХ ДАННЫХ: ИННОВАЦИОННЫЙ ПУТЬ РАЗВИТИЯ ПРЕДПРИНИМАТЕЛЬСТВА - Худайбердиев Отабек Абсаломович	226-229
52	ЦИФРОВОЕ ПРЕДПРИНИМАТЕЛЬСТВО: КАК ЦИФРОВЫЕ ТЕХНОЛОГИИ МЕНЯЮТ ПРЕДПРИНИМАТЕЛЬСКИЙ ПРОЦЕСС - Ибрагимов Улмас Рахмонович	230-232
53	YUQORI MARGANETSLI YEYILISHGA BARDOSHLI 110Г13Л PO'LATNI ERITISH VA QUYISH TEXNOLOGIYASINI TAKOMILLASHTIRISH - Xayitboyev Qudratbek Anvarbek o'g'li	233-237
54	ЦИФРОВАЯ ТЕХНОЛОГИЯ ПРИ СТРОИТЕЛЬНОЙ ЧАСТИ ЗДАНИЙ И СООРУЖЕНИЙ АВТОТРАНСПОРТНЫХ ПРЕДПРИЯТИЙ - Ишмуратов Хикмат Кахарович	238-240

АППАРАТНО-ОРИЕНТИРОВАННЫЕ ПОТОКОВЫЕ ШИФРЫ**¹Алаев Р.Х., ¹Абдуллаев Т.Р., ¹Бозоров О.Н., ¹Фармонов Б.Д.**¹Национальный университет Узбекистана имени Мирзо Улугбека
mr.ruhullo@gmail.com, timurar@yandex.ru, boburfarmonov93@mail.ru

Аннотация: статья посвящена особенностям работы аппаратно-ориентированных потоковых шифров таких как: Trivium, Trivia-SC, TriviA-ck, Kreyvium, а также проблемам их реализации и стойкости к различным атакам.

Ключевые слова: потоковый шифр, аппаратно-ориентированный, Trivium, Kreyvium, кубическая атака.

Серия Trivium - это аппаратно-ориентированные потоковые шифры с чрезвычайно простой конструкцией, которые принимают структуру из трех взаимосвязанных NFSR с функциями обратной связи низкой степени и функциями линейного или квадратичного фильтра.

Trivium принадлежит к финальному портфелю eSTREAM, который принимает 80-битный ключ и 80-битный IV, генерирует до 264 битов ключевого потока. Он содержит 288-битное внутреннее состояние. На каждом этапе 15 битов конкретного состояния извлекаются в трех квадратичных функциях обратной связи для обновления 3 бита внутреннего состояния при инициализации и генерации потока ключей, а 6 из них подвергаются линейной операции XOR для вычисления бита потока ключей.

После загрузки ключа и IV состояние меняется в течение 1152 раундов для инициализации без выходов [1].

Хотя его простая конструкция, вероятно, уязвима для возможных разрушительных атак, несмотря на это, он выдерживает длительный период общественного контроля. Его основные атаки - это кубическая атака против Trivium с уменьшенным количеством раундов, и самый известный результат - 855 раундов, в то время как на его полную версию атаки не было обнаружено, что вселяет больше уверенности в такой простой дизайн.

Trivia-SC - это поточный шифр, модифицированный по сравнению с Trivium, с гораздо большим внутренним состоянием для аутентифицированного алгоритма шифрования TriviA-ck (v2), представленного на конкурс CAESAR. Trivia-SC загружается со 128-битным ключом и 128-битным IV и использует три NFSR размером 132, 105 и 147 бит соответственно. Он также извлекает 15 конкретных битов состояния в трех квадратичных функциях обратной связи для обновления 3 битов внутреннего состояния на каждом шаге,

в то время как квадратичный член других двух битов состояния добавляется к линейной сумме для вычисления бита ключевого потока. Его инициализация аналогична Trivium на 1152 раунда. Trivia-SC поддерживает распараллеливание до 64 бит. Его основные атаки - также кубические атаки против версии с уменьшенным количеством раундов, и самый известный результат просто превышает баррикаду из 1000 раундов.

Kreyvium ориентирован на эффективное сжатие гомоморфного зашифрованного текста, состоящего из пяти регистров. В то время как модификацией Trivium является 128-битный верхний регистр и 128-битный нижний регистр, три средних регистра длиной 93, 84, 111 бит соответствуют Trivium [2]. Kreyvium требует 128-битной защиты и принимает 128-битный ключ и 128-битный IV. Его начальная загрузка отличается от случая с Trivium, то есть IV и ключ также загружаются в верхний и нижний регистры соответственно. Кроме того, инициализация аналогична Trivium на 1152 раунда. На каждом шаге ключ и IV линейно участвуют в обновлении состояния, и ключ также линейно участвует в генерации потока ключей. Самая известная отличительная атака против Крейвия с уменьшенным количеством раундов - 872.

ЛИТЕРАТУРА:

1. Christof Paar, Jan Pelzl, "Stream Ciphers", Chapter 2 of "Understanding Cryptography, A Textbook for Students and Practitioners". Springer, 2009. pp.25-26.
2. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. – Триумф, 2013. – 816 с. – ISBN 978-5-89392-527-2. С.168-170.