Kokand University

RAQAMLI TEXNOLOGIYALARNING YANGI O‘ZBEKISTON RIVOJIGA TA’SIRI

Xalqaro ilmiy-amaliy konferensiyasi to'plami

21 IYUN

2023

kokanduni.uz

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” kafedrasi “Raqamli texnologiyalarning Yangi O‘zbekiston rivojiga ta’siri” mavzusidagi xalqaro miqyosida o‘tkaziladigan ilmiy-amaliy konferensiyasi maqolalar to’plamini e‘lon qiladi

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.

38	**INGLIZ TILI DARSLARIDA ONLINE PLATFORMALARDAN FOYDALANISH ORQALI QIZIQARLI DARS MUHITINI TASHKIL QILISH -** Dilyorjon Solidjonov	156-158
3-SHO‘BA. TIBIIYOTDA RAQAMLI TEXNOLOGIYALARDAN INSON SALAMATLIGI YO‘LIDA FOYDALANISHNING ZAMONAVIY USUL VA VOSITALARI		
39	**SHIFOKORLAR TOMONIDAN BEMORLARGA BERILADIGAN DORI RO‘YHATINI RAQAMLASHTIRISH -** Xakimova 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 CHIQISHDA 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 ПРЕДПРИНИМАТЕЛЬВА -** 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

ПОТОЧНЫЕ АЛГОРИТМЫ ШИФРОВАНИЯ С МАЛЫМ РАЗМЕРОМ ПАМЯТИ

[1]Жураев Г.У., [2]Икрамов А.А., [1]Мухаммадиев Ф.Р.
[1]Национальный университет Узбекистана имени Мирзо Улугбека
[2] Институт математики имени В. И. Романовского АН РУз
gjuraev@mail.ru, a.ikramov@mathinst.uz, firdavsmukhammadiyev@gmail.com

Аннотация: статья посвящена проблемам разработки криптографических алгоритмов для устройств с ограниченными ресурсами, в частности таких алгоритмов как потоковые шифры малого состояния. Рассматриваются различные методы разработки потоковых шифров малого состояния.

Ключевые слова: потоковый шифр, RFID технология, CKU потоковый шифр, атака TMDTO.

Потоковые шифры малого состояния. В настоящее время технология RFID широко используется для контроля доступа, высокоскоростной зарядки, идентификации, отслеживания грузов и других областях. Интернет вещей с комбинацией технологий RFID, который является типичным примером нового поколения информатизации постепенно проникает в жизнь людей в различных аспектах. Надежная передача информации для Интернета вещей должна основываться на криптографических алгоритмах для предоставления услуг безопасности, и как криптографический алгоритм, использующий среду, он в основном имеет следующие характеристики [1]: компоненты приложений, как правило, представляют собой встроенные процессоры с меньшей вычислительной мощностью; хранилище, доступное для вычислений, часто невелико из-за ограниченного ресурса. Потребляемая мощность должна контролироваться в определенном диапазоне с учетом функциональных требований. Следовательно, традиционные криптографи-ческие алгоритмы не могут хорошо адаптироваться к этой ограниченной среде, что делает изучение облегченных криптографических алгоритмов актуальной проблемой. Важным принципом при разработке традиционных потоковых шифров является то, что размер внутреннего состояния как минимум в 2 раза превышает уровень безопасности, чтобы противостоять атакам TMDTO, что затрудняет разработку легких потоковых шифров с точки зрения аппаратной реализации [2,3]. Чтобы решить эту проблему, предлагается несколько новых облегченных конструкций потоковых шифров, основанных на структуре семейства Grain.

Метод первый. Разрешение на ключ фиксируется и хранится в некотором оборудовании, а область для хранения фиксированного значения намного меньше, чем регистр такой же длины, в FSE 2015 Армкнехт предложил метод проектирования, который разделяет внутреннее состояние потокового шифра на две части. частей, одно - это

переменное состояние, изменяющееся со временем, другое - фиксированное, что обычно реализуется путем повторного использования ключа для осуществимости. Таким образом, этот вид потоковых шифров также называется потоковым шифром CKU (непрерывное использование ключа), показанным на рисунке 5.7. Особенность таких потоковых шифров заключается в том, что ключ не только участвует в инициализации, но также работает для обновления состояния в ключевое поколение. Его типичными примерами являются потоковые шифры Sprout, Fruit, Plantlet, в которых ключевой раздел вверху является фиксированным, а разделы NFSR и LFSR являются изменяемыми. Состояния переменных в этих трех шифрах составляют 80, 80 и 101 бит соответственно, но все цели состоят в том, чтобы обеспечить 80-битную безопасность, которая равна длине ключа.

Метод второй. Функция обновления состояния большинства потоковых шифров либо при генерации ключевого потока, либо при инициализации состояния эффективно обратима. Как следствие, если злоумышленнику удастся восстановить какое-либо внутреннее состояние при генерации потока ключей, он также сможет восстановить соответствующее начальное состояние и, инвертируя инициализацию состояния, секретный ключ, который является процессом восстановления ключа при атаках TMDTO. Чтобы разрушить эту основу для атак TMDTO, алгоритм инициализации состояния шифра Lizard представляет собой первую реализацию FP (1) -режима, который работает следующим образом:

- Нагрузка: Sload = (IV, K);
- Смешивание: Sload → Smixed;
- Закалка: Sinit = Smixed ⊕ K.

Структура Lizard аналогична семейству Grain, а его 121-битное внутреннее состояние распределено по двум взаимосвязанным NFSR. Для достижения 80-битной безопасности требуется 120-битный ключ и 64-битный IV. Мы видим, что вычисление начального состояния из любого из более поздних внутренних состояний также возможно для Lizard, но секретный ключ не может быть эффективно вычислен из начального состояния из-за режима FP (1). Было доказано, что при использовании режима FP (1) можно достичь 2 3n-битной защиты от атак TMDTO, направленных на восстановление ключа для генератора ключевого потока с внутренним состоянием длины n вместо n/2-битной защиты.

ЛИТЕРАТУРА:

1. Oleksandr Potii; Nikolay Poluyanenko; Igor Stelnyk; Iryna Revak; Sergii Kavun; Tetiana Kuznetsova. Nonlinear-Feedback Shift Registers for Stream Ciphers. 2019 IEEE 2nd Ukraine

Conference on Electrical and Computer Engineering (UKRCON). 2-6 July 2019. DOI: 10.1109/UKRCON.2019.8879786. pp. 4-6.

2. D. Ajitha; Suhaib Ahmed; Firdous Ahmad; G. K. Rajini. Design of Area Efficient Shift Register and Scan Flip-Flop based on QCA Technology. 2021 International Conference on Emerging Smart Computing and Informatics (ESCI). 5-7 March 2021. DOI: 10.1109/ESCI50559.2021.9396977. – pp. 1-4.

3. Jianghua Zhong; Dongdai Lin. On Minimum Period of Nonlinear Feedback Shift Registers in Grain-Like Structure. IEEE Transactions on Information Theory (Volume: 64, Issue: 9, Sept. 2018). pp. 6429 – 6442. DOI: 10.1109/TIT.2018.2849392.