2.3 форма

ҒЫЛЫМИ ЕҢБЕКТЕР ТІЗІМІ

р/с №	Еңбектерінің аты	Қол жазба немесе баспа	Баспа аты, журналдың аты (№, жыл), авторлық куәлік №	Баспа табақ немесе бет саны,	Жұмыс серіктес авторларының фамилиясы
1	Линейные преобразования в современных симметричных блочных алгоритмах шифрования	Баспа	Материалы III Международной научной конференции «Информатика и прикладная математика», часть 2, 26-29 сентября 2018 г., Алматы, - стр.213-220	8	Капалова Н.А., Хаумен А., Дюсенбаев Д.С.
2	Модуль бойынша дәрежеге шығару негізінде ақпаратты криптографиялық қорғау алгоритмінің модификациясы	Баспа	Хабаршы ҚазККА, №4, 2018ж., - 247-253 б.	7	Капалова Н.А., Хомпыш А.
3	Algebraic cryptanalysis of block ciphers	Баспа	Atlantis press, 2019 International Conference on Wireless Communication, Network and Multimedia Engineering (WCNME 2019). Advances in Computer Science Research, volume 89, P. 129-132	4	Rustem Biyashev, Dilmuhanbet Dyusenbayev, Nursulu Kapalova
4	Криптоанализ генератора псевдослучайных последовательностей и ее модификация	Баспа	Вестник КазНИТУ №3, 2019г., - стр.179-185	6	Р.Г. Бияшев, Н.А. Капалова, Д.С. Дюсенбаев, А. Хомпыш
5	ЕМ түрлендіру әдісі негізінде жасалған блокты шифрлеу алгоритміне жүргізілген бағалау тесттері	Баспа	Материалы IV международной научно-практической конференции "Информатика и прикладная математика", 25-29 сентября 2019 г., Алматы, - стр. 580-587	8	Капалова Н.А., Хомпыш А.

Ізденуші К.Т. Алғазы

Ғалым хатшы О.А. Усатова

6	Результаты проверки «лавинного эффекта» алгоритма «AL01»	Баспа	Материалы IV международной научно-практической конференции "Информатика и прикладная математика", 25-29 сентября 2019 г., Алматы, - стр. 602-607	6	Бияшев Р.Г., Дюсенбаев Д.С., Ержанов Е.Б.
7	Investigation of the different implementations for the new cipher Qamal	Баспа	Proceedings of the 12th International Conference on Security of Information and Networks. Sochi, Russia September, 2019 (в базе scopus)	8	R. Biyashev, N. Kapalova, L. Babenko, E. Ishchukova, S.Nyssanbayeva
8	«AL01» шифрлау алгоритміне криптографиялық талдау	Баспа	Хабаршы ҚазҰТЗУ, №5, 2019ж., - 92-98 б.	7	Капалова Н., Дюсенбаев Д., Сақан Қ.
9	«MODNPSS14» шифрлау алгоритміне криптографиялық талдау	Баспа	Хабаршы ҚазККА, №3, 2019 ж., - стр.235-243 б.	6	ДюсенбаевД.С. Сақан Қ.С., Хомпыш А.
10	Исследование дифференциальных свойств нового Алгоритма шифрования Qamal	Баспа	Материалы Международной научно-практической конференции «Актуальные проблемы информационной безопасности в Казахстане» 15 января 2020 г., - стр.97-105	9	Бабенко Л.К., Бияшев Р.Г., Ищукова Е.А., Капалова Н.А., Нысанбаева С.Е.
11	Исследование разработанных алгоритмов по критерию «лавинного эффекта»	Баспа	Материалы Международной научно-практической конференции «Актуальные проблемы информационной безопасности в Казахстане» 15 января 2020 г., - стр.107-119	12	Бияшев Р.Г., Хомпыш А.

Ізденуші К.Т. Алғазы

Ғалым хатшы О.А. Усатова

12	Encryption algorithm "Qamal NPNS"based on a nonpositional polynomial notation	Баспа	Вестник КазНУ им. аль-Фараби №1, 2020г., - стр.198-208	10	R.G. Biyashev, A. Smolarz, A.Khompysh
13	Результаты линейного криптоанализа шифра Qamal.	Баспа	Вестник АУЭС №2, 2020г., - стр.96-105	9	Бияшев Р.Г., Дюсенбаев Д.С., Сакан К.С.
14	О некоторых способах улучшения производительности вычисления блока mixer2 алгоритма шифрования «Qamal»	Баспа	Вестник КазНИТУ №4, 2020г., - стр.492-499	8	Сакан К.С., Дюсенбаев Д.С.
15	A block encryption algorithm based on exponentiation transform	Баспа	*Cogent Engineering* (2020), No. 7 (1788292) https://doi.org/10.1080/23311916.2020.1788292 (в базе **Scopus, процентиль 62**)	12	Nursulu Kapalova, Ardabek Khompysh, Müslüm Arici
16	Исследование алгоритмов шифровании «Al01» и «Qamal» на основе алгебраического криптоанализа	Баспа	Вестник КазНИТУ №5, 2020г., - стр.620-629	8	Дюсенбаев Д.С., Сакан К.С.
17	Криптографиялық хеш алгоритмдер жасаудың әртүрлі жолдарын қарастыру	Баспа	Материалы V международной научно-практической конференции "Информатика и прикладная математика", 29 сентября – 01 октября 2020 г., Алматы, - стр. 374-378	4	Сакан К.С.
18	Принципы построения блочных шифров и требования к ним	Баспа	Материалы V международной научно-практической конференции "Информатика и прикладная математика", 29 сентября – 01 октября 2020 г., Алматы, - стр. 378-384	4	Сакан К.С.
19	Исследование разработанного алгоритма на основе преобразования ЕМ по критерию «лавинного эффекта»	Баспа	Вестник КазАТК №3, 2020г., - стр.284-292	8	Капалова Н.А., Хомпыш А.

Ізденуші К.Т. Алғазы

Ғалым хатшы О.А. Усатова

20	Differential Cryptanalysis of New Qamal Encryption Algorithm	Баспа	International journal of electronics and telecommunications, No 4, 2020, P. 647-653. (в базе **Scopus, процентиль 27**)	7	L.K. Babenko, R.G. Biyashev, E.A. Ishchukova, N.A. Kapalova, S.E. Nysynbaeva, Andrzej Smolarz
21	Development and Analysis of Symmetric Encryption Algorithm Qamal Based on a Substitution-permutation Network	Баспа	International journal of electronics and telecommunications, No 1, 2021, P. 127-132. (в базе **Scopus, процентиль 27**)	6	R.G. Biyashev, N.A. Kapalova, D.S. Duysenbayev, Waldemar Wojcik, Andrzej Smolarz
22	Программа для шифрования файлов «Qamal v 1.0.1»		Авторлық куәлік 2019 жылғы 06 қыркүйек, № 5200		Бияшев Р.Г., Қапалова Н. А., Дюсенбаева Д.С., Сақан Қ.С.

Ізденуші К.Т. Алғазы

Ғалым хатшы О.А. Усатова