

ҚАЗАҚСТАН РЕСПУБЛИКАСЫ
БІЛІМ ЖӘНЕ ҒЫЛЫМ МИНИСТРЛІГІ

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ
РЕСПУБЛИКИ КАЗАХСТАН



ҚазҰТУ ХАБАРШЫСЫ _____

_____ **ВЕСТНИК КазНУ**

VESTNIK KazNRTU _____

№2 (126)

Главный редактор
И. К. Бейсембетов – ректор

Зам. главного редактора
Б.К. Кенжалиев – проректор по науке

Отв. секретарь
Н.Ф. Федосенко

Редакционная коллегия:

С.Б. Абдыгаппарова, Б.С. Ахметов, З.С. Абишева- акад. НАНРК, Л.Б. Атымтаева, Ж.Ж. Байгунчеков- акад. НАНРК, А.Б. Байбатша, А.О. Байконурова, В.И. Волчихин (Россия), К. Дребенштед (Германия), Г.Ж. Жолтаев, Р.М. Искаков, С.Е. Кудайбергенов, С.Е. Кумеков, В.А. Луганов, С.С. Набойченко – член-корр. РАН, И.Г. Милев (Германия), С. Пежовник (Словения), Б.Р. Ракишев – акад. НАН РК, М.Б. Панфилов (Франция), Н.Т. Сайлаубеков, А.Р. Сейткулов, Фатхи Хабаши (Канада), Бражендра Мишра (США), Корби Андерсон (США), В.А. Гольцев (Россия), В. Ю. Коровин (Украина), М.Г. Мустафин (Россия), Фан Хуаан (Швеция), Х.П. Цинке (Германия), Т.А. Чепуштанова, Г.Ж. Елигбаева, Б.У. Куспангалиев

Учредитель:

Казахский национальный исследовательский технический университет
имени К.И. Сатпаева

Регистрация:

Министерство культуры, информации и общественного согласия
Республики Казахстан № 951 – Ж “25” 11. 1999 г.

Основан в августе 1994 г. Выходит 6 раз в год

Адрес редакции:

г. Алматы, ул. Сатпаева, 22,
каб. 616, тел. 292-63-46
Nina. Fedorovna. 52 @ mail.ru

Пыркова А.Ю., Темирбекова Ж.Е.

Симметриялық шифрлеуді mbed платформасында жүзеге асыру

Түйіндемесі. Бұл мақала криптографиялық бағдарламалау және BLE Nano жиынтығы микроконтроллерінде жұмыс істейтін кодтық ортаны құрайтын Arm Mbed TLS платформасы туралы жазылған. Бағдарламасының тиімділігін арттыру үшін C орнына негізгі тіл ретінде C++ пайдаланылды.

Түйін сөздер: BLE Nano kit микроконтроллері, Mbed платформасы, Arm Mbed TLS, криптография.

UDC 004.056.55

A. Pyrkova, Zh.E. Temirbekova

(Al-farabi Kazakh national university, Almaty, Republic of Kazakhstan,

temyrbekovazhanerke2@gmail.com)

POSSIBILITIES OF USING A BLE NANO KIT MICROCONTROLLER TO DEVELOP CRYPTOGRAPHIC LIBRARIES

Abstract. Nowadays, the number of IoT (Internet of Things) devices are growing rapidly around the world with wide range of purposes. Many types of these devices collect data and depending on their purpose, some of the data can be highly sensitive for the user. This calls for security on the device which has to secure the collected data and send it to a server through the Internet. Using TLS (Transport Layer Security) is a great way to provide such a security and one part of it is the data encryption which is the main focus of this thesis. The problem is that IoT devices are often made out of microprocessors having a low computational power and performance.

This article compiles some of the programming and debugging techniques writing the mbed platform, the code environment running on our BLE Nano kit microcontroller. C++ was used as the core language instead of C, in order to increase programming effectiveness. This turned out to be a good choice, but came at the cost of increased program size. Thus, a big part of optimizing was spent on reducing program and data size. Then demonstrate. The main goal of this thesis is to determine AES (Advanced Encryption Standard) symmetric encryption algorithms, security and space complexity using a specific encryption library from ARM mbed.

Keywords: IOT, BLE Nano kit microcontroller, C++, mbed platform, Arm Mbed TLS, AES cryptography.

BLE Nano kit is the smallest Bluetooth 4.1 Low Energy (BLE) development board in the market [1]. The core is Nordic nRF51822 (an ARM Cortex-M0 SoC plus BLE capability) running at 16MHz with ultra low power consumption.

Developing a Bluetooth Smart enabled 'accessory' (accessory device + companion application) is easier than ever [2]. You can quickly produce prototypes and demos target for IoT and other interesting projects. BLE Nano could operate under 1.8V to 3.3V, therefore it works with a lot of electronic components.

Features:

- Smallest BLE development board, only 18.5mm x 21.0mm
- Nordic nRF51822 ARM Cortex-M0 SoC supports both BLE Central and BLE Peripheral roles
- 2.4 G Hz transceiver
- Ultra low power consumption
- Support voltage from 1.8V to 3.3V
- Software development using mbed.org, GCC, Keil or Arduino
- Lots of libraries and examples available
- Easy firmware deployment with the MK20 USB board
- Work with our free Android App and iOS App

BLE Nano kit microcontroller supported hardware platforms on mbed. The mbed Microcontrollers are a series of ARM microcontroller development boards designed for rapid prototyping [3-4].

The mbed platform is a free C/C++ compiler and IDE provided by ARM and suitable for programming most ARM microcontrollers. The IDE is Web based, something which may back some of us down. I was myself skeptical about the practicality of such IDE compilers, however I must say the mbed compiler has proven to be easy to use, fast and (reasonably) friendly, even for a C/C++ compiler [5-6].

The many available platform libraries are easy to use and well designed, specially for starters, resembling (vaguely) the simplicity you may have enjoyed when using Arduino libraries. Also, mbed

encourages and eases sharing with others your own libraries, or any piece/snippet of code. You have to register a username in the platform from the very beginning, that will allow you to store your projects online, comment, share code and participate in the community forums comfortably [7-8]. Compiling and programming your projects is really easy. You can literally have the blink test application running in a few minutes.

mbed has a dedicated team which develops and maintains a very nice Bluetooth Low Energy API. You can rest assured that using this API for learning to develop BLE accessories will be much easier (and faster) than trying to do so by using directly the BLE libraries (Soft Device) provided by Nordic [9-10]. The BLE API includes also several application examples.

On the not-so-positive side of mbed platform, you have zero control over the compiler/linker. This has proven to be a showstopper for our own BLE development [11-12]. At the time of this writing, within mbed you are only allowed to develop BLE applications for the nRF51822 along with the S110 Soft Device, which only supports peripheral mode. Hence, you can quickly start to develop applications with mbed which only require the Peripheral Role. But if you want to develop an application requiring the Central Role, you will have to switch to a full-fledged GCC (or Keil or IAR) C/C++ compiler [13].

Entry-level Online Compiler–Nothing to Install: Browser-based IDE, Immediately compiling examples or writing your own, Best in class RealView Compiler in the back end (Figure 1).

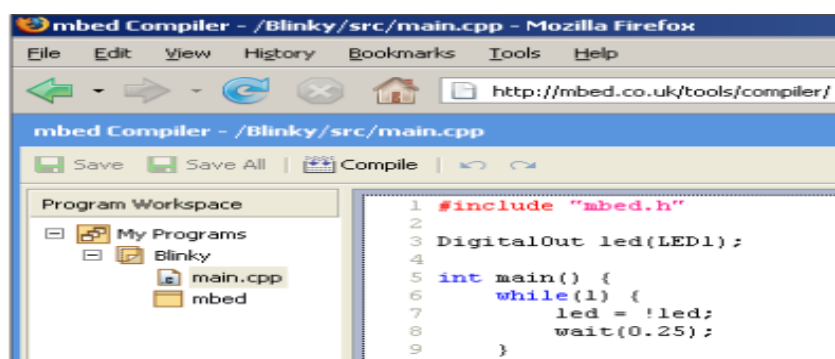


Figure 1. mbed Compiler C++ on a Microcontroller

The first firmware's for our BLE Nano kit microcontrollers were written in the “traditional” language C++ [14-15]. C++ is a pretty convoluted “multi paradigm” programming language: supporting standard structured programming, object-oriented programming as well as metaprogramming. It is one of the few languages giving the programmer absolute control over memory allocation and placement and functions-call overhead, which is crucial on a restricted environment.

Using BLE Nano Kit microcontroller tested program in the ARM mbed platform (read characters).

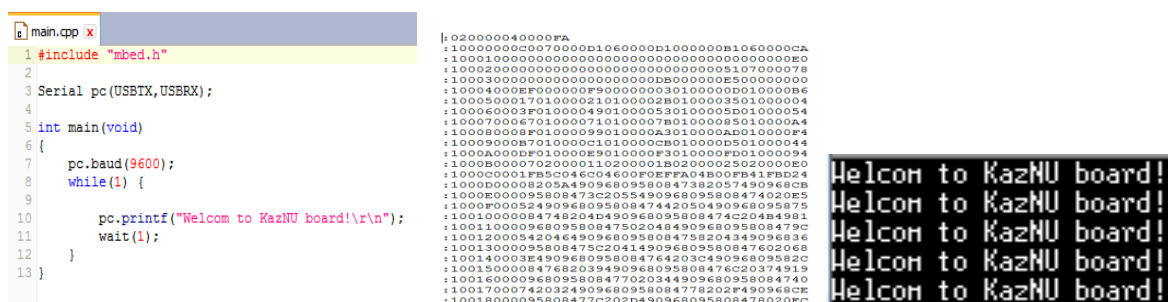


Figure 2. Read characters in C++

In order to provide security of data transmitted back and forth from an IoT device to a server, the communication has to be encrypted. Cryptography is the practice and study of techniques for secure communication and has been around for a long time. One of the cryptographic protocols is the TLS (Transport layer security) protocol where the data are encrypted with ciphers to protect them from third parties through the Internet.

The use of the ARM mbed TLS library with the BLE Nano microcontroller is an appropriate match, because they are made by the same company, so compatibility errors are less likely and cause security problems.

Arm mbed TLS makes it easy for developers to include cryptographic and SSL / TLS functions in their (embedded) products, which facilitates this functionality with minimal code printing [16]. It offers an SSL / TLS library with an intuitive API and readable source code and includes a complex set of tests [17]. You can create it out of the box in most systems or manually select and configure functions.

The mbed TLS library provides a set of cryptographic components that you can use and compile separately, and include or exclude, using a single configuration header file. mbed TLS also provides a central SSL / TLS module, which is based on cryptographic components, abstraction layers and support components to ensure full protocol implementation for SSL and TLS.

Cryptographic library

The cryptographic part of mbed TLS has abstraction layers for Public Key cryptography, Hashing (Message Digests) and Symmetric Ciphers [18]. It also contains standards-based random number generators and an entropy pool.

All cryptographic algorithms are implemented as loosely-coupled modules. You can just take the appropriate header files and source code files and drop them in your project as needed.

mbed TLS provides the most commonly used algorithms, such as AES. mbed TLS supports an alternative implementation for most of its cryptographic modules. The usual use case is for hardware accelerated cryptographic engines. There are several methods for alternative implementations: special function replacement and complete module replacement [19].

The [configuration file](#) contains the cryptography modules, which you can replace with alternative implementation [20]. These are named MBEDTLS_<MODULE NAME>_ALT. In order to support alternative implementation for a module, uncomment the corresponding *_ALT definition. Function replacement is according to the function name, with the suffix of _ALT. To support hardware entropy source, enable MBEDTLS_ENTROPY_HARDWARE_ALT in the configuration file.

AES is based on a design principle known as a substitution-permutation network, a combination of both substitution and permutation, and is fast in both software and hardware. AES is a variant of Rijndael which has a fixed block size of 128 bits, and a key size of 128, 192, or 256 bits. By contrast, the Rijndael specification *per se* is specified with block and key sizes that may be any multiple of 32 bits, with a minimum of 128 and a maximum of 256 bits.

In each round, the AES uses the four following operations [21]:

- SubBytes: Each byte of the array is transformed using a nonlinear substitution box called the AES S-Box. The S-Box in the AES has been carefully constructed and the cipher uses only one S-Box throughout the encryption.

- ShiftRows: Is a transposition step which ensures that the last three rows of the array are shifted by a different number of byte positions.

- MixColumns: Mixes each column in the array to create even more diffusion.

- Addkey: Using bitwise XOR, each byte of the array is mixed with a byte of a sub-key material, also called round-key [22]. The sub-key is made by "key expansion" and is derived from the main cipher key using a Rijndael key-schedule.

The overall structure of the cipher begins with a key expansion before going in to the pre-whitening which only includes AddKey. Then the rounds performing Sub-Bytes, ShiftRows, MixColumns and Add-Key will loop for $n-1$ rounds where n is the numbers of rounds. The n -th round or final round does not include MixColumns and produce the output ciphertext.

AES context structure. buf is able to hold 32 extra bytes, which can be used [23]:

- for alignment purposes if VIA padlock is used.

- to simplify key expansion in the 256-bit case by generating an extra round key.

AES-CBC buffer encryption/decryption. Length should be a multiple of the block size (16 bytes).

Upon exit, the content of the IV is updated so that you can call the function same function again on the following block(s) of data and get the same result as if it was encrypted in one call. This allows a "streaming" usage. If on the other hand you need to retain the contents of the IV, you should either save it manually or use the cipher module instead. param ctx-AES context, param mode-MBEDTLS_AES_ENCRYPT or MBEDTLS_AES_DECRYPT, param length-length of the input data, param iv -initialization vector (updated after use), param input-buffer holding the input data, param output-buffer holding the output data, return 0 if successful, or MBEDTLS_ERR_AES_INVALID_INPUT_LENGTH.

```

small_aes.c
1 #include "small_aes.h"
2
3 static const unsigned int rcon[] = {
4     0x01000000, 0x02000000, 0x04000000, 0x08000000,
5     0x10000000, 0x20000000, 0x40000000, 0x80000000,
6     0x1B000000, 0x36000000,
7 };
8
9
10 static const unsigned int Te[256] = {
11     0xc66363a5U, 0xf87c7c84U, 0xee777799U, 0xf67b7b8dU,
12     0xff2f2f20U, 0xd66b6bbdU, 0xde6f6fb1U, 0x91c5c554U,
13     0xe0303050U, 0x02010103U, 0xce6767a9U, 0x562b2b7dU,
14     0xe7fe7e19U, 0xb5d7d762U, 0x4dabab6eU, 0xec76769aU,
15     0x8fcaca45U, 0x1f82829dU, 0x89c9c940U, 0xfa7d7d87U,
16     0xeffa7a15U, 0xb25959ebU, 0x6e4747c9U, 0xdb70700bU,
17     0x41adadecU, 0xb3d4d467U, 0x5fa2a2fdU, 0x45afa2faU,
18     0x239c9cbfU, 0x53a4a4f7U, 0xe4727296U, 0x9bc0c05bU,
19     0x75b7b7c2U, 0xe1fdfd1cU, 0x3d9393aeU, 0x4c26266aU,
20     0x6c36365aU, 0x7e323241U, 0xf5f7f702U, 0x83ccc44U,
21     0x6834345cU, 0x51a5a5f4U, 0xd1e5e534U, 0xf9f1f108U,
22     0xe2717193U, 0xabdbdb73U, 0x62313153U, 0x2a15153fU,
23     0x0804040cU, 0x95c7c752U, 0x46232365U, 0x9dc3c35eU,
24     0x30181828U, 0x379696a1U, 0x0a05050fU, 0x2f9a9ab5U,
25     0x0e070709U, 0x24121236U, 0x1b80809bU, 0xdfe2e23aU,
26     0xcdcbeb26U, 0x4e272769U, 0x7fb2b2cdU, 0xea75759fU,
27     0x1209091bU, 0x1d83839eU, 0x582c2c74U, 0x341a1a2eU,
28 };
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60
61
62
63
64
65
66
67
68
69
70
71
72
73
74
75
76
77
78
79
80
81
82
83
84
85
86
87
88
89
90
91
92
93
94
95
96
97
98
99
100
101
102
103
104
105
106
107
108
109
110
111
112
113
114
115
116
117
118
119
120
121
122
123
124
125
126
127
128
129
130
131
132
133
134
135
136
137
138
139
140
141
142
143
144
145
146
147
148
149
150
151
152
153
154
155
156
157
158
159
160
161
162
163
164
165
166
167
168
169
170
171
172
173
174
175
176
177
178
179
180
181
182
183
184
185
186
187
188
189
190
191
192
193
194
195
196
197
198
199
200
201
202
203
204
205
206
207
208
209
210
211
212
213
214
215
216
217
218
219
220
221
222
223
224
225
226
227
228
229
230
231
232
233
234
235
236
237
238
239
240
241
242
243
244
245
246
247
248
249
250
251
252
253
254
255
256
257
258
259
260
261
262
263
264
265
266
267
268
269
270
271
272
273
274
275
276
277
278
279
280
281
282
283
284
285
286
287
288
289
290
291
292
293
294
295
296
297
298
299
300
301
302
303
304
305
306
307
308
309
310
311
312
313
314
315
316
317
318
319
320
321
322
323
324
325
326
327
328
329
330
331
332
333
334
335
336
337
338
339
340
341
342
343
344
345
346
347
348
349
350
351
352
353
354
355
356
357
358
359
360
361
362
363
364
365
366
367
368
369
370
371
372
373
374
375
376
377
378
379
380
381
382
383
384
385
386
387
388
389
390
391
392
393
394
395
396
397
398
399
400
401
402
403
404
405
406
407
408
409
410
411
412
413
414
415
416
417
418
419
420
421
422
423
424
425
426
427
428
429
430
431
432
433
434
435
436
437
438
439
440
441
442
443
444
445
446
447
448
449
450
451
452
453
454
455
456
457
458
459
460
461
462
463
464
465
466
467
468
469
470
471
472
473
474
475
476
477
478
479
480
481
482
483
484
485
486
487
488
489
490
491
492
493
494
495
496
497
498
499
500
501
502
503
504
505
506
507
508
509
510
511
512
513
514
515
516
517
518
519
520
521
522
523
524
525
526
527
528
529
530
531
532
533
534
535
536
537
538
539
540
541
542
543
544
545
546
547
548
549
550
551
552
553
554
555
556
557
558
559
560
561
562
563
564
565
566
567
568
569
570
571
572
573
574
575
576
577
578
579
580
581
582
583
584
585
586
587
588
589
590
591
592
593
594
595
596
597
598
599
600
601
602
603
604
605
606
607
608
609
610
611
612
613
614
615
616
617
618
619
620
621
622
623
624
625
626
627
628
629
630
631
632
633
634
635
636
637
638
639
640
641
642
643
644
645
646
647
648
649
650
651
652
653
654
655
656
657
658
659
660
661
662
663
664
665
666
667
668
669
670
671
672
673
674
675
676
677
678
679
680
681
682
683
684
685
686
687
688
689
690
691
692
693
694
695
696
697
698
699
700
701
702
703
704
705
706
707
708
709
710
711
712
713
714
715
716
717
718
719
720
721
722
723
724
725
726
727
728
729
730
731
732
733
734
735
736
737
738
739
740
741
742
743
744
745
746
747
748
749
750
751
752
753
754
755
756
757
758
759
760
761
762
763
764
765
766
767
768
769
770
771
772
773
774
775
776
777
778
779
780
781
782
783
784
785
786
787
788
789
790
791
792
793
794
795
796
797
798
799
800
801
802
803
804
805
806
807
808
809
810
811
812
813
814
815
816
817
818
819
820
821
822
823
824
825
826
827
828
829
830
831
832
833
834
835
836
837
838
839
840
841
842
843
844
845
846
847
848
849
850
851
852
853
854
855
856
857
858
859
860
861
862
863
864
865
866
867
868
869
870
871
872
873
874
875
876
877
878
879
880
881
882
883
884
885
886
887
888
889
890
891
892
893
894
895
896
897
898
899
900
901
902
903
904
905
906
907
908
909
910
911
912
913
914
915
916
917
918
919
920
921
922
923
924
925
926
927
928
929
930
931
932
933
934
935
936
937
938
939
940
941
942
943
944
945
946
947
948
949
950
951
952
953
954
955
956
957
958
959
960
961
962
963
964
965
966
967
968
969
970
971
972
973
974
975
976
977
978
979
980
981
982
983
984
985
986
987
988
989
990
991
992
993
994
995
996
997
998
999
1000
1001
1002
1003
1004
1005
1006
1007
1008
1009
1010
1011
1012
1013
1014
1015
1016
1017
1018
1019
1020
1021
1022
1023
1024
1025
1026
1027
1028
1029
1030
1031
1032
1033
1034
1035
1036
1037
1038
1039
1040
1041
1042
1043
1044
1045
1046
1047
1048
1049
1050
1051
1052
1053
1054
1055
1056
1057
1058
1059
1060
1061
1062
1063
1064
1065
1066
1067
1068
1069
1070
1071
1072
1073
1074
1075
1076
1077
1078
1079
1080
1081
1082
1083
1084
1085
1086
1087
1088
1089
1090
1091
1092
1093
1094
1095
1096
1097
1098
1099
1100
1101
1102
1103
1104
1105
1106
1107
1108
1109
1110
1111
1112
1113
1114
1115
1116
1117
1118
1119
1120
1121
1122
1123
1124
1125
1126
1127
1128
1129
1130
1131
1132
1133
1134
1135
1136
1137
1138
1139
1140
1141
1142
1143
1144
1145
1146
1147
1148
1149
1150
1151
1152
1153
1154
1155
1156
1157
1158
1159
1160
1161
1162
1163
1164
1165
1166
1167
1168
1169
1170
1171
1172
1173
1174
1175
1176
1177
1178
1179
1180
1181
1182
1183
1184
1185
1186
1187
1188
1189
1190
1191
1192
1193
1194
1195
1196
1197
1198
1199
1200
1201
1202
1203
1204
1205
1206
1207
1208
1209
1210
1211
1212
1213
1214
1215
1216
1217
1218
1219
1220
1221
1222
1223
1224
1225
1226
1227
1228
1229
1230
1231
1232
1233
1234
1235
1236
1237
1238
1239
1240
1241
1242
1243
1244
1245
1246
1247
1248
1249
1250
1251
1252
1253
1254
1255
1256
1257
1258
1259
1260
1261
1262
1263
1264
1265
1266
1267
1268
1269
1270
1271
1272
1273
1274
1275
1276
1277
1278
1279
1280
1281
1282
1283
1284
1285
1286
1287
1288
1289
1290
1291
1292
1293
1294
1295
1296
1297
1298
1299
1300
1301
1302
1303
1304
1305
1306
1307
1308
1309
1310
1311
1312
1313
1314
1315
1316
1317
1318
1319
1320
1321
1322
1323
1324
1325
1326
1327
1328
1329
1330
1331
1332
1333
1334
1335
1336
1337
1338
1339
1340
1341
1342
1343
1344
1345
1346
1347
1348
1349
1350
1351
1352
1353
1354
1355
1356
1357
1358
1359
1360
1361
1362
1363
1364
1365
1366
1367
1368
1369
1370
1371
1372
1373
1374
1375
1376
1377
1378
1379
1380
1381
1382
1383
1384
1385
1386
1387
1388
1389
1390
1391
1392
1393
1394
1395
1396
1397
1398
1399
1400
1401
1402
1403
1404
1405
1406
1407
1408
1409
1410
1411
1412
1413
1414
1415
1416
1417
1418
1419
1420
1421
1422
1423
1424
1425
1426
1427
1428
1429
1430
1431
1432
1433
1434
1435
1436
1437
1438
1439
1440
1441
1442
1443
1444
1445
1446
1447
1448
1449
1450
1451
1452
1453
1454
1455
1456
1457
1458
1459
1460
1461
1462
1463
1464
1465
1466
1467
1468
1469
1470
1471
1472
1473
1474
1475
1476
1477
1478
1479
1480
1481
1482
1483
1484
1485
1486
1487
1488
1489
1490
1491
1492
1493
1494
1495
1496
1497
1498
1499
1500
1501
1502
1503
1504
1505
1506
1507
1508
1509
1510
1511
1512
1513
1514
1515
1516
1517
1518
1519
1520
1521
1522
1523
1524
1525
1526
1527
1528
1529
1530
1531
1532
1533
1534
1535
1536
1537
1538
1539
1540
1541
1542
1543
1544
1545
1546
1547
1548
1549
1550
1551
1552
1553
1554
1555
1556
1557
1558
1559
1560
1561
1562
1563
1564
1565
1566
1567
1568
1569
1570
1571
1572
1573
1574
1575
1576
1577
1578
1579
1580
1581
1582
1583
1584
1585
1586
1587
1588
1589
1590
1591
1592
1593
1594
1595
1596
1597
1598
1599
1600
1601
1602
1603
1604
1605
1606
1607
1608
1609
1610
1611
1612
1613
1614
1615
1616
1617
1618
1619
1620
1621
1622
1623
1624
1625
1626
1627
1628
1629
1630
1631
1632
1633
1634
1635
1636
1637
1638
1639
1640
1641
1642
1643
1644
1645
1646
1647
1648
1649
1650
1651
1652
1653
1654
1655
1656
1657
1658
1659
1660
1661
1662
1663
1664
1665
1666
1667
1668
1669
1670
1671
1672
1673
1674
1675
1676
1677
1678
1679
1680
1681
1682
1683
1684
1685
1686
1687
1688
1689
1690
1691
1692
1693
1694
1695
1696
1697
1698
1699
1700
1701
1702
1703
1704
1705
1706
1707
1708
1709
1710
1711
1712
1713
1714
1715
1716
1717
1718
1719
1720
1721
1722
1723
1724
1725
1726
1727
1728
1729
1730
1731
1732
1733
1734
1735
1736
1737
1738
1739
1740
1741
1742
1743
1744
1745
1746
1747
1748
1749
1750
1751
1752
1753
1754
1755
1756
1757
1758
1759
1760
1761
1762
1763
1764
1765
1766
1767
1768
1769
1770
1771
1772
1773
1774
1775
1776
1777
1778
1779
1780
1781
1782
1783
1784
1785
1786
1787
1788
1789
1790
1791
1792
1793
1794
1795
1796
1797
1798
1799
1800
1801
1802
1803
1804
1805
1806
1807
1808
1809
1810
1811
1812
1813
1814
1815
1816
1817
1818
1819
1820
1821
1822
1823
1824
1825
1826
1827
1828
1829
1830
1831
1832
1833
1834
1835
1836
1837
1838
1839
1840
1841
1842
1843
1844
1845
1846
1847
1848
1849
1850
1851
1852
1853
1854
1855
1856
1857
1858
1859
1860
1861
1862
1863
1864
1865
1866
1867
1868
1869
1870
1871
1872
1873
1874
1875
1876
1877
1878
1879
1880
1881
1882
1883
1884
1885
1886
1887
1888
1889
1890
1891
1892
1893
1894
1895
1896
1897
1898
1899
1900
1901
1902
1903
1904
1905
1906
1907
1908
1909
1910
1911
1912
1913
1914
1915
1916
1917
1918
1919
1920
1921
1922
1923
1924
1925
1926
1927
1928
1929
1930
1931
1932
1933
1934
1935
1936
1937
1938
1939
1940
1941
1942
1943
1944
1945
1946
1947
1948
1949
1950
1951
1952
1953
1954
1955
1956
1957
1958
1959
1960
1961
1962
1963
1964
1965
1966
1967
1968
1969
1970
1971
1972
1973
1974
1975
1976
1977
1978
1979
1980
1981
1982
1983
1984
1985
1986
1987
1988
1989
1990
1991
1992
1993
1994
1995
1996
1997
1998
1999
2000
2001
2002
2003
2004
2005
2006
2007
2008
2009
2010
2011
2012
2013
2014
2015
2016
2017
2018
2019
2020
2021
2022
2023
2024
2025
2026
2027
2028
2029
2030
2031
2032
2033
2034
2035
2036
2037
2038
2039
2040
2041
2042
2043
2044
2045
2046
2047
2048
2049
2050
2051
2052
2053
2054
2055
2056
2057
2058
2059
2060
2061
2062
2063
2064
2065
2066
2067
2068
2069
2070
2071
2072
2073
2074
2075
2076
2077
2078
2079
2080
2081
2082
2083
2084
2085
2086
2087
2088
2089
2090
2091
2092
2093
2094
2095
2096
2097
2098
2099
2100
2101
2102
2103
2104
2105
2106
2107
2108
2109
2110
2111
2112
2113
2114
2115
2116
2117
2118
2119
2120
2121
2122
2123
2124
2125
2126
2127
2128
2129
2130
2131
2132
2133
2134
2135
2136
2137
2138
2139
2140
2141
2142
2143
2144
2145
2146
2147
2148
2149
2150
2151
2152
2153
2154
2155
2156
2157
2158
2159
2160
2161
2162
2163
2164
2165
2166
2167
2168
2169
2170
2171
2172
2173
2174
2175
2176
2177
2178
2179
2180
2181
2182
2183
2184
2185
2186
2187
2188
2189
2190
2191
2192
2193
2194
2195
2196
2197
2198
2199
2200
2201
2202
2203
2204
2205
2206
2207
2208
2209
2210
2211
2212
2213
2214
2215
2216
2217
2218
2219
2220
2221
2222
2223
2224
2225
2226
2227
2228
2229
2230
2231
2232
2233
2234
2235
2236
2237
2238
2239
2240
2241
2242
2243
2244
2245
2246
2247
2248
2249
2250
2251
2252
2253
2254
2255
2256
2257
2258
2259
2260
2261
2262
2263
2264
2265
2266
2267
2268
2269
2270
2271
2272
2273
2274
2275
2276
2277
2278
2279
2280
2281
2282
2283
2284
2285
2286
2287
2288
2289
2290
2291
2292
2293
2294
2295
2296
2297
2298
2299
2300
2301
2302
2303
2304
2305
2306
2307
2308
2309
2310
2311
2312
2313
2314
2315
2316
2317
2318
2319
2320
2321
2322
2323
2324
2325
2326
2327
2328
2329
2330
2331
2332
2333
2334
2335
2336
2337
2338
2339
2340
2341
2342
2343
2344
2345
2346
2347
2348
2349
2350
2351
2352
2353
2354
2355
2356
2357
2358
2359
2360
2361
2362
2363
2364
2365
2366
2367
2368
2369
2370
2371
2372
2373
2374
2375
2376
2377
2378
2379
2380
2381
2382
2383
2384
2385
2386
2387
2388
2389
2390
2391
2392
2393
2394
2395
2396
2397
2398
2399
2400
2401
2402
2403
2404
2405
2406
2407
2408
2409
2410
2411
2412
2413
2414
2415
2416
2417
2418
2419
2420
2421
2422
2423
2424
2425
2426
2427
2428
2429
2430
2431
2432
2433
2434
2435
2436
2437
2438
2439
2440
2441
2442
2443
2444
2445
2446
2447
2448
2449
2450
2451
2452
2453
2454
2455
2456
2457
2458
2459
2460
2461
2462
2463
2464
2465
2466
2467
2468
2469
2470
2471
2472
2473
2474
2475
2476
2477
2478
2479
24
```

- [12] Li, S.; Xu, L.D. and Zhao, S., "The internet of things: a survey", Information Systems Frontiers, vol. 17, No.2, pp 243-259, April 2015, DOI:10.1007/s10796-014-9492-7
- [13] Atmel Corporation, "Integrating the Internet of Things: Necessary building blocks for broad market adoption", San Jose, USA: Atmel, 0776 Corporate IOT WhitePaper US 102014.
- [14] Knudsen, L.R.; Robshaw, M.J. The Block Cipher Companion, New York: Springer-Verlag, - 2011. – pp. 225-228
- [15] Nermin Hajdarbegovic, "Are We Creating An Insecure Internet of Things (IoT) Security Challenges and Concerns", 2015. [Online] Available: <https://www.toptal.com/it/are-we-creating-an-insecure-internet-of-things>.
- [16] Jessica Chani Cahuana, Chalmers, A Search for a Convenient Data Encryption Algorithm For an Internet of Things Device. – 2016. - p. 102
- [17] Bartlett, Alan and Richard Silverman "SSH: The Secure Shell The Definitive Guide." - 31 July 2001. – p. 98
- [18] Dierks, T. & C. Allen. "The TLS Protocol Version 1.0." - 1999. -p. 100
- [19] Hiller, Janine S. and Ronnie Cohen. Internet Law & Policy. Upper Saddle River: Prentice Hall, - 2000.
- [20] Martin, Franck. "SSL Certificates HOWTO." - 20 October 2002.
- [21] Alex Biryukov and Dmitry Khovratovich, Related-key Cryptanalysis of the Full AES-192 and AES-256, "Archived copy". Archived from the original on 2009-09-28. Retrieved 2018-02-16.
- [22] "Rijndael". Archived from the original on January 25, 2018. Retrieved March 1, 2018.
- [23] Daemen, Joan; Rijmen, Vincent. "AES Proposal: Rijndael". National Institute of Standards and Technology. – 2003. - p. 10.

Пыркова А.Ю., Темирбекова Ж.Е.

Возможности использования микроконтроллера BLE Nano Kit для разработки криптографических библиотек

Аннотация. В настоящее время количество устройств IoT (Internet of Things) быстро растет во всем мире с широким спектром задач. Многие типы этих устройств собирают данные и в зависимости от их назначения некоторые данные могут быть очень чувствительны для пользователя. Это требует безопасности на устройстве, которое должно защищать собранные данные и отправлять их на сервер через Интернет. Использование TLS (Transport Layer Security) - отличный способ обеспечить такую безопасность, и одна из них - это шифрование данных, которое является основным направлением этого тезиса. Проблема в том, что устройства IoT часто изготавливаются из микропроцессоров с низкой вычислительной мощностью и производительностью.

В этой статье описаны некоторые методы программирования и отладки, написанные на платформе mbed, среда кода, работающая на нашем микроконтроллере BLE Nano. C ++ использовался как основной язык вместо C, чтобы повысить эффективность программирования. Таким образом, большая часть оптимизации была потрачена на сокращение размера программы и данных. Затем продемонстрировано. Основная цель этой статьи - определить симметричные алгоритмы шифрования AES (Advanced Encryption Standard), безопасность и сложность пространства, используя специальную библиотеку шифрования из ARM mbed.

Ключевые слова: IOT, микроконтроллер BLE Nano kit, C ++, платформа mbed, Arm Mbed TLS, криптография AES.

Пыркова А.Ю., Темирбекова Ж.Е.

Криптографиялық кітапханаларды дамыту үшін BLE Nano Kit микроконтроллерді қолдану мүмкіндіктері

Түйіндеме. Қазіргі уақытта IoT (Интернет заттар) құрылғыларының саны бүкіл әлем бойынша тез арада дамып келеді. Бұл құрылғылардың көптеген түрлері деректерді жинайды және олардың мақсаттарына байланысты кейбір деректер пайдаланушыға өте сезімтал болуы мүмкін. Бұл жинақталған деректерді қорғап, Интернет арқылы серверге жіберуге тиіс құрылғыдағы қауіпсіздікті талап етеді. TLS (Transport Layer Security) - бұл қауіпсіздікті қамтамасыз етудің керемет тәсілі және оның бір бөлігі деректерді шифрлау болып табылады, ол осы мақаланың негізгі бағыты болып табылады. Мәселе мынада, IoT құрылғылары жиі есептеу қуаты мен өнімділігі төмен микропроцессорлардан жасалады.

Бұл мақала Mbed платформасында жазатын программалау және BLE Nano kit жинағының микроконтроллерінде жұмыс істейтін шифрлау кодын есептеу ортасы болып табылады. Бағдарламаның тиімділігін арттыру үшін C орнына негізгі тіл ретінде C++ пайдаланылды. Бұл жақсы таңдау болып шықты, бірақ бағдарламаның көлемін ұлғайтты. Осылайша оңтайландырудың үлкен бөлігі бағдарлама мен деректер көлемін азайтуға жұмсалды. Содан кейін есептеу нәтижесі бейнеленген. Осы мақаланың негізгі мақсаты ARM платформасында арнайы шифрлау кітапханасын пайдаланып, AES (Advanced Encryption Standard) симметриялы шифрлау алгоритмін анықтау болып табылады.

Түйін сөздер: IoT, BLE Nano kit микроконтроллері, C ++, Mbed платформасы, Arm Mbed TLS, AES криптографиясы.

<i>Мұстафин М.А.</i>	
ГЕОМЕТРИЯЛЫҚ САЛУҒА ЕСЕП ӘДІСІ А.П.КИСЕЛЕВ КЛАССИФИКАЦИЯСЫ.....	471
<i>Пыркова А.Ю., Темирбекова Ж.Е.</i>	
СИММЕТРИЯЛЫҚ ШИФРЛЕУДІ МВЕД ПЛАТФОРМАСЫНДА ЖҮЗЕГЕ АСЫРУ	473
<i>Пыркова А.Ю., Темирбекова Ж.Е.</i>	
КРИПТОГРАФИЯЛЫҚ КІТАПХАНАЛАРДЫ ДАМУҒА ҮШІН BLE NANO КІТ МИКРОКОНТРОЛЛЕРДІ ҚОЛДАНУ МҮМКІНДІКТЕРІ.....	477
<i>Қадырбаева Ж.М., Абдулла Ж.С.</i>	
ДИФФЕРЕНЦИАЛДЫҚ ТЕНДЕУЛЕРДІ ШЕШУДЕ MAPLE ПРОГРАММАЛЫҚ ПАКЕТІН ҚОЛДАНУ.....	482
<i>Дробышев А., Алдияров А., Ақтаев Д., Жексен Ұ.</i>	
CH ₄ +H ₂ O ҚОСПАСЫНЫҢ КРИОКОНДЕНСАТТАРЫНЫҢ ҮЛДІРЛЕРІН ИҚ-СПЕКТРОМЕТРЛІК ЗЕРТТЕУ.....	486
<i>Қадырбаева Ж.М., Мырзахмет Д.К.</i>	
ЖӘЙ ДИФФЕРЕНЦИАЛДЫҚ ТЕНДЕУЛЕР ЖҮЙЕСІ ҮШІН КӨПНҮКТЕЛІ ШЕТТІК ЕСЕПТІ ШЕШУДІҢ САНДЫҚ ЖҮЗЕГЕ АСЫРЫЛУЫ.....	495
<i>Мұстафин М.А.</i>	
ҚАТАРЛАР ЖАЙЛЫ В.П.ЕРМАКОВТЫҢ ТЕОРЕМАСЫ ЖӘНЕ МАТЕМАТИКАЛЫҚ ТАЛДАУДАҒЫ МАҢЫЗЫ.....	502
<i>Накысбеков Ж.Т., Буранбаев М.Ж., Габдуллин М.Т., Айтжанов М.Б., Суюндыкова Г.С., Досеке У.</i>	
МЫС НАНОҰНТАҒЫНЫҢ РЕНТГЕНҚҰРЫЛЫМДЫҚ ТАЛДАУЫ.....	503
<i>Тастанбек Н.Е.</i>	
ЖЕР СТАНЦИЯСЫНА АРНАЛҒАН L-ДИАПАЗОНДЫ АНАЛОГТЫҚ ҚАБЫЛДАҒЫШТЫ ADS ПРОГРАММАЛЫҚ ЖАБДЫҒЫ АРҚЫЛЫ ҚҰРАСТЫРУ.....	510
<i>Маусымбекова С.Д., Кан К., Тенизбай Р.</i>	
АТМОСФЕРАДА ЗИЯНДЫ ГАЗДАРДЫҢ ТАРАЛУЫНА ТЕМПЕРАТУРАЛЫҚ СТРАТИФИКАЦИЯНЫҢ ӘСЕРІН САНДЫҚ ЗЕРТТЕУ.....	519
<i>Қадирбаева Ж.М., Утегенова А.А.</i>	
ЕКІНШІ РЕТТІ ЖӘЙ ДИФФЕРЕНЦИАЛДЫҚ ТЕНДЕУ ҮШІН СЫЗЫҚТЫҚ ЕМЕС ШЕТТІК ЕСЕПТІ ШЕШУДІҢ САНДЫҚ ЖҮЗЕГЕ АСЫРЫЛУЫ.....	526
<i>Алдабергенова Т.М., Кислицин С.Б.,</i>	
ТОЗАҢДАТУ КОЭФФИЦИЕНТІ ЖӘНЕ 100 КЭВ ЭНЕРГИЯЛЫ АРГОН ИОНДАРЫМЕН СӘУЛЕЛЕНДІРІЛГЕН ГРАФИТ БЕТІНІҢ ҚҰРЫЛЫМЫ.....	533
<i>Божанов Е.Т., Хайруллин Е.М., Сауранбаева А.</i>	
КЕШЕНДІ ҚАТТЫЛЫҚТЫҢ АЙНЫМАЛЫ КОЭФФИЦИЕНТТЕРІ БАР ТІЗБЕКТІК ҮШӨЛШЕМДІ ЖҮЙЕНІҢ ІШКІ ЭКВИВАЛЕНТТІ ҚАБАТЫН БҮГІЛУ.....	540
<i>Божанов Е.Т., Енсебаева М.З., Дадаева А.Н.</i>	
МАТЕМАТИКАЛЫҚ МОДЕЛІН БАҚЫРАЙТУДЫ ТУРАЛЫ ТІЗБЕКТІ ДВУХМАССОВОЙ ҚАТЫСТЫ ЖҮЙЕСІН ТАСЫМАЛДАУҒА МҰНАЙ ҚОСПАЛАРЫ.....	550
<i>Айтқазина Ә.А., Бейсенбекова Г.Ж., Салимханова А.С.</i>	
ОНЛАЙН ОҚЫТУ КУРСТАРЫН ДАЙЫНДАУДЫҢ АҚПАРАТТЫҚ ҚОЛДАУ ЖҮЙЕСІ.....	555
<i>Саитов А.Т., Әзімханова М.Т.</i>	
GEOPORTAL ҚҰРУДЫҢ ӘДІСТЕРІ ЖӘНЕ ESRI GEOPORTAL SERVER-Н БАПТАУ.....	561

Химия-металлургия ғылымдары

<i>Төрепашқызы Б.Т., Бергенжанова Г.Р., Беркутбаева Р.А., Қуандыкова А.А., Шалбулов Ш.Ж.</i>	
ЖЭО-ДАҒЫ МАЗУТТЫ ЖАҒУ.....	569
<i>Жантасов Қ.Т., Зұлхұхар Ж.Т., Шалатаев С.Ш., Әбдікерімова Ұ.Б.</i>	
ИМИНОДИАЦЕТОНИТРИЛДІ ӨНДІРУДІҢ ЗАМАНАУИ ЖАҒДАЙЫ.....	573
<i>Сапарбай Ш.К., Мендыбаев Т.М.</i>	
ТЕМІР-БОРИД ҚОРЫТПАСЫН ПАЙДАЛАНЫП МАШИНА БӨЛШЕКТЕРІН ҚАЛПЫНА КЕЛТІРУ.....	578
<i>Хамитова Б.М., Тасыбаева Ш.Б., Серікұлы Ж.</i>	
ӨСІМДІК МАЙЛАРЫНЫҢ ҚҰРАМЫНДАҒЫ БИОЛОГИЯЛЫҚ БЕЛСЕНДІ ЗАТТЫҢ АНТИОКСИДАНТТЫҚ ӘСЕРІ.....	582

<i>Мурадов А.Д., Сандыбаев Е.Е.</i> АНАЛИЗ СТРУКТУРЫ ПОВЕРХНОСТИ ПОЛИМИДНЫХ КОМПОЗИЦИОННЫХ ПЛЕНОК МЕТОДОМ АТОМНО-СИЛОВОЙ МИКРОСКОПИИ.....	468
<i>Мустафин М.А.</i> КЛАССИФИКАЦИЯ ПО А.П.КИСЕЛЕВУ МЕТОДОВ РЕШЕНИЯ ЗАДАЧ НА ПОСТРОЕНИЕ.....	471
<i>Пыркова А.Ю., Темирбекова Ж.Е.</i> ВЫПОЛНЕНИЕ СИММЕТРИЧНОГО ШИФРОВАНИЯ В MVED ПЛАТФОРМЕ.....	473
<i>Пыркова А.Ю., Темирбекова Ж.Е.</i> ВОЗМОЖНОСТИ ИСПОЛЬЗОВАНИЯ МИКРОКОНТРОЛЛЕРА BLE NANO KIT ДЛЯ РАЗРАБОТКИ КРИПТОГРАФИЧЕСКИХ БИБЛИОТЕК.....	477
<i>Кадирбаева Ж.М., Абдулла Ж.С.</i> ПРИМЕНЕНИЕ ПРОГРАММНОГО ПАКЕТА MAPLE ПРИ РЕШЕНИИ ДИФФЕРЕНЦИАЛЬНЫХ УРАВНЕНИЙ.....	482
<i>Дробышев А., Алдияров А., Ақтаев Д., Жексен У.</i> ИК-СПЕКТРОМЕТРИЧЕСКОЕ ИССЛЕДОВАНИЕ ПЛЕНОК КРИОКОНДЕНСАТОВ СМЕСИ CH ₄ +H ₂ O.....	486
<i>Кадирбаева Ж.М., Мырзахмет Д.К.</i> ЧИСЛЕННАЯ РЕАЛИЗАЦИЯ РЕШЕНИЯ МНОГОТОЧЕЧНОЙ КРАЕВОЙ ЗАДАЧИ ДЛЯ СИСТЕМ ОБЫКНОВЕННЫХ ДИФФЕРЕНЦИАЛЬНЫХ УРАВНЕНИЙ.....	495
<i>Мустафин М.А.</i> ТЕОРЕМА В.П.ЕРМАКОВА О РЯДАХ И ЕЁ ЗНАЧЕНИЕ В МАТЕМАТИЧЕСКОМ АНАЛИЗЕ.....	502
<i>Накысбеков Ж.Т., Буранбаев М.Ж., Габдуллин М.Т., Айтжанов М.Б., Суюндыкова Г.С., Досеке У.</i> РЕНТГЕНОСТРУКТУРНЫЙ АНАЛИЗ НАНОПОРОШКА МЕДИ.....	503
<i>Тастанбек Н.Е.</i> РАЗРАБОТКА АНАЛОГОВОГО ПРИЁМНИКА L-ДИАПАЗОНА ДЛЯ НАЗЕМНОЙ СТАНЦИИ С ПОМОЩЬЮ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ADS.....	510
<i>Маусумбекова С.Д., Кан К., Тенизбай Р.</i> ЧИСЛЕННОЕ ИССЛЕДОВАНИЕ ВЛИЯНИЯ СТРАТИФИКАЦИИ ПО ТЕМПЕРАТУРЕ НА РАСПРОСТРАНЕНИЕ ВРЕДНЫХ ГАЗОВ В АТМОСФЕРЕ.....	519
<i>Кадирбаева Ж.М., Утегенова А.А.</i> ЧИСЛЕННАЯ РЕАЛИЗАЦИЯ РЕШЕНИЯ НЕЛИНЕЙНОЙ КРАЕВОЙ ЗАДАЧИ ДЛЯ ОБЫКНОВЕННОГО ДИФФЕРЕНЦИАЛЬНОГО УРАВНЕНИЯ ВТОРОГО ПОРЯДКА.....	526
<i>Алдабергенова Т.М., Кислицин С.Б.</i> КОЭФФИЦИЕНТ РАСПЫЛЕНИЯ И СТРУКТУРА ПОВЕРХНОСТИ ГРАФИТА, ОБЛУЧЕННОГО ИОНАМИ АРГОНА С ЭНЕРГИЕЙ 100 КЭВ.....	533
<i>Божанов Е.Т., Хайруллин Е.М., Сауранбаева А.</i> ВЫПУЧИВАНИЕ ВНУТРЕННЕГО ЭКВИВАЛЕНТНОГО СЛОЯ ЦЕПНОЙ ТРЕХМАССОВОЙ СИСТЕМЫ С ПЕРЕМЕННЫМИ КОЭФФИЦИЕНТАМИ КОМПЛЕКСНОЙ ЖЕСТКОСТИ.....	540
<i>Божанов Е.Т., Енсебаева М.З., Дадаева А.Н.</i> О МАТЕМАТИЧЕСКОЙ МОДЕЛИ ВЫПУЧИВАНИЯ ЦЕПНОЙ ДВУХМАССОВОЙ СИСТЕМЫ, ПРИМЕНИТЕЛЬНО К ТРАНСПОРТИРОВКЕ НЕФТЯНОЙ СМЕСИ.....	550
<i>Айтказина А.А., Бейсенбекова Г.Ж., Салимханова А.С.</i> СИСТЕМА ИНФОРМАЦИОННОГО СОПРОВОЖДЕНИЯ ПОДГОТОВКИ ОНЛАЙН КУРСОВ.....	555
<i>Саитов А.Т., Азимханова М.Т.</i> СПОСОБЫ ЗАПУСКА СОБСТВЕННОГО ГЕОПОРТАЛА И НАСТРОЙКА ESRI GEOPORTAL SERVER.....	561

Химико-металлургические науки

<i>Төрешақызы Б.Т., Бергенжанова Г.Р., Беркутбаева Р.А., Куандыкова А.А., Шалбулов Ш.Ж.</i> ГОРЕНИЯ ТОПОЧНОГО МАЗУТА НА ТЭЦ.....	569
<i>Жантасов К.Т., Зулпухар Ж. Т., Шалатаев С.Ш., Әбдікерімова Ұ.Б.</i> СОВРЕМЕННОЕ СОСТОЯНИЕ ПРОИЗВОДСТВА ИМИНОДИАЦЕТОНИТРИЛА	573
<i>Сапарбай Ш.К., Мендибаев Т.М.</i> ВОССТАНОВЛЕНИЕ ДЕТАЛИ МАШИН ЖЕЛЕЗОБОРИДНЫМИ ПОКРЫТИЯМИ.....	578
<i>Хамитова Б.М., Тасыбаева Ш.Б., Серікұлы Ж.</i> АНТИОКСИДАНТНЫЕ СВОЙСТВА БИОЛОГИЧЕСКИ АКТИВНЫХ ВЕЩЕСТВ В СОСТАВЕ РАСТИТЕЛЬНЫХ МАСЕЛ.....	582

<i>Pyrkova A., Temirbekova Zh.E.</i> PERFORMING SYMMETRIC ENCRYPTION MBED PLATFORM.....	473
<i>Pyrkova A., Temirbekova Zh.E.</i> POSSIBILITIES OF USING A BLE NANO KIT MICROCONTROLLER TO DEVELOP CRYPTOGRAPHIC LIBRARIES.....	477
<i>Kadirbayeva Zh.M., Abdulla Zh.S.</i> APPLYING OF THE MAPLE PROGRAMMING PACKAGE AT SOLVING DIFFERENTIAL EQUATIONS.....	482
<i>Drobyshev A., Aldiyarov A., Aktayev A., Zhexen U.</i> IR SPECTROMETRIC STUDY OF CRYOCONDENSATE FILMS OF A MIXTURE OF CH ₄ +H ₂ O.....	486
<i>Kadirbayeva Zh.M., Myrzakhmet D.K.</i> NUMERICAL IMPLEMENTATION FOR SOLVING OF MULTIPOINT BOUNDARY VALUE PROBLEM FOR THE SYSTEM OF ORDINARY DIFFERENTIAL EQUATIONS.....	495
<i>Mustafin M.A.</i> V.P.ERMAKOV'S THEOREM ABOUT SERIES AND ITS IMPORTANCE IN MATHEMATICAL ANALYSIS.....	502
<i>Nakysbekov Zh.T., Buranbaev M.Zh., Gabdullin M.T., Aitzhanov M.B., Suyundykova G.S., Doseke U.</i> X-RAY DIFFRACTION ANALYSIS OF COPPER NANOPOWDER.....	503
<i>Tastanbek N.E.</i> DEVELOPMENT OF THE ANALOGUE L-RANGE RECEIVER FOR THE GROUND STATION WITH THE ADS SOFTWARE.....	510
<i>Mausymbekova S., Kan K., Tenizbay R.</i> NUMERICAL STUDY OF THE EFFECT OF TEMPERATURE STRATIFICATION ON THE PROPAGATION OF HARMFUL GASES IN THE ATMOSPHERE.....	519
<i>Kadirbayeva Zh.M., Utegenova A.A.</i> NUMERICAL IMPLEMENTATION FOR SOLVING OF A NONLINEAR BOUNDARY VALUE PROBLEM FOR SECOND-ORDER ORDINARY DIFFERENTIAL EQUATION.....	526
<i>Алдабергенова Т.М., Кислицин С.Б.</i> SPUTTERING COEFFICIENT AND SURFACE STRUCTURE OF GRAPHITE IRRADIATED WITH 100 KEV ARGON IONS.....	533
<i>Bozhanov E.T., Khairullin E.M., Sauranbayeva A.</i> BUCKLING OF THE INTERNAL EQUIVALENT LAYER OF CHAIN THREE MASS SYSTEM WITH COMPLEX STIFFNESS VARIABLE COEFFICIENTS.....	540
<i>Bozhanov E., Yesenbayeva M., Dadayeva A.</i> ABOUT THE VYPUCHIVANIYA MATHEMATICAL MODEL CHAIN TWO-MASS SYSTEM, APPLICABLE TO TRANSPORTATION OF OIL MIXTURE.....	550
<i>Aitkazina A.A., Beisenbekova G.Zh., Salimkhanova A.S.</i> INFORMATION SUPPORT SYSTEM FOR ONLINE COURSES.....	555
<i>Saitov A.T., Azimkhanova M.T.</i> THE WAYS OF LAUNCHING OWN GEOPORTAL AND SETTINGS OF ESRI GEOPORTAL SERVER	561

Chemical and metallurgical sciences

<i>Төрепашқызы Б.Т., Bergenzhanova G.R., Berkutbaeva R.A., Kuandikova A.A., Shalbulov Sh.Zh.</i> CARBONATE-CONTAINING ADDITIVE - CATALYST COMBUSTION OF FUEL OIL.....	569
<i>Zhantasov K.T., Zulpukhar Zh. T., Shalataev S.Sh., Abdikerimova U.B.</i> MODERN CONDITION OF PRODUCTION OF IMINODIACETONITRILE	573
<i>Saparbay S.K., Mendibayev T.M.</i> RESTORATION OF MACHINE PARTS WITH IRON-BORIDE COATINGS.....	578
<i>Khamitova B., Tassymbayeva Sh., Seriklyu Zh.</i> ANTIOXIDANT PROPERTIES OF BIOLOGICALLY ACTIVE SUBSTANCES IN THE COMPOSITION OF VEGETABLE OILS	582

Редакторы:

Н.Ф. Федосенко

Верстка на компьютере:

Л.Т. Касжанова

Подписано в печать 29.03.2018 г.

Формат 60x84 $\frac{1}{8}$. Усл. п.л 37,8.

Тираж 500 экз. Заказ № 207.

Адрес редакции:

ул. Сатпаева, 22, КазННТУ каб. 616, тел. 292-63-46 ,Nina.Fedorovna. 52 @ mail.ru

Департамент маркетинга и коммуникаций КазННТУ

Казахского национального исследовательского технического университета имени К.И. Сатпаева