Validation of implementation Kalyna Block Cipher with the help of test examples

Mariia Domina 1, Valeriy Hlukhov 2

1. Lviv Polytechnic National University, Ukraine, E-mail: [masha\_dyomina@ukr.net](mailto:masha_dyomina@ukr.net)
2. Lviv Polytechnic National University, Ukraine, E-mail: [glukhov@polynet.lviv.ua](mailto:glukhov@polynet.lviv.ua)

Abstract

The Kalyna block cipher was selected during Ukrainian National Public Cryptographic Competition (2007-2010) and its slight modification was approved as the new encryption standard of Ukraine in 2015. In this paper I present the software models of crypto algorithm, which are investigated to verify the correct implementation.

Кеуwords: paper, algorithm, cipher, key, encryption, decryption.

Introduction

“Kalyna” ia a block cipher with SPN-based (Rijndael-like) structure. It has increased MDS matrix size, a new set of four different S-boxes, pre- and postwhitening using modulo 264 addition and the key schedule based on the round function transformations only. “Kalyna” supports block size and key length of 128, 256 and 512 bits (key length can be either equal or double of the block size). In the Table 1, we have the number of rounds and the number of rows in the state matrix for different values of block size and key length.

*Table 1*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| № | Block size (l) | Key length (k) | Rounds (t) | Rows of the matrix (c) |
| 1 | 128 | 128 | 10 | 2 |
| 2 | 128 | 10 |
| 3 | 256 | 256 | 14 | 4 |
| 4 | 256 | 14 |
| 5 | 512 | 512 | 18 | 8 |

Kalyna is adopted as the new Ukrainian encryption standard DSTU 7624:2014 that also includes ten modes of operation and test vectors.

Checking the symmetric implementation of block cryptocurrencies and modes of its application by means of test examples is executed by testing using software module.

Implementation verification includes:

1) verification of correct implementation of the basic procedures defined in the draft perspective (functions deployment of cycle keys and basic transformations encryption and decryption) using test cases;

2) verification of the correct implementation of the modes of application defined in the draft promising national standard (gamma modes (CTR); ciphertext feedback (CFB); simulation insertion (CMAC); ciphertext coupling (CBC); feedback braking gamma code (OFB); selective accelerator production with accelerated imitation insertion (GCM, GMAC); production of imitating inserts and scaling (CCM); indexed replacement (XTS); Key Data Protection (KW)) using test cases.

The verification is performed sequentially - first the basic procedures and then the modes of application of the symmetric block cryptocurrency algorithm.

The implementation is considered validated if the basic procedures and all implemented operating modes of the algorithm have been tested.

Checking the implementation of basic transformations and modes of the algorithm is performed for different key lengths: 128, 256 or 512 bits. Also for different block lengths: 128, 256 or 512 bits.

Conclusion

The proposed promising cryptographic algorithm "Kalyna" provides the possibility of simultaneously ensuring the confidentiality and integrity of the message through the consistent application of appropriate transformations.

The standard software implementation of basic transformations of the block cipher “Kalyna” and corresponding application modes was developed using the high-level programming language C.

The correctness of the test program was investigated.

References

[1] A Melnyk - Advances in cyber-physical systems, 2016. [*Cyber-physical systems multilayer platform and research framework*](https://scholar.google.com.ua/scholar?oi=bibs&cluster=11531840343799784057&btnI=1&hl=ru)*.*

[2] V Hlukhov, A Kostyk, I Zholubak, M Rahma - Advances in Cyber-Physical Systems, 2 (2), 2017, 2017. [*Galois fields elements processing units for cryptographic data protection in cyber-physical systems*](javascript:void(0))*.*

[3] V Hlukhov, A Lukenyuk, S Shenderuk - Advances in Cyber-Physical Systems, 2016. [*Satellite scientific data collection and accumulation system as a basis for cyber-physical systems construction*](https://scholar.google.com.ua/scholar?oi=bibs&cluster=16187406270421515087&btnI=1&hl=ru)*.*

[4]A Melnyk - Advances in Cyber-Physical Systems, 2016. [*Parallel ordered-access machine computational model and architecture*](https://scholar.google.com.ua/scholar?oi=bibs&cluster=11794423692840069770&btnI=1&hl=ru)*.*

[5] A Botchkaryov, Y Kraikin - Advances in Cyber-Physical Systems, 2 (2), 2017, 2017. [*Wireless sensor-actuator network based on the SoC ESP8266 for mobile cyber-physical systems*](javascript:void(0))*.*