Analyses of A Lightweight Stream Cipher for RFID Encryption Model

김정태
목원대학교

RFID 암호 모델을 위한 경량화 스트림 암호 방식의 해석

Jung-Tae Kim
Mokwon University
E-mail : jtkim3050@mokwon.ac.kr

요 약

WG-7 is a stream cipher based on WG Stream Cipher and is designed by Y. Luo, Q. Chai, G. Gong, and X. Lai in 2010. This cipher is designed to implement in low cost and lightweight application such as RFID tags. In this paper, we survey and compare cryptographic module such as stream and block cipher. We can estimate security performance suitable to system.

Ⅰ. Introduction

For security applications in wireless sensor networks (WSNs), choosing best algorithms in terms of energy-efficiency and of small-storage requirements is a real challenge because the sensor networks must be design with limited resources. Sensor networks are made by the tremendous advances and convergence of micro-electro-mechanical systems (MEMS), wireless communication technologies and digital electronics. Sensor networks are composed of a large number of tiny devices or sensors which monitor their surrounding area to measure environmental information, to detect movements, vibrations, etc [1].

We take into consideration the problem of efficiently generating sequences in hardware for use in certain cryptographic algorithms. We show that sequences generated by linear feedback shift registers (LFSRs) in stream cipher can be tailored to pursuit the appropriate algorithms. For hardware implementation, this reduces both time and chip area. WG-7 is proposed as a fast, lightweight and secure stream cipher inspired by family of WG stream ciphers design principles. WG is a synchronous stream cipher submitted to ECRYPT call for stream ciphers. WG-7 and WG are hardware-oriented stream ciphers that use a word-oriented Linear Feedback Shift Register (LFSR) and a filter function based on Welch-Gong (WG) transformation [1].

II. Characteristics of LFSR

The results (computed using the skyeye + eSimu tools) concerning the number of cycles required to perform all the tests are summarized in the table 1.

Table 1. Number of CPU cycles for the stream ciphers using the testing framework

			nJ/byte				nJ/key	nJ/IV	nJ/byte
Algo.	Key	IV	Stream	40 bytes	576 bytes	1500 bytes	Key setup	IV setup	agility
Copy	80	80	38.32	60.85	16.84	142.07	70.54	67.29	145.35
RC4	128	0	465.17	9843.25	948.49	542.06	1243.66	379636.24	354.43
SNOW v2.0	128	128	438.34	1093.46	280.59	414.20	2656.66	41749.08	365.26
AES CTR	128	128	3587.00	2197.89	3437.36	3384.26	11378.81	2861.89	3499.45
DRAGON	128	128	514.26	2912.69	1144.53	1064.58	6846.80	74109.24	575.67
HC-256	128	128	471.39	102473.69	7577.28	3112.48	2540.02	2705307.85	864.11
HC-128	128	128	342.29	24264.78	1838.04	897.21	2540.20	950661.16	559.97
LEX	128	128	804.03	1186.80	670.42	714.16	8250.66	23850.60	868.13
Phelix	128	128	421.15	1470.51	461.14	454.71	20622.78	35111.32	461.26
Py	128	64	3894.22	5822.63	827.52	1101.62	145194.31	154181.03	1141.65
Pypy	128	56	817.35	6008.43	1859.92	1361.36	145194.15	161834.16	1300.67
Salsa20	128	64	952.19	1394.11	907.17	1275.82	6884.19	2215.93	1268.12
SOSEMANUK	128	64	247.93	6727.04	648.50	528.97	286119.29	20860.01	365.30

Table 2. Number of nJ for the stream ciphers using the testing framework

			cycles/byte				cycles/key	cycles/IV	cycles/byte
Algo.	Key	IV	Stream	40 bytes	576 bytes	1500 bytes	Key setup	IV setup	agility
Copy	80	80	2.19	3.72	1.00	7.58	4.40	4.19	7.78
RC4	128	0	26.97	610.95	58.53	33.29	76.41	23581.61	21.24
SNOW v2.0	128	128	25.08	66.38	16.82	23.71	163.41	2273.35	20.87
AES CTR	128	128	206.19	131.52	198.73	195.76	636.49	157.52	202.23
DRAGON	128	128	30.89	177.05	69.76	64.91	421.42	4497.61	33.60
HC-256	128	128	27.00	6044.76	446.11	183.17	141.75	198126.10	49.30
HC-128	128	128	19.35	1484.72	112.12	53.70	141.76	58194.93	31.67
LEX	128	128	47.07	71.41	40.32	41.92	501.41	1415.57	50.71
Phelix	128	128	25.61	90.15	28.36	26.77	1271.42	2154.61	26.99
Py	128	64	214.25	349.23	47.58	60.88	7713.83 z	9327.43	64.40
Pypy	128	56	44.78	360.95	103.91	74.72	7713.82	9660.11	73.46
Salsa20	128	64	57.54	84.57	55.05	73.07	367.70	118.07	72.60
SOSEMANUK	128	64	14.81	385.63	37.95	30.48	16374.01	1264.09	20.78

IV. Conclusion

The comparison between the results obtained in concerning the performances of block ciphers using several modes of operation and the stream ciphers presented will be more pertinent for its demands. We also can estimate the general characteristics for estimating performance produced by the addition of a stream cipher in a real sensor communication environment.

References

[1] D. Sauveron et al. (Eds.): WISTP 2007, LNCS 4462, pp. 202- 214, 2007.

[2] Yee Wei Law, Jeroen Doumen, and Pieter Hartel. Survey and benchmark of block ciphers for wireless sensor networks. ACM Trans. Sen. Netw., 2(1):65- 93, 2006.

[3] M. Gavrilova et al. (Eds.): ICCSA 2006, LNCS 3982, pp. 436- 445, 2006.

Acknowledgement

This research was supported by Basic Science Research Program through the National Research Foundation of Korea(NRF) funded by the Ministry of Education, Science and Technology(grant number:2011-0026950)