A Comparative Study on Lightweight Cryptography

M. U. Bokhari and Shabbir Hassan

Abstract The traditional cryptosystem only fulfills the requirements of desktop computing epoch. Renewable lightweight cryptography algorithms are developing to beat the constraints of traditional cryptosystem, which provide tradeoff among cipher sort, attack immune, key size, plaintext length, and performance. The implementation of LWC algorithms is carried out on retaining in the mind that it will be implemented in minimal power consumption, fewer area requirement and also enough efficiency so it turns out to be ideal for such a resource confine devices such as RFID tags and wireless sensor node. In this, we are trying to emerge with frequent LWC algorithms which are grouped into stream cipher, block cipher, and hybrid model, and also reveal them, at the last a comparison is conducted on the effective parameters.

Keywords Stream cipher · Hummingbird · ECC · WG · Sober PUF · HITAG2 · Grain

1 Introduction

As the current scenario, use of smart devices such as credit card, smart card, personal digital assistant (PDA), RFID tags, wireless sensor nodes, etc., is gaining equipotent role in our daily life. Their use is much ubiquitous. On the other hand, security and performance is one of the severe issues for such devices. So, we can need considerable security as well as performance of these devices, owning minimal storage space, and computational capabilities. This results in raising a research area known as lightweight cryptography. The aim of LWC is to provide the secured information on highly constrain relevant devices owning minimal sources. LWC

M. U. Bokhari (✉) · S. Hassan
Department of Computer Science, Aligarh Muslim University, Aligarh 202002, India
e-mail: mubokhari@gmail.com

S. Hassan
e-mail: hassan.analyst@gmail.com

M. U. Bokhari et al. (eds.), *Cyber Security*, Advances in Intelligent Systems and Computing 729, https://doi.org/10.1007/978-981-10-8536-9_8

algorithms have got certain common features like they must possess low power consumption, lesser communication cost, low area, low energy, as well as little processing time. The implementation of LWC is done in such a way that it increases throughput and efficiency. The ubiquitous use of RFID tags rise concern about equipotent security in RFID system. Since low-cost tags are extremely resource-constrained device, common security approach is no longer applicable to them. Hence, one challenging topic is to purpose a secure lightweight cipher that is suited for RFID tags. This paper describes a comparative study among some well-known lightweight ciphers (Table 1).

2 Stream Cipher

Stream cipher was introduced in 1917 by "Gilbert Vernam". Vernam studies Electrical Engineering at Worcester Polytechnic Institute (WPI) in Massachusetts. Stream cipher sometime refers to Vernam cipher. Stream cipher is a symmetric key cipher where the plaintext digits are combined with a stream of pseudorandom cipher digit is called keystream. Stream cipher encrypts bits individually with a corresponding digit of keystream to obtain the ciphertext digit, i.e., encrypted bit. The pseudorandom keystream is generated from a primary random integer value (is called a seed) using digital shift register and the same seed value is served as a key for decryption of ciphertext stream [1].

3 Lightweight Stream Cipher

A lightweight stream cipher is used in a device (smartphones, tabs, sensor networks) due to the limitation of resources and power consumption. The lightweight stream ciphers are work better and in efficient manner in such situations and are design for targeted to resource-constrained devices like RFID (Radio Frequency Identification) smart cards, and wireless sensor nodes.

Table 1 Types of various cryptographic algorithms

Stream cipher	Block cipher		Hybrid cipher	
BSF-128, Bokhari stream cipher	Symmetric	Asymmetric	Hamming bird 1	Hamming bird 2
GRAIN, RC4	DESL	ECC	–	–
WG-7, WG-8, WG-16	–	–	–	–
HITAG2, Sober t-16/ family	–	–	–	–
PUF, Snow, Edon80	–	–	–	–

3.1 BSF-128

The BSF-128 stream cipher is designed on the basis of grain. It has designed for 128-bit secret key applications. BSF-128 consists two shift registers, one FCSR and one LFSR of 128-bit length each. It also uses an S-Box of 8×16, i.e., it takes 8-bit input and produced output of 16-bit. The S-Box is a combination of Skipjack and an S-Box designed by ISRC at QUT, which has also been used in SOBER t-16 cipher. On the basis of cryptanalysis, we assume that this cipher is secure against many cryptanalysis attacks [2].

3.2 Grain

For the resource constrain environment, grain cryptographic stream cipher is designed. It seems to be much pretty on the situation where there is a limitation of gates, memory space, processing time, low power consumption, etc., there are several stream ciphers that are based on LFSR to produce an arbitrary sequence of numbers. There are mainly three building blocks of grain stream cipher.

- A nonlinear feedback shift registers.
- Two linear feedback shift register.
- A nonlinear filter functions for offering the ideal security.

As we know that an LFSR with feedback chosen from a primitive polynomial can produce a well-balanced sequence of streams, whereas the NLFSR is used to achieve nonlinearity in the ciphers. Due to the inherent weakness of LFSR's, several cryptanalytic attacks [3–6] were reported against grain stream cipher. The size of LFSR, NFSR and key is 80 bits and the size of initial vector is 64 bits. A polynomial of degree 80 is used to provide the feedback to the shift registers LFSR and NFSR, where $\boldsymbol{f}(\boldsymbol{x})$ and $\boldsymbol{g}(\boldsymbol{x})$ represent the feedback function. At first, the LFSR is seeded with a 64-bit initialization vector, and NFSR is seeded with 80 bits of key. Left 16 bits are loaded with ones in order to avoid zero shift registers. At the end, input of NLFSR are masked with the output of LFSR to obtain a stable condition for NLFSR. The nonlinear filtration function $\boldsymbol{h}(\boldsymbol{x})$ needs as an input and the desired bits from both the feedback shift registers. Thereafter, a XOR operation with modulo2 is performed with all of the 7 specific bits of NFSR and then their output is further included with the filter function $\boldsymbol{h}(\boldsymbol{x})$.

3.3 Ron's Code (RC4)

RC4 designed by Ron Rivest in 1987. In the history of cryptography, RC4 has been one of the most popular stream ciphers. Its internal state contains a permutation of

bits overall possible bytes sequence ranging from 0 to 255. Its design analysis and approach are quite different as compared to LFSR-based stream ciphers. The internal state consists a table of $N = 2^n$, n-bit words and two n-bit pointer [7, 8]. There are some attacks on RC4 based on the relationships between the internal states of the S-Boxes [9].

3.4 Welch-Gong (WG-7)

WG-7 [10] stream cipher is based on the primitive WG stream cipher [11]. It is designed by Y. Luo, "Q. Chai", "G. Gong", and "X. Lai" in 2010. WG-7 is a very fast stream cipher for the lightweight devices (for example smart mobile phone, RFID tags, as well as wireless sensor node) WG-7 is design. Both WG and WG-7 are hardware-oriented stream cipher that uses a word-oriented LFSR and a filter function based on WG. WG works on GF(2^{29}) but WG-7 in GF(2^7). WG-7 uses 80-bit secret key and 81-bit IV and the LFSR is clocked 46 times, the internal state consists of 161 bits and the security level claimed by the designer is 80-bits [4, 12].

3.4.1 Algebraic Attack on WG-7

Recently, a distinguishing attack was discovered against the WG-7 stream cipher. Within the time complexity of $O(2^{27})$, an attacker can recover both the secret key and internal state of the cipher [13].

3.5 Welch-Gong (WG-8)

WG-8 is a lightweight discrepancy of the well-known WG stream cipher family and was submitted to eSTREAM project. It inherits excellent randomness properties of WG such as exact linear complexity, balance, ideal tuple distribution, period, and ideal two-level autocorrelations. On AT mega 128 (8-bit) from Atmel and MSP430 (16 bit) from Texas low power microcontroller, WG-8 is able to achieve a throughput of 185.5 and 95.9 kbps on both microcontroller with energy efficiency of 458 and 125 nJ/bit respectively. As compared to other LWC implementation, the throughput of WG-8 is about $2 \approx 15$ times higher and energy consumption is about $2 \approx 220$ times smaller [14].

3.6 HITAG2

A secure version of Crypto-1 cipher has been developed by "Philips/NXP". It is also widely used in RFID cars lock for immobilizers and door opening systems. It has played a great role in the functioning and security of Alfa Romeo 156 and 166 models, Opel, Numerous Nissan, Ford Galaxy and Transit, GM Corsa and Zafira, Peugeot, and also in Volvo models. HITAG2 also seems to be playing a vital role for the access control of buildings. It has 48-bit internal state and 48-bit secret key, due to short length of secret key, the ciphers seems to be vulnerable to brute force attack. It is a lightweight LFSR-based stream cipher [15].

3.6.1 Attack on HITAG2

A cryptanalysis against HITAG2 was founded [15], which easily broke HITAG2 by a SAT solver within several hours. Besides the brute force attack, this is only a unique cryptanalysis on HITAG2 that break the security of cipher. This attack comprises of three phases [16].

- To extract 32 bit of secret key a black box attacks is vulnerable.
- To achieve other key bits the white-box attack seems also vulnerable.
- Brute force searches for the remaining key bits.
- Cost-optimized parallel code-breaker COPACOBANA is able to reveal the secret key of a HITAG2 transponder in less than 2 h (103.5 min) in the worst case [17].

3.7 SOBER

SOBER is a popular family of stream ciphers that are widely used in embedded devices. It was first proposed by G. Rose in 1998. Their family includes several stream ciphers: Sober t-16, sober t-32 [18], sober t-128 [19], and many more. The synchronous stream cipher sober t-16 and sober t-32 were submitted to NESSIE program [12] with 128-bit key and 256-bit key strength, respectively. Almost all ciphers, which belong, to sober are depending on similar principle and virtually have equivalent model structure. Most of the sober family ciphers consist of three basic components [19].

- Linear feedback shift registers (LFSR)
- Nonlinear function
- Stutter control.

3.8 Lightweight Secure PUF

The physical unclonable function (PUF) [20] is promising solution to mitigate the effect of physical attacks. PUF is the physical entity that generates output based on their input and intrinsic physical properties of embedding hardware. It exploits only those physical properties of embedding devices.

3.8.1 Drawback on PUF

Due to small hardware requirement to building a PUF, it is widely used in lightweight applications such as RFID tags. To achieve the feature of low-cost implementation, composite PUFs are developed and are introduced in HOST2014 and RECONFIG 2013. The building of composite PUFs is based on several small primitives; on the basis of cryptanalysis, the introduced PUFs RECONFIG 2013 are not secure and can be penetrated [21].

4 Block Cipher (BC)

A block cipher works on two pair of algorithms, one for encryption e and other for decryption d. A group of plain text namely P of size $L > 1$ are encrypted together by the encryption function $C = e(k, P), C$ yield cipher text under the enciphering function e with key k. A whole block of size L is encrypted with a single key k at a time. The key k is a composition of several values $k_i k_{i-1} \ldots k_1 k_0$. After encryption, the ciphertext C is decrypted by the set of composite key k under the correspondence $P = d(k, C)$. In this cipher, the ciphertext block is totally depends upon the key k. In mathematical terminology, we can also say that

$$e(k, P) = d^{-1}(k, P) = C$$
$$d(k, P) = e^{-1}(k, C) = P$$

By following transitivity can we have?

$$e^{-1}(k, e(k, P)) = P = d\big(k, d^{-1}(k, P)\big)$$
$$d^{-1}(k, d(k, C)) = C = e\big(k, e^{-1}(k, C)\big)$$

It is a deterministic algorithm that operates on a fixed length of data of size L. It is widely used to implements a cryptographic protocol and the encryption of bulk of data. Hence, block cipher encrypts bits slowly than stream cipher.

The modern architecture of block cipher is based on the concept of iteration is called product cipher; data are spitted into several boxes, and then permuted with different sub-keys derived from the main key k to enhance the security and randomization.

5 DESL

The algorithms tend to make use of inside this cipher are the DESL (build up extension of DES) & ECC, DESL is the enhanced lightweight version of DES. The microchip size of DESL is considerably reduced as individual S-Box is utilized frequently for eight times. Which can make DESL compact, tough, efficient, and prevented from linear and also differential cryptanalysis attacks. The DESL is proficient to enciphering 64 bit of plain text in 144 clock rounds while it is working with a frequency of 100 kHz and gaining current of 0.89 μA [22]. The DESL structure involves mainly the building blocks controller, mem-left, mem-right, key program, and S-Box.

6 Elliptic Curve Cryptography (ECC)

In 1985, two American mathematicians Vector Miller and Neal Koblitz proposed the concept of elliptic curve cryptography. Their theory is completely based on elliptic curve discrete logarithms and NP hard problem that requires a complete exponent time. The application of ECC involves information security, personal digital assistant (PDA), wireless communication network, wireless sensor nodes, image encryption, smart cards, e-commerce, and also in economic-based communication protocols. ECC makes use of 162-bit public key by the assist of picking points on elliptic curves, and afford a security strength that is corresponding to 1024-bit key in RSA [23].

6.1 Advantages of ECC Over RSA

- Smaller key size for equivalent security
- Provide higher security per bit.
- Provide higher security for same amount of computation.

- For higher security (Largest ECC & RSA system broken to date are 108-bit 512-bit)
- Largest effort ever expanded in PKC challenge for solving 108-bit ECC. Amount of work required was about 50 times of 512-bit RSA.

7 Hybrid Cipher (HC)

By providing tradeoff between speed [24], size, cost of implementation, efficiency, in a hybrid model of hummingbird ciphers was invented by "ALEXANDRIA" and Viswanath Ananth of Valencia, Calif in 2011. It achieves the characteristic of both stream cipher and block cipher. Their implementation is done on keeping in mind that they are efficiently adopted in low-cost sensible devices and also within microcontroller environment. Hummingbird persistently opposes to most frequent attacks on stream and blocks ciphers such as birthday attack, cube attack, side channel attack, key recovery attack, brute force attack, algebraic attack, correlation attack, timing attack, linear and differential cryptanalysis, time–memory–data tradeoff attack, distinguishing attack, passive attack, and acoustic cryptanalysis. Due to their complex internal state and 256-bit key size, it attains more security and hence it is most suited for embedded applications that are discussed above. The hybrid model of hummingbird is even categorized into two modules namely, Hummingbird-1 and Hummingbird-2. Hummingbird-1 is a nice combination of stream and block cipher [3], with 16-bit block size, 256-bit key, and 80-bit internal states.

8 Conclusion

In this comparative study, we analyzed different lightweight cryptographic algorithms including hybrid model (of Hummingbird1 and Hummingbird2), several lightweight stream ciphers have been discussed with their technologies, attack immune, features as well as drawbacks. Table 2 depicts a comparative study of several stream ciphers by tending their crucial parameters. Obviously, it is a promising work for the better analysis and design of a lightweight stream cipher for resource-constrained devices. Thus, the objective of this comparative study is to propose an efficient modification on enciphering algorithms, which eliminate most common attacks on cipher and provide highest throughput.

Table 2 Summarized comparison to depict the differences among various LWC algorithms

	Cipher type	Block size	Key size	IV	Attacks immune	S-Box	Throughput	Registers	Operator
DESL	Block cipher	64	56		Resist LC and DMA	6 × 4 single	Least among other algorithms	No	XOR and Shift
Grain	Stream cipher	1	80	64	No better KRA beside BFA	No	High but less than Hummingbird	LFSR + NFSR	XOR
ECC	Asymmetric block cipher	No	162	–	Resist SCA and TA	No	Better but less than Hummingbird	No	Point addition and point multiplications
BSF 128	Stream cipher	–	128	128	Resist COA, GDA,DA, DGA	8 × 16	High but less than Hummingbird	NFSR + FCSR	XOR
WG-7	LW stream cipher	–	80	81	Suffer from DGA, AA	No	–	Word-oriented LFSR	XOR and multiplication
WG-8	LW stream cipher	–	80	80	Able to resist AA, COA, DFA, CUA, DGA, DFTA, TMDA	No	High throughput	20 stage LFSR	XOR and multiplication
WG 16	LW stream cipher	–	128	128	Able to resist AA, COA, DFA, CUA, DGA, DFTA, TMDA	No	–	32 stage LFSR	XOR and multiplication
RC4	Stream cipher	No	128	–	Some attack based on relationship between internal state and S-Boxes	Yes	Best	No	XOR
Sober t-32	Stream cipher	–	256	–	Secure, have a good immune	Yes	–	LFSR	XOR
HC	Hybrid cipher	16	128–256	–	Most secure, and immune to most of LA, DA, CUA, BDA, AA etc.	4 × 4	Maximum	LFSR	XOR

AA Algebraic attack; *BDA* Birthday attack; *BFA* Brute force attack; *COA* Correlation attack; *CUA* Cube attack; *DA* Determine attack; *DFA* Differential attack; *DFTA* Discrete Fourier transformation attack; *DGA* Distinguish attack; *DMA* Davies Murphy attack; *GDA* Guess &determine attack; *HB* Hummingbird; *IV* Initialization vector; *KRA* Key recovery attack; *LA* Linear attack; *LC* Linear cryptanalysis; *LW* Lightweight; *SCA* Side channel attack; *TA* Timing attack; *TMDA* Time–memory–data attack

References

1. Online reference from http://en.wikipedia.org/wiki/Stream_cipher
2. Bokhari MU, Alam S (2013) BSF-128: a new synchronous stream cipher design. In: Proceeding of international conference on emerging trends in engineering and technology, pp 541–545
3. Maximov A (2006) Cryptanalysis of the grain family of stream ciphers. In: Proceedings of ACM symposium on information, computer and communications security, pp 283–288
4. Dinur I, Shamir A (2011) Breaking grain-128 with dynamic cube attacks. In Fast software encryption. Springer Berlin Heidelberg, pp 167–187
5. Bjøstad TE (2013) Cryptanalysis of grain using time/memory/data tradeoffs
6. Banik S, Maitra S, Sarkar S (2012) A differential fault attack on the grain family of stream ciphers. Proceeding of 14th international workshop on cryptographic hardware and embedded systems. Springer, Berlin Heidelberg, Leuven, Belgium, pp 122–139
7. Gupta Sen S (2014) (Non-)random sequences from (Non-)random permutations analysis of RC4 stream cipher. J Cryptol 27(1):67–108
8. Lv J, Zhang B, Lin D (2014) Some new weaknesses in the RC4 stream cipher. Inf Secur Appl 27(1):8–38
9. Xie J, Pan X (2010) An improved RC4 stream cipher. Proc Int Conf Comput Appl Syst Model 7:156–159
10. Orumiehchiha AM, Pieprzyk J, Steinfeld R (2012) Cryptanalysis of WG-7: a lightweight stream cipher. Crypt Commun 4(3–4):277–285
11. Nawaz Y, Gong G (2008) WG-7: a family of stream ciphers with designed randomness properties. Int J Inf Sci 178(7):1903–1916
12. Babbage S, Lano J (2011) Probabilistic factors in the Sober-t stream ciphers. In: Proceeding of 3rd NESSIE workshop, pp 1–12
13. Luo Y (2010) A lightweight stream cipher WG-7 for RFID encryption and authentication. In: Proceeding of IEEE global telecommunications conference, pp 1–6
14. Fan X, Mandal K, Gong G (2013) WG-8: a lightweight stream cipher for resource-constrained smart devices. Springer Berlin Heidelberg, pp 617–632
15. Courtois NT, Sean ON, Quisquater JJ (2009) Practical algebraic attacks on the Hitag2 stream cipher. In: Information security. Springer Berlin Heidelberg, pp 167–176
16. Sun S (2011) Cube cryptanalysis of Hitag2 stream cipher. In: Proceeding of 10th international conference cryptology and network security. Springer Berlin Heidelberg, CANS, pp 15–25
17. Stembera P, Novotny M (2011) Breaking Hitag2 with reconfigurable hardware. In: Proceeding on 14th IEEE Euromicro conference on digital system design, pp 558–563
18. Rose G (1998) SOBER II: a stream cipher based on linear feedback over GF (28). In: Proceeding on 3rd Australasian conference, pp 135–146
19. Hawkes P, Rose GG (2003) Primitive specification for SOBER-128. IACR cryptology ePrint archive
20. Nguyen PH, Sahoo DP (2014) Lightweight and secure PUFs: a survey. In: 4th international conference on security, privacy, and applied cryptography engineering. Springer International Publishing, pp 1–13
21. Nguyen HP (2014) Cryptanalysis of composite PUFs (extended abstract-invited talk). In: Proceeding of 18th international symposium on VLSI design and test, pp 1–2
22. John J (2012) Cryptography for resource constrained devices: a survey. Proc Int J Comput Sci Eng 1766–1770

23. Malhotra K, Gardner S, Patz R (2007) Implementation of elliptic-curve cryptography on mobile healthcare devices. In: Proceeding of IEEE international conference on networking, sensing and control, pp 239–244
24. Shende RS, Deshpande MAY (2013) VLSI design of secure cryptographic algorithm. Proc Int J Eng Res Appl 3(2):742–746