Security Analysis of Candidates for Authenticated Encryption and Cryptanalytic Attacks to Check Robustness

Abhishek Kumar
Abhisheikh.kmr@gmail.com

Abstract— **The exponential surge in the computing power of devices and concept of quantum mechanical systems has put the security abilities of traditional block ciphers and public key cryptosystems in peril. Shor's algorithm postulated by the MIT mathematician Shor, exhumed the threats to RSA. Similarly, various mathematical attacks such as linear and differential cryptanalysis undermined the security of DES and AES to great extent. NIST held a competition to invite proposals from mathematicians and cryptographers around the globe to select an encryption mechanism that guarantees authentication and can replace AES. CAESAR (Competition for Authenticated Encryption: Security, Applicability, and Robustness) competition was held to invite proposals from mathematicians and cryptographers around the globe to select an encryption mechanism that guarantees authentication and can replace AES-GCM. The various design parameters to meet the functional requirements such as tag size were fixed to ensure transparency and level playing ground. This work presents a detailed analysis of three main candidates: ACORN-128, AEGIS-128/256, and AES-OTR. AEGIS and ACORN were one of the finalists selected. Furthermore, various mathematical cryptanalytic attacks and side channel attack scenarios have been examined that could be implemented on these candidate algorithms to check their robustness.**

Keywords— ACORN-128, AEGIS, AES-OTR, Algebraic Attacks, Quantum Cryptanalysis

I. ACORN-128

It uses 128 bit key size, 128 bit Initialization Vector (IV) and tag of same size. The authors specify two scenarios for its usage: one is for simpler applications with limited computing resources at disposal and another for high performance computing scenarios. The authentication is done using 128 bit tag.

The maximum plain text length specified is 2^{64} bits. ACORN-128 uses following two Boolean functions:

$$maj(a,b,c) = (a\ AND\ b) \oplus (a\ AND\ c) \oplus (b\ AND\ c)$$
$$ch(a,b,c) = (a\ AND\ b) \oplus ((\sim a)\ AND\ c)$$

It uses a state of size 293 bits comprising of 6 LFSRs. ACORN-128 [1] constitutes three principal functions: Generation of keystream bit, calculating feedback bit and then at last updating the state. IV and tag should not be reused i.e.it can be used to perform encryption and authentication only once. Studies and experiments conducted by authors' claim that success probability of forgery attack is 2^{-s}, where s is tag size and replayed forgery attacks are prevented using unique (state, key) pair.

Differential and cube analysis of initialization suggested that the order of attempts required for exhaustive search increased exponentially with tag size and cube size. The potential attack gets harder if we eliminate the rightmost LFSRs e.g. if there exists a difference between $S_{i,\ 234} \oplus S_{i,\ 229}$, we neutralize that by incorporating a difference in $f_i \oplus K_{S,i}$.

A) SECURITY FEATURES

1. It is fairly robust against any statistical cryptanalytic attack such as linear or differential because each IV is used only once for a key and the states are updated in nonlinear fashion.
2. **Traditional Attacks:** It was experimented to be resilient against conventional attacks such as bit correlation attacks and algebraic attacks. The underlying reason for this is that these attacks intend to exploit linear behavior in implementation of ciphers, whereas in ACORN-128, the states were updated in nonlinear fashion.
3. **Time- memory tradeoff assaults:** If we consider a stream cipher of k bits keysize and 2k bits states, then the efforts required to implement time memory trade off attacks [2] [3] require an effort of order 2^k operations. Furthermore, studies done by Hellman [4] suggested that any cipher that utilizes a state function of twice the keysize, is practically robust against such type of attacks. Since the state size of ACORN-128 is 293 bits and key size is 128 bits, therefore ACORN-128 is secure against such attacks.
4. The security of authentication and finalization stems from the fact that ACORN-128 uses 6 LFSRs concatenated all together and in such a manner that one bit difference is induced from five LFSRs to the sixth LFSR and these bits are injected into state function. Such differences can be neutralized to eliminate the differences in rightmost LFSR bits. The ACORN-128 is robust against forgery as

mathematically it requires an operation of order 2^{-100} after 400 steps.

In terms of hardware efficiency, it has slightly costly implementation platform requirement than AES- GCM. But the software efficiency compared to same is better as it has less lines of codes.

II. AEGIS: FAST AUTHENTICATED ENCRYPTION ALGORITHM

The designers of the algorithm outline three different parameter specifications for this cipher. The following table represents those specifications:

TABLE 1: AEGIS Specification

	Key Size (in bits)	IV (Nonce) (in bits)	State size (in bits)	Tag (in bits)	Usage cases	Plain text length
AEGIS -128L	128	128	1024	128	High Performance Applications	$<2^{64}$ bits
AEGIS -128	128	128	640	128	High performance applications	$<2^{64}$ bits
AEGIS -256	256	256	768	128	High performance applications	$<2^{64}$ bits

AEGIS [5] is derived from AES round functions incorporating different number of rounds for different specifications. AEGIS-128L utilizes 8 AES rounds to process plain text block of 32- bytes in single step; AEGIS-128 utilizes 5 AES round functions for plain text block of 16 bytes and AEGIS-256 implements 6 AES rounds. As it can be inferred from Table 1 that tag size is fixed 128 bits for all the three variants of AEGIS. The state size varies from 640 to 1024 bits. All the three variants work effectively well in case of high performance computing environments. More study needs to be done to examine what effect it has on robustness of AEGIS, if we use a fixed state size of 640 bits for all the three variants. A smaller state size may lead to efficient computations, but that should not come at the expense of lesser security.

A) STATE UPDATING

For AEGIS-128, the updating function updates 80 bytes S_j (jth step state) with 16 bytes plaintext block P_j using following set of Boolean round functions:

$$S_{j+1,0} = AESRND(S_{j,4}, S_{j,0} \oplus P_j)$$

$$S_{j+1,1} = AESRND(S_{j,0}, S_{j,1})$$

$$S_{j+1,2} = AESRND(S_{j,1}, S_{j,2})$$

$$S_{j+1,3} = AESRND(S_{j,2}, S_{j,3})$$

$$S_{j+1,4} = AESRND(S_{j,3}, S_{j,4})$$

Where,

AESRND(X, Y) represents round function of AES with X as 16 bytes state and Y as 16 bytes key for that round.
$S_{m,n}$ represents nth 16- bytes state S_m.

A similar state updating function was constructed for AEGIS-128L and AEGIS-256. In case of AEGIS-256 the input current state S_k is of 96 bytes and plain text data block P_k of 16- bytes.

$$S_{k+1,0} = AESRND(S_{k,5}, S_{k,0} \oplus P_k)$$

State functions for rest other rounds was in a similar fashion to those constructed in AEGIS-128 other 4 rounds.

B) SECURITY FEATURES AND ANALYSIS

1. Analysis suggested that all the three specifications of AEGIS was robust against differential cryptanalysis as difference in the IV would pass or propagate to all rounds of AES e.g. in case of AEGIS-128, it would propagate to a total of 50 round functions in 10 steps overall.
2. **Statistical Attacks:** Linear and differential cryptanalysis could not be efficiently performed because of the similar reasons to that of ACORN-128.
3. **Security of Authentication:**
   - **Assault by recovering state at any step:** Since IV was used exactly once, exhaustive ferret was computationally infeasible to recover secret state. Attacking the tag would not work also as it required an attempt in order of 2^{128} operations.
   - **Collision/Birthday attacks:** A typical birthday attack [6] requires tag of approximately $2^{k/2}$ chosen plaintexts, where k is number of bits in tag and state. AEGIS is robust against above demonstrated attack as it has comparatively large tag size. Furthermore, any attack involving differential cryptanalysis was neutralized as AEGIS uses more than 26 S-Boxes of AES and thus is more secure than AES-GCM, AES-HMAC, and AES-CMAC.

In terms of hardware efficiency, it had slightly costly implementation platform requirement than AES- GCM. But the software efficiency compared to same was better as it had less lines of codes.

III. AES-OTR

AES-OTR [7] is OTR (Offset TwoRound) mode of operation of Advanced Encryption Standard (AES). It has following parameters:

TABLE 2: AES-OTR specifications

	Key size	IV	tag	Data processing
AES128-OTRPV1	128- bits	96-bits	128 bits	Parallel
AES128-OTRSV1	128-bits	96-bits	128 bits	Serial
AES256-OTRPV1	256-bits	96-bits	128 bits	Parallel
AES256-OTRSV1	256-bits	96-bits	128 bits	Serial

A) OPERATION AND SECURITY FEATURES

The security of AES-OTR relies on the fact that AES has a pseudo random operation procedure incorporating a Pseudo Random Function (PRF) and Pseudo Random Permutation (PRP). The encryption and decryption operations were done using AES round functions which is not reversible. Another striking feature of AES-OTR was that by partitioning into two blocks both enciphering and deciphering could be done parallel in one phase.

A critical study of algorithm suggested that breaking AES-OTR required operations in order of 2^{64}. But the entire security relies on the assumption or hypothesis that the nonce or IV was used exactly once. Beyond this no security whatsoever could be claimed.

If one studies deep into the underlying logic behind the parameter specifications and the design criteria, one could conclude that choice seemed to be coinciding with NIST specifications and security capabilities of its parent cipher AES e.g. tag length was 128 bits as per the criteria laid forth by NIST. The key size of 128 bits and 256 bits counteracts the brute force attempts. Furthermore, the entire operation was carried out in GF (2^n) field and with GF doubling the designers of the algorithm were able to mask AES inputs. AES- OTR does not require a full GF Multiplier and computation cost is similar to AES-GCM and AES-OTR. It performs one line, one pass parallel encryption and decryption under two block partition.

B) RESEARCH GAP

Here it is worthwhile to point out that the study of algorithm in context of other attacks such as correlation attacks, bit sum attacks, linear and differential cryptanalysis yet to be done. A somewhat different level of security could be expected with smaller nonce or tag. Another aspect is that, since the cipher was not using any state update functions, algebraic attacks could have deteriorating effects on security of AES-OTR.

IV. PROPOSED CRYPTANALYTIC ATTACKS

A). ALGEBRAIC CRYPTANALYSIS

It has already been observed by cryptanalysts that with access to chunks of known plaintexts and chosen plaintexts in massive amount, the linear and differential cryptanalysis can be performed in order of operations 2^{28}. But it is much needed to study what actually happens to security of DES and AES [8] if one possess very less data about known plaintexts. A detailed analysis reveals that DES [9] does not have any prominent algebraic structure that we can analyze, but AES incorporates a juggernaut of algebraic structures with the operations being carried out in GF (2^8) field. The following axiom must be upheld true for a successful algebraic cryptanalytic robustness:

AXIOM 1: Let us assume a function f*: GF (2^p) -> GF (2^q) and $f(a) = b$*

$$a = (a_0, a_1, \dots\dots, a_{p-1}) \tag{1}$$

$$b = (b_0, b_1, \dots\dots, b_{q-1}) \tag{2}$$

The I/0 degree of above function is the smallest degree in following relation:

$$g(a_0, a_1, \dots\dots, a_{p-1};\ b_0, b_1, \dots\dots, b_{q-1}) = 0 \quad \forall\ (a,b) \text{ such as } f(a)=b \tag{3}$$

A strong authenticated cipher should use core functions with high I/O degree.

B) RESEARCH GAP

The study of ACORN-128, AEGIS and AES-OTR under the algebraic structure with AXIOM 1 yet remains to be done. Prima facie, ACORN-128 and AEGIS involve nonlinear functions and nonlinear state updates, so they can be considered computationally secure. But the security under the Gaussian Elimination in O (n^3) complexity or reduction of SAT family problems with better asymptotes will completely determine the robustness against algebraic class of mathematical cryptanalytic attacks.

Another class of problems such as MQ problems with finite fields and XL family poses deeper threats to AES-OTR. In past, problems belonging to above class have tottered the security of AES and hence their adequacy can be applied on AES-OTR to check their robustness. Axiom 2 illustrates the MQ problem.

AXIOM 2: Let us consider a system of p equations each having q variables in field Therefore, for any variable x_i,

$$\sum_{i,j} a_{i,j,k} x_i x_j + \sum_i b_k x_i + c_k = 0 \tag{4}$$

where i,j,k are indexes of the coefficients a,b, and c. The intent is to find values in field F that satisfy the above criteria.

If we talk about MQ problem over GF (2), the intent is to obtain least one solution of type (y_0, y1, y2,…..,y_{k-1}) such as

$$1 = y_1 + y_0 y_1 + y_0 y_2 + \cdots \quad (5)$$

$$0 = y_1 y_2 + y_0 y_3 + y_{7+\ldots} \quad (6)$$

k is number of variables in each polynomial equation.

Although being NP-hard class of problem, it can be made tractable by considering the field F to be finite. In case of AES-OTR the field to be examined is GF (2^8) or in general GF (2^n).

In the study done by [10], authors suggested novel approach to solve a system of polynomial equations by either increasing the number of monomials or expansion of variable counts by coding (Multiplicative Complexity).

Assume A is the number of polynomial equations, B is the number of monomials and C is number of linearly independent equations. The asymptotic growth of C can't be faster than B but A can grow faster than B.

The principle idea is to multiply initial equations by low degree monomials.

$$1 = y_5 + y_0 y_5 + y_0 y_2 \quad (7)$$

which after multiplication becomes of degree equal to three

$$y_1 . 1 = y_1 . (y_5 + y_0 y_5 + y_0 y_{2)} \quad (8)$$

C) POSSIBLE ATTACK SCENARIOS

Any algebraic class of mathematical cryptanalytic attack involves two primitive steps: First, is to construct the core operating functions of the cipher in form of system of polynomial equations and then in second step solve that system of equations. But the catch is that solving those polynomial equations is a NP-hard problem. (Whether or not it is NP-complete, that is debatable. Some literatures suggest that it is NP-complete, although a proper investigation can be carried by theoretical computer scientists for more clarity in this regard). So, we reduce any well-known problem such as SAT to the problem of solving polynomial equations over GF (2^n) or GF (2^8) for computationally feasible algebraic cryptanalysis of AES-OTR.

AES has already been susceptible to cryptanalysis with massive chunks of known plaintexts. Since AES-OTR uses AES round functions as its core design, reduced SAT class of problems and its combination with relatively fewer known plaintexts can be implemented to perform algebraic cryptanalysis and to check their robustness.

Since AEGIS and ACORN-128 are using nonlinear state updating functions, therefore algebraic cryptanalytic attacks involving system of polynomial equations and NP-hard class of problems seems to be less feasible. The 3SAT problem is reduced into multiple instances and then the system of constructed polynomial equations is transformed corresponding to one of these instances. AES-OTR in its each specification involves use of AES round functions such as mix substituteBytes, shiftRows, mixColumns and addRound Key. Performing algebraic cryptanalysis on entire AES-OTR, having multiple rounds of AES would not be computationally efficient. Therefore the idea is to perform it round wise, where each round function can be translated into an instance of Satisfiability Problem (SAT) and can be solved pretty straight forward.

D). SIDE CHANNEL ATTACKS

The effect of template attack [11] together with Hamming Weight leak (HW) [12] [13] needs to be studied on ACORN-128, AEGIS and AES-OTR. The attack is particularly important to check the robustness of candidates having AES round functions as their core such as AES-OTR and AEZ. We denote S(p⊕k) as hamming weight where p denotes one single byte of plain text and k denotes one single byte of key and S is S-box in AES round function.

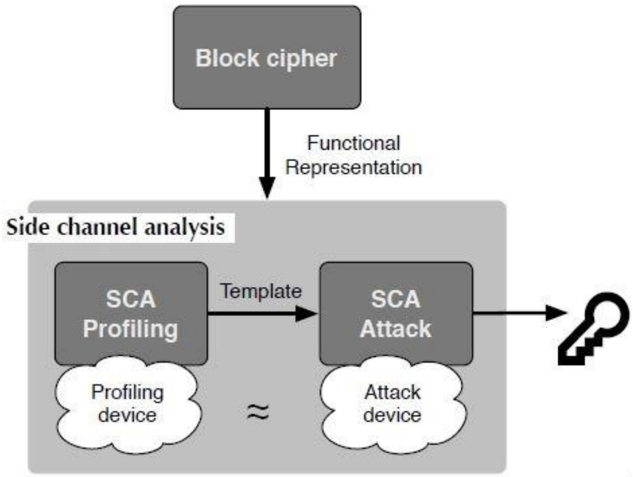

Figure 1: Side channel attack model [14]

The two phases involved in side channel attacks are: First, the profiling phase in which cryptanalyst uses multivariate Gaussian normal distribution. In the next phase, which is attack phase, cryptanalyst applies Maximum Likelihood Estimation (MLE) with an attack vector and secret key or sub key. Using this we can obtain hamming weight of data carried in plain text and further can extract byte of key k. The same process has been illustrated in Figure 1 [14]. Figure 1 gives a functional representation of Side Channel Attack on any block cipher. Using a suitable profiling algorithm, SCA profiling is done to create a template. Then, this template is used to launch SCA attack to extract the key or sub key bytes. The focus of the future research should be to use complex nonlinear transformations, so that a template creation or profiling cannot be done using MLE. The scope of attack vectors or the number of variables involved should also be expanded for a difficult cryptanalysis.

Apart from above research direction, one more aspect that needs to be investigated is the implications of the Side Channel Attacks on MQ based cryptosystems. As it has been already deduced from *AXIOM 2* that MQ problem is a NP complete (hard) problem and is widely used to both bolster and cryptanalyze ciphers, how much the MQ based ciphers are prone to side channel attacks, it needs to be studied.

A study done by Yi and Li in [15] suggested that Multivariate Public Key Cryptosystems (MPKC), which is based on solving multivariate quadratic equations, no no side channel attack or "leakage" was found. However, public key cryptosystems based on calculating multivariate quadratic systems, serial implementation resulted into cube attacks in form of bit leakage.

V. QUANTUM CRYPTANALYSIS

Quantum computers would have unprecedented computational power and efficiency, and would be able to tract problems multiple times faster with better space time complexity than the existing classical algorithms. It could prove to be catastrophic for existing cryptographic protocols and cryptosystems. For example, Shor's algorithm for prime factorization and discrete logarithm problem, has the alleged potential to break existing public key cryptosystems such as RSA and Diffie- Hellman Key Exchange protocols.

In comparison to public key cryptosystems, the private key or symmetric- key cryptosystems are considered to be less prone to quantum attacks. But in recent years, various block ciphers and their modes of operation such as Galois Counter Mode (GCM) and CBC- MAC have been compromised and breached. The work in [16] shows how Simon's algorithm could be used to break existing symmetric cryptographic protocols and candidates of CAESAR competition. The authors in [17] propose NMAC and some other variants of modes of operation that are quantum resistant. It is based on quantum resistant Pseudo Random Function (PRF) and the underlying theory that "if two distributions on the function are indistinguishable, then they remain indistinguishable even in the case when an adversary gets many such samples". Here it is worthwhile to mention that the quantum attacks against hash functions and symmetric key cryptosystems assume that attackers can implement quantum superposition queries. As for the authenticated cipher symmetric key cryptosystems, the effect would be somewhat lesser as compared to asymmetric cryptography. The possible threat studied so far [18] arises from Grover's search algorithm. Using Grover's algorithm, one can search for an element in a list of N elements in $(N)^{1/2}$ operations. This can speed up the exhaustive key search process.

Hence one can investigate the algebraic structures in the design of authenticated encryption algorithms for quantum provable security. A white-box approach, involving investigation of the algebraic structures in the internal operations of authenticated ciphers can be adopted. Reduction technique can be employed to reduce the operations, with emphasis on state update function, into any well-known hard problem such as 3-SAT and other quantum safe problems and thus prove the quantum security of authenticated encryption algorithms.

VI. CONCLUSION AND FUTURE WORK

The candidate algorithms of authenticated ciphers under 'CAESAR' competition of NIST involve computations that can be expressed in polynomial terms over a finite field. This poses a deep threat to the robustness of these algorithm. This paper presented a detailed analysis of three candidates and the algebraic cryptanalysis and quantum cryptanalysis that can be performed to check their robustness.

In future, the study will be done to actually implement the proposed attacks. The results obtained will be put on open archives of cryptology and will be submitted to NIST to further examine and bolster the security and robustness of these ciphers. A comparative study vis-à-vis other block ciphers and stream ciphers under the suggested cryptanalytic attacks can also be performed.

REFERENCES

[1] Hongjun Wu,"ACORN:A Lightweight Authenticated Cipher(v3)" , https://competitions.cr.yp.to/caesar-submissions.html

[2] S. Babbage. A Space/Time Tradeo in Exhaustive Search Attacks on Stream Ciphers." European Convention on Security and Detection, IEEE Conference Publication No. 408, May 1995.

[3] J. Golic. \Cryptanalysis of Alleged A5 Stream Cipher". In Advances in Cryptology, Eurocrypt'97, pp. 239-255.

[4] M. E. Hellman. A Cryptanalytic Time-Memory Trade-Off", IEEE Transactions on Information Theory, Vol. IT- 26, N 4, pp.401406, July 1980.

[5] Hongjun Wu and Bart Preneel,"AEGIS:A Fast Authenticated Encryption Algorithm" , https://competitions.cr.yp.to/caesar-submissions.html

[6] B. Preneel, P. C. van Oorschot. On the Security of Iterated Message Authentication Codes. IEEE Transactions on Information Theory 45(1), 188-199 (1999).

[7] Kazuhiko Minematsu, "AES-OTR v3.1", https://competitions.cr.yp.to/caesar-submissions.html

[8] Harris Nover, ALGEBRAIC CRYPTANALYSIS OF AES: An Overview, Technical report, 2008

[9] NIcholas Courtois and Gregory Bard, "Algebraic Cryptanalysis of DES", In proceedings of AsiaCrypt,(2006)

[10] Nicholas Curtois, Hulme D, Mourouzis T,"Multiplicative complexity and solving Generalized Brent equations with SAT solvers", In proceeding COMPUTATION TOOLS, (2012), Paris

[11] S. Chari, J. R. Rao, and P. Rohatgi, "Template attacks,"in CHES 2002, ser. LNCS, B. K. Jr., C .K Koc, and C. Paar, Eds., 2002, vol. 2523, pp. 13-28.

[12] M. Aabid, S. Guilley, and P. Hoogvorst, \Template attacks with a power model," Cryptology ePrint Archive, Report 2007/443, 2007, http://eprint.iacr.org/.

[13] A. Heuser and M. Zohner, \Intelligent machine homicide- breaking cryptographic devices using support vector machines," in COSADE, ser. LNCS, W. Schindler and S. Huss, Eds., 2012, vol. 7275, pp. 249-264.

[14] Mohammad M, Bulygin S et. al ,"Improved Side Channel Attack on AES", Journal of Crptographic Engineering., (2014)

[15] Weijian Li and Haibo Yi, "Is It Necessary to protect MQ based Cryptosystems from Side channel Attacks", 2016, IEEE Xplore, ISBN: 978-1-4673-9904-3/16

[16] M. Kaplan, G. Leurent, A. Leverrier, and M. Naya-Plasencia, "Breaking symmetric cryptosystems using quantum period finding," Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics), vol. 9815, pp. 207–237, 2016

[17 F. Song and A. Yun, "Quantum security of NMAC and related constructions: PRF domain extension against quantum attacks," Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics), vol. 10402 LNCS, pp. 283–309, 2017.

[18] R. Anand, S. Maitra, A. Maitra, C. S. Mukherjee, and S. Mukhopadhyay, "Resource Estimation of Grovers-kind Quantum Cryptanalysis against {FSR} based Symmetric Ciphers," IACR Cryptol. ePrint Arch., 2020.