Randomized Cryptosystems Attacks and Defenses

Gamal Hussein
Arabic Micro Systems
12 El-Beidak St. Opera Sq.
Down Town Cairo-Egypt
gamal_ams@menanet.net

Abstract - **In this paper, an evaluation of (One Time Pad) OTP, Rabin Everlasting encryption and Two Stage Random number Generator (TSRG) randomized cryptosystems are introduced. TSRG uses randomized encryption techniques for designing an algorithm of a provably secure cryptosystem for message exchange. A built-in TSRG RNG is a distinguishable primitive in the proposed cryptosystem design where instantaneous real time OTP-like data is generated. Most cryptography relies on unproven complexity assumptions like integer factorization being computationally hard, with the adversary limited by computing power. However, advances in cryptanalysis, unpublished researches and computing technology, especially in the emerging quantum cryptography, may make current cryptosystems insecure. Shannon's pessimistic result essentially denotes that if the adversary is all-powerful, then efficient practical solutions for information-theoretic security do not exist. However, the TSRG use the concept of dynamic modeling to achieve provable security based on insoluble problem with respect to attacker. This requires a secure way of exchanging of the OTP-like special seed to be expanded at the receiver side as well as preventing the attackers from mounting state compromise attacks. The paper also explains the relation among the three discussed cryptosystems and randomized encryption techniques.**

I. INTRODUCTION

Practical cryptosystems include several algorithms, out of which many currently used in applications [1] [2] [3] [4] [5] and others waiting their turns (e.g. Rabin everlasting encryption [6]). The wide variety of available cryptosystems indicates that there is a heroic problem of determining the suitability of one of these systems for use in some environment. There is no inclusive theory for establishing the credibility of a cryptosystem. Shannon's contribution is a step in the right direction, but it leaves us with the problem of determining workload and provides no method of doing this [7]. Cryptanalysis is usually performed by finding successively cleverer methods of attack. Since there is no feasible means of finding the optimal attack strategy against a system, we are always left with the possibility that tomorrow, or even today in unpublished work, a clever cryptanalyst will find a shortcut of breaking the scheme we use safely today. So the modern practice of cryptography is thus not about strength or speed in the abstract, but instead about tradeoffs between strength, speed, and other cipher features (e.g. scalability and flexibility). The major features on which a cryptosystem is evaluated are:

1- Strength: Everyone wants a practical cipher which is proven "absolutely secure," but such a cipher does not exist, and probably never will. There is no theory of cipher strength such that, if we only follow the rules, we are guaranteed a strong cipher. Nobody can claim that he can even measure the absolute strength of an arbitrary cipher. This means that cipher construction is fundamentally art instead of science, in spite of the fact that strength is argued in poor technical detail. Unfortunately, these arguments will not be clear to the average customer or cipher user

2- Speed: It is easy to make a fast weak cipher, but making a fast strong cipher is something else. Because a cipher designer cannot measure strength, it is all too easy to make a wrong design decision and end up with a surprisingly complicated weak cipher. As attack technology improves, we need more strength. Since security services are the agreed basic targets of any cipher then it is preferred that ciphering computations do double duty of attaining security services with maximum speed.

3- Flexibility: The most flexible cipher design must support flexible data block length and any type of key of arbitrary length. In these ciphers, there is no need for each applications designer to develop appropriate key processing (e.g. key verification) for every application. AES is an example of flexible block cipher supporting keys with lengths (64,128,196 bits) and data block lengths (64,128,196,256).

4- Scalability: A scalable cipher design can produce a large or small cipher from the exact same construction rules. For example it is possible to design a tiny version of AES which has its features and can yield an experimental test.

The paper is organized as follows. The next section explains briefly the TSRG random number generator, followed by TSRG cryptosystem as a randomized encryption procedure in section three. In section four, the other cryptosystems particularly OTP and Rabin everlasting cryptosystem are discussed. Comparison of the all these cryptosystems is presented in section five. Finally, the conclusions are presented.

II. TSRG GENERATOR

Vernam or One-Time_Pad (OTP) is the exceptional system where the unicity distance is never reached [8]. It is the only theoretically proved unconditional secure cryptosystem provided key is truly random. But the key distribution problem pushes cryptographer to generate key stream from a smaller (base) key. Although this looks very attractive, it is extremely difficult in practice to find a good pseudo-random function that is cryptographically strong. While the statistical features of many PRNGS are excellent, the ability to predict the output of them is a

1-4244-0272-7/06/$20.00 ©2006 IEEE

Authorized licensed use limited to: CITY UNIV OF HONG KONG. Downloaded on April 15,2023 at 06:45:27 UTC from IEEE Xplore. Restrictions apply.

prominent drawback [9][10]. This was the entry point for the design of TSRG.

TSRG is a family of PRNGs. It consists of at least Two Stages of Random number Generators (TSRG). TSRG utilizes the output of any PRNG called Randomizer as an auxiliary synchronized input to a second adapted suitable PRNG (called Modified PRNG). TSRG output is adapted to be a function of the output of randomizer as well as its second PRNG. TSRG mathematical model, characteristics, its attack-oriented design, attack defenses and randomness tests results are studied thoroughly in [11][12]. The randomizer expands a seed or Basic Random Data (BRD) to a pseudo-random output, which is usually of variable length. As shown in figure 1, the Randomizer consists of symmetric encryption in special OFB mode. Normally the key should be chosen uniformly at random (or at least with high entropy), but the seed can be any byte string [13]. Suppose the BRD with length L bytes which is fed to a randomizer whose output word size of length w_p and a modified second stage PRNG with output of length w_m with P parameters. The set of equations describing this system is given by the following:

1- $s=L/w_m$ and for simplicity w_m divides L

2- $k=w_p/w_m >=1$ and w_m divides w_p.

3- The output samples equations are:

$x_1=f(x_o,\ldots,I(1))$,

$x_2=f(x_1,\ldots,I(2))$,

$x_3=f(x_2,\ldots,I(3))$

$,\ldots\ldots\ldots$

$x_k=f(x_{k-1},\ldots,I(k))$,

$x_{k+1}=f(x_k,\ldots,I(k+1)),\ldots\ldots, x_n=f(x_{n-1},\ldots,I(n))$

4- For every k equations of the step 3, there is a controlling equation given by the following:

$I_q(ki+1)||\ I_q(ki+2)||\ \ldots||I_q(ki+k)=SYM\ (I_{q-1}(ki+1)||\ I_{q-1}(ki+2)||\ \ldots\ ||I_{q-1}(ki+k)\ )$

For $i=0,\ldots,(s/k-1)$.

Where SYM is symmetric encryption operator.

Let the number of samples sufficient to crack the system be v then there are v/k equations of the types in step 4 and v equations of the type given in step 3. Equating the number of equations with the number of unknowns:

The number of equations = v+(v/k)

= The number of BRD unknowns+ the number of parameters P + the number of I's unknowns

$v+v/k = s+P+v$ and $v=k(s+P) = (w_p/w_m)((L/w_m)+P)$

From which: *The number of samples sufficient to crack* $= (w_p/w_m)((L/w_m)+P)$ (1)

For the implemented model which consists of adapted Lehmer generator cascaded with IDEA in special output feed back mode, we have L=2048 bytes, $w_m=4$, $w_p=8$ and P=4. Substituting in equation 1.

$v=k(s+P)=(w_p/w_m)((L/w_m)+P)=(8/4)((2048/4)+4)=2*516=1032$ samples

TSRG output is accepted and the prediction of output is practically impossible since the generator changes its states to unpredictable ones at unpredictable instants (with respect to attacker) which has to be described by another set of equations containing number of unknowns greater than the number of equations before the threshold giving in equation (1).

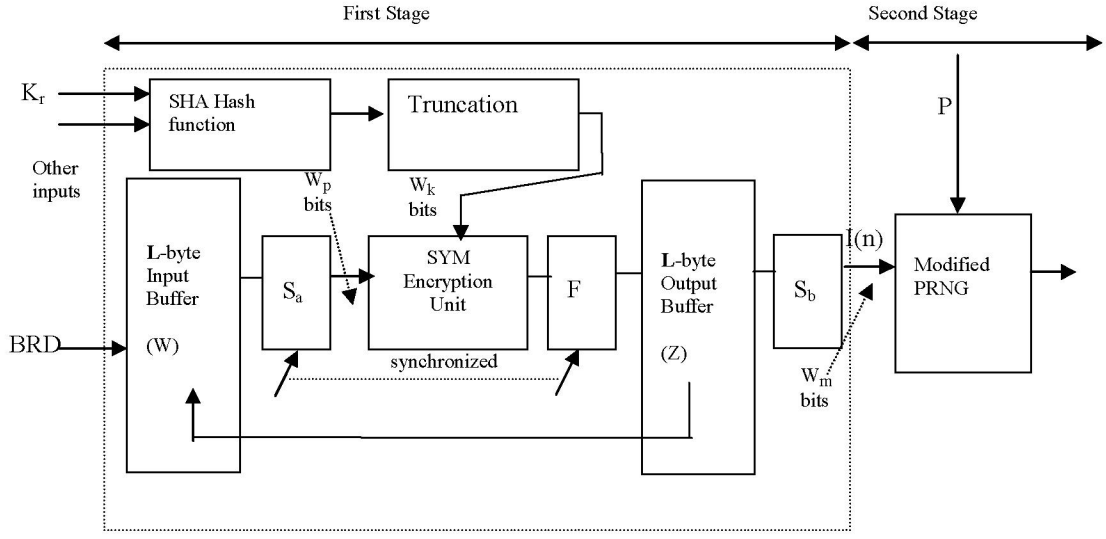

Figure 1. TSRG Diagram

Authorized licensed use limited to: CITY UNIV OF HONG KONG. Downloaded on April 15,2023 at 06:45:27 UTC from IEEE Xplore. Restrictions apply.

In the experimental implementation of TSRG, the cryptanalyst has to solve about 1000 equations in same number of unknowns with two third of them are modular linear equations and one third of them are nonlinear logical equations. Since the TSRG RNG randomly changes its model to unpredictable one before the 1000 samples limit, it is cryptographically secure [11].

III. TSRG CRYPTOSYSTEM

TSRG is the basic primitive in designing the cryptosystem. If the designer of the TSRG is sure that its output is secure (in other words, no attack including state compromise extension attack, can be mounted on it then a simple combing using Xoring or Latin Square combiner, of the TSRG output with plain text is sufficient and the format of the sent message will be as shown in figure (2):

Encrypted BRD	Plaintext message Combined with TSRG RNG output

Figure 2. Perfect Message Format

Figure 3 shows the proposed block diagram for the secure transmission of data over an insecure communications line using TSRG randomized encryption procedure. Note that the TSRG random bit sequence is within the secure area of the encryption unit. In the same time, there is an important dissimilarity between this model and the general model from the typical randomized encryption model as described in [14]. The difference is, the TSRG in our case does not only feed the random data to the deterministic encryption algorithm but also provides its BRD [15][16].

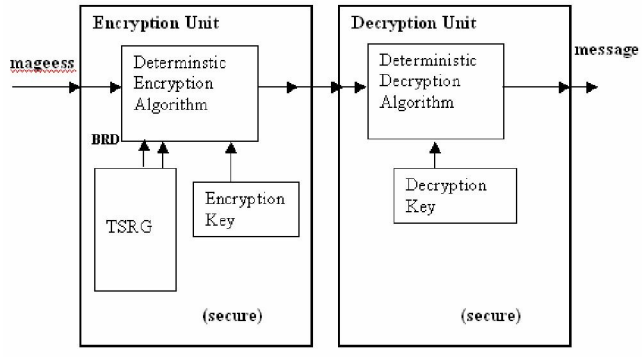

Figure 3. Block Diagram for TSRG transmission

The TSRG encrypted message can be given by the following equations shown in Figure 4:

$$C=R_p||((M\oplus R)||E(BRD))||R_s \quad (2)$$

Where :

R, R_p, R_s : sets of bit sequences generated by TSRG,

M : Plaintext message, C: the cipher text.

: Combiner operator (e.g. xor), ||: concatenation operator.

The ciphertext format consists of a useful encrypted message embedded between the message prefix (R_p) and suffix random data (R_s).

IV. THE OTHER CRYPTOSYSTEMS

OTP ciphering is mathematically-proven to be absolutely secure, and therefore is better than any other cipher. Once one buys into this delusion, the issues become things like Why would anyone use anything else?,
If other ciphers are good, why don't they have proofs like an OTP?

The Fact is, the OTP which is unconditionally secure is not the realized OTP which is used in practice.

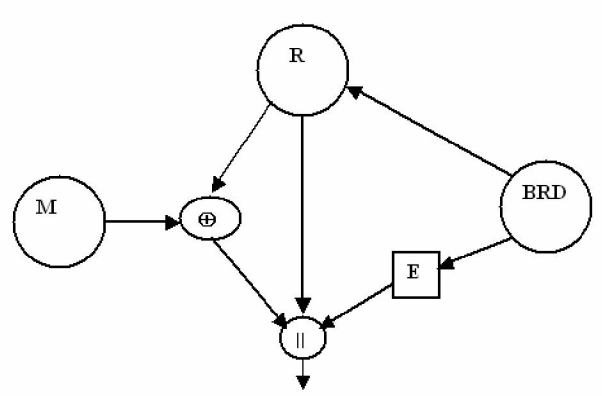

Figure 4. TSRG Message Construction

A. Unconditionally Secure Cryptosystem

When using OTP, we face the difficulty of generating, transporting, and keeping the keying material in absolute security. Each one of the previous processes is an attack entry point. The process of ciphering is simply by combining message bits with the prepared random key (One Time Pad) using XOR or Latin Square combining. The key management is usually solved by saving the key material on magnetic tapes or CD-ROMs to be distributed between parties. These CDs, which contains the lengthy private key, must be exchanged securely among subscribers. When the CD random data is exhausted, it is replaced with another one. It is clear that the opponent agents can copy a CD, so it is washed by encryption before usage. Another problem is that the receiver must save all previous CD's since there is a probability that a previous cipher message with exhausted CD may be required to be decrypted. The use of CD-ROMs, containing true random data, makes this a practical solution to many computer-to-computer communications problems under the assumption that the key can be securely distributed and maintained. Simply, the enemy's agent can copy the CD containing the heart of cryptosystem key material since it is periodically distributed among parties.

B. Rabin Everlasting Cryptosystem

M. Rabin has proposed a solution for everlasting security. Rabin's bounded storage model for everlasting encryption requires an intense continuous stream of random bits; the encoded message is embedded within it, which overwhelms the storage capacity of opponent [6] [17]. The shared key can be used for exponential number of times while adaptive key compromise attack is mounted and if

Authorized licensed use limited to: CITY UNIV OF HONG KONG. Downloaded on April 15,2023 at 06:45:27 UTC from IEEE Xplore. Restrictions apply.

the key is compromised then there is no proof of the previous message is also compromised since the opponent does not recorded all data encompassing the message[18]. It is clear that the overhead in this case is high and cannot be implemented for networks at least for the time being without shared governmental support. Rivest proposed the use of randomized encryption techniques with the expected cost of increasing the required communications bandwidth. If the ratio of the length of random data over that of the message length is tends to infinity then the cipher turns to be everlasting encryption [14]. It is clear that the overhead of using randomized encryption technique is a prominent character of this scheme. This disadvantage has its worst condition when using the Everlasting encryption in order to obtain everlasting security.

V. TSRG CRYPTOSYSTEMS AND OTHERS

In this section, a discussion of trials of various attacks on the previous cryptosystems to be mounted:

A. Attacking OTP Cryptosystem

The OTP is a very difficult system to use properly, and the chance of a terrible key-management failure is too high to neglect in most situations. When using OTP, we face the difficulty of generating, transporting, and keeping the keying material in absolute security. Each one of the previous processes is an attack entry point as shown below:

1. Key Generation: True random generators combine physical phenomena with cryptographic techniques to get appearing random data. The physical phenomena can be biased by intrusion which results in guessable generated random data. Another problem of key generation is the ever-increasing "entropy" in the output of the physically-random generator used for OTP keying material. But, again, we cannot quantify this, and especially we cannot guarantee it. There come a time when the generator produces less entropy than expected, and the plaintext has more "entropy" such that the plaintext leaks information.
2. Key keeping: This is the most known attack entry point since the user carelessly does not save the CD containing random data in secure place. This problem usually solved by ciphering the random data before usage using some shared key but under chosen plaintext attack, the whole system can collapse.
3. Key Transporting: Using officers to carry keys is accomplished with security problems and increase of the running cost of the system.

B. Attacking Everlasting Cipher

Rabin's proposal is cryptographically the same as a one-time pad, but it allows the user to share the pad over an insecure channel as long as he has the ability to communicate in a way that will not be immediately compromised by the eavesdropper. The shared secret key can be accomplished via Diffie-Hellman key construction, conventional public-key cryptography or Quantum Key Exchange (QKE) [19]. QKE protocols can be provably secure because the security relies on fundamental laws of quantum mechanics instead of intractability assumptions. These fundamental laws are the no-cloning theorem and for every attempt to distinguish between two non-orthogonal quantum states, information gain is only possible at the expense of introducing disturbance in the system. This key can be compromised by the three B's "burglary, bribery, or blackmail". Rabin has developed a system in which unlimited compute power in the future doesn't help the adversary without unlimited storage power now. Any particular implementation of these methods will, of course, be subject to numerous attacks:

If Rabin Everlasting cryptosystem depends on traditional key exchange mechanisms to transmit the keys that tell the receiver what parts of the random bitstream to use which means, that if someone can break this key exchange, can break the rest of the cryptosystem. The real challenge of finding a trusted source for random numbers at that high rate which may for practical consideration push the implementation to reuse random data which kicks the base of the system. It relies on the price of connection speed versus the price of storage. With the drops of storage prices, advances in quantum cryptography and the confidence that the recorded random data contains useful message, the problem is reduced to classical cryptanalysis of randomized encryption.

C. TSRG Cryptosystem Defenses

In TSRG Algorithm there is no OTP to be exchanged. Every time a message is ciphered using a new semi-true random data. There is no choice of starting pointer in CD containing true random data. The BRD is changed every time at true random manner. The TSRG built-in generator output is secure (under the condition that its state is not compromised). TSRG output is not directly observed. The hacker can attack the system by physical access to try to mount state compromise extension attack on TSRG and get its states and hence parameters. As a result, a strong access control for the computer containing the application must be made against insiders. Any outsider attack on TSRG cryptosystem must first determine the fields of the TSRG message. To determine the fields of the message, the cracker must specify the start of the useful message and its construction as given by equation 1. If the fields are deduced then the attacker must know three keys as well as TSRG parameters controlling reseeding based on the apparent entropy of the TSRG states.

- TRSG symmetric key for BRD expansion.
- Key and technique of BRD encryption
- The combining method of plaintext with expanded BRD

All the previous keys are saved with the user (e.g. ciphered on smart card) and not sent with the message, so the only imaginable technique is the brute force attack scenario with key length equal the sum of all these keys under the condition of the success of determining the three parts of the useful message and parameters of the internal reseeding mechanism of the TSRG.

Authorized licensed use limited to: CITY UNIV OF HONG KONG. Downloaded on April 15,2023 at 06:45:27 UTC from IEEE Xplore. Restrictions apply.

Trying to mount message related attack on TSRG cryptosystem can not succeed since each time new fresh BRD is created and a different ciphered message with different lengths and contents is generated even for the same plaintext.

1. Strength: Cracking TSRG message is based on solving insoluble problem with built-in all-or-nothing transform [20].
2. Speed : In ciphering a message, there are three major times:
    a. The required time to generate OTP-like pad.
    b. The encryption time of BRD.
    c. The time required to combine and prepare the message. For long messages the time in b can be neglected to a. In this case, the time is approximately that of a hybrid cryptosystem based on cryptographic PRNG.
3. Flexibility: TSRG cryptosystem can accept any data type and of any length.
4. Scalability: For each class of applications, we have to create TSRG generator to fit in its environment with scalable size of BRD and reseeding mechanism that depend on the mathematical model describing it.

VI. CONCLUSIONS

In this paper, OTP and Everlasting and TSRG cryptosystems are briefly studied. The features and possible attacks are exemplified. The danger to base the security of the global information economy on a very small number of mathematical hard to solve problems is illustrated. The proposed TSRG functional security is achieved from using its built-in TSRG whose security is based on insoluble problem. An adapted version of randomized encryption technique is utilized to assure security and have bandwidth expansion factor near unity. The security strength of the scheme has been measured and proved.

References

[1] Priit Karu, Jonne Loikkanen, "A Practical Comparison of Public Key Cryptosystems ", Tik-110.501 Seminar on Network Security, HUT TML 2000.
http://www.tcm.hut.fi/Opinnot/Tik-110.501/2000/papers/abstract_loikkanen_karu.html .

[2] Janne Frosen, "Practical Cryptosystems and their Strength", Department of Computer Science, Helsinki University of Technology.
http://www.tml.hut.fi/opinnot/tik-110.501/1995/practical-crypto.html .

[3] Bruce Lowe, "Attacking the RSA Cryptographic System", (10th May 1999)
http://www.cs.uct.ac.za/courses/CS400W/NIS/papers99/blowe/RSA.html

[4] Thierry Moreau ,"Thirteen Reasons to Say "No" to Public Key Cryptography", CONNOTECH Experts-conseils, Inc, March 4th, 1998.
http://www.connotech.com/13REAS.HTM

[5] Terry Ritter , "Practical Latin Squares Combiner"
http://www.ciphersbyritter.com/ARTS/PRACTLAT.HTM

[6] Yan Zong Ding, Michael Rabin, "*Provable Everlasting Security in the Bounded Storage Model*", PhD thesis, Harvard University, May 2001.

[7] Claude Shannon,"Communication Theory of Secrecy Systems", Bell System Technical Journal, Vol. 28, Oct. 1949, pp.656-715. http://www3.edgenet.net/dcowley/docs.html

[8] Fred Cohen, "Introductory Information Protection", 1995, Fred Cohen& Associates,
http://www.all.net/books/ip/index.html .

[9] John Kelsey, B. Schneier, "Cryptanalytic Attack on Pseudorandom Number Generator", http://www.counterpane.com/pseudorandomnumber.pdf .

[10] H. Krawczyk, "How to Predict Congruential Generators", Journal of Algorithms, Vol.13, No.4, Dec. 1992.

[11] Hussein G., Dakroury Y., Hassan B., Badr A., "TSRG: Analysis and Design of a proposed RNG", DMS 2002, Sep. 2002, San Francisco, USA.

[12] Hussein G., Dakroury Y., Hassan B., Badr A., "TSRG: Attack Oriented Design and Implementation", SECI02, Sep. 2002,Tunis.
http://www.lsv.ens-cachan.fr/~goubault/SECI-02/Final/actes-seci02/pdf/003-ghussein.pdf .

[13] Shafi Goldwasser, Mihir Bellare, " Lecture Notes on Cryptography", August 2001.
http://theory.lcs.mit.edu/shafi .

[14] Ronald L. Rivest, Alan Sherman,"Randomized Encryption Techniques", Proceedings of Crypto `82 (1982) pp. 145-163.
http://seclab.cs.ucdavis.edu/projects/vulnerabilities/scriv/1993-ifipsec.pdf
http://seclab.cs.ucdavis.edu/projects/history/ourpapers/1993c.pdf
http://www.algo.csie.nctu.edu.tw/paper/html/bdf/c82/145.bdf

[15] G. Hussein, Y. Dakroury, A. Badr, "TSRG Cryptosystem: Design and Implementation", In Proceedings of SETIT 2003,17-21 March 2003, Susa, Tunis.

[16] G. Hussein, M. W. David" TSRG Randomized Cryptosystem", Carnahan 03, Taipei, Taiwan.

[17] Y. Aumann, M. O. Rabin, "Information Theoretically Secure Communication in the Limited Storage Space Model ", In Advances in Crypto '99, pages 65-79,1999.

[18] Yan Zong Ding, Michael Rabin, "Hyper-Encryption and Everlasting Security", Springer LINK: Lecture Notes in Computer Science 2285.
http://link.springer.de/link/service/series/0558/bibs/2285/22850001.htm .

[19] D. Stucki, N. Gisin, O. Guinnard, G. Ribordy, H. Zbinden, "Quantum Key Distribution over 67 km with a plug&play system ", GAP-Optique, University of Geneva, quant- ph/ 0203118 v1 22 Mar 2002

[20] Ronald L. Rivest, "All-Or-Nothing Encryption and The Package Transform", Proceedings of the 1997 Fast Software Encryption Conference, Springer lecture notes in Computer Science #1267(1997).
http://theory.lcs.mit.edu/~rivest/fusion.ps

Authorized licensed use limited to: CITY UNIV OF HONG KONG. Downloaded on April 15,2023 at 06:45:27 UTC from IEEE Xplore. Restrictions apply.