International Journal of Computer Theory and Engineering, Vol. 1, No. 3, August, 2009
1793-8201

A New Generation Cryptographic Technique

Swarnendu Mukherjee, Debashis Ganguly and Somnath Naskar

***Abstract*—Cryptography is the science of using mathematics to encrypt and decrypt data. In cryptography, SAFER (Secure And Fast Encryption Routine) is the name of a family of block ciphers designed primarily by James Massey (one of the designers of IDEA) on behalf of Cylink Corporation as anon-proprietary cipher. The early SAFER K and SAFER SK designs share the same encryption function, but differ in the number of rounds and the key schedule. More recent versions — SAFER+ and SAFER++ — were submitted as candidates to the AES process and the NESSIE project respectively. All of the algorithms in the SAFER family are unpatented and available for unrestricted use. This is being a Technical Survey paper represents a concrete overview of SAFER appeared in the above context.**

***Keywords*— Cryptography, cipher, block cipher, AESs.**

I. INTRODUCTION

Cryptography is popularly known as an art and science of secret writing. This enables us to store sensitive information or transmit it across insecure networks (like the Internet) so that it cannot be read by anyone except the intended recipient. You use encryption to ensure that information is hidden from anyone for whom it is not intended, even those who can see the encrypted data.

The un-breakability issues of encrypted text or rather say cipher text is solved by a simple proof by Shannon in 1949. Shannon's bound implies that practical ciphers will have to depend on computational security, i.e., on the difficulty of breaking rather than the impossibility.

The problem of good cipher design is essentially one of finding difficult problems, subject to certain other conditions. This is a rather unusual situation, since one is ordinarily seeking the simple and easily soluble problems in a field.

It is difficult to be sure that a system which is not ideal and therefore has a unique solution for sufficiently large N

will require a large amount of work to break with every method of analysis. So, good ciphers are constructed in such a way that breaking it is equivalent to (or requires at some point in the process) the solution of some problem known to be laborious.

Using the above stated concept James Massey, with cooperation of Xuejia Lai designed a new cipher, which they later named the International Data Encryption Algorithm (IDEA) that used a key of 128 bits (the plaintext and cipher text were each 64 bits). This cipher was publicly available and also strong enough to compete with the already available ciphers. IDEA has been widely used and is included in the software package "Pretty Good Privacy" (PGP) that is available both as freeware and in a commercial version.

After publishing IDEA in 1991, James Massey After publishing IDEA in 1991, James Massey alone designed a publicly available cipher, the Secure and Fast Encryption Routine (SAFER) in 1993 for Cylink Corporation, a Californian Cryptographic Company. SAFER is considered to be far stronger than IDEA, which was secured but a quite slower encryption process. In this paper, we tried to project all the details of this new generation cryptographic technique in an experimental as well as efficient manner to promote all the future endeavors in this field [10].

Swarnendu Mukherjee:Computer Science and Engineering Department, Heritage Institute of Technology, AnandapurKolkata – 700107, India .

Debashis Ganguly, Computer Science and Engineering Department, Heritage Institute of Technology, Anandapur, Kolkata – 700107, India .

Somnath Naskar:Computer Science and Engineering Department, Heritage Institute of Technology, Anandapur, Kolkata – 700107, India.

II. OVERVIEW

The first SAFER cipher was SAFER K-64, published by Massey in 1993, with a 64-bit block size. The "K-64" denotes a key size of 64 bits. There was some demand for a version with a larger 128-bit key, and the following year Massey published such a variant incorporating new key schedule designed by the Singapore Ministry for Home affairs: SAFER K-128. However, both Lars Knudsen and Sean Murphy found minor weaknesses in this version, prompting a redesign of the key schedule to one suggested by Knudsen; these variants were named SAFER SK-64 and SAFER SK-128 respectively — the "SK" standing for "Strengthened Key schedule". Another variant with a reduced key size was published, SAFER SK-40, to comply with 40-bit export restrictions.

There are two more-recent members of the SAFER family that have made changes to the main encryption routine, designed by the Armenian cryptographers Gurgen Khachatrian and Melsik Kuregian in conjunction with Massey.

SAFER+ was designed in 1998 which has a block size of 128 bits. In the year 2000, SAFER++ was submitted to the NESSIE project in two versions, one with 64 bits, and the other with 128 bits [7].

III. DETAILS AND TECHNIQUES

All of these ciphers of SAFER K and SAFER SK generation use the same round function consisting of four stages, as shown in the diagram: a key-mixing stage, a substitution layer, another key-mixing stage, and finally a diffusion layer. In the first key-mixing stage, the plaintext block is divided into eight 8-bit segments, and sub keys are added using either addition modulo 256 (denoted by a "+" in a square) or XOR (denoted by a "+" in a circle). The substitution layer consists of two S-boxes, each the inverse of each other, derived from discrete exponentiation (45x) and logarithm (log45x) functions. After a second key-mixing

stage there is the diffusion layer: a novel cryptographic component termed a Pseudo-Hadamard transform (PHT). The PHT was later used in the Twofish cipher.

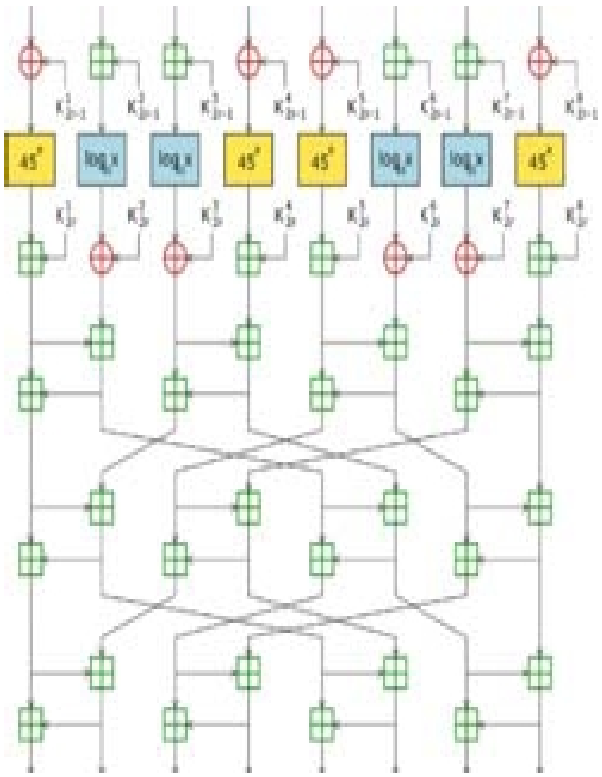

Fig.1: The Circuit diagram for the SAFER technique.

SAFER+ is a substitution-linear transformation network based on the SAFER family of ciphers. There are 8, 12, or 16 rounds, depending on the key size, plus an output transformation after the final round. The round function consists of key-controlled substitution on the sixteen bytes of the data block followed by an invertible linear transformation on the entire data block. The substitution function acts on each individual byte with a combination of key addition, key XOR, and either a fixed permutation or its inverse. The permutation corresponds to discrete exponentiation of a fixed generator in the multiplicative group of integers modulo 257. The linear transformation is generated by a combination of the Pseudo-Hadamard Transform matrix and the "Armenian Shuffle" permutation. The decryption routine is derived from the encryption routine by inverting each step.

A. Key Schedule

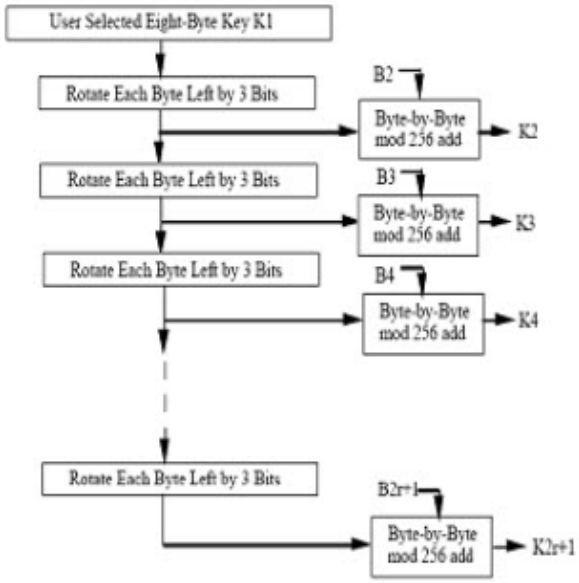

Fig.2: The Schematic diagram for the Key Generation technique.

B. Encryption

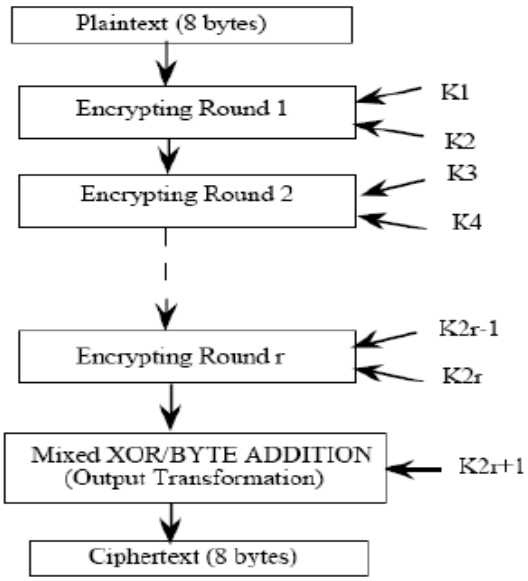

Fig.3: The Schematic diagram for the Text Encryption procedure.

C. Decryption

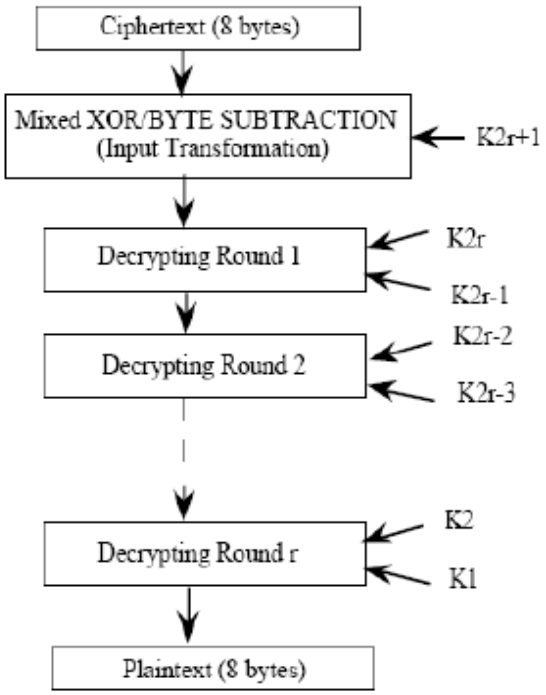

Fig.4: The Schematic diagram for the Text Decryption procedure.

IV. APPLICATIONS

The frequency hopping scheme used by the Bluetooth technology already makes listening in on Bluetooth links very difficult. In fact, the U.S. military considers a communication link using frequency hopping over 79 channels to be secure [8]. Nevertheless, Bluetooth offers encryption and authentication using an algorithm based on the SAFER+ (Secure and Fast Encryption Routine) cipher algorithm. This algorithm [8] generates 128 bit cipher keys from a 128 bit plaintext input. When initializing a security procedure, a 128 bit key is generated from a Personal Identification Number (PIN), the Bluetooth device address of the claimant, and a random number shared between the claimant and the verifier. The authentication procedure checks whether the two devices are using the same 128 bit key to verify that the same PIN number was entered on the two devices. If the authentication procedure is successful, a new 128 bit key is generated using a new random number from each unit, the Bluetooth device addresses of the two units, and the current 128 bit key. This key is used to produce the cipher stream to cipher and decipher the bit-stream data.

A secure, low cost and fast full-duplex on line data and voice encryption systems were designed implemented and tested. The design was based on FPGA technology using SAFER 64 (secure and fast encryption routine) algorithm [3]. The FPGA was designed, simulated and synthesized using ISE and Mentor Graphics EDA tools. The overall system was tested successfully on public switch telephone networks (PSTN). The encryption with key generator, and system control modules was synthesized and implemented using low cost 200, 000-gate Xilinx Spartan-3 XC3S200 FPGA.

V. EVALUATION

The most popular generation of the SAFER cipher family, SAFER+ is neither a Feistel cipher nor a substitution permutation cipher, but rather a generalization of the latter, giving the designer more freedom to seek the best properties. SAFER+ replaces the “Hadamard Shuffle” from the original SAFER family with the “Armenian Shuffle”; this resulted in faster diffusion and better resistance to differential attacks. Some other advantages are the byte orientation, the scalability of the bytes, the lack of “suspicious-looking” tables, and the mixing of additive groups. C implementations of SAFER+ and DES by the same programmers have been compared to argue that the former cipher was much faster on a Pentium platform. SAFER+ with its eight rounds is secure against linear and differential attacks with a margin of safety, acknowledging, however, that there is no proof of complete security [1].

SAFER+ was submitted as a candidate for the Advanced Encryption Standard (AES) in 1998 with the name of Cylink Corporation. The cipher was not selected as a finalist. Bluetooth uses custom algorithms based on SAFER+ for key derivation (called E21 and E22) and authentication as message authentication codes (called E1). Encryption in Bluetooth does not use SAFER+ [5].

SAFER++ is undoubtedly secured than SAFER+. Till now no security flaws have been found in SAPER++ and its performance is also relatively good. Its design has many interesting properties. Therefore it has been selected as an NESSIE project [7].

VI. CONCLUSION

In Section III, we indicated how SAFER K-64 achieves good diffusion and good confusion, the two basic features that contribute to the security of a block cipher. The best measure of security available today for an iterated block cipher is its resistance to attack by differential cryptanalysis. It has been shown that, for the appropriate definition of difference between a pair of plaintext blocks (or a pair of cipher text blocks), SAFER K-64 is a Markov cipher, a fact that greatly simplifies its analysis for resistance to differential cryptanalysis. Cylink Corporation has contracted for such an analysis of SAFER K-64 by a group of cryptanalysts that does not include the designer of the algorithm. A considerable effort has been invested in this effort, whose conclusion is that six-round SAFER K-64 appears to be secure against differential cryptanalysis. This group of cryptanalysts has also done extensive statistical testing of SAFER K-64 with no detection of any weakness. The evidence available today suggests that SAFER K-64 is a strong cipher whose strength is well measured by the length (64 bits) of its user-selected key [3].

REFERENCES

[1] Alex Biryukov, Christophe De Cannire, Gustaf Dellkrantz, “Cryptanalysis of SAFER++”. CRYPTO 2003, Aug: 17-21, 2003, USA, pp:- 195-211.

[2] Lars R. Knudsen, “A Detailed Analysis of SAFER K”, Journal of Cryptology, Volume 13, Issue 4, 2000, pp:- 417-436.

[3] James L. Massey, “SAFER K-64: A Byte-Oriented Block-Ciphering Algorithm”, Fast Software Encryption, Cambridge Security Workshop Proceedings, Springer, 1994, pp:-: 1-17.

[4] James L. Massey, "SAFER K-64: One Year Later", Fast Software Encryption, 2nd International Workshop Poreceedings, Springer, 1994, pp:- 212-241.

[5] James Massey, Gurgen Khachatrian, Melsik Kuregian, "Nomination of SAFER+ as Candidate Algorithm for the Advanced Encryption Standard", 1st Advanced Encryption Standard Canditate Conference, CA, Aug: 20-22, 1998, pp:- 1-14.

[6] Massey, J. L., "Announcement of a Strengthened Key Schedule for the Cipher SAFER", Revision of September 15, 1995.

[7] James Massey, Gurgen Khachatrian, Melsik Kuregian, "Nomination of SAFER++ as Candidate Algorithm for the New European Schemes for Signatures, Integrity, and Encryption (NESSIE), " Presented in First Open NESSIE Workshop, November, 2000.

[8] Lars R. Knudsen, "A Key-schedule Weakness in SAFER K-64", In Proceedings of 15th Annual International Cryptology Conference on Advances in Cryptology, CRYPTO 1995, USA, 1995, pp:- 274-286.

[9] Lars R. Knudsen, Thomas A. Berson, "Truncated Differentials of SAFER", In the book Fast Software Encryption, Springer, Volume 1039, 1996, pp:- 15-26

[10] X. Lai, J. Massey, and S. Murphy, "Markov Ciphers and Di_erential Cryptanalysis", In Proceedings of EUROCRYPT '91, 1991, Brighton, UK, 1991, pp. 17-38

Swarnendu Mukherjee has completed his B. Tech in Computer Science and Engineering from Heritage Institute of Technology, Kolkata, India. His research interest includes Image Processing, Network Security, and Biometric Authentication, Data Mining and etc.
He is currently associated with Indian Statistical Institute and Jadavpur University for projects and research activities. He is an active fellow of Computer Society of India. He is also attached with IACSIT Singapore Section and ACEEE India.He has published more than fifteen research papers in reputed Journals and IEEE International Conferences.

Debashis Ganguly is currently pursuing B. Tech in Computer Science and Engineering from Heritage Institute of Technology, Kolkata, India. His research interest includes Image and Digital Signal Processing, Network Security, and Biometric Authentication, Data Mining and etc.
He is currently associated with Indian Statistical Institute as a Junior Research Fellow for projects and research activities. He is also a fellow of Computer Society of India and an active member of IEEE.
He is author eight research papers in reputed Journals and IEEE International Conferences and also waiting for other nine papers to get published as accepted in different international journals and conferences.

Somnath Naskar is currently pursuing B. Tech in Computer Science and Engineering from Heritage Institute of Technology, Kolkata, India.
He is currently associated with ISI for project which is based on developing a new feature extraction tecnique and classifier for online handwritten bangla characters. His research interest includes Pattern Recognition, Image Processing and Security.
He has already published one paper in a reputed international IEEE conference.