Academic City University College, Accra, Ghana
Society for Multidisciplinary & Advanced Research Techniques (SMART)
Trinity University, Lagos, Nigeria
SMART Scientific Projects & Research Consortium (SMART SPaRC)
Harmarth Global Educational Services
ICT University Foundations USA
IEEE Computer Society Nigeria Chapter

33rd ECOWAS iSTEAMS ETech Multidisciplinary Conference (ECOWAS-ETech)

Differential Cryptanalysis in Stream Ciphers

Emmanuel Ofori-Opoku Adjei
Department of Information Systems and Innovations
School of Technology
Ghana Institute of Management and Public Administration
GreenHills, Accra, Ghana
Email: Emmanuel.ofori-opoku@st.gimpa.edu.gh

ABSTRACT

An introductory introduction to the cryptanalysis of stream ciphers is provided in this paper. In order to clarify the fundamental concept of cryptography and the many characteristics of stream ciphers, a few historical instances are first offered. We explain what cryptographic strength is and how to spot flaws in a cryptosystem. Then, we demonstrate how a variety of cryptanalytic approaches can be used to exploit and combat these cryptographic flaws. The relationships between differential and other types of stream cipher analysis are presented. The conservation laws of patterns and of mutual information are derived. The cryptographic significance of pattern distribution of key stream sequences is shown.

Keywords : Cryptography, Cryptographic Algorithms, Cryptanalysis, Ciphers

Proceedings Citation Format
Emmanuel Ofori-Opoku Adjei (2022): Differential Cryptanalysis in Stream Ciphers. Multidisciplinary Conference. University of Ghana/Academic City University College, Ghana. 29th Sept – 1st Oct, 2022. Pp 215-220.
www.isteams.net/ghanabespoke2022. dx.doi.org/10.22624/AIMS-/ECOWASETECH2022P41

1. INTRODUCTION

Stream ciphers have a long history and are still useful for keeping communications secure. Because of their reasonably tractable structure, additive synchronous stream ciphers are the focus of the majority of the work on stream cipher design and analysis. It was hypothesized that a universal technique for examining diverse cryptographic primitives is differential cryptanalysis. Block ciphers and hash functions were both heavily used as targets for the technique, and numerous new constructions of these primitives have been created with this attack resistance in mind. Several public key cryptosystems were examined using the principles of differential cryptanalysis. Due to its block-cipher-like description, Patarin's 2R cryptosystem was studied using differential cryptanalysis.

Recent differential attacks on another multivariate public key cryptosystem were disclosed in. Differential fault analysis also made use of differential concepts . In this type of attack, the attacker can introduce computation flaws that will affect the outcomes. The attacker can learn details about the computation by comparing the differences between a correct computation and one that is flawed. Several cryptanalytic attacks on stream ciphers made advantage of these concepts.

1.1 Relational Concepts

Several strategies for breaking stream ciphers exist, and they are all fairly similar to the ones described in this paper. Most of these methods are improvised methods for cracking a particular stream cipher. Babbage takes into account a number of streams generated by the same key with various IVs in his attack on LILI-128 [11].Given that the majority of stream ciphers are built to allow a fixed key with a variety of potential IVs, this approach is realistic.

The state machine receives an unprocessed XOR of the key and IVs from the LILI-128 keying mechanism. When using the same key with various IVs, as in Babbage's attack, guessing a little portion of the key yields knowledge of a small portion of the internal state in numerous key streams. With a time complexity of roughly 2^{39} operations, this was used to attack LILI-128 with approximately 64 output streams (generated under the same key but with distinct public IVs). Another similar idea may be found in the analyses of the attacks in [15, 21, 23], where RC4 is discussed. By employing several known IVs in these attacks, it is feasible to compile statistical data about the internal status of RC4.In contrast to Babbage's attack, where any collection of IVs might be used, these RC4 attacks wait for IVs that produce a certain internal state with a distinguishable feature. When the house is recognized, information regarding the secret key is revealed (as for different keys different IVs achieve this property).

A different strategy is outlined in [30] in an assault on Py.Different IVs with a fixed key are used in the attack. The attack on Py [5] demonstrates that for any given key, there is a set of 2^{16} IVs, of which two are expected to initialize the identical internal state, in contrast to the way that RC4 attacks typically wait for some internal state to be established. Therefore, the same output stream is anticipated for these IVs.The requirements for this attack are the tightest of all the attacks because it expects a specific IV circumstance (which is still a very probable model).

3. DIFFERENTIAL CHARACTERISTICS OF STREAM CIPHERS

The kinds of stream ciphers include synchronous, self-synchronizing and those which provide authentication. Each of these choices specify the stream cipher's interface, which in turn specifies the potential differentials for the cipher.

Synchronous Stream Ciphers

These ciphers can be defined using a set of three algorithms — an internal state initialization procedure

S = INIT(key, IV),where S denotes the internal state, an internal state update function S =UPDATE(S), and an output function KS = OUTPUT(S) that produces the key stream.

For such ciphers there are three types of differential characteristics:

(∆key,∆IV) ------>∆S, where a difference in the key or the IV generates a difference in the internal state,

update
∆S ----------→ ∆S through the internal state update function,
Output

output
–∆S ----------→∆KS, where a difference in the internal state generates a key stream difference.

1.2 Self-synchronizing stream cipher

The plaintext is an additional input for the UPDATE and OUTPUT functions for self-synchronizing stream ciphers and ciphers that provide authenticated encryption.There is an additional algorithm TAG for authorized encryption that converts the internal state into a MAC tag.

We now summarize the functions for such stream ciphers:

– S = INIT(K, IV), where K is the key and IV is the IV.
– S = UPDATE(S, P), where P is the plaintext word.
– C = OUTPUT(S, P), where C is the resulting ciphertext word.
– (S, P) = DECRY PT(S,C), where C is the ciphertext word and where P is the resulting plaintext word.
– tag = TAG(S), which is the tag produced by the internal state (if authenticatedencryption is offered).

The possible characteristics in this case are:

– (∆key, ∆IV) ---INIT---→∆S, where a difference in the key or the IV generates adifference in the internal state,

UPDATE
– ∆S ––––––––> ∆S through the internal state update function,

UPDATE
– (∆S, ∆P) ––––––→_S is the differential that predicts the difference in the internal state given the current difference of the internal state and the difference in the plaintext word.

OUTPUT
– (∆S, ∆P) ––––––––>is the differential that predicts the ciphertext difference given the internal state difference and the plaintext difference

DECRY PT
– (∆S, ∆C) ––––––––> (∆S, ∆P) is the differential that predicts the plaintext difference given the internal state difference and the ciphertext difference.

TAG
– ∆S ––––> ∆tag is the differential that predicts the tag difference.

2. RELATED LITERATURE

Numerous scholarly works that represent elementary cryptanalytic approaches using complicated mathematical notations can be found in the literature. In contrast, this work attempts to present the most widely applied cryptanalytic methods using just simplified illustrations. Several academic works mount practical attacks on actual cryptosystems using the discussed methodologies. It is demonstrated that the stream differences may be predicted (with some confidence) from a key difference or even an initial value difference.

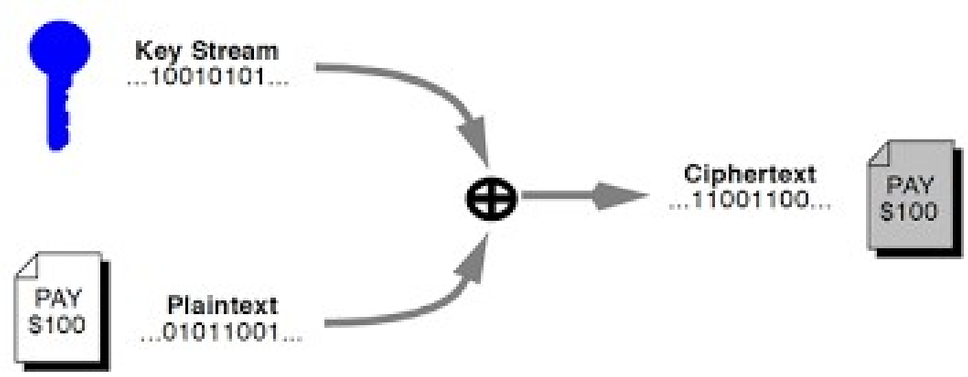

Fig 1: Stream Cipher Crypro System.

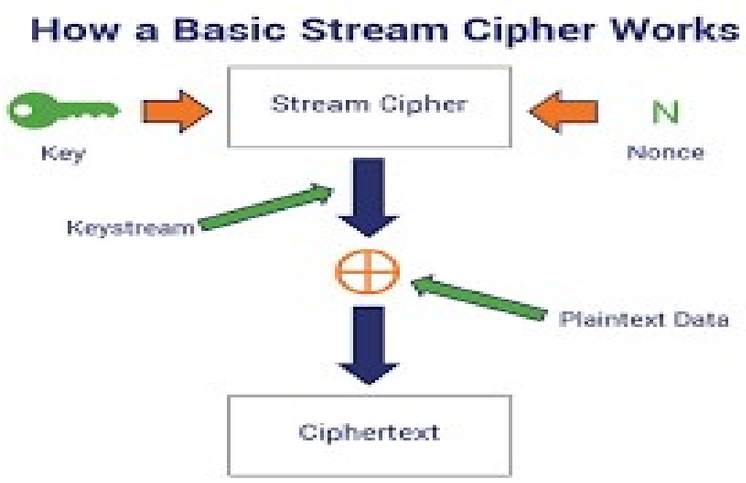

Fig 2: How a Stream Cipher Works

3. FINDINGS

Several strategies for breaking stream ciphers exist, and they are all fairly similar to the ones described in this paper. Most of these methods are improvised methods for cracking a particular stream cipher.

4. RESEARCH GAPS

Is it possible for plaintext of message to be broken down into single bytes instead of bits to be converted individually into ciphertext using key bits?

5. RECOMMENDATIONS FOR PRACTICES,POLICIES,AND DESIGN

Regarding the security of stream ciphers, the presence of differential properties and differentials in the stream cipher has a number of ramifications. Therefore, when creating new stream ciphers, designers should keep these problems in mind.

6. CONCLUSION

Thus, we draw the conclusion that differential cryptanalysis, even when used to crack stream ciphers, is a useful and significant tool in the cryptanalyzer's toolkit.

7. DIRECTION FOR FUTURE WORKS

The study of the possibility of a stream cipher breaking a plain text message down into single bytes instead of bits,which then are converted individually into ciphertext using key bits.

REFERENCES

1. Eli Biham, Adi Shamir, Differential Cryptanalysis of the Data Encryption Standard, Springer-Verlag, 1993.
2. Eli Biham, Adi Shamir, Differential Fault Analysis of Secret Key Cryptosystems, Advances in Cryptology, proceedings of CRYPTO 97, Lecture Notes in ComputerScience 1294, pp. 513–525, Springer, 1997.
3. Dan Boneh, Richard A. DeMillo, Richard J. Lipton, On the Importance of Checking Cryptographic Protocols for Faults (Extended Abstract), Advances in Cryptology,proceedings of EUROCRYPT 97, Lecture Notes in Computer Science 1233, pp. 37–51, Springer, 1997.16
4. Marc Briceno, Ian Goldverg, David Wagner, A Pedagogical Implementation of theGSM A5/1 and A5/2 “voice privacy” encryption algorithms. Available online at http://www.scard.org/gsm/a51.html.
5. Andrew Clark, Ed Dawson, Joanne Fuller, Jovan Dj. Golic, Hoon Jae Lee, WilliamMillan, Sang-Jae Moon, Leone Simpson, The LILI-II Keystream Generator, proceedings of ACISP 2002, Lecture Notes in Computer Science 2384, pp. 25–39, Springer, 2002.
6. Ed Dawson, Andrew Clark, Jovan Dj. Golic, William Millan, Lyta Penna, Leonie R. Simpson, The LILI-128 Keystream Generator, preproceedings of NESSIE 1st workshop, Leuven, 2000.
7. Christophe De Canni`ere, Bart Preneel, Trivium Specifications, eSTREAM proposal, available on-line at http://www.ecrypt.eu.org/stream/p3ciphers/trivium/trivium p3.pdf, 2005.

8. Vivien Dubois, Pierre-Alain Fouque, Jacques Stern, Cryptanalysis of SFLASH with Slightly Modified Parameters, Advances in Cryptology, proceedings of EUROCRYPT2007, Lecture Notes in Computer Science 4515, pp. 327–341, Springer,2007.
9. Niels Ferguson, Doug Whiting, Bruce Schneier, John Kelsey, Stefan Lucks, Tadayoshi Kohno, Helix: Fast Encryption and Authentication in a Single CryptographicPrimitive, proceedings of Fast Software Encryption 10, Lecture Notes inComputer Science 2887, pp. 330–346, Springer, 2003.
10. Scott R. Fluhrer, Itsik Mantin, Adi Shamir, Weakness in the key scheduling algorithm of RC4, proceedings of SAC'01, Lecture Notes in Computer Science 2259, pp. 1–24, Springer, 2001.
11. Scott R. Fluhrer, D. A. McGrew, Statistical Analysis of the Alleged RC4 Stream Cipher, proceedings of Fast Software Encryption 6, Lecture Notes in Computer Science 1978, pp. 19–30, Springer, 2001.
12. Pierre-Alain Fouque, Louis Granboulan, Jacques Stern, Differential Cryptanalysis for Multivariate Schemes, Advances in Cryptology, proceedings of EUROCRYPT 2005, Lecture Notes in Computer Science 3494, pp. 341–353, Springer, 2005.
13. Martin Hell, Thomas Johansson, Willie Meier, Grain — A Stream Cipher for Constrained Environments, preproceedings of ECRYPT's Symmetric Key Encryption Workshop, Aarhus, 2005.
14. Alexander L. Grosul, Dan S. Wallach, A Related-Key Analysis of RC4, Rice Universitechnical report TR00-358, 2000.