# SECURITY WITH WHITE BOX CRYPTOGRAPHY

**[1]Asmita, [2] Ankush**

*[1,2]Computer Science & Engineering Department, M.D.U, (India)*

## ABSTRACT

*This paper presents the study of white box cryptography. . In this paper a study of various papers is done, and in the reviewed paper we explain the white box cryptography for the security purpose. The main part of this paper covers the security assessment of white-box implementation. cryptographic primitives are designed to protect data and keys against black-box attacks.*

***Keywords*: *Cipher, Deliniarization, Strategy, Security, Tabularization***

## I. INTRODUCTION

As we know that we live in information society, we rely on the exchange and processing of information. Evidence of this evolution is rapid growth of communication network and trend awards complex software application with strong security requirement.

Increasing use of portable devices and wireless network are the examples of security requirement. Communication with friends and colleagus via e-mail and chat; the launch of (interactive) digital television and other media platforms(e.g., iTunes); on-line banking and purchase of goods and services; online-gaming;GPS navigation; professional and social networks (e.g., LinkedIn and Facebook);and many more. In one way or another, these new trends affect our daily activities in many ways, at home and in our professional life. On the downside however, we become increasingly dependent on the information infrastructure that empower our information society, and hence potentially vulnerable to attacks on them. In recent years, this has been illustrated by attacks on Internet servers, credit card fraud, hacking of banking applications and on-line games, cell phones and TV set-top boxes, phishing, privacy violation, botnet threat In order to support our information society for the next years, and take advantage of the opportunities that it enables, the need for trustworthy information infrastructure is growing. The trend towards complex software applications with strong security requirements, increasingly demands for qualitative protection technologies. One prominent building block to enable information security is *cryptology* .The word cryptology is derived from the Greek words *krypty´os* meaning ‘hidden ,and *logos*, meaning ‘word’. Strictly speaking, it is the science that studies how to hide confidential information. Cryptology comprises of two complementary fields .*cryptography* is the study and practice of hiding information, while *cryptanalysis* is the study of methods to obtain knowledge from hidden information.

The foundations of cryptography originate from Shannon, who is regarded as the founder of information theory. In his seminal work on a mathematical model for cryptography in 1948 [10],

## II. OBJECTIVE

The objective of White-Box Cryptography is to implement cryptographic primitives in such a way that, within the context of the intended application, having full access to the cryptographic implementation does not present any advantage for a computationally bounded adversary in comparison to the adversary dealing with the implementation as a black box.

The objectives of information security can be categorized into three main goals.

- Confidentiality – Concealing a message against unauthorized eavesdropping.
- Integrity – Protecting a message against tampering.
- Authentication – Refers to entity authentication, related to the identification of the (legitimate) parties, whereas data authentication is equivalent to integrity.

Depending on the application in which a cryptosystem is deployed, a number of other objectives can be formulated, such as non-repudiation, and availability.

A cryptosystem is designed in order to achieve these objectives, and a cryptographic cipher is a pair of algorithms that implements the encryption (E) and decryption (D) primitives for a cryptosystem. In accordance to Kerckhoffs' principle [14], the algorithms are public, while a (secret) key is used to instantiate a cipher.

## III. MODEL OF WHITE BOX

Cryptographic ciphers are generally designed in the standard cryptographic model named as the *black-box model* where the communication end points and computing environments are been trusted. Exist applications do not comply with this model,so for this new model needs to be formulated. We define the *white-box model* as the worst-case attack model, in which adversaries have full access to the implementation of cryptographic primitives, and complete power over their execution environment. Software obfuscation is an active field of research, and many other techniques have been proposed to protect software code and embedded data structures. However, no technique has been presented that is able to obfuscate cryptographic primitives such that a sufficient level of confidentiality of secret key information is obtained. As a result of these efforts, by the end of the nineties, it was believed to be impossible to hide computational information into software binaries. That is, information that is used at execution time (in contrast to *passive* information, such as watermarks). In the *white-box model*, the adversary has total visibility of the software implementation of the cryptosystem, and full control over its execution platform. One could refer to the *white-box model* as the worst-case model, where in contrast to grey-box models, it is impossible for an adversary not to comply with the this model. The white-box model is used to analyze algorithms that are running in an untrusted environment, that is, an environmentin which applications are subject to attacks from the execution.

## IV.INITIAL STRATEGY OF WHITE BOX

The strategy proposed by Chow *et al*.[ 31] consists of transforming a given block ciphers into a randomized, key dependent network of lookup tables. This consists of three main steps-

### 4.1 Partial Evaluation

This can be done by embedding the key into operation by transforming the (fixed)S-boxes $S_i$ into key dependent lookup tables $T_{i.}$

$$T_i(x):=S_i(x+K_i)$$

### 4.2 Tabularizing

In this process transforming of all components of the block cipher including the linear transformations into lookup tables is performed. This process may seem like 'black art' for those who are not familiar with whiteboxing techniques. Also, there is no generic ‘compiler’ or algorithm for transforming a given algorithm into its tabularized equivalent. Instead, in the literature, a list of techniques is presented by means of demonstration on white-box implementations of the DES and the AES.

### 4.3 Randomization and Delinearization

The reason why a transformation to lookup tables is used, is because lookup tables can implement any given function.Hence they are the ideal primitive to hide information.Observe a chain of three consecutive lookup tables in the network $L3$ o$L2$ $oL1$,where $L2$ contains some key information that needs to be hidden (e.g., $L2(x)$ $=x$ © $k$). Because the description of the lookup tables is available to a white-box adversary.

## V. SECURITY

The (black-box) security of any primitive is captured using a security notion where the adversary is given black-box access to some functionality (e.g., encryption), and a white-box implementation can be required to satisfy that security notion when the adversary is given access to at the function of white-boxed version .We would like an obfuscation to ensure that all the security notions are satisfied in the white-box variant when they are satisfied in the black-box.so from prior work, it is not fully clear if any of the existing definitions of obfuscation can be used to achieve such a aim .In respect to this a natural question is arises that the obfuscator satisfying the virtual black-box property for a program P and some security notion that is satisfied when the adversary is given black-box access to P, can it be proved that the security notion remains satisfied when the adversary is also given access to the obfuscated program O(P)? A major area of study in cryptology involves formal security models to assess the security of cryptographic primitives. Formal security models specify how an adversary can interact with (legitimate users of) a cryptosystem, and what should be achieved in order to break the cryptosystem. We refer to Dent [30] for an overview of models in provable security, and their respective issues.

## VI. CONCLUSION

From the above study we conclude that the main aim of White-Box Cryptography is to implement cryptographic primitives in such a way that they achieve a certain level of robustness against an adversary that has full access to and control over the implementation of the primitive. At some extent, this is related to code obfuscation, which attempts to hide certain characteristics of a program. Despite the fact that many formal models for obfuscation have been presented, white-box cryptography lacks foundations. This paper provides an initial step to bring the foundations of white-box cryptography to a same level as obfuscation. Our work made several contributions in this regard. We extend the notion of WBC to arbitrary cryptographic primitives and initiated a formal study of WBC by introducing precise definitions of what it means for a white-box implementation to be secure

## VII. ACKNOWLEDGMENT

I show my thanks to all the departments’ personals and sponsors who give us an opportunity to present and express my paper on this level. We wish to place on my record my deep sense of gratitude to all reference papers authors for them valuable help through their papers, books, websites etc.

## REFERENCES

[1] Carlisle M. Adams and Stafford E. Tavares. Designing S-boxes for ciphers resistant to differential cryptanalysis. In Proceedings of the 3rd Symposium on State and Progress of Research in Cryptography, pages 181–190, 1993.

[2] Ben Adida and Douglas Wikstr¨om. How to Shuffle in Public. In Proceedings of 4th Theory of Cryptography Conference (TCC 2007), volume 4392 of Lecture Notes in Computer Science, pages 555–574. Springer-Verlag, 2007.

[3] Ibrahim A. Al-Kadi. The origins of cryptology: The Arab contributions, volume 16(2) of Cryptologia, pages 97–126. April 1992.

[4] ATMExpress. Understanding ATM Security: Tripe DES Technology, Remote KeyEntry, and EPP's. https://www.atmexpress.com/downloads/tripledes.pdf.

[5] Boaz Barak. How to Go Beyond the Black-Box Simulation Barrier. In Proceedings of the 42nd symposium on Foundations of Computer Science (FOCS 2001), IEEEComputer Society, pages 106–115, Washington, DC, USA, 2001. IEEE Computer Society.

[6] Boaz Barak, Oded Goldreich, Rusell Impagliazzo, Steven Rudich, Amit Sahai, Salil Vadhan, and Ke Yang. On the (Im)possibility of Obfuscating Programs. In Advances in Cryptology - CRYPTO 2001, volume 2139 of Lecture Notes in Computer Science, pages 1–18. Springer-Verlag, 2001.

[7] P. Barreto and V. Rijmen. The Khazad legacy-level block cipher. In First openNESSIE Workshop, page 15. 13-14 November 2000.

[8] Mihir Bellare, Anand Desai, E. Jokipii, and Phillip Rogaway. A Concrete Security Treatment of Symmetric Encryption. In Proceedings of the 38th Symposium on Foundations of Computer Science (FOCS 1997), IEEE Computer Society, pages 394–403, 1997.

[9] Mihir Bellare, Anand Desai, David Pointcheval, and Phillip Rogaway. Relations Among Notions of Security for Public-Key Encryption Schemes. In Advances in Cryptology - CRYPTO 1998, volume 1462 of Lecture Notes in Computer Science, pages 26–45. Springer-Verlag, 1998. 149

[10]. Claude E. Shannon. A mathematical theory of communication

[11] Mihir Bellare and Phillip Rogaway. The Security of Triple Encryption and a Framework for Code-Based Game-Playing Proofs. In Advances in Cryptology -EUROCRYPT 2006, volume 4004 of Lecture Notes in Computer Science, pages 409–426. Springer-Verlag, 2006.

[12] Ryad Benadjila, Olivier Billet, and Stanislas Francfort. Drm to counter sidechannel attacks? In Proceedings of 7th ACM Workshop on Digital Rights Management(DRM 2007), pages 23–32, New York, NY, USA, 2007. ACM Press.

[13] Eli Biham. New types of cryptanalytic attacks using related keys. In Advances in Cryptology - EUROCRYPT 1993, volume 765 of Lecture Notes in Computer Science, pages 398–409, Secaucus, NJ, USA, 1994. Springer-Verlag.

[14] The Bell System Technical Journal, 27:379–423, 623–, july, october 1948.Auguste Kerckhoffs. La cryptography militaire. Journal des sciences militaires, IX:5–38, Janvier 1883. .

[15] Eli Biham, Ross J. Anderson, and Lars R. Knudsen. Serpent: A New Block Cipher Proposal. In Proceedings of the 5th International Workshop on Fast Software Encryption (FSE 1998), volume 1372 of Lecture Notes in Computer Science, pages 222–238, London, UK, 1998. Springer-Verlag.

[16] Eli Biham and Adi Shamir. Differential Cryptanalysis of DES-like Cryptosystems.In Advances in Cryptology - CRYPTO 1990, volume 537 of Lecture Notes in Computer Science, pages 2–21.Springer-Verlag, 1990.

[17] Eli Biham and Adi Shamir. Differential Cryptanalysis of the Data Encryption Standard. Springer-Verlag, London, UK, 1993.

[18] Eli Biham and Adi Shamir. Differential Fault Analysis of Secret Key Cryptosystems. In Advances in Cryptology - CRYPTO 1997, volume 1294 of Lecture Notes in Computer Science, pages 513–525. Springer-Verlag, 1997.

[19] Eli Biham and Adi Shamir. Power Analysis of the Key Scheduling of the AES Candidates. Presented at the 2nd AES Candidate Conference, Rome, March 22–23, 1999.

[20] Olivier Billet and Henri Gilbert. A Traceable Block Cipher. In Advances in Cryptology - ASIACRYPT 2003, volume 2894 of Lecture Notes in Computer Science, pages 331–346. Springer-Verlag, 2003.

[21] Olivier Billet, Henri Gilbert, and Charaf Ech-Chatbi. Cryptanalysis of a White Box AES Implementation. In Proceedings of the 11th International Workshop on Selected Areas in Cryptography (SAC 2004), volume 3357 of Lecture Notes in Computer Science, pages 227–240. Springer-Verlag, 2004.

[22] Alex Biryukov, Christophe De Canni`ere, An Braeken, and Bart Preneel. A Toolbox for Cryptanalysis: Linear and Affine Equivalence Algorithms. In Advances in Cryptology - EUROCRYPT 2003, volume 2656 of Lecture Notes in Computer Science, pages 33–50. Springer-Verlag, 2003.

[23] Dan Boneh, Richard A. Demillo, and Richard J. Lipton. On the importance of eliminating errors in cryptographic computations. Journal of Cryptology,14(2):101–119, 2001.

[24] Dan Boneh and Matthew K. Franklin. Identity-Based Encryption from the Weil Pairing. In Advances in Cryptology - CRYPTO 2001, volume 2139 of Lecture Notes in Computer Science, pages 213–229. Springer-Verlag, 2001.

[25] Dan Boneh, Craig Gentry, Ben Lynn, and Hovav Shacham. Aggregate and Verifiably Encrypted Signatures from Bilinear Maps. In Advances in Cryptology - EUROCRYPT 2003, volume 2656 of Lecture Notes in Computer Science, pages416–432. Springer-Verlag, 2003.

[26] Dan Boneh, Eu-Jin Goh, and Kobbi Nissim. Evaluating 2-DNF Formulas on Ciphertexts. In Proceedings of 2th Theory of Cryptography Conference (TCC 2005),volume 3378 of Lecture Notes in Computer Science, pages 325–341. Springer-Verlag, 2005.

[27] Dan Boneh, Ben Lynn, and Hovav Shacham. Short Signatures from the Weilpairing. In Advances in Cryptology - ASIACRYPT 2001, volume 2248 of LectureNotes in Computer Science, pages 514–532, London, UK, 2001. Springer-Verlag.

[28] Dan Boneh and James Shaw. Collusion-Secure Fingerprinting.

[29]. Christian Collberg, Clark Thomborson, and Douglas Low. A Taxonomy of Obfuscating Transformations. Technical Report 148, July 1997.

[30]. Alexander W. Dent. Fundamental problems in provable security and cryptography .Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences, 364(1849):3215–3230, 2006.

[31]. Stanley Chow, Philip A. Eisen, Harold Johnson, and Paul C. van Oorschot. A white-box DES implementation for DRM applications. In Proceedings of the ACM Workshop on Security and Privacy in Digital Rights Management (DRM 2002),volume 2696 of Lecture Notes in Computer Science,pages 1–15. Springer, 2002