"SIMION STOILOW" INSTITUTE OF MATHEMATICS OF THE ROMANIAN ACADEMY

Cryptographic Protocols

Summary

Supervisor:
Ferucio Laurenţiu Ţiplea

Author:
George Teşeleanu

A thesis submitted in partial fulfillment for the
degree of Doctor of Philosophy

Bucharest, August 2021

Chapter 1

Preface

Throughout history, the main role of cryptography has been to keep sensible information private, even in the presence of an adversary that has control over the communication channel. Even though privacy remains central to cryptography, the field has expanded and it incorporates other goals, such as data integrity and authenticity, access control or electronic payments.

Once used only by the military, cryptography is now in widespread use and people benefit from it daily, even without know it. For example, when buying an item online a secure channel is used to process the transaction and implicitly to ensure the privacy of your credit card. Or, when communicating through messaging apps our private conversations are protected using end-to-end encryption. With such a growing area of applicability, is not surprising that modern cryptography intertwines concepts from mathematics, computer science, engineering and physics.

Although a remarkable science, cryptography is also an art and a puzzling game. We have to think as an attacker would, while defending the system against threats; we have to juggle between speed, usability and security; we have to twist known concepts in order to make them fit our scope; we have to design high level concepts, while keeping in mind the low level ones etc. Influenced by the plethora of concepts a cryptographer has to manage, in this work we touch on different areas of cryptography and we either take the role of the designer or of the attacker. By presenting both sides of the same coin, we wish that the reader will start to appreciate the beauty of this puzzling science and will begin to see the relationships that arise between seemingly different concepts.

1.1 Outline

We further present a brief synopsis of the seven main chapters contained in this work. One of the most difficult things about structuring this work was the interdependency of some of the chapters. We have tried to present the material in this thesis in a logical and natural order. Without further ado, here is the thesis outline.

Chapter 2 tackles secret key cryptography and is split into three parts. The first part analyses the security of the (affine) Hill cipher and their corresponding modes of operation. Definitions and background information are presented in Section 2.1.1. The core of the first part consists of Sections 2.1.2 and 2.1.3 that contain several key ranking functions and ciphertext only attacks. Experimental results are provided in Section 2.1.4 and some possible research directions are given in Section 2.1.5. The letter frequencies and the Vigenère attack used in Section 2.1.4 are given in Appendices A and B. Some possible methods for increasing the brute-force complexity for the Grain family of stream ciphers are presented in the second part of this chapter. We introduce notations and give a quick reminder of the Grain family technical specifications in Section 2.2.1. Section 2.2.2 describes generic attacks against the Grain ciphers. In Section 2.2.3 we provide the reader with a security analysis of IV padding schemes for Grain ciphers. We underline various interesting ideas as future work in Section 2.2.4. We recall Grain v1 in Appendix C, Grain-128 in Appendix D and Grain-128a in Appendix E. We do not recall the corresponding parameters of Grain v0, even though the results presented in this section still hold in that case. In Appendices F and G we provide test values for our proposed algorithms. The last part of this chapter studies the effect of using quasigroups isotopic to groups when designing SPNs. Hence, prerequisites are given in Section 2.3.1. An SPN generalization is introduced in Section 2.3.2 and its security is studied in Section 2.3.3.

In Chapter 3 we discuss several public key protocols and some of their applications. The first part introduces several hardness assumptions necessary for proving the protocols' security. Zero-knowledge protocols are studied in the second part of this chapter. Therefore, we recall zero-knowledge concepts in Section 3.2.1. Inspired by Maurer's Unified-Zero Knowledge construction, in Section 3.2.2 we introduce a Unified Generic Zero-Knowledge protocol and prove it secure. We provide the reader with various special cases of UGZK in Section 3.2.3. A hash variant of our core protocol is tackled in Section 3.2.4 together with its security analysis. As a possible application for UGZK, in Section 3.2.5 we describe a lightweight authentication protocol, discuss security and complexity aspects and present implementation trade-offs which arise from small variations of the proposed result. In Section 3.2.6 we underline future work proposals. The third part of this chapter contains a signature scheme inspired by Maurer's UZK paradigm. The necessary prerequisites are given in Section 3.3.1 and the exact details of the UDS signature

are provided in Section 3.3.2. An application for UDS is given in the fourth part of this chapter. More precisely, after introducing preliminaries in Section 3.4.1, we introduce a co-signing protocol built on the legally fair contract signing protocol of Ferradi *et. al* in Section 3.4.2. We discuss some related open problems in Section 3.4.3. Two public key encryption schemes are presented in the fifth part. In Section 3.5.1 we introduce definitions, security assumptions and schemes used throughout the section. First we introduce in Section 3.5.2 a slight modification of the generalized ElGamal encryption scheme, that will be used in a subsequent chapter. Then, inspired by the Joye-Libert PKE scheme and aiming at obtaining a relevant generalization, in Section 3.5.3 we propose a new scheme based on 2^k residues, prove it secure in the standard model and analyze its performance compared to other related cryptosystems. Future work is presented in Section 3.5.3.5 and in Appendix H we present some optimized decryption algorithms for our proposed scheme. The final part of this chapter provides the reader with an application of our Joye-Libert based scheme to biometric authentication. Thus, definitions and security requirements are presented in Section 3.6.1, while our proposed authentication protocol is described in Section 3.6.2.

Some useful results for understating the security of Cocks' identity based encryption and of certain variations of it are provided in Chapter 4. Basic notions and Cocks' scheme are presented in the first part of the chapter. The second part considers sets of the form $a + X = \{(a + x) \bmod n \mid x \in X\}$, where n is a prime or the product of two primes $n = pq$ and X is a subset of $\mathbb{Z}_n^*$ whose elements have some given Jacobi symbols modulo prime factors of n. The third part of the chapter points out two applications of the previously mentioned results. The first one provides the reader with a deep analysis of some distributions related to Cocks' IBE scheme and Galbraith's test, providing thus rigorous proofs for Galbraith's test. The second application discussed, relates to the computational indistinguishability of some distributions used for proving the security of certain variations of Cocks' IBE. We were able to prove statistical indistinguishability of those distributions without any hardness assumption. The chapter concludes with Section 4.4.

An unconventional method for backdooring cryptographic systems is studied in Chapter 5. The basic notions about kleptographic attacks are given in Section 5.1. The first part of this chapter deal with a threshold kleptographic attack that can be implemented in the generalized ElGamal signature. Thus, in Section 5.2.1 we describe a simplified attack on the generalized ElGamal signature and then extended it in Section 5.2.2. A series of signatures that support the implementation of our attack are provided in Section 5.2.3. Future work is presented in Section 5.2.4 and a two-party malicious signing protocol is presented in Appendix I. We provide a supplementary kleptographic mechanism in Appendix J. A method for infecting Maurer's UZK protocol is studied in the second part

of this chapter. In Sections 5.3.1 and 5.3.2 we present our new general kleptographic attacks and prove them secure. Instantiations of our attacks can be found in Section 5.3.3. Some possible research directions are given in Section 5.3.4. In the third part, we introduce a subscription based marketing model suitable for selling infected devices. Hence, some additional preliminaries are given in Section 5.4.1. Based on the ElGamal encryption algorithm, a series of kleptographic subscriptions that fit different scenarios are provided in Sections 5.4.2 to 5.4.4. We discuss some open problems in Section 5.4.5. Hash channels are tackled in the last part of the chapter. By adapting and improving Wu's mechanism we introduce new hash channels in Section 5.5.1. A series of experiments are conducted in Section 5.5.2, while several applications are provided in Section 5.5.3.

In Chapter 6 we study (pseudo)-random numbers generators. The first part of the chapter deals with Adobe Flash Player's[1] vulnerability in the pseudo-random number generator used for constant blinding. We introduce the necessary prerequisites in Section 6.1.1. The core of our seed recovering mechanism consists of Sections 6.1.2 and 6.1.3 and contains a series of algorithms for inverting a generalized version of the hash function used by the Flash Player. Experimental result are given in Section 6.1.4. Supplementary algorithms may be found in Appendix K. The second part contain an architecture that can be used to implement health tests for random numbers generator. Definitions and background information are presented in Section 6.2.1. Two classes of digital filters that amplify existing biases are described in Sections 6.2.2 and 6.2.3. Some possible applications are given in Section 6.2.4. In Section 6.2.5 we apply our proposed architecture to broken Bernoulli noise sources and present some experimental results. The theoretical model is provided in Section 6.2.6. Some finer measurements are provided in Section 6.2.7. In Section 6.2.8 we underline future work proposals.

Chapter 7 contains several protocols that fall in the category of recreational cryptography. Thus, in Section 7.1 we describe various schemes which aim at solving Yao's millionaires' problem and provide the reader with their corresponding security analyses. In Section 7.2 we present a set of protocols which act as solutions for comparing information without revealing it and discuss their security. In Section 7.3 we describe a public key cryptosystem constructed by means of an electrical scheme and tackle its security. In Appendix L we recall various physical cryptographic solutions which appeared in the literature, while in Appendix M we present a generic physical public key encryption scheme useful for introducing students to different properties of physical systems.

[1] versions 24.0.0.221 and earlier

1.2 Published Papers

[P1] Mariana Costiuc, Diana Maimuţ, and George Teşeleanu. Physical Cryptography. In *SECITC 2019*, volume 12001 of *Lecture Notes in Computer Science*, pages 156–171. Springer, 2019.

[P2] Diana Maimuţ and George Teşeleanu. Secretly Embedding Trapdoors into Contract Signing Protocols. In *SECITC 2017*, volume 10543 of *Lecture Notes in Computer Science*, pages 166–186. Springer, 2017.

[P3] Diana Maimuţ and George Teşeleanu. A Unified Security Perspective on Legally Fair Contract Signing Protocols. In *SECITC 2018*, volume 11359 of *Lecture Notes in Computer Science*, pages 477–491. Springer, 2018.

[P4] Diana Maimuţ and George Teşeleanu. New Configurations of Grain Ciphers: Security Against Slide Attacks. In *BalkanCrypt 2018*, Communications in Computer and Information Science. Springer, 2018.

[P5] Diana Maimuţ and George Teşeleanu. A Generic View on the Unified Zero-Knowledge Protocol and its Applications. In *WISTP 2019*, volume 12024 of *Lecture Notes in Computer Science*, pages 32–46. Springer, 2019.

[P6] Diana Maimuţ and George Teşeleanu. A New Generalisation of the Goldwasser-Micali Cryptosystem Based on the Gap 2^k-Residuosity Assumption. In *SECITC 2020*, Lecture Notes in Computer Science. Springer, 2020.

[P7] George Teşeleanu. Threshold Kleptographic Attacks on Discrete Logarithm Based Signatures. In *LatinCrypt 2017*, volume 11368 of *Lecture Notes in Computer Science*, pages 401–414. Springer, 2017.

[P8] George Teşeleanu. Random Number Generators Can Be Fooled to Behave Badly. In *ICICS 2018*, volume 11149 of *Lecture Notes in Computer Science*, pages 124–141. Springer, 2018.

[P9] George Teşeleanu. Unifying Kleptographic Attacks. In *NordSec 2018*, volume 11252 of *Lecture Notes in Computer Science*, pages 73–87. Springer, 2018.

[P10] George Teşeleanu. Managing Your Kleptographic Subscription Plan. In *C2SI 2019*, volume 11445 of *Lecture Notes in Computer Science*, pages 452–461. Springer, 2019.

[P11] George Teşeleanu. Reinterpreting and Improving the Cryptanalysis of the Flash Player PRNG. In *C2SI 2019*, volume 11445 of *Lecture Notes in Computer Science*, pages 92–104. Springer, 2019.

[P12] George Teşeleanu. Subliminal Hash Channels. In *A2C 2019*, volume 1133 of *Communications in Computer and Information Science*, pages 149–165. Springer, 2019.

[P13] George Teşeleanu. A Love Affair Between Bias Amplifiers and Broken Noise Sources. In *ICICS 2020*, Lecture Notes in Computer Science. Springer, 2020.

[P14] George Teşeleanu. Cracking Matrix Modes of Operation with Goodness-of-Fit Statistics. In *HistoCrypt 2020*, Linköping Electronic Conference Proceedings. Linköping University Electronic Press, 2020.

[P15] George Teşeleanu. Quasigroups and Substitution Permutation Networks: A Failed Experiment. *Cryptologia*, 2020.

[P16] Ferucio Laurentiu Tiplea, Sorin Iftene, George tese, and Anca-Maria Nica. On the Distribution of Quadratic Residues and Non-residues Modulo Composite Integers and Applications to Cryptography. *Appl. Math. Comput.*, 372, 2020.

[P17] Ferucio Laurenţiu Ţiplea, Sorin Iftene, George Teşeleanu, and Anca-Maria Nica. Security of Identity-Based Encryption Schemes from Quadratic Residues. In *SECITC 2016*, volume 10006 of *Lecture Notes in Computer Science*, pages 63–77, 2016.

Chapter 2

Secret Key Cryptography

The simplest and also the most common method for protecting the confidentiality of messages or authenticating a piece of information is to use a shared secret key between the sender and the receiver. This is called secret/symmetric key cryptography. In this scenario both participants use functions dependent on the same predetermined key. Usually, the shared key is randomly generated.

Symmetric key algorithm are assumed to maintain their security properties as long as adversaries cannot find the used key. This can mean three things: either the key is kept secure by the party using it or the key is large enough to avoid brute forcing it or the algorithm does not leak any information. In this chapter we will deal with two of the aforementioned aspects. More precisely, we will show how the (affine) Hill cipher and their corresponding modes of operation leak critical information through the ciphertext. Then we will describe a method for extending the life of Grain instantiations by increasing their corresponding brute force complexity. Finally, we provide the reader with equivalent instantiations of substitution permutation networks.

2.1 (Affine) Hill Cipher

Two classical ciphers based on linear algebra are the Hill cipher [144] and its affine version [145]. Both use invertible matrices over integers modulo a to encipher messages, where a is the size of the language alphabet $\mathcal{A}$. The first step of the encryption process is the encoding of each plaintext letter into a numerical equivalent. The simplest encoding is `"a"` $= 0$, `"b"` $= 1$ and so on. After encoding, the plaintext is divided into blocks of size k and, then, each block is multiplied with an invertible matrix of size k. In the affine case, a second matrix is added to the result. After each block is transformed, the result

is converted back into letters. To decipher messages, one must perform the above steps in reverse.

Although both ciphers are vulnerable to known plaintext attacks[1], efficient ciphertext only attacks have been developed only a decade ago [42] and only for the Hill cipher with small ks. Note that as k increases simple brute force attacks fail. For example, in the case of the Hill cipher with $a = 26$, we have around 2^{17} keys for $k = 2$, 2^{40} keys for $k = 3$ and 2^{73} keys for $k = 4$ [42]. According to [201, 43], given a and k the exact number of invertible matrices can be computed. Note that in the case of the affine Hill cipher the computational effort made to brute force the Hill cipher is multiplied with a^k.

In 2007, Bauer and Millward [42] introduced a ciphertext only attack for the Hill cipher[2], that was later improved in [266, 167, 178]. The attack was independently published by Khazaei and Ahmadi [154]. The main idea of these attacks is to do a brute force attack on the key rows, instead of the whole matrix, and then recover the decryption matrix.

In [157], Kiele suggests the usage of block-chaining procedures to complicate the algebraic cryptanalytic techniques developed for the Hill cipher. We will show in this section how to adapt the attacks described in [42, 266, 154] to different modes of operation (not only the block-chaining one) for both the Hill cipher and its affine version. Note that some modes do not require the key to be invertible, thus the attack presented in [167] does not work for all Hill based modes. For uniformity, we will only extend Yum and Lee's attack and leave as future work the extension of [167] to modes requiring invertible matrices. We stress that out of the three attacks [42, 266, 154] Yum and Lee's attack has the best performance to message recovery ratio.

Another paper that motivated this study is [41]. The authors of [41] conjecture that the fourth cryptogram of the Kryptos sculpture [9] is either encrypted using the affine Hill cipher or some other sort of cipher mode of operation. We provide the reader with a preliminary study of these conjectures. To prove or disprove these conjectures, one has to find a way to adapt all the presented ciphertext attacks to the secret encoding versions of the (affine) Hill cipher and their corresponding modes of operation. Various partial answers for the secret encoding Hill cipher are provided in [266].

[1] *i.e.* after a number of known messages are encrypted, one can easily recover the encryption key(s) if he has access to the corresponding ciphertexts.

[2] Bauer and Millward's attack for $k = 3$ was previously and independently described online by Wutka [257].

2.2 Grain Cipher Family

The Grain family of stream ciphers consists of four instantiations Grain v0 [140], Grain v1 [141], Grain-128 [139] and Grain-128a [211]. Grain v1 is a finalist of the hardware-based eSTREAM portfolio [4], a competition for choosing both hardware and software secure and efficient stream ciphers.

The design of the Grain family of ciphers includes an LFSR. The loading of the LFSR consists of an initialization vector (IV) and a certain string of bits P whose lengths and structures depend on the cipher's version. Following the terminology used in [39], we consider the IV as being padded with P. Thus, throughout this section, we use the term *padding* to denote P. Note that Grain v1 and Grain-128 make use of *periodic* IV padding and Grain-128a uses *aperiodic* IV padding.

A series of attacks against the Grain family padding techniques appeared in the literature [38, 39, 64, 162] during the last decade. In the light of these attacks, we propose the first security analysis[3] of generic IV padding schemes for Grain ciphers in the *periodic* as well as the *aperiodic* cases.

In this context, the concerns that arise are closely related to the security impact of various parameters of the padding, such as the position and structure of the padding block. Moreover, we consider both *compact* and *fragmented* padding blocks in our study. We refer to the original padding schemes of the Grain ciphers as being compact (*i.e.* a single padding block is used). We denote as fragmented padding the division of the padding block into smaller blocks of equal length[4].

By examining the structure of the padding and analyzing its compact and especially fragmented versions, we actually study the idea of extending the key's life. The latter could be achieved by introducing a variable padding according to suitable constraints. Hence, the general question that arises is the following: *what is to be loaded in the LFSRs of Grain ciphers in order to obtain secure settings?*. Note that our study is preliminary, taking into account only slide attacks. We consider other types of attacks as future work.

We stress that finding better attacks than the ones already presented in the literature is outside the scope of this section, as our main goal is to establish sound personalized versions of the Grain cipher. Hence, our work does not have any immediate implication towards breaking any cipher of the Grain family. Nevertheless, our observations become meaningful either in the lightweight cryptography scenario or in the case of an enhanced security context (e.g. secure government applications).

[3] against slide attacks

[4] we consider these smaller blocks as being spread among the linear feedback register's data

Lightweight cryptography lies at the crossroad between cryptography, computer science and electrical engineering. Thus, trade-offs between performance, security and cost must be considered. Given such constraints and the fact that embedded devices operate in hostile environments, there is an increasing need for new and varied security solutions, mainly constructed in view of the current ubiquitous computing tendency. As the Grain family lies precisely within the lightweight primitives' category, we believe that the study presented in the current section is of interest for the industry and, especially, government organizations.

When dealing with security devices for which the transmission and processing of the IV is neither so costly nor hard to handle (e.g. the corresponding communication protocols easily allow the transmission), shrinking the padding up to complete removal might be considered. More precisely, we suggest the use of a longer IV in such a context in order to increase security. Moreover, many Grain-type configurations could be obtained if our proposed padding schemes are used. Such configurations could be considered as personalizations of the main algorithm and, if the associated parameters are kept secret, the key's life can be extended.

2.3 Quasigroup Substitution Permutation Networks

In its most basic form, differential cryptanalysis [55] predicts how certain changes in the plaintext propagate through a cipher. When considering an ideally randomizing cipher, the probability of predicting these changes is $1/2^n$, where n is the number of input bits. Thus, in the ideal case, it is infeasible for an attacker to use these predictions when n is, for example, 128. Unfortunately, designers use theoretical estimates based on certain assumptions that do not always hold in practice. Hence, differential cryptanalysis is often the most effective tool against symmetric key cryptographic algorithms [188].

Quasigroups are group-like structures that, unlike groups, are not required to be associative and to possess an identity element. The usage of quasigroups as building blocks for cryptographic primitives is not very common. Regardless of that, various such cryptosystems can be found in the literature [164, 117, 116, 35, 90, 160].

In this paper we introduce a straightforward generalization of substitution-permutation networks (SPN) and study its security. By replacing the group operation $\star$ between keys and (intermediary) plaintexts with a quasigroup operation $\otimes$ we aimed at extending the usage of quasigroups. Unfortunately, by means of differential cryptanalysis we prove that in the case of quasigroups isotopic with a group[5] the problem of breaking an SPN using

[5]Note that this is the most popular method for generating quasigroups.

$\otimes$ reduces to breaking an SPN using $\star$ and a substitution box (s-box) different from the initial one. Thus, if we initialize the SPN with a random secret s-box, replacing $\star$ with $\otimes$ brings no extra security[6]. In the case of static s-boxes, changing $\star$ with $\otimes$ might even affect the SPN's security.

Although the design presented in this paper is not a successful one, we think that its usefulness is twofold. ① Most scientific reports and papers published appear as sanitized accounts[7] and this gives people a distorted view of scientific research [179, 146, 235, 255]. This leads to a view that implies that failure, serendipity and unexpected results are not a normal part of science [146, 220]. Hence, this report provides students with an indication of the real processes of experimentation. ② Negative results and false directions are rarely reported [146, 248] and, thus, people are bound to repeat the same mistakes. By presenting our results, we hope to provide an opportunity for others to learn where this path leads. Hence, preventing them to make the same mistakes[8].

[6] *i.e.* we simply obtain another instantiation of the SPN

[7] Authors present their results as if they achieved them in a straightforward manner and not through a messy process.

[8] In [236], the author advises people to write down their mistakes so that they avoid making them again in the future.

Chapter 3

Public Key Cryptography

One of the problems associated with secret key cryptography is key distribution. An elegant solution for this inconvenience is provided by public/asymmetric key cryptography. In an asymmetric setting a participant possesses a pair of keys: a public key and an associated secret key. The public key is known by everybody and is bound to the participant's identity. Using the public key, any party can send messages to the owner, while he can read them using his secret key. Compared to secret key systems[1], in the public key setting there is no need for a secure channel in order to disseminate the participants' public keys. Another attractive property of asymmetric algorithms is that their security can, in most cases, be reduced to difficult computational problems.

Although initially developed for solving the key distribution problem, public key cryptography has expanded and incorporates other application such as encryption schemes, digital signatures or zero-knowledge protocols. In this chapter we develop various examples for the previously mentioned applications and relate their security to some well known hardness assumptions.

3.1 Zero-Knowledge Protocols

The main issue addressed by ZKP is represented by *identification schemes* (entity authentication). Thus, building on the most important goal that a ZKP can achieve one may find elegant solutions to various problems that arise in different areas: digital cash, auctioning, IoT, password authentication and so on.

A typical zero knowledge protocol involves a prover *Peggy* which possesses a piece of secret information x associated with her identity and a verifier $Victor$ whose job is to

[1] where a secure channel is needed to distribute the communication key to the participants

check that *Peggy* really owns x. Two classical examples of such protocols (proposed for smartcards) are the Schnorr protocol [219] and the Guillou-Quisquater protocol [131]. Working in an abstract framework, Maurer shows in [176] that the previously mentioned protocols are actually instantiations of the same one.

Building on Maurer's result, we considered of great interest providing the reader with a generalized perspective of the Unified Zero-Knowledge (UZK) protocol as well as a hash variant of it. An important consequence of our generic approach is the unification of Maurer's [176], Feige-Fiat-Shamir's [103] and Chaum-Everste-Van De Graaf's [68] protocols. Moreover, a special case of our protocol's hash version is the *h-variant* of the Fiat-Shamir scheme [108, 115].

As the IoT paradigm arised, lightweight devices[2] became more and more popular. Due to the open and distributed nature of the IoT, proper security is needed for the entire network to operate accordingly. Now let us consider the case of online wireless sensor networks (WSNs). The lightweight nature of sensor nodes heavily restricts cryptographic operations. Thus, the need for specific cryptographic solutions becomes obvious. The Fiat-Shamir-like distributed authentication protocol presented in [78] represents such an example. Based on this previous construction we propose a unified generic zero-knowledge protocol. Just as the result described in [78], our protocol can be applied for securing WSNs and, more generally, IoT-related solutions. Nonetheless, our construction offers flexibility when choosing the assumptions on which its security relies. A secondary feature of our scheme is the possibility of reusing existing certificates when implementing the distributed authentication protocol.

3.2 Signature Schemes

In 1986, Fiat and Shamir [108] described an important technique for deriving digital signatures from zero-knowledge protocols. At its core, the signer uses a hash function in order to create a virtual verifier. This technique was later used by Schnorr to transform his ZKP into a signature. The resulting signature was proven secure in ROM by Pointcheval and Stern [208, 209].

The UZK framework incorporates the Schnorr ZKP. Hence, it is natural to apply the Fiat-Shamir transform to UZK and thus extend Schnorr's signature. We will later use the resulting signature as the main building block for the contract signing protocol we propose in Section 3.3.2.

[2] low-cost devices with limited resources, be it computational or physical

3.3 Legally Fair Contract Signing Protocols

Various contract signing schemes which fall into three different design categories were proposed during the last decades: *gradual release* [122, 207, 111, 127], *optimistic* [29, 63, 181] and *concurrent* [71] or *legally fair* [104] models. A typical co-signing protocol involves two (mutually distrustful) signing partners, *Alice* and *Bob* wishing to compute a common function on their private inputs.

Compared to older paradigms like *gradual release* or optimistic models, concurrent signatures or legally fair protocols do not rely on trusted third parties and do not require too much interaction between co-signers. As such features seem much more attractive for users, we further consider legally fair co-signing protocols (rather than older solutions) in our paper.

Inspired by Maurer's generic perspective, we considered of great interest extending the unification paradigm to contract signing protocols. Therefore, we construct our main idea considering the stringent issue of scheme compatibility which characterizes communication systems. Typical examples are the cases of certificates in a public key infrastructure and the general issue of upgrading the version of a system. Thus, working in a general framework may reduce implementation errors and save application development (and maintenance) time.

In this section we present a unified class of legally fair co-signing protocols without keystones and prove its security. To be more precise, we propose a class of UDS (see Section 3.2) based co-signing protocols that maintains the valuable properties[3] of the scheme presented in [104].

3.4 A Generalisation of the Goldwasser-Micali Cryptosystem

The scope of a public key encryption scheme is to provide confidentiality, while allowing users to distribute their public keys widely and openly. Therefore, only a user in possession of the secret key can decrypt messages, while anyone in possession of the corresponding public key can encrypt data to send it to this one user. Usually, the design of PKEs is typically based on computationally intractable problems in number theory.

The authors of [149] introduced a PKE scheme[4] representing a rather natural extension of the Goldwasser-Micali (GM) [123, 124] cryptosystem, the first probabilistic encryption

[3] legal fairness without keystones, guaranteed output delivery
[4] reconsidered in [51]

scheme. The Goldwasser-Micali cryptosystem achieves ciphertext indistinguishability under the *Quadratic Residuosity* (QR) assumption. Despite being simple and stylish, this scheme is quite uneconomical in terms of bandwidth[5]. Various attempts of generalizing the Goldwasser-Micali scheme were proposed in the literature in order to address the previously mentioned issue. The Joye-Libert scheme can be considered a follow-up of the cryptosystems proposed in [190] and [79] and efficiently supports the encryption of larger messages.

Inspired by the Joye-Libert scheme, we propose a new public key cryptosystem, analyze its security and provide the reader with an implementation and performance discussion. We construct our scheme based on 2^k-th power residue symbols. Our generalization of the Joye-Libert cryptosystem makes use of two important parameters when it comes to the encryption and decryption functions: the number of bits of a message and the number of distinct primes of a public modulus n. Thus, our proposal not only supports the encryption of larger messages (as in the Joye-Libert variant), but also operates on *a variable number of large primes* (instead of two in the Joye-Libert case). Both these parameters can be chosen depending on the desired security application.

Our scheme can be viewed as a flexible solution characterized by the ability of making adequate trade-offs between encryption speed and ciphertext expansion in a given context.

3.5 Biometric Authentication

In biometric authentication protocols, when a user identifies himself using his biometric characteristics (captured by a sensor), the collected data will vary. Thus, traditional cryptographic approaches (such as storing a hash value) are not suitable in this case, since they are not error tolerant. As a result, biometric-based protocols must be constructed in a special way and, moreover, the system must protect the sensitivity and privacy of a user's biometric characteristics. Such a protocol is proposed in [61]. Its core is the Goldwasser-Micali encryption scheme. Thus, a natural extension of the protocol in [61] can be obtained using our generalization of the Joye-Libert scheme. Thus, we describe such a biometric authentication protocol and discuss its security.

[5] $k \cdot \log_2 n$ bits are needed to encrypt a k-bit message, where n is an RSA modulus as described in [123, 124]

Chapter 4

Identity Based Cryptography

Identity-based cryptography was proposed in 1984 by Adi Shamir [222] who formulated its basic principles and provided an identity-based signature scheme. In 2000, Sakai, Ohgishi and Kasahara [216] have proposed an identity-based key agreement scheme, and one year later, Cocks [77] and Boneh and Franklin [59] have proposed the first identity-based encryption schemes. Cocks' scheme is based on quadratic residues, while Boneh and Franklin's scheme is based on bilinear maps. Since then, some other IBE schemes based on quadratic residues have been proposed [60, 147, 31, 76, 99, 100, 148], although some of them are not secure (see [246] for details).

Cocks'scheme encrypts messages bit by bit and each encrypted bit is a pair of two integers. The decryption consists of computing the Jacobi symbol of one of the two integers in each pair. Although Cocks' IBE scheme is efficient only for small messages, it is very elegant and *per se* revolutionary. The scheme attracted the interest of many researchers [60, 31, 76, 148]. A careful analysis of [77, 60, 31, 76, 148] shows that integers of the form $a+r$, where a is an integer and r is a quadratic residue (modulo a given integer n), play an important role in these papers. Particularly, it turns out to be important to know the distribution of quadratic residues among all integers of the form $a + r$. A study in this direction was initiated by Perron [206] for the case of a prime modulus p. However, most applications of quadratic residues to cryptography require the use of a composite modulus $n = pq$. We are thus faced with the need to extend Perron's results to composite moduli. The same was advocated in [31] (see Section 2.3 in [31]). Here, the authors avoided the extension of Perron's results to composite moduli with the price of weaker indistinguishability results (this will be fully discussed in Section 4.3.1).

The contributions presented in this chapter are structured into two parts. The first part (Section 4.2) considers sets of the form $a + X = \{(a + x) \bmod n \mid x \in X\}$, where n is a prime or the product of two primes $n = pq$, and X is a subset of $\mathbb{Z}_n^*$ whose elements

have some given Jacobi symbols modulo prime factors of n. For instance, X may be the set of all integers in $\mathbb{Z}_n^*$ whose Jacobi symbol modulo p is 1 and Jacobi symbol modulo q is -1 (assuming $n = pq$); we say that the *Jacobi pattern* of the integers in X, in this case, is "$+-$". Then, given a set $a + X$, we look for the distribution of the quadratic residues, quadratic non-residues, etc., in $a + X$. We develop complete results for all the Jacobi patterns of length one, $+$ and - (this corresponds to quadratic residues and non-residues modulo a prime) and Jacobi patterns of length two, $++$, $--$, $+-$, and $-+$ (this corresponds to moduli that are product of two distinct primes).

The results presented in Section 4.2 are a major extension of Perron's findings [206], where only the distribution of quadratic residues in the set $a + QR_p$, where p is a prime, has been considered. Related studies to the one conducted in Section 4.3 were performed in [86, 87, 204, 151], where the problem is to calculate the probability that

$$J_p(a)J_p(a+1)\cdots J_p(a+\ell-1)$$

meets some Jacobi residuosity modulo p, a priori given, for the ℓ elements, when a is chosen uniformly at random from $a \in \mathbb{Z}_p^*$ (p is a prime). Thus, in [204] it was shown that the number of integers a with the property above is in between $p/2^\ell - \epsilon$ and $p/2^\ell + \epsilon$, where $\epsilon = \ell(3 + \sqrt{p})$. Dividing these two bounds by p we obtain the probability that an integer a induces a given Jacobi residuosity for the ℓ consecutive elements. A direct extension of this result to the case of RSA moduli may lead to "much larger bound" than ϵ. In [151], an extension to RSA moduli has been proposed by generalizing [87]. Thus, it was shown that the number of integers a with the property above is $n/2^\ell + \mathcal{O}(\sqrt{n}\cdot\log^2 n)$, where n is an RSA modulus and $1 \leqslant \ell \leqslant (1/2 - \delta)\log_2 n$, for some $0 < \delta < 1/2$.

The results developed in this chapter are different than those mentioned above for at least two main reasons. First of all, we have developed exact and not approximate formulas for the number of integers with a given Jacobi pattern in sets $a + X$. Secondly, the increment factor is arbitrary in all our studies, while it is one in all the results mentioned above.

The second part of the chapter's contribution (Section 4.3) points out some applications of the results developed in the first part (Section 4.2). There are two main applications discussed here. The first one relates to Galbraith's test for Cocks' IBE scheme. This test was briefly described in several papers such us [58, 31, 148], except that some claims were not rigorously formulated and/or proved. Based on the results developed in Section 4.2, we were able to make a deep analysis of some distributions related to Cocks' IBE scheme and Galbraith's test, providing thus rigorous proofs for Galbraith's test.

The second application discussed in Section 4.3 relates to the computational indistinguishability of some distributions in [31, 76, 148], under the quadratic residuosity assumption. Based on the results developed in Section 4.2, we were able to prove statistical indistinguishability of those distributions (without any assumption).

In addition to the applications already mentioned in Section 4.3, we believe that our study in Section 4.2 is important also because it contributes to a better understanding of the structure of $\mathbb{Z}_n^*$ with respect to Jacobi patterns of length at most two, which are frequently employed in cryptography.

Chapter 5

Kleptographic Attacks

As more and more countries require individuals and providers to hand over passwords and decryption keys [22], we might observe an increase in the usage of *subliminal channels*. Subliminal channels are secondary channels of communication hidden inside a potentially compromised communication channel. The concept was introduced by Simmons [226, 227, 228] as a solution to the *prisoners' problem*. In the prisoners' problem *Alice* and *Bob* are incarcerated and wish to communicate confidentially and undetected by their guard *Walter* who imposes to read all their communication. Note that *Alice* and *Bob* can exchange a secret key before being incarcerated.

Classical security models assume that the cryptographic algorithms found in a device are correctly implemented and according to technical specifications. Unfortunately, in the real world, users have little control over the design criteria or the implementation of a security module. When using a hardware device, for example a smartcard, the user implicitly assumes an honest manufacturer that builds devices according to the provided specifications. The idea of a malicious manufacturer that tampers with the device or embeds a backdoor in an implementation was first suggested by Young and Yung [261, 262]. As proof of concept, they developed secretly embedded trapdoor with universal protection (SETUP) attacks. These attacks combine subliminal channels and public key cryptography to leak a user's private key or a message. Young and Yung assumed a black-box environment[1], while mentioning the existence of other scenarios. The input and output distributions of a device with SETUP should not be distinguishable from the regular distribution. However, if the device is reverse engineered, the deployed mechanism may be detectable.

[1] A black-box is a device, process or system, whose inputs and outputs are known, but its internal structure or working is not known or accessible to the user (*e.g.* tamper proof devices).

Although SETUP attacks were considered far-fetched by some cryptographers, recent events [36, 205] suggest otherwise. As a consequence, this research area seems to have been revived [32, 45, 94, 214]. In [47], SETUP attacks implemented in symmetric encryption schemes are referred to as *algorithmic substitution attacks* (ASA). The authors of [47] point out that the sheer complexity of open-source software (*e.g.* OpenSSL) and the small number of experts who review them make ASAs plausible not only in the black-box model. ASAs in the symmetric setting are further studied in [45, 88] and, in the case of hash functions, in [28]. A link between *secret-key steganography* and ASAs can be found in [53].

A practical example of leaking user keys is the Dual-EC generator, a cryptographically secure pseudorandom number generator standardized by NIST. Internal NSA documents leaked by Edward Snowden [36, 205] indicated a backdoor embedded into the Dual-EC generator. As pointed out in [54], using the Dual-EC generator facilitates a third party to recover a user's private key. Such an attack is a natural application of Young and Yung's work. Some real world SETUP attack examples may be found in [70, 69]. Building on the earlier work of [250] and influenced by the Dual-EC incident, [94, 89] provide the readers with a formal treatment of backdoored pseudorandom generators (PRNG).

A more general model entitled *subversion attacks* is considered in [32]. This model includes SETUP attacks and ASAs, but generic malware and virus attacks are also included. The authors provide subversion resilient signature schemes in the proposed model. Their work is further extended in [214, 215], where subversion resistant solutions for one-way functions, signature schemes and PRNGs are provided. In [214], the authors point out that the model from [32] assumes the system parameters are honestly generated (but this is not always the case). In the discrete logarithm case, examples of algorithms for generating trapdoored prime numbers may be found in [126, 110].

A different method for protecting users from subversion attacks are *cryptographic reverse firewalls* (RF). RFs represent external trusted devices that sanitize the outputs of infected machines. The concept was introduced in [184, 96]. A reverse firewall for signature schemes is provided in [32].

5.1 Threshold Kleptographic Attacks

In this section, we extend the SETUP attacks of Young and Yung on digital signatures. We introduce the first SETUP mechanism that leaks a user's secret key, only if ℓ out of n malicious parties decide to do this. We assume that the signature schemes are

implemented in a black-box equipped with a volatile memory, erased whenever someone tampers with it.

In the following we give a few examples where a threshold kleptographic signature may be useful.

Since digitally signed documents are just as binding as signatures on paper, if a recipient receives a document signed by A he will act according to A's instructions. Finding A's private key, can aid a law enforcement agency into collecting additional informations about A and his entourage. In order to protect citizens from abuse, a warrant must be issued by a legal commission before starting surveillance. To aid the commission and to prevent abuse, the manufacturer of A's device can implement an ℓ out of n threshold SETUP mechanism. Thus, A's key can be recovered only if there is a quorum in favor of issuing the warrant.

Digital currencies (*e.g.* Bitcoin) have become a popular alternative to physical currencies. Transactions between users are based on digital signatures. When a transaction is conducted, the recipient's public key is linked to the transfered money. Only the owner of the secret key can now spend the money. To protect his secret keys, a user can choose to store them in a tamper proof device, called a hardware wallet. Let's assume that a group of malicious entities manages to infect some hardware wallets and they implement an ℓ out of n threshold SETUP mechanism. When ℓ members decide, they can transfer the money from the infected wallets without the owner's knowledge. If $\ell - 1$ parties are arrested, the mechanism remains undetectable as long as the devices are not reverse engineered.

In accordance with the original works, we prove that the threshold SETUP mechanisms are polynomially indistinguishable from regular signatures. Depending on the infected signature, we obtain security in the standard or random oracle model (ROM). To do so, we make use of a public key encryption scheme (introduced in Section 3.5.2) and Shamir's secret sharing scheme [221]. ROM security proofs are easily deduced from the standard model security proofs provided in this section. Thus, are omitted.

5.2 Unifying Framework

The initial model proposed by Young and Yung is the black-box model. For our intended purposes this model suffices, since the zero-knowledge protocols we attack were designed for smartcards. An important property is that infected smartcards should have inputs and outputs indistinguishable from regular smartcards. However, if the smartcard is reverse engineered, the deployed mechanism may be detectable.

There are two methods to embed backdoors into a system: either you generate special public parameters (SPP) or you infect the random numbers (IRN) used by the system. In the case of discrete logarithm based systems, SPP and IRN were studied in [261, 262, 263, 264, 126, 110]. We only found SPP [83, 261, 262, 265, 264] and not IRN in the case of factorization based systems.

Using the same level of abstraction as in [176], we show how an attacker (called *Mallory*) can insert a backdoor into the UZK protocol and extract *Peggy*'s secret. When instantiated, this attack provides new insight into SETUP attacks. In particular, we provide the first IRN attack on a factoring based system and the first attack on systems based on e^{th}-root representations. We also provide the reader with new instantiations of Maurer's unified protocol: the Girault protocol, a new proof of knowledge for discrete logarithm representation in $\mathbb{Z}_n^*$ and a proof of knowledge of an e^{th}-root representation.

The second SETUP attack we introduce is a generalization of Young and Yung's work. When instantiated with the Schnorr protocol, we obtain their results. We also provide other examples not mentioned by Young and Yung.

5.3 Kleptographic Subscription Plans

One of the classical business models for kleptographic attacks is the following: a client[2] C pays up front a manufacturer M, whom will later implement a certain backdoor in a tamper proof device and deliver that device to a victim. This model puts the manufacturer at an advantage, because he can charge the customer and not implement the requested backdoor. Since this transaction is illegal, the customer can not file a complain and legally retrieve his money. Thus, this might scare off some of the potential clients.

Another classical model is the following: a client pays the manufacturer half the money up front and the rest after checking the correctness of the backdoor. If the manufacturer does not take certain precautions, then the client is at an advantage. For example, C checks the correctness of the backdoor, but fails to pay the second installment. This can be easily avoided if a backdoor deactivation method is put in place by M[3]. A possible deactivation strategy is for M to send D a special input that instructs the device to erase all incriminating evidence. A similar approach is used in [88, 109] to trigger backdoors.

Both classical approaches have an inherent risk for the manufacturer: the client can easily prove that M backdoored D either by decrypting all the messages send through

[2] by definition a malicious entity

[3] As in the previous model, the transaction is illegal and thus, M can not take legal action against C.

that device or by revealing the private keys stored in D. Thus, to make the risk worth while the manufacturer must charge C a high embedding fee. This will certainly scare away certain resource constrained clients (*e.g.* small businesses that do not have the resources of a large corporation). To address this issue, we introduce a subscription based model suitable for the ElGamal encryption algorithm.

Our model draws inspiration from the subscription services offered by companies like Netflix [6], Amazon [7] and HBO [8]. These companies give access to streaming content in exchange for a monthly pay. In our case, a client pays for a backdoor that gives him access to a limited number of private messages. Subsequently, the client has to renew his subscription. This balances the risk and reward factors for the manufacturer[4] and, in consequence, M can lower embedding fees. A risk still remains: no guarantees of output delivery for the clients. But, this is minimum in a subscription based model because the goal of the manufacturer is to keep clients satisfied, so they further renew their subscription[5].

Compared to the classical models, our proposed model has a different issue that needs to be tackled. Clients want access to their services as soon as they pay. But, illegal transactions mostly use cryptocurrencies [75] and the average confirmation time for this type of transactions is large in some cases (*e.g.* for Bitcoin, it takes on average an hour per transaction [2]). Thus, to give the manufacturer sufficient time for deactivating the backdoor[6] if the transaction is not valid, we employ a mechanism similar to time-lock puzzles [213] .

Note that generic kleptographic countermeasures [214, 215, 135] can protect tamper proof device's users against our proposed mechanisms. Unfortunately, unless users do not explicitly require the implementation of these defences, a manufacturer is not obliged to deploy them. Thus, M is free to implement any kleptographic mechanism.

5.4 Hash Channels

Most subliminal channels or SETUP attacks use random numbers to convey information undetected. In consequence, all the proposed countermeasures focus on sanitizing the random numbers used by a system. In the case of digital signatures, a different but laborious method for inserting a subliminal channel in a system is presented in [256]. Instead of using random numbers as information carriers, *Alice* uses the hash of the message to convey the message for *Bob*. In order to achieve this, *Alice* makes small

[4] M is exposed only for a limited period of time
[5] Cheating a client will only bring M a small amount of revenue.
[6] by means of special triggers

changes to the message until the hash has the desired properties. Note that the method presented in [256] bypasses all the countermeasures mentioned so far.

This section studies a generic method that allows the prisoners to communicate through the subliminal-free signatures found in [214, 215, 73, 135, 32, 57]. To achieve our goal we work in a scenario where all messages are time-stamped before signing. Note that we do not break any of the assumptions made by the subversion-free proposals. This work is motivated by the fact that most end-users to do not verify the claims made by manufacturers[7]. Moreover, users often do not know which should be the outputs of a device [163]. A notable incident in which users where not aware of the correct outputs and trusted the developers is the Debian incident [50].

[7]Manufacturers might implement subversion-free signatures just for marketing purposes, while still backdooring some of the devices produced.

Chapter 6

(Pseudo-)Random Number Generators

One of the most essential building blocks of cryptography are random numbers generators. In particular, for ensuring privacy or authenticity is vital that cryptographic keys are randomly generated. Additionally, most cryptographic algorithms are randomized.

Generating random numbers by means of physical processes is usually time consuming and expensive, thus in practice most applications use pseudo-random numbers generators. Such a generator is a deterministic algorithm that takes as input a small random seed and expands it into a much longer sequence of bits. Not all PRNGs are suitable for cryptographic application. One such example is the generator used by Adobe Flash Player. Some of the basic PRNG security requirements are: not to be able to distinguish it from a real RNG and not to be able to recover its internal state from its output. We describe a seed recovering algorithm for the Flash Player PRNG in the first part of this chapter.

A popular method for generating cryptographic keys or other random inputs is to have an entropy pool that accumulates data from a physical noise source and a PRNG that periodically reseeds from the pool and outputs data at a constant rate. To ensure proper operation, before adding data to the entropy pool some lightweight tests are applied to it. In the second part of this chapter we study a possible architecture for adding data to the pool. Therefore, we provide the reader with experimental results and the theoretical framework for our proposed architecture.

6.1 Flash Player PRNG

JIT compilers (*e.g.* JavaScript and ActionScript) translate source code or bytecode into machine code at runtime for faster execution. Due to the fact that the purpose of JIT compilers is to produce executable data, they are normally exempt from data execution prevention (DEP[1]). Thus, a vulnerability in a JIT compiler might lead to an exploit undetectable by DEP. One such attack, called JIT spraying, was proposed in [56]. By coercing the ActionScript JIT engine, Blazakis shows how to write shellcode into the executable memory and thus, bypass DEP. The key insight is that the JIT compiler is predictable and must copy some constants to the executable page. Hence, these constants can encode small instructions and then control flow to the next constant's location.

To defend against JIT spraying attacks, Adobe employs a technique called *constant blinding*. This method prevents an attacker from loading his instructions into constants and thus, blocks the delivery of his malicious script. The idea behind constant blinding is to avoid storing constants in memory in their original form. Instead, they are first XORed with some randomly generated secret cookie and then stored inside the memory. If the secret cookie is generated by means of a weak PRNG[2], the attacker regains his ability to inject malicious instructions.

Instead of using an already proven secure PRNG, the Flash Player designers tried to implement their own PRNG. Unfortunately, in [253, 1] it is shown that the design of the generator is flawed. In [1] a brute force attack is implemented, while in [253] a refined brute force attack is presented. These results have been reported to Adobe under the code CVE-2017-3000 [21] and the vulnerability has been patched in version 25.0.0.127.

In this section, we refine the attack presented in [253] from a time complexity of $\mathcal{O}(2^{21})$ to one of $\mathcal{O}(2^{11})$. We also show that no matter the parameters used by the PRNG, the flaw remains. More precisely we show that for any parameters the worst brute force attack takes $\mathcal{O}(2^{21})$ operations. In [253] the authors do not present the full algorithm for reversing the PRNG, while in [1] we found the full algorithm, but it was not optimized. For completeness, in Appendix K we also present an optimized version of the full algorithm. Note that in this section we only focus on the Flash Player PRNG. For more details about JIT spraying attacks and constant blinding we refer the reader to [33, 56, 212, 253].

[1] The DEP mechanism performs additional checks on memory to help prevent malicious code from running on a system.

[2] *i.e.*, the seed used to generate the cookie can be recovered in reasonable time

6.2 Bias Amplifiers

In [264] the authors propose an interesting mechanism that blurs the line between what constitutes a Trojan horse and what does not. To detect their mechanism, a program needs to somehow differentiate between a naturally unstable random number generator (RNG) and artificially unstable one (obtained by means of certain mathematical transformations). To our knowledge, [264] is the only previous work that discuses this topic.

More precisely, in [264] a digital filter is described. Usually, digital filters are applied to RNGs to correct biases[3], but this filter has an opposite purpose. When applied to a stream of unbiased bits the filter is benign. On the other hand, if applied to a stream of biased bits the filter amplifies their bias. Thereby, making the RNG worse.

In this section we extend the filter from [264][4], provide a new class of filters and discuss some new possible applications. When designing bias amplifiers, a couple of rules must be respected. The first one states that if the input bits are unbiased or have a maximum bias (*i.e.* the probability of obtaining 1 is either 0 or 1) the filter must maintain the original bias. For unbiased bits this rule keeps the amplifiers transparent to a user, as long as the noise source functions according to the original design parameters. For maximum bias the rule is a functional one. Since the RNG is already totally broken, changing the bias does not make sense (from a designing point of view). The second rule states that the filter should amplify the bias in the direction that it already is. This rule helps the designer amplify the bias in an easier manner.

The main application we propose for these filters is RNG testing (*e.g.*, boosting health tests implemented in a RNG). Recent standards [158, 249] require a RNG to detect failures and one such method for early detection can be to apply an amplifier and then do some lightweight testing[5]. Based on the results obtained in Sections 6.2.2 and 6.2.3, we introduce a generic architecture for implementing health tests in Section 6.2.4.1. More precisely, using a lightweight test on the amplified bits the architecture can detect deviations from the uniform distribution. To validate our architecture, we first run a series of experiments on RNGs that generate uniformly independent and identically distributed bits. We also show that our architecture can detect deviation from the initial parameters of the u.i.i.d. source. In Section 6.2.5 we extend the preliminary results to noise sources that have a Bernoulli distribution and show that the architecture can detect, starting from the design phase, badly broken sources. To support our results we

[3] They are called randomness extractors [95].

[4] The filter presented in [264] corresponds to the greedy amplifier with parameter $n = 3$ described in Section 6.2.2.

[5] for example the tests described in [134]

develop a theoretical model and provide the reader with simulations based on our model. Note that our theoretical model also explains why our architecture can detect deviation from the initial parameters

Due to recent events [36, 205, 50, 69] RNGs have been under a lot of scrutiny. Thus, wondering what kind of mechanisms can be implemented by a malicious third party in order to weaken or destabilize a system becomes natural. Amplifying filters provide a novel example of how one can achieve this. Based on the failure detection mechanisms proposed in Section 6.2.4.1, we show, for example, how a manufacturer can manipulate the architecture to become malicious.

Chapter 7

Physical Cryptography

In this chapter we present a security analysis to a series of problems that can be seen as abstract games. Our main motivation for studying such protocols is their teaching utility. Note that we are not aware of any real-world application of any sort, as these problems fall in the category of "recreational cryptography". Although recreational, these protocols can provide interesting insight and techniques that can be useful for understanding the concepts on which the underlying problems are based.

Physical cryptography [130, 44, 191, 218] makes use of physical properties of systems for encrypting and/or exchanging information (*i.e.* without using one-way functions). Although a very interesting teaching tool, it can be shown that some of the proposed methods are not safe in practice. Thus, our aim is to attack such physical protocols using methods similar to classical side channel techniques.

Besides the obvious cryptographic teaching utility of physical cryptography schemes, we believe that some of the schemes tackled in the current chapter may be successfully used for introducing concepts corresponding to other domains. We provide the reader with such examples in the following sections.

Although some authors acknowledge that their proposed protocols are only useful for playing with children or introducing new concepts to non-technical audiences, the authors of [129, 130, 128, 225] claim that their schemes can be securely implemented in real-life scenarios. In [81], Courtois attacks one of the protocols proposed in [129], but the authors contest his results in [130]. We independently conducted a simulation of the attack and our results acknowledge Courtois' claim.

Bibliography

[1] A Full Exploit of CVE-2017-3000 on Flash Player Constant Blinding PRNG. https://github.com/dangokyo/CVE-2017-3000/blob/master/Exploiter.as.

[2] Bitcoin: Average Confirmation Time. https://www.blockchain.com/charts/avg-confirmation-time.

[3] C++ Random Library. www.cplusplus.com/reference/random/.

[4] eSTREAM: the ECRYPT Stream Cipher Project. http://www.ecrypt.eu.org/stream/.

[5] Falstad Electronic Circuit. https://www.falstad.com.

[6] Frequently Asked Questions About Netflix Billing. https://help.netflix.com/en/node/41049?ui_action=kb-article-popular-categories.

[7] How to Manage Your Prime Video Channel Subscriptions. https://www.amazon.com/gp/help/customer/display.html?nodeId=201975160.

[8] How to Order HBO: Subscriptios & Pricing Options. https://www.hbo.com/ways-to-get.

[9] Kryptos. https://en.wikipedia.org/wiki/Kryptos.

[10] Left Shift and Right Shift Operators. https://docs.microsoft.com/en-us/cpp/cpp/left-shift-and-right-shift-operators-input-and-output?view=vs-2017.

[11] mbed TLS. https://tls.mbed.org.

[12] Mining Hardware Comparison. https://en.bitcoin.it/wiki/Mining_hardware_comparison.

[13] NIST SP 800-22: Download Documentation and Software. https://csrc.nist.gov/Projects/Random-Bit-Generation/Documentation-and-Software.

[14] Non-Specialized Hardware Comparison. https://en.bitcoin.it/wiki/Non-specialized_hardware_comparison.

[15] OpenMP. https://www.openmp.org/.

[16] Safe Prime Database. https://2ton.com.au/safeprimes/.

[17] Source Code for the Actionscript Virtual Machine. https://github.com/adobe-flash/avmplus/tree/master/core/MathUtils.cpp.

[18] The Diffie-Hellman Key Exchange Using Paint. https://www.youtube.com/watch?v=3QnD2c4Xovk.

[19] The GNU Multiple Precision Arithmetic Library. https://gmplib.org/.

[20] Using the GNU Compiler Collection. https://gcc.gnu.org/onlinedocs/gcc/Integers-implementation.html.

[21] Vulnerability Details: CVE-2017-3000. https://www.cvedetails.com/cve/CVE-2017-3000/.

[22] World Map of Encryption Laws and Policies. https://www.gp-digital.org/world-map-of-encryption/.

[23] FIPS PUB 186-4: Digital Signature Standard (DSS). Technical report, NIST, 2013.

[24] Michel Abdalla, Mihir Bellare, and Phillip Rogaway. DHAES: An Encryption Scheme Based on the Diffie-Hellman Problem. *IACR Cryptology ePrint Archive*, 1999/7, 1999.

[25] Michel Abdalla, Mihir Bellare, and Phillip Rogaway. The Oracle Diffie-Hellman Assumptions and an Analysis of DHIES. In *CT-RSA 2001*, volume 2020 of *Lecture Notes in Computer Science*, pages 143–158. Springer, 2001.

[26] Carlisle Adams, Pat Cain, Denis Pinkas, and Robert Zuccherato. RFC 3161: Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP). Technical report, Internet Engineering Task Force, 2001.

[27] Gorjan Alagic and Alexander Russell. Quantum-Secure Symmetric-Key Cryptography Based on Hidden Shifts. In *EUROCRYPT 2018*, volume 10212 of *Lecture Notes in Computer Science*, pages 65–93. Springer, 2017.

[28] Ange Albertini, Jean-Philippe Aumasson, Maria Eichlseder, Florian Mendel, and Martin Schläffer. Malicious Hashing: Eve's Variant of SHA-1. In *SAC 2014*, volume 8781 of *Lecture Notes in Computer Science*, pages 1–19. Springer, 2014.

[29] N. Asokan, Matthias Schunter, and Michael Waidner. Optimistic Protocols for Fair Exchange. In *CCS 1997*, pages 7–17. ACM, 1997.

[30] American Bankers Association et al. Working Draft: American National Standard X9. 62-1998 Public Key Cryptography for the Financial Services Industry. Technical report, 1998.

[31] Giuseppe Ateniese and Paolo Gasti. Universally Anonymous IBE Based on the Quadratic Residuosity Assumption. In *CT-RSA 2009*, volume 5473 of *Lecture Notes in Computer Science*, pages 32–47. Springer, 2009.

[32] Giuseppe Ateniese, Bernardo Magri, and Daniele Venturi. Subversion-Resilient Signature Schemes. In *CCS 2015*, pages 364–375. ACM, 2015.

[33] Michalis Athanasakis, Elias Athanasopoulos, Michalis Polychronakis, Georgios Portokalidis, and Sotiris Ioannidis. The Devil is in the Constants: Bypassing Defences in Browser JIT Engines. In *NDSS 2015*. The Internet Society, 2015.

[34] Jean-Philippe Aumasson, Itai Dinur, Luca Henzen, Willi Meier, and Adi Shamir. Efficient FPGA Implementations of High-Dimensional Cube Testers on the Stream Cipher Grain-128. *IACR Cryptology ePrint Archive*, 2009/218, 2009.

[35] Shahram Bakhtiari, Reihaneh Safavi-Naini, and Josef Pieprzyk. A Message Authentication Code Based on Latin Squares. In *ACISP 1997*, volume 1270 of *Lecture Notes in Computer Science*, pages 194–203. Springer, 1997.

[36] James Ball, Julian Borger, and Glenn Greenwald. Revealed: How US and UK Spy Agencies Defeat Internet Privacy and Security. *The Guardian*, 6, 2013.

[37] József Balogh, János A Csirik, Yuval Ishai, and Eyal Kushilevitz. Private Computation Using a PEZ Dispenser. *Theoretical Computer Science*, 306(1-3):69–84, 2003.

[38] Subhadeep Banik, Subhamoy Maitra, and Santanu Sarkar. Some Results on Related Key-IV Pairs of Grain. In *SPACE 2012*, volume 7644 of *Lecture Notes in Computer Science*, pages 94–110. Springer, 2012.

[39] Subhadeep Banik, Subhamoy Maitra, Santanu Sarkar, and Turan Meltem Sönmez. A Chosen IV Related Key Attack on Grain-128a. In *ACISP 2013*, volume 7959 of *Lecture Notes in Computer Science*, pages 13–26. Springer, 2013.

[40] Manuel Barbosa, Thierry Brouard, Stéphane Cauchie, and Simao Melo De Sousa. Secure Biometric Authentication with Improved Accuracy. In *ACISP 2008*, volume 5107 of *Lecture Notes in Computer Science*, pages 21–36. Springer, 2008.

[41] Craig Bauer, Gregory Link, and Dante Molle. James Sanborn's Kryptos and the Matrix Encryption Conjecture. *Cryptologia*, 40(6):541–552, 2016.

[42] Craig Bauer and Katherine Millward. Cracking Matrix Encryption Row by Row. *Cryptologia*, 31(1):76–83, 2007.

[43] Friedrich Ludwig Bauer. *Decrypted Secrets: Methods and Maxims of Cryptology*. Springer, 2002.

[44] Tim Bell, Harold Thimbleby, Mike Fellows, Ian Witten, Neil Koblitz, and Matthew Powell. Explaining Cryptographic Systems. *Computers & Education*, 40(3):199–215, 2003.

[45] Mihir Bellare, Joseph Jaeger, and Daniel Kane. Mass-Surveillance without the State: Strongly Undetectable Algorithm-Substitution Attacks. In *CCS 2015*, pages 1431–1440. ACM, 2015.

[46] Mihir Bellare, Chanathip Namprempre, and Gregory Neven. Security Proofs for Identity-Based Identification and Signature Schemes. *Journal of Cryptology*, 22(1):1–61, 2009.

[47] Mihir Bellare, Kenneth G. Paterson, and Phillip Rogaway. Security of Symmetric Encryption Against Mass Surveillance. In *CRYPTO 2014*, volume 8616 of *Lecture Notes in Computer Science*, pages 1–19. Springer, 2014.

[48] Mihir Bellare and Phillip Rogaway. Minimizing the Use of Random Oracles in Authenticated Encryption Schemes. In *ICICS 1997*, volume 1334 of *Lecture Notes in Computer Science*, pages 1–16. Springer, 1997.

[49] Mihir Bellare and Phillip Rogaway. Introduction to Modern Cryptography. https://web.cs.ucdavis.edu/~rogaway/classes/227/spring05/book/main.pdf, 2005.

[50] Luciano Bello. DSA-1571-1 OpenSSL—Predictable Random Number Generator. https://www.debian.org/security/2008/dsa-1571, 2008.

[51] Fabrice Benhamouda, Javier Herranz, Marc Joye, and Benoît Libert. Efficient Cryptosystems from 2^k-th Power Residue Symbols. *Journal of Cryptology*, 30(2):519–549, 2017.

[52] Côme Berbain, Henri Gilbert, and Alexander Maximov. Cryptanalysis of Grain. In *FSE 2006*, volume 4047 of *Lecture Notes in Computer Science*, pages 15–29. Springer, 2006.

[53] Sebastian Berndt and Maciej Liśkiewicz. Algorithm Substitution Attacks from a Steganographic Perspective. In *CCS 2017*, pages 1649–1660. ACM, 2017.

[54] Daniel J. Bernstein, Tanja Lange, and Ruben Niederhagen. Dual EC: A Standardized Back Door. In *The New Codebreakers*, volume 9100 of *Lecture Notes in Computer Science*, pages 256–281. Springer, 2016.

[55] Eli Biham and Adi Shamir. Differential Cryptanalysis of DES-like Cryptosystems. In *CRYPTO 1990*, volume 537 of *Lecture Notes in Computer Science*, pages 2–21. Springer, 1991.

[56] Dionysus Blazakis. Interpreter Exploitation. In *WOOT 2010*. USENIX Association, 2010.

[57] Jens-Matthias Bohli, Maria Isabel Gonzalez Vasco, and Rainer Steinwandt. A subliminal-free variant of ECDSA. In *IH 2006*, volume 4437 of *Lecture Notes in Computer Science*, pages 375–387. Springer, 2006.

[58] Dan Boneh, Giovanni Di Crescenzo, Rafail Ostrovsky, and Giuseppe Persiano. Public Key Encryption with Keyword Search. In *EUROCRYPT 2004*, volume 3027 of *Lecture Notes in Computer Science*, pages 506–522. Springer, 2004.

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

[60] Dan Boneh, Craig Gentry, and Michael Hamburg. Space-efficient Identity Based Encryption Without Pairings. In *FOCS 2007*, pages 647–657. IEEE Computer Society, 2007.

[61] Julien Bringer, Hervé Chabanne, Malika Izabachéne, David Pointcheval, Qiang Tang, and Sébastien Zimmer. An Application of the Goldwasser-Micali Cryptosystem to Biometric Authentication. In *ACISP 2007*, pages 96–106. Springer, 2007.

[62] Xavier Bultel, Jannik Dreier, Pascal Lafourcade, and Malika More. How to explain modern security concepts to your children. *Cryptologia*, 41(5):422–447, 2017.

[63] Christian Cachin and Jan Camenisch. Optimistic Fair Secure Computation. In *CRYPTO 2000*, volume 1880 of *Lecture Notes in Computer Science*, pages 93–111. Springer, 2000.

[64] Christophe Cannière, Özgül Küçük, and Bart Preneel. Analysis of Grain's Initialization Algorithm. In *AFRICACRYPT 2008*, volume 5023 of *Lecture Notes in Computer Science*, pages 276–289. Springer, 2008.

[65] Anne Canteaut, Pascale Charpin, and Hans Dobbertin. Weight Divisibility of Cyclic Codes, Highly Nonlinear Functions on F_{2^m}, and Crosscorrelation of Maximum-Length Sequences. *SIAM J. Discrete Math.*, 13(1):105–138, 2000.

[66] Héctor Martín Cantero, Sven Peter, and Segher Bushing. Console Hacking 2010–PS3 Epic Fail. In *27th Chaos Communication Congress*, 2010.

[67] Charalambos A Charalambides. *Enumerative Combinatorics*. Chapman and Hall/CRC, 2002.

[68] David Chaum, Jan-Hendrik Evertse, and Jeroen Van De Graaf. An Improved Protocol for Demonstrating Possession of Discrete Logarithms and Some Generalizations. In *EUROCRYPT 1987*, volume 304 of *Lecture Notes in Computer Science*, pages 127–141. Springer, 1987.

[69] Stephen Checkoway, Jacob Maskiewicz, Christina Garman, Joshua Fried, Shaanan Cohney, Matthew Green, Nadia Heninger, Ralf-Philipp Weinmann, Eric Rescorla, and Hovav Shacham. A Systematic Analysis of the Juniper Dual EC Incident. In *CCS 2016*, pages 468–479. ACM, 2016.

[70] Stephen Checkoway, Ruben Niederhagen, Adam Everspaugh, Matthew Green, Tanja Lange, Thomas Ristenpart, Daniel J. Bernstein, Jake Maskiewicz, Hovav Shacham, and Matthew Fredrikson. On the Practical Exploitability of Dual EC in TLS Implementations. In *USENIX Security Symposium*, pages 319–335. USENIX Association, 2014.

[71] Liqun Chen, Caroline Kudla, and Kenneth G. Paterson. Concurrent Signatures. In *EUROCRYPT 2004*, volume 3027 of *Lecture Notes in Computer Science*, pages 287–305. Springer, 2004.

[72] Benoît Chevallier-Mames. An Efficient CDH-Based Signature Scheme with a Tight Security Reduction. In *CRYPTO 2005*, volume 3621 of *Lecture Notes in Computer Science*, pages 511–526. Springer, 2005.

[73] Jong Youl Choi, Philippe Golle, and Markus Jakobsson. Tamper-Evident Digital Signature Protecting Certification Authorities Against Malware. In *DASC 2006*, pages 37–44. IEEE, 2006.

[74] Jae Cha Choon and Jung Hee Cheon. An Identity-Based Signature from Gap Diffie-Hellman Groups. In *PKC 2003*, volume 2567 of *Lecture Notes in Computer Science*, pages 18–30. Springer, 2003.

[75] Nicolas Christin. Traveling the Silk Road: A Measurement Analysis of a Large Anonymous Online Marketplace. In *WWW 2013*, pages 213–224. ACM, 2013.

[76] Michael Clear, Hitesh Tewari, and Ciarán McGoldrick. Anonymous IBE from Quadratic Residuosity with Improved Performance. In *AFRICACRYPT 2014*, volume 8469 of *Lecture Notes in Computer Science*, pages 377–397. Springer, 2014.

[77] Clifford Cocks. An Identity Based Encryption Scheme Based on Quadratic Residues. In *IMACC 2001*, volume 2260 of *Lecture Notes in Computer Science*, pages 360–363. Springer, 2001.

[78] Simon Cogliani, Bao Feng, Houda Ferradi, Rémi Géraud, Diana Maimuţ, David Naccache, Rodrigo Portella do Canto, and Guilin Wang. Public Key-Based Lightweight Swarm Authentication. In *Cyber-Physical Systems Security*, pages 255–267. Springer, 2018.

[79] Josh Cohen and Michael Fischer. A Robust and Verifiable Cryptographically Secure Ellection Scheme (extended abstract). In *FOCS 1985*, pages 372–382. IEEE Computer Society Press, 1985.

[80] Mariana Costiuc, Diana Maimuţ, and George Teşeleanu. Physical Cryptography. In *SECITC 2019*, volume 12001 of *Lecture Notes in Computer Science*, pages 156–171. Springer, 2019.

[81] Nicolas T. Courtois. Cryptanalysis of Grigoriev-Shpilrain Physical Asymmetric Scheme With Capacitors. *IACR Cryptology ePrint Archive*, 2013/302, 2013.

[82] Richard Crandall and Carl Pomerance. *Prime Numbers: A Computational Perspective*. Number Theory and Discrete Mathematics. Springer, 2005.

[83] Claude Crépeau and Alain Slakmon. Simple Backdoors for RSA Key Generation. In *CT-RSA 2003*, volume 2612 of *Lecture Notes in Computer Science*, pages 403–416. Springer, 2003.

[84] Paul Crowley. Mirdek: A Card Cipher Inspired by "Solitaire". http://www.ciphergoth.org/crypto/mirdek/.

[85] Joan Daemen and Vincent Rijmen. *The Design of Rijndael: AES - The Advanced Encryption Standard*. Springer Science & Business Media, 2013.

[86] Harold Davenport. On the Distribution of Quadratic Residues (mod p). *Journal of the London Mathematical Society*, s1-6(1):49–54, 1931.

[87] Harold Davenport. On the Distribution of Quadratic Residues (mod p). *Journal of the London Mathematical Society*, s1-8(1):46–52, 1933.

[88] Jean Paul Degabriele, Pooya Farshim, and Bertram Poettering. A More Cautious Approach to Security Against Mass Surveillance. In *FSE 2015*, volume 9054 of *Lecture Notes in Computer Science*, pages 579–598. Springer, 2015.

[89] Jean Paul Degabriele, Kenneth G. Paterson, Jacob CN Schuldt, and Joanne Woodage. Backdoors in Pseudorandom Number Generators: Possibility and Impossibility Results. In *CRYPTO 2016*, volume 9814 of *Lecture Notes in Computer Science*, pages 403–432. Springer, 2016.

[90] József Dénes and A Donald Keedwell. A New Authentication Scheme Based on Latin Squares. *Discrete Mathematics*, 106:157–161, 1992.

[91] Itai Dinur, Tim Güneysu, Christof Paar, Adi Shamir, and Ralf Zimmermann. An Experimentally Verified Attack on Full Grain-128 Using Dedicated Reconfigurable Hardware. In *ASIACRYPT 2011*, volume 7073 of *Lecture Notes in Computer Science*, pages 327–343. Springer, 2011.

[92] Itai Dinur and Adi Shamir. Breaking Grain-128 with Dynamic Cube Attacks. In *FSE 2011*, volume 6733 of *Lecture Notes in Computer Science*, pages 167–187. Springer, 2011.

[93] Hans Dobbertin. One-to-One Highly Nonlinear Power Functions on GF(2^n). *Appl. Algebra Eng. Commun. Comput.*, 9(2):139–152, 1998.

[94] Yevgeniy Dodis, Chaya Ganesh, Alexander Golovnev, Ari Juels, and Thomas Ristenpart. A Formal Treatment of Backdoored Pseudorandom Generators. In *EUROCRYPT 2015*, volume 9056 of *Lecture Notes in Computer Science*, pages 101–126. Springer, 2015.

[95] Yevgeniy Dodis, Rosario Gennaro, Johan Håstad, Hugo Krawczyk, and Tal Rabin. Randomness Extraction and Key Derivation Using the CBC, Cascade and HMAC Modes. In *CRYPTO 2004*, volume 3152 of *Lecture Notes in Computer Science*, pages 494–510. Springer, 2004.

[96] Yevgeniy Dodis, Ilya Mironov, and Noah Stephens-Davidowitz. Message Transmission with Reverse Firewalls—Secure Communication on Corrupted Machines. In *CRYPTO 2016*, volume 9814 of *Lecture Notes in Computer Science*, pages 341–372. Springer, 2016.

[97] Vasily Dolmatov and Alexey Degtyarev. GOST R 34.10-2012: Digital Signature Algorithm. Technical report, Internet Engineering Task Force, 2013.

[98] Morris Dworkin. Recommendation for Block Cipher Modes of Operation. Methods and Techniques. Technical report, NIST, 2001.

[99] Ibrahim Elashry, Yi Mu, and Willy Susilo. Jhanwar-Barua's Identity-Based Encryption Revisited. In *NSS 2014*, volume 8792 of *Lecture Notes in Computer Science*, pages 271–284. Springer, 2014.

[100] Ibrahim Elashry, Yi Mu, and Willy Susilo. An Efficient Variant of Boneh-Gentry-Hamburg's Identity-Based Encryption Without Pairing. In *WISA 2014*, volume 8909 of *Lecture Notes in Computer Science*, pages 257–268. Springer, 2015.

[101] Taher ElGamal. A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms. *IEEE Transactions on Information Theory*, 31(4):469–472, 1985.

[102] Ronald Fagin, Moni Naor, and Peter Winkler. Comparing Information Without Leaking It. *Communications of the ACM*, 39(5):77–85, 1996.

[103] Uriel Feige, Amos Fiat, and Adi Shamir. Zero-Knowledge Proofs of Identity. *Journal of Cryptology*, 1(2):77–94, 1988.

[104] Houda Ferradi, Rémi Géraud, Diana Maimuţ, David Naccache, and David Pointcheval. Legally Fair Contract Signing Without Keystones. In *ACNS 2016*, volume 9696 of *Lecture Notes in Computer Science*, pages 175–190. Springer, 2016.

[105] Houda Ferradi, Rémi Géraud, Diana Maimuţ, David Naccache, and Amaury de Wargny. Regulating the Pace of von Neumann Correctors. *Journal of Cryptographic Engineering*, pages 1–7, 2017.

[106] Amos Fiat. Batch RSA. In *CRYPTO 1989*, volume 435 of *Lecture Notes in Computer Science*, pages 175–185. Springer, 1989.

[107] Amos Fiat. Batch RSA. *J. Cryptology*, 10(2):75–88, 1997.

[108] Amos Fiat and Adi Shamir. How to Prove Yourself: Practical Solutions to Identification and Signature Problems. In *CRYPTO 1986*, volume 263 of *Lecture Notes in Computer Science*, pages 186–194. Springer, 1986.

[109] Marc Fischlin, Christian Janson, and Sogol Mazaheri. Backdoored Hash Functions: Immunizing HMAC and HKDF. *IACR Cryptology ePrint Archive*, 2018/362, 2018.

[110] Joshua Fried, Pierrick Gaudry, Nadia Heninger, and Emmanuel Thomé. A Kilobit Hidden SNFS Discrete Logarithm Computation. In *EUROCRYPT 2017*, volume 10210 of *Lecture Notes in Computer Science*, pages 202–231. Springer, 2017.

[111] Juan Garay, Philip MacKenzie, Manoj Prabhakaran, and Ke Yang. Resource Fairness and Composability of Cryptographic Protocols. In *TCC 2006*, volume 3876 of *Lecture Notes in Computer Science*, pages 404–428. Springer, 2006.

[112] Rosario Gennaro, Hugo Krawczyk, and Tal Rabin. Secure Hashed Diffie-Hellman over Non-DDH Groups. In *EUROCRYPT 2004*, volume 3027 of *Lecture Notes in Computer Science*, pages 361–381. Springer, 2004.

[113] Marc Girault. An Identity-based Identification Scheme Based on Discrete Logarithms Modulo a Composite Number. In *EUROCRYPT 1990*, volume 473 of *Lecture Notes in Computer Science*, pages 481–486. Springer, 1990.

[114] Marc Girault, Guillaume Poupard, and Jacques Stern. On the Fly Authentication and Signature Schemes Based on Groups of Unknown Order. *Journal of Cryptology*, 19(4):463–487, 2006.

[115] Marc Girault and Jacques Stern. On the Length of Cryptographic Hash-Values Used in Identification Schemes. In *CRYPTO 1994*, volume 839 of *Lecture Notes in Computer Science*, pages 202–215. Springer, 1994.

[116] Danilo Gligoroski, Smile Markovski, and Svein Johan Knapskog. The Stream Cipher Edon80. In *New Stream Cipher Designs*, volume 4986 of *Lecture Notes in Computer Science*, pages 152–169. Springer, 2008.

[117] Danilo Gligoroski, Smile Markovski, and Ljupco Kocarev. Edon-R, An Infinite Family of Cryptographic Hash Functions. *I.J. Network Security*, 8(3):293–300, 2009.

[118] Eu-Jin Goh and Stanisław Jarecki. A Signature Scheme as Secure as the Diffie-Hellman Problem. In *EUROCRYPT 2003*, volume 2656 of *Lecture Notes in Computer Science*, pages 401–415. Springer, 2003.

[119] Dirk Goldhahn, Thomas Eckart, and Uwe Quasthoff. Building Large Monolingual Dictionaries at the Leipzig Corpora Collection: From 100 to 200 Languages. In *LREC 2012*, volume 29, pages 31–43. European Language Resources Association (ELRA), 2012.

[120] Oded Goldreich. *Foundations of Cryptography: Volume 1, Basic Tools*. Cambridge University Press, 2007.

[121] Shafi Goldwasser. Cocks' IBE Scheme. Bilinear Maps. MIT Lecture Notes: "6876: Advanced Cryptography", 2004.

[122] Shafi Goldwasser, Leonid Levin, and Scott A. Vanstone. Fair Computation of General Functions in Presence of Immoral Majority. In *CRYPT0 1990*, volume 537 of *Lecture Notes in Computer Science*, pages 77–93. Springer, 1991.

[123] Shafi Goldwasser and Silvio Micali. Probabilistic Encryption and How to Play Mental Poker Keeping Secret All Partial Information. In *STOC 1982*, pages 365–377. ACM, 1982.

[124] Shafi Goldwasser and Silvio Micali. Probabilistic Encryption. *Journal of Computer and System Sciences*, 28(2):270–299, 1984.

[125] Shafi Goldwasser, Silvio Micali, and Charles Rackoff. The Knowledge Complexity of Interactive Proof Systems. *SIAM J. Comput.*, 18(1):186–208, 1989.

[126] Daniel Gordon. Designing and Detecting Trapdoors for Discrete Log Cryptosystems. In *CRYPTO 1992*, volume 740 of *Lecture Notes in Computer Science*, pages 66–75. Springer, 1993.

[127] S. Dov Gordon, Carmit Hazay, Jonathan Katz, and Yehuda Lindell. Complete Fairness in Secure Two-Party Computation. *Jornal of the ACM*, 58(6):1–37, December 2011.

[128] Dima Grigoriev, Laszlo B. Kish, and Vladimir Shpilrain. Yao's Millionaires' Problem and Public-Key Encryption Without Computational Assumptions. *Int. J. Found. Comput. Sci.*, 28(4):379–390, 2017.

[129] Dima Grigoriev and Vladimir Shpilrain. Secure Information Transmission Based on Physical Principles. In *UCNC 2013*, volume 7956 of *Lecture Notes in Computer Science*, pages 113–124. Springer, 2013.

[130] Dima Grigoriev and Vladimir Shpilrain. Yao's Millionaires' Problem and Decoy-Based Public Key Encryption by Classical Physics. *Int. J. Found. Comput. Sci.*, 25(4):409–418, 2014.

[131] Louis C. Guillou and Jean-Jacques Quisquater. A Practical Zero-Knowledge Protocol Fitted to Security Microprocessor Minimizing Both Transmission and Memory. In *EUROCRYPT 1988*, volume 330 of *Lecture Notes in Computer Science*, pages 123–128. Springer, 1988.

[132] Stuart Haber and W Scott Stornetta. How to Time-Stamp a Digital Document. In *CRYPTO 1990*, volume 537 of *Lecture Notes in Computer Science*, pages 437–455. Springer, 1990.

[133] D. Halliday, R. Resnick, and J. Walker. *Fundamentals of Physics*. John Wiley & Sons, 2010.

[134] Mike Hamburg, Paul Kocher, and Mark E Marson. Analysis of Intel's Ivy Bridge Digital Random Number Generator. Technical report, Rambus, 2012.

[135] Lucjan Hanzlik, Kamil Kluczniak, and Mirosław Kutyłowski. Controlled Randomness - A Defense against Backdoors in Cryptographic Devices. In *MyCrypt 2016*, volume 10311 of *Lecture Notes in Computer Science*, pages 215–232. Springer, 2016.

[136] Dan Harkins and Dave Carrel. RFC 2409: The Internet Key Exchange (IKE). Technical report, Internet Engineering Task Force, 1998.

[137] Sam Hasinoff. Solving Substitution Ciphers. https://people.csail.mit.edu/hasinoff/pubs/hasinoff-quipster-2003.pdf.

[138] Philip Hawkes and Luke O'Connor. XOR and Non-XOR Differential Probabilities. In *EUROCRYPT 1999*, volume 1592 of *Lecture Notes in Computer Science*, pages 272–285. Springer, 1999.

[139] Martin Hell, Thomas Johansson, Alexander Maximov, and Willi Meier. A Stream Cipher Proposal: Grain-128. In *ISIT 2006*, pages 1614–1618. IEEE, 2006.

[140] Martin Hell, Thomas Johansson, and Willi Meier. Grain - A Stream Cipher for Constrained Environments. Technical Report 010, ECRYPT Stream Cipher Project Report, 2005.

[141] Martin Hell, Thomas Johansson, and Willi Meier. Grain: A Stream Cipher for Constrained Environments. *International Journal of Wireless and Mobile Computing*, 2(1):86–93, May 2007.

[142] Florian Hess. Efficient Identity Based Signature Schemes Based On Pairings. In *SAC 2002*, volume 2595 of *Lecture Notes in Computer Science*, pages 310–324. Springer, 2002.

[143] Howard M Heys. A Tutorial on Linear and Differential Cryptanalysis. *Cryptologia*, 26(3):189–221, 2002.

[144] Lester S Hill. Cryptography in an Algebraic Alphabet. *The American Mathematical Monthly*, 36(6):306–312, 1929.

[145] Lester S Hill. Concerning Certain Linear Transformation Apparatus of Cryptography. *The American Mathematical Monthly*, 38(3):135–154, 1931.

[146] Susan M Howitt and Anna N Wilson. Revisiting "Is the Scientific Paper a Fraud?". *EMBO Reports*, 15(5):481–484, 2014.

[147] Mahabir Prasad Jhanwar and Rana Barua. A Variant of Boneh-Gentry-Hamburg's Pairing-Free Identity Based Encryption Scheme. In *INSCRYPT 2008*, volume 5487 of *Lecture Notes in Computer Science*, pages 314–331. Springer, 2009.

[148] Marc Joye. Identity-Based Cryptosystems and Quadratic Residuosity. In *PKC 2016*, volume 9614 of *Lecture Notes in Computer Science*, pages 225–254. Springer, 2016.

[149] Marc Joye and Benoît Libert. Efficient Cryptosystems from 2^k-th Power Residue Symbols. In *EUROCRYPT 2013*, volume 7881 of *Lecture Notes in Computer Science*, pages 76–92. Springer, 2013.

[150] Marc Joye and Benoît Libert. Efficient Cryptosystems from 2^k-th Power Residue Symbols. *IACR Cryptology ePrint Archive*, 2013/435, 2014.

[151] Benjamin Justus. The Distribution of Quadratic Residues and Non-Residues in the Goldwasser-Micali Type of Cryptosystem. *Journal of Mathematical Cryptology*, 8(8):115–140, 2014.

[152] Jonathan Katz and Nan Wang. Efficiency Improvements for Signature Schemes With Tight Security Reductions. In *CCS 2003*, pages 155–164. ACM, 2003.

[153] Charlie Kaufman, Paul Hoffman, Yoav Nir, Parsi Eronen, and Tero Kivinen. RFC7296: Internet Key Exchange Protocol Version 2 (IKEv2). Technical report, Internet Engineering Task Force, 2014.

[154] Shahram Khazaei and Siavash Ahmadi. Ciphertext-Only Attack on $d \times d$ Hill in $O(d13^d)$. *Information Processing Letters*, 118:25–29, 2017.

[155] Shahram Khazaei, Mehdi Hassanzadeh, and Mohammad Kiaei. Distinguishing Attack on Grain. Technical Report 071, ECRYPT Stream Cipher Project Report, 2005.

[156] Tanya Khovanova. One-Way Functions. https://blog.tanyakhovanova.com/2010/11/one-way-functions/.

[157] William A Kiele. A Tensor-Theoretic Enhancement to the Hill Cipher System. *Cryptologia*, 14(3):225–233, 1990.

[158] Wolfgang Killmann and Werner Schindler. A Proposal for: Functionality Classes for Random Number Generators, version 2.0. Technical report, BSI, 2011.

[159] Simon Knellwolf, Willi Meier, and María Naya-Plasencia. Conditional Differential cryptanalysis of NLFSR-Based Cryptosystems. In *ASIACRYPT 2010*, volume 6477 of *Lecture Notes in Computer Science*, pages 130–145. Springer, 2010.

[160] Czesław Kościelny. A Method of Constructing Quasigroup-Based Stream-Ciphers. *Applied Mathematics and Computer Science*, 6:109–122, 1996.

[161] Daniel Kucner and Mirosław Kutyłowski. Stochastic kleptography detection. In *Public-Key Cryptography and Computational Number Theory*, pages 137–149, 2001.

[162] Özgül Küçük. Slide Resynchronization Attack on the Initialization of Grain 1.0. http:www.ecrypt.eu.org/stream, 2006.

[163] Robin Kwant, Tanja Lange, and Kimberley Thissen. Lattice Klepto - Turning Post-Quantum Crypto Against Itself. In *SAC 2017*, volume 10719 of *Lecture Notes in Computer Science*, pages 336–354. Springer, 2017.

[164] Xuejia Lai and James L Massey. A Proposal for a New Block Encryption Standard. In *EUROCRYPT 1990*, volume 473 of *Lecture Notes in Computer Science*, pages 389–404. Springer, 1991.

[165] Xuejia Lai, James L Massey, and Sean Murphy. Markov Ciphers and Differential Cryptanalysis. In *EUROCRYPT 1991*, volume 547 of *Lecture Notes in Computer Science*, pages 17–38. Springer, 1991.

[166] Butler W Lampson. A Note on the Confinement Problem. *Communications of the ACM*, 16(10):613–615, 1973.

[167] Tom Leap, Tim McDevitt, Kayla Novak, and Nicolette Siermine. Further Improvements to the Bauer-Millward Attack on the Hill Cipher. *Cryptologia*, 40(5):452–468, 2016.

[168] Chae Hoon Lim and Pil Joong Lee. A Study on the Proposed Korean Digital Signature Algorithm. In *ASIACRYPT 1998*, volume 1514 of *Lecture Notes in Computer Science*, pages 175–186. Springer, 1998.

[169] Yehuda Lindell. Fast Secure Two-Party ECDSA Signing. In *CRYPTO 2017*, volume 10402 of *Lecture Notes in Computer Science*, pages 613–644. Springer, 2017.

[170] James Lyons. Practical Cryptography, http://practicalcryptography.com/.

[171] Diana Maimuţ and George Teşeleanu. A Unified Security Perspective on Legally Fair Contract Signing Protocols. In *SECITC 2018*, volume 11359 of *Lecture Notes in Computer Science*, pages 477–491. Springer, 2018.

[172] Diana Maimuţ and George Teşeleanu. New Configurations of Grain Ciphers: Security Against Slide Attacks. In *BalkanCrypt 2018*, Communications in Computer and Information Science. Springer, 2018.

[173] Diana Maimuţ and George Teşeleanu. A Generic View on the Unified Zero-Knowledge Protocol and its Applications. In *WISTP 2019*, volume 12024 of *Lecture Notes in Computer Science*, pages 32–46. Springer, 2019.

[174] Diana Maimuţ and George Teşeleanu. A New Generalisation of the Goldwasser-Micali Cryptosystem Based on the Gap 2^k-Residuosity Assumption. In *SECITC 2020*, Lecture Notes in Computer Science. Springer, 2020.

[175] John Malone-Lee and Nigel P. Smart. Modifications of ECDSA. In *SAC 2002*, volume 2595 of *Lecture Notes in Computer Science*, pages 1–12. Springer, 2002.

[176] Ueli Maurer. Unifying Zero-Knowledge Proofs of Knowledge. In *AFRICACRYPT 2009*, volume 5580 of *Lecture Notes in Computer Science*, pages 272–286. Springer, 2009.

[177] Kevin McCurley. A Key distribution System Equivalent to Factoring. *Journal of cryptology*, 1(2):95–105, 1988.

[178] Tim McDevitt, Jessica Lehr, and Ting Gu. A Parallel Time-memory Tradeoff Attack on the Hill Cipher. *Cryptologia*, 42(5):1–19, 2018.

[179] Peter Medawar. Is the Scientific Paper a Fraud? *The Listener*, 70(12):377–378, 1963.

[180] Alfred J. Menezes, Paul C. Van Oorschot, and Scott A. Vanstone. *Handbook of Applied Cryptography*. CRC press, 1996.

[181] Silvio Micali. Simple and Fast Optimistic Protocols for Fair Electronic Exchange. In *PODC 2003*, pages 12–19. ACM, 2003.

[182] Markus Michels, David Naccache, and Holger Petersen. GOST 34.10-A Brief Overview of Russia's DSA. *Computers & Security*, 15(8):725–732, 1996.

[183] Microprocessor, MS Committee, et al. IEEE Standard Specifications for Public-Key Cryptography. *IEEE Computer Society*, 2000.

[184] Ilya Mironov and Noah Stephens-Davidowitz. Cryptographic Reverse Firewalls. In *ASIACRYPT 2015*, volume 9057 of *Lecture Notes in Computer Science*, pages 657–686. Springer, 2015.

[185] Arjan J. Mooij, Nicolae Goga, and Jan Willem Wesselink. *A Distributed Spanning Tree Algorithm for Topology-Aware Networks*. Technische Universiteit Eindhoven, Department of Mathematics and Computer Science, 2003.

[186] Tal Moran and Moni Naor. Polling with Physical Envelopes: A rigorous Analysis of a Human-Centric Protocol. In *EUROCRYPT 2006*, volume 4004 of *Lecture Notes in Computer Science*, pages 88–108. Springer, 2006.

[187] Tal Moran and Moni Naor. Basing Cryptographic Protocols on Tamper-Evident Seals. *Theoretical Computer Science*, 411(10):1283–1310, 2010.

[188] Nicky Mouha. On Proving Security against Differential Cryptanalysis. In *CFAIL 2019*, 2019.

[189] David M'Raïhi, David Naccache, David Pointcheval, and Serge Vaudenay. Computational Alternatives to Random Number Generators. In *SAC 1998*, volume 1556 of *Lecture Notes in Computer Science*, pages 72–80. Springer, 1998.

[190] David Naccache and Jacques Stern. A New Public Key Cryptosytem Based on Higher Residues. In *CCS 1998*, pages 59–66. ACM, 1998.

[191] Moni Naor, Yael Naor, and Omer Reingold. Applied Kid Cryptography or How to Convince Your Children You Are Not Cheating. http://www.wisdom.weizmann.ac.il/~naor/PAPERS/waldo.pdf.

[192] Moni Naor and Omer Reingold. Number-theoretic constructions of efficient pseudo-random functions. In *FOCS 1997*, pages 458–467. IEEE Computer Society, 1997.

[193] Moni Naor and Omer Reingold. Number-Theoretic Constructions of Efficient Pseudo-Random Functions. *Journal of the ACM*, 51(2):231–262, 2004.

[194] Melvyn B. Nathanson. *Elementary Methods in Number Theory*. Graduate Texts in Mathematics. Springer, 2000.

[195] Koki Nishigami and Keiichi Iwamura. Geometric pairwise key-sharing scheme. In *SECITC 2018*, volume 11359 of *Lecture Notes in Computer Science*, pages 518–528. Springer, 2018.

[196] Kaisa Nyberg. Perfect Nonlinear S-boxes. In *EUROCRYPT 1991*, volume 547 of *Lecture Notes in Computer Science*, pages 378–386. Springer, 1991.

[197] Kaisa Nyberg and Rainer A. Rueppel. A New Signature Scheme Based on the DSA Giving Message Recovery. In *CCS 1993*, pages 58–61. ACM, 1993.

[198] Luke O'Connor. On the Distribution of Characteristics in Bijective Mappings. In *EUROCRYPT 1993*, volume 765 of *Lecture Notes in Computer Science*, pages 360–370. Springer, 1994.

[199] Luke O'Connor. On the Distribution of Characteristics in Bijective Mappings. *Journal of Cryptology*, 8(2):67–86, 1995.

[200] Tatsuaki Okamoto. Provably Secure and Practical Identification Schemes and Corresponding Signature Schemes. In *CRYPTO 1992*, volume 740 of *Lecture Notes in Computer Science*, pages 31–53. Springer, 1992.

[201] Jeffrey Overbey, William Traves, and Jerzy Wojdylo. On the Keyspace of the Hill Cipher. *Cryptologia*, 29(1):59–72, 2005.

[202] Pascal Paillier. Public-Key Cryptosystems Based on Composite Degree Residuosity Classes. In *Eurocrypt 1999*, volume 1592 of *Lecture Notes in Computer Science*, pages 223–238. Springer, 1999.

[203] Kenneth G. Paterson. ID-Based Signatures from Pairings on Elliptic Curves. *Electronics Letters*, 38(18):1025–1026, 2002.

[204] René Peralta. On the Distribution of Quadratic Residues and Nonresidues Modulo a Prime Number. *Mathematics of Computation*, 58(197):433–440, 1992.

[205] Nicole Perlroth, Jeff Larson, and Scott Shane. NSA Able to Foil Basic Safeguards of Privacy on Web. *The New York Times*, 5, 2013.

[206] Oskar Perron. Bemerkungen über die Verteilung der quadratischen Reste. *Mathematische Zeitschrift*, 56(2):122–130, 1952.

[207] Benny Pinkas. Fair Secure Two-Party Computation. In *EUROCRYPT 2003*, volume 2656 of *Lecture Notes in Computer Science*, pages 87–105. Springer, 2003.

[208] David Pointcheval and Jacques Stern. Security Proofs For Signature Schemes. In *EUROCRYPT 1996*, volume 1070 of *Lecture Notes in Computer Science*, pages 387–398. Springer, 1996.

[209] David Pointcheval and Jacques Stern. Security Arguments for Digital Signatures and Blind Signatures. *Journal of Cryptology*, 13(3):361–396, 2000.

[210] Jean-Jacques Quisquater, Myriam Quisquater, Muriel Quisquater, Michaël Quisquater, Louis Guillou, Marie Annick Guillou, Gaïd Guillou, Anna Guillou, Gwenolé Guillou, and Soazig Guillou. How to Explain Zero-Knowledge Protocols to Your Children. In *CRYPTO 1989*, volume 435 of *Lecture Notes in Computer Science*, pages 628–631. Springer, 1990.

[211] Martin Ågren, Martin Hell, Thomas Johansson, and Willi Meier. Grain-128a: A New Version of Grain-128 with Optional Authentication. *International Journal of Wireless and Mobile Computing*, 5(1):48–59, December 2011.

[212] Elena Reshetova, Filippo Bonazzi, and N. Asokan. Randomization Can't Stop BPF JIT spray. In *NSS 2017*, volume 10394 of *Lecture Notes in Computer Science*, pages 233–247. Springer, 2017.

[213] Ronald L Rivest, Adi Shamir, and David A Wagner. Time-lock Puzzles and Timed-release Crypto. Technical report, MIT, 1996.

[214] Alexander Russell, Qiang Tang, Moti Yung, and Hong-Sheng Zhou. Cliptography: Clipping the power of kleptographic attacks. In *ASIACRYPT 2016*, volume 10032 of *Lecture Notes in Computer Science*, pages 34–64. Springer, 2016.

[215] Alexander Russell, Qiang Tang, Moti Yung, and Hong-Sheng Zhou. Destroying Steganography via Amalgamation: Kleptographically CPA Secure Public Key Encryption. *IACR Cryptology ePrint Archive*, 2016/530, 2016.

[216] Ryuichi Sakai, Kiyoshi Ohgishi, and Masao Kasahara. Cryptosystems Based on Pairings. In *SCIS 2000*, 2000.

[217] Conrad Sanderson and Ryan Curtin. Armadillo: A Template-Based C++ Library for Linear Algebra. *Journal of Open Source Software*, 1(2):26, 2016.

[218] Bruce Schneier. The Solitaire Encryption Algorithm. https://www.schneier.com/academic/solitaire/.

[219] Claus-Peter Schnorr. Efficient Identification and Signatures For Smart Cards. In *CRYPTO 1989*, volume 435 of *Lecture Notes in Computer Science*, pages 239–252. Springer, 1989.

[220] Martin A Schwartz. The Importance of Stupidity in Scientific Research. *Journal of Cell Science*, 121(11):1771–1771, 2008.

[221] Adi Shamir. How to Share a Secret. *Communications of the ACM*, 22(11):612–613, 1979.

[222] Adi Shamir. Identity-Based Cryptosystems and Signature Schemes. In *CRYPTO 1984*, volume 196 of *Lecture Notes in Computer Science*, pages 47–53. Springer, 1985.

[223] Victor Shoup. Sequences of Games: A Tool for Taming Complexity in Security Proofs. *IACR Cryptology ePrint Archive*, 2004/332, 2004.

[224] Victor Shoup. *A Computational Introduction to Number Theory and Algebra*. Cambridge University Press, 2008.

[225] Vladimir Shpilrain. Decoy-Based Information Security. *Groups Complexity Cryptology*, 6(2):149–155, 2014.

[226] Gustavus J. Simmons. The Subliminal Channel and Digital Signatures. In *EUROCRYPT 1984*, volume 209 of *Lecture Notes in Computer Science*, pages 364–378. Springer, 1984.

[227] Gustavus J. Simmons. Subliminal Communication is Easy Using the DSA. In *EUROCRYPT 1993*, volume 765 of *Lecture Notes in Computer Science*, pages 218–232. Springer, 1993.

[228] Gustavus J Simmons. Subliminal Channels; Past and Present. *European Transactions on Telecommunications*, 5(4):459–474, 1994.

[229] Simon Singh. *The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography*. Anchor, 2000.

[230] Jonathan DH Smith. Four Lectures on Quasigroup Representations. *Quasigroups Related Systems*, 15:109–140, 2007.

[231] Paul Stankovski. Greedy Distinguishers and Nonrandomness Detectors. In *INDOCRYPT 2010*, volume 6498 of *Lecture Notes in Computer Science*, pages 210–226. Springer, 2010.

[232] Neal Stephenson. *Cryptonomicon*. Arrow, 2000.

[233] Douglas R Stinson. *Cryptography: Theory and Practice*. CRC press, 2005.

[234] Fatih Sulak. New Statistical Randomness Tests: 4-bit Template Matching Tests. *Turkish Journal of Mathematics*, 41(1):80–95, 2017.

[235] Terence Tao. Ask Yourself Dumb Questions - and Answer Them! https://terrytao.wordpress.com/career-advice/ask-yourself-dumb-questions-and-answer-them/.

[236] Terence Tao. Use The Wastebasket. https://terrytao.wordpress.com/career-advice/use-the-wastebasket/.

[237] George Teşeleanu. Threshold Kleptographic Attacks on Discrete Logarithm Based Signatures. In *LatinCrypt 2017*, volume 11368 of *Lecture Notes in Computer Science*, pages 401–414. Springer, 2017.

[238] George Teşeleanu. Random Number Generators Can Be Fooled to Behave Badly. In *ICICS 2018*, volume 11149 of *Lecture Notes in Computer Science*, pages 124–141. Springer, 2018.

[239] George Teşeleanu. Unifying Kleptographic Attacks. In *NordSec 2018*, volume 11252 of *Lecture Notes in Computer Science*, pages 73–87. Springer, 2018.

[240] George Teşeleanu. Managing Your Kleptographic Subscription Plan. In *C2SI 2019*, volume 11445 of *Lecture Notes in Computer Science*, pages 452–461. Springer, 2019.

[241] George Teşeleanu. Reinterpreting and Improving the Cryptanalysis of the Flash Player PRNG. In *C2SI 2019*, volume 11445 of *Lecture Notes in Computer Science*, pages 92–104. Springer, 2019.

[242] George Teşeleanu. Subliminal Hash Channels. In *A2C 2019*, volume 1133 of *Communications in Computer and Information Science*, pages 149–165. Springer, 2019.

[243] George Teşeleanu. A Love Affair Between Bias Amplifiers and Broken Noise Sources. In *ICICS 2020*, Lecture Notes in Computer Science. Springer, 2020.

[244] George Teşeleanu. Cracking Matrix Modes of Operation with Goodness-of-Fit Statistics. In *HistoCrypt 2020*, Linköping Electronic Conference Proceedings. Linköping University Electronic Press, 2020.

[245] George Teşeleanu. Quasigroups and Substitution Permutation Networks: A Failed Experiment. *Cryptologia*, 2020.

[246] Ferucio Laurenţiu Ţiplea, Sorin Iftene, George Teşeleanu, and Anca-Maria Nica. Security of Identity-Based Encryption Schemes from Quadratic Residues. In *SECITC 2016*, volume 10006 of *Lecture Notes in Computer Science*, pages 63–77, 2016.

[247] Ferucio Laurentiu Tiplea, Sorin Iftene, George Teseleanu, and Anca-Maria Nica. On the Distribution of Quadratic Residues and Non-residues Modulo Composite Integers and Applications to Cryptography. *Appl. Math. Comput.*, 372, 2020.

[248] Peter Truran. *Practical Applications of the Philosophy of Science: Thinking About Research*. Springer Science & Business Media, 2013.

[249] Meltem Sönmez Turan, Elaine Barker, John Kelsey, Kerry McKay, Mary Baish, and Mike Boyle. NIST DRAFT Special Publication 800-90B: Recommendation for the Entropy Sources Used for Random Bit Generation. Technical report, NIST, 2012.

[250] Umesh V. Vazirani and Vijay V. Vazirani. Trapdoor Pseudo-random Number Generators, with Applications to Protocol Design. In *FOCS 1983*, pages 23–30. IEEE, 1983.

[251] Milan Vojvoda, Marek Sỳs, and Matú Jókay. A Note on Algebraic Properties of Quasigroups in Edon80. Technical report, eSTREAM report 2007/005, 2007.

[252] John Von Neumann. Various Techniques Used in Connection with Random Digits. *Applied Math Series*, 12:36–38, 1951.

[253] Chenyu Wang, Tao Huang, and Hongjun Wu. On the Weakness of Constant Blinding PRNG in Flash Player. In *ICICS 2018*, volume 11149 of *Lecture Notes in Computer Science*, pages 107–123. Springer, 2018.

[254] Greg Ward. A Recursive Implementation of the Perlin Noise Function. In *Graphics Gems II*, pages 396–401. Elsevier, 1991.

[255] Donald R Weidman. Emotional Perils of Mathematics. *Science*, 149(3688):1048–1048, 1965.

[256] Chuan-Kun Wu. Hash channels. *Computers & Security*, 24(8):653–661, 2005.

[257] Mark Wutka. The Crypto Forum, http://s13.zetaboards.com/Crypto/topic/123721/1/.

[258] Akihiro Yamaguchi, Takaaki Seo, and Keisuke Yoshikawa. On the Pass Rate of NIST Statistical Test Suite for Randomness. *JSIAM Letters*, 2:123–126, 2010.

[259] Song Y. Yan. *Number Theory for Computing*. Theoretical Computer Science. Springer, 2002.

[260] Andrew C. Yao. Protocols for Secure Computations. In *SFCS 1982*, pages 160–164. IEEE Computer Society, 1982.

[261] Adam Young and Moti Yung. The Dark Side of "Black-Box" Cryptography or: Should We Trust Capstone? In *CRYPTO 1996*, volume 1109 of *Lecture Notes in Computer Science*, pages 89–103. Springer, 1996.

[262] Adam Young and Moti Yung. Kleptography: Using Cryptography Against Cryptography. In *EUROCRYPT 1997*, volume 1233 of *Lecture Notes in Computer Science*, pages 62–74. Springer, 1997.

[263] Adam Young and Moti Yung. The Prevalence of Kleptographic Attacks on Discrete-Log Based Cryptosystems. In *CRYPTO 1997*, volume 1294 of *Lecture Notes in Computer Science*, pages 264–276. Springer, 1997.

[264] Adam Young and Moti Yung. *Malicious Cryptography: Exposing Cryptovirology*. John Wiley & Sons, 2004.

[265] Adam Young and Moti Yung. Malicious Cryptography: Kleptographic Aspects. In *CT-RSA 2005*, volume 3376 of *Lecture Notes in Computer Science*, pages 7–18. Springer, 2005.

[266] Dae Hyun Yum and Pil Joong Lee. Cracking Hill Ciphers with Goodness-of-Fit Statistics. *Cryptologia*, 33(4):335–342, 2009.

[267] Haina Zhang and Xiaoyun Wang. Cryptanalysis of Stream Cipher Grain Family. *IACR Cryptology ePrint Archive*, 2009/109, 2009.

[268] Yuliang Zheng. Digital Signcryption or How to Achieve Cost (Signature & Encryption) $\ll$ Cost (Signature)+ Cost (Encryption). In *CRYPTO 1997*, volume 1294 of *Lecture Notes in Computer Science*, pages 165–179. Springer, 1997.

[269] Yuliang Zheng and Hideki Imai. How to Construct Efficient Signcryption Schemes on Elliptic Curves. *Information Processing Letters*, 68(5):227–233, 1998.

[270] Yuliang Zheng and Jennifer Seberry. Immunizing Public Key Cryptosystems Against Chosen Ciphertext Attacks. *IEEE Journal on Selected Areas in Communications*, 11(5):715–724, 1993.