

On the Impacts of Mathematical Realization over Practical Security of Leakage Resilient Cryptographic Schemes

Guangjun Fan¹, Yongbin Zhou², François-Xavier Standaert³,
and Dengguo Feng¹

¹ State Key Laboratory of Computer Science, Institute of Software,
Chinese Academy of Sciences, Beijing, China
`guangjunfan@163.com, feng@tca.iscas.ac.cn`

² State Key Laboratory of Information Security, Institute of Information Engineering,
Chinese Academy of Sciences, Beijing, China
`zhouyongbin@iie.ac.cn`

³ ICTEAM/ELEN/Crypto Group, Université catholique de Louvain,
Louvain-la-Neuve, Belgium
`fstandae@uclouvain.be`

Abstract. In real world, in order to transform an abstract and generic cryptographic scheme into actual physical implementation, one usually undergoes two processes: mathematical realization at algorithmic level and physical realization at implementation level. In black-box model (i.e. leakage-free setting), a cryptographic scheme can be mathematically realized without affecting its theoretical security as long as the mathematical components meet the required cryptographic properties. However, up to now, no previous work formally show that whether one can mathematically realize a leakage resilient cryptographic scheme in existent ways without affecting its practical security. Our results give a negative answer to this important question by introducing attacks against several kinds of mathematical realization of a practical leakage resilient cryptographic scheme. To be specific, there may exist a big gap between the theoretical tolerance leakage bits number and the practical tolerance leakage bits number of the same leakage resilient cryptographic scheme if the mathematical components in the mathematical realization are not provably secure in leakage setting.

Keywords: Physical Attacks, Leakage Resilient Cryptography, Mathematical Realization, Physical Realization.

1 Introduction

Countermeasures for protecting against physical attacks (such as the most studied side-channel attacks) are taken on three levels: the software level, the hardware level, and the combination of the above two levels. However, these countermeasures have many issues [2]. In order to solve these pressing issues from the area of practical

security about implementation, Dziembowski et al. firstly proposed one general and theoretical methodology called Leakage Resilient Cryptography (LRC) [2].

In real world, in order to transform an abstract and generic cryptographic scheme into actual physical implementation, one usually undergoes two processes: mathematical realization at algorithmic level and physical realization at implementation level. *Mathematical realization* refers to a process in which an abstract and generic cryptographic scheme is transformed into an exact and specific mathematical scheme (After this process, we say the cryptographic scheme is mathematically realized.). This means that *all* the cryptographic components utilized by the cryptographic scheme are instantiated with exact and specific mathematical components. For example, for a public key encryption scheme based on cycle groups with prime order, the implementor chooses specific mathematical representation of the group elements in this process. Another example is that the implementor chooses AES-128 or 3DES to mathematically realize a cryptographic scheme which uses block ciphers as a building block. *Physical realization* refers to a subsequent process in which any exact and specific mathematical scheme (the output of mathematical realization) is transformed into a physical cryptographic module that runs as a piece of software, or hardware, or combination of both.

For both cryptographic schemes in black-box model and leakage resilient cryptographic schemes, it has turned out that practical security highly depends on the details of the physical realization. For example, the physical cryptanalysis results of the leakage resilient cryptographic scheme in paper [18] do not contradict its theoretical security proof and show that whether the theoretical tolerance leakage bits number can be guaranteed depends on the details of the physical realization.

Motivations. In recent years, in the field of LRC, many leakage models have been proposed. These leakage models are mainly based on two different leakage properties.

“*Only Computation Leaks Information*” There are some leakage models that follow the “*Only Computation Leaks Information*” axiom, which states that memory contents that are not accessed during computation, do not leak [3]. This axiom is regarded as the most representative axiom according to side-channel attacks. Leakage resilient stream cipher [2], practical leakage resilient PRNG [20], and leakage resilient ElGamal encryption scheme [1] follow this axiom are given out.

“*Memory Leakage*” Inspired by [4], Akavia et al. [6] introduced the leakage model of “*security against memory attacks*” where one requires that the scheme remains secure even if the adversary obtains bounded memory leakages about the secret key. Public key encryption schemes under this leakage property were introduced in [7]. *Continuous Memory Leakage* [10,11] extends *Memory Leakage*.

There are some other leakage models, such as *Bounded Retrieval Model* [8,9] and *Auxiliary Input Model* [21,22]. Theoretical security of a leakage resilient cryptographic scheme in these leakage models holds only for physical attacks which *rigorously* fit the claimed leakage model. In this paper, we concentrate on

mathematical realization. In black-box model (i.e. leakage-free setting), a cryptographic scheme can be mathematically realized without affecting its theoretical security as long as all the mathematical components in the mathematical realization meet the required cryptographic properties. In leakage setting, we say a leakage resilient cryptographic scheme is practically secure after it is mathematically realized if the practical tolerance leakage bits number equals to the theoretical tolerance leakage bits number even if the adversary knows all the details of the mathematical realization¹ and can obtain leakage bits from any position of all the mathematical components in the mathematical realization by exploiting efficient computable leakage functions (if possible according to the leakage property, e.g. “*Only Computation Leaks Information*” or “*Memory Leakage*”). If a kind of mathematical realization of the leakage resilient cryptographic scheme can guarantee the practical security of the leakage resilient cryptographic scheme, we call this kind of mathematical realization is practically secure for simplicity. However, up to now, no previous work formally show that whether one can mathematically realize a leakage resilient cryptographic scheme in existent ways without affecting its practical security.

In order to answer this important question, we will take the leakage resilient ElGamal encryption scheme instantiated over arbitrary groups of prime order p (where $p - 1$ is not smooth) in the paper [1]² (i.e. scheme EG^*) as an example. The scheme EG^* is constructed in a leakage model that follow the “*Only Computation Leaks Information*” axiom. For simplicity, we only concentrate on how to mathematically realize the process of generating random numbers r_i for scheme EG^* and ignore other abstract cryptographic components which also need to be mathematically realized. We will introduce four different kinds of mathematical realization of scheme EG^* . In each mathematical realization, we use generic Random Number Generator (RNG) or Pseudorandom Number Generator (PRNG) to mathematically realize the process of generating random numbers r_i (Note that, PRNG is used widely for generating random numbers in practice.). We want to see whether or not the four kinds of mathematical realization are practically secure by attacks against them. Note that, in this paper, we only consider mathematical realization, not physical realization. That is to say, our work is regardless of any specific physical attack against physical realization.

Our Contributions. Main contributions of this paper are two-fold as follows. First, by some counterexamples, our research gives a negative answer to the important question that whether one can mathematically realize a leakage resilient cryptographic scheme in existent ways without affecting its practical security.

¹ According to Kerckhoffs’ principle, this assumption is reasonable.

² The same leakage resilient ElGamal scheme instantiated over bilinear groups of prime order p (where $p - 1$ is not smooth) is leakage resilient in the generic-group model (i.e. scheme BEG^*). However, it is very hard to implement the generic-group model in practice. This drawback of the generic-group model goes against our recommendation to at least provide mathematical realization for a cryptographic scheme. Therefore, in this paper, we consider the scheme EG^* which can be implemented in practice easily.

There may exist a big gap between the theoretical tolerance leakage bits number and the practical tolerance leakage bits number of the same leakage resilient cryptographic scheme if the mathematical components in the mathematical realization are not provably secure in leakage setting.

Second, for any leakage resilient cryptographic scheme, tolerance leakage rate reflects its expected security. Therefore, (accurate or rough) estimation of tolerance leakage rate of any leakage resilient cryptographic scheme does make very good sense. For each of the four kinds of mathematical realization of scheme EG^* , this paper specifies an upper bound of the practical tolerance leakage rate that scheme EG^* can tolerate *by-product*. These upper bounds are the best known so far, even though it might not be the tightest one.

Organization of This Paper. The rest of this paper is organized as follows. In Section 2, we first present some basic symbols, notations, and concepts. Then, we briefly review the scheme EG^* . Section 3 introduces the four kinds of mathematical realization of scheme EG^* and their practical tolerance leakage bits number. Section 4 concludes the whole paper.

2 Preliminaries

In this section, we first present some symbols, notations, and concepts used throughout this paper. Then, we briefly review the scheme EG^* .

2.1 Symbols, Notations, and Concepts

If S is a binary bit string, we denote the most significant a bits of S by $S^{[a]}$ and denote the least significant b bits of S by $S_{[b]}$. We denote the length of S by $|S|$ and assume that the binary bit string representation of all the elements in $\mathbb{Z}_p$ has the same length. We denote the least significant bit of S is the 1^{st} bit of S and the most significant bit of S is the $|S|^{th}$ bit of S . We use the symbol $[S]_{(i)}$ to denote the i^{th} bit of S .

2.2 Brief Description of Scheme EG^*

We describe the scheme $\text{EG}^* = (\text{KG}_{\text{EG}}^*, \text{Enc}_{\text{EG}}^*, \text{Dec1}_{\text{EG}}^*, \text{Dec2}_{\text{EG}}^*)$ and the corresponding security definition in the same way as that in the paper [1]. Let the security parameter of scheme EG^* is κ . Let Gen denote a probabilistic algorithm that outputs a cyclic group $\mathbb{G}$ of order p , where p is a strong prime and $|p| = \kappa$. The scheme EG^* is described as a Key Encapsulation Mechanism (KEM) and is shown as follows:

$\text{KG}_{\text{EG}}^*(\kappa)$: Compute $(\mathbb{G}, p) \xleftarrow{*} \text{Gen}(n)$, $g \xleftarrow{*} \mathbb{G}$, $x \xleftarrow{*} \mathbb{Z}_p$, $h = g^x$. Choose random $\sigma_0 \xleftarrow{*} \mathbb{Z}_p$ and set $\sigma'_0 = x\sigma_0^{-1} \bmod (p)$. The public key is $pk = (\mathbb{G}, p, h)$ and the secret key is $sk = x$. Two secret states are σ_0 and σ'_0 .

$\text{Enc}_{\text{EG}}^*(pk)$: Choose random $r \xleftarrow{*} \mathbb{Z}_p$. Let $C \leftarrow g^r \in \mathbb{G}$ and $K \leftarrow h^r \in \mathbb{G}$. The ciphertext is C and the symmetric key is K .

$\text{Dec1}_{\text{EG}}^*(\sigma_{i-1}, C)$: Choose random $r_i \xleftarrow{*} \mathbb{Z}_p^*$, $\sigma_i = \sigma_{i-1}r_i \bmod (p)$, $K' = C^{\sigma_i}$, return(r_i, K').

$\text{Dec2}_{\text{EG}}^*(\sigma'_{i-1}, (r_i, K'))$: Set $\sigma'_i = \sigma'_{i-1}r_i^{-1} \bmod (p)$, and $K = K'^{\sigma'_i}$. The symmetric key is K and the updated states are σ_i and σ'_i .

The theoretical security definition of scheme EG^* is CCLA1 which was introduced in the paper [1]. In CCLA1, the two leakage functions f_i and g_i are efficient computable functions *adaptively* chosen by the adversary and get as inputs only the secret states that are *actually* accessed during computation. The leakage functions can simulate any computation with the inputs and output any kind of leakages that might occur. The only restriction about the leakage functions is that the ranges of the leakage functions are bounded by leakage parameter λ . For scheme EG^* , the leakage functions f_i and g_i are as follows:

$$A_i \leftarrow f_i(\sigma_{i-1}, r_i), \quad A'_i \leftarrow g_i(\sigma'_{i-1}, (r_i, K'), r_i^{-1}), \text{ and } |A_i| \leq \lambda, |A'_i| \leq \lambda.$$

Note that, when the theoretical security is considered, only $\{\sigma_{i-1}, r_i\}$ and $\{\sigma'_{i-1}, (r_i, K'), r_i^{-1}\}$ are the inputs of the leakage functions. However, when the practical security is considered, according to the “*Only Computation Leaks Information*” axiom, the information in any position of all the mathematical components in the mathematical realization could be the inputs of the leakage functions as long as the position is actually accessed during computation.

Although the authors of the paper [1] didn’t prove the theoretical security of scheme EG^* and only presented the following conjecture, the crucial technique of scheme EG^* (i.e. multiplicative secret sharing) is used widely in the context of LRC [24,25] and scheme EG^* is more practical than other leakage resilient cryptographic schemes. Therefore, we take the scheme EG^* as an example.

Conjecture 1. *The scheme EG^* is CCLA1 secure if $p-1$ has a large prime factor (say, $p-1 = 2q$ for a prime q).*

In [1], the authors conjectured that roughly λ equals to $0.25|p|$ bits in [17] (i.e. the theoretical tolerance leakage rate $\lambda/|p| = 0.25$). Thus total theoretical tolerance leakage bits number in one decapsulation query equals to $2\lambda = 0.5|p|$ bits. We use $\lambda/|p|$ to denote tolerance leakage rate of scheme EG^* and define $\rho = (|f_i| + |g_i|)/|p|$. Any implementation of scheme EG^* will be secure against every side-channel attack that rigorously fits the leakage model, i.e. as long as the amount of information that is leaked during each invocation is sufficiently bounded, and moreover the cryptographic device adheres the “*Only Computation Leaks Information*” axiom. However, the authors said *nothing* about how to mathematically realize the process of generating random numbers r_i for scheme EG^* . Therefore, the implementors may use True Random Number Generator (TRNG) or PRNG to mathematically realize this process in practice.

3 Mathematical Realizations of Scheme EG^*

It is well known that one can use TRNG or PRNG to generate random numbers. Although there exist some TRNGs, PRNG is used more widely than TRNG in

practice. The reasons of this fact are in the following. First, TRNG requires a naturally occurring source of randomness. Designing a hardware device or software program to exploit this randomness and produce a bit sequence that is free of biases and correlations is a difficult task. Second, for most cryptographic applications, the random number generator must not be subject to observation or manipulation by an adversary. However, TRNG is subject to influence by external factors, and also to malfunction. Third, the generation of true random number is an inefficient procedure in most practical environments. Finally, it may be impractical to securely store and transmit a large number of true random bits if these are required in applications. Therefore, we mainly consider the case of utilizing PRNG to mathematically realize the process of generating random numbers in this paper.

In this section, we will introduce four kinds of mathematical realization of scheme EG^* . In each mathematical realization, the process of generating random numbers r_i is mathematically realized by a generic RNG or a specific PRNG. We want to see whether the four kinds of mathematical realization are practically secure by presenting specific attacks against them. The goal of all our attacks is to recover the secret key x . To achieve this goal, our attacks need to obtain all the bits of the random number r_i for each invocation of the decapsulation query of scheme EG^* . The adversary can recover all the bits of σ_i and σ'_i ($i = 0, 1, \dots$) and obtain a candidate value x' of the correct secret key x . The adversary can verify the correctness of x' by a correct pair (C, K) .

In the first kind of mathematical realization, we assume the process of generating random numbers r_i is mathematically realized by a generic RNG and the adversary does not know the internal mathematical structure of the generic RNG. The attack against this kind of mathematical realization (denoted by ATTACK I) can also be viewed as an attack against the theoretical security of scheme EG^* . ATTACK I satisfies the leakage model of scheme EG^* defined in [1] except that it requires a large number of leakage bits. Hence, ATTACK I poses no threat on the theoretical security of scheme EG^* . In the rest three kinds of mathematical realization, we assume the process of generating random numbers r_i is mathematically realized by three specific PRNGs. For convenience, the attacks against the three kinds of mathematical realization are denoted by ATTACK II. ATTACK II have the same basic principle as ATTACK I. However, it is amazing that the results of ATTACK II show that the practical tolerance leakage bits number of scheme EG^* will decrease dramatically when some specific PRNGs are used. *The decrease of the practical tolerance leakage bits number shows the impacts of mathematical realization over practical security of leakage resilient cryptographic schemes.* In the following, we will introduce the four kinds of mathematical realization and the attacks against them. Finally, we will show some discussions and results of the attacks. For both ATTACK I and ATTACK II, we assume the random number r_i is generated by Algorithm 1.

Algorithm 1. The Algorithm of Generating Random Numbers r_i **Input:** no input**Output:** a random number r_i **Step 1** Invoke generic RNG or PRNG to generate a new random number t and $|t| = |r_i|$.**Step 2** If $t = 0$ then return to Step 1 else go to Step 3.**Step 3** If $t < p$ then go to Step 4 else go to Step 5.**Step 4** Let $r_i := t$ and return r_i .**Step 5** Let $r_i := t \bmod p$ and return r_i .**3.1 Mathematical Realization Using Generic RNG**

If the process of generating random numbers r_i is mathematically realized by generic RNG, we can attack this kind of mathematical realization as follows (ATTACK I):

In the 1st invocation of decapsulation query of scheme EG^* , the adversary chooses the leakage functions as follows:

$$f_1(\sigma_0, r_1) = \langle [\sigma_0]_{(1)}, r_1^{\lfloor p/2 \rfloor} \rangle, \quad g_1(\sigma'_0, (r_1, K'), r_1^{-1}) = \langle [\sigma'_0]_{(1)}, r_1^{\lfloor p/2 \rfloor} \rangle.$$

Now, the adversary knows r_1 ($r_1 := r_1^{\lfloor p/2 \rfloor} \parallel r_1^{\lfloor p/2 \rfloor}$), r_1^{-1} (Note that, the prime number p is public.), $\sigma_{0[1]}$, and $\sigma'_{0[1]}$. In the 2nd invocation of decapsulation query, the adversary chooses the leakage functions as follows:

$$f_2(\sigma_1, r_2) = \langle [\sigma_1 r_1^{-1} \bmod p]_{(2)}, r_2^{\lfloor p/2 \rfloor} \rangle = \langle [\sigma_0]_{(2)}, r_2^{\lfloor p/2 \rfloor} \rangle,$$

$$g_2(\sigma'_1, (r_2, K'), r_2^{-1}) = \langle [\sigma'_1 r_1 \bmod p]_{(2)}, r_2^{\lfloor p/2 \rfloor} \rangle = \langle [\sigma'_0]_{(2)}, r_2^{\lfloor p/2 \rfloor} \rangle.$$

After the 2nd invocation of decapsulation query, the adversary knows $r_1, r_1^{-1}, r_2, r_2^{-1}, \sigma_{0[2]}$, and $\sigma'_{0[2]}$. Let $R_{\{a,b\}} := \prod_{s=a}^b r_s \bmod p$ and $R_{\{a,b\}}^{-1} := \prod_{s=a}^b r_s^{-1} \bmod p$. In the i^{th} ($i = 2, \dots, |p| - 1$) invocation of decapsulation query, the adversary chooses the leakage functions as follows:

$$f_i(\sigma_{i-1}, r_i) = \langle [\sigma_{i-1} R_{\{1,i-1\}}^{-1} \bmod p]_{(i)}, r_i^{\lfloor p/2 \rfloor} \rangle = \langle [\sigma_0]_{(i)}, r_i^{\lfloor p/2 \rfloor} \rangle,$$

$$g_i(\sigma'_{i-1}, (r_i, K'), r_i^{-1}) = \langle [\sigma'_{i-1} R_{\{1,i-1\}} \bmod p]_{(i)}, r_i^{\lfloor p/2 \rfloor} \rangle = \langle [\sigma'_0]_{(i)}, r_i^{\lfloor p/2 \rfloor} \rangle.$$

In the $|p|^{\text{th}}$ invocation of decapsulation query, the adversary chooses the leakage functions as follows:

$$f_{|p|}(\sigma_{|p|-1}, r_{|p|}) = \langle [\sigma_{|p|-1} R_{\{1,|p|-1\}}^{-1} \bmod p]_{(|p|)} \rangle = \langle [\sigma_0]_{(|p|)} \rangle,$$

$$g_{|p|}(\sigma'_{|p|-1}, (r_{|p|}, K'), r_{|p|}^{-1}) = \langle [\sigma'_{|p|-1} R_{\{1,|p|-1\}} \bmod p]_{(|p|)} \rangle = \langle [\sigma'_0]_{(|p|)} \rangle.$$

In this way, after invoking the decapsulation query $|p|$ times, the adversary knows all the bits of σ_0 and σ'_0 . Then, he can recover a candidate value

$x' = \sigma_0 \sigma'_0 \bmod p$ of the correct secret key x . Then, the adversary can verify the correctness of x' by a correct pair (C, K) .

To successfully execute ATTACK I, the leakage parameter λ should achieve $0.5|p| + 1$ bits, which is larger than $0.25|p|$. Therefore, ATTACK I poses no threat on the theoretical security of scheme EG^* . Note that, ATTACK I can also be executed after the i^{th} decapsulation query similarly. After the adversary obtaining σ_i and σ'_i , he can recover a candidate value $x' = \sigma_i \sigma'_i \bmod p$ of the correct secret key x .

3.2 Mathematical Realization Using Specific PRNG

Now, we assume that the process of generating random numbers r_i is mathematically realized by specific PRNGs. According to Kerckhoffs' principle, the adversary knows the concrete mathematical structure of the specific PRNG used by the mathematical realization. When the PRNG is invoked to generate a random number r_i in the decapsulation query, all the internal secret states of the PRNG which are actually accessed during computation can be leaked to the adversary due to the "*Only Computation Leaks Information*" axiom.

We know that if the adversary obtains all the bits of all the secret states (such as the seed) of any PRNG, he can totally recover the output of the PRNG trivially. Therefore, for ATTACK II, we *do not* allow the adversary to *directly* obtain all bits of all the secret states of the PRNG from leakages *in one invocation*. Specifically speaking, what the adversary can obtain from leakage functions in one invocation of the decapsulation query of scheme EG^* includes only *part* of bits about the internal secret states of the PRNG and *part* of bits about the output of the PRNG. But the amount of leakages is bounded by λ bits (the leakage parameter). The central idea of ATTACK II is that the adversary tries to recover all bits of the seed of the PRNG (not from direct leakages) by using the specific mathematical structure of the PRNG with at most λ bits from leakages. In this manner, we show the impacts of mathematical realization over the practical security for the leakage resilient scheme EG^* .

We surprisingly find that practical tolerance leakage bits number of scheme EG^* will reduce to a value less than $0.25|p|$ bits when three specific PRNGs are used to mathematically realize the process of generating random numbers r_i . Therefore, the corresponding three kinds of mathematical realization are not practically secure. The three specific PRNGs are ANSI X9.17 PRNG, ANSI X9.31 PRNG, and FIPS 186 PRNG for DSA per-message secrets. We also assume that the seed of the specific PRNG is refreshed in each invocation of the decapsulation query.

3.2.1 Case 1: ANSI X9.17 PRNG and ANSI X9.31 PRNG

The ANSI X9.17 PRNG [12] has been used as a general purpose PRNG in many applications. Let E_{key} (resp. D_{key}) denotes DES E-D-E two-key triple-encryption (resp. decryption) under a key key , which is generated somehow at initialization time and must be reserved exclusively used only for this generator. The key is a internal secret state of the PRNG which is never changed for every invocation of the PRNG. ANSI X9.17 PRNG is shown in Algorithm 2.

Algorithm 2. ANSI X9.17 PRNG**Input:** a random (and secret) 64-bit seed $seed[1]$, integer v , and E_{key} .**Output:** v pseudorandom 64-bit strings (denoted by $output[1], \dots, output[v]$).**Step 1** For l from 1 to v do the following:1.1 Compute $I_l = E_{key}(input[l])$, where $input[l]$ is a 64-bit representation of the system date/time.1.2 $output[l] = E_{key}(I_l \oplus seed[l])$ 1.3 $seed[l+1] = E_{key}(I_l \oplus output[l])$ **Step 2** Return ($output[1], output[2], \dots, output[v]$)

Suppose that each $input[l]$ ($l = 1, 2, \dots, v$) has 10 bits that the adversary does not know (We assume these 10 bits are the least significant 10 bits of each $input[l]$). This is a reasonable assumption for many systems¹ [16]. Before doing our attack, due to the fact that key is never changed for every invocation of the PRNG (*stateless*), the adversary can completely obtain key from leakage function f_i by invoking the decapsulation query repeatedly. In each invocation, the leakage function f_i leaks only part of bits about key (not all the bits of key). After knowing key completely, the adversary continually invoke the decapsulation query for $|p|$ times. Let

$$state_{i+u} := \{output[1]_{i+u}, input[1]_{i+u[10]}, \dots, input[v]_{i+u[10]}\}$$

and the leakage functions are defined as follows. For $u = 1$,

$$f_{i+u}(\sigma_{i+u-1}, r_{i+u}) = \langle [\sigma_i]_{(1)}, state_{i+u} \rangle,$$

$$g_{i+u}(\sigma'_{i+u-1}, (r_{i+u}, K'), r_{i+u}^{-1}) = \langle [\sigma'_i]_{(1)} \rangle.$$

For $u = 2, \dots, |p| - 1$,

$$f_{i+u}(\sigma_{i+u-1}, r_{i+u}) = \langle [\sigma_{i+u-1} R_{\{i+1, i+u-1\}}^{-1} \bmod p]_{(u)}, state_{i+u} \rangle,$$

$$g_{i+u}(\sigma'_{i+u-1}, (r_{i+u}, K'), r_{i+u}^{-1}) = \langle [\sigma'_{i+u-1} R_{\{i+1, i+u-1\}} \bmod p]_{(u)} \rangle.$$

For $u = |p|$,

$$f_{i+u}(\sigma_{i+u-1}, r_{i+u}) = \langle [\sigma_{i+u-1} R_{\{i+1, i+u-1\}}^{-1} \bmod p]_{(|p|)} \rangle = \langle [\sigma_i]_{(|p|)} \rangle$$

$$g_{i+u}(\sigma'_{i+u-1}, (r_{i+u}, K'), r_{i+u}^{-1}) = \langle [\sigma'_{i+u-1} R_{\{i+1, i+u-1\}} \bmod p]_{(|p|)} \rangle = \langle [\sigma'_i]_{(|p|)} \rangle.$$

Now, the adversary obtains

$$\{output[1]_{i+u}, input[1]_{i+u}, \dots, input[v]_{i+u}\}, \quad (u = 1, \dots, |p| - 1)$$

and he can further compute

¹ For example, consider a millisecond timer, and an adversary who knows the nearest second when an output was generated.

$$seed[1]_{i+u} := D_{key}(output[1]_{i+u}) \oplus E_{key}(input[1]_{i+u}).$$

Then the adversary can easily get

$$seed[s]_{i+u} := E_{key}(E_{key}(input[s-1]_{i+u}) \oplus output[s-1]_{i+u})$$

as well as

$$output[s]_{i+u} := E_{key}(E_{key}(input[s]_{i+u}) \oplus seed[s]_{i+u}), (s = 2, 3, \dots, v).$$

Thus the adversary obtain all the bits of r_i for every decapsulation query. Figure 1 and Figure 2 show that the mathematical realization of scheme EG^* is not practically secure any more, if it uses ANSI X9.17 PRNG for strong prime p with size larger than 700 bits.

Note that ANSI X9.31-1998 Appendix A 2.4 in [15] introduces PRNGs using 3-key triple DES or AES. In 3-key triple DES case, due to the fact that $input[l]$, $seed[l]$ and $output[l]$ have the same length as that of ANSI X9.17 PRNG, we can obtain the same attack results as those of the attack against ANSI X9.17 PRNG. Our attack is still valid for this PRNG using AES-128 similarly. Therefore, we do not introduce the attack against this PRNG for AES-128 case here. Figure 1 and Figure 2 show that the mathematical realization of scheme EG^* is not practically secure any more, if it uses ANSI X9.31 PRNG Using AES-128 for strong prime p with size larger than 756 bits.

Analysis. Although these PRNGs are not secure even in leakage-free setting if the adversary knows the *key*, what we want to emphasize here is the drawbacks of the mathematical structures of these PRNGs, which make these PRNGs become insecure in leakage setting. The designers of these PRNGs exploit block ciphers (such as DES, 3DES, and AES-128) to mathematically realize an abstract One-Way Permutation (OWP). These PRNGs themselves can compute the output of the OWP because they know the keys of the block ciphers. In leakage-free setting, if the adversary does not know the keys, he can not recover the inputs of the block ciphers (i.e. the seeds of the PRNGs) and the “One-Way” property holds. However, in leakage setting, the adversary can obtain the keys completely from leakages because they are *stateless*. This means that the One-Way Permutation is replaced by a “One-Way Trapdoor Permutation” and the adversary obtains the trapdoor (i.e. the stateless keys) from leakages. Therefore, the “One-Way” property does not hold any more.

3.2.2 Case 2: FIPS 186 PRNG for DSA Pre-message Secrets

The Digital Signature Standard (DSS) specification (FIPS 186) [13] also describes a fairly simple PRNG based on SHA or DES, which is used for generating DSA per-message secrets. This PRNG is shown in Algorithm 3.

For general purpose PRNG, $\text{mod } q$ operation in this PRNG could be omitted. It is necessary only for DSS where all arithmetic is done $\text{mod } q$. In this paper, we only consider the DES version of this PRNG, where the G function is based on DES. Therefore, the seed (as well as the output) of this PRNG is 160 bits

long. We show the attack against this PRNG when $|p| = 964$ bits as an example. To generate a 964 bits long random number, one needs to invoke this PRNG 7 times ($v = 7$) iteratively to obtain a 1120 bits long random number and discards $output[v]_{[156]}$. Let $state_i = \{output[1]_i^{[40]}, output[2]_i^{[30]}, output[3]_i^{[20]}, output[4]_i^{[10]}, output[5]_i^{[10]}, output[6]_i^{[6]}, output[7]_i^{[4]}\}$. The leakage functions are as follows.

For $i = 1$,

$$f_i(\sigma_{i-1}, r_i) = \langle [\sigma_0]_{(1)}, seed[1]_i^{[120]}, state_i \rangle, \quad g_i(\sigma'_{i-1}, (r_i, K'), r_i^{-1}) = \langle [\sigma'_0]_{(1)} \rangle.$$

For $i = 2, \dots, |p| - 1$,

$$f_i(\sigma_{i-1}, r_i) = \langle [\sigma_{i-1} R_{\{1, i-1\}}^{-1} \bmod p]_{(i)}, seed[1]_i^{[120]}, state_i \rangle,$$

$$g_i(\sigma'_{i-1}, (r_i, K'), r_i^{-1}) = \langle [\sigma'_{i-1} R_{\{1, i-1\}} \bmod p]_{(i)} \rangle.$$

For $i = |p|$,

$$f_i(\sigma_{i-1}, r_i) = \langle [\sigma_{i-1} R_{\{1, i-1\}}^{-1} \bmod p]_{(i)} \rangle = \langle [\sigma_0]_{(|p|)} \rangle,$$

$$g_i(\sigma'_{i-1}, (r_i, K'), r_i^{-1}) = \langle [\sigma'_{i-1} R_{\{1, i-1\}} \bmod p]_{(i)} \rangle = \langle [\sigma'_0]_{(|p|)} \rangle.$$

Algorithm 3. FIPS 186 PRNG for DSA pre-message secrets

Input: an integer v and a 160-bit prime number q .

Output: v pseudorandom numbers $output[1], \dots, output[v]$ in the interval $[0, q - 1]$, which may be used as the per-message secret numbers in the DSA.

Step 1 If the SHA based G function is to be used in step 4.1 then select an integer $160 \leq b \leq 512$. If the DES based G function is to be used in step 4.1 then set $b \leftarrow 160$.

Step 2 Generate a random (and secret) b -bit seed $seed[1]$.

Step 3 Define the 160-bit string $str = efcdab89 \ 98badcfe \ 10325476 \ c3d2e1f0 \ 67452301$ (in hexadecimal).

Step 4 For l from 1 to v do the following:

$$4.1 \ output[l] \leftarrow G(str, seed[l]) \bmod (q).$$

$$4.2 \ seed[l+1] \leftarrow (1 + seed[l] + output[l]) \bmod (2^b).$$

Step 5 Return $(output[1], output[2], \dots, output[v])$.

After the adversary getting the most significant 120 bits of the seed (i.e. $seed[1]_i^{[120]}$ ($i = 1, 2, \dots, |p| - 1$)) from leakages, he could compute all the possible values of the least significant 40 bits of $seed[1]_i$ (i.e. $seed[1]_{i[40]}$) and gets 2^{40} candidate values of $seed[1]_i$. Denote a candidate value by $seed[1]'_i$. For each $seed[1]'_i$, the adversary computes

$$state'_i = \{output[1]_i'^{[40]}, output[2]_i'^{[30]}, output[3]_i'^{[20]}, \\ output[4]_i'^{[10]}, output[5]_i'^{[10]}, output[6]_i'^{[6]}, output[7]_i'^{[4]}\}.$$

using $seed[1]_i'$ and tests the correctness of this candidate value $seed[1]_i'$ using $state_i$ obtained from leakages. For the correct candidate value $seed[1]_i'$ (i.e. $seed[1]_i$), $state_i'$ must equal to $state_i$. This test fails with extremely low probability. For larger size p , the adversary also obtain $seed[1]_i^{[120]}$ from leakages. The number of total leakage bits about the output of the PRNG should keep 120 bits unchanged but the distribution of the leakage bits is changed. For every output block $output[l]$ ($l = 1, 2, \dots, v$), the adversary must obtain some bits about it from leakages (In other words, there does not exist one block of the output blocks of the PRNG ($output[l], l \in \{1, 2, \dots, v\}$) where no leakage occurs.).

We verified our attack by experiments for different size p . The results of experiments verified that our attack against this PRNG is valid. Giving out theoretical success rate of our attack would be interesting but is beyond the scope of this paper. Figure 1 and Figure 2 show that the mathematical realization of scheme EG^* is not practically secure any more, if it uses this PRNG for strong prime p with size larger than 964 bits.

Analysis. It is well known that one bit difference in the input of G function will cause many bits difference in the output of G function. Moreover, this PRNG is invoked *iteratively* to generate random numbers. These drawbacks make our attack become valid.

3.3 The Results of Our Attacks and Discussions

Figure 1. shows the minimum ρ required to successfully recover x for different kinds of mathematical realization. Figure 2. shows the minimum $\lambda/|p|$ required to successfully recover x for different kinds of mathematical realization. According to [23], for long-term security, 1024-bit or larger modulus should be used. Therefore, we can see that if the implementor uses the above-mentioned four PRNGs to mathematically realize the process of generating random numbers r_i for scheme EG^* , the corresponding mathematical realization will not be practically secure any more. From Figure 1 and Figure 2, we find that if the process of

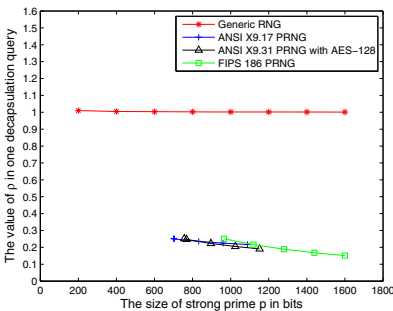


Fig. 1. Minimum ρ required to successfully recover x for different kinds of mathematical realization

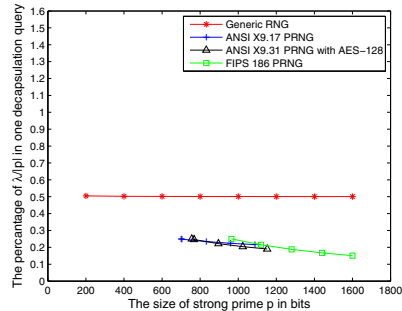


Fig. 2. Minimum $\lambda/|p|$ required to successfully recover x for different kinds of mathematical realization

generating random numbers r_i is leakage-free, our attacks will become invalid. However, assuming the process of generating random numbers r_i is leakage-free contradicts with the “*Only Computation Leaks Information*” axiom. Therefore, we must notice the impacts of mathematical realization over practical security for leakage resilient cryptographic schemes.

The process of generating random numbers r_i for scheme EG^* can also be mathematically realized by TRNGs or other PRNGs. However, it is very difficult to rule out all the attacks against TRNGs or other PRNGs, which can make the corresponding mathematical realizations become practically insecure in leakage setting. The reason is that the security of these specific mathematical algorithms (TRNGs or PRNGs) in leakage setting is usually based on cryptanalysis but is not based on rigorous proof (i.e. in provable security way).

Although practical tolerance leakage rate can be made arbitrarily small for Case 2 with the increase of the size of p , the success of *all* our attacks against these PRNGs is not depend on the size of p but is depend on the drawbacks about the mathematical structures of these PRNGs. The authors of the paper [1] conjectured that the theoretical tolerance leakage rate $\lambda/|p|$ of scheme EG^* equals to 0.25. If the actual value of $\lambda/|p| > 0.25$, all our attacks are valid. Otherwise, if the actual value of $\lambda/|p| < 0.25$, some attacks against these PRNGs *may* become invalid. However, there still exist some kinds of mathematical realization which are not practically secure. For example, for large size p , our attack against FIPS 168 PRNG is still valid.

In paper [20], a practical leakage resilient PRNG in the standard model was introduced. This leakage resilient PRNG is based on $(\epsilon, s, n/\epsilon)$ -secure weak Pseudorandom Function (wPRF) $F(k, pr) : \{0, 1\}^\kappa \times \{0, 1\}^n \rightarrow \{0, 1\}^m$. The symbol pr denotes public randomness. The initial state of this PRNG is (pr_0, pr_1, k_0) for public randomness $(pr_0, pr_1) \xleftarrow{*} (\{0, 1\}^n)^2$ and the random seed $k_0 \xleftarrow{*} \{0, 1\}^\kappa$. This leakage resilient PRNG can be instantiated with any length-expanding wPRF ($m > \kappa$), which in turn can be mathematically realized from any secure block cipher $\text{BC} : \{0, 1\}^\kappa \times \{0, 1\}^n \rightarrow \{0, 1\}^\kappa$. That is, if BC is an $(\epsilon, s, 2q)$ -secure wPRF, then $F(k, pr_l \parallel pr_r) = \text{BC}_k(pr_l) \parallel \text{BC}_k(pr_r)$ is an (ϵ, s, q) -secure wPRF. Note that, the amount of leakages this PRNG can tolerate (denoted by λ_{prng}) equals to $\log(\epsilon^{-1})/6$ and depends on the hardness of the underlying wPRF F [14]. Thus, if F is secure against adversaries of super-polynomial size (i.e. $\epsilon = 2^{\omega(\log \kappa)}$), then the amount of leakages λ_{prng} equals to $\omega(\log \kappa)$, which is quite small. If $\lambda = 0.25|p| \leq \lambda_{\text{prng}}$, the size of the seed k_0 (i.e. κ) should be much larger than $|p|$. Even if the wPRF F is exponentially hard (i.e. $\epsilon = 2^{-\Omega(\kappa)}$), $\epsilon = 2^{-a\kappa}$ ($a \in (0, 1]$) and $\lambda_{\text{prng}} = a\kappa/6$. This PRNG is leakage resilient if and only if $\kappa \geq 1.5|p|$ ($\lambda = 0.25|p| \leq \lambda_{\text{prng}}$). For large size p , to find a secure block cipher with $1.5|p|$ bits long key size is unrealistic. Therefore, this leakage resilient PRNG is not suitable to mathematically realize the process of generating random numbers r_i for scheme EG^* .

The secret key x can also be recovered by exploiting the Hidden Number Problem [17,19] with lower theoretical tolerance leakage bits number (i.e. $\frac{3}{8}|p| + o(|p|)$) than that of ATTACK I. However, practical tolerance leakage bits number

of this attack method (also equals to $\frac{3}{8}|p| + o(|p|)$) is higher than that of ATTACK II when only the process of generating random numbers r_i is mathematically realized with the above PRNGs.

4 Conclusion and Future Work

There may exist a big gap between the theoretical tolerance leakage bits number and the practical tolerance leakage bits number of the same leakage resilient cryptographic scheme if the mathematical components in the mathematical realization are not provably secure in leakage setting even if the theoretical security of the leakage resilient cryptographic scheme still holds. We note that the security of the mathematical components in leakage setting is usually based on cryptanalysis. Moreover, based on the state-of-the-art approach of cryptography, to rigorously prove the security of the mathematical components in leakage setting is rather difficult. Due to the goal of LRC is to theoretically solve the pressing issues from the area of practical security about implementation, we anticipate this great difficulty will hinder the application of leakage resilient cryptographic schemes.

It is well known that specifying all details of implementation in a leakage model is tedious. The paper further [5] shows that it is very difficult to state assumptions at logic gate level. Moreover, it is not clear if it is feasible at all to prove the security with assuming some kind of bounded leakages at higher abstraction level (like mathematical realization at algorithmic level). So, even from the practical point of view, working at mathematical realization in algorithmic level seems appealing. Therefore, we suggest that all (practical) leakage resilient cryptographic schemes should at least come with a kind of mathematical realization. Using this kind of mathematical realization, the practical security of the leakage resilient cryptographic scheme can be guaranteed. Our discoveries also inspire cryptographers to design advanced leakage resilient cryptographic schemes whose practical security is independent of the specific details of mathematical realization.

Whether mathematical realization of other cryptographic components would affect the practical security of a leakage resilient cryptographic scheme is still not known. Furthermore, whether similar problems for other leakage resilient cryptographic schemes in different leakage models are also existent is till unclear. These questions are worthy of research in the future.

Acknowledgments. This work was supported by the National Basic Research Program of China (No. 2013CB338003), National Natural Science Foundation of China (Nos. 61472416, 61272478), and National Key Scientific and Technological Project (No. 2014ZX01032401-001).

References

1. Kiltz, E., Pietrzak, K.: Leakage Resilient ElGamal Encryption. In: Abe, M. (ed.) ASIACRYPT 2010. LNCS, vol. 6477, pp. 595–612. Springer, Heidelberg (2010)

2. Dziembowski, S., Pietrzak, K.: Leakage-Resilient Cryptography, FOCS 2008, pp. 293–302 (2008)
3. Micali, S., Reyzin, L.: Physically Observable Cryptography. In: Naor, M. (ed.) TCC 2004. LNCS, vol. 2951, pp. 278–296. Springer, Heidelberg (2004)
4. Halderman, J.A., Schoen, S.D., Heninger, N., Clarkson, W., Paul, W., Calandrino, J.A., Feldman, A.J., Appelbaum, J., Felten, E.W.: Lest we remember: cold-boot attacks on encryption keys. *Communications of the ACM - Security in the Browser* 52(5), 91–98 (2009)
5. Mangard, S., Popp, T., Gammel, B.M.: Side-Channel Leakage of Masked CMOS Gates. In: Menezes, A. (ed.) CT-RSA 2005. LNCS, vol. 3376, pp. 351–365. Springer, Heidelberg (2005)
6. Akavia, A., Goldwasser, S., Vaikuntanathan, V.: Simultaneous Hardcore Bits and Cryptography against Memory Attacks. In: Reingold, O. (ed.) TCC 2009. LNCS, vol. 5444, pp. 474–495. Springer, Heidelberg (2009)
7. Naor, M., Segev, G.: Public-Key Cryptosystems Resilient to Key Leakage. In: Halevi, S. (ed.) CRYPTO 2009. LNCS, vol. 5677, pp. 18–35. Springer, Heidelberg (2009)
8. Cash, D.M., Ding, Y.Z., Dodis, Y., Lee, W., Lipton, R.J., Walfish, S.: Intrusion-Resilient Key Exchange in the Bounded Retrieval Model. In: Vadhan, S.P. (ed.) TCC 2007. LNCS, vol. 4392, pp. 479–498. Springer, Heidelberg (2007)
9. Alwen, J., Dodis, Y., Wichs, D.: Leakage-Resilient Public-Key Cryptography in the Bounded-Retrieval Model. In: Halevi, S. (ed.) CRYPTO 2009. LNCS, vol. 5677, pp. 36–54. Springer, Heidelberg (2009)
10. Dodis, Y., Haralambiev, K., López-Alt, A., Wichs, D.: Cryptography against Continuous Memory Attacks. In: FOCS 2010, pp. 511–520 (2010)
11. Lewko, A., Lewko, M., Waters, B.: How to Leak on Key Updates. In: STOC 2011, pp. 725–734 (2011)
12. ANSI X 9.17 (Revised), American National Standard for Financial Institution Key Management (Wholesale). American Bankers Association (1985)
13. National Institute for Standards and Technology, Digital Signature Standard. NIST FIPS PUB 186, U.S. Department of Commerce (1994)
14. Pietrzak, K.: A Leakage-Resilient Mode of Operation. In: Joux, A. (ed.) EUROCRYPT 2009. LNCS, vol. 5479, pp. 462–482. Springer, Heidelberg (2009)
15. Keller, S.S.: NIST-Recommended Random Number Generator Based on ANSI X9.31 Appendix A.2.4 Using the 3-Key Triple DES and AES Algorithms
16. Kelsey, J., Schneier, B., Wagner, D., Hall, C.: Cryptanalytic attacks on pseudorandom number generators. In: Vaudenay, S. (ed.) FSE 1998. LNCS, vol. 1372, p. 168. Springer, Heidelberg (1998)
17. http://www.spms.ntu.edu.sg/Asiacrypt2010/AsiaCrypt_slides/pietrzakAC11.pdf
18. Standaert, F.-X.: How Leaky Is an Extractor? In: Abdalla, M., Barreto, P.S.L.M. (eds.) LATINCRYPT 2010. LNCS, vol. 6212, pp. 294–304. Springer, Heidelberg (2010)
19. Galindo, D., Vivek, S.: Limits of a conjecture on a leakage-resilient cryptosystem. *Information Processing Letters* 114(4), 192–196 (2014)
20. Yu, Y., Standaert, F.-X., Pereira, O., Yung, M.: Practical Leakage-Resilient Pseudorandom Generators. In: CCS 2010 (2010)
21. Dodis, Y., Goldwasser, S., Tauman Kalai, Y., Peikert, C., Vaikuntanathan, V.: Public-Key Encryption Schemes with Auxiliary Inputs. In: Micciancio, D. (ed.) TCC 2010. LNCS, vol. 5978, pp. 361–381. Springer, Heidelberg (2010)

22. Dodis, Y., Kalai, Y.T., Lovett, S.: On Cryptography With Auxiliary Input, STOC2009
23. Menezes, A., van Oorschot, P., Vanstone, S.: Handbook of Applied Cryptography, Ch. 8, p. 296. CRC Press (1996)
24. Clavier, C., Joye, M.: Universal exponentiation algorithm. In: Koç, Ç.K., Naccache, D., Paar, C. (eds.) CHES 2001. LNCS, vol. 2162, pp. 300–308. Springer, Heidelberg (2001)
25. Kocher, P.C.: Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems. In: Koblitz, N. (ed.) CRYPTO 1996. LNCS, vol. 1109, pp. 104–113. Springer, Heidelberg (1996)