Leakage Resilience of the Blom's Key Distribution Scheme*

Michał Jastrzębski** and Stefan Dziembowski***

Institute of Informatics, University of Warsaw

Abstract. We initiate the study of the leakage-resilience of the information-theoretic key distribution schemes. Such schemes, originally proposed in the 1980s, have recently attracted a lot of interest in the systems community. This is because, due to their extreme efficiency, they can be executed on low-cost devices such as sensors, where the use of the public-key cryptography is infeasible. We argue that the study of leakage resilience of such schemes is particularly well-motivated, since, unlike more expensive devices, the sensors (or other similar devices) are unlikely to be physically resilient to leakage.

We concentrate on the classical scheme of Blom (CRYPTO 1982), since it is known to be optimal in a large class of such schemes. We model the leakage as an input-shrinking function. In this settings we show that Blom's scheme is leakage-resilient in a very strong model, where the adversary can (1) compromise completely some nodes in a "standard" way, and (2) leak information *jointly* from the remaining nodes. The amount leakage that we can tolerate can be up to $(0.5 - \epsilon)$ of the total amount of information on the leaking nodes. We also show that this bound is optimal, by providing an attack that breaks the scheme if more leakage is available to the adversary. This attack works even in a weaker model, where the nodes leak information independently.

In the proof we make use of the theory of the randomness extractors. In particular we use the fact that inner product over a finite field is a good 2-source extractor. This is possible since the Blom's scheme is based on the matrix multiplication.

1 Introduction

A recent trend in theoretical cryptography, initiated by [34, 29, 28], is to design schemes that are provably-secure even if implemented on devices

* This work was partly supported by the WELCOME/2010-4/2 grant founded within the framework of the EU Innovative Economy Operational Programme. The European Research Council has provided financial support for this work under the European Community's Seventh Framework Programme (FP7/2007-2013) / ERC grant agreement no CNTM-207908.

** Current affiliation: Google Inc., Zurich, Switzerland.

*** On leave from *Sapienza* University of Rome.

that are not fully trusted. The motivation for this research comes from the fact that, instead of breaking the mathematical foundations of a cryptosystem, in real life it is often much easier to attack its physical implementation. Such "physical attacks" are usually based on the *side-channel information* about the internals of the cryptographic device that the adversary can obtain by measuring its running-time, electromagnetic radiation, power consumption (see e.g. [36]), or even by actively tampering with it (see e.g. [3]) in order to force it to reveal information about its secrets. Practitioners have developed several remedies to these attacks, however, they are usually ad-hoc and lack a formal security argument.

Contrary to the approach taken by the practitioners, security of the constructions developed by the theoreticians is always analyzed formally in a well-defined mathematical model, and hence covers a broad class of attacks, including those that are not yet known, but may potentially be invented in the future. Over the last few years several models for passive and active physical attacks have been proposed and schemes secure in these models have been constructed (see e.g. [29, 24, 28, 19, 38, 1, 14, 31, 35, 20, 22, 7, 13, 22, 30, 10, 18, 6, 23, 26, **?**]). Some of these papers [29, 28, 22, 30, 18, 26] present the so-called *general compilers* i.e. algorithms that transform any cryptographic functionality into a "physically-secure" one. These generic constructions, although very inspiring theoretically, are of a limited practical relevance mostly because of the huge blow-up in the complexity of the computed functionality. In another class of papers the authors develop new schemes for concrete cryptographic task such as stream-ciphers [19, 38], public-key primitives [31, 35, 7, 13, 10, 32], multi-party computation protocols [6] or zero-knowledge schemes [23]. While some of these schemes can be quite efficient, it is unclear if they will ever be used in practice, one of the reasons being that their deployment would require a change in the existing industrial standards.

Therefore an alternative natural approach is to analyze the leakage-resilience of *existing* cryptosystems in order to find among them those that exhibit good leakage-resilience properties. One example of such work is the influential paper of Akavia et al. [1] where the authors show leakage-resilience of the public-key encryption scheme of Regev [40] and the identity-based encryption scheme of Gentry et al. [25]. Another example can be found in [2] where the leakage-resilience of the Okamoto identification scheme [37] is shown and used in a construction of a signature scheme secure in the bounded-retrieval model. The schemes in these examples are computationally secure and we are not aware of any non-trivial exam-

ple of a practical information-theoretically secure scheme whose leakage-resilience has been shown in the literature.

Usually the information-theoretically secure schemes are considered not very practical since, for various reasons, they are cumbersome to use in real-life, the classical example being the one time pad encryption scheme that requires the users to store very large keys. Nevertheless, some of the information-theoretically secure schemes have found practical applications, due to their simplicity and efficiency. One of such examples is the Shamir's secret sharing scheme [42], which is used as a building block for several cryptographic protocols. Another prominent example are the information-theoretically secure *key distribution schemes (KDS)*. The leakage resilience of one of such schemes, namely the classical Blom's scheme [4] is the main topic of this paper. Below we first give a brief introduction to the KDS's and then informally describe our leakage model.

Key Distribution Schemes (KDS) Since currently the main application of the KDS's are the sensor networks we will use the sensor network terminology. We note, however, that the mathematical idea appeared much before the emergence of such networks (Blom's paper was published in 1982), and such schemes have also other applications, one example being the HDCP (High-Bandwidth Digital Content Protection) system created by Intel.

A sensor network consists of a large number m of autonomous devices denoted by natural numbers $1, \ldots, m$. In many cases, sensors are being deployed in hostile environment and are exposed to diverse malicious adversaries. In this case security of communication between nodes becomes essential. Sensors need to be able to communicate directly with each other over encrypted and authenticated channels. Such communication requires that each pair of nodes share a common secret key (which is used by this pair for encryption). After they are deployed, the nodes should communicate without relying on any trusted third party. Therefore, before the deployment, a trusted setup phase, called the *key predistribution*, is executed. Since the sensors have a limited computing power the use of the public-key cryptography is not an option, and the solutions based on the symmetric-key primitives are preferred.

One obvious solution is for each sensor to store the secret key to pair with any other node. In this case the common key of a pair would be secret and known only to the nodes in this pair. This approach is not practical because of the nature of sensors - the devices have limited memory, whereas the total number of stored keys grows quadratically in the

size of the network. Another extreme is to give the same fixed key to every sensor in the network. While this scheme would be very memory efficient its security is quite low, since the adversary who *compromises* just one node, and extracts the key from it, would be able to decrypt the communication between each pair of the not compromised nodes sharing the same key.

Rolf Blom in [4] proposed a key distribution scheme which provides a nice tradeoff between security and memory efficiency. Description of the Blom key distribution scheme as well as its security can be found in Section 2. Informally speaking, the idea of [4] is to fix a number n of nodes that the adversary needs to compromise in order to break the security of the system. More precisely: as long as the number of compromised nodes is smaller than n then the keys shared by any pair of not compromised nodes is unknown to the adversary. The size of the stored information on each sensor is $n \cdot |K|$ bits (where $|K|$ is the length of the key that the sensors establish). Note that Blom's scheme can be viewed as a generalization of the schemes described above: by setting $n = m$ we obtain the scheme with high resilience against compromising of the nodes, but high memory requirements, and by setting $n = 1$ we obtain the other extreme case (low resilience and low memory requirements). For a formal analysis of Blom scheme see e.g. [5], where it is also shown that the Blom's scheme is optimal in terms of the amount of data that the sensors need to store (as a function of n, m and $|K|$). Practical key predistribution schemes were also proposed by Eschenauer and Gligor [21] who construct a scheme where two nodes can establish the common key only with some probability. Other *key predistribution* schemes providing different tradeoffs can be found for instance in [8, 16].

Leakage resilience of the KDS's The sensors that execute the key distribution schemes are supposed to be low-cost, and therefore they cannot be assumed to be leakage-proof, as physical protections against leakages is expensive. Therefore analyzing the side-channel leakage-resilience of the key distribution schemes is particularly well-motivated, and it is natural to pick the Blom's scheme as the first target for this analysis (for its optimality and simplicity). Let us start with the description of our leakage model. As we already mentioned, several models have been proposed for reasoning about the side-channel leakages, for example the early approaches considered the leakages of the individual bits only [12, 29]. In this work we follow a very popular paradigm in which the leakage is modeled as an *input shrinking function*, i.e. a function f whose output is much

shorter than its input (the length of the output of f will be called the *amount of leakage*). Such functions were first proposed in cryptography in the so-called bounded-storage model of Maurer [33]. Later, they were used to define the memory leakage occurring during the virus attacks in the bounded-retrieval model [17, 11, 2]. In the context of the side-channel leakages they were first used in [19] with an additional restriction that the memory is divided into two separate parts that do not leak information simultaneously, and in the full generality in the paper of Akavia et al. [1].

Our contribution In this paper we use the model of Akavia et al. i.e. we do not impose any restrictions on the input of the leakage function, except that we require only that the size of its output is bounded. Several other papers in this model, already mentioned in the introduction, have been published in recent years. A popular tool that is used in these works are the randomness extractors (see e.g. [41]). Since some of these extractors are based on linear algebra (in particular the famous inner product extractor of Chor and Goldreich [9]) hence the Blom's scheme, which itself uses the matrix multiplication, seems to be a promising candidate for a leakage-resilient key distribution scheme. We confirm this intuition in this paper.

More precisely, but still informally, we show that the Blom's scheme is leakage-resilient in the following sense. In our model we allow the adversary to both perform the standard "non-leakage" attacks (i.e. to compromise the nodes) and to leak from the uncompromised nodes[1]. Recall that $n-1$ is the maximal number of nodes that the adversary can compromise while attacking the scheme *without* leakage. In order to show the leakage-resilience we will now treat n as a security parameter and allow the adversary to compromise significantly less nodes than $n-1$. Let $j \leq n-1$ denote the number of nodes that the adversary actually compromised. It turns out (cf. Theorem 2) that if j is close to $n-1$ than the leakage-resilience of the Blom's scheme is very low. In particular if $j = n-1$ then the scheme can be broken with leaking just $|K|$ bits from the uncompromised nodes, and in general Blom's scheme can be broken in with leakage of size that is $\approx 0.5(n-j)^2 \cdot |K|$. Therefore we assume that $n-j$ is linear in n. Under this assumption we show (Theorem 1) that the key established between a pair of nodes, 1 and 2, say, remains secret even if the adversary (additionally to the information that he got by compromising the nodes) learns the value of the leakage function f on the concatenation of the internal data of all the other nodes. The maximal

[1] For simplicity of the notation in our formal model the leakage function is in fact also applied to the compromised nodes.

amount of leakage (i.e. the length of the output of f) that we can tolerate is at most $c(n-j)^2 \cdot |K|$, where c can be any constant such that $c < 0.5$. A small caveat is that the leakage function cannot depend on the identifiers[2] of the sensors 1 and 2, and hence in this sense it is non-adaptive.

Traditionally, the leakage resilience of the cryptographic schemes is measured in terms of the *relative leakage* λ that they can tolerate, which is defined as the ratio between the length of the output and the input of the leakage function. In order to talk in these terms let us assume that the parameter n is linear in m, i.e. there exists a constant α such that $n = \alpha m$. Our Theorem 1 implies (cf. Corollary 1) that the maximal achievable value of λ depends on the fraction γ of compromised nodes in the following way: $\lambda \leq c \cdot (\alpha - \gamma)^2/\alpha$ (where c is any constant such that $c < 0.5$). Hence, e.g., if the adversary did not compromise any node then λ can be close to 0.5, if we choose α close to 1.

As highlighted above we also prove that the bound given in Theorem 1 is optimal by showing an attack that uses leakage of size $\approx 0.5(n-j)^2 \cdot |K|$. This attack actually works in a weaker model, where the sensors leak information independently, i.e. separate leakage function is applied to each sensor and the restriction on the leakage size concerns the sum of the lengths of the outputs of these functions (cf. Definition 3). The leakage functions in this attack can be chosen in advance, however they need to adaptively depend on the identifiers of the sensors, hence we call it an *adaptive model*. In Section 8 we show an even weaker attack (with slightly worse bounds) when the adversary does not even need to adaptive in the sense that the leakage functions do not depend on the identifiers of the sensors.

Before we present our contribution in detail we first describe formally (in Section 2) the Blom scheme and its security in the standard model without leakages. Then, in Section 3 we incorporate leakage into this model. Our main results are stated in Section 4 and their proofs are given in Sections 5-6.

2 Blom's key distribution scheme

In this section we give a formal definition of the Blom's scheme that was already informally introduced in Section 1. Let $\mathbb{F}$ denote some finite field (for instance $GF(p)$), $\mathbb{M}_n(\mathbb{F})$ and $\mathbb{S}_n(\mathbb{F})$ will denote respectively the set of all matrices and symmetric matrices of size $n \times n$ over field $\mathbb{F}$. If m is

[2] In the Blom's scheme every node i has its *identifier* i that is chosen randomly and is used by the other nodes to compute the keys for communicating with i.

the size of the network (number of sensors participating in the protocol), then the scheme will be parametrized by n being a security parameter indicating the number of nodes which needs to get compromised before the adversary is able to break the scheme. The protocol setup requires that all secrets are being predistributed before the network is deployed. To formalize, the protocol setup for an $(\mathbb{F}, n, m)$-*Blom scheme* (for the network size m and security parameter n) works as follows

- Central server selects publicly known identifiers $x_1, \ldots, x_m$, where each $x_i \in \mathbb{F}^n$. Nodes are labeled $1, 2, \ldots, m$ so that x_i is the identifier of the node i. Next, server chooses uniformly at random as symmetric matrix $R \in \mathbb{S}_n(\mathbb{F})$. The matrix is kept secret and will be destroyed after this step. The secret stored on device i consists of value $Rx_i \in \mathbb{F}^n$. After this step each node is associated with two values

  $$(x_i, Rx_i)$$

  where x_i is publicly known and Rx_i is kept secret. The network is deployed.
- If nodes i and j wish to establish a shared key, then i computes $x_j^T(Rx_i)$, whereas j computes $x_i^T(Rx_j)$.

  The symmetry of R assures that

  $$x_i^T R x_j = (x_i^T R x_j)^T = x_j^T R^T x_i = x_j^T R x_i$$

which guarantees that computed keys match on both sides of the channel.

It can be proven that if every n of the identifiers $x_1, \ldots, x_m$ are linearly independent, then the adversary compromising any $n-1$ of the nodes (apart from i and j of course), cannot determine the secret key which would be computed by nodes i and j. Moreover, such an adversary cannot gain any knowledge on this key. More formally, we can show [4] that

$$H(x_i^T R x_j | \text{secrets of } n-1 \text{ nodes}) = H(x_i^T R x_j)$$

where $H(\cdot)$ and $H(\cdot|\cdot)$ denote respectively the entropy and conditional entropy of a random variable. Formal proofs and extensions to conference keys can be found, for instance, in [5]. In practical applications, to ensure this notion of security, identifiers can be chosen as columns from a Vandermonde matrix (for definitions, consult for instance [27]). In this paper we will assume that the identifiers are simply uniformly and independently at random from $\mathbb{F}^n$. This, of course, can generate problems if, by accident, the selected identifiers are not linearly independent. Fortunately, the probability that this happens will be negligible and will disappear under the asymptotic notation.

3 Leakage attacks on the Blom's scheme

Consider a regular Blom scheme described in the previous chapter which is determined by $\mathbb{F}$, n and m being respectively the finite field, dimension of the random symmetric matrix and the number of participants. Matrix R is randomly chosen from $\mathbb{S}_n(\mathbb{F})$. Participants are receiving publicly known random identifiers $x_1, \ldots, x_m \in \mathbb{F}^n$ as well as secrets of the form Rx_i. The adversary wants to find the common key of two nodes. To simplify the exposition let us assume that these nodes are always 1 and 2, and therefore the key between them is $x_1^T Rx_2 = x_2^T Rx_1$.

In our work, we will consider the scheme in a general framework of the memory leakage. We allow the adversary to chose any function f and apply it to the secrets $Rx_3, \ldots, Rx_m$ giving $f(Rx_3, \ldots, Rx_m)$. The function f models an arbitrary memory leakage or an eavesdropping device which can be used on stored secrets. It is worth noticing that compromising several nodes is just a simple sub-case of the leakage function. Our results show that if the size of the image of f is *small enough*, the distribution of $x_1^T Rx_2$ conditioned on the value of f is *close* to the uniform.

We wish to make our adversary adaptive, which means that it would choose the leakage function f based on the publicly known identifiers. Note that it is impossible to consider the leakage model when an adversary would be able to choose f based on all the identifiers, namely $x_1, \ldots, x_m$. Indeed, in this case, if $m > n + 2$, f could just compute R based on $Rx_3, \ldots, Rx_m$ and output $x_1^T Rx_2$. Size of the image of f equals $|\mathbb{F}|$ and completely compromises the protocol, which is unacceptable. Instead, we will allow an adversary to chose f based on $x_3, \ldots, x_m$.

A part from the model in which the function f operates simultaneously on $Rx_3, \ldots, Rx_m$ we would consider the leakage model in which the adversary is choosing functions $f_3, \ldots, f_m$ operating respectively on $Rx_3, \ldots, Rx_m$. It seems that such an adversary would be significantly weaker then the one using the joint function. Our results show that it is not the case. We will also consider the non-adaptive adversary which needs to choose f before identifiers are being set up.

Our security models are incorporating both the notion of regular sensor compromising (as considered in the usual security analysis of the Blom scheme) as well as leakage functions. Next sections provide detailed descriptions of our security definitions in terms of games between an *adversary* $\mathcal{A}$ and an *oracle* Ω.

Notation For a random variable X we would define its support as $\mathrm{supp}(X) := \{x : \mathbb{P}(X = x) > 0\}$. We will also need a notion of *min-entropy* $H_\infty(X) := \min_{x \in \mathrm{supp}(X)} - \log(\mathbb{P}(X = x))$. Statistical distance is defined as $\Delta(X;Y) := \frac{1}{2}\sum_x |\mathbb{P}(X = x) - \mathbb{P}(Y = x)|$. By a distance to uniform distribution, conditioned on a random variable we will understand $d(X|Y) := \sum_x \mathbb{P}(Y = x) \cdot d(X|Y = x)$ where $d(X) := \Delta(X;U)$ for U uniform independent on X.

Strong adaptive adversary (joint leakage) Fix some parameters n, m, j, k and the finite field $\mathbb{F}$. There are m participants in the protocol. Consider the following game between the oracle Ω and the adversary $\mathcal{A}$.

1. $\mathcal{A}$: The adversary chooses j nodes among $3, 4, \ldots, m$ which we will call compromised. We may assume that the nodes chosen by an adversary are numbered $3, 4, \ldots, j + 2$.
2. Ω: The oracle chooses $R \in \mathbb{S}_n(\mathbb{F})$ uniformly at random. Oracle chooses $x_1, \ldots, x_m$ from $\mathbb{F}^n$ independently uniformly at random. Values of $x_3, \ldots, x_m$ are sent to $\mathcal{A}$.
3. $\mathcal{A}$: The adversary chooses a function $f : \mathbb{F}^{n(m-2)} \to \{1, \ldots, |\mathbb{F}|^k\}$
4. Ω : The oracle sends to the adversary x_1, x_2 as well as $Rx_3, \ldots, Rx_{j+2}$ (secrets from compromised nodes) and $f(Rx_3, \ldots, Rx_m)$

Observe that, in order to simplify the notation, we measure the size of the leakage not in terms of bits but in terms of the field elements and the function f can also be viewed as having a type $f : \mathbb{F}^{n(m-2)} \to \{0,1\}^{k \log_2 |F|}$. For an adversary $\mathcal{A}$, by $View^{\mathcal{A}}$ we will denote the vector of values of all random variables which were observed by the adversary during its game with the oracle

Definition 1. *We say that the* $(\mathbb{F}, n, m)$*-Blom scheme is* strongly (j, k, ϵ)-secure *if for any Adversary* $\mathcal{A}$ *in the game above we have that*

$$d(x_1^T R x_2 | View^{\mathcal{A}}) \leq \epsilon.$$

Weak adaptive adversary (separate leakages) The setting is the same as in the strong adversary model. The difference between this model and the strong one is in Steps 3 and 4:

3. $\mathcal{A}$: Adversary chooses a functions $f_3, \ldots, f_m$ such that $f_i : \mathbb{F}^n \to \{1, 2, \ldots, |\mathbb{F}|^{k_i}\}$ where $k_3 + \cdots + k_m \leq k$

4. Ω : Oracle sends to the adversary x_1, x_2 as well as $Rx_3, \ldots, Rx_{j+2}$ (secrets from compromised nodes) and $f_3(Rx_3), \ldots, f_m(Rx_m)$

Definition 2. *We say that* $(\mathbb{F}, n, m)$*-Blom scheme described above is* weakly (j, k, ϵ)-secure *if for any Adversary* $\mathcal{A}$ *in the game above we have that*

$$d(x_1^T R x_2 | View^{\mathcal{A}}) \leq \epsilon.$$

4 Our results

In this section we state our main security results.

Theorem 1. *For every* n *consider a* $(\mathbb{F}, n, m)$*-Blom scheme and* $j(n)$ *and* $k(n)$ *such that* $n - j(n) = \Omega(n)$*. Let* $c < 0.5$ *be an arbitrary constant. If* $k(n) \leq c(n - j(n))^2$ *then the scheme is strongly* $\left(j(n), k(n), |\mathbb{F}|^{-\Omega(n)}\right)$*-secure. Moreover the constant hidden in* $\Omega(n)$ *does not depend on* $|\mathbb{F}|$*.*

The proof of this theorem is presented in Section 6 and the main technical machinery is developed in Section 5. Observe that the leakage resilience (measured by the parameters $j(n), k(n)$ and $|\mathbb{F}|^{-\Omega(n)}$) does not depend on the number of the parties, but only on the difference between the parameters n and $j(n)$. Traditionally, the leakage resilience of a scheme is measured in terms of the relative size λ of the leakage with respect to the total size of data that can leak, which in our case is $n(m-2)$. The following corollary of Theorem 1 serves for interpreting our result in this way. We will assume that there exists a constant α such that $n = \alpha m$, in other words: the security parameter (and hence the size of the data stored by each node) is linear in the number of sensors.

Corollary 1. *Let* $\lambda, \gamma, \alpha \in [0, 1]$ *and* $c < 0.5$ *be constants such that*

$$\lambda \leq \frac{c \cdot (\alpha - \gamma)^2}{\alpha}, \tag{1}$$

and let $\mathbb{F}$ *be an arbitrary finite field. Then for every* m *the* $(\mathbb{F}, n, m)$*-Blom scheme (with* $n = \alpha m$*) is* $(\gamma \cdot m, \lambda \cdot n(m-2), |\mathbb{F}|^{-\Omega(n)})$*-secure.*

Proof. Let $j := \gamma \cdot m$ and $k = \lambda \cdot n(m-2)$. It is a straightforward calculation that $k \leq c(n - j(n))^2$. Hence, by Theorem 1, the corollary is true. □

The corollary implies that, as long as the number j of compromised nodes is a constant fraction of the total number of nodes, we can tolerate a constant relative leakage λ with respect to the total size of the data.

Observe that in the extreme case when no parties are compromised we have $\gamma = 0$, and hence λ is at most $c\alpha \approx \alpha/2$, which, for α close to 1, means that the relative leakage can be close to 0.5.

As mentioned in the introduction, the parameters obtained in Theorem 1 are optimal. Indeed, even if we pass to the *weak model*, the adversary can fully compromise the protocol for $k(n) \approx |\mathbb{F}|^{0.5(n-j(n))^2}$. To formalize, we can prove the following.

Theorem 2. *For every n consider a $(\mathbb{F}, n, m)$-Blom scheme and n and $k(n)$ such that $k(n) = 0.5(n - j(n))(n - j(n) + 1)$. Such scheme is not* weakly $(j(n), k(n), \epsilon)$-secure *for any $\epsilon < 0.1$.*

The proof appears in the full version of this paper [**?**]. Theorems 1 and 2 show together, that two considered *adaptive* models, namely models with *joint* and *separate* leakages can be considered as equivalent in terms of asymptotic security. This means that allowing the adversary to compute leakage function "mixing" the secrets stored at different nodes, gives him no significant advantage over the model in which we allow only to leakages from separate nodes. This may be viewed as counterintuitive, as one may expect that *joint leakage* model would allow to significantly reduce the leakage size necessary to compromise the protocol. The main technical tool that we use to prove Theorem 1 is the lemma that appears in the next section.

5 The main technical lemma

Lemma 1. *Let X, Y be independent random vectors uniformly distributed over $\mathbb{F}^n$. If R is a random matrix uniformly distributed among* $\mathrm{supp}(R) \subset \mathbb{M}_n(\mathbb{F})$ *and independent of (X, Y), then for an arbitrary function $f : \mathbb{M}_n(\mathbb{F}) \to \{1, \ldots, |\mathbb{F}|^k\}$ we have that*

$$d(X^T RY | X, Y, f(R)) \leq |\mathbb{F}|^{u-n+1} + \frac{|\mathbb{F}|^{k/8n}}{|\mathrm{supp}(R)|^{1/8n}} |\mathbb{F}|^{(n-u+7)/2}$$

for any $u < n$

One may be tempted to think about this fact as a simple corollary from leftover hash lemma (LHL), because we can treat the variable $X^T RY$ as coming from a family of hash functions $H_{(x,y)}(R) = x^T Ry$ indexed by random choice of (x, y). It turns out that this is not the case since this hash family is only about $2/|\mathbb{F}|$ - almost universal which does not allow us to use the LHL. Trying modifications of the LHL proof using, for instance,

conditioning on the rank of the random matrix R also does not seem to provide sufficiently good estimates.

Before we present our proof we need some technical tools. We start with the useful notion of an inner product extractor, then develop linear algebra lemmas and finally move towards the core of the proof.

5.1 Strong two source extractors [9]

Definition 3. *We will call a function* $\mathrm{Ext} : \mathbb{F}^n \times \mathbb{F}^n \to \mathbb{F}$ *a* strong (k_1, k_2, ϵ)-two-source extractor *if and only if for any independent random variables* X, Y *in* $\mathbb{F}^n$ *such that* $H_\infty(X) \geq k_1$ *and* $H_\infty(Y) \geq k_2$ *we have*

$$d(\mathrm{Ext}(X, Y)|X) \leq \epsilon.$$

If X and Y are random vectors in $\mathbb{F}^n$, then recall that by $X^T Y$ we will denote the regular dot product of vectors X and Y. For $\mathrm{Ext}(X, Y) = X^T Y$, [15] provides a simple proof of the bound on ϵ for $|\mathbb{F}| = 2$. This result can be extended to an arbitrary finite field $\mathbb{F}$ and follows easily from the work of [39].

Theorem 3 ([39]). ***(Inner product extractor)*** *The function* $\mathrm{Ext} : \mathbb{F}^n \times \mathbb{F}^n \to \mathbb{F}$ *defined as* $\mathrm{Ext}(X, Y) = X^T Y$ *is a strong* $(k_X, k_Y, |\mathbb{F}|(2^{u-k_X} + |\mathbb{F}|^{(n+1)/2} 2^{-(u+k_Y)/2}))$*-two source extractor for any* $u \leq k_X$.

5.2 Linear algebra tools

This section develops linear algebra tools ending with a following combinatorial lemma which is crucial for the proof of our results.

Lemma 2. *Let* $\{\mathcal{M}_v\}_{v \in \mathbb{F}^n}$ *be any family of subsets of* $\mathbb{M}_n(\mathbb{F})$ *satisfying*

$$\forall_{v \in \mathbb{F}^n} \forall_{M_1, M_2 \in \mathcal{M}_v} M_1 v = M_2 v.$$

Then

$$\sum_{v \in \mathbb{F}^n} |\mathcal{M}_v| \leq |\mathbb{F}|^4 \cdot |\mathbb{F}|^n \cdot \left| \bigcup_{v \in \mathbb{F}^n} \mathcal{M}_v \right|^{1 - 1/4n}.$$

Lemma 2 shows that sets $\mathcal{M}_v$, $v \in \mathbb{F}^n$ must be overlapping *considerably* compared to $|\bigcup \mathcal{M}_v|$. Technical proof of this lemma appears in the full version of this paper [**?**].

5.3 Proof of Lemma 1

Let us recall that we have set an integer n and an arbitrary function $f : \mathbb{M}_n(\mathbb{F}) \to \{1, 2, \ldots, |\mathbb{F}|^k\}$ for some k. We are given independent random variables X, Y, R such that X, Y are uniformly random vectors from $\mathbb{F}^n$ and R is random matrix chosen uniformly at random from $\mathrm{supp}(R) \subset \mathbb{M}_n(\mathbb{F})$. Let us define

$$\mathcal{M}_i = \{M \in \mathrm{supp}(R) : f(M) = i\}.$$

and note that $\sum_i |\mathcal{M}_i| = |\mathrm{supp}(R)|$. Also, let $|R| := |\mathrm{supp}(R)|$. We wish to estimate

$$\begin{aligned} & d(X^T RY | X, Y, f(R)) \\ = & \underbrace{\sum_i \left(\mathbb{P}(R \in \mathcal{M}_i) \sum_{y \in \mathbb{F}^n} \mathbb{P}(Y = y) d\left(X^T Ry \middle| X, Y = y, R \in \mathcal{M}_i \right) \right)}_{(*)} \end{aligned}$$

For a fixed y and $\mathcal{M}_i$ we may look at

$$d\left(X^T Ry \middle| X, Y = y, R \in \mathcal{M}_i \right)$$

as an inner product extraction from independent random variables X and Ry, conditioned on event that $\{R \in \mathcal{M}_i, Y = y\}$. By $H^i_\infty(y)$ we will denote

$$H^i_\infty(y) := H_\infty(Ry | R \in \mathcal{M}_i).$$

Of course $H_\infty(X) = n \log(|\mathbb{F}|)$. Let us fix some $u < n \log(|\mathbb{F}|)$. Using independency of X, Y, R, Theorem 3 concerning inner product extraction gives us

$$d\left(X^T Ry \middle| X, Y = y, R \in \mathcal{M}_i \right) \leq |\mathbb{F}| \left(\frac{2^u}{|\mathbb{F}|^n} + |\mathbb{F}|^{(n+1)/2} 2^{-(u + H^i_\infty(y))/2} \right)$$

Pluging this estimation into $(*)$ gives us

$$
\begin{aligned}
(*) &\leq |\mathbb{F}| \cdot \frac{2^u}{|\mathbb{F}|^n} + \sum_i \left(\mathbb{P}(R \in \mathcal{M}_i) \sum_{y \in \mathbb{F}^n} \mathbb{P}(Y = y) |\mathbb{F}|^{(n+3)/2} 2^{-(u + H^i_\infty(y))/2} \right) \\
&\leq |\mathbb{F}| \cdot \frac{2^u}{|\mathbb{F}|^n} + \frac{|\mathbb{F}|^{-n}}{|R|} \sum_i \left(|\mathcal{M}_i| \sum_{y \in \mathbb{F}^n} |\mathbb{F}|^{(n+3)/2} 2^{-(u + H^i_\infty(y))/2} \right) \\
&= |\mathbb{F}| \cdot \frac{2^u}{|\mathbb{F}|^n} + \frac{|\mathbb{F}|^{-n}}{|R|} |\mathbb{F}|^{(n+3)/2} 2^{-u/2} \sum_i \left(|\mathcal{M}_i| \sum_{y \in \mathbb{F}^n} 2^{-H^i_\infty(y)/2} \right) \qquad (2)
\end{aligned}
$$

Let us focus on estimating the term $\sum_i \left(|\mathcal{M}_i| \sum_{y \in \mathbb{F}^n} 2^{-H^i_\infty(y)/2} \right)$. We will use the following Holder inequality

$$
\sum_i^r x_i^\alpha \leq r^{1-\alpha} \left(\sum_i^r x_i \right)^\alpha \qquad (3)
$$

valid for any $0 < \alpha < 1$ and $x_i > 0$. Definition of $H^i_\infty(y)$ and Lemma 2 yield

$$
\begin{aligned}
&\sum_i \left(|\mathcal{M}_i| \sum_{y \in \mathbb{F}^n} 2^{-H^i_\infty(y)/2} \right) \\
&= \sum_i \left(|\mathcal{M}_i| \sum_{y \in \mathbb{F}^n} \sqrt{\max_{z \in \mathbb{F}^n} \mathbb{P}(Ry = z | R \in \mathcal{M}_i)} \right) \\
&= \sum_i \left(\sqrt{|\mathcal{M}_i|} \sum_{y \in \mathbb{F}^n} \sqrt{\max_{z \in \mathbb{F}^n} |\{R : Ry = z\} \cap \mathcal{M}_i|} \right) \\
&\leq |\mathbb{F}|^{n/2} \sum_i \left(\sqrt{|\mathcal{M}_i|} \cdot \sqrt{\sum_{y \in \mathbb{F}^n} \max_{z \in \mathbb{F}^n} |\{R : Ry = z\} \cap \mathcal{M}_i|} \right) \qquad (4) \\
&\leq |\mathbb{F}|^n |\mathbb{F}|^2 \sum_i \left(|\mathcal{M}_i|^{1 - 1/8n} \right) \qquad (5) \\
&\leq |\mathbb{F}|^n |\mathbb{F}|^2 |\mathbb{F}|^{k/8n} |R|^{1 - 1/8n} \qquad (6)
\end{aligned}
$$

Inequalities (5) and (7) come from applying (4) for $\alpha = 1/2$ and $\alpha = 1 - 1/8n$ respectively. Estimation in (6) can be deduced by applying Lemma 2

to receive that

$$\sum_{y\in\mathbb{F}^n}\max_{z\in\mathbb{F}^n}|\{R:Ry=z\}\cap\mathcal{M}_i|\leq|\mathbb{F}|^4|\mathbb{F}|^n|\mathcal{M}_i|^{1-1/4n}$$

Plugging obtained inequality (7) into (3) we receive

$$\begin{aligned}d(X^TRY|X,Y,f(R))&\leq|\mathbb{F}|\frac{2^u}{|\mathbb{F}|^n}+\frac{|\mathbb{F}|^{-n}}{|R|}\mathbb{F}^{(3n+7)/2}2^{-u/2}|\mathbb{F}|^{k/8n}|R|^{1-1/8n}\\&=2^u|\mathbb{F}|^{-n+1}+\frac{|\mathbb{F}|^{k/8n}}{|\mathrm{supp}(R)|^{1/8n}}2^{-u/2}|\mathbb{F}|^{(n+7)/2}\end{aligned}$$

for any $u\leq n\log|\mathbb{F}|$, which completes the proof with substitution $u:=u/\log|\mathbb{F}|$.

□

6 Proof of Theorem 1

Theorem 1 can be seen as a corollary from Lemma 1. We will need a following lemma, counting the number of symmetric matrices given its values on a chosen set of vectors.

Lemma 3. *Let $c_1,c_2,\ldots,c_j$ and $v_1,v_2,\ldots,v_j$ be vectors such that $c_i\in\mathbb{F}^n$, $v_i\in\mathbb{F}^n$ and $j\leq n$. In this setting, either*

$$\{M\in\mathbb{S}_n(\mathbb{F}):\forall_i Mv_i=c_i\}=\emptyset$$

or

$$|\{M\in\mathbb{S}_n(\mathbb{F}):\forall_i Mv_i=c_i\}|\geq|\mathbb{F}|^{(n-j)(n-j+1)/2}$$

Proof. The size of such set is minimal for $v_1,\ldots,v_j$ being linearly independent which we will assume from this point. We are able to choose vectors $v_{j+1},\ldots,v_n$ so that $v_1,\ldots,v_n$ form a basis of $\mathbb{F}^n$. To uniquely determine M it is enough to set $Mv_{j+1},\ldots,Mv_n$. Note, that

$$M\in\mathbb{S}_n(\mathbb{F})\iff\forall_{a,b}:v_a^TMv_b=v_b^TMv_a.$$

This means, that if there exist $a,b\leq j$ such that $v_a^Tc_b\neq v_b^Tc_a$ then we fall into the first case of our lemma. Otherwise, Mv_{j+1} can be set into one of $|\mathbb{F}|^{n-j}$ ways. Indeed, $c_{j+1}:=Mv_{j+1}$ must fulfill $v_a^Tc_{j+1}=v_{j+1}^Tc_a$ for all $a<j+1$, which gives us a linear space of dimension $n-j$. Similarly, having set c_{j+1}, the value $c_{j+2}:=Mv_{j+2}$ can be set into one of $|\mathbb{F}|^{n-j-1}$ possibilities, etc. In total we receive $|\mathbb{F}|^{(n-j)+(n-j-1)+\ldots+1}$ possibilities of choosing M which completes the proof.

□

Proof (of Theorem 1). Proving the Theorem 1 is equivalent to estimating

$$d\left(X_1^T R X_2 \middle| X_1, \ldots, X_m, RX_3, \ldots, RX_{j+2}, f(X_3, \ldots, X_m, RX_3, \ldots, RX_m)\right) \tag{7}$$

where $X_1, \ldots, X_m$ are m independent random vectors from $\mathbb{F}^n$, R is a random matrix from $\mathbb{S}_n(\mathbb{F})$ independent on $(X_1, \ldots, X_m)$ and f has a type $\mathbb{F}^{n(m-2)+n(m-2)} \to \mathbb{F}^k$. Denote (**??**) with D.

$X_1, \ldots, X_m$ are random variables denoting identifiers attached to participants. Values of $RX_3, \ldots, RX_{j+2}$ come from fully compromised nodes. One may easily observe that the statistical distance described above indeed corresponds to our model, as allowing the adversary to adapt to $X_3, \ldots, X_m$ is equivalent to increasing the number of arguments of function f.

Assume that we have set $m-2$ vectors $x_3, x_4, \ldots, x_m$, $x_i \in \mathbb{F}^n$. To shorten notation, $R(c_3, \ldots, c_{j+2})$ will denote the event $\{Rx_3 = c_3, \ldots, Rx_{j+2} = c_{j+2}\}$. Define $D(x_3, \ldots, x_m)$ to be equal to

$$d\left(X_1^T R X_2 \middle| X_1, X_2, Rx_3, \ldots, Rx_{j+2}, f(x_3, \ldots, x_m, Rx_3, \ldots, Rx_m)\right).$$

Obviously, this is equal to

$$\sum_{(c_3,\ldots,c_{j+2}) \in \mathbb{F}^{jn}} \mathbb{P}(R(c_3, \ldots, c_{j+2})) \cdot d\left(X_1^T R X_2 \middle| X_1, X_2, f(x_3, \ldots, x_m, Rx_3, \ldots, Rx_m), R(c_3, \ldots, c_{j+2})\right)$$

Lemma 6 implies, that for any $c_3, \ldots, c_{j+2}$, we receive

$$|\{a : \mathbb{P}(R = a | R(c_3, \ldots, c_{j+2})) > 0\}| = 0$$

or

$$|\{a : \mathbb{P}(R = a | R(c_3, \ldots, c_{j+2})) > 0\}| \geq |\mathbb{F}|^{(n-j)(n-j+1)/2}.$$

Also, computing $f(x_3, \ldots, x_m, Rx_3, \ldots, Rx_m)$ is equivalent to computing $g(R)$ for some $g : \mathbb{M}_n(\mathbb{F}) \to \mathbb{F}^k$. Using Lemma 1 we obtain

$$D(x_3, \ldots, x_m) \leq |\mathbb{F}|^{u-n+1} + |\mathbb{F}|^{k/8n-(n-j)(n-j+1)/16n} |\mathbb{F}|^{(n-u+7)/2}.$$

Averaging over $x_3, \ldots, x_m$ results in the same estimation for D :

$$D \leq |\mathbb{F}|^{u-n+1} + |\mathbb{F}|^{k/8n-(n-j)(n-j+1)/16n} |\mathbb{F}|^{(n-u+7)/2}.$$

Plugging $k = c(n-j)^2$ leads us to

$$D \leq |\mathbb{F}|^{u-n+1} + |\mathbb{F}|^{7/2} \exp\left\{\log(|\mathbb{F}|)\left(\frac{n-u}{2} + \frac{(2c-1)(n-j)^2}{16n}\right)\right\}$$

As $n - j(n) = \Omega(n)$, there is a constant j_0 such that $n - j(n) \geq j_0 n$, which gives

$$D \leq |\mathbb{F}|^{u-n+1} + |\mathbb{F}|^{7/2} \exp\left\{\log(|\mathbb{F}|)\left(\frac{n-u}{2} - \frac{(1-2c)j_0^2 n}{16}\right)\right\}$$

By an arbitrary choice of $u < n$ we obtain $D = |\mathbb{F}|^{-\Omega(n)}$.

□

7 An even weaker adversary

As described in Section 1 we can weaken our adversary even more (with respect to the one in the proof on Theorem 2), and the negative result will still hold (with slightly worse parameters). The definition of this new weaker model follows.

Weak non-adaptive adversary (separate leakages) The setting and the security definition is the same as in the weak adaptive model (cf. Definition 3). This only difference is that in this case the adversary will not adapt to $x_3, \ldots, x_m$. More precisely, the security game is as follows:

1. $\mathcal{A}$: Adversary chooses j nodes among $3, 4, \ldots, m$ which we will call compromised. We may assume that the nodes chosen by an adversary are numbered $3, 4, \ldots, j+2$. Adversary chooses functions $f_3, \ldots, f_m$ such that $f_i : \mathbb{F}^n \to \{1, 2, \ldots, |\mathbb{F}|^{k_i}\}$ where $k_3 + \cdots + k_m \leq k$
2. Ω: Oracle chooses $R \in \mathbb{S}_n(\mathbb{F})$ uniformly at random. Oracle chooses $x_1, \ldots, x_m$ from $\mathbb{F}^n$ independently uniformly at random. Oracle sends to the adversary $x_1, x_2, x_3, \ldots, x_m$ as well as $Rx_3, \ldots, Rx_{j+2}$ (secrets from compromised nodes) and $f_3(Rx_3), \ldots, f_m(Rx_m)$

Definition 4. *We say that* $(\mathbb{F}, n, m)$ *scheme described above is* weakly non-adaptively (j, k, ϵ)-secure *if for any Adversary* $\mathcal{A}$ *in the game above we have*

$$d(x_1^T R x_2 | View^{\mathcal{A}}) \leq \epsilon.$$

Theorem 4. *For every* n *consider a* $(\mathbb{F}, n, m)$*-Blom and* $j(n)$ *and* $k(n)$ *such that* $k(n) = 0.5(n - j(n))(n - j(n) + 1)$*. Such scheme is is not weakly non-adaptively* $(j(n), k(n), \epsilon)$*-secure for any* $\epsilon < 0.5(1 - 1/|\mathbb{F}|)^{n-1}$

Proof of this theorem can be found in a full version of this paper [**?**].

In fact, in proofs of Theorem 2 as well as Theorem 4 we are *explicitly* constructing adversaries breaking the scheme with probabilities as indicated in statements. Obtained result would suggest that the scheme in the non-adaptive model cannot be yet considered as *compromised*, as $(1-1/|\mathbb{F}|)^{n-1}$ for growing n tends exponentially to 0. Note, however, that this term is strongly dependent on $|\mathbb{F}|$ (as we already mentioned, this is not the case in Theorem 1). In fact, for practical consideration, if we would take $|F| \approx 2 \cdot 10^9$, (32-bit integers) then even for very large $n \approx 2 \cdot 10^9$ we have

$$(1 - 1/|\mathbb{F}|)^{n-1} \approx 1/e$$

which allows us to treat this error as constant for practical applications. Thus, we may say that the leakage of size $k(n) \approx 0.5(n - j(n))^2$ compromises the protocol in practical setting and demonstrates that in practice *non-adaptive* and *adaptive* models are also equivalent in terms of security.

References

1. Adi Akavia, Shafi Goldwasser, and Vinod Vaikuntanathan. Simultaneous hardcore bits and cryptography against memory attacks. In *Theory of Cryptography, 6th Theory of Cryptography Conference, TCC 2009, San Francisco, CA, USA, March 15-17, 2009. Proceedings*, Lecture Notes in Computer Science, pages 474–495. Springer, 2009.
2. Joël Alwen, Yevgeniy Dodis, and Daniel Wichs. Leakage-resilient public-key cryptography in the bounded-retrieval model. In Shai Halevi, editor, *Advances in Cryptology - CRYPTO 2009, 29th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 16-20, 2009. Proceedings*, volume 5677 of *Lecture Notes in Computer Science*, pages 36–54. Springer, 2009.
3. R. Anderson and M. Kuhn. Tamper resistance - a cautionary note. In *The Second USENIX Workshop on Electronic Commerce Proceedings*, November 1996.
4. Rolf Blom. Non-public key distribution. In David Chaum, Ronald L. Rivest, and Alan T. Sherman, editors, *Advances in Cryptology: Proceedings of CRYPTO '82, Santa Barbara, California, USA, August 23-25, 1982*, pages 231–236. Plenum Press, New York, 1982.
5. Carlo Blundo, Alfredo De Santis, Amir Herzberg, Shay Kutten, Ugo Vaccaro, and Moti Yung. Perfectly secure key distribution for dynamic conferences. *Inf. Comput.*, 146(1):1–23, 1998.
6. Elette Boyle, Shafi Goldwasser, and Yael Tauman Kalai. Leakage-resilient coin tossing. In David Peleg, editor, *Distributed Computing - 25th International Symposium, DISC 2011, Rome, Italy, September 20-22, 2011. Proceedings*, volume 6950 of *Lecture Notes in Computer Science*, pages 181–196. Springer, 2011.
7. Zvika Brakerski, Yael Tauman Kalai, Jonathan Katz, and Vinod Vaikuntanathan. Overcoming the hole in the bucket: Public-key cryptography resilient to continual memory leakage. In *51th Annual IEEE Symposium on Foundations of Computer Science, FOCS 2010, October 23-26, 2010, Las Vegas, Nevada, USA*, pages 501–510. IEEE Computer Society, 2010.

8. Haowen Chan, Adrian Perrig, and Dawn Xiaodong Song. Random key predistribution schemes for sensor networks. In *2003 IEEE Symposium on Security and Privacy (S&P 2003), 11-14 May 2003, Berkeley, CA, USA*, pages 197–, 2003.
9. Benny Chor and Oded Goldreich. Unbiased bits from sources of weak randomness and probabilistic communication complexity. *SIAM J. Comput.*, 17(2):230–261, 1988.
10. Sherman S. M. Chow, Yevgeniy Dodis, Yannis Rouselakis, and Brent Waters. Practical leakage-resilient identity-based encryption from simple assumptions. In Ehab Al-Shaer, Angelos D. Keromytis, and Vitaly Shmatikov, editors, *Proceedings of the 17th ACM Conference on Computer and Communications Security, CCS 2010, Chicago, Illinois, USA, October 4-8, 2010*, pages 152–161. ACM, 2010.
11. Giovanni Di Crescenzo, Richard J. Lipton, and Shabsi Walfish. Perfectly secure password protocols in the bounded retrieval model. In *Theory of Cryptography, Third Theory of Cryptography Conference, TCC 2006, New York, NY, USA, March 4-7, 2006, Proceedings*, volume 3876 of *Lecture Notes in Computer Science*, pages 225–244. Springer, 2006.
12. Yevgeniy Dodis. *Exposure-Resilient Cryptography.* PhD thesis, Massachussetts Institute of Technology, August 2000.
13. Yevgeniy Dodis, Kristiyan Haralambiev, Adriana López-Alt, and Daniel Wichs. Cryptography against continuous memory attacks. In *51th Annual IEEE Symposium on Foundations of Computer Science, FOCS 2010, October 23-26, 2010, Las Vegas, Nevada, USA*, pages 511–520. IEEE Computer Society, 2010.
14. Yevgeniy Dodis, Yael Tauman Kalai, and Shachar Lovett. On cryptography with auxiliary input. In *Proceedings of the 41st Annual ACM Symposium on Theory of Computing, STOC 2009, Bethesda, MD, USA, May 31 - June 2, 2009*, pages 621–630. ACM, 2009.
15. Yevgeniy Dodis, Roberto Oliveira, and Krzysztof Pietrzak. On the generic insecurity of the full domain hash. In Victor Shoup, editor, *Advances in Cryptology - CRYPTO 2005: 25th Annual International Cryptology Conference, Santa Barbara, California, USA, August 14-18, 2005, Proceedings*, volume 3621 of *Lecture Notes in Computer Science*, pages 449–466. Springer, 2005.
16. Wenliang Du, Jing Deng, Yunghsiang S. Han, Pramod K. Varshney, Jonathan Katz, and Aram Khalili. A pairwise key predistribution scheme for wireless sensor networks. *ACM Trans. Inf. Syst. Secur.*, 8(2):228–258, 2005.
17. Stefan Dziembowski. Intrusion-resilience via the bounded-storage model. In *Theory of Cryptography, Third Theory of Cryptography Conference, TCC 2006, New York, NY, USA, March 4-7, 2006, Proceedings*, volume 3876 of *Lecture Notes in Computer Science*, pages 207–224. Springer, 2006.
18. Stefan Dziembowski and Sebastian Faust. Leakage-resilient circuits without computational assumptions. In *Theory of Cryptography - 9th Theory of Cryptography Conference, TCC 2012, Taormina, Sicily, Italy, March 19-21, 2012. Proceedings*, volume 7194 of *Lecture Notes in Computer Science*, pages 230–247. Springer, 2012.
19. Stefan Dziembowski and Krzysztof Pietrzak. Leakage-resilient cryptography. In *49th Annual IEEE Symposium on Foundations of Computer Science, FOCS 2008, October 25-28, 2008, Philadelphia, PA, USA*, pages 293–302. IEEE Computer Society, 2008.
20. Stefan Dziembowski, Krzysztof Pietrzak, and Daniel Wichs. Non-malleable codes. In *Innovations in Computer Science - ICS 2010, Tsinghua University, Beijing, China, January 5-7, 2010. Proceedings*, pages 434–452. Tsinghua University Press, 2010.

21. Laurent Eschenauer and Virgil D. Gligor. A key-management scheme for distributed sensor networks. In Vijayalakshmi Atluri, editor, *Proceedings of the 9th ACM Conference on Computer and Communications Security, CCS 2002, Washington, DC, USA, November 18-22, 2002*, pages 41–47. ACM, 2002.
22. Sebastian Faust, Tal Rabin, Leonid Reyzin, Eran Tromer, and Vinod Vaikuntanathan. Protecting circuits from leakage: the computationally-bounded and noisy cases. In *Advances in Cryptology - EUROCRYPT 2010, 29th Annual International Conference on the Theory and Applications of Cryptographic Techniques, French Riviera, May 30 - June 3, 2010. Proceedings*, volume 6110 of *Lecture Notes in Computer Science*, pages 135–156. Springer, 2010.
23. Sanjam Garg, Abhishek Jain, and Amit Sahai. Leakage-resilient zero knowledge. In Phillip Rogaway, editor, *Advances in Cryptology - CRYPTO 2011 - 31st Annual Cryptology Conference, Santa Barbara, CA, USA, August 14-18, 2011. Proceedings*, volume 6841 of *Lecture Notes in Computer Science*, pages 297–315. Springer, 2011.
24. Rosario Gennaro, Anna Lysyanskaya, Tal Malkin, Silvio Micali, and Tal Rabin. Algorithmic tamper-proof (atp) security: Theoretical foundations for security against hardware tampering. In *Theory of Cryptography, First Theory of Cryptography Conference, TCC 2004, Cambridge, MA, USA, February 19-21, 2004, Proceedings*, volume 2951 of *Lecture Notes in Computer Science*. Springer, 2004.
25. Craig Gentry, Chris Peikert, and Vinod Vaikuntanathan. Trapdoors for hard lattices and new cryptographic constructions. In Cynthia Dwork, editor, *Proceedings of the 40th Annual ACM Symposium on Theory of Computing, Victoria, British Columbia, Canada, May 17-20, 2008*, pages 197–206. ACM, 2008.
26. Shafi Goldwasser and Guy N. Rothblum. How to compute in the presence of leakage. *Electronic Colloquium on Computational Complexity (ECCC)*, 19:10, 2012.
27. Roger A. Horn and Charles R. Johnson. *Topics in matrix analysis*. Cambridge University Press, 1991.
28. Yuval Ishai, Manoj Prabhakaran, Amit Sahai, and David Wagner. Private circuits ii: Keeping secrets in tamperable circuits. In *Advances in Cryptology - EUROCRYPT 2006, 25th Annual International Conference on the Theory and Applications of Cryptographic Techniques, St. Petersburg, Russia, May 28 - June 1, 2006, Proceedings*, volume 4004 of *Lecture Notes in Computer Science*. Springer, 2006.
29. Yuval Ishai, Amit Sahai, and David Wagner. Private circuits: Securing hardware against probing attacks. In *Advances in Cryptology - CRYPTO 2003, 23rd Annual International Cryptology Conference, Santa Barbara, California, USA, August 17-21, 2003, Proceedings*, volume 2729 of *Lecture Notes in Computer Science*, pages 463–481. Springer, 2003.
30. Ali Juma and Yevgeniy Vahlis. Protecting cryptographic keys against continual leakage. In *Advances in Cryptology - CRYPTO 2010, 30th Annual Cryptology Conference, Santa Barbara, CA, USA, August 15-19, 2010. Proceedings*, volume 6223 of *Lecture Notes in Computer Science*, pages 41–58. Springer, 2010.
31. Jonathan Katz and Vinod Vaikuntanathan. Signature schemes with bounded leakage resilience. In Mitsuru Matsui, editor, *Advances in Cryptology - ASIACRYPT 2009, 15th International Conference on the Theory and Application of Cryptology and Information Security, Tokyo, Japan, December 6-10, 2009. Proceedings*, volume 5912 of *Lecture Notes in Computer Science*, pages 703–720. Springer, 2009.
32. Allison Lewko, Mark Lewko, and Brent Waters. How to leak on key updates. In *Proceedings of the 43rd annual ACM symposium on Theory of computing*, STOC '11, pages 725–734, New York, NY, USA, 2011. ACM.

33. Ueli M. Maurer. Conditionally-perfect secrecy and a provably-secure randomized cipher. *J. Cryptology*, 5(1):53–66, 1992.
34. Silvio Micali and Leonid Reyzin. Physically observable cryptography (extended abstract). In *Theory of Cryptography, First Theory of Cryptography Conference, TCC 2004, Cambridge, MA, USA, February 19-21, 2004, Proceedings*, volume 2951 of *Lecture Notes in Computer Science*, pages 278–296. Springer, 2004.
35. Moni Naor and Gil Segev. Public-key cryptosystems resilient to key leakage. In Shai Halevi, editor, *Advances in Cryptology - CRYPTO 2009, 29th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 16-20, 2009. Proceedings*, volume 5677 of *Lecture Notes in Computer Science*, pages 18–35. Springer, 2009.
36. European Network of Excellence (ECRYPT). Side channel cryptanalysis lounge. `http://www.emsec.rub.de/research/projects/sclounge`.
37. Tatsuaki Okamoto. Provably secure and practical identification schemes and corresponding signature schemes. In Ernest F. Brickell, editor, *Advances in Cryptology - CRYPTO '92, 12th Annual International Cryptology Conference, Santa Barbara, California, USA, August 16-20, 1992, Proceedings*, volume 740 of *Lecture Notes in Computer Science*, pages 31–53. Springer, 1992.
38. Krzysztof Pietrzak. A leakage-resilient mode of operation. In Antoine Joux, editor, *Advances in Cryptology - EUROCRYPT 2009, 28th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Cologne, Germany, April 26-30, 2009. Proceedings*, volume 5479 of *Lecture Notes in Computer Science*, pages 462–482. Springer, 2009.
39. Anup Rao. An exposition of bourgain's 2-source extractor. *Electronic Colloquium on Computational Complexity (ECCC)*, 14(034), 2007.
40. Oded Regev. On lattices, learning with errors, random linear codes, and cryptography. In Harold N. Gabow and Ronald Fagin, editors, *Proceedings of the 37th Annual ACM Symposium on Theory of Computing, Baltimore, MD, USA, May 22-24, 2005*, pages 84–93. ACM, 2005.
41. Ronen Shaltiel. Recent developments in explicit constructions of extractors. *Bulletin of the EATCS*, 77:67–95, 2002.
42. Adi Shamir. How to share a secret. *Commun. ACM*, 22(11):612–613, November 1979.