

# Subspace LWE

Krzysztof Pietrzak \*

IST Austria

**Abstract.** The (decisional) learning with errors problem (LWE) asks to distinguish “noisy” inner products of a secret vector with random vectors from uniform. The learning parities with noise problem (LPN) is the special case where the elements of the vectors are bits. In recent years, the LWE and LPN problems have found many applications in cryptography.

In this paper we introduce a (seemingly) much stronger *adaptive* assumption, called “subspace LWE” (SLWE), where the adversary can learn the inner product of the secret and random vectors after they were projected into an adaptively and adversarially chosen subspace. We prove that, surprisingly, the SLWE problem mapping into subspaces of dimension  $d$  is almost as hard as LWE using secrets of length  $d$  (the other direction is trivial.)

This result immediately implies that several existing cryptosystems whose security is based on the hardness of the LWE/LPN problems are provably secure in a much stronger sense than anticipated. As an illustrative example we show that the standard way of using LPN for symmetric CPA secure encryption is even secure against a very powerful class of related key attacks.

## 1 Introduction

The (search version of the) learning with errors problem (LWE) is specified by parameters  $\ell, q \in \mathbb{N}$  and an error distribution  $\chi$  over  $\mathbb{Z}_q$ . It asks to find a secret vector  $\mathbf{s} \in \mathbb{Z}_q^\ell$  given any number of “noisy” inner products of  $\mathbf{s}$  with random vectors. Formally, these products are samples from a distribution  $A_{\chi, \ell}(\mathbf{s})$  over  $\mathbb{Z}_q^{\ell+1}$  which is defined by sampling a uniform  $\mathbf{r} \xleftarrow{\$} \mathbb{Z}_q^\ell$  and an error  $e \leftarrow \chi$ , and outputting  $(\mathbf{r}, \mathbf{r}^\top \cdot \mathbf{s} + e)$  (where multiplications and additions are all modulo  $q$ .)

An important special case of this problem is Regev’s LWE problem [Reg05] where  $\chi$  is a so called discrete Gaussian distribution and  $q$  is polynomial or exponential in a security parameter. Another important case is the learning parities with noise problem (LPN) where  $q = 2$ .

The decisional version of the LWE problem asks to *distinguish* samples of the form  $A_{\chi, \ell}(\mathbf{s})$  from uniform (which might be easier than to actually output  $\mathbf{s}$  as required by the search version of the problem). The decisional LWE problem has been proven polynomially equivalent to the search version if  $q$  is a polynomial

---

\* Supported by the European Research Council under the European Union’s Seventh Framework Programme (FP7/2007-2013) / ERC Starting Grant (259668-PSPC)

size prime [Reg05], and in particular for LPN [BFKL94,KS06]. In this paper we will always consider the decisional version of the problem, and we also only prove the main result for the case where  $q$  is prime.

**Regev’s LWE.** The LWE problem has proven to be extremely useful to construct cryptographic schemes. One reason is its versatility, pretty much any cryptographic primitive known to date can be based on LWE. Another reason is its hardness. The best known algorithms against Regev’s LWE (where  $\chi$  is a discrete Gaussian and  $q = \text{poly}(\ell)$ ) need time and space  $2^{\Theta(\ell)}$  [BKW00] to recover  $\mathbf{s} \in \mathbb{Z}_q^\ell$ ,<sup>1</sup> and unlike for most other assumptions on which public-key crypto can be based, no faster quantum algorithms for the problem are known. But most strikingly, Regev’s LWE is as hard as *worst-case* (standard) lattice assumptions [Reg05,Pei09].

An incomplete list of cryptosystems whose security can be reduced to LWE is public-key encryption secure against chosen plaintext [Reg05,KTX08,PVW08] and chosen ciphertext attacks [PW08,Pei09], circular-secure encryption [ACPS09], identity-based encryption [GPV08,CHKP10,ABB10a,ABB10b], oblivious transfer [PVW08], collision-resistant hash functions [PR06,LMPR08] and public-key identification schemes [Lyu08,Lyu09].

**LPN.** The learning parity with noise (LPN) problem [BFKL94,BKW00,Kea93] is the special case of the LWE problem where  $q = 2$  (i.e. we work over bits) and the error distribution is the Bernoulli distribution for some constant parameter  $\tau, 0 < \tau < 1/2$ , denoted  $\text{Ber}_\tau$ , and defined as  $\Pr[x = 1 ; x \leftarrow \text{Ber}_\tau] = \tau$ . The LPN problem is closely related to the problem of decoding random linear codes,<sup>2</sup> a well studied question in coding theory. The LPN problem seems less versatile than the general LWE problem, and so far only “minicrypt” primitives (i.e. primitives known to be equivalent to one-way functions) were constructed under the LPN assumption. Alekhnovich [Ale03] constructs a public-key encryption scheme from a relaxed LPN assumption where the error  $\tau$  is not constant but upper bounded as a function of  $\ell$  as  $\tau = O(1/\sqrt{\ell})$ .

The Appeal of the LPN problem comes from the fact that LPN based schemes can be extremely efficient, just requiring relatively few bit-level operations to compute an inner product of two bit-vectors. Constructions from LPN include PRGs [FS96], encryption schemes [GRS08,ACPS09] and public-key authentication schemes [Ste94], but by far most work has been done on efficient LPN based secret-key authentication schemes which we’ll discuss in more detail in Section 4.

**Subspace LWE.** The LWE problem has been shown to be very robust with respect to *leakage*. Distinguishing LWE samples remains hard even if we the ad-

<sup>1</sup> This is slightly better than a trivial brute-force search which takes time  $\approx 2^{\ell \log q} = 2^{\Theta(\ell \log \ell)}$  but only linear space.

<sup>2</sup> The only difference is that in the decoding problem one is given a fixed number of samples (typically a small multiple of the length of the secret), whereas in the LPN problem the adversary can ask for arbitrary many samples.

versary can learn a function  $f(\mathbf{s})$  about the secret  $\mathbf{s}$  as long as  $f(\cdot)$  is compressing [AGV09] or hard to invert [DKL09,DGK<sup>+</sup>10,GKPV10]. In this paper we show that the LWE problem is also very robust to *tampering* with the secret vector  $\mathbf{s}$  and the randomness vector  $\mathbf{r}$  (albeit not with the noise  $e$ .)

We define a (seemingly) much stronger *adaptive* version of LWE which we call “Subspace LWE”, or SLWE for short. In the SLWE problem the adversary is not restricted to just ask for samples  $\mathbf{r}, \mathbf{r}^\top \cdot \mathbf{s} + e$  from  $\Lambda_{\chi, \ell}(\mathbf{s})$  as in LWE, but has access to a more powerful oracle which she can query adaptively. The oracle takes as input the description of two affine mappings  $\phi_r, \phi_s : \mathbb{Z}_q^\ell \rightarrow \mathbb{Z}_q^\ell$  and outputs a sample

$$\mathbf{r}, \phi_r(\mathbf{r})^\top \phi_s(\mathbf{s}) + e \quad \text{where } \mathbf{r} \xleftarrow{\$} \mathbb{Z}_q^\ell, e \leftarrow \chi$$

An affine mapping  $\phi_r : \mathbb{Z}_q^\ell \rightarrow \mathbb{Z}_q^\ell$  (similarly  $\phi_s$ ) is given by a matrix and a vector  $\phi_r = [\mathbf{X}_r \in \mathbb{Z}_q^{\ell \times \ell}, \mathbf{x}_r \in \mathbb{Z}_q^\ell]$  and its evaluation is defined as

$$\phi_r(\mathbf{r}) = \mathbf{X}_r \cdot \mathbf{r} + \mathbf{x}_r$$

Without additional restrictions, the SLWE problem as just defined is easy to break. By choosing the input to the oracle appropriately,<sup>3</sup> one can e.g. learn samples of the form  $\mathbf{s}[i] + e$ ,  $e \leftarrow \chi$  ( $\mathbf{s}[i]$  denotes the  $i$ th element of  $\mathbf{s}$ .) For distributions  $\chi$  as used in LPN or Regev’s LWE one can efficiently learn  $\mathbf{s}[i]$  (and thus the entire  $\mathbf{s}$ ) from just a few such samples.

We prove that the SLWE problem (using secrets in  $\mathbb{Z}_q^\ell$  and error distribution  $\chi$ ) is almost as hard as the standard  $(q, \chi, d)$ -LWE problem with secrets of length  $d \leq \ell$  if the adversary is restricted in the sense that she is only allowed to query  $\phi_r, \phi_s$  which “overlap” in an  $d + \delta$  (or more) dimensional subspace where  $\delta \in \mathbb{N}$  is a statistical security parameter. Formally this means  $\mathbf{X}_r^\top \cdot \mathbf{X}_s$  must have rank at least  $d + \delta$ . We call this the  $(q, \chi, \ell, d + \delta)$ -SLWE problem. Let us mention that the other direction – showing that  $(q, \chi, \ell, d)$ -SLWE is at most as hard as  $(q, \chi, d)$ -LWE – is trivial.

The precise statement of our result asserts that for any  $\ell, d, \delta \in \mathbb{N}, d + \delta \leq \ell$ , the  $(q, \chi, \ell, d + \delta)$ -SLWE problem is at most an additive term  $2/q^{\delta+1}$  easier than the standard  $(q, \chi, d)$ -LWE problem. For large fields, where  $q$  is superpolynomial,  $2/q^{\delta+1}$  is negligible already for  $\delta = 0$ . For small fields, in particular the important case  $q = 2$  as used in LPN, we must choose some  $\delta$  to be a statistical security parameter.

The above formulation of SLWE is somewhat redundant, in the sense that an adversary who is restricted to always choose  $\phi_s$  to be the identity function, is as powerful (i.e. can learn exactly the same distribution from the SLWE oracle) as the adversary described above. We chose to explicitly allow the adversary to choose affine mappings for the randomness and the secret separately, as for the applications it is sometimes more convenient to think of the adversary being able to apply a mapping to the secret key (like in the setting of related key attacks

<sup>3</sup> Set  $\mathbf{x}_r = \mathbf{x}_s = \mathbf{0}^\ell$  and  $\mathbf{X}_r, \mathbf{X}_s$  the zero matrix with a single one in the  $i$ th diagonal element. The oracle will output  $\mathbf{r}, \mathbf{r}[i]\mathbf{s}[i] + e$ , the last element is  $\mathbf{s}[i] + e$  if  $\mathbf{r}[i] = 1$ .

we'll discuss), or to the randomness (e.g. to show that LWE is hard, even if the randomness comes from a bit-fixing source.)

**When  $q$  is not Prime.** Our reduction from SLWE to LWE assumes that  $q$  is prime, as we use the fact that  $\mathbb{Z}_q$  is a field and  $\mathbb{Z}_q^m$  is a vector space.<sup>4</sup> We believe that the proof of the reduction can be adapted to the case where  $q$  is composite.

The case where  $q$  is prime covers the cryptographically most interesting cases of LPN and Regev's LWE. Also the reduction from the search to decision version of LWE [Reg05] only works for prime  $q$  (of polynomial size.) But the case where  $q$  is not prime has found cryptographic applications too. In particular, the case where  $q = p^e$  for a prime  $p$  and  $e > 1$  has been used in the construction of an encryption scheme with circular security [ACPS09]. The case where  $q$  is a product of distinct, small primes has been used in [Pei09].

**Applications of SLWE.** In Section 4 we'll discuss some applications of the SLWE problem. In particular, the fact that SLWE is equivalent to LWE implies stronger security notions – like security against related-key attacks – that one can give for existing schemes whose security is reduced to the LWE problem. In subsequent work, the hardness of SLPN has been used to construct efficient authentication schemes and even MACs from LPN. These schemes differ significantly from previous schemes which all were extensions of the Hopper-Blum protocol.

**Outline.** In Section 2 we first define the LWE and the new subspace LWE (SLWE) problem. In Section 3 we state and prove our main technical result (Theorem 1) which bounds the hardness of the SLWE problem in terms of the hardness of the standard LWE problem. In Section 4 we describe in more detail some applications of this result which were already mentioned in the introduction.

## 2 Hard Learning Problems

### 2.1 Notation

We denote the set of integers modulo an integer  $q \geq 1$  by  $\mathbb{Z}_q$ . We will use normal, bold and capital bold letters like  $x$ ,  $\mathbf{x}$ ,  $\mathbf{X}$  to denote single elements, vectors and matrices over  $\mathbb{Z}_q$ , respectively. For  $\mathbf{x} \in \mathbb{Z}_q^\ell$ ,  $|\mathbf{x}| = \ell$  denotes the length and  $\text{wt}(\mathbf{x})$  denotes the Hamming weight of the vector  $\mathbf{x}$ , i.e. the number of indices  $i \in \{1, \dots, |\mathbf{x}|\}$  where  $\mathbf{x}[i] \neq 0$ . For  $\mathbf{v} \in \mathbb{Z}_2^m$  we denote with  $\bar{\mathbf{v}}$  its inverse, i.e.  $\bar{\mathbf{v}}[i] = 1 - \mathbf{v}[i]$  for all  $i$ . For a distribution  $\chi$ ,  $x \leftarrow \chi$  denotes sampling a value  $x$  with distribution  $\chi$ . For a set  $\mathcal{S}$ ,  $x \xleftarrow{\$} \mathcal{S}$  denotes sampling a value  $x$  with the uniform distribution over  $\mathcal{S}$ .

<sup>4</sup> The fact that  $\mathbb{Z}_q^m$  is a vector space is e.g. used in the proof of Lemma 1.

$\mathbf{x}_{\downarrow \mathbf{v}}, \mathbf{X}_{\downarrow \mathbf{v}}$  : For two vectors  $\mathbf{v} \in \mathbb{Z}_2^\ell$  and  $\mathbf{x} \in \mathbb{Z}_q^\ell$ , we denote with  $\mathbf{x}_{\downarrow \mathbf{v}}$  the vector (of length  $\mathbf{wt}(\mathbf{v})$ ) which is derived from  $\mathbf{x}$  by deleting all the bits  $\mathbf{x}[i]$  where  $\mathbf{v}[i] = 0$ . If  $\mathbf{X} \in \mathbb{Z}_q^{\ell \times m}$  is a matrix, then  $\mathbf{X}_{\downarrow \mathbf{v}} \in \mathbb{Z}_q^{\mathbf{wt}(\mathbf{v}) \times m}$  denotes the submatrix we get by deleting the  $i$ th row if  $\mathbf{v}[i] = 0$ .

$\mathbf{x}_{\mathbf{v}}, \mathbf{X}_{\mathbf{v}}$  : For  $\mathbf{x}, \mathbf{X}, \mathbf{v}$  as in the previous item,  $\mathbf{x}_{\mathbf{v}}$  denotes the vector where the  $i$ th entry is  $\mathbf{x}[i] \wedge \mathbf{v}[i]$ . Think of  $\mathbf{x}_{\mathbf{v}}$  as  $\mathbf{x}$  where all entries of  $\mathbf{x}$  where  $\mathbf{v}$  is 0 are set to 0.  $\mathbf{X}_{\mathbf{v}}$  denotes the matrix  $\mathbf{X}$  where the  $i$ th row is set to all 0 if  $\mathbf{v}[i] = 0$ .

## 2.2 The (Subspace) LWE Problem.

The (search version of the) learning with errors (LWE) problem is specified by parameters  $\ell, q \in \mathbb{N}$  and an error distribution  $\chi$  over  $\mathbb{Z}_q$ . It asks to find a secret vector  $\mathbf{s} \in \mathbb{Z}_q^\ell$  given any number of “noisy” inner products of  $\mathbf{s}$  with random vectors.

Formally, let  $\Lambda_{\chi, \ell}(\mathbf{s})$  be the distribution over  $\mathbb{Z}_q^{\ell+1}$  where a sample is given by

$$(\mathbf{r}, \mathbf{r}^\top \cdot \mathbf{s} + e) \leftarrow \Lambda_{\chi, \ell}(\mathbf{s}) \quad \text{where} \quad \mathbf{r} \stackrel{\$}{\leftarrow} \mathbb{Z}_q^\ell, e \leftarrow \chi$$

Let  $U_q^m$  denote the uniform distribution over  $\mathbb{Z}_q^m$  and  $U_q = U_q^1$ . The decisional LWE problem asks to distinguish samples from  $\Lambda_{\chi, \ell}(\mathbf{s})$  with a uniform  $\mathbf{s}$  from a random oracle (outputting  $U_q^{\ell+1}$  samples.) For any  $\mathbf{s}$ ,  $\Lambda_{U_q, \ell}(\mathbf{s})$  is the same as the uniform distribution  $U_q^{\ell+1}$ . It will be convenient for the proof to think of the random oracle as outputting samples from  $\Lambda_{U_q, \ell}(\mathbf{s})$  for some random  $\mathbf{s}$  instead of  $U_q^{\ell+1}$ .

**Definition 1 (Decisional Learning with Errors Problem (LWE)).** *The (decisional)  $(q, \chi, \ell)$ -LWE problem is  $(t, Q, \varepsilon)$  hard if for every distinguisher  $D$  running in time  $t$  and making  $Q$  oracle queries,*

$$\left| \Pr \left[ \mathbf{s} \stackrel{\$}{\leftarrow} \mathbb{Z}_q^\ell : D^{\Lambda_{\chi, \ell}(\mathbf{s})} = 1 \right] - \underbrace{\Pr \left[ \mathbf{s} \stackrel{\$}{\leftarrow} \mathbb{Z}_q^\ell : D^{\Lambda_{U_q, \ell}(\mathbf{s})} = 1 \right]}_{\Pr[D^{U_q^{\ell+1}} = 1]} \right| \leq \varepsilon. \quad (1)$$

Usually one defines the LWE problem by considering a distinguisher who gets a polynomial number of samples as input and not access to an oracle (which doesn't take inputs anyway.) We use this oracle based definition so it is more similar to the SLWE problem we define below, where the oracle does take adaptively chosen inputs.

An affine projection  $\phi : \mathbb{Z}_q^\ell \rightarrow \mathbb{Z}_q^\ell$  is given by a matrix/vector tuple  $\mathbf{X} \in \mathbb{Z}_q^{\ell \times \ell}, \mathbf{x} \in \mathbb{Z}_q^\ell$  and defined as  $\phi(\mathbf{v}) \stackrel{\text{def}}{=} \mathbf{X}^\top \mathbf{v} + \mathbf{x}$ .

For  $\mathbf{s} \in \mathbb{Z}_q^{\ell \times \ell}$  and affine projections  $\phi_r = [\mathbf{X}_r, \mathbf{x}_r], \phi_s = [\mathbf{X}_s, \mathbf{x}_s]$  we define the distribution  $\Gamma_{\chi, \ell, d}(\mathbf{s}, \phi_r, \phi_s)$  over  $\mathbb{Z}_q^{\ell+1} \cup \perp$  as

$$\perp \leftarrow \Gamma_{\chi, \ell, d}(\mathbf{s}, \phi_r, \phi_s) \quad \text{if} \quad \text{rank}(\mathbf{X}_r^\top \mathbf{X}_s) < d$$

and

$$[\mathbf{r}, \phi_r(\mathbf{r})^\top \cdot \phi_s(\mathbf{s}) + e] \leftarrow \Gamma_{\chi, \ell, d}(\mathbf{s}, \phi_r, \phi_s) \quad \text{where} \quad \mathbf{r} \xleftarrow{\$} \mathbb{Z}_q^\ell, e \leftarrow \chi$$

otherwise. With  $\Gamma_{\chi, \ell, d}(\mathbf{s}, \cdot)$  we denote the oracle which on input  $\phi_r, \phi_s$  outputs a sample of  $\Gamma_{\chi, \ell, d}(\mathbf{s}, \phi_r, \phi_s)$ .

**Definition 2 (Subspace Learning with Errors Problem (SLWE)).** *The (decisional)  $(q, \chi, \ell, d)$ -SLWE problem is  $(t, Q, \varepsilon)$  hard if for every distinguisher  $D$  running in time  $t$  and making  $Q$  oracle queries,*

$$\left| \Pr \left[ \mathbf{s} \xleftarrow{\$} \mathbb{Z}_q^\ell : D^{\Gamma_{\chi, \ell, d}(\mathbf{s}, \cdot)} = 1 \right] - \Pr \left[ \mathbf{s} \xleftarrow{\$} \mathbb{Z}_q^\ell : D^{\Gamma_{U_q, \ell, d}(\mathbf{s}, \cdot)} = 1 \right] \right| \leq \varepsilon. \quad (2)$$

Note that by definition the  $\Gamma_{U_q, \ell, d}(\mathbf{s}, \cdot)$  oracle outputs  $\perp$  if the input satisfies  $\text{rank}(\mathbf{X}_r^\top \mathbf{X}_s) < d$  and a uniform sample  $U_q^{\ell+1}$  otherwise. In particular, like  $\Lambda_{U_q, \ell}(\mathbf{s})$ , the output distribution of  $\Gamma_{U_q, \ell, d}(\mathbf{s}, \cdot)$  is independent of  $\mathbf{s}$ .

### 3 The Hardness of SLWE

Theorem 1 below is the main technical result stating that the SLWE problem mapping into subspaces of dimension  $d$  is almost as hard as the standard LWE problem with secrets of length  $d$ . But let's first look at the (easy) other direction as stated by Claim 1 below.

**Claim 1 ( $(q, \chi, \ell, d)$ -SLWE at most as hard as  $(q, \chi, d)$ -LWE)**

*If  $(q, \chi, \ell, d)$ -SLWE is  $(s, t, \varepsilon)$  hard then  $(q, \chi, d)$ -LWE is  $(s', t, \varepsilon)$  hard where  $s' = s - \text{poly}(t, \ell)$ .*

*Proof (of Claim).* To prove this claim we will show how, for any error distribution  $\chi'$ , one can efficiently generate  $(q, \chi', d)$ -LWE samples which have distribution  $\Lambda_{\chi', d}(\mathbf{s}')$  (for some uniform  $\mathbf{s}' \in \mathbb{Z}_q^d$ ) given access to a  $(q, \chi', \ell, d)$ -SLWE oracle  $\Gamma_{\chi', \ell, d}(\mathbf{s}, \cdot)$  (for some uniform  $\mathbf{s} \in \mathbb{Z}_q^\ell$ .) We do so without known knowing the distribution  $\chi'$  or  $\mathbf{s}$ .

Given such a transformation, we then can use any distinguisher  $D$  who breaks the  $(q, \chi, d)$ -LWE assumption with advantage  $\varepsilon$  as defined in eq.(1), to break the  $(q, \chi, \ell, d)$ -SLWE assumption as in eq.(2) with the same advantage by simply transforming the SLWE samples (where the oracle uses either the error distribution  $\chi' = \chi$  or  $\chi' = U_q^{\ell+1}$ , but we don't know which) to LWE samples (with the same unknown error distribution  $\chi'$ ) before forwarding them to  $D$ .

Let  $\mathbf{v} \stackrel{\text{def}}{=} 1^d \| 0^{\ell-d}$ . To generate samples as described above, query  $\Gamma_{\chi', \ell, d}(\mathbf{s}, \cdot)$  so it outputs samples  $\Lambda_{\chi', d}(\mathbf{s}')$  where  $\mathbf{s}' \in \mathbb{Z}_q^d$  consists of, say, the first  $d$  elements of  $\mathbf{s} \in \mathbb{Z}_q^\ell$ , i.e.  $\mathbf{s}' := \mathbf{s}_{\downarrow \mathbf{v}}$ . This can be done by making  $q$  queries  $\mathbf{X}_s, \mathbf{X}_r, \mathbf{x}_s, \mathbf{x}_r$  to  $\Gamma_{\chi', \ell, d}(\mathbf{s}, \cdot)$  where  $\mathbf{x}_s = \mathbf{x}_r = 0^\ell$  and  $\mathbf{X}_s = \mathbf{X}_r$  is 1 in the first  $d$  diagonal entries and 0 everywhere else. The output of the SLWE oracle on these queries are samples of the form

$$\mathbf{r}, \underbrace{(\mathbf{X}_r \mathbf{r} + \mathbf{x}_r)^\top}_{\mathbf{r}_{\downarrow \mathbf{v}}^\top} \underbrace{(\mathbf{X}_s \mathbf{s} + \mathbf{x}_s)}_{\mathbf{s}_{\downarrow \mathbf{v}}} + e \quad \text{where} \quad e \leftarrow \chi', \mathbf{r} \xleftarrow{\$} \mathbb{Z}_q^\ell$$

from which we then get an  $\Lambda_{\chi',d}(\mathbf{s}_{\downarrow \mathbf{v}})$  sample  $\mathbf{r}_{\downarrow \mathbf{v}}, \mathbf{r}_{\downarrow \mathbf{v}}^\top \mathbf{s}_{\downarrow \mathbf{v}} + e$  by replacing  $\mathbf{r}$  with  $\mathbf{r}_{\downarrow \mathbf{v}}$ . Note that these samples have the right distribution, which means  $\mathbf{s}_{\downarrow \mathbf{v}}$  and the  $q$   $\mathbf{r}_{\downarrow \mathbf{v}}$ 's are uniformly random as required. This is easy to see recalling that  $\mathbf{s}$  and the  $q$   $\mathbf{r}$ 's are uniform.  $\square$

In the proof of Theorem 1, we'll need the following simple technical Lemma:

**Lemma 1.** *For  $q, d, \delta \in \mathbb{N}$ , let  $\Delta(q, d, \delta)$  denote the probability that a random matrix in  $\mathbb{Z}_q^{(d+\delta) \times d}$  has rank less than  $d$ , then*

$$\Delta(q, d, \delta) \leq \frac{2}{q^{\delta+1}}.$$

*Proof.* Assume we sample the  $d$  columns of a matrix  $M \in \mathbb{Z}_q^{(d+\delta) \times d}$  one by one. For  $i = 1, \dots, d$  let  $E_i$  denote the event that the first  $i$  columns are linearly independent, then

$$\Pr[\neg E_i | E_{i-1}] = \frac{q^{i-1}}{q^{d+\delta}} = q^{i-1-d-\delta}$$

as  $\neg E_i$  happens iff the  $i$ th column (sampled uniformly from a space of size  $q^{d+\delta}$ ) falls into the space (of size  $q^{i-1}$ ) spanned by the first  $i-1$  columns. We get further

$$\Delta(q, d, \delta) = \Pr[\neg E_d] \leq \sum_{i=1}^d \Pr[\neg E_i | E_{i-1}] = \sum_{i=1}^d q^{i-1-d-\delta} \leq \frac{2}{q^{\delta+1}}$$

$\square$

**Theorem 1 (( $q, \chi, \ell, d$ )-SLWE almost as hard as ( $q, \chi, d$ )-LWE).**

*For  $q, d, \delta, \ell \in \mathbb{N}$ . If the ( $q, \chi, d$ )-LWE problem is  $(s, t, \epsilon)$  hard, then the ( $q, \chi, \ell, d + \delta$ )-SLWE problem is  $(s', t, \epsilon')$  hard where*

$$s' = s - \text{poly}(\ell, t) \quad \epsilon' = \epsilon + \frac{2 \cdot t}{q^{\delta+1}}$$

*Proof (of Theorem 1).* To prove the theorem we will show how to sample outputs of an SLWE oracle  $\Gamma_{\chi', \ell, d+\delta}(\hat{\mathbf{s}}, \cdot)$  for some uniformly random  $\hat{\mathbf{s}} \in \mathbb{Z}_q^\ell$  and adversarially chosen inputs, given only standard LWE samples  $\Lambda_{\chi', d}(\mathbf{s})$  for some uniform  $\mathbf{s} \in \mathbb{Z}_q^d$ . This sampling is done without knowing  $\mathbf{s}$  or the error distribution  $\chi'$ .

Given such a transformation, we then can use any distinguisher  $D$  who breaks the ( $q, \chi, \ell, d + \delta$ )-SLWE assumption with advantage  $\epsilon$  to break the standard ( $q, \chi, d$ )-LWE assumption with the same advantage, minus the probability that the transformation will fail (which, unlike in the previous claim, is non-zero.)

Recall that an LWE sample  $\Lambda_{\chi', d}(\mathbf{s} \in \mathbb{Z}_q^d)$  is of the form

$$\mathbf{r}, \mathbf{r}^\top \cdot \mathbf{s} + e \quad \text{where} \quad e \leftarrow \chi' \quad \mathbf{r} \xleftarrow{\$} \mathbb{Z}_q^d \quad (3)$$

For  $\mathbf{X}_r, \mathbf{X}_s \in \mathbb{Z}_q^{\ell \times \ell}$ ,  $\mathbf{x}_s, \mathbf{x}_r \in \mathbb{Z}_q^\ell$ , we'll show how to transform such a sample into an SLWE sample  $L_{\chi', \ell, d+\delta}(\hat{\mathbf{s}}, [\mathbf{X}_r, \mathbf{x}_r, \mathbf{X}_s, \mathbf{x}_s])$ . If  $\text{rank}(\mathbf{X}_r^\top \cdot \mathbf{X}_s) < d + \delta$  this sample is simply  $\perp$ , so from now on we assume that this rank is at least  $d + \delta$ , in this case the sample has the form

$$\hat{\mathbf{r}}, (\mathbf{X}_r \cdot \hat{\mathbf{r}} + \mathbf{x}_r)^\top \cdot (\mathbf{X}_s \cdot \hat{\mathbf{s}} + \mathbf{x}_s) + e \quad \text{where} \quad e \leftarrow \chi' \quad \hat{\mathbf{r}} \stackrel{\$}{\leftarrow} \mathbb{Z}_q^\ell \quad (4)$$

In our transformation, the SLWE secret  $\hat{\mathbf{s}} \in \mathbb{Z}_q^\ell$  is defined as a function of the LWE secret  $\mathbf{s} \in \mathbb{Z}_q^d$  as follows

$$\mathbf{R} \stackrel{\$}{\leftarrow} \mathbb{Z}_q^{\ell \times d} \quad \mathbf{b} \stackrel{\$}{\leftarrow} \mathbb{Z}_q^\ell \quad \hat{\mathbf{s}} = \mathbf{R} \cdot \mathbf{s} + \mathbf{b} \quad (5)$$

Note that we only know  $\mathbf{R}, \mathbf{b}$  (which we sampled), but will not get  $\hat{\mathbf{s}}$  as we don't know  $\mathbf{s}$ . Also note that  $\hat{\mathbf{s}}$  is uniformly random as it is blinded with a uniform  $\mathbf{b}$ . Define the set  $\mathcal{L} \subseteq \mathbb{Z}_q^\ell$ , which is the set of solutions to a system of linear equations, as

$$\mathcal{L} = \{\mathbf{y} : \mathbf{y} \cdot \mathbf{X}_r^\top \cdot \mathbf{X}_s \cdot \mathbf{R} = \mathbf{r}^\top - \mathbf{x}_r^\top \cdot \mathbf{X}_s \cdot \mathbf{R}\}. \quad (6)$$

If  $\mathbf{X}_r^\top \cdot \mathbf{X}_s \cdot \mathbf{R}$  has rank at least  $d$ , then  $\mathcal{L}$  is not empty as the linear equation considered in eq.(6) is (over)defined (we will bound the probability that the rank is  $d$  later.) In this case the LWE sample is transformed into an SLWE sample as

$$\underbrace{\mathbf{r}, \mathbf{r}^\top \cdot \mathbf{s} + e}_{\text{LWE Sample (3)}} \quad \rightarrow \quad \underbrace{\hat{\mathbf{r}}, \mathbf{r}^\top \cdot \mathbf{s} + z + e}_{\text{SLWE Sample (4)}} \quad \text{where} \quad \hat{\mathbf{r}} \stackrel{\$}{\leftarrow} \mathcal{L} \quad (7)$$

and the  $z$  is computed from known values as

$$z \stackrel{\text{def}}{=} (\hat{\mathbf{r}}^\top \cdot \mathbf{X}_r^\top + \mathbf{x}_r^\top) \cdot \mathbf{X}_s \cdot \mathbf{b} + (\mathbf{X}_r \cdot \hat{\mathbf{r}} + \mathbf{x}_r)^\top \cdot \mathbf{x}_s$$

It follows from the three claims below that this sampling gives the right distribution.

*Claim.* If  $\mathbf{T} \stackrel{\text{def}}{=} \mathbf{X}_r^\top \cdot \mathbf{X}_s \cdot \mathbf{R}$  has rank  $\geq d$  then  $\hat{\mathbf{r}} \stackrel{\$}{\leftarrow} \mathcal{L}$  is uniformly random (given  $\mathbf{x}_s, \mathbf{x}_r, \mathbf{X}_s^\top, \mathbf{X}_r^\top, \mathbf{R}, \mathbf{b}$ .)

*Proof (of Claim).* Fix some  $\mathbf{t} \in \mathbb{Z}_2^\ell$  of weight  $\text{wt}(\mathbf{t}) = d$  such that  $\mathbf{T}_{\downarrow \mathbf{t}}$  has full rank. Such a  $\mathbf{t}$  exists as  $\mathbf{T}$  has rank  $d$ .

By eq.(6),  $\hat{\mathbf{r}} \stackrel{\$}{\leftarrow} \mathcal{L}$  is a random solution to the equation

$$\hat{\mathbf{r}} \cdot \mathbf{T} = \mathbf{r}^\top - \mathbf{x}_r^\top \cdot \mathbf{X}_s \cdot \mathbf{R}$$

or equivalently (using  $\hat{\mathbf{r}} \cdot \mathbf{T} = \hat{\mathbf{r}}_{\downarrow \mathbf{t}} \cdot \mathbf{T}_{\downarrow \mathbf{t}} + \hat{\mathbf{r}}_{\downarrow \bar{\mathbf{t}}} \cdot \mathbf{T}_{\downarrow \bar{\mathbf{t}}}$ )

$$\hat{\mathbf{r}}_{\downarrow \mathbf{t}} \cdot \mathbf{T}_{\downarrow \mathbf{t}} = \mathbf{r}^\top - \mathbf{x}_r^\top \cdot \mathbf{X}_s \cdot \mathbf{R} - \hat{\mathbf{r}}_{\downarrow \bar{\mathbf{t}}} \cdot \mathbf{T}_{\downarrow \bar{\mathbf{t}}} \quad (8)$$

Now sampling a random  $\hat{\mathbf{r}}$  can be done as follows. First sample  $\hat{\mathbf{r}}_{\downarrow \bar{\mathbf{t}}} \stackrel{\$}{\leftarrow} \mathbb{Z}_q^{\ell-d}$  uniformly. The remaining  $d$  positions  $\hat{\mathbf{r}}_{\downarrow \mathbf{t}} \in \mathbb{Z}_q^d$  are then uniquely determined by  $\mathbf{r}$  and given by the solution to the equation (8).

As  $\mathbf{T}_{\downarrow t}$  is a full rank square matrix eq.(8) defines a bijection between  $\hat{\mathbf{r}}_{\downarrow t}$  and  $\mathbf{r}$ . As  $\mathbf{r}$  is chosen uniformly at random, also  $\hat{\mathbf{r}}_{\downarrow t}$  is uniformly random. Thus the entire  $\hat{\mathbf{r}}$  is uniform as claimed.  $\square$

*Claim.* The  $\hat{\mathbf{r}}, \mathbf{r}^\top \cdot \mathbf{s} + z + e$  as sampled in (7) is an SLWE sample for secret  $\hat{\mathbf{s}}$ , randomness  $\hat{\mathbf{r}}$  and error  $e$ .

*Proof (of Claim).*

$$\begin{aligned}
& \hat{\mathbf{r}}, (\mathbf{X}_r \cdot \hat{\mathbf{r}} + \mathbf{x}_r)^\top (\mathbf{X}_s \cdot \hat{\mathbf{s}} + \mathbf{x}_s) + e && \text{(SLWE sample)} \\
&= \hat{\mathbf{r}}, (\mathbf{X}_r \cdot \hat{\mathbf{r}} + \mathbf{x}_r)^\top (\mathbf{X}_s \cdot \hat{\mathbf{s}}) + (\mathbf{X}_r \cdot \hat{\mathbf{r}} + \mathbf{x}_r)^\top \cdot \mathbf{x}_s + e \\
&\stackrel{(5)}{=} \hat{\mathbf{r}}, (\mathbf{X}_r \cdot \hat{\mathbf{r}} + \mathbf{x}_r)^\top (\mathbf{X}_s \cdot (\mathbf{R} \cdot \mathbf{s} + \mathbf{b})) + (\mathbf{X}_r \cdot \hat{\mathbf{r}} + \mathbf{x}_r)^\top \cdot \mathbf{x}_s + e \\
&= \hat{\mathbf{r}}, (\hat{\mathbf{r}}^\top \cdot \mathbf{X}_r^\top + \mathbf{x}_r^\top) (\mathbf{X}_s \cdot \mathbf{R} \cdot \mathbf{s}) + \underbrace{(\hat{\mathbf{r}}^\top \cdot \mathbf{X}_r^\top + \mathbf{x}_r^\top) \cdot \mathbf{X}_s \cdot \mathbf{b}}_z + (\mathbf{X}_r \cdot \hat{\mathbf{r}} + \mathbf{x}_r)^\top \cdot \mathbf{x}_s + e \\
&\stackrel{(6)}{=} \hat{\mathbf{r}}, \mathbf{r}^\top \cdot \mathbf{s} + z + e
\end{aligned}$$

$\square$

We have shown how to simulate an SLWE oracle  $\Gamma_{\chi', \ell, d+\delta}(\hat{\mathbf{s}}, \cdot)$  from standard LWE samples  $A_{\chi', d}(\mathbf{s})$ . This simulation goes well as long as we never get a query containing  $\mathbf{X}_r, \mathbf{X}_s$  where  $\text{rank}(\mathbf{X}_r^\top \cdot \mathbf{X}_s) \geq d + \delta$  (so the sample is not just  $\perp$ ) but where  $\text{rank}(\mathbf{X}_r^\top \cdot \mathbf{X}_s \cdot \mathbf{R}) < d$  (in this case  $\mathcal{L}$  can be empty.) The following claims bounds the probability of this happening.

*Claim.* Consider any  $\mathbf{X} \in \mathbb{Z}_q^{\ell \times \ell}$  with  $\text{rank}(\mathbf{X}) \geq d + \delta$ , then (with  $\Delta$  as defined in Lemma 1)

$$\Pr[\text{rank}(\mathbf{X} \cdot \mathbf{R}) < d : \mathbf{R} \stackrel{\$}{\leftarrow} \mathbb{Z}_q^{\ell \times d}] \leq \Delta(q, d, \delta)$$

*Proof (of Claim).* Since the matrix  $\mathbf{X}$  has rank at least  $d + \delta$ , without loss of generality, we can assume that the first  $d + \delta$  rows of  $\mathbf{X}$  are linearly independent. Since  $\mathbf{R}$  is a random matrix, the upper  $(d + \delta) \times d$  submatrix of  $\mathbf{X} \cdot \mathbf{R}$  is a random matrix in  $\mathbb{Z}_q^{(d+\delta) \times d}$  and (by definition) such a matrix has rank strictly less than  $d$  with probability at most  $\Delta(q, d, \delta)$ . Thus  $\mathbf{X} \cdot \mathbf{R}$  has rank strictly less than  $d$  with at most the same probability.  $\square$

Using the union bound, we can upper bound the probability that for any of the  $t$  queries the matrix  $\mathbf{X} = \mathbf{X}_r^\top \cdot \mathbf{X}_s$  chosen by the distinguisher  $D$  will satisfy  $\text{rank}(\mathbf{X} \cdot \mathbf{R}) < d$  by

$$t \cdot \Delta(q, n, d) \leq \frac{2 \cdot t}{q^{\delta+1}}$$

This error probability is thus an upper bound on the gap of the success probability  $\epsilon'$  of  $D$  (in breaking SLWE) and the success probability  $\epsilon$  we get in breaking LWE using the transformation.

Above we ignored the fact that  $D$  can choose its queries, and thus the matrix  $\mathbf{X} = \mathbf{X}_r^\top \cdot \mathbf{X}_s$ , *adaptively*. To show that adaptivity does not help in picking an  $\mathbf{X}$

where  $\mathbf{X}\mathbf{R}$  has rank  $< d$  we must show that the view of  $D$  is *independent* of  $\mathbf{R}$  (except for the fact that so far no query was made where  $\text{rank}(\mathbf{X}\mathbf{R}) < d$ .) To see this first note that  $\hat{\mathbf{s}} = \mathbf{s}\mathbf{R} + \mathbf{b}$  is independent of  $\mathbf{R}$  as it is blinded with a uniform  $\mathbf{b}$ . In fact, the only reason we use this blinding is to enforce this independence. The  $\hat{\mathbf{r}}$  are independent as they are uniform given  $\mathbf{R}$  as shown in the first Claim in the proof of this theorem.  $\square$

## 4 Applications

In this section we discuss some consequences and applications which use the fact that the new subspace LWE problem is as hard as the classical LWE problem.

### 4.1 Security against Related Key Attacks

Theorem 1 implies that many existing schemes whose security is based on the standard LWE/LPN assumption are secure against attacks not anticipated by the designers of the schemes.

As an illustrative example below we discuss the simple construction of symmetric CPA secure encryption from LPN [GRS08]. We show that this simple scheme is not only CPA secure, but it's even secure against powerful related key-attacks. The scheme from [GRS08] is defined as follows

**Public Parameters:**

- Constants  $0 < \tau < 0.5$ ,  $\delta > 0$ ,  $\ell \in \mathbb{N}$ .
- An error correcting code  $\mathbf{E} : \mathbb{Z}_2^m \rightarrow \mathbb{Z}_2^n$ ,  $\mathbf{D} : \mathbb{Z}_2^n \rightarrow \mathbb{Z}_2^m$ , where  $\mathbf{D}$  can correct up to  $(\tau + \delta)\ell$  errors.

**Key Generation:**  $\text{KG}(\ell)$  samples and outputs  $\mathbf{s} \xleftarrow{\$} \mathbb{Z}_2^\ell$ .

**Encryption:**  $\text{Enc}(K, \mathbf{m})$  samples  $\mathbf{R} \xleftarrow{\$} \mathbb{Z}_2^{\ell \times n}$ ,  $\mathbf{e} \xleftarrow{\$} \text{Ber}_\tau^n$  and outputs the ciphertext  $(\mathbf{R}, \mathbf{R}^T \cdot \mathbf{s} \oplus \mathbf{e} \oplus \mathbf{E}(\mathbf{m}))$ .

**Decryption:**  $\text{Dec}(K, (\mathbf{R}, \mathbf{z}))$  outputs  $\mathbf{D}(\mathbf{z} \oplus \mathbf{R}^T \cdot \mathbf{s})$ .

**Correctness.** To see that this scheme is correct, note that on input a correctly generated ciphertext  $(\mathbf{R}, \mathbf{R}^T \cdot \mathbf{s} \oplus \mathbf{e} \oplus \mathbf{E}(\mathbf{m}))$ , the decryption algorithm outputs  $\mathbf{D}(\mathbf{e} \oplus \mathbf{E}(\mathbf{m}))$ , which is equal to  $\mathbf{m}$  unless the error vector  $\mathbf{e}$  has weight more than  $(\tau + \delta)\ell$ . As the bits of  $\mathbf{e}$  are i.i.d. with each bit being one with probability  $\tau$ , the probability of  $\mathbf{e}$  having such high weight can be upper bounded (using the Chernoff bound) by an exponentially small probability  $2^{-\gamma \cdot \ell}$  (for some  $\gamma > 0$  which depends on  $\tau, \delta$ ).

**CPA Security.** Recall that an encryption scheme is IND-CPA secure if no efficient adversary  $\mathcal{A}$  can win the following game with probability noticeably better than 1/2:

1. We sample a key  $\mathbf{s} \xleftarrow{\$} \mathbb{Z}_2^\ell$  and a bit  $b \xleftarrow{\$} \{0, 1\}$ .

2.  $\mathcal{A}$  gets access to an oracle  $\text{Enc}_b(\mathbf{s}, \cdot)$  where
  - $\text{Enc}_0(\mathbf{s}, \mathbf{m}) = \text{Enc}(\mathbf{s}, \mathbf{m})$  (encrypt  $\mathbf{m}$ )
  - $\text{Enc}_1(\mathbf{s}, \mathbf{m}) = \text{Enc}(\mathbf{s}, 0^{|\mathbf{m}|})$  (encrypt dummy message)
3.  $\mathcal{A}$  outputs  $b'$  and wins if  $b = b'$ .

The IND-CPA security of the [GRS08] encryption scheme follows quite easily from the LPN assumption, i.e. the fact that samples  $(\mathbf{R}, \mathbf{R}^\top \cdot \mathbf{s} + \mathbf{e})$  are pseudo-random.

**RKA Security.** Classical security notions, like IND-CPA security, model the encryption scheme as a “black-box”, where an adversary can only observe the legitimate input-output behavior of the scheme. Unfortunately, in the last decade it became evident that such idealized models fail to capture many real-world attacks where an adversary can attack an actual physical implementation of the scheme. An important example is direct leakage from the secret state, typically by side-channel attacks or malware. To deal with this issue, in the last years many “intrusion-resilient” and “leakage-resilient” schemes have been proposed [ISW03,MR04,Dzi06,DP07,DP08,ADW09,Pie09,CDD<sup>+</sup>07,KV09,DW09,DKL09].

But the key can also leak indirectly, for example due to key-dependent messages [BRS03,HK07,BHHO08,HU08,ACPS09,BHHI10,BG10,ABBC10]. Here, as the name suggest, one considers a setting where the encrypted message can depend on the secret key. Another important setting are related-key attacks (RKA). In an RKA attack on an encryption scheme the adversary can not only ask for encryptions under the secret key  $\mathbf{s}$ , but also under “related” keys. RKA attacks were first considered by Biham [Bih94] and Knudsen [Knu92], and were extensively studied in the last decade [Luc04,BDK06,BDK08,FKL<sup>+</sup>00,JD04,ZZWF07,BC10]. Bellare and Kohno [BK03] initiated a formal study of RKA attacks. All this works consider RKA security of deterministic primitives, usually block-ciphers.

Very recently [AHI11] initiated a formal study of RKA security for probabilistic encryption [GM84]. As in [BK03], they define RKA with respect to related-key-deriving functions (RKD)  $\Phi$ .  $\Phi$ -RKA-IND-CPA security of an encryption scheme is then defined almost like standard IND-CPA security, but where the adversary can additionally apply any function  $\phi \in \Phi$  to the secret key  $\mathbf{s}$ , i.e.

1. We sample a key  $\mathbf{s} \xleftarrow{\$} \mathbb{Z}_2^\ell$  and a bit  $b \xleftarrow{\$} \{0, 1\}$ .
2.  $\mathcal{A}$  gets access to an oracle  $\text{Enc}_b^\Phi(\mathbf{s}, \cdot, \cdot)$  where
  - $\text{Enc}_0^\Phi(\mathbf{s}, \mathbf{m}, \phi \in \Phi) = \text{Enc}(\phi(\mathbf{s}), \mathbf{m})$  (encrypt  $\mathbf{m}$ )
  - $\text{Enc}_1^\Phi(\mathbf{s}, \mathbf{m}, \phi \in \Phi) = \text{Enc}(\phi(\mathbf{s}), 0^{|\mathbf{m}|})$  (encrypt dummy message)
3.  $\mathcal{A}$  outputs  $b'$  and wins if  $b = b'$ .

In [AHI11] it is shown that [GRS08] is  $\Phi^\oplus$ -RKA-IND-CPA secure where  $\Phi^\oplus$  is the class of XOR relations. This class contains, for every  $\Delta \in \mathbb{Z}_2^\ell$ , the function  $\phi_\Delta(\mathbf{s}) \stackrel{\text{def}}{=} \mathbf{s} \oplus \Delta$ .

This is an interesting class of relations as (1) it captures realistic RKA and (2) many existing schemes (mostly block-ciphers) have actually been shown to

be insecure against  $\Phi^\oplus$ -RKA. Unfortunately  $\Phi^\oplus$ -RKA security does not imply any security in the realistic scenario where an adversary can not only flip, but set some of the bit of the secret key. Neither does it cover the case where the adversary can exchange the *position* of the key bits.

Using Theorem 1 we can show that the scheme is in fact secure against a much more powerful class of “affine relations”, which as special cases contains the relations just mentioned. Let  $\Phi_d^{\text{aff}}$  be the class which contains the functions

$$\phi_{\mathbf{X},\mathbf{x}}(\mathbf{s}) = \mathbf{X}^T \cdot \mathbf{s} \oplus \mathbf{x}$$

for every  $\mathbf{X} \in \mathbb{Z}_2^{\ell \times \ell}$ ,  $\mathbf{x} \in \mathbb{Z}_2^\ell$  where  $\text{rank}(\mathbf{X}) \geq d$ .

**Proposition 1.** *Under the (decisional)  $(\tau, \ell, d)$ -SLPN assumption<sup>5</sup> (which by Theorem 1 is equivalent to the standard LPN assumption), the encryption scheme from [GRS08] is  $\Phi_d^{\text{aff}}$ -RKA-IND-CPA secure.*

*Proof.* For any  $\phi \in \Phi_d^{\text{aff}}$ , samples of the form  $\mathbf{R}, \mathbf{R}^T \cdot \phi(\mathbf{s}) + \mathbf{e}$  are pseudorandom by assumption. So the outputs of both  $\text{Enc}_0^{\Phi_d^{\text{aff}}}(\mathbf{s}, \cdot, \cdot)$  and  $\text{Enc}_1^{\Phi_d^{\text{aff}}}(\mathbf{s}, \cdot, \cdot)$  are pseudorandom and thus indistinguishable.  $\square$

$\Phi_d^{\text{aff}}$  is a very powerful class of relations, and captures many realistic settings. It contains  $\Phi^\oplus$ , but also the class of relations  $\Phi_d^{\text{set}} \subset \Phi_d^{\text{aff}}$  which allows to overwrite all but  $d$  bits of the input, and the class  $\Phi^{\text{perm}} \subset \Phi_0^{\text{aff}}$  which allows to permute the key bits.<sup>6</sup> Previous to our work no scheme was known to be provably secure against  $\Phi_d^{\text{aff}}$ , or even just for one of the special cases  $\Phi_d^{\text{set}}$  (for  $d > 0$ ) or  $\Phi^{\text{perm}}$ . In fact, no *deterministic* encryption scheme can be secure against  $\Phi^{\text{perm}}$ , and no “natural”<sup>7</sup> deterministic scheme can be secure against  $\Phi_1^{\text{set}}$ .

## 4.2 Weak Randomness and New Constructions

The RKA security example from the previous section used the fact that an adversary can apply any affine function to the LWE secret. There are also natural implications from the fact that she can apply a mapping to the randomness  $\mathbf{r}$ . For example, it implies that LWE is hard, even if the randomness  $\mathbf{r}$  used to generate the samples  $\mathbf{r}^T \mathbf{s} + e$  is not uniform, but comes from a bit-fixing source [CGH<sup>+</sup>85]. Let us stress that the (comparably small) amount of randomness necessary to sample the error  $e$  must be uniform.

Theorem 1 not only has implications for existing constructions, but in subsequent work has inspired completely new constructions, most notably the authentication schemes and message authentications codes proposed in [KPC<sup>+</sup>11].

<sup>5</sup> This is the  $(2, \text{Ber}_\tau, \ell, d)$ -SLWE problem as given in Definition 2.

<sup>6</sup>  $\Phi^{\text{perm}} \subset \Phi_0^{\text{aff}}$  as it only contains  $\phi_{\mathbf{X},\mathbf{x}}$  where  $\mathbf{x} = \mathbf{0}^\ell$  and  $\mathbf{X}$  is a (full rank) permutation matrix.

<sup>7</sup> We need that every bit of the secret key is relevant, i.e.  $\text{Enc}(\mathbf{s}, \mathbf{m}) \neq \text{Enc}(\mathbf{s}', \mathbf{m})$  with good probability for  $\mathbf{s} \neq \mathbf{s}'$ .

## References

- [ABB10a] Shweta Agrawal, Dan Boneh, and Xavier Boyen. Efficient lattice (H)IBE in the standard model. In *EUROCRYPT 2010*, LNCS, pages 553–572. Springer, May 2010.
- [ABB10b] Shweta Agrawal, Dan Boneh, and Xavier Boyen. Lattice basis delegation in fixed dimension and shorter-ciphertext hierarchical IBE. In *CRYPTO 2010*, LNCS, pages 98–115. Springer, August 2010.
- [ABBC10] Tolga Acar, Mira Belenkiy, Mihir Bellare, and David Cash. Cryptographic agility and its relation to circular encryption. In *EUROCRYPT 2010*, LNCS, pages 403–422. Springer, May 2010.
- [ACPS09] Benny Applebaum, David Cash, Chris Peikert, and Amit Sahai. Fast cryptographic primitives and circular-secure encryption based on hard learning problems. In Shai Halevi, editor, *CRYPTO 2009*, volume 5677 of *LNCS*, pages 595–618. Springer, August 2009.
- [ADW09] Joël Alwen, Yevgeniy Dodis, and Daniel Wichs. Leakage-resilient public-key cryptography in the bounded-retrieval model. In Shai Halevi, editor, *CRYPTO 2009*, volume 5677 of *LNCS*, pages 36–54. Springer, August 2009.
- [AGV09] Adi Akavia, Shafi Goldwasser, and Vinod Vaikuntanathan. Simultaneous hardcore bits and cryptography against memory attacks. In Omer Reingold, editor, *TCC 2009*, volume 5444 of *LNCS*, pages 474–495. Springer, March 2009.
- [AHI11] Benny Applebaum, Danny Harnik, and Yuval Ishai. Semantic security under related-key attacks and applications. In *2nd Innovations in Computer Science (ICS)*, pages 45–60, 2011.
- [Ale03] Michael Alekhnovich. More on average case vs approximation complexity. In *44th FOCS*, pages 298–307. IEEE Computer Society Press, October 2003.
- [BC10] Mihir Bellare and David Cash. Pseudorandom functions and permutations provably secure against related-key attacks. In *CRYPTO 2010*, LNCS, pages 666–684. Springer, August 2010.
- [BDK06] Eli Biham, Orr Dunkelman, and Nathan Keller. New cryptanalytic results on IDEA. In Xuejia Lai and Kefei Chen, editors, *ASIACRYPT 2006*, volume 4284 of *LNCS*, pages 412–427. Springer, December 2006.
- [BDK08] Eli Biham, Orr Dunkelman, and Nathan Keller. A unified approach to related-key attacks. In Kaisa Nyberg, editor, *FSE 2008*, volume 5086 of *LNCS*, pages 73–96. Springer, February 2008.
- [BFKL94] Avrim Blum, Merrick L. Furst, Michael J. Kearns, and Richard J. Lipton. Cryptographic primitives based on hard learning problems. In Douglas R. Stinson, editor, *CRYPTO'93*, volume 773 of *LNCS*, pages 278–291. Springer, August 1994.
- [BG10] Zvika Brakerski and Shafi Goldwasser. Circular and leakage resilient public-key encryption under subgroup indistinguishability - (or: Quadratic residuosity strikes back). In *CRYPTO 2010*, LNCS, pages 1–20. Springer, August 2010.
- [BHII10] Boaz Barak, Iftach Haitner, Dennis Hofheinz, and Yuval Ishai. Bounded key-dependent message security. In *EUROCRYPT 2010*, LNCS, pages 423–444. Springer, May 2010.
- [BHOO08] Dan Boneh, Shai Halevi, Michael Hamburg, and Rafail Ostrovsky. Circular-secure encryption from decision diffie-hellman. In David Wagner, editor, *CRYPTO 2008*, volume 5157 of *LNCS*, pages 108–125. Springer, August 2008.

- [Bih94] Eli Biham. New types of cryptanalytic attacks using related keys. *Journal of Cryptology*, 7(4):229–246, 1994.
- [BK03] Mihir Bellare and Tadayoshi Kohno. A theoretical treatment of related-key attacks: RKA-PRPs, RKA-PRFs, and applications. In Eli Biham, editor, *EUROCRYPT 2003*, volume 2656 of *LNCS*, pages 491–506. Springer, May 2003.
- [BKW00] Avrim Blum, Adam Kalai, and Hal Wasserman. Noise-tolerant learning, the parity problem, and the statistical query model. In *32nd ACM STOC*, pages 435–440. ACM Press, May 2000.
- [BRS03] John Black, Phillip Rogaway, and Thomas Shrimpton. Encryption-scheme security in the presence of key-dependent messages. In Kaisa Nyberg and Howard M. Heys, editors, *SAC 2002*, volume 2595 of *LNCS*, pages 62–75. Springer, August 2003.
- [CDD<sup>+</sup>07] David Cash, Yan Zong Ding, Yevgeniy Dodis, Wenke Lee, Richard J. Lipton, and Shabsi Walfish. Intrusion-resilient key exchange in the bounded retrieval model. In Salil P. Vadhan, editor, *TCC 2007*, volume 4392 of *LNCS*, pages 479–498. Springer, February 2007.
- [CGH<sup>+</sup>85] Benny Chor, Oded Goldreich, Johan Hastad, Joel Friedman, Steven Rudich, and Roman Smolensky. The bit extraction problem of t-resilient functions (preliminary version). In *FOCS*, pages 396–407, 1985.
- [CHKP10] David Cash, Dennis Hofheinz, Eike Kiltz, and Chris Peikert. Bonsai trees, or how to delegate a lattice basis. In *EUROCRYPT 2010*, *LNCS*, pages 523–552. Springer, May 2010.
- [DGK<sup>+</sup>10] Yevgeniy Dodis, Shafi Goldwasser, Yael Tauman Kalai, Chris Peikert, and Vinod Vaikuntanathan. Public-key encryption schemes with auxiliary inputs. In *TCC 2010*, *LNCS*, pages 361–381. Springer, 2010.
- [DKL09] Yevgeniy Dodis, Yael Tauman Kalai, and Shachar Lovett. On cryptography with auxiliary input. In Michael Mitzenmacher, editor, *41st ACM STOC*, pages 621–630. ACM Press, May / June 2009.
- [DP07] Stefan Dziembowski and Krzysztof Pietrzak. Intrusion-resilient secret sharing. In *48th FOCS*, pages 227–237. IEEE Computer Society Press, October 2007.
- [DP08] Stefan Dziembowski and Krzysztof Pietrzak. Leakage-resilient cryptography. In *49th FOCS*, pages 293–302. IEEE Computer Society Press, October 2008.
- [DW09] Yevgeniy Dodis and Daniel Wichs. Non-malleable extractors and symmetric key cryptography from weak secrets. In Michael Mitzenmacher, editor, *41st ACM STOC*, pages 601–610. ACM Press, May / June 2009.
- [Dzi06] Stefan Dziembowski. Intrusion-resilience via the bounded-storage model. In Shai Halevi and Tal Rabin, editors, *TCC 2006*, volume 3876 of *LNCS*, pages 207–224. Springer, March 2006.
- [FKL<sup>+</sup>00] Niels Ferguson, John Kelsey, Stefan Lucks, Bruce Schneier, Michael Stay, David Wagner, and Doug Whiting. Improved cryptanalysis of Rijndael. In Bruce Schneier, editor, *FSE 2000*, volume 1978 of *LNCS*, pages 213–230. Springer, April 2000.
- [FS96] Jean-Bernard Fischer and Jacques Stern. An efficient pseudo-random generator provably as secure as syndrome decoding. In Ueli M. Maurer, editor, *EUROCRYPT'96*, volume 1070 of *LNCS*, pages 245–255. Springer, May 1996.

- [GKPV10] Shafi Goldwasser, Yael Kalai, Chris Peikert, and Vinod Vaikuntanathan. Robustness of the learning with errors assumption. In *1st Innovations in Computer Science (ICS)*, 2010.
- [GM84] Shafi Goldwasser and Silvio Micali. Probabilistic encryption. *Journal of Computer and System Sciences*, 28(2):270–299, 1984.
- [GPV08] Craig Gentry, Chris Peikert, and Vinod Vaikuntanathan. Trapdoors for hard lattices and new cryptographic constructions. In Richard E. Ladner and Cynthia Dwork, editors, *40th ACM STOC*, pages 197–206. ACM Press, May 2008.
- [GRS08] Henri Gilbert, Matthew J. B. Robshaw, and Yannick Seurin. How to encrypt with the LPN problem. In Luca Aceto, Ivan Damgard, Leslie Ann Goldberg, Magnús M. Halldórsson, Anna Ingólfssdóttir, and Igor Walukiewicz, editors, *ICALP 2008, Part II*, volume 5126 of *LNCS*, pages 679–690. Springer, July 2008.
- [HK07] Shai Halevi and Hugo Krawczyk. Security under key-dependent inputs. In Peng Ning, Sabrina De Capitani di Vimercati, and Paul F. Syverson, editors, *ACM CCS 07*, pages 466–475. ACM Press, October 2007.
- [HU08] Dennis Hofheinz and Dominique Unruh. Towards key-dependent message security in the standard model. In Nigel P. Smart, editor, *EUROCRYPT 2008*, volume 4965 of *LNCS*, pages 108–126. Springer, April 2008.
- [ISW03] Yuval Ishai, Amit Sahai, and David Wagner. Private circuits: Securing hardware against probing attacks. In Dan Boneh, editor, *CRYPTO 2003*, volume 2729 of *LNCS*, pages 463–481. Springer, August 2003.
- [JD04] Goce Jakimoski and Yvo Desmedt. Related-key differential cryptanalysis of 192-bit key AES variants. In Mitsuru Matsui and Robert J. Zuccherato, editors, *SAC 2003*, volume 3006 of *LNCS*, pages 208–221. Springer, August 2004.
- [Kea93] Michael J. Kearns. Efficient noise-tolerant learning from statistical queries. In *25th ACM STOC*, pages 392–401. ACM Press, May 1993.
- [Knu92] Lars R. Knudsen. Cryptanalysis of LOKI91. In Jennifer Seberry and Yuliang Zheng, editors, *AUSCRYPT'92*, volume 718 of *LNCS*, pages 196–208. Springer, December 1992.
- [KPC<sup>+</sup>11] Eike Kiltz, Krzysztof Pietrzak, David Cash, Abhishek Jain, and Daniele Venturi. Efficient authentication from hard learning problems. In *EUROCRYPT 2011*, *LNCS*, pages 7–26. Springer, 2011.
- [KS06] Jonathan Katz and Ji Sun Shin. Parallel and concurrent security of the HB and HB+ protocols. In Serge Vaudenay, editor, *EUROCRYPT 2006*, volume 4004 of *LNCS*, pages 73–87. Springer, May / June 2006.
- [KTX08] Akinori Kawachi, Keisuke Tanaka, and Keita Xagawa. Concurrently secure identification schemes based on the worst-case hardness of lattice problems. In Josef Pieprzyk, editor, *ASIACRYPT 2008*, volume 5350 of *LNCS*, pages 372–389. Springer, December 2008.
- [KV09] Jonathan Katz and Vinod Vaikuntanathan. Signature schemes with bounded leakage resilience. In Mitsuru Matsui, editor, *ASIACRYPT 2009*, volume 5912 of *LNCS*, pages 703–720. Springer, December 2009.
- [LMPR08] Vadim Lyubashevsky, Daniele Micciancio, Chris Peikert, and Alon Rosen. SWIFFT: A modest proposal for FFT hashing. In Kaisa Nyberg, editor, *FSE 2008*, volume 5086 of *LNCS*, pages 54–72. Springer, February 2008.
- [Luc04] Stefan Lucks. Ciphers secure against related-key attacks. In Bimal K. Roy and Willi Meier, editors, *FSE 2004*, volume 3017 of *LNCS*, pages 359–370. Springer, February 2004.

- [Lyu08] Vadim Lyubashevsky. Lattice-based identification schemes secure under active attacks. In Ronald Cramer, editor, *PKC 2008*, volume 4939 of *LNCS*, pages 162–179. Springer, March 2008.
- [Lyu09] Vadim Lyubashevsky. Fiat-Shamir with aborts: Applications to lattice and factoring-based signatures. In Mitsuru Matsui, editor, *ASIACRYPT 2009*, volume 5912 of *LNCS*, pages 598–616. Springer, December 2009.
- [MR04] Silvio Micali and Leonid Reyzin. Physically observable cryptography (extended abstract). In Moni Naor, editor, *TCC 2004*, volume 2951 of *LNCS*, pages 278–296. Springer, February 2004.
- [Pei09] Chris Peikert. Public-key cryptosystems from the worst-case shortest vector problem: extended abstract. In Michael Mitzenmacher, editor, *41st ACM STOC*, pages 333–342. ACM Press, May / June 2009.
- [Pie09] Krzysztof Pietrzak. A leakage-resilient mode of operation. In Antoine Joux, editor, *EUROCRYPT 2009*, volume 5479 of *LNCS*, pages 462–482. Springer, April 2009.
- [PR06] Chris Peikert and Alon Rosen. Efficient collision-resistant hashing from worst-case assumptions on cyclic lattices. In Shai Halevi and Tal Rabin, editors, *TCC 2006*, volume 3876 of *LNCS*, pages 145–166. Springer, March 2006.
- [PVW08] Chris Peikert, Vinod Vaikuntanathan, and Brent Waters. A framework for efficient and composable oblivious transfer. In David Wagner, editor, *CRYPTO 2008*, volume 5157 of *LNCS*, pages 554–571. Springer, August 2008.
- [PW08] Chris Peikert and Brent Waters. Lossy trapdoor functions and their applications. In Richard E. Ladner and Cynthia Dwork, editors, *40th ACM STOC*, pages 187–196. ACM Press, May 2008.
- [Reg05] Oded Regev. On lattices, learning with errors, random linear codes, and cryptography. In Harold N. Gabow and Ronald Fagin, editors, *37th ACM STOC*, pages 84–93. ACM Press, May 2005.
- [Ste94] Jacques Stern. A new identification scheme based on syndrome decoding. In Douglas R. Stinson, editor, *CRYPTO'93*, volume 773 of *LNCS*, pages 13–21. Springer, August 1994.
- [ZZWF07] Wentao Zhang, Lei Zhang, Wenling Wu, and Dengguo Feng. Related-key differential-linear attacks on reduced AES-192. In K. Srinathan, C. Pandu Rangan, and Moti Yung, editors, *INDOCRYPT 2007*, volume 4859 of *LNCS*, pages 73–85. Springer, December 2007.