

Cryptography from Learning Parity with Noise^{*}

Krzysztof Pietrzak

Institute of Science and Technology (IST) Austria

Abstract. The Learning Parity with Noise (LPN) problem has recently found many applications in cryptography as the hardness assumption underlying the constructions of “provably secure” cryptographic schemes like encryption or authentication protocols. Being provably secure means that the scheme comes with a proof showing that the existence of an efficient adversary against the scheme implies that the underlying hardness assumption is wrong.

LPN based schemes are appealing for theoretical and practical reasons. On the theoretical side, LPN based schemes offer a very strong security guarantee. The LPN problem is equivalent to the problem of decoding random linear codes, a problem that has been extensively studied in the last half century. The fastest known algorithms run in exponential time and unlike most number-theoretic problems used in cryptography, the LPN problem does not succumb to known quantum algorithms. On the practical side, LPN based schemes are often extremely simple and efficient in terms of code-size as well as time and space requirements. This makes them prime candidates for light-weight devices like RFID tags, which are too weak to implement standard cryptographic primitives like the AES block-cipher.

This talk will be a gentle introduction to provable security using simple LPN based schemes as examples. Starting from pseudorandom generators and symmetric key encryption, over secret-key authentication protocols, and, if time admits, touching on recent constructions of public-key identification, commitments and zero-knowledge proofs.

1 Learning Parity with Noise and Related Problems

The *search* version of the learning parity with noise problem with parameters $\ell \in \mathbb{N}$ (the length of the secret), $\tau \in \mathbb{R}$ where $0 < \tau < 0.5$ (the noise rate) and $q \in \mathbb{N}$ (the numbers of samples) asks to find a fixed random ℓ bit secret $\mathbf{s} \in \mathbb{Z}_2^\ell$ from q samples of the form $\mathbf{a}, \langle \mathbf{a}, \mathbf{s} \rangle \oplus e$ where $\mathbf{a} \in \mathbb{Z}_2^\ell$ is random and $e \in \mathbb{Z}_2$ has Bernoulli distribution with parameter τ (we denote this distribution with Ber_τ), i.e. $\Pr[e = 1] = \tau$. The *decisional* LPN problem is defined similarly, except that we require that one cannot even distinguish noisy inner products from random. The distinction between the search and the decisional version of a problem is often made for problems used in cryptography. Typically, assuming the decisional version of a problem allows for much simpler and more efficient constructions

^{*} This survey paper accompanies an invited talk at SOFSEM 2012.

of cryptosystems, whereas the search version is a weaker assumption and thus constructions based on it require less “faith” in the presumed hardness of the assumption.¹ Interestingly, for the LPN problem one can show that the distinction between the search and the decisional version is irrelevant, more on this below. Before we formally define the LPN problem, let us set the notational conventions for the rest of this paper.

Notation. \mathbb{Z}_q denotes the set $\{0, 1, \dots, q-1\}$, and addition is always modulo q . In particular, $\mathbb{Z}_2 = \{0, 1\}$ are bits and \oplus denotes bitwise XOR. We use bold small and capital letters like \mathbf{x}, \mathbf{X} to denote vectors and matrices, respectively. Calligraphic letters like \mathcal{X} denote sets. For a set \mathcal{X} , $x \xleftarrow{\$} \mathcal{X}$ denotes that x is assigned a value sampled uniformly at random from \mathcal{X} . For a distribution D , $x \leftarrow D$ denotes that x is sampled according to D . With Ber_τ we denote the Bernoulli distribution with parameter τ , i.e. $\Pr[x = 1 ; x \leftarrow \text{Ber}_\tau] = \tau$. For $m \in \mathbb{N}$, U_m denotes the uniform distribution over \mathbb{Z}_2^m . $X \sim D$ denotes that X is a random variable with distribution D . $\langle \mathbf{a}, \mathbf{b} \rangle = \sum_{i=1}^n \mathbf{a}[i] \cdot \mathbf{b}[i] \bmod p$ denotes the inner product of $\mathbf{a}, \mathbf{b} \in \mathbb{Z}_p^n$.

The Basic LPN Problem

Definition 1 (search/decisional LPN Problem). For $\tau \in]0, 1/2[$, $\ell \in \mathbb{N}$, the decisional $\text{LPN}_{\tau, \ell}$ problem is (q, t, ϵ) -hard if for every distinguisher D running in time t

$$\left| \Pr_{\mathbf{s}, \mathbf{A}, \mathbf{e}} [D(\mathbf{A}, \mathbf{A} \cdot \mathbf{s} \oplus \mathbf{e}) = 1] - \Pr_{\mathbf{r}, \mathbf{A}} [D(\mathbf{A}, \mathbf{r}) = 1] \right| \leq \epsilon \quad (1)$$

Where $\mathbf{s} \xleftarrow{\$} \mathbb{Z}_2^\ell$, $\mathbf{A} \xleftarrow{\$} \mathbb{Z}_2^{q \times \ell}$, $\mathbf{e} \leftarrow \text{Ber}_\tau^q$ and $\mathbf{r} \xleftarrow{\$} \mathbb{Z}_2^q$. The search $\text{LPN}_{\tau, \ell}$ problem is (q, t, ϵ) -hard if for every D running in time t

$$\Pr_{\mathbf{s}, \mathbf{A}, \mathbf{e}} [D(\mathbf{A}, \mathbf{A} \cdot \mathbf{s} \oplus \mathbf{e}) = \mathbf{s}] \leq \epsilon \quad (2)$$

The Learning with Errors (LWE) Problem. A problem closely related to LPN is the learning with errors (LWE) problem introduced by Regev [43]. LWE is a generalization of LPN to larger moduli. For some prime p ,² we have a secret $\mathbf{s} \in \mathbb{Z}_p^\ell$, and the adversary is asked to find \mathbf{s} given samples $\langle \mathbf{a}, \mathbf{s} \rangle + e$. Here \mathbf{a} is uniform in \mathbb{Z}_p^ℓ and the noise $e \in \mathbb{Z}_p$ is sampled according to some distribution χ , typically this distribution is a “discrete Gaussian”. A good survey paper on LWE and its applications is [44].³ LWE seems much more versatile than LPN. Besides all the cryptographic primitives we can construct from LPN, there are

¹ A typical example is public-key encryption based on the Diffie-Hellman problem, which is quite straight forward and efficient using the decisional version of the problem [14], but much more tricky and less practical using the search version [11].

² The case where the moduli is a the power of a prime has also been used [2].

³ A bibliography of LWE (and more generally, lattice) based cryptosystems is maintained on <http://xagawa.net/bib-lattice/>