Public-Key Encryption from the Lattice Isomorphism Problem

– Extended Abstract –

Léo Ackermann[1], Adeline Roux-Langlois[1], and Alexandre Wallet[2]

[1] Normandie Univ, UNICAEN, ENSICAEN, CNRS, GREYC, 14000 Caen, France
{leo.ackermann, adeline.roux-langlois}@cnrs.fr
[2] Inria, Univ Rennes, CNRS, IRISA, Rennes, France
alexandre.wallet@inria.fr

Abstract. We build a public-key encryption scheme relying on the Lattice Isomorphism Problem, which is the problem of deciding whether two lattices are rotations of each other. We generalize a restricted-to-$\mathbb{Z}^n$ scheme from *Benett et al.* using the quadratic form formalism. Our proposal benefits from more versatility, no floating points arithmetics, and relies on a plausibly falsifiable assumption.

Keywords: Public-key Encryption · Lattice Isomorphism Problem

Modern cryptography is challenged by the advent of quantum computers with enough quantum-bits and efficient error correction. In this still hypothetical setup both factorization and discrete logarithm problem are no longer hard as Shor's algorithm [**?**] can solve them in polynomial time. Lattices, or discrete subgroups of a real multidimensional space, have proven themselves as strong candidates for quantum-resistant cryptography. Besides conjectured quantum-resilient, the *average-case-worst-case* connection of lattice problems accounts for their attractivity. Decades of lattice-based cryptography gave birth to well understood hypotheses — eg. NTRU, the Learning With Errors (LWE) and the Small Integer Solution (SIS) problems — and a thick variety of constructions, ranging from public-key encryption scheme [**?**] and signatures [**?**] to fully homomorphic encryption [**?**] going through anonymous credentials [**?**,**?**]. Algebraically structured variants of those problems, relying on number theoretic structures, yield fast and compact schemes. Recent lines of works consider agressive variations of standard hypotheses to reach attractive performances [**?**,**?**,**?**].

At a high level, the current lattice-based schemes generate a public *random* lattice together with a trapdoor that forms the secret key. Typically, a random basis of the lattice is made public while a particular one, made of short and as orthogonal as possible vectors is kept secret. Breaking these schemes reduces to solving well-identified and well-studied hard problems over random lattices. One such problem is Bounded Distance Decoding (BDD): given a point very close to a lattice Λ, one is asked to return the closest lattice point. Heuristically, the concrete hardness of this problem is driven by the gap $\mathrm{gap}(\Lambda, \rho)$ between ρ,

the distance between Λ and the target, and half the Gaussian heuristic, which predicts the length of the shortest vectors in "random enough" lattices. It turns out that solvers perform much better when $\mathrm{gap}(\rho, \Lambda)$ gets large. For LWE, SIS, NTRU schemes, one expects a $O(\sqrt{n})$-gap, but other classes of lattices can reach much smaller gaps. For example, Barnes-Sloane lattices [**?**] have decoding gap as small as $\Theta(\sqrt{\log n})$. Consequently, these lattices give a much better concrete BDD security at a given dimension; equivalently, they require quite smaller dimension to reach a given security level, leading to efficiency improvements. This is an unfortunate aspect of the current "standard" lattice-based cryptography: hypotheses on random lattices and their subsequent constructions barely connect with the luxuriant litterature on remarkable lattices.

■ Minimal preliminaries

Vectors and matrices. Matrices are denoted by bold capital letters (eg. $\mathbf{B}$), the transpose operator by $\cdot^{\mathsf{T}}$ and the dual by $\cdot^{\vee}$. (Column) vectors are denoted by bold letters (eg $\mathbf{x}$).

Spaces. Let $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{R}$ denote respectively the set of natural numbers, integers and reals. The discretized n-dimensional hypercube is $\mathcal{H}_q^n = \{0, 1/q, \ldots, (q-1)/q\}^n$. We denote the general linear group of degree n over $\mathbb{Z}$ by $\mathrm{GL}_n(\mathbb{Z})$, the set of symmetric positive definite matrices of dimension $n \times n$ over $\mathbb{R}$ by $\mathrm{S}_n^{++}(\mathbb{R})$.

Lattices. A (full-rank) lattice Λ is an n-dimensional discrete subgroup of $\mathbb{R}^n$. As such, it admits a smallest non-zero vector of length $\lambda_1(\Lambda)$. The gaussian heuristics $gh(\Lambda)$ gives an estimate of $\lambda_1(\Lambda)$ and is accurate for random lattices[3].

Quadratic forms. Quadratic forms can be represented by real symmetric matrices. In this work we will only be interested in the positive definite case, i.e. elements of $\mathrm{S}_n^{++}(\mathbb{R})$. A quadratic form Q represented by a matrix $\mathbf{Q} \in \mathrm{S}_n^{++}(\mathbb{R})$ defines a scalar product $\langle \mathbf{x}, \mathbf{y} \rangle_Q = \mathbf{x}^{\mathsf{T}}\mathbf{Q}\mathbf{y}$, with its associated Euclidean norm $\|\mathbf{x}\|_Q^2 = \mathbf{x}^{\mathsf{T}}\mathbf{Q}\mathbf{x}$. The relation $\mathcal{R}$ that relates $\mathbf{Q}$ to $\mathbf{Q}'$ whenever there exists $\mathbf{U} \in \mathrm{GL}_n(\mathbb{Z})$ such that $\mathbf{Q}' = \mathbf{U}^{\mathsf{T}}\mathbf{Q}\mathbf{U}$ is an equivalence relation, and $[Q]$ denotes the class of Q. The smallest length of a vector of $\mathbb{Z}^n$ through the induced norm, ie. $\min_{\mathbf{x} \in \mathbb{Z}^n \setminus \{0\}} \sqrt{\mathbf{x}^{\mathsf{T}}\mathbf{Q}\mathbf{x}}$, only depends on the class and is written $\lambda_1([Q])$. The n-th minima is the infimum of the radii of 0-centered balls[4] containing i linearly independent $\mathbb{Z}^n$ vectors.

Gaussians. The gaussian function for the quadratic form Q with width parameter σ is $\rho_{Q,\sigma}(\mathbf{x}) = \exp(-\pi\|\mathbf{x}\|_Q^2/\sigma^2)$, for all $\mathbf{x} \in \mathbb{R}^n$. When $\sigma = 1$, the subscript is omitted. Elliptic Gaussians behave much like spherical ones: if $\mathbf{Q} = \mathbf{L}^{\mathsf{T}}\mathbf{L}$, then $\|\mathbf{x}\|_Q = \|\mathbf{L}\mathbf{x}\|$. The discrete Gaussian distribution $\mathcal{D}_{Q,\sigma}$ with width parameter σ is defined by the probability density function $\Pr_{\mathbf{x} \hookleftarrow \mathcal{D}_{Q,\sigma}}(\mathbf{x} = \mathbf{y}) = \frac{\rho_{Q,\sigma}(\mathbf{y})}{\rho_{Q,\sigma}(\mathbb{Z}^n)}$,

[3] We refer to [**?**] for an intelligible definition of a random lattice.
[4] Note that *balls* are implicitly defined using the quadratic norm.

for any $\mathbf{y} \in \mathbb{Z}^n$. Sampling along this distribution can be done efficiently [?]. We denote by $\eta_\epsilon([Q])$ the smoothing parameter of a class. Informally, above this threshold, the reduction *mod 1* of a (continuous) Gaussian vector of covariance $Q' \in [Q]$ is indistinguishable from a uniformly distributed point in $[0,1)^n$.

■ The Lattice Isomorphism Problem

The Lattice Isomorphism Problem (LIP) is a tentative at giving more attention to remarkable lattices and their strong geometric properties. It was first introduced in [?] and further studied in [?]. In its search variant, it asks to find an isomorphism between two lattices given as input, should it exist. In [?], Ducas and van Woerden bring the LIP problem on the cryptographic frontline and showed how to build core primitives founded on this problem. In an independent work [?], Bennett *et al.* study similar ideas but restricted to the $\mathbb{Z}^n$ lattice. This new approach for building primitives from lattices shares the flavour of first code-based and multivariate constructions [?]. In the former, illustrated for example by McEliece's public key encryption scheme, a code G with an efficient decoder is hidden by permutation S, P as $G^{pub} = SGP$; in the latter, an easy-to-invert quadratic map $\mathcal{Q}$ is masked by affine transformations T, S as $\mathcal{Q}^{pub} = T \circ \mathcal{Q} \circ S$. In the LIP paradigm, a lattice of known good basis is hidden by $\mathbf{B}^{\mathsf{pub}} = \mathbf{OBU}$ where $\mathbf{U}$ is unimodular (integer entries and determinant ± 1) and $\mathbf{O}$ is a rotation. Only someone knowing $(\mathbf{U}, \mathbf{O})$ can benefit from the good properties of $\mathbf{B}$. Should one only use $\mathbf{U}$, as in the GGH encryption scheme [?], then attacks exist, so on the first look, one would need to deal with rotation matrices having irrational entries.

LIP-based cryptography can fortunately be rephrased using quadratic forms instead of lattices bases. Therefore, rather than considering rotated lattices as in [?], one can essentially work *modulo rotation*. We have $(\mathbf{B}^{\mathsf{pub}})^\mathsf{T}\mathbf{B}^{\mathsf{pub}} = \mathbf{U}^\mathsf{T}(\mathbf{B}^\mathsf{T}\mathbf{B})\mathbf{U}$ which gives a nice reformulation over the Gram matrix of $\mathbf{B}$ and $\mathbf{B}^{\mathsf{pub}}$, that are quadratic forms. In other words, the lattices described by the bases $\mathbf{B}$ and $\mathbf{B}'$ are isomorphic if and only if the corresponding Gram matrices $Q_\mathbf{B}, Q_{\mathbf{B}'}$ are congruent *using unimodular matrices*. With such a reformulation, a natural playground for representing the space is to work within $\mathbb{Z}^n$ but with a norm that reflects the geometry of lattices of one's choice. This observation gives rise to the following formulation of the search version of LIP.

Definition 1 (wc-LIP^{Q_0}, quadratic form version). *Given quadratic forms Q and Q_0 from $\mathrm{S}_n^{++}(\mathbb{R})$, find $\mathbf{U} \in \mathrm{GL}_n(\mathbb{Z})$ such that $Q = \mathbf{U}^T Q_0 \mathbf{U}$, should it exists.*

Staying concretely within $\mathbb{Z}^n$ seems to significantly ease implementations of LIP-based scheme, compared to their equivalent in standard lattice-based cryptography. The recent `Hawk` proposal [?] to NIST's second call for standardization can be compared performance-wise to `Falcon` [?], boasting much simpler[5] implementation constraints on top.

[5] Implementing the Gaussian sampler of `Falcon` is a notoriously difficult task.

As many cryptographic problems, LIP is unlikely to be NP hard. Nevertheless, it benefits from worst-case to average-case self-reduction *within* an instantiation *class*. Informally, for a fixed equivalence class $[Q_0] = \{\mathbf{U}^\mathsf{T} Q_0 \mathbf{U} \mid \mathbf{U} \in \mathrm{GL}_n(\mathbb{Z})\}$ of quadratic forms, there is an efficient way [**?**, lem. 3.9] of generating a random member of the class with corresponding LIP instance being *as hard as possible*[6]. In this document, we denote by $\mathtt{QFS}_{Q,s}$ the (non-deterministic) sampler within the class of $[Q]$ with parameter s, and by $\mathcal{D}_s([Q])$ its output distribution. Additionally, the connection of LIP with the Graph Isomorphism Problem (GIP) [**?**] accounts for its assumed theoritical hardness.

Besides the work of [**?**], the LIP problem restricted to the $\mathbb{Z}^n$ lattice has been the focus of [**?**,**?**], to improve understanding of LIP hardness in what is arguably the most simple lattice one can think of. In particular, it helps driving throughout hazardous choices when instantiating the LIP problem on concrete quadratic form classes.

For now, despite the exciting connection with other isomorphism problems, such as the GIP problem, only low-level constructions exist: an identification scheme, two hash-and-sign signatures and a key-exchange mechanism, all described in [**?**].

■ A LIP-based public-key encryption scheme

We propose the *first* public-key encryption scheme *founded on LIP*. More precisely, it relies on a mild restriction of its distinguishing variant that we note $\Delta\mathsf{LIP}_{\mathsf{pke}}$. Under the assumption that the aforementionned problem is hard for the considered classes of quadratic forms, our scheme achieves IND-CPA security. The latter essentially means that any adversary has negligible probability of guessing the encrypted bit. This completes the set of fundamental primitives that can be built from the LIP assumption.

It should be noted that encryption of communications can already be done relying on LIP, using the key-exchange mechanism from [**?**]. In such a scheme, two parties agree upon a common private key by decoding a small (Gaussian) element. Private communications follow using symmetric encryption. Our scheme's target is beyond: besides encryption, a PKE scheme is a first step toward more advanced cryptography. For example, one could think of identity-based or attribute-based encryption as future objectives.

The new ΔLIP$_{pke}$ security assumption. This new assumption stems from the distinguishing variant of LIP that appears in [**?**], and consists in guessing to which which class a quadratic form belongs to given two proposals. At a high level our assumption $\Delta\mathsf{LIP}_{\mathsf{pke}}$ states that this variant remains secure when one restricts the set of possible instances to those where the smoothing parameter differ significantly between classes. Formally, the corresponding cryptographic game is defined as such.

[6] This is an example of worst-case to average-case reduction

Definition 2 ($\Delta\mathsf{LIP}^{Q_0,Q_1}_{\mathsf{pke},s}$[7]). *Given Q_0 and Q_1 from $\mathrm{S}^{++}_n(\mathbb{R})$ such that there exists an efficient algorithm for bounded distance decoding at distance $r \leq \lambda_1([Q_0])/2$ in $[Q_0]$ and $\eta_\varepsilon([Q_1]) < r$, and a quadratic form sampled as $(Q,\cdot) \leftarrow \mathtt{QFS}_{Q_b,s}$ where $b \hookleftarrow_\$ \{0,1\}$, guess b.*

The scheme. At a high-level, our PKE scheme can be seen as an adaptation of the Dual-Regev PKE from [**?**] with a LIP flavour. The design is inspired from [**?**], but our approach 1) is not restricted to (rotations of) the $\mathbb{Z}^n$ lattice (ie. with the class of equivalence of the n-dimensional identity); 2) is founded on a concrete assumption such as LIP — recall that rotations involves irrational numbers, while LIP can be dealt with mostly with rationals. The encryption correctness relies on the strong concentration of high-dimensional Gaussian vectors. Ciphertexts live in the unit discretised n-cube $\mathcal{H}^n_q$ with lower vertice at the origin; if the ciphertext corresponds to 0, it is uniformly distributed; if it corresponds to a 1, it is the reduction of an Gaussian modulo $\mathbb{Z}^n$, with a covariance matrix corresponding to the public quadratic form, and the closeness is therefore measured in the induced norm. On the one hand, once reduced modulo the cubic lattice, the Gaussian distribution will strongly concentrate around the vertices of $\mathcal{H}^n$, as shown in Figure 1. On the other hand, uniformly distributed vectors are much more likely to be in the inner part of the domain, since this is where most of the mass is. In the full version, we show that encryptions of 1 are in fact so close to the vertices that there is essentially no chance that they be mistaken for an element sampled uniformly at random within $\mathcal{H}^n_q$ or a discretized version of it, thanks to the properties of the smoothing parameter. Using the decoding algorithm $\mathtt{Dec}$ associated to the public form, the secret key owner can know how far the ciphertext was from the $\mathbb{Z}^n$ lattice, and conclude: a ciphertext close to the lattice corresponds to a 1, and a ciphertext far away from the lattice to a 0.

Theorem 1. *Restricted to instantiation where $\lambda_1(S_n)$ is smaller that 2 – which can always be achieved by rescaling[8] – any generated keypair (pk, sk) is such that for any bit b it holds with overwhelming probability that $\mathtt{Dec}(sk, \mathtt{Enc}(pk, b)) = b$.*

An intuition for the hardness, illustrated in Figure 1, is the following: an adversary ignoring the secret key is unable to observe $\mathcal{H}^n$ through the good norm, and distribution of points of $\mathcal{H}^n$ that are close to the vertices of the hypercube is mixed up in their point of view. In other words, given a ciphertext, they cannot compute efficiently the closeness of the cipher to a vertice without the secret key. More formally, we rely on the $\Delta\mathsf{LIP}_{\mathsf{pke}}$ hypothesis. Indeed, if the adversary cannot find which class the public form belongs to, in their view everything happens as if the smoothing parameter is big enough that the reduced Gaussian distribution mimics uniform distribution.

Theorem 2. *If the ΔLIP_{pke} problem is hard, then the scheme is IND-CPA secure.*

[7] When $Q_0, Q_1$and s are clear from context, sub/super-scripts are omitted.

[8] Recall that one of the purpose of LIP is to instantiate scheme on remarkable lattices: the first minimum of such lattices is likely to be known.

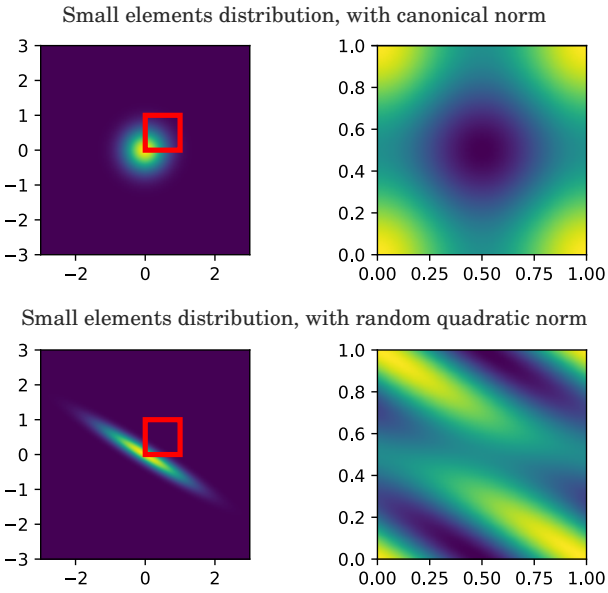

Fig. 1. Distribution of 2-dimensional small elements reduced modulo $\mathcal{H}^2$, either for the Euclidean norm or the norm induced by a random quadratic form.

The scheme is fully specified in Figure 2. At the core of the proof of Theorem 1 is a counting argument. We describe the number of points that are likely to be output by the reduced-gaussian sampler as the cardinal of the intersection of $\mathbb{Z}^n$ and an ellipsoid. Such estimates are the topic of classic mathematical problems, and we find a good-enough approximation thanks to a result of Landau [**?**]. The proof of Theorem 2 is then a game-based proof that turns the original IND-CPA game into a variant where encryptions of 0 and 1 follow the same distribution.

Looking for a concrete scheme, one can deviate from the parameter regime deduced from our proof, as is standard in cryptography. Then, the scheme can be instantiated on any particular lattice with efficient decoder, such as the hypercubic lattice $\mathbb{Z}^n$ as before, but also (again) Barnes-Wall lattices, and many more, enjoying possibly strong properties. For example, having a lattice minima closer to the Gaussian heuristics gives better concrete security at given dimension.

Encryption of bits may seems limiting but this is the case of many unstructured lattice encryption schemes (eg. Regev and Dual-Regev schemes). Pratical schemes in fact considered algebraically structured lattices to achieve m bits messages at the cost of possibly weaker assumptions, that restrict standard assumptions to specific classes[9] of lattices.

[9] The typical choices nowadays are lattices coming from ideals in cyclotomic number field field. See eg. [**?**] for details.

Protocol 1. Public-key encryption

Let $(S_n)_{n\in\mathbb{N}} = (\mathbf{B}_{S_n}^\mathsf{T}\mathbf{B}_{S_n})_{n\in\mathbb{N}}$ be a family of n-dimensional quadratic forms with an efficient decoding algorithm $\mathtt{Dec}_{\mathbf{S}_n}$ of known decoding radius $r_n < \lambda_1(S_n)/2$, and such that

$$\psi(n) = 1/\sqrt{\pi n} \cdot \det(S_n)^{-1/2} \cdot (2e\pi r_n^2)^{n/2}$$

is negligible. Let $n \in \mathbb{N}$, $s \geq \max\left\{\lambda_n(S), \|\mathbf{B}_S^*\| \cdot \sqrt{\ln(2n+4)/\pi}\right\}$. Further, let $q = \left\lceil \frac{sn}{r} \cdot \sqrt{\ln(2n+4)/\pi} \right\rceil$.

— **Key Generation** —

1: Sample $(P, \mathbf{U}) \leftarrow \mathtt{QFS}_{S,s}$ ▷ $P = \mathbf{U}^\mathsf{T} S \mathbf{U}$, see [?, lem. 3.9] for details
2: Return $(pk, sk) = (P, \mathbf{U})$

— **Encryption of 0** —

1: Sample $\mathbf{e} \hookleftarrow 1/q \cdot D_{P,qr/\sqrt{n}}$
2: Compute $\mathbf{c} \leftarrow \mathbf{e} \mod \mathbb{Z}^n$
3: Return $\mathbf{c}$, living in $\mathcal{H}_q^n$

— **Encryption of 1** —

1: Sample $\mathbf{c} \hookleftarrow \mathcal{U}(\mathcal{H}_q^n)$
2: Return $\mathbf{c}$, living in $\mathcal{H}_q^n$

— **Decryption** —

1: Compute $\mathbf{y} \leftarrow \mathtt{Dec}_S(\mathbf{Uc})$ ▷ Algorithm of protocol requierements
2: Compute $\mathbf{z} = \mathbf{c} - \mathbf{U}^{-1}\mathbf{y}$
3: If $\mathbf{z} \in \mathcal{H}_q^n$ and $\|\mathbf{z}\|_P \leq r$:
4: Return 0
5: Return 1

Fig. 2. Public-key encryption scheme

■ Security and cryptanalysis discussion

We briefly discuss possible candidates to found the hardness of $\Delta\mathsf{LIP}_{pke}$. As observed in prior works, easy instances exist: any pair of forms that do not have the same determinant; or the same parity; or more generally, that do not belong to the same genus, that is, the set of all equivalence classes for the relation $\mathcal{R}$ over p-adic integers for all prime p, can be distinguished in polynomial time. When restricted to pairs sharing at least these identified invariants, there are reasons to believe that $\Delta\mathsf{LIP}_{\mathsf{pke}}$ is a difficult problem. Our efforts unfortunately could not go beyond the current state of the art of the hardness of $\Delta\mathsf{LIP}$.

Another invariant of a lattice is its *theta series*, a power series used to encode all lattice points by sorting them by (squared) norm. We however observe that theta series does not seem to be useful in the context of breaking $\Delta\mathsf{LIP}_{\mathsf{pke}}$. On the one hand, while the theta series can give accurate estimates of the smoothing parameter of lattices [?], computing the first terms of the series amounts

to solving the shortest vector problem by enumeration. This certainly requires exponential time at current state of knowledge. On the other hand, starting with dimension 4 [**?**], the theta series does not carry enough information to completely characterize a lattice. Lattices sharing the same theta series but not equivalent to one another are called *isospectral*. Knowing one such pair, one can build many other: if (L_1, L_2) is isospectral, then $(\Lambda \oplus L_1, \Lambda \oplus L_2)$ is also isospectral, for any lattice Λ.

Restricted to unimodular lattices, that is, self-dual lattices, the IND-CPA security of our scheme relies on the following mild assumption, which is reminiscent of [**?**].

Conjecture 1 (Mild version). For any (Q_0, Q_1) instance of $\Delta\mathsf{LIP}_{\mathsf{pke}}$ of dimension n, with equal polytime computable $\mathcal{R}$-invariants arithmetic quantities, $1 \leq \max\{gh(Q_i)/\lambda_1(Q_1), gh(Q_i^\vee)/\lambda_1(Q_i^\vee)\}$, the problem wc-$\Delta\mathsf{LIP}_{\mathsf{pke}}^{Q_0,Q_1}$ is $2^{\Theta(n)}$-hard.

While we gave clues that distinguishing between quadratic classes should not be easier if they differ by their smoothing parameter it may seem quite tricky to find family of lattices that could give an instance of $\Delta\mathsf{LIP}_{\mathsf{pke}}$ in the regime of parameter we need. Therefore, falsifying our security assumption seems tough at first sight. This is not surprising: the authors of [**?**] had already observed that it was quite unclear how to instantiate their $\mathbb{Z}^n$, rotation-based scheme with parameters reasonably close to their proof's regime (if possible at all!). Similar observation appear in [**?**]. This is partly due to the difficulty of understanding the genus of high-dimensional lattices. Nevertheless, in the full-version we support[10] our new assumption by showing that the famous Barnes-Wall lattices actually provide candidates for its plausibility, only missing the exact requirement by small *constant* factors. In dimension 2^m with m odd, these are unimodular even lattices, which are also known to form a single genus on top of many of fascinating properties: this may suggest to look more into these class of lattices.

■ Open questions

The first research direction we want to highlight is further reductionist effort. It seems reasonable to think that $\Delta\mathsf{LIP}$ problems restricted to classes that mainly differ by a gap on some quantity $\chi(\Lambda)$ is a problem simpler than a Gap problem (eg. GapSVP is a famous problem Gap on lattices, regarding the shortest vector's length) on this quantity. Is this even true? What can be said of the opposite direction? See that if those problems were in fact equivalent, $\Delta\mathsf{LIP}$ could be seen as a generic way to consider Gap problems in cryptography while easing space requirements.

The second one concerns falsifiability of the assumption: can the $\Delta\mathsf{LIP}_{\mathsf{pke}}$ assumption we rely on be effectively instantiated, and concretely cryptanalysed? As priorly stressed, gaps of $\mathbb{Z}^n$ are not that small, and one could expect better performances at fixed security level with our scheme instantiated on lattices with smaller gaps, such as Barnes-Wall lattices [**?**]. As highlighted in the previous

[10] More precisely, besides cryptanalysis, we give clues for its falsifiability.

paragraph, this question is open since [**?**]. A way of tackling this problem is a further study of the existence of optimal unimodular even quadratic form — a form is optimal when its minimum is the largest possible in a genus, and extremal when it reaches a known upper bound for these forms, of $2\lfloor n/24 \rfloor + 2$. It is known that extremal forms cannot exist above dimensions 163264, but they may exist for cryptographic sizes; nonetheless, we propose the conjecture that optimal forms could have minima large enough to answer the problem. Another promising direction is to use the Siegel-Weill mass formula that give (efficiently) the *average* theta series of a given genus: a mean argument could suffice to deduce the existence of quadratic forms that fit our requirements[11].

[11] This would not necessarily give *concrete* falsifiability as the matching form may remain unknown.