# Weiqiang Wen, LIP, ENS de Lyon

Age: 27
Nationality: Chinese

## Address

École Normale Supérieure de Lyon
46 allée d'Italie
69364 Lyon Cedex, France
Télephone: +33 06 70 50 40 71
Fax: +86-020-8521 5418
E-mail: weiqiang.wen@ens-lyon.fr
Homepage: perso.ens-lyon.fr/weiqiang.wen

## Education

- Since 09/2015, Ph.D., École Normale Supérieure de Lyon, France; working on "Algorithms for hard lattice problems".
  Supervisor: Prof. Damien Stehlé
- 09/2012–07/2015, Master, South China Normal University, China; working on "Key exchange for post quantum era".
  Supervisor: Prof. Libin Wang
- 09/2008–07/2012, Bachlor, South China Normal University, China; major in "Computer Science and Technology".

## Publications

- Shi Bai, Damien Stehlé and W. Wen. Improved Reduction from the Bounded Distance Decoding Problem to the Unique Shortest Vector Problem in Lattices, ICALP'16, 2016.
- W. Wen, Libin Wang and Jiaxin Pan. Unified Security Model of Authenticated Key Exchange with Specific Adversarial Capabilities. IET Information Security, 2016, 10(1), pp. 8–17.

## Preprint

- Zvika Brakerski, Elena Kirshanova, Damien Stehlé, W. Wen. Learning With Errors and Extrapolated Dihedral Cosets. In submission to Crypto.

## Training

- 19/01/2017–24/01/2017, Course “Writing A Scientific Paper Step by Step", 20 hours, instructor: Martha Boeglin, Université de Lyon, France.
- 14/11/2016–18/11/2016, “COST-IACR" School on Randomness in Cryptography, 24 hours, instructors: Yevgeniy Dodis et al., Pompeu Fabra University, Barcelona, Spain.
- 10/2015–05/2016, Course “Français Langue Étrangère", 40 hours, instructor: Claire Deslauriers, ENS de Lyon, France.

## Internship

- 01/2015–08/2015, Internship student at LIP, ENS de Lyon; working on algorithms for hard lattice problems under the supervision of Prof. Damien Stehlé.

## Awards

- National Scholarship, 2009-2010.
- Excellent graduate, 2012.
- Funded by Postgraduate Science Foundation (SCNU), 2013-2014.
- Outstanding master thesis, 2015.

## Languages

| | |
|---|---|
| Chinese | mother language |
| English | read, write, speak |

## Computer skills

- Systems: Linux and Windows.
- Languages: proficient in Java, C/C++, LaTeX; familiar with Python, C#, Sage, Prolog.

Damien STEHLÉ
Professor, ENS de Lyon
LIP [UMR5668 – ENSL, CNRS, INRIA, UCBL, U. Lyon]
46 Allée d'Italie 69007 Lyon
04 72 72 85 47
damien.stehle@ens-lyon.fr

Lyon, le 16 mars 2017

**Avis sur l'avancée des travaux de thèse de Weiqiang Wen**

Chère collègue, cher collègue,

Weiqiang est arrivé au LIP au printemps 2015, dans le cadre d'une période d'essai prédoctorale, après des études universitaires à la *South China Normal University* (Canton, Chine). Ce stage portait sur la difficulté du problème *Learning With Rounding*. En particulier, nous avions obtenu une réduction efficace depuis le problème *Learning With Errors* (LWE), améliorant significativement l'état de l'art. Malheureusement, une équipe concurrente dirigée par Alon Rosen avait obtenu les mêmes résultats et nous a devancés (avec publication dans les actes de la conférence TCC 2016). Ces travaux n'ont donc pas donné lieu à publication de notre part. Néanmoins, les capacités que Weiqiang avaient démontrées m'ont tout-à-fait convaincu d'accepter sa demande de poursuivre en doctorat.

À l'automne 2015, suite à une suggestion de Shi Bai qui était alors post-doctorant dans l'équipe, Weiqiang s'est intéressé au lien entre les problèmes *Bounded Distance Decoding* (BDD) et *Unique Shortest Vector* (uSVP). BDD est une variante pire-cas de *Learning With Errors* utilisée en cryptographie et théorie des communications. Weiqiang, Shi et moi-même avons amélioré la meilleure réduction connue de BDD à uSVP en utilisant des techniques de sous-réseaux aléatoires et d'empilements de sphères. Après des suggestions initiales de pistes de recherche, Weiqiang a été le moteur de ce projet. L'article correspondant a été accepté pour publication dans les actes de la conférence ICALP 2016. Weiqiang est allé y présenter le résultat.

Depuis l'été dernier, Weiqiang étudie la difficulté quantique du problème LWE. Regev avait proposé en 2003 une réduction de BDD au *Dihedral Coset Problem* (DCP), et une réduction de DCP à *Subset Sum*. Ces réductions permettent de situer les problèmes de réseaux euclidiens par rapport à un problème quantique naturel et bien étudié. LWE étant une version randomisée de BDD, cette chaîne de réductions s'y applique également, mais elle est très lâche, dans le sens où *Subset Sum* est potentiellement bien plus difficile que LWE (et BDD). Dans un travail en commun avec Zvika Brakerski, Elena Kirshanova, et moi-même, Weiqiang a proposé une variant de DCP admettant une réduction depuis LWE et une autre vers LWE. L'article correspondant a été soumis à la conférence CRYPTO 2017.

Depuis cette soumission, Weiqiang envisage plusieurs directions pour la poursuite de sa thèse : l'étude de l'impact pratique de sa réduction de BDD à uSVP, la résistance de cryptosystèmes reposant sur les réseaux face à des adversaires quantiques, et enfin la conception de protocoles cryptographiques prouvés sûrs sous l'hypothèse que LWE est difficile.

Depuis sa venue, Weiqiang effectue un travail de très bonne qualité. Il s'est bien intégré dans l'équipe et participe activement à sa vie scientifique (il a donné plusieurs séminaires, et plusieurs exposés dans le cadre d'un groupe de travail hebdomadaire, il a construit le site internet du pôle crypto de l'équipe AriC, etc). Son autonomie scientifique est grandissante, et ses qualités d'intelligence et de travail me rendent totalement confiant quant à sa capacité à progresser dans ses recherches et à produire des résultats de toute première classe.

Damien Stehlé

Stehlé

# ÉCOLE NORMALE SUPÉRIEURE DE LYON

March 16th, 2017

Weiqiang Wen
*LIP, ENS Lyon*

Mission: **progress report (09.2015–03.2017) and future plan (from 03.2017)**

**PhD advisor.** Damien Stehlé (ENS de Lyon professor, LIP)
**PhD project.** Algorithm for hard lattice problems.
**PhD duration.** From September, 2015 to August, 2018 (planned).

**Research during 09.2015–03.2017.**

A (full-rank) Euclidean lattice $\mathcal{L}$ is the set of all integer linear relations of some linearly independent vectors in a Euclidean space. These vectors form a basis of this lattice. There are two central computational problems on lattice.

- The shortest vector problem (SVP). Given as input a basis of a lattice, find a shortest non-zero vector in the lattice.
- The closest vector problem (CVP). Given as inputs a basis of a lattice and a (target) vector in the real span of the lattice, find a lattice vector closest to the target vector.

The first minimum $\lambda_1(\mathcal{L})$ is the smallest length between two distinct lattice vectors in lattice $\mathcal{L}$. A commonly used variant of CVP is the Bounded Distance Decoding problem with parameter $\alpha > 0$ ($\mathrm{BDD}_\alpha$): Given as inputs a basis of a lattice $\mathcal{L}$ and a (target) vector $\mathbf{t} \in \mathbb{Q}^n$ within distance $\alpha \cdot \lambda_1(\mathcal{L})$ of $\mathcal{L}$, the goal is to find a vector $\mathbf{b} \in \mathcal{L}$ closest to $\mathbf{t}$. The second minimum $\lambda_2(\mathcal{L})$ is defined as the minimal radius of a zero-centered ball that contains two or more linearly independent vectors from $\mathcal{L}$. Respectively, we also consider a variant of SVP, called the unique Shortest Vector Problem with parameter $\gamma \geq 1$ ($\mathrm{uSVP}_\gamma$). $\mathrm{uSVP}_\gamma$ consists in finding a shortest non-zero vector in a given lattice $\mathcal{L}$, under the promise that $\lambda_2(\mathcal{L}) \geq \gamma \cdot \lambda_1(\mathcal{L})$.

A solution for solving BDD is to use Kannan's embedding technique to reduce it to uSVP, and then use a uSVP oralce (typically, a lattice reduction algorithm). The principle of Kannan's embedding is to map the offset between $\mathbf{t}$ and a closest vector to $\mathbf{t}$, to a shortest non-zero vector in a lattice of larger dimension. In that lattice, the minimum $\lambda_1$ corresponds to that offset, is much shorter than $\lambda_2$, which is related to the first minimum of the initial lattice.

My main result this year defines the hardness relationship between BDD and uSVP. The reduction from BDD to uSVP is initially given by Lyubashevsky and Micciancio in [1], who showed that $\mathrm{BDD}_{1/(2\gamma)}$ reduces to $\mathrm{uSVP}_\gamma$ for any $\gamma \geq 1$. Later, Liu *et al.* [2] refined the analysis of Lyubashevsky and Micciancio and proved that $\mathrm{BDD}_{1/\gamma_1}$ reduces to $\mathrm{uSVP}_\gamma$ with $\gamma_1 = \sqrt{3/(4-\gamma^2)}\gamma + 1$, for any $\gamma \in (1, 1.9318)$. It is folklore [3, 4] that the analysis can be tightened even more, resulting in a proof that $\mathrm{BDD}_{1/\gamma_1}$ reduces to $\mathrm{uSVP}_\gamma$ with $\gamma_1 = (2\gamma^2 + 2\lfloor\gamma\rfloor\lfloor\gamma+1\rfloor)/(2\lfloor\gamma\rfloor + 1)$, for any $\gamma \geq 1$.

We give a probabilistic polynomial-time reduction from $\mathrm{BDD}_{1/(\sqrt{2}\gamma)}$ to $\mathrm{uSVP}_\gamma$ for any $\gamma \geq 1$ that is polynomially bounded as a function of dimension. This new reduction supersedes all prior results mentioned above. This work has been accepted to ICALP'16, and I presented it in Italy, in July, 2016. Later on, I also gave an extended talk on this in Seminar Crypto, Université de Caen, in December, 2016.

My second work is to study the quantum hardness of lattice problems in terms of Learning with Error (LWE) problem, which is introduced by Regev in [5]. The $\mathrm{LWE}_{n,q,\alpha}$ with parameters $n, q \in \mathbb{Z}$ and

$\alpha \in (0,1)$ consists in finding a vector $\mathbf{s} \in \mathbb{Z}_q^n$ from arbitrarily many samples $(\mathbf{a}_i, \langle \mathbf{a}_i, \mathbf{s}\rangle + e_i) \in \mathbb{Z}_q^n \times \mathbb{Z}_q$, where $\mathbf{a}_i$ is uniformly sampled in $\mathbb{Z}_q^n$ and $e_i$ is sampled from $\mathcal{D}_{\mathbb{Z},\alpha q}$, the discrete Gaussian distribution of standard deviation parameter $\alpha q$ (i.e., the distribution such that $\mathcal{D}_{\mathbb{Z},\alpha q}(k) \sim \exp(-\pi k^2/(\alpha q)^2)$ for all $k \in \mathbb{Z}$). LWE is tightly connected to worst-case approximation problems over Euclidean lattices. In particular, LWE is an (average-case) instance of the Bounded Distance Decoding problem (BDD) (see, e.g., [6, Section 5.4]), but is also known to be as hard as *worst-case* BDD (with some polynomial loss in parameters) [7]. Classical and quantum connections between BDD and other problems such as SIVP, GapSVP, uSVP are also known [8, 1, 9, 7].

In 2002, Regev [10] showed that uSVP, and therefore also BDD and LWE, are no harder to solve than the quantumly-defined Dihedral Coset Problem (DCP). An instance of $\mathrm{DCP}_{N,\ell}$, for integer parameters $N$ and $\ell$, consists of $\ell$ quantum registers in superposition $|0, x_k\rangle + |1, x_k + s\rangle$, with a common $s \in \mathbb{Z}_N$ and random and independent $x_k \in \mathbb{Z}_N$ for $k \in [\ell]$. The goal is to find $s$ (information theoretically $\ell = \mathcal{O}(\log N)$ is sufficient for this task [11]).

Still, it is quite possible that DCP is in fact much harder to solve than LWE. The best known algorithm for DCP, due to Kuperberg [12], runs in time $2^{\mathcal{O}(\log \ell + \log N/\log \ell)}$ which does not improve upon classical methods for solving LWE. Other variants of the problem were explored in [11, 13], and of particular relevance to this work is a "vector" variant of the problem where $\mathbb{Z}_N$ is replaced with $\mathbb{Z}_q^n$ (i.e. $s$ and $x_k$ are now vectors), these problems behave similarly to DCP with $N = q^n$.

The focus of this work is a generalization of the DCP problem, i.e. rather than considering registers containing $|0, x_k\rangle + |1, x_k + s\rangle$, we allow (1) $x_i$'s and $s$ be $n$-dimensional vectors, and (2) other than non-uniform distribution for amplitudes. We name this problem Extrapolated DCP (EDCP). To be more precise, $\mathrm{EDCP}^{\ell}_{n,N,f}$, with parameters three integers $n, N, \ell$ and a function $f : \mathbb{Z} \mapsto \mathbb{C}$ with $\sum_{j\in\mathbb{Z}} j \cdot |f(j)|^2 < +\infty$, consists in recovering $\mathbf{s} \in \mathbb{Z}_N^n$ from the following $\ell$ states over $\mathbb{Z} \times \mathbb{Z}_N^n$:

$$\left\{ \frac{1}{\sqrt{\sum_{j\in\mathbb{Z}} |f(j)|^2}} \cdot \sum_{j\in\mathbb{Z}} f(j)\, |j, \mathbf{x}_k + j \cdot \mathbf{s}\rangle \right\}_{k \leq \ell},$$

where the $\mathbf{x}_k$'s are arbitrary in $\mathbb{Z}_N^n$.[1] Note that DCP is the special case of EDCP for $n = 1$ and $f$ being the indicator function of $\{0, 1\}$. In [14], Childs and van Dam consider the particular case of EDCP where $f$ is the indicator function of $\{0, \ldots, M-1\}$ for some integer $M$, which we will refer to as uniform EDCP (or, $\text{U-EDCP}^{\ell}_{n,N,M}$).

Our second main result is that there exists a quantum polynomial-time reduction from $\mathrm{LWE}_{n,q,\alpha}$ to $\text{U-EDCP}^{\ell}_{n,N,M}$, with $N = q$, $\ell = \mathrm{poly}(n \log q)$ and $M = \frac{\mathrm{poly}(n \log q)}{\alpha}$. Conversely, there exists a polynomial-time reduction from U-EDCP to LWE with the same parameter relationships, up to $\mathrm{poly}(n \log q)$ factors. This work is in submission to Crypto.

**Research plan for 03.2017-08.2018.**

I am working/plan to work on the following directions.

**Improving the reductions between BDD and uSVP.** We have a conjecture on this relation between BDD and uSVP that computational equality holds between $\mathrm{BDD}_{1/(\sqrt{2}\gamma)}$ and $\mathrm{uSVP}_{\gamma}$. Currently, we already know that $\mathrm{BDD}_{1/(\sqrt{2}\gamma)}$ is reduced to $\mathrm{uSVP}_{\gamma}$. For the opposite direction, there is a reduction from $\mathrm{uSVP}_{\gamma}$ to $\mathrm{BDD}_{1/\gamma}$ given by Lyubashevsky and Micciancio [1]. To obtain the conjectured equality,

[1] Note that the assumption on $f$ implies, via Markov's inequality, that one may restrict the sum to a finite index set and obtain a superposition which remains within negligible $\ell_2$ distance from the countable superposition above.

we need to improve this result to reduce uSVP$_\gamma$ to BDD$_{1/(\sqrt{2}\gamma)}$. I am also considering the practical relevance of the improved uSVP to BDD.

**Hardness of** EDCP **with more input states.** We show in this work that LWE and U-EDCP are computationally equivalent up to small parameter losses, when the number of U-EDCP states $\ell$ is polynomial. In these reductions, the U-EDCP bound $M$ is within a polynomial factor of the LWE noise rate $1/\alpha$. When more states are available, U-EDCP is likely to become easier. For instance, with $M = 2$, the best known algorithms when $\ell$ is polynomially bounded are exponential. Oppositely, Kuperberg's algorithm [12] runs in time $2^{\widetilde{O}(\sqrt{\log N})}$ when $\ell = 2^{\widetilde{O}(\sqrt{\log N})}$. This suggests that there may be a U-EDCP self-reduction allowing to trade $\ell$ for $M$: Is it possible to reduce $\text{EDCP}^{\ell}_{N,M}$ to $\text{EDCP}^{\ell'}_{N,M'}$ with $\ell' \leq \ell$, while allowing for $M' \geq M$?

**Circular security related to LWE.** Circular security assumption, first introduced by Gentry in [15], is used to upgrade a leveled homomorphic encryption into a fully homomorphic encryption. The circular security assumption in terms of Regev's encryption (based on LWE assumption) is (briefly) to distinguish the following elements

$$\mathbf{A}, \mathbf{As} + \mathbf{e}_1, \mathbf{At} + \mathbf{Gs} + \mathbf{f}_1, \mathbf{B}, \mathbf{Bt} + \mathbf{e}_2, \mathbf{Bs} + \mathbf{Gt} + \mathbf{f}_2,$$

where $\mathbf{A}$, $\mathbf{B} \in \mathbb{Z}_q^{m\times n}$ are randomly chosen, $\mathbf{e}_1$, $\mathbf{e}_2$, $\mathbf{f}_1$ and $\mathbf{f}_2$ are all chosen from some specific distribution with sufficiently large entropy, with randomly chosen and independent elements. Until now, there is not hardness proof under classical technique. Thus it will be interesting to investigate from another aspect - quantum computation. One idea is to show the hardness of the assumption above by reducing (variance of) EDCP to it using quantum computation.

**Quantum random oracle.** Lattice-based primitives are one of the most attractive candidates for post-quantum cryptography. Many efficient lattice-based constructions are built based on the random oracle (RO) model. First, one of the most efficient chosen-ciphertext attack (CCA) secure public key encryption can be built based on chosen-plaintext attack secure encryption, by using the Fujisaki and Okamoto's RO-based OAEP generic construction [16]. Second, the highly efficient signature can be obtained from identification using Fiat-Shamir transformation, where the RO is heavily relied on. As RO is public and can be implemented as quantum circuit, it is necessary to show that the schemes stay secure while providing the adversary with quantum access to the RO. Recent work of Targhi and Unruh [17] partly solve this by assuming the existence of a quantum partial-domain one-way trapdoor injective function. One would prefer to obtain the same result basing on weaker assumption, e.g., with known instances with assumed hardness based on LWE etc.. The question on how to prove security of Fiat-Shamir generic transformation with quantum access to the RO, is first given by Boneh et al. [18], and later studied by Dagdelen et al. [19]. In [19], an extreme difficulty on “rewinding" is pointed out for quantum computation because of the “no cloning" principle of quantum computation. Thus the first question will be how the forking lemma should be simulated in the quantum setting.

# References

[1] V. Lyubashevsky and D. Micciancio. On bounded distance decoding, unique shortest vectors, and the minimum distance problem. In *Proc. of CRYPTO*, pages 577–594, 2009.

[2] M. Liu, X. Wang, G. Xu, and X. Zheng. A note on BDD problems with $\lambda_2$-gap. *Inf. Process. Lett.*, 114(1-2):9–12, January 2014.

[3] D. Micciancio. Private communication, 2015.

[4] S. Galbraith. Private communication, 2015.

[5] O. Regev. On lattices, learning with errors, random linear codes, and cryptography. In *Proc. of STOC*, pages 84–93. ACM, 2005.

[6] D. Micciancio and O. Regev. Lattice-based cryptography. In *Post-Quantum Cryptography, D. J. Bernstein, J. Buchmann, E. Dahmen (Eds)*, pages 147–191. Springer, 2009.

[7] O. Regev. On lattices, learning with errors, random linear codes, and cryptography. *J. ACM*, 56(6), 2009.

[8] Z. Brakerski, A. Langlois, C. Peikert, O. Regev, and D. Stehlé. Classical hardness of learning with errors. In *Proc. of STOC*, pages 575–584. ACM, 2013.

[9] C. Peikert. Public-key cryptosystems from the worst-case shortest vector problem. In *Proc. of STOC*, pages 333–342. ACM, 2009.

[10] O. Regev. Quantum computation and lattice problems. In *Proceedings of the 43rd Symposium on Foundations of Computer Science*, FOCS '02, pages 520–529. IEEE Computer Society, 2002.

[11] M. Ettinger and P. Høyer. On quantum algorithms for noncommutative hidden subgroups. In *Proc. of STACS*, volume 1563 of *LNCS*, pages 478–487. Springer, 1999.

[12] G. Kuperberg. A subexponential-time quantum algorithm for the dihedral hidden subgroup problem. *SIAM J. Comput*, 35(1):170–188, 2005.

[13] K. Friedl, G. Ivanyos, F. Magniez, M. Santha, and P. Sen. Hidden translation and translating coset in quantum computing. *SIAM J. Comput*, 43(1):1–24, 2014.

[14] A. M. Childs and W. van Dam. Quantum algorithm for a generalized hidden shift problem. In *Proc. of SODA*, pages 1225–1232. SIAM, 2007.

[15] C. Gentry. Fully homomorphic encryption using ideal lattices. In *Proc. of STOC*, pages 169–178. ACM, 2009.

[16] E. Fujisaki, T. Okamoto, D. Pointcheval, and J. Stern. RSA-OAEP is secure under the RSA assumption. In J. Kilian, editor, *Proc. of CRYPTO*, pages 260–274, 2001.

[17] E.E. Targhi and D. Unruh. Post-quantum security of the Fujisaki-Okamoto and OAEP transforms. In M. Hirt and A. Smith, editors, *Proc. of TCC, Part II*, 2016.

[18] D. Boneh, Ö. Dagdelen, M. Fischlin, A. Lehmann, C. Schaffner, and M. Zhandry. Random oracles in a quantum world. In D.H. Lee and X. Wang, editors, *Proc. of ASIACRYPT*, 2011.

[19] Ö. Dagdelen, M. Fischlin, and T. Gagliardoni. The fiat–shamir transformation in a quantum world. In K. Sako and P. Sarkar, editors, *Proc. of ASIACRYPT*, 2013.