

ADDRESS

École Normale Supérieure de Lyon
46 allée d'Italie
69364 Lyon Cedex, France
Téléphone: +33 07 67 63 58 15
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, Bachelor, South China Normal University, China; major in “Computer Science and Technology”.
-

PUBLICATIONS

- Zvika Brakerski, Elena Kirshanova, Damien Stehlé, W. Wen. Learning With Errors and Extrapolated Dihedral Cosets. PKC 2018.
 - Shi Bai, Damien Stehlé and W. Wen. Improved Reduction from the Bounded Distance Decoding Problem to the Unique Shortest Vector Problem in Lattices, ICALP 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

- Shi Bai, Damien Stehlé and W. Wen. Measuring, simulating and exploiting the head concavity phenomenon in BKZ, submitted to Asiacrypt 2018.
 - W. Wen, Libin Wang and Min Xie. One-Round Deniable Key Exchange with Perfect Forward Security. Cryptology ePrint archive, report 2014/661.
-

PRESENTATIONS

- 19-20/04/2018: Toward a more accurate BKZ simulator, Lattice Meeting, ENS de Lyon, France.
- 29/03/2018: Learning With Errors and Extrapolated Dihedral Cosets Problem, PKC 2018, Rio de Janeiro, Brazil.
- 23/02/2018: Learning With Errors and Extrapolated Dihedral Cosets Problem, Séminaire de Cryptographie in Institut de Recherche en Mathématiques de Rennes, France.
- 15-16/12/2016: Learning With Errors and the Generalized Hidden Shift Problem, Lattice Meeting, ENS de Lyon, France.
- 05/10/2016: Improved reduction from BDD to uSVP, Séminaire Cryptologie & Sécurité, Université de Caen, France.
- 15/07/2016: Improved reduction from BDD to uSVP, ICALP 2016, Rome, Italy.
- 02/06/2016: Improved reduction from BDD to uSVP, AriC Seminar, Lyon, France.

TRAINING

1. Complementary Scientific Formations (45 hours):
 - 23/04/2017–28/04/2017, Journées Codage et Cryptographie 2017, 21 hours, organizer: AnneLise Charbonnier (Inria Nancy - Grand Est), La Bresse, 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.
2. Professional Insertion Training (80 hours):
 - 10/2016–05/2017, Course "Français Langue Étrangère A2", 80 hours (first (40 hours) and second (40 hours) semesters), 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 2623 3932
damien.stehle@ens-lyon.fr

Lyon, le 29 mai 2018

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

Chère collègue, cher collègue,

Weiqiang Wen a démarré son doctorat à l'automne 2015, il y a donc presque 3 ans. Il avait auparavant fait ses études à Canton (Chine), dont un stage de Master sous ma direction.

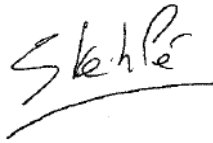
Lors de son doctorat, Weiqiang a obtenu 3 résultats principaux, que je décris ici par ordre chronologique.

- Tout d'abord, suite à une suggestion de Shi Bai, alors post-doctorant au LIP, 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 publié dans les actes de la conférence ICALP 2016.
- À partir de l'été 2016, Weiqiang a travaillé sur 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 variante de DCP admettant une réduction depuis LWE et une autre vers LWE. L'article correspondant a été publié dans les actes de la conférence PKC 2018.
- Depuis l'été dernier, Weiqiang a travaillé sur les aspects pratiques de l'algorithme BKZ, le meilleur algorithme connu pour résoudre les problèmes de réseaux euclidiens, tels que BDD et LWE. Weiqiang a proposé une modélisation (efficace) de l'algorithme BKZ, qui est très fidèle

au comportement pratique (coûteux) de BKZ. Ceci permet notamment d'extrapoler le comportement de BKZ. Cela a aussi mis en lumière des phénomènes alors mal compris dans le comportement pratique de BKZ, et de proposer une variante de l'algorithme qui en tire parti. Ce travail est de nature très différente des précédents : il est principalement expérimental alors qu'ils étaient complètement théoriques. L'article, en commun avec Shi Bai et moi-même, a été soumis à la conférence Asiaticrypt'18.

Weiqiang a démarré la rédaction de sa thèse il y a 2 semaines, après la date butoir pour soumettre à la conférence Asiaticrypt. Il vise une fin de rédaction en août, pour une soutenance autour de novembre. À partir du 1er septembre, il rejoindra l'équipe de Pierre-Alain Fouque à l'Université de Rennes. Bien entendu, je soutiens sa réinscription en doctorat, pour qu'il puisse soutenir à l'Automne.

Damien Stehlé

A handwritten signature in black ink, appearing to read 'Stehlé', with a horizontal line underneath.

Mission: **progress report (09.2015–05.2018) and future plan (from 05.2018)**

PhD advisor. Damien Stehlé (ENS de Lyon professor, LIP)

PhD project. Algorithm for hard lattice problems.

PhD duration. From September, 2015 to November, 2018 (planned).

Research during 09.2015–05.2018.

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), which gives as input a basis of a lattice, asks to find a shortest non-zero vector in the lattice; and the closest vector problem (CVP), which gives as inputs a basis of a lattice and a (target) vector in the real span of the lattice, asks to 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 $\alpha > 0$ (BDD_α): 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 $\gamma \geq 1$ (USVP_γ). USVP_γ consists in finding a shortest non-zero vector in a given lattice \mathcal{L} , under the promise that $\lambda_2(\mathcal{L}) \geq \gamma \cdot \lambda_1(\mathcal{L})$.

My main result in the first 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 $\text{BDD}_{1/(2\gamma)}$ reduces to USVP_γ for any $\gamma \geq 1$. Later, Liu *et al.* [2] refined the analysis of Lyubashevsky and Micciancio and proved that BDD_{1/γ_1} reduces to USVP_γ 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 BDD_{1/γ_1} reduces to USVP_γ 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 $\text{BDD}_{1/(\sqrt{2}\gamma)}$ to USVP_γ 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.

Next, I studied the quantum hardness of lattice problems in terms of Learning with Error (LWE) problem, which is introduced by Regev in [5]. The $\text{LWE}_{n,q,\alpha}$ 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 $\mathcal{D}_{\mathbb{Z}, \alpha q}$. In 2002, Regev [6] 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 $\text{DCP}_{N,\ell}$, for integer parameters N and ℓ , consists of ℓ 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 .

My main result in the second year focuses on 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, $\text{EDCP}_{n,N,f}^\ell$, with parameters three integers n, N, ℓ 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 ℓ 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 . Note that DCP is the special case of EDCP for $n = 1$ and f being the indicator function of $\{0, 1\}$. We show that there exists a quantum polynomial-time reduction from $\text{LWE}_{n,q,\alpha}$ to $\text{EDCP}_{n,N,M}^\ell$, with $N = q$, $\ell = \text{poly}(n \log q)$ and $M = \frac{\text{poly}(n \log q)}{\alpha}$. Conversely, there exists a polynomial-time reduction from U-EDCP to LWE with the same parameter relationships, up to $\text{poly}(n \log q)$ factors. This work has been accepted to PKC'18.

The most recent result is on the cryptanalysis of lattice-based cryptography. The Blockwise-Korkine-Zolotarev (BKZ) lattice reduction algorithm is central in cryptanalysis for lattice-based cryptography. A precise understanding of its practical behavior in terms of run-time and output quality is necessary for parameter selection in cryptographic design. As the provable worst-case bounds poorly reflect the practical behavior, cryptanalysts rely instead on the heuristic BKZ simulator of Chen and Nguyen [7]. It better fits with practical experiments, but not quite accurately. In particular, it over-estimates the norm of the first several vectors in the output basis. Put differently, BKZ performs better than its Chen-Nguyen simulation. We first report experiments providing more insight on this shorter-than-expected phenomenon. We then propose a refined BKZ simulator by taking the distribution of short vectors in random lattices into consideration. We report experiments suggesting that this refined simulator more accurately predicts the concrete behavior of BKZ. Furthermore, we design a new BKZ variant that exploits the shorter-than-expected phenomenon. For the same cost assigned to the underlying SVP-solver, the new BKZ variant produces bases of better quality.

Research plan for 05.2018-11.2018.

I will be mainly writing my PhD thesis and preparing for my PhD defense at this period. On the way, I will also work on the following topic.

Improving the reductions between BDD and uSVP. We have a conjecture on this relation between BDD and uSVP that computational equality holds between $\text{BDD}_{1/(\sqrt{2}\gamma)}$ and uSVP_γ . Currently, we already know that $\text{BDD}_{1/(\sqrt{2}\gamma)}$ is reduced to uSVP_γ . For the opposite direction, there is a reduction from uSVP_γ to $\text{BDD}_{1/\gamma}$ given by Lyubashevsky and Micciancio [1]. To obtain the conjectured equality, we need to improve this result to reduce uSVP_γ to $\text{BDD}_{1/(\sqrt{2}\gamma)}$. I am also considering the practical relevance of the improved uSVP to BDD.

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 λ_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] 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.
- [7] Y. Chen and P. Q. Nguyen. BKZ 2.0: Better lattice security estimates. In *ASIACRYPT*, pages 1–20, 2011.

Cadre B	Informations relatives au chercheur ou à l'enseignant chercheur
----------------	--

Nom (M., ~~Mme~~, ~~Mlle~~) : WEN. Prénom : Weiqiang.

Date de naissance : 14/09/1989

Nationalité : Chinoise

Qualité : Doctorant

Adresse (dans le pays de résidence habituelle) : 106 Building n°20, South China normal University

Nom de l'organisme/employeur ou établissement d'enseignement supérieur fréquenté dans le pays de résidence :
South China normal University

Pour le projet de recherche ou d'enseignement universitaire suivant :

Recherche sur la Cryptographie reposant sur les réseaux euclidiens

Durée prévue du séjour :

du.....01/09/2015..... au.....31/08/2018

à durée déterminée

Adresse du domicile prévue en France (à défaut, adresse de l'unité de recherche) :

.....ENS - LIP.....46 allée d'Italie 69363 Lyon cedex 07

[6][9][3][6][4][] [L][Y][O][N][] [C][E][D][E][X][] [7][] [] [] [] [] [] [] [] [] [] []
Code postal Commune / arrondissement

Sous le statut de :

Salarié dont le salaire est versé en France ou étranger détaché en application de l'article L. 342-2 du code du travail
(durée du contrat conclu-montant du salaire brut mensuel) : ...

Rémunération brute mensuelle :

Autre (préciser) : Doctorant-1657 euros brut mensuel

Cas spécifique des doctorants salariés (salaire obligatoire si le chercheur est accueilli en qualité de doctorant :

Si le scientifique envisage de s'inscrire ou s'est inscrit dans un établissement d'enseignement supérieur pour y préparer
une thèse de doctorat, veuillez indiquer :

Le nom de l'établissement : ENS DE LYON

Le sujet de la thèse de doctorat : ...

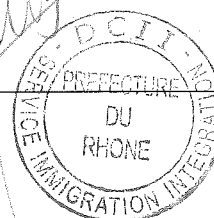
Organisme auprès duquel est souscrit le contrat (contrat de travail, contrat d'agent non titulaire de l'Etat) sur la base
duquel le scientifique est rémunéré : ENS DE LYON

Le chercheur ou l'enseignant chercheur atteste sur l'honneur l'exactitude des déclarations ci-dessus :

Fait àLyon..... le.....01/09/2015.....

Signature : *Weiqiang Wen*

Autorité consulaire (Lorsque l'entrée en France est subordonnée à la présentation d'un visa)	Préfecture :
Date et cachet :	Date et cachet : 05 OCT. 2015





Charte du Doctorat de l'Université de Lyon *PhD Charter of the Université de Lyon*

Protocole de signature / Signature protocole

Je soussigné e (NOM du/de la doctorant e) / I undersigned (NAME of the PhD student):

Weiyoung Wen

Atteste avoir pris connaissance de la Charte du doctorat et m'engage à la respecter.
Have taken note of the PhD Charter and I am committed to respecting it.

Date et Signature / Date and signature:

31/05/2018 Weiyoung Wen

Je soussigné e (NOM du/de la directeur/trice de thèse) / I undersigned (NAME of the thesis director):

Danie STEHE

Atteste avoir pris connaissance de la Charte du doctorat et m'engage à la respecter.
Have taken note of the PhD Charter and I am committed to respecting it.

Date et Signature / Date and signature of the supervisor:

31/05/2018 Skohlé

Je soussigné e (NOM du/de la codirecteur/trice de thèse) / I undersigned (NAME of the thesis co-director):

Atteste avoir pris connaissance de la Charte du doctorat et m'engage à la respecter.
Have taken note of the PhD Charter and I am committed to respecting it.

Date et Signature / Date and signature:

NOM du/de la directeur/trice de l'unité de recherche / NAME of the director of the research unit:

Date et Signature / Date and signature :

4/6/2018

Patrick BAILLOT
Directeur du LIP

Rapport du comité de suivi individuel – Ecole Doctorale InfoMaths

Nom & prénom(s) du (de la) doctorant(e) : WEN Weiqiang

Laboratoire : LIP

Etablissement : ENS Lyon

Directrice(s)/Directeur(s) de thèse : Damien STEHLÉ

Titre du projet de thèse : Algorithms for hard lattice problems

Année d'inscription : D..2

Date du début de la thèse : Septembre 2015

Co-tutelle ☐ **CIFRE** ☐

NB : Pour les thèses en partenariat industriel ou international, le comité veillera à l'équilibre entre les partenaires (communication, cohérence, présence sur chaque site, répartition du temps).

Composition du comité :

Personnalité(s) extérieure(s) : Pierre-Alain FOUQUE

Personnalité de l'ED InfoMaths : Frédéric VIVIEN

Date du comité :

CRITERES	AVIS		COMMENTAIRES
	-	+	
Avancement des travaux de recherche	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Le doctorant a obtenu d'excellents résultats qui ouvrent de larges perspectives
Publications	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
Présentations orales	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
Formations doctorales	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
Intégration au sein du laboratoire	<input type="checkbox"/>	<input type="checkbox"/>	Rien à signaler
Conditions matérielles	<input type="checkbox"/>	<input type="checkbox"/>	Rien à signaler
Interactions entre le(la) doctorant(e) et l'équipe encadrante (fréquence des réunions, communication, réactivité)	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
Activités complémentaires	<input type="checkbox"/>	<input type="checkbox"/>	Pas d'activité complémentaire vue la barrière de la langue

- : point faible + : point fort

		Acceptées	Soumises
Publications	Revues Internationales : Revues Nationales : Conférences Internationales : Conférences Nationales : Autres :	1	1
Présentations orales	Séminaires : 3 Conférences : 1 Posters : Autres :		
Formations doctorales	Nombre heures FSC : 24 Nombre heures FIP : 101		
Activités complémentaires	Enseignement (contrat, vacations) : Mandat électif : Autres :		

Progression du projet de thèse et appréciation globale

Weiqliang Wen a obtenu deux résultats majeurs en cryptographie, l'un en approche classique et l'autre en approche quantique. La première moitié de thèse est plus que satisfaisante. Weiqliang Wen nous a présenté plusieurs pistes ambitieuses pour la poursuite de ses travaux.


Recommandations pour l'année suivante

Avis pour la réinscription en D.. 3

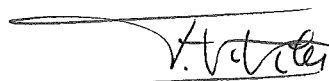
Avis favorable ☒

Avis favorable sous réserve ☐

Avis défavorable ☐



Pierre-Alain FOUQUE



Frédéric VIVIEN