Research Report of the Second Year During the INdAM - DP COFUND 2015 fellowship

Manoj Gyawali
Department of Mathematics and Physics, Roma Tre
2019

1. **Course Attended**
   Title : Algebraic Number Theory (AL420)
   Period : 26-2-201 to 16-5-2019
   Lectures: 52 hrs
   Place : Department of Mathematics and Physics, Roma, Tre.
   Course Website : `http://www.mat.uniroma3.it/users/pappa/CORSI/AL420_18_19/AL420.htm`

2. **Workshop Attended**
   Title : ECC 2019: 23rd Workshop on Elliptic Curve Cryptography
   Period : 2-4 December 2019
   Place: Bochum, Germany.
   Website : `https://eccworkshop.org/2019/`

3. **Conference attended**
   Title : The fifth mini symposium of the Roman Number Theory Association
   Period : April 10-12, 2019
   Place: Università Roma Tre
   Website : `http://www.rnta.eu/5MSRNTA/index.html`
4. **Seminar attended**
   I have participated almost all the seminar and colloquium related to Number Theory and Cryptography at University of Roma Tre.
   Website: `http://www.matfis.uniroma3.it/Attivita/Altri_eventi/altri_eventi.php?&anno=2019`

5. **Publications and Preprints**
   Title : Elliptic Curve of Nearly Prime Order (iacr arxiv pre-print)
   Authors: Daniele Di Tullio and Manoj Gyawali.
   Website : `https://eprint.iacr.org/2020/001`
6. **Attended INdAM Day**
   Place: Bari, Italy
   Period: June 3 2019

- **Research Area :**
  My area of research is "Isogeny based cryptography". This is one of the candidates of post quantum cryptography which has relatively smaller key size in comparison to other purposed candidates. Well known Isogeny based protocols are CSIDH-Commutative SIDH (Supersingular Isogeny Deffie Hellman) [2], [11, 16]. CSIDH is quantum vulnerable due to a quantum subexponential time attack [3]. Supersingular isogeny based cryptography are mainly based on the problems of finding an isogeny between two supersingular elliptic curves and computing an endomorphism ring of a supersingular elliptic curve, which are considered the post quantum problems.
  The Charles, Goren and Lauter hash function [9] is based on the quaternion version of l isogeny path problem, which is also solvable by the algorithm of Kohel, Lauter, Petit and Tignol(KLPT) [5]. But, this algorithm finds a path between two maximal orders of a quaternion algebra passing through a special maximal order.
  Christophe Petit's attack for the some varients of SIDH in [4], which are called unbalanced degree variant and optimal degree variant. In SIDH, some torsion point images of of the secret isogeny must be sent in order to agree on a same key. Petit uses this fact to construct an endormorphism of an elliptic curve under some assumptions on the torsion point orders but he is not successful to break the SIDH, not even a variant of SIDH.

- **Research Progress :**
  We studied the Denis Simon's algorith [7] in dimension 5 analysing its complexity in case of diemsion 5, which works in polynomial time when the determinant of the underlying quadratic form is known. We have been working to accelerate the Petit's attack to a variant of SIDH.
  Furthermore, our project includes a problem to find an algorithm that extends the KLPT [5] algorithm, which reduces an isogeny path problem to a quaternion ideal problem i.e. given a left $\mathcal{O}$-ideal I, compute an equivalent left $\mathcal{O}$-ideal J of smooth norm, where $\mathcal{O}$ is a maximal order in quaternion algebra $B_{p,\infty}$. The probabilistic polynomial time algorithm developed in [5] finds a path between two maximal orders passing through a special order. Our approach to solve the quaternion path problem is to use SIMON's Algorithm and not required to pass through a special maximal order.

The following are the references as well as the papers that I have read.

References

[1] Arnold Pizer. *An algorithm for computing modular forms on* $\Gamma_0(N)$, *J. Algebra*, 64(2)(1980),340-390.

[2] Castryck, W., Lange, T., Martindale, C., Panny, L., Renes, J. *CSIDH: an efficient post-quantum commutative group action*, *Peyrin, T., Galbraith, S. (eds.) ASIACRYPT,Springer, Cham*, 11274(2018), 395-427.

[3] Childs, A., Jao, D., Soukharev, V. *Constructing elliptic curve isogenies in quantum subexponential time*, *J. Math. Cryptol*, 8(1)(2014), 1-29.

[4] Christophe Petit. *Faster Algorithms for Isogeny Problems Using Torsion Point Images*, *Advances in Cryptology – ASIACRYPT 2017*, (2017),330-353.

[5] David Kohel,Kristin Lauter,Christophe Petit,Jean-pierre Tignol. *On the quaternion l-isogeny path problem*, *LMS Journal of Computation and Mathematics*, 17A(2014),418-432.

[6] David Kohel. *Endomorphism rings of elliptic curve over finite fields*, *PhD thesis,University of Californiа,Berkeley*, 1996.

[7] Denis Simon. *Quadraticequationsin dimensions 4, 5 and more*, 2005. `http://web.archive.org/web/20080221173916/http://www.math.unicaen.fr/~simon/maths/Dim4.pdf`

[8] D. Simon. *Solving quadratic equations using reduced unimodular quadratic forms. Math. Comp.*, 74 nb 251(2005),1531-1543.

[9] D. X. Charles, K. E. Lauter, and E. Z. Goren. *Cryptographic hash functions from expander graphs*, *J. Cryptology*, 22(1)(2009), 93-113.

[10] D. Simon. *Solving quadratic equations using reduced unimodular quadratic forms. Math. Comp.*, 74 nb 251(2005),1531-1543.

[11] Jao, D., De Feo, L., Plût, J. *Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies*, *J. Math. Cryptol*, 8(3)(2014), 209-247.

[12] Joseph H. silverman, *The Arithmetic of Elliptic Curves. Springer*, 1986.

[13] John Voight. *Quaternion algebras*, 2018.
`http://https://math.dartmouth.edu/~jvoight/quat-book.`

[14] Marie-France Vignéras. *The arithmetic of quaternion algebra*, 2006.
`http://maths.nju.edu.cn/~guoxj/notes/qa.pdf`

[15] Pierre Castel. *Solving quadratic equations in dimension 5 or more without factoring. The Open Book Series*, 1(2013),213-233.

[16] Steven D. Galbraith, Christophe Petit and Javier Silva. *Identification protocols and Signature Schemes Based on Supersingular Isogeny problems. ASIACRYPT 2017 23rd International Conference on the Theory and Application of Cryptology and Information Security Hong Kong,China*, (2017),03-33.

[17] W. Bosma and P. Stevenhagen, *On the computation of quadratic 2- class group. J. Théorie Nombres bordeaux* , 8(1996),no. 2, 283-313.