North Carolina State University

Poster: Cryptography in a Post-Quantum World

Katharine Ahrens
Graduate Student
kaahrens@ncsu.edu

ABSTRACT

Lattice-based hard problems are a leading candidate for implementation in future public key cryptographic schemes due to their conjectured quantum resilience. Lattice-based problems offer certain advantages over non-lattice-based cryptosystems, such as a relatively short key length [3] and versatility, since lattice cryptosystems can offer both encryption schemes (to securely transmit data from sender to receiver) and signature schemes (used for a receiver to verify that information actually originated from the claimed sender) [2]. Notably, they are also the only known class of problems which give rise to fully homomorphic encryption schemes, in which computations can be securely performed on encrypted data [1]. Many of the 2017 submissions to the NIST Post-Quantum Cryptography challenge are based on lattice problems [4].

Some lattice cryptosystems, most notably the ring-LWE [7] scheme proposed in 2013, rely on solving a hard problem over a subclass of lattices known as ideal lattices. However, it is currently unknown whether the additional algebraic structure found in ideal lattices make them less secure for cryptographic purposes, although it is widely conjectured that the ideal case is as secure as the general case [1].

In this poster presentation, we give an overview of past attempts to approach a lattice hard problem known as the shortest vector problem (SVP) in a class of ideal lattices generated using the cyclotomic integers, which is a type of mathematical object known as a ring. The cyclotomic integers have a lot of algebraic structure, and some researchers have speculated that this structure

HoTSoS '18, April 10–11, 2018, Raleigh, NC, USA
© 2018 Copyright held by the owner/author(s).
This is the author's version of the work. It is posted here for your personal use. Not for redistribution. The definitive Version of Record was published in *HoTSoS '18: Hot Topics in the Science of Security: Symposium and Bootcamp, April 10–11, 2018, Raleigh, NC, USA*, https://doi.org/10.1145/3190619.3191677.

could potentially make these lattices less secure [6]. The discovery that the ideal-lattice based cryptosystem Soliloquy is not quantum-secure [5] has motivated cryptographers to examine the feasibility of using new types of rings to generate lattices, such as the variant of the crytosystem NTRU proposed in [6]. This poster will include our preliminary results on the security of the SVP in ideal lattices generated in a ring which has been previously unstudied and discuss the practically of using the ring in place of the cyclotomic integers in some lattice cryptosystems.

CCS CONCEPTS

• **Security and privacy** → **Public key encryption**; *Mathematical foundations of cryptography*;

KEYWORDS

Asymmetric cryptography; mathematical cryptography; post-quantum cryptography.

ACM Reference Format:
Katharine Ahrens. 2018. Poster: Cryptography in a Post-Quantum World. In *HoTSoS '18: Hot Topics in the Science of Security: Symposium and Bootcamp, April 10–11, 2018, Raleigh, NC, USA*. ACM, New York, NY, USA, 2 pages. https://doi.org/10.1145/3190619.3191677

REFERENCES

[1] Chris Peikert, *A Decade of Lattice Cryptography*, 2016.
[2] J. Howe, T. Poppelmann, M. O'Neill, E. O'Sullivan, T. Guneysu. *Practical Lattice-based Digital Signature Schemes*. ACM Transactions on Embedded Computer Systems, 2015.
[3] Jeffrey Hoffstein, Jill Pipher, and Jack H. Silverstein. *An Introduction to Mathematical Cryptography.* Springer, 2010.
[4] National Institute of Standards and Technology Computer Security Resource Center. *Post Quantum Cryptography* Round 1 submissions page. https://csrc.nist.gov/projects/post-quantum-cryptography/round-1-submissions Last updated 20 Feb 2018. .
[5] Peter Campbell, Michael Groves and Dan Shepherd. *Soliloquy: A Cautionary Tale.* ETSI 2nd Quantum-Safe Crypto Workshop, 2014.
[6] Daniel J. Bernstein, Chitchanok Chuengsatiansup, Tanja Lange, Christine van Vredendaal. *NTRU Prime: reducing attack surface at low cost*. Cryptology ePrint Archive, 2017.
[7] Vadim Lyubashevsky, Christ Peikert, Oded Regev. *On Ideal Lattices and Learning with Errors over Rings*. Eurocrypt 2010.