2018 IEEE European Symposium on Security and Privacy

CRYSTALS – Kyber: a CCA-secure module-lattice-based KEM

Joppe Bos , L o Ducas[†], Eike Kiltz[‡], Tancrède Lepoint[§], Vadim Lyubashevsky[¶],
John M. Schanck[‖], Peter Schwabe , Gregor Seiler[††], Damien Stehl [‡‡],
NXP Semiconductors, Belgium. Email: joppe.bos@nxp.com
[†]*CWI Amsterdam, The Netherlands. Email:* ducas@cwi.nl
[‡]*Ruhr-University Bochum, Germany. Email:* eike.kiltz@rub.de
[§]*SRI International, USA. Email:* tancrede.lepoint@sri.com
[¶]*IBM Research Zurich, Switzerland. Email:* vad@zurich.ibm.com
[‖]*University of Waterloo, Canada. Email:* jschanck@uwaterloo.ca
Radboud University, The Netherlands. Email: peter@cryptojedi.org
[††]*IBM Research Zurich, Switzerland. Email:* grs@zurich.ibm.com
[‡‡]*ENS de Lyon, France. Email:* damien.stehle@ens-lyon.fr

***Abstract*—Rapid advances in quantum computing, together with the announcement by the National Institute of Standards and Technology (NIST) to define new standards for digital-signature, encryption, and key-establishment protocols, have created significant interest in post-quantum cryptographic schemes.**

This paper introduces yber **(part of CRYSTALS – *Cryp tographic Suite for Algebraic Lattices* – a package submitted to NIST post-quantum standardization effort in November 2017), a portfolio of post-quantum cryptographic primitives built around a key-encapsulation mechanism (KEM), based on hardness assumptions over module lattices. Our KEM is most naturally seen as a successor to the** NEWHOPE **KEM (Usenix 2016). In particular, the key and ciphertext sizes of our new construction are about half the size, the KEM offers CCA instead of only passive security, the security is based on a more general (and flexible) lattice problem, and our optimized implementation results in essentially the same running time as the aforementioned scheme.**

We first introduce a CPA-secure public-key encryption scheme, apply a variant of the Fujisaki–Okamoto transform to create a CCA-secure KEM, and eventually construct, in a black-box manner, CCA-secure encryption, key exchange, and authenticated-key-exchange schemes. The security of our primitives is based on the hardness of Module-LWE in the classical and quantum random oracle models, and our concrete parameters conservatively target more than 28 **bits of post-quantum security.**

1. Introduction

There has been an increased interest in post-quantum cryptographic schemes triggered by recent advances in quantum computing [35] and the announcement by the National Institute of Standards and Technology (NIST) to define new standards for digital-signature, encryption, and key-establishment protocols [28]. Constructions based on the hardness of lattice problems are considered to be one of the leading candidates to replace the currently used schemes based on the believed hardness of the traditional number-theoretic problems such as integer factorization and discrete logarithms.

Lattice cryptography initially gained a lot of interest in the theoretical community due to the fact that the designs for cryptographic constructions were accompanied by security proofs based on *worst-case* instances of lattice problems. The first lattice-based encryption scheme was proposed by Ajtai and Dwork [1]. This scheme was later simplified and improved upon by Regev in [67], [68]. One of the major achievements of Regev's work was the introduction of an intermediate problem – the Learning With Errors (LWE) Problem – which was relatively simple to use in cryptographic constructions and asymptotically at least as hard as some standard worst-case lattice problems [61], [25].

The LWE assumption states that it is hard to distinguish from uniform the distribution $(\quad, \quad \mathbf{s} + \mathbf{e})$, where is a uniformly-random matrix in $\mathbb{Z}_q^{m \times n}$, $\mathbf{s}$ is a uniformly-random vector in $\mathbb{Z}_q^n$, and $\mathbf{e}$ is a vector with random "small" coefficients chosen from some distribution. Applebaum et al. [6] showed that the secret $\mathbf{s}$ in the LWE problem does not need to be chosen uniformly at random: the problem remains hard if $\mathbf{s}$ is chosen from the same narrow distribution as the errors $\mathbf{e}$. Based on the idea from the NTRU cryptosystem [43] of working with elements over polynomial rings rather than over the integers, and following a series of works on this topic [58], [56], [63], [71], Lyubashevsky et al. [57] showed that it is also hard to distinguish a variant of the LWE distribution from the uniform one over certain polynomial rings, thus defining the Ring-LWE assumption.

The combination of all of the above results finally led

DOI 10.1109/EuroSP.2018.00032

IEEE computer society