

Lepton ¹: Key Encapsulation Mechanisms from a variant of Learning Parity with Noise

Name: Lepton

Principal submitters: Yu Yu, Shanghai Jiao Tong University, China
Jiang Zhang, State Key Laboratory of Cryptology, China

Inventors: Yu Yu, Shanghai Jiao Tong University, China
Jiang Zhang, State Key Laboratory of Cryptology, China

Owners: Yu Yu, Shanghai Jiao Tong University, China
Jiang Zhang, State Key Laboratory of Cryptology, China

Contact information: Yu Yu & Jiang Zhang
Postal addresses: #4-2803, 688 South Xizang Rd, Shanghai, China 200011
P.O. Box 5159, Beijing, China 100878
E-mail addresses: yyuu@sjtu.edu.cn jiangzhang09@gmail.com
Contact numbers: +86-15000088966 +86-15110204521

Date: November 28, 2017

Signature:

The image shows two handwritten signatures in black ink. The first signature, on the left, is 'Yu Yu' (俞昱) and the second signature, on the right, is 'Jiang Zhang' (张江). The characters are written in a fluid, cursive style.

¹ The design and analysis of the Lepton crypto-system [51] are based on preliminary results obtained in [52], which is currently in submission and will appear in IACR ePrint at an appropriate time.