

Lepton¹: 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 Chinese ink. The first signature on the left consists of three characters: 郁 (Yu), 显 (Xian), and 张 (Zhang). The second signature on the right consists of two characters: 江 (Jiang) and 张 (Zhang).

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.