TP: Implementation of DGHV Fully Homomorphic Encryption Scheme

Jean-Sébastien Coron

Université du Luxembourg

1 DGHV Somowhat Homormorphic Encryption Scheme

Implement the basic DGHV encryption scheme [4], without the squashed decryption and without the bootstrapping, but using the compression of the public-key as described in [3]. You can use the SAGE library [1].

2 Optional: DGHV with Squashed Decryption

Implement DGHV with squashed decryption, as described in [4, 2].

3 Optional: full DGHV

Implement the fully homomorphic DGHV encryption scheme, including the bootstrapping procedure, as described in [4, 3].

References

1. Sage Mathematical Library, Available at `http://www.sagemath.org/`
2. Jean-Sebastien Coron, Avradip Mandal, David Naccache, Mehdi Tibouchi: Fully Homomorphic Encryption over the Integers with Shorter Public Keys. CRYPTO 2011: 487-504.
3. Jean-Sebastien Coron, David Naccache, Mehdi Tibouchi: Public Key Compression and Modulus Switching for Fully Homomorphic Encryption over the Integers. EUROCRYPT 2012: 446-464
4. Marten van Dijk, Craig Gentry, Shai Halevi, Vinod Vaikuntanathan: Fully Homomorphic Encryption over the Integers. EUROCRYPT 2010: 24-43.