BIKE: Bit Flipping Key Encapsulation
Summary of Changes for Round 2 Submission

Nicolas Aragon, University of Limoges, France

Paulo S. L. M. Barreto, University of Washington Tacoma, USA

Slim Bettaieb, Worldline, France

Loïc Bidoux, Worldline, France

Olivier Blazy, University of Limoges, France

Jean-Christophe Deneuville, INSA-CVL Bourges and University of Limoges, France

Philippe Gaborit, University of Limoges, France

Shay Gueron, University of Haifa, and Amazon Web Services, Israel

Tim Güneysu, Ruhr-Universität Bochum, and DFKI, Germany,

Carlos Aguilar Melchor, University of Toulouse, France

Rafael Misoczki, Intel Corporation, USA

Edoardo Persichetti, Florida Atlantic University, USA

Nicolas Sendrier, INRIA, France

Jean-Pierre Tillich, INRIA, France

Valentin Vasseur, INRIA, France

Gilles Zémor, IMB, University of Bordeaux, France

The BIKE team has made the the following changes targeting the 2nd round of the NIST Post-Quantum Cryptography Standardization project:

- **Decoder**: The Backflip decoder has been devised and added to our proposal as an alternative decoder. This algorithm attains negligible decoding failure rates which enabled the development of IND-CCA BIKE variants. The decoder algorithm should be seen as a building-block that users can pick and choose according to their requirements (static/ephemeral keys, decoding failure rate, performance, etc).

- **IND-CCA BIKE Variants**: Three new BIKE variants that attain IND-CCA security have been devised: BIKE-1-CCA, BIKE-2-CCA, BIKE-3-CCA. These are modified versions of BIKE-1, BIKE-2 and BIKE-3 schemes, respectively. These new variants allow for static keys.

- **Spec**: The specification document has been updated to integrate the Backflip decoder description, the IND-CCA BIKE variants description, the IND-CCA security proof, the suggested parameters for the IND-CCA variants, and the analysis of the BIKE hardware design.

- **Reference and Optimized Implementations**: The reference and optimized implementations have been updated to integrate the alternative Backflip decoder and the IND-CCA BIKE variants.

- **Hardware Implementation**: A BIKE hardware design targeting the Xilinx Artix-7 has been developed and benchmarked.

- **Team members**: Valentin Vasseur joined the BIKE team.