Version 1.0.1.

- Fixed some typos in Algorithms 14 and 15. Thanks to Markku-Juhani O. Saarinen for bringing them to our attention.

Version 1.0.2.

- References to [LS17, LS19, BN24] added in Section 1.1. Thanks to Alice Silverberg for bringing them to our attention.

Version 1.1.

- Updated the omSVP game to include ω as a 'trivial win' in Fig. 5 and updated the reduction to the SUF-CMA security of HAWK, see Section 6. The original omSVP game [DPPvW22] could be trivially won using the results of [LJPW24].
- Updated the introduction to reflect new understanding of the BUFF transform [DFHS24, ADM+24], side channel analysis [GR24] and the cryptanalysis of smLIP [MPPW24, CFM+24, EP24, LJPW24, APvW25] and omSVP [LJPW24].
- Switched the adaptive reprogramming lemma (Lemma 4) to that of [GHHM21] and amended the upper bound on distinguishing advantage.

References

[ADM+24] Thomas Aulbach, Samed Düzlü, Michael Meyer, Patrick Struck, and Maximiliane Weishäupl, *Hash your keys before signing - BUFF security of the additional NIST PQC signatures*, Post-Quantum Cryptography - 15th International Workshop, PQCrypto 2024, Part II (Markku-Juhani Saarinen and Daniel Smith-Tone, eds.), Springer, Cham, June 2024, pp. 301–335.

[APvW25] Bill Allombert, Alice Pellet-Mary, and Wessel P. J. van Woerden, *Cryptanalysis of rank-2 module-lip: a single real embedding is all it takes*, EUROCRYPT 2025 (Serge Fehr and Pierre-Alain Fouque, eds.), LNCS, Springer, 2025, to appear.

[BN24] Henry Bambury and Phong Q. Nguyen, *Improved provable reduction of NTRU and hypercubic lattices*, Post-Quantum Cryptography - 15th International Workshop, PQCrypto 2024, Part I (Markku-Juhani Saarinen and Daniel Smith-Tone, eds.), Springer, Cham, June 2024, pp. 343–370.

[CFM+24] Clémence Chevignard, Pierre-Alain Fouque, Guilhem Mureau, Alice Pellet-Mary, and Alexandre Wallet, *A reduction from hawk to the principal ideal problem in a quaternion algebra*, Cryptology ePrint Archive, Report 2024/1147, 2024.

[DFHS24] Jelle Don, Serge Fehr, Yu-Hsuan Huang, and Patrick Struck, *On the (in)security of the BUFF transform*, CRYPTO 2024, Part I (Leonid Reyzin and Douglas Stebila, eds.), LNCS, vol. 14920, Springer, Cham, August 2024, pp. 246–275.

[DPPvW22] Léo Ducas, Eamonn W. Postlethwaite, Ludo N. Pulles, and Wessel P. J. van Woerden, *Hawk: Module LIP makes lattice signatures fast, compact and simple*, ASIACRYPT 2022, Part IV (Shweta Agrawal and Dongdai Lin, eds.), LNCS, vol. 13794, Springer, Cham, December 2022, pp. 65–94.

[EP24] Thomas Espitau and Heorhii Pliatsok, *On hermitian decomposition lattices and the module-LIP problem in rank 2*, Cryptology ePrint Archive, Report 2024/1148, 2024.

[GHHM21] Alex B. Grilo, Kathrin Hövelmanns, Andreas Hülsing, and Christian Majenz, *Tight adaptive reprogramming in the QROM*, ASIACRYPT 2021, Part I (Mehdi Tibouchi and Huaxiong Wang, eds.), LNCS, vol. 13090, Springer, Cham, December 2021, pp. 637–667.

[GR24] Morgane Guerreau and Mélissa Rossi, *A not so discrete sampler: Power analysis attacks on hawk signature scheme*, IACR Transactions on Cryptographic Hardware and Embedded Systems **2024** (2024), no. 4, 156–178.

[LJPW24] Hengyi Luo, Kaijie Jiang, Yanbin Pan, and Anyu Wang, *Cryptanalysis of rank-2 module-LIP with symplectic automorphisms*, ASIACRYPT 2024, Part IV (Kai-Min Chung and Yu Sasaki, eds.), LNCS, vol. 15487, Springer, Singapore, December 2024, pp. 359–385.

[LS17] Hendrik W. Lenstra, Jr. and Alice Silverberg, *Lattices with symmetry*, Journal of Cryptology **30** (2017), no. 3, 760–804.

[LS19] Hendrik W. Lenstra Jr. and Alice Silverberg, *Testing isomorphism of lattices over CM-Orders*, SIAM Journal on Computing **48** (2019), no. 4, 1300–1334.

[MPPW24] Guilhem Mureau, Alice Pellet-Mary, Georgii Pliatsok, and Alexandre Wallet, *Cryptanalysis of rank-2 module-LIP in totally real number fields*, EUROCRYPT 2024, Part VII (Marc Joye and Gregor Leander, eds.), LNCS, vol. 14657, Springer, Cham, May 2024, pp. 226–255.