Mathematics and Computer Science Seminary
Djilali Liabès University - Sidi Bel Abbès - Saturday, 23/05/2026

# Extending Constant-Time Simplified SWU Mapping to handle Twists of BLS24 and BLS48 Pairing-Friendly Curves

**Kamel Mohamed Faraoun**
Evolutionary Engeneering & Distributed Information Systems Laboratory (EEDIS-L)
Djillali Liabès University of Sidi Bel Abbès
kamel_mh@yahoo.fr

**Abstract**

We presents a novel advancements in extending the simplified Shallue–van de Woestijne–Ulas (SWU) mapping technique to BLS24 and BLS48 elliptic curves. The SWU method ensures constant-time execution for point mapping on these curves, effectively mitigating side-channel vulnerabilities and addressing limitations in existing implementations. An innovative formalism is introduced to enable the efficient computation of isogeny maps for curve twists over corresponding high-order extension fields, supported by rigorous mathematical justifications and proofs. The proposed method is evaluated on several widely used BLS24 and BLS48 curves, with the computed isogenies benchmarked through an optimized Rust implementation. Additionally, an enhanced variant of the simplified SWU mapping is presented, eliminating the costly inversion operation and thereby improving overall performance. Finally, four optimized constructions of BLS48 curves are proposed, enhancing their suitability for security applications at both 256-bit and 128-bit levels.

**Mathematics Subject Classification:** 11G20, 11T71, 14G50, 11Y16.
**Keywords and phrases:** SWU Mapping, Pairing-based cryptography, BLS Curves, Constant-time implementation.

## References

[1] Faraoun, K-M. Extending constant-time simplified SWU mapping to handle twists of BLS24 and BLS48 pairing-friendly curves. Journal of Information Security and Applications, 2025, vol. 93, p. 104–107.