Séminaire de Mathématiques et Informatique

Université Djilali Liabès - Sidi Bel Abbès - le 25 janvier 2025

Bilinear Pairings on Elliptic Curves and Applications in Cryptography

Kamel Mohamed FARAOUN

Evolutionary Engeneering and Distributed Information System Laboratory - UDL

Abstract :

Bilinear pairings on elliptic curves, a fascinating and impressive field, have revolutionized modern cryptography by paving the way for new classes of secure and efficient protocols. Thanks to their unique mathematical properties, these tools have enabled protocols to venture into previously inaccessible areas, such as identity-based encryption (IBE), aggregate digital signatures, zero-knowledge proofs (z-SNARKs), and delegation systems. By leveraging the interaction between additive and multiplicative groups through bilinear functions, pairings provide a powerful framework for constructing cryptographic primitives with advanced properties, including public verifiability, data aggregation, and flexible key management. This presentation will explore the foundations of bilinear pairings, their essential properties, and their transformative impact on modern cryptography, while highlighting concrete applications that redefine the security and efficiency of distributed systems.

Keywords : Bilinear Pairings, Elliptic Curves, Group Theory, Algorithmic Complexity, Cryptographic Protocols.

Mathematics Subject Classification : 11G05, 11T71, 14G50, 14H52, 94A60.

ACM Computing Classification System : [E.3], [G.1.4.7], [G.2], [F.2.1.1], [K.6.5.1].

References

[1] Boneh, D. *Pairing-based cryptography: Past, present, and future. In : International Conference on the Theory and Application of Cryptology and Information Security.* Springer, Berlin Heidelberg, (2012).

[2] Boneh, D. and Boyen, X. *Secure identity based encryption without random oracles. In : Annual International Cryptology Conference.* Springer, Berlin Heidelberg, pp. 443–459, (2004).

[3] El Mrabet, N. and Joye, M. *Guide to Pairing-Based Cryptography.* CRC Press, (2017).

[4] Miller, V. S. *The Weil pairing, and its efficient calculation.* Journal of cryptology, **17**(4), pp. 235–26, (2004).

[5] Waters, B. *Pairing-Based Cryptography-Pairing* Springer-Verlag Berlin Heidelberg, (2009).