ICRAMCS 2026

THE EIGHTH EDITION OF THE INTERNATIONAL CONFERENCE ON RESEARCH IN APPLIED MATHEMATICS AND COMPUTER SCIENCE
April 23-24-25, 2026 | Marrakech, Morocco

A Generalization of Dickson and Chebyshev Polynomials: Commutative Families for Cryptographic Applications

Communication Info

Authors:
Khalid KHALLOUKI[1]
Najat RAFI[1]
Khadija BOUZKOURA[1]
Abedelhakim CHILLALI[2]

[1] LAMS laboratory, Department of Mathematics and Computer Science, Faculty of Sciences Ben M'Sick, Hassan II University of Casablanca,, Morocco.
[2] LMSD laboratory, Department of Mathematics, Sidi Mohamed Ben Abdallah University-USMBA, Polydisciplinary Faculty of Taza, Morocco.

Keywords:
(1) Chebyshev polynomials
(2) Dickson polynomials
(3) Polynomial generalization
(4) Commutativity
(5) Cryptographic protocols

Abstract

Chebyshev and Dickson polynomials are commutative families used in cryptography for protocols like Diffie-Hellman and ElGamal. We introduce a new family generalizing both to arbitrary order $k \geq 2$, preserving the commutativity property $P_m \circ P_n = P_{mn}$. We study their algebraic properties and present cryptographic applications including key exchange and encryption schemes.

References

[1] Diffie, W., & Hellman, M. (1976). New directions in cryptography. IEEE Transactions on Information Theory, 22(6), 644-654.
[2] Lidl, R., Mullen, G. L., & Turnwald, G. (1993). Dickson Polynomials. Chapman and Hall/CRC.
[3] Prabhakar, N. V. S. S., et al. (2025). Chebyshev Polynomial based ElGamal Encryption with Chaotic Greater Cane Algorithm. International Journal of Computational and Experimental Science and Engineering, 11(2).
[4] Fried, M., & Lidl, R. (1987). On Dickson Polynomials and Rédei Functions. Contributions to General Algebra, 5, 139-149.
[5] Lidl, R., & Niederreiter, H. (1997). Finite Fields. Cambridge University Press.
[6] Ritt, J. F. (1922). Prime and composite polynomials. Transactions of the American Mathematical Society, 23(1), 51-66.
[7] Dickson, L. E. (1897). The analytic representation of substitutions. Annals of Mathematics, 11(1), 65-120