Contribution ID: **303** Type: **Paper presentation**

Practical Cryptanalysis of ECDSA: Comparative Efficiency Analysis of Brute-Force and Baby-Step Giant-Step Key Recovery Methods

Friday 19 September 2025 15:15 (15 minutes)

The Elliptic Curve Digital Signature Algorithm (ECDSA) is pivotal for securing digital information across various applications. This paper investigates ECDSA's security by focusing on two generic attack methodologies: brute-force and Baby-Step Giant-Step (BSGS). We evaluate their theoretical effectiveness and practical implications by analyzing existing research and known vulnerabilities. Our findings underscore the practical limits of ECDSA security, highlighting the critical roles of robust key generation and secure implementation practices. This work aims to provide insights for practitioners and researchers in applied cryptography, emphasizing the ongoing need for vigilance and adaptation in cryptographic security.

Author: PATRASCU, Ionel

Co-author: Mr SIMINIUC, Sergiu (Technical University of Moldova)

Presenter: PATRASCU, Ionel

Session Classification: Technologies for Future Internet