2nd International Conference on Security & Privacy (ICSP2021)

www.icsp.co.in

November 16-17, 2021

Organized by

Department of Mathematics, National Institute of Technology Jamshedpur

List of Accepted Papers

1. **Title:** Higher Order c-Differentials.
   Authors: Aaron Geary, Marco Calderini, Constanza Riera, and Pantelimon Stănică
2. **Title:** First-Order Side-Channel Leakage Analysis of Masked but Asynchronous AES.
   Authors: Antoine Bouvet, Sylvain Guilley, and Lukas Vlasak
3. **Title:** Side-Channel Analysis of CRYSTALS-Kyber and A Novel Low-Cost Countermeasure.
   Authors: Meziane Hamoudi, Amina Bel Korchi, Sylvain Guilley, Sofiane Takarabt, Khaled Karray, and Youssef Souissi
4. **Title:** Symmetric Cryptography and Hash Functions, Mathematical Foundations of Cryptography A Suitable Proposal of S-Boxes (Inverse-Like) for the AES, Their Analysis and Performances.
   Authors: Said Eddahmani and Sihem Mesnager
5. **Title:** A Method of Integer Factorization.
   Authors: Zhizhong Pan and Xiao Li
6. **Title:** Embedded Systems Security, Security in Hardware Towards a Black-Box Security Evaluation Framework.
   Authors: Mosabbah Mushir Ahmed, Youssef Souissi, Oualid Trabelsi, Sylvain Guilley, Antoine Bouvet, and Sofiane Takarabt
7. **Title:** Multi-source Fault Injection Detection Using Machine Learning and Sensor Fusion.
   Authors: Ritu-Ranjan Shrivastwa, Sylvain Guilley, and Jean-Luc Danger
8. **Title:** Authentication, Key Management, Public Key (Asymmetric) Techniques, Information-Theoretic Techniques Secure Multi-Party Computation Using Pre-distributed Information from an Initializer.
   Authors: Amirreza Hamidi and Hossein Ghodosixii
9. **Title:** Contents Evolving Secret Sharing in Almost Semi-honest Model.
   Authors: Jyotirmoy Pramanik and Avishek Adhikari
10. **Title:** Traceable and Verifier-Local Revocable Attribute-Based Signature with Constant Length.
    Authors: Syed Taqi Ali