Indocrypt 2025: List of Accepted Papers

1. **On the Classical Hardness of the Semidirect Discrete Logarithm Problem in Finite Groups**
   Mohammad Ferry Husnil Arif (Universitas Indonesia) and Muhammad Imran (Universitas Indonesia).

2. **Smooth twins for cryptographic applications from Pell equations**
   Daniel Berger (DLR).

3. **BOIL: Proof-Carrying Data from Accumulation of Correlated Holographic IOPs**
   Maksim Nikolaev , Tohru Kohrita and Javier Silva.

4. **Multivariate Encryptions with LL' perturbations - Is it possible to repair HFE in encryption?**
   Pierre Varjabedian (THALES DIS, Université de Versailles Saint-Quentin en Yvelines) and Jacques Patarin (THALES DIS, Université de Versailles Saint-Quentin en Yvelines).

5. **Hardened CTIDH: Dummy-Free and Deterministic CTIDH**
   Gustavo Banegas (Inria and Laboratoire d'Informatique de l'Ecole polytechnique), Andreas Hellenbrand (RheinMain University of Applied Sciences Wiesbaden) and Matheus Saldanha (Universidade Federal de Santa Catarina).

6. **Efficient Identity-Based Inner Product Functional Encryption from RLWE**
   Anushree Belel (ROVIRA I VIRGILI UNIVERSITY) and Junji Shikata (YOKOHAMA NATIONAL UNIVERSITY).

7. **New Results in Quantum Analysis of LED: Featuring One and Two Oracle Attacks**
   Siyi Wang (Nanyang Technological University), Kyungbae Jang (Hansung University), Anubhab Baksi (Nanyang Technological University), Sumanta Chakraborty (Techno International New Town), Anupam Chattopadhyay (Nanyang Technological University) and Hwajeong Seo (Hansung University).

8. **Traceable Bottom-Up Secret Sharing and Law & Order on Community Social Key Recovery**
   Rittwik Hajra (Indian Statistical Institute, Kolkata, India), Subha Kar (Indian Statistical Institute, Kolkata), Pratyay Mukherjee (Supra Research) and Soumit Pal (Indian Statistical Institute, Kolkata).

9. **Rejection-Free Framework of Zero-Knowledge Proof based on Hint-MLWE**
   Antoine Douteau (Université Caen Normandie) and Adeline Roux-Langlois (Université Caen Normandie).

10. **One-Time Memories Secure against Depth-Bounded Quantum Circuits**
    Kyosuke Sekii (University of Tsukuba) and Takashi Nishide (University of Tsukuba).

11. **Practically Implementable Minimal Universal Gate Sets for Multi-Qudit Systems with Cryptographic Validation**
    Anisha Dutta (Tata Steel Ltd.), Sayantan Chakraborty (Accenture), Chandan Goswami (Presidency University) and Avishek Adhikari (Presidency University).
12. **Key-Updatable Identity-Based Signature Schemes**
    Tobias Guggemos (Ludwig-Maximilians-Universität Munich) and Farzin Renan (Middle East Technical University).

13. **Module Lattice based constant-size group signature with Verifier Local Revocation and Backward Unlinkability**
    Komal Pursharthi (Maulana Azad National Institute of Technology, Bhopal) and Dheerendra Mishra (Maulana Azad National Institute of Technology, Bhopal).

14. **High-Performance FPGA Implementation of a Recursive Modular Karatsuba Multiplier over GF(2^m)**
    Ruby Kumari (CEERI, Pilani, India), Sumeet Saurav (CEERI, Pilani, India) and Abhijit Karmakar (CEERI, Pilani, India).

15. **Improved Modeling for Substitution Boxes with Negative Samples and Beyond**
    Debranjan Pal (Indian Institute of Technology Kanpur), Anubhab Baksi (Lund University, Sweden), Surajit Mandal (Indian Institute of Technology Madras) and Santanu Sarkar (Indian Institute of Technology Madras).

16. **COMPASS: A Compact PASS-lineage Accumulator with Succinct Proofs**
    Tao-Hsiang Chang (National Chengchi University), Jen Chieh Hsu (National Chengchi University), Hao-Yi Hsu (National Chengchi University), Raylin Tso (National Chengchi University) and Masahiro Mambo (Kanazawa University).

17. **Beyond Confidentiality: Framing-Resistant Secure Vault Schemes**
    Meghna Sengupta (University of Edinburgh).

18. **Refined Linear Approximations for ARX Ciphers and Their Application to ChaCha**
    Yurie Okada (The University of Osaka), Atsuki Nagai (KDDI CORPORATION) and Atsuko Miyaji (The University of Osaka).

19. **Beyond Sequential Walks: Parallelizing the GA-dlog Problem**
    Sudeshna Karmakar (IIT Madras), Abul Kalam (IIT Madras) and Santanu Sarkar (IIT Madras).