

Fault analysis in cryptography

Deskripsi Lengkap: <https://lib.ui.ac.id/detail?id=20409533&lokasi=lokal>

Abstrak

Preventing fault attacks without sacrificing performance is nontrivial and this is the subject of this book. Part I deals with side-channel analysis and its relevance to fault attacks. The chapters in Part II cover fault analysis in secret key cryptography, with chapters on block ciphers, fault analysis of DES and AES, countermeasures for symmetric-key ciphers, and countermeasures against attacks on AES. Part III deals with fault analysis in public key cryptography, with chapters dedicated to classical RSA and RSA-CRT implementations, elliptic curve cryptosystems and countermeasures using fault detection, devices resilient to fault injection attacks, lattice-based fault attacks on signatures, and fault attacks on pairing-based cryptography. Part IV examines fault attacks on stream ciphers and how faults interact with countermeasures used to prevent power analysis attacks. Finally, Part V contains chapters that explain how fault attacks are implemented, with chapters on fault injection technologies for microprocessors, and fault injection and key retrieval experiments on a widely used evaluation board.