Automated methods in cryptographic fault analysis

Deskripsi Lengkap: https://lib.ui.ac.id/detail?id=20506932&lokasi=lokal

----

Abstrak

This book presents a collection of automated methods that are useful for different aspects of fault analysis in cryptography. The first part focuses on automated analysis of symmetric cipher design specifications, software implementations, and hardware circuits. The second part provides automated deployment of countermeasures. The third part provides automated evaluation of countermeasures against fault attacks. Finally, the fourth part focuses on automating fault attack experiments. The presented methods enable software developers, circuit designers, and cryptographers to test and harden their products.