

UNIVERSITY OF SOUTH FLORIDA

Defense of a Doctoral Dissertation

Secure Lightweight Cryptographic Hardware Constructions for Deeply Embedded
Systems

by

Jasmin Kaur

For the Ph.D. degree in Computer Science and Engineering

Lightweight cryptography plays a vital role in securing various resource-constrained embedded systems, including deeply-embedded systems, implantable and wearable medical devices, smart homes, RFID tags, sensor networks, and privacy-constrained usage models. However, the security of these systems can be compromised by fault analysis attacks, a type of side-channel attack. This dissertation presents novel cryptographic hardware constructions for resource-constrained embedded systems, including deeply-embedded systems, implantable and wearable medical devices, smart homes, RFID tags, sensor networks, and privacy-constrained usage models. The dissertation is organized as follows: Chapter 1: Introduction. Chapter 2: Preliminaries. Chapter 3: Fault Analysis Attacks. Chapter 4: Fault Analysis Attacks on Stream Ciphers. Chapter 5: Fault Analysis Attacks on Block Ciphers. Chapter 6: Fault Analysis Attacks on Elliptic Curve Cryptography. Chapter 7: Fault Analysis Attacks on RSA. Chapter 8: Fault Analysis Attacks on ECC. Chapter 9: Fault Analysis Attacks on RSA. Chapter 10: Fault Analysis Attacks on ECC. Chapter 11: Fault Analysis Attacks on RSA. Chapter 12: Fault Analysis Attacks on ECC. Chapter 13: Fault Analysis Attacks on RSA. Chapter 14: Fault Analysis Attacks on ECC. Chapter 15: Fault Analysis Attacks on RSA. Chapter 16: Fault Analysis Attacks on ECC. Chapter 17: Fault Analysis Attacks on RSA. Chapter 18: Fault Analysis Attacks on ECC. Chapter 19: Fault Analysis Attacks on RSA. Chapter 20: Fault Analysis Attacks on ECC. Chapter 21: Fault Analysis Attacks on RSA. Chapter 22: Fault Analysis Attacks on ECC. Chapter 23: Fault Analysis Attacks on RSA. Chapter 24: Fault Analysis Attacks on ECC. Chapter 25: Fault Analysis Attacks on RSA. Chapter 26: Fault Analysis Attacks on ECC. Chapter 27: Fault Analysis Attacks on RSA. Chapter 28: Fault Analysis Attacks on ECC. Chapter 29: Fault Analysis Attacks on RSA. Chapter 30: Fault Analysis Attacks on ECC. Chapter 31: Fault Analysis Attacks on RSA. Chapter 32: Fault Analysis Attacks on ECC. Chapter 33: Fault Analysis Attacks on RSA. Chapter 34: Fault Analysis Attacks on ECC. Chapter 35: Fault Analysis Attacks on RSA. Chapter 36: Fault Analysis Attacks on ECC. Chapter 37: Fault Analysis Attacks on RSA. Chapter 38: Fault Analysis Attacks on ECC. Chapter 39: Fault Analysis Attacks on RSA. Chapter 40: Fault Analysis Attacks on ECC. Chapter 41: Fault Analysis Attacks on RSA. Chapter 42: Fault Analysis Attacks on ECC. Chapter 43: Fault Analysis Attacks on RSA. Chapter 44: Fault Analysis Attacks on ECC. Chapter 45: Fault Analysis Attacks on RSA. Chapter 46: Fault Analysis Attacks on ECC. Chapter 47: Fault Analysis Attacks on RSA. Chapter 48: Fault Analysis Attacks on ECC. Chapter 49: Fault Analysis Attacks on RSA. Chapter 50: Fault Analysis Attacks on ECC. Chapter 51: Fault Analysis Attacks on RSA. Chapter 52: Fault Analysis Attacks on ECC. Chapter 53: Fault Analysis Attacks on RSA. Chapter 54: Fault Analysis Attacks on ECC. Chapter 55: Fault Analysis Attacks on RSA. Chapter 56: Fault Analysis Attacks on ECC. Chapter 57: Fault Analysis Attacks on RSA. Chapter 58: Fault Analysis Attacks on ECC. Chapter 59: Fault Analysis Attacks on RSA. Chapter 60: Fault Analysis Attacks on ECC. Chapter 61: Fault Analysis Attacks on RSA. Chapter 62: Fault Analysis Attacks on ECC. Chapter 63: Fault Analysis Attacks on RSA. Chapter 64: Fault Analysis Attacks on ECC. Chapter 65: Fault Analysis Attacks on RSA. Chapter 66: Fault Analysis Attacks on ECC. Chapter 67: Fault Analysis Attacks on RSA. Chapter 68: Fault Analysis Attacks on ECC. Chapter 69: Fault Analysis Attacks on RSA. Chapter 70: Fault Analysis Attacks on ECC. Chapter 71: Fault Analysis Attacks on RSA. Chapter 72: Fault Analysis Attacks on ECC. Chapter 73: Fault Analysis Attacks on RSA. Chapter 74: Fault Analysis Attacks on ECC. Chapter 75: Fault Analysis Attacks on RSA. Chapter 76: Fault Analysis Attacks on ECC. Chapter 77: Fault Analysis Attacks on RSA. Chapter 78: Fault Analysis Attacks on ECC. Chapter 79: Fault Analysis Attacks on RSA. Chapter 80: Fault Analysis Attacks on ECC. Chapter 81: Fault Analysis Attacks on RSA. Chapter 82: Fault Analysis Attacks on ECC. Chapter 83: Fault Analysis Attacks on RSA. Chapter 84: Fault Analysis Attacks on ECC. Chapter 85: Fault Analysis Attacks on RSA. Chapter 86: Fault Analysis Attacks on ECC. Chapter 87: Fault Analysis Attacks on RSA. Chapter 88: Fault Analysis Attacks on ECC. Chapter 89: Fault Analysis Attacks on RSA. Chapter 90: Fault Analysis Attacks on ECC. Chapter 91: Fault Analysis Attacks on RSA. Chapter 92: Fault Analysis Attacks on ECC. Chapter 93: Fault Analysis Attacks on RSA. Chapter 94: Fault Analysis Attacks on ECC. Chapter 95: Fault Analysis Attacks on RSA. Chapter 96: Fault Analysis Attacks on ECC. Chapter 97: Fault Analysis Attacks on RSA. Chapter 98: Fault Analysis Attacks on ECC. Chapter 99: Fault Analysis Attacks on RSA. Chapter 100: Fault Analysis Attacks on ECC.