

(((特集2)))

LSIを“盗聴”から守る

暗号回路へのサイドチャンネル攻撃とその対策



本特集では、正規の通信経路(I/Oピン)以外からLSIの秘密情報(例えば暗号の秘密かぎ)を取り出す「サイドチャンネル攻撃」を取り上げます。サイドチャンネル攻撃は、例えば、LSIの動作時にチップそのものが発する電磁波や熱、消費電力の変化を解析して、データを読み取ります。特集では、サイドチャンネル攻撃のからくりをpushしつつ、DES(Data Encryption Standard)やRSA、AES(Advanced Encryption Standard)などの暗号回路について、どのように対策を施すべきかその指針を述べます。

第1章

あなたが設計したLSIから秘密情報が漏れてます

暗号回路のトレンドはアルゴリズムの標準化から実装の安全性評価へ

佐藤 証

第2章

サイドチャンネル攻撃のからくりを理解する

DESとRSAに対する攻撃と基本的な防御法

佐藤 証

Appendix

乱数マスクを用いて差分電力解析に対抗

佐藤 証, 高橋 芳夫

第3章

電力、電磁波から暗号回路の内部動作を解析する

DES暗号回路を実測し、差分電力解析を行う

高橋 芳夫, 佐藤 証

第4章

システムLSI設計におけるDPA対策の指針とAES暗号の対策例

対策の有効性と回路コストのバランスをじょうずにとる

森岡 澄夫