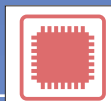


特集 2

Design Wave

設計コンテスト2004
入賞デザイン



デバイスの記事



関連データ



ビギナーズ



暗号回路設計の トライ&エラー

Design Wave設計コンテスト2004のProfessional部門とStudent部門のそれぞれで1位となった設計を紹介します。課題は「共通かぎ暗号AES (Advanced Encryption Standard) 用SubBytes変換回路」です。比較的シンプルな課題に対して、どのように工夫を施し、オリジナリティのある回路を設計したかについて詳しく解説します。

Contents

第1章 共通かぎブロック暗号AES用SubBytes変換回路設計のポイント

和田知久, 森屋和喜

第2章 合成体とパイプラインで小規模・高速な回路を目ざす — Design Wave設計コンテスト2004 Professional部門 第1位

近藤靖浩

第3章 AES暗号化処理を考えてSubBytes変換回路を最適化 — Design Wave設計コンテスト2004 Student部門 第1位

チームショツチュウ焼酎泡盛ーズ (重信優也, 中川陽介, 松村友哉)