

RSA暗号化回路設計の トライ&エラー

～Design Wave設計コンテスト2008 入賞デザイン～

Contents

Design Wave設計コンテスト2008]のProfessional部門で優勝した設計の詳細を、開発者の試行錯誤の過程とともに紹介します。また、Student部門で入賞した各設計の概要を紹介します。コンテストの課題はRSA暗号化回路です。RSA暗号は、米国MIT(Massachusetts Institute of Technology)が開発した公開鍵暗号方式です。電子メールなどの暗号化に用いられるPGPや、電子商取引で使われるSSLなど、広く実用化されています。



— Design Wave設計コンテスト2008総評

第1章

RSA暗号化器設計のポイント

和田知久, 林 輝彦



— Design Wave設計コンテスト2008 Professional部門 優勝

回路規模最小を目指した
FPGA向けRSA暗号化器の設計

上原昭宏