

機能メモリ混載システムLSI研究室 (Network System On Chip Lab.)

1

機能メモリ混載システムLSI研究室紹介

- 設立: 2003年4月
- 研究テーマ
 - カスタムシステムLSIの設計技術
 - マスク(ビア)プログラマブルロジック技術 **VPEX**
 - フィールドプログラマブルロジック技術 **ePLX**
 - 対タンパ性(電力差分析)回路設計技術 **Domino-RSL**
 - ネットワークシステムへの応用
 - パターン(ウイルス)検知システム(マイコン, FPGA, ePLX)
 - 暗号処理システム(ePLX, VPEX)
 - セキュリティデバイスを用いた個人認証システム(VPEX)
- 研究メンバー
 - 教授: 藤野 毅
 - 大学院学生(社会人D1) 1名, (M2): 5名, (M1): 7名
 - 学部学生(M0): 1名, (B4): 9名

2

本日の内容

- 研究を説明する単語解説
 - 可変論理LSI
 - EB直描
 - 暗号技術
- 特徴あるLSI設計技術
 - ビアプログラマブルロジック回路 **VPEX**
 - リコンフィギャラブルロジック回路 **ePLX**
 - 耐タンパ性回路設計技術 **Domino-RSL**
- ネットワークシステムへの応用
 - **FPGA/ARMマイコン**を用いたセキュリティシステム

3

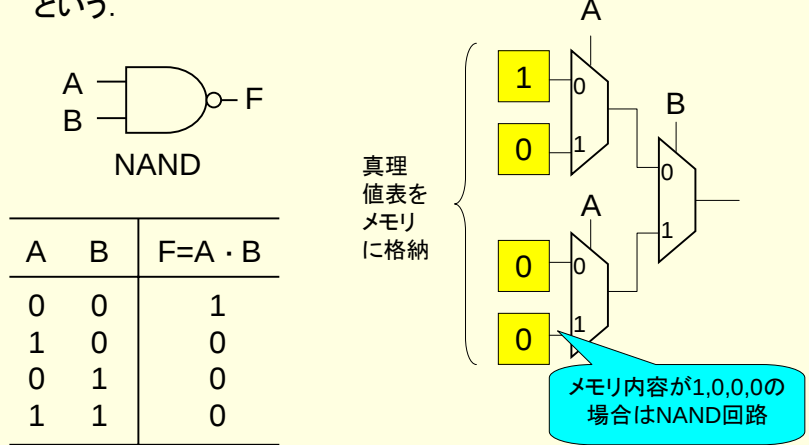
藤野研究室の研究テーマ

- 新機能メモリを搭載したLSI設計技術をコアテクノロジーとして
⇒メモリの技術を使用した **可変論理LSI**
- システムLSIの高性能化 & 低コスト化を実現する設計技術を開発し
⇒可変論理LSI & **EB直描**で低コスト化
- ネットワーク情報機器のアプリケーションへ応用
⇒ **暗号回路**, 文字列検索回路

4

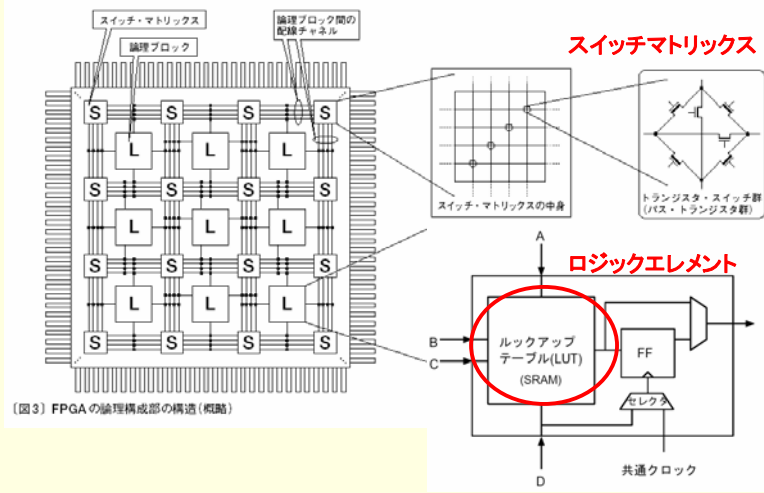
メモリを使った論理素子

- 右図のように4ビットのメモリとセレクタを組み合わせることにより、2入力のすべての論理を実現できる
- この素子名をルックアップテーブル(LUT: Look Up Table)という。

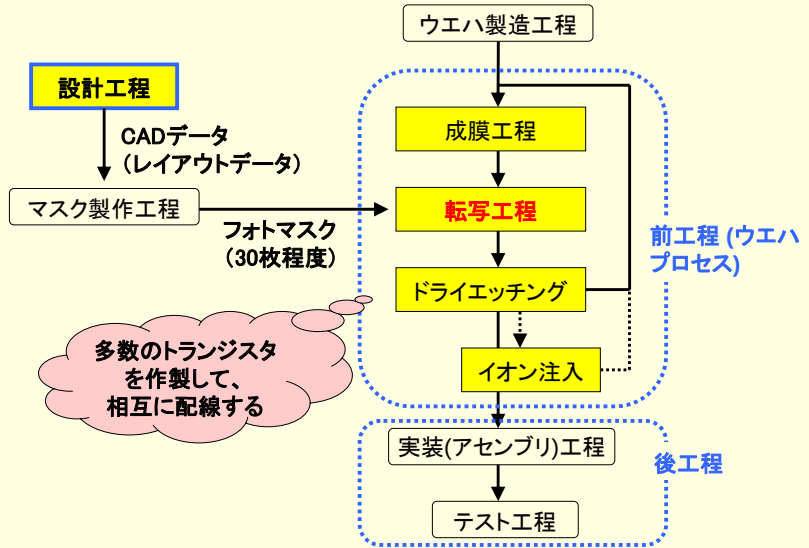


FPGAの構造

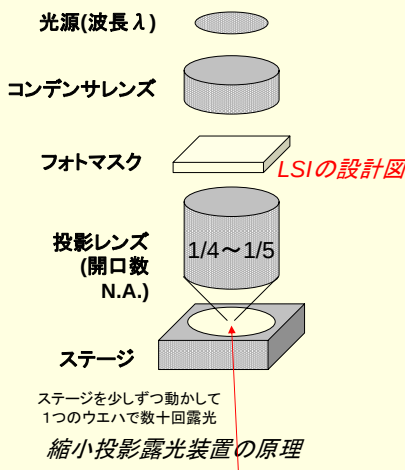
- 論理変更: ロジックエレメント (LUTとFFより構成)
- 配線変更: スイッチマトリックス



LSIの設計・製造工程



パターン転写装置(光転写)



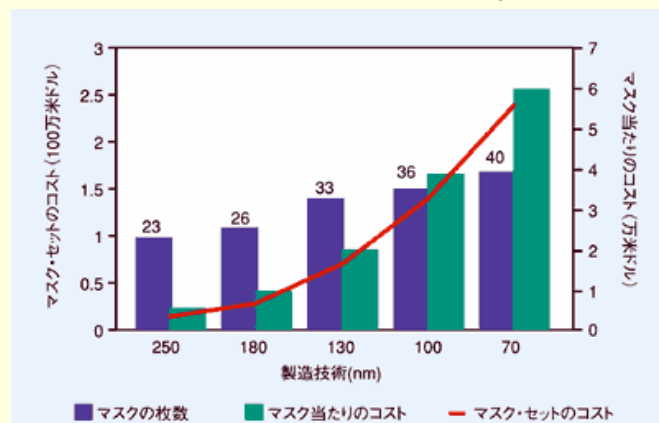
光転写装置(ステッパー)外観

大量に同じLSIが作られる!

* 栃木ニコンホームページより引用

微細化とともに増大するマスクコスト

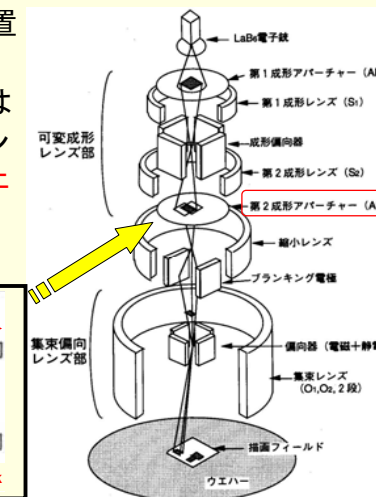
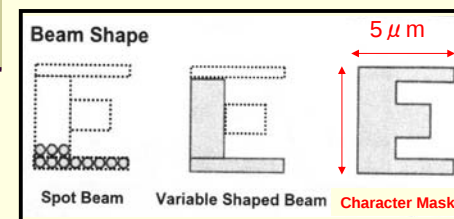
- 90nm世代で1億円を突破している
⇒生涯生産個数10万個でも1000円/chip



出典:ライトスピード・セミコンダクター社

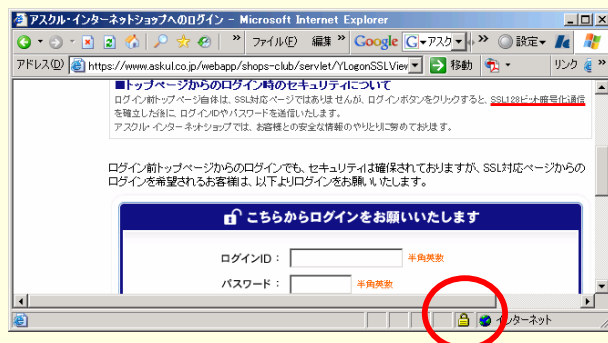
パターン転写装置(EB直描)

- パターンを形成するためには右記のような電子ビーム描画装置を使用する。
- $5\mu\text{m}$ 角以下の定型パターンは「はんこ押し」で高速のパターン作成が可能(キャラクタープロジェクション露光)



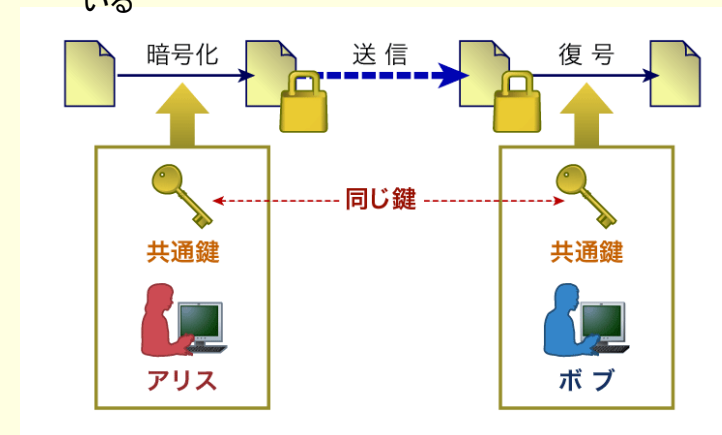
暗号技術の用途

- インターネット上での買い物(クレジットカード番号の送信時)
- PCのHDDやUSBメモリ紛失時対策(内部データ情報を暗号化して保存)
- ICカード(身分証明, 定期券, 電子マネー)
- 無線LAN接続(無線アクセスポイントとPCの間の通信)



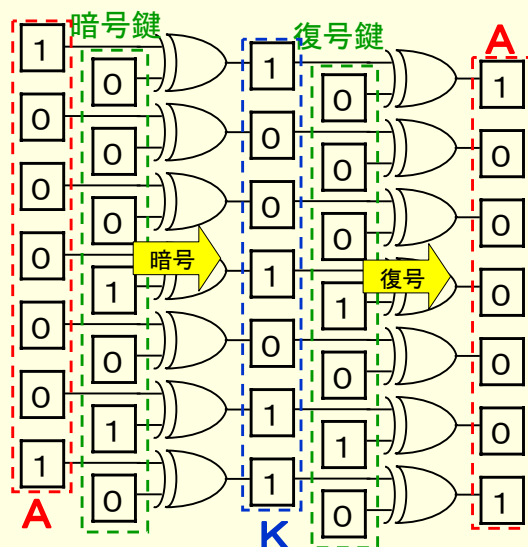
共通鍵暗号

- DES, AESなどの実用暗号があり
 - 転置処理やEXOR回路を用いた換字処理が使用されている



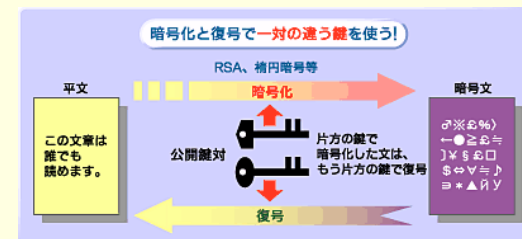
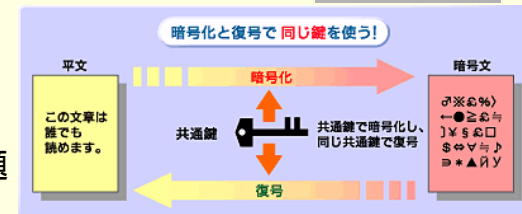
共通鍵暗号の原理

- 同じ暗号鍵でE XOR回路を利用すると復号できる



暗号技術

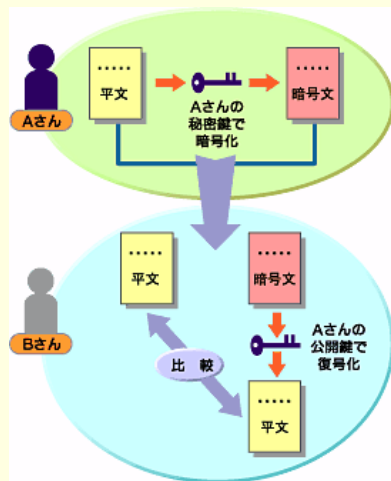
- 共通鍵暗号
 - 高速
 - DES, AES
 - 鍵の配送が問題
- 公開鍵暗号
 - 低速
 - RSA
 - 鍵の配送
 - 個人認証 (電子署名)



<http://www.atmarkit.co.jp/fnetwork/rensai/pki01/pki01.html>より引用

公開鍵暗号による個人認証(電子署名)

- Aさんは平文と自分の秘密鍵で暗号化した暗号文を送付
- Bさんは送付された暗号文をAさんの公開鍵で復号化し平文を比較
- 一致すればAさんの文章であることが証明される



この暗号文を作成できるのは秘密鍵を所有しているAさんの他にはいないから

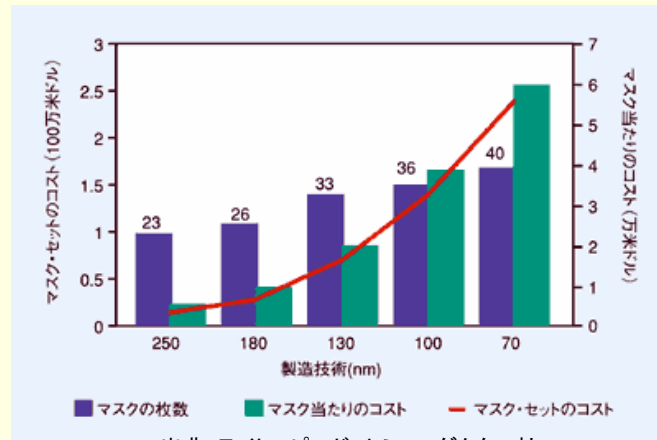
<http://www.atmarkit.co.jp/fnetwork/rensai/pki01/pki01.html>より引用

本日の内容

- 研究を説明する単語解説
 - 可変論理LSI
 - EB直描
 - 暗号技術
- 特徴あるLSI設計技術
 - ビアプログラマブルロジック回路 **VPEx**
 - リコンフィギャラブルロジック回路 **ePLX**
 - 耐サイドチャネルアタック回路設計技術 **Domino-RSL**
- ネットワークシステムへの応用
 - **FPGA/ARMマイコン**を用いたセキュリティーシステム

微細化とともに増大するマスクコスト

- 90nm世代で1億円を突破している
⇒生涯生産個数10万個でも1000円/chip



出典: ライトスピード・セミコンダクター社

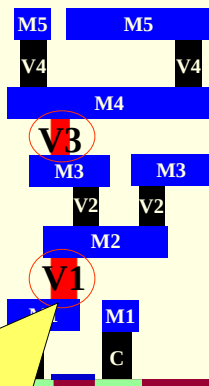
マスクを使用せず論理変更できるLSI

- ビアプログラマブルロジック回路 **VPEX**
 - ビア2層のマスクパターンを変更することで論理を変化させることのできるLSI
 - ビア2層はEB直描を使用することで「個別LSI」を製造可能
 - 固定秘密鍵暗号回路(電子印鑑)へ応用
- リコンフィギャラブルロジック回路 **ePLX**
 - 2入力のLUTをアレイ上に配置したFPGAと同様の機能(製造後に論理書き換え可能)を持つLSI
 - 暗号化回路, 文字列検索回路への応用

ビアプログラマブルデバイスとは?

VPEX

- Via1,3レイアのレイアウト変更により論理変更できるLSI製造手法
- Via1,3以外のマスクは共通
 - 製造コストを削減できる
 - 少量多品種のLSIを低コストに製造可能
- ASICより初期開発費を安価に
FPGAよりチップコストを安価に



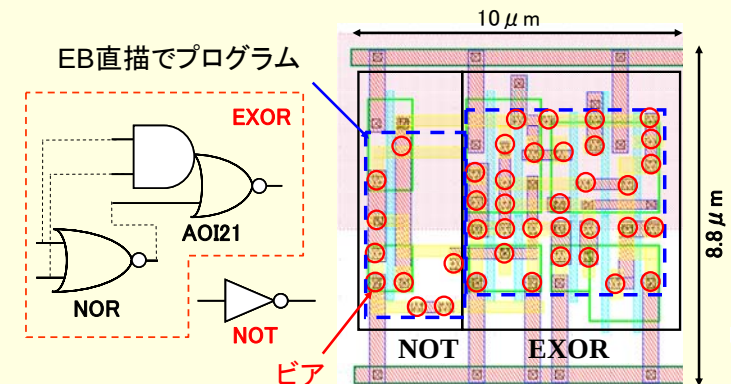
EB直接描画の最大の弱点: スループットが低い
⇒ビア2層のパターン切り替えで論理を変更
(穴系パターンはEB直描の得意パターン)

造

VPEX (Via Programmable logic device using EXclusive-or array)

VPEX

- 複合ゲート型XORゲートをベースに素子を構成
 - 論理を出力するために、入力、出力端子を分割
 - Via1の変更だけで、12種の論理が出力可能



(a) 基本素子回路

(b) 基本素子レイアウト

LEによるAND回路の構成例

VPEX

- 赤丸の部分にVia1を打つことでAND回路が構成できる

INVを無効化

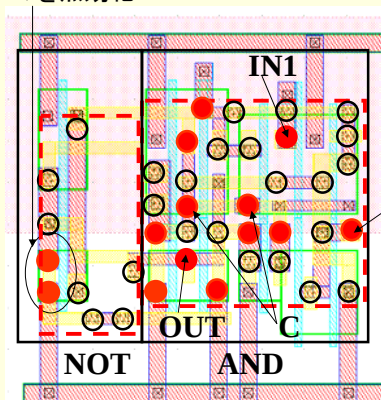


図6.1 VPEXでのAND論理の構成

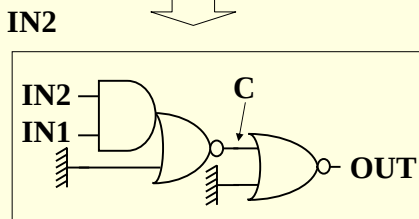
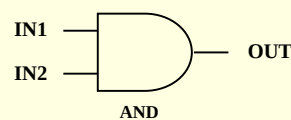
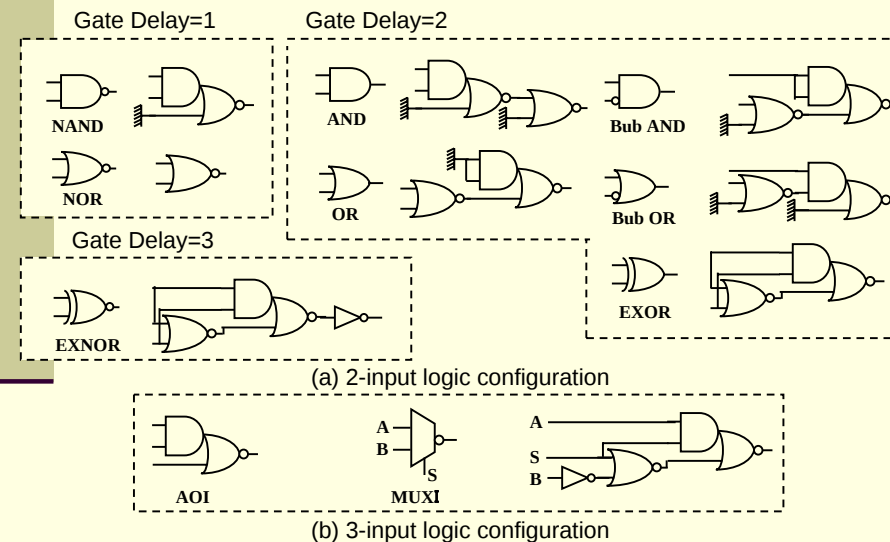


図6.2 AND論理の構成

21

基本素子から出力できる論理(全12種類)

VPEX



22

マスクを使用せず論理変更できるLSI

Rits
立命館大学

■ ビアプログラマブルロジック回路 VPEX

- ビア2層のマスクパターンを変更することで論理を変化させることのできるLSI
- ビア2層はEB直描を使用することで「個別LSI」を製造可能
- 固定秘密鍵暗号回路(電子印鑑)へ応用

■ リンコンフィギャラブルロジック回路 ePLX

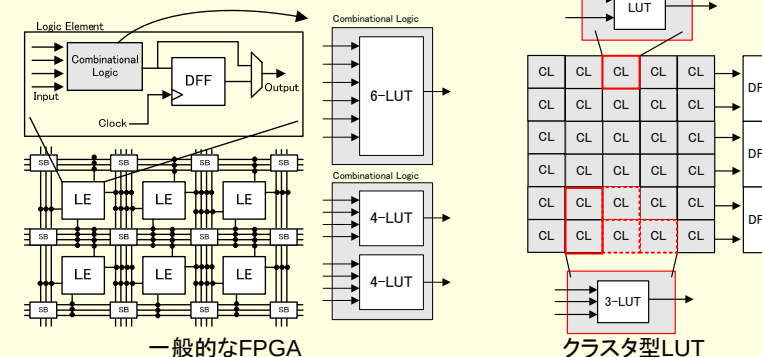
- 2入力のLUTをアレイ上に配置したFPGAと同様の機能(製造後に論理書き換え可能)を持つLSI
- 暗号化回路, 文字列検索回路への応用

23

クラスタ型FPGAアーキテクチャ

ePLX

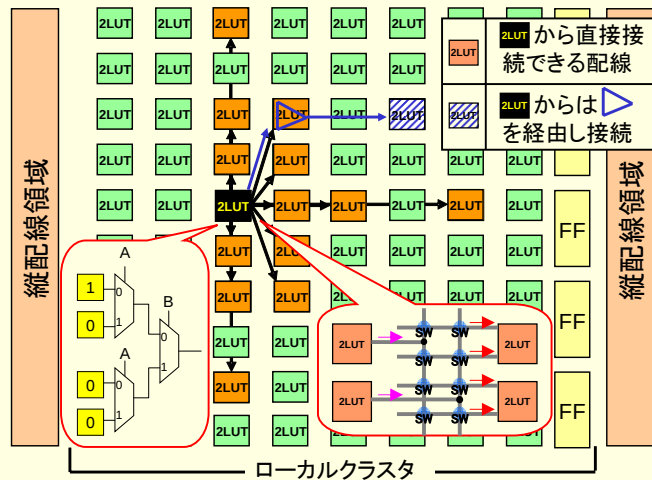
- ePLX (embedded Programmable Logic matrixX)
LUT(ルックアップテーブル)、FF、それらを接続するスイッチをマトリックス状に配置したリコンフィギャラブル回路
- クラスタ型LUTアーキテクチャ
 - 細粒度のロジックエレメントを並べたクラスタ型アーキテクチャ
 - 配置・配線の単純化→省面積化



24

ePLXアーキテクチャ

- LUTをマトリクス状に配置しクラスター化
- 1つのLUT出力から13箇所のLUTに接続可能

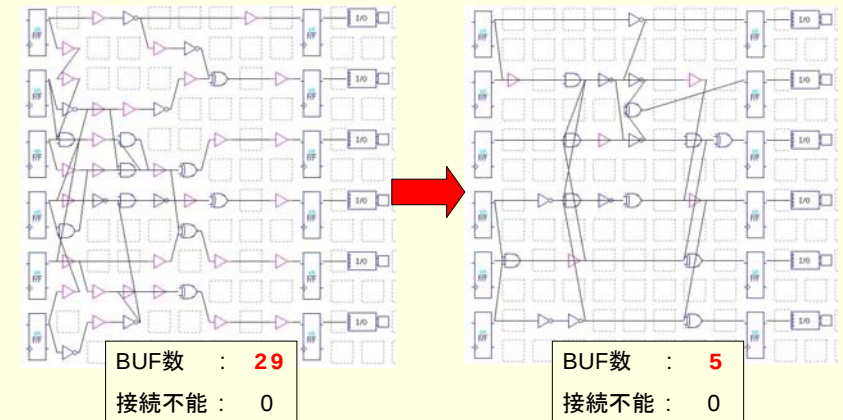


ePLX

25

ePLX用自動マッピングツール

- 前スライドのような特徴的なアーキテクチャのため、効率的なマッピングツール開発が必須



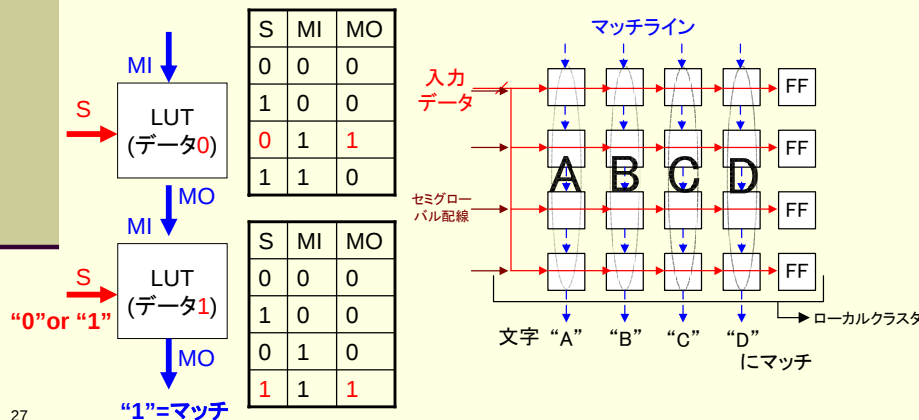
従来プログラムによる処理

新規プログラムによる処理

26

ePLXを使用したパターンマッチング回路

- 複数パターンマッチング手法
 - 一つのローカルクラスタに複数のパターンを配置
 - 同時に複数パターンのマッチングを行なう

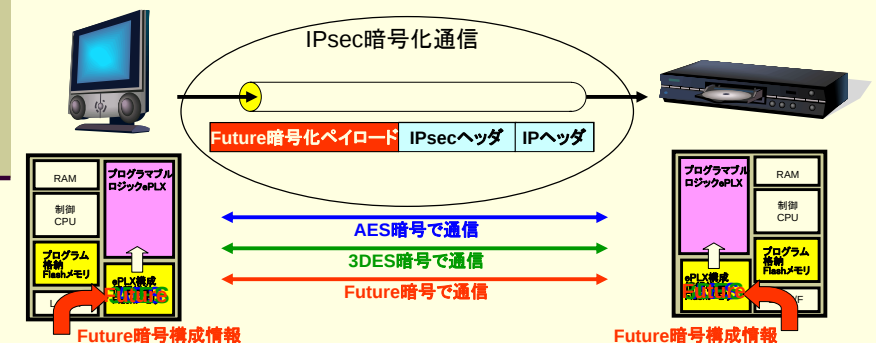


ePLX

27

ePLXの将来: 進化型ハードウェア

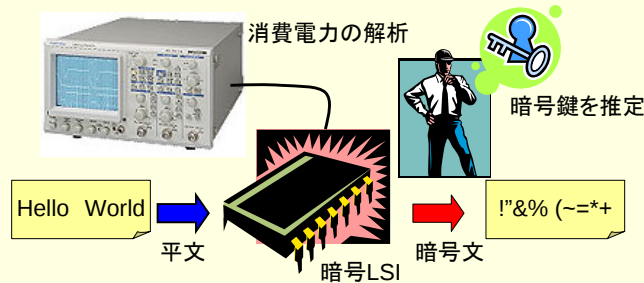
- 進化型ハードウェア
 - ネットワークを通じてハードウェアをアップデート
 - ハードウェアの修正, 新しい企画への対応が可能



28

サイドチャネルアタック

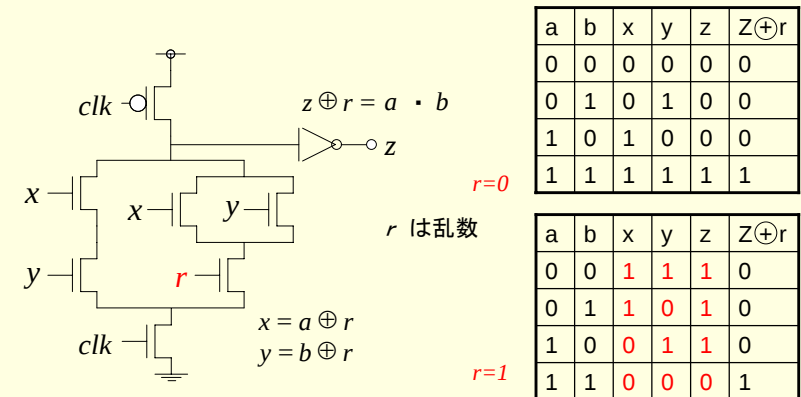
- 一般に実績のある暗号回路(3DES, AES等)では, 暗号文の解析では暗号鍵はわからない
- 暗号回路動作時の消費電力・電磁波により暗号鍵を推定→サイドチャネルアタック
- 特に1999年に消費電力を使用するDPA (Differential Power Analysis)が強力



29

耐サイドチャネルアタック回路

- DPA対策⇒どのような演算を行っても消費電力が一定になる回路
- 乱数を用いて, 正/負論理をランダムに反転
⇒Domino-RSL回路(ハザードフリー)



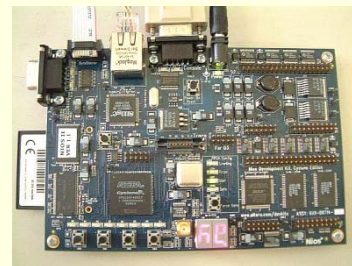
30

ネットワーク実験と研究

- 侵入検知システムSnortの性能評価
- IPv6のトンネリング実験
- FPGA/ARMマイコンを使ったネットワーク通信



実験室内模擬ネットワーク実験

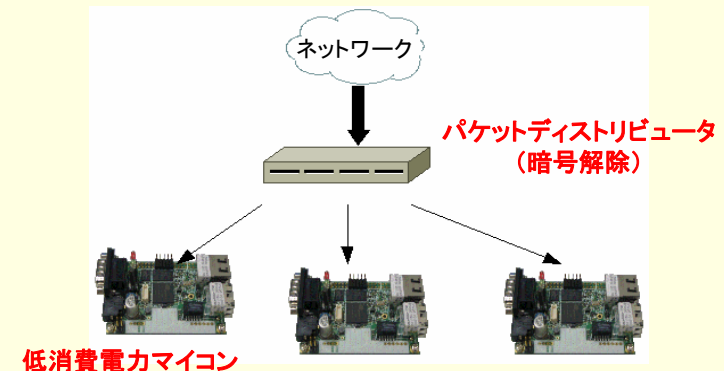


EthernetポートつきFPGA

31

セキュリティシステムの例

- ネットワークのウイルス検知をLinux搭載低消費電力マイコンで分散処理
- 分散処理用のパケットディストリビュータはFPGAボードで開発(暗号処理, ヘッダー検知は実施)



32

卒論までのながれ

応用演習	2007/12-2008/1	・ネットワーク,Cygwin環境セットアップ ・Cプログラミング, SPICE復習 ・研究紹介
春季演習 (週1回)	2008/2-3	C言語の演習(簡単な暗号プログラム) 論理回路演習(SPICEシミュレーション)
院生ゼミ演習 (週2回)	2008/4-6	・LSI設計ツール(回路図, レイアウト, SPICE & 論理シミュレーション, 論理合成)修得 ・FPGAおよびマイコンボード演習 ・ネットワークプログラミング実習 ・Ciscoルータによるネットワーク構築
卒業論文 テーマ選定	2008/7-9	院生ゼミの結果から希望調査 やる気のある学生は夏休みも研究 9月に正式決定(B4学生発表)
卒論目次作成	2008/12	卒論作成前に内容を整理
卒論提出	2008/2	卒論提出

33

休み(ゼミの無い間)は, 3月下旬(春休み)に2~3週間, 8月に3~4週間あります。

大学院について

- 研究の主体は大学院生
- 学会発表
 - M1の秋の「システムLSIワークショップ」+「デザインガイア」が目標です(今年M2 1名, M1 5名発表)
<http://icd.ac.isp.ne.jp/ja/workshop/>
 - M2には海外発表が目標(M2 1名:サンノゼ)
- 対外交流
 - ePLX
 - VPExネットワーク, Domino-RSL
 - 今年のM2の就職先
日立, ルネサステクノロジ, 富士通, 三菱自動車
ケイ・オプティコム

34

研究室訪問

- 今週(アポイントメントなし, 個人研究室)
 - 10/22(月) 17:30~19:00(このあとすぐ)
 - 10/23(火) 15:50~17:20
 - 10/26(金) 10:30~12:00
 - 上記以外の個別相談はメールで予約してください
- 配属直前
 - 研究室院生の発表も予定しています
(詳細日程はHPで確認してください)
 - 11/12(月) 17:30~19:00 研究室デモ展示
 - 11/13(火) 午後 院生による研究発表予定
 - 11/15(木) 午後 教員面談, 院生懇談予定

35

終わりに

- HDL~レイアウトまで, LSI設計の実践力を修得しよう
 - 自分のチップを作って評価?
- 新しいLSIの設計技術を研究して, 安全で快適なネットワークシステムへ応用しよう
- 日進月歩のネットワーク(セキュリティ)技術に興味をもとう
- 歓迎する学生像
 - いろいろなことに好奇心があり興味を深める
 - 自分で考えて行動できる
 - 責任感を持ってコミュニケーションできる
- 研究室学生のWiki(イントラネット)を見ると当研究室のアクティビティーの一端が感じられるでしょう!
⇒<http://rh5pt200.bkc.ritsumeai.ac.jp/wiki/>

36