電子情報デザイン学科　藤野　毅

応用演習研究室紹介　2006.10.2

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

機能メモリ混載システムLSI研究室

- 2003年4月　開設
  - URL: http://www.ritsumei.ac.jp/se/re/fujinolab
- 構成員
  - 教授：藤野　毅
    - 1962.3.17　大阪府生まれ
    - 2003年まで半導体メーカ勤務，専門は集積回路工学全般（プロセス：リソグラフィー，設計：メモリ）
  - 大学院生：M2　7名，M1　5名
  - 学部生：9名（内8名大学院進学予定）
- 場所：ローム記念館　3F（個研室1，学生2），1F（学生1）
- 研究内容
  - メモリ混載システムLSI
  - 低コストLSIデザイン技術
  - ネットワーク技術
- 研究設備
  - LSI設計設備（ソフト＆ハード）
  - FPGAボード，マイコン（ARM)ボード
  - ネットワーク実験設備（Cisco）

本日の内容

- 研究を説明する単語解説
  - 可変論理LSI
  - EB直描
  - 暗号回路
- 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
- ネットワークシステムへの応用
  - 電子印鑑LSI
  - 暗号/侵入検知一体型セキュリティーシステム

藤野研究室の研究テーマ

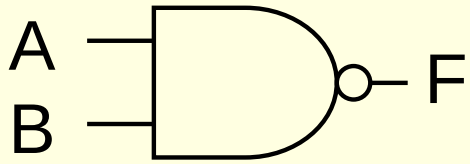
- 新機能メモリを搭載したLSI設計技術をコアテクノロジーとして
  ⇒メモリの技術を使用した可変論理LSI

- 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

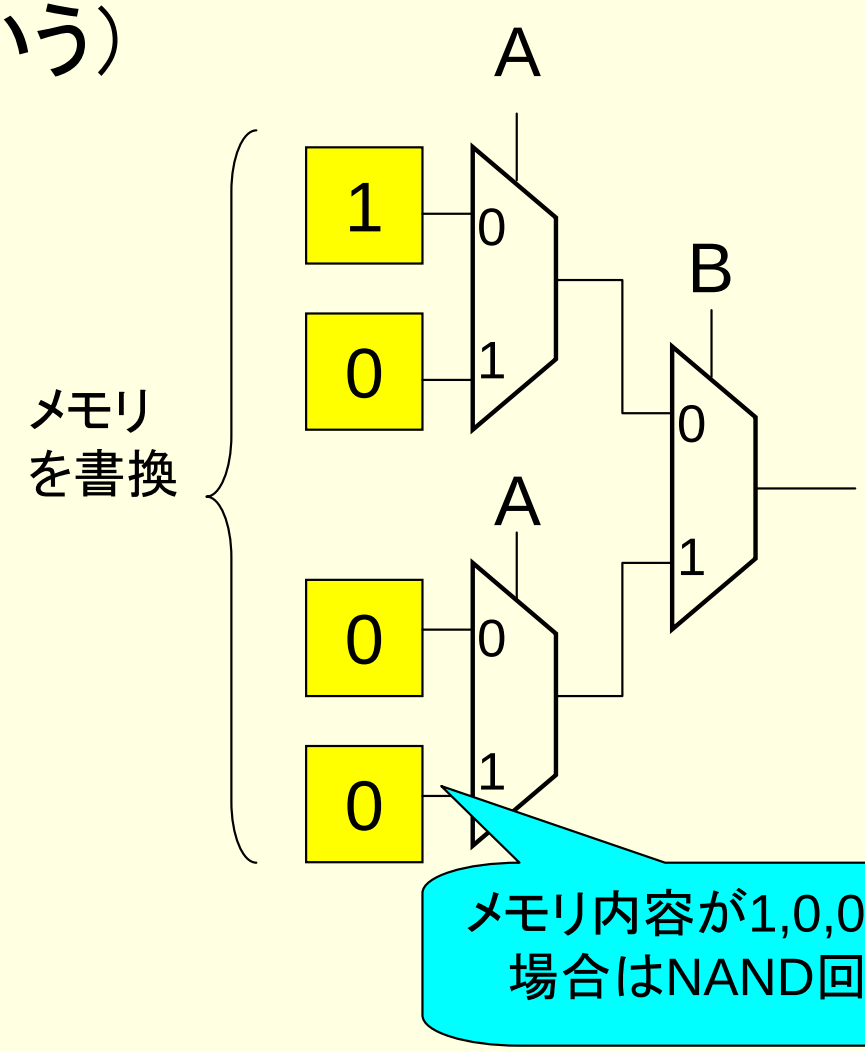
メモリを使った論理素子

- 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（Look Up Tableという）



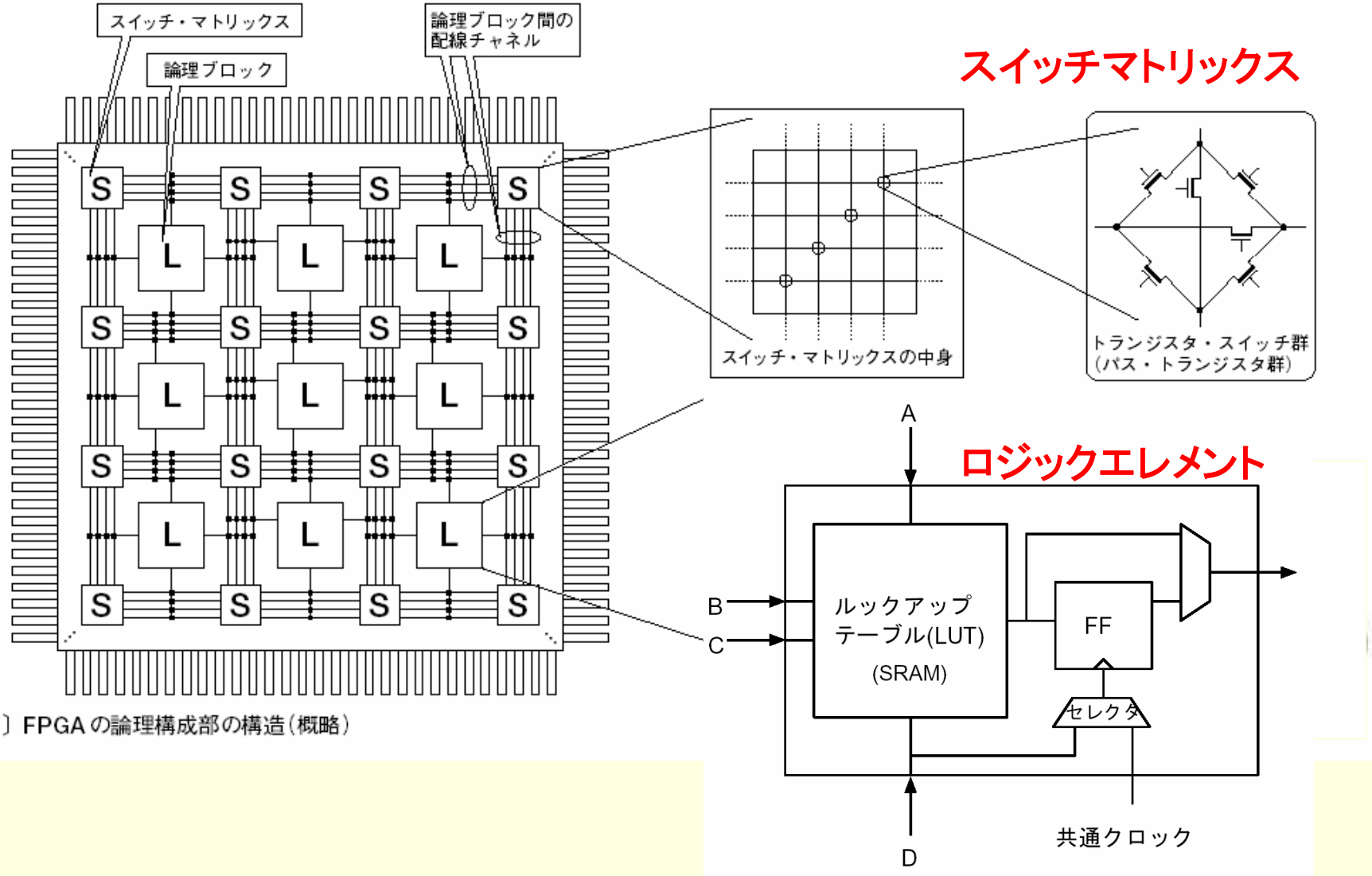
NAND

A	B	F=A・B
0	0	1
1	0	0
0	1	0
1	1	0



FPGAの構造

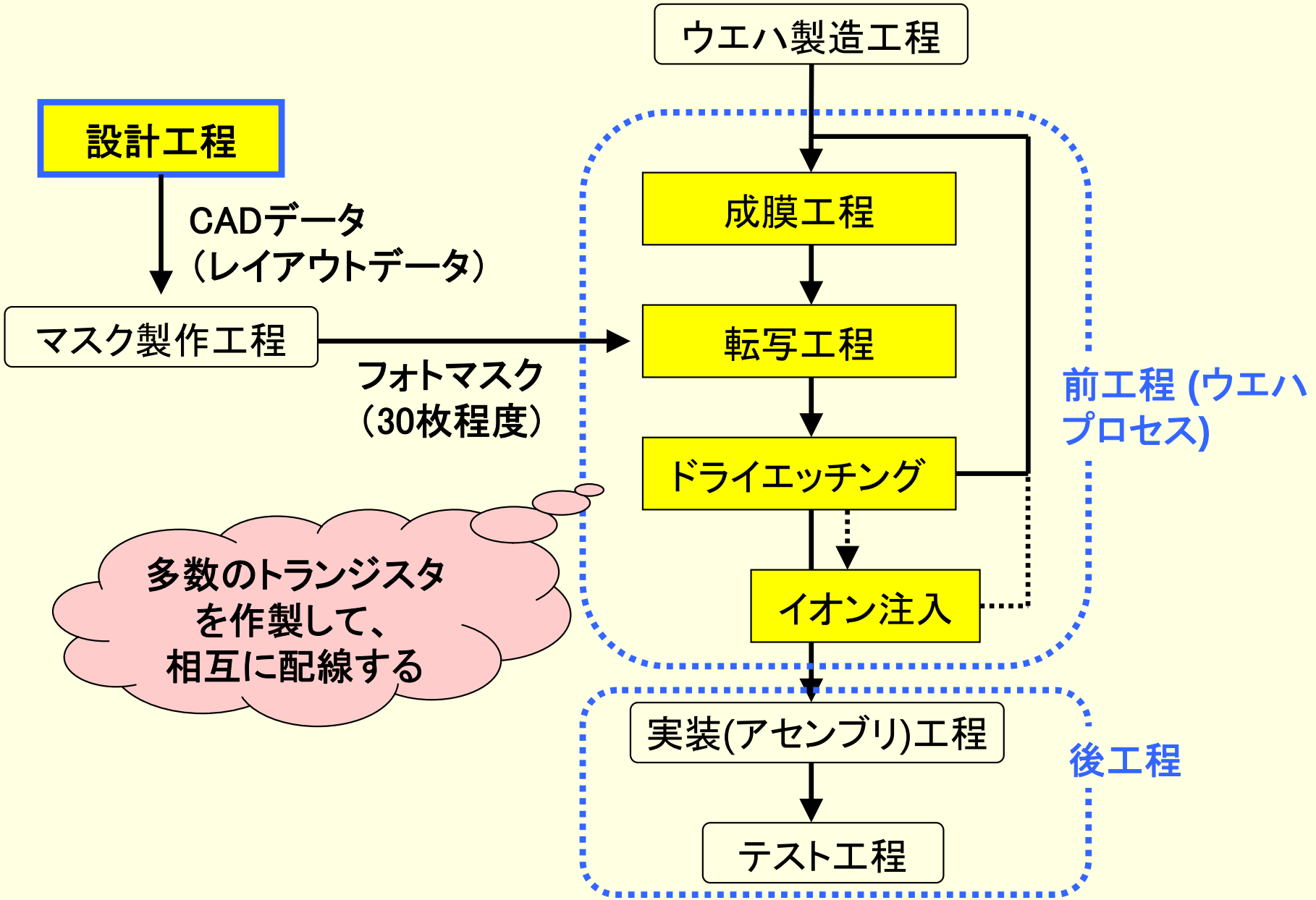
- 論理変更：ロジックエレメント（LUTとFFより構成）
- 配線変更：スイッチマトリックス



〔図3〕FPGA の論理構成部の構造（概略）

EB直描?

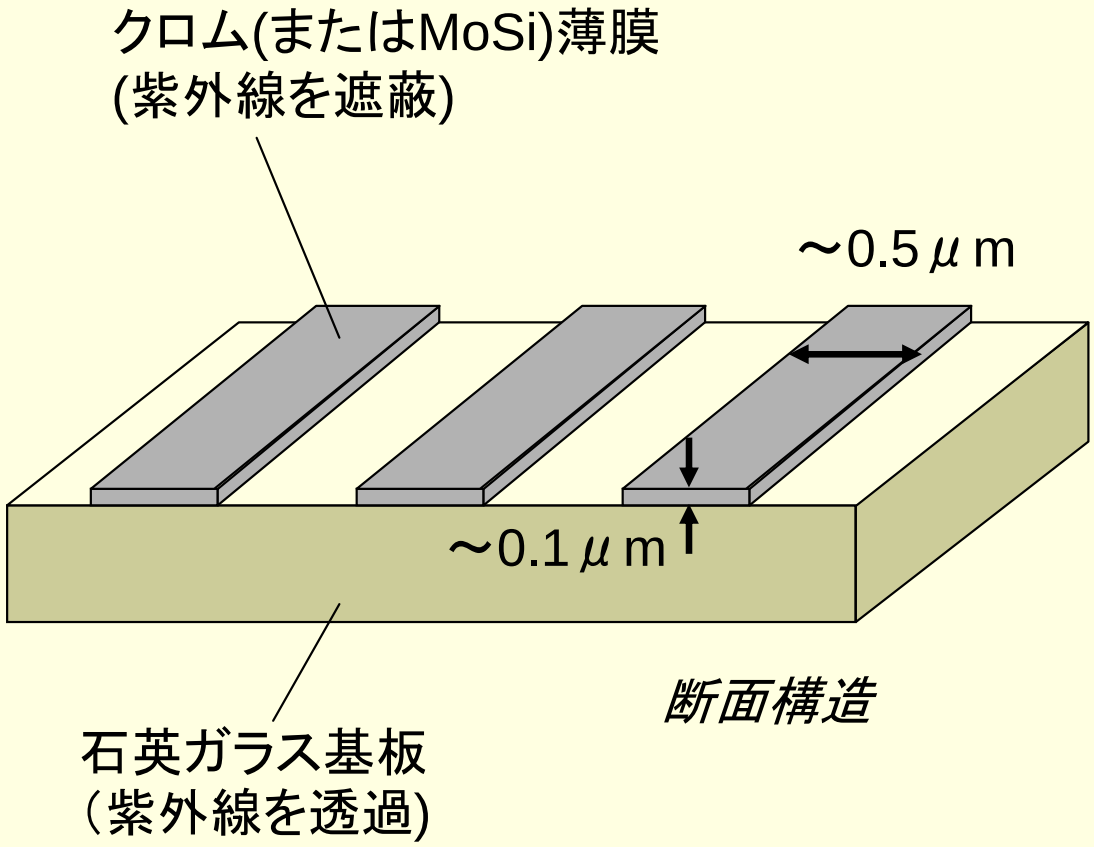
LSIの設計・製造工程



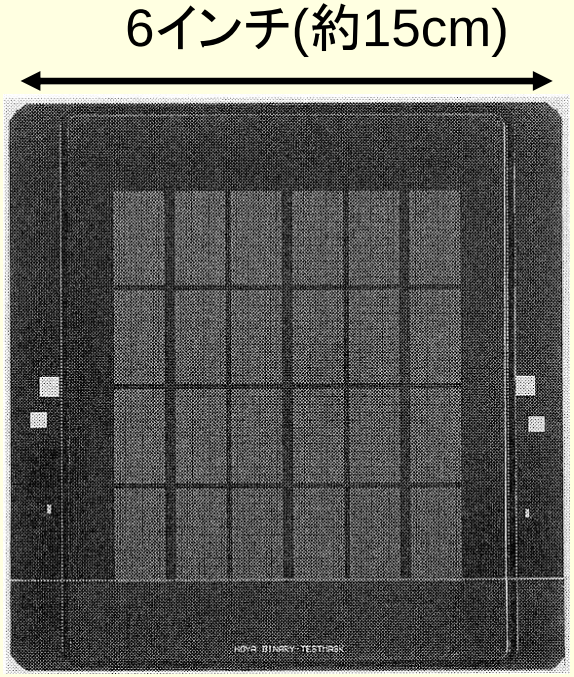
EB直描?

マスク製作工程(1)

- 工程ごとに分離したパターンを使って、下記のような構造のフォトマスクを形成する



断面構造

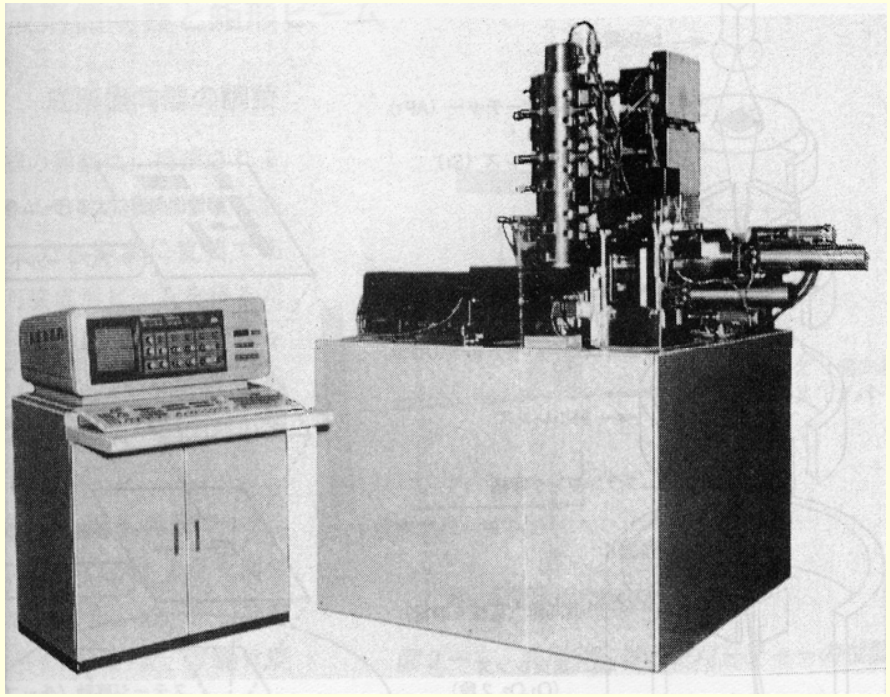


外観

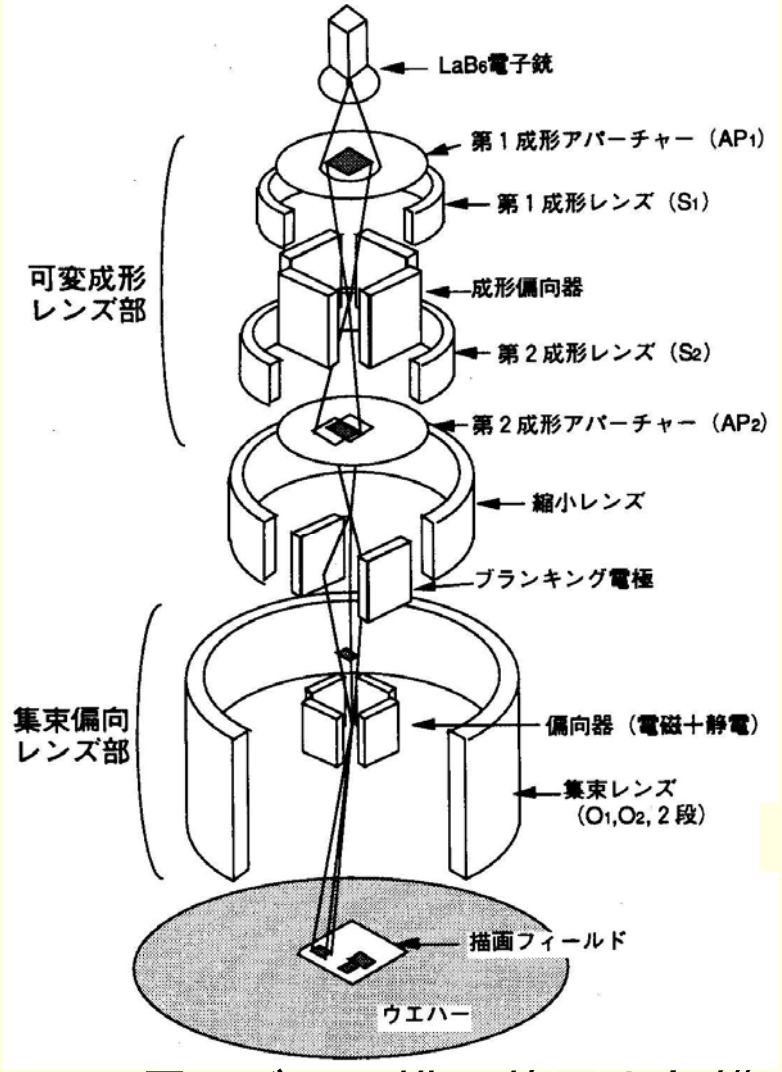
マスク製作工程(2)

EB直描?

- パターンを形成するためには下記のような電子ビーム描画装置を使用する。



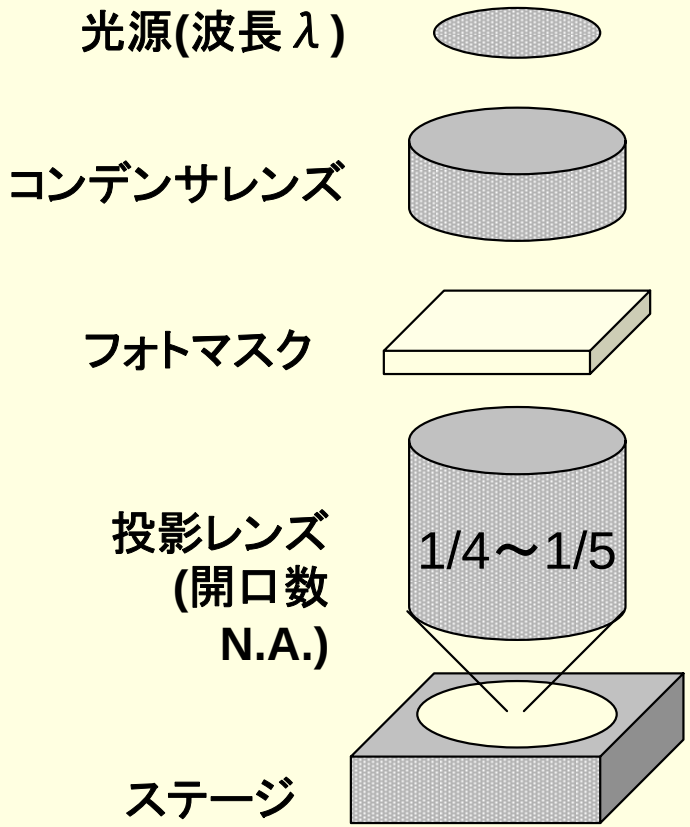
電子ビーム描画装置外観
（日立HL700）



電子ビーム描画装置内部構造

EB直描?

パターン転写装置



ステージを少しずつ動かして
1つのウエハで数十回露光

縮小投影露光装置の原理

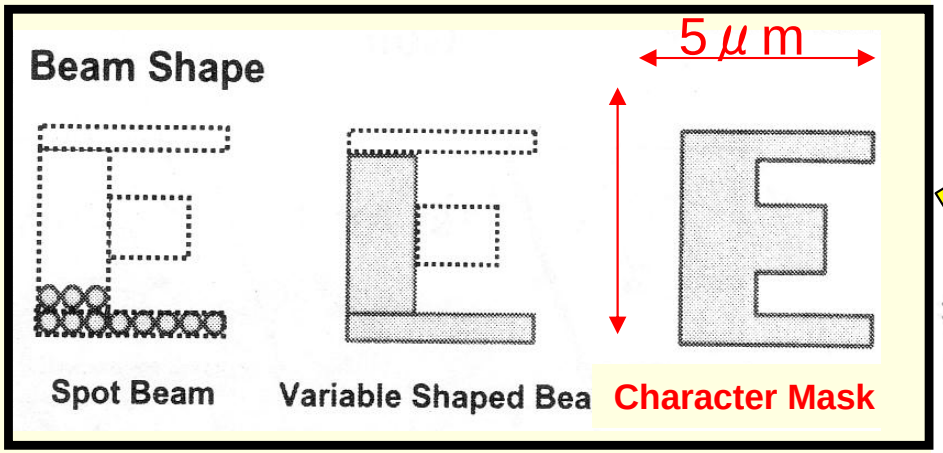
光転写装置(ステッパー)外観

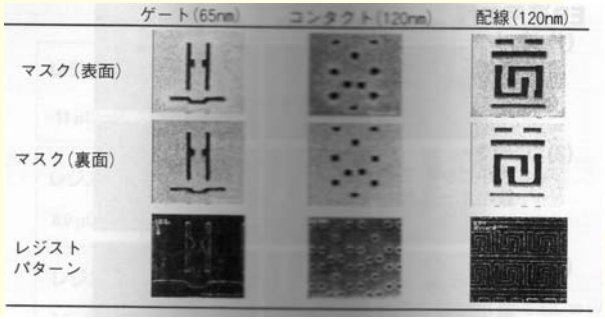
＊栃木ニコンホームページより引用

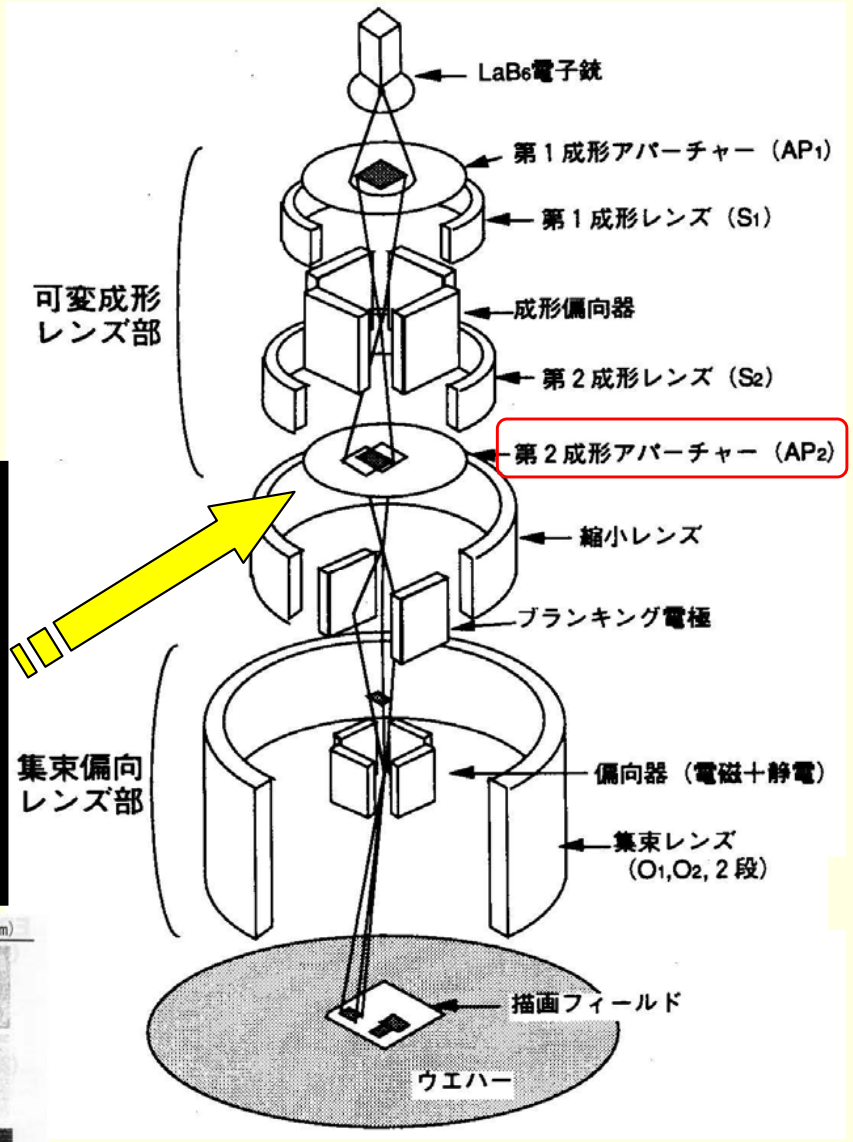
EB直描?

キャラクタプロジェクションEB直描原理

- ５μm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（キャラクタプロジェクション露光）
- 装備できることのできるキャラクター数が100-400個のEB直描装置が開発済/中







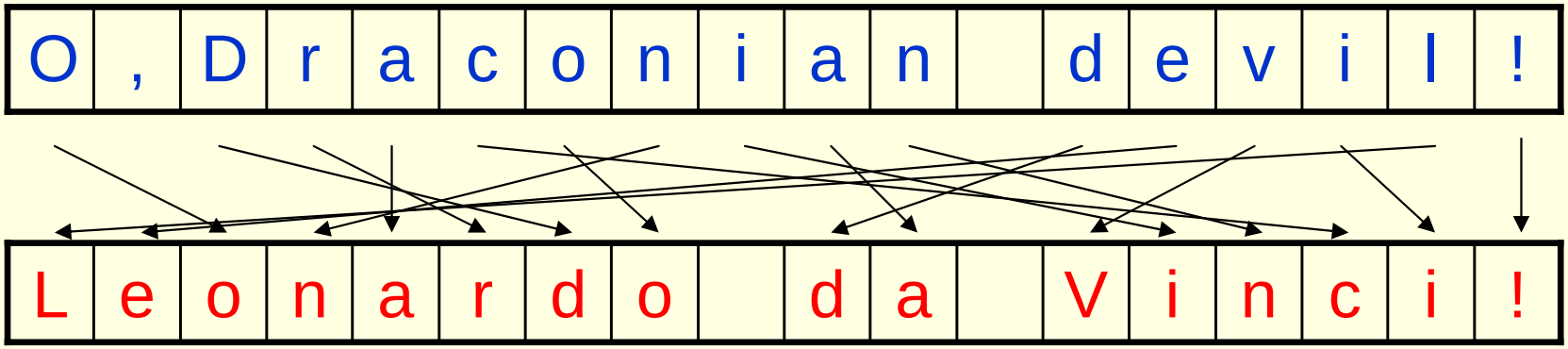
暗号回路?

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
- 携帯電話やPC紛失時の対策
  - 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
- パソコンの無線LAN接続
  - 無線アクセスポイントとPCの間の通信

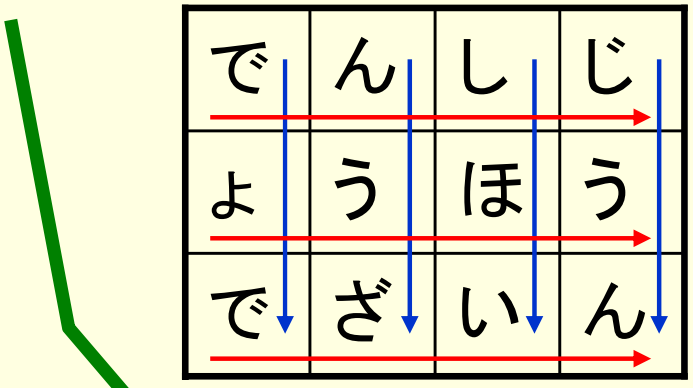
転置暗号

- 文章の文字の順番を入れ替える(アナグラム)



- ランダムに入れ替えると復号できないので単純には以下のように変換する

でんしじょうほうでざいん(平文)



暗号鍵は
4X3のマス目

でょでんうざしほいじうん(暗号文)

暗号回路?

換字暗号(1)

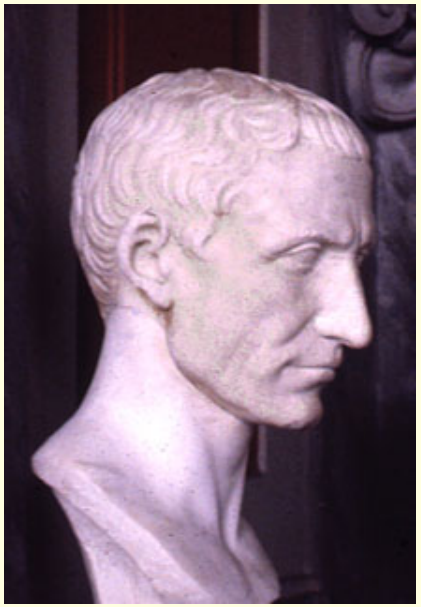
- シーザー暗号(アルファベットを所定の文字数ずらす)

HELLO(平文)

変換テーブル(鍵はシフト量3)

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R

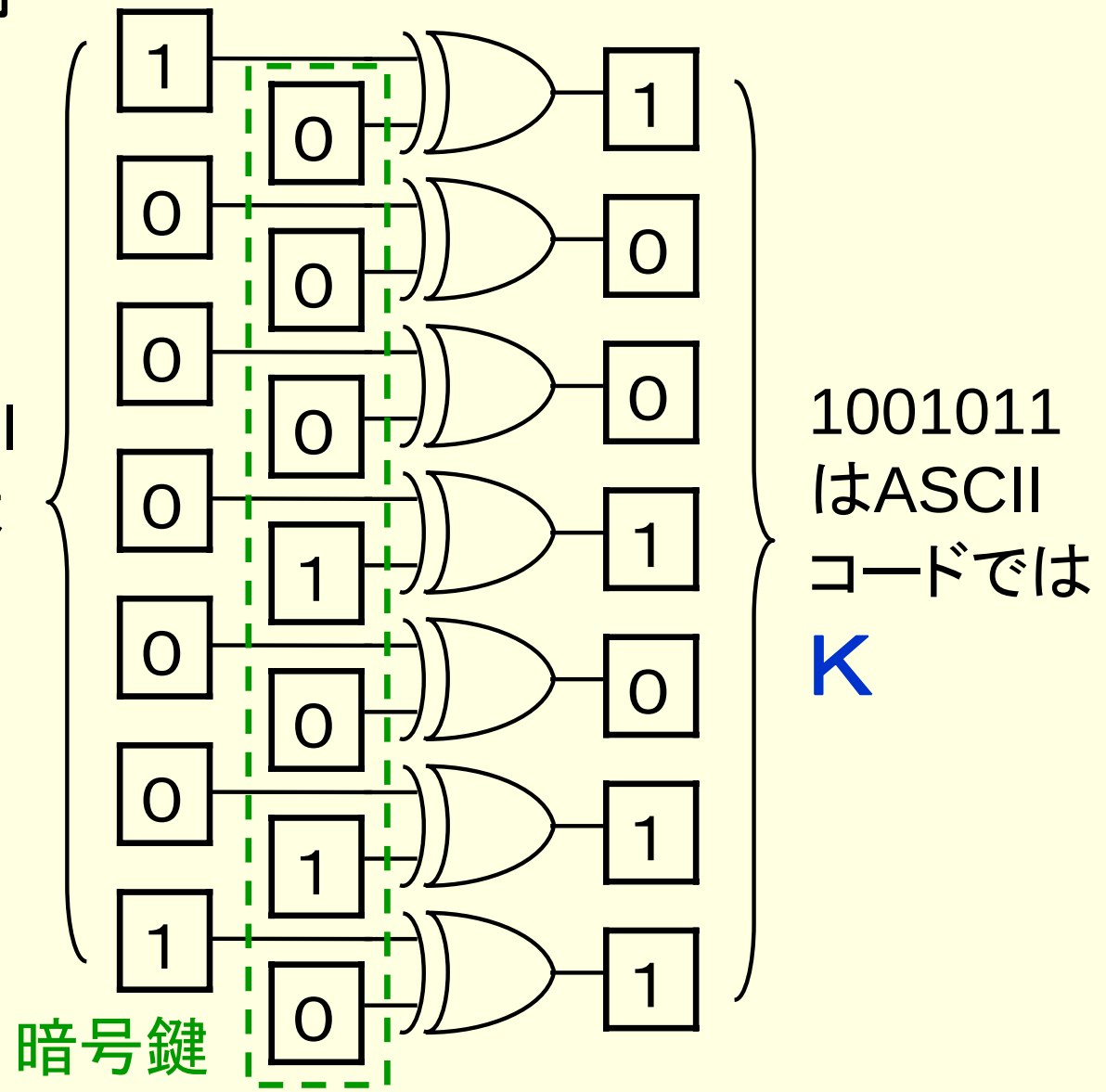
KHOOR(暗号文)



暗号回路?

換字暗号(2)

- EXOR回路を使用すると換字処理が簡単に実現できる



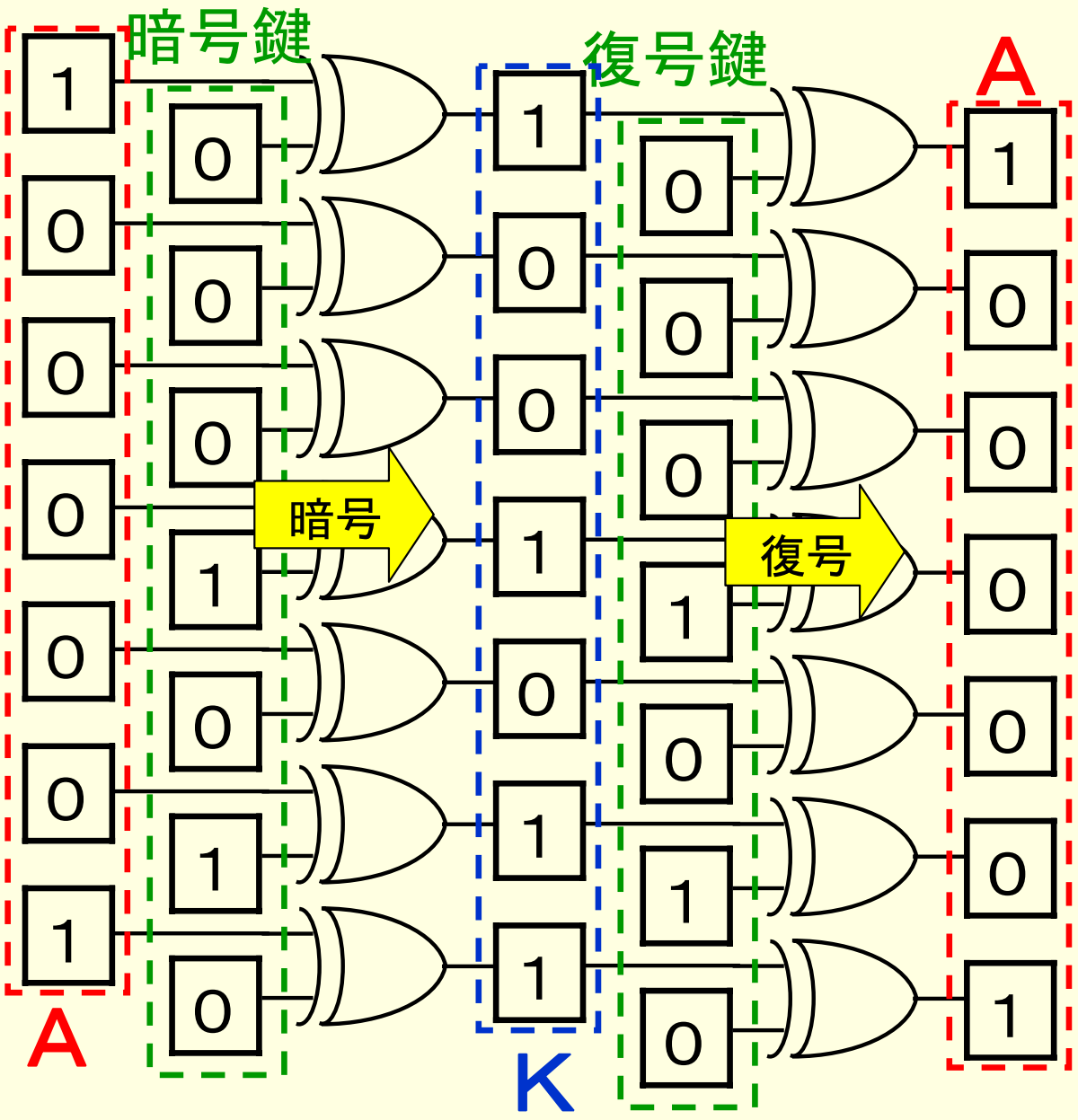
AはASCIIコードでは1000001

1001011はASCIIコードでは K

暗号回路?

換字暗号(3)

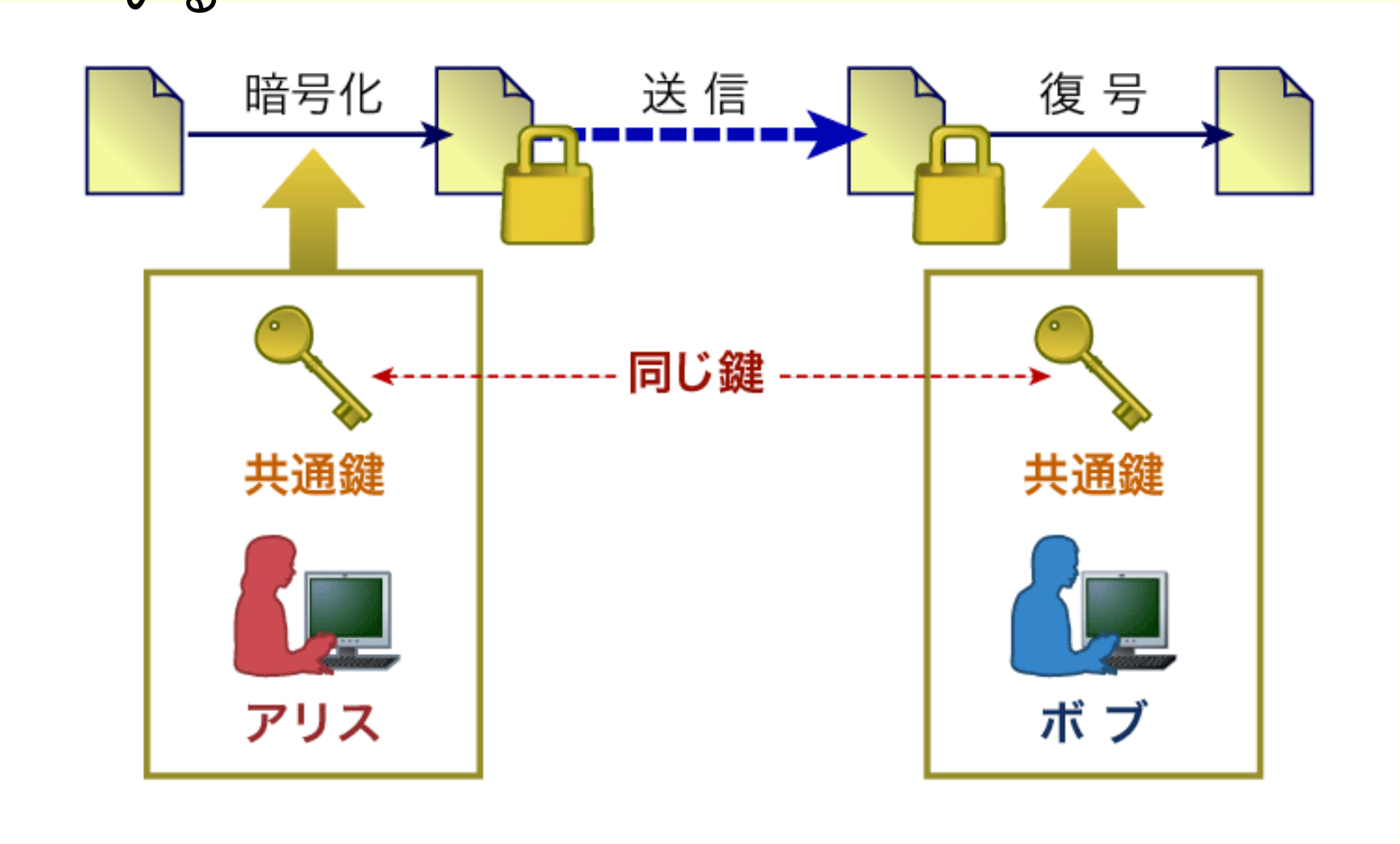
- 同じ暗号鍵でEXOR回路を利用すると復号できる



暗号回路?

共通鍵暗号

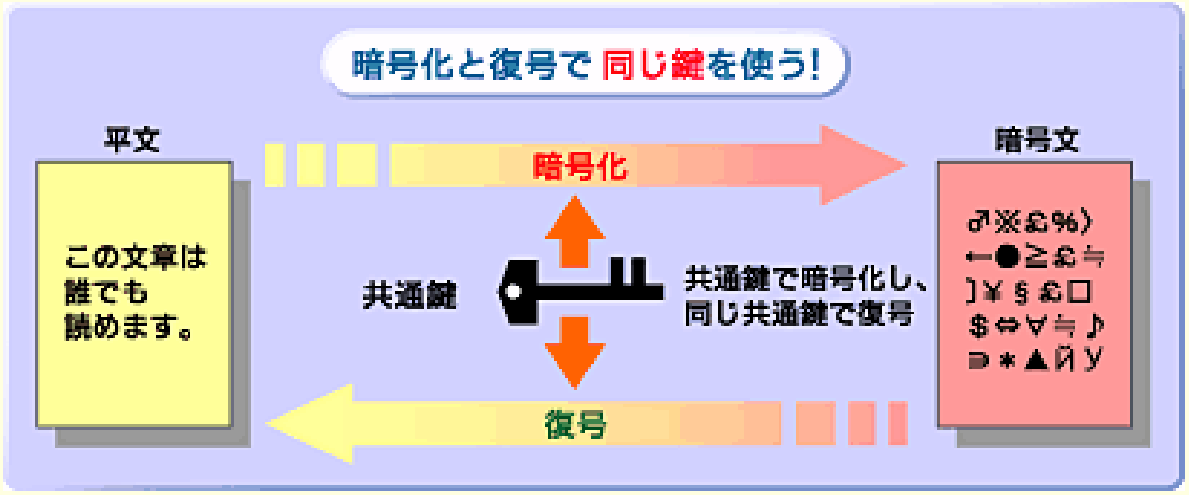
- DES，AESなどの実用暗号があり
  - 転置処理やEXOR回路を用いた換字処理が使用されている



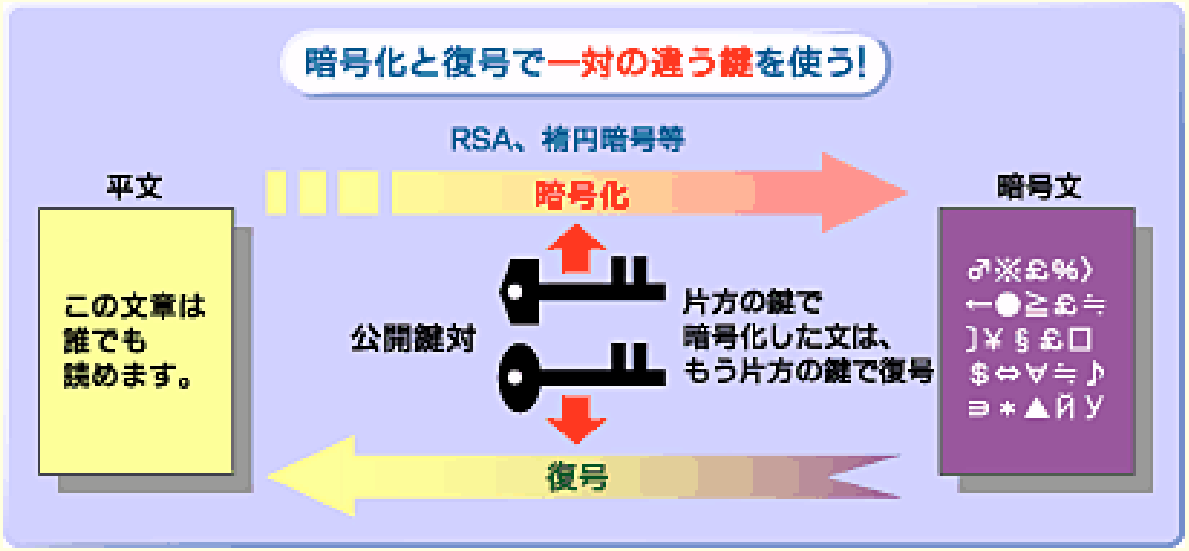
暗号回路?

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）

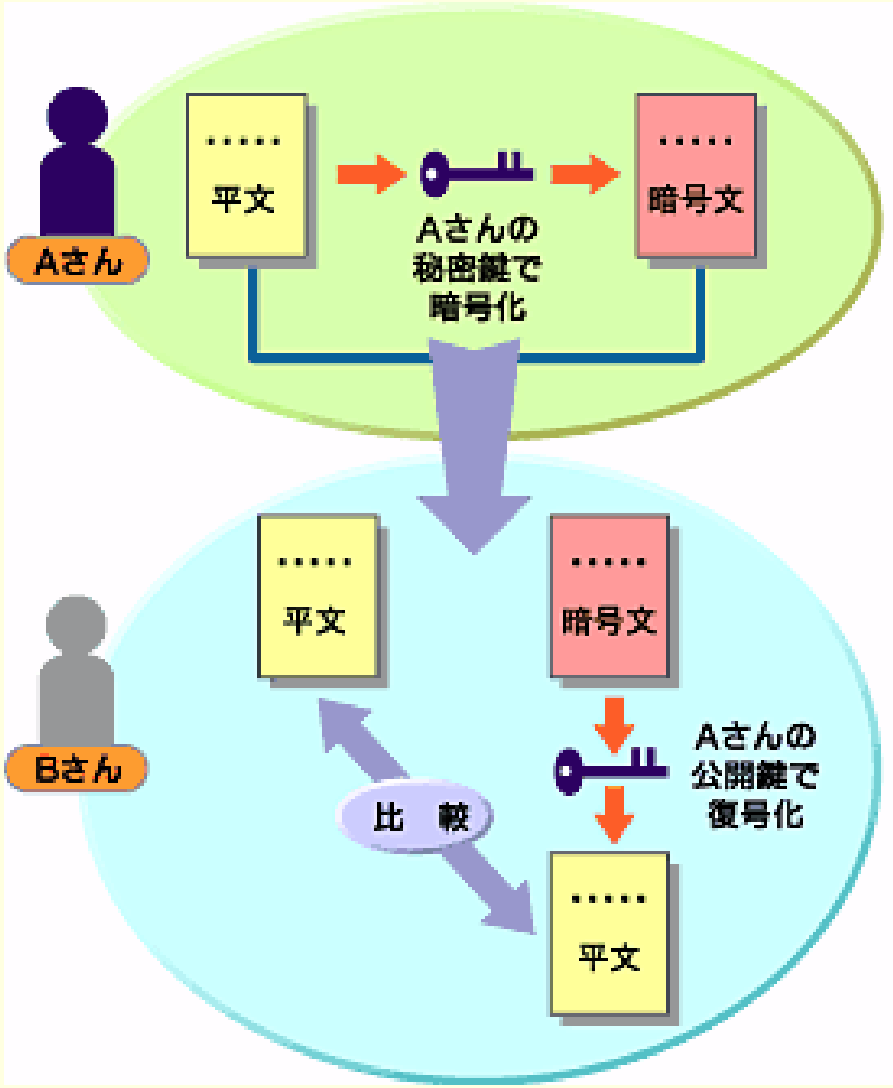


http://www.atmarkit.co.jp/fnetwork/rensai/pki01/pki01.htmlより引用

公開鍵暗号による個人認証(電子署名)

暗号回路?

- 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

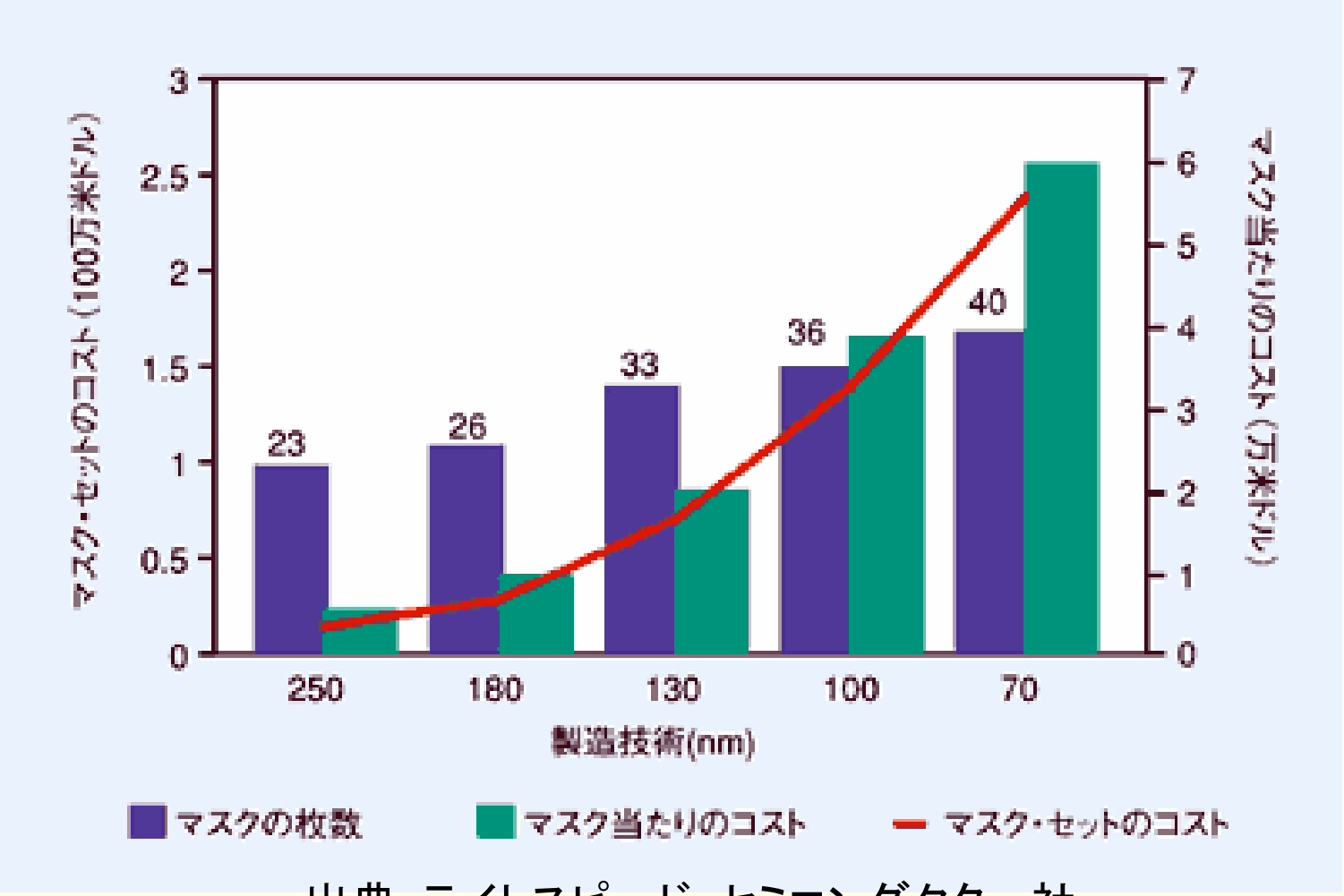
http://www.atmarkit.co.jp/fnetwork/rensai/pki01/pki01.htmlより引用

本日の内容

- 研究を説明する単語解説
  - 可変論理LSI
  - EB直描
  - 暗号回路
- 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
- ネットワークシステムへの応用
  - 電子印鑑LSI
  - 暗号/侵入検知一体型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

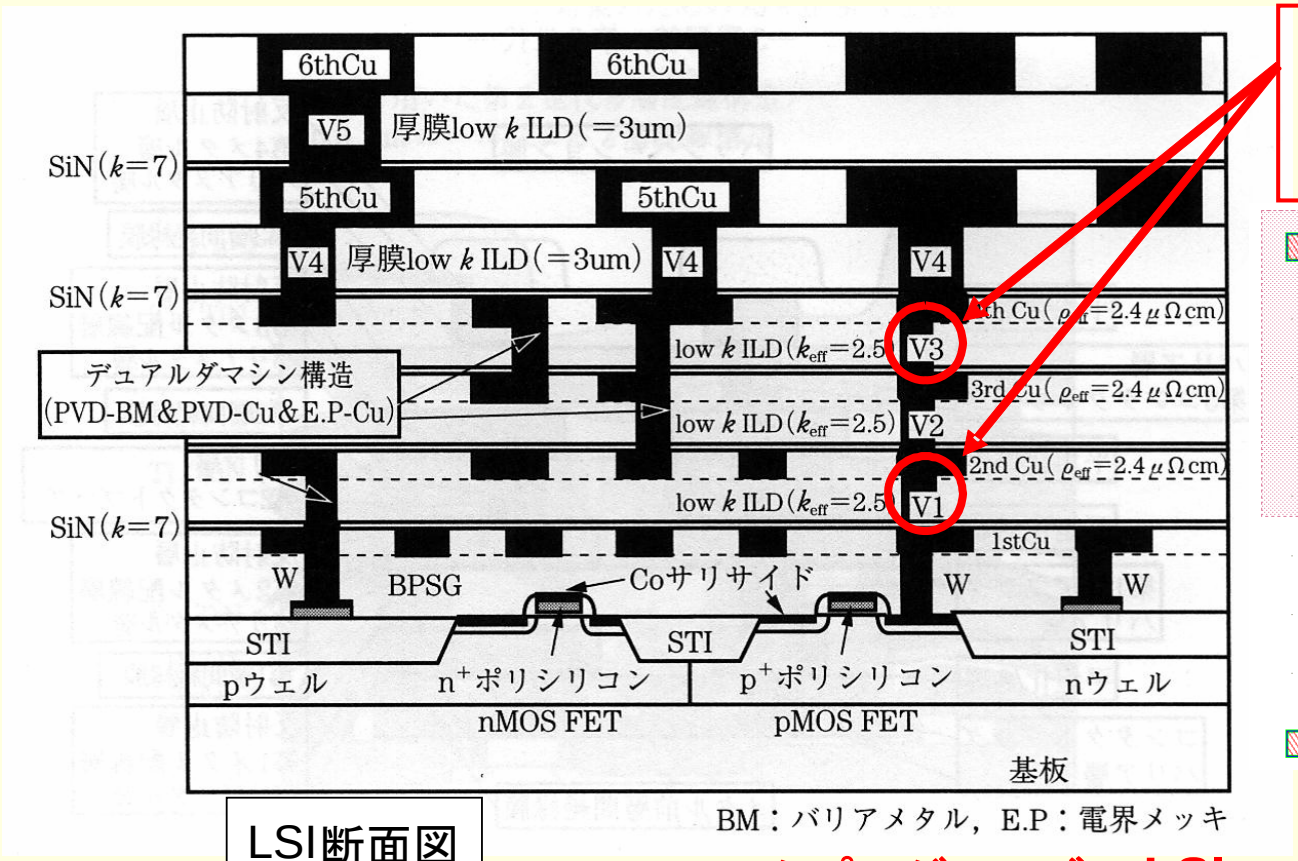
- ビアプログラマブルロジック回路　VPEX
  - ビア2層のマスクパターンを変更することで論理を変化させることのできるLSI
  - ビア2層はEB直描を使用することで「個別LSI」を製造可能
  - 固定秘密鍵暗号回路（電子印鑑）へ応用

- 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

特徴LSI1?

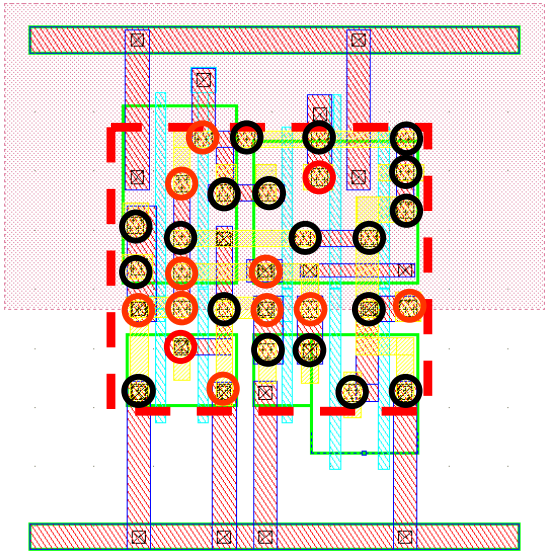
ビアプログラマブルロジックLSI：VPEX

- EXORゲートをベースとして，V1,V3の2つのレイアのマスクを切り替えることで論理および配線が変更可能なプログラマブルロジックLSI
- V1,V3のレイアウトはキャラクタEB直接描画に最適化



LSI断面図

V1,V3の2レイアのビアマスクパターンを変更することで回路論理を変更



LSI平面図

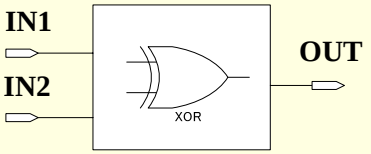
マスクプログラマブルLSI

（EB直描によって作成するビアパターンで論理を変更）

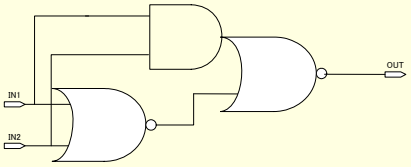
特徴LSI1?

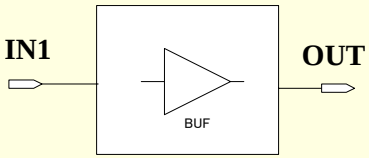
VPEXから出力できる論理：全10種類

- 下記の論理のみをライブラリとして使用して論理合成を実施する

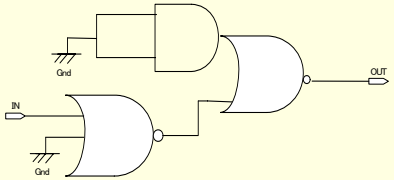


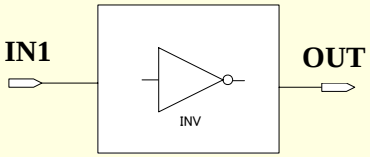
XOR



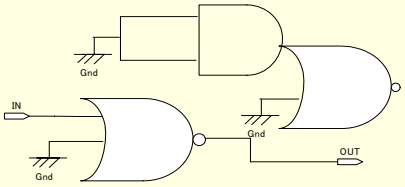


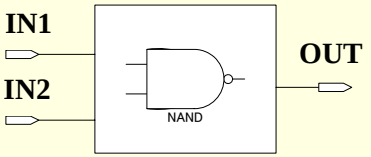
BUF



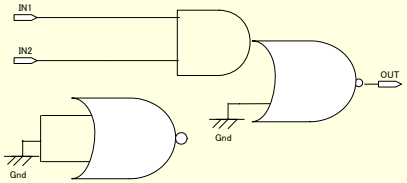


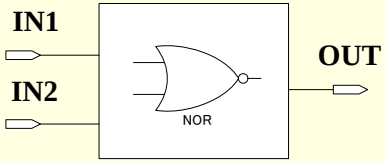
INV



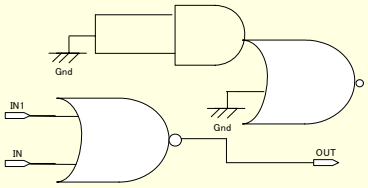


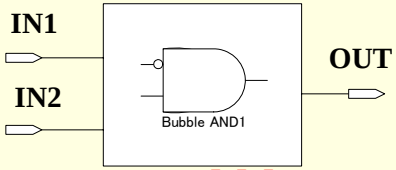
NAND



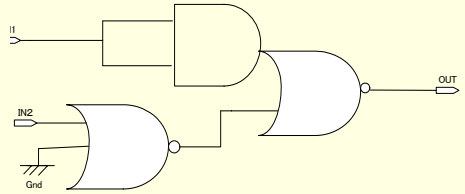


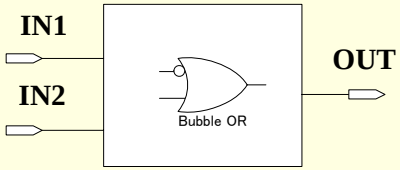
NOR



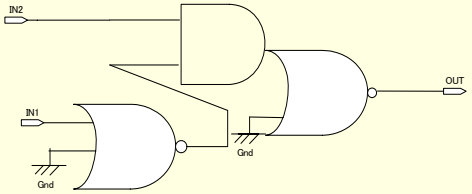


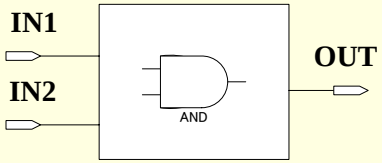
Bubble AND



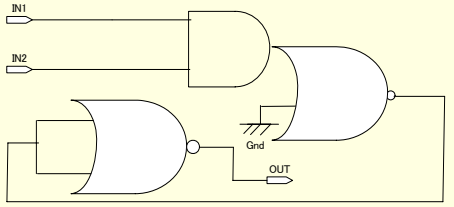


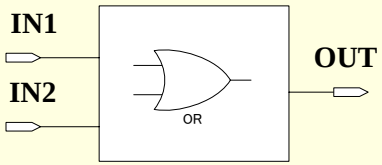
Bubble OR



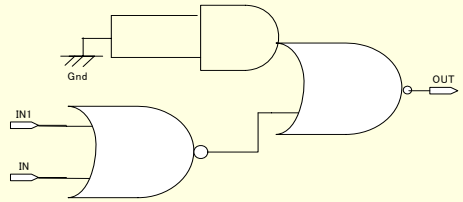


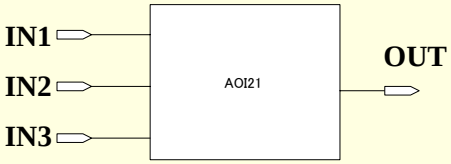
AND



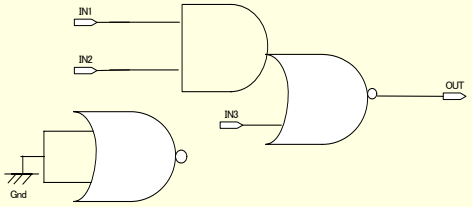


OR





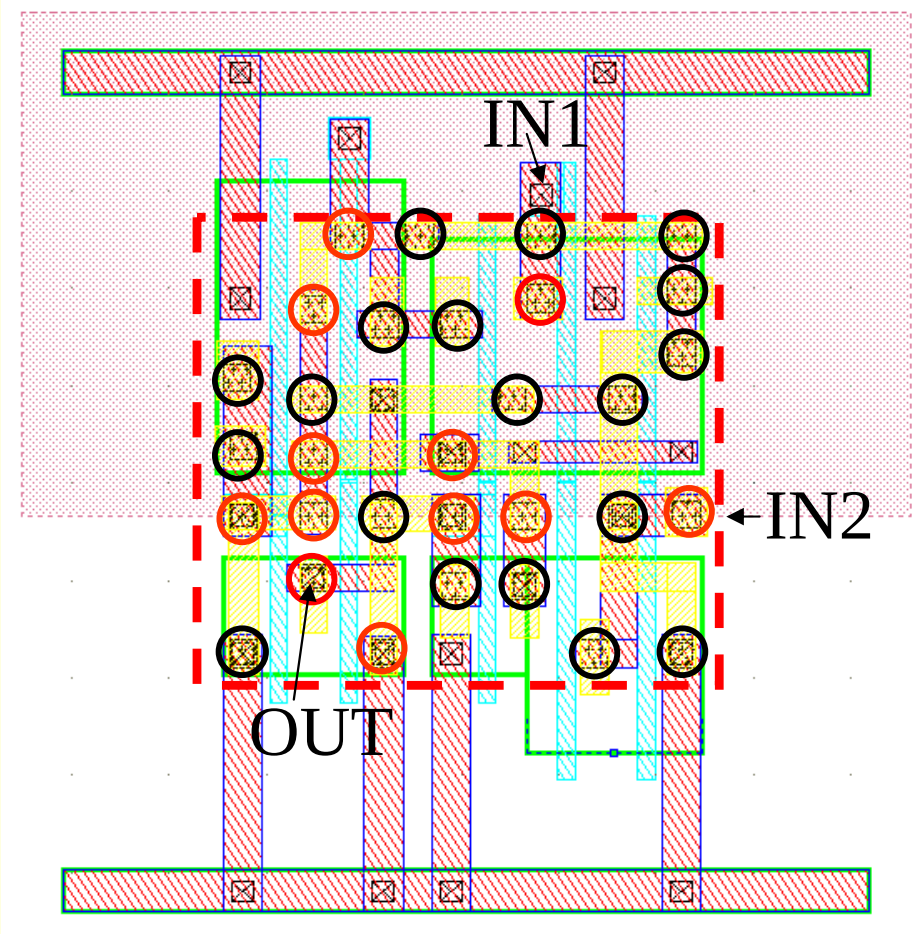
AOI



VPEXによるAND回路の構成例

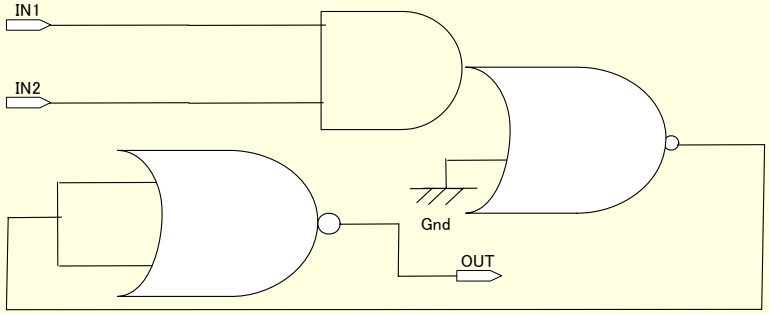
特徴LSI1?

- 赤丸の部分にVia1を打つことでAND回路が構成できる



レイアウト図

- 水色： ゲート
- 赤色： M1
- 黄色： M2
- ×印： コンタクト
- 緑色： 拡散
- 薄赤： n-Well
- 赤丸印： Via1



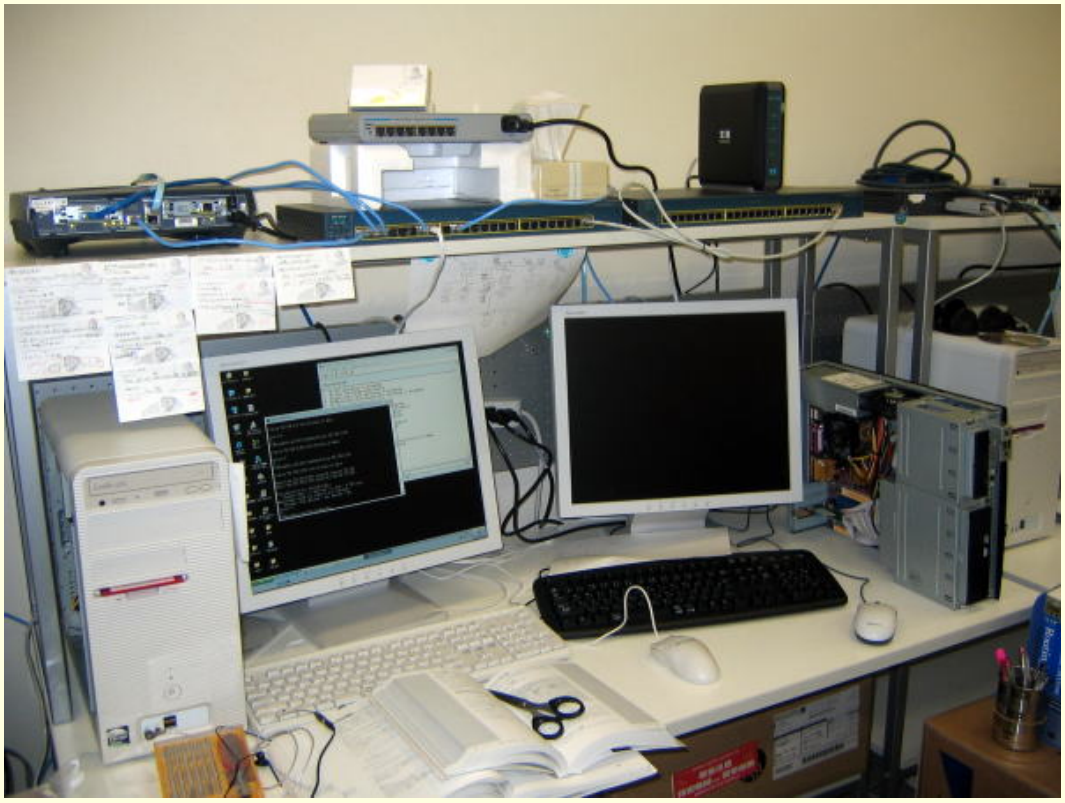
AND論理の構成

本日の内容

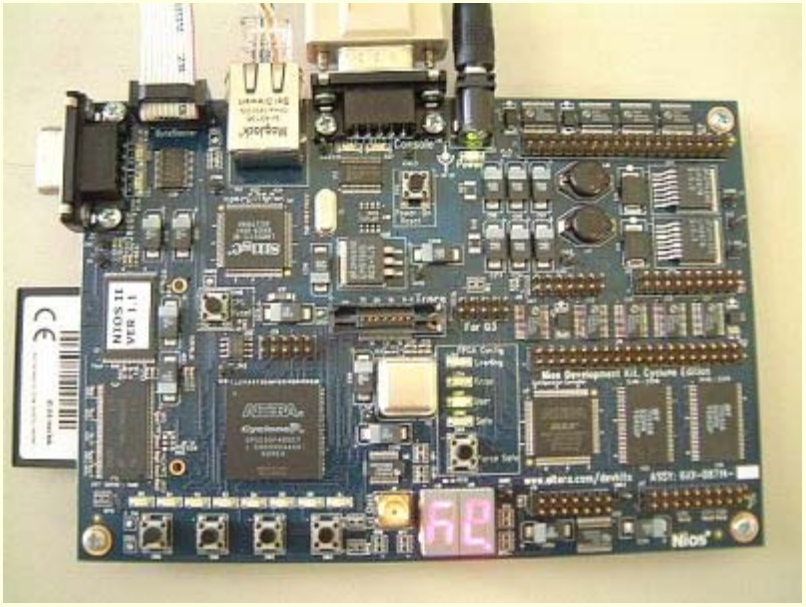
- 研究を説明する単語解説
  - 可変論理LSI
  - EB直描
  - 暗号回路
- 特徴あるLSI設計技術
  - ビアプログラマブルロジック回路　VPEX
  - リコンフィギャラブルロジック回路　ePLX
- ネットワークシステムへの応用
  - 電子印鑑LSI
  - 暗号/侵入検知一体型セキュリティーシステム

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



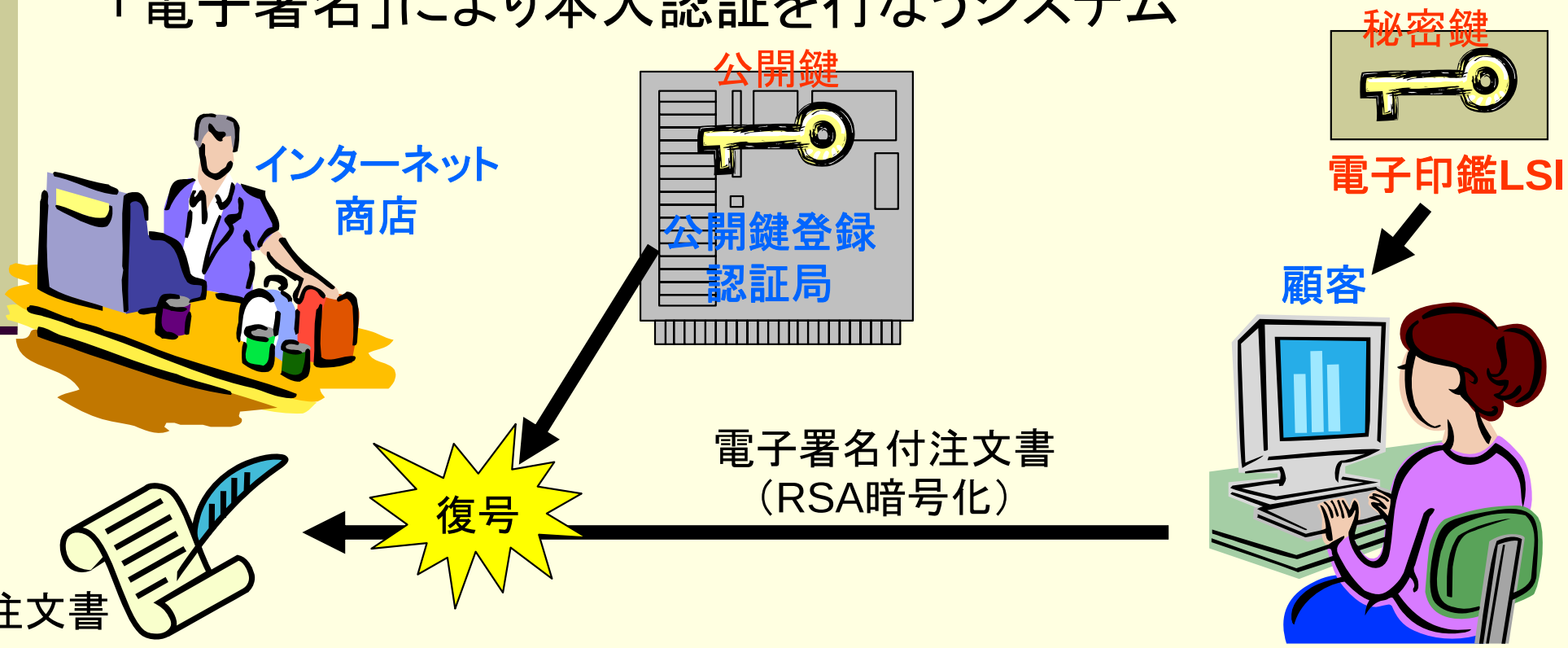
EthernetポートつきFPGA

作りたいネットワークシステム　例1

- インターネット上の個人認証
  - インターネット上のサーバーのログイン
  - インターネットの物品購入
  - ID/パスワードの管理が困りませんか？
- 公開鍵暗号基盤（PKI）を使い，個人が保管するセキュリティーデバイスに秘密鍵を保管
  ⇒個人認証に使用（電子印鑑）
- 偽造や改ざんを防止するために
  「EB直描技術を使用したビアプログラマブルLSI」を使用する

公開鍵暗号を使用した電子印鑑LSI

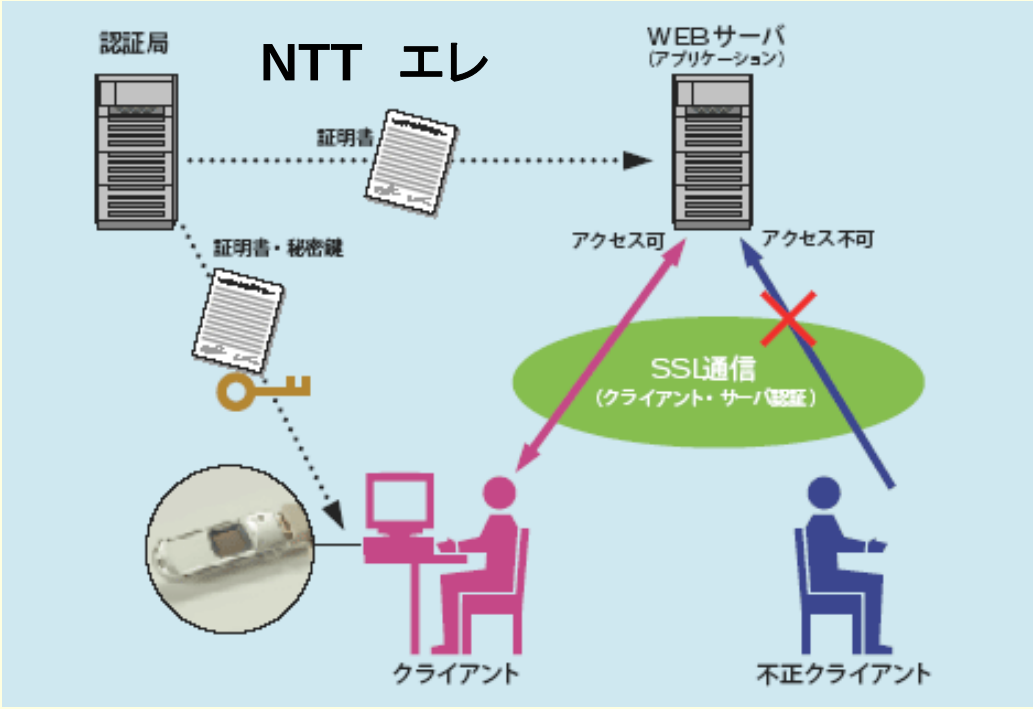
- RSA公開鍵暗号方式において生成される「秘密鍵」をマスクデータとして埋め込んだ電子印鑑LSIを製造し個人が保持
- 上記秘密鍵に対応する「公開鍵」を認証局に登録
- インターネット上の電子商取引など，あらゆるパスワードを要求される場面において，電子印鑑LSI上の「秘密鍵」を用いた「電子署名」により本人認証を行なうシステム



既存のセキュリティーデバイス

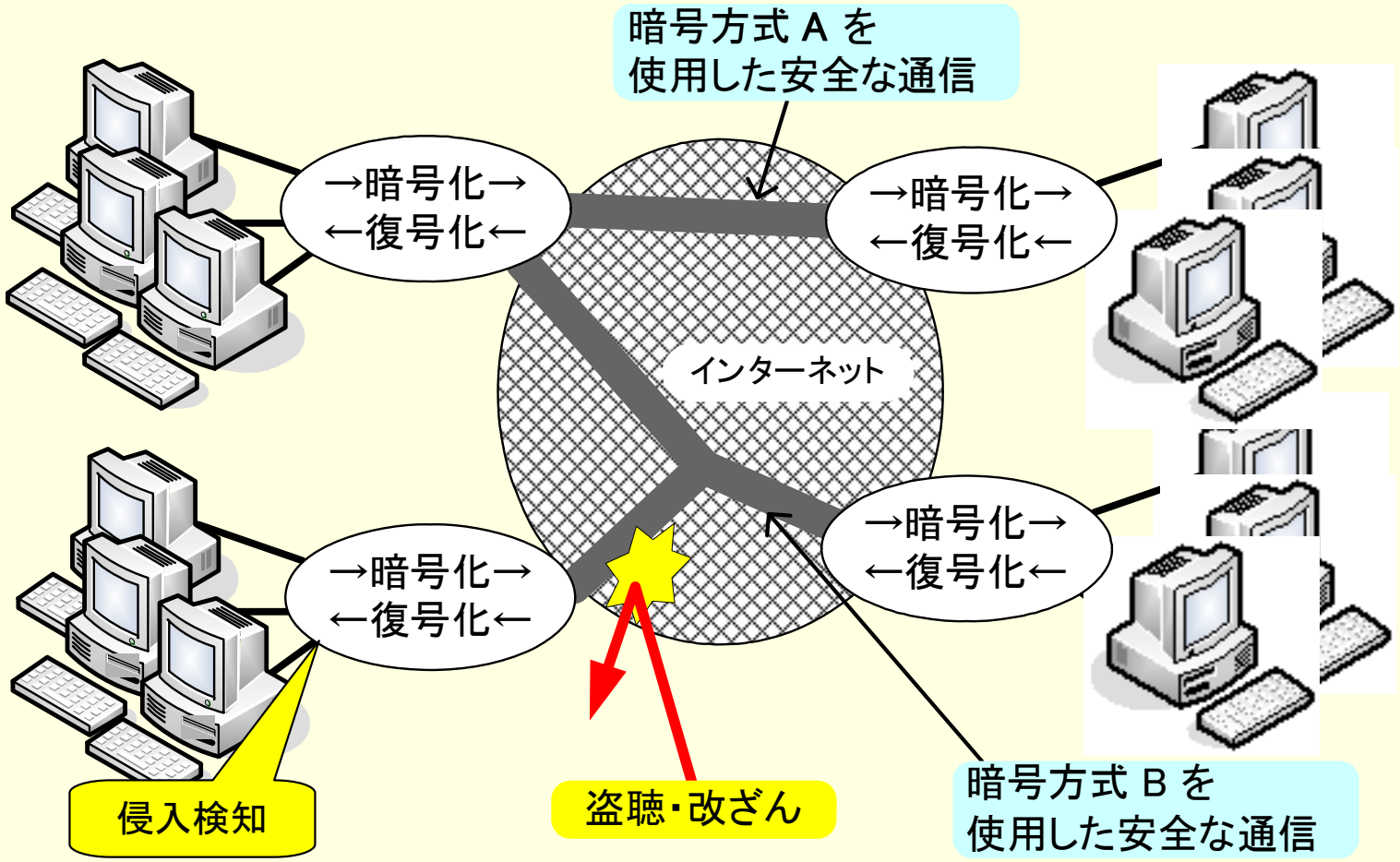
- デバイス例
  - 日立　KeyMobile
  - NTTエレ　Finger　Quick
  - Pentio　USB　Token
- フラッシュメモリ・公開鍵暗号化ロジックを搭載
- 指紋認証付きもあり

Pentio



作りたいネットワークシステム　例2

- ウイルス検知/暗号化一体型分散セキュリティーシステム
- 暗号化/文字列パターンマッチングに「リコンフィギャラブルロジックLSI」を使用する.



卒論までのながれ

応用演習	2006/12-2007/1	・暗号回路（共通鍵，公開鍵）技術紹介 ・簡単なネットワークおよびCプログラミングの演習
春季演習 （週1回）	2007/2-3	LSI設計の基礎 （MOSトランジスタ回路）
院生ゼミ演習 （週2回）	2007/4-6	・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	2007/7-9	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（発表）
卒論目次作成	2007/12	卒論作成前に内容を整理
卒論提出	2007/2	卒論を出してスノボ/スキーに！

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．

研究室訪問

- 今週～来週（アポイントメントなし）
  - 10/5（木） 16:00～17:30
  - 10/16（月） 17:30～19:00
  - 上記以外の個別相談はメイ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）
  - 11/13 (月) 17:30～19:00 研究室デモ展示
  - 11/14（火） 午後 院生による研究発表予定
  - 11/17（金） 午後 教員面談，院生懇談予定

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
- 日進月歩のインターネット技術に興味をもとう
- LSIの設計技術を応用して安全で快適なネットワークシステムを実現しよう

- 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ことのできる人
  - 手を動かして物を作ってみたい人

- 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.ritsumei.ac.jp/wiki/