電子署名とは

2002年7月24日

東京大学　生産技術研究所
今井秀樹，花岡悟一郎，米沢祥子

1．電子署名の定義

- 背景
- 登場人物
- 電子署名の要件
- 印鑑と電子署名

背景

- 「紙」文書→「電子」文書
- ネットワークの普及→ネットワーク上での電子商取引

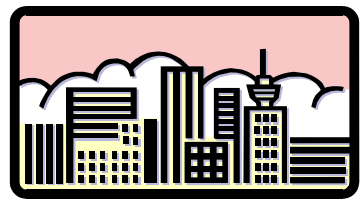
- 紙の上での印鑑に相当する機能を持つ技術が必要
  - 本人確認性
  - 改ざん･偽造不可能性

登場人物

署名者

署名生成アルゴリズム

署名生成鍵(秘密)



(信頼機関)

受領者

検証者

署名検証アルゴリズム

署名生成鍵に対応する検証鍵

電子署名アルゴリズムの要件

- **署名の生成**
  - 署名者は電子文書に対し，**署名者だけがもつ秘密データ（秘密鍵）**を用いて，電子文書と秘密データに依存するデジタルデータ（署名）を効率的に生成できる（信頼機関は署名者の秘密鍵を持つ場合もある）
- **署名の検証**
  - 検証者は**署名に対応付けられた検証鍵**（および検証者に与えられたその他の情報）を用いて，署名が正当な秘密鍵を用いてこの電子文書に対し生成されたものであるか否かを確実かつ効率よく確認できる
- **偽造不可能性**
  - いかなる電子文書に対しても，それに対する正当な署名を持っていなければ，署名者の秘密鍵を用いないで，検証者が正当と判断する署名を生成することが極めて困難→否認不可性

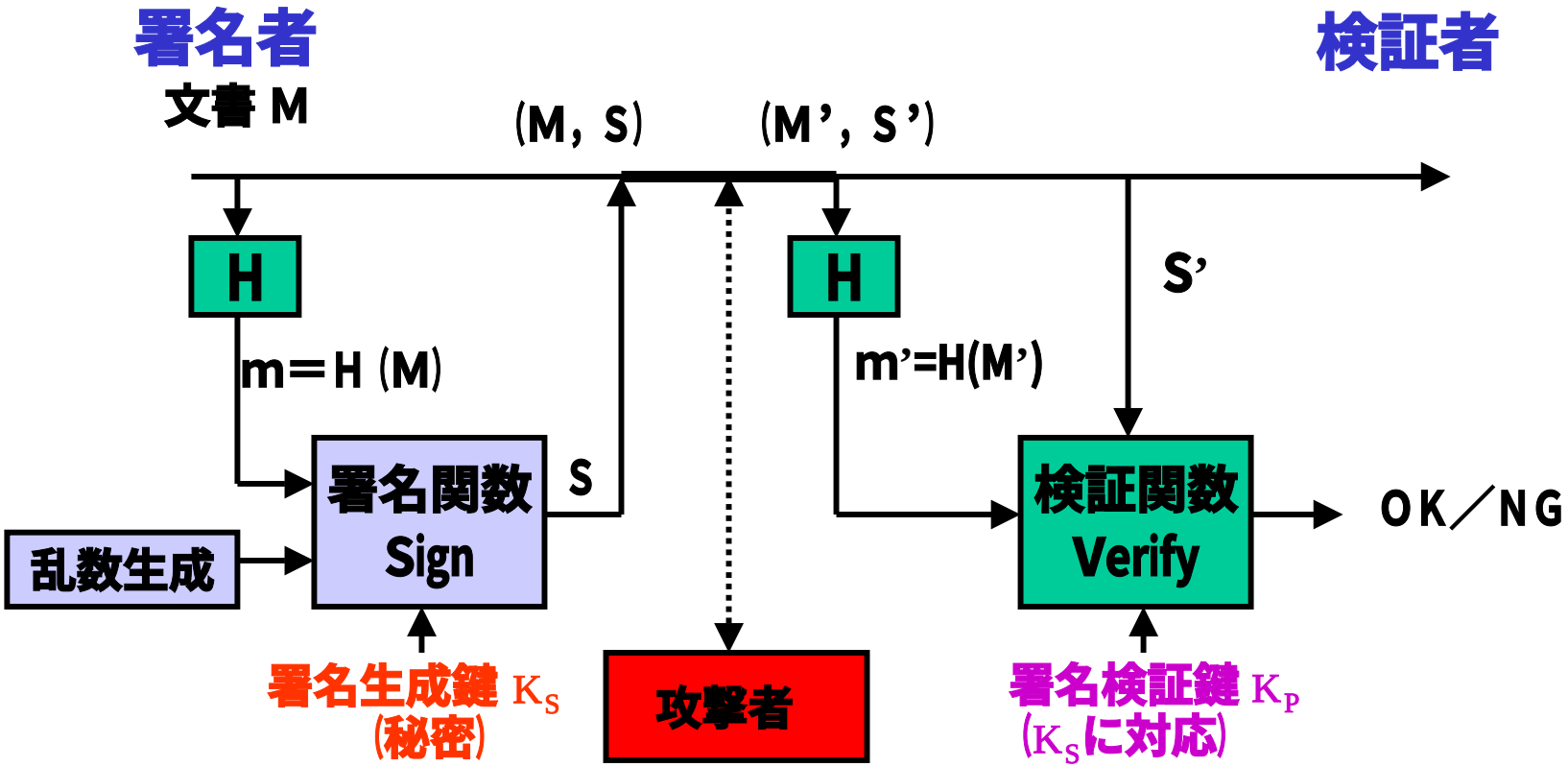
印鑑と電子署名

印鑑		電子署名
物理的な道具を用いる	署名生成	秘密鍵を用いて，数学的な演算により生成
人の目（またはそれに対応するもの）で判断するため，本物と偽物の境界はあいまい	署名検証	数学的な演算で確認するため，本物と偽物の境界が明確
物理的安全性	安全性	通常数学的安全性（計算量的安全性）/長期間の保証は困難
コピーはできるが痕跡が残る	コピー	文書のコピーはたやすく，痕跡も残らない
紙と一体化しているため，物理的制約がある	利便性	ネットワークを介しても署名できる/多様な機能を付加できる
今見ている文書に押印しているという実感がある	実感性	何に署名しているかの実感が得難い

2．電子署名の基本モデル

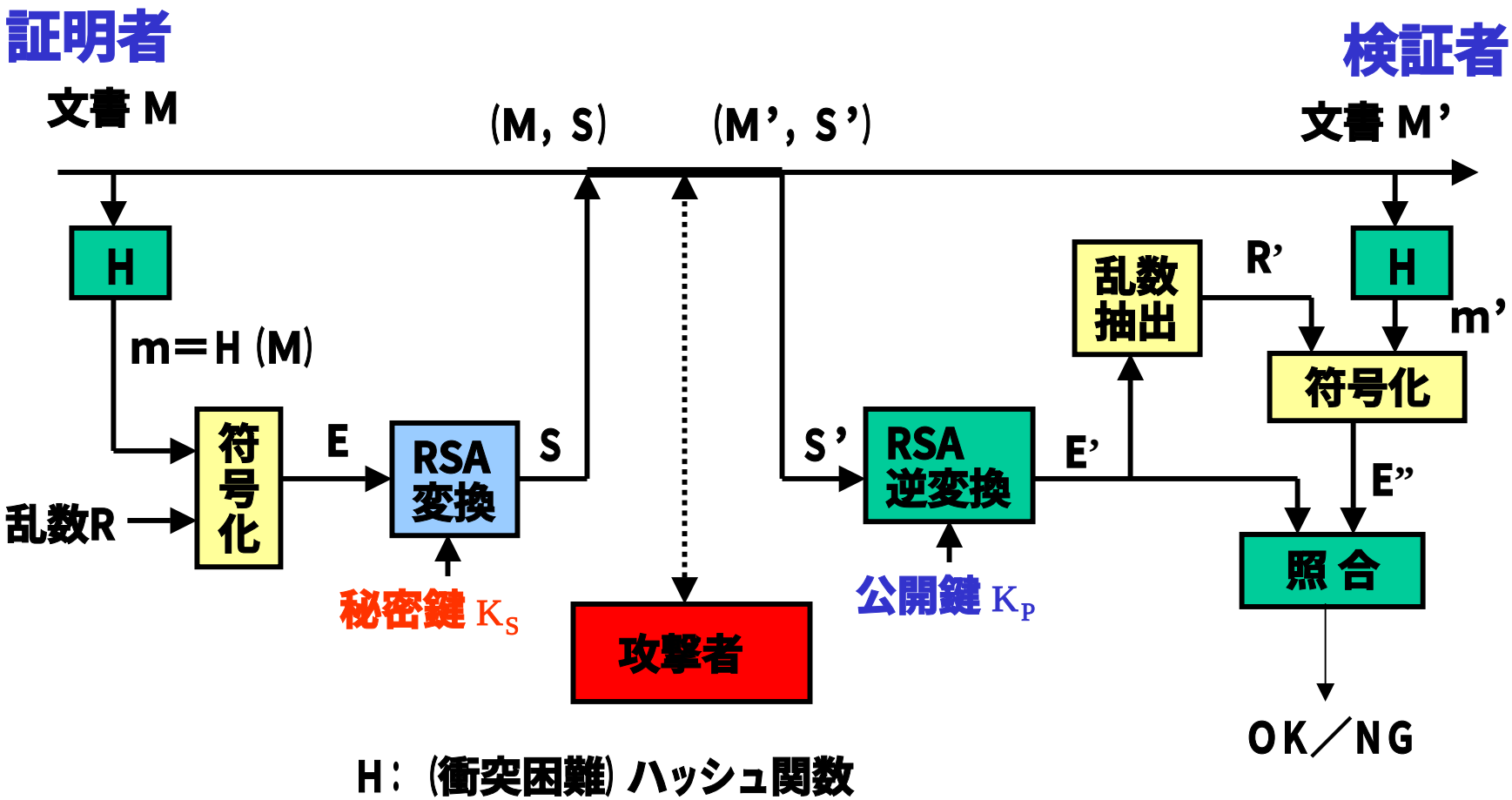
- 電子署名（添付型）
  - ✓例）RSA署名
  - ✓ハッシュ関数
  - ✓乱数生成器
  - ✓一方向性関数
- 検証に用いる情報
- 公開鍵の確認方法
- 公開鍵認証基盤（PKI）

電子署名 (添付型)



H：(衝突困難) ハッシュ関数

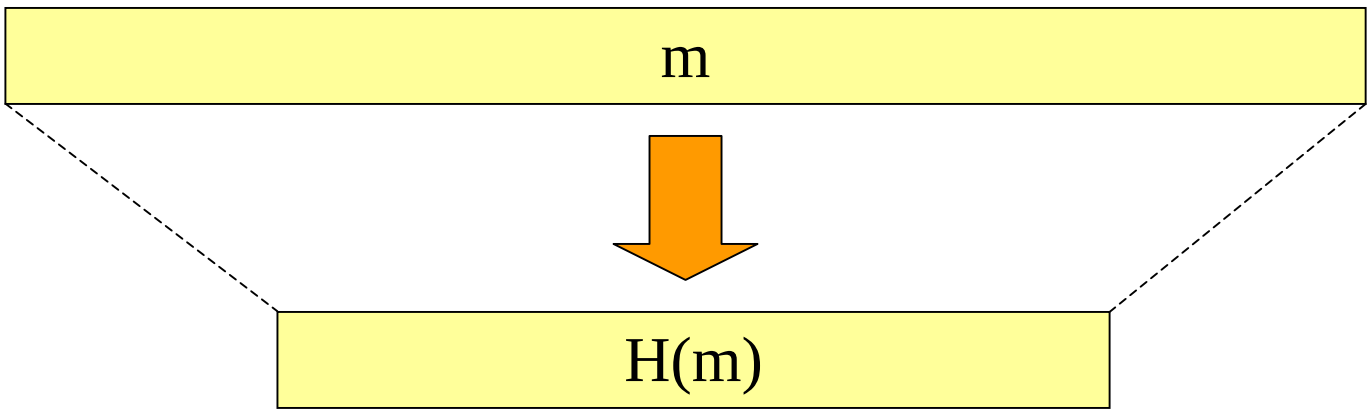
例) RSA署名


証明者
検証者
文書 M
(M, S)
(M', S')
文書 M'
H
m=H (M)
符号化
乱数R
E
RSA
変換
S
秘密鍵 K_S
攻撃者
S'
RSA
逆変換
公開鍵 K_P
E'
乱数
抽出
R'
H
m'
符号化
E"
照 合
OK／NG
H：(衝突困難) ハッシュ関数

電子署名の要素技術

- ハッシュ関数
  - メッセージを圧縮
- 乱数生成器
  - 確率的な署名のために乱数を生成
- 一方向性関数

ハッシュ関数

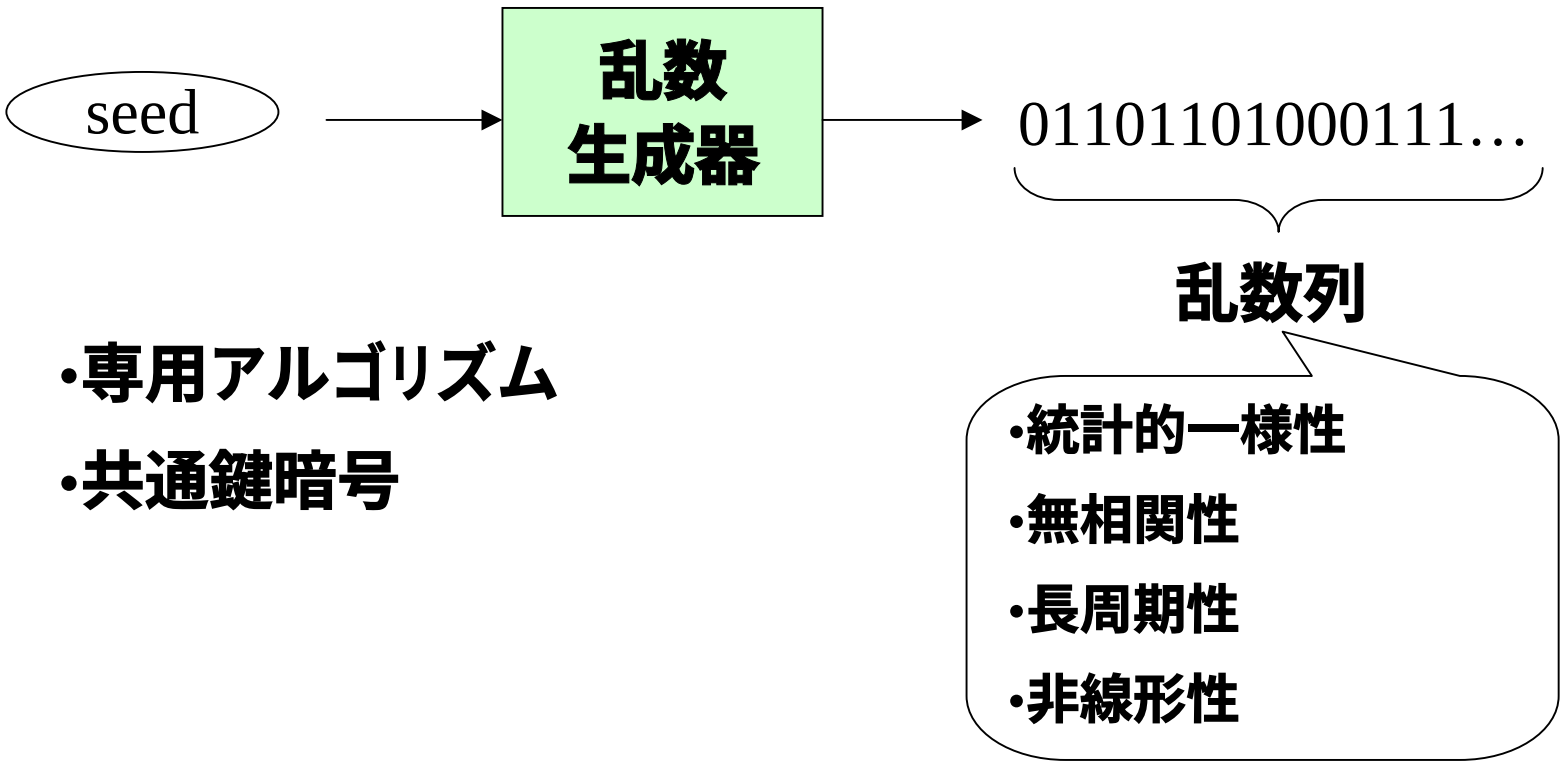


- **一方向性**
- **衝突困難性**

アルゴリズムの例…MD5（**安全性に問題**），SHA-1, SHA-256/384/512（**現段階では**Draft）**など**

乱数生成器

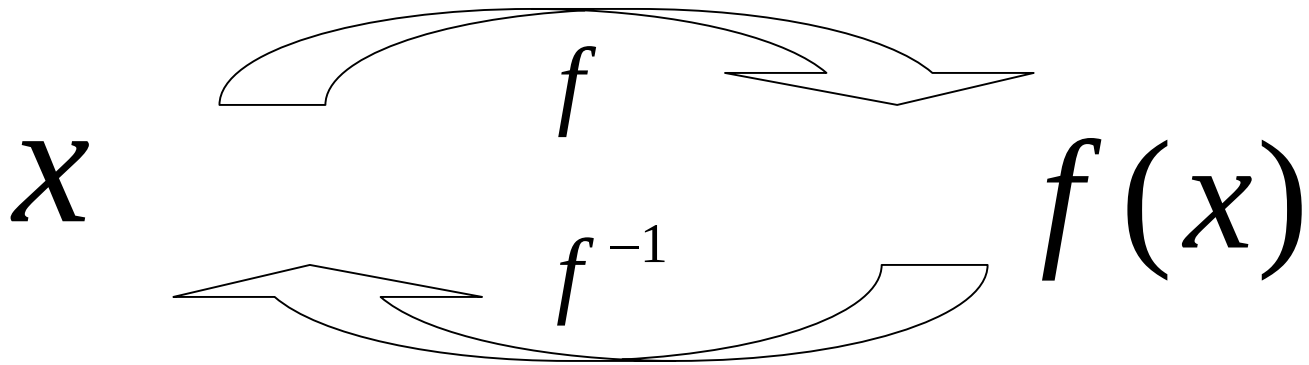
安全な暗号系を構成するためには乱数が重要！



- **専用アルゴリズム**
- **共通鍵暗号**

一方向性関数

多項式時間で計算可能



現実的な時間で計算不可能

例：べき乗剰余/離散対数 $f(x)=g^x \bmod p$　$f^{-1}(y)=\log_g y \bmod p$

一方向性関数が存在⇔電子署名が存在

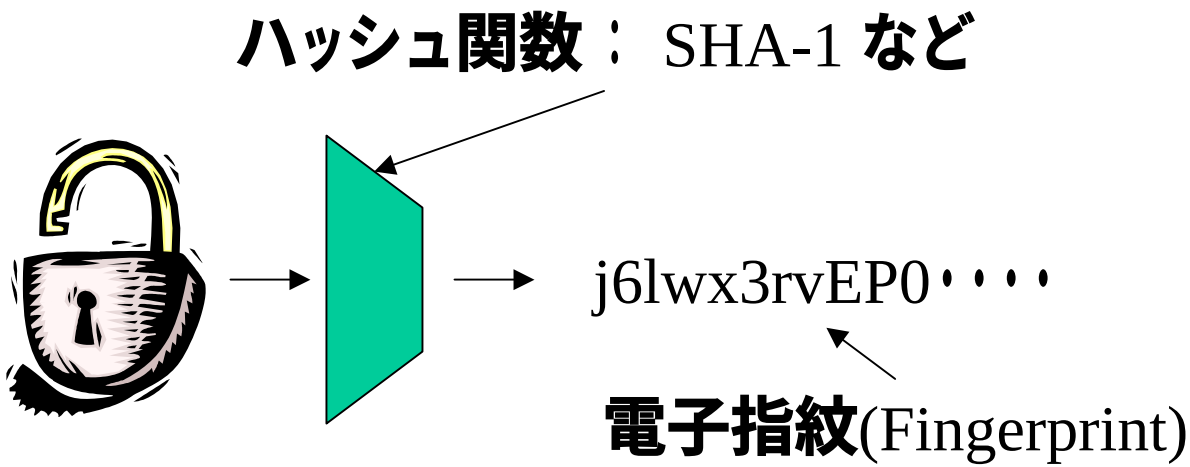
検証に用いる情報

- 公開鍵
  - 電子署名検証のため，秘密鍵と対応付けて生成する情報
  - 公開鍵と（その時点で署名の権限を持つ）署名者とを関連付けることが重要
- ID (IDベース署名)
  - 署名者を一意に表す情報
  - このIDが通用しているコミュニティにおいては，署名者と関連付けるための情報を省略できる（ただし，その時点で署名の権限を持つことを確認できるしくみが必要となることもある）

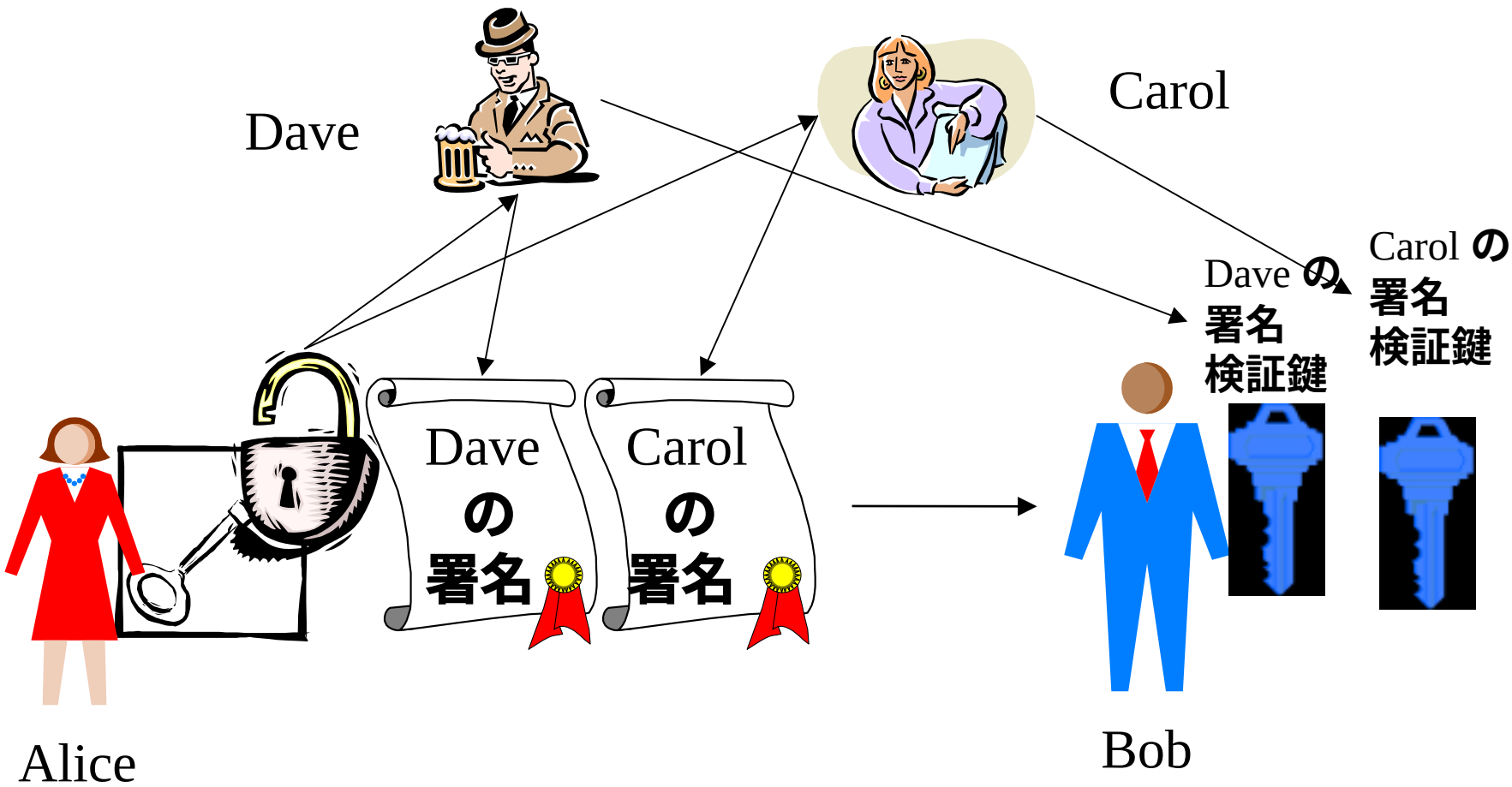
公開鍵の確認方法

ー電子署名システムの鍵管理の基本ー

- 手渡し（または信頼できる広報など）
- Fingerprint を手渡し，鍵はオンラインで入手
  - 改ざんおよび偽造のみに対処できればよい
  - 盗聴は問題とはならない



• 信頼できる共通の友人の署名を利用

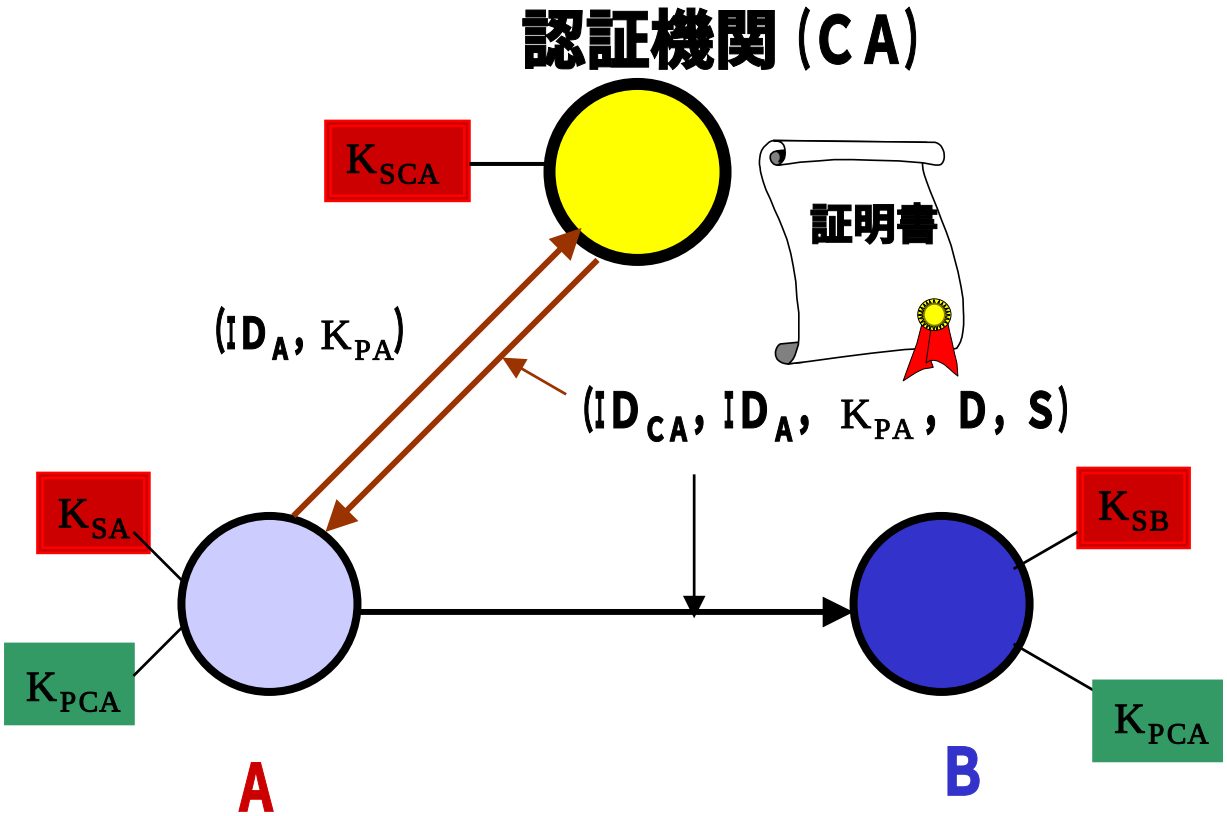


- **暗号・認証基盤**
  - –ネットワークにおいて暗号・認証技術を誰でも容易に利用できる仕組み
  - –共通鍵暗号の鍵共有と**電子署名**が中心

公開鍵認証基盤 (PKI：Public-Key Infrastructure)

- –現在の主流
- –公開鍵方式と認証機関 (CA)に基づく
- –計算量的安全性に依存
- –公開鍵方式としては，RSA暗号が中心
- –安全性の点から以下の点が特に重要
  - –CAの公開鍵をユーザに周知すること
  - –証明書の失効管理

公開鍵認証基盤 (PKI)



ID_{CA}：認証機関名　K_{SCA}：認証機関の秘密鍵　K_{PCA}：認証機関の公開鍵
S：認証機関の署名　D：有効期限等の情報
ID_A：Aの名前　K_{PA}：Aの公開鍵　K_{SA}：Aの秘密鍵
K_{SB}：Bの秘密鍵

3．電子署名の安全性

- 安全性の概要
  - ✓攻撃モデル
  - ✓安全性レベル
  - ✓安全性定義の相互関係
- 安全性の根拠
  - ✓計算量的安全性に基づく方式
  - ✓情報理論的安全性に基づく方式
  - ✓物理的安全性に基づく方式
  - ✓システム的安全性に基づく方式
- マルチレベルセキュリティの構成

電子署名の安全性の概要

- 証明可能安全性
  - 電子署名を偽造することが，ある種の解くことが難しい問題と同等に難しいことが証明されるとき，(計算量的) **証明可能安全性**を持つという
  - 電子署名の偽造に成功する確率が，署名のパラメータによって定まる十分小さい確率以下であることが証明されるとき，(情報理論的) 証明可能安全性を持つ，または単に**情報理論的に安全**という
- 安全性の表現：攻撃モデル＋安全性レベル

攻撃モデル

- **受動攻撃** (passive attack; key-only attack)
- **文書攻撃** (message attack)
  - **既知文書攻撃 (known-message attack)**：十分な数の文書とそれに対する署名とを持っている
  - **選択文書攻撃 (chosen-message attack: CMA)**：攻撃者が予め選択した文書に対する署名が得られる
  - **適応的選択文書攻撃 (adaptive chosen-message attack: ACMA)**：攻撃者がそれまでに得た文書を見て適応的に選択した文書に対する署名が得られる

安全性レベル

- **一般的偽造不可** (universally unforgeable)
  - 署名偽造が不可能な文書が存在する
- **選択的偽造不可** (selectively unforgeable)
  - 特定の文書に対して署名偽造が不可能
- **存在的偽造不可** (existentially unforgeable)
  - 既に署名が得られている文書以外のいかなる文書にも署名偽造が不可能

安全性定義の相互関係

- EUF-ACMA（適応的選択文書攻撃に対して存在的偽造不可）が最強の安全性なので，これを達成できればいい
  - EUF-ACMA・・・攻撃者が毎回適応的に任意に選んだ文書に対して署名オラクルに署名させるとき，そこで得た情報からどんな文書に対する署名も偽造できない

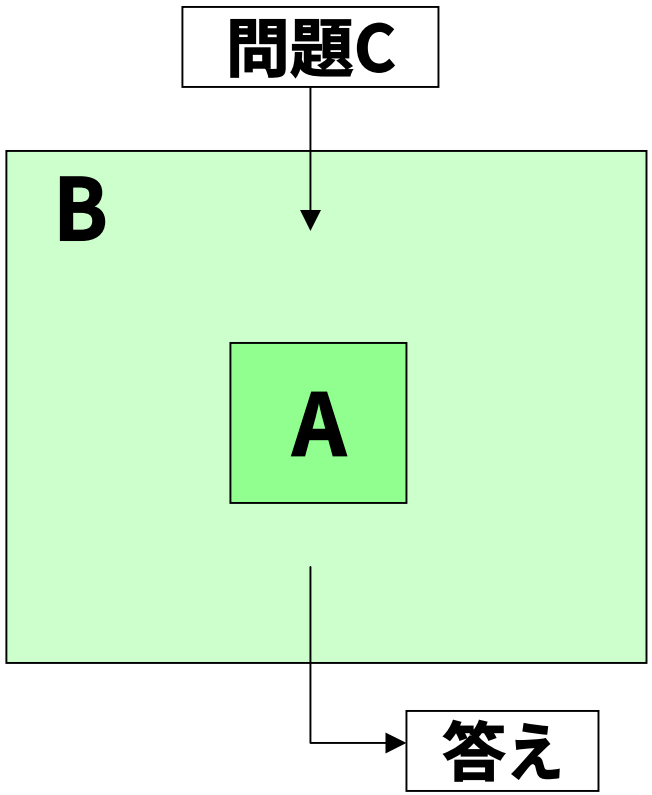
安全性の根拠

- 計算量的安全性
- 情報理論的安全性
- 物理的安全性
- システム的安全性

★信頼機関の信頼性

＜方式によって信頼性に対する要求が異なる＞

計算量的安全性に基づく方式



A：署名方式を破るアルゴリズム

B：計算量的に難しい問題Cを解くアルゴリズム

署名方式を破れる
⇒計算量的に難しい問題が解ける

対偶

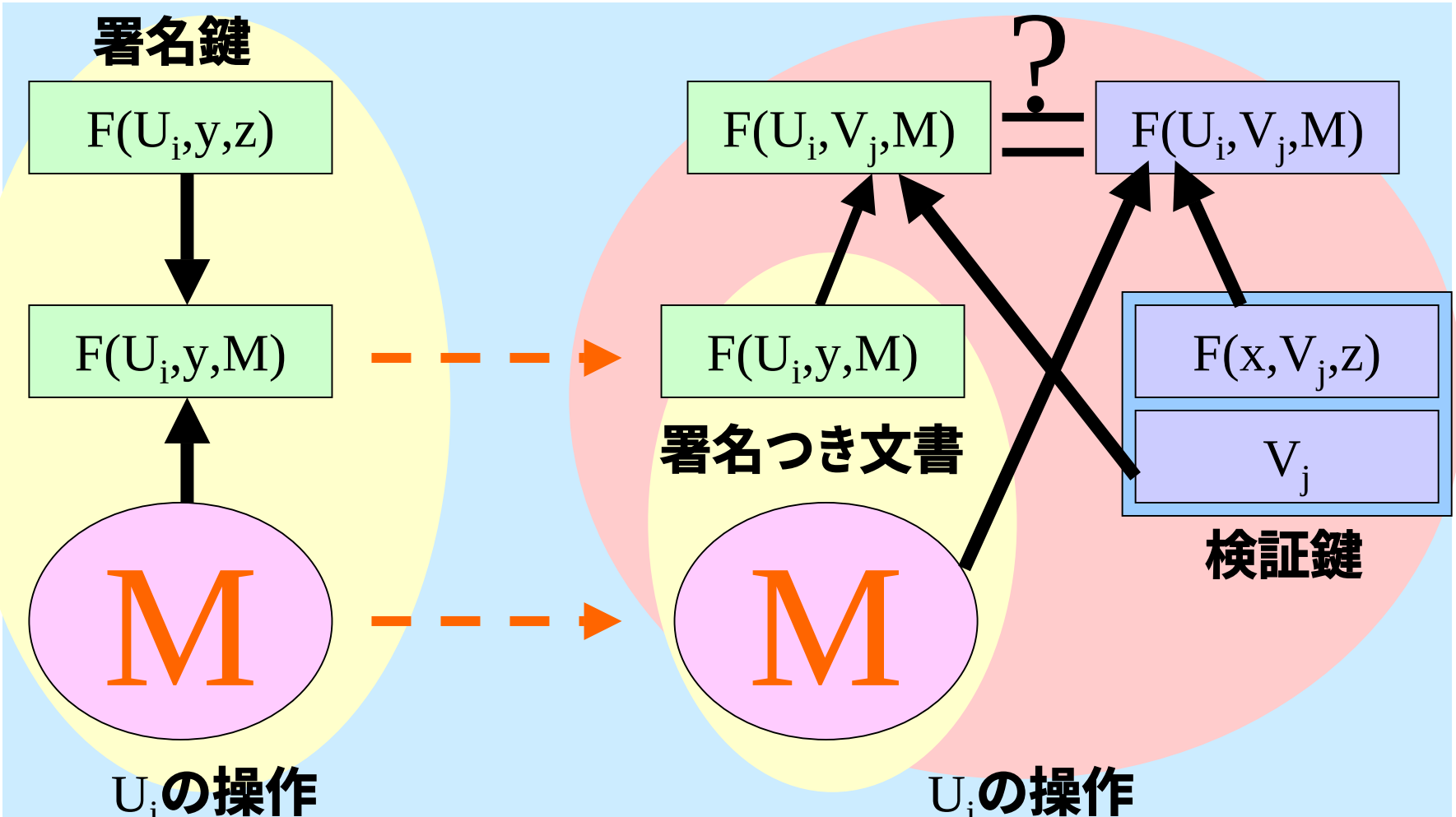
計算量的に難しい問題が解けない
⇒署名方式が破れない

計算量的仮定

- 離散対数問題
- 素因数分解問題
- 多変数多項式問題

情報理論的安全性に基づく方式

花岡・四方・今井・鄭による電子署名方式



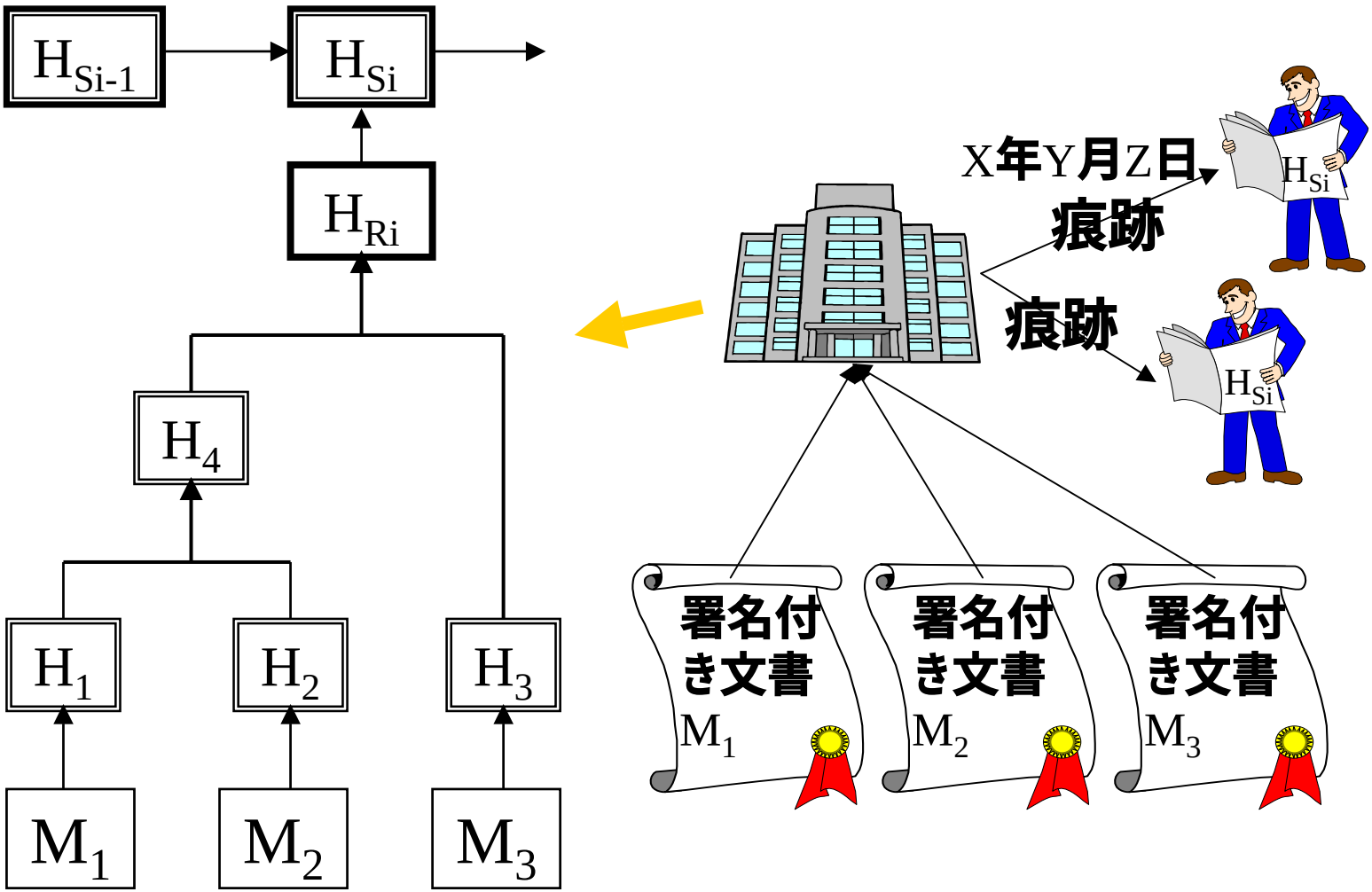
物理的安全性に基づく方式

- 耐タンパー性に基づく方式
  - システム鍵方式
  - KPS署名[松本・今井(1987), 西岡・花岡・今井(1999)]
- 量子暗号技術
  - 鍵交換：証明可能安全性，認証要
  - 署名：攻撃者の能力に何らかの仮定が必要
    [Lo・Chau(1996), Mayers(1997), Salvail(1998), Mueller-Quade・Nascimento・今井(2000)]
    - 一時的計算量的仮定では不可能
    - 一時的物理的仮定（量子メモリの制約等）では可能

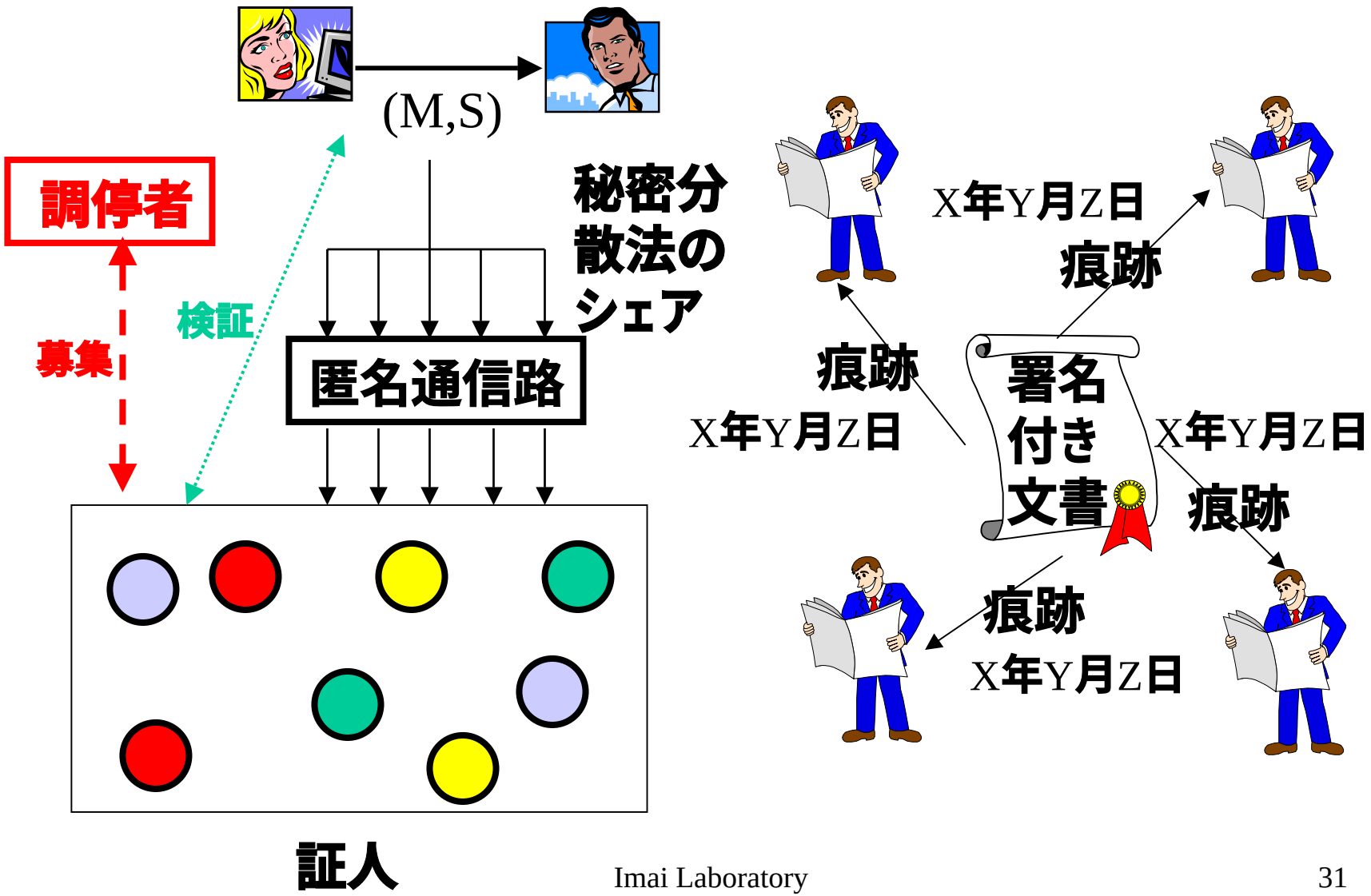
システム的安全性に基づく方式

- タイムスタンプ方式
  - ハッシュ関数の安全性に依存する場合が多い
- Witness-based 署名
  - Nacsimento・Mueller-Quade・今井(2000)：人の証言を利用，その時点における計算量的仮定が成立すれば，情報量的安全性
- 連鎖署名
  - 松本・岩村・佐々木・松木(2000)：署名の連鎖を作る
- その他
  - 再署名法（本人または代理人による再署名），．．．

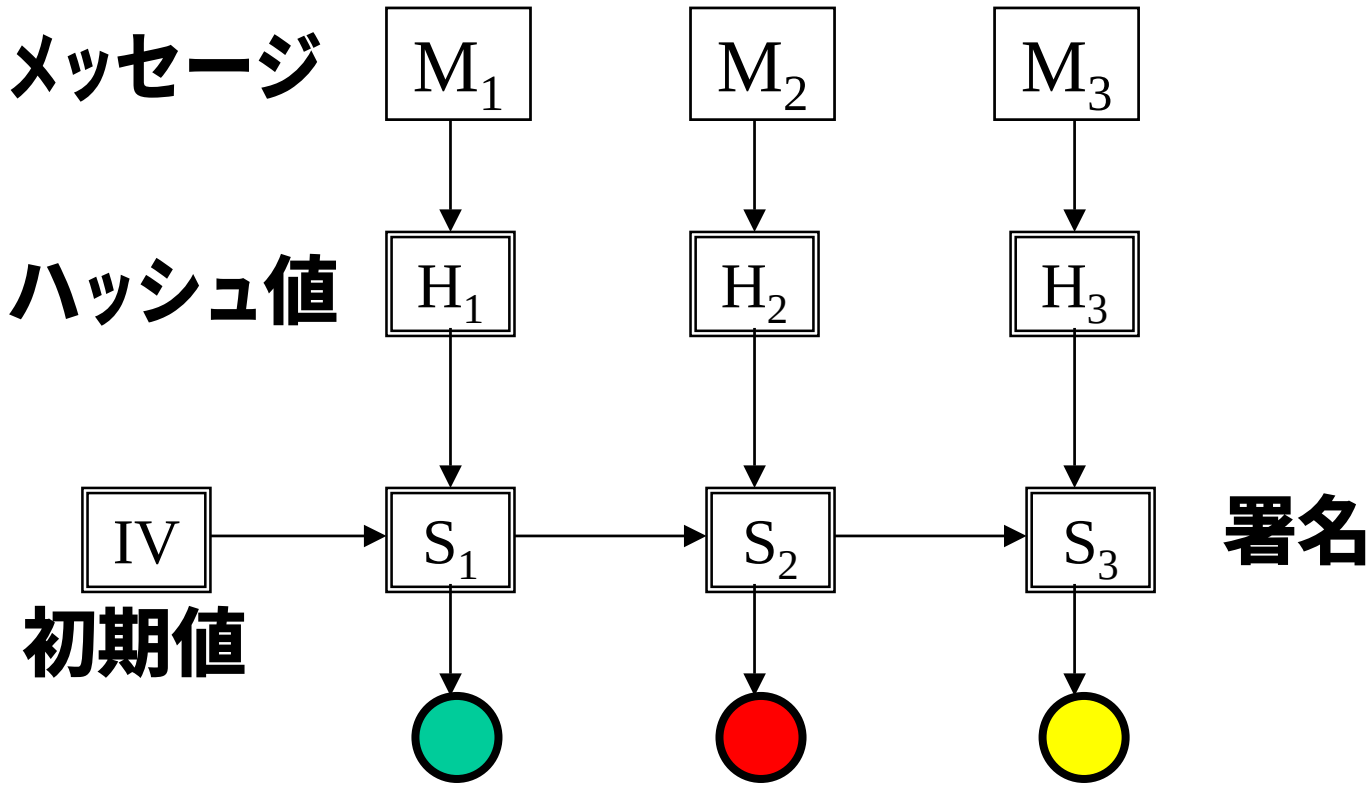
タイムスタンプ方式の一例



Witness-based署名



連鎖署名の一例



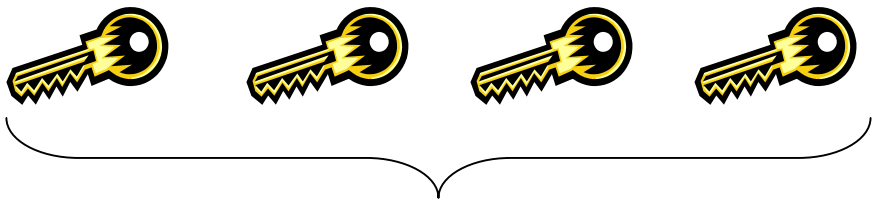
マルチレベルセキュリティの構成

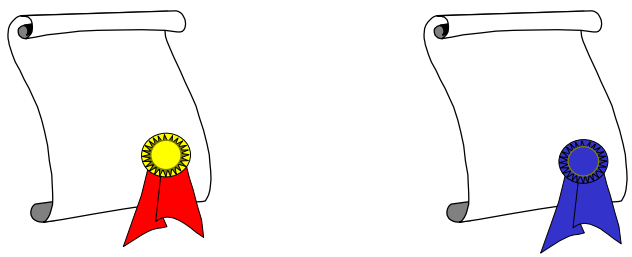
- フェイルストップ署名
  - 秘密鍵を見つけることは情報理論的に難しい
  - 署名の偽造は計算量的に難しい
  - 署名者が偽造を証明できる
- Forward-secure署名
  - 期間を分割し，分割した期間ごとに署名鍵を更新
  - ある時点で署名鍵が破られても，それ以前の期間の署名を偽造することはできない

フェイルストップ署名

複数の秘密鍵

秘密鍵に関する情報は一切洩れない

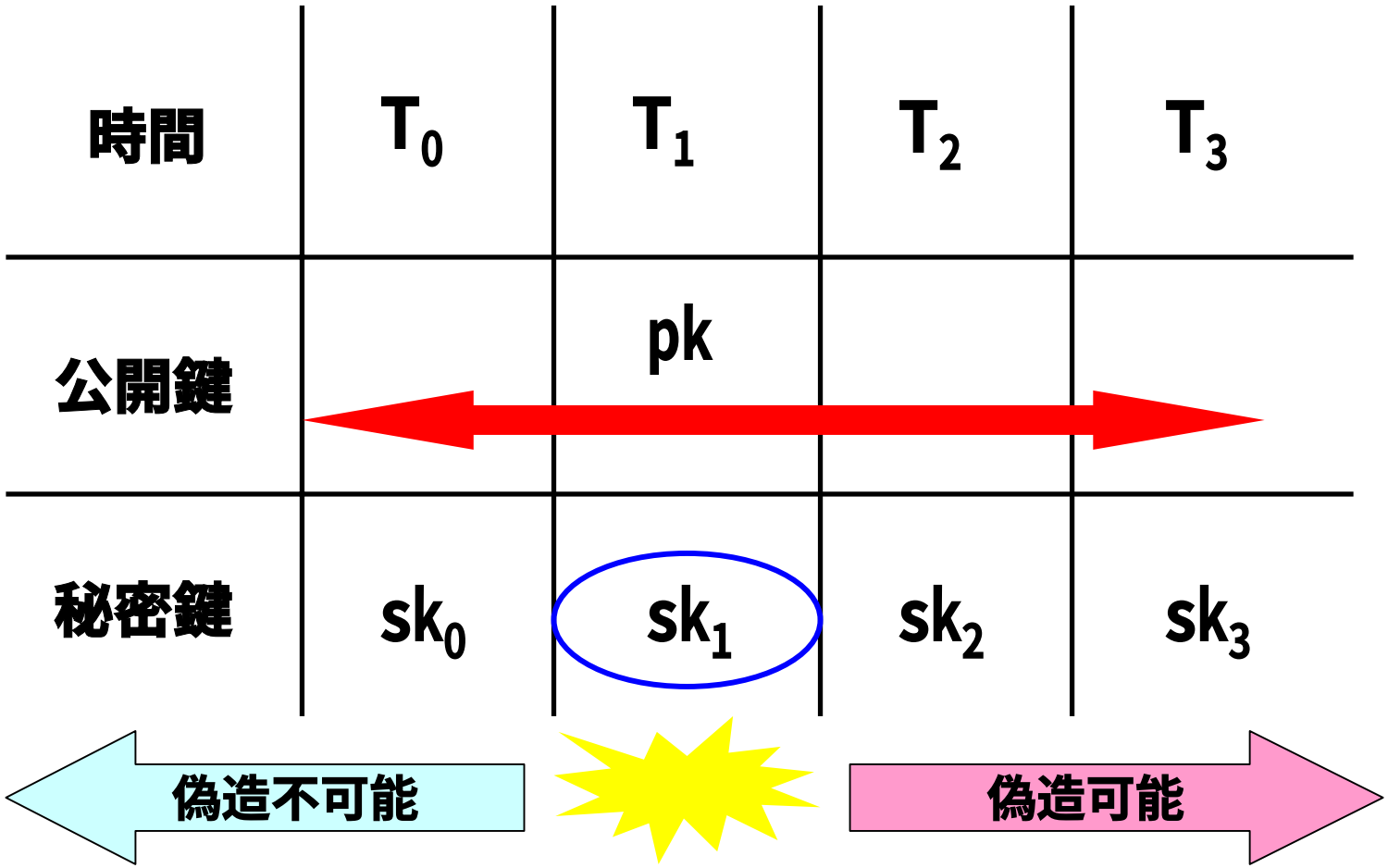




偽造

偽造を証明可能

Forward-secure署名



4．代表的な電子署名方式
-アルゴリズムと実装-

- 代表的なアルゴリズム
- 離散対数問題に基づく方式
- 素因数分解問題に基づく方式
- 多変数多項式問題に基く方式
- 電子署名方式の標準化

代表的なアルゴリズム

- **離散対数問題に基づく方式**
  - ElGamal**署名方式** (1985)
  - Schnorr**署名方式** (1991)
  - DSA (1991)
    - ECDSA (1998)
- **素因数分解問題に基づく方式**
  - RSA**署名方式** (1978)
  - Fiat-Shamir**署名方式** (1986)
  - ESIGN (1991)
- **多変数多項式問題に基づく方式**
  - SFLASH (2001)
  - QUARTZ (2001)

離散対数問題に基づく方式

- ElGamal署名方式
  - 初めての離散対数問題の困難性に依拠する方式
  - 厳密な意味では安全でない (つまりEUF-ACMAでない)
    - ただし, 簡単な変形で証明可能安全性を実現
- Schnorr署名方式
  - 有限体全体ではなく部分群を利用するアイデアに基く
  - ElGamal署名に比べ非常に小さい署名長を実現
  - 厳密な意味での安全性を証明可能
    - 離散対数問題と同等の困難性
- DSA (Digital Signature Algorithm)
  - NISTによって定められた米国標準電子署名方式
  - ElGamal署名方式に部分群を用いるアイデアを適用
  - 安全性の証明はなされていない
  - ECDSA…楕円曲線上の離散対数問題に基くDSA

素因数分解問題に基づく方式

- RSA署名方式
  - 初めての電子署名方式
  - RSA問題...素因数分解問題との等価性は不明
  - PSS, FDHと呼ばれる簡単な変形で安全性を証明可能
    - ただし，安全性はRSA問題に帰着
- Fiat-Shamir署名方式
  - 証明可能安全性を有する
    - 素因数分解の困難性に帰着
- ESIGN
  - 署名生成がRSA署名より高速
    - e乗根近似問題, 素因数分解の困難性に依拠
    - パラメータの選択によっては，安全でない場合がある
    - 簡単な変形で安全性を証明可能．ただし，やや限定された安全性．

多変数多項式問題に基く方式

- SFLASH, QUARTZ
  - NESSIEに応募
  - 松本･今井 (1985) の多変数多項式タプル非対称暗号系の流れ
  - 署名サイズが非常に小さいのが特長
    - QUARTZの場合, 128bitの署名長
  - ただし, 公開鍵のサイズは非常に大きい
  - 安全性は証明されていない

電子署名方式の標準化

- **離散対数問題に基づく方式**
  - DSA…**米国**NIST**標準**, **電子署名法指針**, CRYPTREC
  - ECDSA in SEC1…CRYPTREC
  - ECDSA (ANSI X9.62)…ANSI, **電子署名法指針**, CRYPTREC
- **素因数分解問題に基づく方式**
  - RSA-PKCS#1v1.5...**電子署名法指針**, CRYPTREC
  - RSA-PSS…IEEE P1363a, CRYPTREC, NESSIE (2nd Phase)
  - ESIGN…**電子署名法指針**
  - TSH-ESIGN…IEEE P1363a, NESSIE (2nd Phase)
- **多変数多項式問題に基づく方式**
  - SFLASH…NESSIE (2nd Phase)
  - QUARTZ…NESSIE (2nd Phase)

＜電子署名法指針：電子認証業務認定指針＞

5．さまざまな機能を持つ電子署名

- 匿名性を追求する署名
  - ✓受領者のプライバシー
  - ✓署名者のプライバシー
  - ✓検証者を限定する方式
  - ✓受領者および署名者のプライバシー
- 効率性･利便性を追求する署名

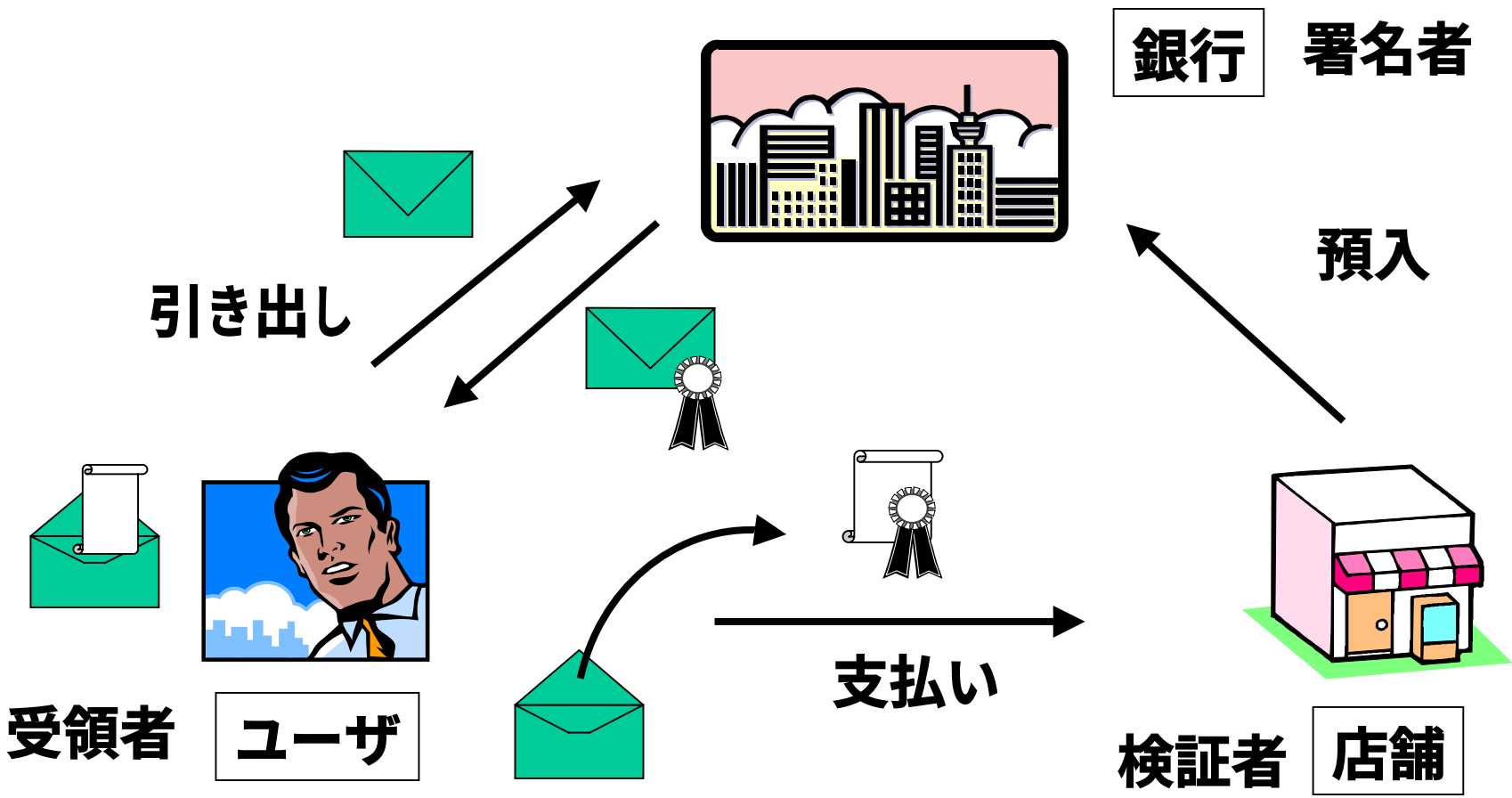
匿名性を追求する署名

- 受領者のプライバシー
  - ブラインド署名
- 署名者のプライバシー
  - グループ署名
  - リング署名
- 検証者を限定する方式
  - 否認不可署名
  - 指名検証者署名
- 受領者および署名者のプライバシー
  - 不正者追跡署名
  - グループブラインド署名

受領者のプライバシー

- ブラインド署名
  - 署名すべきデータを隠したままで署名を発行
  - 受領者は自分の秘密情報を知られることなく受領した署名を利用することができる
  - 電子マネー・電子投票

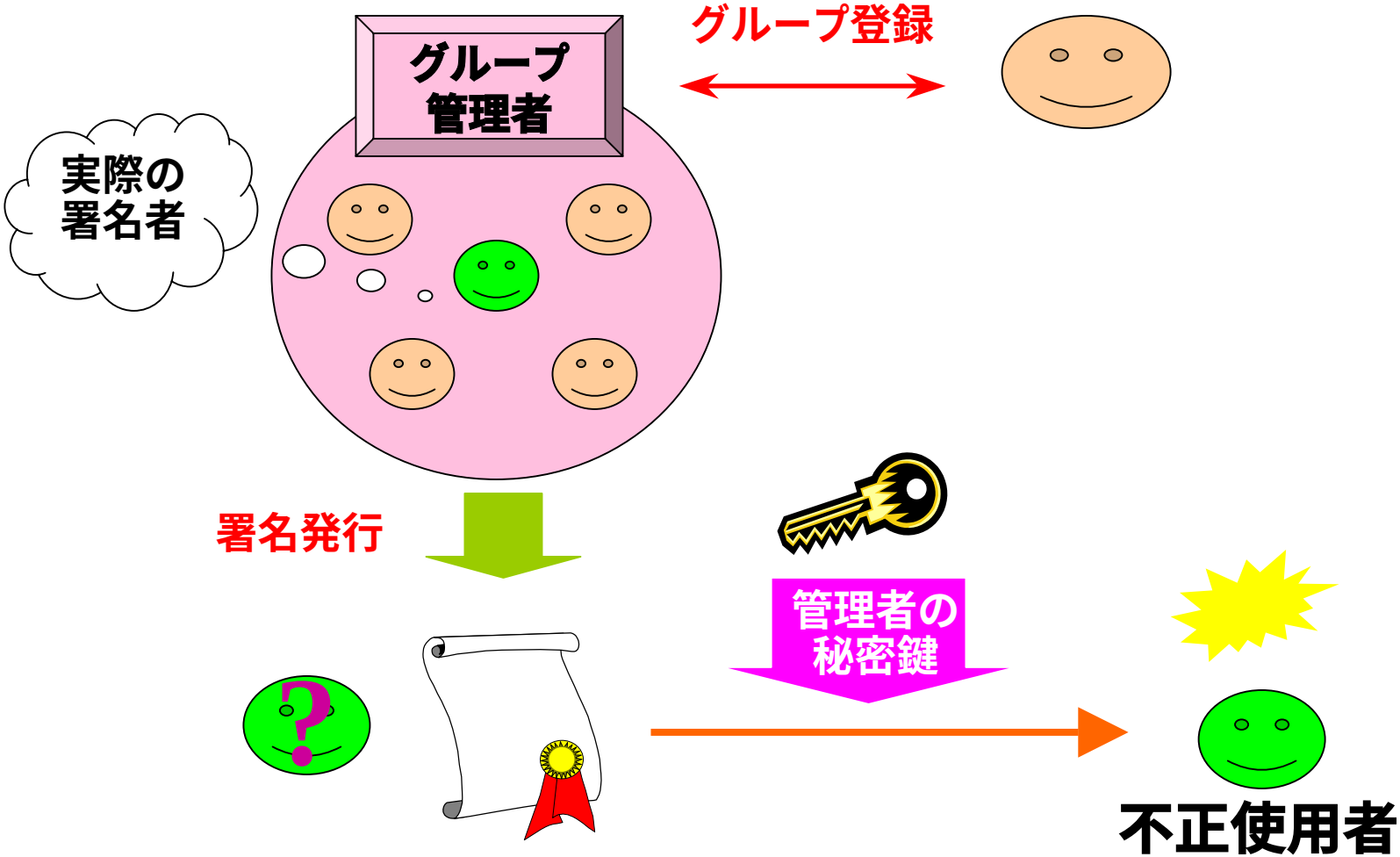
ブラインド署名



署名者のプライバシー

- 署名者本人を隠す方式
  - グループ署名
  - リング署名
- 署名者は，個人情報を明かさずに電子文書に署名
- 実際の署名者が誰なのかはわからないが，ある集合に含まれていることはわかる

グループ署名

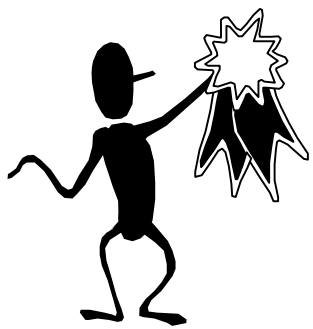


リング署名

- 管理者なしグループ署名に近い
- 登録制度なく，署名者が勝手にグループメンバーを選んで，グループメンバーの公開情報を利用し，グループ署名を作る
- 従って，最終的に本当の署名者を特定することは不可能

グループメンバー

＋



署名者

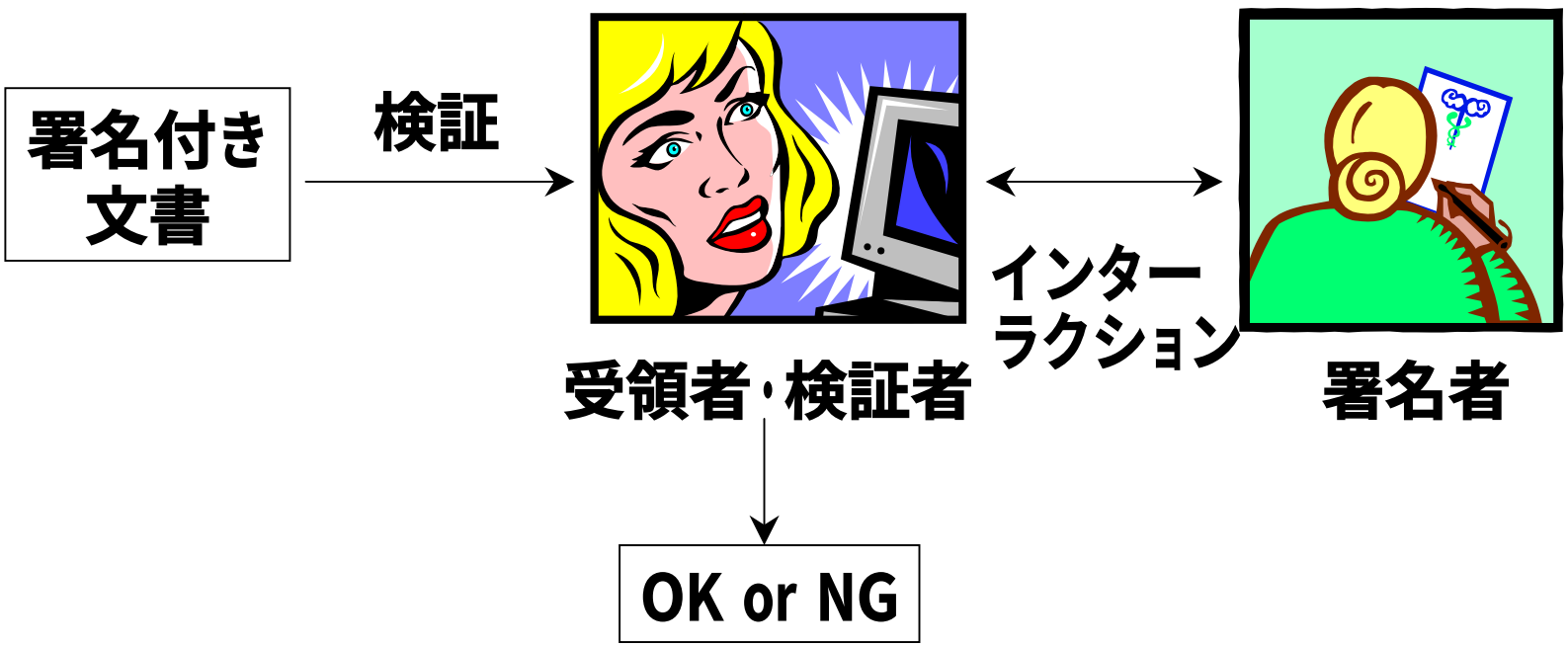
署名

検証者を限定する方式

- 検証者を限定
  - 否認不可署名 (Invisible署名)
  - 指名検証者署名
- 署名を検証できるエンティティを限定することにより，署名つき文書の不正流出を防ぐ
- 結果的に，署名者に関する情報が広まるのを防いでいる

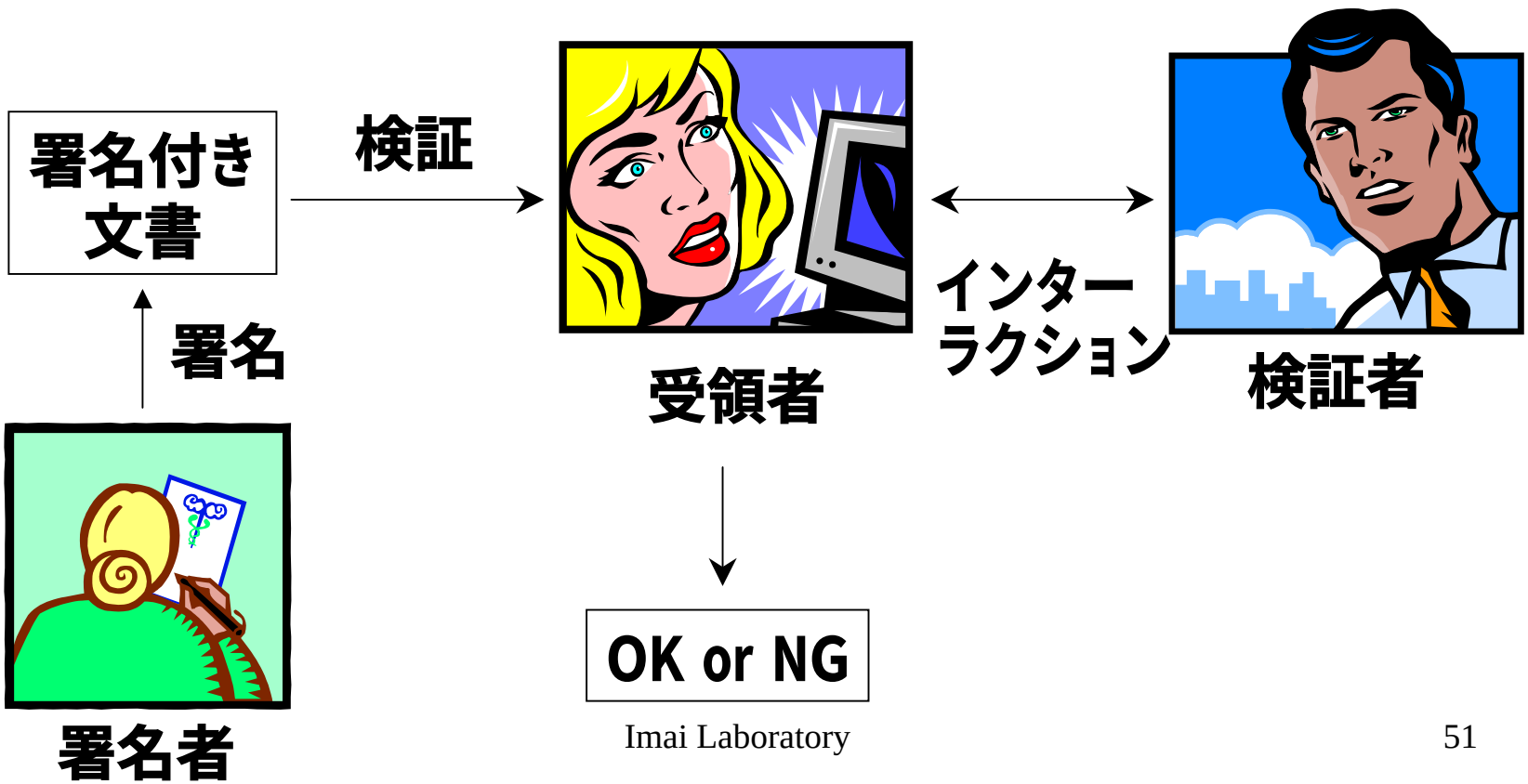
否認不可署名 (Invisible署名)

- 署名の検証に署名者本人の介在が必要



指名検証者署名

- 署名者が署名生成時に検証者を指定
- 正当性の確認は検証者に問い合わせる



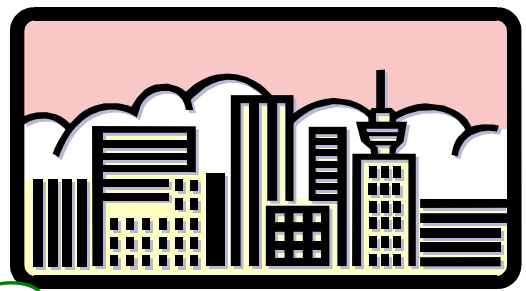
受領者および署名者のプライバシー

- 不正者追跡署名
  - 受領者の身元は署名者に知られない
  - 署名者の発行した署名の不正流出を抑止
- グループブラインド署名
  - 受領者の秘密情報は署名者に知られない
  - 署名者の身元は受領者に知られない

不正者追跡署名

システム
管理者

登録機関

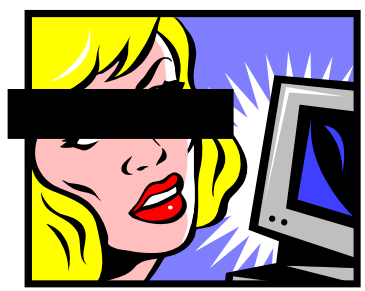


不正受領者
の追跡

システム
加入

署名発行

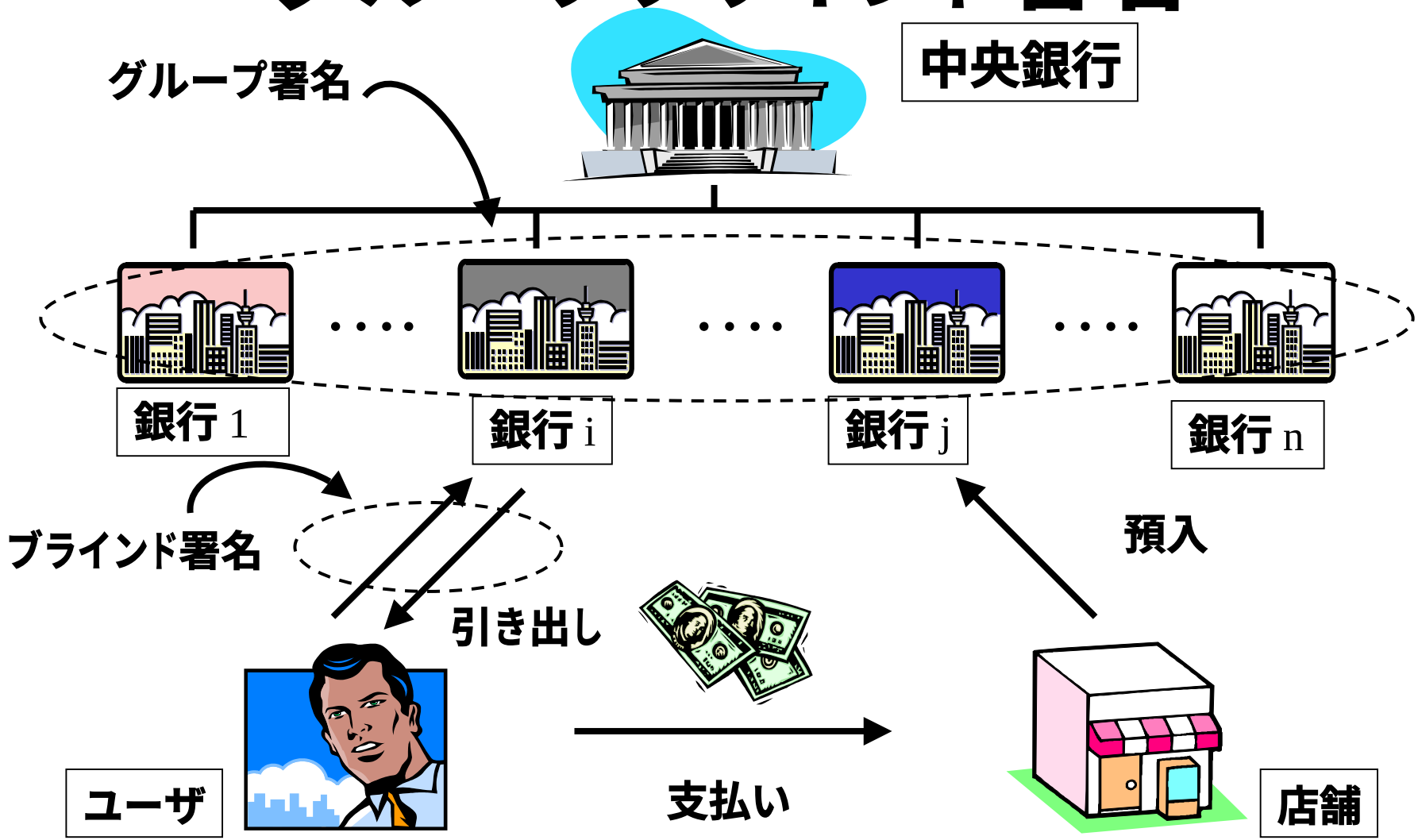
インターラクション



署名者

受領者・検証者

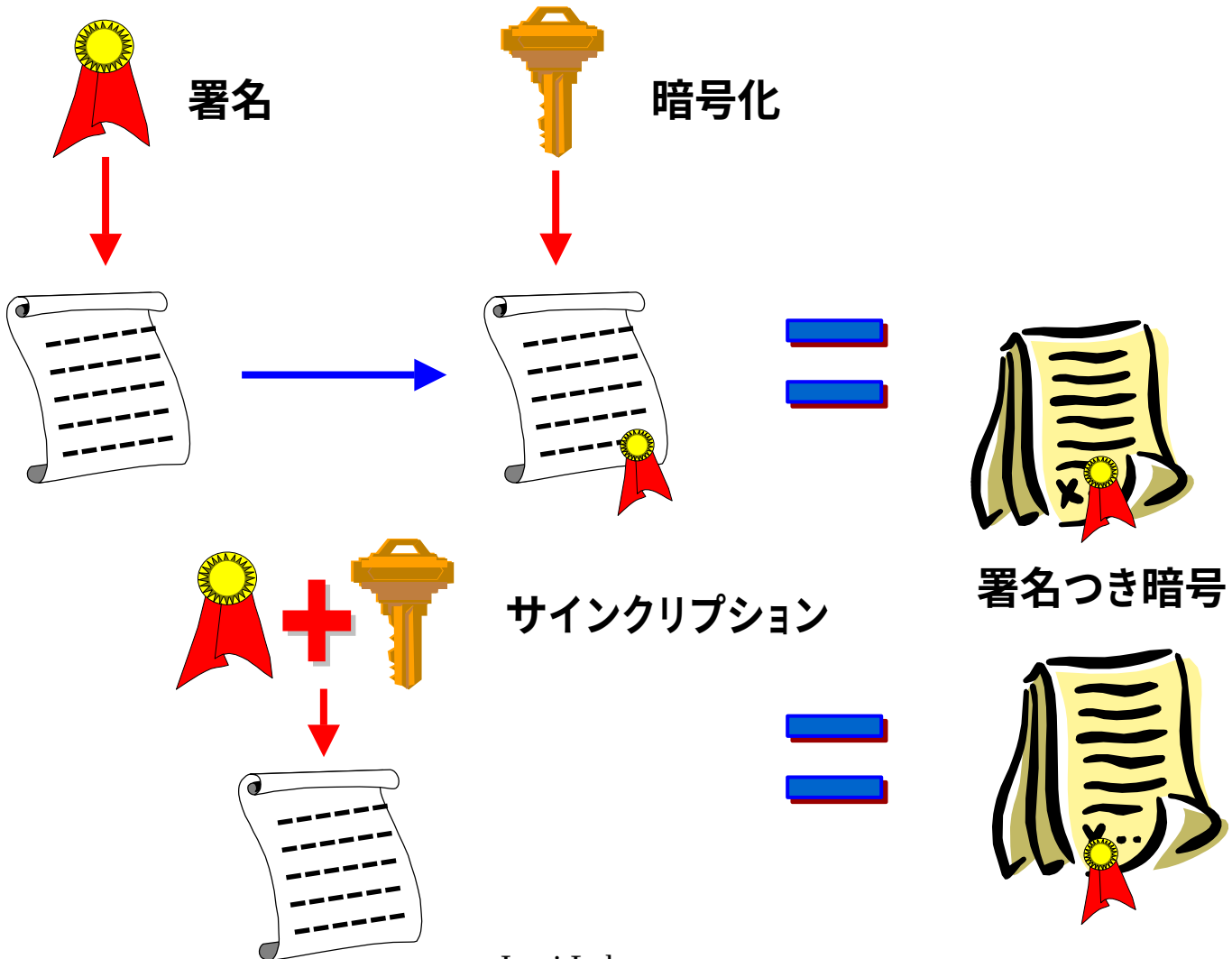
グループブラインド署名



効率性・利便性を追求する署名

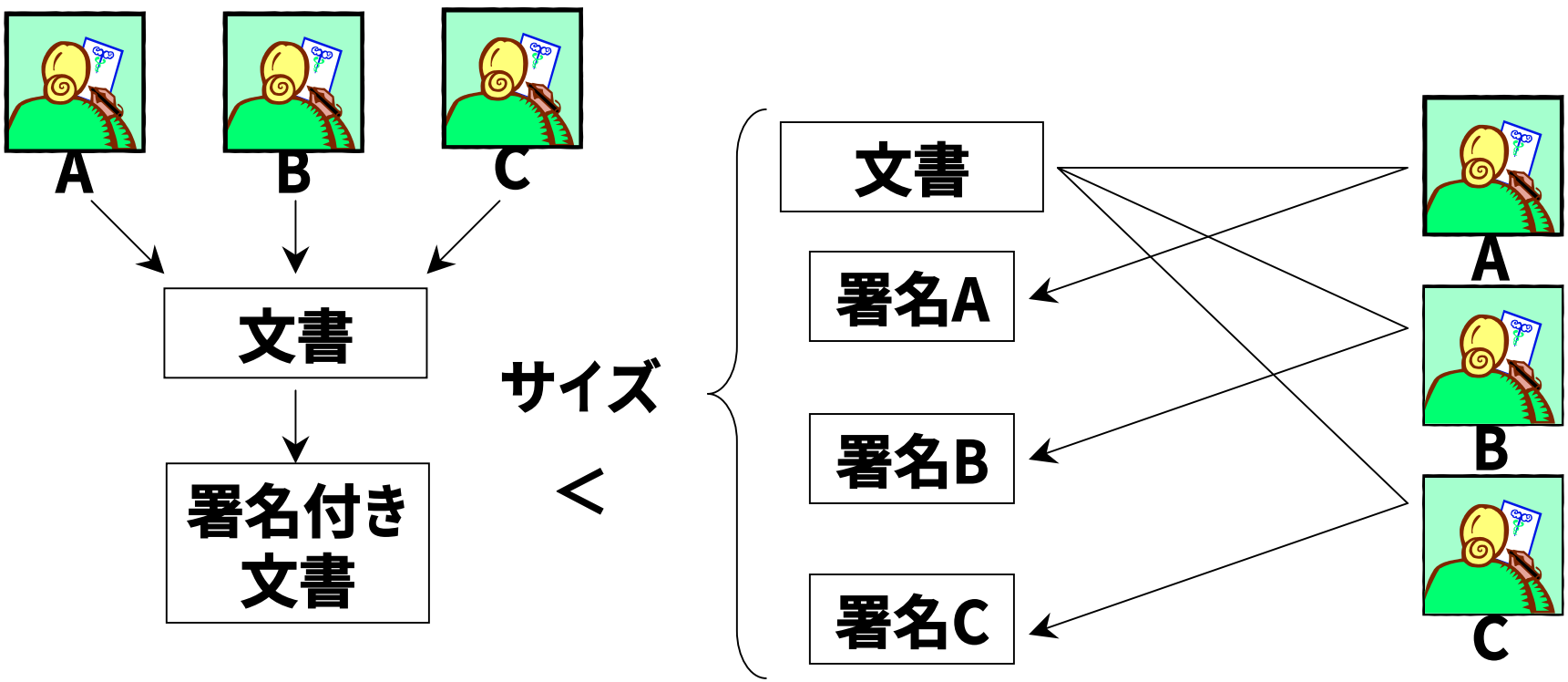
- サインクリプション
  - 署名＋暗号化の処理を効率化
- 多重署名
  - ひとつの文書に複数人が署名するときのメモリ量削減
- 代理署名
  - ある署名者の委任を受け，署名を生成する方式
- 閾値署名
  - 安全性の向上
- メッセージ復元型署名

サインクリプション

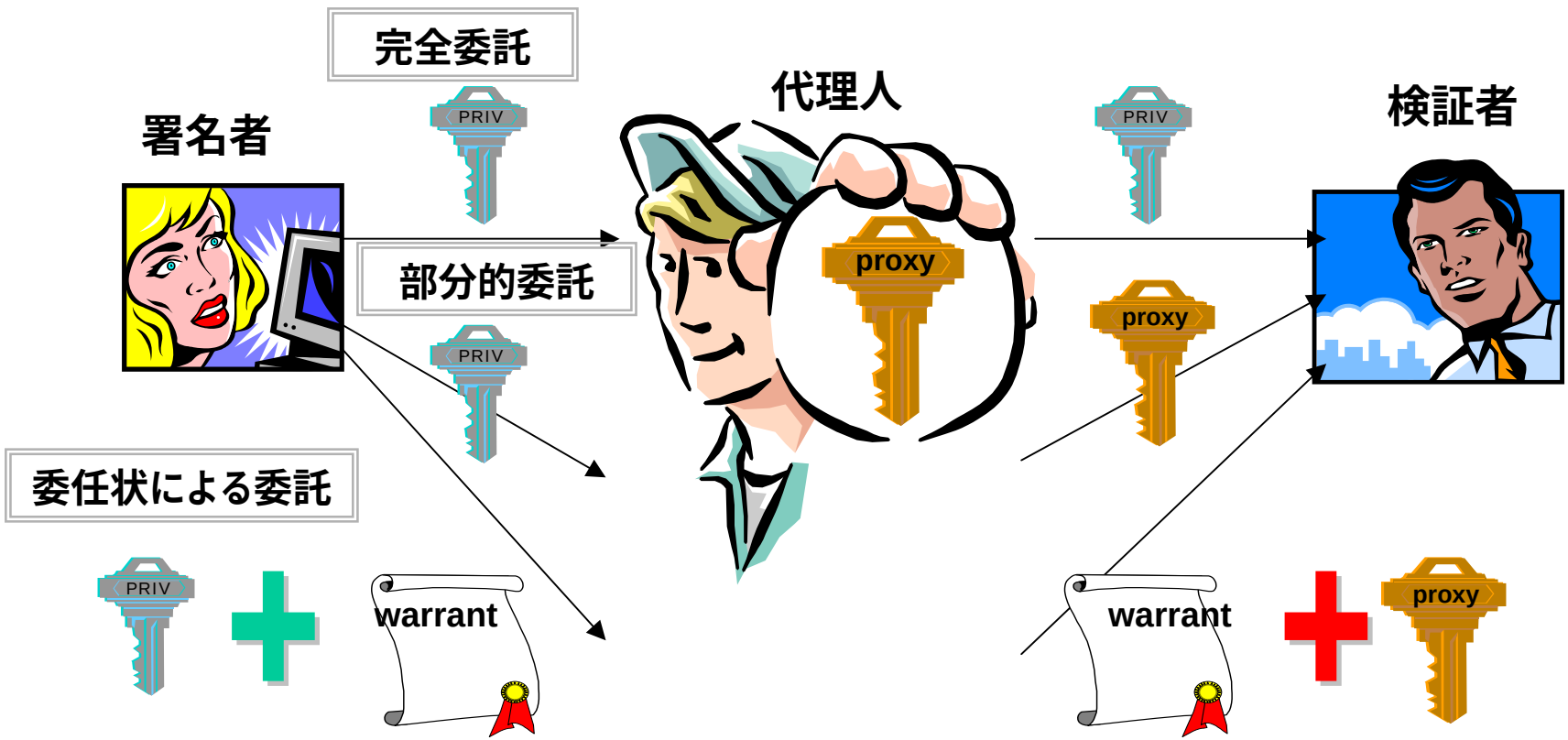


多重署名

- 一つの文書に複数人が署名

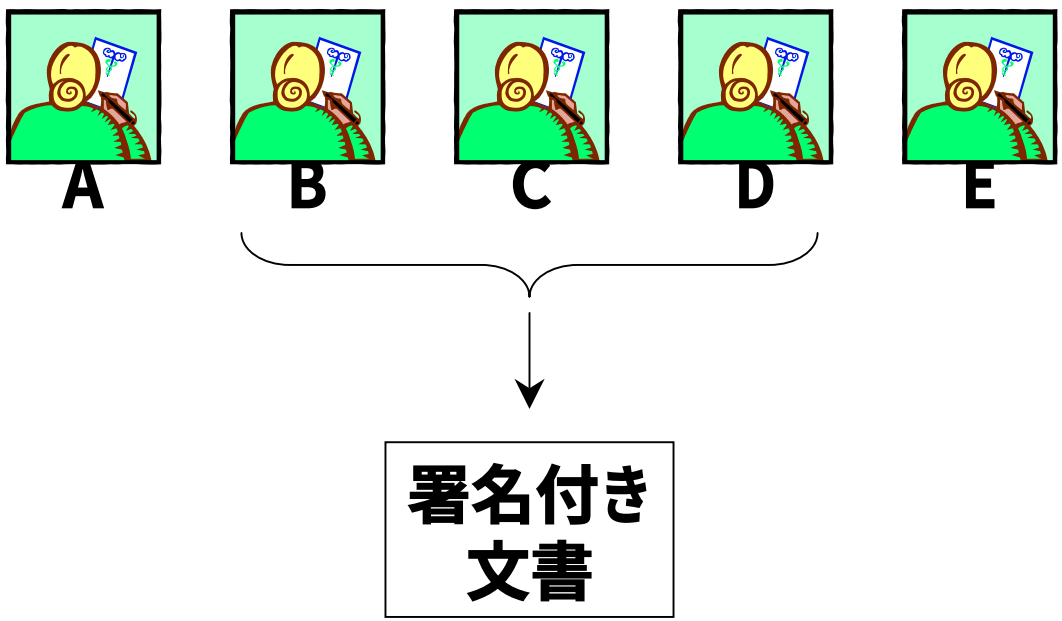


代理署名


完全委託
署名者
PRIV
代理人
PRIV
検証者
proxy
部分的委託
PRIV
proxy
委任状による委託
PRIV
warrant
warrant
proxy

閾値署名

- 閾値以上の人から一つの署名を生成
- 例） (5,3)-閾値署名

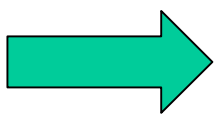


6．今後に向けて

- 電子署名の長期保存
- ヒューマンクリプト
- システムとしての安全性

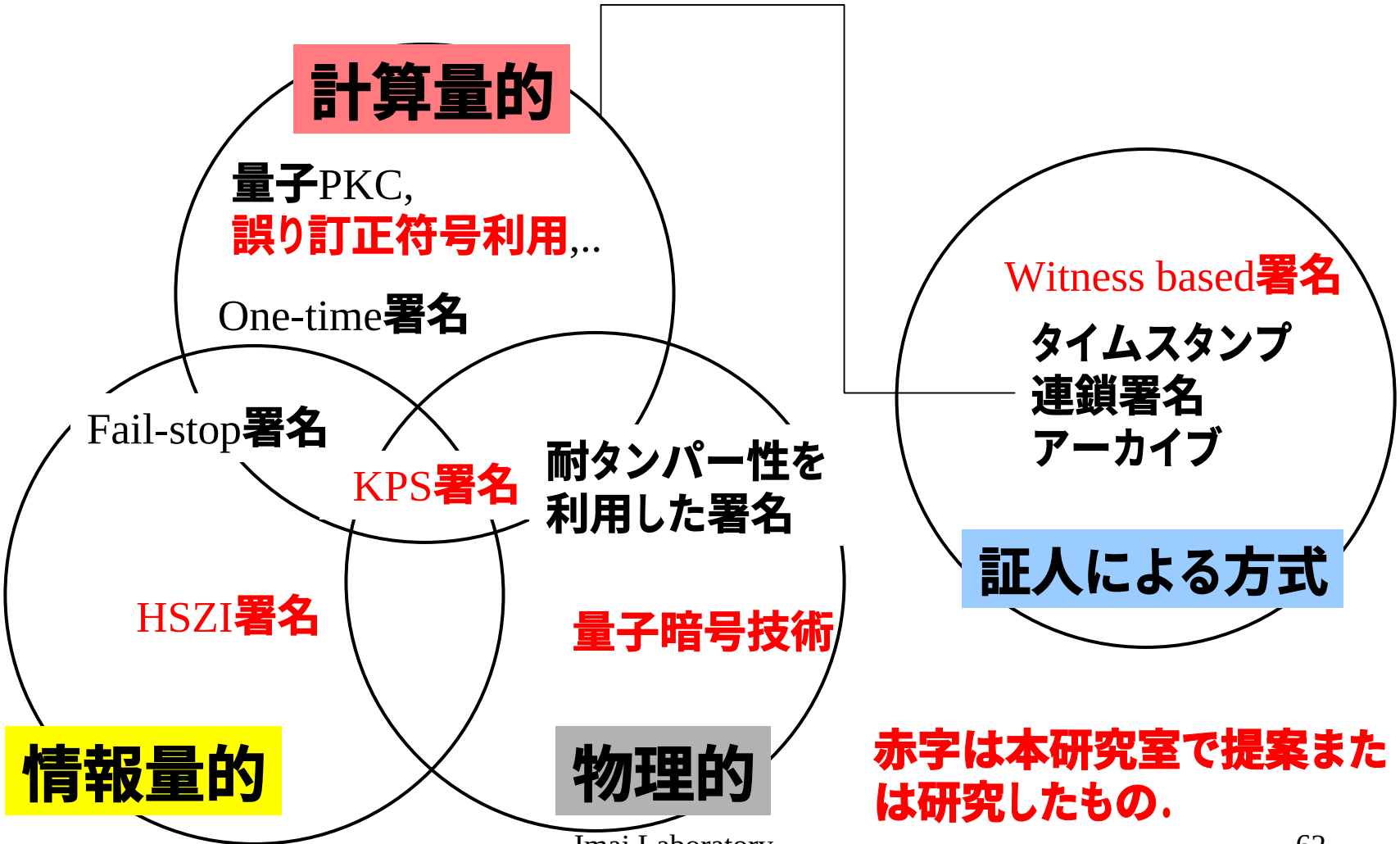
電子署名の長期保存

- 長期にわたる偽造困難性確保の難しさ
  - 計算速度の増加
    - Moore の法則：1年半で計算速度・記憶量2倍
  - 計算機の数の増加
  - アルゴリズムの改良
    - RSA-155(512 bit RSA)の素因数分解　August 99, 8000 mips years
  - 新たな原理に基づく計算法
    - 量子コンピュータ：実用化されればRSA方式も楕円曲線暗号もDSAも多項式時間で解析可能



情報理論的安全性に基づく方式，・・・

長期間安全な可能性のある電子署名



赤字は本研究室で提案または研究したもの.

ヒューマンクリプト

- 電子署名の欠点：署名生成過程の不透明さ
  - 署名している実感が持てない
  - 本当に正しく署名できているのか？
- ユーザーが安心して電子署名を使えるための対策が必要

  例)電子署名ソフトのインターフェースを工夫する

  できた署名を画像として出力する

システムとしての安全性

- 署名システムとしての安全性
  - 署名アルゴリズムの安全性
  - 実装の安全性
  - 鍵管理の安全性
  - 信頼機関の信頼性
  - ヒューマンクリプト･個人認証･本人意志
  - セキュリティ評価
  - ･･･