ディジタル署名

ネットワークと情報セキュリティ6

菊池浩明

CONTENTS

- ディジタル署名の必要性
  - メッセージ認証
- ハッシュ関数
  - 誕生日パラドックス
- 署名アルゴリズム

ディジタル偽札

- ディジタルの特徴
  - コピーしても品質劣化がない
  - コピーにコストがかからない
  - ネットワークで交換できる

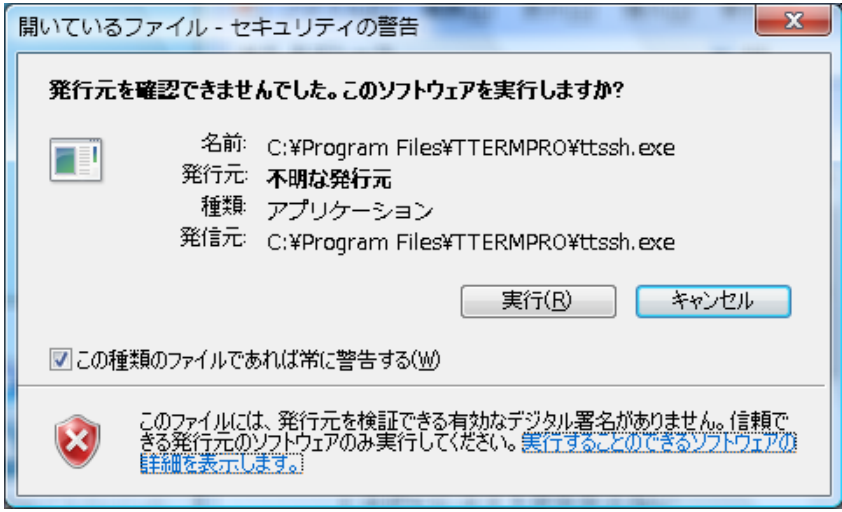
↓

偽造が容易

物理的手段に代わる偽造対策

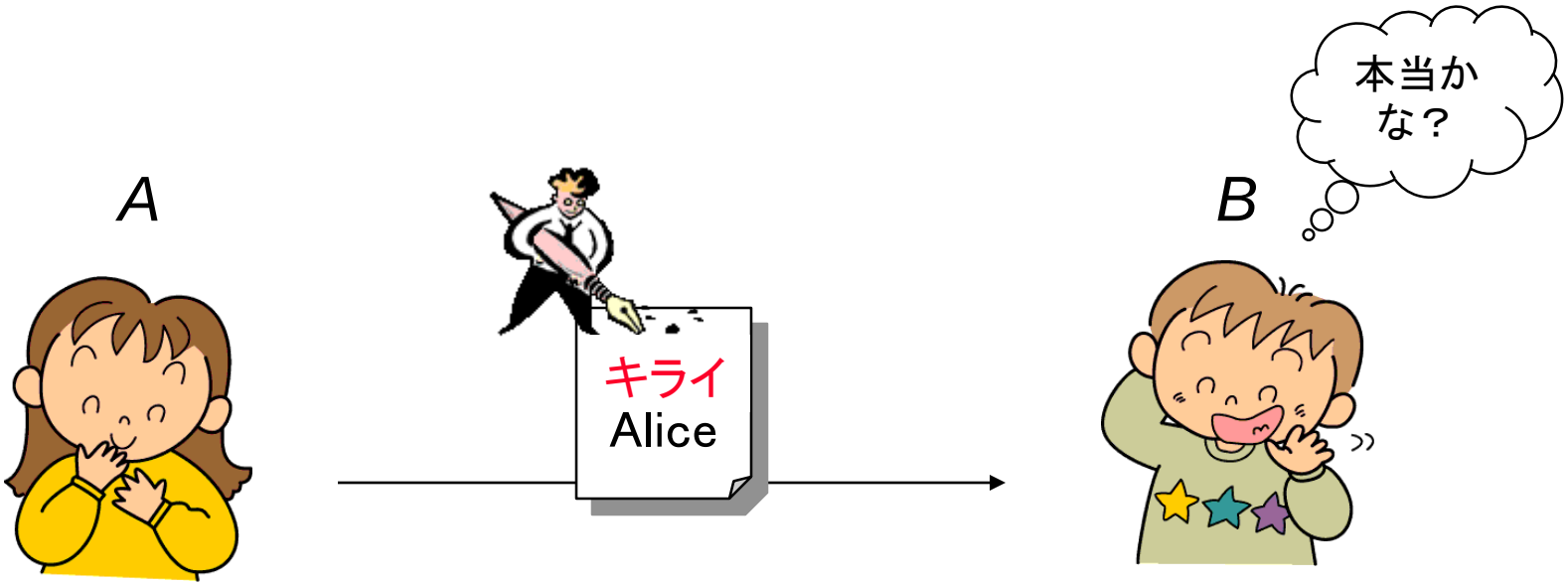
ディジタル署名の応用

- メールの署名
  - 偽造不能な本人の証明(PGP, S/MIME)
- ソフトウェアの製造元証明
  - Code signing コードサイニング
  - Java Signed Applet
- ウェブサイトの偽造対策
  - Oh-o Meiji (SSL/TLS)
- 電子申告
  - E-TAX, PKI



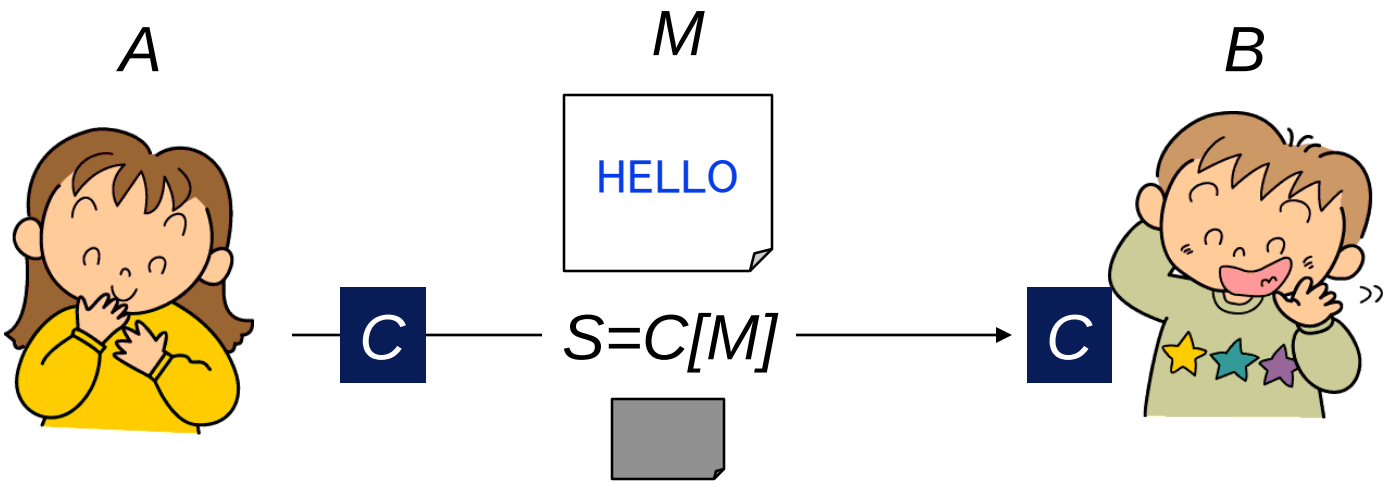
問題 「メッセージ認証」

- 本物であることの証明



案1. メッセージの改ざん防止

- チェックサムC

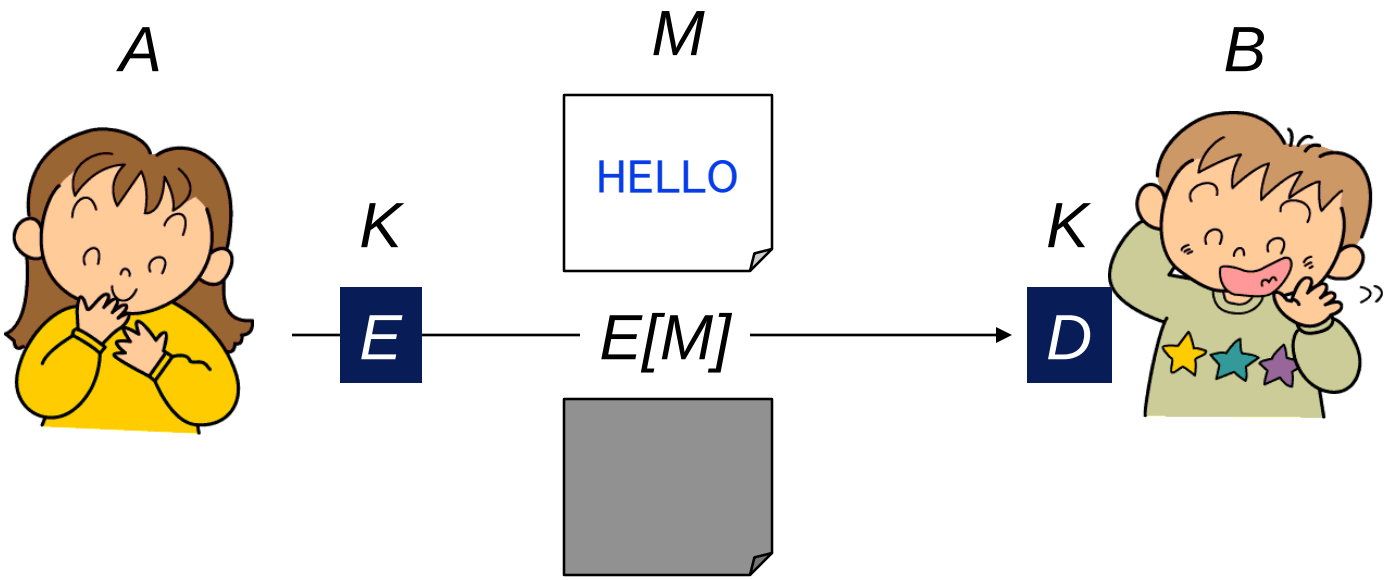


S=H+E+L+L+Oの下位1バイト

欠点： S’ = I + D + L + L +O = S

案2. メッセージの改ざん防止

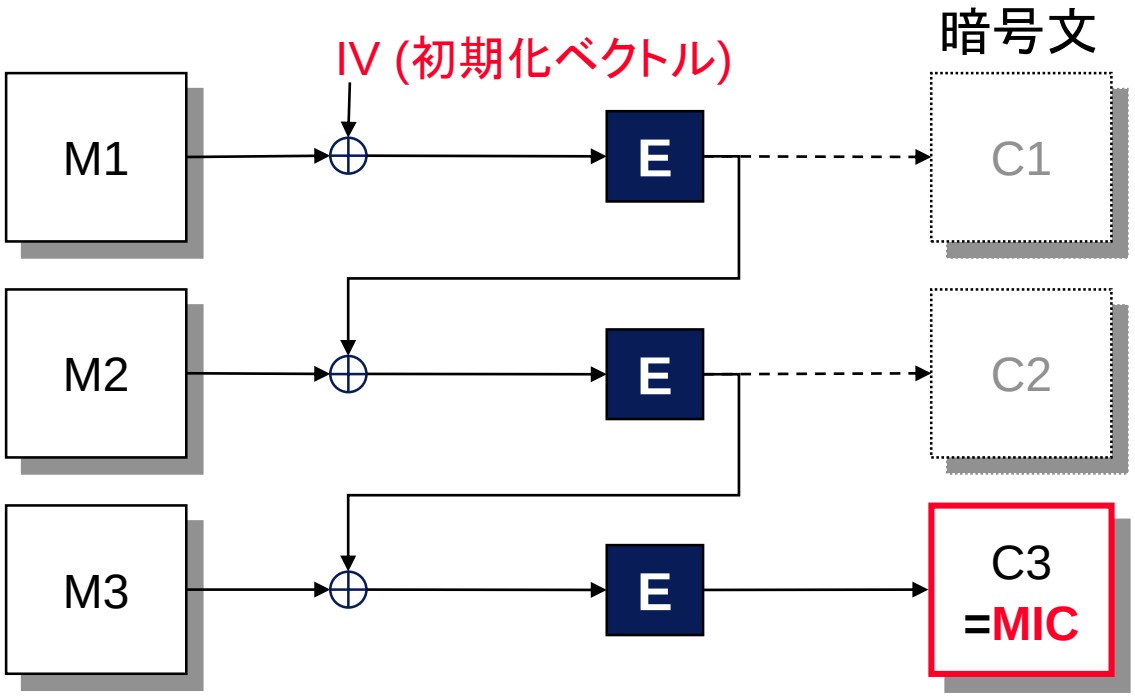
- メッセージの暗号化



欠点： Mの2倍の通信量

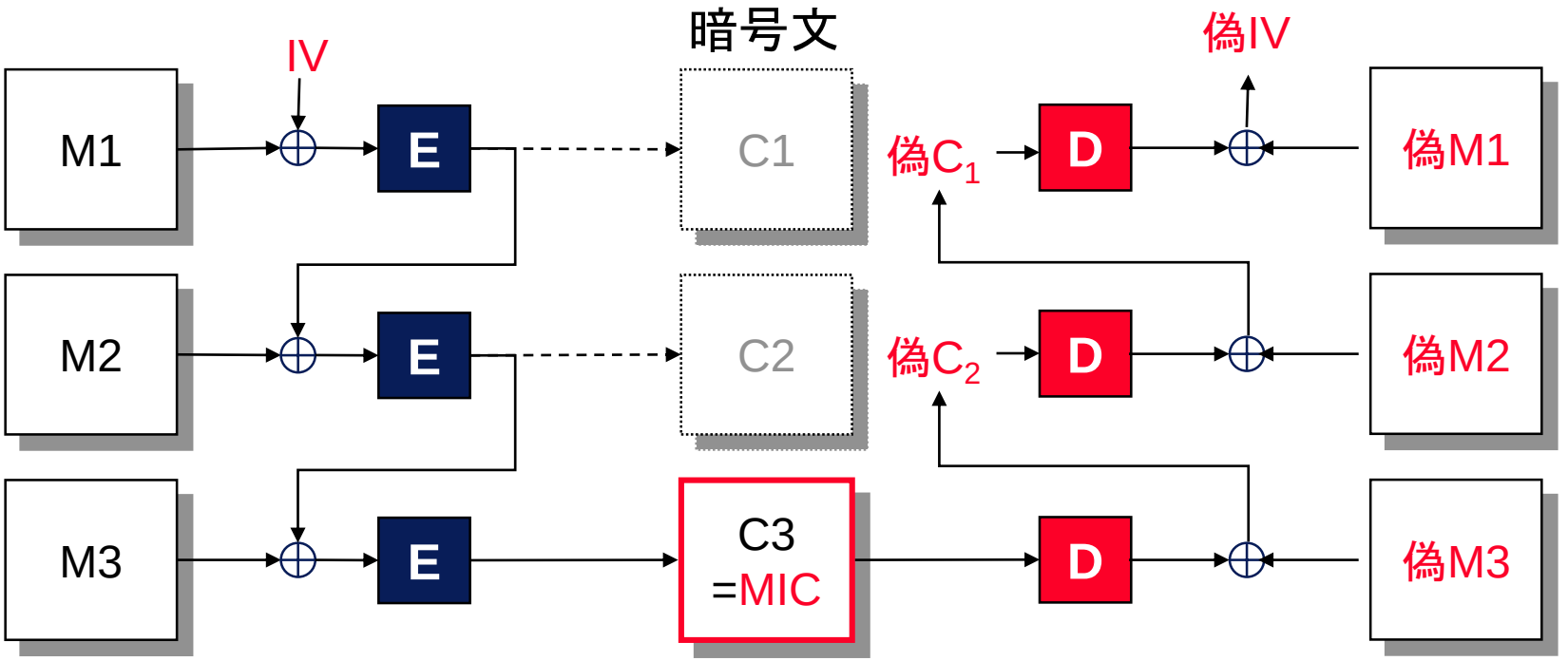
案3. メッセージの改ざん防止

- メッセージ完全性コード
  Message Integrity Code/Check: MIC



MICの問題1: 双方向性

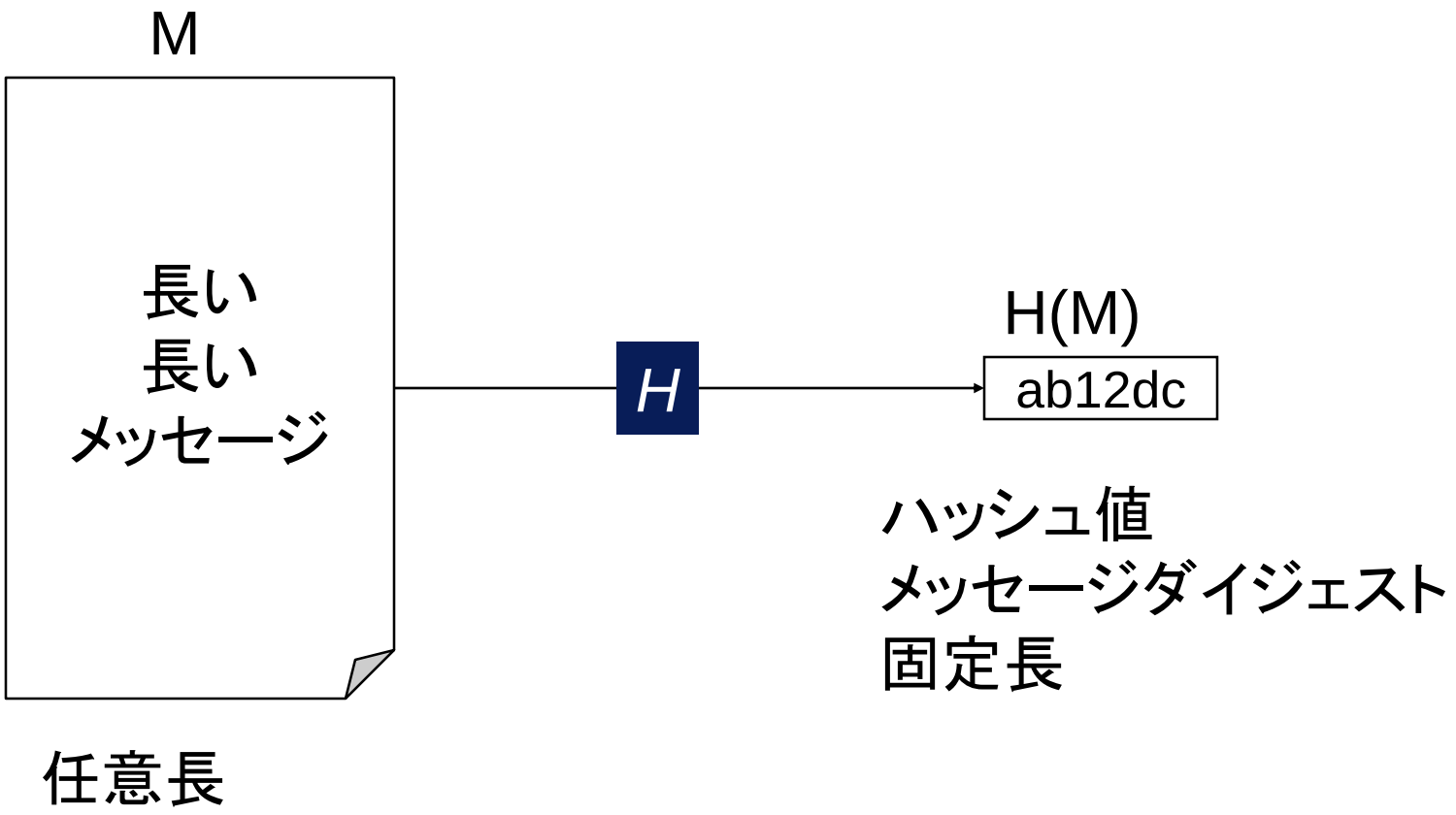
- 送信者による不正
  - MICを変えない文書の偽造



ハッシュ関数

暗号学的ハッシュ関数のしくみ

ハッシュ関数



電子政府推奨暗号

技術分類		名称
公開鍵暗号	署名	DSA
		ECDSA
		RSA-PSS(注1)
		RSASSA-PKCS1-v1_5(注1)
	守秘	RSA-OAEP(注1)
	鍵共有	DH
		ECDH
共通鍵暗号	64ビットブロック暗号(注2)	3-key Triple DES(注3)
	128ビットブロック暗号	AES
		Camellia
	ストリーム暗号	KCipher-2
ハッシュ関数		SHA-256
		SHA-384
		SHA-512
暗号利用モード	秘匿モード	CBC
		CFB
		CTR
		OFB
	認証付き秘匿モード	CCM
		GCM(注4)
メッセージ認証コード		CMAC
		HMAC
エンティティ認証		ISO/IEC 9798-2
		ISO/IEC 9798-3

[1] 総務省政策統括官（情報通信担当）及び経済産業省商務情報政策局長が有識者の参集を求め、暗号技術の普及による情報

ハッシュ

- hash

  [動] 切り刻む，台無しにする

  [名] 細切れ料理

ハッシュポテト

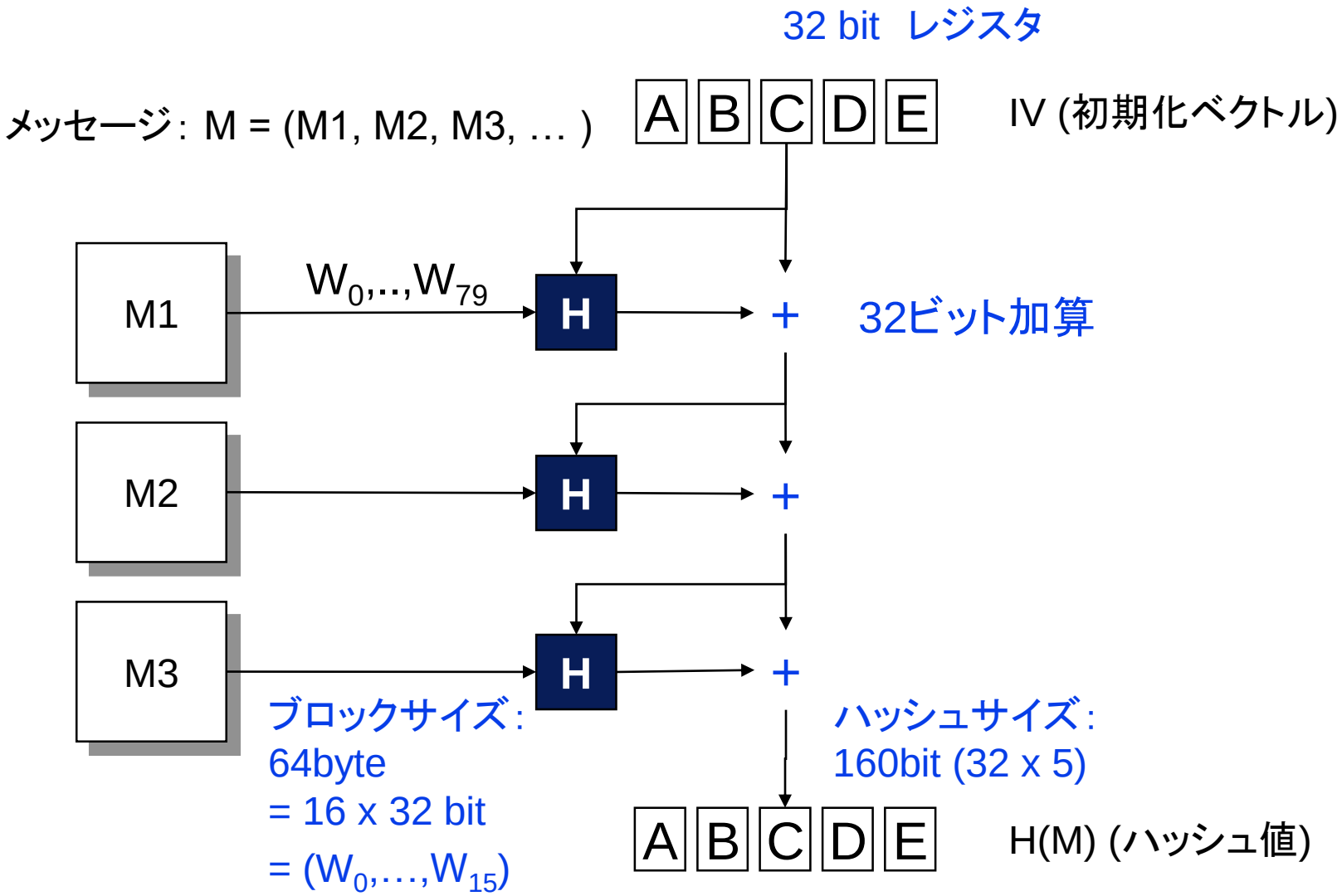
- ハッシュテーブル
  - 検索技術
  - キーの特徴量（チェックサム，先頭文字）

注意: cryptographical hash function とは異なる

ハッシュ関数と共通鍵の違い

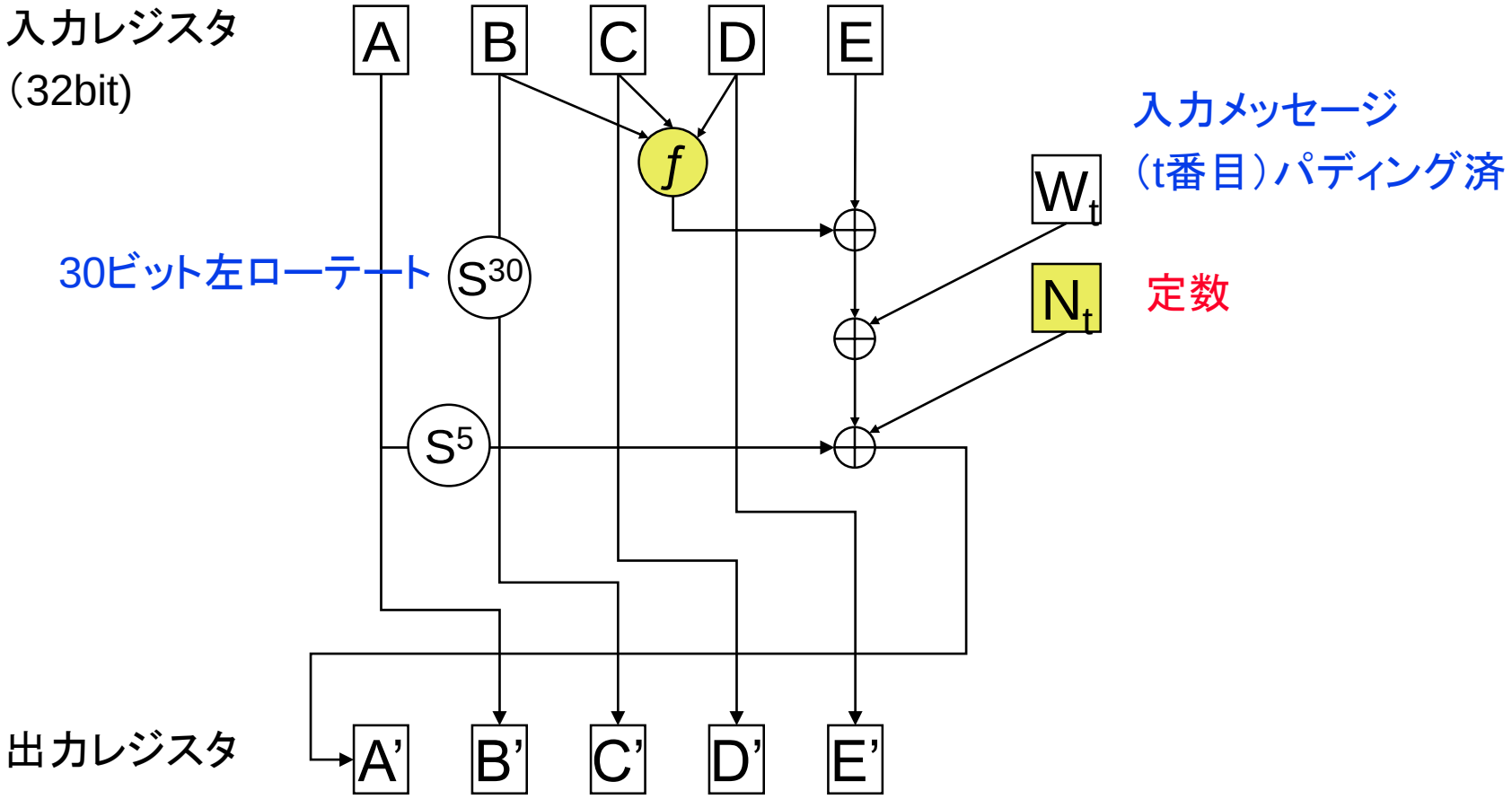
	共通鍵暗号	ハッシュ関数
例	DES, AES	SHA256
基本技術	置換と換字	置換と換字
処理速度	高速	高速
復号化	可能	不能
衝突困難性	不要	必要
秘密鍵	ある	ない ※(keyed hash)

SHAシリーズ – ブロック処理



SHA – メインストリーム

H の中身

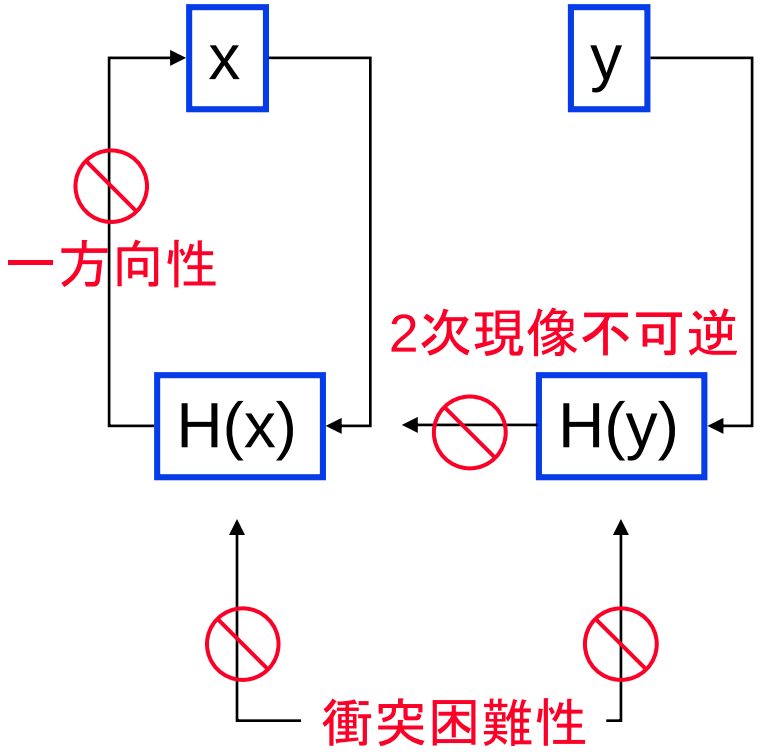


SHA – 論理演算と定数

t (0,…,79)	f(B,C,D)	意味	Nt	意味
0~19	B∧C ∨ ~B∧D	選択	5A82799	$2^{30} \cdot \sqrt{2}$
20~39	B⊕C⊕D	加算	6ED9EBA1	$2^{30} \cdot \sqrt{3}$
40~59	B∧C ∨ B∧D ∨ C∧D	多数決	8F1BBCDC	$2^{30} \cdot \sqrt{5}$
60~79	B⊕C⊕D	加算	CA62C1D6	$2^{30} \cdot \sqrt{7}$

よいハッシュ関数の条件

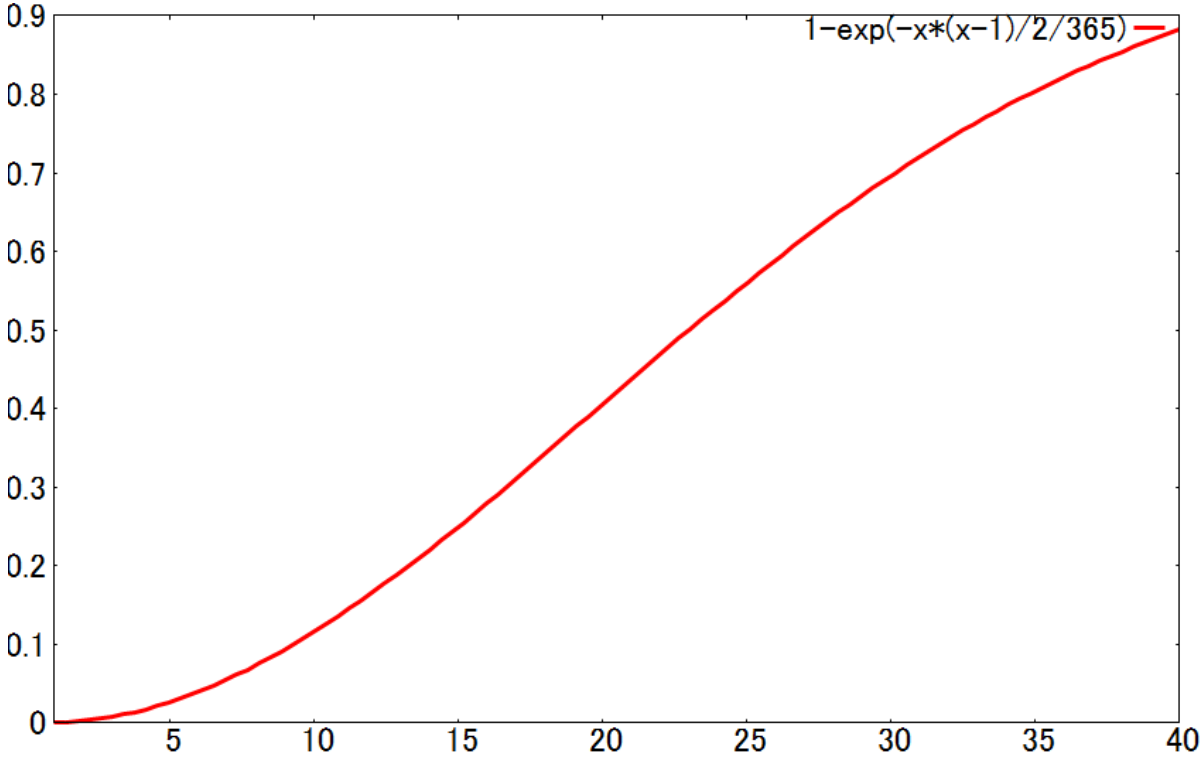
- 安全性条件
  - 一方向性 (one-wayness)
    - » H(x)からH(y)=H(x)を満たすyを求めるのが困難
  - 2次現像不可逆性 (second pre-image resistance)
    - » xから H(y)=H(x)を満たすyを求めるのが困難
  - 衝突困難性 (collision resistance)
    - » H(y)=H(x)を満たすx,yの組を求めるのが困難



誕生日パラドックス

- 問題

「23人以上いれば，その中に同じ誕生日の人がいる確率は50%以上である」



誕生日問題の原理

- 誕生日関数 = k通りの出力 (k = 365)
- ある人が4月1日生である確率: p = 1/k
- 2人が同じ誕生日である確率: $k * p^2 = p$
- 3人(A,B,C)の一組が同じとなる確率: 3p
  - » A=B?, A=C?, B=C?
- n人のグループの一組が同じとなる確率: n^2p
  - » （試行）マッチの数 $m = \frac{n(n-1)}{2} = \frac{n^2 - n}{2}$
  - » m回の試行の「当たり」の回数の期待値 mp
    mp = 1 とすると, $k = m = O(n^2)$
  - » 50%の確率で衝突が起きるのは n = $1.18\sqrt{k} \approx \sqrt{k}$
    n = 1.18 √365 = 22.5 ≈ 23人

バースデーアタック

- メッセージ M1

  菊池拓真様,

  先日行われた中間試験の貴方の成績は80点でした.

- メッセージ M2

  菊池拓真殿,

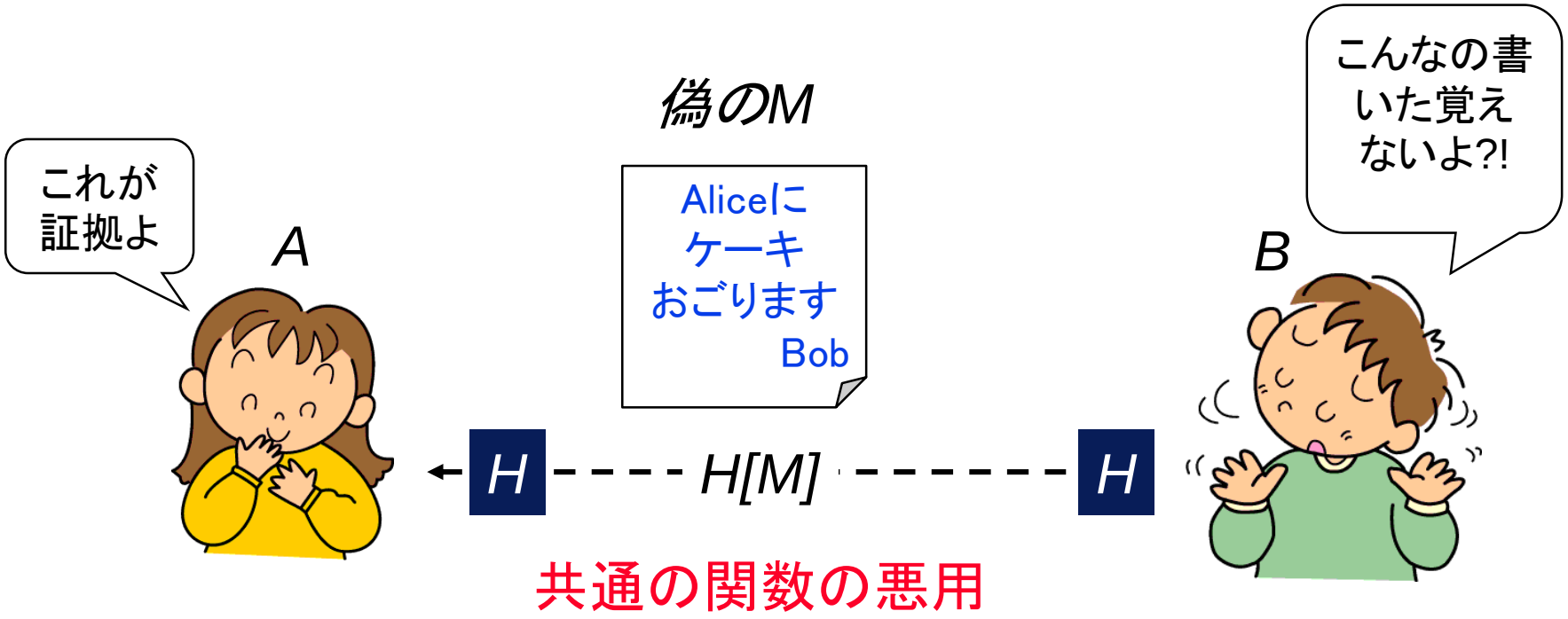
  先日の中間試験のあなたの成績は80点です.

署名アルゴリズム

非対称公開鍵暗号の応用

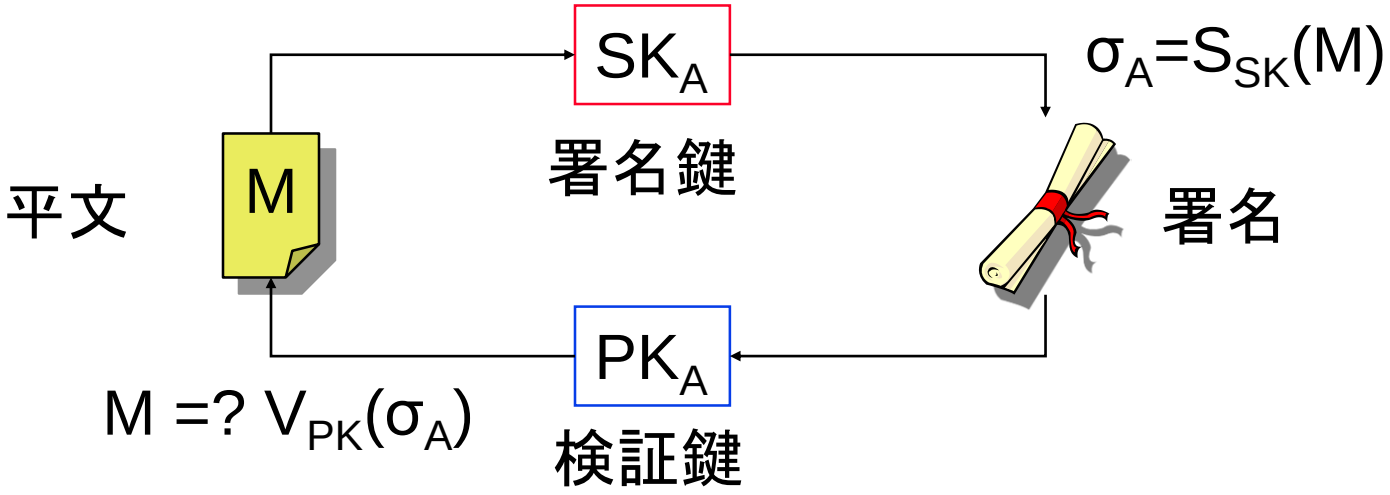
メッセージ認証の問題2： 否認

- 否認不可性 (Non-repudiation)
  - 第三者に対して，（Bは）そのメッセージを作ったことを否定できないこと

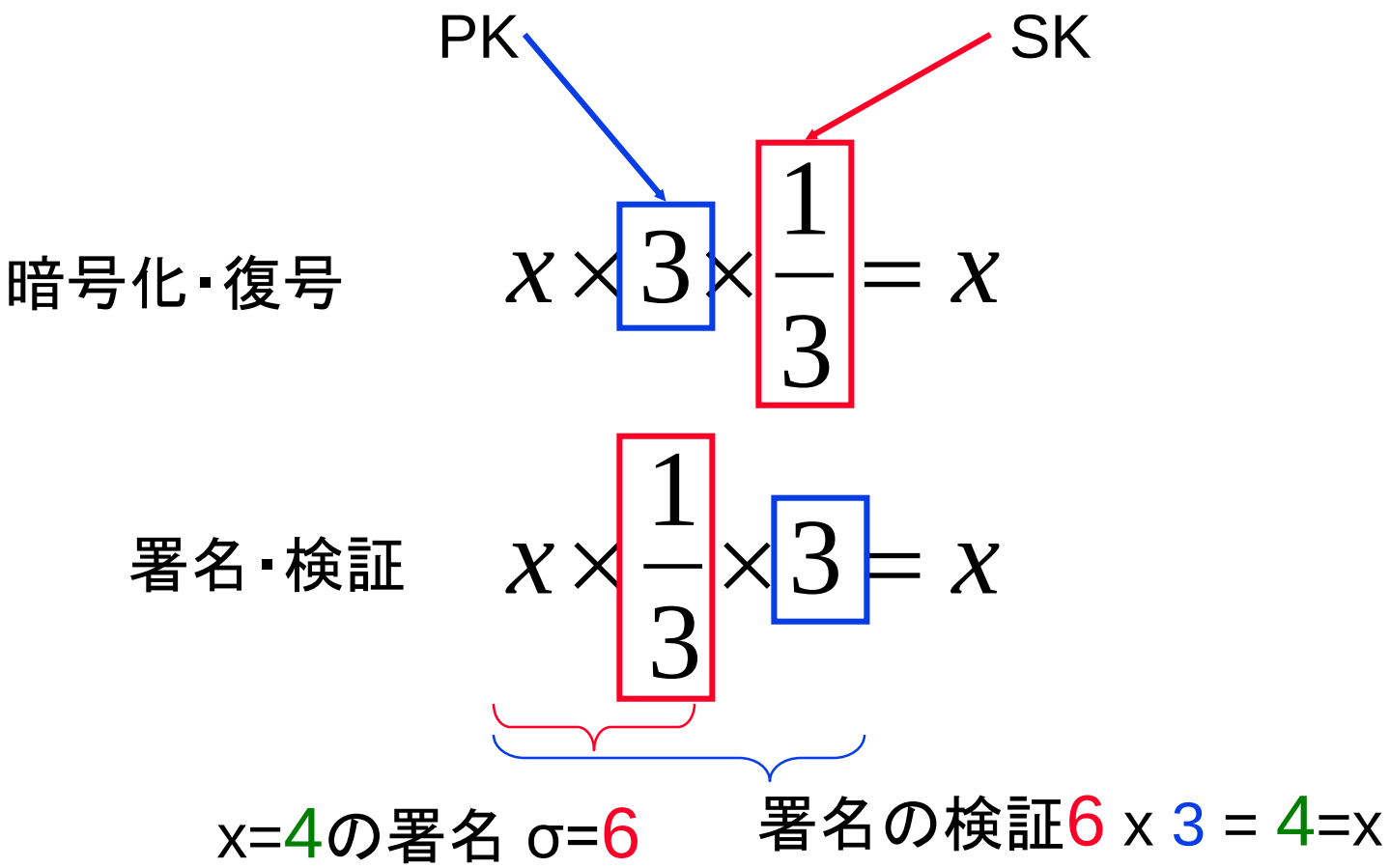


ディジタル署名の原理

- ディジタル署名 (digital signature)
  - メッセージの真の発信者である証明
  - (署名鍵を持たない)他人による偽造不能
  - (公開鍵を持つ)誰もが検証可能



ディジタル署名のイメージ



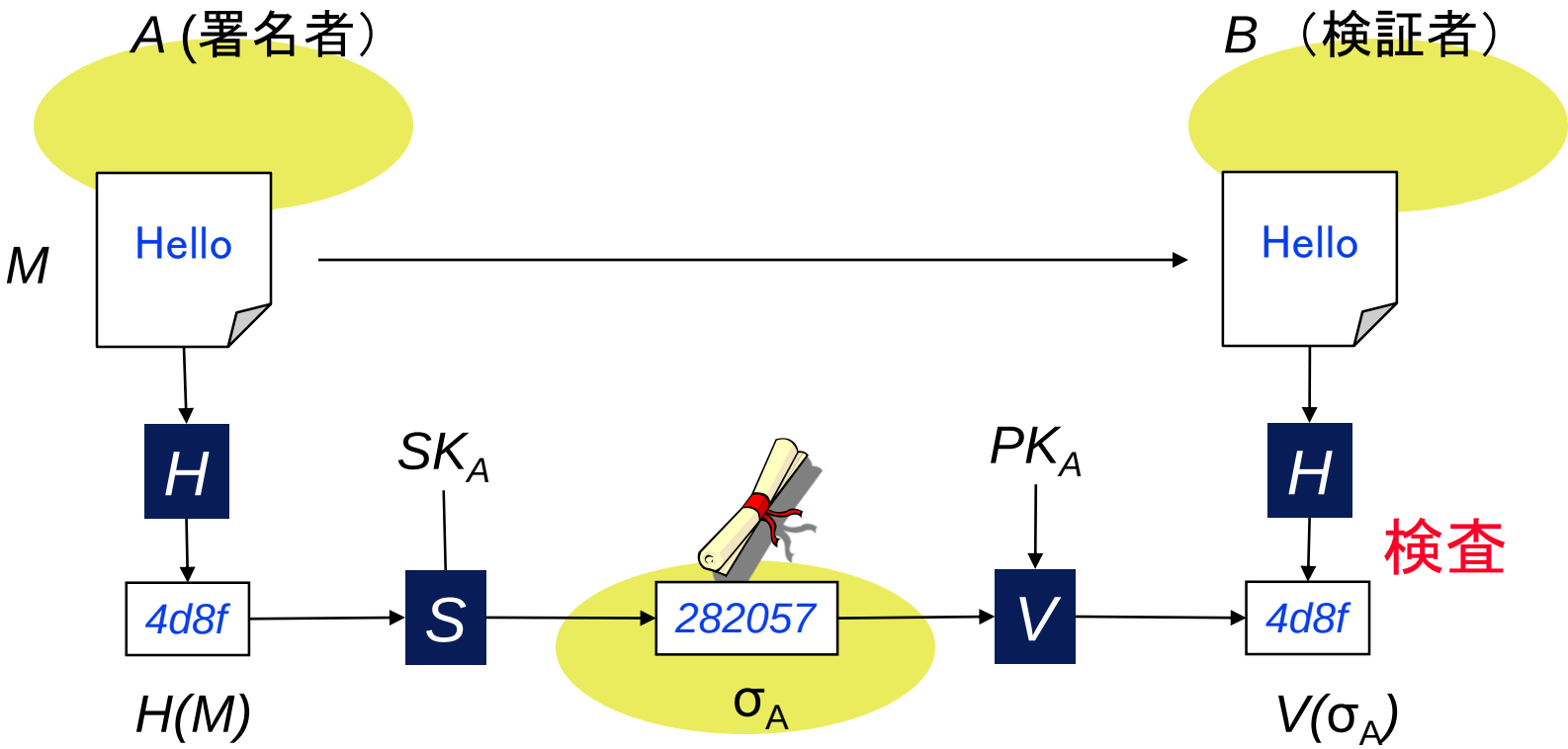
署名アルゴリズム

名称	発表年	提案者	原理	特徴
DSA	1991	NIST	DLP	Java applet, エルガマル
シュノア	1991	C. Schnorr	DLP	ゼロ知識証明
ニバーグ・リュッペル	1996	Nyberg, Rueppel	DLP	メッセージ回復形
RSA	1978	Rivest, Shamir, Adelman	IF	SSL, PKI
ESIGN	1992	T. Okamoto	IF	高速，NTT

電子政府推奨暗号

技術分類		名称
公開鍵暗号	署名	DSA
		ECDSA
		RSA-PSS(注1)
		RSASSA-PKCS1-v1_5(注1)
	守秘	RSA-OAEP(注1)
	鍵共有	DH
		ECDH
共通鍵暗号	64ビットブロック暗号(注2)	3-key Triple DES(注3)
	128ビットブロック暗号	AES
		Camellia
	ストリーム暗号	KCipher-2
ハッシュ関数		SHA-256
		SHA-384
		SHA-512
暗号利用モード	秘匿モード	CBC
		CFB
		CTR
		OFB
	認証付き秘匿モード	CCM
		GCM(注4)
メッセージ認証コード		CMAC
		HMAC
エンティティ認証		ISO/IEC 9798-2
		ISO/IEC 9798-3

ディジタル署名（ハッシュ関数）



MのAによる署名

RSA署名

- 鍵

  公開鍵 PK: $n = pq$, e

  秘密鍵 SK: $d = e^{-1} \bmod \lambda(n)$

- 署名

  $\sigma = H(M)^d \bmod n$

- 検証

  $H(M) =? \sigma^e \bmod n$

DSA署名（ElGamal署名）

- 鍵

  秘密鍵 SK: x in Z_q

  公開鍵 PK: $y = g^x \bmod p$, g = 位数qの生成元

- 署名

  $r = (g^k \bmod p) \bmod q$, ただしk は Z_qの乱数

  $s = (H(M) + xr)/k \bmod q$

  $\sigma = (r, s)$

- 検証

  $v = g^{H(m)/s} y^{r/s} \bmod p$,

  v =? r をテスト

公開鍵暗号と署名アルゴリズム

アルゴリズム	暗号化	署名
DH	Yes	No
エルガマル	Yes	No
DSA	No	Yes
RSA	Yes	Yes

暗号化と復号が可逆
D[E[m]]=E[D[m]]

演習

- 0から255までの値を出力する8 bitのハッシュ関数 H: $\{0,1\}^* \rightarrow \{0,1\}^8$がある.
  1. あるメッセージmが H(m) = 1 となる確率p_1.
  2. ある2組のm_1とm_2が $H(m_1) = H(m_2)$となる確率p_2.
  3. H(m) = 1となる，mを見つけるための平均試行回数 k_1.
  4. （50%の確からしさで）衝突を見つけるために必要なメッセージ集合の平均サイズk_2

まとめ

- MICやMACなどによりメッセージの完全性を保証する技術を（　　）という.
- ハッシュ関数には，関数を不可逆にする（　　）性，二次現像不可能性，バースディパラドックスに関わる（　　）性の必要条件がある.
- RSA署名などにより保証される送信者が送信の事実を否定できない性質を（　　）性という.