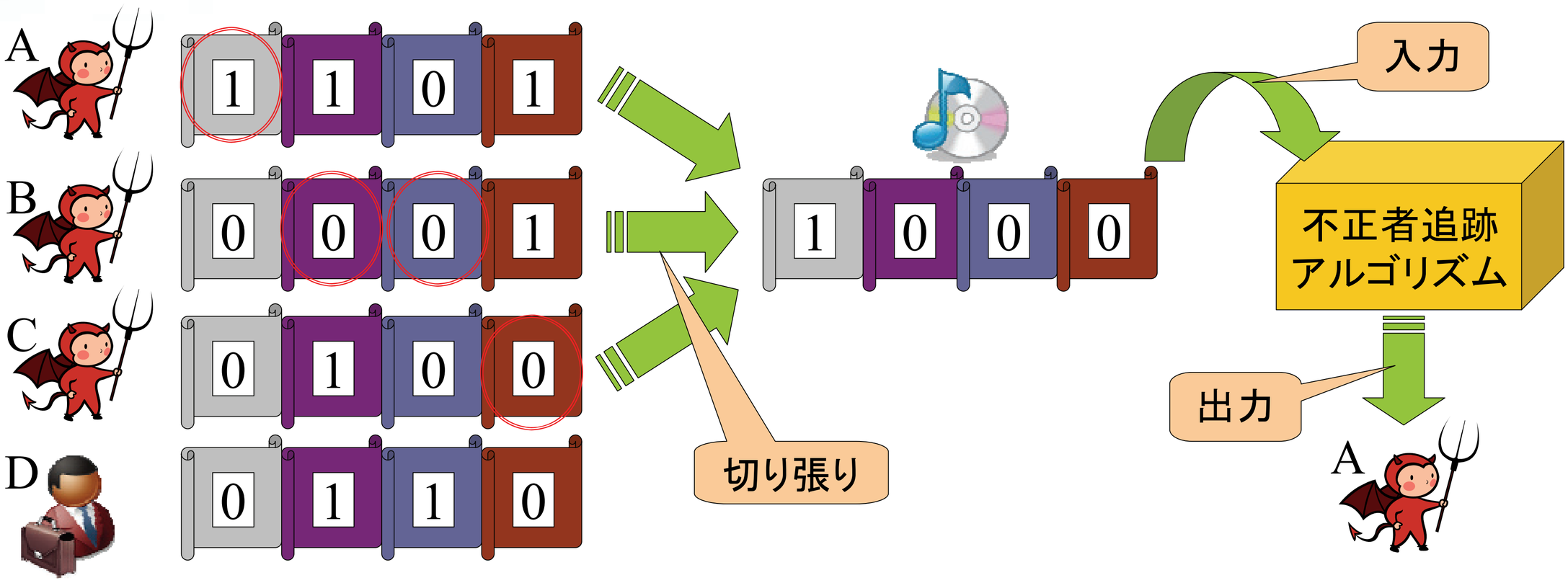
# Collusion-secure codes under more realistic assumptions

物理解析研究チーム　縫田　光司（NUIDA, Koji）

- Collusion-secure code（結託耐性符号）
  - 電子コンテンツ（動画、音楽等）の不正再配布者を特定する技術要素
  - ユーザ毎に符号語を埋め込み、再配布された際に再配布主特定の目印とする
  - 複数のコンテンツの「切り張り」による攻撃（結託攻撃）に耐性を持つ
    - 通常は、その方式が耐え得る攻撃者数の最大値を予め設定




- マーキング仮定 [Boneh-Shaw 1995] ・・・従来研究の標準的な仮定
  - 攻撃者が異なるビットを持っている場所は、自由に切り張り・情報消去できる
  - 全攻撃者のビットが一致する場所（「検知不可ビット」）は攻撃後も変化しない

- 従来研究における標準的仮定の問題点
  - 現実には検知不可ビットの消失・反転も生じ得る（ランダムノイズ、部分的消去）
  - 攻撃者の最大人数を事前に見積もるのが難しい

- 結果１：無実ユーザの誤検出（false-positive）が極めて起きにくい方式
  - 攻撃者が２人以下、かつマーキング仮定成立時には誤検出確率ゼロ
  - 攻撃者が３人以上、かつマーキング仮定不成立でも誤検出確率を抑えられる
    - 数値例：ユーザ数１０万、符号長１３０ビットのとき、
      - 特定失敗確率（攻撃者２人以下、マーキング仮定成立時）０．０００１％
      - 攻撃者１５３人以下なら、マーキング仮定不成立でも誤検出確率０．２％

- 結果２：検知不可ビットの消失・反転が起きても特定が可能な方式
  - 数値例：ユーザ数１０万、符号長３７８ビット、攻撃者２人以下のとき、各検知不可ビットの消失誤り確率１０％または反転誤り確率５％でも特定失敗確率０．０１％

National Institute of Advanced Industrial Science and Technology
AIST

Research Center for Information Security

# Collusion-secure codes under more realistic assumptions

情報セキュリティ研究センター（RCIS）
縫田　光司

National Institute of Advanced Industrial Science and Technology
AIST

# 研究の背景

Research Center for Information Security

- 各種コンテンツの電子データ化
  - 例：動画、音楽、文書
- 複製・配布のコスト低下
  - 利便性の大幅な向上
  - ユーザによる不正な複製・再配布の増加

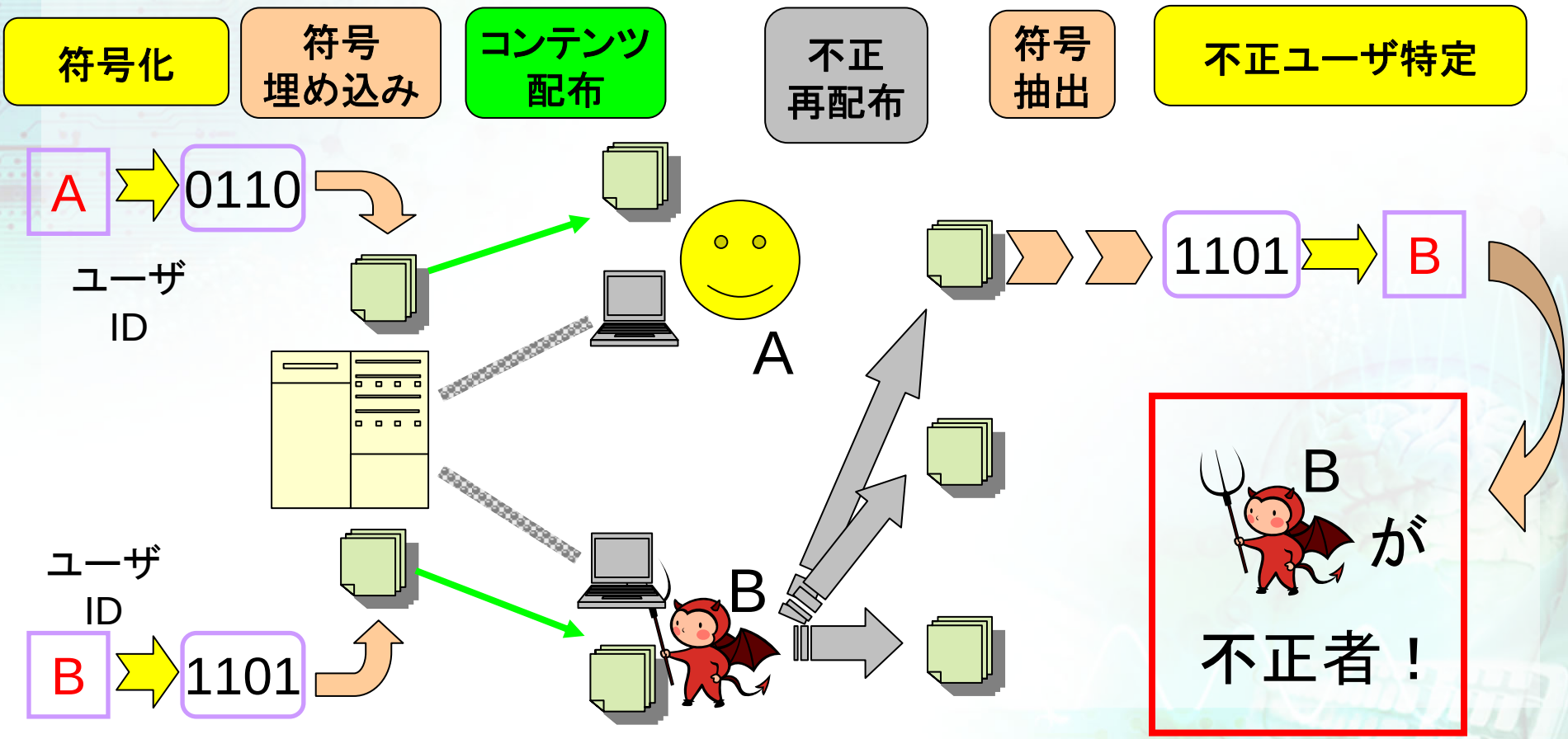

- 電子指紋方式：上記の問題解決法の一つ
  - 再配布を行ったユーザの特定

National Institute of Advanced Industrial Science and Technology AIST

Research Center for Information Security

# 電子指紋方式

- ユーザ特定の目印(符号語)を予め埋め込む

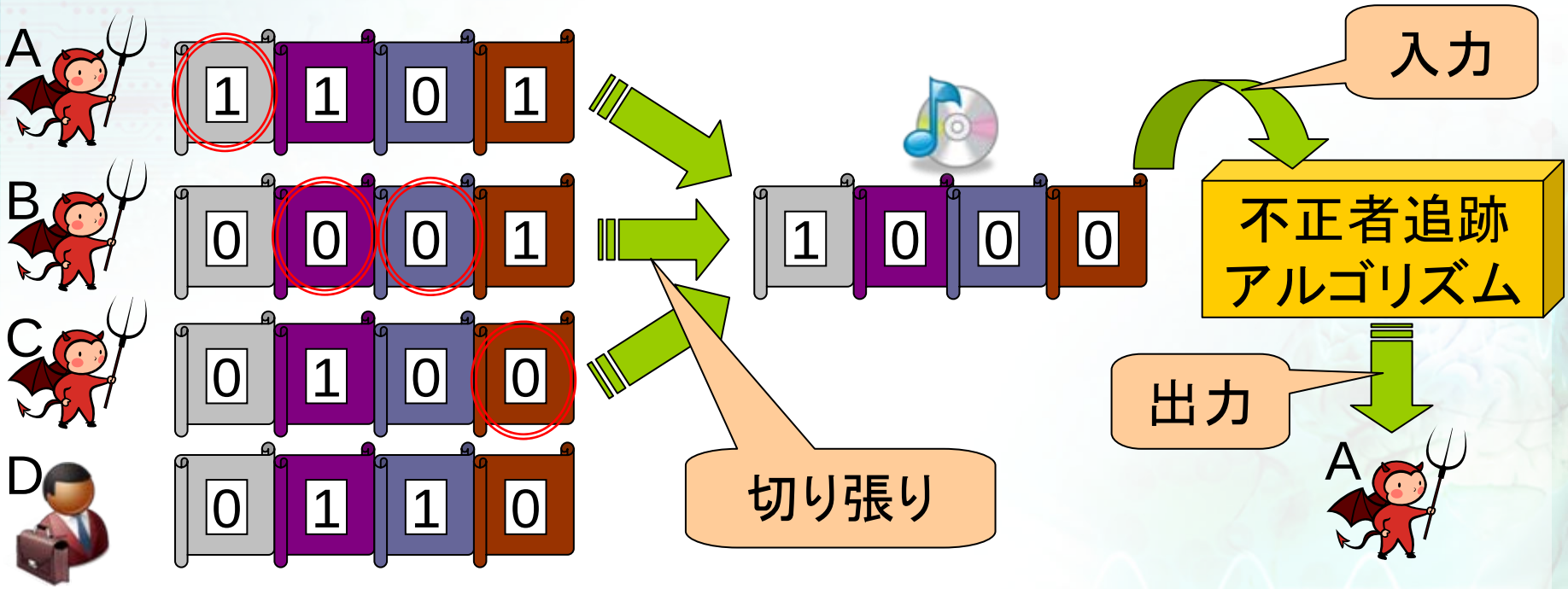


National Institute of Advanced Industrial Science and Technology
AIST

# 結託耐性符号

Research Center for Information Security

- 複数のコンテンツの「切り張り」による攻撃に耐性を持つ符号化・不正者特定方式



National Institute of Advanced Industrial Science and Technology AIST

# 標準的仮定とその問題点

Research Center for Information Security

従来研究での標準的仮定[Boneh-Shaw 1995]

- 攻撃者全員のビットが一致する位置(「検知不可位置」)は、改竄も消去もされない

  ⇒ 現実には改竄や消去も生じ得る(攻撃者によるランダムノイズ付加、コンテンツ部分消去など)

- 攻撃者の最大人数を予め設定する

  ⇒ 現実には攻撃者の最大人数の見積もりは困難

⇒ **より弱い仮定下での構成・安全性解析**

National Institute of Advanced Industrial Science and Technology
AIST

# 結果1：誤特定を防ぐ方式

Research Center for Information Security

- 誤特定（false-positive）と特定漏れ（false-negative）のうち、誤特定については弱い仮定の下でも起こりにくい方式を提案
- 数値例：ユーザ数10万、符号長130ビット、攻撃者数153人以下のとき、誤特定確率0．2%以下を理論的に証明
  - 特定失敗確率は、攻撃者2人以下で0.0001%

**K. Nuida, "*An Improvement of Short 2-Secure Fingerprint Codes Strongly Avoiding False-Positive*", to appear in Information Hiding 2009**

National Institute of Advanced Industrial Science and Technology AIST

# 結果2：改竄・消去に強い方式

Research Center for Information Security

- 検知不可ビットの反転・消去が起こる（従来より現実的）状況でも、誤特定と特定漏れの両方を起こりにくくする方式を提案
- 数値例：ユーザ数10万、攻撃者数2人以下のとき、各検知不可ビットの消失確率10%（または反転確率5%）の状況で、符号長378ビットで特定失敗確率0．01%以下を理論的に証明

（国際学会へ投稿中）