技術を社会へ
Integration for Innovation

National Institute of
Advanced Industrial Science
and Technology
AIST

独立行政法人
産業技術総合研究所

RCIS 情報セキュリティ研究センター
RCIS (Research Center for Information Security)

電子指紋技術に用いる符号の設計と安全性評価

縫田　光司（NUIDA, Koji）
産総研RCIS　物理解析研究チーム　研究員

RCIS Workshop 2008, 2008/05/16

あらすじ

- 研究の背景と目的
- RCISにおける研究体制
- 主な研究成果
  - 2006年度以前
  - 2007年度
- デモ展示のご案内（@NHK技研公開）
- まとめ、今後の方針

研究の背景と目的

研究の背景(1)

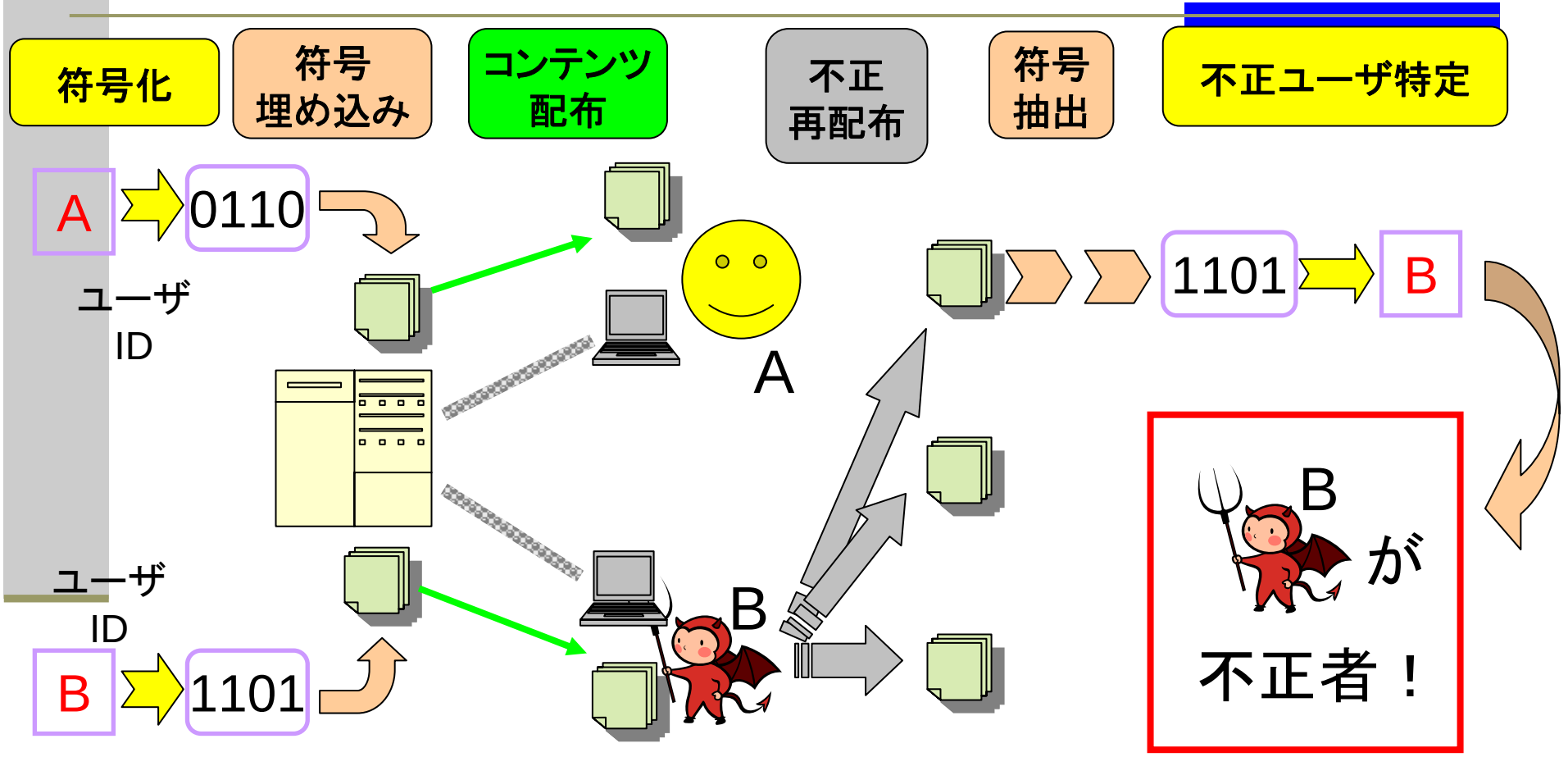
- 各種コンテンツの電子データ化
  - 例:動画、音楽、文書
- 複製・配布のコスト低下

  → 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

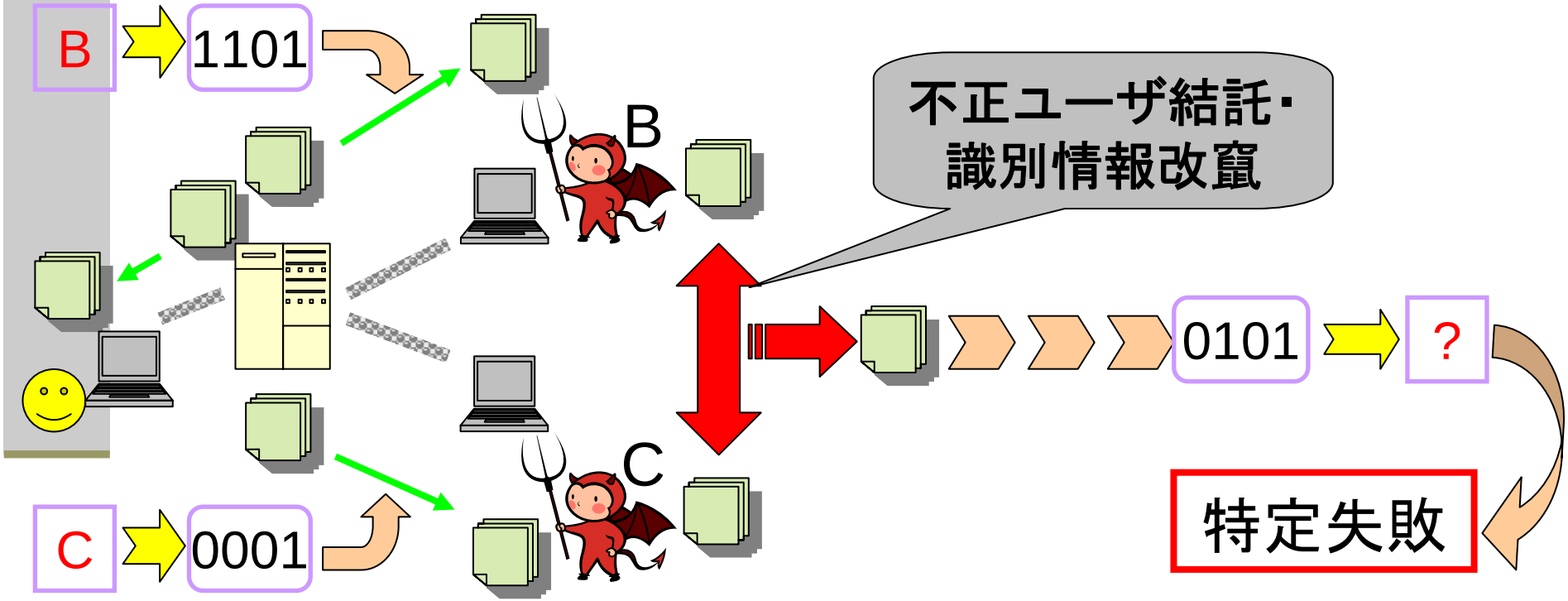
電子指紋方式の図



単独ユーザによる識別情報改竄は困難

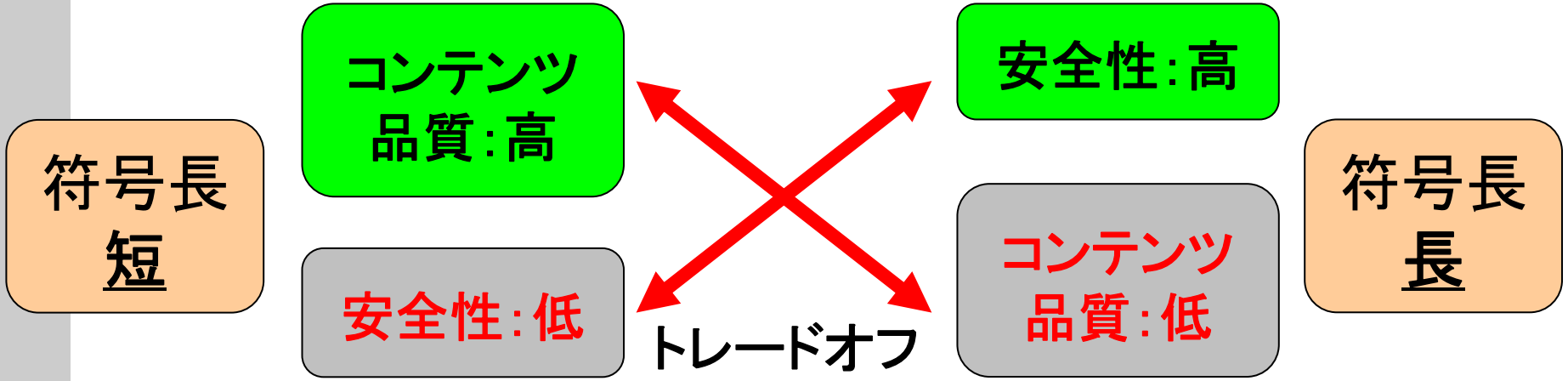
結託攻撃

複数ユーザの結託による識別情報改竄



結託耐性符号：結託攻撃に耐性を持つ符号

研究の背景(2)



- 従来法:実用には長すぎる符号長が必要
  (例:数千～数万ビット)
- 研究テーマ:安全性と実用性の両立

研究体制

研究体制(1)

RCISでは、ソフトウェア、量子物理技術を含むハードウェア、基盤
活動だけでなく他チームと協力し合いながら、幅広い視点から総
ます。

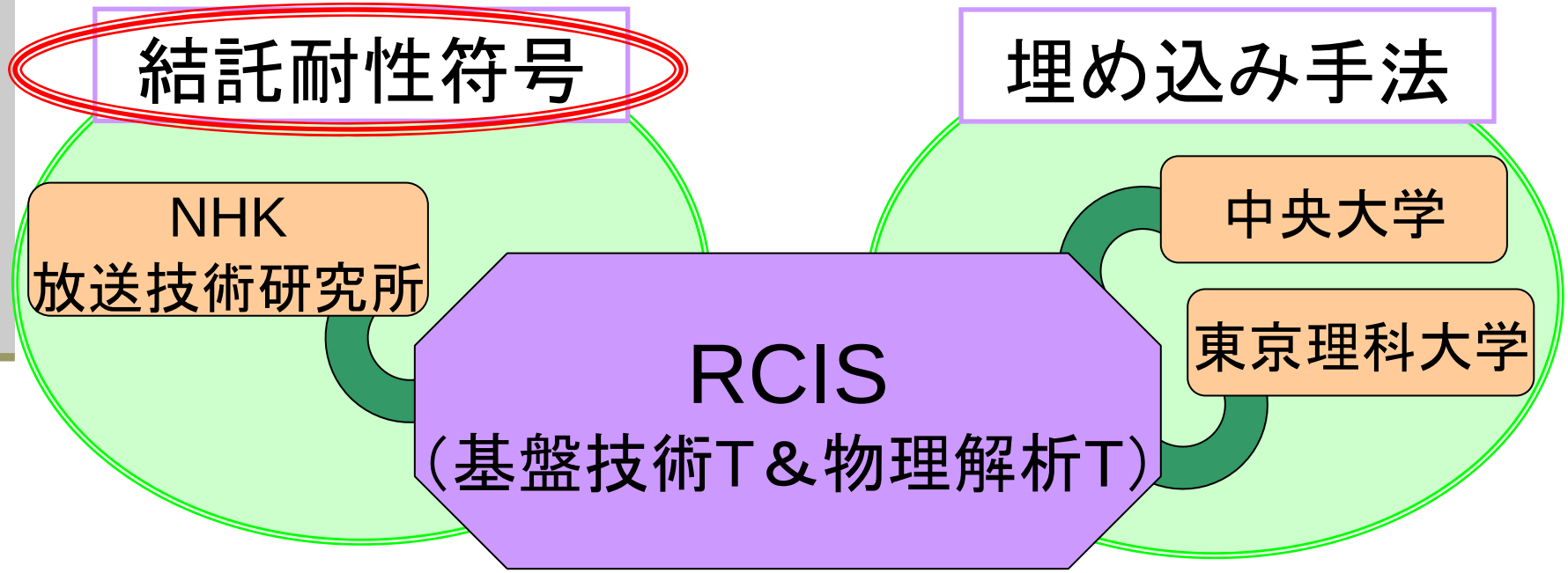
主な研究テーマ

- 暗号・セキュリティ基盤技術分野
  - 情報漏えいに堅牢な暗号・認証方式
  - 情報セキュリティインシデントの実践的調査研究
  - プライバシ保護に関する研究
  - IDベース暗号に関する研究
  - バイオメトリクスセキュリティに関する研究
  - 電子透かし用結託耐性符号に関する研究

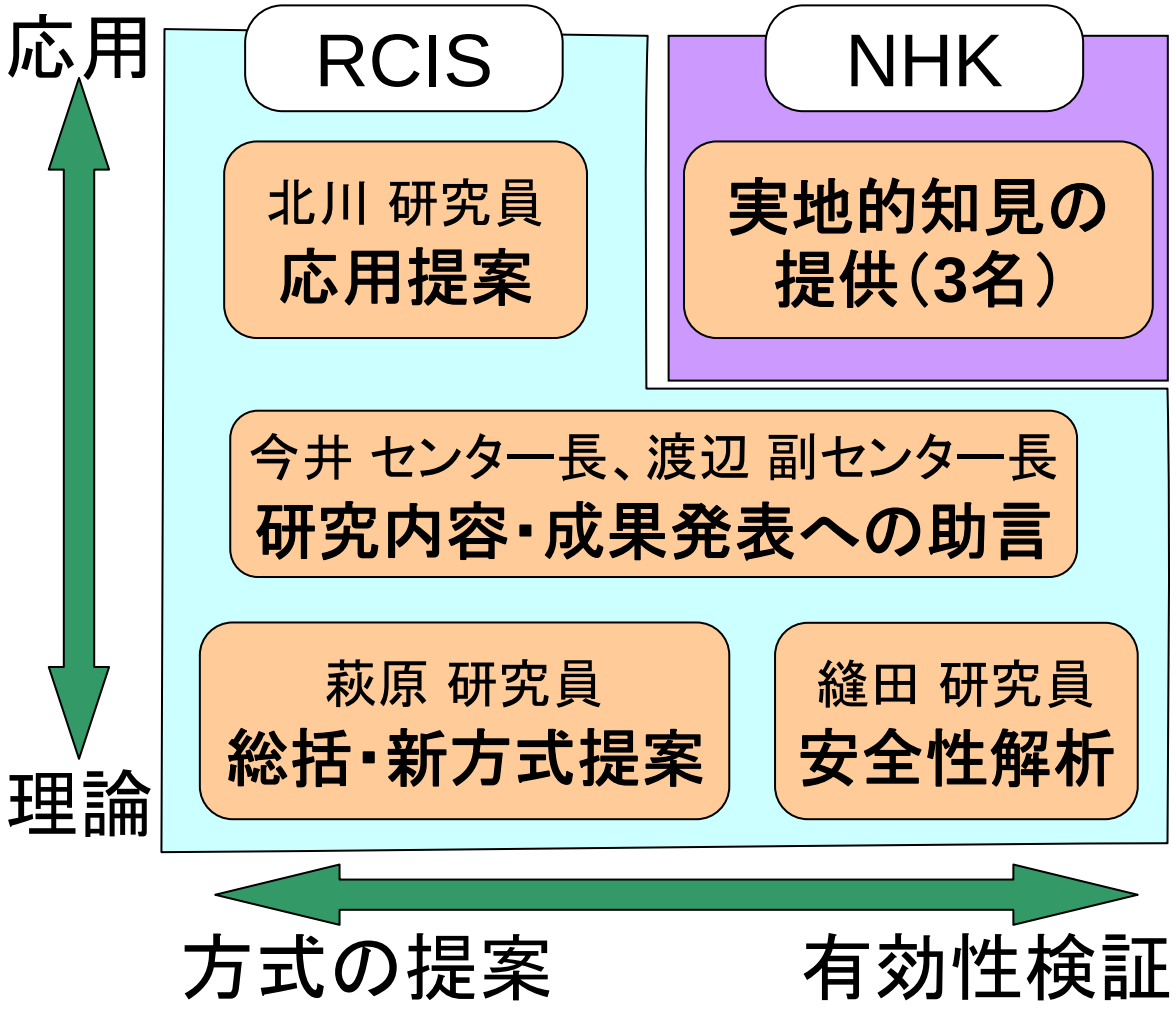
http://www.rcis.aist.go.jp/project/index-ja.html

研究体制(2)

研究テーマ:符号長の短い、実用的な
結託耐性符号の開発と安全性評価



研究体制(3)



外部資金
(終了分含む)

- 経済産業省
研究開発事業
- 科研費
(若手(B))
- 国際科学技術
財団　助成金

等

主な研究成果

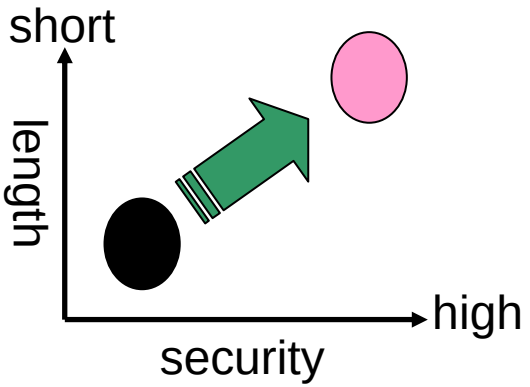
成果1:実用的符号長での実現

従来法:実用には長すぎる符号長が必要

- 例:ユーザ数10,000人、最大結託人数2人、特定誤り確率10^{-3} ⇒ 符号長**6,800ビット**

成果: **100～200ビット長程度の符号提案**

短い符号長と
高い安全性の両立



実用的符号長での実現（1）

IEEE CCNC 2007 DRM Workshop

- 結託人数2人以下なら、**誤特定（冤罪）は発生しない**
- ユーザ数10,000人、最大結託人数2人、**100ビット**
  - ⇒ 誤り確率**8.2×10^{-4}**
- ユーザ数1,000人、**100ビット**、**結託人数任意**
  - ⇒ 冤罪確率**1.6×10^{-4}**

極めて高い安全性

実用的符号長での実現(2)

(方式提案)*SCIS 2007*, *IFIPTM 2007 IH Workshop*

(安全性証明)*SCIS 2008*

★:2007年度

- 前方式よりも大幅に**計算量削減**
- ユーザ数10,000人、最大結託人数2人、**100ビット**
  - ⇒ 誤り確率**3.4×10^{-6}**
- ユーザ数100,000人、最大結託人数2人、**128ビット**
  - ⇒ 誤り確率**7.2×10^{-8}**

高い安全性と実用的計算量の両立

成果2:符号の実用性向上

- 従来の代表的方式:ランダム符号、生成したパラメータの記憶に**大容量のメモリが必要**
- 改竄アルゴリズムについてある性質を仮定

成果:

- 必要な記憶容量の**最適化**
- より**現実的仮定**で安全性証明
- **符号長の削減**

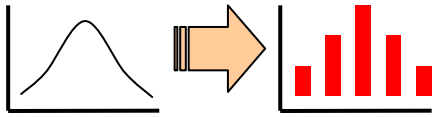
実用的観点からの研究

符号の実用性向上(1)

AAECC-16（LNCS 3857）, *IH 2007*（LNCS 4567）★

★：2007年度

- ランダム符号に適した確率分布の特定と構成
  - 必要な**記憶容量の最適化**
  - **符号長の削減**
  - コンピュータ上で**厳密な実装が可能**



- 例：パラメータ記憶に要する記憶容量の変化
  - **48.5**キロバイト → **0**バイト （**0%**）
  - **200**キロバイト → **2.5**キロバイト （**1.25%**）

符号の実用性向上（2）

AAECC-17（LNCS 4851）★

★：2007年度

- 従来方式の改良

  ⇒ 符号長の削減

- より弱い仮定の下で安全性証明

  ⇒ 安全性・実用性向上

例：ユーザ数百万人、最大結託4人、誤り確率0.1%

符号長　33,600ビット ⇒ 1774ビット　（5.28%）

実用性と安全性の向上

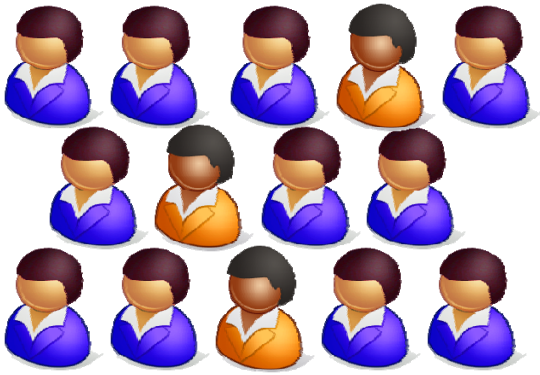
成果3: 多人数結託への対応

- 多人数結託耐性には**膨大な符号長**が必要
- 成果1を一般化 → **計算量の爆発的増加**

成果: **計算量の増加を軽減する新手法提案**

（「グループテスティング」の応用）

他分野の知見を
情報セキュリティに応用



多人数結託への対応

HISC 2007, *SCIS 2008*, *SCIS 2008*

★ :2007年度

- ユーザ数100人、最大結託**3人**、符号長**128ビット**

  誤り確率**1.0×10^{-4}**

  計算量 : 成果1の応用に比べて**6.3%**

短い符号長で多人数結託への耐性を初めて実現

National Institute of Advanced Industrial Science and Technology
AIST
技術を社会へ
Integration for Innovation

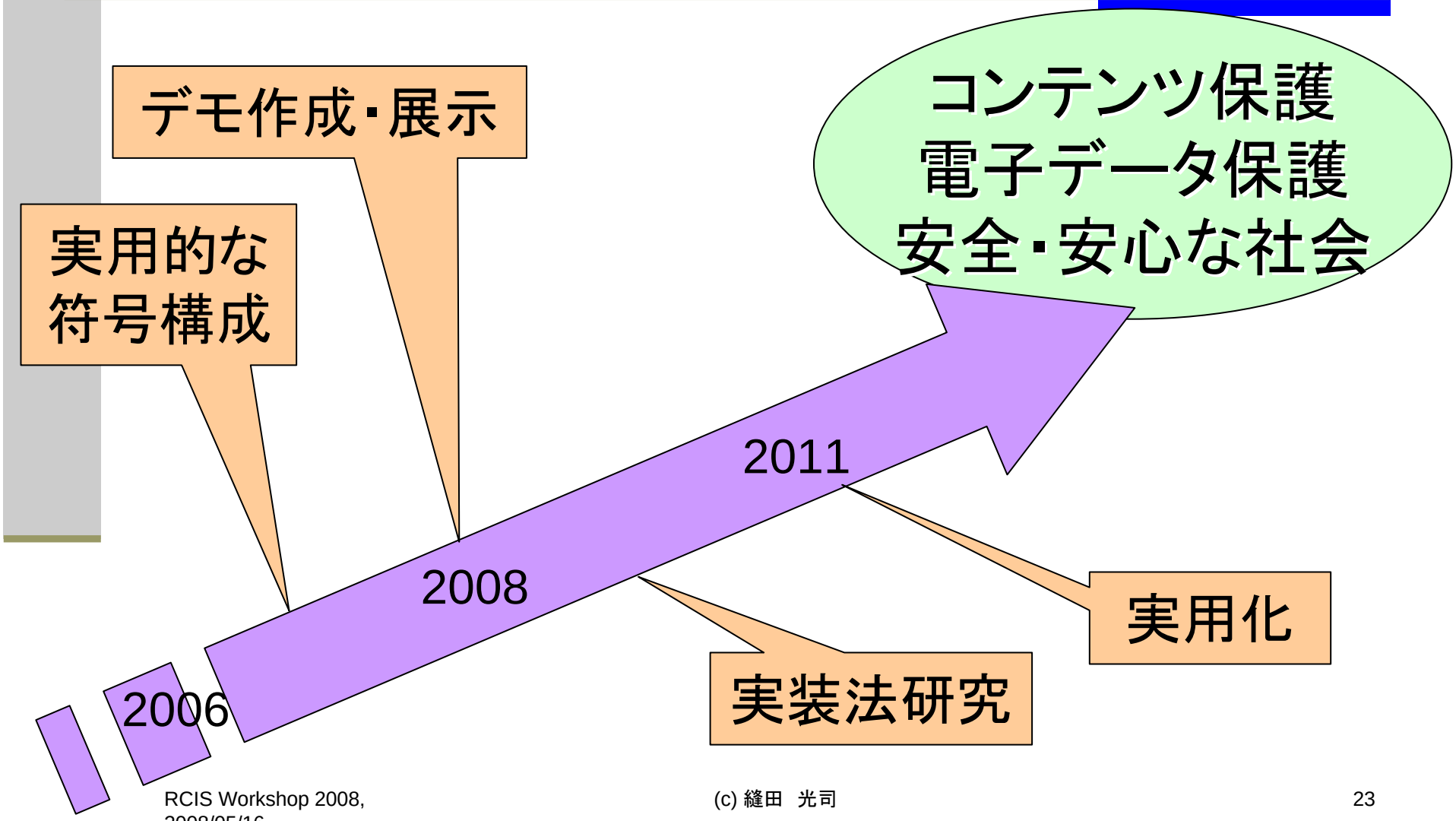
情報セキュリティ研究センター
RCIS (Research Center for Information Security)

デモ展示のご案内

デモ展示@NHK技研公開

NHK放送技術研究所「技研公開2008」にて、
結託耐性符号の性能体験ソフトを展示予定

まとめ、今後の方針


デモ作成・展示
実用的な
符号構成
コンテンツ保護
電子データ保護
安全・安心な社会
2011
2008
2006
実用化
実装法研究

ご清聴ありがとうございました

National Institute of
Advanced Industrial Science
and Technology
AIST

技術を社会へ
Integration for Innovation

情報セキュリティ研究センター
RCIS (Research Center for Information Security