情報セキュリティ研究センター

より高度に安全な実用的公開鍵暗号方式

産総研RCIS 花岡 悟一郎

主たる成果: ほとんどの(実用的)既存方式よりも高度に安全で、実用性も併せ持つ公開鍵暗号方式を実現した。

より詳しくは…

IND-CCA安全性を、CDH仮定のみに基づいて証明可能で、なおかつ、暗号文サイズがCramer-Shoup暗号[1]のものと等しい公開鍵暗号方式を提案した。

背景

従来の実用的公開鍵暗号が依拠する数学的仮定:

- DDH仮定 (CS,KD暗号等)
- BDH仮定 (BMW暗号等)
- GDH仮定 (Kiltz暗号等)

しかし、いずれの仮定も…

- 10年程度の歴史のみ (CDH仮定は約30年)
- CDH仮定より真に強い

実現の困難さ

CDH仮定に基づく方式の実現のためには…

従来の方法論[1]では判定問題(例: DDH問題)に強く依存。

方法論自体の再構築が必要。

新たな方法論・方式

放送暗号の概念を介した、新たな方法論[2]を提示。

- ほとんど**すべての既存方式**を説明可能
- さまざまな**新方式**も創出可能。

その一例が

CDH仮定に基づく新方式[2]

秘密鍵: $f(x)=a_0+a_1x+a_2x^2+a_3x^3$

公開鍵: $g, g^{a0},\cdots,g^{a3}$

KEM: $C = (g^r, g^{r\cdot f(g^r\|0)}, g^{r\cdot f(g^r\|1)})$

$K = g^{a0r}$

復号: 整合性を確認し、$K = (g^r)^{a0}$

比較

	|C| − |M|	数学的仮定
CS暗号[1]	480 bit	DDH仮定
提案方式[2]	480 bit	CDH仮定

[1] Cramer, Shoup, CRYPTO'98, [2]Hanaoka, Kurosawa, ASIACRYPT'08

http://www.aist.go.jp
独立行政法人 産業技術総合研究所

National Institute of
Advanced Industrial Science
and Technology
AIST

Research Center for
Information Security

より高度に安全な
実用的公開鍵暗号方式

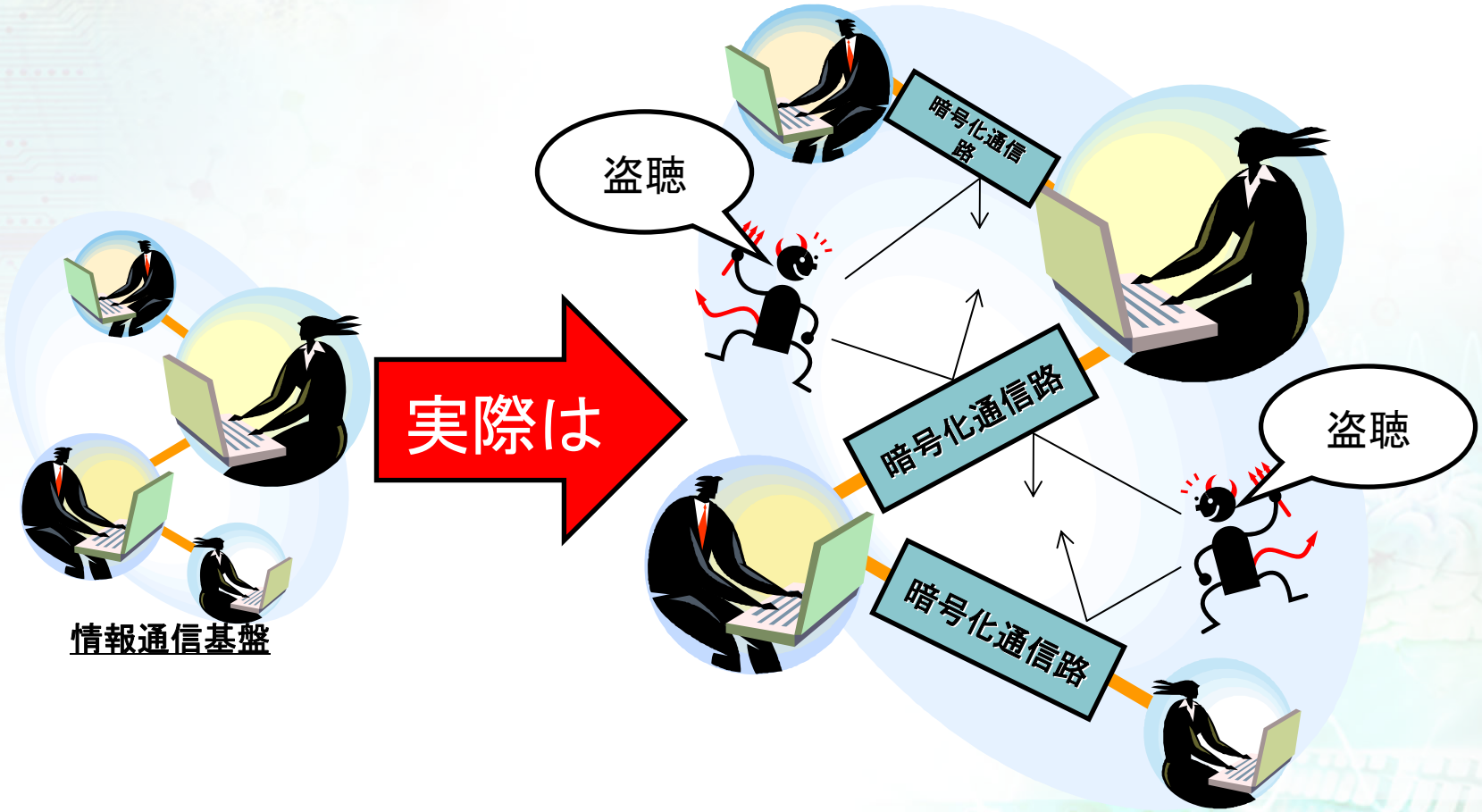
セキュリティ基盤技術研究チーム
花岡 悟一郎

National Institute of Advanced Industrial Science and Technology
AIST

研究の背景: 公開鍵暗号

Research Center for Information Security

- 公開鍵暗号: 暗号化通信路を確立するための最も重要な要素技術のひとつ



本研究の目的

- より安全で効率的な公開鍵暗号を設計することで、**より実用的な情報通信基盤**の実現に貢献する。

- その際の一般的問題:

効率性 VS. 安全性

トレードオフ

National Institute of Advanced Industrial Science and Technology
AIST

提案方式

花岡, 黒澤, Asiacrypt'08

Research Center for Information Security

公開鍵暗号の安全な構成 と 放送暗号の構成 の非自明な関係を発見。
それに基き、Naor-Pinkas放送暗号を変形し、新たな方式を設計

検証可能Naor-Pinkas放送暗号の秘密鍵

Setup(1^k): Generate a random polynomial $f(x) = a_0 + a_1 x + \cdots + a_{k+2} x^{k+2}$ over $\mathbb{Z}_p$, and compute $y_i = g^{a_i}$ for $0 \le i \le k+2$. The decryption key is $f(x)$, and the public key is $PK = (\mathbb{G}, g, y_0, y_1, ..., y_{k+2}, \mathsf{TCR}_0, \mathsf{TCR}_1, h)$, where $\mathsf{TCR}_b : \mathbb{G} \to \mathcal{S}_b$ $(b = 0, 1)$ are target collision resistant hash functions such that $\mathcal{S}_0 \cup \mathcal{S}_1 \subseteq \mathbb{Z}_p^*$, $\mathcal{S}_0 \cap \mathcal{S}_1 = \emptyset$, and $h : \mathbb{G} \to \{0,1\}$ is a hardcore bit function for the Diffie-Hellman key in $\mathbb{G}$.[3]

Encrypt(PK): Pick a random $r \xleftarrow{R} \mathbb{Z}_p$, and compute

暗号文サイズが小さい!

$$\psi = (g^r, g^{r \cdot f(\mathsf{i})}, g^{r \cdot f(\mathsf{i})}), \qquad K = (h(y_0^r) || h(y_1^r) || ... || h(y_{k-1}^r))$$

where $\mathsf{i} = \mathsf{TCR}_0(g^r)$ and $\mathsf{i} = \mathsf{TCR}_1(g^r)$. The final output is (ψ, K). (Notice that one can easily compute $g^{f(x)}$ as $g^{f(x)} = \prod_{0 \le i \le k+2} y_i^{x^i}$.)

Decrypt(dk, ψ, PK): For a ciphertext $\psi = (C_0, C_1, C_2)$, check whether $(C_1, C_2) \stackrel{?}{=} (C_0^{f(\mathsf{i})}, C_0^{f(\mathsf{i})})$, where $\mathsf{i} = \mathsf{TCR}_0(C_0)$ and $\mathsf{i} = \mathsf{TCR}_1(C_0)$. If not, output $\perp$. Otherwise, output $K = (h(C_0^{a_0}) || h(C_0^{a_1}) || ... || h(C_0^{a_{k-1}}))$.

検証可能Naor-Pinkas放送暗号の暗号文

従来技術との比較

- Cramer-Shoup暗号（Crypto 98）
  - DDH仮定, 冗長度 = 480 bit
- 黒澤-Desmedt暗号（Crypto 04）
  - DDH仮定, 冗長度 = 400 bit
- Cash-Kiltz-Shoup暗号（Eurocrypt 08）
  - **CDH仮定**, 冗長度 = 3200 bit
  - 提案方式と独立の結果
- 提案方式（Asiacrypt 08）
  - **CDH仮定**, 冗長度 = 480 bit

冗長度: 暗号文長 と 平文長の差