縫田 光司

暗号の安全性を定義し、解析し、実現する

Institute of Mathematics for Industry
Kyushu University

目に見えない「安全性」を、数学の力で照らす

背景と動機　暗号の安全性は、専門家にとってさえ扱いが難しい。
その技術は**本当に安全**か？また、**安全性が過剰**ではないか？

現状
- **未証明**の「仮定」や「原理」に基づく安全性の主張の存在
- 安全性の定義の「正しさ」が**未検証**なこともある

研究の例

安全性の **定義**

秘密計算

標準ライン
（共通鍵暗号）

- 安全性強度の差（**過剰さ**）を指摘
- **新たな安全性定義**を提案

（2026年、DOI: 10.1587/transfun.2025EAP1084）

安全性の **解析**

安全（秘密計算） ＋ 安全（疑似乱数） → **非**安全

（2021年、DOI: 10.1007/978-3-030-75248-4_16）

- 「合成の原理」が**破綻**する現象（反例）を初めて指摘

安全性の **実現**

$$\widetilde{\pi} \leftarrow \widetilde{\mathsf{HPS}}.\mathsf{pub}(1^{\ell}, \Lambda, \widetilde{s}, (x, e), \omega)$$

（2018年、DOI: 10.1007/s10623-017-0417-6）

- 既存方式の安全性の**不備を指摘**＆**修正**

$$\widetilde{\pi} \leftarrow \widetilde{\mathsf{HPS}}.\mathsf{pub}(1^{\ell}, \Lambda, \widetilde{s}, (x, e, \underline{\widehat{\pi}}), \omega)$$

展開
- 実システムで「安全 ＋ 安全 ⇒ 安全」と**保証**できる条件の解明
- 安全かつより効率的な暗号技術の**実現**、安全性の**検証**