

目に見えない「安全性」を、数学の力で照らす

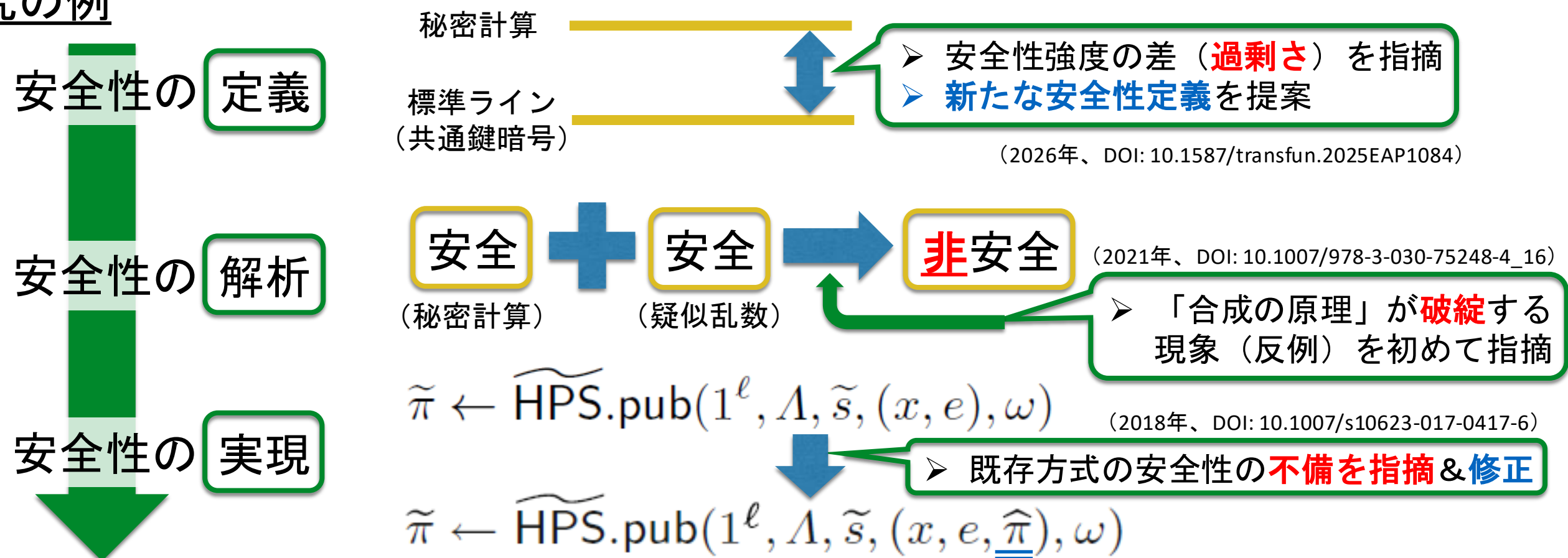
背景と動機

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



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**