RISEC次世代セキュリティRG における暗号技術の 証明可能安全性への取り組み

RISEC次世代セキュリティRG
研究グループ長 花岡 悟一郎

2012.09.10

セキュアシステム研究部門

- 日本の産業や社会をサイバー攻撃から守り、製品やサービスに「安全・安心」価値を付加することで、産業の振興を図る

セキュアシステム研究部門

部門長　：松井俊浩
副部門長: 寶木和夫

主に、暗号理論に関する最先端の知見を蓄積し、他の研究組織における「次世代情報システム」の設計に対して入力を行う

- セキュアサービスRG（インターネット等）
- 制御システムセキュリティRG（電気・ガス・水道インフラ等）
- システムライフサイクルRG（組み込みシステム等）
- 高信頼ソフトウェアRG（ソフトウェア実装等）
- **次世代セキュリティRG**

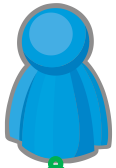
次世代セキュリティRG構成員

- 花岡悟一郎 グループ長
- 今福健太郎 主任研究員
- 縫田光司 研究員
- Nuttapong Attrapadung 研究員
- Miodrag Mihaljevic 招聘研究員
- Jacob Schuldt（学振PD(8月末退職)）
- 松田隆宏（学振PD）
- Jun Wu（ポスドク）
- Zongyang Zhang（ポスドク）

- 外来協力研究員
  - 坂井祐介(電通大)
  - 山田翔太(東大)
- テクニカルスタッフ
  - 矢内直人(筑波大)
  - 笠松宏平(中央大)
  - 大畑幸矢(東大)
  - 山川高志(東大)
- 事務スタッフ
  - 軽部恭子

証明可能安全性

過去



暗号設計者

色々な攻撃を試したし、
この暗号は安全だろう！

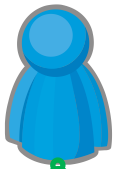
攻撃者

新しい攻撃
見つけた！

安全性
破綻

攻撃が判明した実システムの例
- (SSL) RSA PKCS#1 ver.1.5
- ISO/IEC 9796-2 (Scheme 1)

現在の暗号理論



暗号設計者

安全性が数学的に
証明できた！

攻撃者

攻撃のしよう
がない・・・

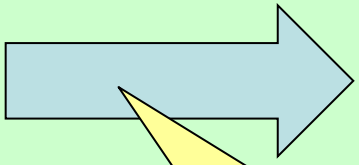
安全性
実現

証明可能安全性は現在の標準的要請

暗号技術の証明可能安全性

Q. 暗号技術の証明可能安全性とは？

A. （例）巨大な整数の素因数分解が（現在の計算機で）現実的には不可能



数学的証明

この暗号技術の安全性を破るのは現実的に不可能

Q. どうやって示す？

A. 上記の「**対偶**」を数学的に証明

困難なはずの問題を解くアルゴリズムが存在

矛盾 !!

暗号技術の安全性を破る攻撃者が存在

Rabin暗号

- 秘密鍵: 二つの素数p,q, 公開鍵: $N=p \times q$
- 暗号化: $C=M^2 \bmod N$
- 復号: $C \equiv x^2 \bmod p \equiv y^2 \bmod q$になるx,yを計算(簡単)。中国人剰余定理によりx,yからMを求める。

Rabin暗号の機能

- pが素数のとき、mod pにおけるM^2の平方根は簡単に求まる。
- 一方、Nが合成数のとき、mod NにおけるM^2の平方根を求めることは困難である。

要するに…

$M^2 \bmod a \Rightarrow M$

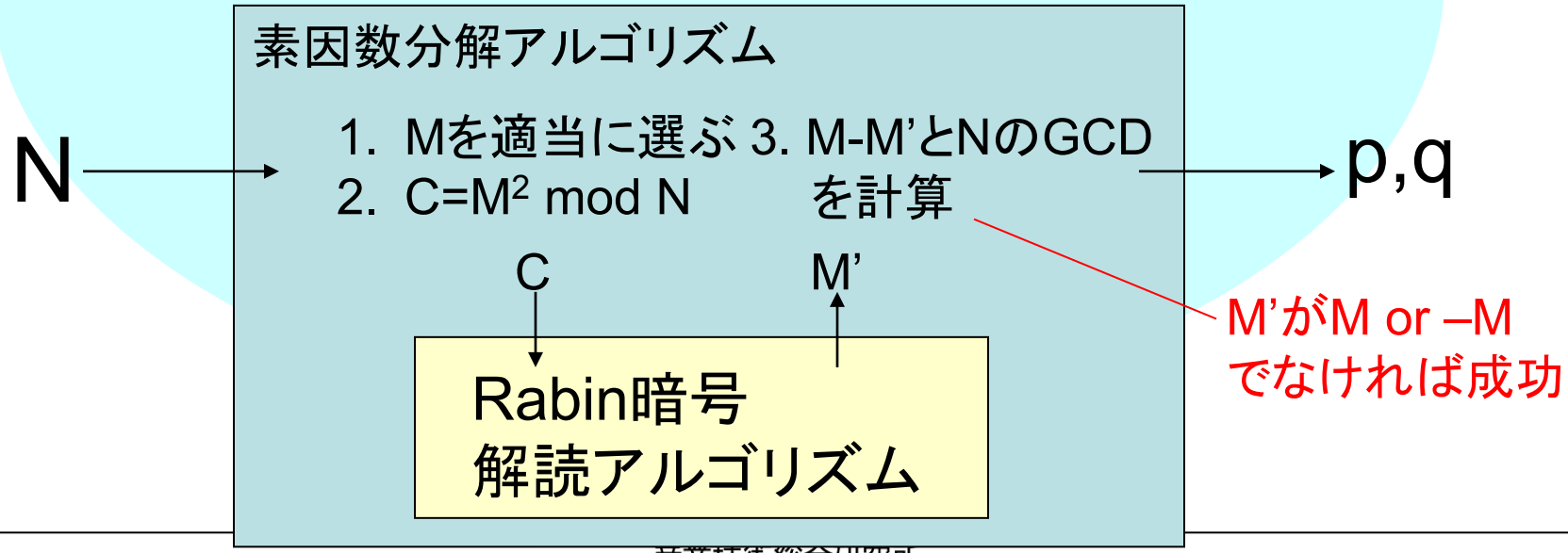
- 簡単（aが素数の時）
- 困難（aが合成数の時）

数値例

- 二つの素数を選ぶ: p=3,q=11
- 合成数Nを計算: N=p×q=33
- 公開鍵: 33, 秘密鍵: {3,11}
- 平文: $7 \in Z_{33}$
- 暗号化: $16 = 7^2 \bmod 33$
- 復号: $16 \equiv 1^2 = 2^2 \bmod 3$, $16 \equiv 4^2 = 7^2 \bmod 11$, {1 mod 3, 4 mod 11}, {1 mod 3, 7 mod 11}, {2 mod 3, 4 mod 11}, {2 mod 3, 7 mod 11}のすべてに対し、中国人剰余定理を適用し、{4,7,26,29}を導出。（復号結果はこの4つのどれか）

Rabin暗号の安全性証明

- Rabin暗号の解読アルゴリズムが存在するのであれば、それを用いて素因数分解アルゴリズムを構成できる。
- 対偶：素因数分解アルゴリズムが存在しないのであれば、Rabin暗号解読アルゴリズムも存在しない。



本研究グループのコア技術

- 公開鍵暗号、電子署名、関数暗号、放送暗号、時限暗号、準同型暗号、IDベース暗号、属性ベース暗号、代理人再暗号化暗号、フォワード安全暗号、鍵隔離暗号、量子暗号、耐量子計算機暗号、ゼロ知識証明、秘匿計算、否認可能認証、匿名認証、グループ署名、…

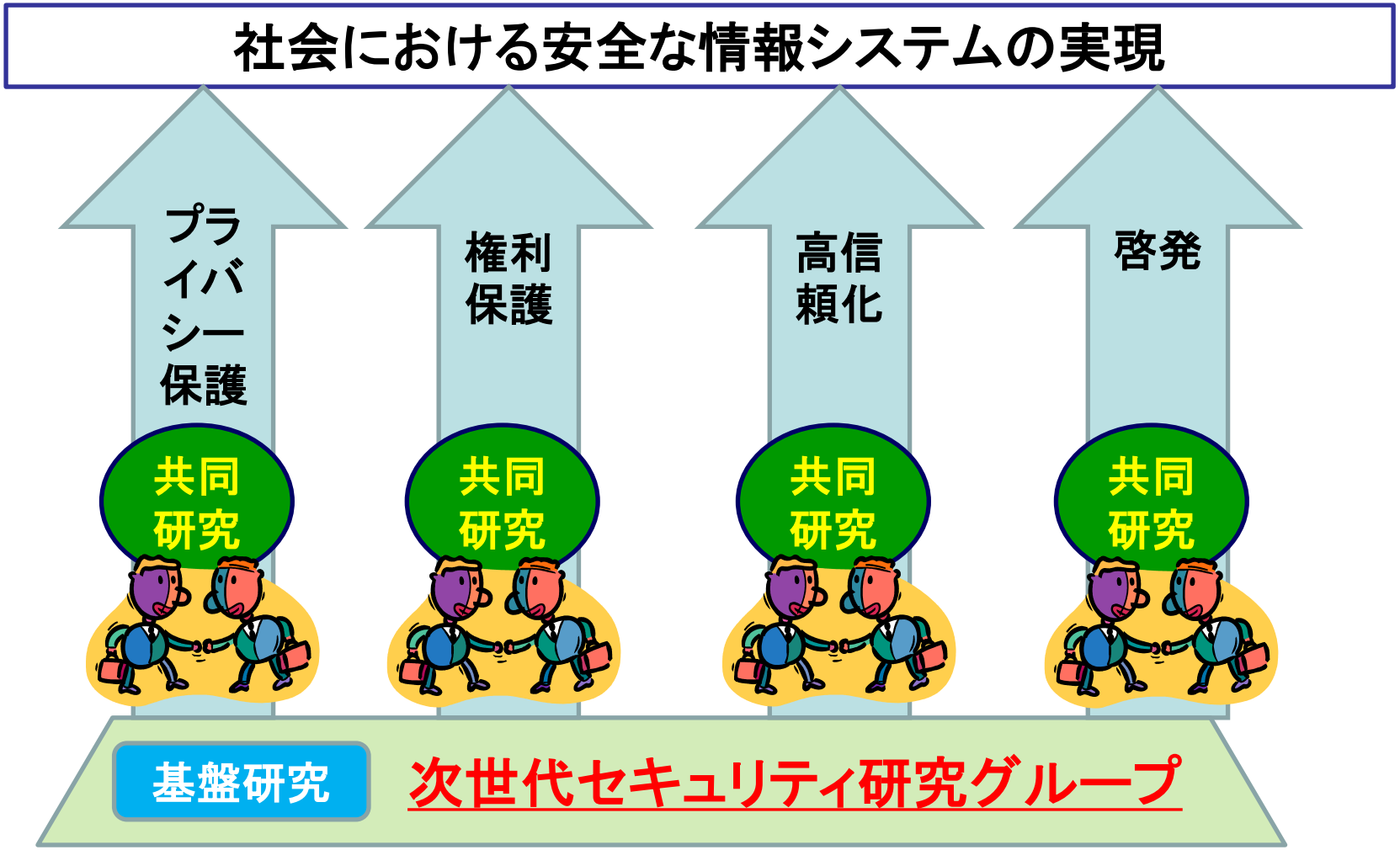
本年度(H24.4～9月)の主な成果

- 国際会議CRYPTO 2012 採録
- 国際会議ASIACRYPT 2012 採録
- 国際会議PKC 2012 採録(5件)

IACR会議

- 国際会議SCN 2012 採録
- 国際会議Pairing 2012 採録
- 国際査読誌 IEEE Trans. on IT 採録
- 国際査読誌 Info. Processing Letters採録

独自の知見の連携機関への提供



まとめ

- **暗号・認証技術に関する証明可能安全性についての知見**
  - 公開鍵暗号、電子署名、関数暗号、放送暗号、時限暗号、準同型暗号、IDベース暗号、属性ベース暗号、代理人再暗号化暗号、フォワード安全暗号、鍵隔離暗号、量子暗号、耐量子計算機暗号、ゼロ知識証明、秘匿計算、否認可能認証、匿名認証、グループ署名、…
- **権威ある国際会議・英文査読誌における実績**
  - **CRYPTO, ASIACRYPT, PKC, SCN, Pairing, IEEE ToIT, IPL**
- **これらの知見・実績をもとにした外部機関との連携**
  - **設計技術の安全性の理論的根拠付け**
  - **お気軽に声をおかけください！**