ブラックボックス構成と
その限界

安永 憲司（金沢大学）

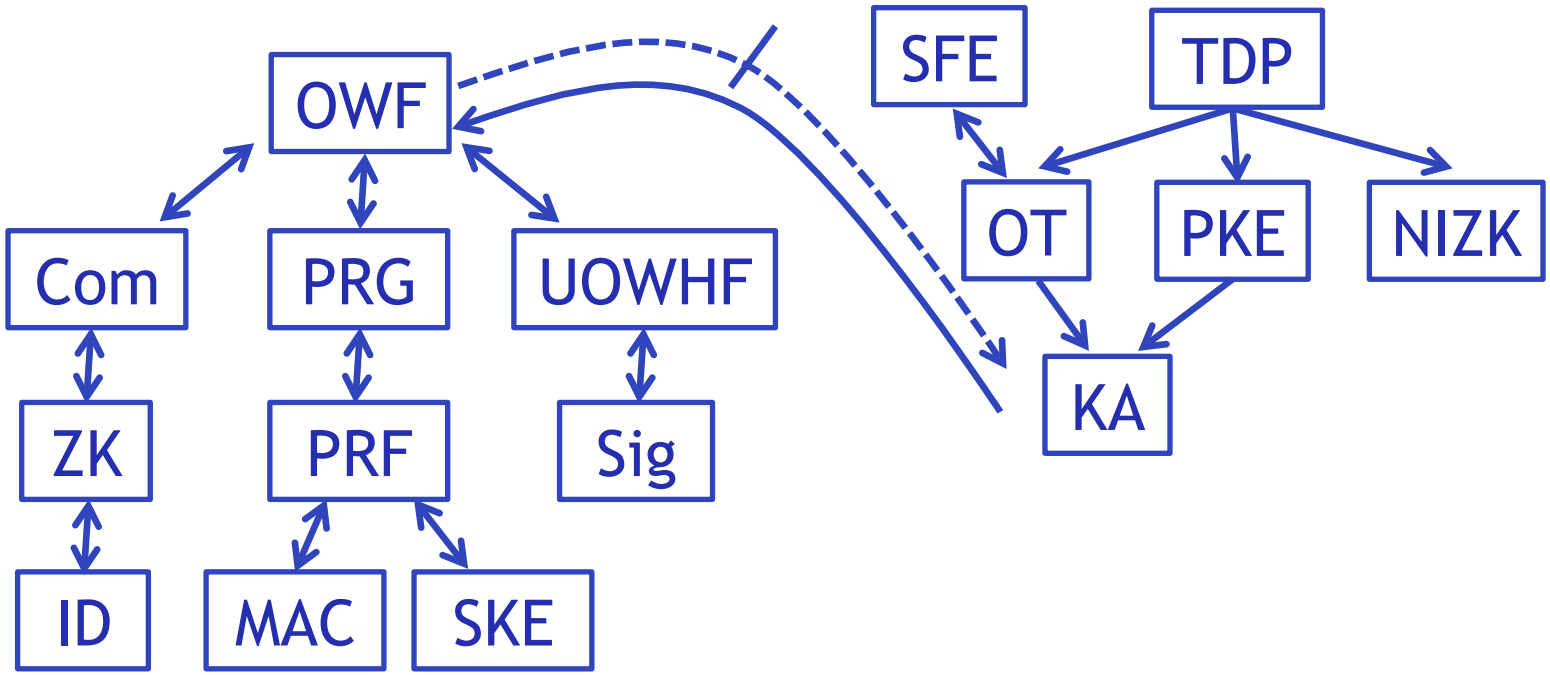
暗号理論

- 情報の秘匿性・正当性等を保証する技術の基礎理論
  - 秘匿性：公開鍵暗号、鍵共有、ゼロ知識証明
  - 正当性：電子署名、メッセージ認証、相手認証
  - その他：一方向性関数、擬似乱数生成器、擬似ランダム関数

- P ≠ NP の先の世界
  - 一方向性関数の存在性を仮定した上で議論

暗号技術の帰着関係

- 「技術 A → 技術 B」
  技術 A を実現する任意の方法が与えられれば、
  技術 B を実現可能
  - 「B の安全性を A の安全性に帰着させる」
    という



帰着の例（OWP + hardcore → PRG）

- OWP f とその hardcore predicate h に対し、
  G(x) = (f(x), h(x)) は PRG である
- 証明
  - PRG G の安全性を破る PPT A を仮定
  - A は i bit まで与えられ、i+1 bit 目が予測可能
  - G の最初 n bit は置換であり一様分布
    → A は n+1 bit 目を予測
  - A が n+1 bit 目を予測できることは
    h が hardcore であることに反する（証明終）

PRG の安全性を hardcore の安全性に帰着

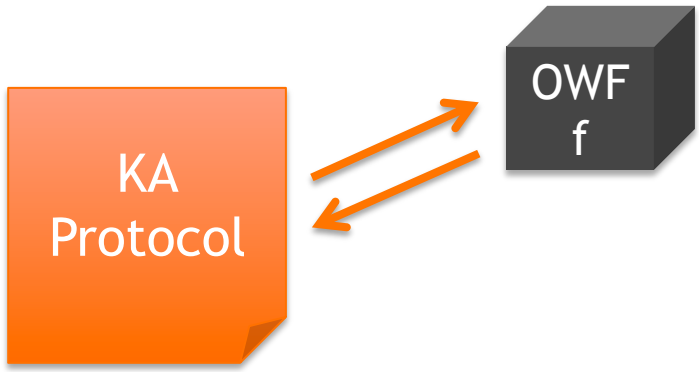
ブラックボックス帰着

- 各技術の中身（実現方法）を見ずに帰着関係を示すこと
  - 暗号技術の入出力と安全性が分かれば十分
- 暗号理論の帰着の多くはブラックボックス
- ブラックボックス帰着の限界 [IR89]
  - OWF → Key Agreement (KA)

２つの意味のブラックボックス

例. OWF → KA

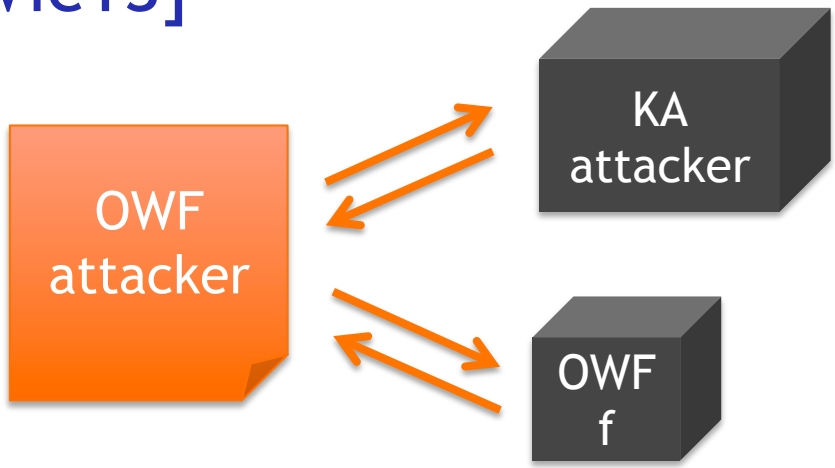
1. 構成方法がブラックボックス：
   - 任意の OWF f が与えられたとき、f の中身を見ずに、KA を構成
   - 限界に関する研究 [IR89, Rud92, Sim98, GKM+00, Fis02, RTV04, HR04, DOP05, GGK+05, BCFW09, FLR+10, FS12, HMS12]



２つの意味のブラックボックス

例. OWF → KA

2. 安全性証明（帰着）がブラックボックス：
   - KA を破る敵対者 A が与えられたとき、
     A の中身を見ずに、OWF を破る敵対者を構成
   - 限界に関する研究 [BV98, Cor02, Bro05, PV05, BMV08, HRS09, FS10, Pas11, GW11, DHT12, Pas13, Wic13]



Impagliazzo, Rudich (STOC ‘89)

定理

以下のオラクル Π が存在：
Π で相対化されて OWP は存在するが、KA は存在しない

定義 (相対化されて存在)

技術 P が Π で相対化されて存在
⇔ PPT M に対し、$f = M^{\Pi}$ が P を実現し、
　任意の PPT A に対し、$A^{\Pi,f}$ は f を破れない

Π で相対化された世界でも存在する

定義 (相対化帰着)

技術 P から Q への相対化帰着が存在
⇔ 任意のオラクル Π に対して、
　Π で相対化されて Q が存在するならば、
　Π で相対化されて P も存在

Π で相対化された世界でも帰着が成り立つ

定義 (fully black-box (BB) 帰着)

技術 P から Q への fully-BB 帰着が存在
⇔ PPT G, S が存在し
　1. Q の任意の実現方法 f に対して、G^f は P を実現
　2. Q の任意の実現方法 f, 任意の A に対して、
　　(G^f, A) で P を破る → $(f, S^{A,f})$ で Q を破る

(f, A) で P を破る ⇔ f という P の実現方法に対して A がその安全性を破る

命題 (fully-BB 帰着 → 相対化帰着)

技術 P から Q への fully-BB 帰着が存在するとき、
P から Q への相対化帰着が存在

直観的には、fully-BB は任意のオラクルアクセスを許しても成立するため

証明：

・P から Q への相対化帰着が存在しないと仮定
→ ∃ Π s.t. Π で相対化されて Q は存在し P は存在しない

・fully-BB 帰着の存在から PPT G, S が存在

・G の性質より、
Q の任意の実現方法 $f = M^{\Pi}$ に対し、G^f は P を実現するが、
P は存在しないため、∃ PPT A s.t. $(G^f, A^{\Pi,f})$ で P を破る

・$A' = A^{\Pi,f}$ の存在と S の性質より、$(f, S^{A', f})$ で Q を破る
→ Q が Π で相対化されて存在することに矛盾（証明終）

Impagliazzo, Rudich (STOC ’89)（再掲）

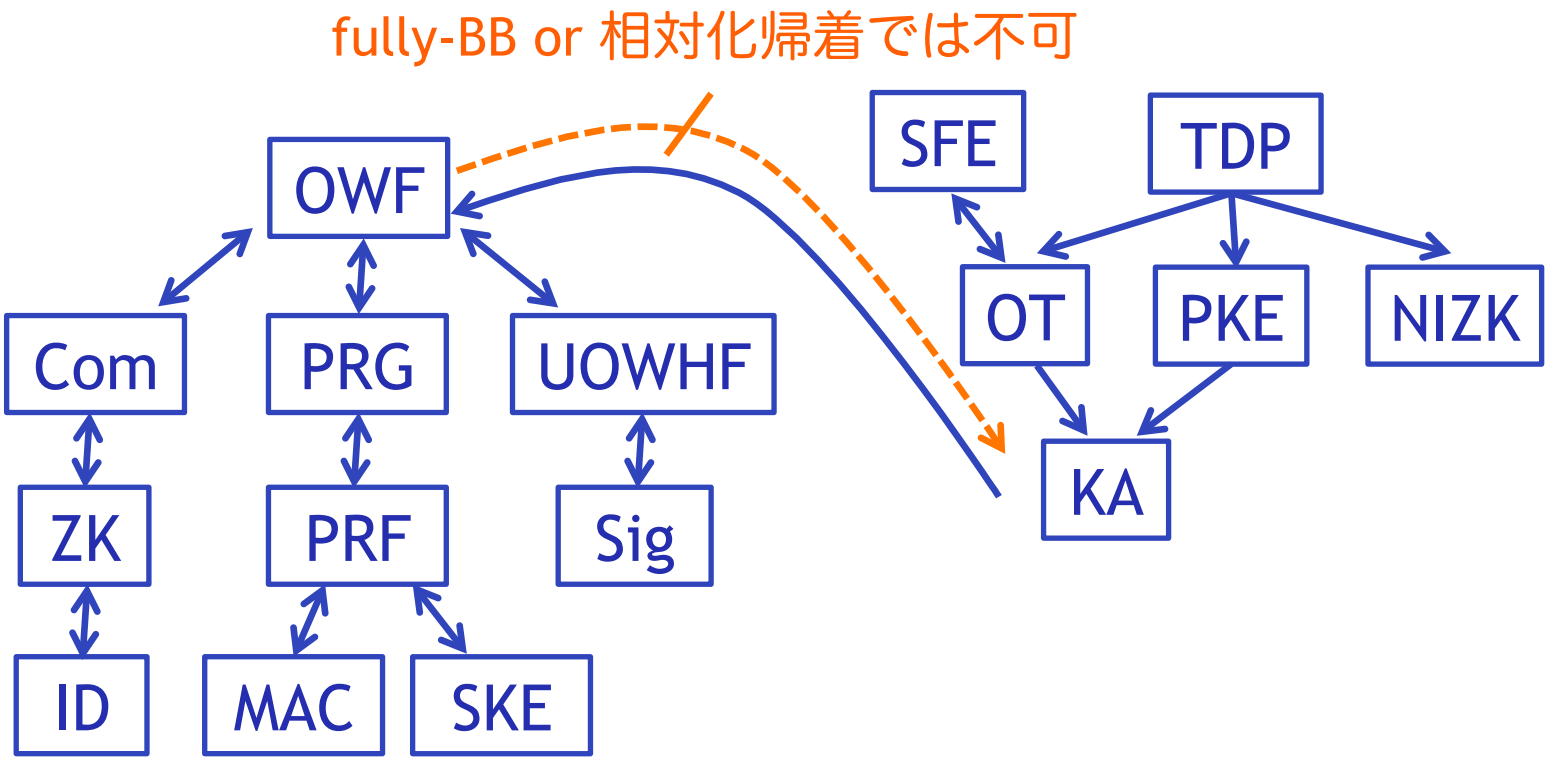
定理

以下のオラクル Π が存在：
Π で相対化されて OWP は存在するが、KA は存在しない
（Π は PSPACE + ランダム関数）

系

KA から OWP への fully-BB 帰着は存在しない

暗号技術の帰着関係


fully-BB or 相対化帰着では不可
OWF
Com
PRG
UOWHF
ZK
PRF
Sig
ID
MAC
SKE
SFE
TDP
OT
PKE
NIZK
KA

ブラックボックスでない帰着方法とは？

- Karp 帰着（NP 完全性等）を利用した構成法
  - Cook-Levin の NP 完全性証明では、TM の状態をブール関数で表現
  - 任意の NP に対するゼロ知識証明 [GMW91] では、NP 完全性を利用するため、TM のコードが必要
- Barak (FOCS ‘01) のテクニック
  - 敵対者のコードを利用
  - ブラックボックスによる限界を回避
- 回路を利用した構成方法
  - Randomized Encoding [AIK04,06] では NC^1 回路で実現された暗号技術を NC^0 に変換
  - 完全準同型暗号の構成法

BB 帰着不可能性に関する研究

- BB 帰着による効率の限界
  - BB 構成アルゴリズムのクエリ下界 [GGKT05]
    - OWP → PRG,UOWHF, Signature;　TDP → PKE
  - BB 帰着アルゴリズムのクエリ下界 [Lu09]
    - weak OWF → strong OWF;　OWF → PRG

- メタ帰着による不可能性
  - 「BB 帰着の存在 → 安全性仮定の否定」
  - 安全性仮定に対して議論可能

参考文献

- [IR89] R. Impagliazzo and S. Rudich: Limits on the provable consequences of one-way permutations. STOC 1989.
- [GGKT05] Rosario Gennaro, Yael Gertner, Jonathan Katz, Luca Trevisan: Bounds on the Efficiency of Generic Cryptographic Constructions. SIAM J. Comput. (2005)
- [Lu09] Chi-Jen Lu: On the Security Loss in Cryptographic Reductions. EUROCRYPT 2009.
- [BCPT13] Eleanor Birrell, Kai-Min Chung, Rafael Pass, Sidharth Telang: Randomness-Dependent Message Security. TCC 2013
- [RTV04] Omer Reingold, Luca Trevisan, Salil P. Vadhan: Notions of Reducibility between Cryptographic Primitives. TCC 2004.
- [BBF13] Paul Baecher, Christina Brzuska, Marc Fischlin. Notions of Black-Box Reductions, Revisited. Asiacrypt 2013.