証明可能安全性の形式的証明

Reynald Affeldt, David Nowak and Miki Tanaka
ソフトウェアセキュリティ研究チーム

ゲームの手法

・暗号化スキーム等には何らかの形の安全性証明が付随
・ゲームの手法は安全性証明の一手法
・安全性性質は「ゲーム」として、安全性証明は「ゲーム」の変換列として表現される

$$
\begin{array}{l}
(pk, sk) \leftarrow \mathrm{keygen}() ; \\
r \xleftarrow{R} R ; \\
(m_1, m_2) \leftarrow A_1(r, pk) ; \\
b \xleftarrow{R} \{1,2\} ; \\
c \leftarrow \mathrm{encrypt}(pk, m_b) ; \\
\hat{b} \leftarrow A_2(r, pk, c) ; \\
\mathit{return}\ \ \hat{b} = b
\end{array}
$$

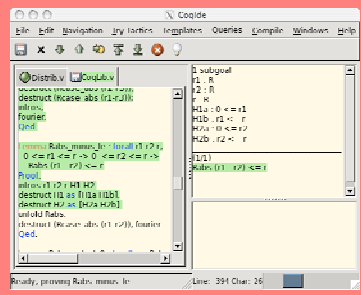
・ここでいう「ゲーム」とは:
要求される安全性性質に対する攻撃を、攻撃者が解くべき挑戦、課題として表現したもの。
攻撃者が無視できない確率でゲームに勝てば、安全性性質は保証されない。

例:強秘匿性(*semantic security*)を定義するゲーム

PROBLEM:
"暗号理論分野における証明の多くは、本質的に検証不能になってしまった。この分野は厳密さに関して危機的状況に陥りつつあるのかもしれない。"
(Bellare and Rogaway, 2004)

定理証明ツール

・証明の正しさをチェックし、頻出する簡単な証明を自動的に行うためのソフトウェア
・定理証明ツールを使えば、推論ミスや、暗黙の仮定などによる証明の誤りを防ぐことが可能となる

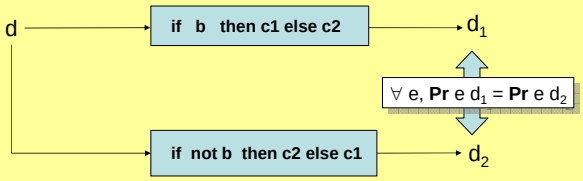


例:定理証明支援系Coq (フランスのINRIAで1984より開発)

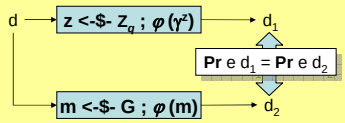
OUR SOLUTION:
・定理証明ツールを利用して安全性性質を証明
・ゲーム変換、確率等に関するライブラリを構成

Results: 定理証明ツールによるゲームの手法:再利用可能ゲーム変換例

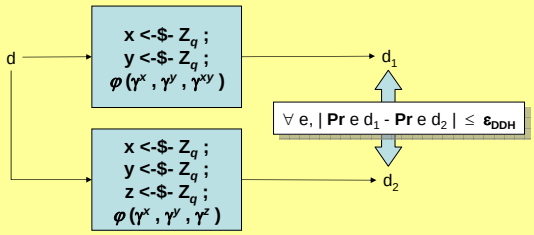
ライブラリには、以下のようなゲーム変換とその証明が再利用可能な形で含まれている。これらを組み合わせて安全性証明を構成する。



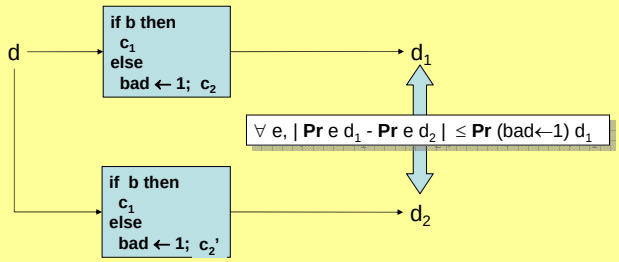
基本的な変換



巡回群に基づく変換



決定Diffie-Hellman問題に基づく変換



ゲーム変換の基本補題

Applications: 暗号化スキーム等に関する安全性の形式的証明

- ElGamal暗号化スキームの強秘匿性の形式的証明
- ブロック暗号の安全性証明などに応用されるSwitching補題の形式的証明

R. Affeldt, M. Tanaka, and N. Marti. **Formal proof of provable security by game-playing in a proof assistant.**
International Conference on Provable Security (ProvSec 2007), LNCS 4784
D. Nowak. **A framework for game-based security proofs.**
International Conference on Information and Communications Security (ICICS 2007), LNCS 4861