

FCS-ARSPA-WITS, CSF, FCC' 08 参加報告

— 安全性の形式化について —

川本 裕輔 † アフェルト レナルド ‡

† 東京大学大学院情報理工学系研究科

‡ 産業技術総合研究所情報セキュリティ研究センター

概要

6月に開かれた国際会議 / ワークショップ

- FCS-ARSPA-WITS'08 **15件** (+ 招待講演 2件)

Joint Workshop on Foundations of Computer Security,
Automated Reasoning for Security Protocol Analysis
and Issues in the Theory of Security

- CSF'08 **23件** (+ 招待講演 1件)

IEEE Computer Security Foundations Symposium

- FCC'08 **8件** (+ 招待講演 1件)

Workshop on Formal and Computational Cryptography

の中からいくつかの研究を紹介する

目次

- 汎用的結合可能性 (UC) の改良

R. Küsters and M. Tuengerthal,

“Joint State Theorems for Public-Key Encryption & Digital Signature Functionalities with Local Computation”

- 記号モデルの計算論的健全性

M. Backes and D. Unruh,

“Computational Soundness of Symbolic Zero-knowledge Proofs Against Active Attackers”

- FCC の話題

目次

- 汎用的結合可能性 (UC) の改良

R. Küsters and M. Tuengerthal,

“Joint State Theorems for Public-Key Encryption & Digital Signature Functionalities with Local Computation”

- 記号モデルの計算論的健全性

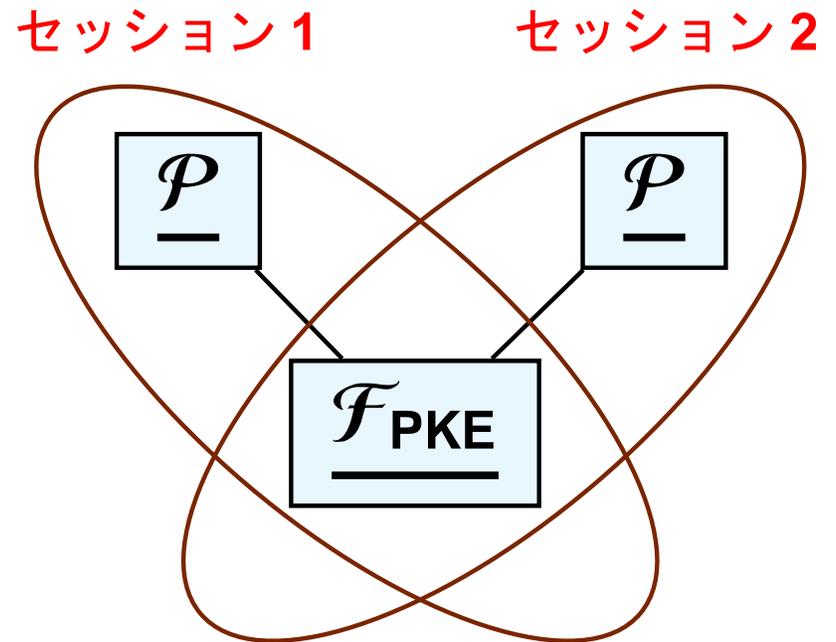
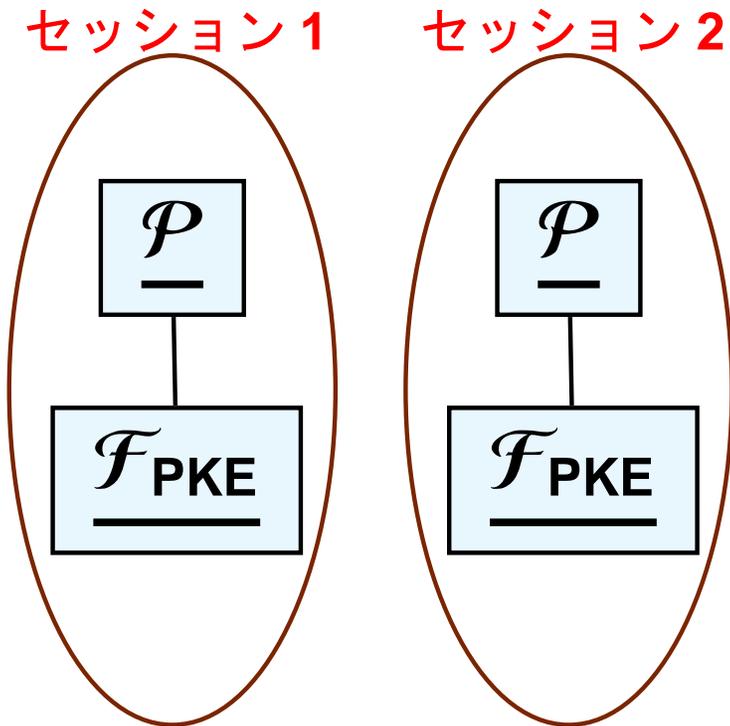
M. Backes and D. Unruh,

“Computational Soundness of Symbolic Zero-knowledge Proofs Against Active Attackers”

- FCC の話題

[Küsters-Tuengerthal'08] の概要

- ジョイント状態 (Joint State) 定理の必要性
 - 通常の UC では、異なるセッションの間で、鍵や乱数を共有できない。



[Küsters-Tuengerthal'08] の概要

- ジョイント状態 (Joint State) 定理の必要性
 - 通常の UC では, 異なるセッションの間で, 鍵や乱数を共有できない.
- UC におけるジョイント状態定理の問題点.
- UC を改良し, ジョイント状態定理を得る.
- 電子署名, IND-CCA / IND-RCCA 公開鍵暗号の理想機能を定式化.

IITM (Inexhaustive ITM)

● UC と [Küsters-Tuengerthal'08] の比較

	UC	[Küsters-Tuengerthal'08]
ジョイント状態定理	問題あり	容易に得られる
対話的チューリング機械 (ITM)	exhaustive	inexhaustive

IITM (Inexhaustive ITM)

● UC と [Küsters-Tuengerthal'08] の比較

	UC	[Küsters-Tuengerthal'08]
ジョイント状態定理	問題あり	容易に得られる
対話的チューリング機械 (ITM)	exhaustive	inexhaustive

● (exhaustive) ITM の問題点

- ITM は, **総入力長**と... に関して多項式時間で動作.
→ 入力は, 遮断される**不要メッセージ**を含む.
- 「複数の ITM からなるシステム」を「一つの ITM」
で**模倣 (simulate) できない**ことがある.

安全性の定式化

- strong simulatability

プロトコルと実現したい理想機能の識別不能性

プロトコル \mathcal{P} が理想機能 \mathcal{F} を実現する ($\mathcal{P} \leq^{\text{SS}} \mathcal{F}$)

def

$\Leftrightarrow \exists S: \text{Simulator} \quad \forall \mathcal{E}: \text{Environment} \quad \mathcal{E} \parallel \mathcal{P} \equiv \mathcal{E} \parallel S \parallel \mathcal{F}$

- black-box simulatability と等価.
- \mathcal{F} がある条件を満たすとき, universal simulatability (UC) と等価.

結合可能性定理

● 結合可能性定理 (Composition Theorem)

1. $\mathcal{P}_1 \leq^{SS} \mathcal{F}_1, \mathcal{P}_2 \leq^{SS} \mathcal{F}_2$ ならば $\mathcal{P}_1 \parallel \mathcal{P}_2 \leq^{SS} \mathcal{F}_1 \parallel \mathcal{F}_2$
2. $\mathcal{P} \leq^{SS} \mathcal{F}$ ならば $Q \parallel \underline{\mathcal{P}} \leq^{SS} Q \parallel \underline{\mathcal{F}}$

ジョイント状態定理

- ジョイント状態定理 (Joint State Theorem)

- $\hat{\rho} \leq^{ss} \underline{\mathcal{F}}$ ならば $Q \parallel \hat{\rho} \leq^{ss} Q \parallel \underline{\mathcal{F}}$

(このような $\hat{\rho}$ を見つけることはあまり簡単ではない.)

ジョイント状態定理

● ジョイント状態定理 (Joint State Theorem)

$$\bullet \hat{\mathcal{P}} \leq^{ss} \underline{\mathcal{F}} \text{ ならば } Q \parallel \hat{\mathcal{P}} \leq^{ss} Q \parallel \underline{\mathcal{F}}$$

※ UC の場合 [Canetti-Rabin03] \mathcal{F} を記述できない

Q : 理想機能 \mathcal{F} の複数のインスタンスを用いるプロトコル

$\hat{\mathcal{F}}$: \mathcal{F} を模倣する ITM

$$\bullet \hat{\mathcal{P}} \leq \hat{\mathcal{F}} \text{ ならば } Q^{[\hat{\mathcal{P}}]} \leq Q$$

ジョイント状態定理

● ジョイント状態定理 (Joint State Theorem)

● $\hat{\mathcal{P}} \leq^{ss} \underline{!F}$ ならば $Q \parallel \hat{\mathcal{P}} \leq^{ss} Q \parallel \underline{!F}$

※ UC の場合 [Canetti-Rabin03] $\underline{!F}$ を記述できない

Q : 理想機能 F の複数のインスタンスを用いるプロトコル

\hat{F} : $\underline{!F}$ を模倣する ITM \hat{F} をとれない可能性あり

● $\hat{\mathcal{P}} \leq \hat{F}$ ならば $Q^{[\hat{\mathcal{P}}]} \leq Q$ $Q^{[\hat{\mathcal{P}}]}$ の定義を明記せず

IITM (Inexhaustive ITM)

● UC と [Küsters-Tuengerthal'08] の比較

	UC	[Küsters-Tuengerthal'08]
ジョイント状態定理	問題あり	容易に得られる
対話的チューリング機械 (ITM)	exhaustive	inexhaustive
入力に関する多項式時間制約	不要メッセージ含む	不要メッセージ以外
システムを一つの ITM で	模倣できないかも	模倣できる

目次

- 汎用的結合可能性 (UC) の改良

R. Küsters and M. Tuengerthal,

“Joint State Theorems for Public-Key Encryption & Digital Signature Functionalities with Local Computation”

- 記号モデルの計算論的健全性

M. Backes and D. Unruh,

“Computational Soundness of Symbolic Zero-knowledge Proofs Against Active Attackers”

- FCC の話題

計算論的健全性とは

記号的手法 \Rightarrow 計算論的手法

(フォーマルメソッド)

計算論的健全性

計算論的健全性とは

記号的手法 \Rightarrow 計算論的手法

(フォーマルメソッド)

計算論的健全性

マッピング健全性 [Micciancio-Warinschi'04]

各計算論的トレースに対して、圧倒的な確率で、対応する記号トレースが存在する。

[Backes-Unruh'08] の概要

- 非対話ゼロ知識証明の記号モデルを提案

※ ゼロ知識証明に対する記号モデルの研究は、最近になって始まった。

[Backes-Maffei-Unruh'08] (2008 IEEE Symposium on Security and Privacy)

“Zero-Knowledge in the Applied Pi-calculus and Automated Verification of the Direct Anonymous Attestation Protocol”

[Backes-Hrițcu-Maffei'08a] (FCS-ARSPA-WITS'08)

“Type-checking Zero-knowledge”

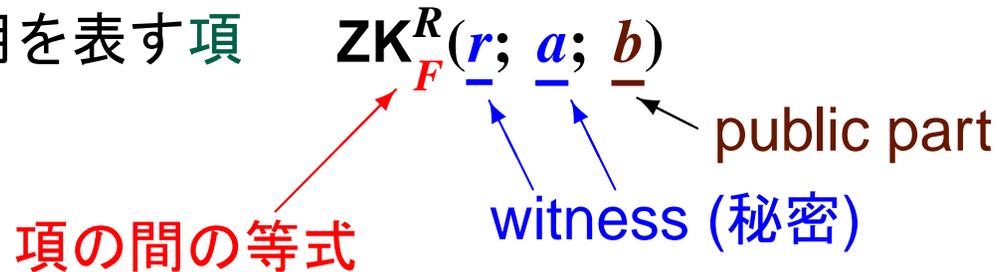
[Backes-Hrițcu-Maffei'08b] (CSF'08)

“Automated Verification of Remote Electronic Voting Protocols in the Applied Pi-calculus”

[Backes-Unruh'08] の概要

- 非対話ゼロ知識証明の記号モデルを提案

- ゼロ知識証明を表す項



例: $F := (\beta_6 = \{\{\langle\beta_7, \alpha_1\rangle, \alpha_2\} \}_{\text{ek}(\beta_5)}^{\rho_1} \}_{\text{ek}(\beta_4)}^{\rho_2})$

- ゼロ知識証明のための推論規則

$$\varphi \vdash \underline{a} \quad \varphi \vdash \underline{b} \quad R \in \text{Rand}_{adv} \quad F \in \text{Formula} \quad F\{\underline{r}, \underline{a}, \underline{b}\} \text{ is true}$$

$$\forall i : r_i \in \text{Rand}_{adv} \quad \forall (\exists t, a : \varphi \vdash \{t\}_{\text{ek}(a)}^{r_i} \wedge \varphi \vdash \text{dk}(a))$$

$$\varphi \vdash ZK_F^R(\underline{r}; \underline{a}; \underline{b})$$

$$\varphi \vdash ZK_F^R(\underline{r}; \underline{a}; \underline{b})$$

$$\varphi \vdash \underline{b}$$

[Backes-Unruh'08] の概要

- 非対話ゼロ知識証明の記号モデルを提案
- 非対話ゼロ知識証明の安全性定義を提案
 - Completeness
 - Extractability
(新たに提案, soundness よりも強い)
 - Extraction zero-knowledge
([Groth-Ostrovsky'07], zero-knowledge よりも強い)
 - Unpredictability
(新たに提案)
 - これらを満たす具体的なスキームが存在する。

[Backes-Unruh'08] の概要

- 非対話ゼロ知識証明の記号モデルを提案
- 非対話ゼロ知識証明の安全性定義を提案
- この記号モデルの**計算論的健全性**を証明
 - **マッピング健全性**のみ
 - 「トレースの集合」で表される安全性に有効
(例: `completeness`, `extractability`)
 - 「トレースの確率分布の間の識別不能性」で表される安全性にはあまり役立たない. (例: `zero-knowledge`)
 - **識別不能性の健全性**は将来の課題

目次

- 汎用的結合可能性 (UC) の改良

R. Küsters and M. Tuengerthal,

“Joint State Theorems for Public-Key Encryption & Digital Signature Functionalities with Local Computation”

- 記号モデルの計算論的健全性

M. Backes and D. Unruh,

“Computational Soundness of Symbolic Zero-knowledge Proofs Against Active Attackers”

- FCC の話題

ゲーム列による安全性証明の自動検査

ゲーム列による安全性証明とは？

- 「攻撃者と挑戦者の間で行われるゲーム」として安全性を記述.
- 初期ゲームを次々に変換しながら,
 - 変換の前後で「攻撃者が勝つ確率」がほとんど変わらないこと
 - 最終ゲームで「攻撃者が勝つ確率」が無視できることを証明することにより,
 - 初期ゲームで「攻撃者が勝つ確率」が無視できることを証明する.

ゲーム列による安全性証明の自動検査

CryptoVerif と異なる目的で設計された2つの検査器

- 「ユーザが用意したコードベースの安全性証明」を機械的に検査.
 - 自動証明は行わない.
 - 「安全性証明の計算論的妥当性」をより厳密に保証する.
- G. Barthe, B. Grégoire, R. Janvier, F. Olmedo, S. Z. Béguelin
“Formal Certification of Code-Based Cryptographic Proofs”
 - M. Backes, M. Berg and D. Unruh
“A Formal Language for Cryptographic Pseudocode”

ゲーム列による安全性証明の自動検査

CryptoVerif と異なる目的で設計された2つの検査器

- 「ユーザーが用意したコードベースの安全性証明」を機械的に検査.
 - 自動証明は行わない.
 - 「安全性証明の計算論的妥当性」をより厳密に保証する.
- G. Barthe, B. Grégoire, R. Janvier, F. Olmedo, S. Z. Béguelin
“Formal Certification of Code-Based Cryptographic Proofs”
 - 定理証明器 Coq を用いる検査器 CertiCrypt
 - 適用例: ElGamal, OAEP, Full Domain Hash lemma
 - M. Backes, M. Berg and D. Unruh
“A Formal Language for Cryptographic Pseudocode”
 - 定理証明器 Isabelle/HOL を用いる検査器
 - CertiCrypt よりも記述力がある. (オラクルや情報量的安全性)

情報流解析の計算論的健全性

情報流解析とは？

- 機密情報の流出を調べるためのプログラムの解析

非干渉性: 識別不能性として定義

- 機密度の高いデータを**変更**してプログラムを実行しても、機密度の低いデータが**影響を受けない**という性質.

情報流解析の計算論的健全性

● C. Fournet, G. L. Guernic and T. Rezk

“A Cryptographic Compiler for Information-Flow Security”

- 分散プログラムが信頼性の低い共有メモリを介して通信する.
- 暗号技術を利用して情報流安全性ポリシーを実現する.

||

機密情報が流出しない

情報流解析の計算論的健全性

● C. Fournet, G. L. Guernic and T. Rezk

“A Cryptographic Compiler for Information-Flow Security”

- 分散プログラムが信頼性の低い共有メモリを介して通信する.
- 暗号技術を利用して情報流安全性ポリシーを実現する.
- 「安全性の注釈を書ける小さな命令型言語のコード」を
「暗号ライブラリを用いる分散 F# のコード」に変換する **コンパイラ**

情報流解析の計算論的健全性

● C. Fournet, G. L. Guernic and T. Rezk

“A Cryptographic Compiler for Information-Flow Security”

- 分散プログラムが信頼性の低い共有メモリを介して通信する.
- 暗号技術を利用して情報流安全性ポリシーを実現する.
- 「安全性の注釈を書ける小さな命令型言語のコード」を
「暗号ライブラリを用いる分散 F# のコード」に変換する **コンパイラ**
 - 「命令型言語のコード」：共有メモリの読み書きのための情報流安全性ポリシーを注釈として記述.
 - 「分散 F# コード」：情報流安全性ポリシーを強制するために、暗号化や署名生成の命令が挿入されている.
- **型システム**が **命令の挿入**の正しさ (計算論的な非干渉性) を保証.

FCC その他

- H. Comon-Lundh and V. Cortier,
“Computational soundness of observational equivalence”
- P. Adao, C. Fournet, N. Guts and F. Z. Nardelli,
“High-Level Programming for E-Cash (work in progress)”
- K. Bhargavan, R. Corin, C. Fournet and E. Zalinescu,
“Cryptographically Verified Implementations for TLS”
- C. Ene, J. Courant, Y. Lakhnech, M. Daubignard and P. Lafourcade,
“Automated Proofs for Asymmetric Encryption”
- A. Jaggard, C. Meadows, M. Mislove and R. Segala,
“Task Probabilistic Input/Output Automata as Domains”
- A. Datta, J. Halpern, J. Mitchell, R. Pucella and A. Roy,
“Reasoning about Conditional Probability and Concrete Security
in Protocol Proofs (Work in Progress)”

ご清聴ありがとうございました。