CSF, FCC'09参加報告

櫻田英樹
日本電信電話(株)
NTTコミュニケーション科学基礎研究所

CSF概要

IEEE computer society

22nd IEEE
Computer Security
Foundations Symposium

期間	7月8日～7月10日
会場	Port Jefferson, NY, USA
発表件数	22件（採択率24%）
参加者数	約100名（日本から3名）

- 情報セキュリティの理論、数理的モデル、検証に関する国際会議
- 発表の内容：
  - セキュリティ・プロトコルの設計・解析・検証
  - プログラムなどの情報流解析
  - アクセス制御

FCC概要

5th Workshop on Formal and Computational Cryptography

期間	7月11日～7月12日
会場	Port Jefferson, NY, USA
発表件数	12件
参加者数	約30名（日本から2名）

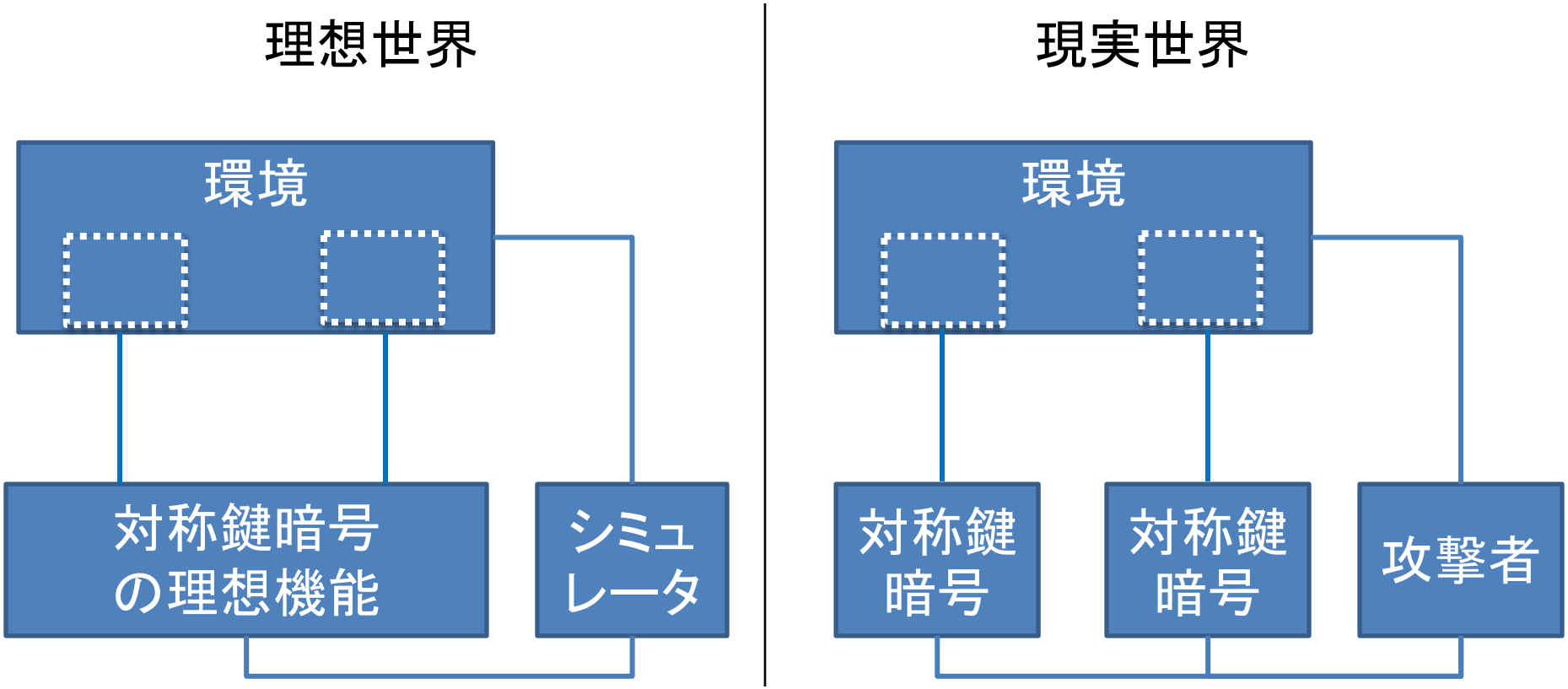
- 情報セキュリティにおける、計算論的方法と記号的方法の関係・融合に関するワークショップ
- プロトコルの記号的解析方法の提案と、その計算論的裏付けの話題が中心

対称鍵暗号の汎用的結合可能性

Universally Composable Symmetric Encryption (R. Küsters and M. Tuengarthal)

課題　シミュレーションベースのセキュリティ（UCなど）において、対称鍵暗号の理想機能がなかった。

貢献
- 対称鍵暗号の理想機能を提案し、対称鍵暗号による実現をIND-CCA安全性を仮定して示した。
- また、認証暗号についても同様のことをINT-CTXT安全性を仮定して行った。
- さらに、鍵の配布についても公開鍵暗号および対称鍵暗号を用いる場合について理想機能を提案し、実現方法を示した。



- 鍵を他の鍵を用いて暗号化する場合を考慮した理想機能を提案（鍵のポインタを暗号化）
- 対称鍵暗号が理想機能を実現することを示した
  ＝ 環境（多項式時間Turing機械）が
  理想世界と現実世界を区別できない

Diffie-Hellman exponentiationを持つプロトコルの自動解析

Using ProVerif to Analyze Protocols with Diffie-Hellman Exponentiation

(R. Küsters and T. Truderung)

課題　Diffie-Hellman exponentiationを持つプロトコルの証明では様々な等式（$g^x g^y = g^{x+y}$ など）を適切な順序で用いる必要があり、自動検証が困難。

貢献　プロトコルをexponent-groundなものに制限し、この制限の下で攻撃者の能力を定義。
これに基づき自動検証方法を提案。

exponent-groundなプロトコルの例
（SIGMA-BASICプロトコル）

g^N

変数（ネットワークから受け取ったもの）が
exponentに出現しない

$$A \to B: \quad g^{\uparrow N}$$

$$B \to A: \quad g^{\uparrow M},\ B,\ \mathsf{sig}_{k_B}(\langle g^{\uparrow N}, g^{\uparrow M}\rangle),\ \mathsf{mac}_K(B)$$

$$A \to B: \quad A,\ \mathsf{sig}_{k_A}(\langle g^{\uparrow M}, g^{\uparrow N}\rangle),\ \mathsf{mac}_K(A)$$

攻撃者の能力
（知識の導出規則）

exponentialを全て

の形で表現

この導出規則で
攻撃者の能力が
網羅できることを示した

$$\mathrm{I}(0)$$

$$\mathrm{I}(x) \to \mathrm{I}(\mathsf{succ}(x))$$

$$\mathrm{I}(x) \to \mathrm{I}(\mathsf{prev}(x))$$

$$\mathrm{I}(x) \to \mathrm{I}(\mathsf{exp}(x,0,\ldots,0))$$

$$\mathrm{I}(\mathsf{exp}(x,0,\ldots,0)) \to \mathrm{I}(x)$$

$$\mathrm{I}(c_i),\ \mathrm{I}(y),\ \mathrm{I}(\mathsf{exp}(x_0,x_1,\ldots,x_m)) \to \mathrm{I}(\mathsf{exp}(x_0,\ldots,x_{i-1},y,x_{i+1},\ldots,x_m)) \quad \text{for each } c_i \in \mathsf{C}$$

ゼロ知識証明によるプロトコルの耐侵害化

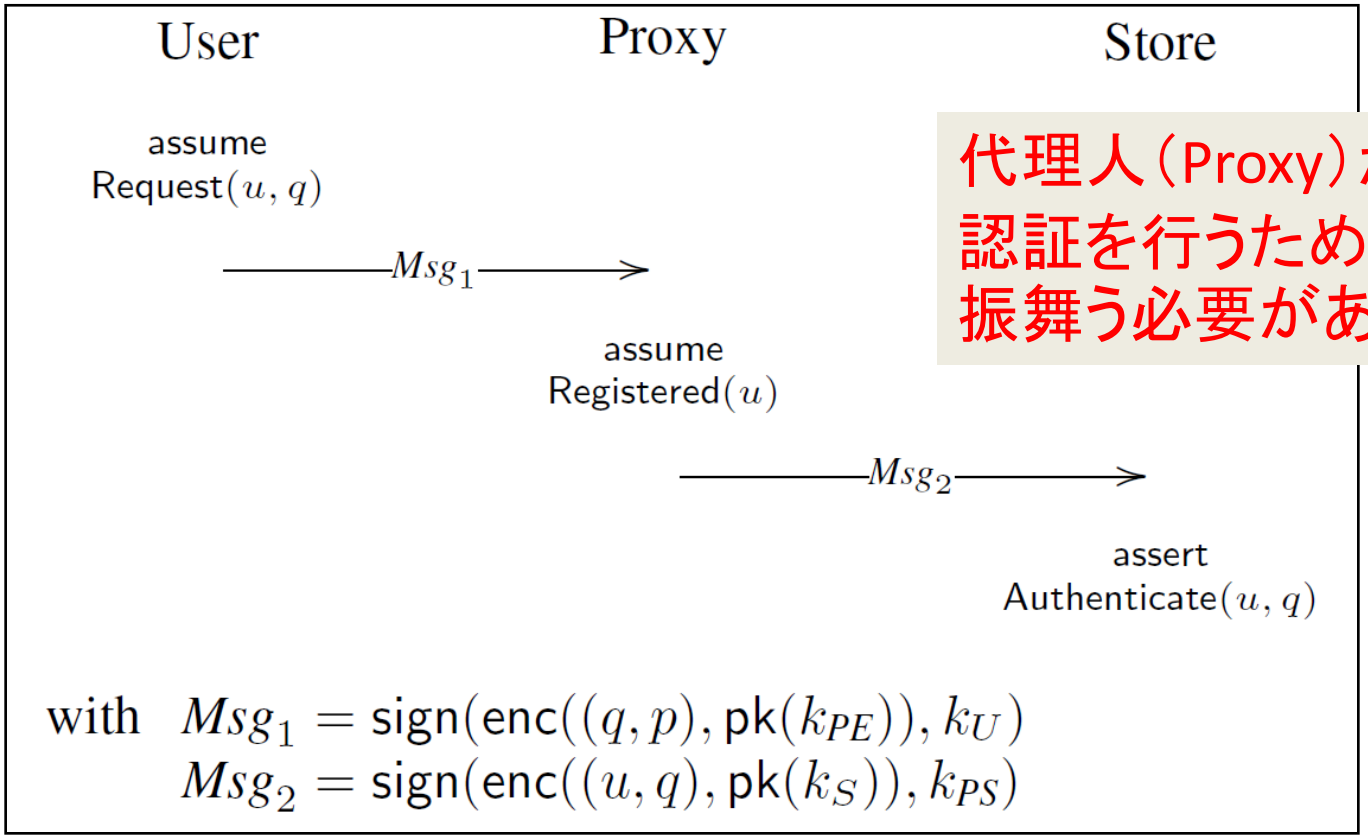
Achieving Security Despite Compromise Using Zero-knowledge

(M. Backes, M. Grochulla, C. Hriţcu and M. Maffei)

課題　プロトコルの参加者がプロトコルに従わない場合に、安全性でなくなる場合がある。

貢献
- プロトコルの変換法を提案。参加者は「プロトコルに従って動作したこと」の非対話ゼロ知識証明を送る。
- 変換後のプロトコルの安全性検証方法を提案
  ※変換により必ず安全になるとはいえないため

プロトコルの参加者がプロトコルに従わない場合に、
安全性でないプロトコルの例



代理人（Proxy）がユーザ（User）の認証を行うため、代理人が正しく振舞う必要がある。

変換後のプロトコルでは、代理人は「ユーザの認証を正しく行ったこと」を証明するゼロ知識証明を送信。
これにより、正しく動作したことを、署名鍵を漏らさずに商店（Store）に伝えることができる。

暗号化ハードウェアのAPIの提案と安全性証明

A Secure Cryptographic Token Interface
（C. Cachin and N. Chandran）

課題　暗号化ハードウェアのAPI（PKCS#11など）にセキュリティの欠陥が多く見つかっている。既存研究ではAPIの解析方法が提案されている。

貢献
- 安全なAPIを提案
- 安全性をゲームとして定義し、暗号・署名の安全性に帰着

API(PKCS#11)の欠陥例（Clulow, 2003）

攻撃者

pk, pl :
鍵k, lのID
(ポインタ)

wrap(pk, pl)

c（鍵lを鍵kで暗号化）

decrypt(pk, c)

l

暗号化ハードウェア

APIを用いて鍵lを盗みだせる

本研究のAPI

- 鍵の使用履歴を記録し、wrapとdecryptで同じ鍵の使用を禁止を禁止
- アクセス制御リストを用い、ユーザによる鍵へのアクセスを制御

無線ネットワークにおけるプロトコルの物理的性質のモデル化と検証

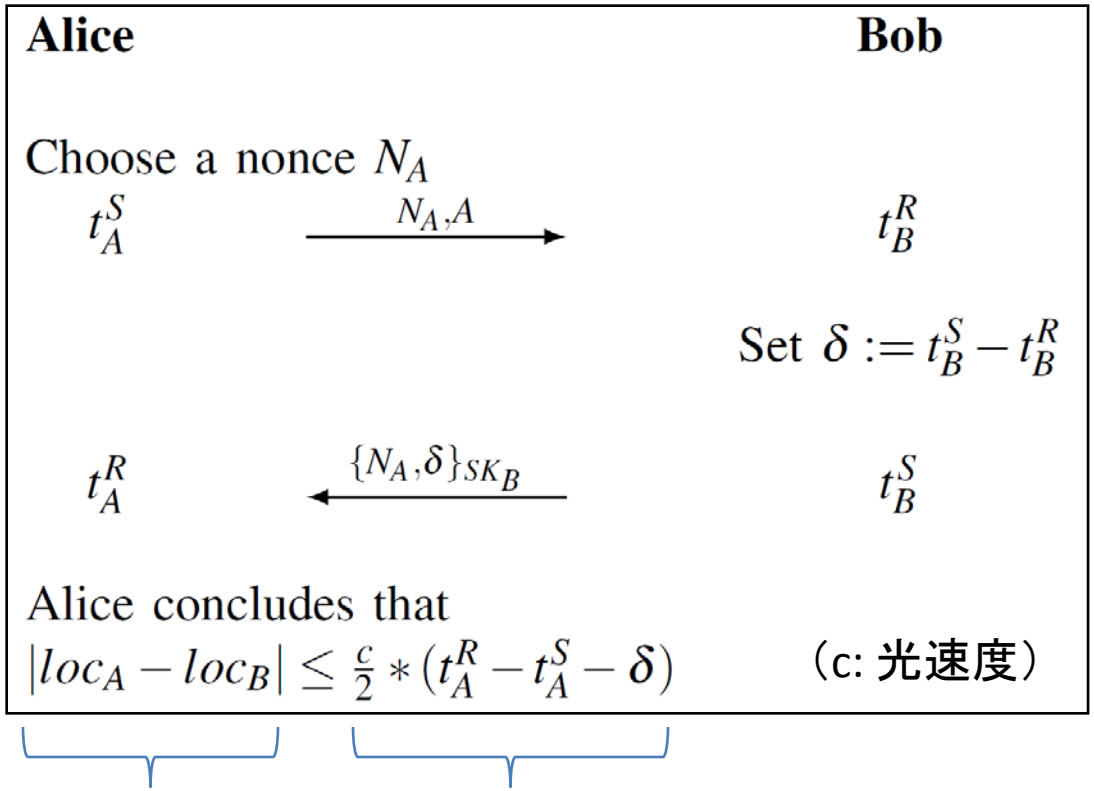
Modeling and Verifying Physical Properties of Security Protocols for Wireless Networks

（P. Schaller, B. Schmidt, D. Basin, and S. Capkun）

課題　鍵交換や認証プロトコルの解析方法は多くあるが、無線により参加者の物理的位置を検出するプロトコルのような、物理的性質に関するプロトコルの解析を行う方法はなかった。

貢献
- メッセージの伝送に必要な時間と、参加者間の距離との関係について推論するモデルを提案
- このモデルに基づいてプロトコルの安全性を検証。（定理証明支援系Isabelle/HOLを利用）

物理的位置を検出するプロトコル例（Authenticated Ranging Protocol)



両者の距離　　電波が直線的に飛んだ場合の到達可能距離

<u>提案モデル</u>

- 通信媒体（電磁波・音波）ごとの速度が定義されている
- 上の不等式を用いて距離を導出
- 物理的制約を受ける複数の攻撃者（≠単一の攻撃者）

非有界なネットワークにおける計算論的に健全な匿名性検証

Computational and Symbolic Anonymity in an Unbounded Network

（H. Comon-Lundh, 川本, 櫻田, 萩谷）

課題
- プロトコルの匿名性について、記号モデルの計算論的健全性を示す研究はこれまでなかった。
- 既存の計算論的健全性の研究は、ビット列を記号列にパーズできることを仮定していた。（ハッシュ関数などではこの仮定は成り立たない。）

貢献
- プロトコルの匿名性を検証するため、公開鍵暗号とリング署名を持つ記号モデルを提案。
- パーズを仮定しない健全性証明を与えた。

感想

- CSFでは、新しい課題に取り組んだ研究は高めに評価される（難しい課題でなくても）
- FCCは、計算論的安全性と記号的安全性の関連についてより深く研究・議論する場
- 研究の動向としては、プロトコルの仕様ではなく、それを実装したプログラムのレベルで安全性を検証する研究が増えつつある。

  （Microsoft Researchなど）