数理的技法による情報セキュリティの2024年度前半の研究動向

荒井 研一（長崎大学）
鈴木 幸太郎（豊橋技術科学大学）
中林 美郷（NTT社会情報研究所）
花谷 嘉一（東芝）
三重野 武彦（EPSON AVASYS）
山本 光晴（千葉大学）
吉田 真紀（情報通信研究機構）
米山 一樹（茨城大学）

発表概要

昨年度に引き続き

本分野の研究および実用化の促進を目的とし，

数理的技法による情報セキュリティの
最近の研究動向を紹介

- 各トップ会議における関連論文の発表件数や特色
- 全体を通したトレンド
- 関連論文の紹介

調査した国際会議

- IEEE S&P
- USENIX Security
- NDSS
- IEEE CSF
- CAV

セキュリティ4大会議

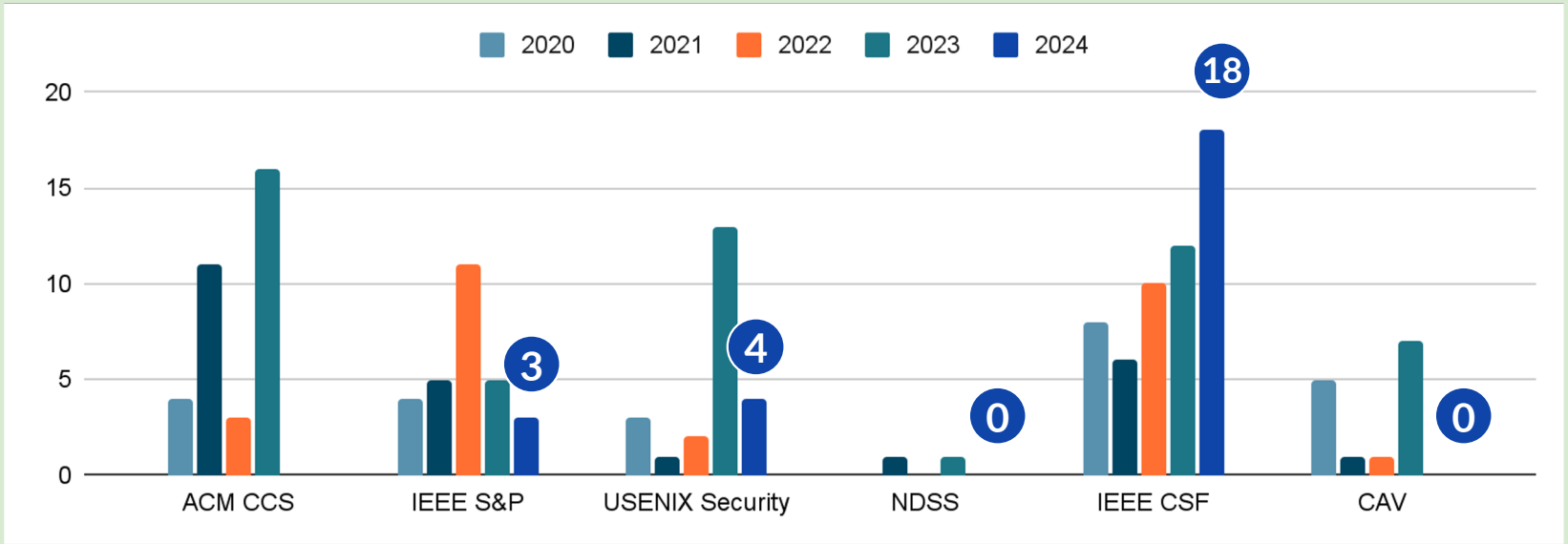
ACM CCSは年度後半のため
本発表の対象外

セキュリティ理論のトップ会議

自動検証のトップ会議

関連論文の発表件数

今回の対象は
全部で25件



収集基準（ただし，明らかに内容が遠いものは除く）

- タイトルまたはアブストラクトに Formalの語句が入る　または
- それらしいセッションにある（セキュリティの会議での Formal Analysis，CAVでのSecurityなど）

各会議の特色

ACM CCS

ACM Conference on Computer and Communications Security

暗号寄りの理論的な発表と実利用システム対象の実用的な発表がバランスよく含まれる．形式手法を用いた事例研究が盛ん．

IEEE S&P

IEEE Symposium on Security and Privacy

CCSと同じく理論・実用の両方が含まれるが，より実用を意識した発表が多い．形式手法を用いた事例研究が盛ん．

USENIX Security

評価実験による実証を伴う実利用システムの安全性解析に関する発表が多い．形式手法分野ではツールに関する発表が多め．

NDSS

Network and Distributed System Security

特に分散環境下でのシステムなどの安全性解析や安全な開発に関する実用的な発表が多い．
形式手法の応用は少なめ．

各会議の特色

IEEE CSF

Computer Security Foundations Symposium

形式手法によるセキュリティを主要なフォーカスの1つとした歴史ある会議．その後の研究に大きな影響を与えるような理論的な成果が集まる．

事例研究は少なく，フレームワークの提案や拡張，性質の証明，理論的限界の解明など理論系に関する発表が多い．

CAV

Computer Aided Verification

1980年代から続く形式検証分野のトップ会議．

検証の基礎となる理論から応用までを幅広くカバーする．

例年セキュリティのセッションもあるが，2024年は残念ながら無し．

本分野の研究テーマざっくり分類

① 具体的なシステムの安全性検証

標準化中のプロトコルや有名なシステムを検証.

新たな攻撃を発見しているとより評価される.

5件

② ツールの提案・拡張

新しいツールの提案や既存のツールの拡張など.

検証できるシステム・要件の範囲や抽象度，計算コストなどがポイント.

5件

③ 形式化手法の提案

安全性要件やシステムの形式化手法の提案などの理論的な成果.

自動判定手法と一緒に提案されることも多い.

15件

※複合的な研究の場合はメインの貢献で分類

よく見るキーワード –安全性要件–

記号論的安全性

暗号プリミティブは完全なものとして，メッセージや暗号文などは項として扱われる．通称Dolev-Yaoモデル．

```
type skey.
type pkey.

fun pk(skey): pkey.
fun aenc(bitstring, pkey):bitstring.

reduc forall m: bitstring, k: skey;
adec(aenc(m, pk(k)),k) = m.
```

秘密鍵を知らない限り
暗号文を復号できない

検証の自動化がしやすいが捉えられる攻撃の範囲が限定的．

計算論的安全性

暗号学者による安全性モデルの定義と同等の安全性．メッセージは文字列として扱われる．攻撃者は確率的チューリングマシン．

検証の完全な自動化は難しいが強い安全性が示せる．

「計算論的安全ならば記号論的安全」は
成り立つが逆は一般に成り立たない

よく見るキーワード　–ツール–

モデル検査ツール

システムの初期状態から到達できる状態を全て列挙するモデルを構築し，モデルが要件を満たしているかどうかを網羅的に検証する.

自動化しやすい.

ProVerif（記号論的安全性），CryptoVerif（計算論的安全性）など

定理証明支援系ツール

数学的な証明を形式言語を用いて記述し，その厳密さを確かめる.

完全な自動化は難しく，インタラクティブな証明が一般的.

Tamarin Prover（記号論的安全性），EasyCrypt（計算論的安全性），Coq，Isabelle/HOL，Agda（数学一般）など

① 具体的なシステムの安全性検証論文

キーワード：X.509，耐量子，DRM，SCTP

タイトル	会議	対象	安全性	貢献	手法（ツール）
ARMOR: A Formally Verified Implementation of X.509 Certificate Chain Validation	S&P	X.509証明書チェーン検証ロジック (X.509 CCVL)	証明書チェーンがRFC 5280に準拠していること	ARMORと呼ばれる形式検証による正当性が保証されたX.509 CCVLの実装を導入．いくつかの不適合を検出．	Agda
Verification of Correctness and Security Properties for CRYSTALS-KYBER	CSF	耐量子計算機暗号CRYSTALS-KYBER	δ-correctness	Isabelleを用いてKyberのPKEスキームの形式化とIND-CPA安全性を証明．	Isabelle/HOL
Formal Security Analysis of Widevine through the W3C EME Standard	USENIX	GoogleのDigital Rights Management (Widevine)	機密性，完全性，ライセンス有効期限に焦点を当てた7つの安全性要件	Tamarin Proverを用いてWidevine EMEの安全性を検証し重大な脆弱性を発見．検証済みの修正版を提案．	Tamarin Prover
Formal verification of the PQXDH Post-Quantum key agreement protocol for end-to-end secure messaging	USENIX	E2Eメッセージング用耐量子非同期鍵交換プロトコルPQXDH	相互認証，耐量子フォワード安全性	PQXDHプロトコルに対して初めて形式化と検証を行い，7つの潜在的脆弱性発見．	ProVerif, CryptoVerif
A Formal Analysis of SCTP: Attack Synthesis and Patch Verification	USENIX	トランスポートプロトコルSCTP	正当性，可用性（DoS攻撃耐性など）	RFC仕様に対して初めて形式化と正当性の検証を行い，4つの攻撃者モデルに対して攻撃の発見，パッチの有効性を実証．	モデル検査器SPIN，トランスポートプロトコル用攻撃生成ツールKORG

② ツールの提案・拡張論文

キーワード：ファジング，Wasm，セルラーネットワーク，CryptVerif

タイトル	会議	対象	安全性	貢献	手法（ツール）
DY Fuzzing: Formal Dolev-Yao Models Meet Cryptographic Protocol Fuzz Testing	S&P	暗号プロトコルの実装（検証事例：OpenSSL，LibreSSL. wolfSSL，libssh）	メモリ安全性，Dolev-Yao攻撃者に対する安全性	DY攻撃を考慮したファジング自動検証フレームワークDY Fuzzingを提案し，主要な暗号ライブラリの4つの未知の脆弱性を発見.	DY Fuzzing
Dealing with Dynamic Key Compromise in CryptoVerif	CSF	鍵の漏洩が考慮される暗号プロトコル	forward securityなどを含む鍵の漏洩の下での安全性	CryptoVerifをdynamic key compromiseが扱える機能を追加して拡張.	CryptoVerif
Wappler: Sound Reachability Analysis for WebAssembly	CSF	低レベル言語WebAssembly (Wasm)	メモリアクセス制限，整数オーバーフロー，アサーションチェックなど	Wasm用の健全かつ自動静的解析技術WAPPLERを提案.	定理証明器Z3
Post-quantum sound CryptoVerif and verification of hybrid TLS and SSH key-exchanges	CSF	耐量子計算機暗号を使ったプロトコル	秘匿性，対応性，識別不可能性	CryptoVerifを耐量子健全なものに拡張し，SSHとTLSの耐量子鍵交換の検証に適用.	CryptoVerif
Hermes: Unlocking Security Analysis of Cellular Network Protocols by Synthesizing Finite State Machines from Natural Language Specifications	USENIX	セルラーネットワークプロトコル	ダウングレード攻撃・DoS攻撃などへの耐性を含む20個の性質	自然言語から形式モデルを自動的に抽出する枠組みHermesを提案し，4Gと5Gの設計に対して既知の脆弱性19件と新たな脆弱性3件を検出.	ニューラル構文解析モデル，モデル検査

③ 形式化手法の提案論文(1/4)

キーワード：暗号通貨，Assertion，命令型，プライバシ, Sumcheck

タイトル	会議	対象	安全性	貢献	手法（ツール）
Formal Model-Driven Analysis of Resilience of GossipSub to Attacks from Misbehaving Peers	S&P	暗号通貨に応用されるP2P通信プロトコルGossipSub	公平性（不正者にペナルティ）	GossipSubと公平性を初めて形式化し，Eth2.0への応用で攻撃発見.	Lispベースの定理証明器ACL2s
Solving the insecurity problem for assertions	CSF	Assertionを含む暗号プロトコル（電子投票プロトコルなど）	機密性など	等式，存在量化子，論理積・和を含む論理的記述を持つプロトコルの安全性を検証する問題はNP に属することを証明.	ヒューリスティック
Security Properties through the Lens of Modal Logic	CSF	（命令型言語で書かれた）プログラム	機密性，完全性など	様相論理を用いたシステムの安全性要件を推論するためのフレームワークを導入.	様相論理
A Decision Procedure for Alpha-Beta Privacy for a Bounded Number of Transitions	CSF	暗号プロトコル	プライバシ	(α, β)-プライバシというプライバシ要件の自動検証手順を提案し，プロトタイプを実装.	（実装のために）SMTソルバー
Formal Verification of the Sumcheck Protocol	CSF	多項式を複数の入力で評価した結果の和になっていることを証明するsumcheck protocol	soundnessとcompleteness	一般化されたsumcheck protocolの安全性を証明	Isabelle/HOL

③ 形式化手法の提案論文(2/4)

キーワード：プライバシ，Sancus，Spectre

タイトル	会議	対象	安全性	貢献	手法（ツール）
Epistemic Model Checking for Privacy	CSF	暗号プロトコル	一般的なプライバシ要件やリストのメンバーシップに関するプライバシ	認識論理に基づくプライバシ論理 (PL)を導入．Dolev-Yaoモデルと組み合わせてプライバシ特性を統一的に表現・検証できるようにし．プロトタイプを実装.	認識論理
Bridging the Gap: Automated Analysis of Sancus	CSF	エンクレーブ実行をサポートした組込デバイス向けセキュリティアーキテクチャ Sancus	非干渉性（タイミング攻撃の有無など）	形式モデルでは安全だが実装上で安全でないケースなどのギャップを解消するためのモデル化・検証手法を提案.	アクティブ・オートマトン学習を用いた対話による形式モデル構築，自動検証ツール ALVIE
Relative Security: Formally Modeling and (Dis)Proving Resilience Against Semantic Optimization Vulnerabilities	CSF	セマンティック最適化を備えたプロセッサ	タイミングベースのサイドチャネル攻撃耐性	脆弱性と安全性をモデル化し，その検証手法を提案．標準的な Spectre の形式化と検証事例を提示.	定理証明器 Isabelle/HOL

③ 形式化手法の提案論文(3/4)

キーワード：確率論的論理，分散システム，IDアテステーション

タイトル	会議	対象	安全性	貢献	手法（ツール）
A Probabilistic Logic for Concrete Security	CSF	暗号プロトコル	計算完全記号攻撃者に対する安全性	暗号推論のための確率論的論理をセキュリティ設定に拡張し，その証明システムを提案.	証明支援システムSquirrel
Nothing is out-of-band: formal modeling of ceremonies	CSF	パーティの型を任意に一般化した分散システム	投票における対応性など	分散システムのパーティ間の相互作用をモデル化する形式的枠組を提案し，Tamarinでプロトタイプ実装.	Tamarin Prover
A Logic of Sattestation	CSF	SATAs (Self-Authenticating Traditional Adresses, 公開鍵へのコミットメントがアドレス自体に含まれているURLまたはDNSアドレス)	IDのAttestationの信頼性	IDのAttestationについての形式言語，公理的論理とそれらに対するKripke意味論を導入しし，その健全性を証明. 最初の信頼についてのステートメントから導出可能なすべての信頼ステートメントを列挙するアルゴリズムを与えた.	ヒューリスティック

③ 形式化手法の提案論文(4/4)

セキュリティポリシー，確率的機密性，計算量的独立性，分離論理，リアルタイムシステム

タイトル	会議	対象	安全性	貢献	手法（ツール）
Brewer-Nash Scrutinised: Mechanised Checking of Policies featuring Write Revocation	CSF	セキュリティポリシーモデル	Brewer-Nashセキュリティポリシーモデル	Brewer-Nashセキュリティポリシーモデルの定義を再検討し，{log}とCoqを用いて関連定理を証明.	{log}，Coq
Probability from Possibility: Probabilistic Confidentiality for Storage Systems Under Nondeterminism	CSF	ストレージシステム	出力の確率分布が秘密情報に依存することによる漏洩をモデル化したprobabilistic confidentiality	probabilistic confidentialityを定式化したモデルRDNIを提案し，RDNIについて安全性が証明されたなファイルシステムConFsをを実装.	Coq，Haskell
On Separation Logic, Computational Independence, and Pseudorandomness	CSF	暗号プリミティブ全般	計算量的独立性	計算量的な独立性の概念を提案し，それを用いて暗号プリミティブの安全性証明が簡明に記述できることを証明.	separation logic
Deciding branching hyperproperties for real time systems CSF'24 Distinguished paper award	CSF	メトリック時間論理の分岐時間，超特性拡張に関する計算問題	リアルタイムシステムのセキュリティ特性	区間ベースと点ベースの両方のセマンティクスのタイムドオートマトンに対してリアルタイムシステムの安全性を検証し，検証問題が決定不能であることを証明.	HCMTL*と次元オートマトン

全体を通したトレンド

- 具体的な検証対象は複雑化，多様化している.
- 耐量子分野への応用が期待されている.
- （CSF論文が多めということもあり）形式化手法に関する理論的な成果が多かった.

（参考）昨年度の全体を通したトレンド

全体を通したトレンド

- 暗号プリミティブ/プロトコルの実装への検証ツールの提案が多い
- 具体的なプロトコルの検証論文は少ない
- プロトコルの検証ツールはProVerifとTamarinの二強
- 検証要件では機密性・認証に加えてプライバシの検証が多くなってきている

個別紹介 –形式検証技術の耐量子暗号への応用–

3件の関連論文あり

- Verification of Correctness and Security Properties for CRYSTALS-KYBER（CSF 2024）
- Formal verification of the PQXDH Post-Quantum key agreement protocol for end-to-end secure messaging（USENIX2024）
- Post-quantum sound CryptoVerif and verification of hybrid TLS and SSH key-exchanges（CSF 2024）
- 【番外編】Formally Verifying Kyber Episode V: Machine-checked IND-CCA security and correctness of ML-KEM in EasyCrypt（Crypto 2024）
- 【番外編】Integrating Formal Verification in Cryptographic Standards and Implementations（Crypto 2024招待講演）

耐量子計算機暗号（PQC）の社会実装が進む中，形式検証技術を用いたPQCの安全性検証に関する論文が2024年のトップ会議で多数採録！

標準化やプロトコルの設計プロセスに形式検証技術を取り入れることの有用性が評価されている.

個別紹介 –形式検証技術の耐量子計算機暗号への応用–

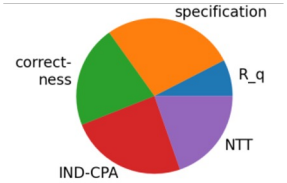
使っているツールや検証対象の安全性が異なる

NIST PQC標準化で取り上げられている方式の検証

Verification of Correctness and Security Properties for CRYSTALS-KYBER（CSF 2024，K. Kreuzer）

定理証明器Isabelleとその暗号用ライブラリCryptHOLを用いてCRYSTALS-Kyber※の公開鍵暗号方式のδ-correctness，IND-CPA安全性の証明を厳密化.

Isabelleのコードは約6.7k行.



コードの内訳

【番外編】 Formally Verifying Kyber Episode V: Machine-checked IND-CCA security and correctness of ML-KEM in EasyCrypt（Crypto 2024，J. B. Almeida et al.）

定理証明器EasyCryptを用いてML-KEM※のcorrectness，IND-CCA安全性を証明.

さらにプログラミング言語Jasminで記述されたML-KEMの実装の安全性と実装がNISTの仕様と合っていることを検証.

※CRYSTALS-KyberとML-KEMは同一の方式を指す（CRYSTALS-KyberはML-KEMに名称変更された）.

個別紹介 –形式検証技術の耐量子暗号への応用–

PQC向けのモデル検査ツールの開発・利用

Formal verification of the PQXDH Post-Quantum key agreement protocol for end-to-end secure messaging
（USENIX2024，K. Bhargavan et al.）

E2Eメッセージング用非同期鍵交換プロトコルPQXDH（PostQuantum Extended Diffie-Hellman）の相互認証，耐量子前方安全性を検証し，v1仕様における7つの潜在的な脆弱性を発見．Signal実装の場合の安全性を証明.

ProVerifとCryptoVerifを組み合わせて使用し安全性を保証するための適切な仮定を探索.

Post-quantum sound CryptoVerif and verification of hybrid TLS and SSH key-exchanges
（CSF 2024，B. Blanchet et al.）

形式検証ツールCryptoVerifを耐量子健全に拡張し，SSHとTLSの耐量子版を検証.

従来のCryptoVerifの攻撃者は古典的な攻撃者のみを対象としていたが，ブラックボックスの対話的な攻撃者を設計し計算能力を暗号的仮定のみによって制約することで耐量子健全な攻撃者を実現.

まとめ

- 数理的技法による情報セキュリティ分野の2024年度前半の研究動向を紹介.
- セキュリティのトップ会議では多数の同分野の論文が採択されている（S&P 3本，USENIX 4本，CSF 18本）.
  - 具体的な検証対象は複雑化，多様化.
  - 耐量子分野への応用が活発化.
  - 形式化手法に関する理論的な成果も多く採択.