数理的技法による情報セキュリティの最近の研究動向2024

中林 美郷（NTT社会情報研究所）
鈴木 幸太郎（豊橋技術科学大学）
花谷 嘉一（東芝）
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

昨年に引き続き

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

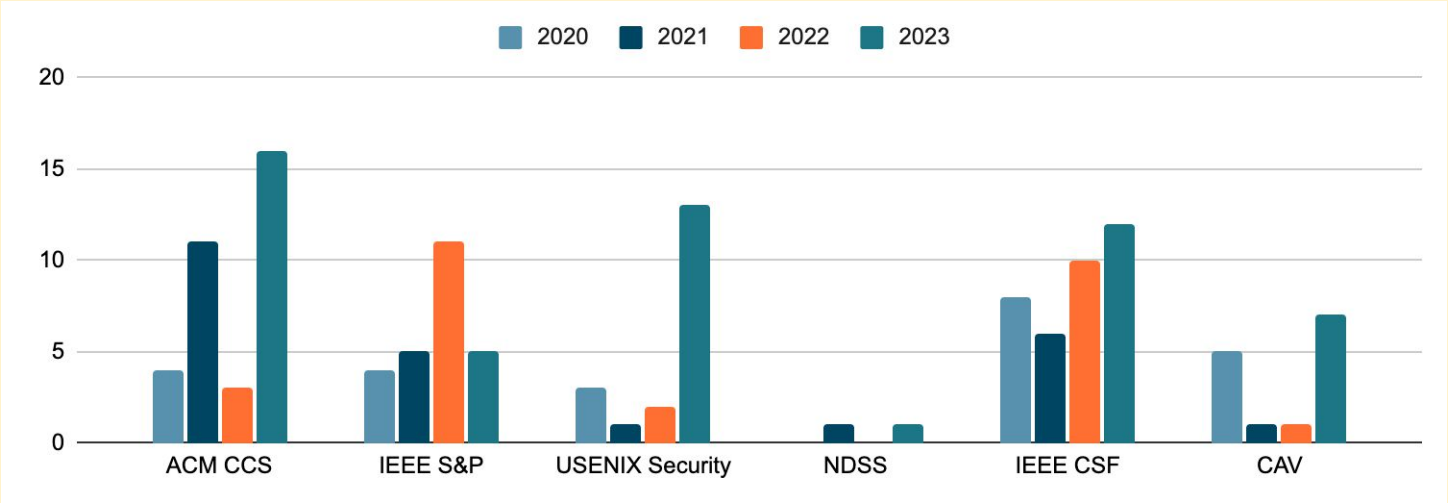
- ACM CCS
- IEEE S&P
- USENIX Security
- NDSS
- IEEE CSF
- CAV

セキュリティ4大会議

理論のトップ会議

検証のトップ会議

関連論文の発表件数



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（セキュリティ会議でのFormal Analysis，CAVでのSecurityなど）

各会議の特色

ACM CCS

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

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

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

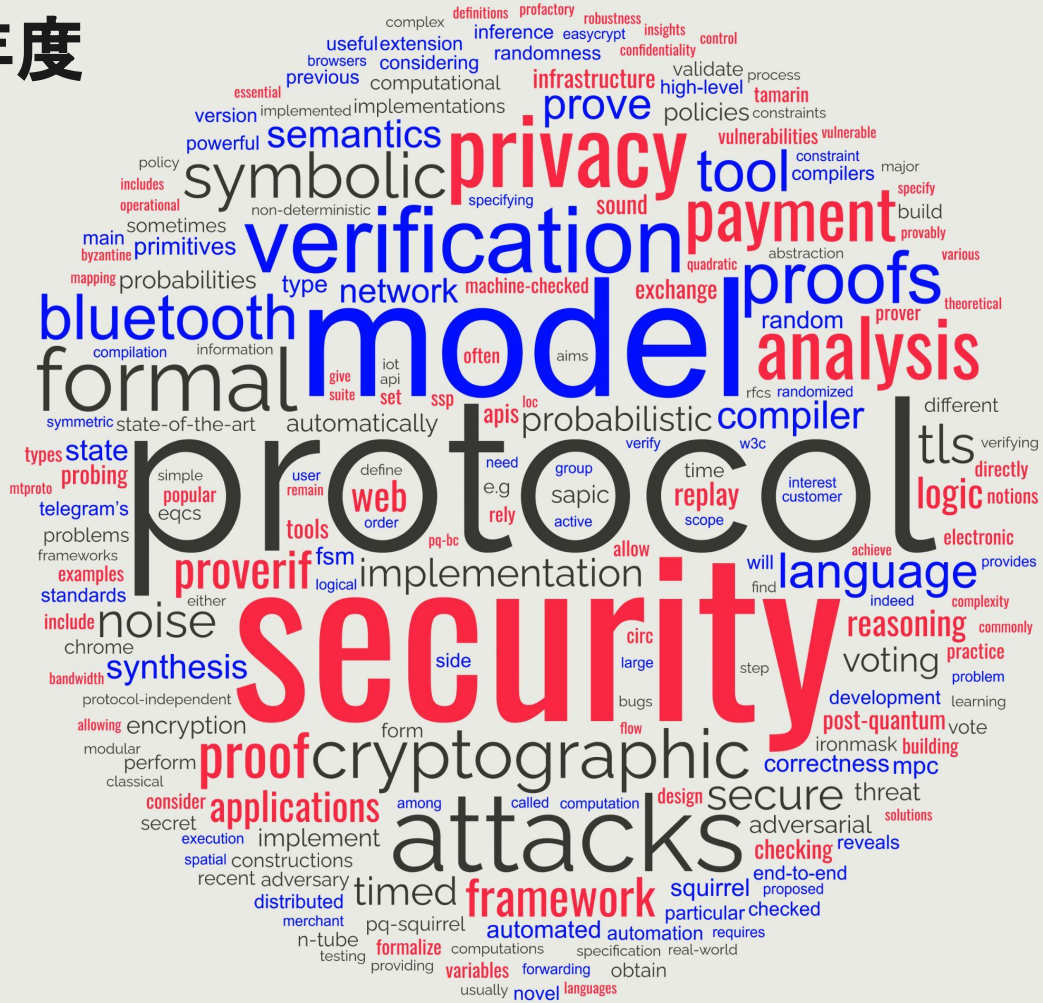
形式手法によるセキュリティを主要なフォーカスの1つとした
歴史ある会議．その後の研究に大きな影響を与えるような理論的な成果が集まる．
事例研究は少なく，フレームワークの提案や拡張，性質の証明，理論的限界の解明などに関する発表が多い．

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．

対象がプロトコルに限らない研究が多くなってきた？

比較:2022年度


complex
definitions
profactory
robustness
inference
easycrypt
insights
control
useful
extension
randomness
confidentiality
browsers
considering
validate
process
previous
computational
infrastructure
high-level
tamarin
essential
implementations
prove
policies
constraints
version
implemented
powerful
semantics
privacy
vulnerabilities
vulnerable
policy
symbolic
tool
constraint
compilers
major
includes
specifying
sound
specify
operational
non-deterministic
payment
build
sometimes
verification
provably
main
primitives
abstraction
various
byzantine
quadratic
mapping
probabilities
type
network
machine-checked
exchange
proofs
bluetooth
model
random
prover
theoretical
compilation
information
formal
often
aims
analysis
give
iot
api
suite
set
ssp
loc
rfcs
randomized
different
symmetric
state-of-the-art
automatically
apis
probabilistic
compiler
types
state
protocol
verify
w3c
tls
verifying
mtproto
probing
simple
user
define
need
time
directly
popular
remain
web
e.g
group
replay
interest
customer
logic
notions
telegram's
eqcs
order
sapic
rely
active
scope
problems
tools
pq-bc
electronic
frameworks
allow
achieve
examples
proverif
fsm
implementation
will
language
provides
standards
logical
find
either
indeed
complexity
include
noise
security
reasoning
commonly
chrome
circ
voting
practice
bandwidth
synthesis
side
large
step
problem
protocol-independent
bugs
development
learning
allowing
encryption
form
flow
post-quantum
vote
modular
perform
proof
cryptographic
ironmask
building
classical
correctness
mpc
consider
applications
among
called
computation
design
secure
threat
secret
attacks
adversarial
solutions
execution
implement
checking
reveals
spatial
constructions
recent
adversary
timed
framework
squirrel
end-to-end
distributed
proposed
particular
checked
merchant
pq-squirrel
automated
automation
requires
n-tube
testing
formalize
computations
specification
real-world
providing
variables
forwarding
obtain
usually
novel
languages

2023年の関連論文の紹介（1/14）

- 攻撃発見
- ツール拡張・提案
- 形式化・その他

タイトル	会議	対象	安全性	貢献	手法（ツール）
Extrapolating Formal Analysis to Uncover Attacks in Bluetooth Passkey Entry Pairing	NDSS	Bluetoothのペアリング	ペアリングの認証性	3つの既知の攻撃の再発見と2つの新たな攻撃の発見	Tamarin Prover
Token meets Wallet: Formalizing Privacy and Revocation for FIDO2	S&P	FIDO2	なりすまし不可能生，Unlinkability,	プライバシを考慮したWebAuthnの検証モデルを提案	
★ Owl: Compositional Verification of Security Protocols via an Information-Flow Type System	S&P	暗号プロトコル	計算論的安全性	自動検証と検証のモジュール性を両立したツールOwlの提案	Owl（提案）
Sound Verification of Security Protocols: From Design to Interoperable Implementations	S&P	暗号プロトコルの実装	記号論的検証における安全性	記号論的検証における安全性を保存する実装の入出力仕様の抽出法を提案	Tamarin Prover, Gobrafor Go, Verifastfor JAVA, Nagini for Python

2023年の関連論文の紹介(2/14)

- 攻撃発見
- ツール拡張・提案
- 形式化・その他

タイトル	会議	対象	安全性	貢献	手法(ツール)
Typing High-Speed Cryptography against Spectre v1	S&P	暗号ライブラリの実装	タイミング攻撃耐性	Spectre v1攻撃に耐性を持つ効率の良い暗号実装を書くためのアプローチを提案	型システム
AUC: Accountable Universal Composability	S&P	Universal Composabilityモデル	責任追跡性 (Accountability)	UCモデルにおける責任追跡性のための初の汎用フレームワークAUCを提案	
Indistinguishability Beyond Diff-Equivalence in ProVerif	CSF	匿名認証や電子投票などの暗号プロトコル	Unlinkability, Anonymity, Voting privacy	may-testing, 観測的等価性, pre-ordersなどをProVeriffで検証可能にする変換手法を提案	ProVerif
Zero-Knowledge in EasyCrypt	CSF	Σプロトコル	完全性, 健全性, ゼロ知識性 , Special soundness, 抽出可能性	EasyCryptにおいてΣプロトコルの安全性を証明	EasyCrypt

2023年の関連論文の紹介（3/14）

- 攻撃発見
- ツール拡張・提案
- 形式化・その他

タイトル	会議	対象	安全性	貢献	手法（ツール）
Election Verifiability with ProVerif	CSF	電子投票システム	プライバシ，検証可能性	検証可能性の証明のための補題ライブラリと汎用的なフレームワークを導入.	ProVerif
Election Verifiability in Receipt-free Voting Protocols	CSF	Receipt-Free電子投票プロトコル	検証可能性	Receipt-FreeプロトコルのProVerifによる検証方法を提案.	ProVerif
Proving Unlinkability using Proverif through Desynchronized Bi-Processes	CSF	RFID protocolなどの暗号プロトコル	Unlinkability	ProVerifでunlinkabilityのbi-process expressionを検証する変換手法を提案	ProVerif
Subterm-based proof techniques for improving the automation and scope of security protocol analysis	CSF	木構造，ハッシュチェーン，セッションカウンタ	秘匿性，フォワード安全性，認証性，リプレイ攻撃耐性，リンク不可能性	Unboundedに項の深さが伸びる状況の表現能力の向上，自動化効率（時間，マニュアル操作の排除）の向上	部分項の概念を導入したTamarin拡張

2023年の関連論文の紹介（4/14）

- 攻撃発見
- ツール拡張・提案
- 形式化・その他

タイトル	会議	対象	安全性	貢献	手法（ツール）
Extending the Authentication Hierarchy with One-Way Agreement	CSF	一方向認証（リモートアテステーション）	Aliveness, 一方向(non-)Injective Agreement	Loweの（双方向）認証階層を一方向に拡張し従来の性質との関係を証明	Tamarin Prover
HoRStify: Sound Security Analysis of Smart Contracts	CSF	イーサリアムのスマートコントラクト	依存関係と呼ばれる二種の不干渉的性質	依存関係を静的解析する初めての健全な手法を提案	健全かつ静的なプログラムスライシング
Towards End-to-End Verified TEEs via Verified Interface Conformance and Certified Compilers	CSF	TEE	Non-interference property	ソースコードの検証結果を用いてコンパイル済みバイナリコードの安全性を保証する手法を提案	Corinthian Abstract State Machine (CASM)
Formalizing Stack Safety as a Security Property	CSF	コンパイラ・ランタイム・ハードウェア	関数のコールスタックに関する安全性	スタックの安全性に関する新しい特徴付けを与え，既存のメカニズムが安全性を満たさないことを発見	Coq

2023年の関連論文の紹介（5/14）

- 攻撃発見
- ツール拡張・提案
- 形式化・その他

タイトル	会議	対象	安全性	貢献	手法（ツール）
A generic framework to develop and verify security mechanisms at the microarchitectural level: application to control-flow integrity	CSF	ハードウェアシステム	ハードウェアレベル(特にマイクロアーキテクチャレベル)の安全性要件一般	ハードウェア開発における安全性要件を記述・証明するための現実的な手法の提案と例証	Coq
π_RA: A π-calculus for Verifying Protocols that Use Remote Attestation	CSF	リモートアテステーション	相互認証性	リモートアテステーションの安全性検証を可能にするために応用π計算を拡張	πRA
Symbolic Quantum Simulation with Quasimodo [Tool Paper]	CAV	量子回路	（シミュレーション，デバッグ，）出力の性質の検証	量子回路の記号的検証シミュレーション用のPythonライブラリを提案	Quasimodo（提案）
AutoQ: An Automata-based Quantum Circuit Verifier [Tool Paper]	CAV	量子回路	回路の実行前後の関係	オートマトンベースの量子回路シミュレーションツールを提案	AUTOQ（提案）

2023年の関連論文の紹介（6/14）

- 攻撃発見
- ツール拡張・提案
- 形式化・その他

タイトル	会議	対象	安全性	貢献	手法（ツール）
Formally Verified EVM Block-Optimizations [Tool Paper]	CAV	Ethereumスマートコントラクトの最適化	最適化前後の正当性	EVMブロックのシンボリック実行から状態を記号化し，最適化前後の意味的等価性を証明	Coq
Verifying the Verifier: eBPF Range Analysis Verification	CAV	eBPF（カーネル空間で動作する機能拡張用仮想マシン）	eBPF検証器の健全性	検証器のソースコードから一階述語論理変換，健全性条件の導出，健全性検証を自動化	Agni（提案），SMTソルバ
Bounded Verification for Finite-Field-Blasting (in a Compiler for Zero Knowledge Proofs)	CAV	ゼロ知識証明 (ZKP) コンパイラ	ZKP対象の命題から数式への変換の正当性	ブール論理とビットベクトル論理を変換する処理の検証手法の提案，CirC ZKPコンパイラへの実装，バグの発見	ドメイン固有言語 (DSL)であるAlive
SR-SFLL: Structurally Robust Stripped Functionality Logic Locking	CAV	集積回路 (IC)のロジックロッキング	ICの構造分析攻撃への頑強性	構造分析攻撃に堅牢なストリップ機能ロジックロック (SR-SFLL) を提案	SAT ソルバーに基づく回路合成

2023年の関連論文の紹介（7/14）

- 攻撃発見
- ツール拡張・提案
- 形式化・その他

タイトル	会議	対象	安全性	貢献	手法（ツール）
CoqCryptoLine: A Verified Model Checker with Certified Results [Tool Paper]	CAV	暗号に関する複雑な非線形整数計算を行うアセンブリプログラム	実装の機能的正当性	検証済モデル検査器を提供	Coq, MathCom, Singular, CoqQFBV
A comprehensive, formal and automated analysis of the EDHOC protocol	USENIX	IoTデバイス向け鍵交換プロトコル EDHOC	機密性、認証性、アイデンティティ保護、否認防止	バージョン12に対する弱点を発見し緩和策を提案（ver. 14で採用）	Sapic+
★ Hash Gone Bad: Automated discovery of protocol attacks that exploit hash function weaknesses	USENIX	暗号学的ハッシュ関数を利用したプロトコル	秘匿性、認証性、データの対応関係など	脆弱なハッシュ関数を利用した場合のセキュリティプロトコルの安全性を自動で検証する方法を開発	Tamarin, ProVerif
Automated Analysis of Protocols that use Authenticated Encryption: How Subtle AEAD Differences can impact Protocol Security	USENIX	AEADを使用する暗号プロトコル	鍵の機密性，認証，Accountability, Agreement	AEADの性質を悪用する攻撃を検証する手法を開発．いくつかの攻撃を再発見．	Tamarin

2023年の関連論文の紹介（8/14）

- 攻撃発見
- ツール拡張・提案
- 形式化・その他

タイトル	会議	対象	安全性	貢献	手法（ツール）
Machine-checking Multi-Round Proofs of Shuffle: Terelius-Wikstrom and Bayer-Groth	USENIX	シャッフル	完全生，健全性，ゼロ知識性	複雑な場合のシャッフルの形式的な証明を与えた	Coq
Automated Security Analysis of Exposure Notification Systems	USENIX	感染者接触通知フレームワーク	健全性（誤ったリスク通知が起きない）	接触通知フレームワークの健全性の初めての形式検証	Tamarin
Formal Analysis of SPDM: Security Protocol and Data Model version 1.2	USENIX	SPDM（DMTFによって標準化されているHW間有線通信用のセキュリティプロトコル）	認証性、ハンドシェイク鍵の秘匿性とフォワード安全性	SPDMの全3種類のハンドシェイクモードやオプション実行を含む初めての形式検証を与え，潜在的な設計上の欠陥を発見	Tamarin
TreeSync: Authenticated Group Management for Messaging Layer Security	USENIX	メッセージング層セキュリティのための非同期グループメッセージングプロトコル	グループ状態の一貫性、整合性、認証	MLS に対してテスト可能かつ機械検証された最初の形式仕様を提示し，そこから完全なMLSプロトコルを実装する方法を提案	プログラミング言語F，Dolev-Yao検証手法DY*

2023年の関連論文の紹介（9/14）

- 攻撃発見
- ツール拡張・提案
- 形式化・その他

Formal Analysis of Session-Handling in Secure Messaging: Lifting Security from Sessions to Conversations	USENIX	セッション処理層も含めたメッセージング層セキュリティ	Forward Secrecy (FS), Post-Compromise Security (PCS)	Signalのセッション処理層の安全性解析，PCSが侵害される可能性があるシナリオの特定，対策手法の提案	Tamarin
Design of Access Control Mechanisms in Systems-on-Chip with Formal Integrity Guarantees	USENIX	SoCレベルのアクセス制御システム	セキュリティクリティカルな操作の完全性	形式検証手法UPEC-OIを提案，OpenTitan の Earl Grey SoC で例証	Interval Property Checking (IPC, SATベースの形式検証技術)
Automated Inference on Financial Security of Ethereum Smart Contracts	USENIX	Ethereumのスマートコントラクト	財務的不変性・トランザクションに関する等価性	スマートコントラクトの再粒度解析のための自動推論システムを提案 549のコントラクトで他のツールと比較，1700のコントラクト中13についてバグを発見	Tamarin, Z3
A Verified Confidential Computing as a Service Framework for Privacy Preservation	USENIX	Confidential Computing	忘却証明（Proof of Being Forgotten）	エンクレーブ内の秘密に関わる忘却証明の定義と検証器を提案し、Rustで実装して評価	Rust言語向けのテイント解析ツールなど

2023年の関連論文の紹介（10/14）

- 攻撃発見
- ツール拡張・提案
- 形式化・その他

タイトル	会議	対象	安全性	貢献	手法（ツール）
Detecting Multi-Step IAM Attacks in AWS Environments via Model Checking	USENIX	AWSのIAM	不正な権限昇格などの攻撃耐性	IAMコンポーネントのモデルを抽出し，モデル検査手法を用いて検証する方法を提案	Z3
CipherH: Automated Detection of Ciphertext Side-channel Vulnerabilities in Cryptographic Implementations	USENIX	暗号ソフトウェア	サイドチャネル耐性	サイドチャネル攻撃耐性を検証するフレームワークを提案. RSAやECDSA/ECDHの実装に対する200以上の脆弱なポイントを発見	CipherH（提案）
Ou: Automating the Parallelization of Zero-Knowledge Protocols	CCS	ゼロ知識証明プロトコル		効率的なゼロ知識証明の作成をサポートするプログラミングフレームワークを提案	Ou, Lian（提案）
Comparse: Provably Secure Formats for Cryptographic Protocols	CCS	暗号プロトコル	フォーマット混乱攻撃などの攻撃耐性	暗号プロトコルにおけるデータ形式に依存する攻撃を検証するフレームワークを提案	Comparse（提案），F*

2023年の関連論文の紹介（11/14）

- 攻撃発見
- ツール拡張・提案
- 形式化・その他

タイトル	会議	対象	安全性	貢献	手法（ツール）
Formal Analysis of Access Control Mechanism of 5G Core Network	CCS	5Gコアネットワークのアクセス制御フレームワーク	不正アクセスへの耐性	5GコアNの形式モデルを与え，アクセス制御メカニズムの検証フレームワークを提案．新しい攻撃を発見	5GCVerif（提案），nuXmv
Security Verification of Low-Trust Architectures	CCS	Sequestered Encryption (SE) アーキテクチャ	秘密情報の機密性，サイドチャネル耐性	SEアーキテクチャの検証を行うフレームワークを提案し，いくつかのケーススタディを検証	Information Flow Tracking Tool
Lifting Network Protocol Implementation to Precise Format Specification with Security Applications	CCS	ネットワークプロトコルのソースコード		プロトコル実装からメッセージフォーマットを推測する静的解析ツールを開発	Netlifter（提案），Z3
CryptoBap: A Binary Analysis Platform for Cryptographic Protocols	CCS	暗号プロトコル	weak secrecy，認証性	プロトコルのバイナリから自動検証に適したモデルに変換するプラットフォームを提案	CryptoBap（提案），ProVerif，CryptoVerif

2023年の関連論文の紹介（12/14）

- 攻撃発見
- ツール拡張・提案
- 形式化・その他

タイトル	会議	対象	安全性	貢献	手法（ツール）
A Generic Methodology for the Modular Verification of Security Protocol Implementations	CCS	暗号プロトコルの実装	認証，機密性など	幅広い実装とプログラミング言語をサポートする暗号プロトコルの検証手法を提案	
Provably Unlinkable Smart Card-based Payments	CCS	スマートカードベースの支払いプロトコル	認証，機密性，プライバシ	プライバシを考慮した支払いプロトコルを提案し，その安全性を形式的に検証	ProVerif
CheckMate: Automated Game-Theoretic Security Reasoning	CCS	ブロックチェーンのトランザクション	ゲーム理論的な性質（Byzantine fault-tolerance, incentive-compatibility）	ゲーム理論に基づく健全かつ完全な自動検証フレームワークを提案	CheckMate（提案），SMTソルバ
A Novel Analysis of Utility in Privacy Pipelines, Using Kronecker Products and Quantitative Information Flow	CCS	プライバシパイプライン	プライバシの有用性	定量的情報フローに基づくプライバシの有用性の形式的な検証手法を提案	

2023年の関連論文の紹介（13/14）

- 攻撃発見
- ツール拡張・提案
- 形式化・その他

タイトル	会議	対象	安全性	貢献	手法（ツール）
Assume but Verify: Deductive Verification of Leaked Information in Concurrent Applications	CCS	コンカレントプログラム	情報の機密性	意図的に情報を漏洩するようなコンカレントプログラムに対して許可されていない情報が漏洩しないことを演繹的な手法で検証する手法を提案	Verdeca（提案）
Deciding Differential Privacy of Online Algorithms with Multiple Variables	CCS	オンラインのランダマイズアルゴリズム	差分プライバシ	差分プライバシのためのオートマトンモデルを定義し，オートマトンのクラスがPSPACE完全であることを示した	DiPAut（提案）
Formalizing, Verifying and Applying ISA Security Guarantees as Universal Contracts	CCS	命令セットアーキテクチャ	ユニバーサルコントラクトに対する安全性	命令セットアーキテクチャの実装を形式的に検証するための手法を導入	Katamaran（提案），Coq

2023年の関連論文の紹介（14/14）

- 攻撃発見
- ツール拡張・提案
- 形式化・その他

タイトル	会議	対象	安全性	貢献	手法（ツール）
Boosting the Performance of High-Assurance Cryptography: Parallel Execution and Optimizing Memory Access in Formally-Verified Line-Point Zero-Knowledge	CCS	暗号プロトコルの実装	計算論的安全性	暗号プロトコルの安全性検証済み実装を安全性を保証したまま最適化（高速化）する手法を提案	EasyCrypt
Galápagos: Developing Verified Low Level Cryptography on Heterogeneous Hardwares	CCS	暗号プリミティブの実装	実装に対する安全性	様々なISAによる暗号実装を検証するための拡張可能なフレームワークを提案	Galapagos（提案），SMTソルバー
Specification and Verification of Side-channel Security for Open-source Processors via Leakage Contracts	CCS	命令セットアーキテクチャ	サイドチャネル耐性など	ISAレベルのリークコントラクトに対してレジスタ転送レベルの設計を検証するためのツールを開発	LeaVe（提案）

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

個別論文紹介①

Owl: Compositional Verification of Security Protocols via an Information-Flow Type System

Joshua Gancher et al., S&P 2023

暗号プロトコルの計算論的安全性検証ツールOwlを提案

- 自動検証と結合可能安全性保証（それぞれ個別に安全ならば組み合わせた物も安全）を両立
- OWLコードからRustでの安全な実行可能コードが生成可能（ただし効率は度外視）
- RFID, Kerberos, DH鍵交換, などに適用して実証

個別論文紹介①

Owl: Compositional Verification of Security Protocols via an Information-Flow Type System (Joshua Gancher et al., S&P 2023)

- 計算論的安全性
  - 具体的なビット列や確率的な攻撃者モデルを考慮

- 従来の計算論的安全性検証ツールとOwlの比較

Tool		RF	Auto	Modular	CB	Link	TCB
CertiCrypt	[12]	◑	○	○	●	●	Coq
CryptHOL	[57]	◑	○	●	●	○	Isabelle
EasyCrypt	[13]	◑	○	●	●	●	self, SMT
FCF	[64]	◑	○	●	●	●	Coq
F*	[68]	◐	○	●	○	●	self, SMT
CryptoVerif	[23]	◐	●	◐	●	●	self
Squirrel	[7]	◑	○	◐	○	○	self
OWL		◐	●	●	○	●	self, SMT

Reasoning Focus (RF)
◐ – automation focus
◑ – expressiveness focus

Concrete Bounds (CB)
● – Yes
○ – No

Modular
● – tool is modular
◐ – modular with on-paper proofs

自動検証と結合可能
安全性保証を両立
↓
検証の利便性向上

個別論文紹介②

Best Paper

Hash Gone Bad: Automated discovery of protocol attacks that exploit hash function weaknesses

Vincent Cheval et al., USENIX 2023

ハッシュ関数の脆弱性を悪用するようなプロトコル攻撃を自動で発見する手法を提案

- 古典的な安全性定義では表現されていないハッシュ関数の現実世界の攻撃クラスの記号モデルを定義
- 等式理論を用いてそれらをProVerif/Tamarin Proverでモデリング

個別論文紹介②

Hash Gone Bad: Automated discovery of protocol attacks that exploit hash function weaknesses（Vincent Cheval et al., USENIX 2023）

- Tamarin ProverとProVerifを用いて実装し，20種のケーススタディを通じて過去に発見されたすべての攻撃といくつかの新しい亜種を発見

Protocol	Broken properties	Main attack requirements	New?	In-text ref.	Time (s)	Note
Sigma	Sec,Agr(transcript)	chsnPrfx,colExt	[9]	AT(S1)	28	
	Sec,Agr(transcript)	chsnPrfx,colExt	∼ [9]	AT(S2)	manual	collisions on shares
	Sec,Agr(transcript,role)	chsnPrfx	new	AT(S3)	55	role-confusion, no need for colExt
SSH	Agr(nego)	CI(*)	new	AT(SSH1)	3	see Figure 6
	Agr(nego)	idtclPrfx,colExt	[9]	AT(SSH2)	28	
	Agr(nego)	CI(I),sndPreImg,colExt	new	AT(SSH3)	41	
IKEv2	Sec(R)	CI(*)	new	AT(IKE1)	6	CI should be on the cookie
	Auth(I)	idtclPrfx,colExt	[9]	AT(IKE2)	20	
	Agr(cookie,transcript)	∃,colExt	new	AT(IKE3)	9	disagreement on cookies only
Flickr	Auth(I)	hashExt	[21]	AT(F)	9	