数理的技法による情報セキュリティの最近の研究動向

中林 美郷（NTT社会情報研究所）
吉田 真紀（国立研究開発法人 情報通信研究機構）
花谷 嘉一（東芝）
山本 光晴（千葉大学）
米山 一樹（茨城大学）

発表概要

数理的技法による情報セキュリティの最近（2021-2022）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

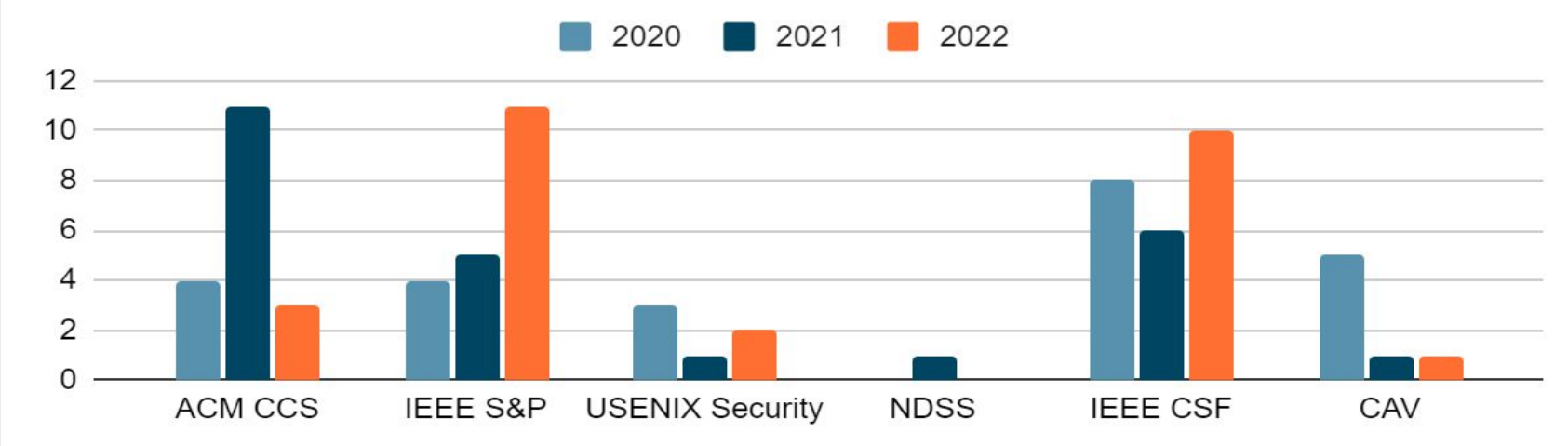
- ACM CCS
- IEEE S&P
- USENIX Security
- NDSS
- IEEE CSF
- CAV

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
  - 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（ 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
形式手法による情報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．

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

2022年の関連論文の紹介（1/7）

- 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）
Automated Attack Synthesis by Extracting Finite State Machines from Protocol Specification Documents	S&P	プロトコル（BGPv4, DCCP, LTP, PPTP, SCTP, TCP）	LTLで書かれた安全性	新たな攻撃発見	Spin, Korg
★ ProVerif with Lemmas, Induction, Fast Subsumption, and Much More	S&P	検証ツール ProVerif		ツールの拡張	ProVerif
Four Attacks and a Proof for Telegram	S&P	Telegram（MTProto）	秘匿性，完全性	新たな攻撃発見	手動
Noise: A Library of Verified High-Performance Secure Channel Protocol Implementations	S&P	Noise Protocol Framework	メッセージレベル安全性（機密性，認証など）	Noiseプロトコルコンパイラの検証済み実装を示す	F*

2022年の関連論文の紹介(2/7)

- 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 Logic and an Interactive Prover for the Computational Post-Quantum Security of Protocols	S&P	耐量子プロトコル	強秘匿性，認証，Unlinkability	BCロジックとSQUIRRELを拡張し，量子攻撃者に対して健全な検証器を開発	PQ-SQUIRREL
Versatile Verification of Masking Security	S&P	マスキング（サイドチャネル攻撃対策）	ランダム盗聴に対する安全性	ランダム盗聴に対する検証ツールを提案	IronMask（提案）
A Formal Security Analysis of the W3C Web Payment APIs: Attacks and Verification	S&P	Web Payment API	Webインフラモデル用に拡張されたDY攻撃者に対する安全性	WPAの安全性の定式化と評価，攻撃発見	手動
Cats vs. Spectre: An Axiomatic Approach to Modeling Speculative Execution Attacks	S&P	投機的コードを実行する並行性メモリモデルのマイクロアーキテクチャ	投機的実行攻撃SPECTER ファミリーに対する安全性	モデル化と分析のための軽量な公理的枠組みの提案	公理的アプローチCAT モデリング言語

2022年の関連論文の紹介(3/7)

- 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)
CirC: Compiler infrastructure for proof systems, software verification, and more	S&P	暗号証明システム(ゼロ知識証明など)		制約表現(SATやSMTなど)へのコンパイル構築基盤の構築	存在論的に定量化された回路
HAMRAZ: Resilient Partitioning and Replication	S&P	部分的な信頼しかないサブシステムを組み合わせたシステム	機密性・完全性・可用性, ビザンチン故障に対する耐性	分散システムの自動合成のための理論的基礎を構築、ツールHAMRAZとして実装	HAMRAZ (提案)
Formal Model-Driven Discovery of Bluetooth Protocol Design Vulnerabilities	S&P	Bluetoothプロトコルスイート(Classic, Low Energy, Mesh)	真正性, 機密性	5つの既知の脆弱性と2つの新規の問題を検出	ProVerif
A Formal Model of Checked C	CSF	Checked C	Spatial memory safety	安全性の定式化と検証	Coq

2022年の関連論文の紹介(4/7)

- 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)
N-Tube: Formally Verified Secure Bandwidth Reservation in Path-Aware Internet Architectures	CSF	ドメイン間帯域幅予約アルゴリズム	公平性, DDoSなど	アルゴリズムN-Tubeを提案し, 安全性を検証	手動, 統計モデル検査
How Efficient are Replay Attacks against Vote Privacy? A Formal Quantitative Analysis	CSF	投票プロトコル	リプレイ攻撃に対するプライバシー	リプレイ攻撃を分類し実際の投票結果を用いて攻撃の可能性を解析	Formal Quantitative Analysis Tool
Bringing State-Separating Proofs to EasyCrypt -- A Security Proof for Cryptobox	CSF	State-Separating Proofs (SSP)	ゲーム変換を用いた安全性	EasyCryptの形式化に応用して証明をモジュール化	EasyCrypt
Cracking the Stateful Nut -- Computational Proofs of Stateful Security Protocols using the Squirrel Proof Assistant	CSF	statefulなプロトコル(Yubi-Keyなど)	識別不可能安全、リプレイ攻撃耐性	可変な状態を扱えるように計算論的完全な記号論的攻撃者の論理を拡張	Squirrel Prover

2022年の関連論文の紹介(5/7)

- 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)
Symbolic protocol verification with dice: process equivalences in the presence of probabilities	CSF	確率的暗号プロトコル	確率的攻撃者に対する識別不可能安全	プロトコルと攻撃者の両方に非決定論的かつ確率的な枠組みを導入しDeepSecで検証可能であることを示す	応用π計算, DeepSec
So near and yet so far: formal verification of distance bounding protocols	CSF	近距離無線通信(NFC)タグを利用した非接触型決済	マフィア詐欺、遠隔ハイジャック攻撃、テロリスト攻撃	新たな証明と攻撃の発見	ProVerif
Machine-Checked Proofs of Privacy Against Malicious Boards for Selene & Co	CSF	投票用紙	プライバシー	セキュリティ概念mb-BPRIVを集計後の検証に対応させた安全性に拡張	EasyCrypt
Adversarial Robustness Verification and Attack Synthesis in Stochastic Systems	CSF	離散時間マルコフ鎖で表現されるシステム	Adversarial Robustness	安全性を形式化し，確率的モデル検査ツールで検証可能にする	PRISMなど

2022年の関連論文の紹介(6/7)

- 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)
	Adversary Safety by Construction in a Language of Cryptographic Protocols	CSF	暗号プロトコル	Ideal World仕様において自明に成立するか手で簡単に証明できる性質	2種類のDSL(Ideal /Real World)でそれぞれ記述されたプログラムが詳細化の関係にあることをモデル検査等を用いて示す	SPICY(提案)Coq上の実装4種類のプロトコルで評価
☆	Tidy: Symbolic Verification of Timed Cryptographic Protocols	CCS	Timed Cryptography	Reachability, Liveness, Indistinguishability	応用Pi計算を時間制約を扱えるように拡張し時間特性に関する論理を開発．Timed cryptographyを使ったいくつかのプロトコルを検証.	Tamarin Proverをバックエンドとして利用して自動的な証明を実現
☆	A Symbolic Analysis of Privacy for TLS 1.3 with Encrypted Client Hello	CCS	TLS1.3 ハンドシェイクプロトコル（ECH）	プライバシー	TLS1.3のプライバシーモデルを定義し，安全性を検証.	ProVerif

2022年の関連論文の紹介(7/7)

- 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)
★	Themis: an accountable on-site voting system with systematic cast-as-intended verification	CCS	オンサイト投票	プライバシ，検証可能性，部分的説明可能性	オンサイト投票プロトコルThemisの提案	ProVerif
	PoS4MPC: Automated Security Policy Synthesis for Secure Multi-Party Computation	CAV	秘密計算フレームワーク	シミュレーションベース安全性	安全性と効率がバランスする適切な秘密変数の自動設定を行うツールPoS4MPCの提案	型システム、記号論的推論
☆	SAPIC+: protocol verifiers of the world, unite!	USENIX	暗号プロトコル	プロトコルの到達可能性	Sapic+の記述からProVerif/DeepSecの入力への自動変換，変換の正しさの証明	SAPIC, ProVerif, Tamarin, DeepSec
	ProFactory: Improving IoT Security via Formalized Protocol Customization	USENIX	IoTプロトコル	メッセージ解析とネットワークステートマシン実装の不適切さ	フォーマルにプロトコルをモデル化し正確性を検査，安全なプロトコル実装を生成するPROFACTORY を提案	DSL (Domain Specific Language), ツールVCC, Frame-C

全体を通したトレンド

- プロトコル・安全性の多様化と複雑化
  - 投票プロトコルやプライバシー要件が人気？
- 半分弱はツールの提案（拡張）論文
  - 耐量子暗号プリミティブに対応したものも

個別論文紹介①

ProVerif with Lemmas, Induction, Fast Subsumption, and Much More (Bruno Blanchet et al., S&P 2022)

- セキュリティプロトコルのシンボリック検証ツールProVerifの拡張を行った.
  - ProVerifを補題，公理，帰納法による証明，自然数，時相的問い合わせで拡張．正確性を向上させ，より多くの場合で停止できるように.
  - ProVerifで使用されているアルゴリズムを最適化.
    大規模な例において大幅なスピードアップを実現.

個別論文紹介①

ProVerif with Lemmas, Inductions, Fast Subsumption, and Much More (Bruno Blanchet et al., S&P2022)

- Ver. 2.00とVer. 2.02pl1の比較

Protocol	Q	O	#	N	P	I	R	ℕ	A
published files									
PCV Otway-Rees	eq	✗	1	✓	x				
PCV Needham-Schroeder	inj	✗	6 3	✓ ↯	x	x			
PCV Denning-Sacco	inj	✗	1	↯					
JFK	cor inj	✗[1]	2 2	↯ ✓		x			
Arinc823	cor	✗	6	↯				x	
Helios-norevote	eq	✗	4	✓	x				
Signal	cor	✗	2	↯					
TLS12-TLS13-draft18	cor	✗	1	↯					

Q: type of query *cor*: correspondence query *eq*: equivalence query
inj: correspondence query with injective events
O: old result ✗: "cannot be proved" ⏱: out of time (>24h)
#: number of queries N: new result ✓: proof ↯: attack
ℕ: use of natural numbers A: use of axioms, lemmas
P, I, R: use of newly introduced options, see text.

unpublished files									
QBC_4qubits	cor	✗	1 1	✓ ↯	x				
voting-draft	eq	✗	1	✓	x				
LAK-simplified	cor	⏱	1	✓		x			
PACE_v3_sequence	cor	✗	1 3	✓ ↯	x			x	x
DP-3T-simpl-draft	cor	⏱	1 2	✓ ↯	x	x	x	x	x
Student1	cor inj	⏱	2 1	✓ ↯	x		x		
Student2	inj	✗	1	✓					
Student3	cor	⏱	1	↯	x		x		
Student4	cor	✗	2	↯	x		x		
Student5	cor	⏱	1	↯					

個別論文紹介①

ProVerif with Lemmas, Inductions, Fast Subsumption, and Much More (Bruno Blanchet et al., S&P2022)

- Ver. 2.00とVer. 2.02pl1の比較

Protocol	# files	2.00	(a)	(b)	(c)	(d)	(e)	gain ($\frac{t_{2.00}}{t_{(e)}}$)
Distrib	134	4min 39s	2min 05s	1min 55s	1min 51s	1min 52s	1min 14s	×3.8
Noise	42	≥ 170h 32min	≥ 124h 36min	29h 45min	13h 47min	3h 37min	20min	×516
TLS	3	8h 39min	47min	47min	44min	39min	32min	×16
Arinc823	18	11h 35min	24min	23min	20min	18min	17min	×42
Signal	13	30h 52min	23h 45min	16h 11min	3h 35min	1h 04min	58min	×32
Neuchâtel	9	≥ 73h 33min	≥ 24h 24min	6min	6min	5min	5min	×945

TABLE 2. TIME GAIN

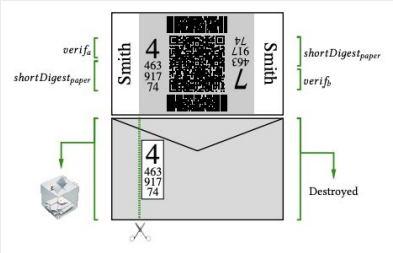
Protocol	# files	2.00	(e)	gain ($\frac{m_{2.00}}{m_{(e)}}$)
Distrib	134	5.0GB	4.3GB	×1.2
Noise	40	58.3GB	7.4GB	×7.9
TLS	3	11.2GB	9.1GB	×1.2
Arinc823	18	8.2GB	8.4GB	×1
Signal	13	29.9GB	23.9GB	×1.2
Neuchâtel	6	0.3GB	0.2GB	×1.7

TABLE 3. MEMORY GAIN

個別論文紹介②

Themis: an accountable on-site voting system with systematic cast-as-intended verification (M. Bougon et al., CCS 2022)

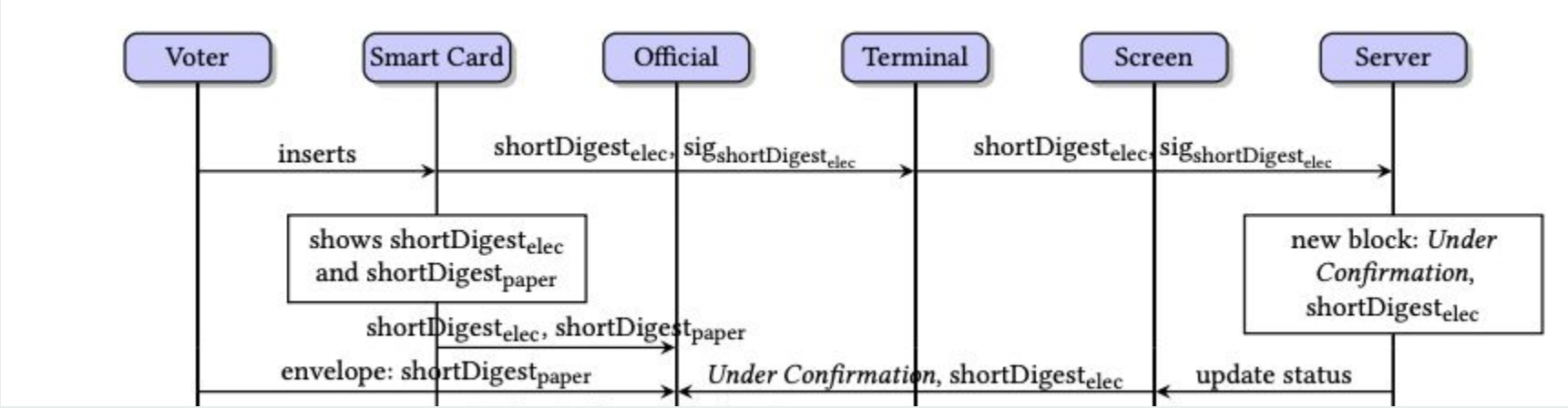
- オンサイト投票プロトコルThemisを提案し
  その形式化とProVerifを用いた安全性検証を行った.
  - プライバシ，検証可能性，部分的説明可能性について検証.
  - 実際にプロトタイプ実装とユーザ実験を実施.

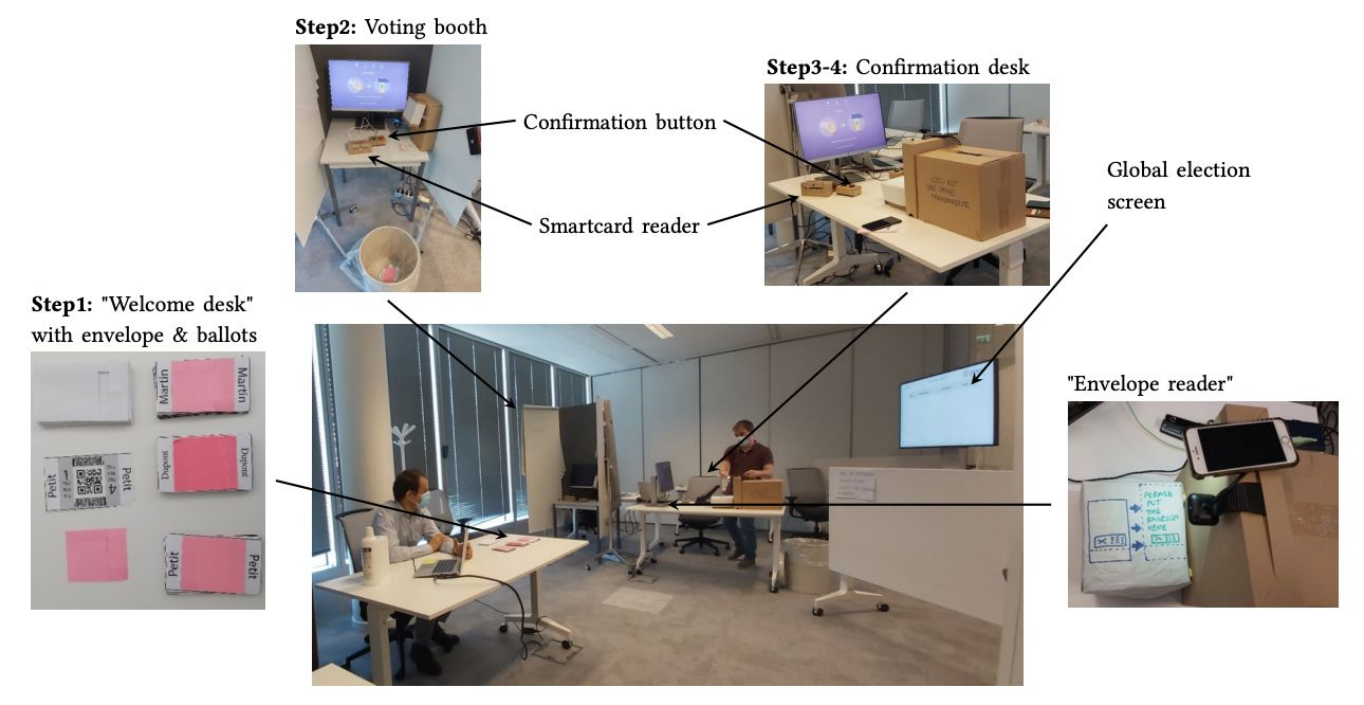


個別論文紹介②

Themis: an accountable on-site voting system with systematic cast-as-intended verification
(M. Bougon et al., CCS 2022)

- 検証した安全性
  - プライバシ：SCとターミナルが結託しない限り投票内容は漏れない
  - 検証可能性：投票内容が正しく結果に反映されることを検証可能
  - 部分的説明可能性：不正な参加者（のグループ）を特定可能



個別論文紹介②

Themis: an accountable on-site voting system with systematic cast-as-intended verification
(M. Bougon et al., CCS 2022)