From Proofs to Practice: Formal Verification for Real-World Security

6th International Conference on **Public Key Infrastructure and its Applications**

Dr. Roberto **Metere**

✉ roberto.metere@york.ac.uk

Department of Computer Science

4th September 2025

Part I

PKI and Formal Methods: What is missing?

Context and Relevance

UNIVERSITY of York
Department of Computer Science

- Trusted CAs issue certs claiming trust properties - but who proves it?
- Formal methods can expose some gaps and trigger monitors or remediation.
- Tools: ProVerif, Tamarin, CryptoVerif, EasyCrypt, PRISM, and many others.

Challenges in PKI Formalisation

UNIVERSITY of York
Department of Computer Science

Real PKI Failures

- Recent NDSS 2024 study finds third-party CT monitors sometimes fail to return the complete set of certificates, undermining detection of mis-issuance.
- 18% of certificates contain structural defects (source: Keyfactor – 2025)

Some are not maths failures - they're real-world breakdowns in trust infrastructure - we use formal models to expose and possibly verify patches.

Challenges

- Complexity, scale, ambiguous specs, evolving standards, and static models.
- Need not just proofs, but workflows, tooling, integration.

What Is Formal Verification?

UNIVERSITY of York
Department of Computer Science

Definition

Formal Verification is uses symbolic or computational models to rigorously prove security properties - not just test for bugs.

Tool types

- **Symbolic** – fast, may over-approximate
- **Computational** – game-based, tight guarantees

Barbosa et al. – IEEE Symposium on Security and Privacy (S&P) (2021)
SoK: Computer-Aided Cryptography.

Bridge the Specification Gap

UNIVERSITY of York
Department of Computer Science

- Fixes ambiguity: structured spec replaces ad-hoc textual modelling.
- Applies to Diffie-Hellman, Needham–Schroeder, Needham–Schroeder–Lowe.
- Implication for PKI: potential to formalise certificate issuance, validation, revocation workflows seamlessly—reducing mismatch between spec and model.

This is the kind of tooling PKI needs—structured, reusable, less error-prone conversions from intended specification to provable model.

Part II

Verified Protocol Insights

Protocol Analysis and Certificate Transparency

UNIVERSITY of York
Department of Computer Science

- **TLS**: symbolic proofs analysing various handshake modes, and computational proofs applied to TLS 1.3 draft-18 (2017)
- Third-party **CT monitors** sometimes fail to return the complete set of certificates

Bhargavan et al. – IEEE Symposium on Security and Privacy (2017)
Verified models and reference implementations for the TLS 1.3 standard candidate.

Cremers et al. – ACM SIGSAC conference on computer and communications security (2017)
A comprehensive symbolic analysis of TLS 1.3.

Sun et al. – NDSS (2024)
Certificate Transparency Revisited: The Public Inspections on Third-party Monitors.

WPA3-SAE Verification

UNIVERSITY of York
Department of Computer Science

- Symbolic verification of Authentication Protocol (ProVerif).
- Executable/State machine (ASMETA) verification.
- Uncovered real flaws in the IEEE 802.11 specification.
- Demonstrates silent failures and high-impact payoff.
- Provides **verified patches** to the specification.

WPA3-SAE Formal Verifications in ProVerif and ASMETA (2025)
https://zenodo.org/records/15384714

Physical-Layer Security Proofs and Other Primitives

UNIVERSITY of York
Department of Computer Science

As quantum-era and wireless PKIs emerge, the physical layer itself becomes part of the trust chain—if your bits can be spoofed on the air, no digital signature will save you.

Physical Layer

- At the physical layer, attackers can jam signals to block communication or subtly watermark them to leak secrets; both directly threaten the authenticity and availability guarantees that PKI is supposed to underpin.
- Isabelle models for watermarking and jamming – provable secrecy/auth authenticity in next-gen networks

Relevance to PKI

UNIVERSITY of York
Department of Computer Science

- Protocols that *look* secure falter under formal scrutiny - PKI chains can too.
- Formal methods can expose subtle trust breaches before exploitation.

Towards Verified Standards

- Standards like TLS 1.3 and Wi-Fi have benefited from formal models in shaping their design.
- Formal modelling of certificate validation and CT ecosystems can highlight implicit assumptions and guide implementation.

Where Models Fail (Sometimes Quietly)

UNIVERSITY of York
Department of Computer Science

- Over-approximation — false alarms
- Non-termination/exploding state — inconclusive results
- Out-of-model issues (timing, caches, UX) — real-world failures

Example: Dragonblood side-channels not caught at protocol level.

Vanhoef et al. – IEEE Symposium on Security and Privacy (2020)
Dragonblood: Analyzing the Dragonfly Handshake of WPA3 and EAP-pwd.

Part III

Why PKI Still Isn't Solved

Core Limitations of Formal Verification for PKI

UNIVERSITY of York
Department of Computer Science

- Model–Reality Gap: abstraction not equal to actual CA deployments.
- Scale: millions of certs, complex trust graphs.
- Ambiguous Standards: X.509 extensions, revocation, cross-certs.
- Tool Usability: steep learning curve, misuse breeds false confidence.
- Static vs Dynamic: proofs don't adapt to revocations, compromises.
- Deep Trust Properties: cross-certification, path shortening—hard to encode fully.

Structured-Spec Tools + Runtime Monitoring = the Way Forward

UNIVERSITY of York
Department of Computer Science

- Structured specification tools like Metere's reduce modelling errors and improve reuse.
- Runtime monitoring (Cert Transparency, mis-issuance detection) complements proofs.
- Combine tooling + proofs + monitoring for robust PKI security.

Call to Action

UNIVERSITY of York
Department of Computer Science

The way forward

- Structured specification tools like Metere's reduce modelling errors and improve reuse.
- Runtime monitoring (Cert Transparency, mis-issuance detection) complements proofs.
- Combine tooling + proofs + monitoring for robust PKI security.

- "PKI won't be secure until its trust claims aren't only assumed—but formally proven and continuously enforced."
- Academia and industry shall adopt **structured-spec workflows** and **runtime checks**.

Questions & Answers

Roberto **Metere**

UNIVERSITY of York

roberto.metere@york.ac.uk