A Symbolic Analysis of ECC-based Direct Anonymous Attestation

Jorden Whitefield, Liqun Chen, Ralf Sasse, Steve Schneider,
Helen Treharne, Stephan Wesemeyer

Surrey Centre for Cyber Security, University of Surrey
Department of Computer Science, ETH Zurich

17 June 2019

Outline

Direct Anonymous Attestation

Contributions

Formal Analysis of ECC DAA

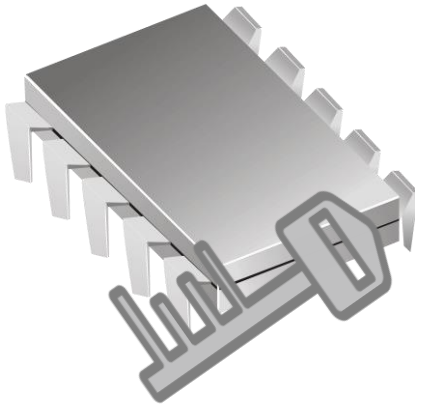
Summary

Direct Anonymous Attestation (DAA)

Anonymous Digital Signature scheme

- Strong but privacy-preserving authentication
- ISO/IEC 20008 2013

Hardware-backed attestation using TPMs



Properties of DAA

- User-controlled Anonymity
- User-controlled Traceability
  - Host controls whether signatures can be linked.

DAA Schemes

TPM 1.2 (RSA-based)

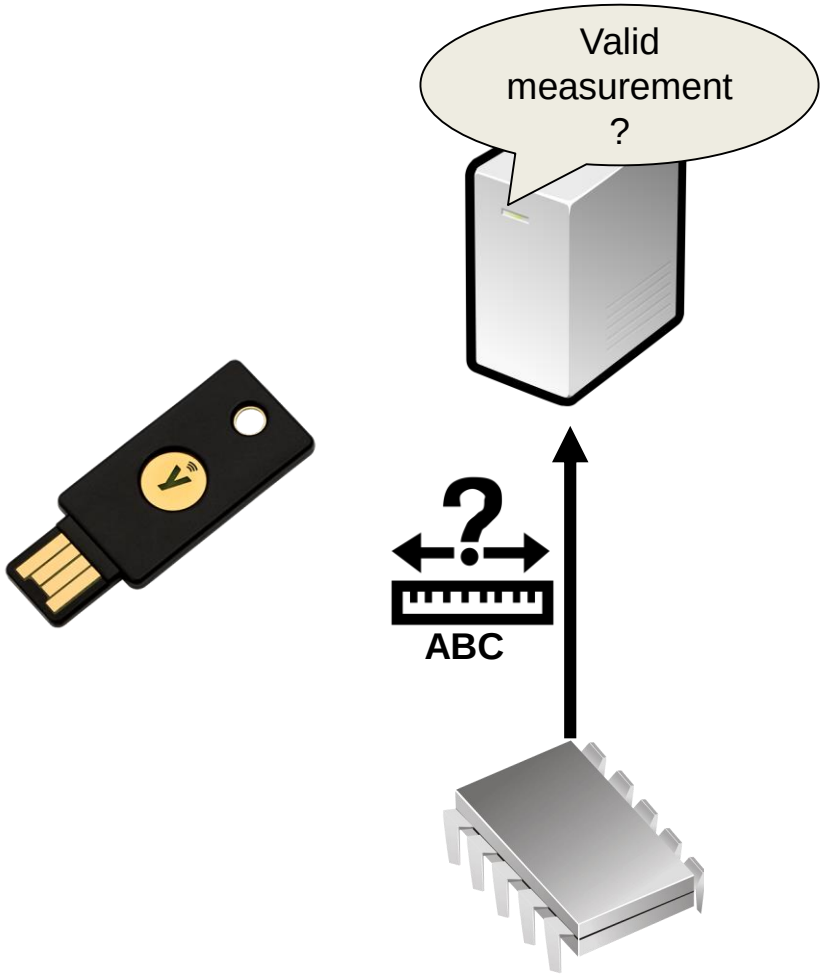
- ISO/IEC 20008-2 mechanism 2

TPM 2.0 (pairing-based)

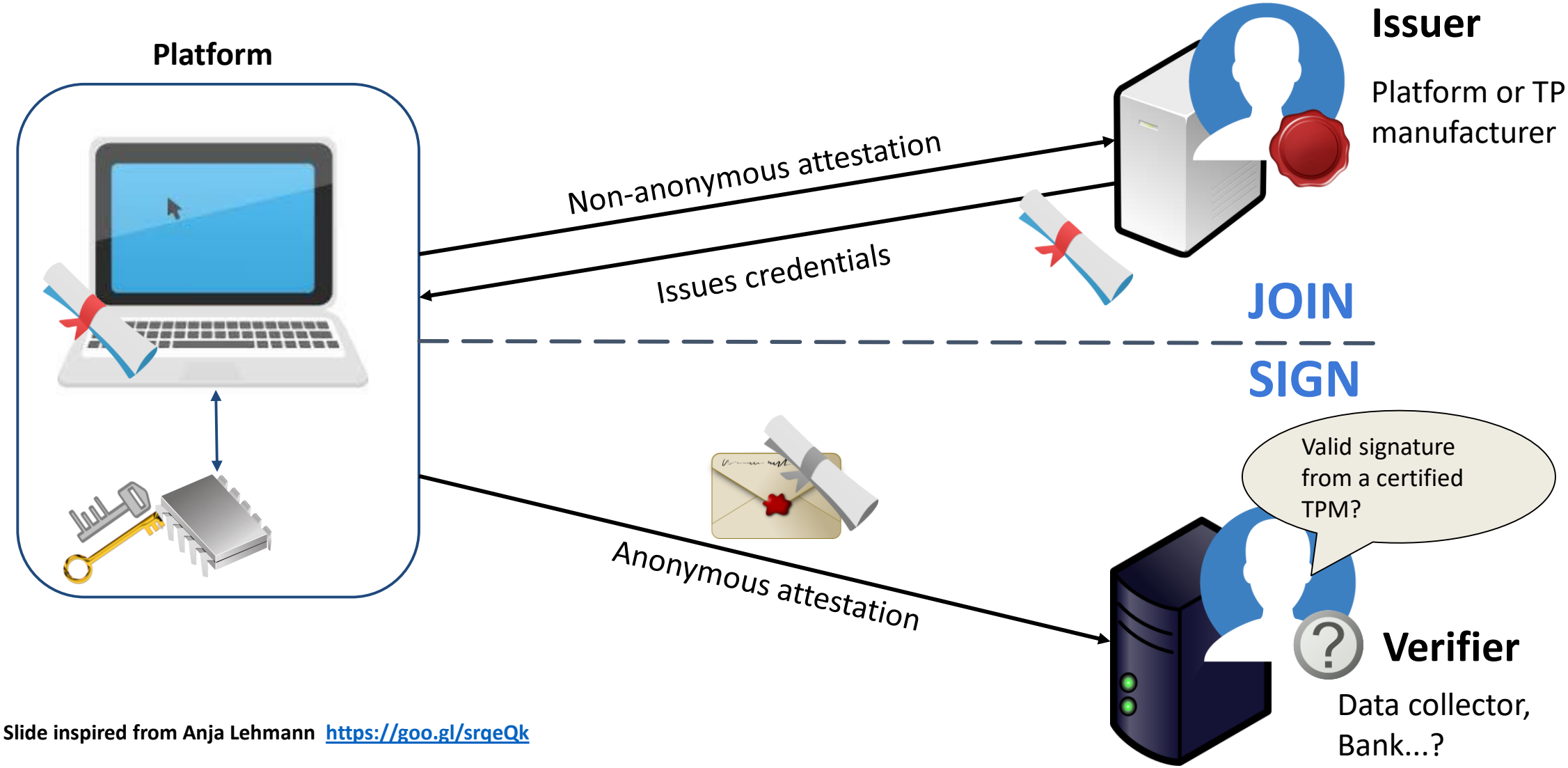
- ISO/IEC 20008-2 mechanism 4 & ISO/IEC 11889
- Smaller keys & signatures!
- Proposed for FIDO 2

Enhanced Privacy ID (EPID)

- Used by Intel SGX
- Improved revocation



Overview of DAA operations



* Slide inspired from Anja Lehmann https://goo.gl/srqeQk

Is ECC DAA secure?

Need proof that ECC DAA is secure

Challenge: Can we formally verify the security and privacy of ECC DAA?

The Tamarin Prover

- State-of-the-art symbolic security protocol analysis tool
- Successfully applied to TLS 1.3, 5G, eVoting, V2X, etc

Contributions

Formalization of ISO/IEC 20008-2

- First faithful automatable models of all ECC DAA operations
- Propose authentication goals for the JOIN operation and find a flaw
- Encode symbolic variants of goals from game-based security (secrecy, privacy)

Security Evaluation of ECC DAA

- Security goals
  - Authentication: does not hold when a single TPM is compromised
  - Secrecy: does not hold when a single TPM is compromised
  - Privacy: holds in the presence of an adversary
- Recommend and provably secure fix for the JOIN operation

What did we model?

Analysed ISO/IEC 20008-2 mechanism 4

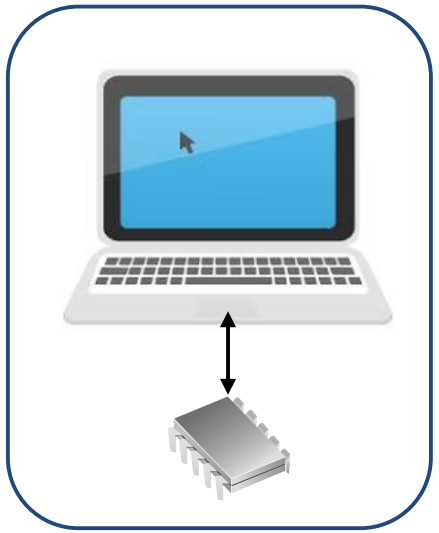
- "*a secure and authentic channel between the principal signer and Issuer*"
- The standard does not provide a way to establish the channel

Two additions

- Message Authentication Codes (MAC)
  - Chen, Page, Smart "*On the design and implementation of an efficient DAA scheme*".
- TPM Endorsement Keys
  - TPM Library – Part 1: Architecture

Restriction: Only consider a single Issuer

Challenges



Separation of Host and TPM

- Communicate over secure I/O in practice
- Restricted analysis to only consider unique 1:1 pairing

Zero Knowledge Proofs

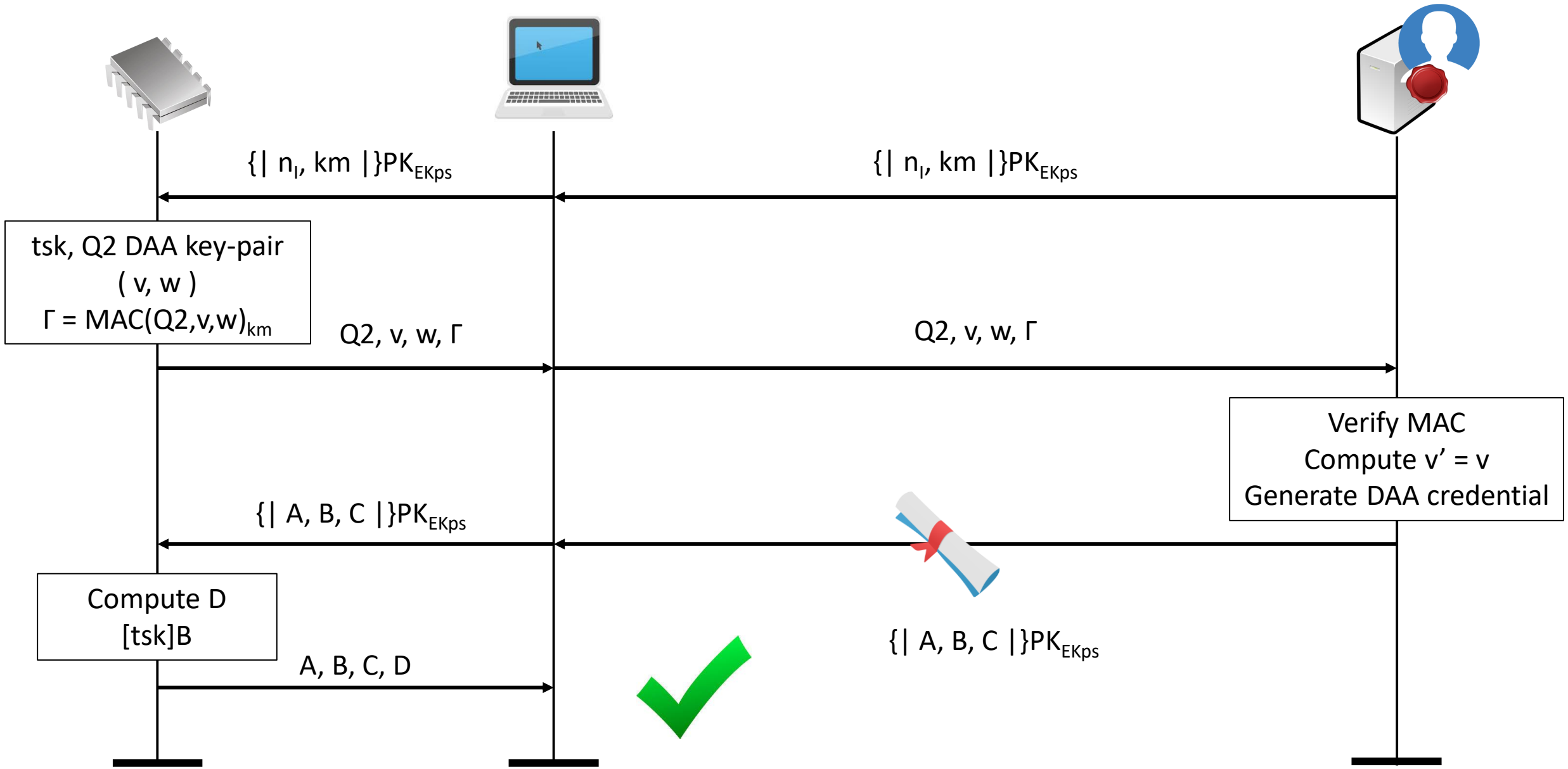
- Defined functions and equations to represent ZKPs symbolically

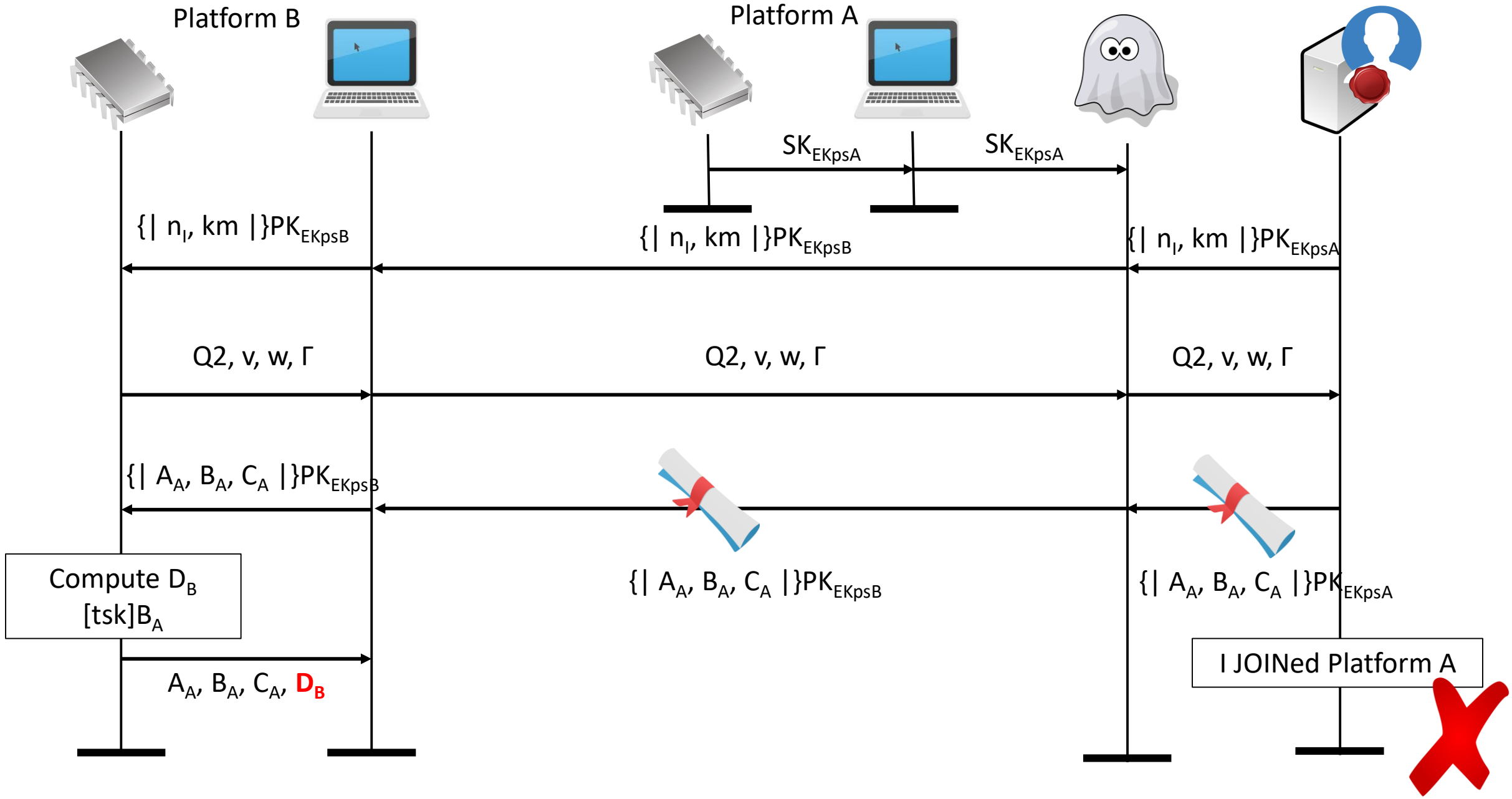
Proof Strategies

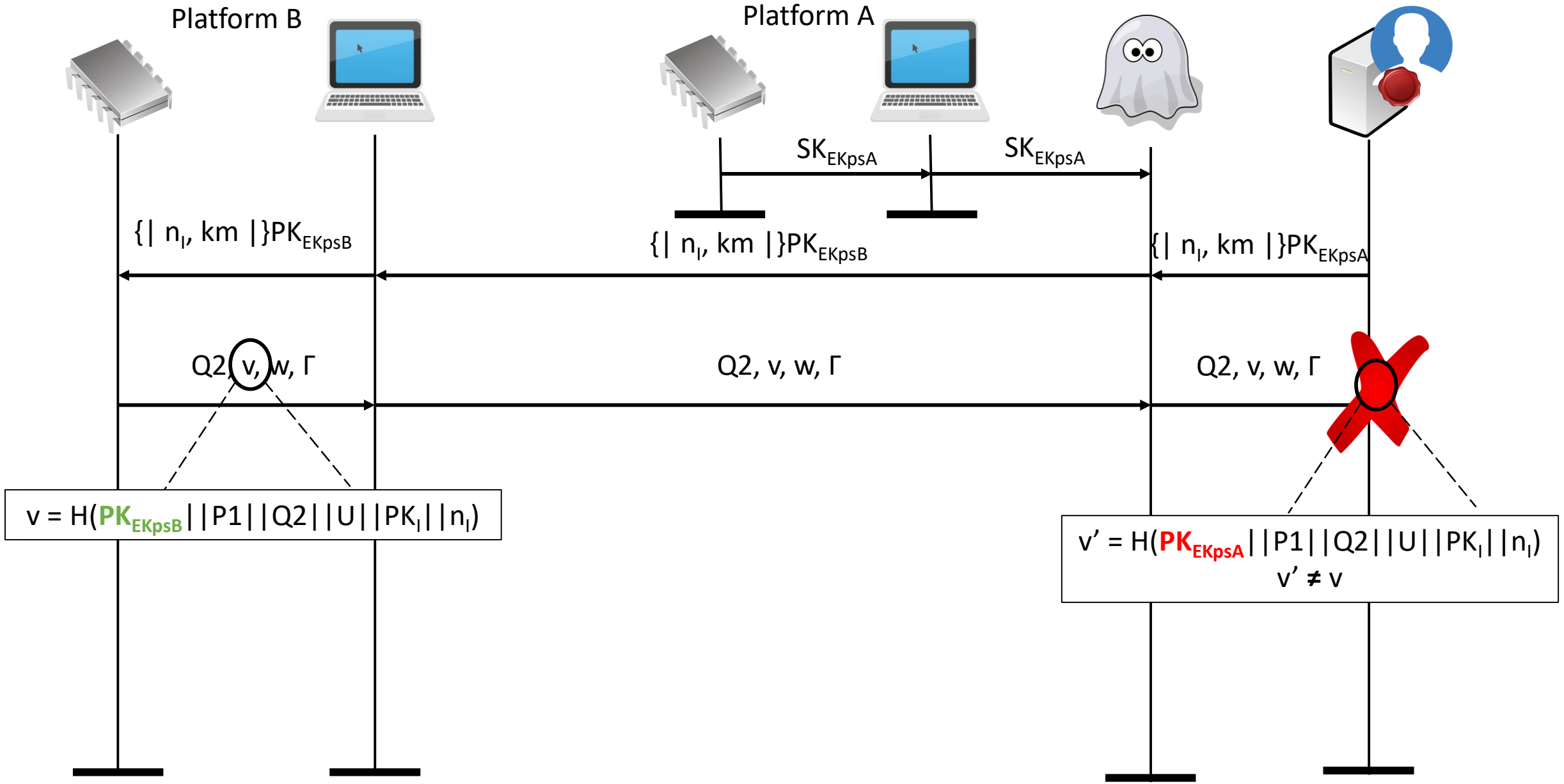
- Guided proof required for unlinkability, codified and automated in an Oracle
- All other lemmas automated using default heuristics

Security and Privacy Properties

Goal	Lemma	Model A	Model B
G1	functional_correctness_group_verification	✓	✓
G2	functional_correctness	✓	✓
G3	functional_correctness_dishonest_send	✓	✓
G4	aliveness	✓	✓
G5	weak_agreement_any_reveal	✓	✓
G6	weak_agreement	×	×
G7	ni_agreement_any_reveal	✓	✓
G8	ni_agreement	×	×
G9	i_agreement	×	×
G10	secrecy_cre	×	×
G11	can_be_deanonymised	✓	✓
G12	user_controlled_independent_link_tokens	✓	n/a
G13	user_controlled_linkability	n/a	✓
Goal	**Observational Equivalence**	**Model C**	
G14	unlinkability	✓	


{| n_I, km |}PK_{EKps}
{| n_I, km |}PK_{EKps}
tsk, Q2 DAA key-pair
(v, w)
Γ = $MAC(Q2,v,w)_{km}$
Q2, v, w, Γ
Q2, v, w, Γ
Verify MAC
Compute v' = v
Generate DAA credential
{| A, B, C |}PK_{EKps}
{| A, B, C |}PK_{EKps}
Compute D
[tsk]B
A, B, C, D


Platform B
Platform A
SK_{EKpsA}
SK_{EKpsA}
{| n_I, km |}PK_{EKpsB}
{| n_I, km |}PK_{EKpsB}
{| n_I, km |}PK_{EKpsA}
Q2, v, w, Γ
Q2, v, w, Γ
Q2, v, w, Γ
{| A_A, B_A, C_A |}PK_{EKpsB}
{| A_A, B_A, C_A |}PK_{EKpsB}
{| A_A, B_A, C_A |}PK_{EKpsA}
Compute D_B
[tsk]B_A
A_A, B_A, C_A, D_B
I JOINed Platform A


Platform B
Platform A
SK_{EKpsA}
SK_{EKpsA}
$\{|\ n_I, km\ |\}PK_{EKpsB}$
$\{|\ n_I, km\ |\}PK_{EKpsB}$
$\{|\ n_I, km\ |\}PK_{EKpsA}$
Q2, v, w, Γ
Q2, v, w, Γ
Q2, v, w, Γ
$v = H(PK_{EKpsB}||P1||Q2||U||PK_I||n_I)$
$v' = H(PK_{EKpsA}||P1||Q2||U||PK_I||n_I)$
$v' \neq v$

Summary

Discovered a flaw in the JOIN operation + proposed a fix

The security of a DAA should not rely on integrity of all TPMs

Fine-grained analysis of ECC DAA

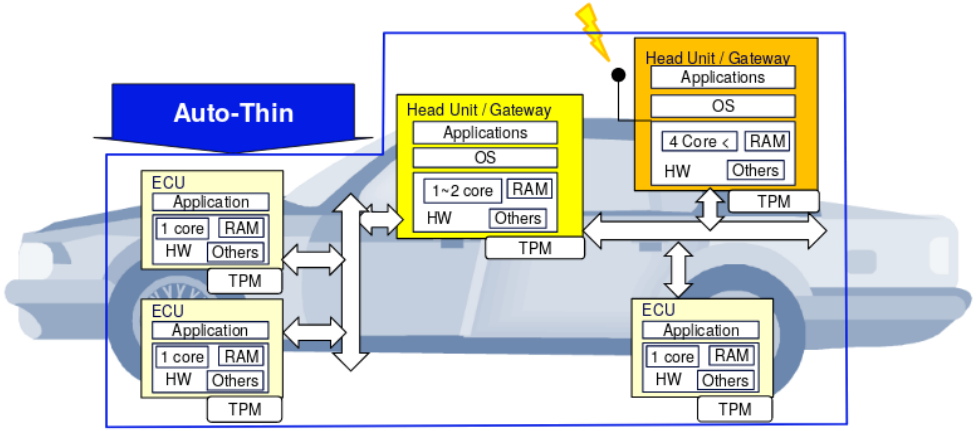
- Capture implementation detail including TPM command calls
- Allow adversary control over secure I/O between TPM and Host

@sudo_jorden

A DAA Scheme for V2X

Use-case targeting V2X communication using DAA

- V2X requires authentication and privacy
- State-of-the-art: Public Key Infrastructure



TCG Automotive-thin profile for TPMs in vehicles

Vehicle credentials (pseudonyms) can be created, signed, and verified using DAA

"Privacy-Enhanced Capabilities for VANETS Using Direct Anonymous Attestation."
In *2017 IEEE Vehicular Networking Conference, VNC 2017*