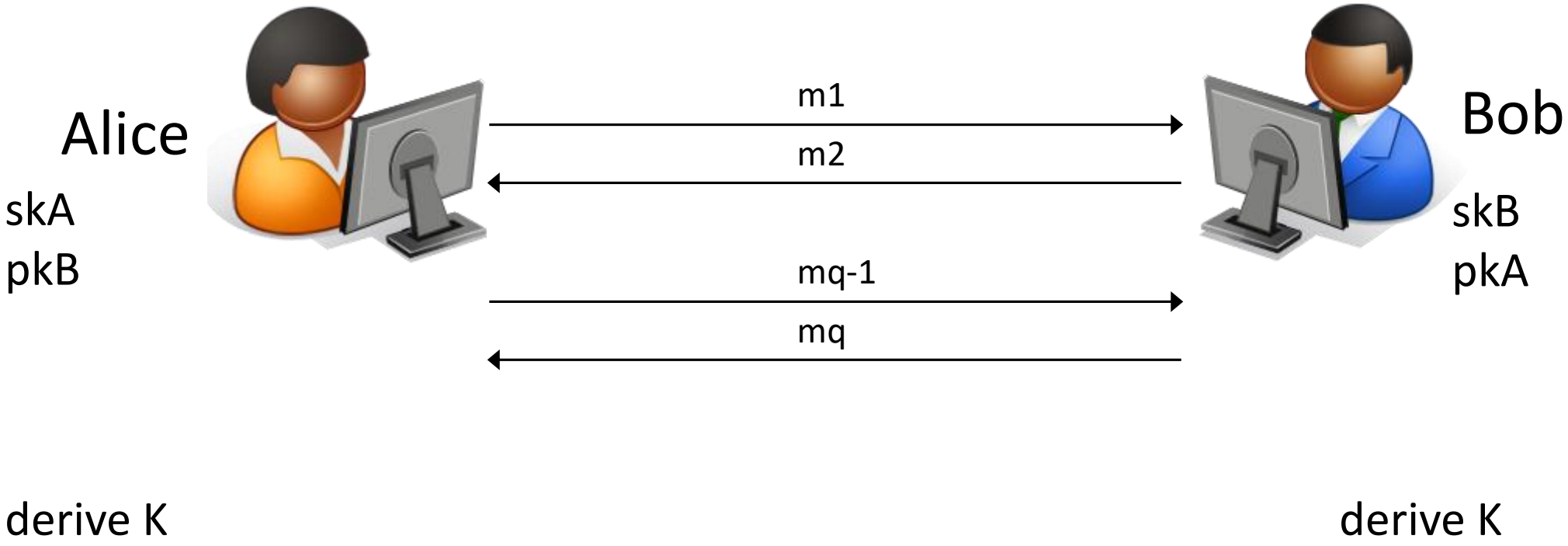
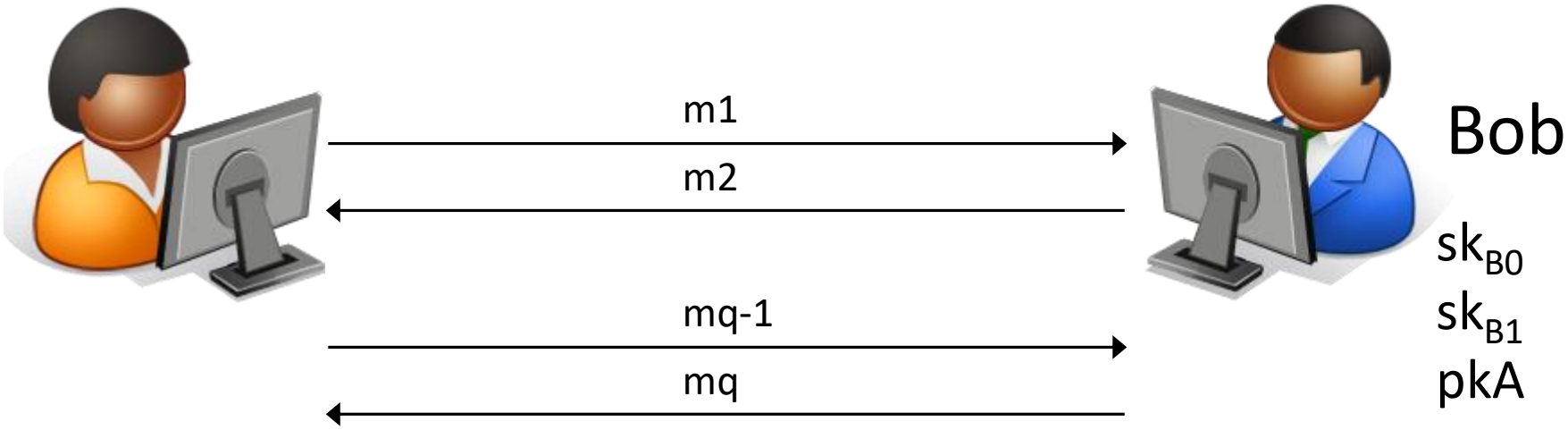
Privacy-Preserving Authenticated Key Exchange and the Case of IKEv2

Sven Schäge, Jörg Schwenk, Sebastian Lauer
Ruhr-University Bochum

Classical Key Exchange Setting



Multi-Homed Servers



General Case

Alice

sk_{A0}
sk_{A1}
pk_{B0}
pk_{B1}

m1

m2

mq-1

mq

Bob

sk_{B0}
sk_{B1}
pk_{A0}
pk_{A1}

derive K

derive K

Motivation for PPAKE

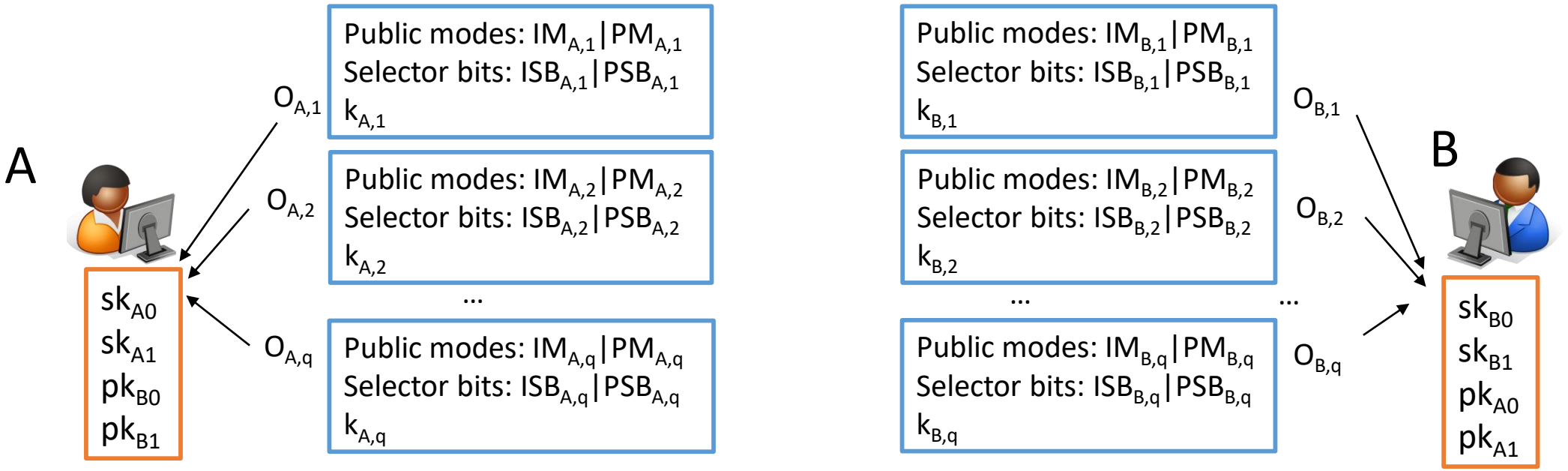
- Privacy
- Censorship Circumvention

- PPAKE is not a substitution for TOR!
  PPAKE does not hide the endpoint but only the virtual identity on/behind that endpoint.

Contribution

- New security model for PPAKE
  - Besides key indistinguishability, additionally captures indistinguishability of used identities
  - General and strong security notion that requires that privacy is cryptographically independent of key indistinguishability
  - Proper extension of classical AKE
  - Introduced changes extendable to unilateral authentication, ACCE, explicit authentication
- New conceptual feature: Modes
  - Modes model protocol options
  - Formulate expectations of parties on who is responsible for choosing identities
- Security proof of IPsec with signature-based authentication

Overview Security Model



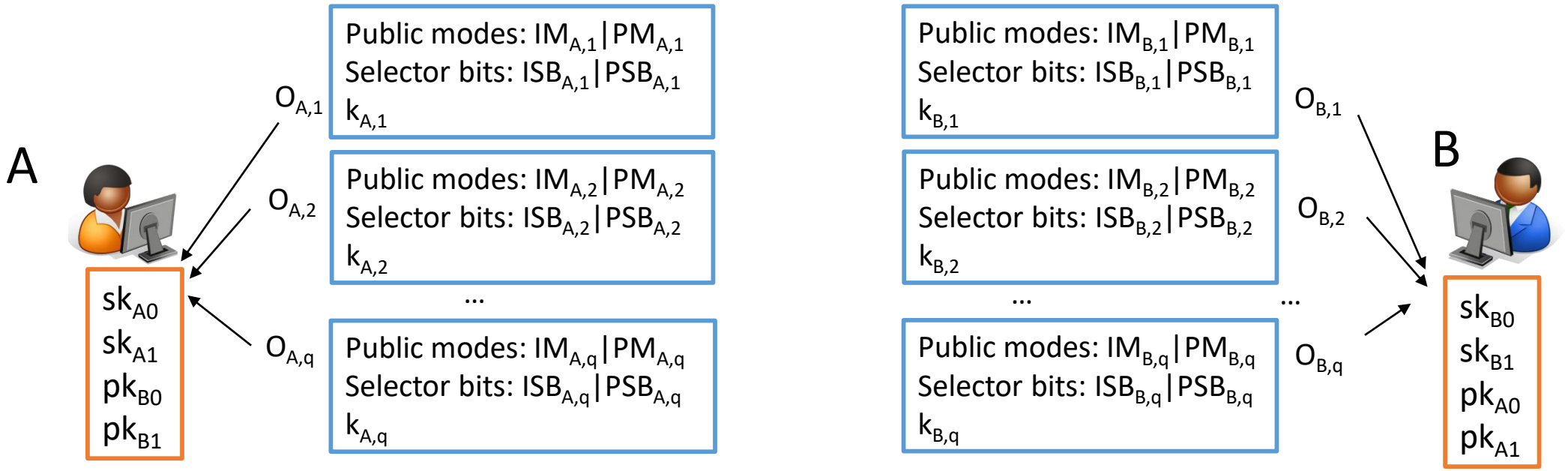
Overview Security Model

Identity Mode (IM) ∈ {me,partner}

Partner Mode (PM) ∈ {me,partner}

Identity Selector Bit (ISB) ∈ {0,1}

Partner Selector Bit (PSB) ∈ {0,1}



PPAKE Security Model: Attack Capabilities

- New Attack Queries to Sessions:
  - Unmask(own/partner)
  - Test(ID,own/partner)->0/1
- Other (Classical) Attack Queries:
  - Send
  - RevealKey
  - Corrupt
  - Test(Key)

PPAKE Security Experiment

- Each party is equipped with two key pairs
- If mode requires so, each session chooses random identity for itself or communication partner
- Attacker always has access to **all** attack capabilities
  - Adding a new security proof for identity indistinguishability to existing security analyses is not enough!
  - Old proof may become invalidated when also given access to Unmask query!

PPAKE Security Guarantees

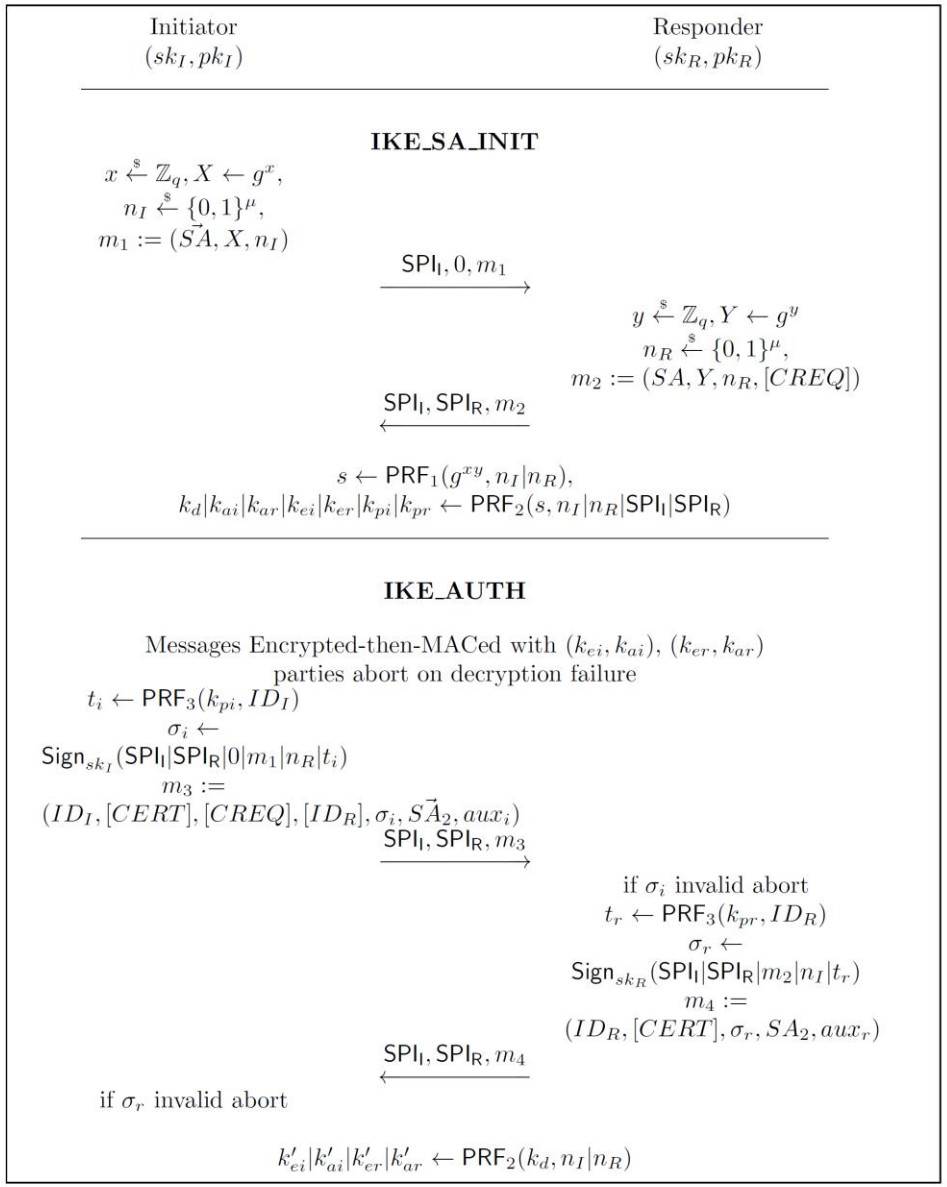
- Key indistinguishability for session key of test session - even if identity is revealed
  - Pre-requisite to show that new PPAKE model is proper extension of classical AKE model
- Indistinguishability of identities of test session - even if session key is revealed

Applicability to other Security Models

- Selector bits, modes, Unmask queries and Test(ID) may be used to extend other security models
  - AKE with explicit authentication
  - Unilateral authentication
  - ACCE->PPACCE

IPsec with Signature-based Authentication

- Phase 1:
  Anonymous DH Key exchange with fresh nonces.
  Result: symmetric keys
- Phase 2:
  Use symmetric keys to encrypt all data including authentication step with signatures



Phase 1

Initiator (sk_I, pk_I)		Responder (sk_R, pk_R)
	IKE_SA_INIT	
$x \xleftarrow{\$} \mathbb{Z}_q, X \leftarrow g^x,$ $n_I \xleftarrow{\$} \{0,1\}^\mu,$ $m_1 := (\vec{SA}, X, n_I)$		
	$\mathsf{SPI_I}, 0, m_1 \longrightarrow$	
		$y \xleftarrow{\$} \mathbb{Z}_q, Y \leftarrow g^y$ $n_R \xleftarrow{\$} \{0,1\}^\mu,$ $m_2 := (SA, Y, n_R, [CREQ])$
	$\mathsf{SPI_I}, \mathsf{SPI_R}, m_2 \longleftarrow$	
$s \leftarrow \mathsf{PRF}_1(g^{xy}, n_I \vert n_R),$ $k_d \vert k_{ai} \vert k_{ar} \vert k_{ei} \vert k_{er} \vert k_{pi} \vert k_{pr} \leftarrow \mathsf{PRF}_2(s, n_I \vert n_R \vert \mathsf{SPI_I} \vert \mathsf{SPI_R})$		

Phase 2

Initiator (sk_I, pk_I)		Responder (sk_R, pk_R)
	Messages Encrypted-then-MACed with (k_{ei}, k_{ai}), (k_{er}, k_{ar}) parties abort on decryption failure	
$t_i \leftarrow \mathsf{PRF}_3(k_{pi}, ID_I)$		
$\sigma_i \leftarrow \mathsf{Sign}_{sk_I}(\mathsf{SPI_I}\|\mathsf{SPI_R}\|0\|m_1\|n_R\|t_i)$		
$m_3 := (ID_I, [CERT], [CREQ], [ID_R], \sigma_i, S\vec{A}_2, aux_i)$		
	$\xrightarrow{\mathsf{SPI_I}, \mathsf{SPI_R}, m_3}$	
		if σ_i invalid abort
		$t_r \leftarrow \mathsf{PRF}_3(k_{pr}, ID_R)$
		$\sigma_r \leftarrow \mathsf{Sign}_{sk_R}(\mathsf{SPI_I}\|\mathsf{SPI_R}\|m_2\|n_I\|t_r)$
		$m_4 := (ID_R, [CERT], \sigma_r, SA_2, aux_r)$
	$\xleftarrow{\mathsf{SPI_I}, \mathsf{SPI_R}, m_4}$	
if σ_r invalid abort		

$$k'_{ei}|k'_{ai}|k'_{er}|k'_{ar} \leftarrow \mathsf{PRF}_2(k_d, n_I|n_R)$$

Option 1: Initiator may specify Responder's identity

Option 2: Responder may specify Responder's identity

PPAKE Security Proof

- Protocol is PPAKE secure assuming security of
  - PRF-ODH assumption
  - Pseudo-Random Functions (PRF)
  - Digital Signature Scheme (SIG)
  - Authenticated Encryption (AE) Scheme

- Length-hiding to hide identities
  - Signatures should be length-preserving or
  - Use length-hiding authenticated encryption

Conclusion

- Model for Privacy-Preserving AKE
  - Emphasizes cryptographic independence of identity indistinguishability and key indistinguishability
  - Captures options for distinct ways to decide on used identities
  - A set of ingredients to extend existing models to become privacy-preserving
  - Supports comparability of models since new models are proper extensions
- Proof of IPsec with Signature-based Authentication
  - Take Home Message:
    Data that depends on the identity should have same length for all identities

- Thank you very much for your attention!