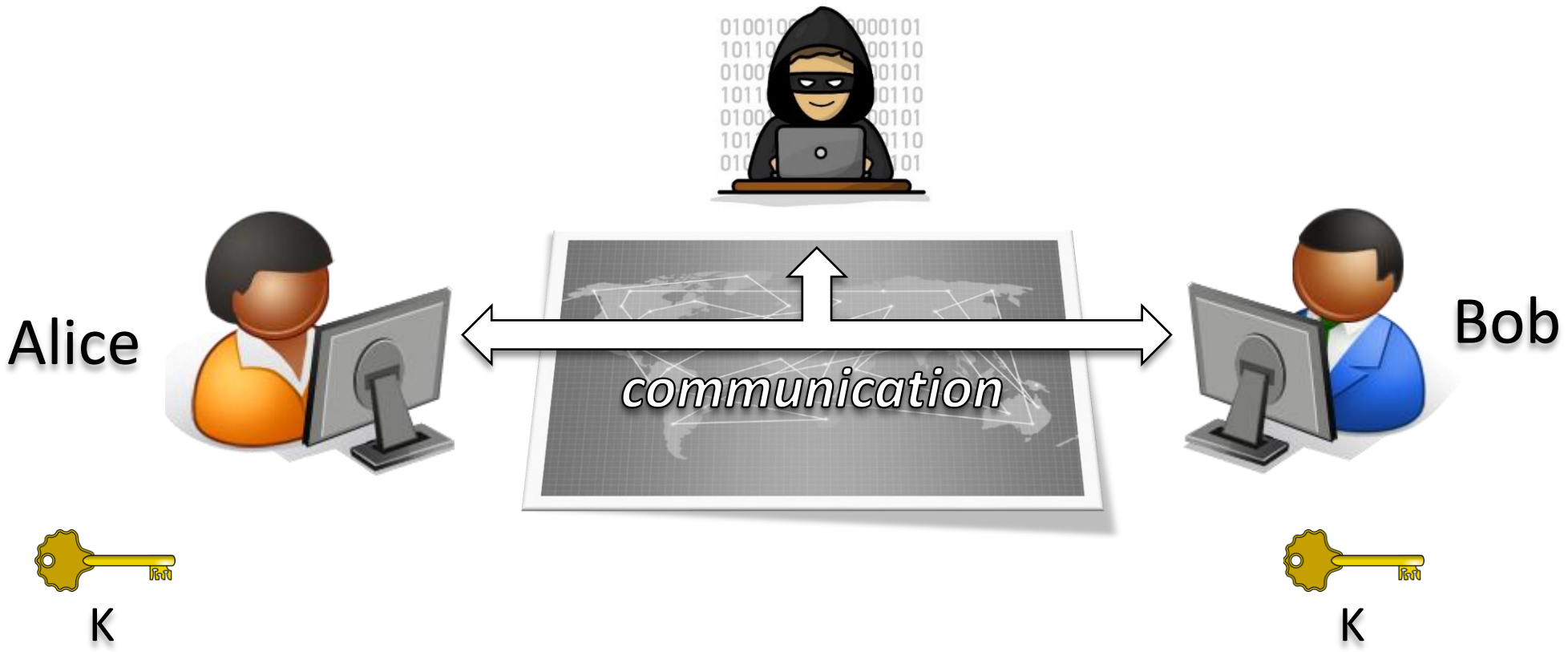
Privacy-Preserving Authenticated Key Exchange and the Case of IKEv2

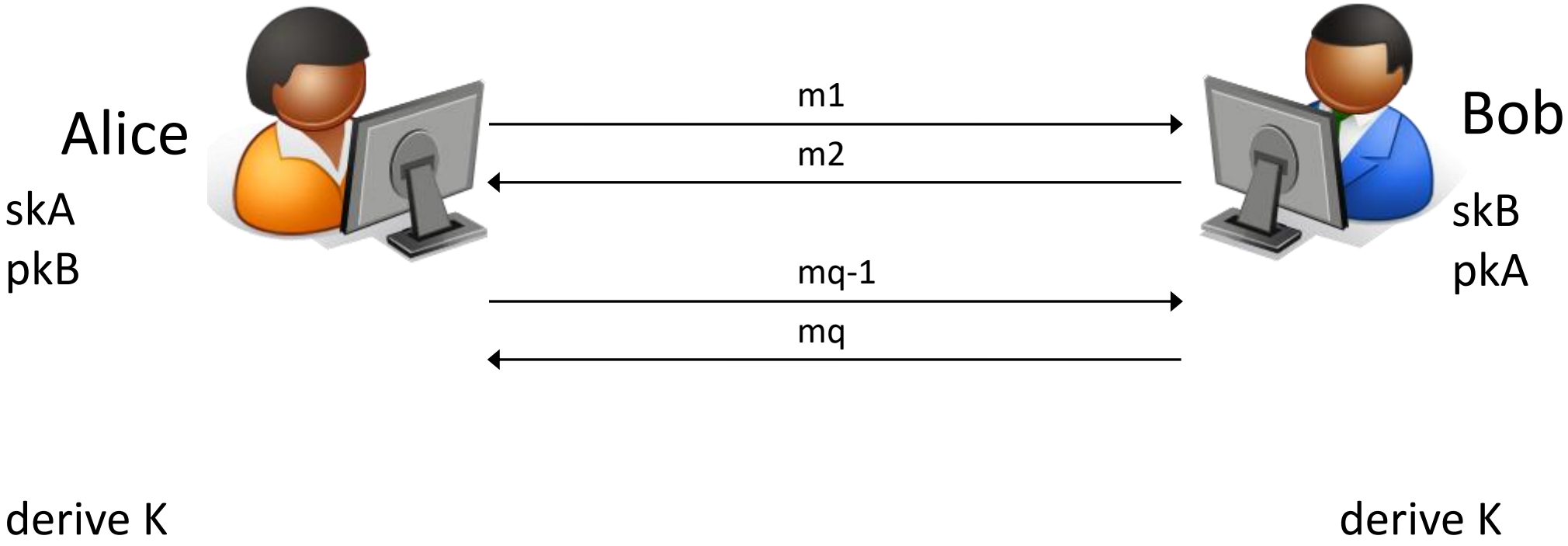
Sven Schäge
Eindhoven University of Technology

(joint work with: Jörg Schwenk, Sebastian Lauer)

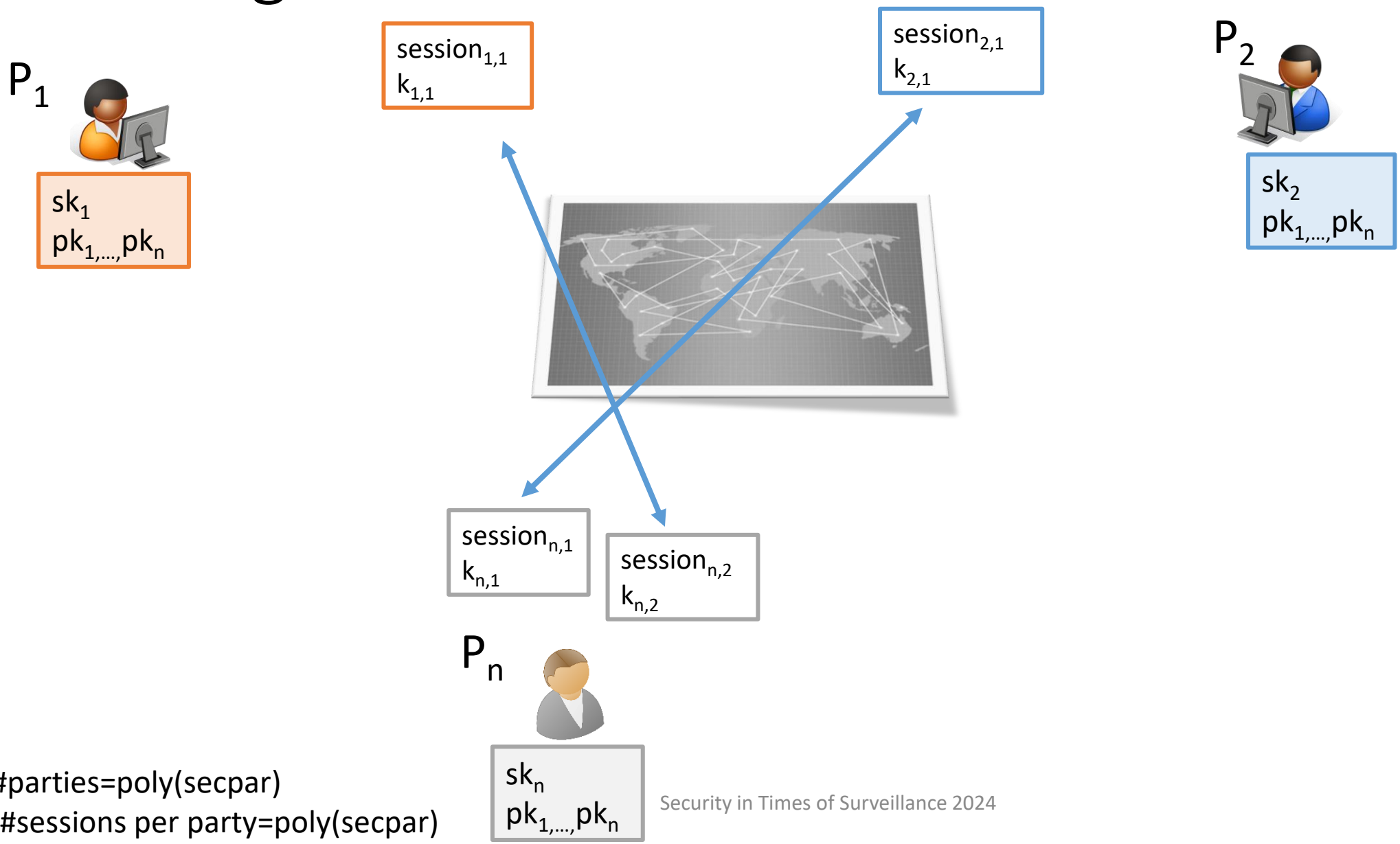
Authenticated Key Exchange (AKE)



Classical Key Exchange Setting

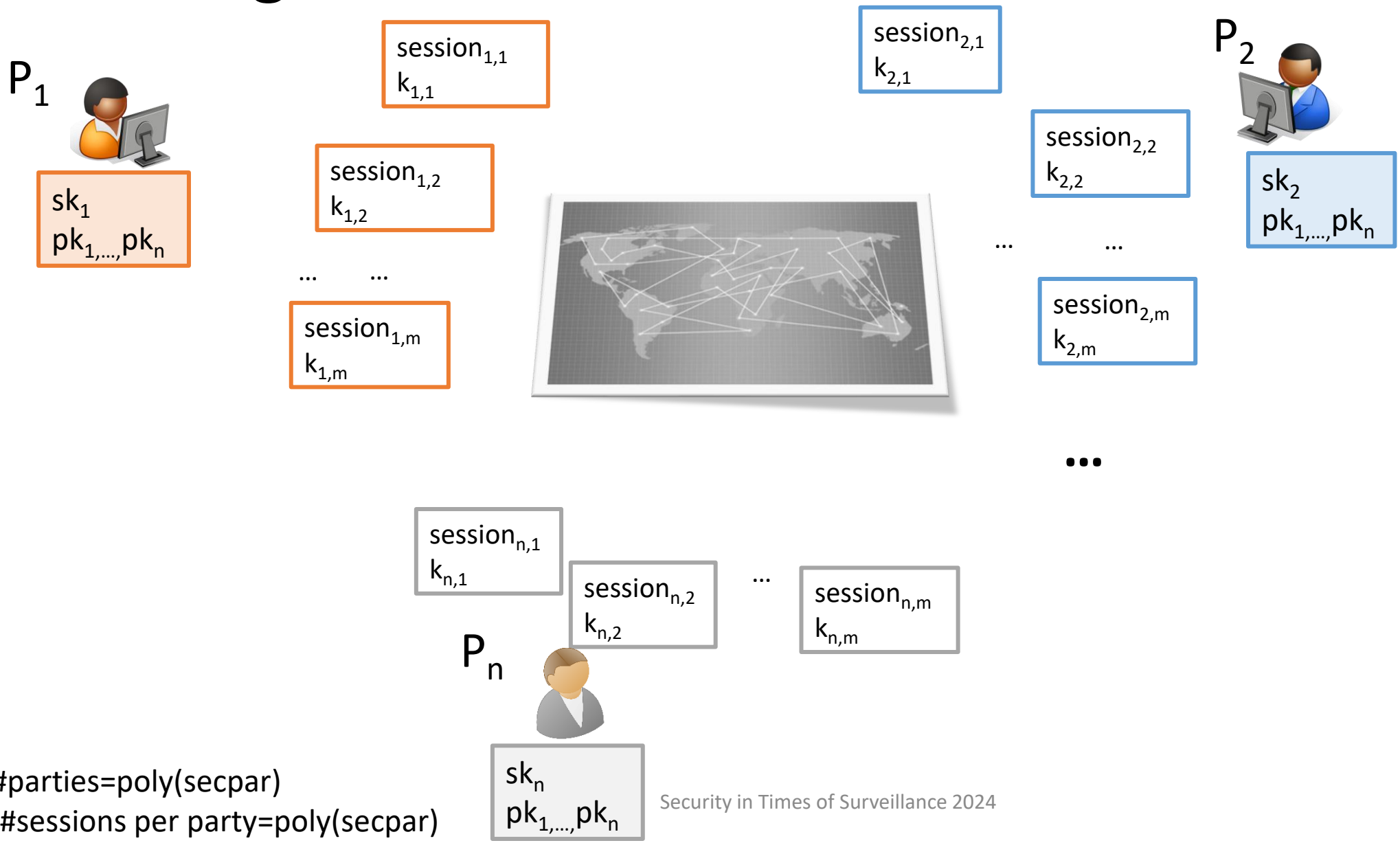


Running AKE Protocols in Networks



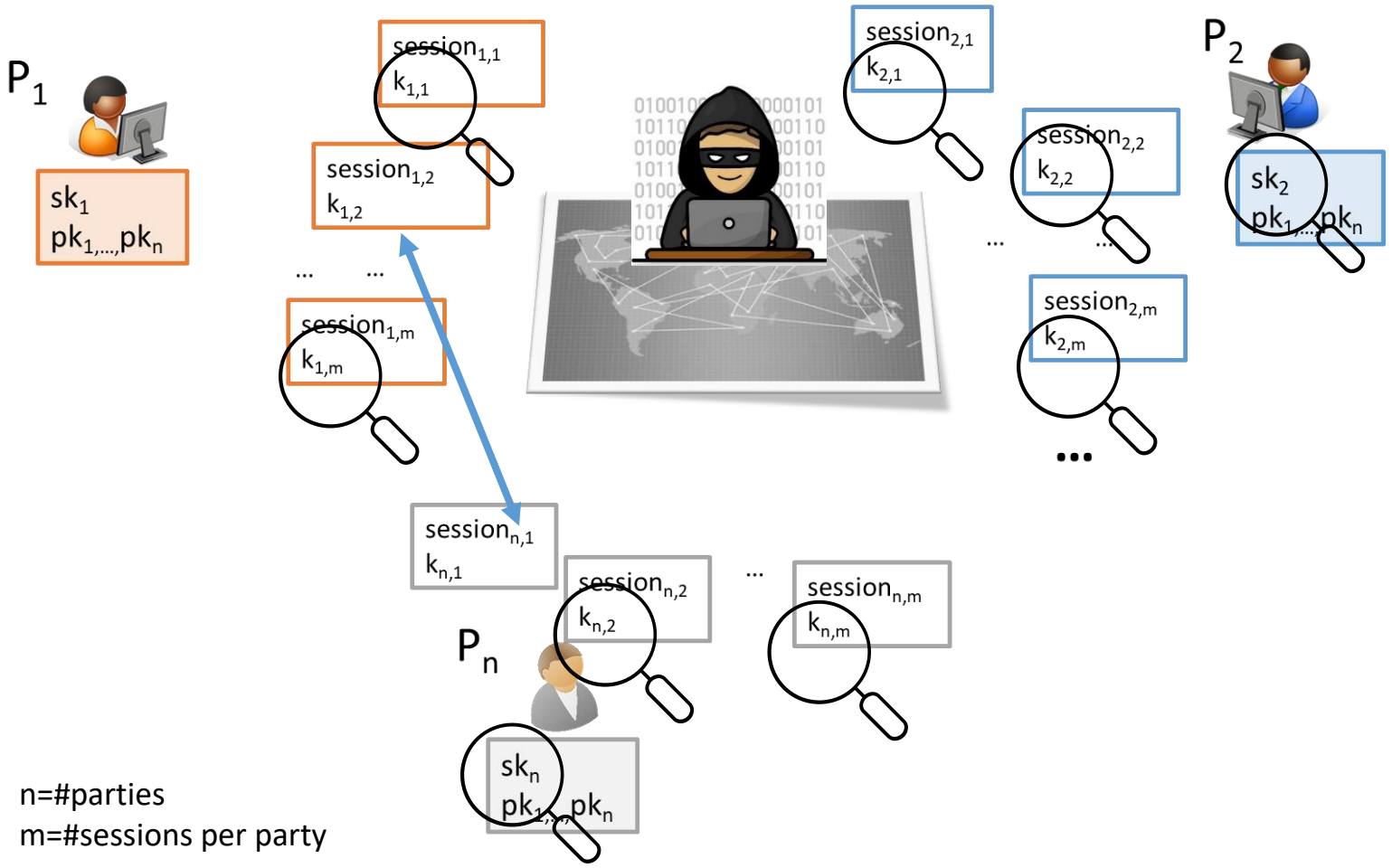
n=#parties=poly(secpar)
m=#sessions per party=poly(secpar)

Running AKE Protocols in Networks



n=#parties=poly(secpar)
m=#sessions per party=poly(secpar)

(Simplified) Classical AKE Security Model



n=#parties
m=#sessions per party

Attack Capabilities:

- **Send(i,s)**: send messages to session i,s
- **Corrupt(i):** obtain sk_i
- **RevealKey (i,s):** obtain $key_{i,s}$
- **Test(i,s)**: obtain random key or $k_{i,s}$

Winning Event:

Attacker wins if
-it correctly **distinguishes real from random key** and
-key **k has not been revealed** for each of the two participating communication partners.

Multi-Homed Servers

Alice

skA

pk_{B0}

pk_{B1}

m1

m2

mq-1

mq

Bob

sk_{B0}

sk_{B1}

pkA

derive K

derive K

General Case

Alice

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

derive K

m1

m2

mq-1

mq

Bob

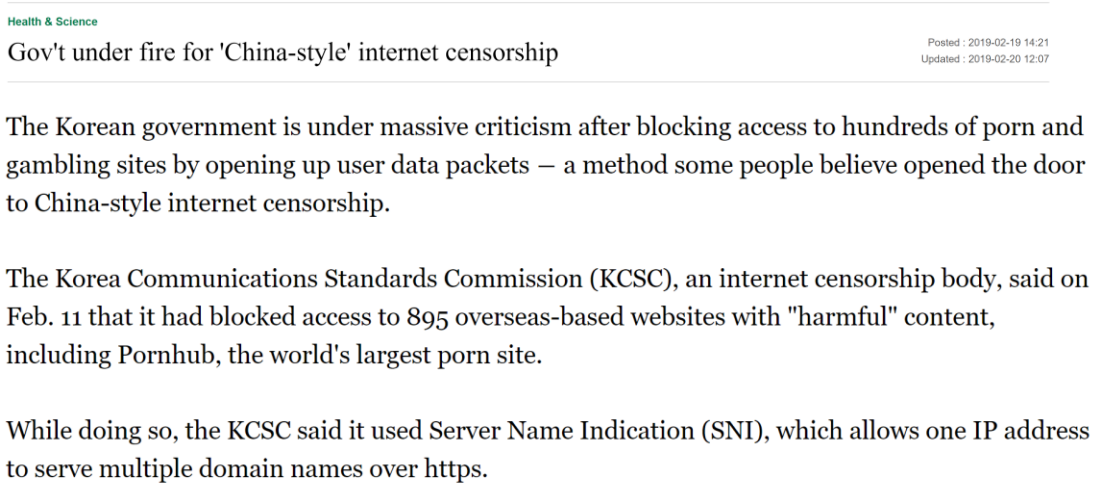
sk_{B0}
sk_{B1}
pk_{A0}
pk_{A1}

derive K

Motivation for PPAKE

- Privacy
- Censorship Circumvention
  - In TLS, SNI Filtering can be used to control access to websites

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



Health & Science

Gov't under fire for 'China-style' internet censorship

Posted : 2019-02-19 14:21
Updated : 2019-02-20 12:07

The Korean government is under massive criticism after blocking access to hundreds of porn and gambling sites by opening up user data packets – a method some people believe opened the door to China-style internet censorship.

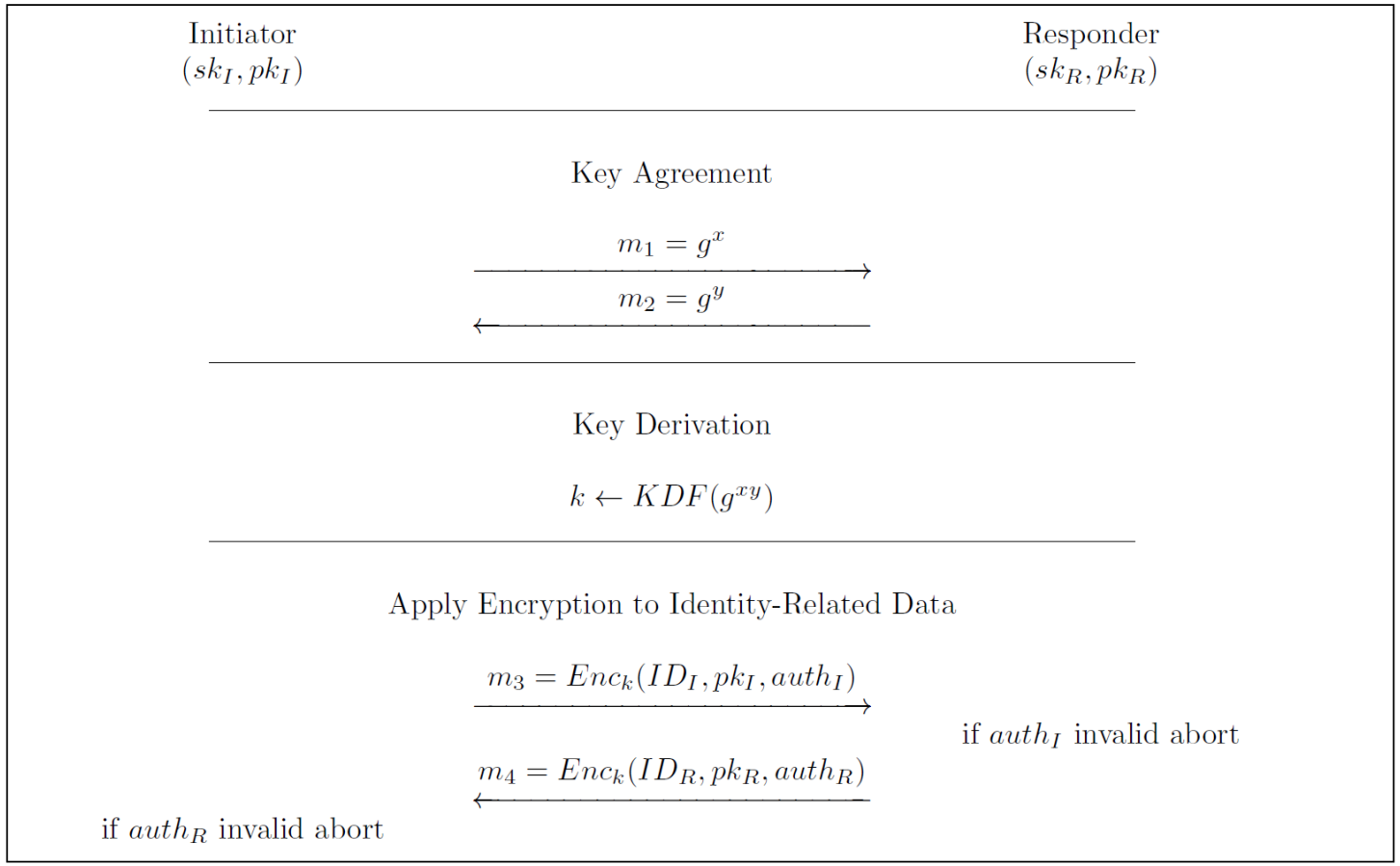
The Korea Communications Standards Commission (KCSC), an internet censorship body, said on Feb. 11 that it had blocked access to 895 overseas-based websites with "harmful" content, including Pornhub, the world's largest porn site.

While doing so, the KCSC said it used Server Name Indication (SNI), which allows one IP address to serve multiple domain names over https.

Contribution

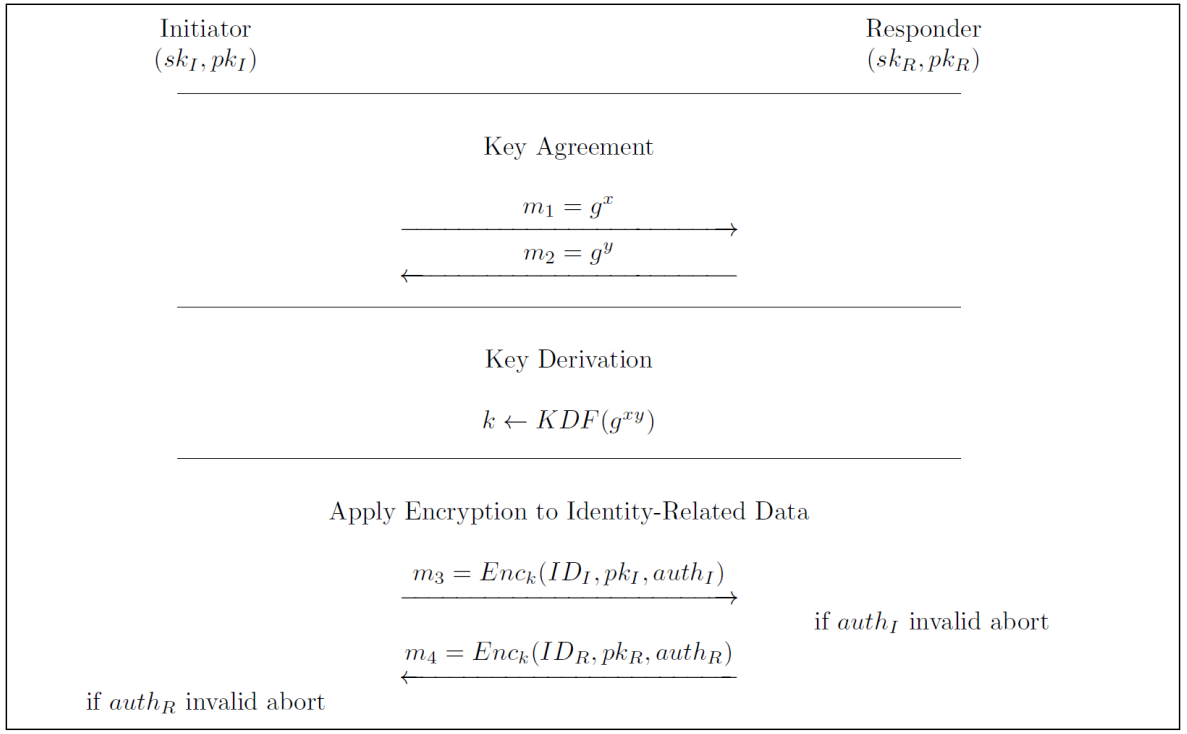
- New security model for PPAKE
  - Besides key indistinguishability, additionally captures indistinguishability of used identities
  - General and strong security notion that requires that privacy is cryptographically independent of key indistinguishability
  - Proper extension of classical AKE
- New conceptual feature: Modes
  - Modes model protocol options
  - Formulate expectations of parties on who is responsible for choosing identities
- Security proof of IPsec’s IKEv2 with signature-based authentication

Generic Construction



Generic Weakness

- active attacker can always reveal the identity of the first party which uses the anonymous DH keying material, at the cost of causing a fatal error in the handshake



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!

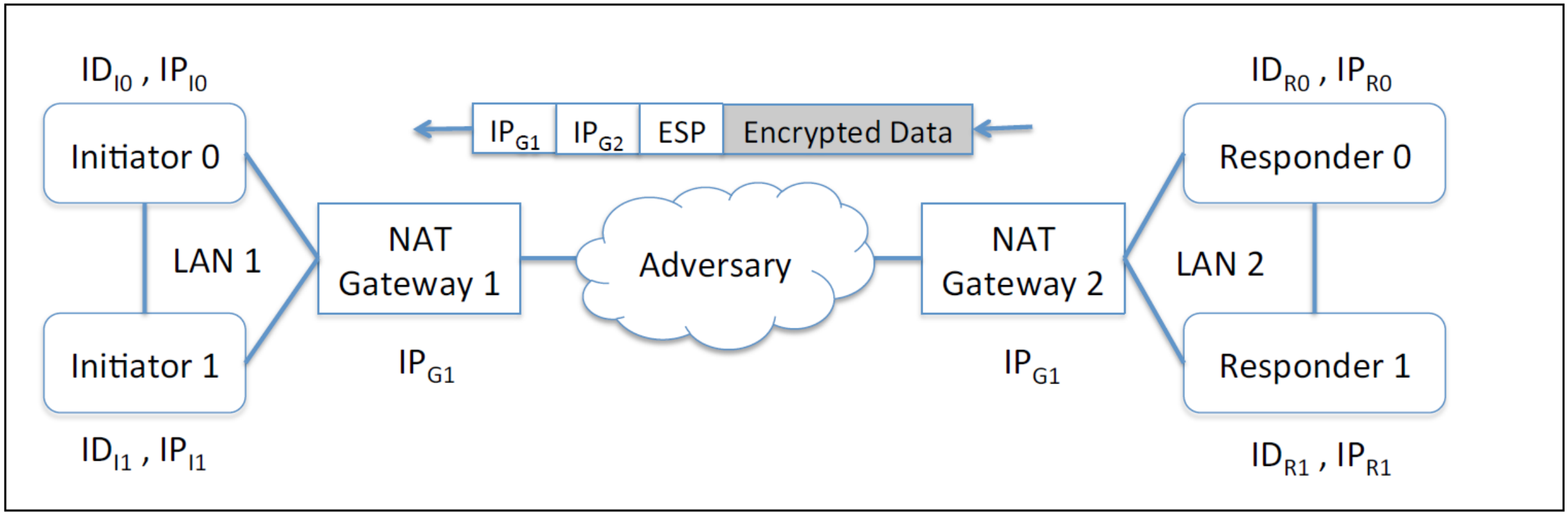
PPAKE Security Guarantees

- 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

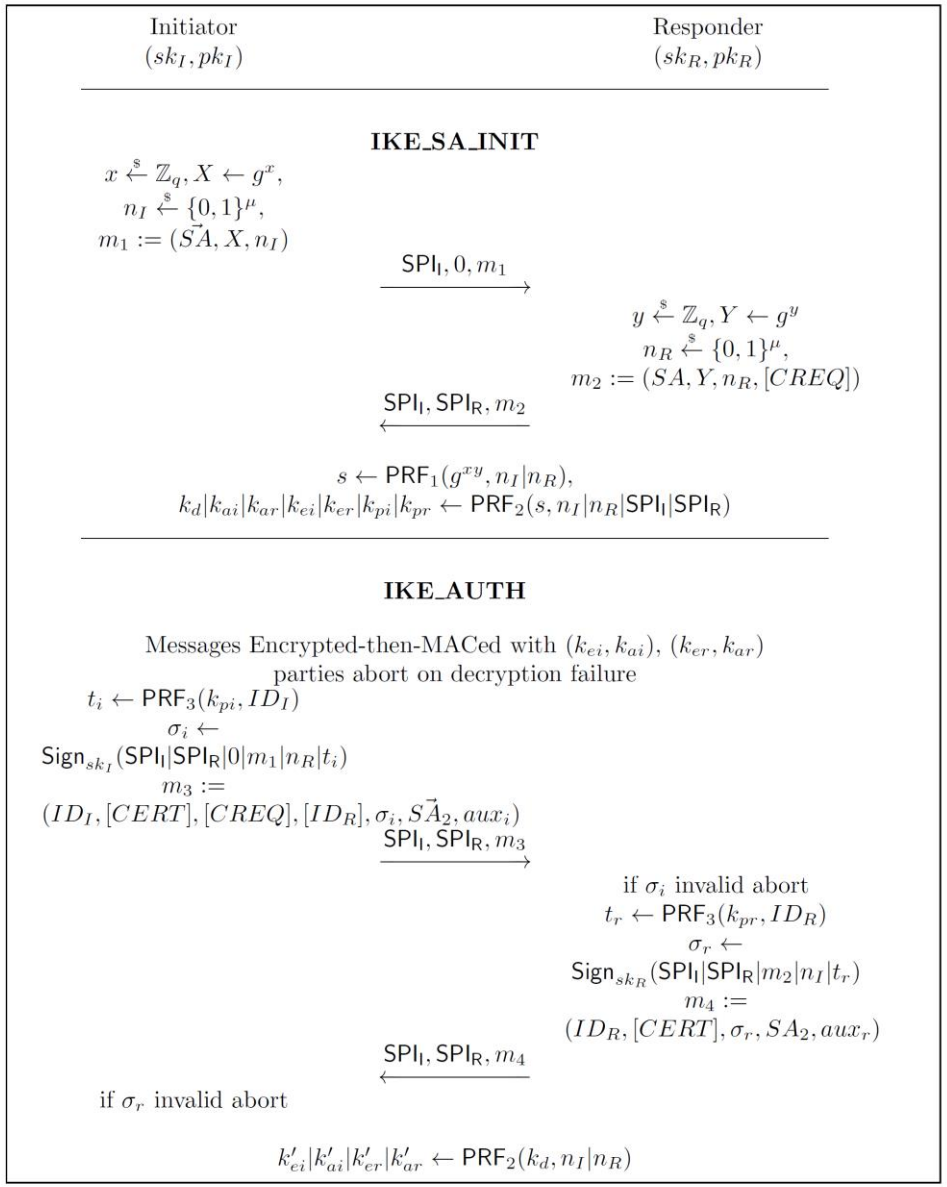
- Selector bits, modes, Unmask queries and Test(ID) may be used to extend other security models
  - AKE with explicit authentication
  - Unilateral authentication
  - ACCE->PPACCE

Host-to-Host IPSec



IPsec (IKEv2) with Signature-based Authentication

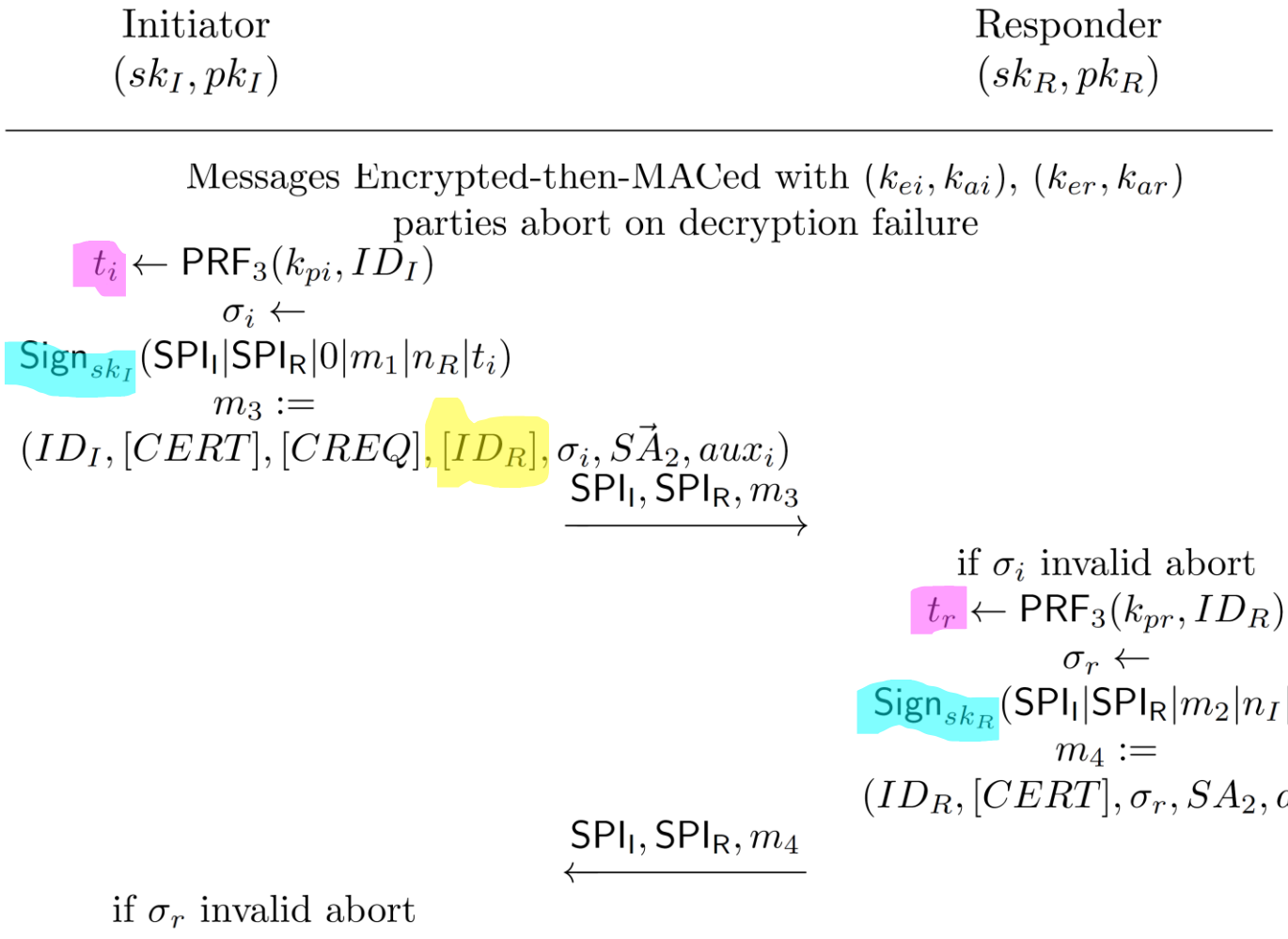
- Phase 1:
  Anonymous DH Key exchange with fresh nonces.
  Result: symmetric keys
- Phase 2:
  Use symmetric keys to encrypt all data including authentication step with signatures



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



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 properties to conceal identities
  - Signatures should be length-preserving or
  - Use length-hiding authenticated encryption
- Output of PRF3 does not add to security

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 for designers:
    Data that depends on the identity should have same length for all identities

- Thank you very much for your attention!

PRF-ODH Assumption

- Given random $g^u, g^v\ n_I|n_R$

- and access to oracle $y \leftarrow \mathsf{PRF}(S^u, x)$

  for queries $(S, x) = (g^v, n_I|n_R)$

  such that $(S, x) \neq (g^v, n_I|n_R)$

- distinguish $z_0 := \mathsf{PRF}(g^{uv}, n_I|n_R)$

  from $z_1 \xleftarrow{\$} \{0,1\}^\mu$