Efficient Asymmetric Message Franking in the Plain Model

Milan Gonzalez-Thauvin[1] and Keitaro Hashimoto[2]

[1]ETH Zurich, Switzerland

[2]National Institute of Advanced Industrial Science and Technology (AIST), Japan

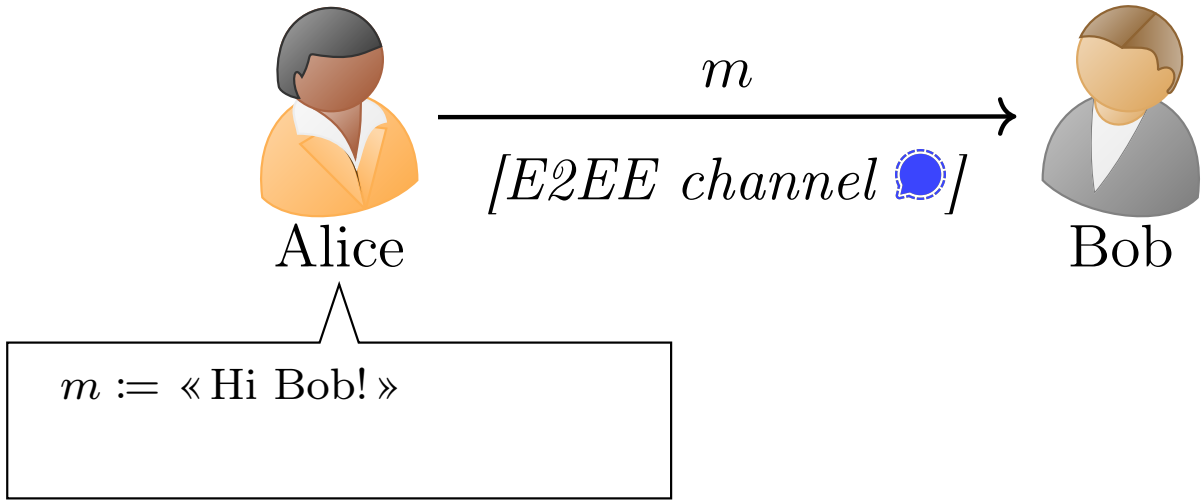
Sunday, May 10th 2026

Paper accepted at Crypto 2026

Summary

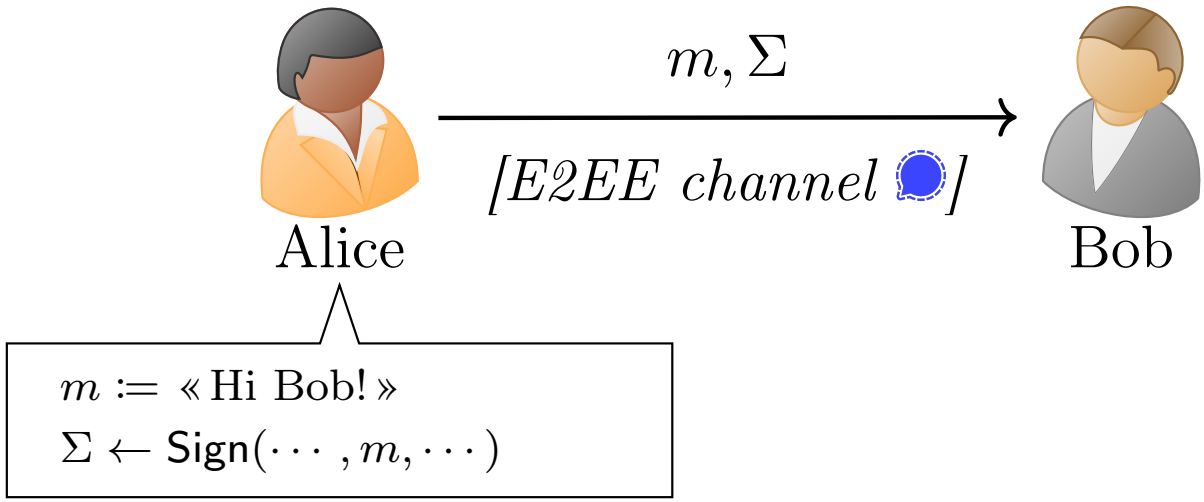
Milan Gonzalez-Thauvin and Keitaro Hashimoto
ETH Zurich, Switzerland, National Institute of Advanced Industrial Science and Technology (AIST), Japan

Asymmetric Message Franking: a moderation mechanism



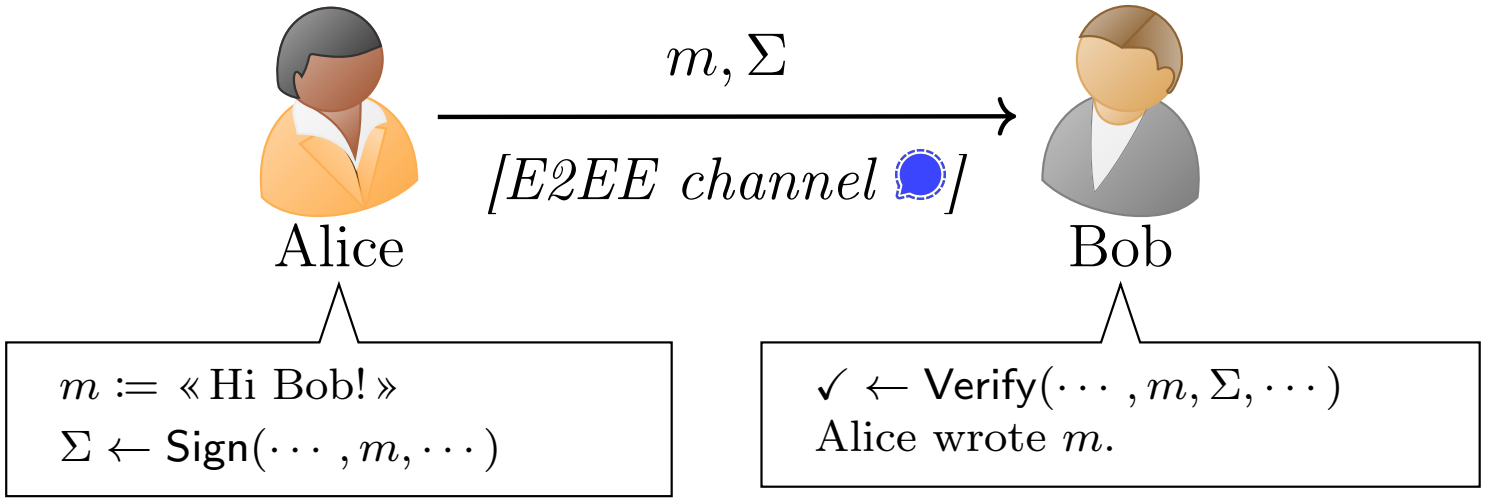
Milan Gonzalez-Thauvin and Keitaro Hashimoto
ETH Zurich, Switzerland, National Institute of Advanced Industrial Science and Technology (AIST), Japan

Asymmetric Message Franking: a moderation mechanism



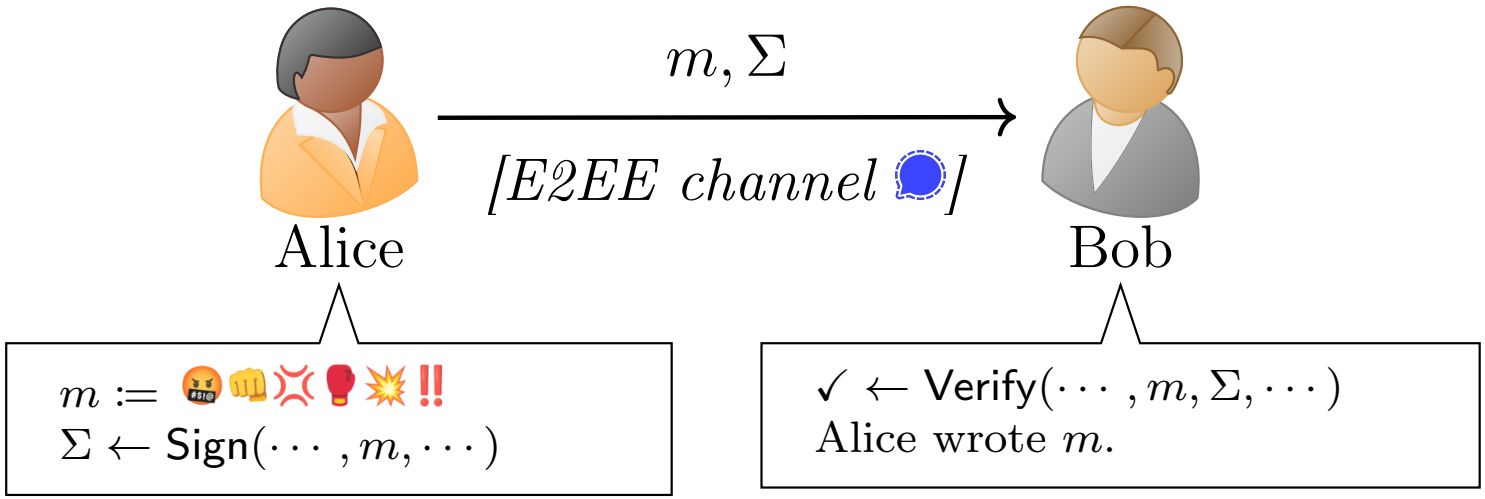
Milan Gonzalez-Thauvin and Keitaro Hashimoto
ETH Zurich, Switzerland, National Institute of Advanced Industrial Science and Technology (AIST), Japan

Asymmetric Message Franking: a moderation mechanism



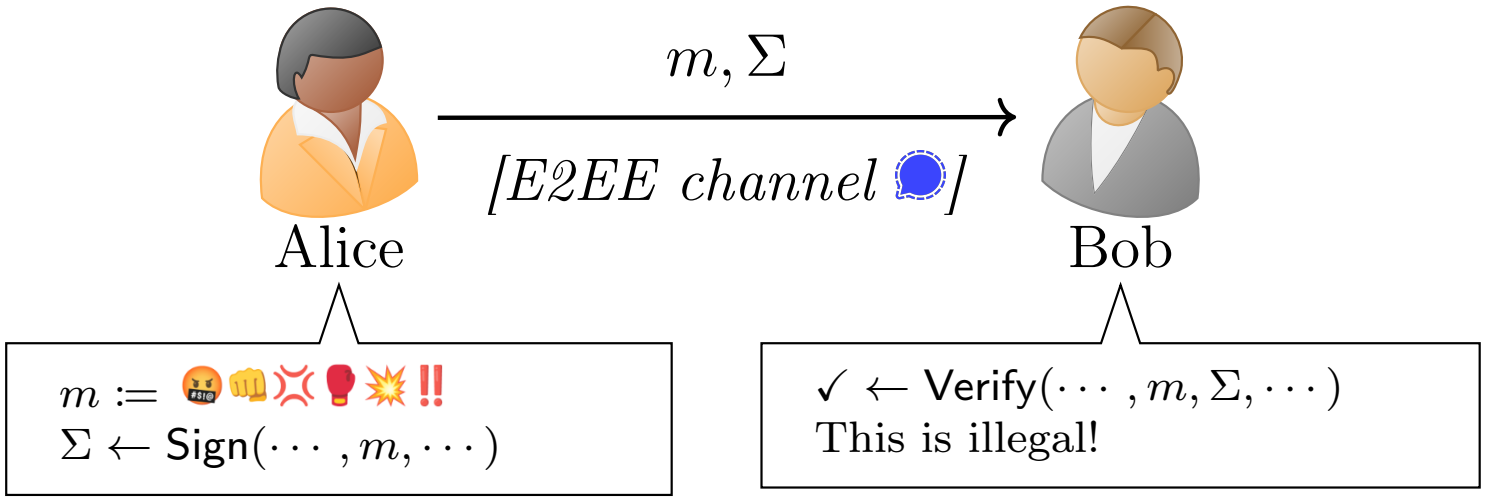
Milan Gonzalez-Thauvin and Keitaro Hashimoto
ETH Zurich, Switzerland, National Institute of Advanced Industrial Science and Technology (AIST), Japan

Asymmetric Message Franking: a moderation mechanism



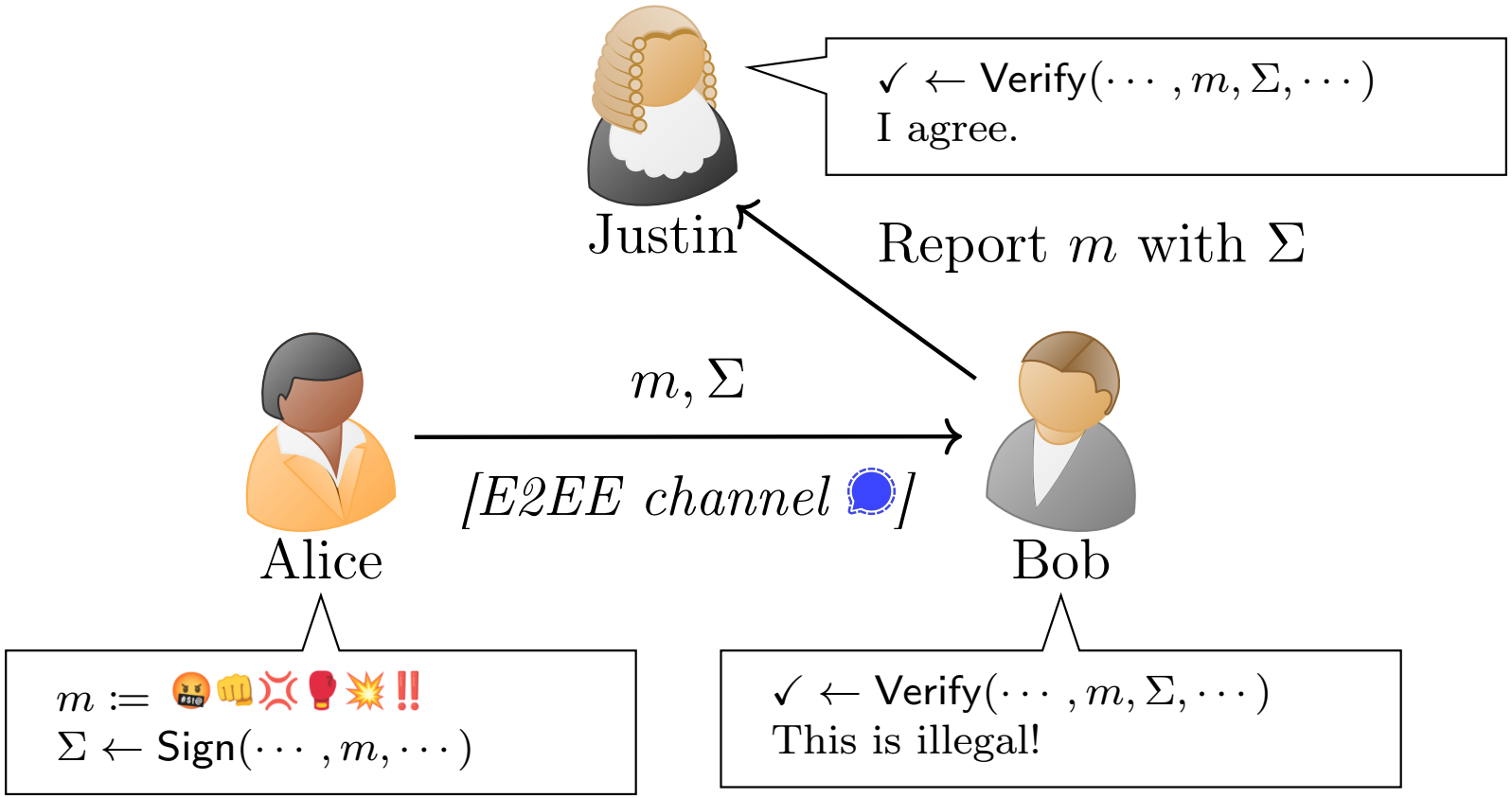
Milan Gonzalez-Thauvin and Keitaro Hashimoto
ETH Zurich, Switzerland; National Institute of Advanced Industrial Science and Technology (AIST), Japan

Asymmetric Message Franking: a moderation mechanism



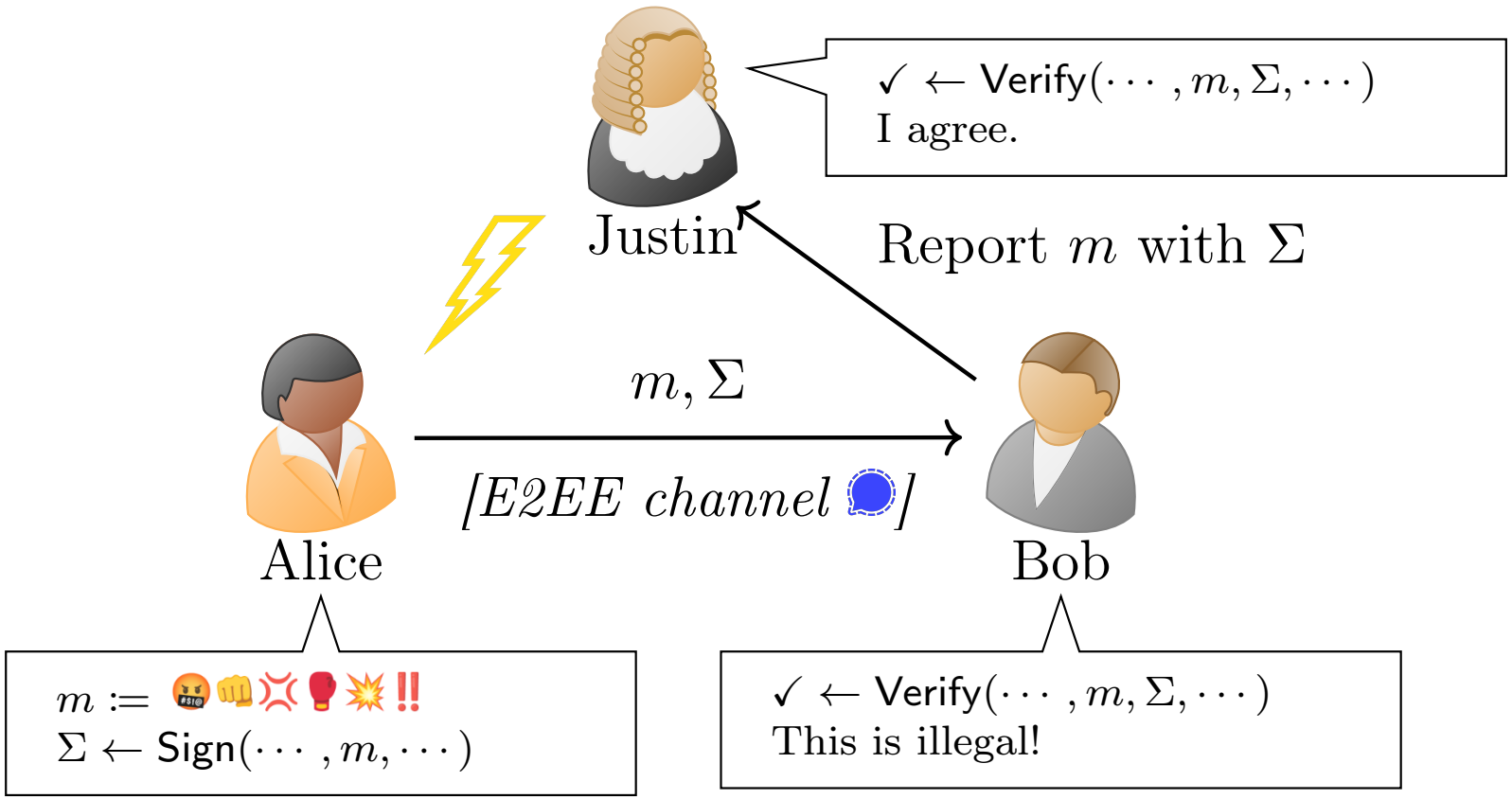
Milan Gonzalez-Thauvin and Keitaro Hashimoto
ETH Zurich, Switzerland; National Institute of Advanced Industrial Science and Technology (AIST), Japan

Asymmetric Message Franking: a moderation mechanism



Milan Gonzalez-Thauvin and Keitaro Hashimoto
ETH Zurich, Switzerland; National Institute of Advanced Industrial Science and Technology (AIST), Japan

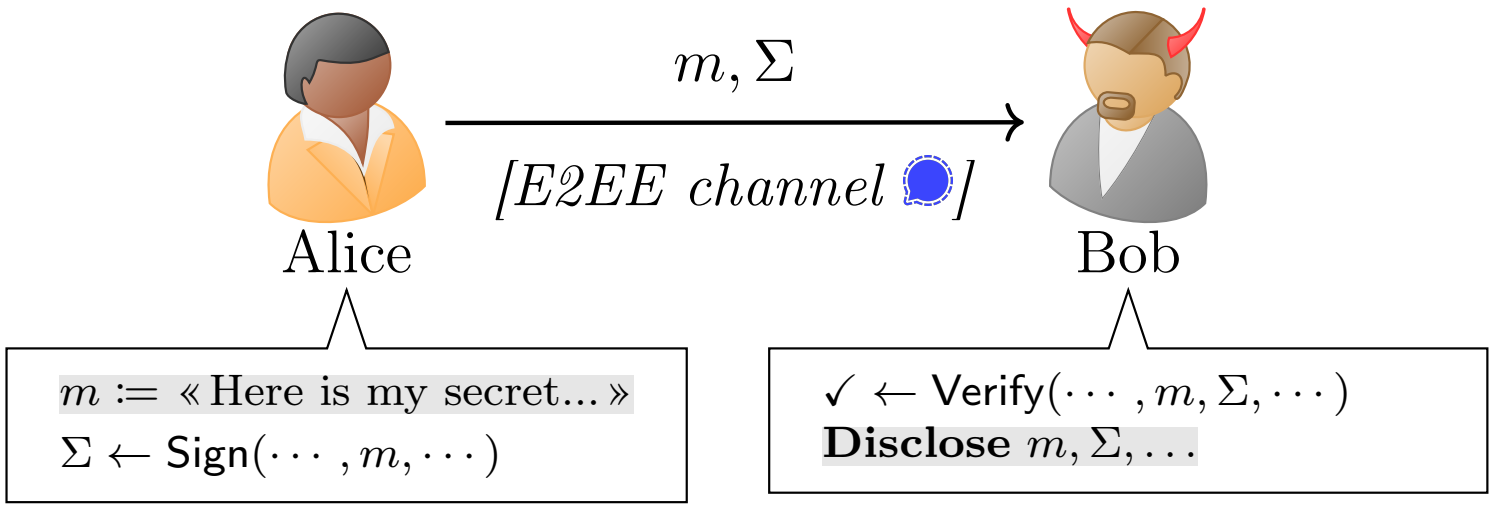
Asymmetric Message Franking: a moderation mechanism



Milan González-Thauvin and Keitaro Hashimoto
ETH Zurich, Switzerland; National Institute of Advanced Industrial Science and Technology (AIST), Japan

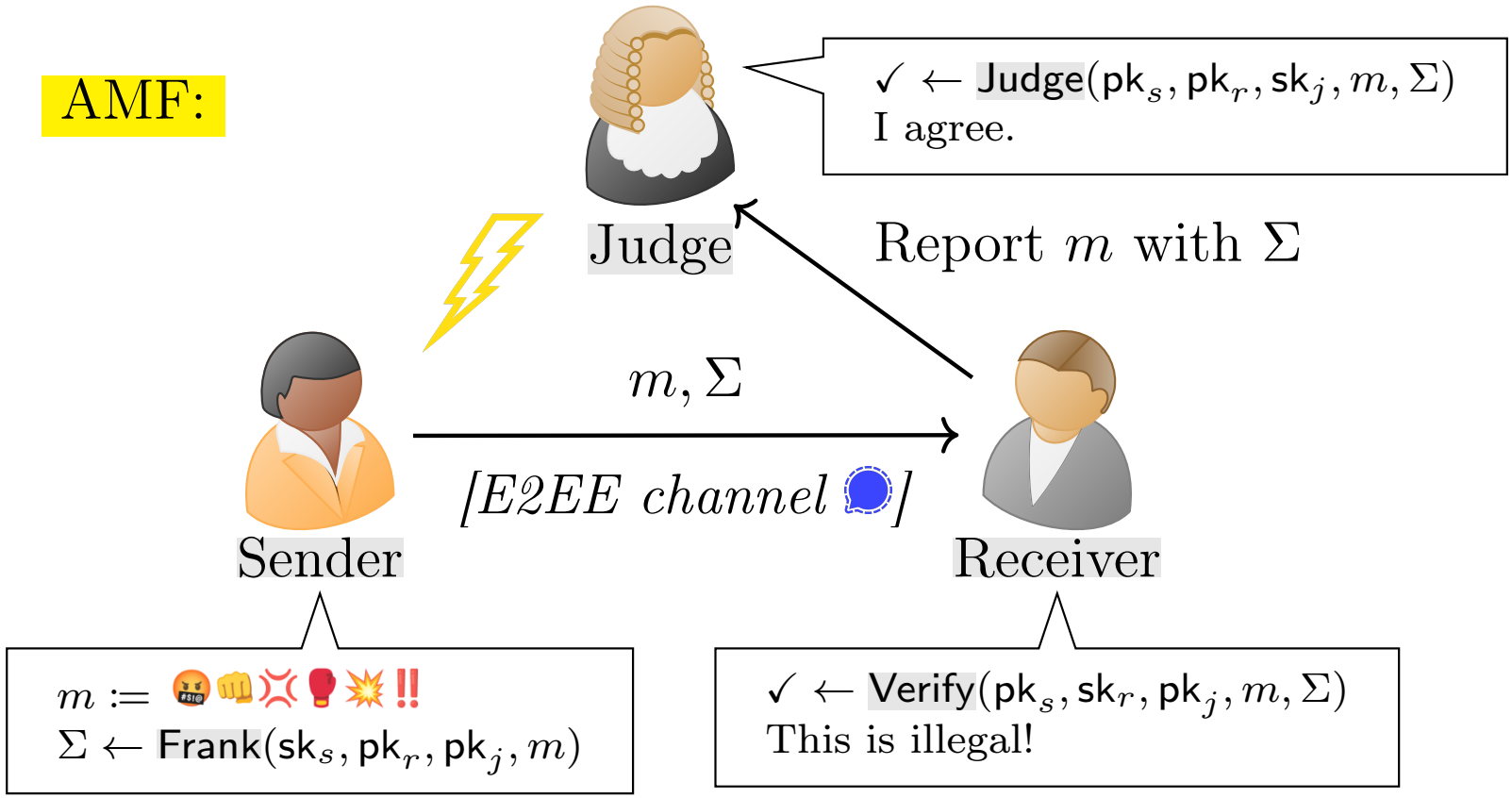
Asymmetric Message Franking: a moderation mechanism

No deniability!



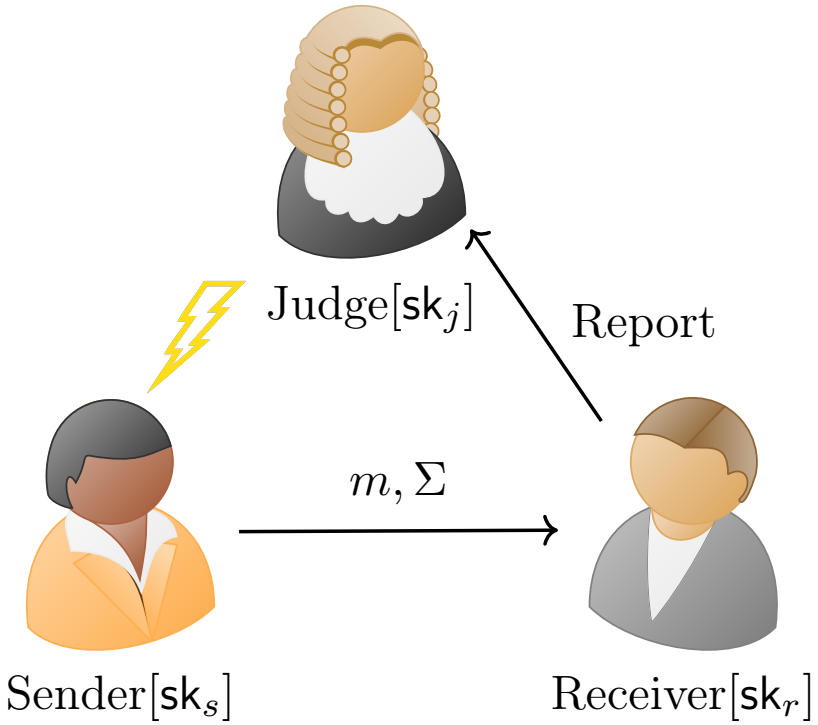
Milan González-Thauvin and Keitaro Hashimoto
ETH Zurich, Switzerland; National Institute of Advanced Industrial Science and Technology (AIST), Japan

Asymmetric Message Franking: a moderation mechanism



Milan Gonzalez-Thauvin and Keitaro Hashimoto
ETH Zurich, Switzerland; National Institute of Advanced Industrial Science and Technology (AIST), Japan

Security Properties of AMF



Correctness

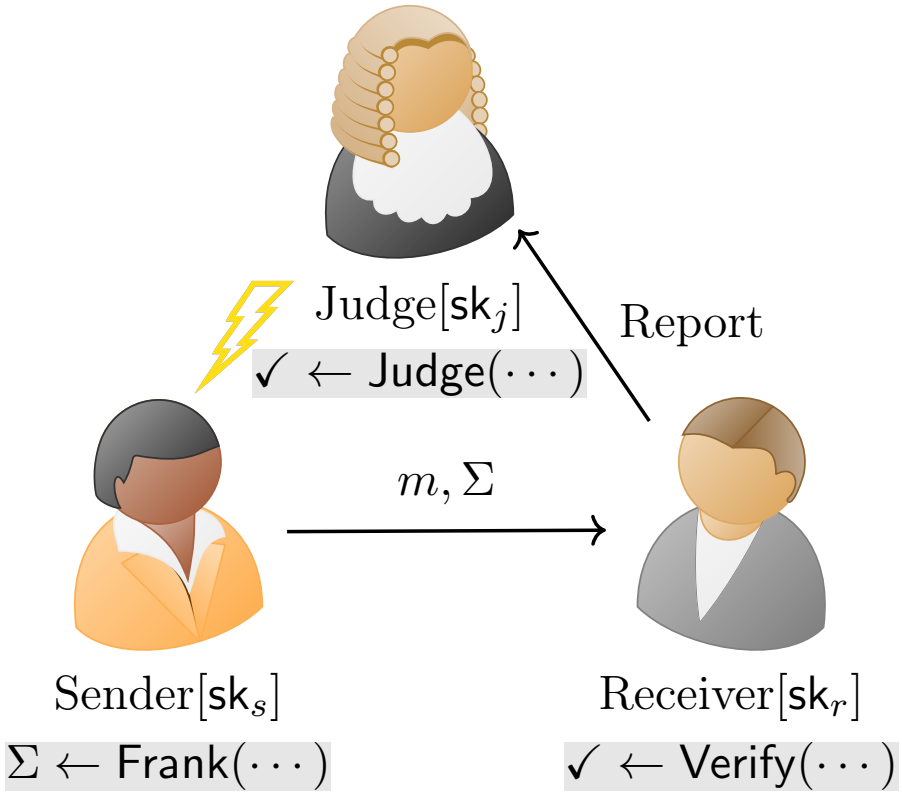
- Correctness

Accountability

- Unforgability
- Receiver-Binding
- Sender-Binding

Milan Gonzalez-Thauvin and Keitaro Hashimoto
ETH Zurich, Switzerland; National Institute of Advanced Industrial Science and Technology (AIST), Japan

Security Properties of AMF



Correctness

- Correctness

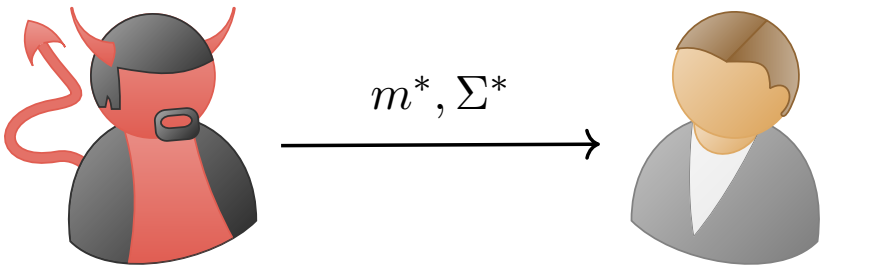
Accountability

- Unforgability
- Receiver-Binding
- Sender-Binding

Milan González-Thauvin and Keitaro Hashimoto
ETH Zurich, Switzerland; National Institute of Advanced Industrial Science and Technology (AIST), Japan

Security Properties of AMF

[Hard]



Correctness

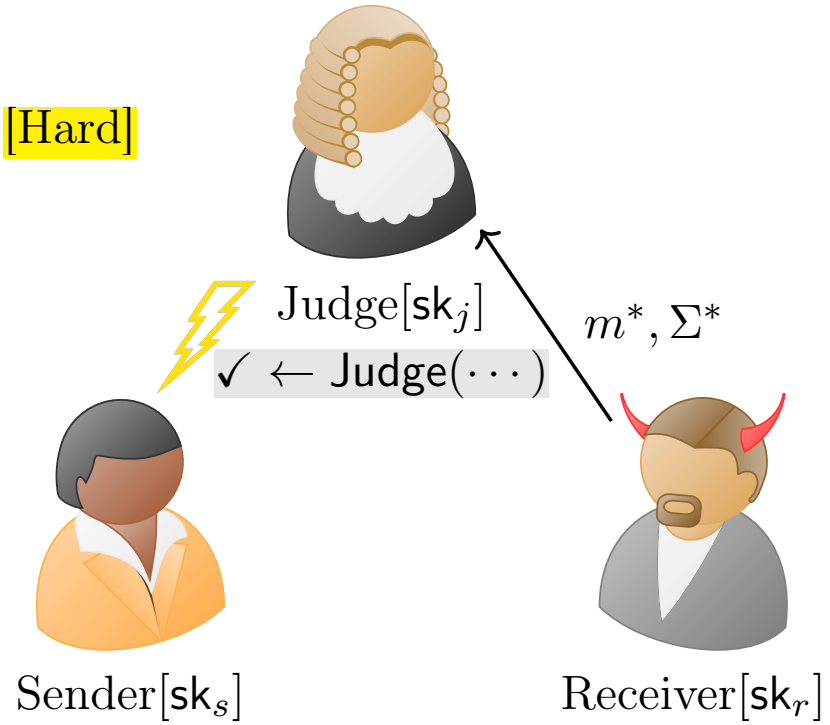
- Correctness

Accountability

- Unforgability
- Receiver-Binding
- Sender-Binding

Milan Gonzalez-Thauvin and Keitaro Hashimoto
ETH Zurich, Switzerland, National Institute of Advanced Industrial Science and Technology (AIST), Japan

Security Properties of AMF



Correctness

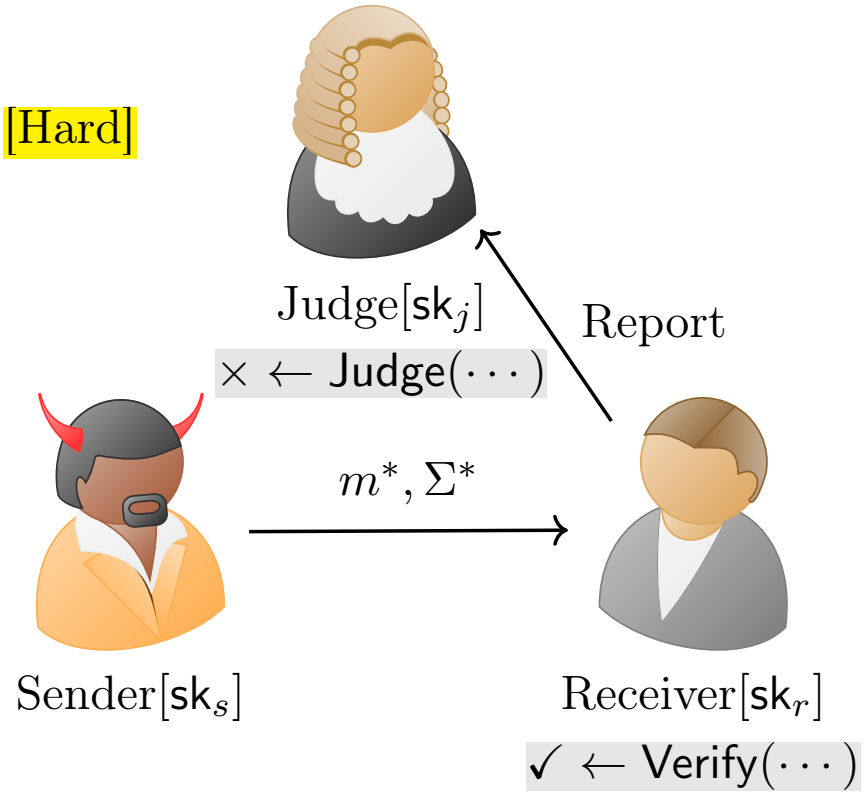
- Correctness

Accountability

- Unforgability
- Receiver-Binding
- Sender-Binding

Milan González-Thauvin and Keitaro Hashimoto
ETH Zurich, Switzerland; National Institute of Advanced Industrial Science and Technology (AIST), Japan

Security Properties of AMF



Correctness

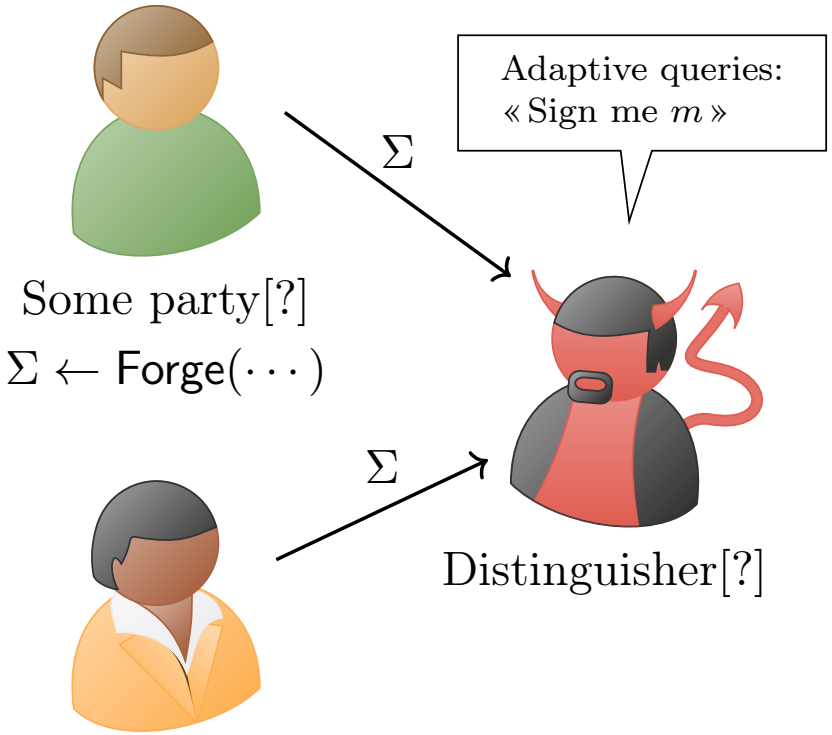
- Correctness

Accountability

- Unforgability
- Receiver-Binding
- Sender-Binding

Milan González-Thauvin and Keitaro Hashimoto
ETH Zurich, Switzerland; National Institute of Advanced Industrial Science and Technology (AIST), Japan

Security Properties of AMF



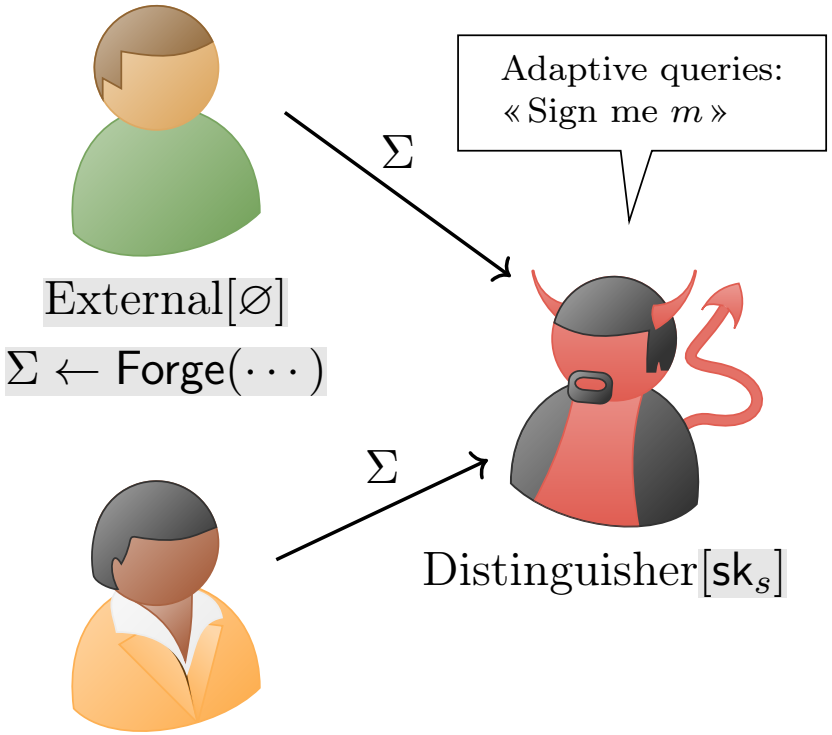
[Hard]

Deniability

- Universal Deniability
- Receiver Compromise Deniability
- Judge Compromise Deniability

Milan Gonzalez-Thauvin and Keitaro Hashimoto
ETH Zurich, Switzerland; National Institute of Advanced Industrial Science and Technology (AIST), Japan

Security Properties of AMF



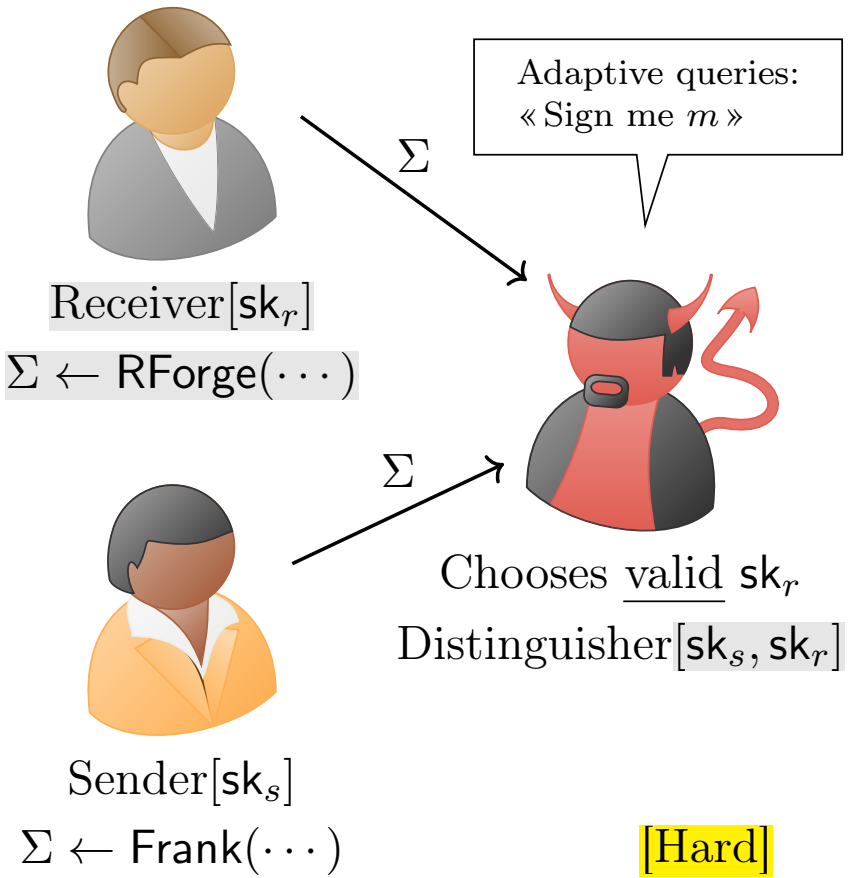
[Hard]

Deniability

- Universal Deniability
- Receiver Compromise Deniability
- Judge Compromise Deniability

Milan Gonzalez-Thauvin and Keitaro Hashimoto
ETH Zurich, Switzerland; National Institute of Advanced Industrial Science and Technology (AIST), Japan

Security Properties of AMF

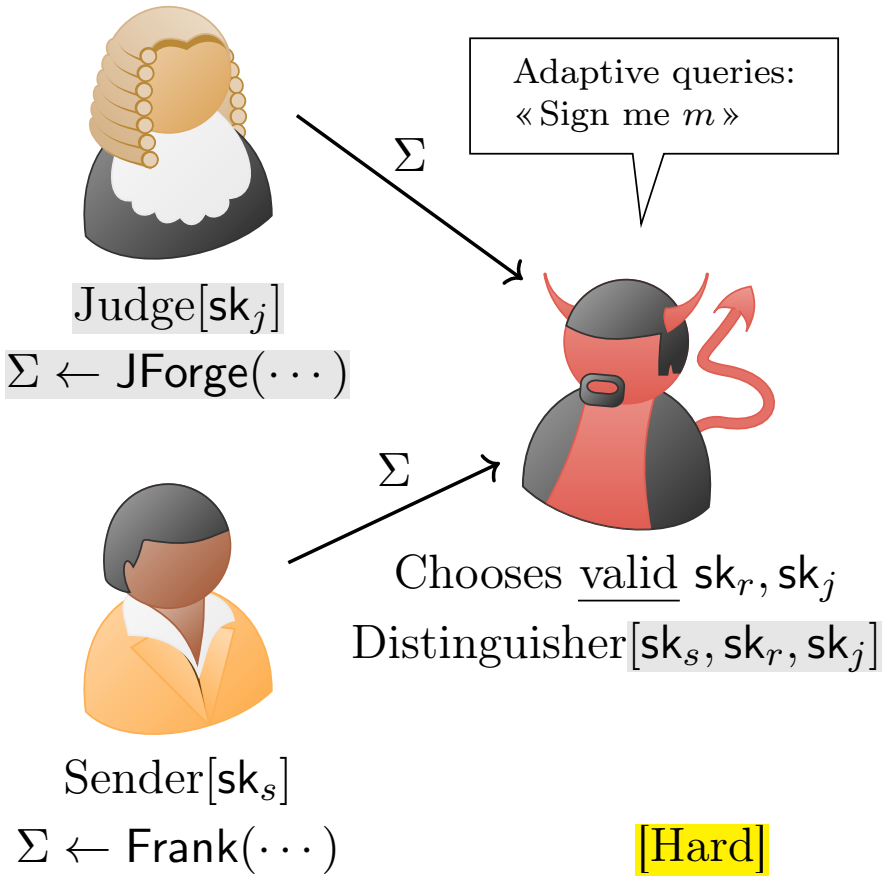


Deniability

- Universal Deniability
- Receiver Compromise Deniability
- Judge Compromise Deniability

Milan Gonzalez-Thauvin and Keitaro Hashimoto
ETH Zurich, Switzerland; National Institute of Advanced Industrial Science and Technology (AIST), Japan

Security Properties of AMF



Deniability

- Universal Deniability
- Receiver Compromise Deniability
- Judge Compromise Deniability

Milan Gonzalez-Thauvin and Keitaro Hashimoto
ETH Zurich, Switzerland; National Institute of Advanced Industrial Science and Technology (AIST), Japan

State of the Art

Main Related work

- [TGL+19] Asymmetric Message Franking: Content Moderation for Metadata-Private End-to-End Encryption, CRYPTO'19: **seminal work and first construction**
- [LZH+23] Asymmetric Group Message Franking: Definitions and Constructions, EuroCrypt'23: **context of group messaging and slightly different approach**

Technique: signature of knowledge derived from a Sigma protocol made non-interactive using the *Fiat-Shamir heuristic*.

Milan Gonzalez-Thauvin and Keitaro Hashimoto
ETH Zurich, Switzerland, National Institute of Advanced Industrial Science and Technology (AIST), Japan

State of the Art

Main Related work

- [TGL+19] Asymmetric Message Franking: Content Moderation for Metadata-Private End-to-End Encryption, CRYPTO'19: **seminal work and first construction**
- [LZH+23] Asymmetric Group Message Franking: Definitions and Constructions, EuroCrypt'23: **context of group messaging and slightly different approach**

Technique: signature of knowledge derived from a Sigma protocol made non-interactive using the *Fiat-Shamir heuristic*.

Milan Gonzalez-Thauvin and Keitaro Hashimoto
ETH Zurich, Switzerland, National Institute of Advanced Industrial Science and Technology (AIST), Japan

State of the Art

Main Related work

- [TGL+19] Asymmetric Message Franking: Content Moderation for Metadata-Private End-to-End Encryption, CRYPTO'19: **seminal work and first construction**
- [LZH+23] Asymmetric Group Message Franking: Definitions and Constructions, EuroCrypt'23: **context of group messaging and slightly different approach**

Technique: signature of knowledge derived from a Sigma protocol made non-interactive using the *Fiat-Shamir heuristic*.

Milan Gonzalez-Thauvin and Keitaro Hashimoto
ETH Zurich, Switzerland, National Institute of Advanced Industrial Science and Technology (AIST), Japan

Our Results [new]

Generic construction from signature, PKE and ZAP proofs

- Plain model
- Tight security
- Instantiation from various assumptions (incl. lattice-based)

(Somewhat) efficient construction from group-based assumptions

- Plain model
- 47 group elements (vs. ∼800 for generic construction)
- From group-based assumptions (requires pairings)

Milan Gonzalez-Thauvin and Keitaro Hashimoto
ETH Zurich, Switzerland, National Institute of Advanced Industrial Science and Technology (AIST), Japan

Our Results [new]

Generic construction from signature, PKE and ZAP proofs

- Plain model
- Tightly secure
- Instantiation from various assumptions (incl. lattice-based)

(Somewhat) efficient construction from group-based assumptions

- Plain model
- 47 group elements (vs. ∼800 for generic construction)
- From group-based assumptions (requires pairings)

Milan Gonzalez-Thauvin and Keitaro Hashimoto
ETH Zurich, Switzerland, National Institute of Advanced Industrial Science and Technology (AIST), Japan

Our Results [new]

Generic construction from signature, PKE and ZAP proofs

- Plain model
- Tightly secure
- Instantiation from various assumptions (incl. lattice-based)

(Somewhat) efficient construction from group-based assumptions

- Plain model
- 47 group elements (vs. ∼800 for generic construction)
- From group-based assumptions (requires pairings)

Milan Gonzalez-Thauvin and Keitaro Hashimoto
ETH Zurich, Switzerland, National Institute of Advanced Industrial Science and Technology (AIST), Japan

Our Results [new]

Generic construction from signature, PKE and ZAP proofs

- Plain model
- Tightly secure
- Instantiation from various assumptions (incl. lattice-based)

(Somewhat) efficient construction from group-based assumptions

- Plain model
- 47 group elements (vs. ∼800 for generic construction)
- From group-based assumptions (requires pairings)

Milan Gonzalez-Thauvin and Keitaro Hashimoto
ETH Zurich, Switzerland, National Institute of Advanced Industrial Science and Technology (AIST), Japan

Our Results [new]

Generic construction from signature, PKE and ZAP proofs

- Plain model
- Tightly secure
- Instantiation from various assumptions (incl. lattice-based)

(Somewhat) efficient construction from group-based assumptions

- Plain model
- 47 group elements (vs. ∼800 for generic construction)
- From group-based assumptions (requires pairings)

Milan Gonzalez-Thauvin and Keitaro Hashimoto
ETH Zurich, Switzerland, National Institute of Advanced Industrial Science and Technology (AIST), Japan

Our Results [new]

Generic construction from signature, PKE and ZAP proofs

- Plain model
- Tightly secure
- Instantiation from various assumptions (incl. lattice-based)

(Somewhat) efficient construction from group-based assumptions

- Plain model
- 47 group elements (vs. ∼800 for generic construction)
- From group-based assumptions (requires pairings)

Milan Gonzalez-Thauvin and Keitaro Hashimoto
ETH Zurich, Switzerland, National Institute of Advanced Industrial Science and Technology (AIST), Japan

Our Results [new]

Generic construction from signature, PKE and ZAP proofs

- Plain model
- Tightly secure
- Instantiation from various assumptions (incl. lattice-based)

(Somewhat) efficient construction from group-based assumptions

- Plain model
- 47 group elements (vs. ∼800 for generic construction)
- From group-based assumptions (requires pairings)

Milan Gonzalez-Thauvin and Keitaro Hashimoto
ETH Zurich, Switzerland, National Institute of Advanced Industrial Science and Technology (AIST), Japan

Our Results [new]

Generic construction from signature, PKE and ZAP proofs

- Plain model
- Tightly secure
- Instantiation from various assumptions (incl. lattice-based)

(Somewhat) efficient construction from group-based assumptions

- Plain model
- 47 group elements (vs. ∼800 for generic construction)
- From group-based assumptions (requires pairings)

Milan Gonzalez-Thauvin and Keitaro Hashimoto
ETH Zurich, Switzerland, National Institute of Advanced Industrial Science and Technology (AIST), Japan

Summary

Milan Gonzalez-Thauvin and Keitaro Hashimoto
ETH Zurich, Switzerland, National Institute of Advanced Industrial Science and Technology (AIST), Japan

Generic Construction: Starting Point

Signing algorithm	Signer's knowledge	Expected output	
		 Verify	 Judge
 Frank	sk_s	✓	✓
 Forge	$\varnothing$	×	×
 RForge	sk_r	✓	×
 JForge	sk_j	✓	✓

Expected output derived from AMF security properties

Milan Gonzalez-Thauvin and Keitaro Hashimoto
ETH Zurich, Switzerland; National Institute of Advanced Industrial Science and Technology (AIST), Japan

Generic Construction: Starting Point

Signing algorithm	Signer's knowledge	Expected output	
		 Verify	 Judge
 Frank	sk_s	✓	✓
 Forge	$\varnothing$	×	×
 RForge	sk_r	✓	×
 JForge	sk_j	✓	✓

Expected output derived from AMF security properties

Milan Gonzalez-Thauvin and Keitaro Hashimoto
ETH Zurich, Switzerland; National Institute of Advanced Industrial Science and Technology (AIST), Japan

Generic Construction: Starting Point

Signing algorithm	Signer's knowledge	Expected output	
		 Verify	 Judge
 Frank	sk_s	✓	✓
 Forge	$\varnothing$	×	×
 RForge	sk_r	✓	×
 JForge	sk_j	✓	✓

Expected output derived from AMF security properties

Milan Gonzalez-Thauvin and Keitaro Hashimoto
ETH Zurich, Switzerland; National Institute of Advanced Industrial Science and Technology (AIST), Japan

Generic Construction: Starting Point

Signing algorithm	Signer's knowledge	Expected output	
		 Verify	 Judge
 Frank	sk_s	1	1
 Forge	$\varnothing$	0	0
 RForge	sk_r	1	0
 JForge	sk_j	1	1

Expected output derived from AMF security properties

Milan Gonzalez-Thauvin and Keitaro Hashimoto
ETH Zurich, Switzerland; National Institute of Advanced Industrial Science and Technology (AIST), Japan

1) Mimic expected output

Signing algorithm	Signer's knowledge	Expected output	
		Verify	Judge
Frank	sk_s	1	1
Forge	$\varnothing$	0	0
RForge	sk_r	1	0
JForge	sk_j	1	1
	↓	↓	↓
	σ or 0	b_r	b_j

Milan Gonzalez-Thauvin and Keitaro Hashimoto
ETH Zurich, Switzerland; National Institute of Advanced Industrial Science and Technology (AIST), Japan

1) Mimic expected output

Signing algorithm	Signer's knowledge	Expected output	
		Verify	Judge
Frank	sk_s	1	1
Forge	$\varnothing$	0	0
RForge	sk_r	1	0
JForge	sk_j	1	1
	$\downarrow$	$\downarrow$	$\downarrow$
	σ or 0	b_r	b_j

Milan Gonzalez-Thauvin and Keitaro Hashimoto
ETH Zurich, Switzerland; National Institute of Advanced Industrial Science and Technology (AIST), Japan

2) Use encryption to parsimoniously disclose information

Signing algorithm	Signer's knowledge	Expected output	
		Verify	Judge
Frank	sk_s	1	1
Forge	$\varnothing$	0	0
RForge	sk_r	1	0
JForge	sk_j	1	1
	$\downarrow$	$\downarrow$	$\downarrow$
	$\mathsf{Enc}_{\mathsf{sky}}(\sigma \text{ or } 0)$ $\hookrightarrow \mathbf{c}_\sigma$	$\mathsf{Enc}_{\mathsf{ek}_r}(b_r)$ $\hookrightarrow \mathbf{c_r}$	$\mathsf{Enc}_{\mathsf{ek}_j}(b_j)$ $\hookrightarrow \mathbf{c_j}$

Milan Gonzalez-Thauvin and Keitaro Hashimoto
ETH Zurich, Switzerland; National Institute of Advanced Industrial Science and Technology (AIST), Japan

3) Add ZAP proof to hide author and prevent cheating

Signing algorithm	Signer's knowledge	Expected output	
		Verify	Judge
Frank	sk_s	1	1
Forge	$\varnothing$	0	0
RForge	sk_r	1	0
JForge	sk_j	1	1
	$\downarrow$	$\downarrow$	$\downarrow$
	$\mathsf{Enc}_{\mathsf{sky}}(\sigma \text{ or } 0)$ $\hookrightarrow \mathbf{c}_\sigma$	$\mathsf{Enc}_{\mathsf{ek}_r}(b_r)$ $\hookrightarrow \mathbf{c_r}$	$\mathsf{Enc}_{\mathsf{ek}_j}(b_j)$ $\hookrightarrow \mathbf{c_j}$

$\pi \leftarrow$ ZAP proof that the 3 ciphertexts follow one of the row using judge ZAP randomness zr_j

Add construction tricks to achieve provable security

Milan Gonzalez-Thauvin and Keitaro Hashimoto
ETH Zurich, Switzerland; National Institute of Advanced Industrial Science and Technology (AIST), Japan

3) Add ZAP proof to hide author and prevent cheating

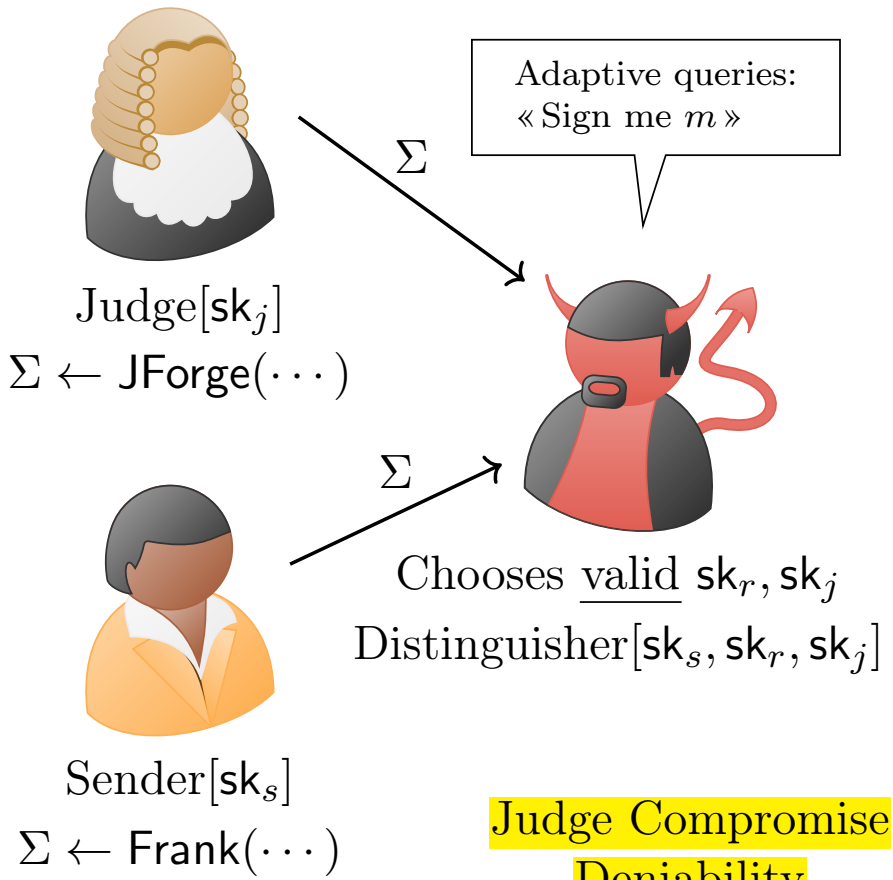
Signing algorithm	Signer's knowledge	Expected output	
		Verify	Judge
Frank	sk_s	1	1
Forge	$\varnothing$	0	0
RForge	sk_r	1	0
JForge	sk_j	1	1
	$\downarrow$	$\downarrow$	$\downarrow$
	$\mathsf{Enc}_{\mathsf{sky}}(\sigma \text{ or } 0)$ $\hookrightarrow \mathbf{c}_\sigma$	$\mathsf{Enc}_{\mathsf{ek}_r}(b_r)$ $\hookrightarrow \mathbf{c_r}$	$\mathsf{Enc}_{\mathsf{ek}_j}(b_j)$ $\hookrightarrow \mathbf{c_j}$

$\pi \leftarrow$ ZAP proof that the 3 ciphertexts follow one of the row using judge ZAP randomness zr_j

Add construction tricks to achieve provable security

Milan Gonzalez-Thauvin and Keitaro Hashimoto
ETH Zurich, Switzerland; National Institute of Advanced Industrial Science and Technology (AIST), Japan

Why using judge random coins for the ZAP proof?



Judge Compromise Deniability

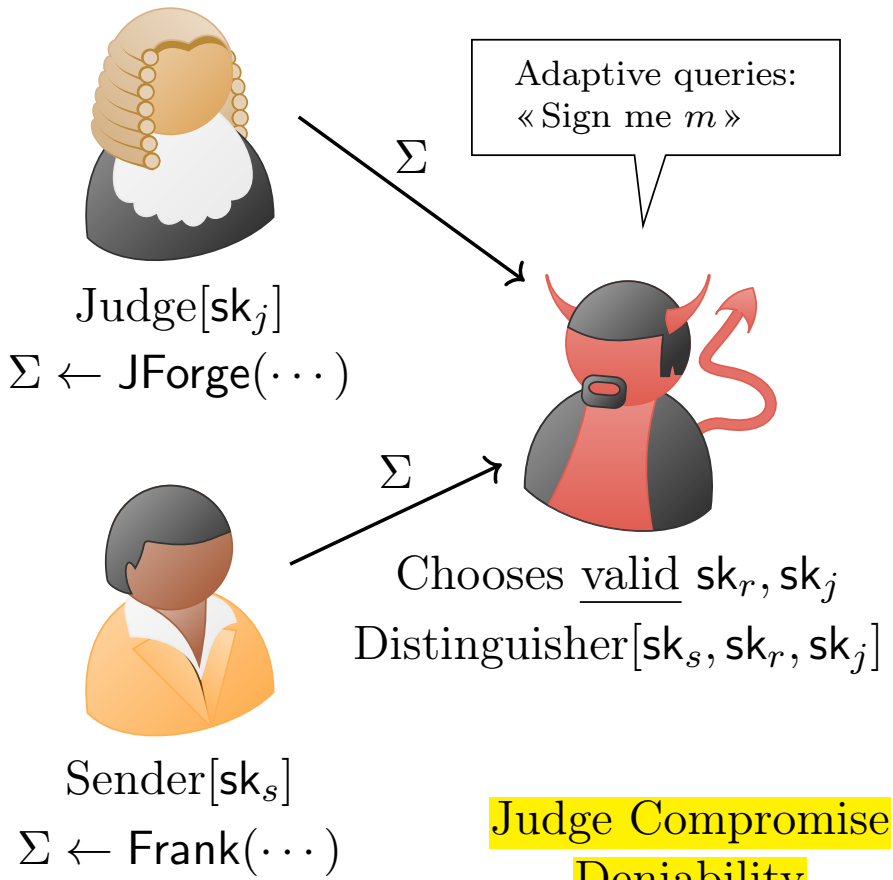
ZAP proofs

Subversion-resistant witness indistinguishable

→ WI remains even with maliciously chosen first message

Milan Gonzalez-Thauvin and Keitaro Hashimoto
ETH Zurich, Switzerland, National Institute of Advanced Industrial Science and Technology (AIST), Japan

Why using judge random coins for the ZAP proof?



Judge Compromise Deniability

ZAP proofs

Subversion-resistant witness indistinguishable

→ WI remains even with maliciously chosen first message

Milan Gonzalez-Thauvin and Keitaro Hashimoto
ETH Zurich, Switzerland; National Institute of Advanced Industrial Science and Technology (AIST), Japan

Instantiations

With this construction we obtain:

- A tightly secure AMF scheme from standard group-based assumptions

Problem: signature size ($\sim$ 800 group elements using group-based building blocks and Groth-Sahai proof system)

Milan Gonzalez-Thauvin and Keitaro Hashimoto
ETH Zurich, Switzerland, National Institute of Advanced Industrial Science and Technology (AIST), Japan

Summary

Milan Gonzalez-Thauvin and Keitaro Hashimoto
ETH Zurich, Switzerland, National Institute of Advanced Industrial Science and Technology (AIST), Japan

Reduce signature size: our approach

Use ZAP proof system for restricted class of languages

- ZAP for NP languages: $\times$ (too inefficient)
- ZAP for linear languages: $\times$ (need an OR, and because of impossibility results on unforgeable signature [DHH+21])
- ZAP for algebraic language [CH20]: ✓
  $\rightarrow$ contains linear languages and disjunctions

Embed authenticity into the ZAP

- No more signature to encrypt, the proof *is* the signature
- Use proof-based Waters-like signature (inspired by [DH26])

Milan Gonzalez-Thauvin and Keitaro Hashimoto
ETH Zurich, Switzerland, National Institute of Advanced Industrial Science and Technology (AIST), Japan

Reduce signature size: our approach

Use ZAP proof system for restricted class of languages

- ZAP for NP languages: × (too inefficient)
- ZAP for linear languages: × (need an OR, and because of impossibility results on unforgeable signature [DHH+21])
- ZAP for algebraic language [CH20]: ✓
  → contains linear languages and disjunctions

Embed authenticity into the ZAP

- No more signature to encrypt, the proof *is* the signature
- Use proof-based Waters-like signature (inspired by [DH26])

Milan Gonzalez-Thauvin and Keitaro Hashimoto
ETH Zurich, Switzerland, National Institute of Advanced Industrial Science and Technology (AIST), Japan

Reduce signature size: our approach

Use ZAP proof system for restricted class of languages

- ZAP for NP languages: × (too inefficient)
- ZAP for linear languages: × (need an OR, and because of impossibility results on unforgeable signature [DHH+21])
- ZAP for algebraic language [CH20]: ✓
  → contains linear languages and disjunctions

Embed authenticity into the ZAP

- No more signature to encrypt, the proof *is* the signature
- Use proof-based Waters-like signature (inspired by [DH26])

Milan Gonzalez-Thauvin and Keitaro Hashimoto
ETH Zurich, Switzerland; National Institute of Advanced Industrial Science and Technology (AIST), Japan

Reduce signature size: our approach

Use ZAP proof system for restricted class of languages

- ZAP for NP languages: × (too inefficient)
- ZAP for linear languages: × (need an OR, and because of impossibility results on unforgeable signature [DHH+21])
- ZAP for algebraic language [CH20]: ✓
  → contains linear languages and disjunctions

Embed authenticity into the ZAP

- No more signature to encrypt, the proof *is* the signature
- Use proof-based Waters-like signature (inspired by [DH26])

Milan Gonzalez-Thauvin and Keitaro Hashimoto
ETH Zurich, Switzerland, National Institute of Advanced Industrial Science and Technology (AIST), Japan

Reduce signature size: our approach

Use ZAP proof system for restricted class of languages

- ZAP for NP languages: × (too inefficient)
- ZAP for linear languages: × (need an OR, and because of impossibility results on unforgeable signature [DHH+21])
- ZAP for algebraic language [CH20]: ✓
  → contains linear languages and disjunctions

Embed authenticity into the ZAP

- No more signature to encrypt, the proof *is* the signature
- Use proof-based Waters-like signature (inspired by [DH26])

Milan Gonzalez-Thauvin and Keitaro Hashimoto
ETH Zurich, Switzerland, National Institute of Advanced Industrial Science and Technology (AIST), Japan

Waters-like signature in more detail

bit i of $\mathcal{M}$	0	1	2	3	4	5	6	$\cdots$	λ
$\mathsf{sk} \in \mathbb{Z}_p :=$	1	0	0	0	0	0	0	$\cdots$	0
$\mathsf{pk} = \mathsf{HCom}(\uparrow) :=$	C_0	C_1	C_2	C_3	C_4	C_5	C_6	$\cdots$	C_λ
$m \in \{0,1\}^\lambda :=$		1	0	1	0	1	1	$\cdots$	1
Keep only $m_i = 1$	C_0	C_1		C_3		C_5	C_6	$\cdots$	C_λ

$C_{\text{hash}} := \sum(\cdots) = \mathsf{HCom}(1)$

$\mathsf{sk}' :=$	1	0	0	0	0	0	0	$\cdots$	0
$\mathsf{pk}' :=$	C'_0	C'_1	C'_2	C'_3	C'_4	C'_5	C'_6	$\cdots$	C'_λ
$C'_{\text{hash}} :=$	$\sum(\cdots) = \mathsf{HCom}(1)$								

$\sigma :=$ ZAP proof that C_h or C'_h contains a non-zero element in $\mathbb{Z}_p$

Milan Gonzalez-Thauvin and Keitaro Hashimoto
ETH Zurich, Switzerland, National Institute of Advanced Industrial Science and Technology (AIST), Japan

Waters-like signature in more detail

bit i of $\mathcal{M}$	0	1	2	3	4	5	6	$\cdots$	λ
$\mathsf{sk} \in \mathbb{Z}_p :=$	1	0	0	0	0	0	0	$\cdots$	0
$\mathsf{pk} = \mathsf{HCom}(\uparrow) :=$	C_0	C_1	C_2	C_3	C_4	C_5	C_6	$\cdots$	C_λ
$m \in \{0,1\}^\lambda :=$		1	0	1	0	1	1	$\cdots$	1
Keep only $m_i = 1$	C_0	C_1		C_3		C_5	C_6	$\cdots$	C_λ

$C_{\text{hash}} := \sum(\cdots) = \mathsf{HCom}(1)$

$\mathsf{sk}' :=$	1	0	0	0	0	0	0	$\cdots$	0
$\mathsf{pk}' :=$	C'_0	C'_1	C'_2	C'_3	C'_4	C'_5	C'_6	$\cdots$	C'_λ
$C'_{\text{hash}} :=$	$\sum(\cdots) = \mathsf{HCom}(1)$								

$\sigma :=$ ZAP proof that C_h or C'_h contains a non-zero element in $\mathbb{Z}_p$

Milan Gonzalez-Thauvin and Keitaro Hashimoto
ETH Zurich, Switzerland, National Institute of Advanced Industrial Science and Technology (AIST), Japan

Waters-like signature in more detail

bit i of $\mathcal{M}$	0	1	2	3	4	5	6	$\cdots$	λ
$\mathsf{sk} \in \mathbb{Z}_p :=$	1	0	0	0	0	0	0	$\cdots$	0
$\mathsf{pk} = \mathsf{HCom}(\uparrow) :=$	C_0	C_1	C_2	C_3	C_4	C_5	C_6	$\cdots$	C_λ
$m \in \{0,1\}^\lambda :=$		1	0	1	0	1	1	$\cdots$	1
Keep only $m_i = 1$	C_0	C_1		C_3		C_5	C_6	$\cdots$	C_λ

$C_{\text{hash}} := \sum(\cdots) = \mathsf{HCom}(1)$

$\mathsf{sk}' :=$	1	0	0	0	0	0	0	$\cdots$	0
$\mathsf{pk}' :=$	C'_0	C'_1	C'_2	C'_3	C'_4	C'_5	C'_6	$\cdots$	C'_λ
$C'_{\text{hash}} :=$	$\sum(\cdots) = \mathsf{HCom}(1)$								

$\sigma :=$ ZAP proof that C_h or C'_h contains a non-zero element in $\mathbb{Z}_p$

Milan Gonzalez-Thauvin and Keitaro Hashimoto
ETH Zurich, Switzerland, National Institute of Advanced Industrial Science and Technology (AIST), Japan

Waters-like signature in more detail

bit i of $\mathcal{M}$	0	1	2	3	4	5	6	$\cdots$	λ
$\mathsf{sk} \in \mathbb{Z}_p :=$	1	0	0	0	0	0	0	$\cdots$	0
$\mathsf{pk} = \mathsf{HCom}(\uparrow) :=$	C_0	C_1	C_2	C_3	C_4	C_5	C_6	$\cdots$	C_λ
$m \in \{0,1\}^\lambda :=$		$\underline{1}$	0	$\underline{1}$	0	$\underline{1}$	$\underline{1}$	$\cdots$	$\underline{1}$
Keep only $m_i = 1$	C_0	C_1		C_3		C_5	C_6	$\cdots$	C_λ

$C_{\text{hash}} := \sum(\cdots) = \mathsf{HCom}(1)$

$\mathsf{sk}' :=$	1	0	0	0	0	0	0	$\cdots$	0
$\mathsf{pk}' :=$	C'_0	C'_1	C'_2	C'_3	C'_4	C'_5	C'_6	$\cdots$	C'_λ
$C'_{\text{hash}} :=$	$\sum(\cdots) = \mathsf{HCom}(1)$								

$\sigma :=$ ZAP proof that C_h or C'_h contains a non-zero element in $\mathbb{Z}_p$

Milan Gonzalez-Thauvin and Keitaro Hashimoto
ETH Zurich, Switzerland; National Institute of Advanced Industrial Science and Technology (AIST), Japan

Waters-like signature in more detail

bit i of $\mathcal{M}$	0	1	2	3	4	5	6	$\cdots$	λ
$\mathsf{sk} \in \mathbb{Z}_p :=$	1	0	0	0	0	0	0	$\cdots$	0
$\mathsf{pk} = \mathsf{HCom}(\uparrow) :=$	C_0	C_1	C_2	C_3	C_4	C_5	C_6	$\cdots$	C_λ
$m \in \{0,1\}^\lambda :=$		$\underline{1}$	0	$\underline{1}$	0	$\underline{1}$	$\underline{1}$	$\cdots$	$\underline{1}$
Keep only $m_i = 1$	C_0	C_1		C_3		C_5	C_6	$\cdots$	C_λ

$C_{\text{hash}} := \sum(\cdots) = \mathsf{HCom}(1)$

$\mathsf{sk}' :=$	1	0	0	0	0	0	0	$\cdots$	0
$\mathsf{pk}' :=$	C'_0	C'_1	C'_2	C'_3	C'_4	C'_5	C'_6	$\cdots$	C'_λ
$C'_{\text{hash}} :=$	$\sum(\cdots) = \mathsf{HCom}(1)$								

$\sigma :=$ ZAP proof that C_h or C'_h contains a non-zero element in $\mathbb{Z}_p$

Milan Gonzalez-Thauvin and Keitaro Hashimoto
ETH Zurich, Switzerland; National Institute of Advanced Industrial Science and Technology (AIST), Japan

Waters-like signature in more detail

bit i of $\mathcal{M}$	0	1	2	3	4	5	6	$\cdots$	λ
$\mathsf{sk} \in \mathbb{Z}_p :=$	1	0	0	0	0	0	0	$\cdots$	0
$\mathsf{pk} = \mathsf{HCom}(\uparrow) :=$	C_0	C_1	C_2	C_3	C_4	C_5	C_6	$\cdots$	C_λ
$m \in \{0,1\}^\lambda :=$		$\underline{1}$	0	$\underline{1}$	0	$\underline{1}$	$\underline{1}$	$\cdots$	$\underline{1}$
Keep only $m_i = 1$	C_0	C_1		C_3		C_5	C_6	$\cdots$	C_λ

$$C_{\text{hash}} := \sum(\cdots) = \mathsf{HCom}(1)$$

$\mathsf{sk}' :=$	1	0	0	0	0	0	0	$\cdots$	0
$\mathsf{pk}' :=$	C'_0	C'_1	C'_2	C'_3	C'_4	C'_5	C'_6	$\cdots$	C'_λ
$C'_{\text{hash}} :=$	$\sum(\cdots) = \mathsf{HCom}(1)$								

$\sigma :=$ ZAP proof that C_h or C'_h contains a non-zero element in $\mathbb{Z}_p$

Milan Gonzalez-Thauvin and Keitaro Hashimoto
ETH Zurich, Switzerland; National Institute of Advanced Industrial Science and Technology (AIST), Japan

Waters-like signature in more detail

bit i of $\mathcal{M}$	0	1	2	3	4	5	6	$\cdots$	λ
$\mathsf{sk} \in \mathbb{Z}_p :=$	1	0	0	0	0	0	0	$\cdots$	0
$\mathsf{pk} = \mathsf{HCom}(\uparrow) :=$	C_0	C_1	C_2	C_3	C_4	C_5	C_6	$\cdots$	C_λ
$m \in \{0,1\}^\lambda :=$		$\underline{1}$	0	$\underline{1}$	0	$\underline{1}$	$\underline{1}$	$\cdots$	$\underline{1}$
Keep only $m_i = 1$	C_0	C_1		C_3		C_5	C_6	$\cdots$	C_λ

$C_{\text{hash}} := \sum(\cdots) = \mathsf{HCom}(1)$

$\mathsf{sk}' :=$	1	0	0	0	0	0	0	$\cdots$	0
$\mathsf{pk}' :=$	C'_0	C'_1	C'_2	C'_3	C'_4	C'_5	C'_6	$\cdots$	C'_λ
$C'_{\text{hash}} :=$	$\sum(\cdots) = \mathsf{HCom}(1)$								

$\sigma :=$ ZAP proof that C_h or C'_h contains a non-zero element in $\mathbb{Z}_p$

Milan Gonzalez-Thauvin and Keitaro Hashimoto
ETH Zurich, Switzerland; National Institute of Advanced Industrial Science and Technology (AIST), Japan

Waters-like signature in more detail

bit i of $\mathcal{M}$	0	1	2	3	4	5	6	$\cdots$	λ
$\mathsf{sk} \in \mathbb{Z}_p :=$	1	0	0	0	0	0	0	$\cdots$	0
$\mathsf{pk} = \mathsf{HCom}(\uparrow) :=$	C_0	C_1	C_2	C_3	C_4	C_5	C_6	$\cdots$	C_λ
$m \in \{0,1\}^\lambda :=$		$\underline{1}$	0	$\underline{1}$	0	$\underline{1}$	$\underline{1}$	$\cdots$	$\underline{1}$
Keep only $m_i = 1$	C_0	C_1		C_3		C_5	C_6	$\cdots$	C_λ

$C_{\text{hash}} := \sum(\cdots) = \mathsf{HCom}(1)$

$\mathsf{sk}' :=$	1	0	0	0	0	0	0	$\cdots$	0
$\mathsf{pk}' :=$	C'_0	C'_1	C'_2	C'_3	C'_4	C'_5	C'_6	$\cdots$	C'_λ
$C'_{\text{hash}} :=$	$\sum(\cdots) = \mathsf{HCom}(1)$								

$\sigma :=$ ZAP proof that C_h or C'_h contains a non-zero element in $\mathbb{Z}_p$

Milan Gonzalez-Thauvin and Keitaro Hashimoto
ETH Zurich, Switzerland, National Institute of Advanced Industrial Science and Technology (AIST), Japan

Waters-like signature in more detail

bit i of $\mathcal{M}$	0	1	2	3	4	5	6	$\cdots$	λ
$\mathsf{sk} \in \mathbb{Z}_p :=$	x_0	x_1	x_2	x_3	x_4	x_5	x_6	$\cdots$	x_λ
$\mathsf{pk} = \mathsf{HCom}(\uparrow) :=$	C_0	C_1	C_2	C_3	C_4	C_5	C_6	$\cdots$	C_λ
$m \in \{0,1\}^\lambda :=$		$\underline{1}$	0	$\underline{1}$	0	$\underline{1}$	$\underline{1}$	$\cdots$	$\underline{1}$
Keep only $m_i = 1$	C_0	C_1		C_3		C_5	C_6	$\cdots$	C_λ

$C_{\text{hash}} := \sum(\cdots) = ?$

$\mathsf{sk}' :=$	x'_0	x'_1	x'_2	x'_3	x'_4	x'_5	x'_6	$\cdots$	x'_λ
$\mathsf{pk}' :=$	C'_0	C'_1	C'_2	C'_3	C'_4	C'_5	C'_6	$\cdots$	C'_λ
$C'_{\text{hash}} :=$	$\sum(\cdots) = ?$								

$\sigma :=$ ZAP proof that C_h or C'_h contains a non-zero element in $\mathbb{Z}_p$

Milan Gonzalez-Thauvin and Keitaro Hashimoto
ETH Zurich, Switzerland; National Institute of Advanced Industrial Science and Technology (AIST), Japan

Concrete results

	Signature size†	PK size†	Model
[TGL+19]	9 GE + 6 S	1 GE	RO
Generic construction§	∼800 GE	7 GE	Plain
Efficient construction	47 GE	$\mathcal{O}(\lambda)$ GE	Plain

Comparison of different group-based AMF schemes

†: GE = Group element / S = scalar in $\mathbb{Z}_p$

§: Using Groth-Sahai NIWI and trusted setup

Milan Gonzalez-Thauvin and Keitaro Hashimoto
ETH Zurich, Switzerland, National Institute of Advanced Industrial Science and Technology (AIST), Japan

Questions?

G. Couteau and D. Hartmann.
Shorter non-interactive zero-knowledge arguments and ZAPs for algebraic languages.
Crypto, 2020.

N. Döttling, D. Hartmann, D. Hofheinz, E. Kiltz, S. Schäge, and B. Ursu.
On the impossibility of purely algebraic signatures.
TCC, 2021.

J. Lai, G. Zeng, Z. Huang, S. M. Yiu, X. Mu, and J. Weng.
Asymmetric group message franking: Definitions and constructions.
Eurocrypt, 2023.

N. Tyagi, P. Grubbs, J. Len, I. Miers, and T. Ristenpart.
Asymmetric message franking: Content moderation for metadata-private end-to-end encryption.
Crypto, 2019.

Milan Gonzalez-Thauvin and Keitaro Hashimoto
ETH Zurich, Switzerland, National Institute of Advanced Industrial Science and Technology (AIST), Japan