Threshold Signatures with Private Accountability

Dan Boneh[1] Chelsea Komlo[2]

Stanford University

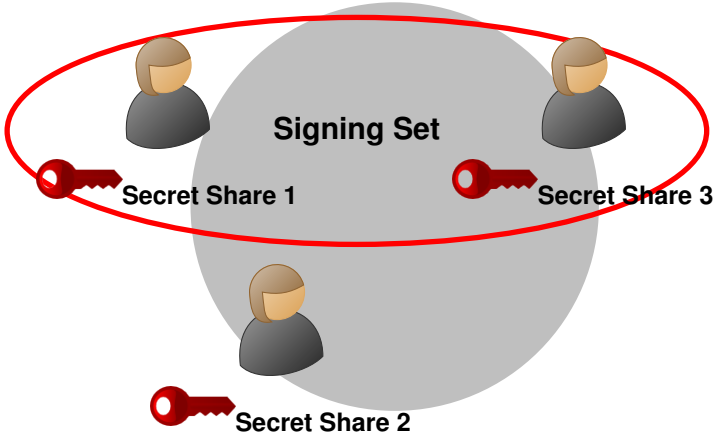
University of Waterloo

CRYPTO, August 13, 2022

https://eprint.iacr.org/2022/TODO

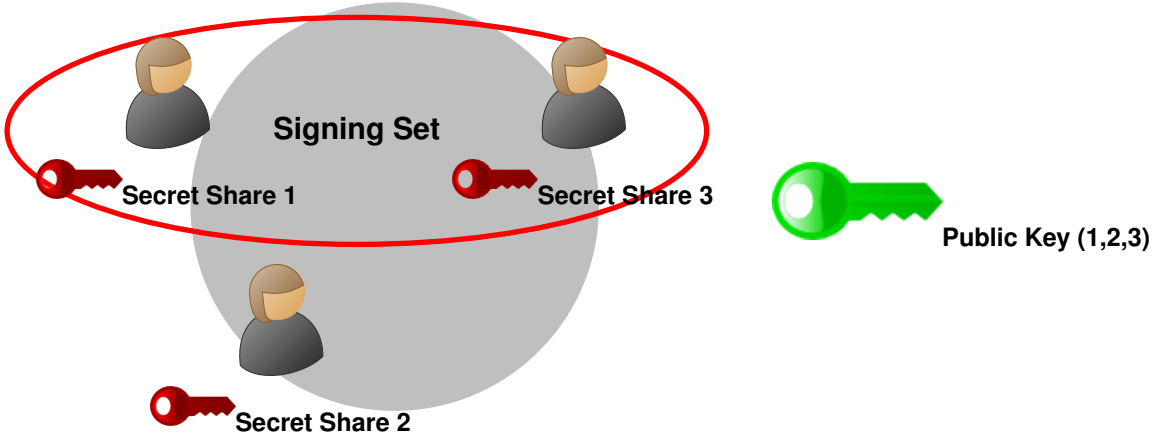
Threshold Signatures: Joint Public Key, Secret-Shared Private Key

(2, 3) Example



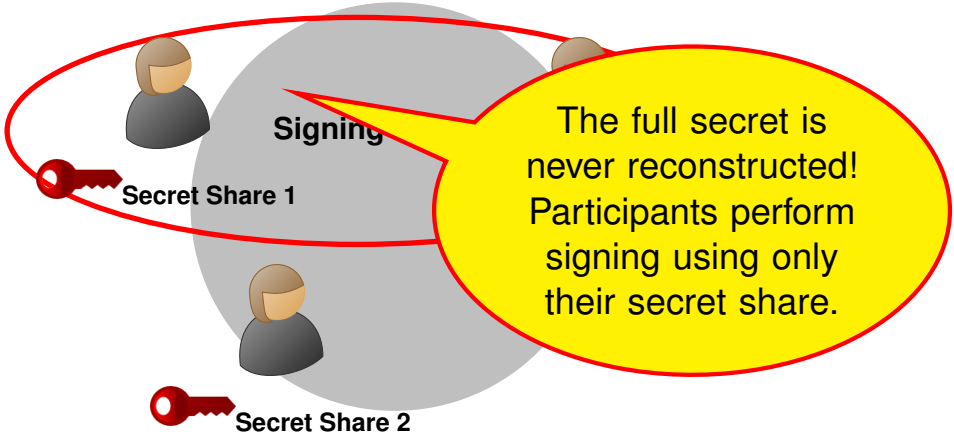
Threshold Signatures: Joint Public Key, Secret-Shared Private Key

(2, 3) Example



Threshold Signatures: Joint Public Key, Secret-Shared Private Key

(2, 3) Example



Private Threshold Scheme (PTS)

- The signature reveals nothing nothing about:
  - the threshold
  - the quorum of signers

- Implicit in existing threshold signature schemes that employ Shamir secret sharing (FROST).

Private Threshold Scheme (PTS)

- The signature reveals nothing nothing about:
  - the threshold
  - the quorum of signers

- Implicit in existing threshold signature schemes that employ Shamir secret sharing (FROST).

Accountable Threshold Scheme (ATS)

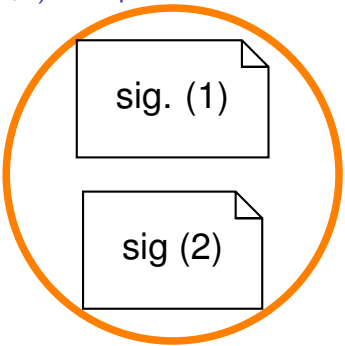
- Reveals the identity of each signer (and hence the threshold).
- Can be constructed from a multisignature scheme such as MuSig2.

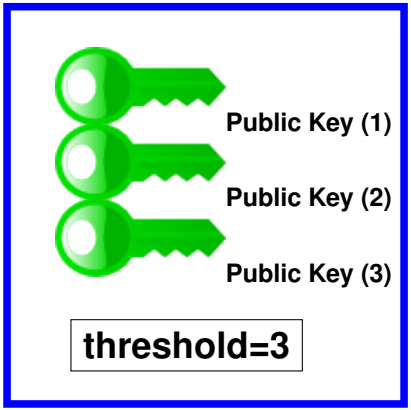
Accountable Threshold Scheme (ATS)

- Reveals the identity of each signer (and hence the threshold).
- Can be constructed from a multisignature scheme such as MuSig2.

Trivial ATS

(2, 3) Example





Verification: Perform one single-party verification for each signer.

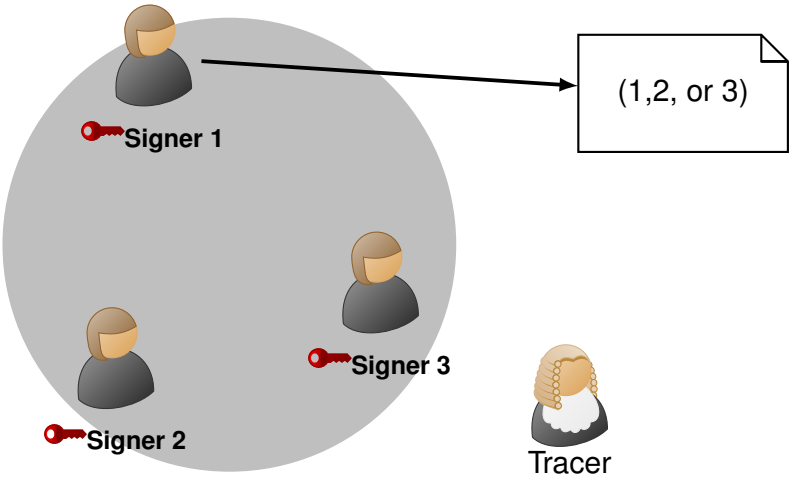
TAPS

- Achieves *both* privacy and accountability
- Applications include:
  - Financial institutions- to prove or disprove issuance of funds.
  - Identification of t misbehaving entities (i.e, TLS servers).

TAPS

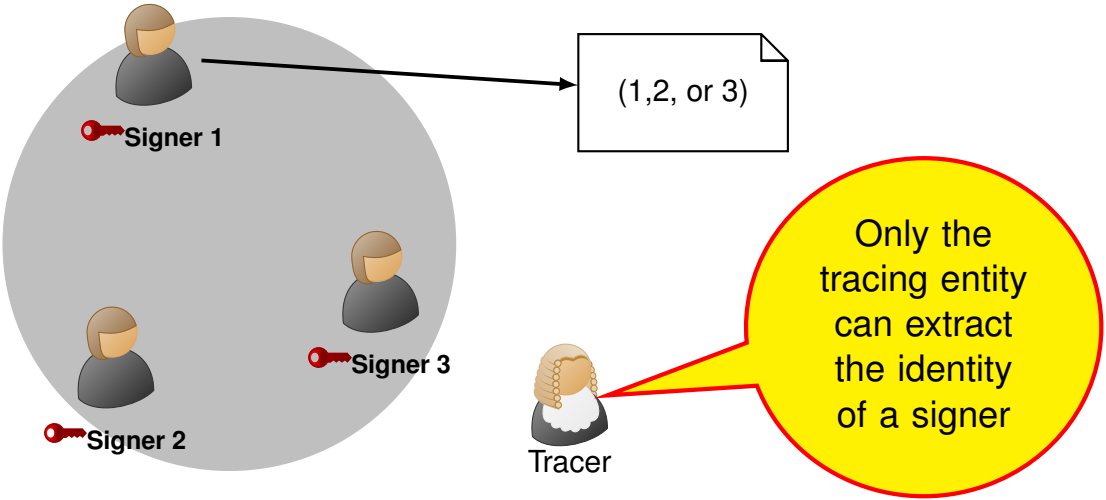
- Achieves *both* privacy and accountability
- Applications include:
  - Financial institutions- to prove or disprove issuance of funds.
  - Identification of t misbehaving entities (i.e, TLS servers).

Group Signatures

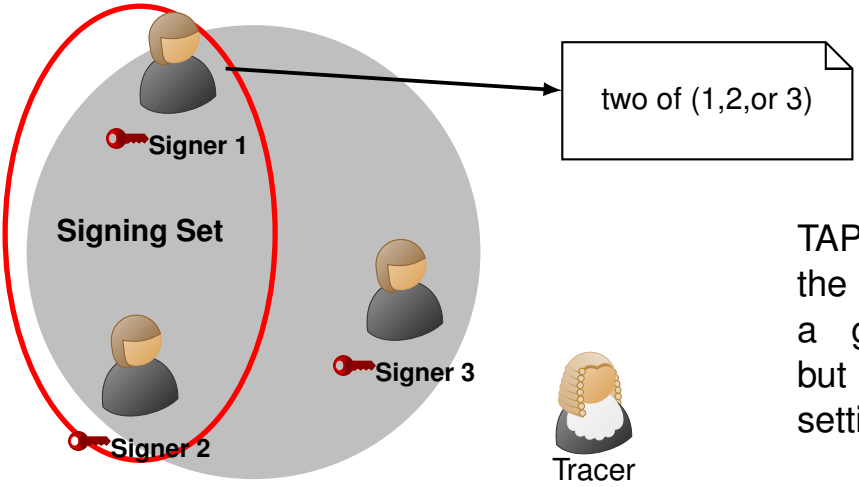


Group signatures prove that a member of a group signed, but not *which* member.

Group Signatures

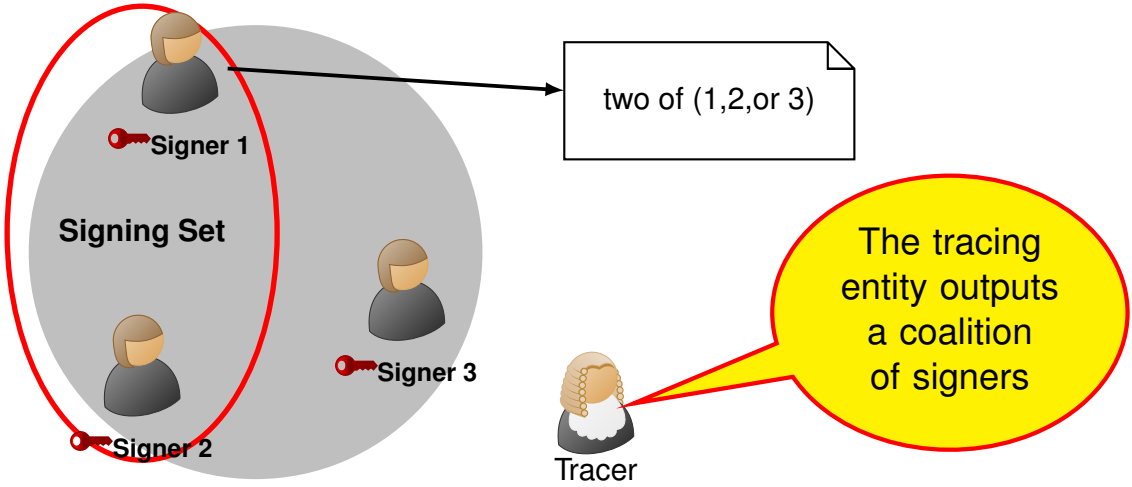


TAPS: Another Perspective



TAPS generalizes the same notion of a group signature, but to a threshold setting.

TAPS: Another Perspective



TAPS

Definition

A **private and accountable threshold signature** scheme, or **TAPS**, is a tuple of five polynomial time algorithms

$$\mathcal{S} = (\mathit{KeyGen}, \mathit{Sign}, \mathit{Combine}, \mathit{Verify}, \mathit{Trace})$$

TAPS

$$KeyGen(1^{\lambda}, n, t) \rightarrow \left(pk, (sk_1, \ldots, sk_n), sk_c, sk_t\right)$$

- pk: The group's public key
- $(sk_1, \ldots, sk_n)$: Secret keys for each of the n participants.
- sk_c: Secret key for the combiner
- sk_t: Secret key for the tracer

TAPS

$Sign(sk_i, m, C) \rightarrow \delta_i$

- m: Message to be signed
- C: Coalition of signers
- δ_i: Partial signature for participant i

$Combine(sk_c, m, C, \{\delta_i\}_{i \in C}) \rightarrow \sigma$

- Outputs σ, a TAPS signature

TAPS

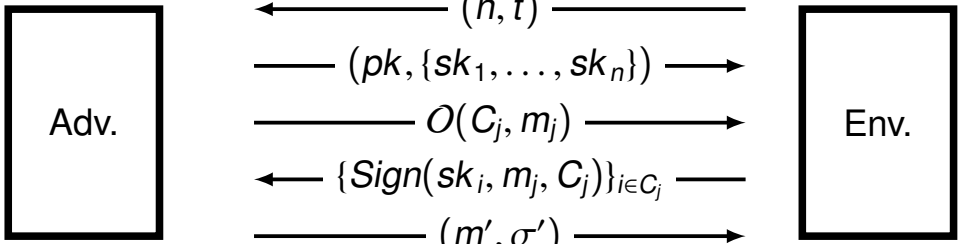
$\mathit{Verify}(pk, m, \sigma) \rightarrow 0/1$:

- Outputs a bit indicating if σ is valid for pk, m

$\mathit{Trace}(sk_t, m, \sigma) \rightarrow C/\text{fail}$:

- Outputs either the coalition of signers or fails.

Unforgeability and Accountability



Adv wins if:

(1) It produces a valid signature and controls fewer than t parties **(unforgeability)**

(2) It controls more than t parties, and outputs a valid signature that traces to an honest non-signer **(accountability)**

TAPS is *unforgable* and *accountable* if Pr[Adv wins] is negligible.

Privacy

- Privacy against the public
- Privacy against (non)-signers
- Privacy against other signers (which we don't consider)

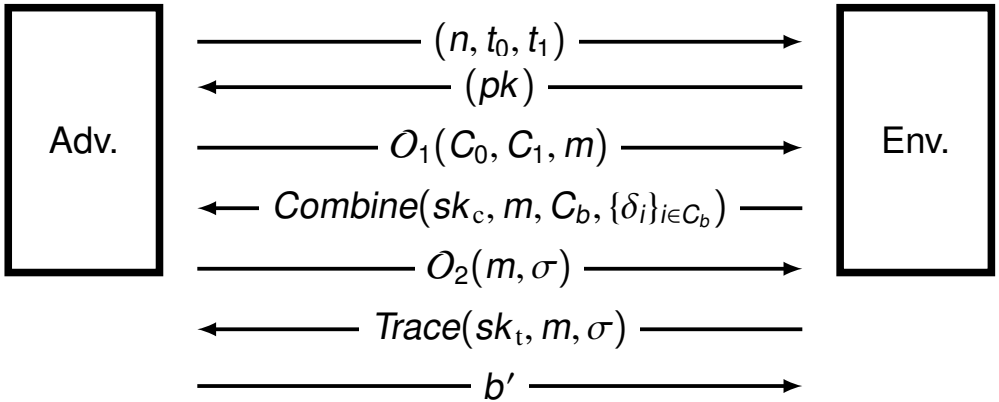
Privacy

- Privacy against the public
- Privacy against (non)-signers
- Privacy against other signers (which we don't consider)

Privacy

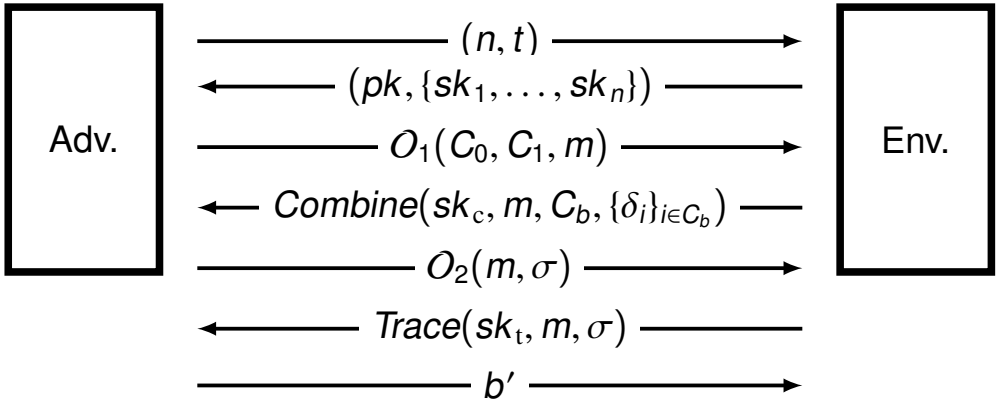
- Privacy against the public
- Privacy against (non)-signers
- Privacy against other signers (which we don't consider)

Privacy Against The Public



Restriction: Inputs to $\mathcal{O}_2$ cannot be outputs from $\mathcal{O}_1$.
Adv wins if it can can gain information about t or the set of signers.
TAPS is *private against the public* if Pr[Adv wins] is negligible.

Privacy Against Signers



Restriction: Inputs to O_2 cannot be outputs from O_1.
Adv. wins if it can gain information about the set of signers.
TAPS is *private against signers* if Pr[Adv wins] is negligible.

Generic TAPS

Instantiated with:

- An ATS
- A public-key encryption scheme
- A commitment scheme
- A signature scheme
- A non-interactive zero-knowledge argument of knowledge

Generic TAPS

Instantiated with:

- An ATS
- A public-key encryption scheme
- A commitment scheme
- A signature scheme
- A non-interactive zero-knowledge argument of knowledge

Generic TAPS

Instantiated with:

- An ATS
- A public-key encryption scheme
- A commitment scheme
- A signature scheme
- A non-interactive zero-knowledge argument of knowledge

Generic TAPS

Instantiated with:

- An ATS
- A public-key encryption scheme
- A commitment scheme
- A signature scheme
- A non-interactive zero-knowledge argument of knowledge

Generic TAPS

Instantiated with:

- An ATS
- A public-key encryption scheme
- A commitment scheme
- A signature scheme
- A non-interactive zero-knowledge argument of knowledge

Generic TAPS

Instantiated with:

- An ATS
- A public-key encryption scheme
- A commitment scheme
- A signature scheme
- A non-interactive zero-knowledge argument of knowledge

Schnorr TAPS

- Requires a Schnorr ATS, such as MuSig2
- Can be instantiated with either sigma proofs or bulletproofs as the zero-knowledge argument system.

Schnorr TAPS

- Requires a Schnorr ATS, such as MuSig2
- Can be instantiated with either sigma proofs or bulletproofs as the zero-knowledge argument system.

Performance

	Public Key Size		Signature Size	
	$\mathbb{G}$	$\mathbb{Z}_q$	$\mathbb{G}$	$\mathbb{Z}_q$
Sigma	$2n+4$	0	$n+4$	$2n+5$
Bulletproofs	$n+\frac{n}{e}+O(1)$	0	$\frac{n}{e}+O(\log n)$	4

- Bulletproofs TAPS is shorter by a factor of about e.

Performance

	Verify Time	Trace Time
Sigma	$O(n)$	$O(n)$
Bulletproofs	$O(n)$	$O(n \cdot 2^{e/2})$

- Measured in number of group operations.

Takeaways

- TAPS are a new type of threshold signature with both privacy and accountability.
- We define a generic construction that employs an ATS and other standard building blocks.
- We then define a Schnorr construction with both sigma and bulletproofs as the zero-knowledge argument system.

Thank You!

https://eprint.iacr.org/2022/TODO

Takeaways

- TAPS are a new type of threshold signature with both privacy and accountability.
- We define a generic construction that employs an ATS and other standard building blocks.
- We then define a Schnorr construction with both sigma and bulletproofs as the zero-knowledge argument system.

Thank You!

https://eprint.iacr.org/2022/TODO

Takeaways

- TAPS are a new type of threshold signature with both privacy and accountability.
- We define a generic construction that employs an ATS and other standard building blocks.
- We then define a Schnorr construction with both sigma and bulletproofs as the zero-knowledge argument system.

Thank You!

https://eprint.iacr.org/2022/TODO

Takeaways

- TAPS are a new type of threshold signature with both privacy and accountability.
- We define a generic construction that employs an ATS and other standard building blocks.
- We then define a Schnorr construction with both sigma and bulletproofs as the zero-knowledge argument system.

Thank You!

https://eprint.iacr.org/2022/TODO