

On the Adaptive Security of Threshold Schnorr Signatures: New Frontiers

Elizabeth Crites
Parity Technologies

Jan. 26, 2026 - NIST Workshop on Multi-Party Threshold Schemes

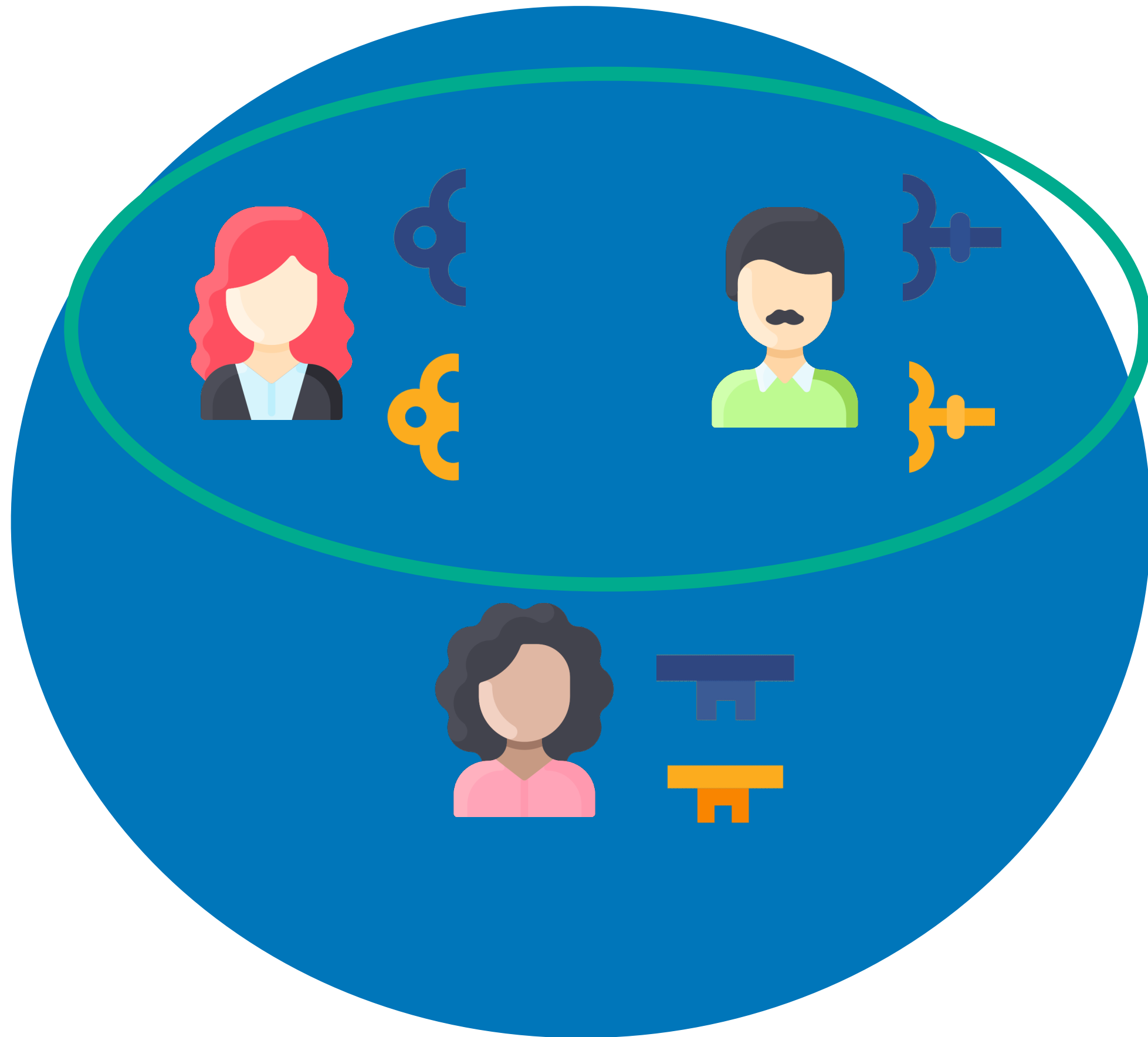
On the Adaptive Security of Key-Unique Threshold Signatures

Elizabeth Crites
Parity Technologies

Chelsea Komlo
University of Waterloo
NEAR One

Mary Maller
Inversed Tech

Key-Unique Threshold Signatures



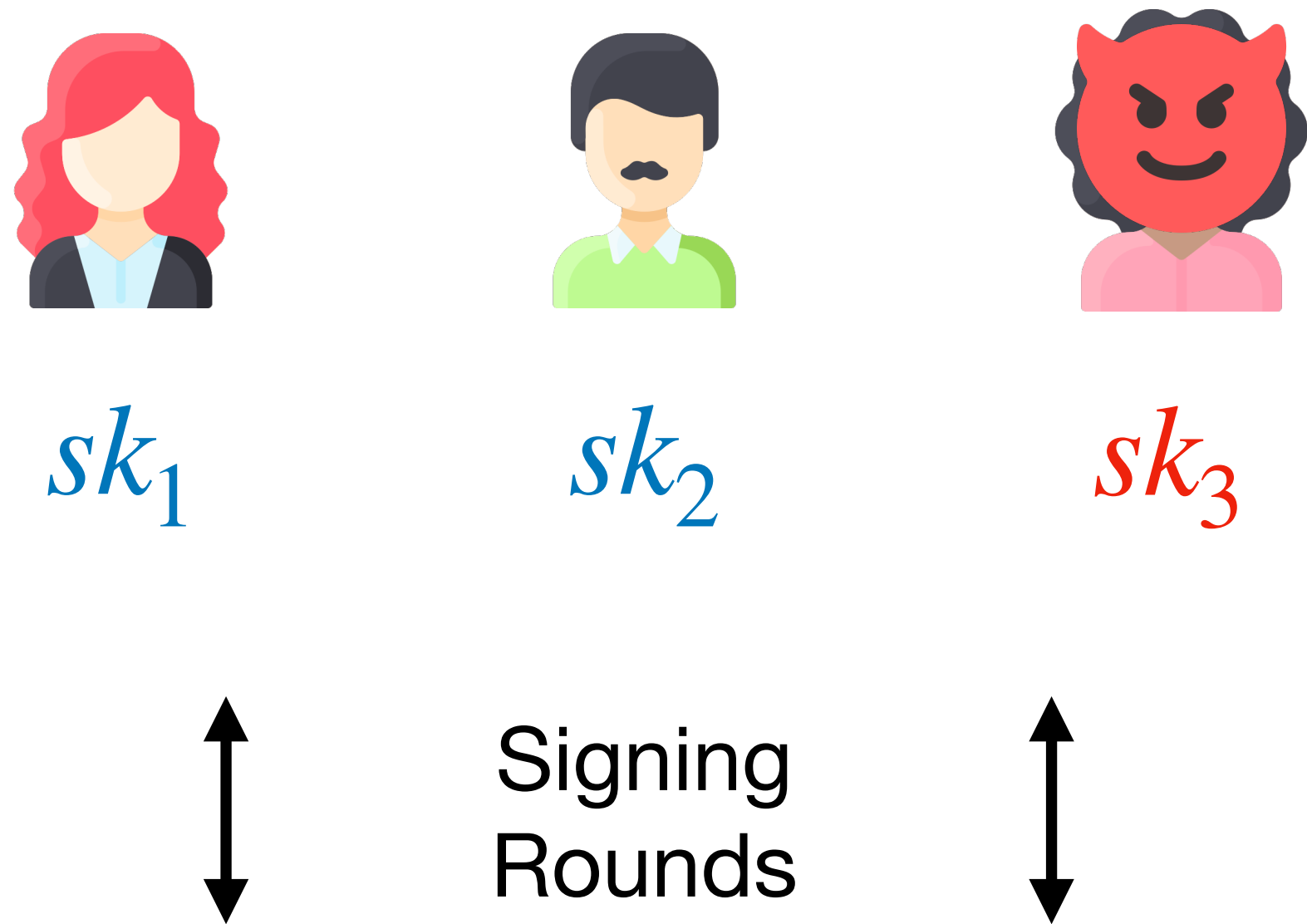
 public key PK

- key generation to produce PK and shares PK_1, PK_2, PK_3
- PK_i is perfectly binding commitment to sk_i of secret-shared sk
- example: g^{sk_i} non-example: $g^{sk_i}h^{r_i}$
- many schemes are key unique

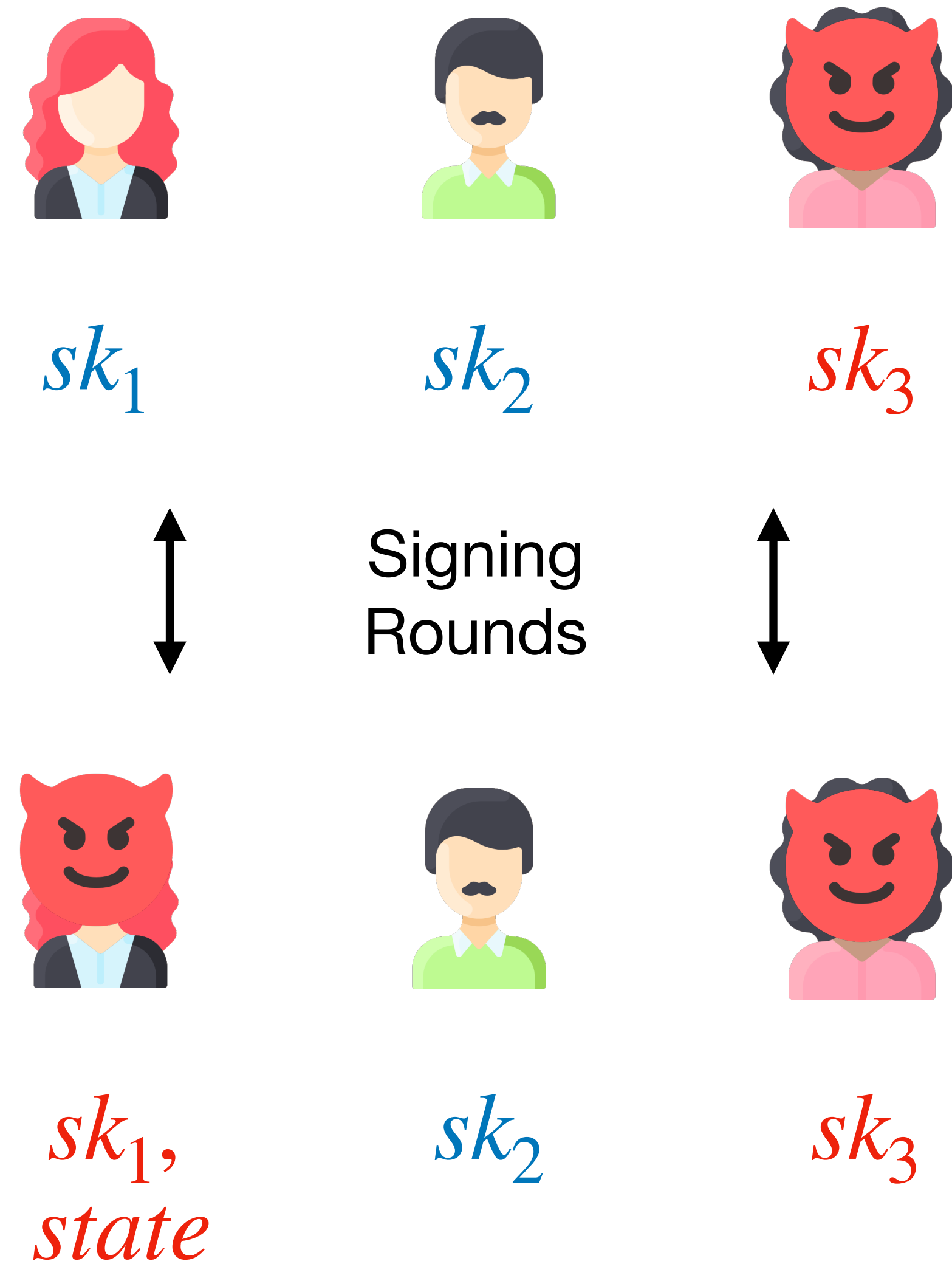
(2,3) example

Adaptive Security

Static Corruption



Adaptive Corruption



Adaptive Security

- NIST Call draft emphasizes a strong preference for schemes achieving provable adaptive security:

“Given the possibility of adaptive corruptions in the real world, it is important to consider for any proposed threshold signature scheme whether the major safety properties of interest (such as unforgeability) are safeguarded against such an adversary.”

- presumption: no adaptive security proof \neq security failure under adaptive adversary
- however, any such failure could have catastrophic consequences -> e.g., complete loss of funds in cryptocurrency wallets

Main Result #1

key-unique + NICA = adaptive security above $t/2$
not possible!

(for a broad class of security reductions)



Non-Interactive Computational Assumption

~all ROM

NICAs

Scheme	Static Security	Adaptive Security	Impossibility Results Apply
Threshold BLS (I) [19]	GDH	\times	1
Threshold BLS (I) [7]	-	OMDL+AGM (full)	1
Threshold BLS (III) [43]	co-CDH	co-CDH+DDH (full)	\times^*
Libert et al. [67]	-	SXDH [†]	\times^*
Threshold Waters [78]	-	CDH [†] (full)	\times^*
Threshold RSA [2]	RSA [†]	RSA [†] (full)	\times^*
HBTS-Mask [33]	-	DL (full)	\times^*
Threshold ECDSA [55]	Various [†]	\times	1
Threshold ECDSA [29]	Various	\times	1
Threshold BBS+ [45]	Various [†]	\times	1
Twinkle ₁ [9]	-	AOMCDH (full)	1
Twinkle ₂ [9]	-	DDH (full)	\times^*
Dazzle/-T [32]	-	DDH (full)	\times^*
FROST/2/3 [65, 41, 14, 75, 35, 38]	(A)OMDL	AOMDL+LDVR+AGM (full)	1,2
FROST-Mask [33]	-	AOMDL (t/2)	\times^*
ms-FROST [4]	-	AOMDL (full)	\times^*
FaFROST [11]	-	AOMDL+AGM (full)	\times^*
Sparkle+ [40]	DL	-	\times^*
[34]	CDL	AOMDL (t/2)	1,2
Lindell [68]	Schnorr, \mathcal{F}_{zk}	\times	1,2
Classic S. [70]	DL	\times	1,2
Zero S. [70]	DL	DL (full, erasures)	\times^*
Crackle & Snap [62]	-	DL (full)	\times^*
Glacius [6]	-	DDH (full)	\times^*
Gargos [5]	-	DDH (full)	\times^*
GCRS [57]	-	DDH (full)	\times^*
Abe-Fehr [1]	-	Schnorr+DDH (full)	\times^*
Stinson-Strobl [77]	Schnorr	\times	1,2
ROAST [75]	OMDL	\times	1,2
SPRINT [17]	DL	\times	1,2
HARTS [8]	-	-	1,2
GKMN [54]	n-party Schnorr,	\times	1,2
	$\mathcal{F}_{com,zk}^{RDL}$		
Arctic [64]	DL	\times	1,2

\times^* = not key unique

impossible in ROM and AGM

Schnorr schemes

Main Result #2

interactive

key-unique Schnorr + (A)OMDL = adaptive
security above $t/2$ with rewinding
not possible!

~all ROM

(A)OMDL

Scheme	Static Security	Adaptive Security	Impossibility Results Apply
Threshold BLS (I) [19]	GDH	\times	1
Threshold BLS (I) [7]	-	OMDL+AGM (full)	1
Threshold BLS (III) [43]	co-CDH	co-CDH+DDH (full)	\times^*
Libert et al. [67]	-	SXDH [†]	\times^*
Threshold Waters [78]	-	CDH [†] (full)	\times^*
Threshold RSA [2]	RSA [†]	RSA [†] (full)	\times^*
HBTS-Mask [33]	-	DL (full)	\times^*
Threshold ECDSA [55]	Various [†]	\times	1
Threshold ECDSA [29]	Various	\times	1
Threshold BBS+ [45]	Various [†]	\times	1
Twinkle ₁ [9]	-	AOMCDH (full)	1
Twinkle ₂ [9]	-	DDH (full)	\times^*
Dazzle/-T [32]	-	DDH (full)	\times^*
FROST/2/3 [65, 41, 14, 75, 35, 38]	(A)OMDL	AOMDL+LDVR+AGM (full)	1,2
FROST-Mask [33]	-	AOMDL ($t/2$)	\times^*
ms-FROST [4]	-	AOMDL (full)	\times^*
FaFROST [11]	-	AOMDL+AGM (full)	\times^*
Sparkle+ [40]	DL	-	\times^*
[34]	CDL	AOMDL ($t/2$)	1,2
Lindell [68]	Schnorr, \mathcal{F}_{zk}	\times	1,2
Classic S. [70]	DL	\times	1,2
Zero S. [70]	DL	DL (full, erasures)	\times^*
Crackle & Snap [62]	-	DL (full)	\times^*
Glacius [6]	-	DDH (full)	\times^*
Gargos [5]	-	DDH (full)	\times^*
GCRS [57]	-	DDH (full)	\times^*
Abe-Fehr [1]	-	Schnorr+DDH (full)	\times^*
Stinson-Strobl [77]	Schnorr	\times	1,2
ROAST [75]	OMDL	\times	1,2
SPRINT [17]	DL	\times	1,2
HARTS [8]	-	-	1,2
GKMN [54]	n -party Schnorr,	\times	1,2
	$\mathcal{F}_{com-zk}^{RDL}$		
Arctic [64]	DL	\times	1,2

Schnorr schemes

(A)OMDL common
rewinding common

Ways to Bypass Impossibilities?

- decisional assumptions, like DDH, where public keys are typically variants of

$$PK_i = g^{sk_i} h^{r_i}$$

- typically cannot identify malicious party from their partial signatures (identifiable abort) without extra zero-knowledge proofs

~all ROM

DDH

Scheme	Static Security	Adaptive Security	Impossibility Results Apply
Threshold BLS (I) [19]	GDH	\times	1
Threshold BLS (I) [7]	-	OMDL+AGM (full)	1
Threshold BLS (III) [43]	co-CDH	co-CDH+DDH (full)	\times^*
Libert et al. [67]	-	SXDH[†]	\times^*
Threshold Waters [78]	-	CDH [†] (full)	\times^*
Threshold RSA [2]	RSA [†]	RSA [†] (full)	\times^*
HBTS-Mask [33]	-	DL (full)	\times^*
Threshold ECDSA [55]	Various [†]	\times	1
Threshold ECDSA [29]	Various	\times	1
Threshold BBS+ [45]	Various [†]	\times	1
Twinkle ₁ [9]	-	AOMCDH (full)	1
Twinkle ₂ [9]	-	DDH (full)	\times^*
Dazzle/-T [32]	-	DDH (full)	\times^*
FROST/2/3 [65, 41, 14, 75, 35, 38]	(A)OMDL	AOMDL+LDVR+AGM (full)	1,2
FROST-Mask [33]	-	AOMDL (full)	\times^*
ms-FROST [4]	-	AOMDL+AGM (full)	\times^*
FaFROST [11]	-	-	\times^*
Sparkle+ [40]	DL	AOMDL (t/2)	1,2
[34]	CDL	\times	1,2
Lindell [68]	Schnorr, \mathcal{F}_{zk}	\times	1,2
Classic S. [70]	DL	\times	1,2
Zero S. [70]	DL	DL (full, erasures)	\times^*
Crackle & Snap [62]	-	DL (full)	\times^*
Glacius [6]	-	DDH (full)	\times^*
Gargos [5]	-	DDH (full)	\times^*
GCRS [57]	-	DDH (full)	\times^*
Abe-Fehr [1]	-	Schnorr+DDH (full)	\times^*
Stinson-Strobl [77]	Schnorr	\times	1,2
ROAST [75]	OMDL	\times	1,2
SPRINT [17]	DL	\times	1,2
HARTS [8]	-	-	1,2
GKMN [54]	n -party Schnorr, $\mathcal{F}_{com-zk}^{RDL}$	\times	1,2
Arctic [64]	DL	\times	1,2

\times^* = not key unique

Schnorr schemes

Ways to Bypass Impossibilities?

- decisional assumptions, like DDH, where public keys are typically variants of $PK_i = g^{sk_i}h^{r_i}$
 - typically cannot identify malicious party from their partial signatures (identifiable abort) without extra zero-knowledge proofs
- require secrecy of the public key shares PK_1, \dots, PK_n
 - can be leaked through partial signing, so need masking

~all ROM

Hiding PK's

Scheme	Static Security	Adaptive Security	Impossibility Results Apply
Threshold BLS (I) [19]	GDH	\times	1
Threshold BLS (I) [7]	-	OMDL+AGM (full)	1
Threshold BLS (III) [43]	co-CDH	co-CDH+DDH (full)	\times^*
Libert et al. [67]	-	SXDH [†]	\times^*
Threshold Waters [78]	-	CDH [†] (full)	\times^*
Threshold RSA [2]	RSA [†]	RSA [†] (full)	\times^*
HBTS-Mask [33]	-	DL (full)	\times^*
Threshold ECDSA [55]	Various [†]	\times	1
Threshold ECDSA [29]	Various	\times	1
Threshold BBS+ [45]	Various [†]	\times	1
Twinkle ₁ [9]	-	AOMCDH (full)	1
Twinkle ₂ [9]	-	DDH (full)	\times^*
Dazzle/-T [32]	-	DDH (full)	\times^*
FROST/2/3 [65, 41, 14, 75, 35, 38]	(A)OMDL	AOMDL+LDVR+AGM (full)	1,2
FROST-Mask [33]	-	AOMDL (full)	\times^*
ms-FROST [4]	-	AOMDL+AGM (full)	\times^*
FaFROST [11]	-	-	\times^*
Sparkle+ [40]	DL	AOMDL (t/2)	1,2
[34]	CDL	\times	1,2
Lindell [68]	Schnorr, \mathcal{F}_{zk}	\times	1,2
Classic S. [70]	DL	\times	1,2
Zero S. [70]	DL	DL (full, erasures)	\times^*
Crackle & Snap [62]	-	DL (full)	\times^*
Glacius [6]	-	DDH (full)	\times^*
Gargos [5]	-	DDH (full)	\times^*
GCRS [57]	-	DDH (full)	\times^*
Abe-Fehr [1]	-	Schnorr+DDH (full)	\times^*
Stinson-Strobl [77]	Schnorr	\times	1,2
ROAST [75]	OMDL	\times	1,2
SPRINT [17]	DL	\times	1,2
HARTS [8]	-	-	1,2
GKMN [54]	n -party Schnorr,	\times	1,2
	$\mathcal{F}_{com-zk}^{RDL}$		
Arctic [64]	DL	\times	1,2

Schnorr schemes

public keys cannot be revealed

A Plausible Attack on the Adaptive Security of Threshold Schnorr Signatures

Elizabeth Crites & Alistair Stewart
Parity Technologies

Paper #2: eprint 2025/1001

The Problem P

- we define a search problem P and show a concrete, efficient attack if P is easy to solve

Definition 2. P is the following search problem. Given $\mathbf{w} \in \mathbb{Z}_p^{t+1}$ and $\mathbf{v}_1, \dots, \mathbf{v}_n \in \mathbb{Z}_p^{t+1}$, find a set $CS \subset \{1, \dots, n\}$ with $|CS| = t_c$ such that $\mathbf{w} \in \text{span}(\{\mathbf{v}_i\}_{i \in CS})$ if one exists.

- in the context of threshold signatures, n = number of parties, $t + 1$ = threshold, t_c = number of corrupted parties (up to $t_c = t$)
- P does not rely on group elements or operations (field elements only) and is not stated in terms of a random oracle

Plausible Attack Conditions

Plausible attack applies to any scheme with the following 3 properties:

1. Public key shares PK_1, \dots, PK_n are public
2. Secret keys sk_1, \dots, sk_n lie on a degree- t polynomial with coefficients in \mathbb{Z}_p
 - e.g., Shamir secret sharing & other DL-based key generation protocols
 - key-unique!
3. Final signature is compatible with Schnorr verification: $g^z = R \cdot PK^c$

Scheme	Attack		
	Static Security	Adaptive Security	Impossibility Results Apply
FROST/2/3 [65, 41, 14, 75, 35, 38]	(A)OMDL	AOMDL+LDVR+AGM (full)	1,2
FROST-Mask [33]	-	AOMDL ($t/2$)	\mathbf{x}^*
ms-FROST [4]	-	AOMDL (full)	\mathbf{x}^*
FaFROST [11]	-	AOMDL+AGM (full)	\mathbf{x}^*
Sparkle+ [40]	DL	-	\mathbf{x}^*
Lindell [68]	Schnorr, \mathcal{F}_{zk}	AOMDL ($t/2$)	1,2
Classic S. [70]	DL	\mathbf{x}	1,2
Zero S. [70]	DL	\mathbf{x}	1,2
Crackle & Snap [62]	-	DL (full, erasures)	\mathbf{x}^*
Glacius [6]	-	DL (full)	\mathbf{x}^*
Gargos [5]	-	DDH (full)	\mathbf{x}^*
GCRS [57]	-	DDH (full)	\mathbf{x}^*
Abe-Fehr [1]	-	DDH (full)	\mathbf{x}^*
Stinson-Strobl [77]	-	Schnorr+DDH (full)	\mathbf{x}^*
ROAST [75]	Schnorr	\mathbf{x}	1,2
SPRINT [17]	OMDL	\mathbf{x}	1,2
HARTS [8]	DL	\mathbf{x}	1,2
GKMN [54]	-	-	1,2
Arctic [64]	n -party Schnorr, $\mathcal{F}_{\text{com-zk}}^{R_{\text{DL}}}$ DL	\mathbf{x}	1,2

The Plausible Attack

- attack where the forgery is simply a linear combination of PK and public key shares PK_1, \dots, PK_n
- uniquely, our attack allows a forgery using *public key shares alone* - no partial signatures are required
 - key-only attack is what's used in key-unique paper too
- attack works *even for a single signing session*

The Plausible Attack

- adversary sets $R^* = PK^{\alpha_0} PK_1^{\alpha_1} \dots PK_n^{\alpha_n}$ for random $\alpha_0, \alpha_1, \dots, \alpha_n \in \mathbb{Z}_p$
- valid Schnorr forgery (R^*, z^*) on message m^* satisfies:

$$g^{z^*} = R^* \cdot PK^{c^*} = PK^{c^* + \alpha_0} PK_1^{\alpha_1} \dots PK_n^{\alpha_n}, \text{ where } c^* = H(PK, m^*, R^*)$$

$$z^* = \sum_{j \in CS} \beta_j s k_j$$

Definition 2. P is the following search problem. Given $\mathbf{w} \in \mathbb{Z}_p^{t+1}$ and $\mathbf{v}_1, \dots, \mathbf{v}_n \in \mathbb{Z}_p^{t+1}$, find a set $CS \subset \{1, \dots, n\}$ with $|CS| = t_c$ such that $\mathbf{w} \in \text{span}(\{\mathbf{v}_i\}_{i \in CS})$ if one exists.

- adversary gets set CS from problem P , can corrupt PK_j for $j \in CS$, and forge
- what is the probability an adversary could do this?

Plausible Attack Success

$(n, t + 1)$	$t_c = t$	$t_c = t - 1$	$t_c = t - 2$	$t_c = t - 3$
(64,43)	195.84	446.97	698.2	949.52
(128,86)	137.87	388.92	640.02	891.17
(196,131)	75.41	326.45	577.53	828.64
(512,342)	0.0	37.25	288.28	539.32
(768,513)	0.0	0.0	53.8	304.82
(1024,683)	0.0	0.0	0.0	69.29

Table 2. The probability that our attack succeeds is 2^{-x} for x given in the table, with $p \approx 2^{252}$, where x is computed as in Theorem 2. Here, n is the total number of potential signers, $t + 1$ is the threshold, and t_c is the corruption threshold.

Insecure if P is easy

Main Result #1

If P is easy to solve, all schemes meeting Conditions 1-3 are statically secure but not adaptively secure near t corruptions

Would be first such separation for any natural protocol, solving a long-standing open problem in MPC

Moreover, would apply to a large class of schemes and would hold even in the strongest idealized models: the AGM and the GGM

Main Result #2

Regardless, the full adaptive security (and slightly below) of these schemes cannot be proven without an assumption that implies the hardness of some instances of P

Call to Action



- attack is “plausible” because problem P is currently not known to be easy
- in fact, we show equivalence of P to a coding theory problem
 - well-studied problem
 - many results showing NP-hardness, but not quite for the parameters used in Schnorr signatures

On the Adaptive Security of FROST

Elizabeth Crites
Parity Technologies

Jonathan Katz
Google

Chelsea Komlo
University of Waterloo
NEAR One

Stefano Tessaro
University of Washington

Chenzhi Zhu
University of Washington

Main Result #1

FROST/2/3 + AOMDL + ROM
= $t/2$ adaptive security

(same assumptions/proof strategy as for FROST static security)

Main Result #2

new assumption 

FROST/2/3 + ROM + AGM + AOMDL + LDVR
= t (i.e., full) adaptive security

The LDVR Problem

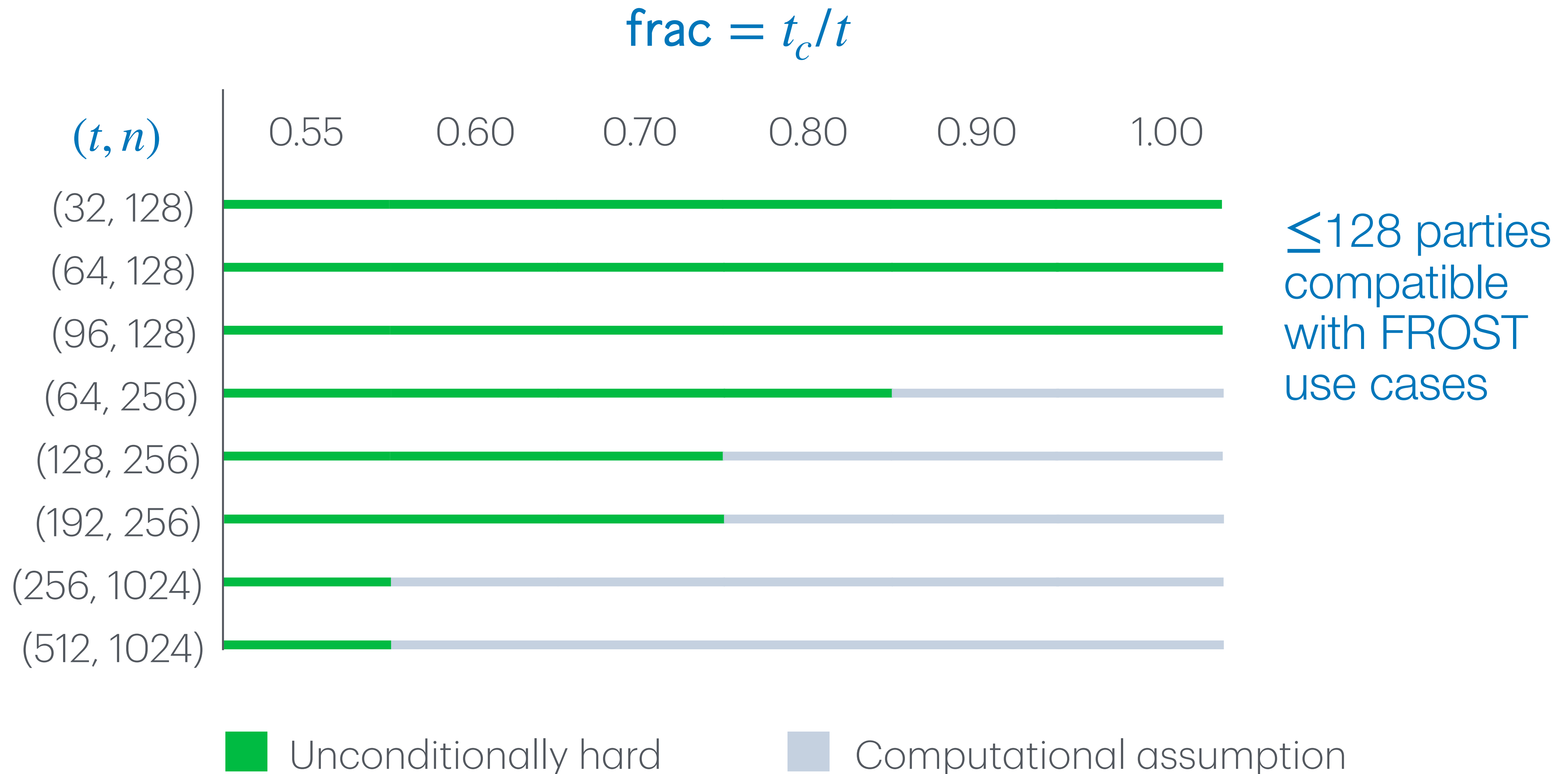
Definition 2. P is the following search problem. Given $w \in \mathbb{Z}_p^{t+1}$ and $v_1, \dots, v_n \in \mathbb{Z}_p^{t+1}$, find a set $CS \subset \{1, \dots, n\}$ with $|CS| = t_c$ such that $w \in \text{span}(\{v_i\}_{i \in CS})$ if one exists.

MAIN Expt $_{\mathcal{A}}^{(t_c, t, n)\text{-ldvr}}(\kappa)$	$\mathcal{O}(\alpha)$
ctr := 0	// $\alpha \in \mathbb{Z}_p^{n+1}$
$(p, st) \leftarrow_{\$} \mathcal{A}(\kappa)$	ctr := ctr + 1
// $2^\kappa < p < 2^{\kappa+1}$, p prime	$\alpha_{\text{ctr}} := \alpha$
for $j \in \{0, \dots, n\}$ do	$c_{\text{ctr}} \leftarrow_{\$} \mathbb{Z}_p$
$v_j := (1, j, \dots, j^t) \in \mathbb{Z}_p^{t+1}$	return c_{ctr}
$(CS, i^*) \leftarrow_{\$} \mathcal{A}^{\mathcal{O}}(st)$	
// $CS \subseteq \{1, \dots, n\}, CS \leq t_c, i^* \in [ctr]$	
$w := c_{i^*} v_0 + \sum_{j=0}^n \alpha_{i^*}[j] \cdot v_j \longrightarrow$ recall from attack	
if $w \in \text{span}(\{v_i\}_{i \in CS})$	
return 1	
return 0	

random oracle queries:
 $c_i = H(PK, m_i, R_i)$

Fig. 6. The LDVR experiment with parameters $t_c \leq t < n$.

Unconditional Hardness of LDVR



Call to Action

- Hardness of P (NP-hardness of classical coding theory problem)
- LDVR is unconditionally hard for many parameters
- other schemes may be proven under variants of these assumptions
- new frontiers!

Thank you!