Twinkle: Threshold Signatures from DDH with Full Adaptive Security





Renas Bacho

Julian Loss

Stefano Tessaro

Benedikt Wagner

Chenzhi Zhu

erc

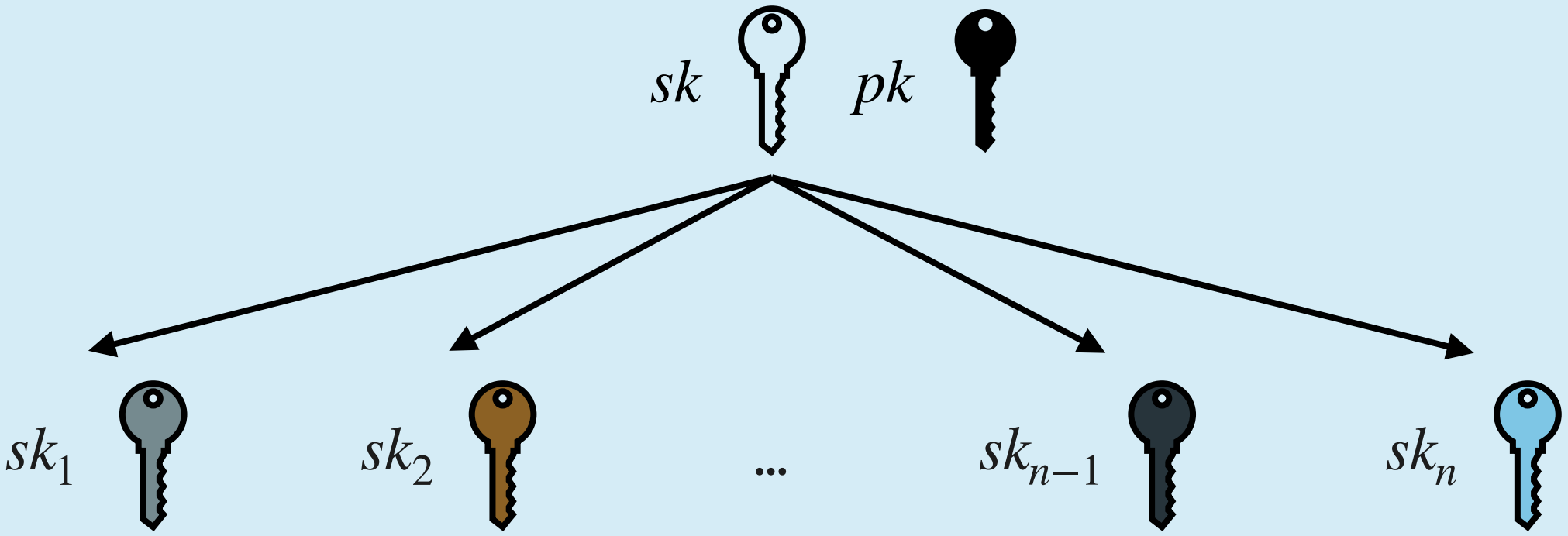
CISPA HELMHOLTZ CENTER FOR INFORMATION SECURITY

PAUL G. ALLEN SCHOOL OF COMPUTER SCIENCE & ENGINEERING

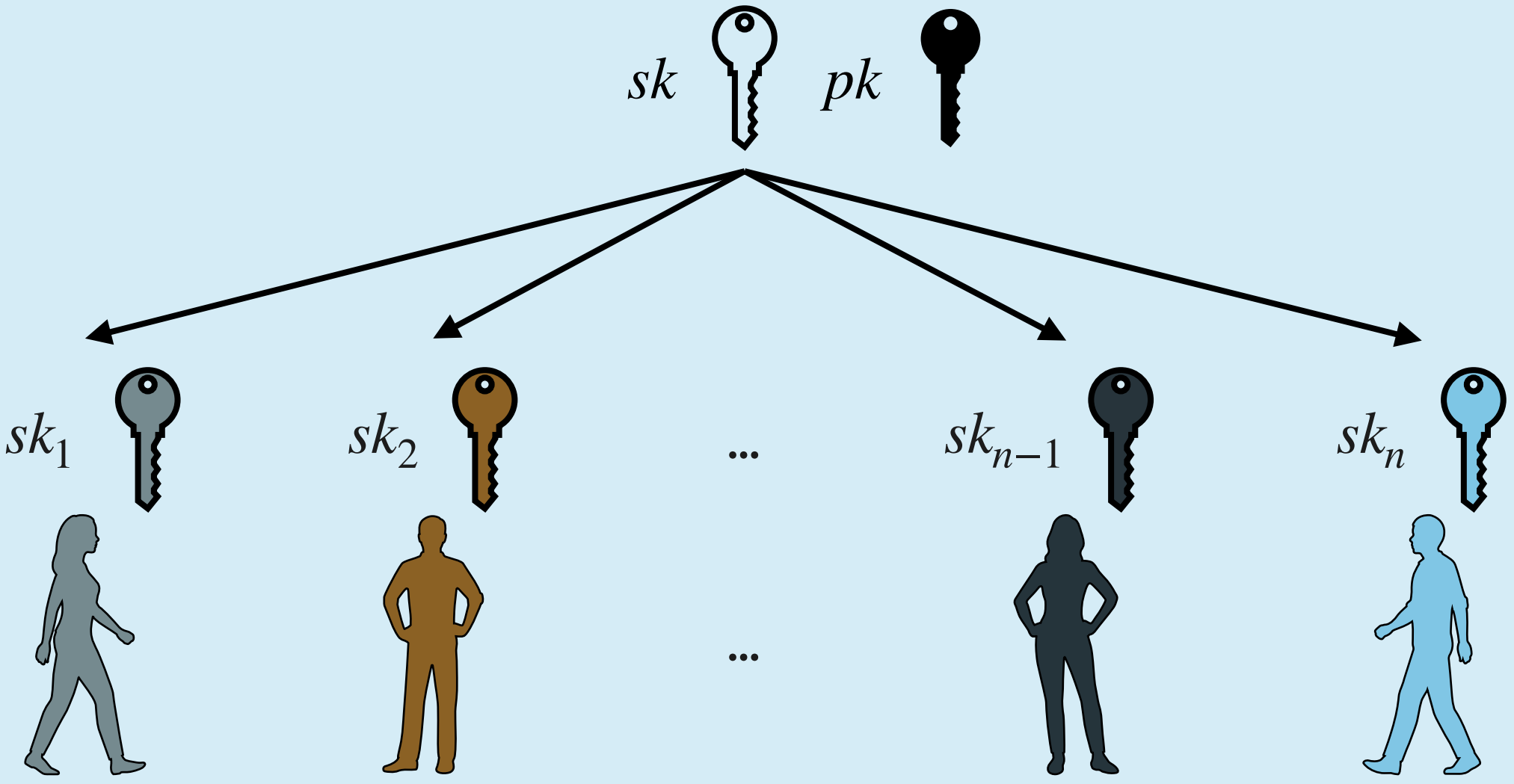
Threshold Signatures

Threshold Signatures

Threshold Signatures



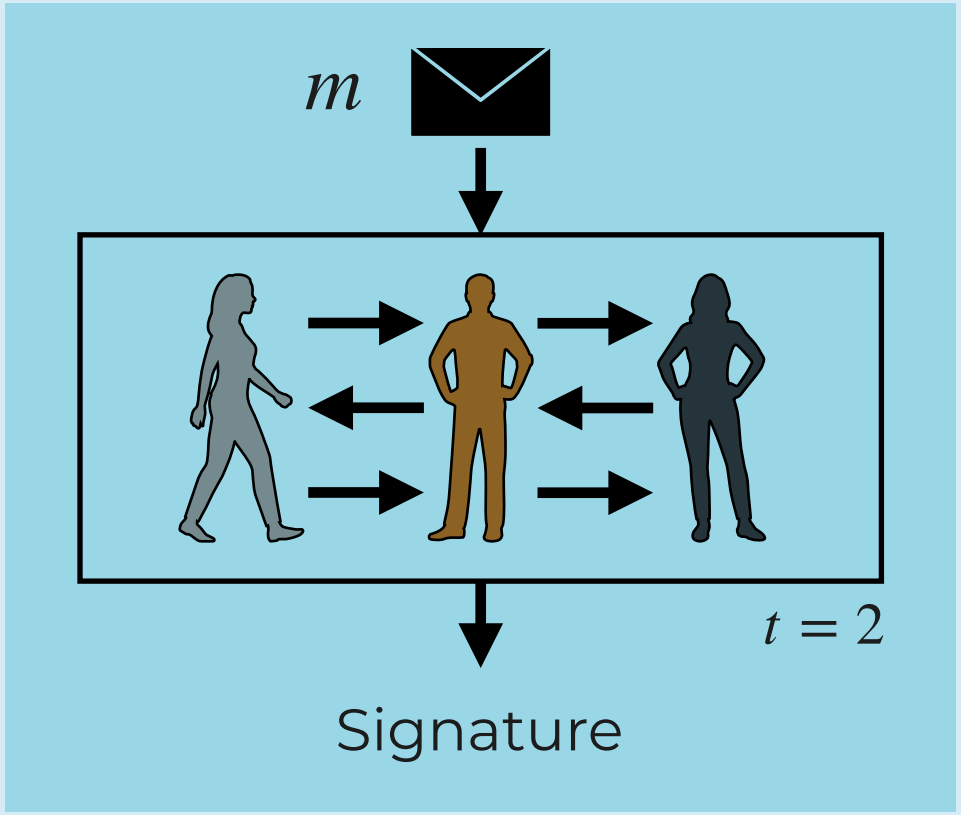
Threshold Signatures



n Signers

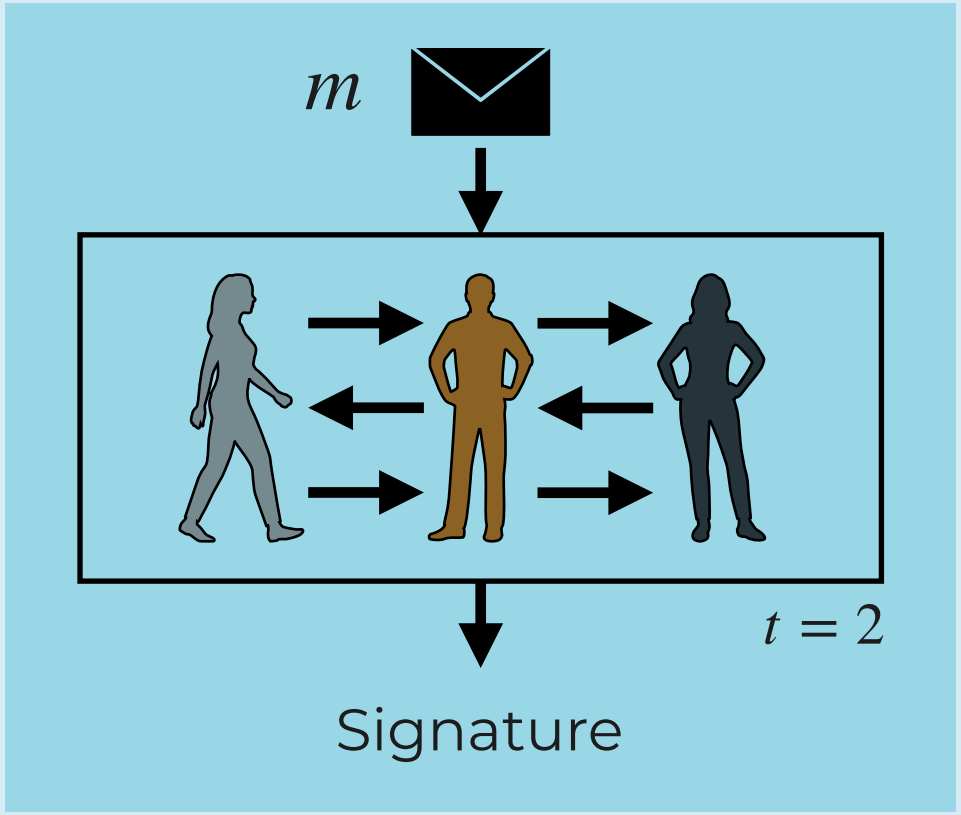
Threshold Signatures with Threshold $t < n$

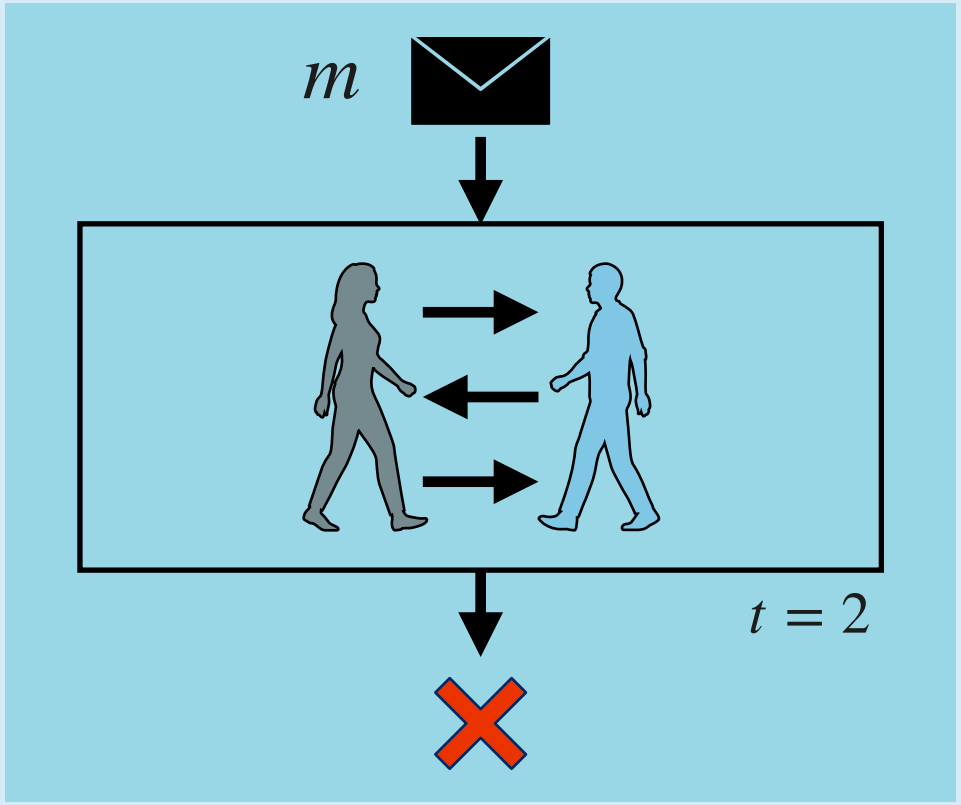
Threshold Signatures with Threshold $t < n$



$> t$ Signers can sign

Threshold Signatures with Threshold $t < n$





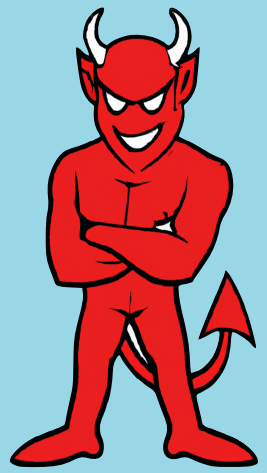
$> t$ Signers can sign

$\leq t$ Signers can not sign

Security of Threshold Signatures

Security of Threshold Signatures

Static Security

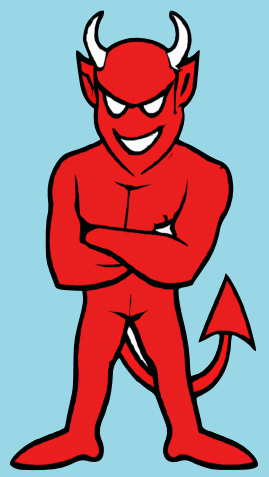


Security of Threshold Signatures

Static Security

Corruptions

$C \subset [n], \quad |C| \leq t$



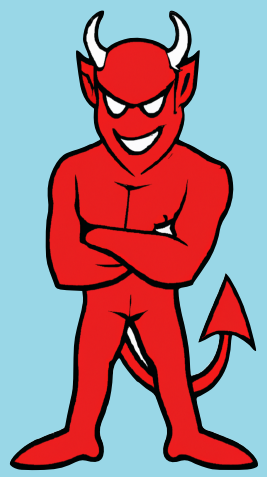
Security of Threshold Signatures

Static Security

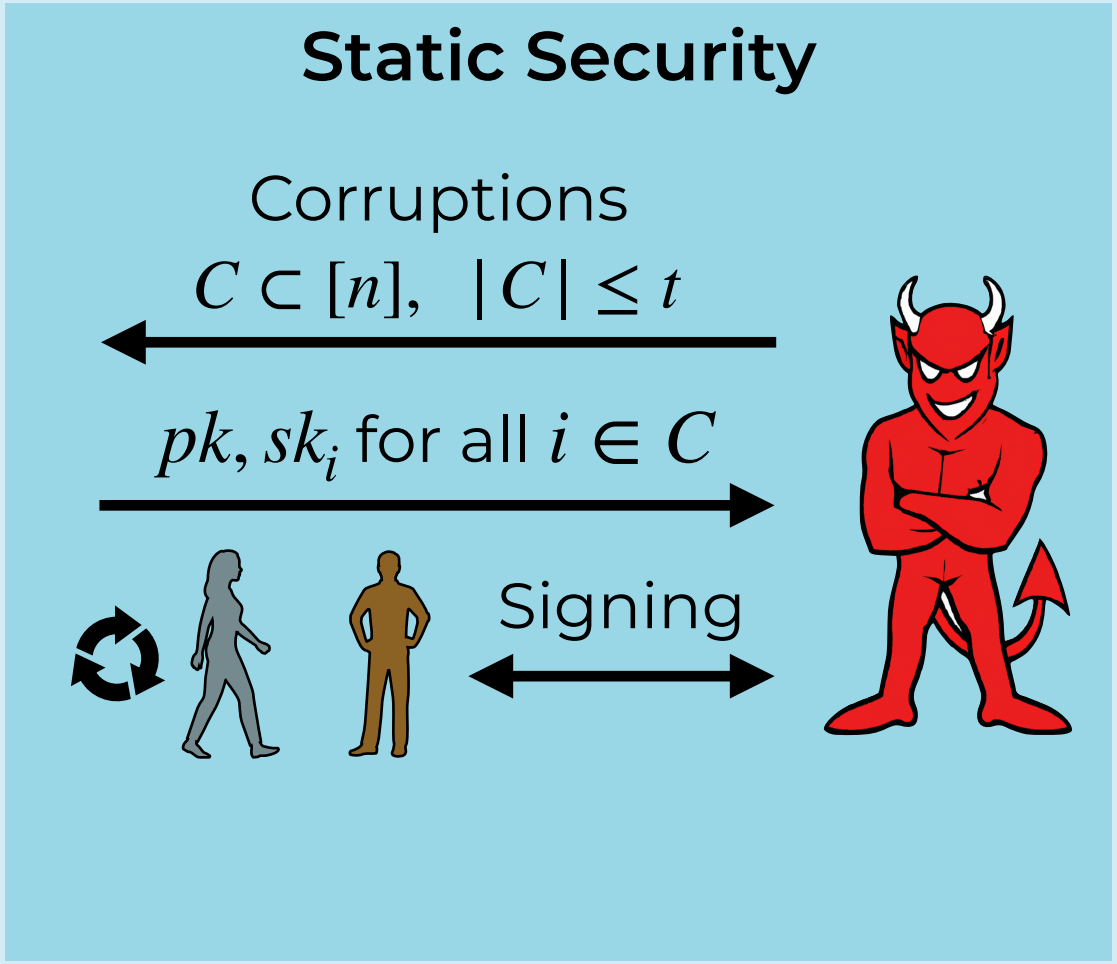
Corruptions

$C \subset [n], \quad |C| \leq t$

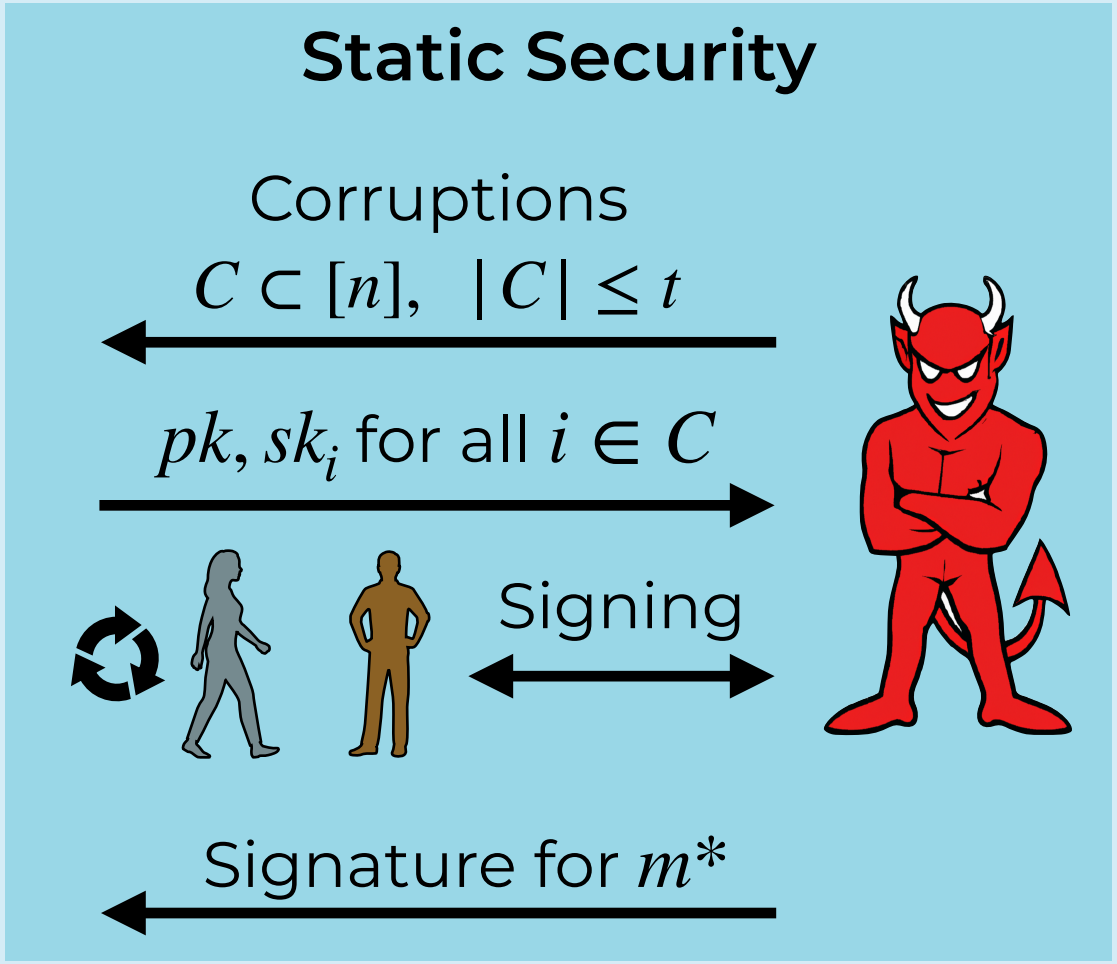
pk, sk_i for all $i \in C$



Security of Threshold Signatures



Security of Threshold Signatures



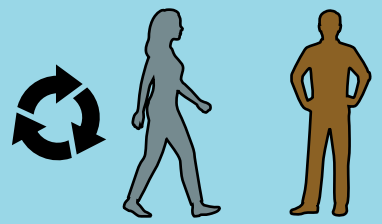
Security of Threshold Signatures

Static Security

Corruptions

$C \subset [n], \quad |C| \leq t$

pk, sk_i for all $i \in C$



Signing

Signature for m^*

Adaptive Security

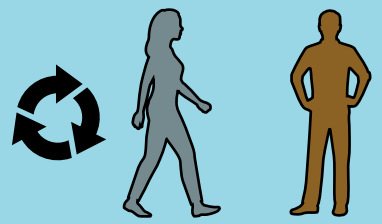
Security of Threshold Signatures

Static Security

Corruptions

$C \subset [n], \quad |C| \leq t$

pk, sk_i for all $i \in C$



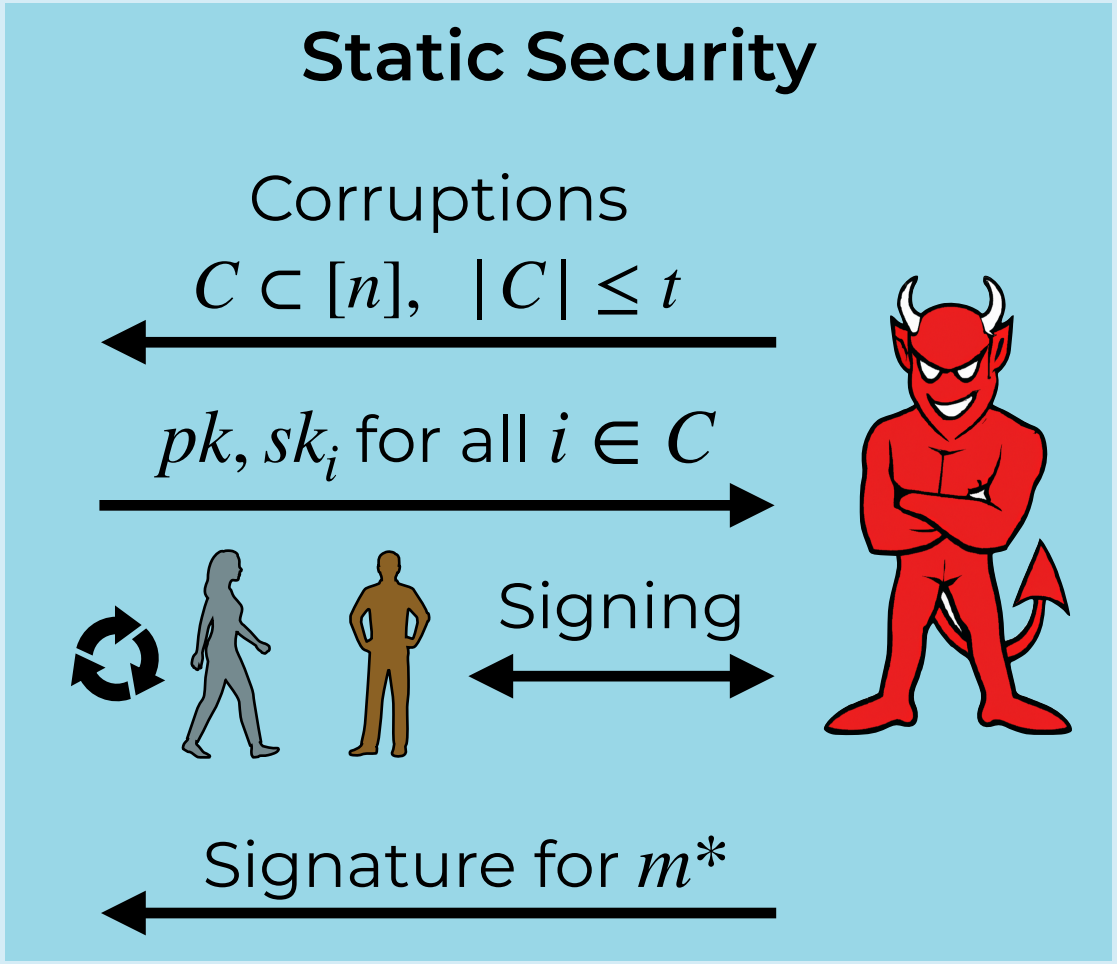
Signing

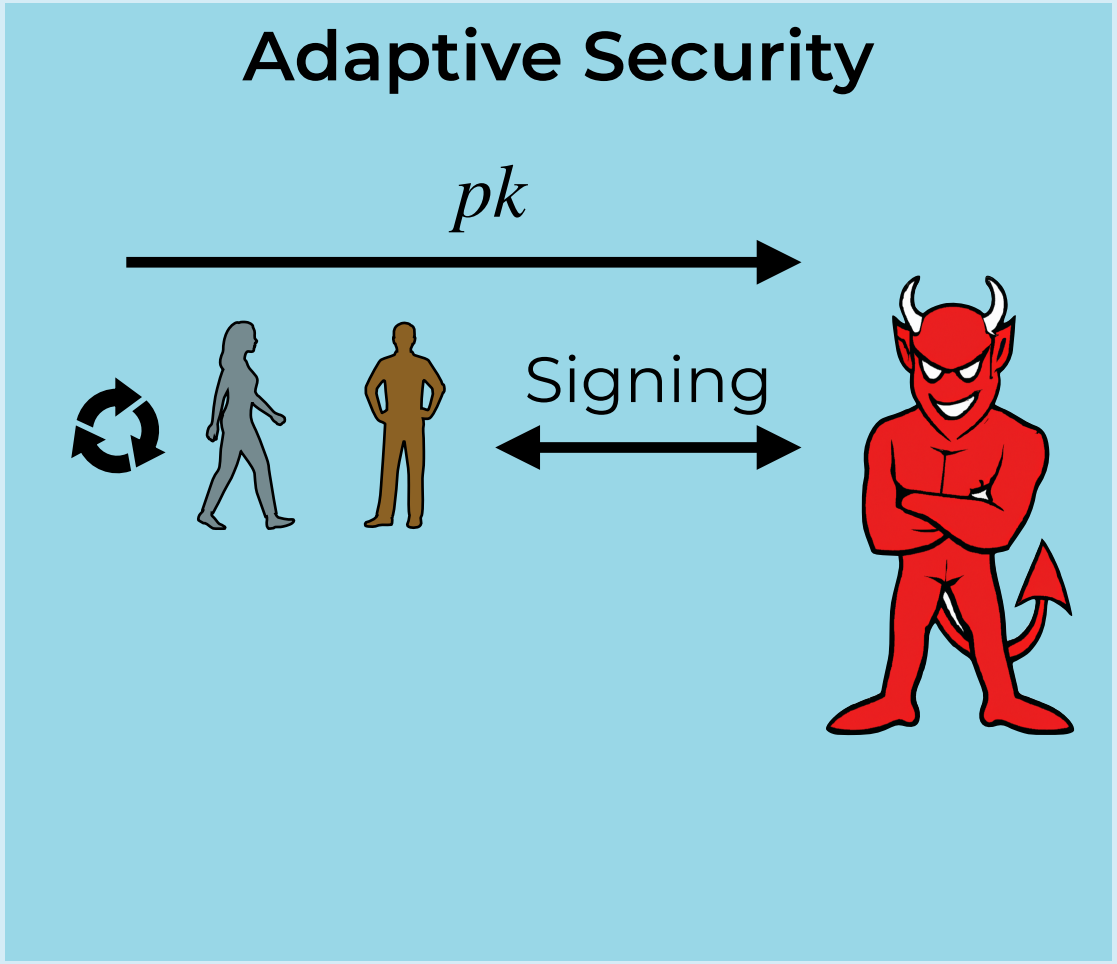
Signature for m^*

Adaptive Security

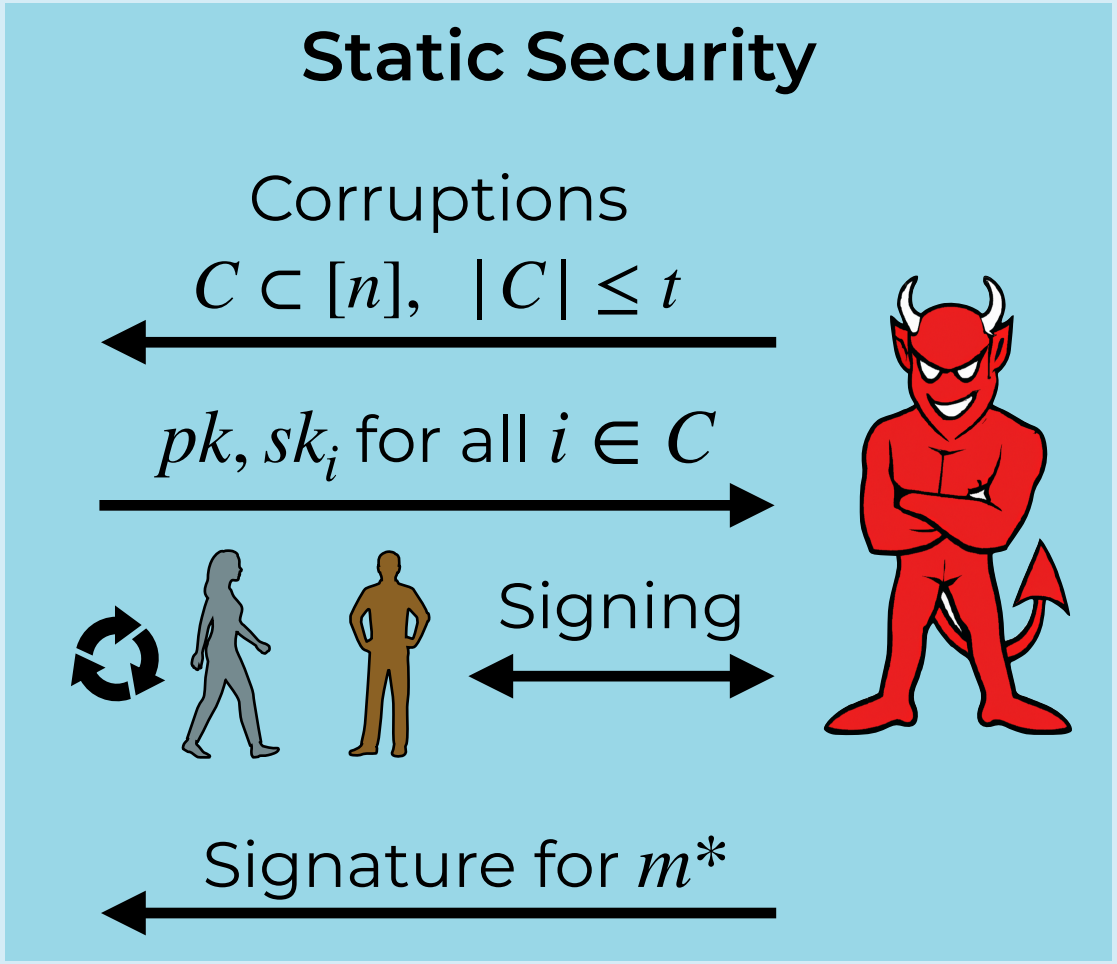
pk

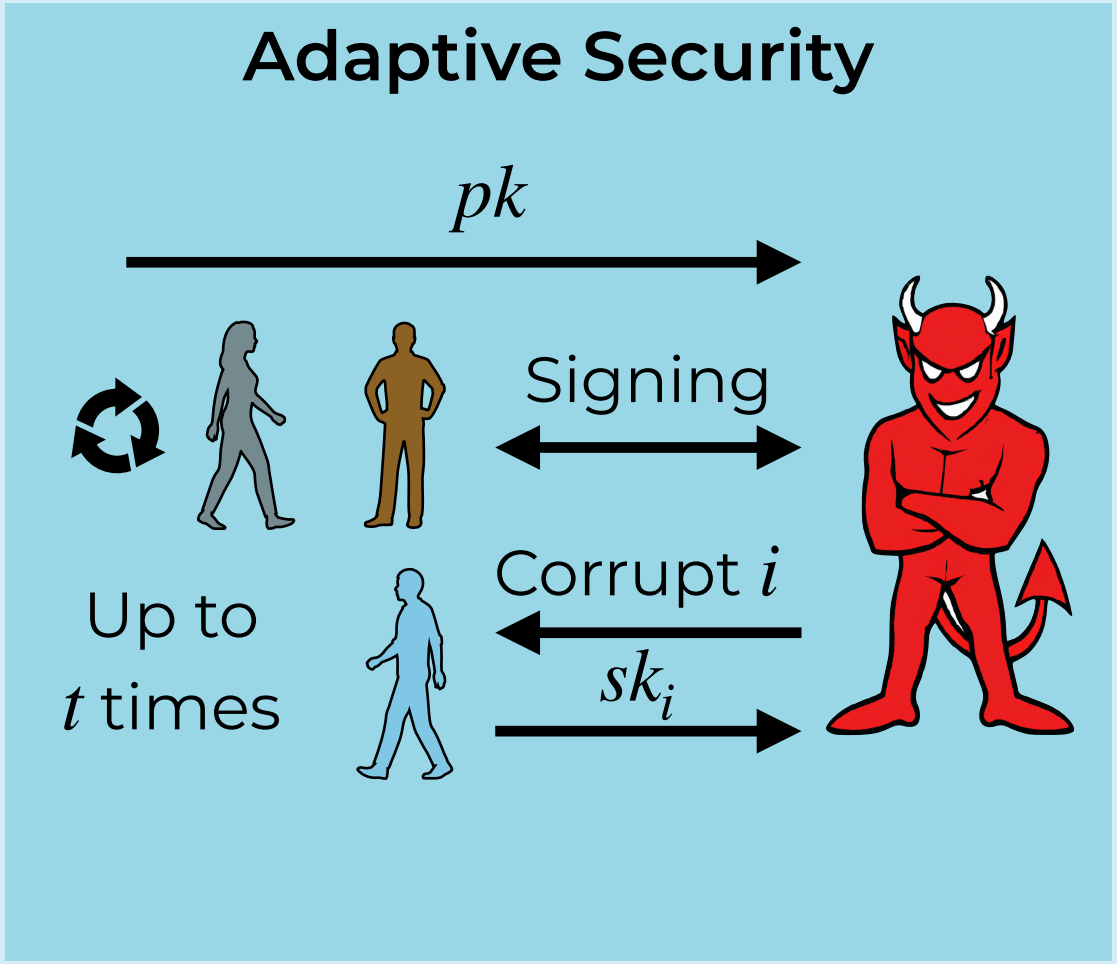
Security of Threshold Signatures



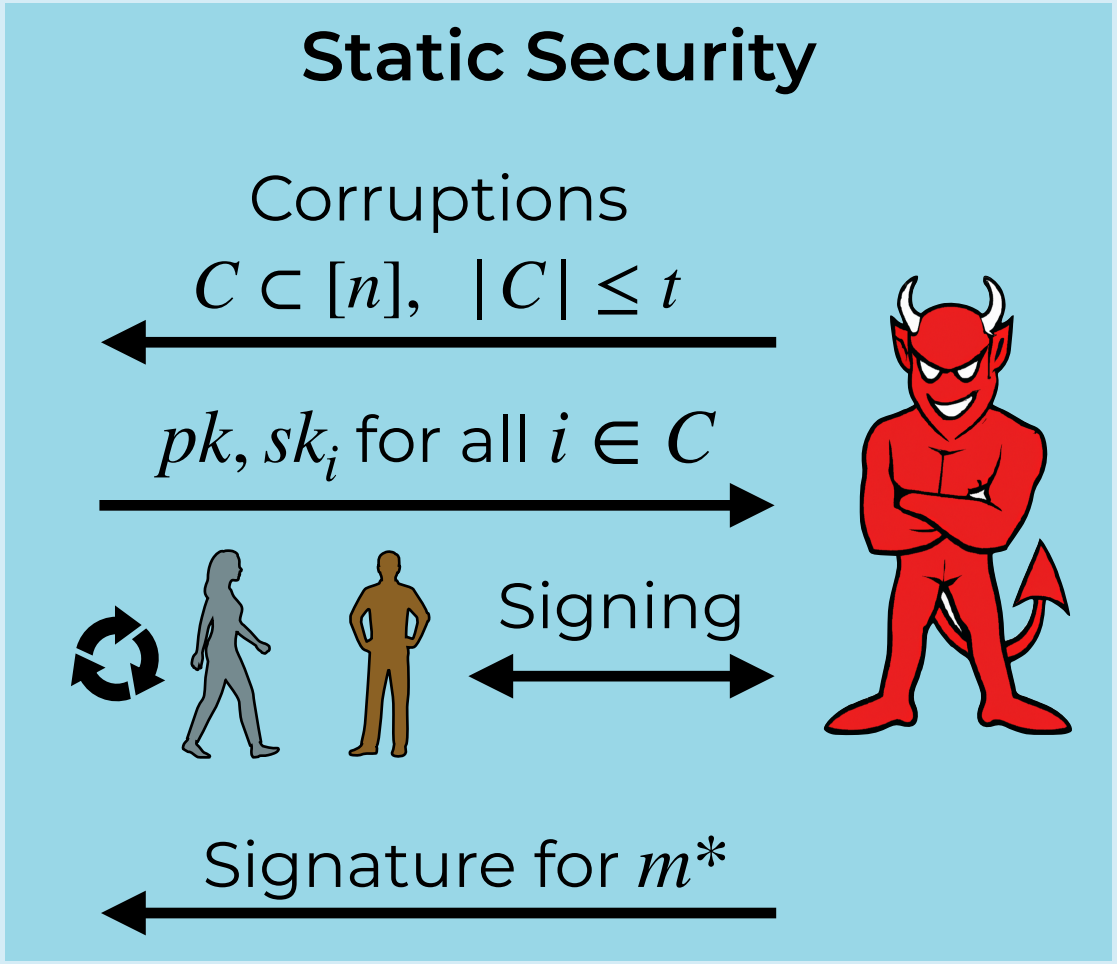


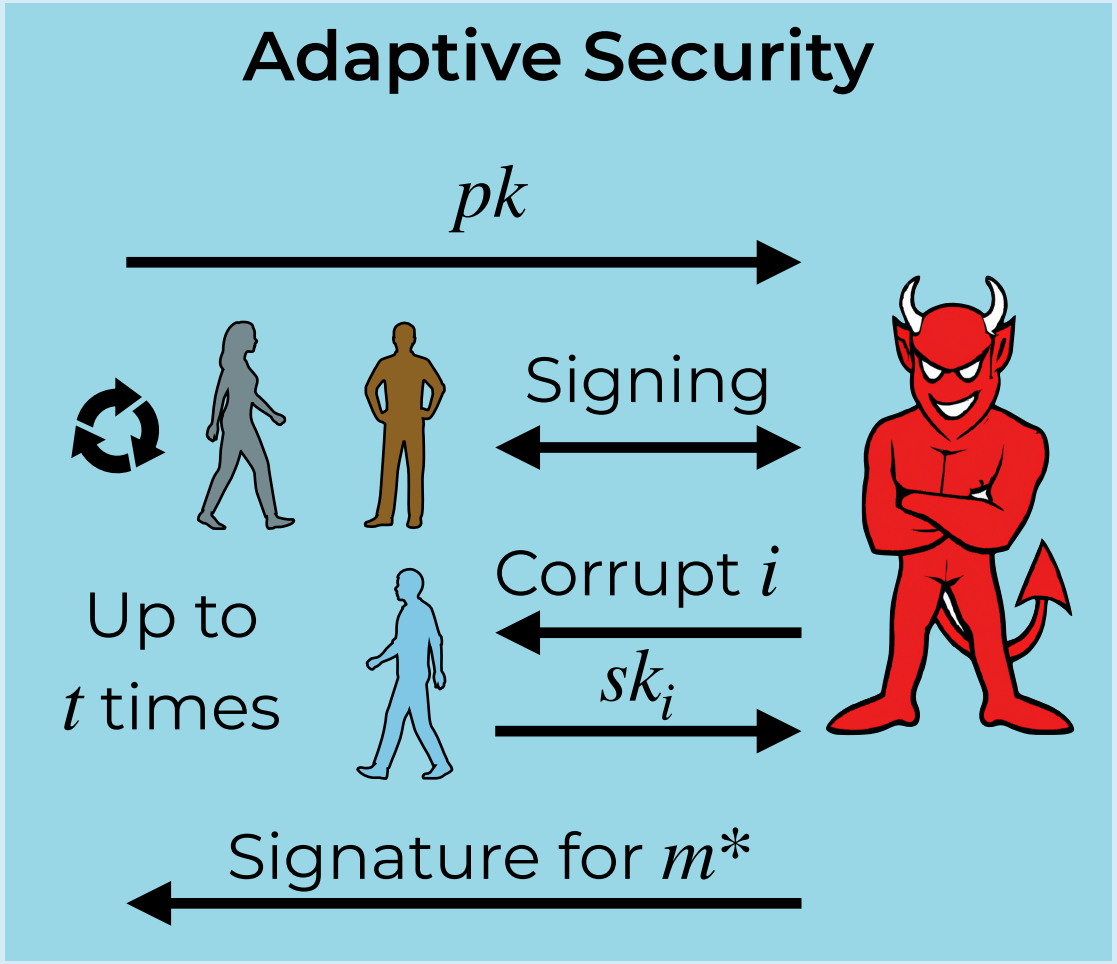
Security of Threshold Signatures



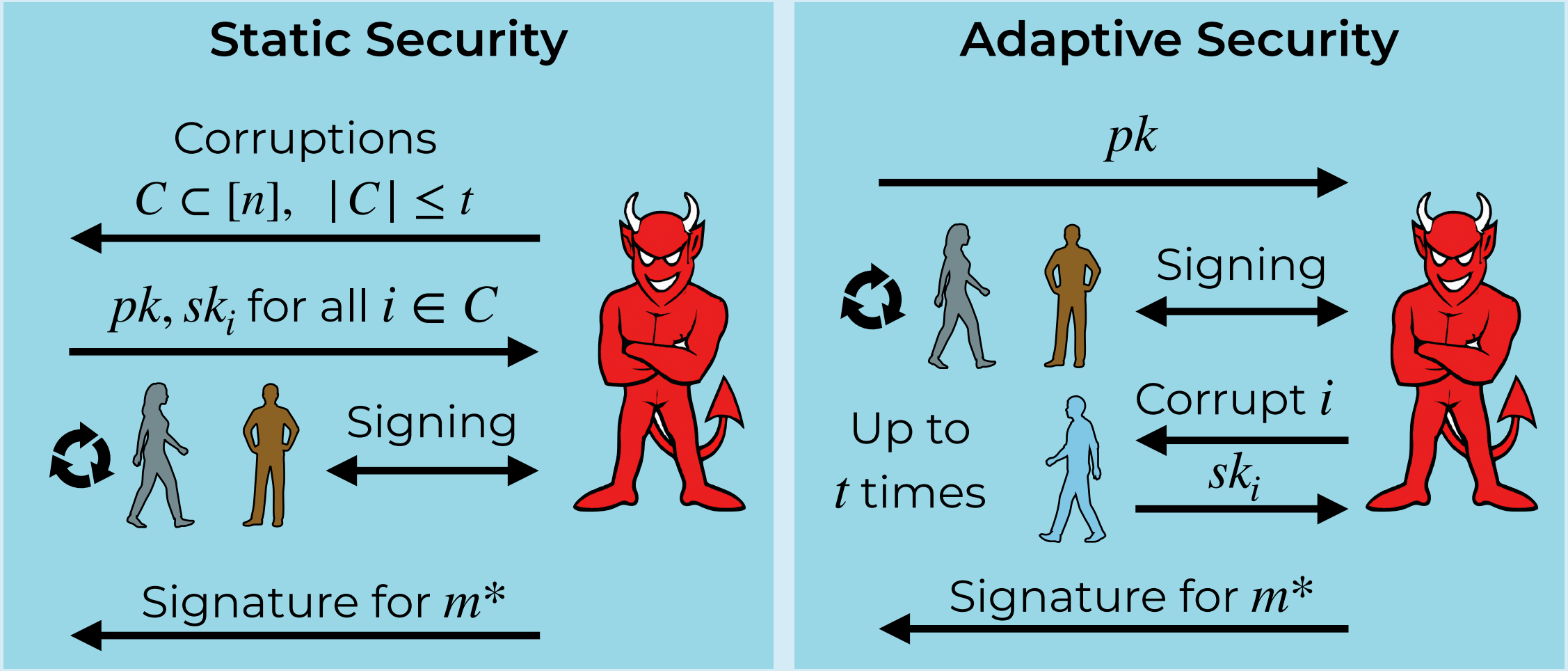


Security of Threshold Signatures





Security of Threshold Signatures



Goal: Adaptive Security

Threshold Signatures in Pairing-Free Groups

Threshold Signatures in Pairing-Free Groups

Frost Family

Threshold Signatures in Pairing-Free Groups

Frost Family

Frost 1-3	TZ
OMDL	DLOG
Static	Static

Frost [SAC 20, KG and Crypto 23, CKM+], Frost2 [Crypto 23, CKM+], Frost3 [CCS 22, RRJ+], TZ [Eurocrypt 23, TZ], Sparkle [Crypto 23, CKM]

Threshold Signatures in Pairing-Free Groups

Frost Family

Frost 1-3	TZ
OMDL	DLOG
Static	Static

Sparkle

Frost [SAC 20, KG and Crypto 23, CKM+], Frost2 [Crypto 23, CKM+], Frost3 [CCS 22, RRJ+], TZ [Eurocrypt 23, TZ], Sparkle [Crypto 23, CKM]

Threshold Signatures in Pairing-Free Groups

Frost Family

Frost 1-3	TZ
OMDL	DLOG
Static	Static

Sparkle

Proof 1	Proof 2

Frost [SAC 20, KG and Crypto 23, CKM+], Frost2 [Crypto 23, CKM+], Frost3 [CCS 22, RRJ+], TZ [Eurocrypt 23, TZ], Sparkle [Crypto 23, CKM]

Threshold Signatures in Pairing-Free Groups

Frost Family

Frost 1-3	TZ
OMDL	DLOG
Static	Static

Sparkle

Proof 1	Proof 2
DLOG	
Static	

Frost [SAC 20, KG and Crypto 23, CKM+], Frost2 [Crypto 23, CKM+], Frost3 [CCS 22, RRJ+], TZ [Eurocrypt 23, TZ], Sparkle [Crypto 23, CKM]

Threshold Signatures in Pairing-Free Groups

Frost Family

Frost 1-3	TZ
OMDL	DLOG
Static	Static

Sparkle

Proof 1	Proof 2
DLOG	OMDL
Static	Adaptive

Frost [SAC 20, KG and Crypto 23, CKM+], Frost2 [Crypto 23, CKM+], Frost3 [CCS 22, RRJ+], TZ [Eurocrypt 23, TZ], Sparkle [Crypto 23, CKM]

Threshold Signatures in Pairing-Free Groups

Frost Family

Frost 1-3	TZ
OMDL	DLOG
Static	Static

Sparkle

Proof 1	Proof 2
DLOG	OMDL
Static	Adaptive

$\leq t/2$ **corruptions**

Frost [SAC 20, KG and Crypto 23, CKM+], Frost2 [Crypto 23, CKM+], Frost3 [CCS 22, RRJ+], TZ [Eurocrypt 23, TZ], Sparkle [Crypto 23, CKM]

Threshold Signatures in Pairing-Free Groups

Frost Family

Frost 1-3	TZ
OMDL	DLOG
Static	Static

Sparkle

Proof 1	Proof 2
DLOG	OMDL
Static	Adaptive
	$\leq t/2$ corruptions

Adaptive Security for $\leq t$ Corruptions?

Frost [SAC 20, KG and Crypto 23, CKM+], Frost2 [Crypto 23, CKM+], Frost3 [CCS 22, RRJ+], TZ [Eurocrypt 23, TZ], Sparkle [Crypto 23, CKM]

Threshold Signatures in Pairing-Free Groups

Frost Family		Sparkle	
Frost 1-3	**TZ**	**Proof 1**	**Proof 2**
OMDL	DLOG	DLOG	OMDL
Static	Static	Static	Adaptive
			$\leq t/2$ **corruptions**

Adaptive Security for $\leq t$ Corruptions?

Adaptive Security without Interactive Assumptions?

Frost [SAC 20, KG and Crypto 23, CKM+], Frost2 [Crypto 23, CKM+], Frost3 [CCS 22, RRJ+], TZ [Eurocrypt 23, TZ], Sparkle [Crypto 23, CKM]

Our Result: Twinkle Threshold Signatures

Frost Family		Sparkle	
Frost 1-3	**TZ**	**Proof 1**	**Proof 2**
OMDL	DLOG	DLOG	OMDL
Static	Static	Static	Adaptive
			$\leq t/2$ **corruptions**

Frost [SAC 20, KG and Crypto 23, CKM+], Frost2 [Crypto 23, CKM+], Frost3 [CCS 22, RRJ+], TZ [Eurocrypt 23, TZ], Sparkle [Crypto 23, CKM]

Our Result: Twinkle Threshold Signatures

Frost Family

Frost 1-3	TZ
OMDL	DLOG
Static	Static

Sparkle

Proof 1	Proof 2
DLOG	OMDL
Static	Adaptive

$\leq t/2$ **corruptions**

Twinkle

DDH Assumption

Full Adaptive Security

Frost [SAC 20, KG and Crypto 23, CKM+], Frost2 [Crypto 23, CKM+], Frost3 [CCS 22, RRJ+], TZ [Eurocrypt 23, TZ], Sparkle [Crypto 23, CKM]

Technical Challenges

Allow up to t Corruptions

Non-Interactive Assumption

Technical Challenges

Allow up to t Corruptions

Non-Interactive Assumption

One-More Discrete Logarithm Assumption

Cyclic Group $\mathbb{G} = \{g^0, \ldots, g^{p-1}\}$

One-More Discrete Logarithm Assumption

Cyclic Group $\mathbb{G} = \{g^0, \ldots, g^{p-1}\}$

OMDL Solver

OMDL Assumption: There is no Efficient OMDL Solver

One-More Discrete Logarithm Assumption

Cyclic Group $\mathbb{G} = \{g^0, \ldots, g^{p-1}\}$

$$f = a_0 + a_1 X + \cdots + a_t X^t$$

OMDL Solver

OMDL Assumption: There is no Efficient OMDL Solver

One-More Discrete Logarithm Assumption

Cyclic Group $\mathbb{G} = \{g^0, \ldots, g^{p-1}\}$

$$f = a_0 + a_1 X + \cdots + a_t X^t$$

$$g^{f(0)}, \ldots, g^{f(n)} \longrightarrow \boxed{\text{OMDL Solver}}$$

OMDL Assumption: There is no Efficient OMDL Solver

One-More Discrete Logarithm Assumption

Cyclic Group $\mathbb{G} = \{g^0, \ldots, g^{p-1}\}$

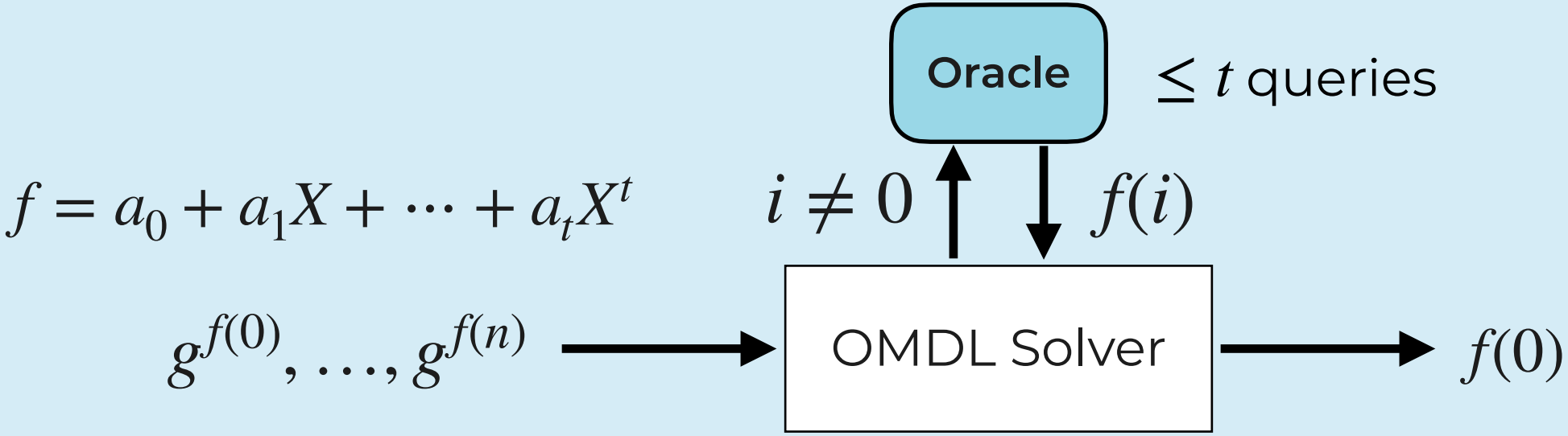
$$f = a_0 + a_1 X + \cdots + a_t X^t$$

$$g^{f(0)}, \ldots, g^{f(n)} \longrightarrow \boxed{\text{OMDL Solver}} \longrightarrow f(0)$$

OMDL Assumption: There is no Efficient OMDL Solver

One-More Discrete Logarithm Assumption

Cyclic Group $\mathbb{G} = \{g^0, \ldots, g^{p-1}\}$



OMDL Assumption: There is no Efficient OMDL Solver

Sparkle Threshold Signatures

Sparkle Threshold Signatures

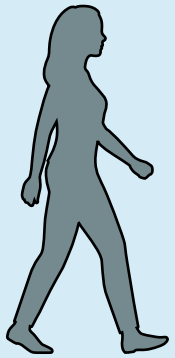
$$f = a_0 + a_1 X + a_2 X^2 + \cdots + a_t X^t$$

Sparkle Threshold Signatures

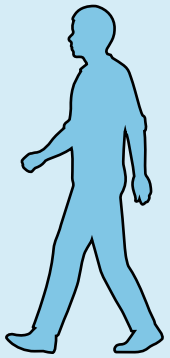
$$f = a_0 + a_1 X + a_2 X^2 + \cdots + a_t X^t \qquad pk = g^{f(0)} \qquad sk = f(0)$$

Sparkle Threshold Signatures

$$f = a_0 + a_1 X + a_2 X^2 + \cdots + a_t X^t \qquad pk = g^{f(0)} \qquad sk = f(0)$$



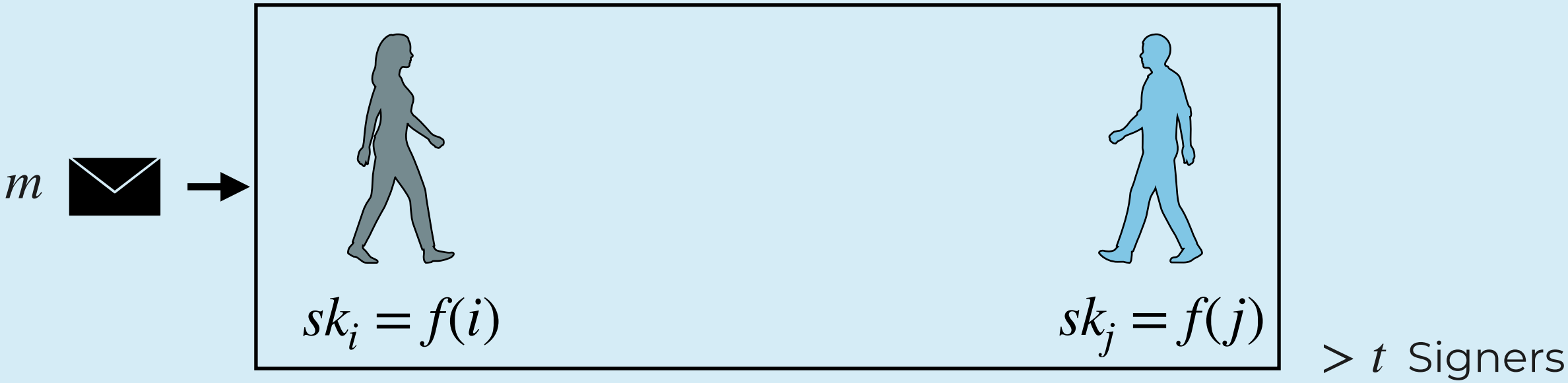
$$sk_i = f(i)$$



$$sk_j = f(j)$$

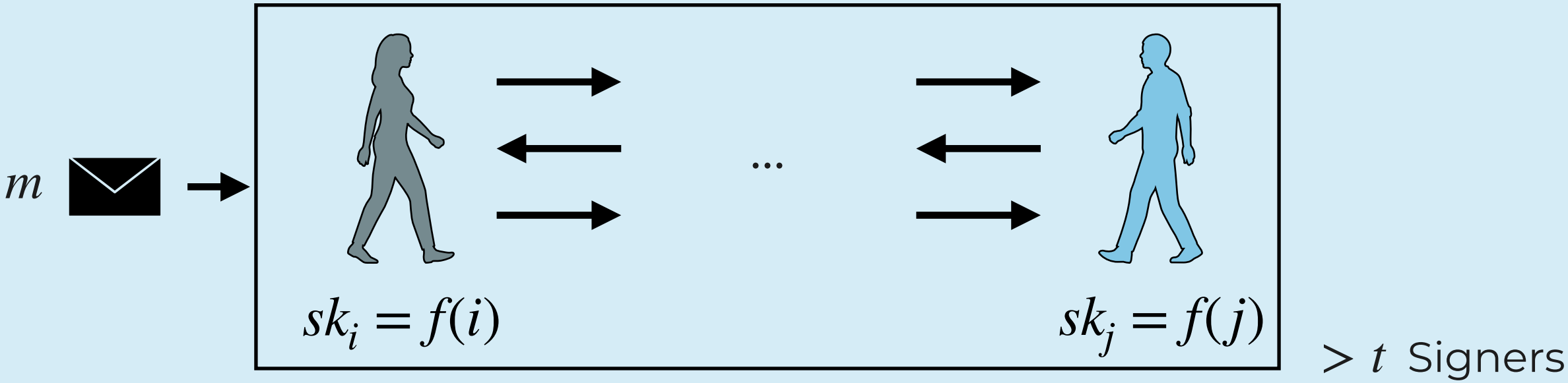
Sparkle Threshold Signatures

$$f = a_0 + a_1 X + a_2 X^2 + \cdots + a_t X^t \qquad pk = g^{f(0)} \qquad sk = f(0)$$



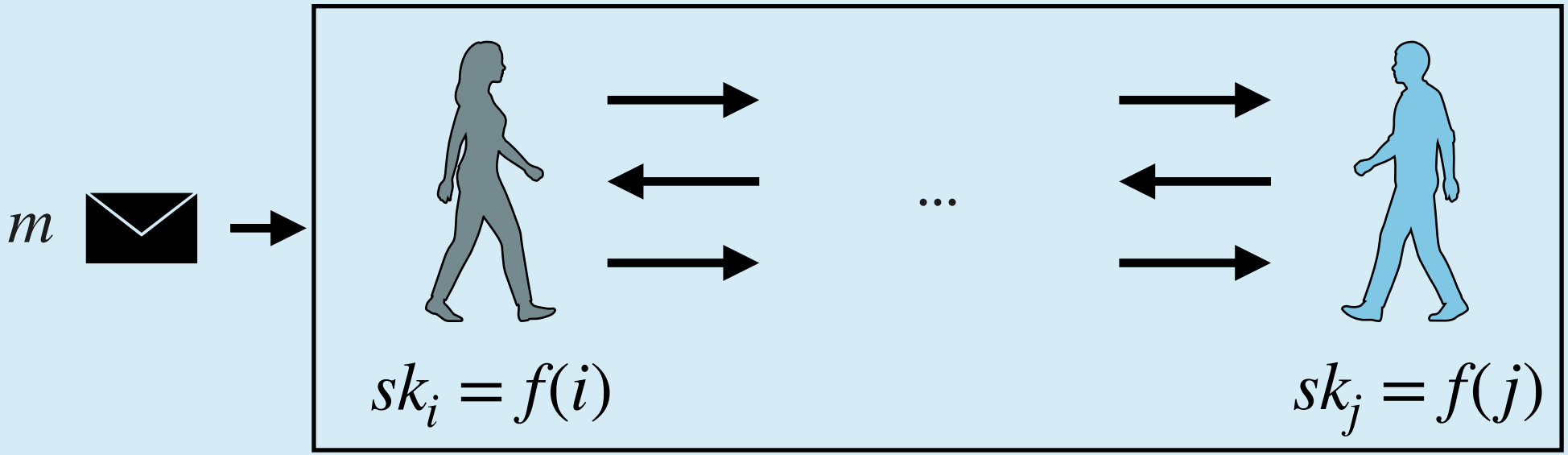
Sparkle Threshold Signatures

$$f = a_0 + a_1 X + a_2 X^2 + \cdots + a_t X^t \qquad pk = g^{f(0)} \qquad sk = f(0)$$

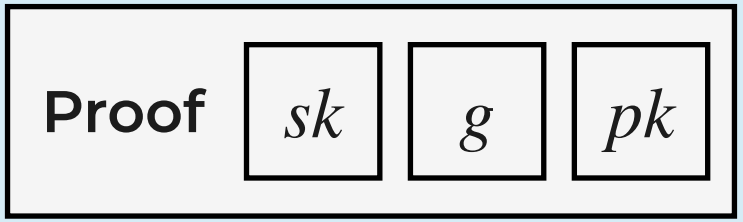


Sparkle Threshold Signatures

$$f = a_0 + a_1 X + a_2 X^2 + \cdots + a_t X^t \qquad pk = g^{f(0)} \qquad sk = f(0)$$



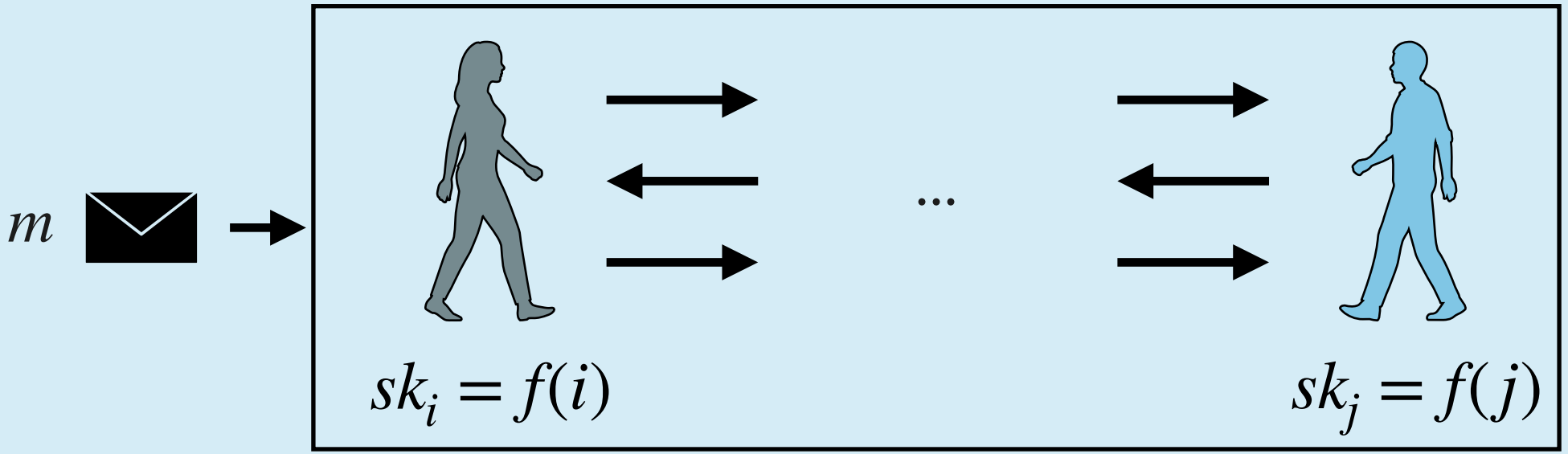
$> t$ Signers



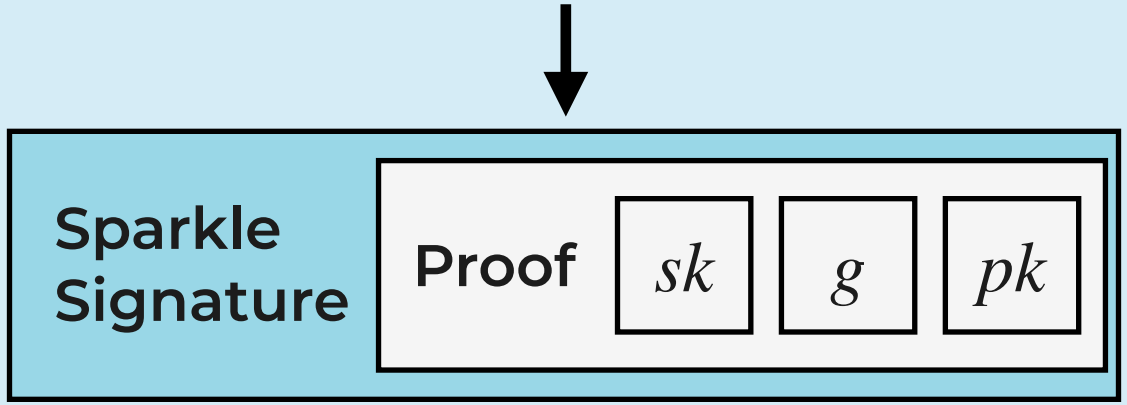
"We know sk such that $pk = g^{sk}$"

Sparkle Threshold Signatures

$$f = a_0 + a_1 X + a_2 X^2 + \cdots + a_t X^t \qquad pk = g^{f(0)} \qquad sk = f(0)$$



$> t$ Signers



"We know sk such that $pk = g^{sk}$"

Sparkle’s Security Proof

Sparkle's Security Proof

One-More DLOG

Reduction

Sparkle Adversary

Sparkle's Security Proof

One-More DLOG

Reduction

Sparkle Adversary

Simplification: No Signing Query

Sparkle's Security Proof

One-More DLOG

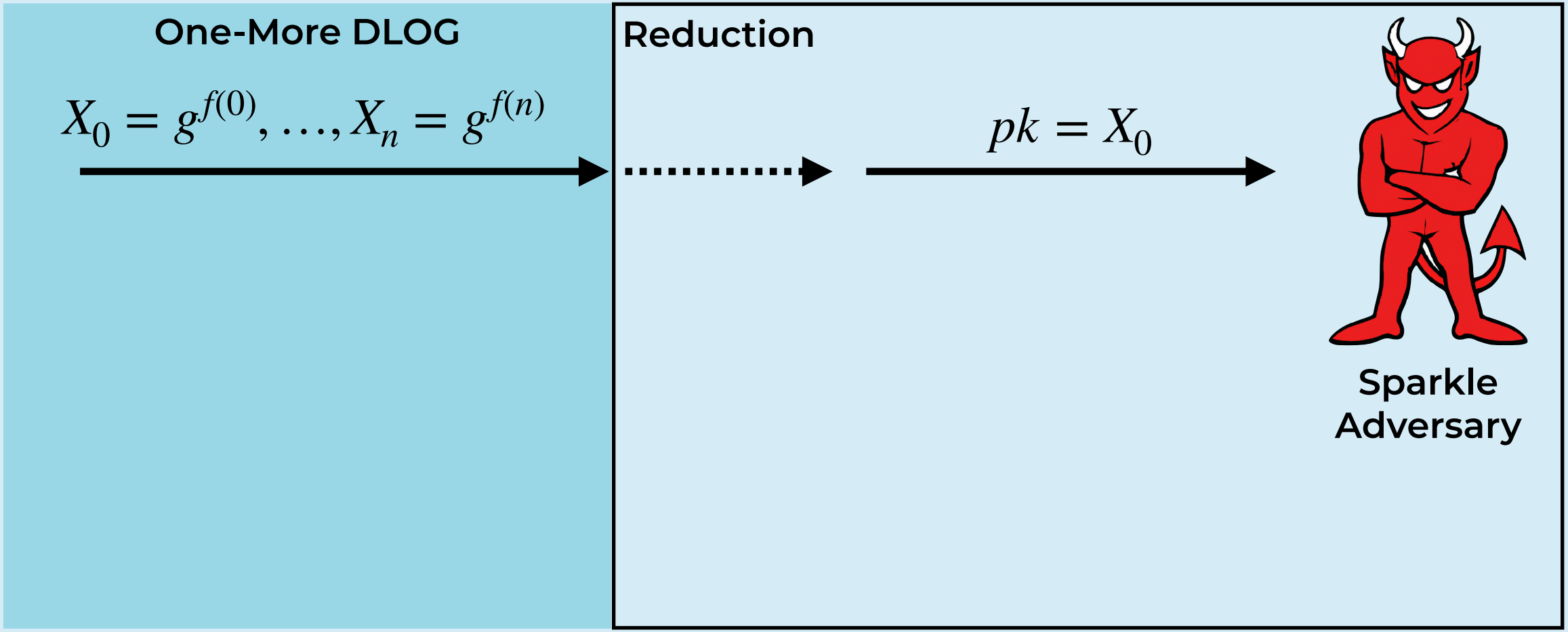
$$X_0 = g^{f(0)}, \ldots, X_n = g^{f(n)}$$

Reduction

Sparkle Adversary

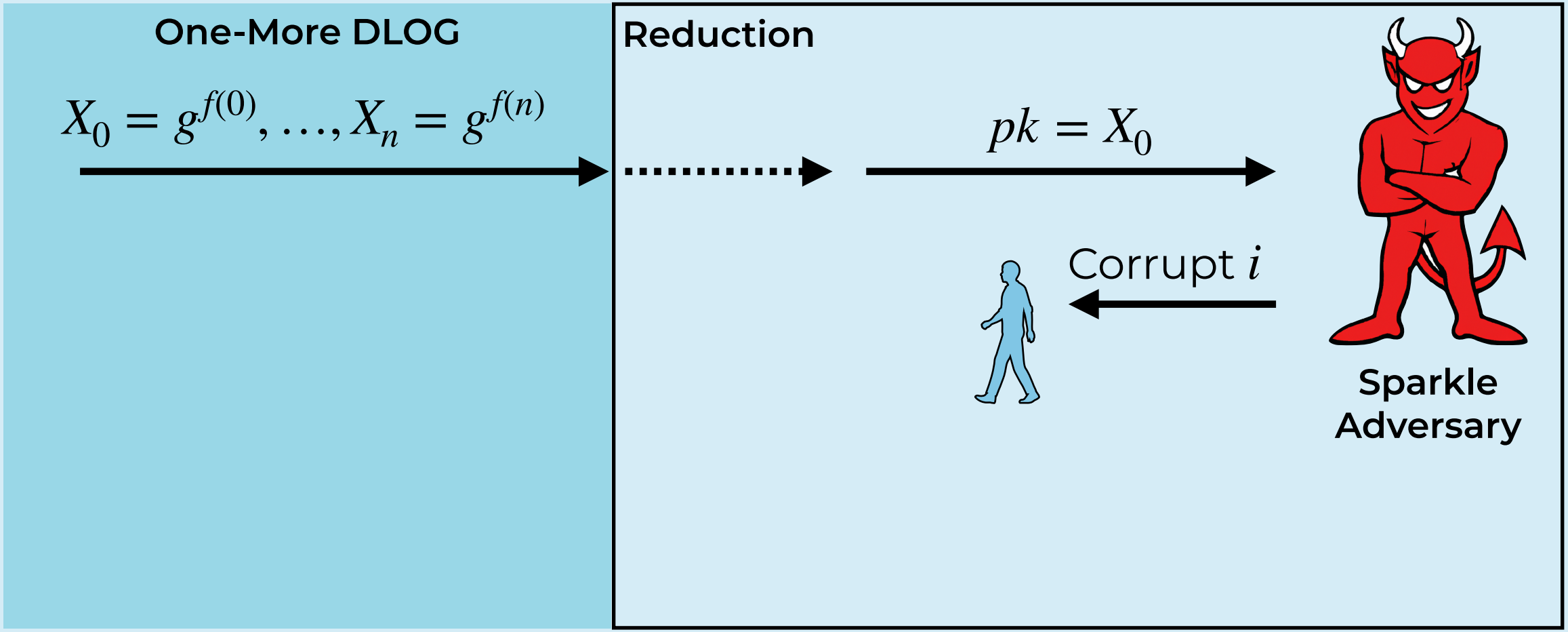
Simplification: No Signing Query

Sparkle's Security Proof



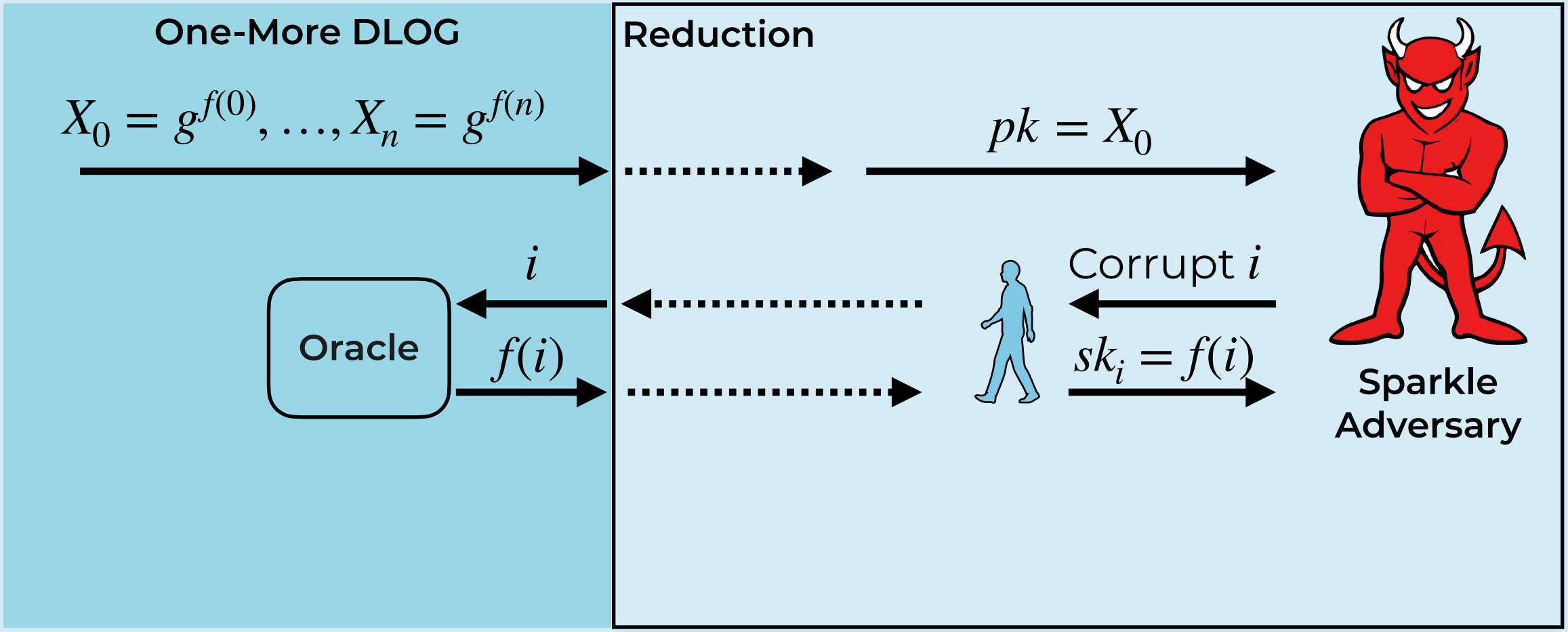
Simplification: No Signing Query

Sparkle's Security Proof



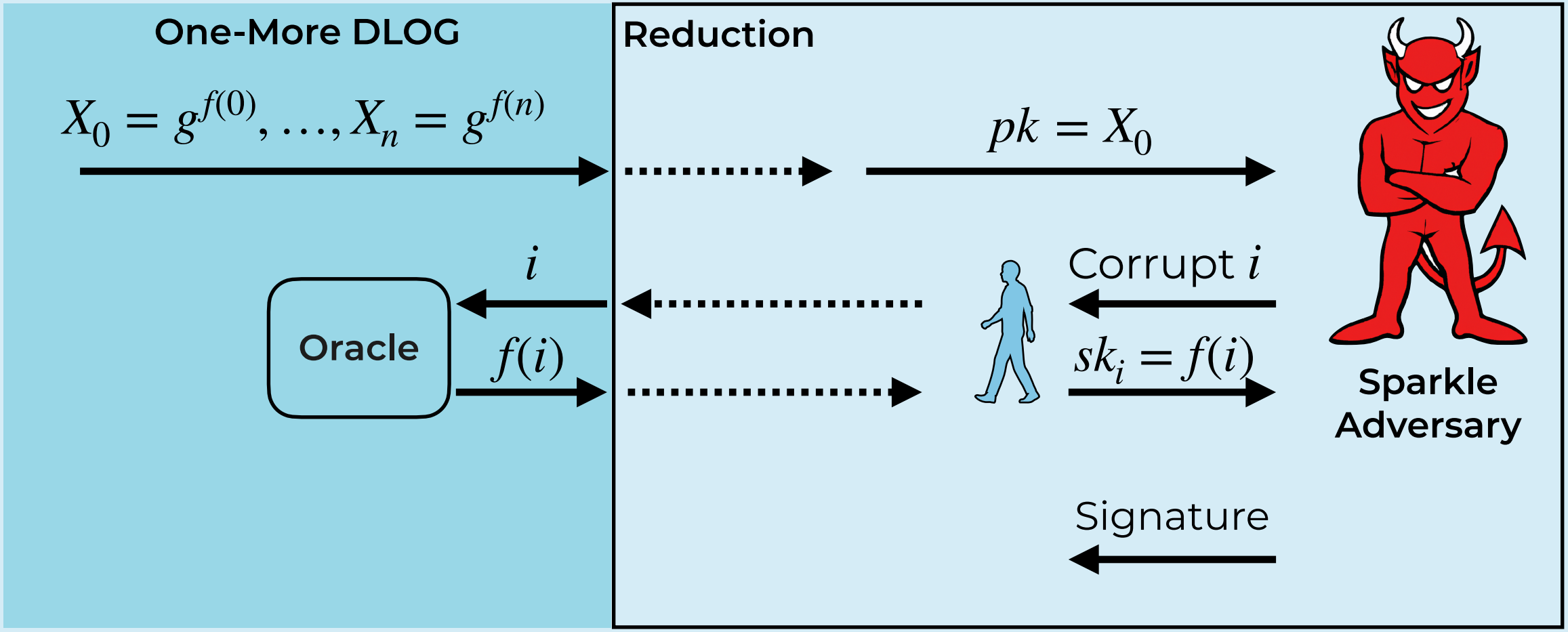
Simplification: No Signing Query

Sparkle's Security Proof



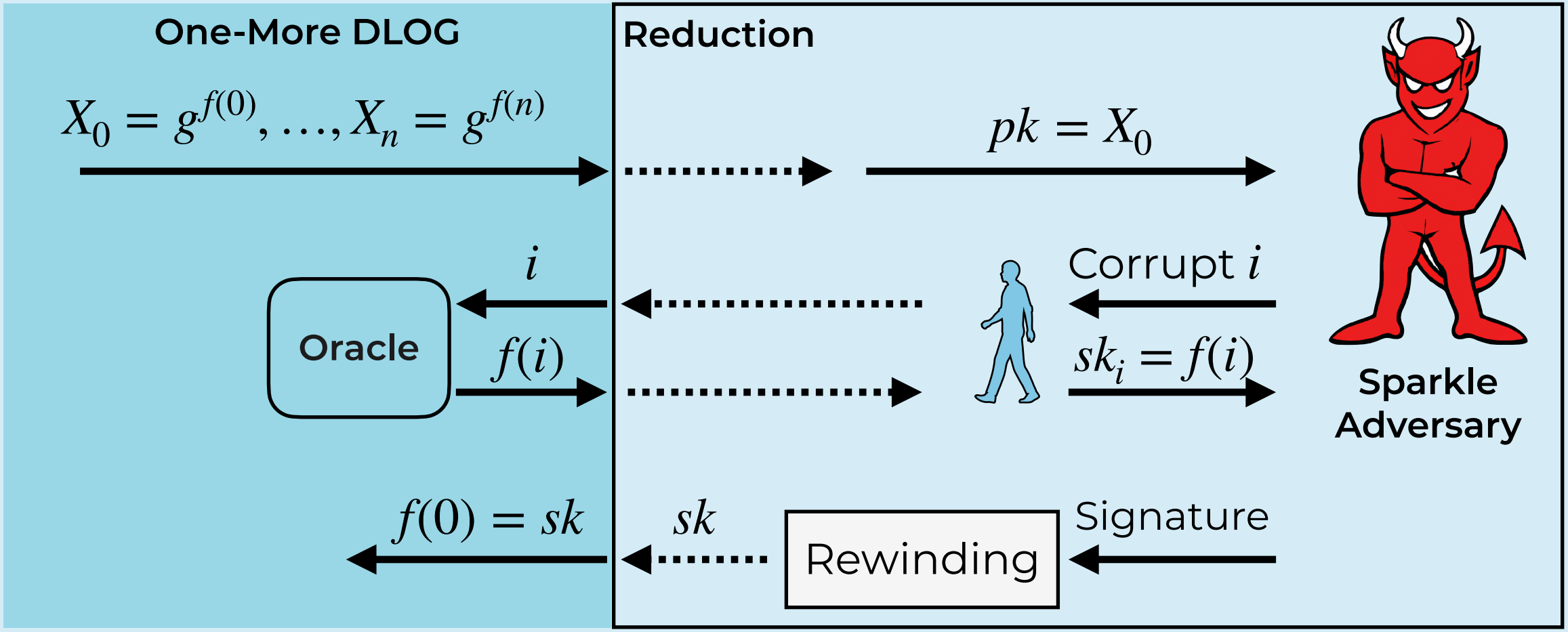
Simplification: No Signing Query

Sparkle's Security Proof



Simplification: No Signing Query

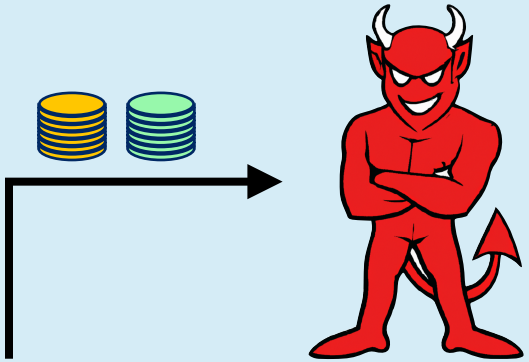
Sparkle's Security Proof



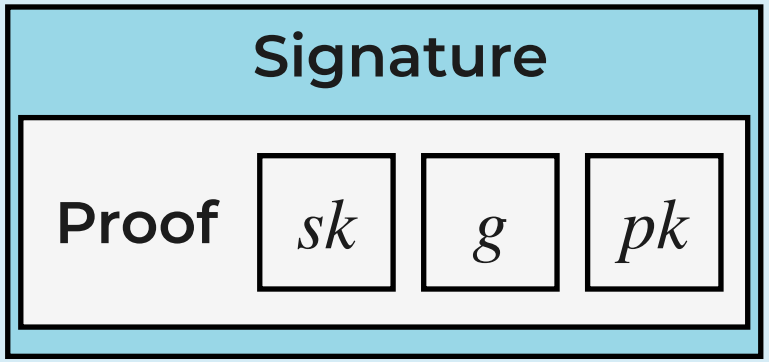
Simplification: No Signing Query

Sparkle’s Security Proof

Sparkle's Security Proof

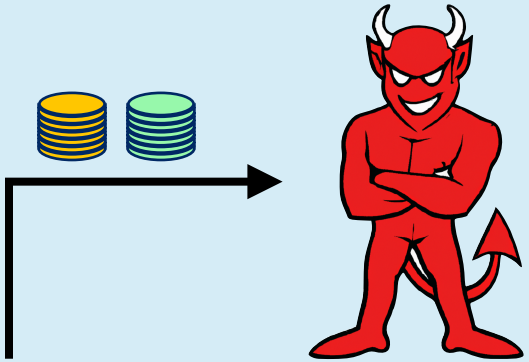


t_c corruptions

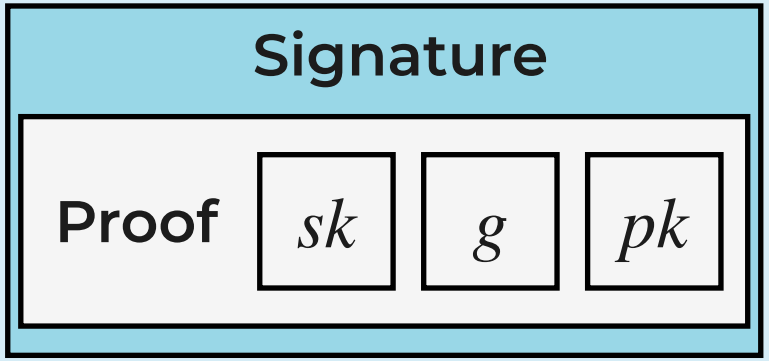


$pk = X_0$

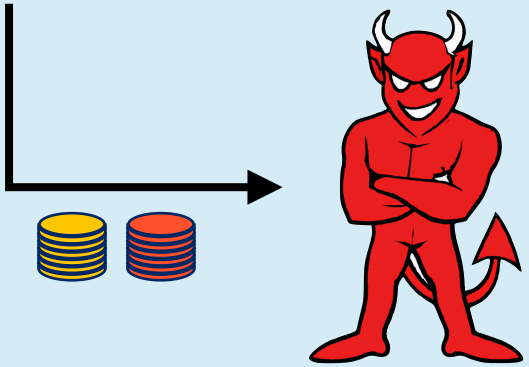
Sparkle's Security Proof



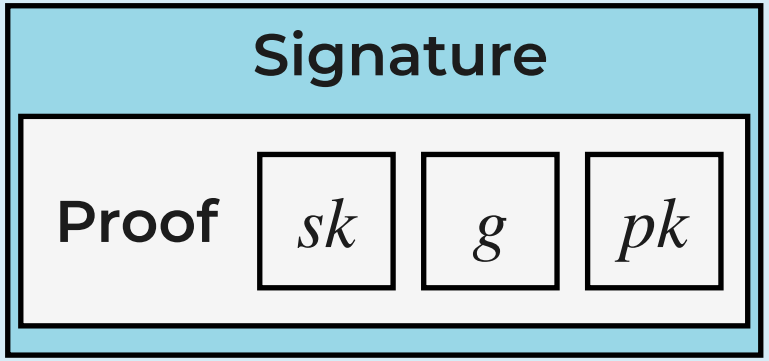
t_c corruptions



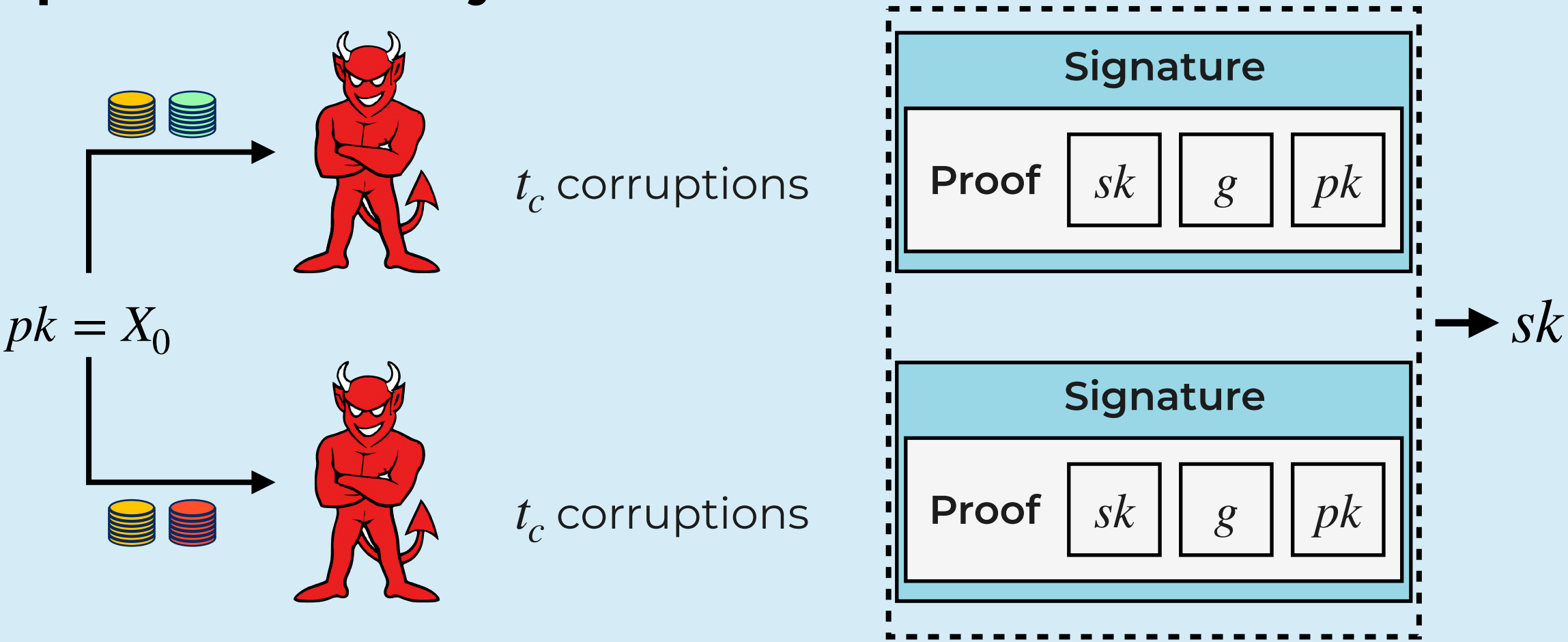
$pk = X_0$



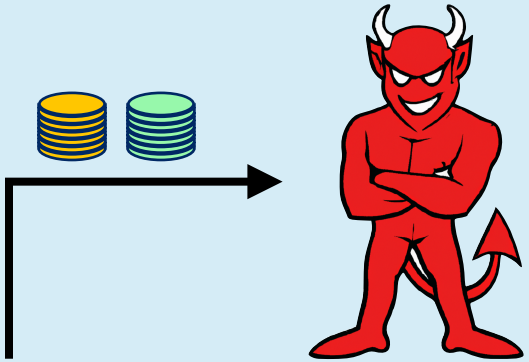
t_c corruptions



Sparkle's Security Proof

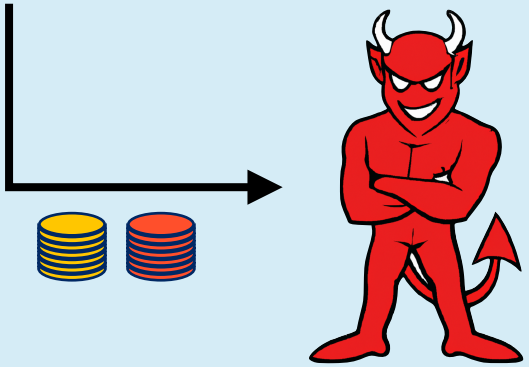


Sparkle's Security Proof



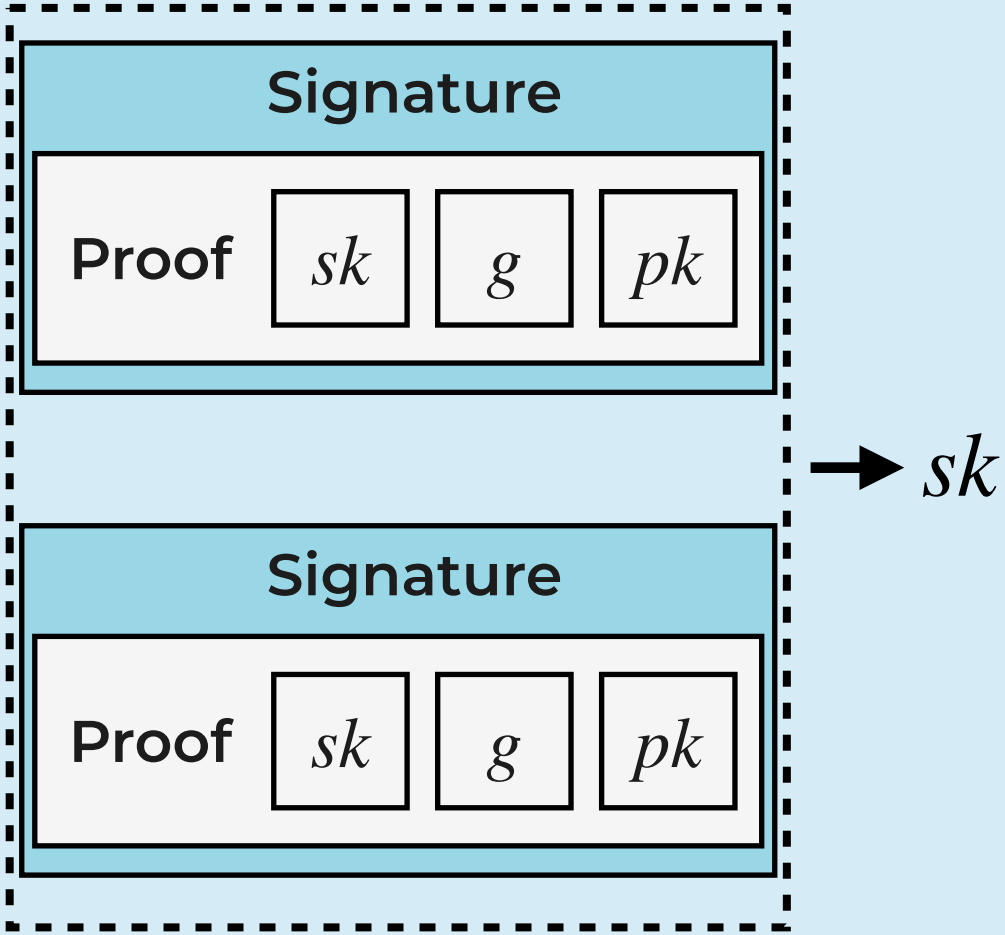
t_c corruptions

$pk = X_0$

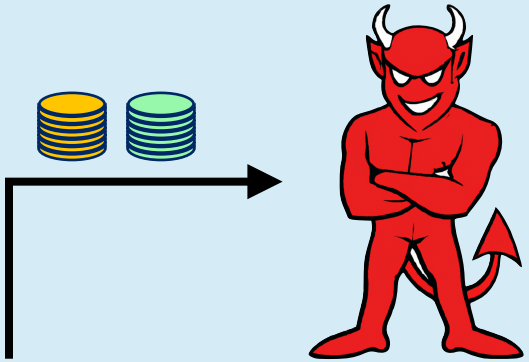


t_c corruptions

$\Longrightarrow 2t_c$ corruptions

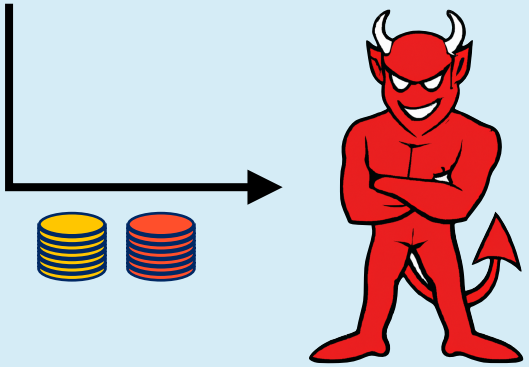


Sparkle's Security Proof

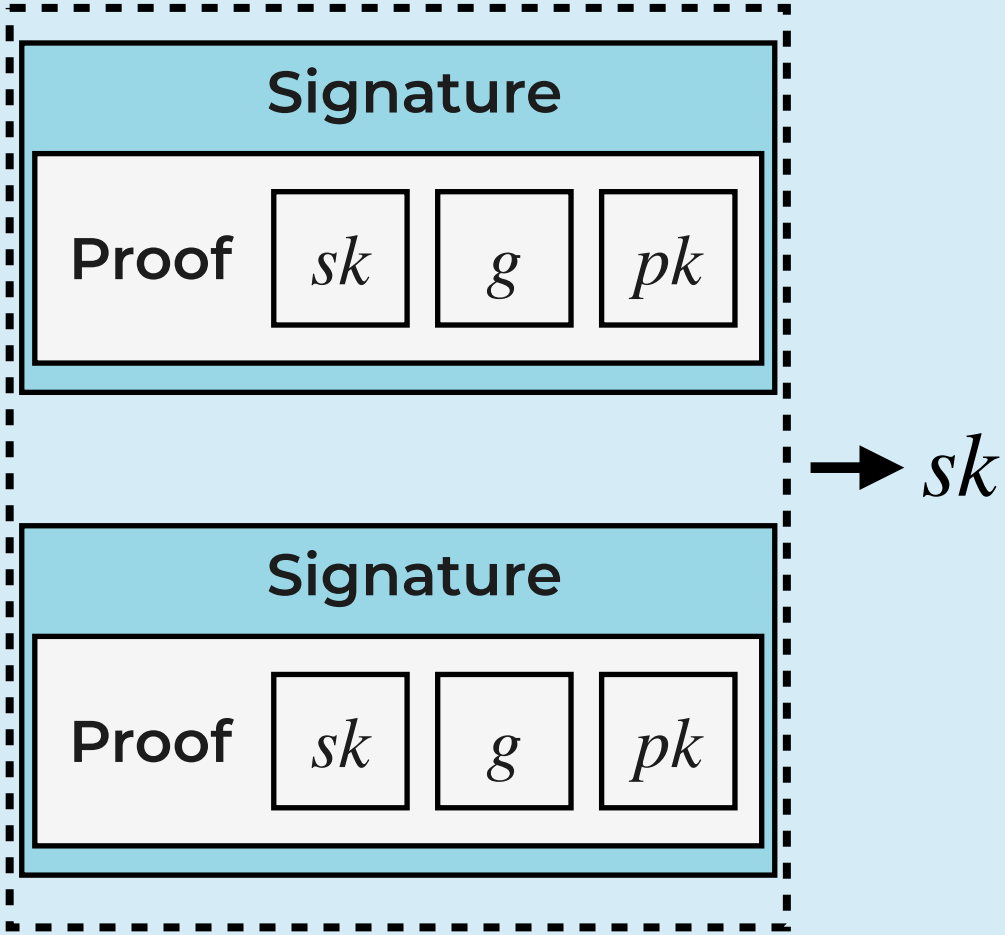


t_c corruptions

$pk = X_0$



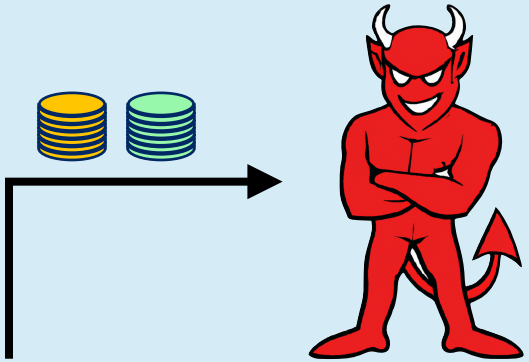
t_c corruptions



$\Longrightarrow 2t_c$ corruptions

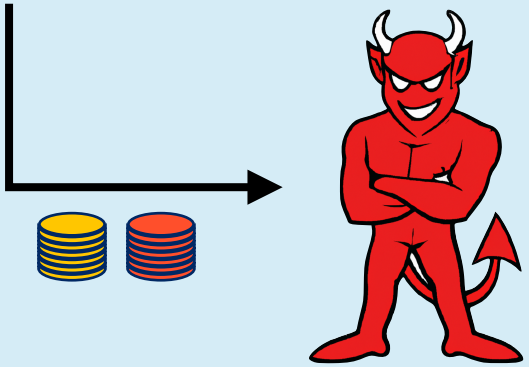
$\Longrightarrow 2t_c$ DLOG queries

Sparkle's Security Proof

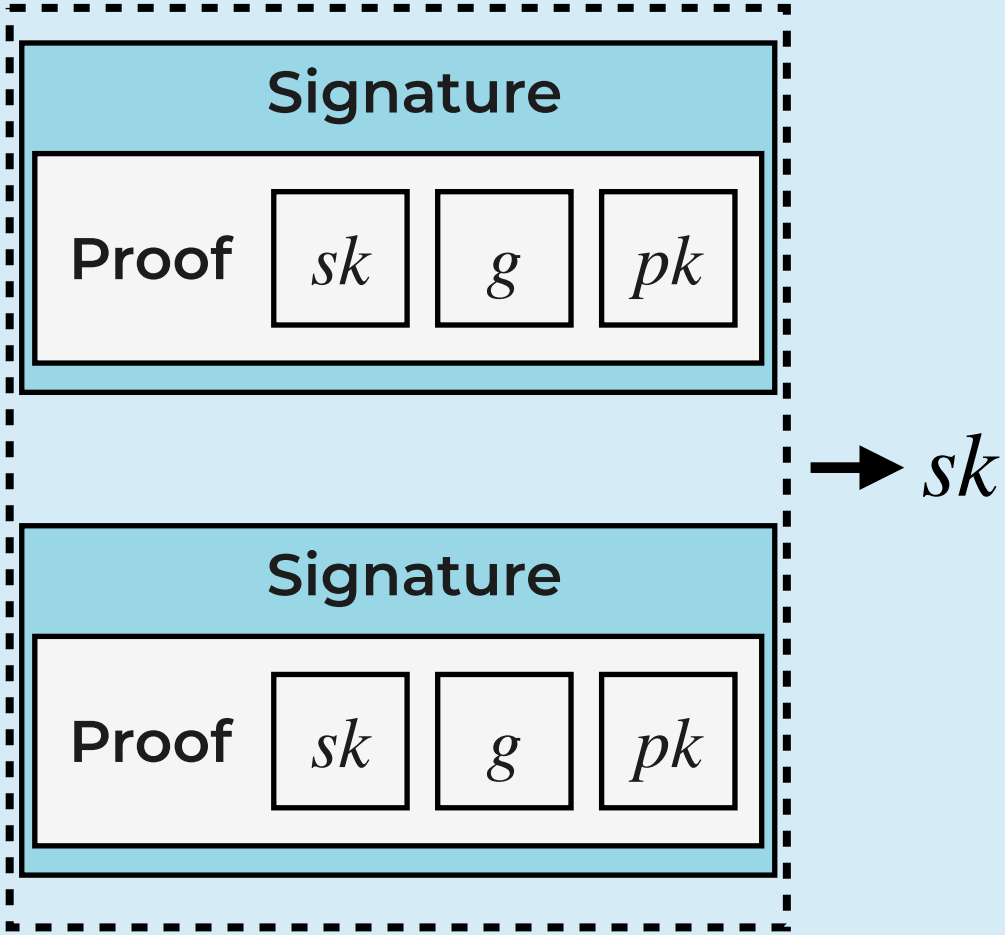


t_c corruptions

$pk = X_0$



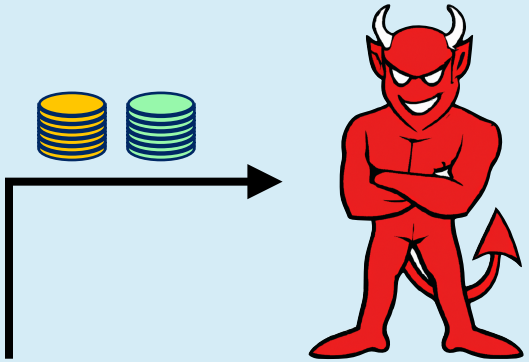
t_c corruptions



$\Longrightarrow 2t_c$ corruptions

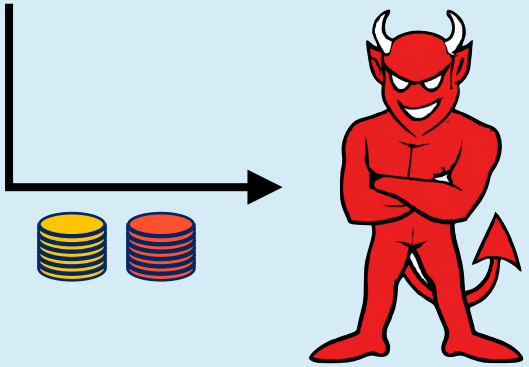
$\Longrightarrow 2t_c$ DLOG queries $\Longrightarrow 2t_c \leq t$

Sparkle's Security Proof

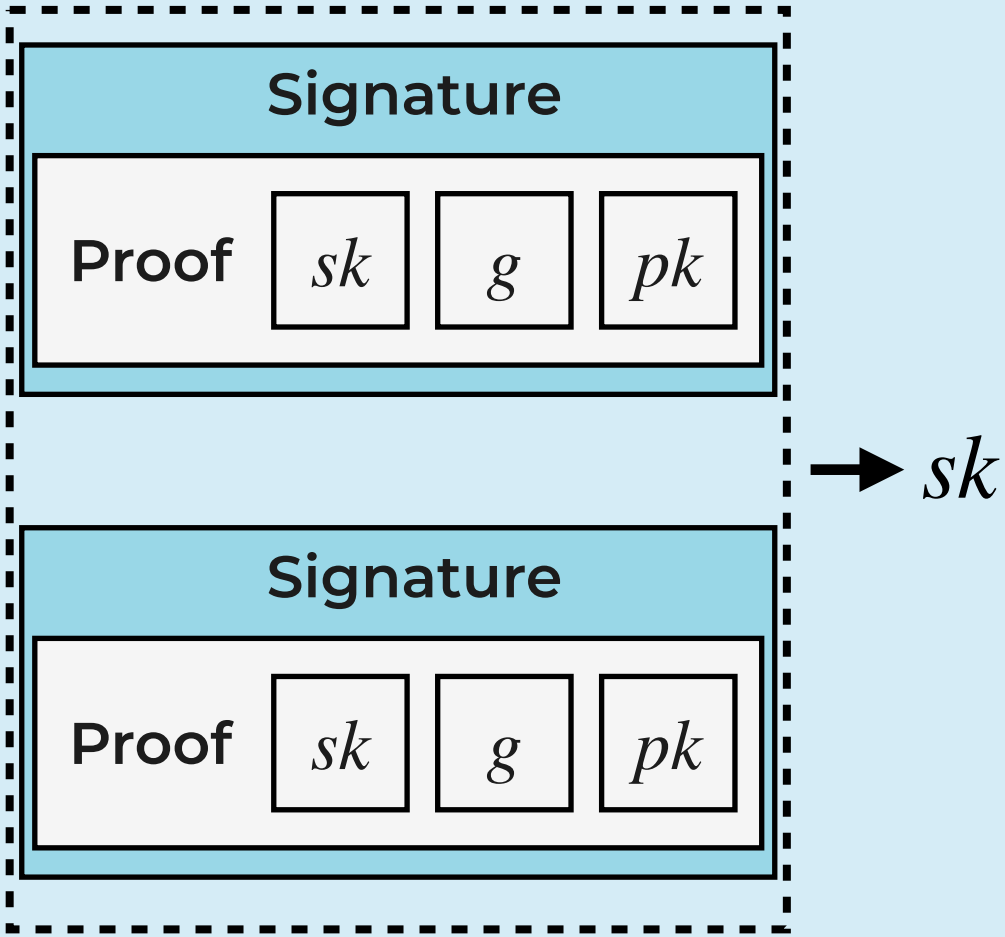


t_c corruptions

$pk = X_0$



t_c corruptions



$\Longrightarrow 2t_c$ corruptions

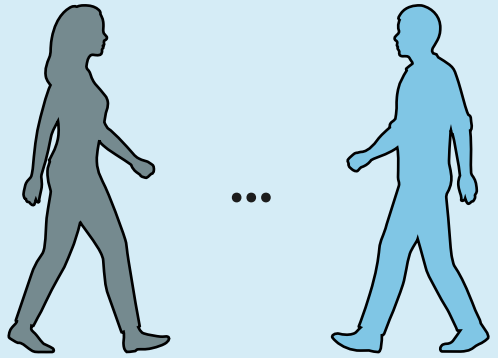
$\Longrightarrow 2t_c$ DLOG queries $\Longrightarrow 2t_c \leq t$

Goal: Avoid Rewinding

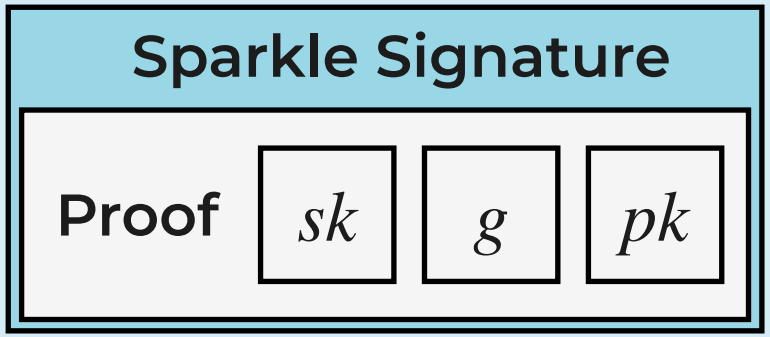
Our Solution

Our Solution

$$pk = g^{sk}$$



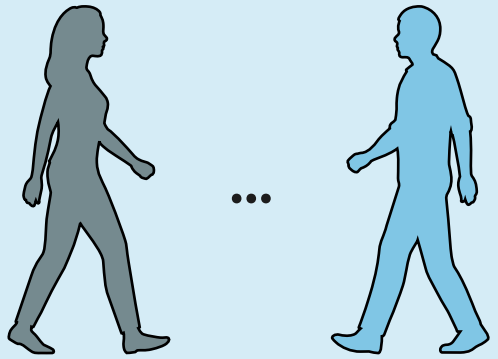
$sk_i = f(i)$ $sk_j = f(j)$



*"We **know** sk such that $pk = g^{sk}$"*

Our Solution

$$pk = g^{sk}$$



$sk_i = f(i)$ ... $sk_j = f(j)$

Sparkle Signature

Proof	sk	g	pk

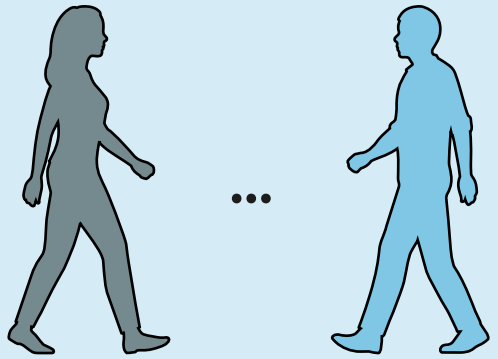
*"We **know** sk such that $pk = g^{sk}$"*

Twinkle Signature

$pk' = h^{sk}$ for $h = H(m)$

Our Solution

$$pk = g^{sk}$$



$sk_i = f(i)$ ... $sk_j = f(j)$

Sparkle Signature

Proof	sk	g	pk

*"We **know** sk such that $pk = g^{sk}$"*

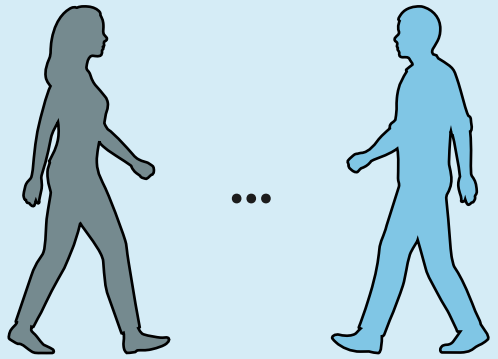
Twinkle Signature

$pk' = h^{sk}$ for $h = H(m)$

Proof	sk	g	pk
		h	pk'

Our Solution

$$pk = g^{sk}$$



$sk_i = f(i)$ ... $sk_j = f(j)$

Sparkle Signature

Proof	sk	g	pk

*"We **know** sk such that $pk = g^{sk}$"*

Twinkle Signature

$pk' = h^{sk}$ for $h = H(m)$

Proof	sk	g	pk
		h	pk'

*"There **is** sk such that $pk = g^{sk}$ and $pk' = h^{sk}$"*

Our Solution

Our Solution

$$pk = g^{sk}$$

Twinkle
Adversary

Our Solution

$$pk = g^{sk}$$

Twinkle Adversary

Twinkle Signature

pk' for $h = H(m^*)$

Proof

Our Solution

$pk = g^{sk}$

Twinkle Adversary

Twinkle Signature

pk' for $h = H(m^*)$

Proof

Case 1. $pk' = h^{sk}$

Our Solution

$pk = g^{sk}$

Twinkle Adversary

Twinkle Signature

pk' for $h = H(m^*)$

Proof

Case 1. $pk' = h^{sk}$

Solve CDH for $pk = g^{sk}, h$

Our Solution

$pk = g^{sk}$

Twinkle Adversary

Twinkle Signature

pk' for $h = H(m^*)$

Proof

Case 1. $pk' = h^{sk}$

Solve CDH for $pk = g^{sk}, h$

No Rewinding!

Our Solution

$pk = g^{sk}$

Twinkle Adversary

Twinkle Signature

pk' for $h = H(m^*)$

Proof

Case 1. $pk' = h^{sk}$

Solve CDH for $pk = g^{sk}, h$

No Rewinding!

Case 2. $pk' \neq h^{sk}$

Our Solution

$pk = g^{sk}$

Twinkle Adversary

Twinkle Signature

pk' for $h = H(m^*)$

Proof

Case 1. $pk' = h^{sk}$

Solve CDH for $pk = g^{sk}, h$

No Rewinding!

Case 2. $pk' \neq h^{sk}$

Generating Proof statistically hard

Our Solution

$pk = g^{sk}$

Twinkle Adversary

Twinkle Signature

pk' for $h = H(m^*)$

Proof

Case 1. $pk' = h^{sk}$

Solve CDH for $pk = g^{sk}, h$

No Rewinding!

Case 2. $pk' \neq h^{sk}$

Generating Proof statistically hard

No Reduction Needed!

Our Solution

CDH

No Corruptions

No Signing

No Rewinding

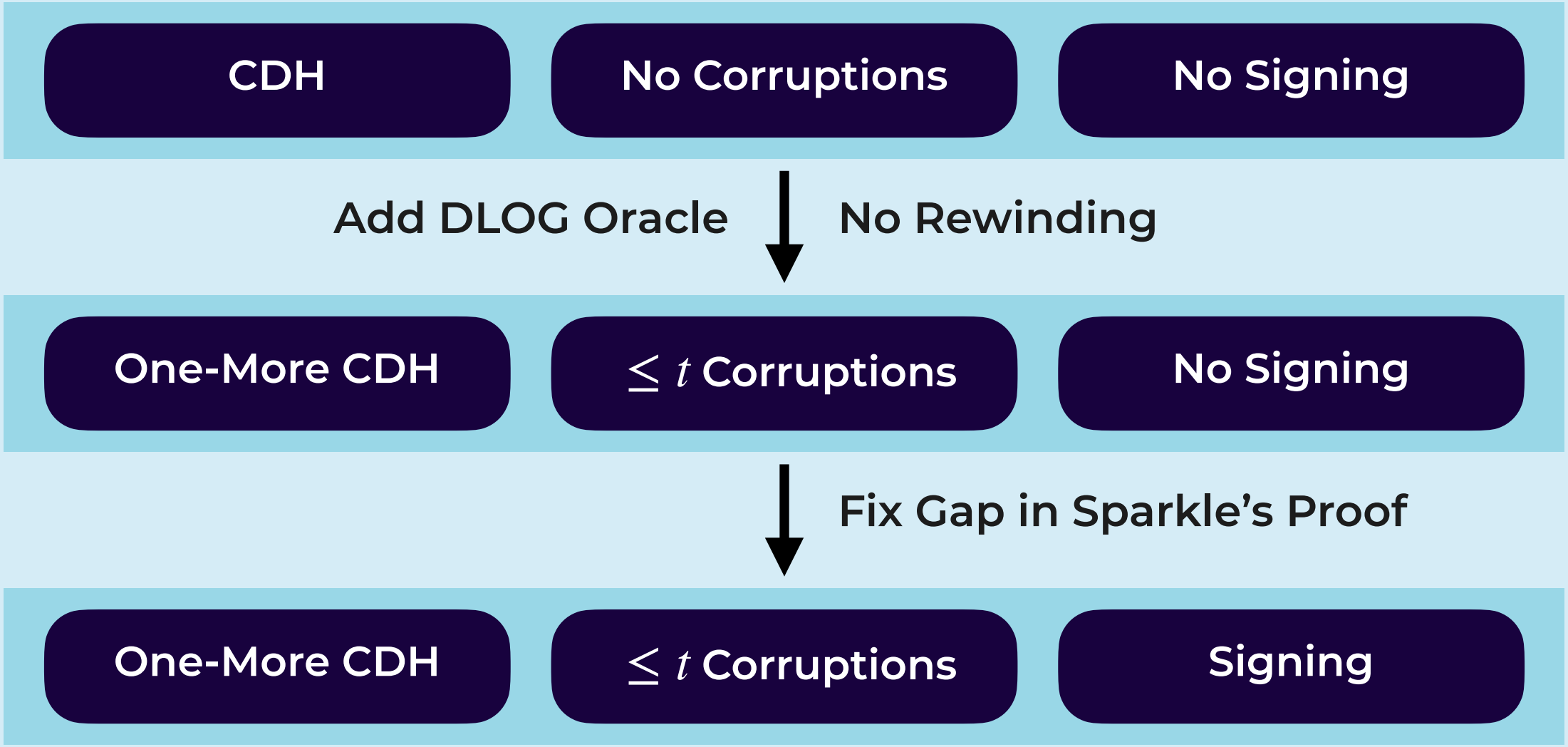
Our Solution

CDH | No Corruptions | No Signing

Add DLOG Oracle ↓ No Rewinding

One-More CDH | $\leq t$ Corruptions | No Signing

Our Solution



Summary and Future Work

Summary and Future Work

Twinkle

DDH Assumption

Full Adaptive Security

Summary and Future Work

Twinkle

DDH Assumption

Full Adaptive Security

Two-Round Construction?

Summary and Future Work

Twinkle

DDH Assumption

Full Adaptive Security

Two-Round Construction?

Non-Interactive Search Assumption?

Twinkle: Threshold Signatures from DDH with Full Adaptive Security

Renas Bacho [1,3] Julian Loss [1] Stefano Tessaro [2]

Benedikt Wagner [1,3] Chenzhi Zhu [2]

February 26, 2024

[1] CISPA Helmholtz Center for Information Security, Saarbrücken, Germany
{renas.bacho,loss,benedikt.wagner}@cispa.de
[2] Paul G. Allen School of Computer Science and Engineering, University of Washington, Seattle, USA
{tessaro,zhucz20}@cs.washington.edu
[3] Saarland University, Saarbrücken, Germany

Abstract

Sparkle is the first threshold signature scheme in the pairing-free discrete logarithm setting (Crites, Komlo, Maller, Crypto 2023) to be proven secure under adaptive corruptions. However, without using the algebraic group model, Sparkle's proof imposes an undesirable restriction on the adversary. Namely, for a signing threshold $t < n$, the adversary is restricted to corrupt at most $t/2$ parties. In addition, Sparkle's proof relies on a strong one-more assumption.

In this work, we propose Twinkle, a new threshold signature scheme in the pairing-free setting which overcomes these limitations. Twinkle is the first pairing-free scheme to have a security proof under up to t adaptive corruptions without relying on the algebraic group model. It is also the first such scheme with a security proof under adaptive corruptions from a well-studied non-interactive assumption, namely, the Decisional Diffie-Hellman (DDH) assumption.

We achieve our result in two steps. First, we design a generic scheme based on a linear function that satisfies several abstract properties and prove its adaptive security under a suitable one-more assumption related to this function. In the context of this proof, we also identify a gap in the security proof of Sparkle and develop new techniques to overcome this issue. Second, we give a suitable instantiation of the function for which the corresponding one-more assumption follows from DDH.

Keywords: Threshold Signatures, Adaptive Security, Pairing-Free, Non-Interactive Assumptions

eprint
2023/1482

DFG