Exclusive Ownership of Fiat–Shamir Signatures: ML-DSA, SQIsign, LESS, and More

Michael Meyer[1] Patrick Struck[2] Maximiliane Weishäupl[1]

CRYPTO 2025

[1]Universität Regensburg

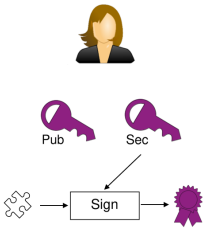
[2]Universität Konstanz

Motivation & Background

Motivation: Let's Encrypt Protocol

Generate 

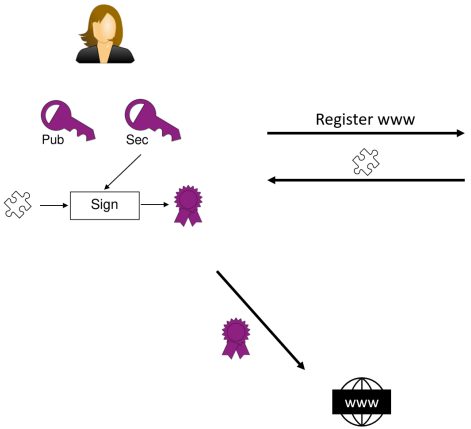
Motivation: Let's Encrypt Protocol



Let's Encrypt

Generate

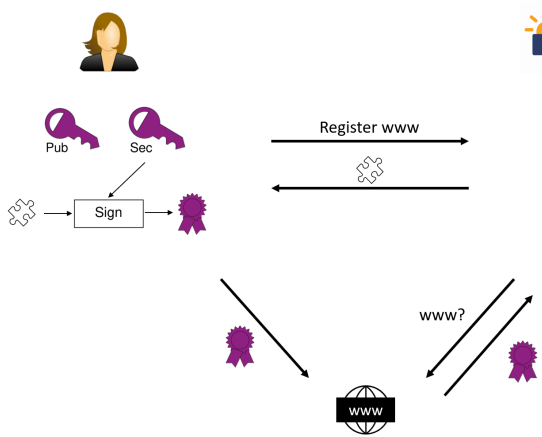
Motivation: Let's Encrypt Protocol



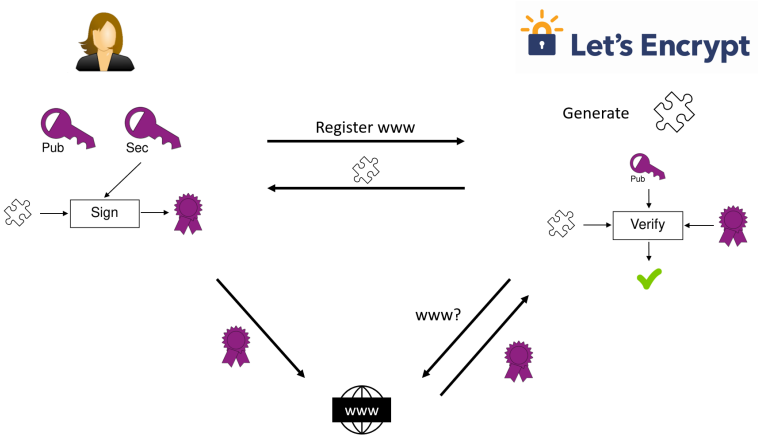
Let's Encrypt

Generate

Motivation: Let's Encrypt Protocol



Motivation: Let's Encrypt Protocol



Motivation: Let's Encrypt Attack

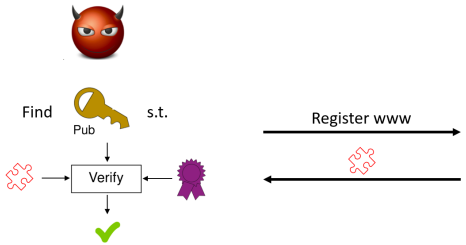
Let's Encrypt

Generate

Register www

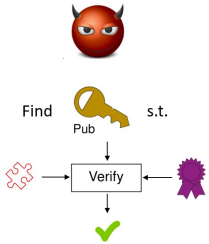
Andrew Ayer. *Duplicate Signature Key Selection Attack in Let's Encrypt*, 2015.

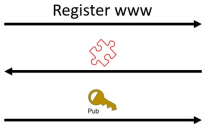
Motivation: Let's Encrypt Attack



Andrew Ayer. *Duplicate Signature Key Selection Attack in Let's Encrypt*, 2015.

Motivation: Let's Encrypt Attack





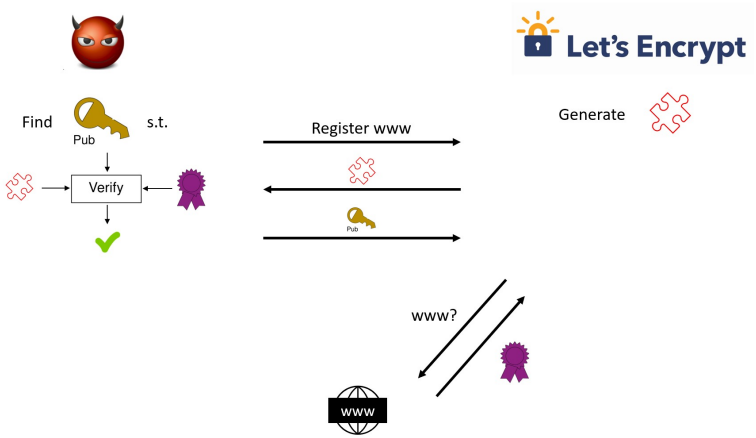
Let's Encrypt

Generate

www

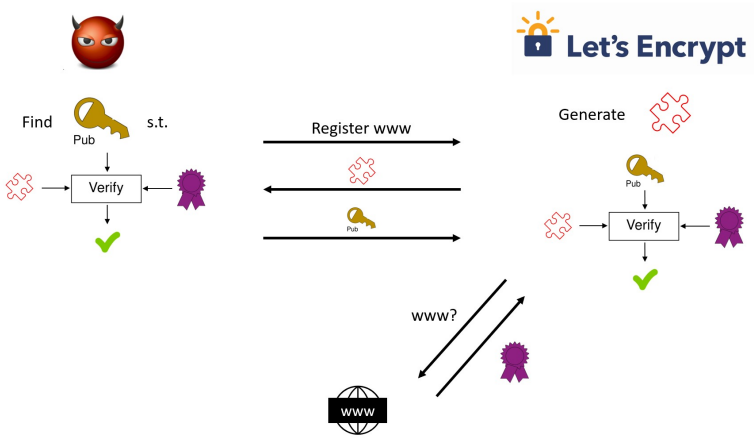
Andrew Ayer. *Duplicate Signature Key Selection Attack in Let's Encrypt*, 2015.

Motivation: Let's Encrypt Attack



Andrew Ayer. *Duplicate Signature Key Selection Attack in Let's Encrypt*, 2015.

Motivation: Let's Encrypt Attack



Andrew Ayer. *Duplicate Signature Key Selection Attack in Let's Encrypt*, 2015.

Security Features for Signatures: EUF-CMA and Beyond

Essential security notion for signatures:

Existential **U**n**F**orgeability under (adaptive) **C**hosen **M**essage **A**ttacks (EUF-CMA)

Security Features for Signatures: EUF-CMA and Beyond

Essential security notion for signatures:

Existential **U**n**F**orgeability under (adaptive) **C**hosen **M**essage **A**ttacks (EUF-CMA)

→ Limited to *one* key-pair that is *honestly generated*

Security Features for Signatures: EUF-CMA and Beyond

Essential security notion for signatures:

Existential **U**n**F**orgeability under (adaptive) **C**hosen **M**essage **A**ttacks (EUF-CMA)

→ Limited to *one* key-pair that is *honestly generated*

But: More attack scenarios led to the development of the BUFF notions

Security Features for Signatures: EUF-CMA and Beyond

Essential security notion for signatures:

Existential **U**n**F**orgeability under (adaptive) **C**hosen **M**essage **A**ttacks (EUF-CMA)

→ Limited to *one* key-pair that is *honestly generated*

But: More attack scenarios led to the development of the BUFF notions

- **E**xclusive **O**wnership (EO)
- **M**essage-**B**ound **S**ignatures (MBS)
- **N**on-**R**esignability (NR)

Security Features for Signatures: EUF-CMA and Beyond

Essential security notion for signatures:

Existential **U**n**F**orgeability under (adaptive) **C**hosen **M**essage **A**ttacks (EUF-CMA)

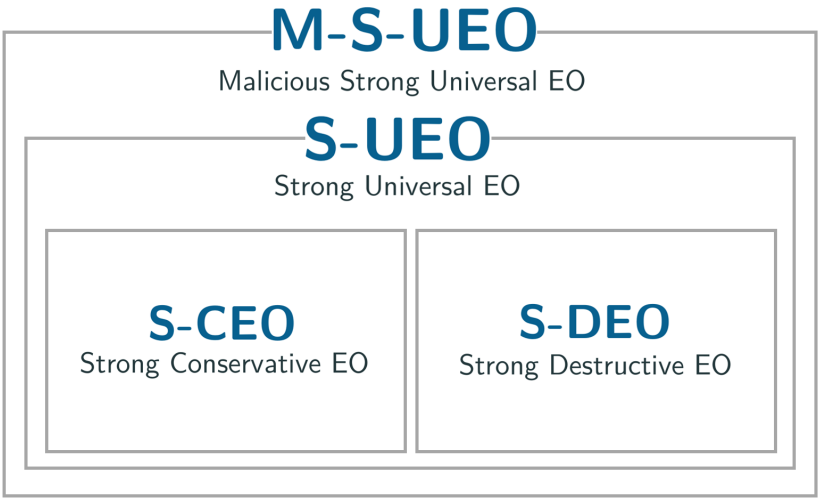
→ Limited to *one* key-pair that is *honestly generated*

But: More attack scenarios led to the development of the BUFF notions

- **E**xclusive **O**wnership (EO)
- **M**essage-**B**ound **S**ignatures (MBS)
- **N**on-**R**esignability (NR)

} → Allow *maliciously* generated keys

Exclusive Ownership: Overview of Notions



Exclusive Ownership: Definitions

Exclusive Ownership: Can a signature verify under several public keys?

S-UEO

$(\mathtt{sk}, \mathtt{pk}) \leftarrow \mathtt{KGen}()$

$(\overline{\mathtt{pk}}, \overline{\mathtt{msg}}, \overline{\mathtt{sig}}) \leftarrow \mathcal{A}^{\mathsf{Sign}(\mathtt{sk},\cdot)}(\mathtt{pk})$

Exclusive Ownership: Definitions

Exclusive Ownership: Can a signature verify under several public keys?

S-UEO

$(\mathtt{sk}, \mathtt{pk}) \leftarrow \mathtt{KGen}()$

$(\overline{\mathtt{pk}}, \overline{\mathtt{msg}}, \overline{\mathtt{sig}}) \leftarrow \mathcal{A}^{\mathsf{Sign}(\mathtt{sk},\cdot)}(\mathtt{pk})$

- $\overline{\mathtt{pk}} \neq \mathtt{pk}$

Exclusive Ownership: Definitions

Exclusive Ownership: Can a signature verify under several public keys?

S-UEO

$(\mathtt{sk}, \mathtt{pk}) \leftarrow \mathtt{KGen}()$

$(\overline{\mathtt{pk}}, \overline{\mathtt{msg}}, \overline{\mathtt{sig}}) \leftarrow \mathcal{A}^{\mathsf{Sign}(\mathtt{sk},\cdot)}(\mathtt{pk})$

- $\overline{\mathtt{pk}} \neq \mathtt{pk}$
- $\mathtt{Verify}(\overline{\mathtt{pk}}, \overline{\mathtt{msg}}, \overline{\mathtt{sig}}) = 1$

Exclusive Ownership: Definitions

Exclusive Ownership: Can a signature verify under several public keys?

S-UEO

$(\mathtt{sk}, \mathtt{pk}) \leftarrow \mathtt{KGen}()$

$(\overline{\mathtt{pk}}, \overline{\mathtt{msg}}, \overline{\mathtt{sig}}) \leftarrow \mathcal{A}^{\mathsf{Sign}(\mathtt{sk},\cdot)}(\mathtt{pk})$

- $\overline{\mathtt{pk}} \neq \mathtt{pk}$
- $\mathtt{Verify}(\overline{\mathtt{pk}}, \overline{\mathtt{msg}}, \overline{\mathtt{sig}}) = 1$
- $\overline{\mathtt{sig}}$ stems from a Sign query

slight variations give { **S-CEO** , **S-DEO** }

Exclusive Ownership: Definitions

Exclusive Ownership: Can a signature verify under several public keys?

S-UEO

$(\mathtt{sk}, \mathtt{pk}) \leftarrow \mathtt{KGen}()$

$(\overline{\mathtt{pk}}, \overline{\mathtt{msg}}, \overline{\mathtt{sig}}) \leftarrow \mathcal{A}^{\mathsf{Sign}(\mathtt{sk},\cdot)}(\mathtt{pk})$

- $\overline{\mathtt{pk}} \neq \mathtt{pk}$
- $\mathtt{Verify}(\overline{\mathtt{pk}}, \overline{\mathtt{msg}}, \overline{\mathtt{sig}}) = 1$
- $\overline{\mathtt{sig}}$ stems from a Sign query

slight variations give { **S-CEO** , **S-DEO** }

M-S-UEO

$(\mathtt{pk}, \overline{\mathtt{pk}}, \mathtt{msg}, \overline{\mathtt{msg}}, \mathtt{sig}) \leftarrow \mathcal{A}()$

Exclusive Ownership: Definitions

Exclusive Ownership: Can a signature verify under several public keys?

S-UEO

$(\mathtt{sk}, \mathtt{pk}) \leftarrow \mathtt{KGen}()$

$(\overline{\mathtt{pk}}, \overline{\mathtt{msg}}, \overline{\mathtt{sig}}) \leftarrow \mathcal{A}^{\mathsf{Sign}(\mathtt{sk},\cdot)}(\mathtt{pk})$

- $\overline{\mathtt{pk}} \neq \mathtt{pk}$
- $\mathtt{Verify}(\overline{\mathtt{pk}}, \overline{\mathtt{msg}}, \overline{\mathtt{sig}}) = 1$
- $\overline{\mathtt{sig}}$ stems from a Sign query

slight variations give { **S-CEO** , **S-DEO** }

M-S-UEO

$(\mathtt{pk}, \overline{\mathtt{pk}}, \mathtt{msg}, \overline{\mathtt{msg}}, \mathtt{sig}) \leftarrow \mathcal{A}()$

- $\overline{\mathtt{pk}} \neq \mathtt{pk}$

Exclusive Ownership: Definitions

Exclusive Ownership: Can a signature verify under several public keys?

S-UEO

$(\mathtt{sk}, \mathtt{pk}) \leftarrow \mathtt{KGen}()$

$(\overline{\mathtt{pk}}, \overline{\mathtt{msg}}, \overline{\mathtt{sig}}) \leftarrow \mathcal{A}^{\mathsf{Sign}(\mathtt{sk},\cdot)}(\mathtt{pk})$

- $\overline{\mathtt{pk}} \neq \mathtt{pk}$
- $\mathtt{Verify}(\overline{\mathtt{pk}}, \overline{\mathtt{msg}}, \overline{\mathtt{sig}}) = 1$
- $\overline{\mathtt{sig}}$ stems from a Sign query

slight variations give { **S-CEO** , **S-DEO** }

M-S-UEO

$(\mathtt{pk}, \overline{\mathtt{pk}}, \mathtt{msg}, \overline{\mathtt{msg}}, \mathtt{sig}) \leftarrow \mathcal{A}()$

- $\overline{\mathtt{pk}} \neq \mathtt{pk}$
- $\mathtt{Verify}(\mathtt{pk}, \mathtt{msg}, \mathtt{sig}) = 1$
- $\mathtt{Verify}(\overline{\mathtt{pk}}, \overline{\mathtt{msg}}, \mathtt{sig}) = 1$

The Fiat–Shamir Transform

Three-round identification

Prover: $(\mathtt{sk}, \mathtt{pk})$ **Verifier:** $\mathtt{pk}$

The Fiat–Shamir Transform

Three-round identification

Prover: $(\mathtt{sk}, \mathtt{pk})$ **Verifier:** $\mathtt{pk}$

generate commitment $\mathtt{cmt}$

$$\xrightarrow{\mathtt{cmt}}$$

The Fiat–Shamir Transform

Three-round identification

Prover: $(\mathtt{sk}, \mathtt{pk})$

Verifier: $\mathtt{pk}$

generate commitment $\mathtt{cmt}$

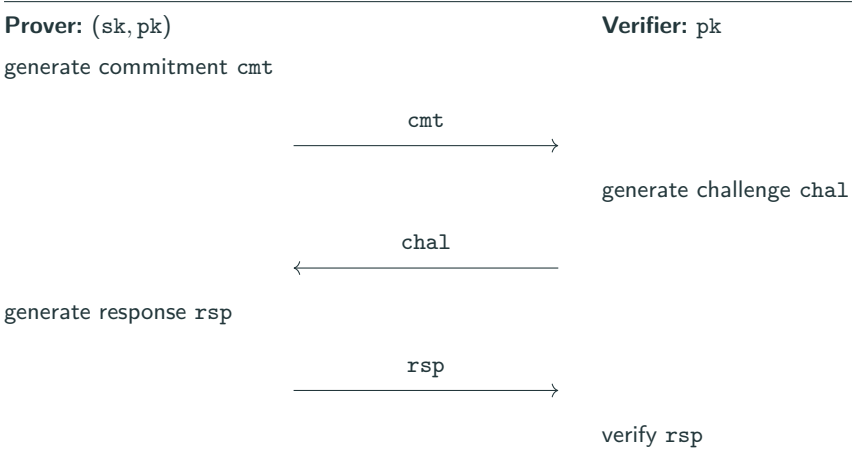
$\mathtt{cmt}$ →

generate challenge $\mathtt{chal}$

← $\mathtt{chal}$

The Fiat–Shamir Transform

Three-round identification



The Fiat–Shamir Transform

Fiat–Shamir FS

Signer: $(\mathtt{sk}, \mathtt{pk})$ **Verifier:** $\mathtt{pk}$

generate $\mathtt{cmt}$

$\mathtt{chal} = \mathtt{H}(\mathtt{pk}, \mathtt{cmt}, \mathtt{msg})$ **key pre-fixing**

generate $\mathtt{rsp}$

The Fiat–Shamir Transform

Fiat–Shamir FS

Signer: $(\mathtt{sk}, \mathtt{pk})$ **Verifier:** $\mathtt{pk}$

generate $\mathtt{cmt}$

$\mathtt{chal} = \mathtt{H}(\mathtt{pk}, \mathtt{cmt}, \mathtt{msg})$ **key pre-fixing**

generate $\mathtt{rsp}$

$\mathtt{sig} = (\mathtt{cmt}, \mathtt{chal}, \mathtt{rsp})$	**transcript variant** $\mathrm{FS}_{\mathsf{tr}}$
$\mathtt{sig} = (\mathtt{cmt}, \mathtt{rsp})$	**commitment variant** $\mathrm{FS}_{\mathsf{ct}}$
$\mathtt{sig} = (\mathtt{chal}, \mathtt{rsp})$	**challenge variant** $\mathrm{FS}_{\mathsf{ch}}$

$(\mathtt{msg}, \mathtt{sig})$ →

verify $\mathtt{sig}$

The Fiat–Shamir Transform

Fiat–Shamir FS

Signer: $(\mathtt{sk}, \mathtt{pk})$ **Verifier:** $\mathtt{pk}$

generate $\mathtt{cmt}$

$\mathtt{chal} = \mathtt{H}(\mathtt{pk}, \mathtt{cmt}, \mathtt{msg})$ **key pre-fixing**

generate $\mathtt{rsp}$

$\mathtt{sig} = (\mathtt{cmt}, \mathtt{chal}, \mathtt{rsp})$	**transcript variant** $\mathrm{FS}_{\mathrm{tr}}$
$\mathtt{sig} = (\mathtt{cmt}, \mathtt{rsp})$	**commitment variant** $\mathrm{FS}_{\mathrm{ct}}$
$\mathtt{sig} = (\mathtt{chal}, \mathtt{rsp})$	**challenge variant** $\mathrm{FS}_{\mathrm{ch}}$

$\Downarrow$

$\mathrm{FS}_{\mathrm{ch}}$ **requires commitment recovery**

$(\mathtt{msg}, \mathtt{sig})$ $\longrightarrow$

verify $\mathtt{sig}$

Achieving Exclusive Ownership

Generic transformation to achieve all BUFF notions: The BUFF transform[1]

$\mathtt{KGen}^*()$	$\mathtt{Sign}^*(\mathtt{sk}, \mathtt{msg})$	$\mathtt{Verify}^*(\mathtt{pk}, \mathtt{msg}, (\mathtt{sig}, \mathtt{h}))$
$(\mathtt{sk}, \mathtt{pk}) \leftarrow \mathtt{KGen}()$	$\mathtt{h} \leftarrow \mathtt{H}(\mathtt{msg}, \mathtt{pk})$	$\overline{\mathtt{h}} \leftarrow \mathtt{H}(\mathtt{msg}, \mathtt{pk})$
return $(\mathtt{sk}, \mathtt{pk})$	$\mathtt{sig} \leftarrow \mathtt{Sign}(\mathtt{sk}, \mathtt{h})$	$\mathtt{v} \leftarrow \mathtt{Verify}(\mathtt{pk}, \overline{\mathtt{h}}, \mathtt{sig})$
	return $(\mathtt{sig}, \mathtt{h})$	**return** $(\mathtt{v} = 1 \wedge \mathtt{h} = \overline{\mathtt{h}})$

[1] Cremers et al. *Buffing signature schemes beyond unforgeability and the case of post-quantum signatures*, S&P, 2021.

Achieving Exclusive Ownership

Generic transformation to achieve all BUFF notions: The BUFF transform[1]

$\underline{\mathtt{KGen}^*()}$	$\underline{\mathtt{Sign}^*(\mathtt{sk},\mathtt{msg})}$	$\underline{\mathtt{Verify}^*(\mathtt{pk},\mathtt{msg},(\mathtt{sig},\mathtt{h}))}$
$(\mathtt{sk},\mathtt{pk}) \leftarrow \mathtt{KGen}()$	$\mathtt{h} \leftarrow \mathtt{H}(\mathtt{msg},\mathtt{pk})$	$\overline{\mathtt{h}} \leftarrow \mathtt{H}(\mathtt{msg},\mathtt{pk})$
return $(\mathtt{sk},\mathtt{pk})$	$\mathtt{sig} \leftarrow \mathtt{Sign}(\mathtt{sk},\mathtt{h})$	$\mathtt{v} \leftarrow \mathtt{Verify}(\mathtt{pk},\overline{\mathtt{h}},\mathtt{sig})$
	return $(\mathtt{sig},\mathtt{h})$	**return** $(\mathtt{v}=1 \wedge \mathtt{h}=\overline{\mathtt{h}})$

- **Disadvantages:** 1. increase in signature size

[1] Cremers et al. *Buffing signature schemes beyond unforgeability and the case of post-quantum signatures*, S&P, 2021.

Achieving Exclusive Ownership

Generic transformation to achieve all BUFF notions: The BUFF transform[1]

$\underline{\mathtt{KGen}^*()}$	$\underline{\mathtt{Sign}^*(\mathtt{sk},\mathtt{msg})}$	$\underline{\mathtt{Verify}^*(\mathtt{pk},\mathtt{msg},(\mathtt{sig},\mathtt{h}))}$
$(\mathtt{sk},\mathtt{pk}) \leftarrow \mathtt{KGen}()$	$\mathtt{h} \leftarrow \mathtt{H}(\mathtt{msg},\mathtt{pk})$	$\overline{\mathtt{h}} \leftarrow \mathtt{H}(\mathtt{msg},\mathtt{pk})$
return $(\mathtt{sk},\mathtt{pk})$	$\mathtt{sig} \leftarrow \mathtt{Sign}(\mathtt{sk},\mathtt{h})$	$\mathtt{v} \leftarrow \mathtt{Verify}(\mathtt{pk},\overline{\mathtt{h}},\mathtt{sig})$
	return $(\mathtt{sig},\mathtt{h})$	**return** $(\mathtt{v}=1 \wedge \mathtt{h}=\overline{\mathtt{h}})$

- **Disadvantages:** 1. increase in signature size
  2. λ-bit hash-output length $\rightarrow$ $\frac{\lambda}{2}$-bit EO security

[1] Cremers et al. *Buffing signature schemes beyond unforgeability and the case of post-quantum signatures*, S&P, 2021.

Achieving Exclusive Ownership

Generic transformation to achieve all BUFF notions: The BUFF transform[1]

$\underline{\mathtt{KGen}^*()}$	$\underline{\mathtt{Sign}^*(\mathtt{sk},\mathtt{msg})}$	$\underline{\mathtt{Verify}^*(\mathtt{pk},\mathtt{msg},(\mathtt{sig},\mathtt{h}))}$
$(\mathtt{sk},\mathtt{pk}) \leftarrow \mathtt{KGen}()$	$\mathtt{h} \leftarrow \mathtt{H}(\mathtt{msg},\mathtt{pk})$	$\overline{\mathtt{h}} \leftarrow \mathtt{H}(\mathtt{msg},\mathtt{pk})$
return $(\mathtt{sk},\mathtt{pk})$	$\mathtt{sig} \leftarrow \mathtt{Sign}(\mathtt{sk},\mathtt{h})$	$\mathtt{v} \leftarrow \mathtt{Verify}(\mathtt{pk},\overline{\mathtt{h}},\mathtt{sig})$
	return $(\mathtt{sig},\mathtt{h})$	**return** $(\mathtt{v}=1 \wedge \mathtt{h}=\overline{\mathtt{h}})$

- **Disadvantages:** 1. increase in signature size
  2. λ-bit hash-output length $\rightarrow$ $\frac{\lambda}{2}$-bit EO security
- **Note:** $\mathrm{FS}_{\mathsf{tr}}$ and $\mathrm{FS}_{\mathsf{ch}}$ implicitly apply this transform!

[1] Cremers et al. *Buffing signature schemes beyond unforgeability and the case of post-quantum signatures*, S&P, 2021.

Achieving Exclusive Ownership

Generic transformation to achieve all BUFF notions: The BUFF transform[1]

$\mathtt{KGen}^*()$	$\mathtt{Sign}^*(\mathtt{sk}, \mathtt{msg})$	$\mathtt{Verify}^*(\mathtt{pk}, \mathtt{msg}, (\mathtt{sig}, \mathtt{h}))$
$(\mathtt{sk}, \mathtt{pk}) \leftarrow \mathtt{KGen}()$	$\mathtt{h} \leftarrow \mathtt{H}(\mathtt{msg}, \mathtt{pk})$	$\overline{\mathtt{h}} \leftarrow \mathtt{H}(\mathtt{msg}, \mathtt{pk})$
return $(\mathtt{sk}, \mathtt{pk})$	$\mathtt{sig} \leftarrow \mathtt{Sign}(\mathtt{sk}, \mathtt{h})$	$\mathtt{v} \leftarrow \mathtt{Verify}(\mathtt{pk}, \overline{\mathtt{h}}, \mathtt{sig})$
	return $(\mathtt{sig}, \mathtt{h})$	**return** $(\mathtt{v} = 1 \wedge \mathtt{h} = \overline{\mathtt{h}})$

- **Disadvantages:** 1. increase in signature size
  2. λ-bit hash-output length $\rightarrow$ $\frac{\lambda}{2}$-bit EO security
- **Note:** $\mathrm{FS}_{\mathsf{tr}}$ and $\mathrm{FS}_{\mathsf{ch}}$ implicitly apply this transform!
- **Can we achieve better bounds for the EO security of Fiat–Shamir signatures?**

[1] Cremers et al. *Buffing signature schemes beyond unforgeability and the case of post-quantum signatures*, S&P, 2021.

Results

Results: Overview

	M-S-UEO	S-UEO	
		Our Results	Prior Results
$\mathrm{FS}_{\mathsf{tr}}$	✗		
$\mathrm{FS}_{\mathsf{ch}}$	✗		
$\mathrm{FS}_{\mathsf{ct}}$	✗		

✗ $\leq$ 64-bit security (for 128-bit challenge length)

Results: Overview

	M-S-UEO	S-UEO	
		Our Results	Prior Results
$\mathrm{FS}_{\mathrm{tr}}$	✗	✓	
$\mathrm{FS}_{\mathrm{ch}}$	✗	✓	
$\mathrm{FS}_{\mathrm{ct}}$	✗	✗	

✗ $\leq$ 64-bit security (for 128-bit challenge length)

Results: Overview

	M-S-UEO	S-UEO	
		Our Results	Prior Results
$\mathrm{FS}_{\mathsf{tr}}$	✗	✓	$\frac{q_H^2}{2^{\lvert \mathtt{chal} \rvert}}$
$\mathrm{FS}_{\mathsf{ch}}$	✗	✓	$\frac{q_H^2}{2^{\lvert \mathtt{chal} \rvert}}$
$\mathrm{FS}_{\mathsf{ct}}$	✗	✗	

✗ $\leq$ 64-bit security (for 128-bit challenge length)

q_H number of random oracle queries

Results: Overview

	M-S-UEO	S-UEO	
		Our Results	Prior Results
$\mathrm{FS}_{\mathrm{tr}}$	✗	✓ $\frac{q_S^2}{\lvert S_{\mathtt{cmt}}\rvert} + \frac{q_H}{2^{\lvert \mathtt{chal}\rvert}}$	$\frac{q_H^2}{2^{\lvert \mathtt{chal}\rvert}}$
$\mathrm{FS}_{\mathrm{ch}}$	✗	✓	$\frac{q_H^2}{2^{\lvert \mathtt{chal}\rvert}}$
$\mathrm{FS}_{\mathrm{ct}}$	✗	✗	

✗ $\leq$ 64-bit security (for 128-bit challenge length)

q_H number of random oracle queries

q_S number of signing queries

$S_{\mathtt{cmt}}$ commitment space

Results: Overview

	M-S-UEO	S-UEO	
		Our Results	Prior Results
$\mathrm{FS}_{\mathrm{tr}}$	✗	✓ $\frac{q_S^2}{\lvert S_{\mathtt{cmt}}\rvert} + \frac{q_H}{2^{\lvert \mathtt{chal}\rvert}}$	$\frac{q_H^2}{2^{\lvert \mathtt{chal}\rvert}}$
$\mathrm{FS}_{\mathrm{ch}}$	✗	✓ $\mathbf{Adv}^{t\text{-Cmt-CR}_r} + \frac{(t-1)q_H}{2^{\lvert \mathtt{chal}\rvert}}$	$\frac{q_H^2}{2^{\lvert \mathtt{chal}\rvert}}$
$\mathrm{FS}_{\mathrm{ct}}$	✗	✗	

✗	$\leq$ 64-bit security (for 128-bit challenge length)
q_H	number of random oracle queries
q_S	number of signing queries
$S_{\mathtt{cmt}}$	commitment space
t-Cmt-CR$_r$	notion for a signature scheme built from $\mathrm{FS}_{\mathrm{ch}}$

S-UEO Proof for $\mathrm{FS}_{\mathsf{tr}}$ (Transcript Variant)

S-UEO:

$(\mathtt{sk}, \mathtt{pk}) \leftarrow \mathtt{KGen}()$
$(\overline{\mathtt{pk}}, \overline{\mathtt{msg}}, \overline{\mathtt{sig}}) \leftarrow \mathcal{A}^{\mathsf{Sign}(\mathtt{sk},\cdot)}(\mathtt{pk})$

s.t.:
- $\overline{\mathtt{pk}} \neq \mathtt{pk}$
- $\mathtt{Verify}(\overline{\mathtt{pk}}, \overline{\mathtt{msg}}, \overline{\mathtt{sig}}) = 1$
- $\overline{\mathtt{sig}}$ stems from a Sign query

S-UEO Proof for $\mathrm{FS}_{\mathsf{tr}}$ (Transcript Variant)

S-UEO:

$(\mathtt{sk}, \mathtt{pk}) \leftarrow \mathtt{KGen}()$

$(\overline{\mathtt{pk}}, \overline{\mathtt{msg}}, \overline{\mathtt{sig}}) \leftarrow \mathcal{A}^{\mathsf{Sign}(\mathtt{sk},\cdot)}(\mathtt{pk})$

s.t.:
- $\overline{\mathtt{pk}} \neq \mathtt{pk}$
- $\mathtt{Verify}(\overline{\mathtt{pk}}, \overline{\mathtt{msg}}, \overline{\mathtt{sig}}) = 1$
- $\overline{\mathtt{sig}}$ stems from a Sign query

$\mathrm{FS}_{\mathsf{tr}}.\mathtt{Verify}(\mathtt{pk}, \mathtt{msg}, \mathtt{sig})$

$(\mathtt{cmt}, \mathtt{chal}, \mathtt{rsp}) \leftarrow \mathtt{sig}$

if $\mathtt{chal} \neq \mathtt{H}(\mathtt{pk}, \mathtt{cmt}, \mathtt{msg})$

  return 0

$\mathtt{v} \leftarrow \mathtt{Rsp.V}(\mathtt{pk}, \mathtt{cmt}, \mathtt{chal}, \mathtt{rsp})$

return $\mathtt{v}$

S-UEO Proof for $\mathrm{FS}_{\mathsf{tr}}$ (Transcript Variant)

S-UEO:

$(\mathtt{sk}, \mathtt{pk}) \leftarrow \mathtt{KGen}()$
$(\overline{\mathtt{pk}}, \overline{\mathtt{msg}}, \overline{\mathtt{sig}}) \leftarrow \mathcal{A}^{\mathsf{Sign}(\mathtt{sk},\cdot)}(\mathtt{pk})$

s.t.:
- $\overline{\mathtt{pk}} \neq \mathtt{pk}$
- $\mathtt{Verify}(\overline{\mathtt{pk}}, \overline{\mathtt{msg}}, \overline{\mathtt{sig}}) = 1$
- $\overline{\mathtt{sig}}$ stems from a Sign query

If there are no commitment collisions, each random oracle query has exactly one valid target:

$$\mathbf{Adv}^{\mathsf{S\text{-}UEO}}_{\mathrm{FS}_{\mathsf{tr}}}(\mathcal{A}) \leq \frac{q_S^2}{|\mathcal{S}_{\mathtt{cmt}}|} + \frac{q_H}{2^{|\mathtt{chal}|}}$$

$\mathrm{FS}_{\mathsf{tr}}.\mathtt{Verify}(\mathtt{pk}, \mathtt{msg}, \mathtt{sig})$

$(\mathtt{cmt}, \mathtt{chal}, \mathtt{rsp}) \leftarrow \mathtt{sig}$
if $\mathtt{chal} \neq \mathtt{H}(\mathtt{pk}, \mathtt{cmt}, \mathtt{msg})$
  return 0
$\mathtt{v} \leftarrow \mathtt{Rsp.V}(\mathtt{pk}, \mathtt{cmt}, \mathtt{chal}, \mathtt{rsp})$
return $\mathtt{v}$

S-UEO Proof for $\mathrm{FS}_{\mathsf{ch}}$ (Challenge Variant)

$\underline{\mathrm{FS}_{\mathsf{ch}}.\mathtt{Verify}(\mathtt{pk}, \mathtt{msg}, \mathtt{sig})}$

$(\mathtt{chal}, \mathtt{rsp}) \leftarrow \mathtt{sig}$

$\mathtt{cmt} \leftarrow \mathtt{Cmt.R}(\mathtt{pk}, \mathtt{chal}, \mathtt{rsp})$

if $\mathtt{cmt} = \bot$

    return 0

if $\mathtt{chal} \neq \mathtt{H}(\mathtt{pk}, \mathtt{cmt}, \mathtt{msg})$

    return 0

return 1

S-UEO Proof for $\mathrm{FS}_{\mathsf{ch}}$ (Challenge Variant)

$\underline{\mathrm{FS}_{\mathsf{ch}}.\mathtt{Verify}(\mathtt{pk}, \mathtt{msg}, \mathtt{sig})}$

$(\mathtt{chal}, \mathtt{rsp}) \leftarrow \mathtt{sig}$

$\mathtt{cmt} \leftarrow \mathtt{Cmt.R}(\mathtt{pk}, \mathtt{chal}, \mathtt{rsp})$

if $\mathtt{cmt} = \bot$

  return 0

if $\mathtt{chal} \neq \mathtt{H}(\mathtt{pk}, \mathtt{cmt}, \mathtt{msg})$

  return 0

return 1

- **Sign queries:**

$$
\begin{aligned}
(\mathtt{msg}_1, \mathtt{sig}_1 &= (\mathtt{chal}_1, \mathtt{rsp}_1)),\\
(\mathtt{msg}_2, \mathtt{sig}_2 &= (\mathtt{chal}_2, \mathtt{rsp}_2)),\\
&\vdots\\
(\mathtt{msg}_{qs}, \mathtt{sig}_{qs} &= (\mathtt{chal}_{qs}, \mathtt{rsp}_{qs}))
\end{aligned}
$$

S-UEO Proof for $\mathrm{FS}_{\mathsf{ch}}$ (Challenge Variant)

$\underline{\mathrm{FS}_{\mathsf{ch}}.\mathtt{Verify}(\mathtt{pk}, \mathtt{msg}, \mathtt{sig})}$

$(\mathtt{chal}, \mathtt{rsp}) \leftarrow \mathtt{sig}$

$\mathtt{cmt} \leftarrow \mathtt{Cmt.R}(\mathtt{pk}, \mathtt{chal}, \mathtt{rsp})$

if $\mathtt{cmt} = \bot$

  return 0

if $\mathtt{chal} \neq \mathtt{H}(\mathtt{pk}, \mathtt{cmt}, \mathtt{msg})$

  return 0

return 1

- **Sign queries:**

$$(\mathtt{msg}_1, \mathtt{sig}_1 = (\mathtt{chal}_1, \mathtt{rsp}_1)),$$
$$(\mathtt{msg}_2, \mathtt{sig}_2 = (\mathtt{chal}_2, \mathtt{rsp}_2)),$$
$$\vdots$$
$$(\mathtt{msg}_{qs}, \mathtt{sig}_{qs} = (\mathtt{chal}_{qs}, \mathtt{rsp}_{qs}))$$

- **Problem case:** $\mathcal{A}$ finds $\overline{\mathtt{pk}}$ s.t.

$$\mathtt{sig}_1 \quad \mathtt{sig}_2 \quad \mathtt{sig}_3 \quad \cdots \quad \mathtt{sig}_{qs}$$
$$\Downarrow \ \mathtt{Cmt.R}(\overline{\mathtt{pk}}, \cdot)$$
$$\underbrace{\mathtt{cmt}_1 \quad \mathtt{cmt}_2 \quad \mathtt{cmt}_3 \quad \cdots \quad \mathtt{cmt}_{qs}}_{t \text{ equal commitments}}$$

S-UEO Proof for $\mathrm{FS}_{\mathsf{ch}}$ (Challenge Variant)

- tColl = event that $\mathcal{A}$ finds $\overline{\mathsf{pk}}$ s.t. at least t of the recovered commitments agree

S-UEO Proof for $\mathrm{FS}_{\mathsf{ch}}$ (Challenge Variant)

- tColl = event that $\mathcal{A}$ finds $\overline{\mathsf{pk}}$ s.t. at least t of the recovered commitments agree

$$\begin{aligned}\mathbf{Adv}^{\text{S-UEO}}_{\mathrm{FS}_{\mathsf{ch}}}(\mathcal{A}) &\leq \Pr[\text{tColl}] + \Pr[\mathcal{A} \text{ wins S-UEO} \mid \neg\text{tColl}] \\ &\leq \mathbf{Adv}^{t\text{-Cmt-CR}_r} + \frac{q_H(t-1)}{2^{|\mathtt{chal}|}}\end{aligned}$$

S-UEO Proof for $\mathrm{FS}_{\mathsf{ch}}$ (Challenge Variant)

- tColl = event that $\mathcal{A}$ finds $\overline{\mathtt{pk}}$ s.t. at least t of the recovered commitments agree

$$\begin{aligned}\mathbf{Adv}^{\text{S-UEO}}_{\mathrm{FS}_{\mathsf{ch}}}(\mathcal{A}) &\leq \Pr[\text{tColl}] + \Pr[\mathcal{A} \text{ wins S-UEO} \mid \neg\text{tColl}] \\ &\leq \mathbf{Adv}^{t\text{-Cmt-CR}_r} + \frac{q_H(t-1)}{2^{|\mathtt{chal}|}}\end{aligned}$$

- Game t-Cmt-CR$_r$:

$(\mathtt{sk}, \mathtt{pk}) \leftarrow \mathtt{KGen}()$
$(\overline{\mathtt{pk}}, (\mathtt{chal}_i, \mathtt{rsp}_i)_{i=1,\ldots,t}) \leftarrow \mathcal{A}^{\mathsf{Sign}(\mathtt{sk},\cdot)}(\mathtt{pk})$

s.t.:
- $\overline{\mathtt{pk}} \neq \mathtt{pk}$
- $(\mathtt{chal}_i, \mathtt{rsp}_i)$ stem from Sign queries
- all recovered commitments agree

Application

Application: Overview

	t	S-UEO Security (in bits)		Our Bound
		Prior Results	Our Results	
Schnorr[1]	6	64	≈ 125	$\binom{q_S}{6}\frac{1}{2^{512}} + \frac{5q_H}{2^{128}}$
ML-DSA II	2	128	≈ 256	$\binom{q_S}{2}\frac{q_H}{2^{1068}} + \frac{q_H}{2^{256}}$
SQIsign I	2	64	≈ 128	$\binom{q_S}{2}\frac{1}{2^{256}} + \frac{q_H}{2^{128}}$
CSI-FiSh[1]	2	64	≈ 128	$\binom{q_S}{2}\frac{1}{N^{127}} + \frac{q_H}{2^{128}}$
LESS I[1]	/	64	≈ 128	$\frac{q_S^2}{2^{257}} + \frac{q_H}{2^{128}}$

[1]When deploying key pre-fixing.

Conclusion

Conclusion

	S-UEO Security	
$\mathrm{FS}_{\mathrm{tr}}$	✓	$\frac{q_S^2}{\lvert S_{\mathtt{cmt}}\rvert} + \frac{q_H}{2^{\lvert \mathtt{chal}\rvert}}$
$\mathrm{FS}_{\mathrm{ch}}$	✓	$\mathbf{Adv}^{t\text{-Cmt-CR}_r} + \frac{(t-1)q_H}{2^{\lvert \mathtt{chal}\rvert}}$
$\mathrm{FS}_{\mathrm{ct}}$	✗	

	S-UEO Security
Schnorr	$\binom{q_S}{6}\frac{1}{2^{512}} + \frac{5q_H}{2^{128}}$
ML-DSA II	$\binom{q_S}{2}\frac{q_H}{2^{1068}} + \frac{q_H}{2^{256}}$
SQIsign I	$\binom{q_S}{2}\frac{1}{2^{256}} + \frac{q_H}{2^{128}}$
CSI-FiSh	$\binom{q_S}{2}\frac{1}{N^{127}} + \frac{q_H}{2^{128}}$
LESS I	$\frac{q_S^2}{2^{257}} + \frac{q_H}{2^{128}}$

Conclusion

	S-UEO Security	
$\mathsf{FS}_{\mathsf{tr}}$	✓	$\frac{q_S^2}{\lvert S_{\mathtt{cmt}}\rvert} + \frac{q_H}{2^{\lvert \mathtt{chal}\rvert}}$
$\mathsf{FS}_{\mathsf{ch}}$	✓	$\mathbf{Adv}^{t\text{-Cmt-CR}_r} + \frac{(t-1)q_H}{2^{\lvert \mathtt{chal}\rvert}}$
$\mathsf{FS}_{\mathsf{ct}}$	✗	

	S-UEO Security
Schnorr	$\binom{q_S}{6}\frac{1}{2^{512}} + \frac{5q_H}{2^{128}}$
ML-DSA II	$\binom{q_S}{2}\frac{q_H}{2^{1068}} + \frac{q_H}{2^{256}}$
SQIsign I	$\binom{q_S}{2}\frac{1}{2^{256}} + \frac{q_H}{2^{128}}$
CSI-FiSh	$\binom{q_S}{2}\frac{1}{N^{127}} + \frac{q_H}{2^{128}}$
LESS I	$\frac{q_S^2}{2^{257}} + \frac{q_H}{2^{128}}$

Questions?

Meyer, Struck, Weishäupl:
Exclusive Ownership of Fiat–Shamir Signatures: ML-DSA, SQIsign, LESS, and More
https://ia.cr/2025/900

Contact: maximiliane.weishaeupl@ur.de