BUFFing FALCON without Increasing the Signature Size

Samed Düzlü[1] Rune Fiedler[2] Marc Fischlin[2]

Presentation for the *SAC Workshop* in Montréal, Québec
August, 28th 2024

[1]University of Regensburg [2]TU Darmstadt

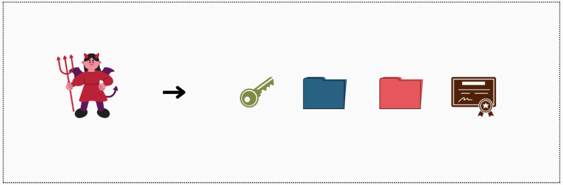
TECHNISCHE UNIVERSITÄT DARMSTADT

Beyond UnForgeability Features

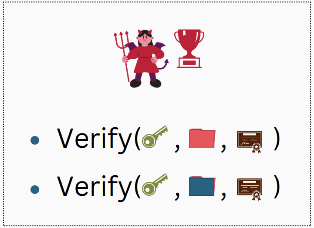
Security of Signature Schemes

- Existential UnForgeability (EUF) is the standard security assumption
  - *no adversary can in a reasonable amount of time, create signatures to new messages*
- In practice, signatures may be used in ways that EUF is **not sufficient**
  - An adversary may use maliciously generated public keys
- **B**eyond **U**n**F**orgeability **F**eatures (BUFF) formalize this defect
  - Message-Bound Signatures (MBS)
  - Exclusive Ownership (EO)
  - Non-Resignability (NR)

Message-Bound Signatures (MBS)

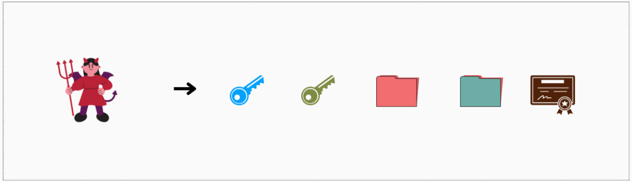


An adversary produces a public key, two distinct messages, and a signature.

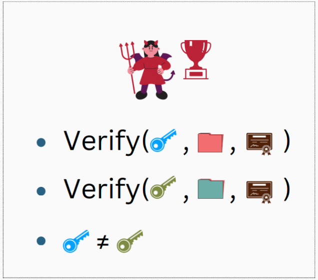


The adversary wins if both messages verify.

Malicious-Strong-Universal Exclusive Ownership (M-S-UEO)

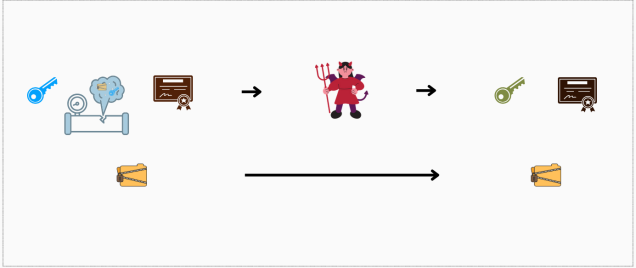


An adversary outputs two public keys, two messages, and one signature.

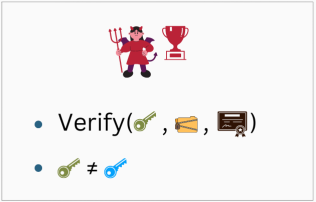


The adversary wins if two respective verifications hold and the public keys are distinct.

Non-Resignability (NR)



An adversary sees a public key and a signature, but not the message itself.
Additionally, the adversary gets *auxiliary information* about the message.



The adversary wins if the public key is *new* and the verification with the unknown message holds.

(Why) should we care about anything Beyond UnForgeability?

- Requiring BUFF security helps secure protocol designs
- NIST acknowledges the benefit of BUFF security
  - NIST declares BUFF as desirable features for the additional signatures round.

FALCON's **BUFF security**

FALCON has been analyzed in [CDFFJ21] regarding the BUFF security:

Scheme	M-S-UEO	MBS	NR	Size (B)
FALCON	✗	✓	✗	1280

The BUFF Transform

Generic transformation to achieve all BUFF notions: The BUFF transform [CDFFJ21]

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

Figure: $(\mathtt{H}, \Sigma = (\mathtt{KGen}, \mathtt{Sign}, \mathtt{Verify})) \xrightarrow{\textsc{Buff}} \textsc{Buff}[\mathtt{H}, \Sigma] = (\mathtt{KGen}^*, \mathtt{Sign}^*, \mathtt{Verify}^*)$

$\Rightarrow$ Increased signature size by a hash digest h

$\Rightarrow$ Efficiency overhead due to hashing of $\mathtt{msg}, \mathtt{pk}$

BUFFed FALCON

Using the generic BUFF transform, FALCON achieves BUFF security:

Scheme	M-S-UEO	MBS	NR	Size (B)	Increase
FALCON	✗	✓	✗	1280	-
FALCON-BUFF	✓	✓	✓	1344	5%

BUFFed FALCON

Using the generic BUFF transform, FALCON achieves BUFF security:

Scheme	Sig. target	Sig. format	M-S-UEO	MBS	NR	Size (B)	Increase
FALCON	$\mathsf{H}(r\|m)$	(r, s)	✗	✓	✗	1280	-
FALCON-BUFF	$\mathsf{H}(r\|\mathrm{pk}\|m)$	$(r, s, \mathsf{H}(r\|\mathrm{pk}\|m))$	✓	✓	✓	1344	5%

BUFFed FALCON

- The FALCON Team announced that they would incorporate the BUFF transform in future versions
- Increasing the signature size by a hash digest is the main disadvantage

Research Question

Is it possible to ensure FALCON*'s BUFF security without increasing the signature size?*

BUFF Transform vs. PS-3 Transform

The more lightweight $\mathrm{PS\text{-}3}$ transform [PS05] in comparison with the ~~BUFF~~ transform

$\texttt{KGen}^*()$	$\texttt{Sign}^*(\texttt{sk}, \texttt{msg})$	$\texttt{Verify}^*(\texttt{pk}, \texttt{msg}, (\texttt{sig}, \cancel{\texttt{h}}))$
$(\texttt{sk}, \texttt{pk}) \leftarrow \texttt{KGen}()$	$\texttt{h} \leftarrow \texttt{H}(\texttt{msg}, \texttt{pk})$	$\bar{\texttt{h}} \leftarrow \texttt{H}(\texttt{msg}, \texttt{pk})$
return $(\texttt{sk}, \texttt{pk})$	$\texttt{sig} \leftarrow \texttt{Sign}(\texttt{sk}, \texttt{h})$	$\texttt{v} \leftarrow \texttt{Verify}(\texttt{pk}, \bar{\texttt{h}}, \texttt{sig})$
	return $(\texttt{sig}, \cancel{\texttt{h}})$	**return** $(\texttt{v} = 1 \land \cancel{\texttt{h} = \bar{\texttt{h}}})$

Figure: $(\texttt{H}, \Sigma = (\texttt{KGen}, \texttt{Sign}, \texttt{Verify})) \xrightarrow{\mathrm{PS\text{-}3}} \mathrm{PS\text{-}3}[\texttt{H}, \Sigma] = (\texttt{KGen}^*, \texttt{Sign}^*, \texttt{Verify}^*)$

$\Rightarrow$ ~~Increased signature size by a hash digest h~~

$\Rightarrow$ Efficiency overhead due to hashing of $\texttt{msg}, \texttt{pk}$

Generically, $\mathrm{PS\text{-}3}$ **transform does not ensure BUFF security**

FALCON-PS-3's **BUFF security – Main Result**

For FALCON, the PS-3 transform *does* ensure BUFF security:

Scheme	Sig. target	Sig. format	M-S-UEO	MBS	NR	Size (B)	Increase
FALCON	$\mathsf{H}(r\|m)$	(r, s)	✗	✓	✗	1280	-
FALCON-BUFF	$\mathsf{H}(r\|\mathrm{pk}\|m)$	$(r, s, \mathsf{H}(r\|\mathrm{pk}\|m))$	✓	✓	✓	1344	5%
FALCON-PS-3	$\mathsf{H}(r\|\mathrm{pk}\|m)$	(r, s)	✓	✓	✓	1280	0%

Description of FALCON

FALCON **Setup**

FALCON makes use of NTRU lattices and the GPV framework

- Two parameter sets for $n = 512$ and 1024, respectively
- ϕ an integer polynomial of degree n
- q an integer, $q = 12\,289$
- Elements are in $\mathbb{Z}[x]/(q, \phi)$
- Bound β
  - $\lfloor \beta \rfloor^2 = 34\,034\,726$ and $70\,265\,242$, respectively

FALCON **Key Pairs**

- Public key $\mathtt{pk} = h \in \mathbb{Z}[x]/(q, \phi)$
- Idea of the secret key: a (kind of) trapdoor of multiplication with h
- Secret key $\mathtt{sk} = (B, T)$, where
  - $B = \begin{bmatrix} g & -f \\ G & -F \end{bmatrix}$, with $f, g \in \mathbb{Z}[x]/(q, \phi)$ short and $h = gf^{-1}$
  - T is a FalconTree

FALCON **Signature**

Given a public key $\texttt{pk} = h$ and a message m, a signature $\texttt{sig}$ is a pair (r, s), where

- r is a random salt
- $s \in \mathbb{Z}[x]/(q, \phi)$, such that

$$\|(\mathsf{H}(r\|m) - hs, s)\|^2 \leq \lfloor \beta \rfloor^2 \qquad // \text{ FALCON}$$

$$\|(\mathsf{H}(r\|h\|m) - hs, s)\|^2 \leq \lfloor \beta \rfloor^2 \qquad // \text{ FALCON-PS-3}$$

Details of the signing procedure is not important for BUFF security

FALCON **Verification**

Given a public key $\texttt{pk} = h$, a message m, and a signature $\texttt{sig} = (r, s)$, the verification

- Computes $c = \begin{cases} \mathsf{H}(r \| m) & \text{// FALCON} \\ \mathsf{H}(r \| h \| m) & \text{// FALCON-PS-3} \end{cases}$
- Checks, if $\|(c - hs, s)\|^2 \leq \lfloor \beta \rfloor^2$ holds

FALCON **Sign and Verifiy in Pseudocode**

$\mathtt{Sign}(\mathrm{sk}, \mathrm{pk}, m)$

$h \leftarrow \mathrm{pk}$

$(\hat{\mathbf{B}}, T) \leftarrow \mathrm{sk}$

$r \leftarrow_{\$} \{0,1\}^{320}$

$c \leftarrow \mathsf{H}(r \| m)$ // FALCON

$c \leftarrow \mathsf{H}(r \| h \| m)$ // FALCON-PS-3

$\mathbf{t} \leftarrow (\mathsf{FFT}(c), \mathsf{FFT}(0)) \cdot \hat{\mathbf{B}}^{-1}$

$\mathbf{s} \leftarrow_{\$} \mathsf{FFSampling}(\mathbf{t}, T, \lfloor \beta^2 \rfloor)$

$(s_1, s_2) \leftarrow \mathsf{FFT}^{-1}(\mathbf{s})$

$s \leftarrow \mathtt{Compress}(s_2)$

$\mathtt{sig} \leftarrow (r, s)$

return $\mathtt{sig}$

$\mathtt{Verify}(\mathrm{pk}, m, \mathtt{sig})$

$h \leftarrow \mathrm{pk}$

$(r, s) \leftarrow \mathtt{sig}$

$c \leftarrow \mathsf{H}(r \| m)$ // FALCON

$c \leftarrow \mathsf{H}(r \| h \| m)$ // FALCON-PS-3

$s_2 \leftarrow \mathtt{Decompress}(s)$

$s_1 \leftarrow c - s_2 h$

return $\left[\|(s_1, s_2)\|^2 \leq \lfloor \beta^2 \rfloor \right]$

BUFF Security of FALCON-PS-3

M-S-UEO of FALCON-PS-3 – 1

Suppose $n = 2^k$.

Theorem

Assuming H *is a random oracle, for any adversary* $\mathcal{A}$ *against* M-S-UEO *security of* FALCON-PS-3 *that makes* q_{H} *queries to the random oracle, the advantage satisfies*

$$\mathbf{Adv}^{\text{M-S-UEO}}_{\text{FALCON-PS-3},\mathcal{A}} \leq (q_{\mathsf{H}} + 2)^2 \cdot 2^{(5-k)\frac{n}{2}}.$$

For the two parameter sets of FALCON, *the bounds are thus* $(q_{\mathsf{H}} + 2)^2 \cdot 2^{-1024}$ *for security level I and* $(q_{\mathsf{H}} + 2)^2 \cdot 2^{-2560}$ *for security level V, respectively.*

Further, we show that FALCON-PS-3 satisfies S-UEO in the QROM

M-S-UEO of FALCON-PS-3 – 2

An adversary is supposed to find

- two distinct public keys $\texttt{pk}_1 = h_1$ and $\texttt{pk}_2 = h_2$
- two messages m_1 and m_2
- and a signature $\texttt{sig} = (r, s)$

such that, setting $c_1 = \mathsf{H}(r \| h_1 \| m_1)$ and $c_2 = \mathsf{H}(r \| h_2 \| m_2)$, both verifications hold, i.e.,

$$\|(c_1 - h_1 s, s)\|^2 \leq \lfloor \beta \rfloor^2 \qquad \text{and} \qquad \|(c_2 - h_2 s, s)\|^2 \leq \lfloor \beta \rfloor^2$$

M-S-UEO of FALCON-PS-3 – 3

Idea. Any attack is required to output h_1, h_2 before c_1, c_2 are determined.

- We assume that H is a random oracle
- c_1 and c_2 are uniformly sampled after h_1 and h_2 are chosen

It suffices to check:

For any $h_1, h_2 \in \mathbb{Z}[x]/(q, \phi)$, the probability that for uniformly chosen c_1, c_2, there exists s such that

- $\|c_1 - h_1 s\|^2 \leq \lfloor \beta \rfloor^2$
- $\|c_2 - h_2 s\|^2 \leq \lfloor \beta \rfloor^2$

holds, is negligible.

Interlude on Lattices

For h_1, h_2, we define $\Lambda_{h_1,h_2} := \{(h_1 z, h_2 z) \mid z \in \mathbb{Z}[x]/(q,\phi)\}$.

With $n = 2^k$, we have

Proposition

For uniform $c = (c_1, c_2) \in (\mathbb{Z}[x]/(q,\phi))^2$, it holds

$$\mathbb{P}(\mathrm{dist}(c, \Lambda_{h_1,h_2}) \leq \sqrt{2}\beta) < 2^{(5-k)\frac{n}{2}}$$

In the application, $k = 9$ or $k = 10$, hence the bound is $2^{-1\,024}$ and $2^{-2\,560}$

Essentially, this follows from the fact that Λ_{h_1,h_2} has rank n, but c is in rank $2n$

M-S-UEO of FALCON-PS-3 – 4

- The bound is independent of the choice of h_1, h_2
- An adversary making q_{H} queries can construct $O(q_{\mathrm{H}}^2)$ pairs $c = (c_1, c_2)$ with the goal to achieve $\mathrm{dist}(c, \Lambda_{h_1,h_2}) < \sqrt{2}\beta$
- For each, this bound is satisfied with probability less than $2^{(5-k)\frac{n}{2}}$

MBS and NR of FALCON-PS-3

- MBS security of FALCON-PS-3 is inherited from FALCON
- Can be shown directly for FALCON-PS-3 with the lattice techniques presented here
- NR security proceeds in two steps
  - First, a formal reduction via game hops to assume that the message is never queried to the hash oracle
  - Second, a FALCON specific lattice reduction similar to the presented one

Takeaways – Questions

Scheme	Sig. target	Sig. format	M-S-UEO	MBS	NR	Size (B)
FALCON	$\mathsf{H}(r\|m)$	(r, s)	✗	✓	✗	1280
FALCON-BUFF	$\mathsf{H}(r\|\mathrm{pk}\|m)$	$(r, s, \mathsf{H}(r\|\mathrm{pk}\|m))$	✓	✓	✓	1344
FALCON-PS-3	$\mathsf{H}(r\|\mathrm{pk}\|m)$	(r, s)	✓	✓	✓	1280

Questions?

Contact: samed.duzlu@ur.de

BUFFing FALCON *without Increasing the Signature Size*

Düzlü, Fiedler, Fischlin

https://ia.cr/2024/710

Use-cases of BUFF notions

MBS Repute signed messages

EO Draft of Let's Encrypt certification protocol

NR DRKey protocol

- Static part of message is publicly known (*auxiliary data*), the remaining part is unknown (*entropy*)

M-S-UEO Insecurity of FALCON

- Suppose $c = \mathsf{H}(r\|m)$
- and $\texttt{pk} = h$ and $\texttt{sig} = (r, s)$ are valid public key and signature for a message m
- Then a new $h' \neq h$ can be found:
  - if s is not invertible, there is $\alpha \neq 0$ with $\alpha s = 0$; then set $h' = h + \alpha$
  - if s is invertible, set $h = cs^{-1}$

NR Insecurity of FALCON

- Suppose $c = \mathrm{H}(r \| m)$
- Given $\mathtt{pk} = h$ and $\mathtt{sig} = (r, s)$, without knowing m, we know c is close to hs
- Then a new $h' \neq h$ can be found:
  - if s is not invertible, there is $\alpha \neq 0$ with $\alpha s = 0$; then set $h' = h + \alpha$
  - otherwise, pick a short s' which is invertible, set $h' = hss'^{-1}$