Blinding Post-Quantum Hash-and-Sign Signatures

Charles Bouillaguet, Thibauld Feneuil, Jules Maire,
Matthieu Rivain, Julia Sauvage, Damien Vergnaud

May 19, 2026

IEEE S&P 2026, San Francisco

Sorbonne Université, France
CryptoExperts, France
ENS - PSL, France

Source: `https://eprint.iacr.org/2025/895`

Blind Signature Schemes

The Authority

Authority's private key

The User

Message to sign

Blind Signature Schemes

The Authority

Authority's private key

The User

Message to sign

Commitment of the message

① The User **commits** the message to sign.

Blind Signature Schemes

The Authority

Authority's private key

The User

Message to sign

① The User **commits** the message to sign.

Commitment of the message

② Produce signing material using the private key

Blind Signature Schemes

The Authority

Authority's private key

The User

Message to sign

① The User **commits** the message to sign.

Commitment of the message

② Produce signing material using the private key

③ Deduce a **valid signature** for the message

Message **signed**

Blind Signature Schemes

The Authority

Authority's private key

The User

Message to sign

① The User **commits** the message to sign.

Commitment of the message

② Produce signing material using the private key

③ Deduce a **valid signature** for the message

Message **signed**

Unforgeability: After interacting with the authority to obtain signatures on a set of messages, the user should remain unable to forge a valid signature on any new message by itself.

Blind Signature Schemes

The Authority

Authority's private key

The User

Message to sign

① The User **commits** the message to sign.

Commitment of the message

② Produce signing material using the private key

③ Deduce a **valid signature** for the message

Message **signed**

Blindness: The authority must be unable to learn either the content of the message being signed or the resulting signature.

Blind Signature Schemes

The Authority

Authority's private key

The User

Message to sign

① The User **commits** the message to sign.

Commitment of the message

② Produce signing material using the private key

③ Deduce a **valid signature** for the message

Message **signed**

It has applications in many **privacy-enhancing technologies** (PETs), such as electronic voting systems.

The Fischlin Framework (simplified)

[Fis06] Fischlin. Round-optimal composable blind signatures in the common referee string model. CRYPTO 2006.

The Authority

Authority's private key sk

The User

Message m to sign

① $\text{com} \leftarrow \text{Commit}(m; r)$

com

② $\sigma \leftarrow \text{Sign}(\text{sk}, \text{com})$

σ

③ Generate a proof π that he know σ and r such that

$\text{Verif}(\text{pk}, \sigma, \text{Commit}(\text{m}; \text{r})) = 1.$

The final signature is π.

The Fischlin Framework (simplified)

[Fis06] Fischlin. Round-optimal composable blind signatures in the common referee string model. CRYPTO 2006.

The Authority

Authority's private key sk

The User

Message m to sign

① $\text{com} \leftarrow \text{Commit}(m; r)$

com

② $\sigma \leftarrow \text{Sign}(\text{sk}, \text{com})$

σ

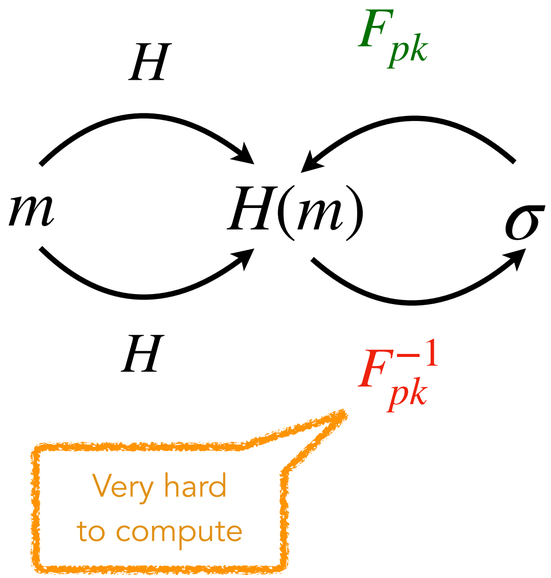
③ Generate a proof π that he know σ and r such that

$\text{Verif}(\text{pk}, \sigma, \text{Commit}(\text{m}; \text{r})) = 1.$

The final signature is π.

The overall performance (proof size, running times) will highly depend on how complex is the verification algorithm.

Post-Quantum Hash-and-sign signatures



Examples:

- Falcon / FN-DSA (lattice)
- Wave, Miranda (code)
- UOV, Mayo (multivariate)

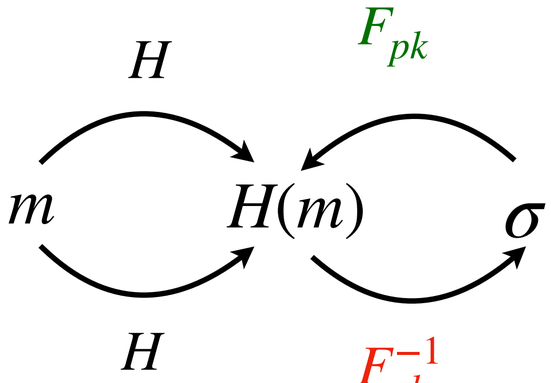
Proving knowledge of signature:

Denoting $h' := H(m)$,

The User proves that he knows σ and h' such that

$$h' = H(m) \quad \text{and} \quad h' = \mathcal{G}_{pk}(\sigma)$$

Post-Quantum Hash-and-sign signatures



Very hard to compute

Easy to prove, as it is an algebraic relation

Examples:

- Falcon / FN-DSA (lattice)
- Wave, Miranda (code)
- UOV, Mayo (multivariate)

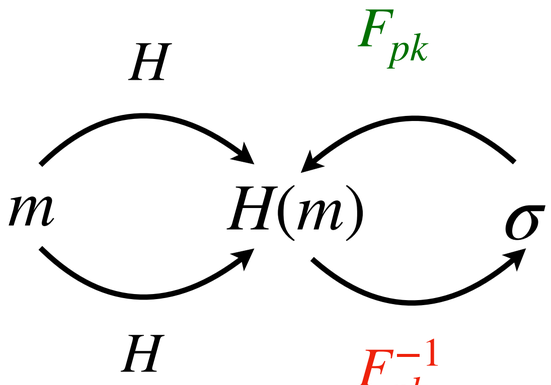
Proving knowledge of signature:

Denoting $h' := H(m)$,

The User proves that he knows σ and h' such that

$h' = H(m)$ and $h' = \mathcal{G}_{pk}(\sigma)$

Post-Quantum Hash-and-sign signatures



Very hard to compute

More ***complex/expensive*** to prove

Examples:

- Falcon / FN-DSA (lattice)
- Wave, Miranda (code)
- UOV, Mayo (multivariate)

Proving knowledge of signature:

Denoting $h' := H(m)$,

The User proves that he knows σ and h' such that

$h' = H(m)$ and $h' = \mathcal{G}_{pk}(\sigma)$

Prior work

[BLNS23] Beullens, Lyubashevsky, Nguyen, Seiler. Lattice-based blind signatures: Short, efficient, and round-optimal. CCS 2023.

> [BLNS23] succeeds in removing the need to prove correctness of the hash computation within the proved statement.
>
> $$\begin{aligned} \text{com} &\leftarrow \text{Commit}(m; r) \\ &:= Br + H(m, H(r)) \end{aligned}$$
>
> with r small and B a public matrix, and by removing the hashing in the signing routine.

Drawbacks:

- The security of the construction relies on **lattice assumptions**, and can ***not*** be generalized with other types of security assumptions.
- The security of the scheme can not be reduced to the security of a well-known hash-and-sign signature scheme.
- It still produces ***quite large*** blind signatures (22 kilobytes).

Contributions

Based on the ideas of [BLNS23], we propose a **new construction for blind signatures** that offers several advantages over [BLNS23]:

- It enables the transformation of ***any*** post-quantum hash-and-sign signature scheme into a blind signature. It relies on a commit-and-prove (CP) scheme.

$$\begin{aligned} \mathrm{com}_0 &:= \mathrm{CP}.\mathrm{Commit}(r;\rho) \\ \mathrm{com} &:= r + H(m, \mathrm{com}_0) \end{aligned}$$

  The user needs to send a SNARK proving that com has been well-built (also true in [BLNS23]).

- The security of the resulting blind signature can be ***reduced to that of the original signature scheme***, without introducing additional assumptions.

- It yields ***efficient multivariate blind signatures*** ($\approx 5 - 8$ KB), when applied to UOV-like signature schemes.

Comparison - Multivariate Blind signatures

Comparison with more recent works

	Same security as the original scheme	*Signature Size*	*Communication Size*
Our Work	Yes	5-8 KB	Few MB
[BFMR+25]	No	7 KB	< 1 KB
[BBBMR26] Conservative	Yes	24 KB	< 1 KB
[BBBMR26] Non-conservative	No	6-7 KB	< 1 KB

Based on the trade-offs targeting short signatures

[BFMR+25] Bouillaguet, Feneuil, Maire, Rivain, Sauvage, Vergnaud. Multivariate Commitment and Signatures with Efficient Protocols. ePrint 2025/2035.

[BBBMR26] Baum, Beckmann, Beullens, Mukherjee, Rechberger. Concretely Efficient Blind Signatures Based on VOLE-in-the-Head Proofs and the MAYO Trapdoor. ePrint 2026/109.

Comparison - Multivariate Blind signatures

Comparison with more recent works

	Same security as the original scheme	*Signature Size*	*Communication Size*
Our Work	Yes	5-8 KB	Few MB
[BFMR+25]	No	7 KB	< 1 KB
[BBBMR26] Conservative	Yes	24 KB	< 1 KB
[BBBMR26] Non-conservative	No	6-7 KB	< 1 KB

Based on the trade-offs targeting short signatures

Our work enables the construction of short blind signatures without introducing any additional security assumptions.

Comparison - Multivariate Blind signatures

Comparison with more recent works

	Same security as the original scheme	*Signature Size*	*Communication Size*
Our Work	Yes	5-8 KB	Few MB
[BFMR+25]	No	7 KB	< 1 KB
[BBBMR26] Conservative	Yes	24 KB	< 1 KB
[BBBMR26] Non-conservative	No	6-7 KB	< 1 KB

Based on the trade-offs targeting short signatures

The proved statement must include the correctness of the hash operation, which results in a **large** signature.

Comparison - Multivariate Blind signatures

Comparison with more recent works

	Same security as the original scheme	*Signature Size*	*Communication Size*
Our Work	Yes	5-8 KB	Few MB
[BFMR+25]	No	7 KB	< 1 KB
[BBBMR26] Conservative	Yes	24 KB	< 1 KB
[BBBMR26] Non-conservative	No	6-7 KB	< 1 KB

Based on the trade-offs targeting short signatures

The trade-off is a **substantial** communication overhead between the user and the authority, caused by the use of a generic SNARK to prove that the user's commitment is correctly constructed.

Note: since the literature of SNARK is evolving fast, we might expect improve on that point.

Comparison - Multivariate Blind signatures

Comparison with more recent works

	Same security as the original scheme	*Signature Size*	*Communication Size*
Our Work	Yes	5-8 KB	Few MB
[BFMR+25]	No	7 KB	< 1 KB
[BBBMR26] Conservative	Yes	24 KB	< 1 KB
[BBBMR26] Non-conservative	No	6-7 KB	< 1 KB

Based on the trade-offs targeting short signatures

Need to be stored
Will be used in many protocols

Do not need to stored
Can be deleted after the protocol

Comparison - Multivariate Blind signatures

Comparison with more recent works

	Same security as the original scheme	*Signature Size*	*Communication Size*
Our Work	Yes	5-8 KB	Few MB
[BFMR+25]	No	7 KB	< 1 KB
[BBBMR26] Conservative	Yes	24 KB	< 1 KB
[BBBMR26] Non-conservative	No	6-7 KB	< 1 KB

Based on the trade-offs targeting short signatures

Thank you for your attention.