ATMACA

Lattice-Based Threshold Signing for FALCON

Metin BEKTAŞ

TÜBİTAK BİLGEM
Joint work with: Erdem ALKIM, Erem ERSOY, Muhammed Said GÜNDOĞAN

NIST Threshold Call Preview Talks, 2026

Presented on 2026-10-06

Introduction: FALCON

FALCON [FHK+20][1]: $\mathcal{R} = \mathbb{Z}[X]/(X^d + 1)$, $q = 12289$, $d \in \{512, 1024\}$.

Keys

- Trapdoor $(f, g, F, G) \in \mathcal{R}^4$, $fG - gF = q$; public $h = gf^{-1} \bmod q \in R_q$.
- Short basis $B = (\mathbf{b}_1, \mathbf{b}_2)$ of $\Lambda_h = \{(a, b) \in \mathcal{R}^2 : a + bh \equiv 0 \pmod q\}$.

Verify (salt, s_2) on M

- $c \leftarrow \mathsf{HashToPoint}(\mathsf{salt}, M)$, $s_1 \leftarrow c - s_2 h \bmod q$.
- Accept iff $\|s_1\|_2^2 + \|s_2\|_2^2 \leq \lfloor \beta^2 \rfloor$.

Sign M

- Fresh 320-bit salt; $\mathbf{c} = (c, 0)$, $c = \mathsf{HashToPoint}(\mathsf{salt}, M) \in R_q$.
- $\mathbf{v} \sim D_{\Lambda_h, \mathbf{c}, \sigma}$ using the trapdoor; $(s_1, s_2) = \mathbf{c} - \mathbf{v}$.
- Output salt and the encoded/compressed signature

[1] [FHK+20] Pierre-Alain Fouque, Jeffrey Hoffstein, Paul Kirchner, Vadim Lyubashevsky, Thomas Pornin, Thomas Prest, Thomas Ricosset, Gregor Seiler, William Whyte, and Zhenfei Zhang. Falcon: Fast-fourier lattice-based compact signatures over NTRU, specification v1.2, 2020. NIST PQC submission.

Motivation for threshold FALCON

Why

- t-of-n signing: no single party ever holds the key after key generation; fewer than t parties learn nothing, any t can sign.
- Any application that adopts FALCON can later move to the threshold version if it ever needs thresholdization.

Why it is hard

- The arithmetic is real-valued.
- ffSampling requires d sequential steps inside MPC.

Threshold FALCON paper [GEP+26][1]

- First threshold protocol whose signatures pass the unmodified FALCON verifier.
- Klein (GPV) sampler inside MPC: the MPC discrete-Gaussian sampler of Wei et al. (CCS 2023) with private centres *and* widths.
- Rényi analysis of the Klein sampler in fixed point: 73 bits of precision suffice.

What we change

Klein walks the $2d$ basis vectors sequentially, each a private-centre, private-width Gaussian. ATMACA uses the two-stage ring-level hybrid sampler [DP15][2] with a *public* width r: d coefficients per stage in parallel, two stages instead of $2d$ steps.

[1] [GEP+26] Radhika Garg, Daniel Escudero, Antigoni Polychroniadou, Akira Takahashi, and Xiao Wang. Thresholdizing standardized FALCON signatures. In *ACM CCS 2026*, 2026. Cryptology ePrint Archive, Report 2026/1300.

[2] [DP15] Léo Ducas and Thomas Prest. A hybrid Gaussian sampler for lattices over rings, 2015. Cryptology ePrint Archive, Report 2015/660. Withdrawn; corrected proof in MITAKA [EFG+22].

Which sampler to thresholdize?

	Klein (GPV nearest-plane; Threshold FALCON [GEP+26])	**ffSampling** (FALCON)	**Hybrid** (MITAKA [EFG+22][1]; ATMACA)
Sequential stages	$2d$, one per basis vector	d, one per each tree leaf	2, one per ring stage
Parallel samples per stage	1	2, the leaf pair	d, one per coefficient
Key	FALCON trapdoor	FALCON trapdoor	ANTRAG trapdoor

All three are FALCON-verifiable; only the hybrid sampler has a single sequential dependency, its two stages.

[1] [EFG+22] Thomas Espitau, Pierre-Alain Fouque, François Gérard, Mélissa Rossi, Akira Takahashi, Mehdi Tibouchi, Alexandre Wallet, and Yang Yu. MITAKA: A simpler, parallelizable, maskable variant of FALCON. In *EUROCRYPT 2022*, 2022. Cryptology ePrint Archive, Report 2021/1486.

Hybrid sampler

Hybrid sampler [DP15], input c, basis $(\mathbf{b}_1, \mathbf{b}_2)$, $(\boldsymbol{\beta}_i, \sigma_i)$, width r

1: $\mathbf{c}_2 \leftarrow (c, 0)^t$.
2: **for** $i = 2, 1$ **do**
3: $\quad d_i \leftarrow \beta_{i,1} c_{i,1} + \beta_{i,2} c_{i,2}$.
4: $\quad y_i \leftarrow \sigma_i u_i$ with $u_i \sim \mathcal{N}(0,1)^d$.
5: $\quad t_i \leftarrow d_i - y_i$; $x_{i,j} \leftarrow D_{\mathbb{Z}, t_{i,j}, r}$.
6: $\quad \mathbf{c}_{i-1} \leftarrow \mathbf{c}_i - x_i \mathbf{b}_i$.
7: **return** $(s_1, s_2) \leftarrow \mathbf{c}_0$.

What it computes

- Per stage: a nearest-plane centre d_i, a perturbation y_i, a discrete Gaussian sample x_i of the perturbed centre, and a step $x_i \mathbf{b}_i$ along the basis vector.
- $\mathbf{c}_2 - \mathbf{c}_0 = x_2 \mathbf{b}_2 + x_1 \mathbf{b}_1 \in \Lambda_h$: (s_1, s_2) is short and $s_1 + s_2 h \equiv c \pmod{q}$.

MITAKA signing

Sign(sk, M) with $\mathsf{sk} = (\mathbf{b}_1, \mathbf{b}_2, \boldsymbol{\beta}_1, \boldsymbol{\beta}_2, \sigma_1, \sigma_2)$, $\mathsf{pk} = h$

1: $\mathsf{salt} \xleftarrow{\$} \{0,1\}^{320}$; $c \leftarrow \mathsf{HashToPoint}(\mathsf{salt}, M)$.
2: **repeat**
3: $(s_1, s_2) \leftarrow$ hybrid sampler on c
4: **until** $\|s_1\|_2^2 + \|s_2\|_2^2 \leq \lfloor \beta^2 \rfloor$ and $s \leftarrow \mathsf{Compress}_{\mathrm{FALCON}}(s_2) \neq \perp$
5: **return** $\Sigma = (\mathsf{salt}, s)$

Offline / online

- Offline, per signature: $u_i \sim \mathcal{N}(0,1)^d$ and $y_i = \sigma_i u_i$ for $i = 2, 1$; they depend on the key only.
- Online: the hash, the centres d_i, the ring roundings, the steps along $\mathbf{b}_i$, norm test, compression.

MITAKA and ANTRAG

Why the hybrid sampler suits MPC

- All of the expensive sampling is message-independent.
- The d coefficients of a stage are independent one-dimensional samplers: one synchronized batch per stage.
- Only two sequential stages, against d for ffSampling and $2d$ for Klein.
- Public r: every sampler table is a public constant.

ANTRAG

- ANTRAG [ENS+23][1] generates the trapdoor (f, g) in an annulus of the embedding space, where the quality α keeps $\sigma = \alpha\,\eta_{\varepsilon_{\mathrm{lat}}}(\mathcal{R}^2)\sqrt{q}$ inside FALCON's bound β: FALCON's NIST security levels, with the hybrid sampler kept as the signer.

[1] [ENS+23] Thomas Espitau, Thi Thu Quyen Nguyen, Chao Sun, Mehdi Tibouchi, and Alexandre Wallet. Antrag: Annular NTRU trapdoor generation. In *ASIACRYPT 2023*, 2023.

What do we change further?

Fixed-point arithmetic throughout

- Every real x is $X = \lfloor 2^{\kappa} x \rceil$, $\kappa = 55$, in $\mathbb{F}_{p_{\mathrm{MPC}}}$ with a 120-bit prime, $m_p = 2\kappa + 10$.

A discrete lattice normal sampler

- MITAKA draws u_i from a real $\mathcal{N}(0, 1)$. $\Pi_{\mathrm{NormalPoly}}$ samples on the grid $2^{-\kappa}\mathbb{Z} \cap [-U_{\max}, U_{\max}]$ with a public cutoff $U_{\max}$.
- Offline, key- and message-independent, d coefficients in parallel.

Trusted-party key setup, offline phase, online phase

Setup: dealer, once per key epoch

- ANTRAG.KeyGen: (f, g, F, G), $h = gf^{-1} \bmod q$, size-reduced basis $\mathbf{b}_1, \mathbf{b}_2$.
- Hybrid fixed-point data $(\bar{\mu}, \sigma_1, \sigma_2)$, $\bar{\mu} = \mu - \lfloor \mu \rceil$.
- MAC keys α_A, α_B; degree-$(t-1)$ Shamir shares of each secret z and of $\alpha_A z$; erase.

Offline: per session, message unknown

- Basic shared randomness: triples, daBits, edaBits, random bits, the salt.
- Perturbations $[\![y_2]\!]_{\mathrm{A}}, [\![y_1]\!]_{\mathrm{A}}$.
- Non-message dependent parts of the coefficient sample: Π_{RevCDT}, a daBit and the Bernoulli factors.

Online: active set $\mathcal{S}$, $|\mathcal{S}| \geq t$

- Shamir $\rightarrow$ additive.
- Open salt; $c = \mathsf{HashToPoint}(\mathsf{salt}, M)$.
- Stages $i = 2, 1$: centres $d_2 = fc/q$, $d_1 = -Fc/q + \bar{\mu}(d_2 - x_2)$, minus $[\![y_i]\!]_{\mathrm{A}}$, Π_{RingDG}, times $[\![\mathbf{b}_i]\!]_{\mathrm{A}}$.
- Open s_2; norm test, $\mathrm{Compress}_{\mathrm{FALCON}}$, FALCON encoding; $\perp$ if either fails.

The one-dimensional sampler Π_{1DG}

$\Pi_{\mathrm{1DG}}(\llbracket t \rrbracket_{\mathrm{A}}; r, K_{\mathrm{HG}})$: private fixed-point centre $\llbracket t \rrbracket_{\mathrm{A}}$, public width r and cutoff K_{HG}; output an integer sample $\llbracket x \rrbracket_{\mathrm{A}}$.

1: $\llbracket a \rrbracket_{\mathrm{A}} \leftarrow \mathsf{Floor}_{\kappa}(\llbracket t \rrbracket_{\mathrm{A}})$; $\llbracket D \rrbracket_{\mathrm{A}} \leftarrow \llbracket t \rrbracket_{\mathrm{A}} - 2^{\kappa} \llbracket a \rrbracket_{\mathrm{A}}$.
2: **loop**
3: Take preprocessed $\llbracket k \rrbracket_{\mathrm{A}}$, a half-Gaussian of width r from a reverse CDT; $\llbracket b \rrbracket_{\mathrm{A}}$, a daBit sign bit; $\llbracket z \rrbracket_{\mathrm{A}} = -\llbracket k \rrbracket_{\mathrm{A}} + \llbracket b \rrbracket_{\mathrm{A}}(2\llbracket k \rrbracket_{\mathrm{A}} + 1)$; and Bernoulli-exponential factors $(\llbracket B_\ell \rrbracket_{\mathrm{B}})_\ell$.
4: $\llbracket U \rrbracket_{\mathrm{A}} \leftarrow \llbracket D \rrbracket_{\mathrm{A}} + \llbracket b \rrbracket_{\mathrm{A}} (2^{\kappa} - 2\llbracket D \rrbracket_{\mathrm{A}})$.
5: $\llbracket X \rrbracket_{\mathrm{A}} \leftarrow \llbracket U \rrbracket_{\mathrm{A}} (2^{\kappa+1} \llbracket k \rrbracket_{\mathrm{A}} + \llbracket U \rrbracket_{\mathrm{A}})$.
6: $\llbracket A \rrbracket_{\mathrm{B}} \leftarrow \mathsf{BerExp}(\llbracket X \rrbracket_{\mathrm{A}}; \frac{2^{-2\kappa}}{2r^2}, (\llbracket B_\ell \rrbracket_{\mathrm{B}})_\ell)$.
7: Authenticated-open A.
8: **if** $A = 1$ **then return** $\llbracket x \rrbracket_{\mathrm{A}} \leftarrow \llbracket a \rrbracket_{\mathrm{A}} + \llbracket z \rrbracket_{\mathrm{A}}$.

Centre. $t = a + \delta$, $a = \lfloor t \rfloor$, $\delta \in [0, 1)$, D the backing of δ. With $u = \delta + b(1 - 2\delta)$ and $U = D + b(2^{\kappa} - 2D)$: $(z - \delta)^2 - k^2 = u(2k + u)$, so the exact rejection exponent is $\xi = u(2k + u)/(2r^2)$.

Output law. $\Pr[A = 1] = e^{-\xi}$ up to table rounding, so an accepted z has mass $\propto q(k) e^{-\xi} \propto e^{-(z-\delta)^2/(2r^2)}$: $x = a + z \sim D_{\mathbb{Z},t,r}$. Accept rate $p_{\mathrm{DG}} \approx 0.77$ independent of the centre.

Security assumptions and guarantees

Assumptions

- Static, active adversary corrupting up to $t-1$ of the n parties (dishonest majority).
- Trusted dealer at key setup only; signers generate all signing randomness.

Guarantees

- Unforgeability against $t-1$ corrupt signers under chosen-message attacks.
- Security with abort: MAC-checked openings, abort on a failed check; without a fairness guarantee.
- A rushing adversary can abort but cannot bias the signatures.

Security level

The claim rests on FALCON and on the MPC layer; categories 1 and 5 also on the hardness of ANTRAG keys [ENS+23] and on the fixed-point sampler being close to the ideal lattice Gaussian.

Rigorous fixed-point precision analysis

Implemented versus ideal

- Implemented: κ-bit fixed point, κ'-bit tables, cutoffs $U_{\max}$ and K_{HG}.
- Ideal: the lattice Gaussian $D_{\Lambda_h,\mathbf{c},\sigma}$ of the security proof.
- Range bounds: nothing wraps around modulo p_{MPC}, so roundings are the only arithmetic errors.
- We are careful not to multiply a fixed-point internal with a large number during execution in order not to increase the error caused by the fixed-point implementation.

Rényi divergence and security bits

- Rényi divergence charging every approximation, and the hybrid sampler's own smoothing gap.
- Moment bounds, composed over both stages, $2d$ coefficient samples and all attempts.
- Forgery bounds transfer: $p_{\mathrm{impl}} \le (R_\lambda\, p_{\mathrm{ideal}})^{1-1/\lambda}$, i.e. lost security bits.

Outcome

The bits lost depend on κ, κ', the cutoffs, σ, r, α and the number of attempts. At $\kappa = 55$ and 2^{64} attempts, tuning only α and r gives below 1 bit for $d = 512$ ($\alpha = 1.13$, $r \approx 1.36$) and below 5 bits for $d = 1024$ ($\alpha = 1.19$, $r \approx 1.34$).

Imported MPC primitives

Primitive	Role in ATMACA	Source
$[\![x]\!]_{\mathrm{A}}$, $[\![b]\!]_{\mathrm{B}}$	Authenticated sharings over $\mathbb{F}_{p_{\mathrm{MPC}}}$ (MAC in $\mathbb{F}_{p^2_{\mathrm{MPC}}}$) and $\mathbb{F}_2$ (MAC in $\mathbb{F}_{2^{k_B}}$); long-lived Shamir shares, session-local additive shares	SPDZ [DPSZ12, DKL+13]; MP-SPDZ [Kel20][1]
Beaver triples	Arithmetic, Boolean (AND)	[EGK+20][2]
daBit, edaBit, random bits	Domain conversion; canonical edaBits uniform in $[0, p_{\mathrm{MPC}})$; κ'-bit random words	[RW19, EGK+20]; as in [BdCE+26][3]
B2A	One daBit, one masked Boolean opening	[EGK+20]
Π_{BitDec}	Nishide–Ohta decomposition with one canonical edaBit, $2\lceil \log_2 m_p \rceil + 2$ rounds	[NO07]; pattern of [BdCE+26]

[1] [Kel20] Marcel Keller. MP-SPDZ: A versatile framework for multi-party computation. In *ACM CCS 2020*, 2020. Cryptology ePrint Archive, Report 2020/521; https://github.com/data61/MP-SPDZ.

[2] [EGK+20] Daniel Escudero, Satrajit Ghosh, Marcel Keller, Rahul Rachuri, and Peter Scholl. Improved primitives for MPC over mixed arithmetic-binary circuits. In *CRYPTO 2020*, 2020. Cryptology ePrint Archive, Report 2020/338.

[3] [BdCE+26] Alexander Bienstock, Leo de Castro, Daniel Escudero, Antigoni Polychroniadou, and Akira Takahashi. Quorus: Efficient, scalable threshold ML-DSA signatures from MPC. In *USENIX Security 2026*, 2026. Full version.

Online rounds, online and offline communication complexity

Illustrative parameters $d = 512$, $\kappa = 55$, $m_p = 120$, $m_{\mathrm{tr}} = 4$; bits per ordered pair of parties and per signature attempt; estimates from the component protocols, not benchmarks.

Online round complexity

One rejection iteration (m_{tr} trials per coefficient)	31
One ring call with T iterations, $\mathbb{E}[T] \approx 1.8$	$17 + 31T$
Outside the samplers (salt 3, products 3, s_2 5)	11
Best case, both calls accept at once	107
Expected	154
Worst case (exceeded with probability $< 2^{-45}$)	324

Offline communication

Preprocessing protocols	71 MB
$\Pi_{\mathrm{NormalPoly}}$ ($2d$ coefficients)	45 MB
proposal records ($\Pi = 5057$)	24 MB
canonical edaBits, perturbations	0.7, 0.5 MB
Correlated randomness	0.83 GB
of which 2.9×10^8 Boolean triples	0.58 GB
Offline total per pair and attempt	0.90 GB

Comparison with the previous work

	Threshold ML-DSA [CdPE$^+$26][1]	**Threshold FALCON** [GEP$^+$26]	**ATMACA**
Signature	ML-DSA verifier	FALCON verifier	FALCON verifier
Rounds	$2 + 4$ expected	≈ 6200	154 expected (≤ 324 with probability more than $1 - 2^{-45}$)
MB per party per signature, off + online, at $(4, 4)$	$\approx 0 + 0.08$ expected	$2470 + 163$	$2700 + 8.7$

Threshold FALCON: rounds are the 12.4 million rounds of 2000 parallel signing attempts divided by 2000; communication is per signature, averaged over those signatures.

[1] [CdPE$^+$26] Sofía Celi, Rafael del Pino, Thomas Espitau, Guilhem Niot, and Thomas Prest. Efficient threshold ML-DSA. In *USENIX Security 2026*, 2026. Full version.

Future work

Cut the preprocessing volume

- Cheaper offline circuits?
- Fewer conversions?
- Smaller randomness pool?

DKG?

- Today: a trusted dealer per key epoch; the threshold property concerns signing only.
- A distributed ANTRAG.KeyGen needs annulus sampling of (f, g), NTRU solving for (F, G) and the hybrid data $(\bar{\mu}, \sigma_i)$ under MPC.
- For the Call: is a dealer acceptable in this category, or is a DKG expected?

Questions?

References I

[BdCE+26] Alexander Bienstock, Leo de Castro, Daniel Escudero, Antigoni Polychroniadou, and Akira Takahashi.
Quorus: Efficient, scalable threshold ML-DSA signatures from MPC.
In *USENIX Security 2026*, 2026.
Full version.

[CdPE+26] Sofía Celi, Rafael del Pino, Thomas Espitau, Guilhem Niot, and Thomas Prest.
Efficient threshold ML-DSA.
In *USENIX Security 2026*, 2026.
Full version.

[DKL+13] Ivan Damgård, Marcel Keller, Enrique Larraia, Valerio Pastro, Peter Scholl, and Nigel P. Smart.
Practical covertly secure MPC for dishonest majority – or: Breaking the SPDZ limits.
In *ESORICS 2013*, 2013.
Cryptology ePrint Archive, Report 2012/642.

[DP15] Léo Ducas and Thomas Prest.
A hybrid Gaussian sampler for lattices over rings, 2015.
Cryptology ePrint Archive, Report 2015/660. Withdrawn; corrected proof in MITAKA [EFG+22].

References II

[DPSZ12] Ivan Damgård, Valerio Pastro, Nigel P. Smart, and Sarah Zakarias.
Multiparty computation from somewhat homomorphic encryption.
In *CRYPTO 2012*, 2012.
Cryptology ePrint Archive, Report 2011/535.

[EFG+22] Thomas Espitau, Pierre-Alain Fouque, François Gérard, Mélissa Rossi, Akira Takahashi, Mehdi Tibouchi, Alexandre Wallet, and Yang Yu.
MITAKA: A simpler, parallelizable, maskable variant of FALCON.
In *EUROCRYPT 2022*, 2022.
Cryptology ePrint Archive, Report 2021/1486.

[EGK+20] Daniel Escudero, Satrajit Ghosh, Marcel Keller, Rahul Rachuri, and Peter Scholl.
Improved primitives for MPC over mixed arithmetic-binary circuits.
In *CRYPTO 2020*, 2020.
Cryptology ePrint Archive, Report 2020/338.

[ENS+23] Thomas Espitau, Thi Thu Quyen Nguyen, Chao Sun, Mehdi Tibouchi, and Alexandre Wallet.
Antrag: Annular NTRU trapdoor generation.
In *ASIACRYPT 2023*, 2023.

References III

[FHK+20] Pierre-Alain Fouque, Jeffrey Hoffstein, Paul Kirchner, Vadim Lyubashevsky, Thomas Pornin, Thomas Prest, Thomas Ricosset, Gregor Seiler, William Whyte, and Zhenfei Zhang.
Falcon: Fast-fourier lattice-based compact signatures over NTRU, specification v1.2, 2020.
NIST PQC submission.

[GEP+26] Radhika Garg, Daniel Escudero, Antigoni Polychroniadou, Akira Takahashi, and Xiao Wang.
Thresholdizing standardized FALCON signatures.
In *ACM CCS 2026*, 2026.
Cryptology ePrint Archive, Report 2026/1300.

[Kel20] Marcel Keller.
MP-SPDZ: A versatile framework for multi-party computation.
In *ACM CCS 2020*, 2020.
Cryptology ePrint Archive, Report 2020/521; `https://github.com/data61/MP-SPDZ`.

[NO07] Takashi Nishide and Kazuo Ohta.
Multiparty computation for interval, equality, and comparison without bit-decomposition protocol.
In *PKC 2007*, 2007.

References IV

[RW19] Dragos Rotaru and Tim Wood.
MArBled circuits: Mixing arithmetic and Boolean circuits with active security.
In *INDOCRYPT 2019*, 2019.
Cryptology ePrint Archive, Report 2019/207.