



Ringtail: Practical Two-Round Threshold Signatures from Learning with Errors



Cecilia Boschini
ETH Zürich

Darya Kaviani
UC Berkeley

Russell W. F. Lai
Aalto University

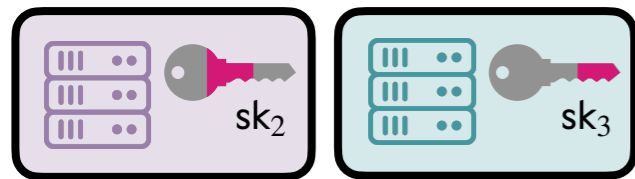
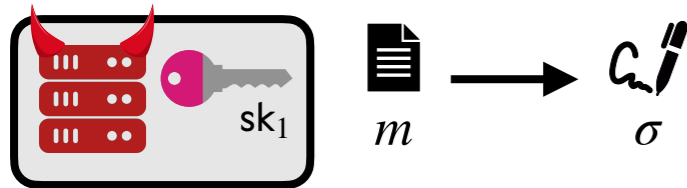
Giulio Malavolta
Bocconi University

Akira Takahashi
J.P. Morgan

Mehdi Tibouchi
NTT (Japan)

IEEE S&P '25

(t, n) -Threshold Signatures



Even if a subset of servers are corrupted, the secret key is safe.

Signing key is split into several **shares** such that no server holds the original secret key.

Any t of n parties can jointly produce a signature, but not $t - 1$.

The Road to Ringtail



Generic approaches (MPC or FHE) are not concretely efficient.

Enables 2 rounds

FROST thresholdization [KG20]

Fiat-Shamir

Raccoon ID [dPE+23]

Raccoon Signature [dPE+23]
T-Raccoon masking [dPK+24]

Enables reduction to (M)LWE

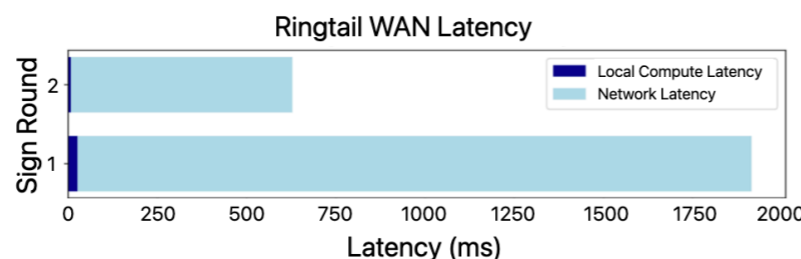
MuSig-L Simulation [BTT22]



Ringtail

Performance

Network time dominates → minimize rounds.



Simplified Ringtail

Offline $(\mathbf{r}_i, \mathbf{e}_i^*) \leftarrow \bar{D}^{n+m}$

$\mathbf{R}_i \leftarrow D^{n \times d}, \mathbf{E}_i \leftarrow D^{m \times d}$
 $\mathbf{D}_i = \mathbf{A}[\mathbf{r}_i | \mathbf{R}_i] + [\mathbf{e}_i^* | \mathbf{E}_i]$

Online $\mathbf{D} = \sum_{j \in \mathcal{T}} \mathbf{D}_j$

$\mathbf{u} = \mathbf{H}(\mathbf{pk}, m, (\mathbf{D}_j)_{j \in \mathcal{T}})$

$\mathbf{h} = \mathbf{D}\mathbf{u}$

$c = \mathbf{H}(\mathbf{pk}, m, \mathbf{h})$

$\mathbf{z}_i = c \cdot \lambda_{\mathcal{T}, i} \cdot \mathbf{sk}_i + \mathbf{r}_i + \mathbf{R}_i \mathbf{u} + \mathbf{m}_i$

Finalize $\mathbf{z} = \sum_{j \in \mathcal{T}} \mathbf{z}_j$

(c, \mathbf{z})

FROST-Schnorr random linear combination [KG20] prevents interactive adversary forging.

One-time PRF mask with 0-share [dPK+24] [KRT24]

$\mathbf{D}_i \in R_q^{m \times (d+1)}$

\mathbf{D}_j for $j \in \mathcal{T} \setminus \{i\}$

\mathbf{z}_i

\mathbf{z}_j for $j \in \mathcal{T} \setminus \{i\}$

\mathbf{sk}
LWE secret key
 $\mathbf{pk} = \mathbf{A} \cdot \mathbf{sk} + \mathbf{e}$
LWE public key

Security

Provably secure from standard (module) **LWE** & **SelfTarget SIS** assumptions in the classical **ROM**.

Bandwidth (KB)

Scheme	Public Key Size	Signature Size	Sign (Total)	Sign (Online)
Ringtail	4.50	13.38	598.50 + 0.02 t	10.50
tRaccoon [dPK+24]	3.77	12.44	39.84 + 0.02 t	39.84 + 0.02 t
EKT [EKT24]	5.50	10.80	275.69	14.06