# Sanitizable Signatures with Different Admissibility Policies for Multiple Sanitizers

**Osama Allabwani**[1, 3], Olivier Blazy[2], Pascal Lafourcade[1, 4], Charles Olivier-Anclin[1], Olivier Raynaud[1]

[1] Université Clermont Auvergne, LIMOS, CNRS
[2] École Polytechnique, [3] BeYs, [4] ASTEROIDE, Trust4Sign

**AsiaCCS 2026**

# Signature

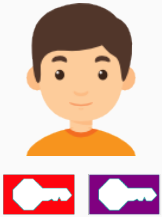
signer

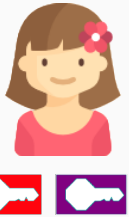
verifier

# Sanitizable Signature, Atenise et al. 2005

signer

sanitizer





# Unforgeability, Atenise et al. 2005

No unauthorized user can generate a valid signature

# Immutability, Atenise et al. 2005

signer

sanitizer

Sanitizer cannot modify unauthorized parts of a signature

# Privacy, Atenise et al. 2005

All original sanitized information is unrecoverable

# Accountability, Atenise et al. 2005

# Sanitizer Anonymity, Canard et al. 2012

Identity of the sanitizer is hidden

# Invisibility, Ateniese et al. 2005

Admissible blocks hidden from external parties

# Unlinkability, Bruzuska et al 2010

Impossible to link a sanitized signature to the original one

# Transparency, Atenise et al. 2005

Nobody can say if a signature is sanitized or not

### Multiple Sanitizers



A signature is valid if and only if all admissible blocks are sanitized

# Contributions: Impossibility results



**Full-sanitization verifiability ⇒ no Transparency**

*Recall* : Transparency : nobody can say if a signature is sanitized or not



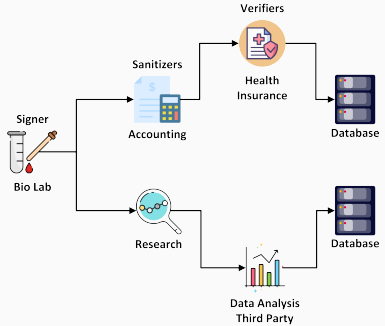

**Full-sanitization verifiability ⇒ no Invisibility**

*Recall* : Admissible blocks hidden from external parties

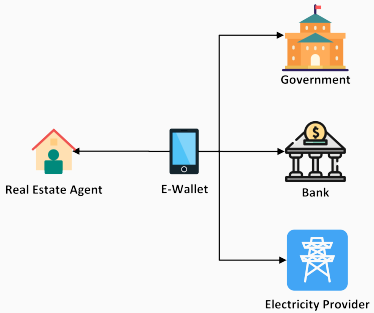


# Contributions: IUT-k-SAN and FSV-k-SAN

## Multi-Sanitizer Sanitizable Signatures with Different Admissibility Policies




Invisible-Unlinkable-Transparent k-SAN




Full-Sanitization Verifiable k-SAN

**Security Properties:**

- Unforgeability
- Immutability
- Privacy
- Accountability
- Sanitizer Anonymity

# Related Works

| Security Property | FSV-k-SAN | IUT-k-SAN | [1] | [7] | [14] | [15] | [25] | [30] |
|---|---|---|---|---|---|---|---|---|
| Unforgeability | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Immutability | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Privacy | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Accountability | ✓ | ✓ | ✓ | ✓ | ✓ | ✗ | ✓ | ✓ |
| Sanitizer Anonymity | ✓ | ✓ | ✗ | ✗ | ✓ | ✗ | ✗ | ✓ |
| Unlinkability | ✗ | ✓ | ✓ | ✗ | ✓ | ✗ | ✗ | ✗ |
| Full-Sanitization Verif. | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ |
| Transparency | ✗ | ✓ | ✓ | ✗ | ✓ | ✓ | ✓ | ✓ |
| Invisibility | ✗ | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ |

# FSV-k-SAN Construction

| | |
|---|---|
| **PKE**<br>A Public key encryption | **VRS**<br>A verifiable ring signature scheme |
| **CHash**<br>A Chameleon hash function | **SIG**<br>A digital signature scheme |

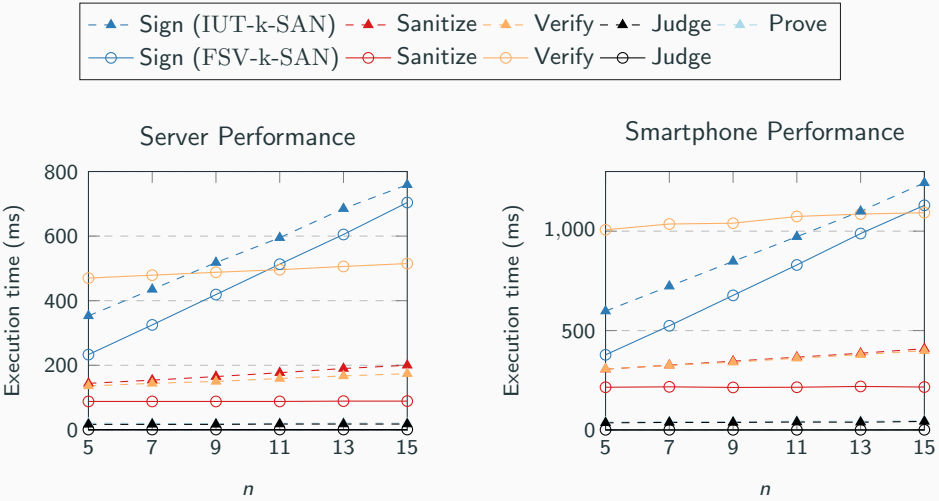
# IUT-k-SAN Construction

Builds on the work of Bultel *et al.* [1].

| **PKE** | **VRS** |
| --- | --- |
| A Public key encryption with homomorphic scalar multiplication | A verifiable ring signature scheme |
| **BLS** | **EQS** |
| A short signature scheme with key and signature randomization | A structure preserving signature on equivalence classes |

[1] Bultel, Lafourcade, Lai, Malavolta, Schröder, Thyagarajan. Efficient Invisible and Unlinkable Sanitizable Signatures. PKC 2019.

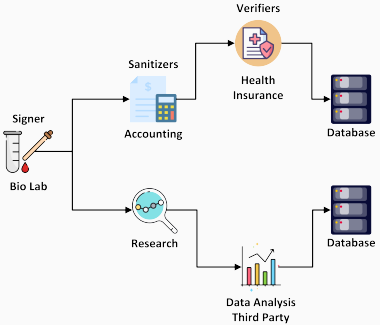
# Rust Implementation Performance[2]



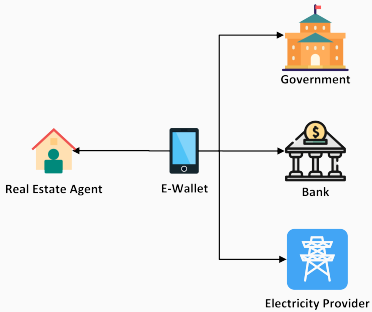

[2] www.github.com/be-ys/ksan

# Conclusion

## Multi-Sanitizer Sanitizable Signatures with Different Admissibility Policies




Invisible-Unlinkable-Transparent k-SAN




Full-Sanitization Verifiable k-SAN

# End[3]

Thanks for your attention!

Questions : osama.allabwani@limos.fr

[3] Used icons from www.flaticon.com