# 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]

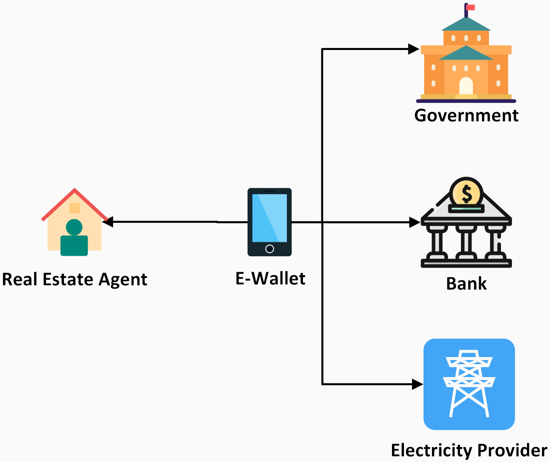
[1] Université Clermont Auvergne, LIMOS, CNRS
[2] École Polytechnique, [3] BeYs, [4] ASTEROIDE, Trust4Sign

24 February 2026

# Plan

- Motivation
- Sanitizable signatures and our contribution
- Building blocks
- Constructions
- Implementation

# Rental Application



# Sanitizable Signatures

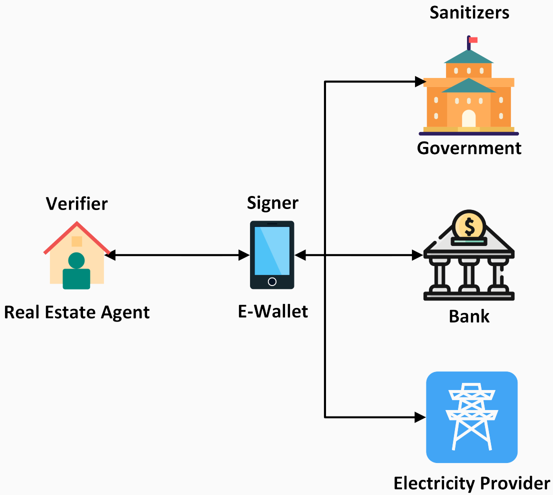

**Idea:** Multi-Sanitizer Sanitizable Signatures with Different Admissibility Policies


**Idea:** Multi-Sanitizer Sanitizable Signatures with Different Admissibility Policies

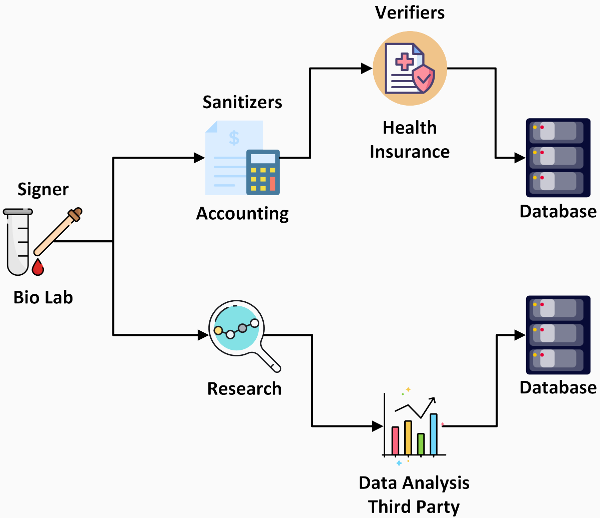
**Security Properties:**

- Unforgeability
- Accountability
- Immutability
- Invisibility
- Privacy
- Unlinkability
- Transparency
- Sanitizer Anonymity

# Use Case 1: Full-Sanitization Verifiable k-SAN (FSV-k-SAN)



# Use Case 2: Invisible-Unlinkable-Transparent k-SAN (IUT-k-SAN)



# Building Blocks

| | |
|---|---|
| **PKE**<br>A Public key encryption with homomorphic scalar multiplication | **VRS**<br>A verifiable ring signature scheme |
| **CHash**<br>A Chameleon hash function | **SIG**<br>A digital signature scheme |
| **BLS**<br>A short signature scheme with key and signature randomization | **EQS**<br>A structure preserving signature on equivalence classes |

# Notation

**Algorithms:** Setup, $\mathsf{KGen_S}$, $\mathsf{KGen_Z}$, Sign, Sanitize, Verify, Prove, Judge.

$$m = \begin{array}{|c|c|c|c|}\hline m_1 & m_2 & \dots & m_n \\ \hline \end{array}$$

$$\mathbf{A} = \begin{array}{|c|c|c|c|}\hline a_{1,1} & a_{1,2} & \dots & a_{1,n} \\ \hline a_{2,1} & a_{2,2} & \dots & a_{2,n} \\ \hline \vdots & \vdots & \vdots & \vdots \\ \hline a_{k,1} & a_{k,2} & \dots & a_{k,n} \\ \hline \end{array}$$

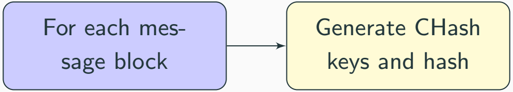
$$\mathbf{PKZ} = \begin{array}{|c|c|c|c|}\hline \mathsf{pk}_Z^1 & \mathsf{pk}_Z^2 & \dots & \mathsf{pk}_Z^k \\ \hline \end{array}$$

$$\mathrm{MOD} = \begin{array}{|c|c|c|}\hline j_1 & j_2 & \dots \\ m'_{j_1} & m'_{j_2} & \dots \\ \hline \end{array}$$

# 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 |

# FSV-k-SAN Construction: Sign $(n = 3, k = 2)$



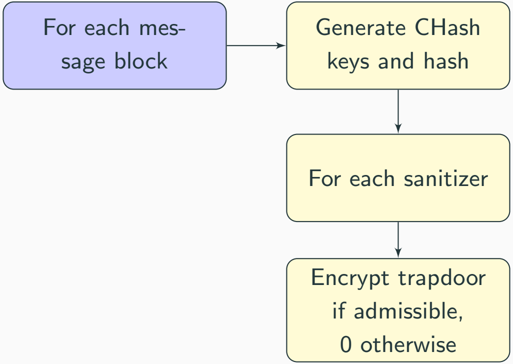

$m =$

| | | |
|---|---|---|
| $m_1$ | $m_2$ | $m_3$ |

**CH** $=$

| | | |
|---|---|---|
| $h_1$ | $h_2$ | $h_3$ |
| $r_1$ | $r_2$ | $r_3$ |
| $\mathrm{pk}_{\mathrm{CH}}^1$ | $\mathrm{pk}_{\mathrm{CH}}^2$ | $\mathrm{pk}_{\mathrm{CH}}^3$ |

# FSV-k-SAN Construction: Sign $(n = 3, k = 2)$




$m =$

| | | |
|---|---|---|
| $m_1$ | $m_2$ | $m_3$ |

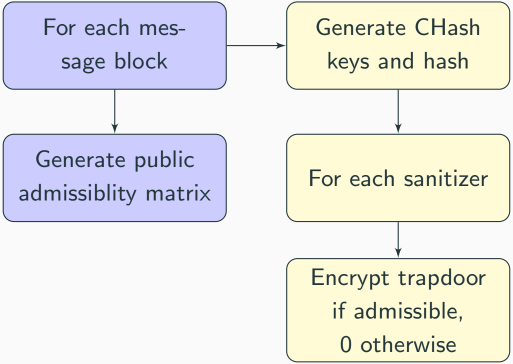
**CH** $=$

| | | |
|---|---|---|
| $h_1$ <br> $r_1$ <br> $\mathsf{pk}^1_{\mathsf{CH}}$ | $h_2$ <br> $r_2$ <br> $\mathsf{pk}^2_{\mathsf{CH}}$ | $h_3$ <br> $r_3$ <br> $\mathsf{pk}^3_{\mathsf{CH}}$ |

**SKCH** $=$

| | | |
|---|---|---|
| $\{0\}_{\mathsf{pk}^1_{\mathsf{ZE}}}$ | $\{\mathsf{sk}^2_{\mathsf{CH}}\}_{\mathsf{pk}^1_{\mathsf{ZE}}}$ | $\{\mathsf{sk}^3_{\mathsf{CH}}\}_{\mathsf{pk}^1_{\mathsf{ZE}}}$ |
| $\{0\}_{\mathsf{pk}^2_{\mathsf{ZE}}}$ | $\{0\}_{\mathsf{pk}^2_{\mathsf{ZE}}}$ | $\{\mathsf{sk}^3_{\mathsf{CH}}\}_{\mathsf{pk}^2_{\mathsf{ZE}}}$ |

# FSV-k-SAN Construction: Sign $(n = 3, k = 2)$



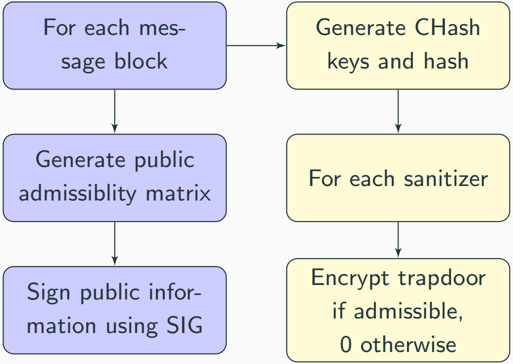

$$m = \begin{array}{|c|c|c|}\hline m_1 & m_2 & m_3 \\ \hline \end{array}$$

$$\mathbf{CH} = \begin{array}{|c|c|c|}\hline h_1 & h_2 & h_3 \\ r_1 & r_2 & r_3 \\ \mathsf{pk}^1_{\mathsf{CH}} & \mathsf{pk}^2_{\mathsf{CH}} & \mathsf{pk}^3_{\mathsf{CH}} \\ \hline \end{array}$$

$$\mathbf{SKCH} = \begin{array}{|c|c|c|}\hline \{0\}_{\mathsf{pk}^1_{\mathsf{ZE}}} & \{\mathsf{sk}^2_{\mathsf{CH}}\}_{\mathsf{pk}^1_{\mathsf{ZE}}} & \{\mathsf{sk}^3_{\mathsf{CH}}\}_{\mathsf{pk}^1_{\mathsf{ZE}}} \\ \hline \{0\}_{\mathsf{pk}^2_{\mathsf{ZE}}} & \{0\}_{\mathsf{pk}^2_{\mathsf{ZE}}} & \{\mathsf{sk}^3_{\mathsf{CH}}\}_{\mathsf{pk}^2_{\mathsf{ZE}}} \\ \hline \end{array}$$

$$\mathbf{PA} = \begin{array}{|c|c|c|}\hline 0 & 1 & 1 \\ \hline \end{array}$$

# FSV-k-SAN Construction: Sign $(n = 3, k = 2)$




$$m = \begin{array}{|c|c|c|}\hline m_1 & m_2 & m_3 \\ \hline\end{array}$$

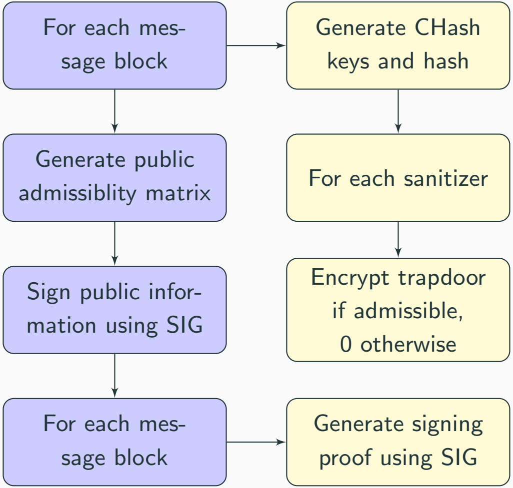
$$\mathbf{CH} = \begin{array}{|c|c|c|}\hline h_1 & h_2 & h_3 \\ r_1 & r_2 & r_3 \\ \mathsf{pk}^1_{\mathsf{CH}} & \mathsf{pk}^2_{\mathsf{CH}} & \mathsf{pk}^3_{\mathsf{CH}} \\ \hline\end{array}$$

$$\mathbf{SKCH} = \begin{array}{|c|c|c|}\hline \{0\}_{\mathsf{pk}^1_{\mathsf{ZE}}} & \{\mathsf{sk}^2_{\mathsf{CH}}\}_{\mathsf{pk}^1_{\mathsf{ZE}}} & \{\mathsf{sk}^3_{\mathsf{CH}}\}_{\mathsf{pk}^1_{\mathsf{ZE}}} \\ \hline \{0\}_{\mathsf{pk}^2_{\mathsf{ZE}}} & \{0\}_{\mathsf{pk}^2_{\mathsf{ZE}}} & \{\mathsf{sk}^3_{\mathsf{CH}}\}_{\mathsf{pk}^2_{\mathsf{ZE}}} \\ \hline\end{array}$$

$$\mathbf{PA} = \begin{array}{|c|c|c|}\hline 0 & 1 & 1 \\ \hline\end{array}$$

$$s = \mathsf{Sign}_{\mathsf{SIG}}\left(\begin{array}{c}(\mathbf{CH}_j.h, \mathbf{CH}_j.\mathsf{pk}_{\mathsf{CH}})_{j \in [\![n]\!]}, \mathbf{SKCH}, \\ \mathbf{PA}, \mathsf{pk}_{\mathsf{S}}, \mathbf{PKZ}, n\end{array}\right)$$

# FSV-k-SAN Construction: Sign $(n = 3, k = 2)$




$$m = \begin{array}{|c|c|c|}\hline m_1 & m_2 & m_3 \\ \hline\end{array}$$

$$\mathbf{CH} = \begin{array}{|c|c|c|}\hline h_1 & h_2 & h_3 \\ r_1 & r_2 & r_3 \\ \mathsf{pk}^1_{\mathsf{CH}} & \mathsf{pk}^2_{\mathsf{CH}} & \mathsf{pk}^3_{\mathsf{CH}} \\ \hline\end{array}$$

$$\mathbf{SKCH} = \begin{array}{|c|c|c|}\hline \{0\}_{\mathsf{pk}^1_{\mathsf{ZE}}} & \{\mathsf{sk}^2_{\mathsf{CH}}\}_{\mathsf{pk}^1_{\mathsf{ZE}}} & \{\mathsf{sk}^3_{\mathsf{CH}}\}_{\mathsf{pk}^1_{\mathsf{ZE}}} \\ \hline \{0\}_{\mathsf{pk}^2_{\mathsf{ZE}}} & \{0\}_{\mathsf{pk}^2_{\mathsf{ZE}}} & \{\mathsf{sk}^3_{\mathsf{CH}}\}_{\mathsf{pk}^2_{\mathsf{ZE}}} \\ \hline\end{array}$$

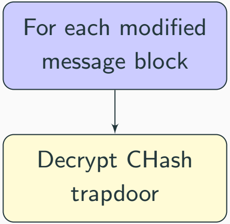
$$\mathbf{PA} = \begin{array}{|c|c|c|}\hline 0 & 1 & 1 \\ \hline\end{array}$$

$$s = \mathsf{Sign}_{\mathsf{SIG}}\left(\begin{array}{c}(\mathbf{CH}_j.h, \mathbf{CH}_j.\mathsf{pk}_{\mathsf{CH}})_{j \in [\![n]\!]}, \mathbf{SKCH}, \\ \mathbf{PA}, \mathsf{pk}_{\mathsf{S}}, \mathbf{PKZ}, n\end{array}\right)$$

$$\rho = \begin{array}{|c|c|c|}\hline \rho_1 & \rho_2 & \rho_3 \\ \hline\end{array}$$

$$\sigma = (s, \mathbf{CH}, \mathbf{SKCH}, \mathbf{PA}, n, \rho)$$

# FSV-k-SAN Construction: Sanitize $m_2$ by sanitizer 1




$m' =$

| | | |
|---|---|---|
| $m_1$ | $m'_2$ | $m_3$ |

$\mathbf{CH} =$

| | | |
|---|---|---|
| $h_1$ | $h_2$ | $h_3$ |
| $r_1$ | $r_2$ | $r_3$ |
| $\mathsf{pk}^1_{\mathsf{CH}}$ | $\mathsf{pk}^2_{\mathsf{CH}}$ | $\mathsf{pk}^3_{\mathsf{CH}}$ |

$\mathbf{SKCH} =$

| | | |
|---|---|---|
| $\{0\}_{\mathsf{pk}^1_{\mathsf{ZE}}}$ | $\{\mathsf{sk}^2_{\mathsf{CH}}\}_{\mathsf{pk}^1_{\mathsf{ZE}}}$ | $\{\mathsf{sk}^3_{\mathsf{CH}}\}_{\mathsf{pk}^1_{\mathsf{ZE}}}$ |
| $\{0\}_{\mathsf{pk}^2_{\mathsf{ZE}}}$ | $\{0\}_{\mathsf{pk}^2_{\mathsf{ZE}}}$ | $\{\mathsf{sk}^3_{\mathsf{CH}}\}_{\mathsf{pk}^2_{\mathsf{ZE}}}$ |

$\mathbf{PA} =$

| | | |
|---|---|---|
| 0 | 1 | 1 |

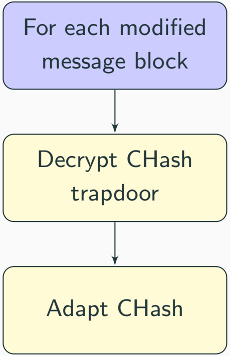
$$s = \mathsf{Sign}_{\mathsf{SIG}}\left( \begin{array}{c} (\mathbf{CH}_j.h, \mathbf{CH}_j.\mathsf{pk}_{\mathsf{CH}})_{j \in [\![n]\!]}, \mathbf{SKCH}, \\ \mathbf{PA}, \mathsf{pk}_{\mathsf{S}}, \mathbf{PKZ}, n \end{array} \right)$$

$\rho =$

| | | |
|---|---|---|
| $\rho_1$ | $\rho_2$ | $\rho_3$ |

$$\sigma = (s, \mathbf{CH}, \mathbf{SKCH}, \mathbf{PA}, n, \rho)$$

# FSV-k-SAN Construction: Sanitize $m_2$ by sanitizer 1




$m' =$

| | | |
|---|---|---|
| $m_1$ | $m'_2$ | $m_3$ |

$\mathbf{CH}' =$

| | | |
|---|---|---|
| $h_1$ | $h_2$ | $h_3$ |
| $r_1$ | $r'_2$ | $r_3$ |
| $\mathsf{pk}^1_{\mathsf{CH}}$ | $\mathsf{pk}^2_{\mathsf{CH}}$ | $\mathsf{pk}^3_{\mathsf{CH}}$ |

$\mathbf{SKCH} =$

| | | |
|---|---|---|
| $\{0\}_{\mathsf{pk}^1_{\mathsf{ZE}}}$ | $\{\mathsf{sk}^2_{\mathsf{CH}}\}_{\mathsf{pk}^1_{\mathsf{ZE}}}$ | $\{\mathsf{sk}^3_{\mathsf{CH}}\}_{\mathsf{pk}^1_{\mathsf{ZE}}}$ |
| $\{0\}_{\mathsf{pk}^2_{\mathsf{ZE}}}$ | $\{0\}_{\mathsf{pk}^2_{\mathsf{ZE}}}$ | $\{\mathsf{sk}^3_{\mathsf{CH}}\}_{\mathsf{pk}^2_{\mathsf{ZE}}}$ |

$\mathbf{PA} =$

| | | |
|---|---|---|
| 0 | 1 | 1 |

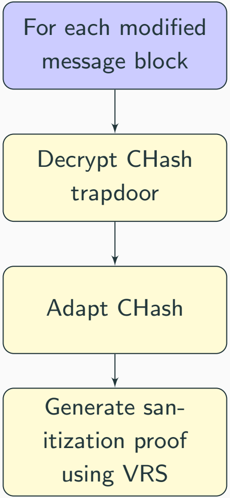
$$s = \mathsf{Sign}_{\mathsf{SIG}}\left( \begin{array}{c} (\mathbf{CH}_j.h, \mathbf{CH}_j.\mathsf{pk}_{\mathsf{CH}})_{j \in [\![n]\!]}, \mathbf{SKCH}, \\ \mathbf{PA}, \mathsf{pk}_{\mathsf{S}}, \mathbf{PKZ}, n \end{array} \right)$$

$\rho =$

| | | |
|---|---|---|
| $\rho_1$ | $\rho_2$ | $\rho_3$ |

$$\sigma = (s, \mathbf{CH}, \mathbf{SKCH}, \mathbf{PA}, n, \rho)$$

# FSV-k-SAN Construction: Sanitize $m_2$ by sanitizer 1




$m' = $

| | | |
|---|---|---|
| $m_1$ | $m'_2$ | $m_3$ |

$\mathbf{CH}' = $

| | | |
|---|---|---|
| $h_1$ | $h_2$ | $h_3$ |
| $r_1$ | $r'_2$ | $r_3$ |
| $\mathsf{pk}^1_{\mathsf{CH}}$ | $\mathsf{pk}^2_{\mathsf{CH}}$ | $\mathsf{pk}^3_{\mathsf{CH}}$ |

$\mathbf{SKCH} = $

| | | |
|---|---|---|
| $\{0\}_{\mathsf{pk}^1_{\mathsf{ZE}}}$ | $\{\mathsf{sk}^2_{\mathsf{CH}}\}_{\mathsf{pk}^1_{\mathsf{ZE}}}$ | $\{\mathsf{sk}^3_{\mathsf{CH}}\}_{\mathsf{pk}^1_{\mathsf{ZE}}}$ |
| $\{0\}_{\mathsf{pk}^2_{\mathsf{ZE}}}$ | $\{0\}_{\mathsf{pk}^2_{\mathsf{ZE}}}$ | $\{\mathsf{sk}^3_{\mathsf{CH}}\}_{\mathsf{pk}^2_{\mathsf{ZE}}}$ |

$\mathbf{PA} = $

| | | |
|---|---|---|
| 0 | 1 | 1 |

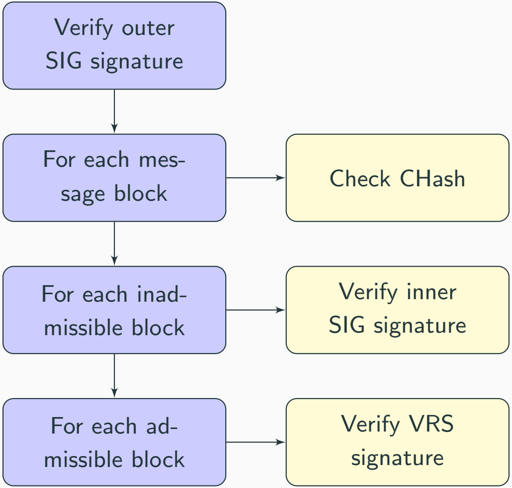
$$s = \mathsf{Sign}_{\mathsf{SIG}}\left(\begin{array}{c}(\mathbf{CH}_j.h, \mathbf{CH}_j.\mathsf{pk}_{\mathsf{CH}})_{j \in [\![n]\!]}, \mathbf{SKCH}, \\ \mathbf{PA}, \mathsf{pk}_{\mathsf{S}}, \mathbf{PKZ}, n\end{array}\right)$$

$\rho' = $

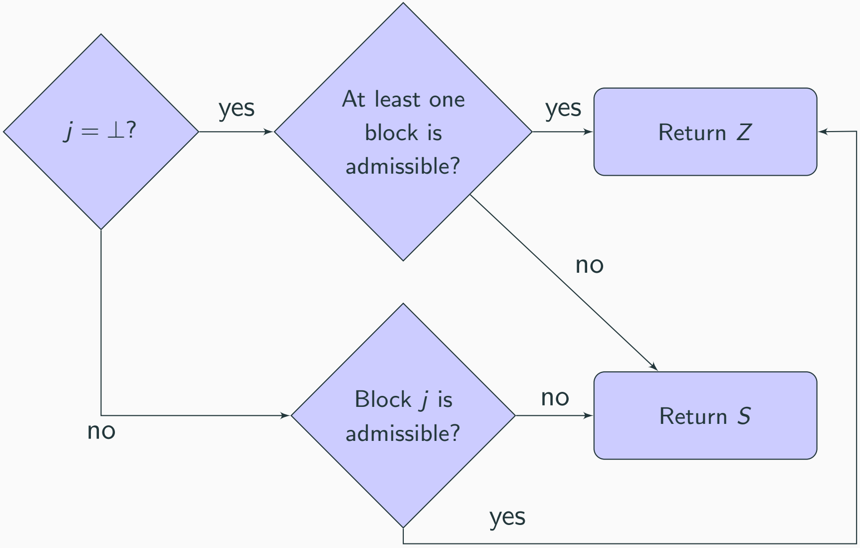
| | | |
|---|---|---|
| $\rho_1$ | $\rho'_2$ | $\rho_3$ |

$$\sigma' = (s, \mathbf{CH}', \mathbf{SKCH}, \mathbf{PA}, n, \rho')$$

# FSV-k-SAN Construction: Verify



# FSV-k-SAN Construction: Judge



# FSV-k-SAN Security

- **Unforgeability** implied by accountability.
- **Immutability** relies on the unforgeability of SIG, the IND-CPA security of PKE, and the collision resistance of CHash.
- **Privacy** relies on the indistinguishability of CHash.
- **Accountability** relies on the unforgeability of SIG and VRS.
- **Full-Sanitization Verifiability** relies on the unforgeability of SIG and VRS.
- **Sanitizer Anonymity** relies on the anonymity of VRS and the IND-CPA security of PKE.

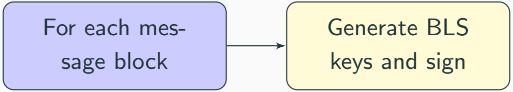
# IUT-k-SAN Construction

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.

# IUT-k-SAN Construction: Sign $(n = 3, k = 2)$




$$m = \boxed{m_1 \mid m_2 \mid m_3 \mid \textbf{PKZ}}$$

$$x = \boxed{x_1 \mid x_2 \mid x_3 \mid x_4}$$

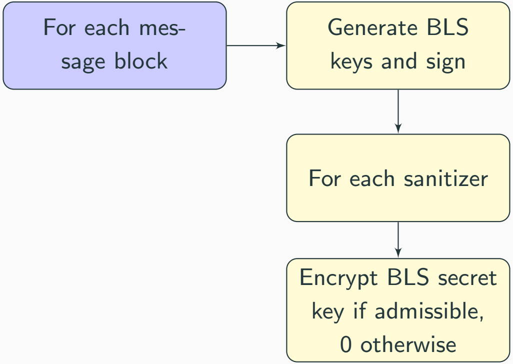
$$y = \boxed{y_1 \mid y_2 \mid y_3 \mid y_4}$$

$$X = \boxed{X_1 \mid X_2 \mid X_3 \mid X_4}$$

$$Y = \boxed{Y_1 \mid Y_2 \mid Y_3 \mid Y_4}$$

$$\sigma = \boxed{\sigma_1 \mid \sigma_2 \mid \sigma_3 \mid \sigma_4}$$

# IUT-k-SAN Construction: Sign $(n = 3, k = 2)$




$$m = \boxed{m_1 \mid m_2 \mid m_3 \mid \mathbf{PKZ}}$$

$$x = \boxed{x_1 \mid x_2 \mid x_3 \mid x_4}$$

$$y = \boxed{y_1 \mid y_2 \mid y_3 \mid y_4}$$

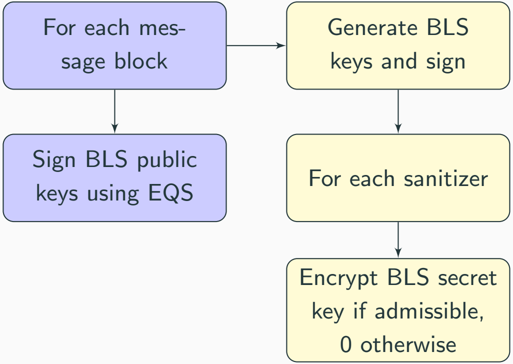
$$X = \boxed{X_1 \mid X_2 \mid X_3 \mid X_4}$$

$$Y = \boxed{Y_1 \mid Y_2 \mid Y_3 \mid Y_4}$$

$$\sigma = \boxed{\sigma_1 \mid \sigma_2 \mid \sigma_3 \mid \sigma_4}$$

$$\mathbf{SKZ} = \begin{array}{|c|c|c|c|} \hline \{0\}_{\mathsf{pk}^1_{\mathsf{ZE}}} & \{y_2\}_{\mathsf{pk}^1_{\mathsf{ZE}}} & \{y_3\}_{\mathsf{pk}^1_{\mathsf{ZE}}} & \{0\}_{\mathsf{pk}^1_{\mathsf{ZE}}} \\ \hline \{0\}_{\mathsf{pk}^2_{\mathsf{ZE}}} & \{0\}_{\mathsf{pk}^2_{\mathsf{ZE}}} & \{y_3\}_{\mathsf{pk}^2_{\mathsf{ZE}}} & \{0\}_{\mathsf{pk}^2_{\mathsf{ZE}}} \\ \hline \end{array}$$

# IUT-k-SAN Construction: Sign $(n = 3, k = 2)$




$$m = \begin{array}{|c|c|c|c|}\hline m_1 & m_2 & m_3 & \textbf{PKZ} \\ \hline \end{array}$$

$$x = \begin{array}{|c|c|c|c|}\hline x_1 & x_2 & x_3 & x_4 \\ \hline \end{array}$$

$$y = \begin{array}{|c|c|c|c|}\hline y_1 & y_2 & y_3 & y_4 \\ \hline \end{array}$$

$$X = \begin{array}{|c|c|c|c|}\hline X_1 & X_2 & X_3 & X_4 \\ \hline \end{array}$$

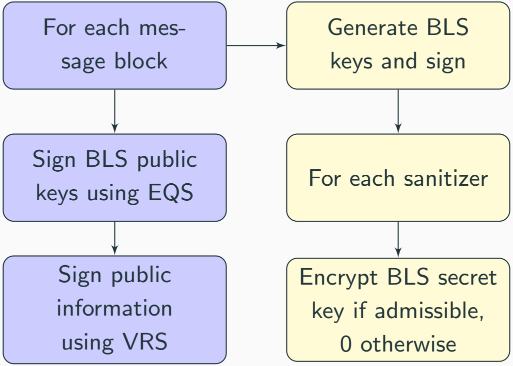
$$Y = \begin{array}{|c|c|c|c|}\hline Y_1 & Y_2 & Y_3 & Y_4 \\ \hline \end{array}$$

$$\sigma = \begin{array}{|c|c|c|c|}\hline \sigma_1 & \sigma_2 & \sigma_3 & \sigma_4 \\ \hline \end{array}$$

$$\textbf{SKZ} = \begin{array}{|c|c|c|c|}\hline \{0\}_{\mathsf{pk}^1_{\mathsf{ZE}}} & \{y_2\}_{\mathsf{pk}^1_{\mathsf{ZE}}} & \{y_3\}_{\mathsf{pk}^1_{\mathsf{ZE}}} & \{0\}_{\mathsf{pk}^1_{\mathsf{ZE}}} \\ \hline \{0\}_{\mathsf{pk}^2_{\mathsf{ZE}}} & \{0\}_{\mathsf{pk}^2_{\mathsf{ZE}}} & \{y_3\}_{\mathsf{pk}^2_{\mathsf{ZE}}} & \{0\}_{\mathsf{pk}^2_{\mathsf{ZE}}} \\ \hline \end{array}$$

$$\mu = \mathsf{Sign}_{\mathsf{EQS}}(X), \eta = \mathsf{Sign}_{\mathsf{EQS}}(Y)$$

# IUT-k-SAN Construction: Sign $(n = 3, k = 2)$




$$m = \begin{array}{|c|c|c|c|}\hline m_1 & m_2 & m_3 & \textbf{PKZ} \\ \hline\end{array}$$

$$x = \begin{array}{|c|c|c|c|}\hline x_1 & x_2 & x_3 & x_4 \\ \hline\end{array}$$

$$y = \begin{array}{|c|c|c|c|}\hline y_1 & y_2 & y_3 & y_4 \\ \hline\end{array}$$

$$X = \begin{array}{|c|c|c|c|}\hline X_1 & X_2 & X_3 & X_4 \\ \hline\end{array}$$

$$Y = \begin{array}{|c|c|c|c|}\hline Y_1 & Y_2 & Y_3 & Y_4 \\ \hline\end{array}$$

$$\sigma = \begin{array}{|c|c|c|c|}\hline \sigma_1 & \sigma_2 & \sigma_3 & \sigma_4 \\ \hline\end{array}$$

$$\textbf{SKZ} = \begin{array}{|c|c|c|c|}\hline \{0\}_{\mathsf{pk}^1_{\mathsf{ZE}}} & \{y_2\}_{\mathsf{pk}^1_{\mathsf{ZE}}} & \{y_3\}_{\mathsf{pk}^1_{\mathsf{ZE}}} & \{0\}_{\mathsf{pk}^1_{\mathsf{ZE}}} \\ \hline \{0\}_{\mathsf{pk}^2_{\mathsf{ZE}}} & \{0\}_{\mathsf{pk}^2_{\mathsf{ZE}}} & \{y_3\}_{\mathsf{pk}^2_{\mathsf{ZE}}} & \{0\}_{\mathsf{pk}^2_{\mathsf{ZE}}} \\ \hline\end{array}$$

$$\mu = \mathsf{Sign}_{\mathsf{EQS}}(X), \eta = \mathsf{Sign}_{\mathsf{EQS}}(Y)$$

$$\sigma_{\mathsf{SS}} = (\mu, \eta, (\sigma_j, X_j, Y_j)_{j \in [\![n]\!]}, \textbf{SKZ})$$

$$\sigma_{\mathsf{VRS}} = \mathsf{Sign}_{\mathsf{VRS}}(\mathsf{pk}_{\mathsf{S}} \| m \| \sigma_{\mathsf{SS}})$$

# IUT-k-SAN Construction: Sanitize $m_2$ by sanitizer 1

Randomize BLS keys

$m' =$

| | | | |
|---|---|---|---|
| $m_1$ | $m_2'$ | $m_3$ | **PKZ** |

$X' =$

| | | | |
|---|---|---|---|
| $X_1^r$ | $X_2^r$ | $X_3^r$ | $X_4^r$ |

$Y' =$

| | | | |
|---|---|---|---|
| $Y_1^{r\cdot s}$ | $Y_2^{r\cdot s}$ | $Y_3^{r\cdot s}$ | $Y_4^{r\cdot s}$ |

$\sigma =$

| | | | |
|---|---|---|---|
| $\sigma_1$ | $\sigma_2$ | $\sigma_3$ | $\sigma_2$ |

**SKZ** $=$

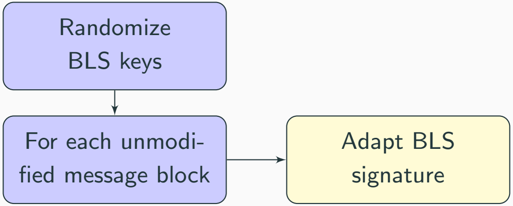
| | | | |
|---|---|---|---|
| $\{0\}_{\mathsf{pk}^1_{\mathsf{ZE}}}$ | $\{y_2\}_{\mathsf{pk}^1_{\mathsf{ZE}}}$ | $\{y_3\}_{\mathsf{pk}^1_{\mathsf{ZE}}}$ | $\{0\}_{\mathsf{pk}^1_{\mathsf{ZE}}}$ |
| $\{0\}_{\mathsf{pk}^2_{\mathsf{ZE}}}$ | $\{0\}_{\mathsf{pk}^2_{\mathsf{ZE}}}$ | $\{y_3\}_{\mathsf{pk}^2_{\mathsf{ZE}}}$ | $\{0\}_{\mathsf{pk}^2_{\mathsf{ZE}}}$ |

$$\mu = \mathsf{Sign}_{\mathsf{EQS}}(X), \eta = \mathsf{Sign}_{\mathsf{EQS}}(Y)$$

$$\sigma_{\mathsf{SS}} = (\mu, \eta, (\sigma_j, X_j, Y_j)_{j\in[\![n]\!]}, \mathbf{SKZ})$$

$$\sigma_{\mathsf{VRS}} = \mathsf{Sign}_{\mathsf{VRS}}(\mathsf{pk}_{\mathsf{S}} \| m \| \sigma_{\mathsf{SS}})$$

# IUT-k-SAN Construction: Sanitize $m_2$ by sanitizer 1




$m' =$

| | | | |
|---|---|---|---|
| $m_1$ | $m_2'$ | $m_3$ | **PKZ** |

$X' =$

| | | | |
|---|---|---|---|
| $X_1^r$ | $X_2^r$ | $X_3^r$ | $X_4^r$ |

$Y' =$

| | | | |
|---|---|---|---|
| $Y_1^{r \cdot s}$ | $Y_2^{r \cdot s}$ | $Y_3^{r \cdot s}$ | $Y_4^{r \cdot s}$ |

$\sigma' =$

| | | | |
|---|---|---|---|
| $\sigma_1^s$ | $\sigma_2$ | $\sigma_3^s$ | $\sigma_2^s$ |

**SKZ** $=$

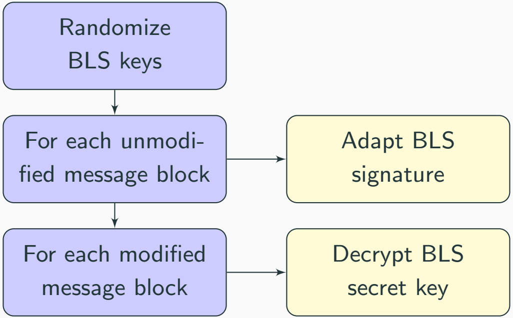
| | | | |
|---|---|---|---|
| $\{0\}_{\mathsf{pk}^1_{\mathsf{ZE}}}$ | $\{y_2\}_{\mathsf{pk}^1_{\mathsf{ZE}}}$ | $\{y_3\}_{\mathsf{pk}^1_{\mathsf{ZE}}}$ | $\{0\}_{\mathsf{pk}^1_{\mathsf{ZE}}}$ |
| $\{0\}_{\mathsf{pk}^2_{\mathsf{ZE}}}$ | $\{0\}_{\mathsf{pk}^2_{\mathsf{ZE}}}$ | $\{y_3\}_{\mathsf{pk}^2_{\mathsf{ZE}}}$ | $\{0\}_{\mathsf{pk}^2_{\mathsf{ZE}}}$ |

$$\mu = \mathsf{Sign}_{\mathsf{EQS}}(X), \eta = \mathsf{Sign}_{\mathsf{EQS}}(Y)$$

$$\sigma_{\mathsf{SS}} = (\mu, \eta, (\sigma_j, X_j, Y_j)_{j \in [\![n]\!]}, \mathbf{SKZ})$$

$$\sigma_{\mathsf{VRS}} = \mathsf{Sign}_{\mathsf{VRS}}(\mathsf{pk}_S \| m \| \sigma_{\mathsf{SS}})$$

# IUT-k-SAN Construction: Sanitize $m_2$ by sanitizer 1




$m' =$

| | | | |
|---|---|---|---|
| $m_1$ | $m'_2$ | $m_3$ | **PKZ** |

$X' =$

| | | | |
|---|---|---|---|
| $X_1^r$ | $X_2^r$ | $X_3^r$ | $X_4^r$ |

$Y' =$

| | | | |
|---|---|---|---|
| $Y_1^{r \cdot s}$ | $Y_2^{r \cdot s}$ | $Y_3^{r \cdot s}$ | $Y_4^{r \cdot s}$ |

$\sigma' =$

| | | | |
|---|---|---|---|
| $\sigma_1^s$ | $\sigma_2$ | $\sigma_3^s$ | $\sigma_2^s$ |

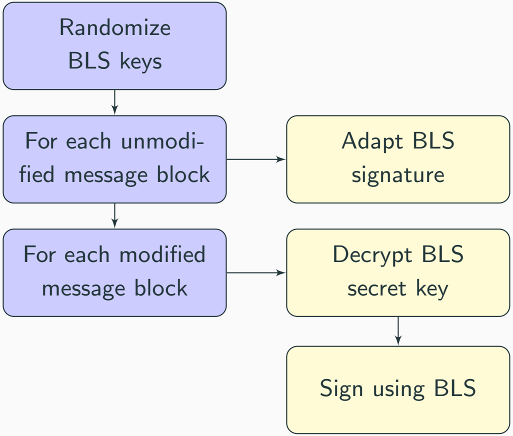
**SKZ** $=$

| | | | |
|---|---|---|---|
| $\{0\}_{\mathsf{pk}_{\mathsf{ZE}}^1}$ | $\{y_2\}_{\mathsf{pk}_{\mathsf{ZE}}^1}$ | $\{y_3\}_{\mathsf{pk}_{\mathsf{ZE}}^1}$ | $\{0\}_{\mathsf{pk}_{\mathsf{ZE}}^1}$ |
| $\{0\}_{\mathsf{pk}_{\mathsf{ZE}}^2}$ | $\{0\}_{\mathsf{pk}_{\mathsf{ZE}}^2}$ | $\{y_3\}_{\mathsf{pk}_{\mathsf{ZE}}^2}$ | $\{0\}_{\mathsf{pk}_{\mathsf{ZE}}^2}$ |

$$\mu = \mathsf{Sign}_{\mathsf{EQS}}(X), \eta = \mathsf{Sign}_{\mathsf{EQS}}(Y)$$

$$\sigma_{\mathsf{SS}} = (\mu, \eta, (\sigma_j, X_j, Y_j)_{j \in [\![n]\!]}, \mathbf{SKZ})$$

$$\sigma_{\mathsf{VRS}} = \mathsf{Sign}_{\mathsf{VRS}}(\mathsf{pk}_{\mathsf{S}} \| m \| \sigma_{\mathsf{SS}})$$




$$m' = \begin{array}{|c|c|c|c|}\hline m_1 & m_2' & m_3 & \textbf{PKZ} \\ \hline \end{array}$$

$$X' = \begin{array}{|c|c|c|c|}\hline X_1^r & X_2^r & X_3^r & X_4^r \\ \hline \end{array}$$

$$Y' = \begin{array}{|c|c|c|c|}\hline Y_1^{r\cdot s} & Y_2^{r\cdot s} & Y_3^{r\cdot s} & Y_4^{r\cdot s} \\ \hline \end{array}$$

$$\sigma' = \begin{array}{|c|c|c|c|}\hline \sigma_1^s & \color{blue}{\sigma_2'} & \sigma_3^s & \sigma_2^s \\ \hline \end{array}$$

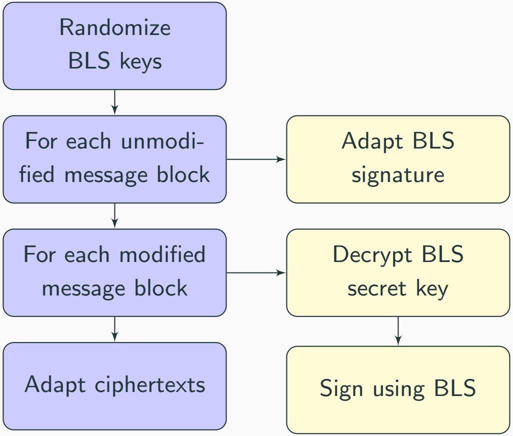
$$\textbf{SKZ} = \begin{array}{|c|c|c|c|}\hline \{0\}_{\mathsf{pk}_{\mathsf{ZE}}^1} & \{y_2\}_{\mathsf{pk}_{\mathsf{ZE}}^1} & \{y_3\}_{\mathsf{pk}_{\mathsf{ZE}}^1} & \{0\}_{\mathsf{pk}_{\mathsf{ZE}}^1} \\ \hline \{0\}_{\mathsf{pk}_{\mathsf{ZE}}^2} & \{0\}_{\mathsf{pk}_{\mathsf{ZE}}^2} & \{y_3\}_{\mathsf{pk}_{\mathsf{ZE}}^2} & \{0\}_{\mathsf{pk}_{\mathsf{ZE}}^2} \\ \hline \end{array}$$

$$\mu = \mathsf{Sign}_{\mathsf{EQS}}(X), \eta = \mathsf{Sign}_{\mathsf{EQS}}(Y)$$

$$\sigma_{\mathsf{SS}} = (\mu, \eta, (\sigma_j, X_j, Y_j)_{j \in [\![n]\!]}, \textbf{SKZ})$$

$$\sigma_{\mathsf{VRS}} = \mathsf{Sign}_{\mathsf{VRS}}(\mathsf{pk}_{\mathsf{S}} \| m \| \sigma_{\mathsf{SS}})$$

# IUT-k-SAN Construction: Sanitize $m_2$ by sanitizer 1




$m' =$

| | | | |
|---|---|---|---|
| $m_1$ | $m'_2$ | $m_3$ | **PKZ** |

$X' =$

| | | | |
|---|---|---|---|
| $X_1^r$ | $X_2^r$ | $X_3^r$ | $X_4^r$ |

$Y' =$

| | | | |
|---|---|---|---|
| $Y_1^{r\cdot s}$ | $Y_2^{r\cdot s}$ | $Y_3^{r\cdot s}$ | $Y_4^{r\cdot s}$ |

$\sigma' =$

| | | | |
|---|---|---|---|
| $\sigma_1^s$ | $\sigma'_2$ | $\sigma_3^s$ | $\sigma_2^s$ |

**SKZ**$' =$

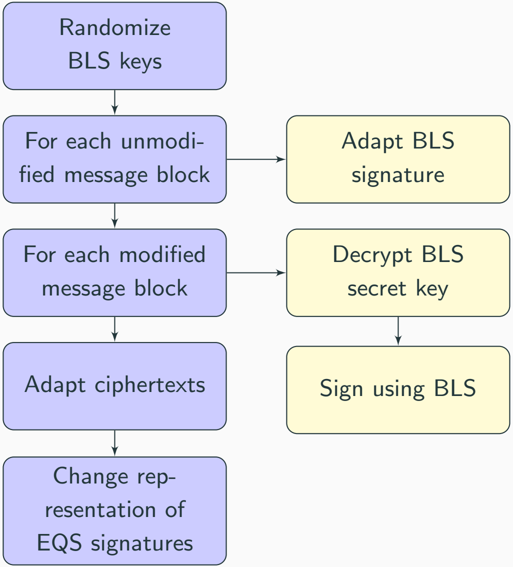
| | | | |
|---|---|---|---|
| $\{0\}^s_{\mathsf{pk}^1_{\mathsf{ZE}}}$ | $\{y_2\}^s_{\mathsf{pk}^1_{\mathsf{ZE}}}$ | $\{y_3\}^s_{\mathsf{pk}^1_{\mathsf{ZE}}}$ | $\{0\}^s_{\mathsf{pk}^1_{\mathsf{ZE}}}$ |
| $\{0\}^s_{\mathsf{pk}^2_{\mathsf{ZE}}}$ | $\{0\}^s_{\mathsf{pk}^2_{\mathsf{ZE}}}$ | $\{y_3\}^s_{\mathsf{pk}^2_{\mathsf{ZE}}}$ | $\{0\}^s_{\mathsf{pk}^2_{\mathsf{ZE}}}$ |

$$\mu = \mathsf{Sign}_{\mathsf{EQS}}(X), \eta = \mathsf{Sign}_{\mathsf{EQS}}(Y)$$

$$\sigma_{\mathsf{SS}} = (\mu, \eta, (\sigma_j, X_j, Y_j)_{j\in[\![n]\!]}, \mathbf{SKZ})$$

$$\sigma_{\mathsf{VRS}} = \mathsf{Sign}_{\mathsf{VRS}}(\mathsf{pk}_{\mathsf{S}} \| m \| \sigma_{\mathsf{SS}})$$

# IUT-k-SAN Construction: Sanitize $m_2$ by sanitizer 1




$$m' = \begin{array}{|c|c|c|c|}\hline m_1 & m_2' & m_3 & \mathbf{PKZ} \\ \hline\end{array}$$

$$X' = \begin{array}{|c|c|c|c|}\hline X_1^r & X_2^r & X_3^r & X_4^r \\ \hline\end{array}$$

$$Y' = \begin{array}{|c|c|c|c|}\hline Y_1^{r\cdot s} & Y_2^{r\cdot s} & Y_3^{r\cdot s} & Y_4^{r\cdot s} \\ \hline\end{array}$$

$$\sigma' = \begin{array}{|c|c|c|c|}\hline \sigma_1^s & \sigma_2' & \sigma_3^s & \sigma_2^s \\ \hline\end{array}$$

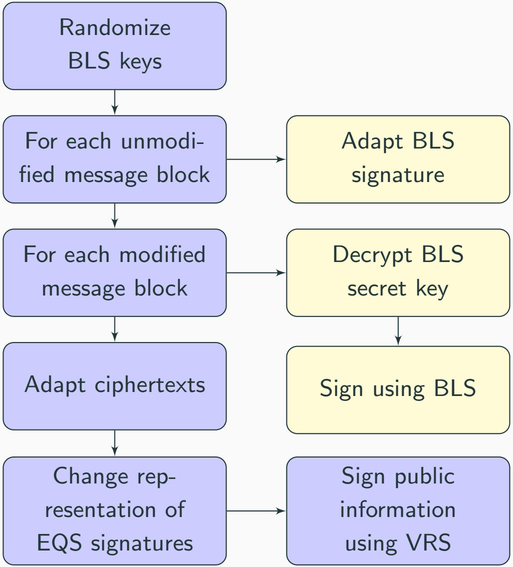
$$\mathbf{SKZ}' = \begin{array}{|c|c|c|c|}\hline \{0\}^s_{\mathsf{pk}^1_{\mathsf{ZE}}} & \{y_2\}^s_{\mathsf{pk}^1_{\mathsf{ZE}}} & \{y_3\}^s_{\mathsf{pk}^1_{\mathsf{ZE}}} & \{0\}^s_{\mathsf{pk}^1_{\mathsf{ZE}}} \\ \hline \{0\}^s_{\mathsf{pk}^2_{\mathsf{ZE}}} & \{0\}^s_{\mathsf{pk}^2_{\mathsf{ZE}}} & \{y_3\}^s_{\mathsf{pk}^2_{\mathsf{ZE}}} & \{0\}^s_{\mathsf{pk}^2_{\mathsf{ZE}}} \\ \hline\end{array}$$

$$\mu' = \mathsf{ChgRep}_{\mathsf{EQS}}(\mu, r), \eta' = \mathsf{ChgRep}_{\mathsf{EQS}}(\eta, r \cdot s)$$

$$\sigma_{\mathsf{SS}} = (\mu, \eta, (\sigma_j, X_j, Y_j)_{j\in[\![n]\!]}, \mathbf{SKZ})$$

$$\sigma_{\mathsf{VRS}} = \mathsf{Sign}_{\mathsf{VRS}}(\mathsf{pk}_{\mathsf{S}} \| m \| \sigma_{\mathsf{SS}})$$

# IUT-k-SAN Construction: Sanitize $m_2$ by sanitizer 1




$$m' = \begin{array}{|c|c|c|c|}\hline m_1 & m_2' & m_3 & \textbf{PKZ} \\ \hline\end{array}$$

$$X' = \begin{array}{|c|c|c|c|}\hline X_1^r & X_2^r & X_3^r & X_4^r \\ \hline\end{array}$$

$$Y' = \begin{array}{|c|c|c|c|}\hline Y_1^{r\cdot s} & Y_2^{r\cdot s} & Y_3^{r\cdot s} & Y_4^{r\cdot s} \\ \hline\end{array}$$

$$\sigma' = \begin{array}{|c|c|c|c|}\hline \sigma_1^s & \sigma_2' & \sigma_3^s & \sigma_2^s \\ \hline\end{array}$$

$$\textbf{SKZ}' = \begin{array}{|c|c|c|c|}\hline \{0\}^s_{\mathsf{pk}^1_{\mathsf{ZE}}} & \{y_2\}^s_{\mathsf{pk}^1_{\mathsf{ZE}}} & \{y_3\}^s_{\mathsf{pk}^1_{\mathsf{ZE}}} & \{0\}^s_{\mathsf{pk}^1_{\mathsf{ZE}}} \\ \hline \{0\}^s_{\mathsf{pk}^2_{\mathsf{ZE}}} & \{0\}^s_{\mathsf{pk}^2_{\mathsf{ZE}}} & \{y_3\}^s_{\mathsf{pk}^2_{\mathsf{ZE}}} & \{0\}^s_{\mathsf{pk}^2_{\mathsf{ZE}}} \\ \hline\end{array}$$

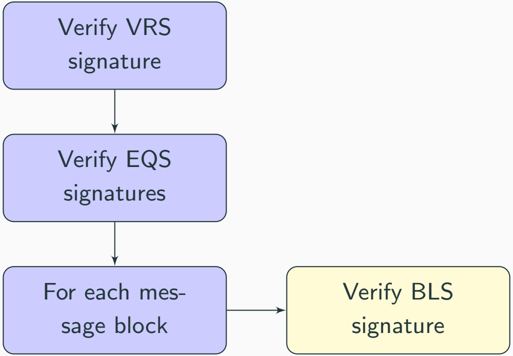
$$\mu' = \mathsf{ChgRep}_{\mathsf{EQS}}(\mu, r), \eta' = \mathsf{ChgRep}_{\mathsf{EQS}}(\eta, r \cdot s)$$

$$\sigma_{\mathsf{SS}}' = (\mu', \eta', (\sigma_j', X_j', Y_j')_{j \in [\![n]\!]}, \textbf{SKZ}')$$

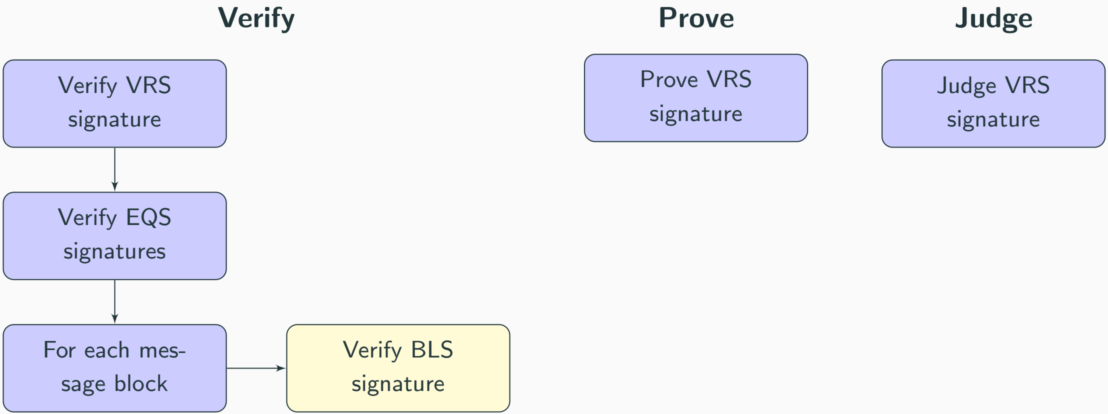
$$\sigma_{\mathsf{VRS}}' = \mathsf{Sign}_{\mathsf{VRS}}(\mathsf{pk}_{\mathsf{S}} \| m' \| \sigma_{\mathsf{SS}}')$$

# IUT-k-SAN Construction: Verify, Prove, and Judge

## Verify



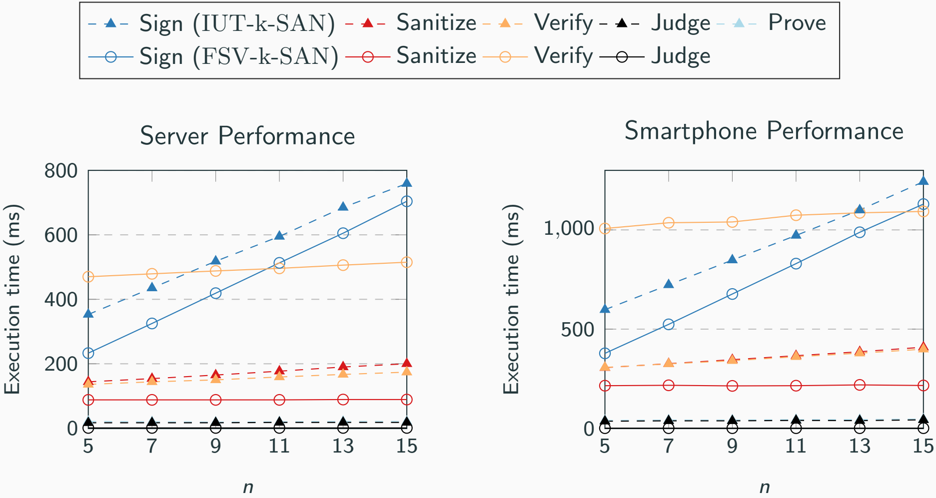
# IUT-k-SAN Construction: Verify, Prove, and Judge



# IUT-k-SAN Security

- **Unforgeability** implied by accountability.
- **Immutability** relies on the unforgeability of BLS-like and EQS signatures and the IND-CPA security of PKE.
- **Accountability** relies on the accountability and non-seizability of VRS.
- **Privacy** implied by proof-restricted transparency.
- **Proof-Restricted Transparency** relies on perfect adaptation of EQS, the unlinkability of PKE, the anonymity of VRS, and the unlinkable randomization of BLS-like signatures.
- **Unlinkability** relies on the correctness and IND-CPA security of PKE, the perfect adaptation of EQS, and the unlinkable randomization of BLS-like signatures and public keys.
- **Invisibility** relies on the IND-CPA security of PKE.
- **Sanitizer Anonymity** relies on the anonymity of VRS and the IND-CPA security of PKE.

# Rust Implementation Performance



# End

Thanks for your attention!

# Appendix

# FSV-k-SAN Construction

**$\mathsf{Sign}(\mathsf{sk_S}, \mathbf{PKZ}, m, \mathbf{A})$**

$$
\begin{aligned}
&\textbf{foreach } j \in [\![n]\!] \textbf{ do}\\
&\quad (\mathsf{sk_{CH}}, \mathbf{CH}_j.\mathsf{pk_{CH}}) \leftarrow \mathsf{KGen_{CHash}}(\mathsf{pp})\\
&\quad (\mathbf{CH}_j.h, \mathbf{CH}_j.r) \leftarrow \mathsf{Hash_{CHash}}(\mathsf{pk_{CH}}, (j \| m_j))\\
&\quad \textbf{foreach } i \in [\![k]\!] \textbf{ do}\\
&\quad\quad \mathbf{SKCH}_{i,j} \leftarrow \mathsf{Encrypt_{PKE}}(\mathsf{pk^i_{ZE}}, \mathsf{sk_{CH}} \cdot a_{i,j})\\
&\mathbf{PA} := (\mathsf{ADM}^{\mathbf{A}}(j))_{j \in [\![n]\!]}\\
&ms := \begin{pmatrix} (\mathbf{CH}_j.h, \mathbf{CH}_j.\mathsf{pk_{CH}})_{j \in [\![n]\!]}, \mathbf{SKCH}, \\ \mathbf{PA}, \mathsf{pk_S}, \mathbf{PKZ}, n \end{pmatrix}\\
&s \leftarrow \mathsf{Sign_{SIG}}(\mathsf{sk_S}, ms)\\
&\textbf{foreach } j \in [\![n]\!] \textbf{ do}\\
&\quad \rho_j \leftarrow \mathsf{Sign_{SIG}}(\mathsf{sk_S}, (j \| m_j \| s))\\
&\sigma := (s, \mathbf{CH}, \mathbf{SKCH}, \mathbf{PA}, n, \rho)\\
&\textbf{return } \sigma
\end{aligned}
$$

**$\mathsf{Sanitize}(\mathsf{sk_Z}, \mathsf{pk_S}, \mathbf{PKZ}, m, \mathsf{MOD}, \sigma)$**

$$
\begin{aligned}
&m' = \mathsf{MOD}(m), L := \{\mathsf{pk^i_{ZP}}\}_{i \in [\![k]\!]}, \mathbf{CH}' := \mathbf{CH}\\
&\rho' := \rho, i' := i \in [\![k]\!] \mid \mathsf{pk_Z} = (\mathsf{pk^i_{ZE}}, \mathsf{pk^i_{ZP}})\\
&\textbf{foreach } j \in [\![n]\!] \textbf{ do}\\
&\quad \textbf{if } j \in \mathsf{MOD} \textbf{ then}\\
&\quad\quad \tau \leftarrow \mathsf{Decrypt_{PKE}}(\mathsf{sk_{ZE}}, \mathbf{SKCH}_{i',j})\\
&\quad\quad \mathbf{CH}'_j.r \leftarrow \mathsf{Adapt_{CHash}}(\tau, (j \| m_j), (j \| m'_j), r_j, h_j)\\
&\quad\quad \rho'_j \leftarrow \mathsf{Sign_{VRS}}(\mathsf{sk_{ZP}}, L, (j \| m'_j \| s))\\
&\sigma' := (s, \mathbf{CH}', \mathbf{SKCH}, \mathbf{PA}, n, \rho')\\
&\textbf{return } \sigma'
\end{aligned}
$$

# FSV-k-SAN Construction

**Verify**$(\mathsf{pk_S}, \mathbf{PKZ}, m, \sigma)$

$$ms := \begin{pmatrix} (h_j, \mathsf{pk}^j_{\mathsf{CH}})_{j\in[\![n]\!]}, \mathbf{SKCH}, \\ \mathbf{PA}, \mathsf{pk_S}, \mathbf{PKZ}, n \end{pmatrix}$$

$$b_1 \leftarrow \mathsf{Verify_{SIG}}(\mathsf{pk_S}, ms, s)$$

$$b_2 := \bigwedge_{j=1}^{n} \left\{ \mathsf{Check_{CHash}}(\mathsf{pk}^j_{\mathsf{CH}}, (j\|m_j), r_j, h_j) \right\}$$

$$L := \{\mathsf{pk}^i_{\mathsf{ZP}}\}_{i\in[\![k]\!]}$$

$$b_3 := \bigwedge_{j=1}^{n} \left\{ \begin{array}{c} \begin{pmatrix} \neg\mathbf{PA}_j \wedge \\ \mathsf{Verify_{SIG}}(\mathsf{pk_S}, (j\|m_j\|s), \rho_j) = 1 \end{pmatrix} \\ \vee \begin{pmatrix} \mathbf{PA}_j \wedge \\ \mathsf{Verify_{VRS}}(L, (j\|m_j\|s), \rho_j) = 1 \end{pmatrix} \end{array} \right\}$$

**return** $b_1 \wedge b_2 \wedge b_3$

**Judge**$(\mathsf{pk_S}, \mathbf{PKZ}, m, \sigma, \pi, j)$

**if** $j = \perp$ **then**
  **if** $\exists j \in [\![n]\!], \mathbf{PA}_j = 1$ **then return** $Z$
  **else return** $S$
**else**
  **if** $\mathbf{PA}_j = 1$ **then return** $Z$
  **else return** $S$

# IUT-k-SAN Construction

**$\mathsf{Sign}(\mathsf{sk_S}, \mathbf{PKZ}, m, \mathbf{A})$**

$m := m \| \mathbf{PKZ}, \mathbf{A} \leftarrow \mathsf{AppendC}(\mathbf{A}, (0)^{[\![k]\!]})$
$x_j, y_j \leftarrow\!\!\$\ \mathbb{Z}_q^*, X_j := G_1^{x_j}, Y_j := X_j^{y_j}, \forall j \in [\![n]\!]$
$\mu := \mathsf{Sign_{EQS}}(\mathsf{sk_{EQS}}, (X_j)_{j \in [\![n]\!]})$
$\eta := \mathsf{Sign_{EQS}}(\mathsf{sk_{EQS}}, (Y_j)_{j \in [\![n]\!]})$
$\sigma_j := \mathsf{H}(j \| m_j)^{y_j}, \forall j \in [\![n]\!]$
**foreach** $i \in [\![k]\!], j \in [\![n]\!]$ **do**
  $\mathbf{SKZ}_{i,j} \leftarrow \mathsf{Encrypt_{PKE}}(\mathsf{pk_{ZE}^i}, y_j \cdot a_{i,j})$
$\sigma_{\mathsf{SS}} := (\mu, \eta, (\sigma_j, X_j, Y_j)_{j \in [\![n]\!]}, \mathbf{SKZ})$
$t := \mathsf{pk_S} \| m \| \sigma_{\mathsf{SS}}, L := \{\mathsf{pk_{SP}}\} \cup \{\mathsf{pk_{ZP}^i}\}_{i \in [\![k]\!]}$
$\sigma_{\mathsf{VRS}} \leftarrow \mathsf{Sign_{VRS}}(\mathsf{sk_{SP}}, L, t)$
$\sigma := (\sigma_{\mathsf{SS}}, \sigma_{\mathsf{VRS}})$
**return** $\sigma$

**$\mathsf{Sanitize}(\mathsf{sk_Z}, \mathsf{pk_S}, \mathbf{PKZ}, m, \mathsf{MOD}, \sigma)$**

$m := m \| \mathbf{PKZ}, m' = \mathsf{MOD}(m), r, s \leftarrow\!\!\$\ \mathbb{Z}_q^*$
$i' := \{i \in [\![k]\!] \mid \mathsf{pk_Z} = (\mathsf{pk_{ZE}^i}, \mathsf{pk_{ZP}^i})\}$
$(X_j')_{j \in [\![n]\!]} := (X_j^r)_{j \in [\![n]\!]}, (Y_j')_{j \in [\![n]\!]} := (Y_j^{r \cdot s})_{j \in [\![n]\!]}$
$\mu' \leftarrow \mathsf{ChgRep_{EQS}}(\mathsf{pk_{EQS}}, (X_j)_{j \in [\![n]\!]}, \mu, r)$
$\eta' \leftarrow \mathsf{ChgRep_{EQS}}(\mathsf{pk_{EQS}}, (Y_j)_{j \in [\![n]\!]}, \eta, r \cdot s)$
**foreach** $j \in [\![n]\!]$ **do**
  **if** $j \in \mathsf{MOD}$ **do**
    $\zeta \leftarrow \mathsf{Decrypt_{PKE}}(\mathsf{sk_{ZE}}, \mathbf{SKZ}_{i',j}), \sigma_j' := \mathsf{H}(j \| m_j')^{\zeta \cdot s}$
  **else** $\sigma_j' := \sigma_j^s$
  **foreach** $i \in [\![k]\!]$ **do**
    $\mathbf{SKZ}'_{i,j} \leftarrow \mathsf{Multiply_{PKE}}(\mathsf{pk_{ZE}^i}, \mathbf{SKZ}_{i,j}, s)$
$\sigma_{\mathsf{SS}}' := (\mu', \eta', (\sigma_j', X_j', Y_j')_{j \in [\![n]\!]}, \mathbf{SKZ}')$
$t := \mathsf{pk_S} \| m' \| \sigma_{\mathsf{SS}}', L := \{\mathsf{pk_{SP}}\} \cup \{\mathsf{pk_{ZP}^i}\}_{i \in [\![k]\!]}$
$\sigma_{\mathsf{VRS}}' \leftarrow \mathsf{Sign_{VRS}}(\mathsf{sk_{ZP}}, L, t)$
**return** $\sigma' := (\sigma_{\mathsf{SS}}', \sigma_{\mathsf{VRS}}')$

# IUT-k-SAN Construction

**Verify**$(\mathsf{pk_S}, \mathbf{PKZ}, m, \sigma)$

$m := m \| \mathbf{PKZ}, t := \mathsf{pk_S} \| m \| \sigma_{SS}$
$L := \{\mathsf{pk_{SP}}\} \cup \{\mathsf{pk^i_{ZP}}\}_{i \in [\![k]\!]}$
$b_1 \leftarrow \mathsf{Verify_{VRS}}(L, t, \sigma_{VRS})$
$b_2 := (\forall j \in [\![n]\!], Y_j \neq G_1)$
$b_3 \leftarrow \mathsf{Verify_{EQS}}(\mathsf{pk_{EQS}}, (X_j)_{j \in [\![n]\!]}, \mu)$
$b_4 \leftarrow \mathsf{Verify_{EQS}}(\mathsf{pk_{EQS}}, (Y_j)_{j \in [\![n]\!]}, \eta)$
$b_5 := (\forall j \in [\![n]\!], (e(X_j, \sigma_j) = e(Y_j, \mathsf{H}(j \| m_j))))$
**return** $\bigwedge_{j=1}^{5} b_j$

**Prove**$(\mathsf{sk_S}, \mathbf{PKZ}, m, \sigma, j)$

$m := m \| \mathbf{PKZ}, t := \mathsf{pk_S} \| m \| \sigma_{SS}$
$L := \{\mathsf{pk_{SP}}\} \cup \{\mathsf{pk^i_{ZP}}\}_{i \in [\![k]\!]}$
$\pi \leftarrow \mathsf{Prove_{VRS}}(L, t, \sigma_{VRS}, \mathsf{pk_{SP}}, \mathsf{sk_{SP}})$
**return** $\pi$

**Judge**$(\mathsf{pk_S}, \mathbf{PKZ}, m, \sigma, \pi, j)$

$m := m \| \mathbf{PKZ}, t := \mathsf{pk_S} \| m \| \sigma_{SS}$
$L := \{\mathsf{pk_{SP}}\} \cup \{\mathsf{pk^i_{ZP}}\}_{i \in [\![k]\!]}$
$b \leftarrow \mathsf{Judge_{VRS}}(L, t, \sigma_{VRS}, \mathsf{pk_{SP}}, \pi)$
**return** $Z$ **if** $b = 0$ and $S$ **if** $b = 1$