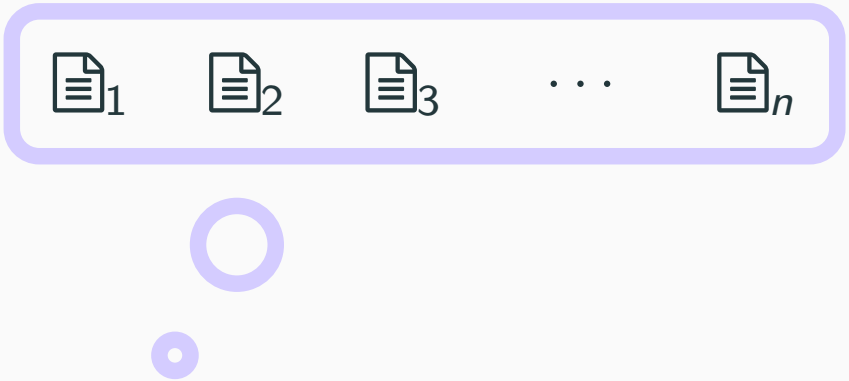
On the Impossibility of Algebraic Vector Commitments in Pairing-Free Groups

Dario Catalano[1] Dario Fiore[2] Rosario Gennaro[3] Emanuele Giunta[2,4]

1. University of Catania, Italy.
2. IMDEA Software Institute, Madrid, Spain.
3. Protocol Labs.
4. Universidad Politecnica de Madrid, Spain.

Università di Catania

Vector Commitments

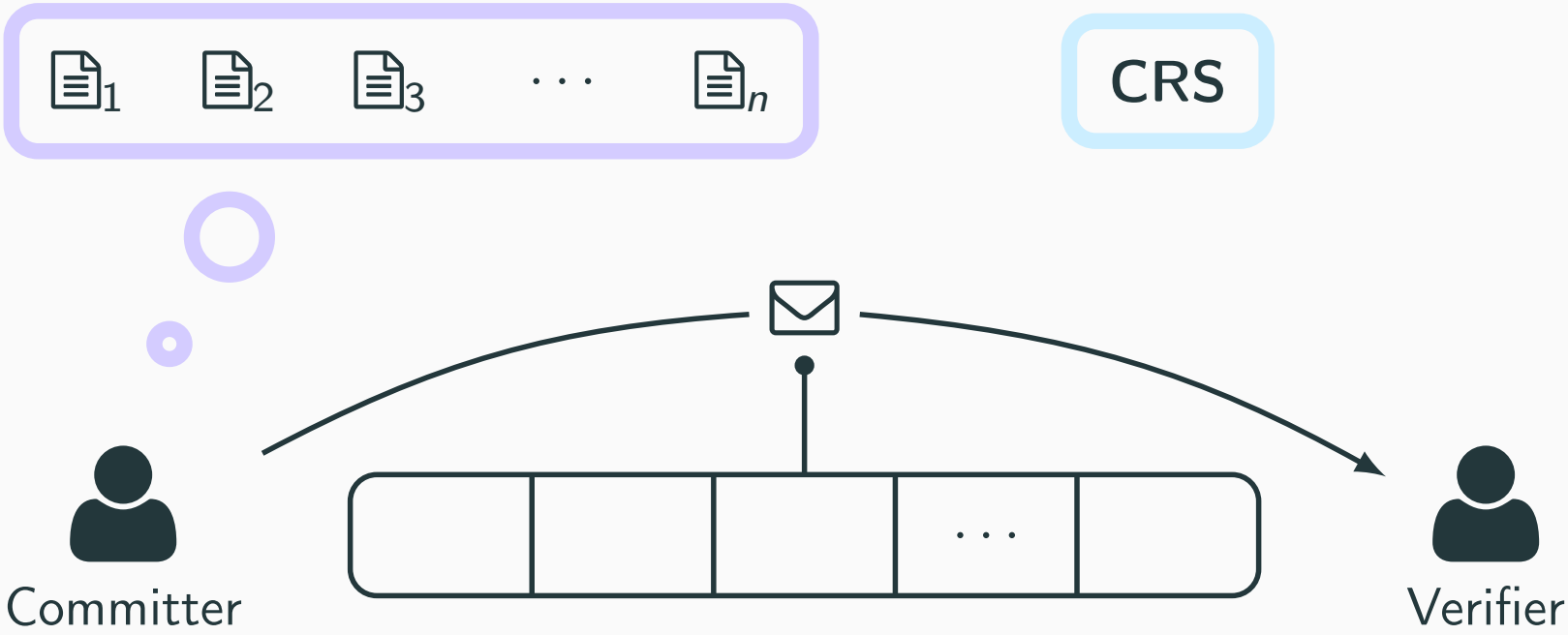


CRS

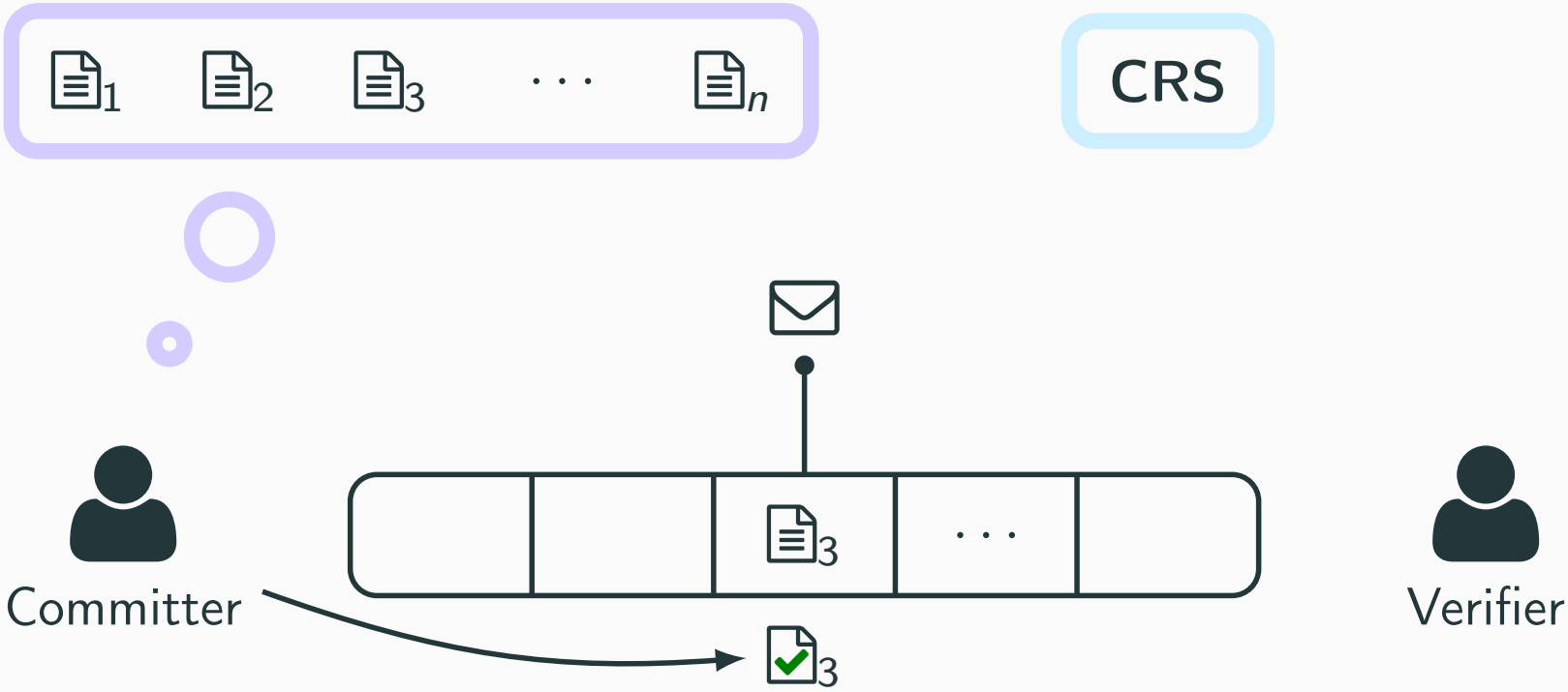
Committer

Verifier

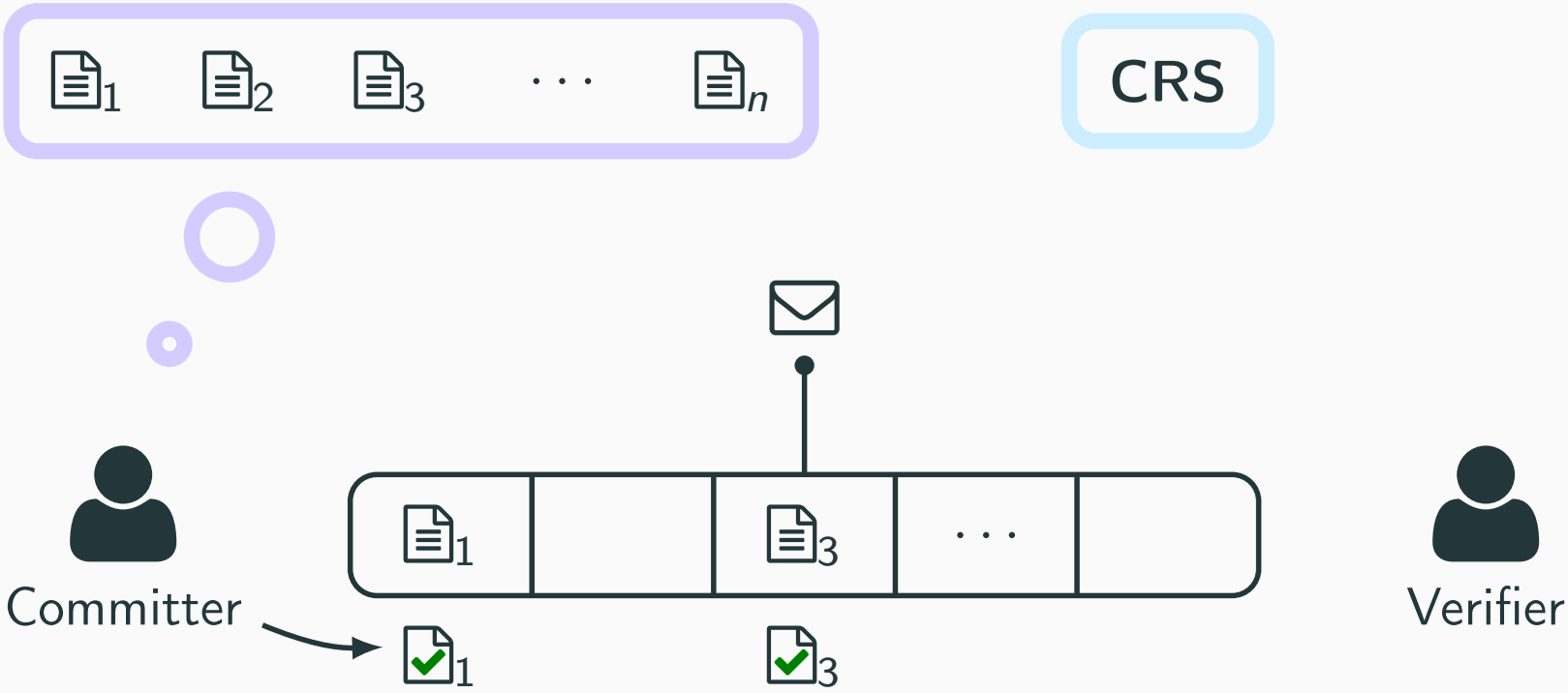
Vector Commitments



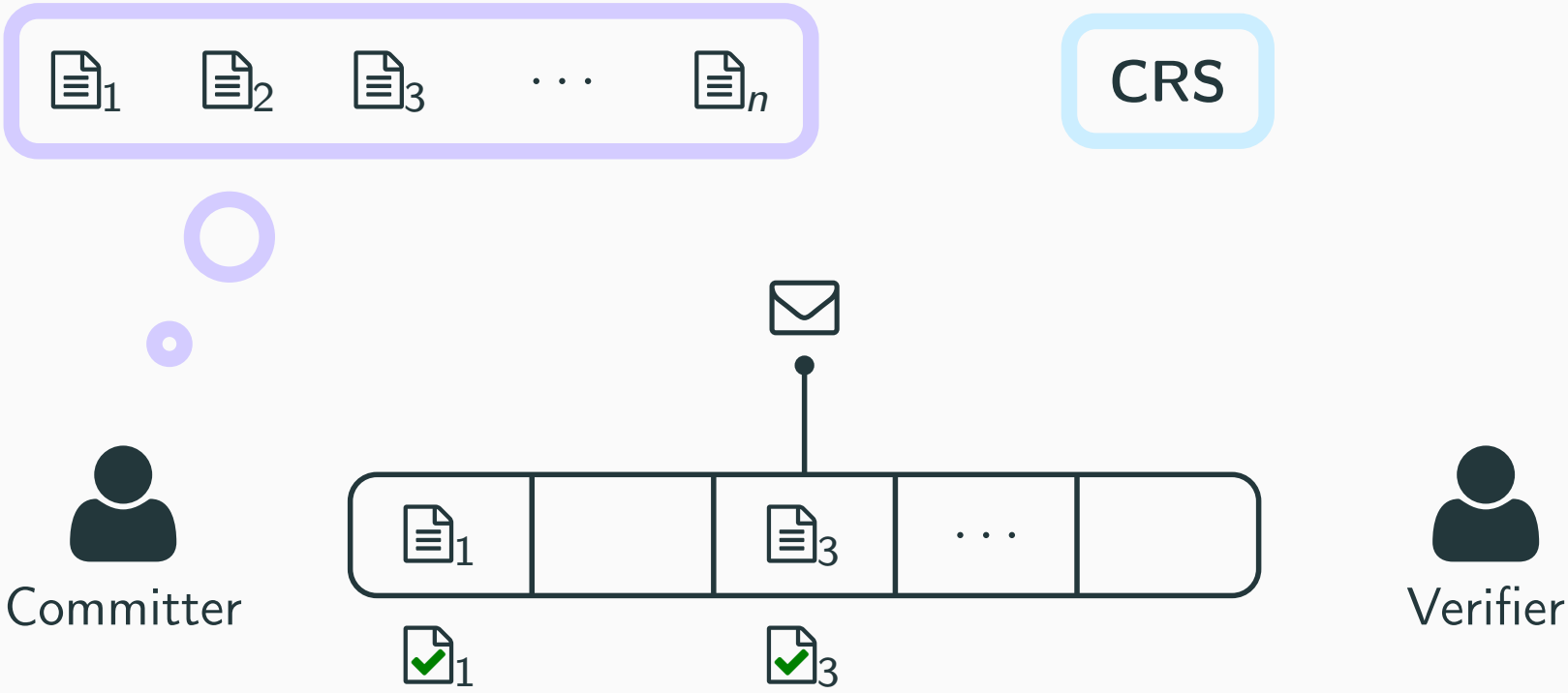
Vector Commitments



Vector Commitments



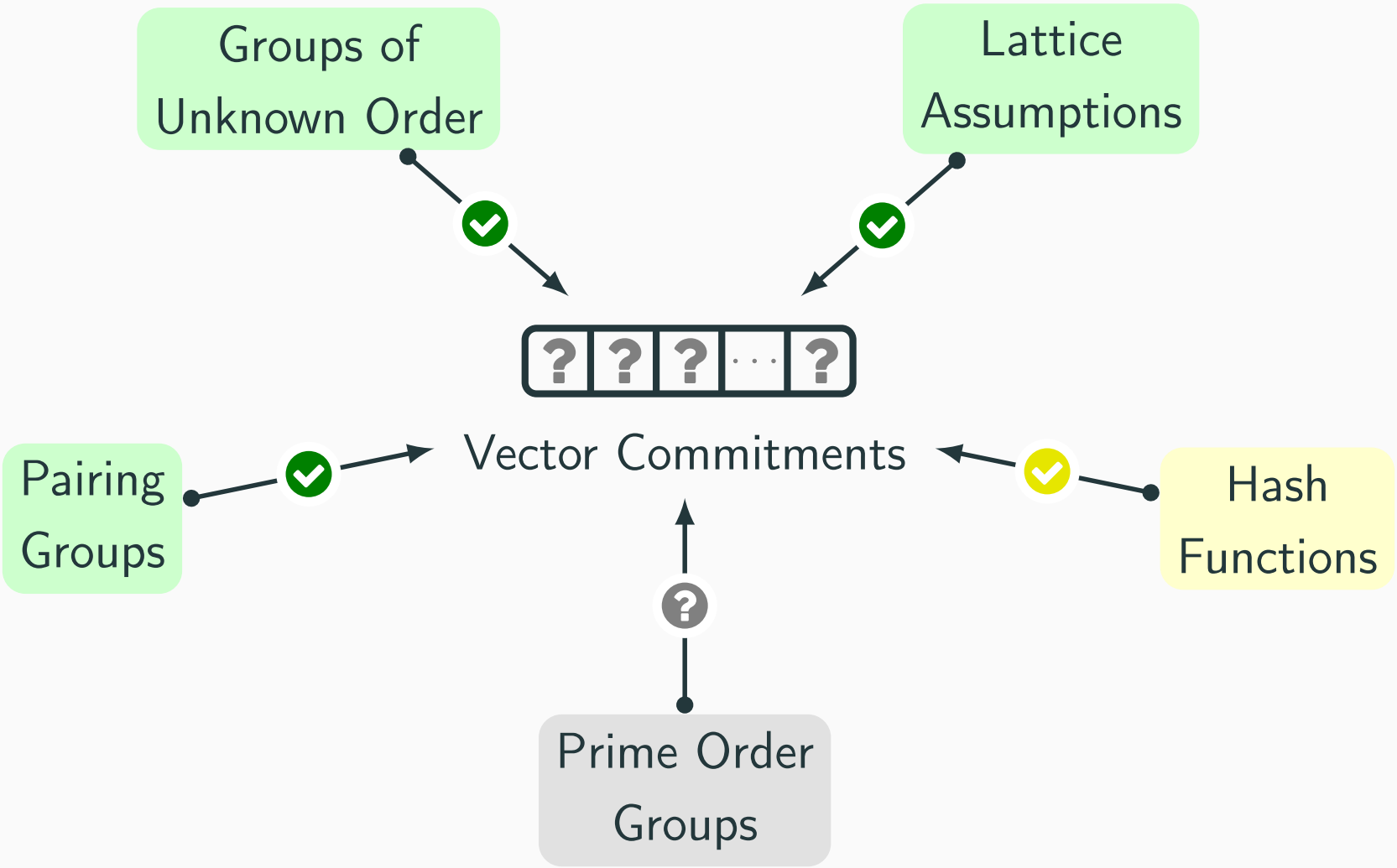
Vector Commitments



Succinctness: $\square$ and $\square$ have length $O(\log n)$.

Position Binding: hard to open $\square$ to two different m_i, m_i^* at position i.

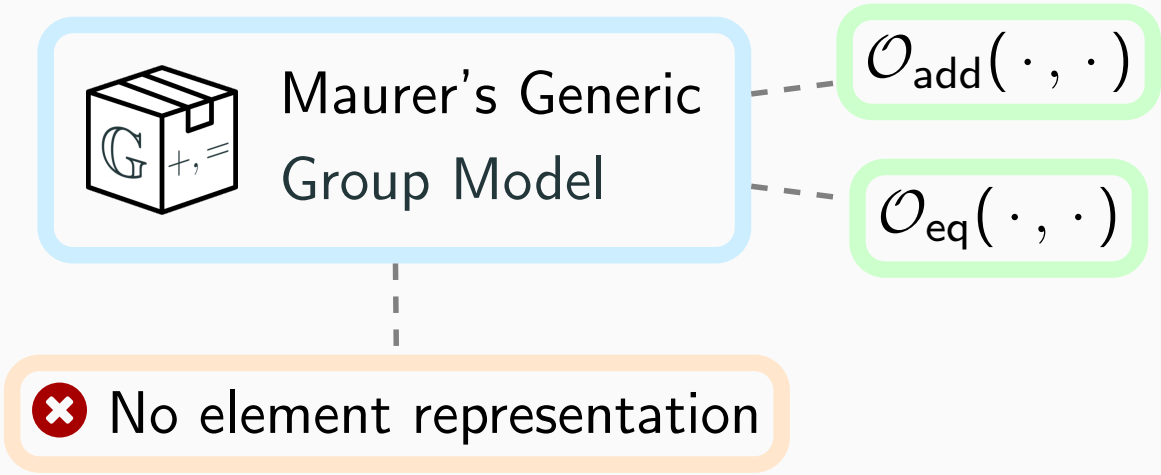
State of the Art



Algebraic Vector Commitments

A Vector Commitment is **Algebraic** if

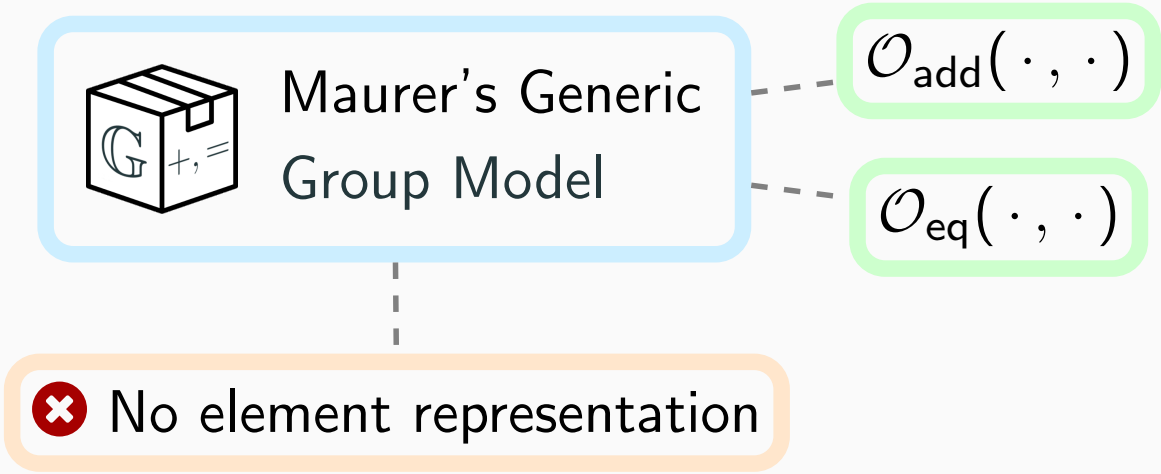
- Uses a **black box** pairing-free prime order group $\mathbb{G}$.
- Its security reduces **only** to hard problems in $\mathbb{G}$.



Algebraic Vector Commitments

A Vector Commitment is **Algebraic** if

- Uses a **black box** pairing-free prime order group $\mathbb{G}$.
- Its security reduces **only** to hard problems in $\mathbb{G}$.



Question: Do Algebraic Vector Commitments exists?

Our Result - Impossibility of Algebraic VC

Strictly Linear Verification VC

$$\boxed{} = (\mathbf{Y}, \mathbf{z}) \in \mathbb{G}^k \times \mathbb{F}_q^h$$

Verification[1]: $A(\mathbf{z})\mathbf{X} == B\mathbf{Y}$
with $A(\mathbf{z})$ affine function of $\mathbf{z}$

Unconditionally Impossible:

$$\ell(\boxed{}) \cdot \ell(\boxed{}) = \Omega(n)$$

[1] $\mathbf{X} \in \mathbb{G}^\nu$ denotes the CRS and commitment's group elements

Our Result - Impossibility of Algebraic VC

Strictly Linear Verification VC

$\boxed{\checkmark} = (\mathbf{Y}, \mathbf{z}) \in \mathbb{G}^k \times \mathbb{F}_q^h$

Verification[1]: $A(\mathbf{z})\mathbf{X} == B\mathbf{Y}$
with $A(\mathbf{z})$ affine function of $\mathbf{z}$

Unconditionally Impossible:
$\ell(\boxtimes) \cdot \ell(\boxed{\checkmark}) = \Omega(n)$

Generic Verification VC

No restriction

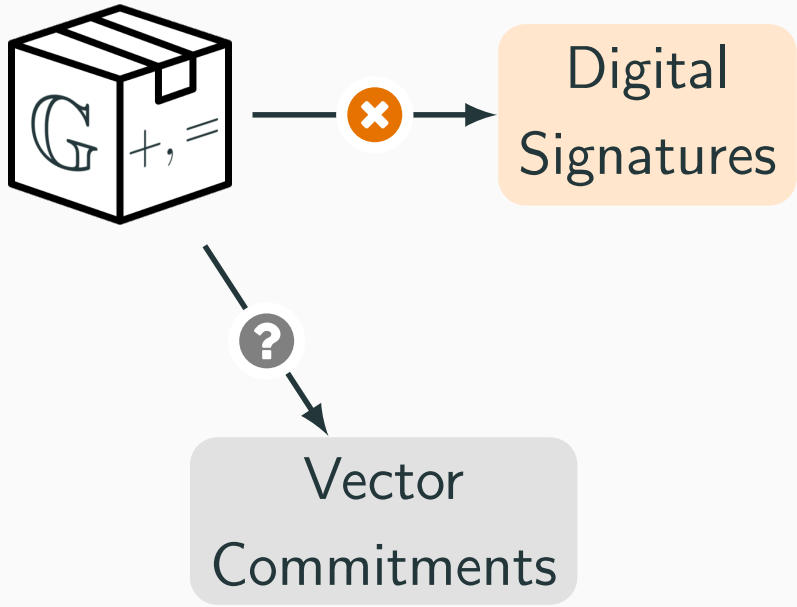
Black-Box Separation:
$\ell(\boxtimes) \cdot \ell(\boxed{\checkmark}) = \Omega(n)$

[1] $\mathbf{X} \in \mathbb{G}^\nu$ denotes the CRS and commitment's group elements

Black-Box Separation Roadmap

Roadmap

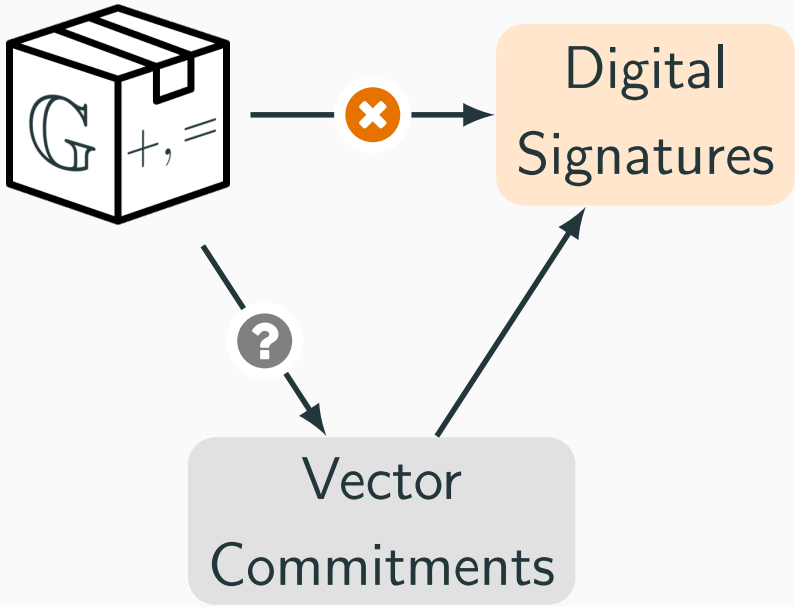
1. **Starting point:** [DHH+21].



Black-Box Separation Roadmap

Roadmap

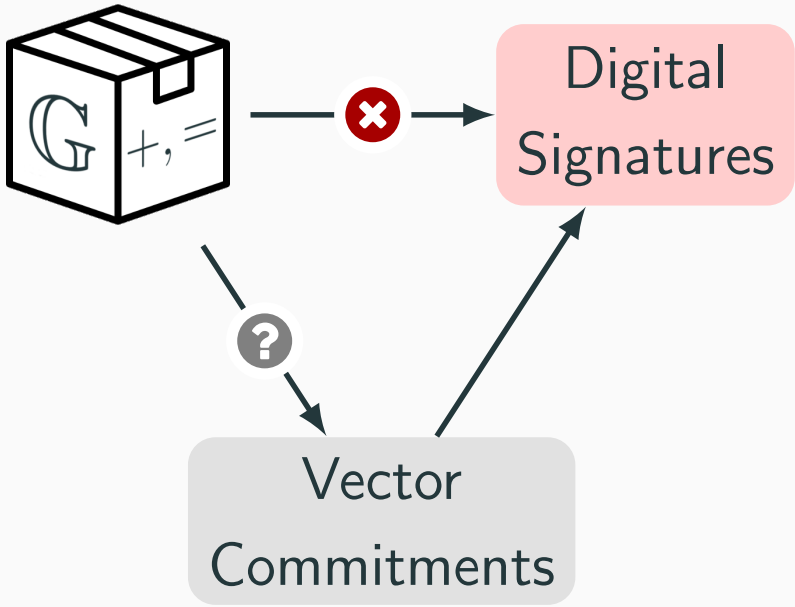
1. **Starting point:** [DHH+21].
2. Build DS from VC.



Black-Box Separation Roadmap

Roadmap

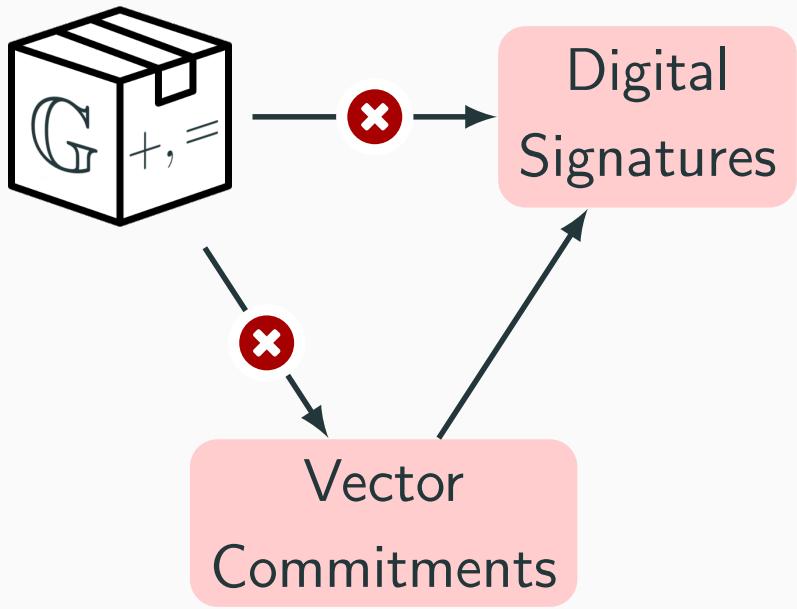
1. **Starting point:** [DHH+21].
2. Build DS from VC.
3. Describe an attack for Algebraic Signatures.



Black-Box Separation Roadmap

Roadmap

1. **Starting point:** [DHH+21].
2. Build DS from VC.
3. Describe an attack for Algebraic Signatures.
4. Conclude Algebraic VC are impossible.



Signatures from Vector Commitments

Message Space

$1 \quad 2 \quad 3 \quad \cdots \quad n$

CRS

Signer

Verifier

Signatures from Vector Commitments

Signer

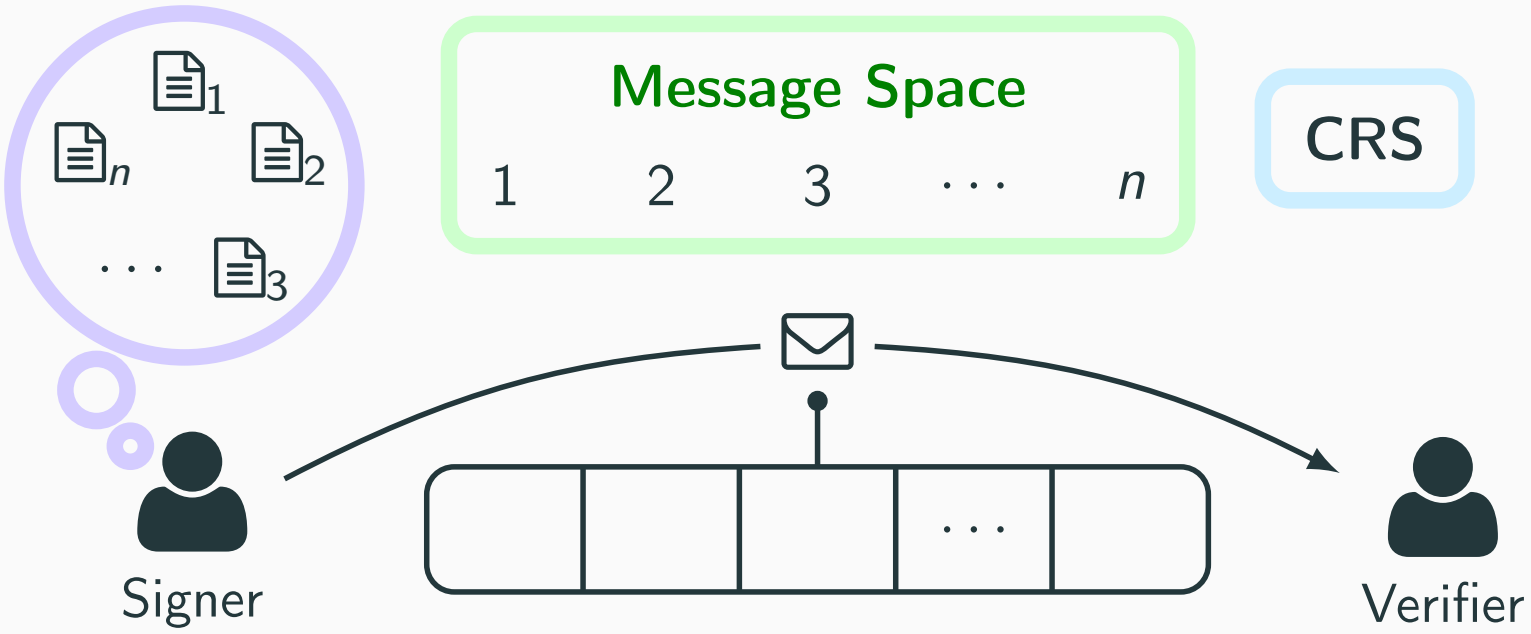
Message Space

1 2 3 ··· n

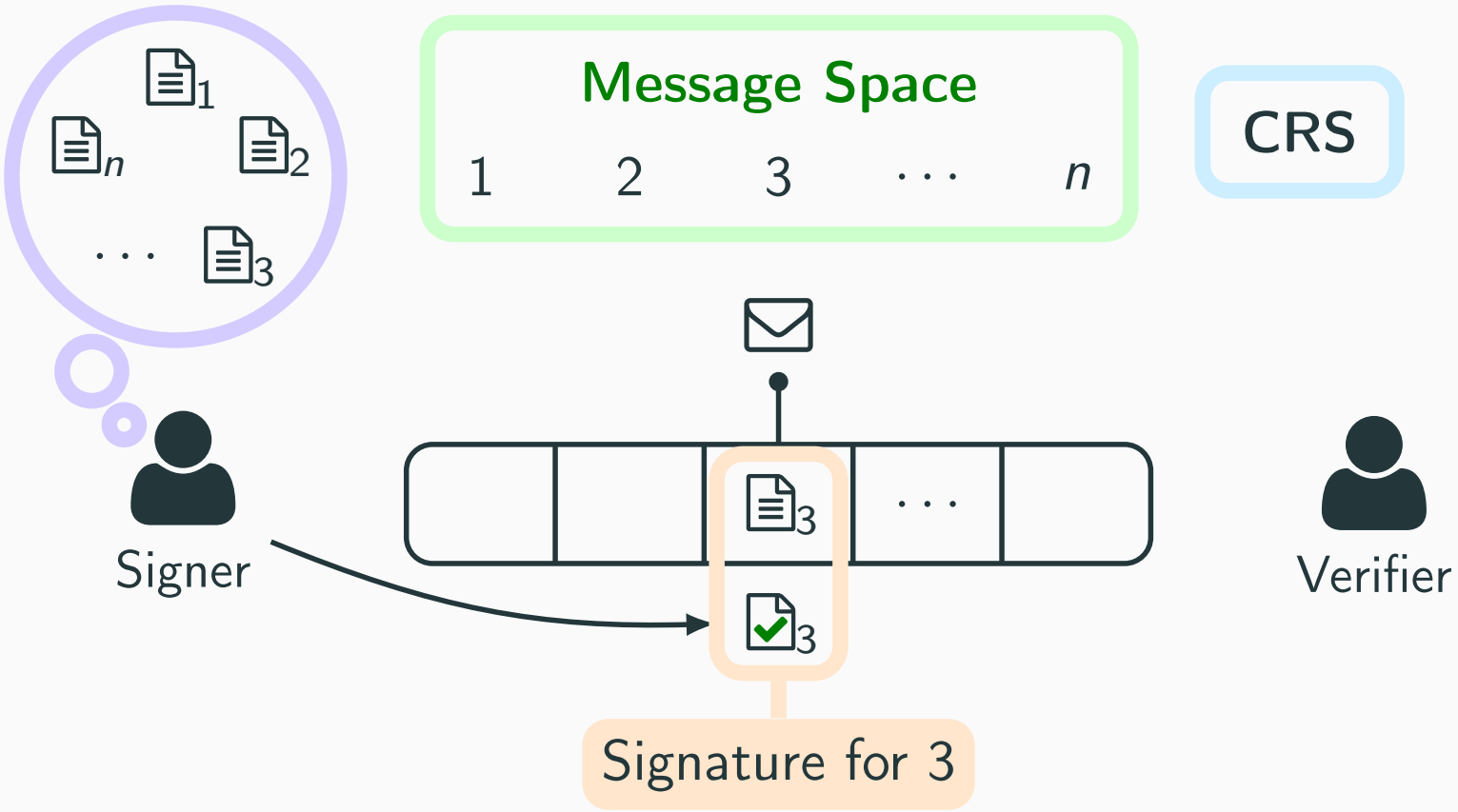
CRS

Verifier

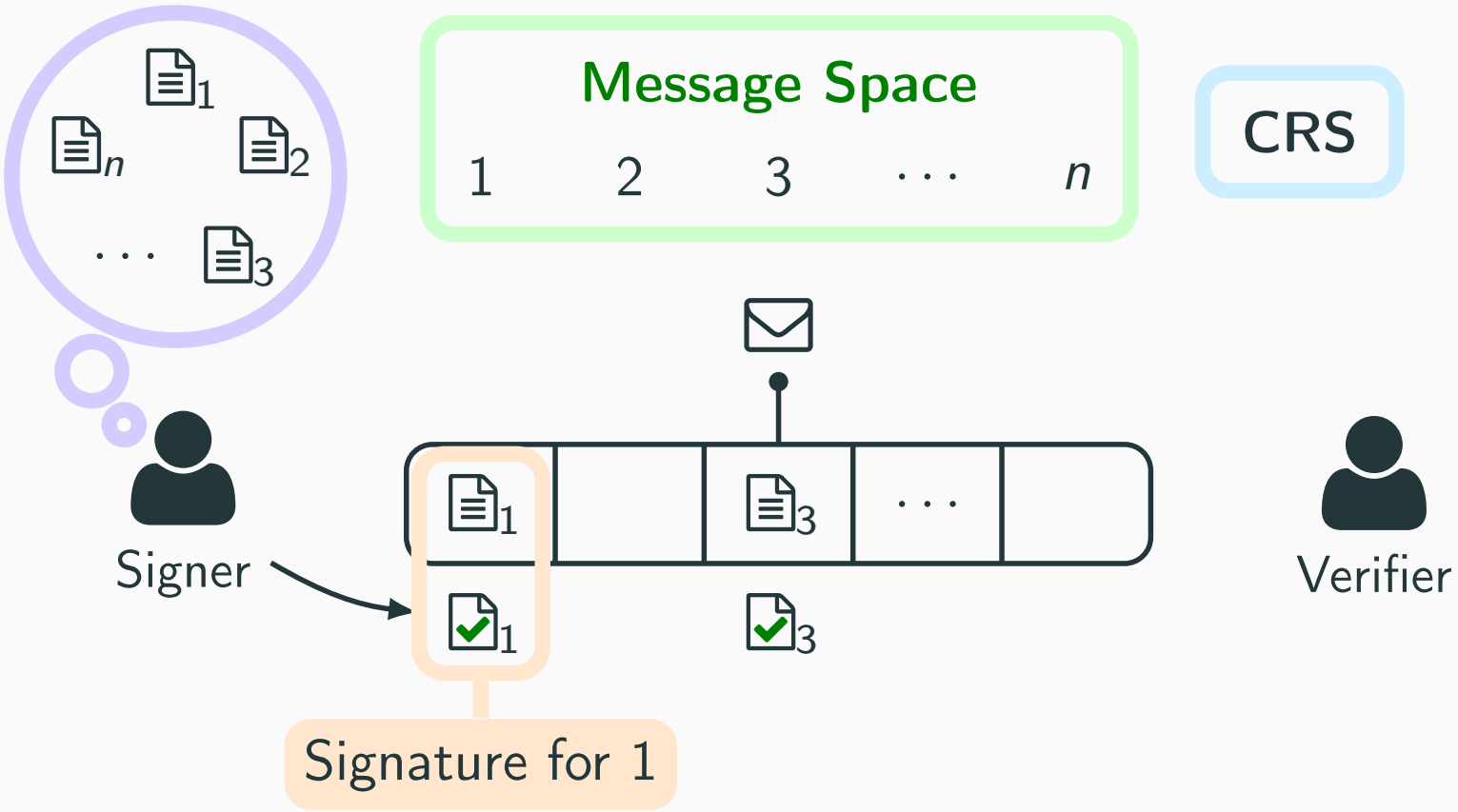
Signatures from Vector Commitments



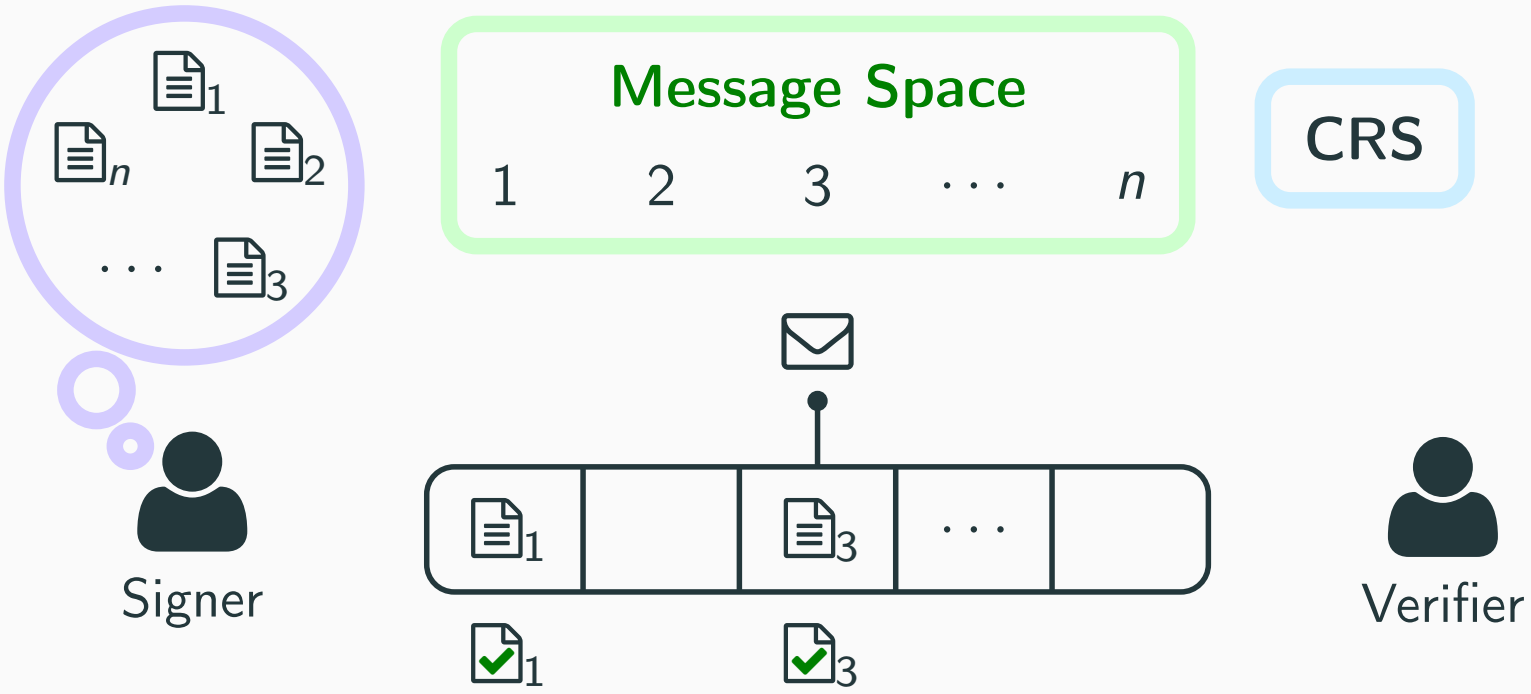
Signatures from Vector Commitments



Signatures from Vector Commitments

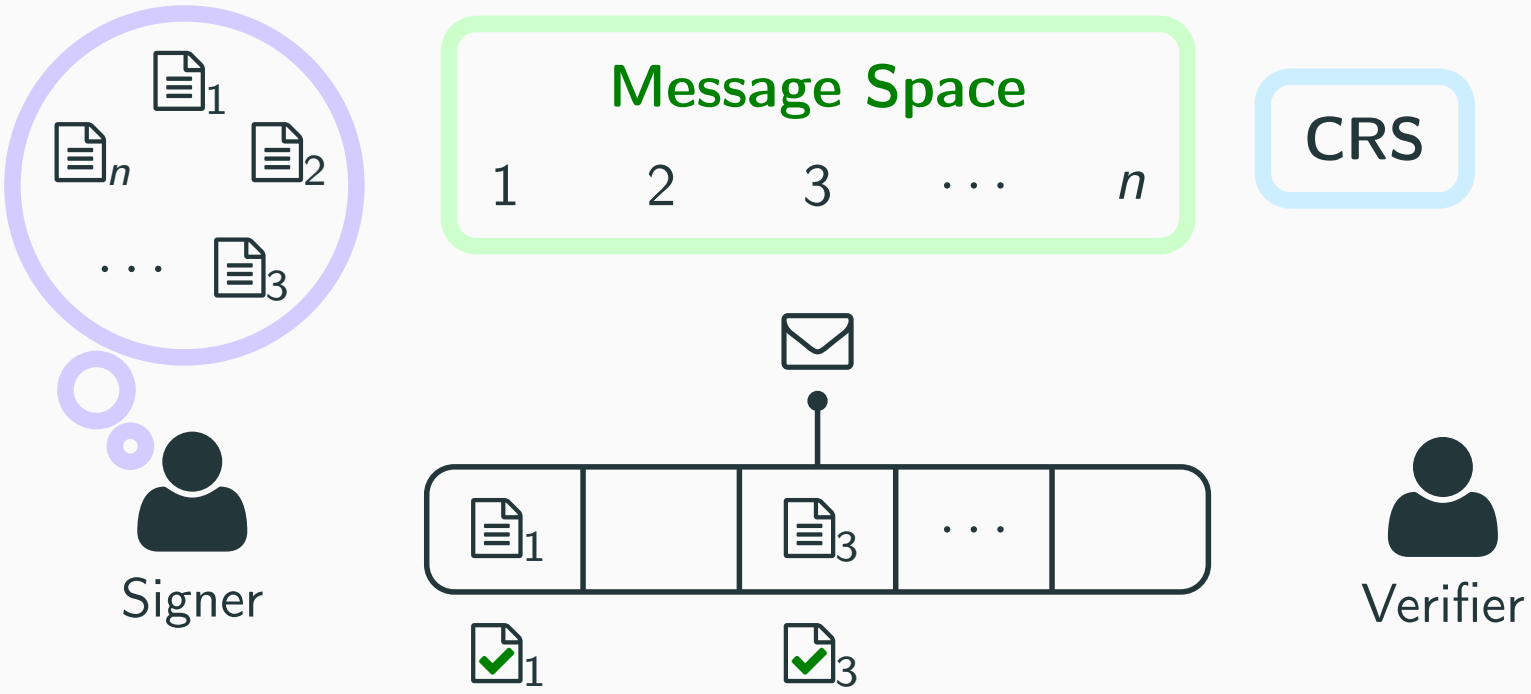


Signatures from Vector Commitments



Question: Is this **Unforgeable**?

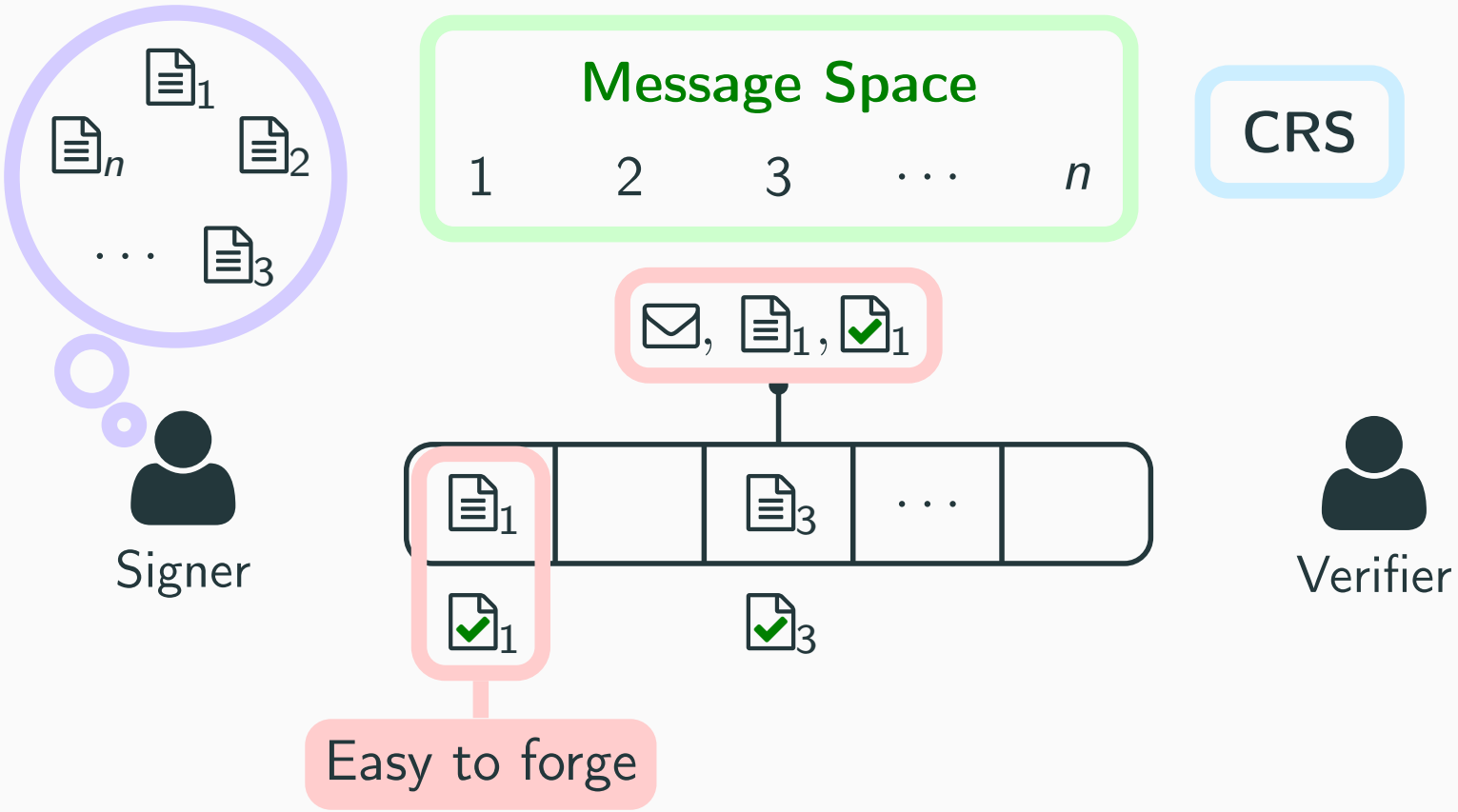
Signatures from Vector Commitments



Question: Is this **Unforgeable**?

Not Necessarily!

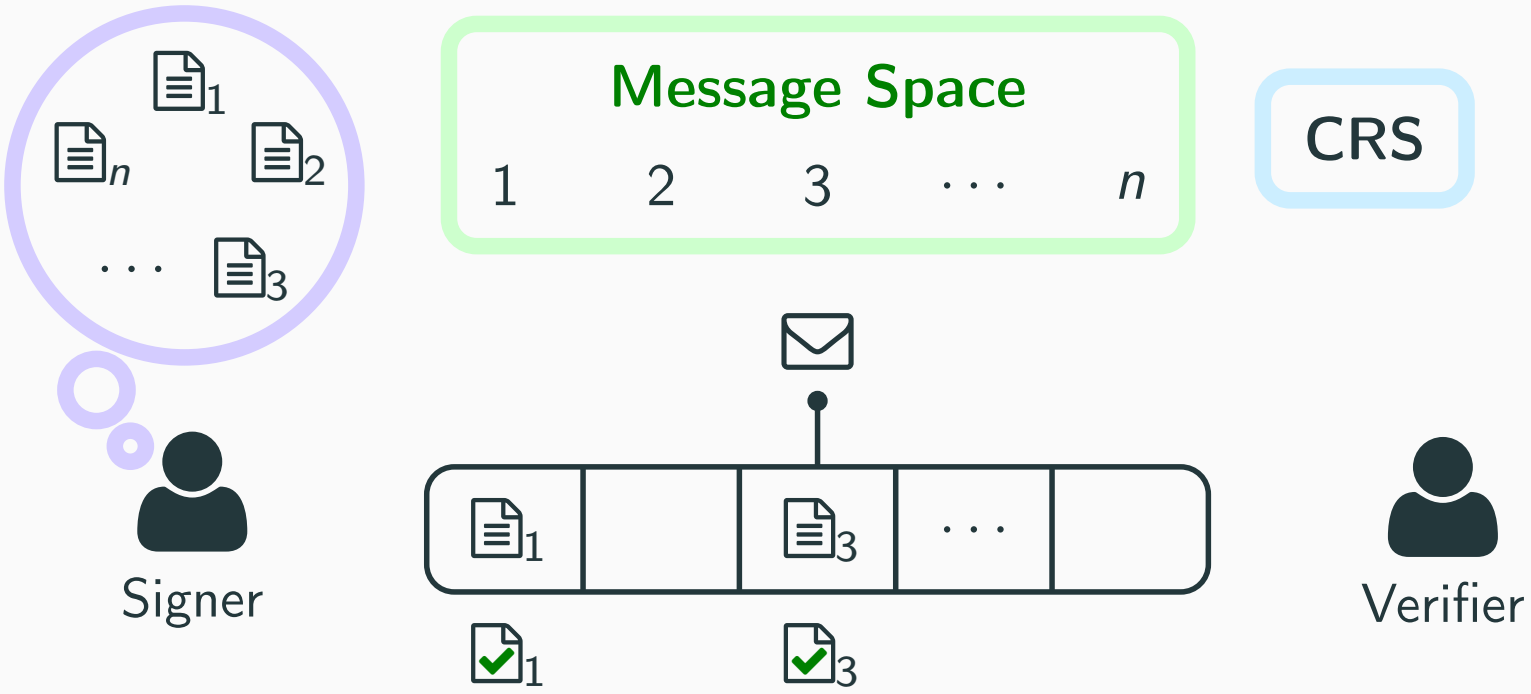
Signatures from Vector Commitments



Question: Is this **Unforgeable**?

✗ **Not Necessarily!**

Signatures from Vector Commitments

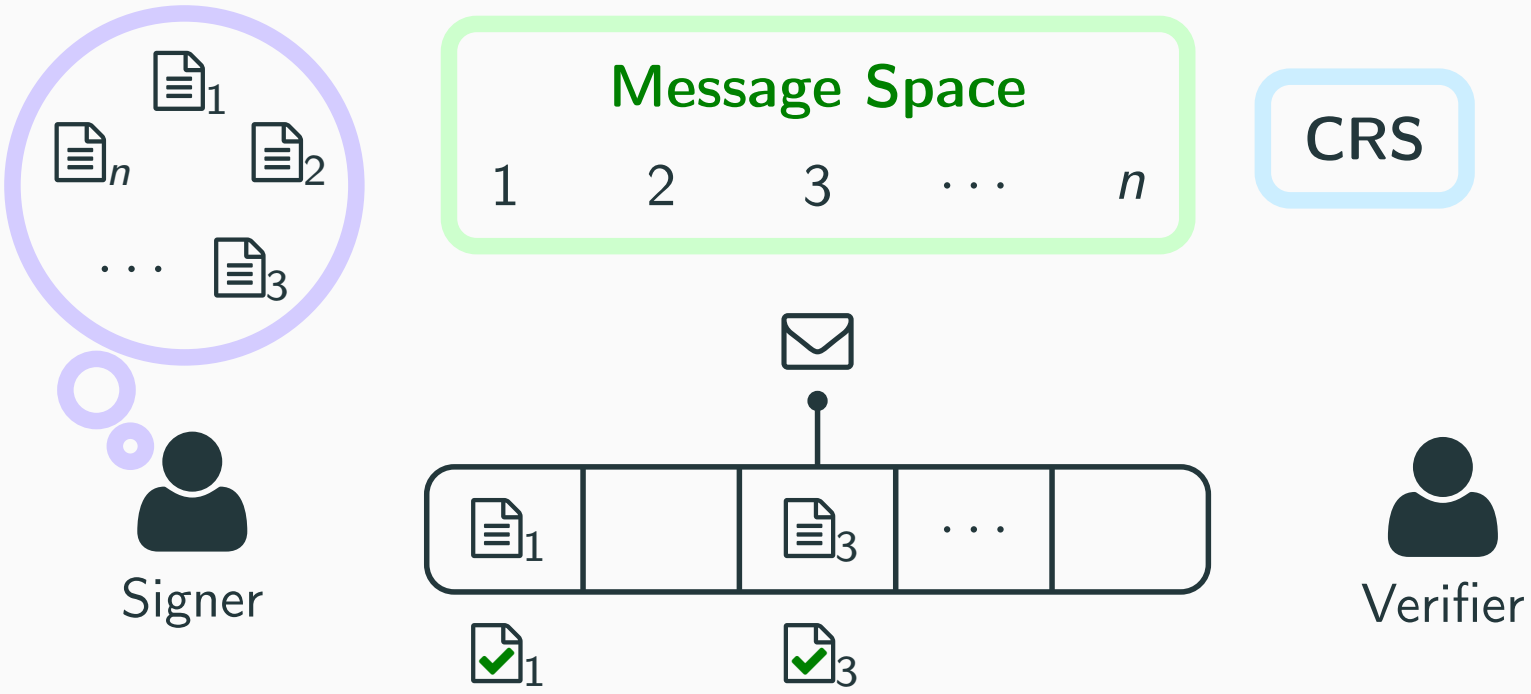


Question: Is this **Unforgeable**?

Question: Is this ϑ-**Unforgeable**?

Not Necessarily!

Signatures from Vector Commitments



Question: Is this **Unforgeable**? ✗ Not Necessarily!

Question: Is this ϑ-**Unforgeable**? ✓ Yes!

Impossibility of Algebraic Signatures

Result: There is no ϑ-unforgeable **Algebraic Signature** such that

- The verification key (excluding the CRS) has n group elements.
- The message space has size $\geq n + \vartheta$.

Impossibility of Algebraic Signatures

Result: There is no ϑ-unforgeable **Algebraic Signature** such that

- The verification key (excluding the CRS) has n group elements.
- The message space has size $\geq n + \vartheta$.

[DHH+21]

Verification Equation
$A\mathbf{X} = B\mathbf{Y}$

Does not exclude
CRS group elements

Impossibility of Algebraic Signatures

Result: There is no ϑ-unforgeable **Algebraic Signature** such that

- The verification key (excluding the CRS) has n group elements.
- The message space has size $\geq n + \vartheta$.

[DHH+21]

Verification Equation
$A\mathbf{X} = B\mathbf{Y}$

Does not exclude
CRS group elements

Corollary: Signatures with large message space are impossible in Maurer's GGM.

Putting all Together

Signatures from VC

- ϑ-unforgeable for $\vartheta \approx \ell(✉) + |Q| \cdot \ell(📄)$.
- vk has at most $\ell(✉)$ group elements (not in the CRS).

Putting all Together

Signatures from VC

- ϑ-unforgeable for $\vartheta \approx \ell(✉) + |Q| \cdot \ell(✓)$.
- vk has at most $\ell(✉)$ group elements (not in the CRS).

Impossibility for Signatures

There exists no ϑ-unforgeable algebraic signature s.t.

- vk has m group elements (not in the CRS).
- The **message space** has size $n \geq \vartheta + m$

Putting all Together

Signatures from VC

- ϑ-unforgeable for $\vartheta \approx \ell(✉) + |Q| \cdot \ell(✔)$.
- vk has at most $\ell(✉)$ group elements (not in the CRS).

Impossibility for Signatures

There exists no ϑ-unforgeable algebraic signature s.t.

- vk has m group elements (not in the CRS).
- The **message space** has size $n \geq \vartheta + m$

Impossibility for Vector Commitments

$\ell(✉) \cdot \ell(✔) = \Omega(n)$

Conclusions and Open Problems

In Maurer's Generic Group Model **Vector Commitments** cannot be both **position binding** and **succinct**.

Consequences: **Succinct** Polynomial and Functional Commitments are also impossible in Maurer's GGM.

Open problems: Extension to **Shoup's GGM**.

Thanks for your attention!