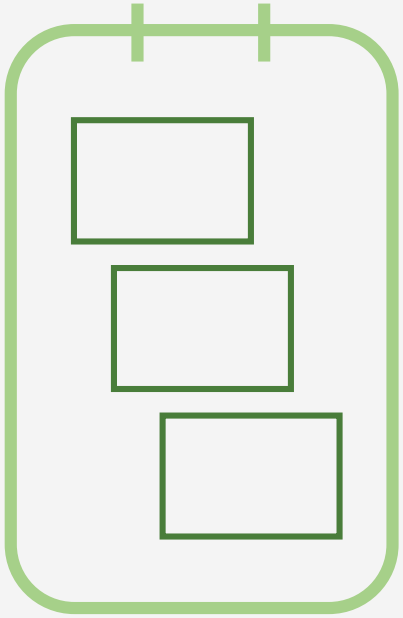
Linearly-Homomorphic Signatures and Scalable Mix-Nets

Chloé Hébant, Duong Hieu Phan and David Pointcheval

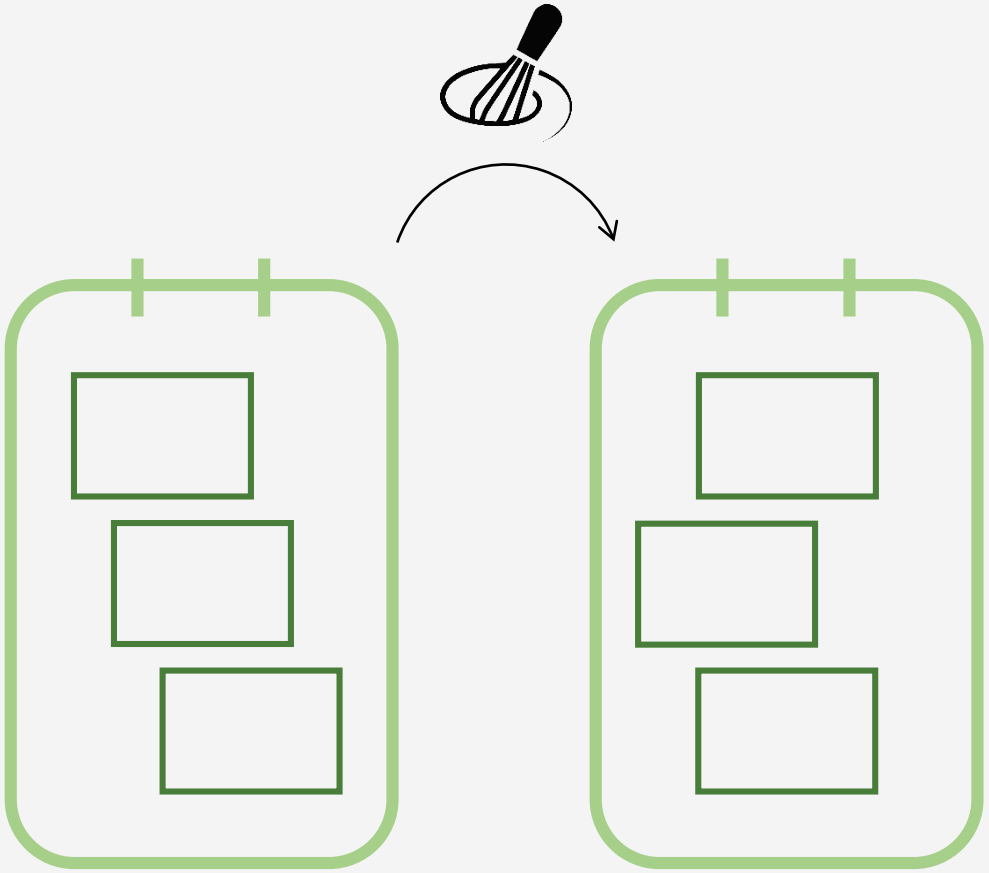
Outline

1. Mix-Nets in drawings
2. Building blocks
3. Spirit of our scheme
4. Difficulties

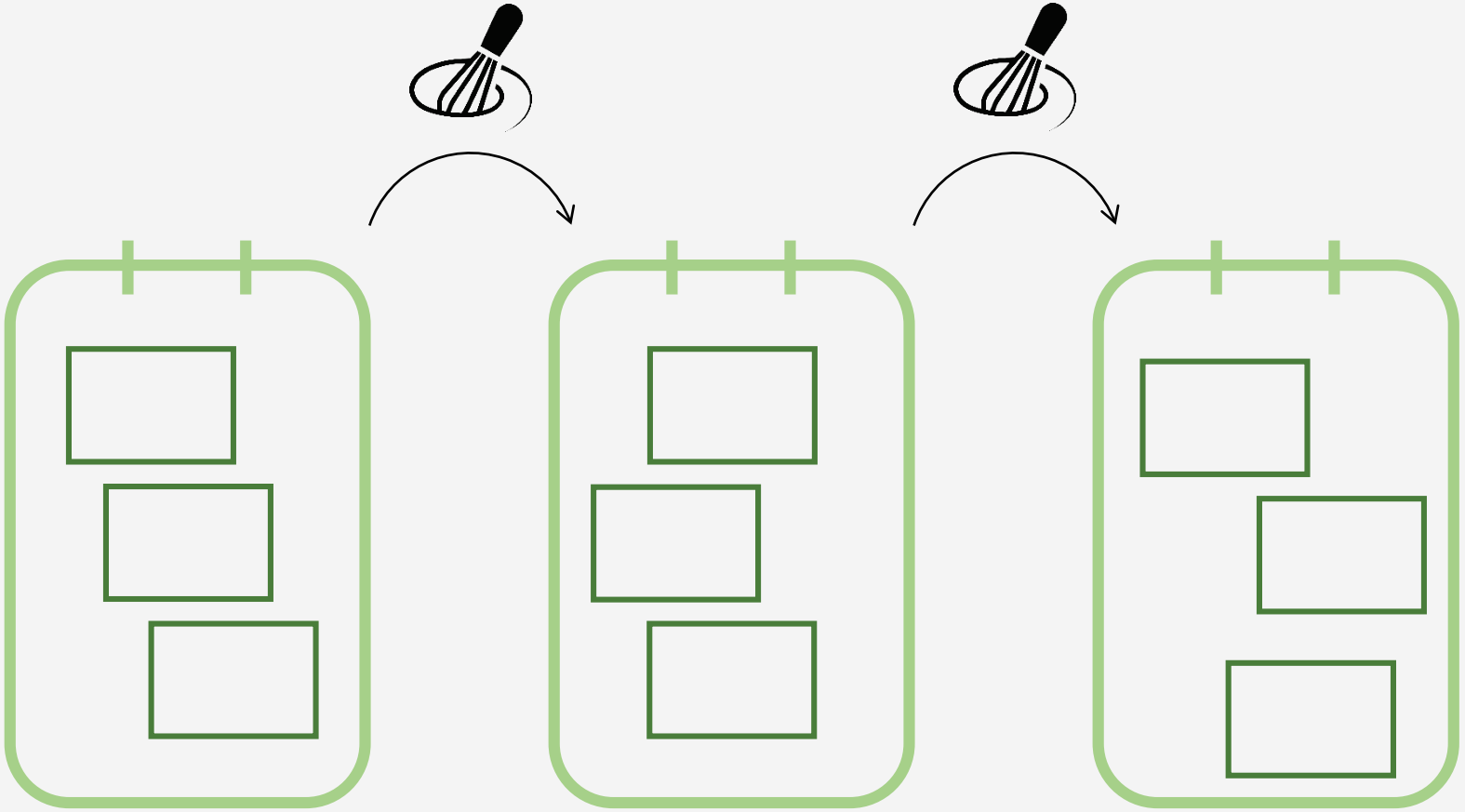
Mix-Net



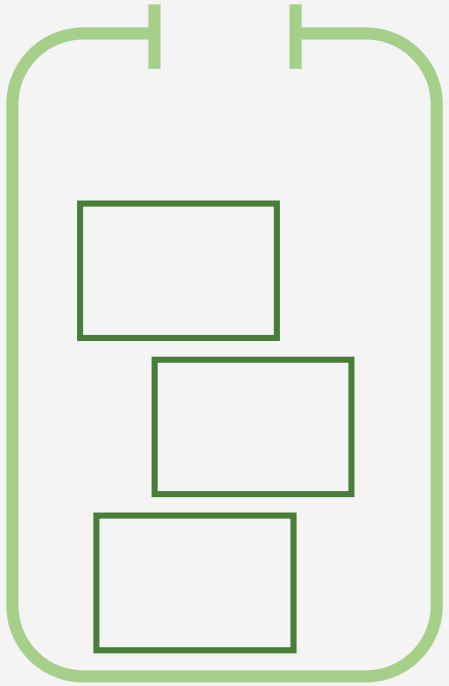
Mix-Net



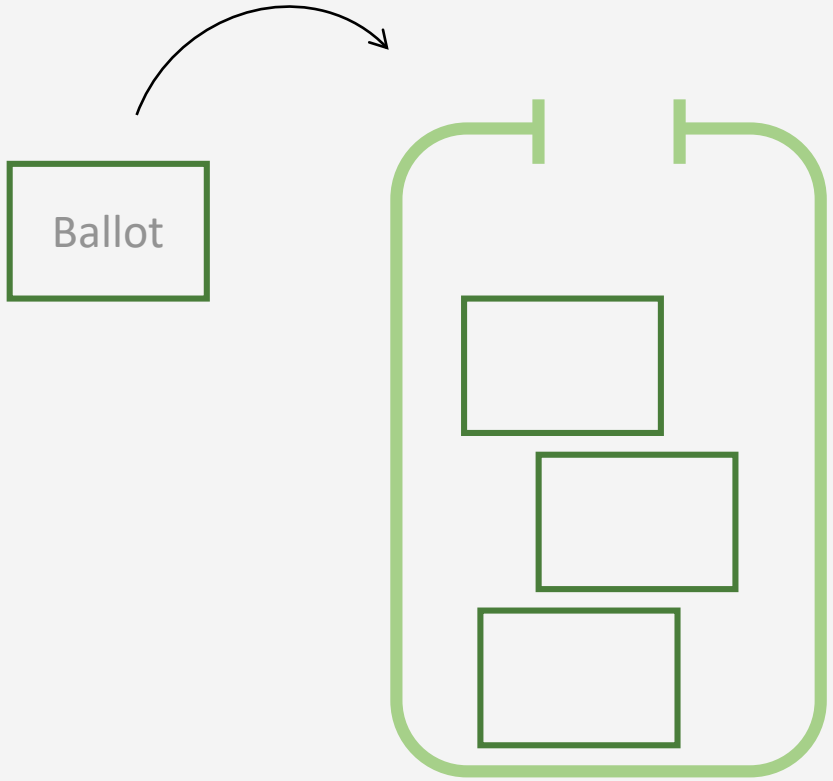
Mix-Net



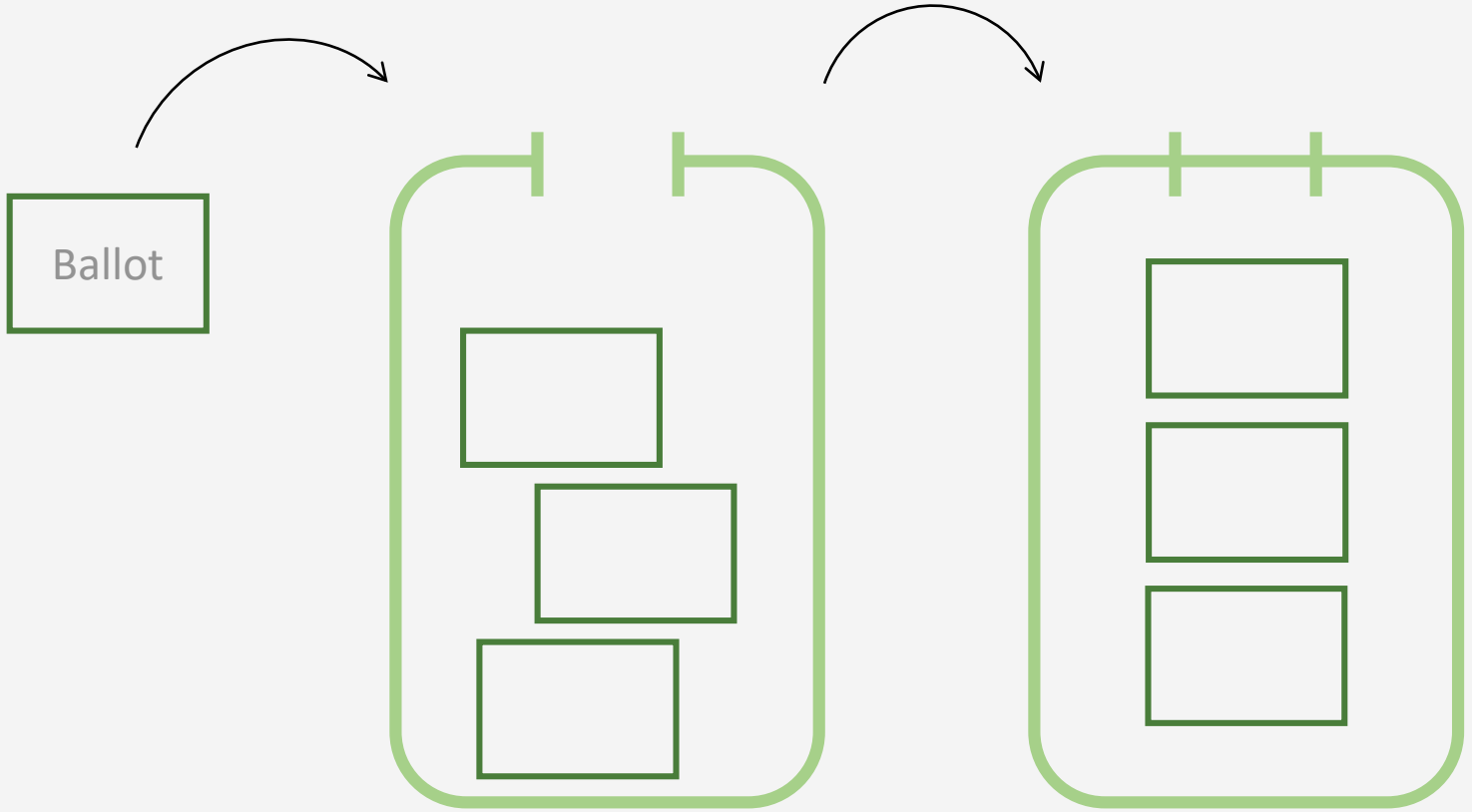
Electronic Voting



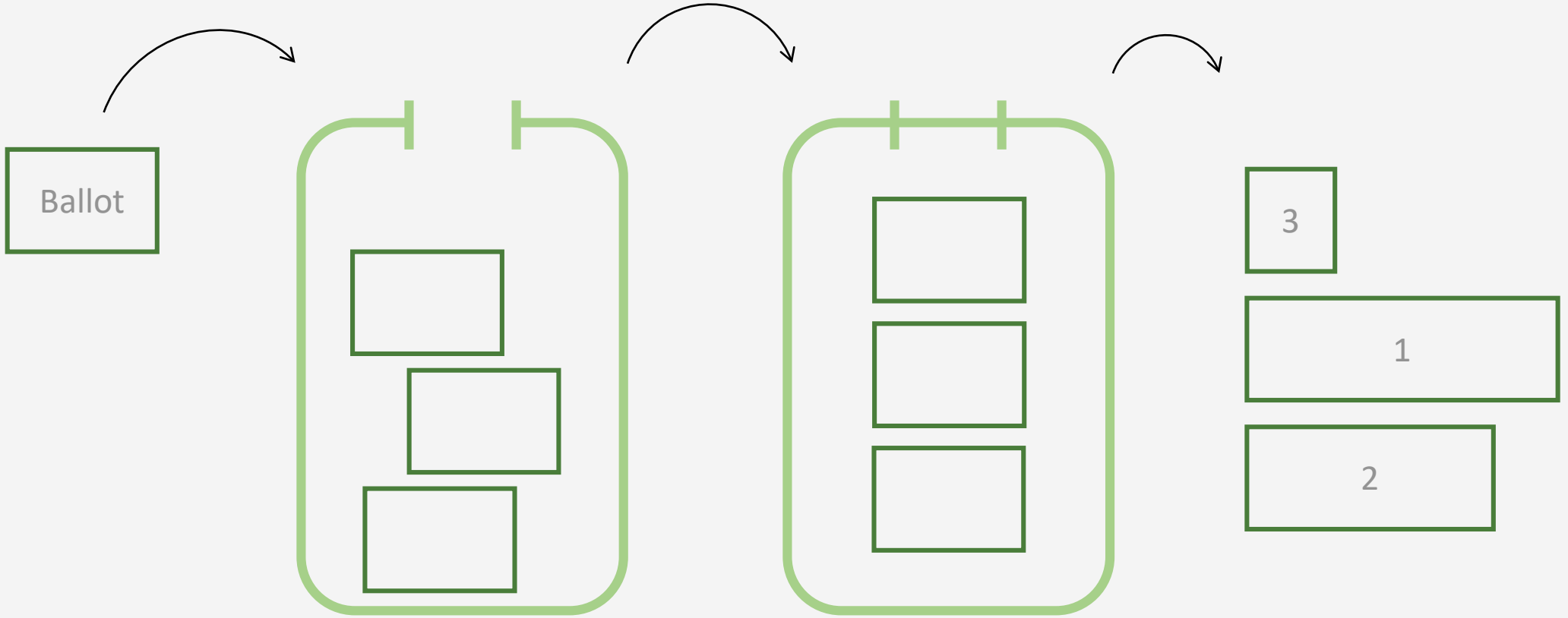
Electronic Voting



Electronic Voting



Electronic Voting



Some Guarantees

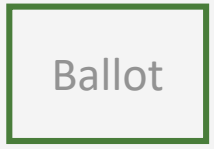
Authorized voters

Ballot

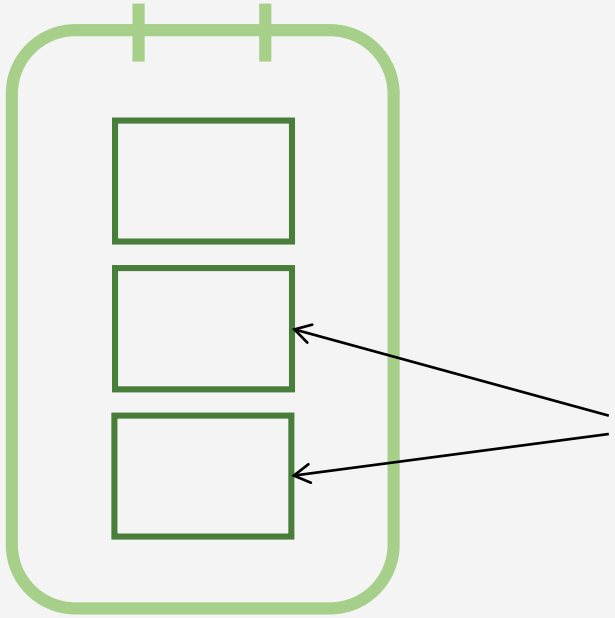
Unforgeability

Some Guarantees

Authorized voters



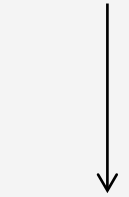
Unforgeability

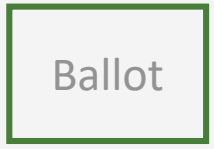


Indistinguishable

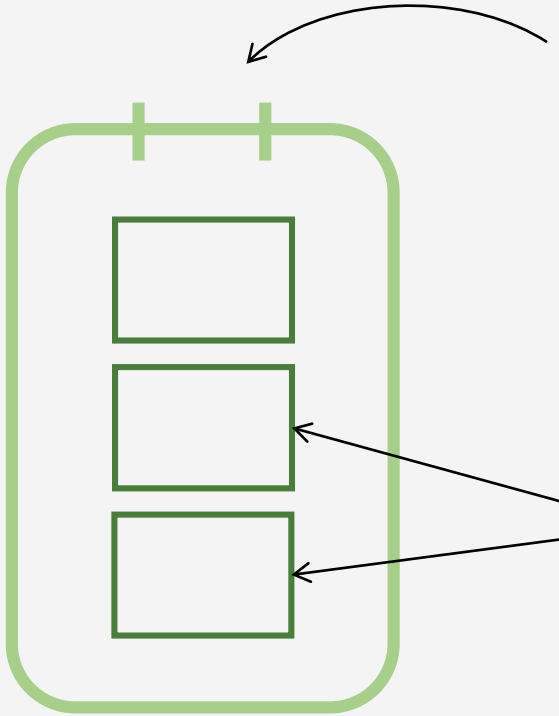
Some Guarantees

Authorized voters





Unforgeability



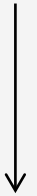
Sealed

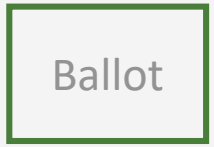
- No added ballot
- No deleted ballot
- No modified ballot

Indistinguishable

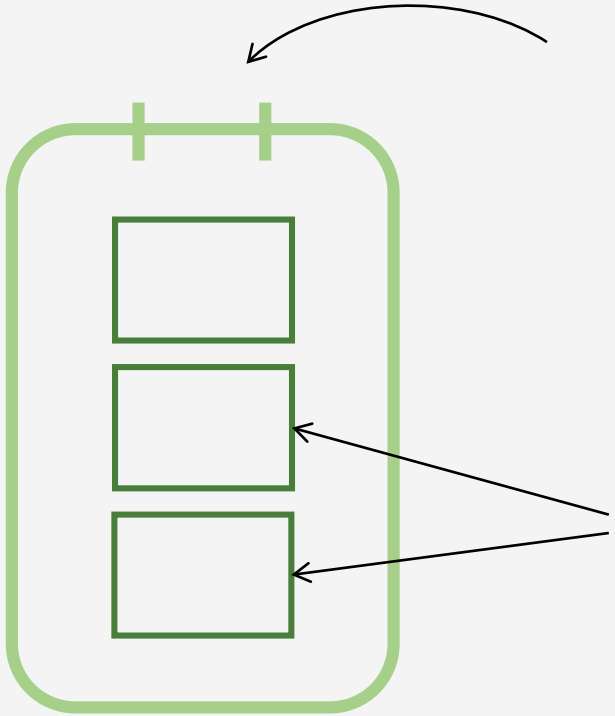
Some Guarantees

Authorized voters





Unforgeability

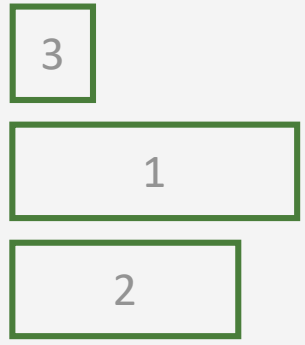


Sealed

- No added ballot
- No deleted ballot
- No modified ballot

Indistinguishable

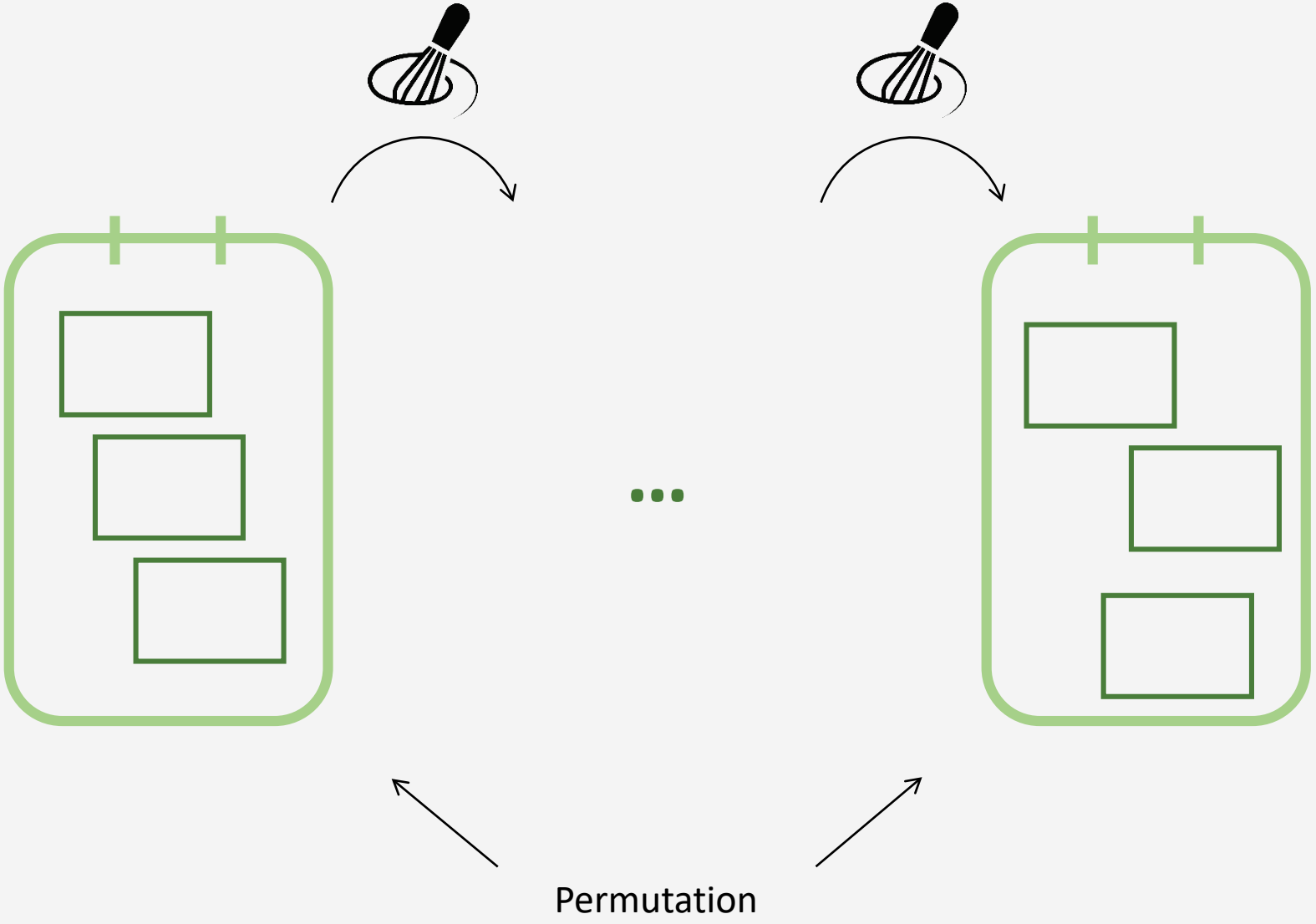
Publicly verifiable



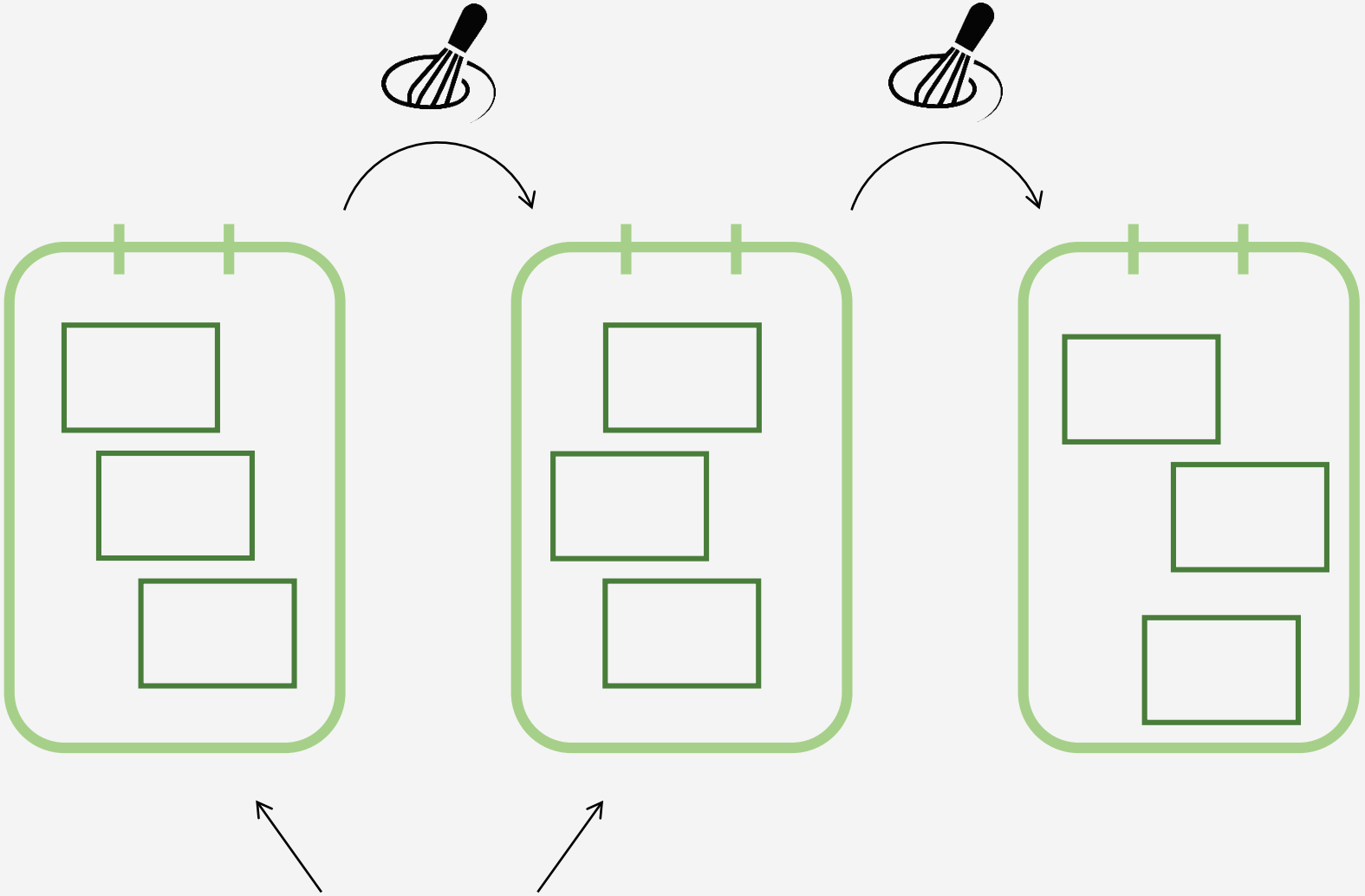
Mix-Net: Security Notions

1. Soundness
2. Unlinkability

Mix-Net: Soundness



Mix-Net: Unlinkability



Building Blocks

Key Ingredients

- Ciphertext randomization
- “Signature randomization”

Key Ingredients

- Ciphertext randomization
  - e.g. El Gamal
- “Signature randomization”

Key Ingredients

- Ciphertext randomization
  - e.g. El Gamal
- “Signature randomization”
  - Linearly Homomorphic Signature

Signature

$\mathsf{Setup}(1^\kappa) \to \mathsf{param}$

$\mathsf{Keygen}(\mathsf{param}, n) \to (\mathsf{sk}, \mathsf{vk})$

$\mathsf{Sign}(\mathsf{sk}, \quad \vec{M} = (M_i)_i \in \mathbb{G}^n) \to \sigma$

$\mathsf{Verif}(\mathsf{vk}, \quad \vec{M}, \sigma) \to 1 \text{ if } \sigma \text{ valid relative to } \mathsf{vk}, 0 \text{ otherwise}$

One-Time Linearly Homomorphic Signature (OT-LH-Sig)

$\mathsf{Setup}(1^\kappa) \to$ param

$\mathsf{Keygen}(\mathsf{param}, n) \to (\mathsf{sk}, \mathsf{vk})$

$\mathsf{Sign}(\mathsf{sk}, \quad \vec{M} = (M_i)_i \in \mathbb{G}^n) \to \sigma$

$\mathsf{DerivSign}(\mathsf{vk}, \quad (\omega_i, \vec{M}_i, \sigma_i)_{i=1}^{\ell}) \to \sigma$ (on the vector $\vec{M} = \prod_{i=1}^{\ell} \vec{M}_i^{\omega_i}$)

$\mathsf{Verif}(\mathsf{vk}, \quad \vec{M}, \sigma) \to 1$ if σ valid relative to vk , 0 otherwise

Linearly Homomorphic Signature (LH-Sig)

$\mathsf{Setup}(1^\kappa) \to$ param

$\mathsf{Keygen}(\mathsf{param}, n) \to (\mathsf{sk}, \mathsf{vk})$

$\mathsf{Sign}(\mathsf{sk}, \quad \vec{M} = (M_i)_i \in \mathbb{G}^n) \to \sigma$

$\mathsf{DerivSign}(\mathsf{vk}, \quad (\omega_i, \vec{M}_i, \sigma_i)_{i=1}^{\ell}) \to \sigma$ (on the vector $\vec{M} = \prod_{i=1}^{\ell} \vec{M}_i^{\omega_i}$)

$\mathsf{Verif}(\mathsf{vk}, \quad \vec{M}, \sigma) \to 1$ if σ valid relative to vk , 0 otherwise

Linearly Homomorphic Signature (LH-Sig)

$\mathsf{Setup}(1^\kappa) \to$ param (includes a tag space $\mathcal{T}$)

$\mathsf{Keygen}(\mathsf{param}, n) \to (\mathsf{sk}, \mathsf{vk})$

$\mathsf{Sign}(\mathsf{sk}, \quad \vec{M} = (M_i)_i \in \mathbb{G}^n) \to \sigma$

$\mathsf{DerivSign}(\mathsf{vk}, \quad (\omega_i, \vec{M}_i, \sigma_i)_{i=1}^{\ell}) \to \sigma$ (on the vector $\vec{M} = \prod_{i=1}^{\ell} \vec{M}_i^{\omega_i}$)

$\mathsf{Verif}(\mathsf{vk}, \quad \vec{M}, \sigma) \to 1$ if σ valid relative to vk , 0 otherwise

Linearly Homomorphic Signature (LH-Sig)

$\mathsf{Setup}(1^\kappa) \to$ param (includes a tag space $\mathcal{T}$)

$\mathsf{Keygen}(\mathsf{param}, n) \to (\mathsf{sk}, \mathsf{vk})$

$\mathsf{NewTag}(\mathsf{sk}) \to (\tilde{\tau}, \tau)$

$\mathsf{VerifTag}(\mathsf{vk}, \tau) \to$ 1 if the tag is valid, 0 otherwise

$\mathsf{Sign}(\mathsf{sk}, \quad \vec{M} = (M_i)_i \in \mathbb{G}^n) \to \sigma$

$\mathsf{DerivSign}(\mathsf{vk}, \quad (\omega_i, \vec{M}_i, \sigma_i)_{i=1}^{\ell}) \to \sigma$ (on the vector $\vec{M} = \prod_{i=1}^{\ell} \vec{M}_i^{\omega_i}$)

$\mathsf{Verif}(\mathsf{vk}, \quad \vec{M}, \sigma) \to$ 1 if σ valid relative to vk , 0 otherwise

Linearly Homomorphic Signature (LH-Sig)

$\mathsf{Setup}(1^\kappa) \to$ param (includes a tag space $\mathcal{T}$)

$\mathsf{Keygen}(\mathsf{param}, n) \to (\mathsf{sk}, \mathsf{vk})$

$\mathsf{NewTag}(\mathsf{sk}) \to (\tilde{\tau}, \tau)$

$\mathsf{VerifTag}(\mathsf{vk}, \tau) \to$ 1 if the tag is valid, 0 otherwise

$\mathsf{Sign}(\mathsf{sk}, \tilde{\tau}, \vec{M} = (M_i)_i \in \mathbb{G}^n) \to \sigma$ (under the tag τ)

$\mathsf{DerivSign}(\mathsf{vk}, (\omega_i, \vec{M}_i, \sigma_i)_{i=1}^{\ell}) \to \sigma$ (on the vector $\vec{M} = \prod_{i=1}^{\ell} \vec{M}_i^{\omega_i}$)

$\mathsf{Verif}(\mathsf{vk}, \vec{M}, \sigma) \to$ 1 if σ valid relative to vk, 0 otherwise

Linearly Homomorphic Signature (LH-Sig)

$\mathsf{Setup}(1^\kappa) \to$ param (includes a tag space $\mathcal{T}$)

$\mathsf{Keygen}(\mathsf{param}, n) \to (\mathsf{sk}, \mathsf{vk})$

$\mathsf{NewTag}(\mathsf{sk}) \to (\tilde{\tau}, \tau)$

$\mathsf{VerifTag}(\mathsf{vk}, \tau) \to$ 1 if the tag is valid, 0 otherwise

$\mathsf{Sign}(\mathsf{sk}, \tilde{\tau}, \vec{M} = (M_i)_i \in \mathbb{G}^n) \to \sigma$ (under the tag τ)

$\mathsf{DerivSign}(\mathsf{vk}, \tau, (\omega_i, \vec{M}_i, \sigma_i)_{i=1}^{\ell}) \to \sigma$ (on the vector $\vec{M} = \prod_{i=1}^{\ell} \vec{M}_i^{\omega_i}$ under the tag τ)

$\mathsf{Verif}(\mathsf{vk}, \vec{M}, \sigma) \to$ 1 if σ valid relative to vk , 0 otherwise

Linearly Homomorphic Signature (LH-Sig)

$\mathsf{Setup}(1^\kappa) \to$ param (includes a tag space $\mathcal{T}$)

$\mathsf{Keygen}(\mathsf{param}, n) \to (\mathsf{sk}, \mathsf{vk})$

$\mathsf{NewTag}(\mathsf{sk}) \to (\tilde{\tau}, \tau)$

$\mathsf{VerifTag}(\mathsf{vk}, \tau) \to$ 1 if the tag is valid, 0 otherwise

$\mathsf{Sign}(\mathsf{sk}, \tilde{\tau}, \vec{M} = (M_i)_i \in \mathbb{G}^n) \to \sigma$ (under the tag τ)

$\mathsf{DerivSign}(\mathsf{vk}, \tau, (\omega_i, \vec{M}_i, \sigma_i)_{i=1}^{\ell}) \to \sigma$ (on the vector $\vec{M} = \prod_{i=1}^{\ell} \vec{M}_i^{\omega_i}$ under the tag τ)

$\mathsf{Verif}(\mathsf{vk}, \tau, \vec{M}, \sigma) \to$ 1 if $\mathsf{VerifTag}(\mathsf{vk}, \tau) = 1$ and σ valid relative to vk and τ, 0 otherwise

Linearly Homomorphic Signature (LH-Sig)

$\mathsf{Setup}(1^\kappa) \to$ param (includes a tag space $\mathcal{T}$)

$\mathsf{Keygen}(\mathsf{param}, n) \to (\mathsf{sk}, \mathsf{vk})$

$\mathsf{NewTag}(\mathsf{sk}) \to (\tilde{\tau}, \tau)$

$\mathsf{VerifTag}(\mathsf{vk}, \tau) \to$ 1 if the tag is valid, 0 otherwise

$\mathsf{Sign}(\mathsf{sk}, \tilde{\tau}, \vec{M} = (M_i)_i \in \mathbb{G}^n) \to \sigma$ (under the tag τ)

$\mathsf{DerivSign}(\mathsf{vk}, \tau, (\omega_i, \vec{M}_i, \sigma_i)_{i=1}^{\ell}) \to \sigma$ (on the vector $\vec{M} = \prod_{i=1}^{\ell} \vec{M}_i^{\omega_i}$ under the tag τ)

$\mathsf{Verif}(\mathsf{vk}, \tau, \vec{M}, \sigma) \to$ 1 if $\mathsf{VerifTag}(\mathsf{vk}, \tau) = 1$ and σ valid relative to vk and τ, 0 otherwise

$\mathsf{RandTag}(\mathsf{vk}, \tau, m, \sigma)$: $(m, \sigma', \mathsf{vk}, \tau')$

Summary

- Randomizable Ciphertexts: ElGamal
- Linearly Homomorphic Signatures
  - 3 properties:
    - Message Homomorphism
    - Key Homomorphism
    - Tag Randomizability

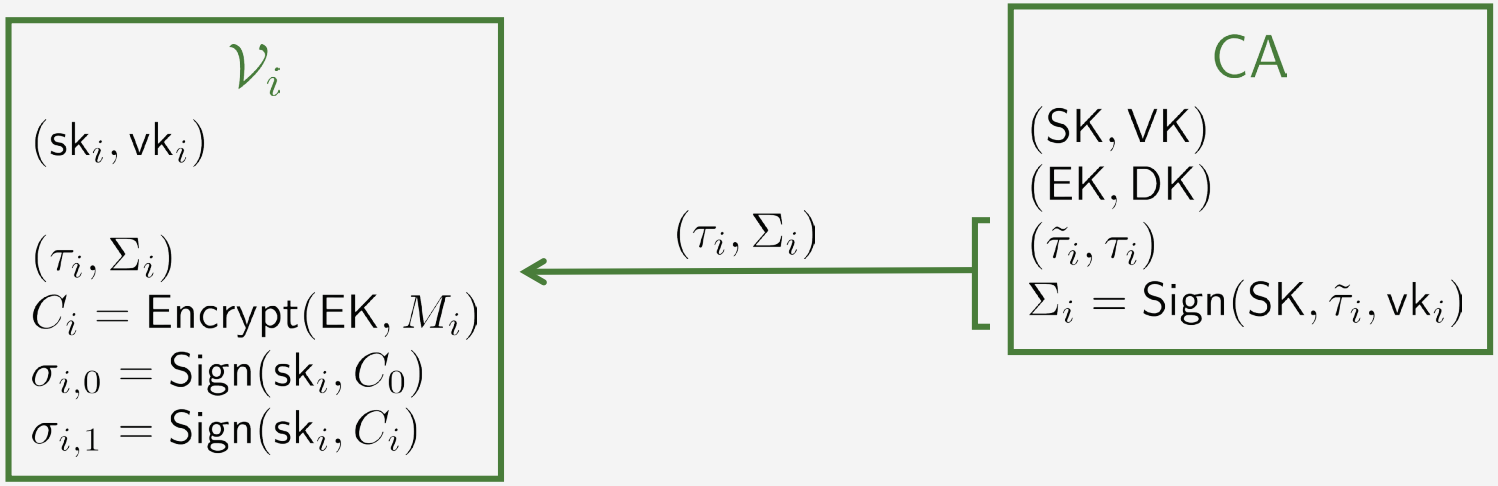
Summary

- Randomizable Ciphertexts: ElGamal
- Linearly Homomorphic Signatures
  - 3 properties:
    - Message Homomorphism
    - Key Homomorphism
    - Tag Randomizability
  - 2 schemes:
    - One-Time Linearly Homomorphic Signature (Keygen,Sign,Verif,…)
    - Linearly Homomorphic Signature (Keygen*,Sign*,Verif*,…)

Spirit of our Mix-Net

Mix-Nets

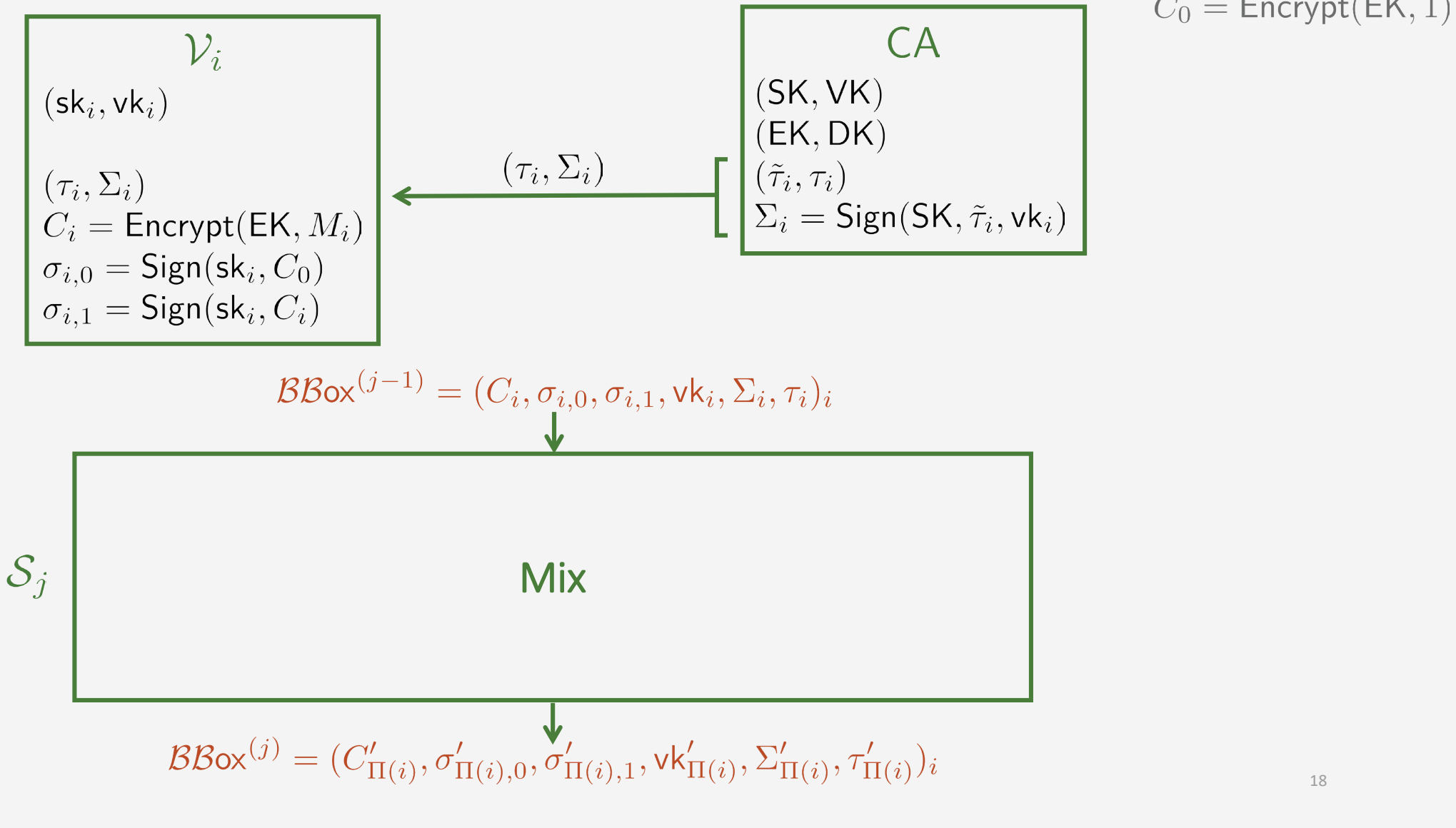
$C_0 = \mathsf{Encrypt}(\mathsf{EK}, 1)$



$$\mathcal{BB}\mathsf{ox}^{(0)} = (C_i, \sigma_{i,0}, \sigma_{i,1}, \mathsf{vk}_i, \Sigma_i, \tau_i)_i$$

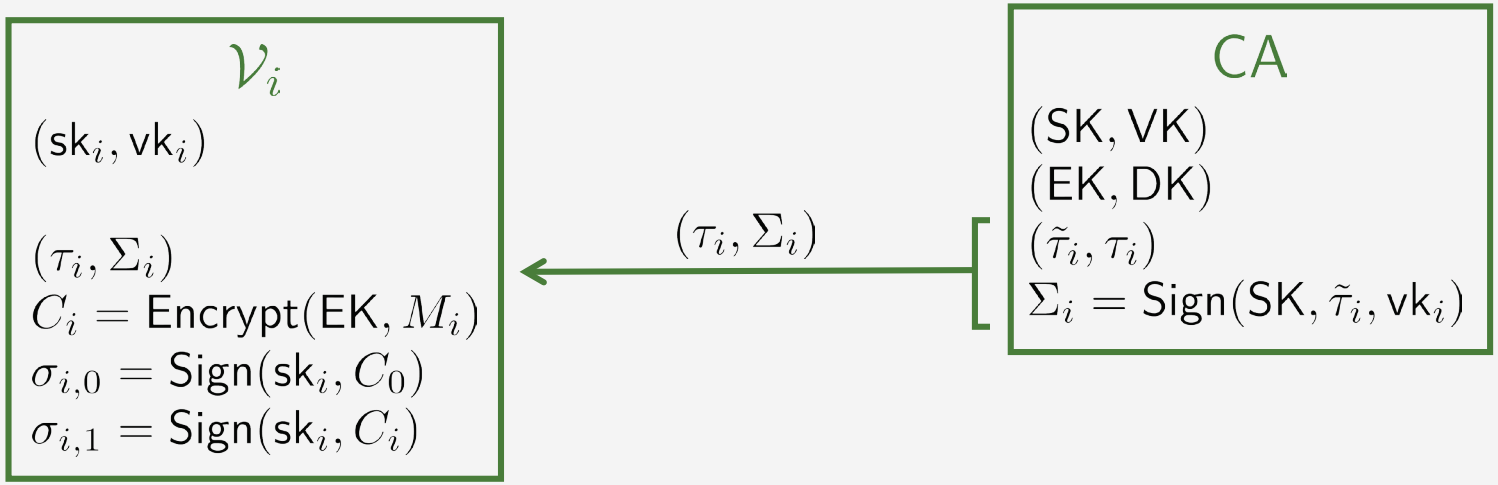
Mix-Nets

$C_0 = \mathsf{Encrypt}(\mathsf{EK}, 1)$



Mix-Nets

$C_0 = \mathsf{Encrypt}(\mathsf{EK}, 1)$



$\mathcal{BB}\mathsf{ox}^{(j-1)} = (C_i, \sigma_{i,0}, \sigma_{i,1}, \mathsf{vk}_i, \Sigma_i, \tau_i)_i$

$\mathcal{S}_j$

1. Rand C_i (and adapt $\sigma_{i,1}$) — Message Hom.
2. Rand vk_i (and adapt Σ_i)
   Rand τ_i (which change Σ_i) — Message Hom. Tag Randomizability
3. Because vk_i has changed, adapt $\sigma_{i,1}$ again and $\sigma_{i,0}$ — Key Hom.

$\mathcal{BB}\mathsf{ox}^{(j)} = (C'_{\Pi(i)}, \sigma'_{\Pi(i),0}, \sigma'_{\Pi(i),1}, \mathsf{vk}'_{\Pi(i)}, \Sigma'_{\Pi(i)}, \tau'_{\Pi(i)})_i$

Problems

Problems

- Expanded vectors

Problems

- Expanded vectors
- Non-trivial transformation

Problems

- Expanded vectors
- Non-trivial transformation
- Legitimate ballots

Problems

- Expanded vectors
- Non-trivial transformation
- Legitimate ballots
- Multiple servers

Aggregation

Aggregation

- Groth-Sahai proofs 2008

Aggregation

- Groth-Sahai proofs 2008
- Multi-signatures of Boneh-Drijvers-Neven 2018

Conclusion

We saw:

- (One-Time) Linearly Homomorphic Signatures schemes
- Their properties
  - Message Homomorphism
  - Key Homomorphism
  - Tag Randomizability
- A new method to construct scalable Mix-Nets