ETH zürich

Giving an Adversary Guarantees (Or: How to Model Designated Verifier Signatures in a Composable Framework)

Ueli Maurer, Christopher Portmann, Guilherme Rito

Asiacrypt' 21

Outline

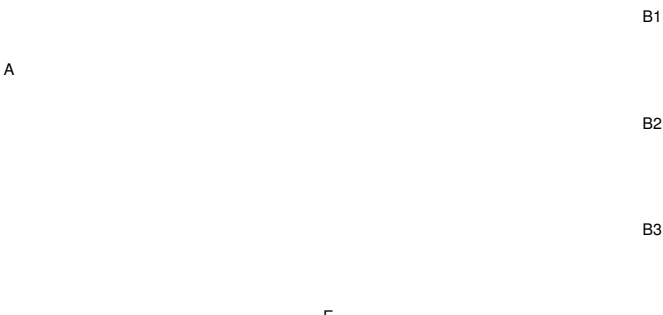
Introduction

Security notions typically restrict what dishonest parties can do.

Introduction

Security notions typically restrict what dishonest parties can do.

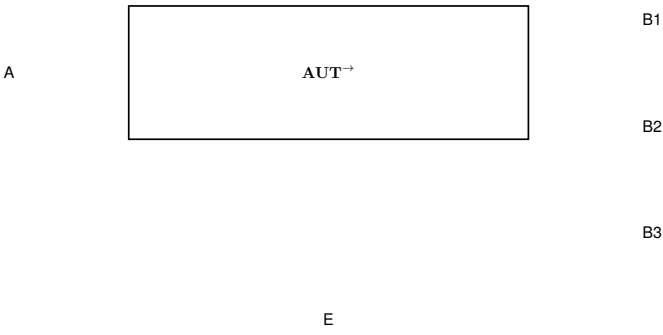
Authenticity:



Introduction

Security notions typically restrict what dishonest parties can do.

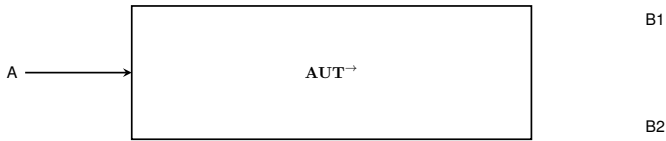
Authenticity:



Introduction

Security notions typically restrict what dishonest parties can do.

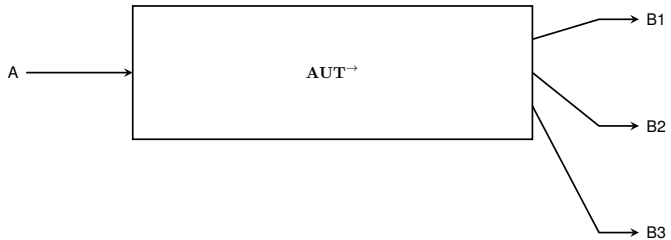
Authenticity:



Introduction

Security notions typically restrict what dishonest parties can do.

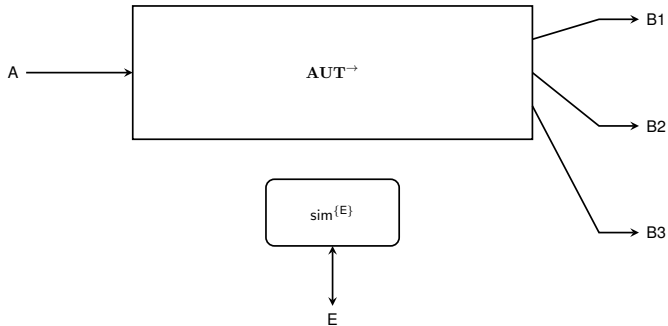
Authenticity:



Introduction

Security notions typically restrict what dishonest parties can do.

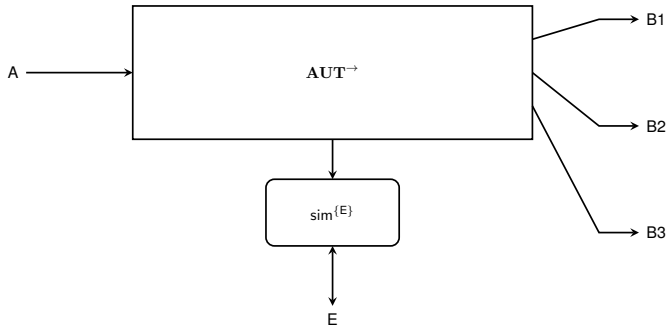
Authenticity:



Introduction

Security notions typically restrict what dishonest parties can do.

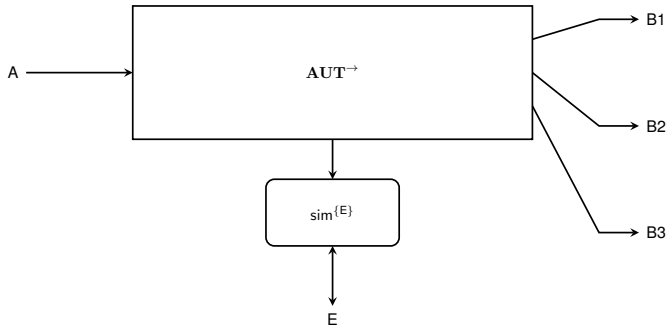
Authenticity:



Introduction

Security notions typically restrict what dishonest parties can do.

Authenticity:



If a Bob reads a message, then Alice wrote it.

Introduction

Introduction

However, some notions rely on **giving** guarantees to dishonest parties;

Introduction

However, some notions rely on **giving** guarantees to dishonest parties;

(Multi-)Designated Verifier Signatures:

Introduction

However, some notions rely on **giving** guarantees to dishonest parties;

(Multi-)Designated Verifier Signatures:

➔ Alice can designate the receivers of her messages

Introduction

However, some notions rely on **giving** guarantees to dishonest parties;

(Multi-)Designated Verifier Signatures:

➔ Alice can designate the receivers of her messages
say Bob 1, Bob 2 and Bob 3;

Introduction

However, some notions rely on **giving** guarantees to dishonest parties;

(Multi-)Designated Verifier Signatures:

- ➔ Alice can designate the receivers of her messages
  say Bob 1, Bob 2 and Bob 3;

- ➔ Authenticity is **exclusive** to these Bobs:

Introduction

However, some notions rely on **giving** guarantees to dishonest parties;

(Multi-)Designated Verifier Signatures:

- ➔ Alice can designate the receivers of her messages
  say Bob 1, Bob 2 and Bob 3;

- ➔ Authenticity is **exclusive** to these Bobs:
  only a Bob can learn Alice sent a message

Introduction

However, some notions rely on **giving** guarantees to dishonest parties;

(Multi-)Designated Verifier Signatures:

- ➔ Alice can designate the receivers of her messages
  say Bob 1, Bob 2 and Bob 3;

- ➔ Authenticity is **exclusive** to these Bobs:
  only a Bob can learn Alice sent a message — **Off-The-Record**

Introduction

However, some notions rely on **giving** guarantees to dishonest parties;

(Multi-)Designated Verifier Signatures:

- ➔ Alice can designate the receivers of her messages
  say Bob 1, Bob 2 and Bob 3;
- ➔ Authenticity is **exclusive** to these Bobs:
  only a Bob can learn Alice sent a message — **Off-The-Record**
- ➔ Eve cannot tell if Alice sent a message,

Introduction

However, some notions rely on **giving** guarantees to dishonest parties;

(Multi-)Designated Verifier Signatures:

- ➔ Alice can designate the receivers of her messages
  say Bob 1, Bob 2 and Bob 3;

- ➔ Authenticity is **exclusive** to these Bobs:
  only a Bob can learn Alice sent a message — **Off-The-Record**

- ➔ Eve cannot tell if Alice sent a message,
  even if any subset of these Bobs is dishonest.

Introduction — Off-The-Record

Why can’t Eve tell if Alice sent a message?

Introduction — Off-The-Record

Why can't Eve tell if Alice sent a message?

If all Bobs are **honest**:

Any dishonest party can simulate Alice sending a message;

Eve cannot tell the difference;

Introduction — Off-The-Record

Why can't Eve tell if Alice sent a message?

If all Bobs are **honest**:

Any dishonest party can simulate Alice sending a message;
Eve cannot tell the difference;

If some (or all) Bobs are **dishonest**:

Introduction — Off-The-Record

Why can't Eve tell if Alice sent a message?

If all Bobs are **honest**:

Any dishonest party can simulate Alice sending a message;
Eve cannot tell the difference;

If some (or all) Bobs are **dishonest**:

Dishonest Bobs can cooperatively simulate Alice sending a message;
Eve cannot tell the difference

Introduction — Off-The-Record

Why can't Eve tell if Alice sent a message?

If all Bobs are **honest**:

Any dishonest party can simulate Alice sending a message;
Eve cannot tell the difference;

If some (or all) Bobs are **dishonest**:

Dishonest Bobs can cooperatively simulate Alice sending a message;
Eve cannot tell the difference, even if she knows all dishonest Bobs' secrets;

Introduction — Off-The-Record

Why can't Eve tell if Alice sent a message?

If all Bobs are **honest**:

Any dishonest party can simulate Alice sending a message;
Eve cannot tell the difference;

If some (or all) Bobs are **dishonest**:

Dishonest Bobs can cooperatively simulate Alice sending a message;
Eve cannot tell the difference, even if she knows all dishonest Bobs' secrets;

➔ In any case, Eve cannot tell if Alice sent a message.

Introduction — Off-The-Record

Why can't Eve tell if Alice sent a message?

If all Bobs are **honest**:

Any dishonest party can simulate Alice sending a message;
Eve cannot tell the difference;

If some (or all) Bobs are **dishonest**:

Dishonest Bobs can cooperatively simulate Alice sending a message;
Eve cannot tell the difference, even if she knows all dishonest Bobs' secrets;

➔ In any case, Eve cannot tell if Alice sent a message.

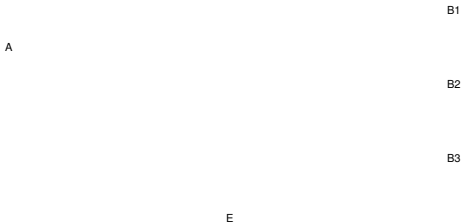
Off-The-Record does not violate Authenticity:

Off-The-Record: Eve cannot tell if Alice sent a message
Authenticity: **honest Bobs can!**

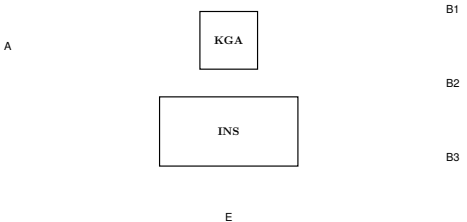
Introduction — Off-The-Record

How to model the Authenticity and Off-The-Record guarantees?

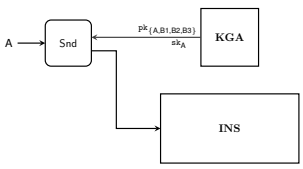
Introduction — Capturing Authenticity and Off-The-Record



Introduction — Capturing Authenticity and Off-The-Record



Introduction — Capturing Authenticity and Off-The-Record

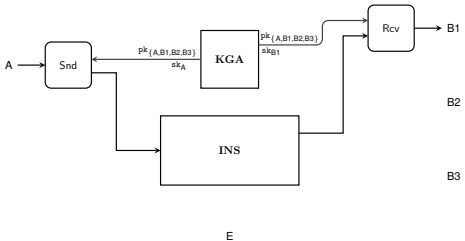


B1

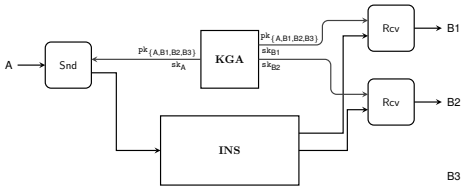
B2

B3

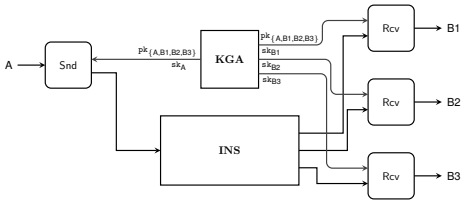
Introduction — Capturing Authenticity and Off-The-Record



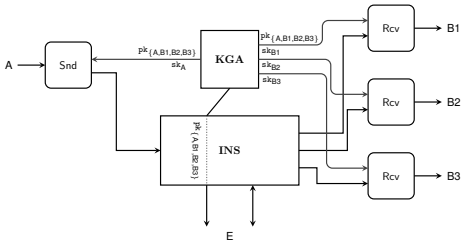
Introduction — Capturing Authenticity and Off-The-Record



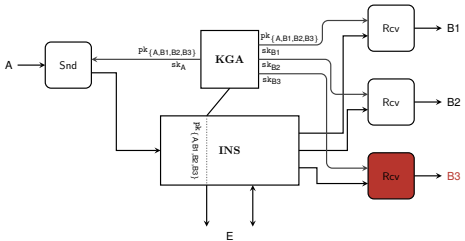
Introduction — Capturing Authenticity and Off-The-Record



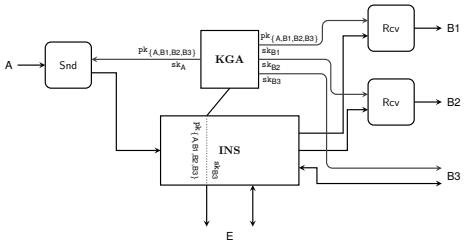
Introduction — Capturing Authenticity and Off-The-Record



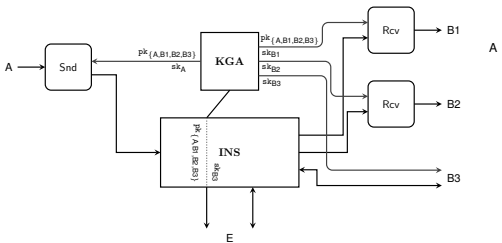
Introduction — Capturing Authenticity and Off-The-Record



Introduction — Capturing Authenticity and Off-The-Record

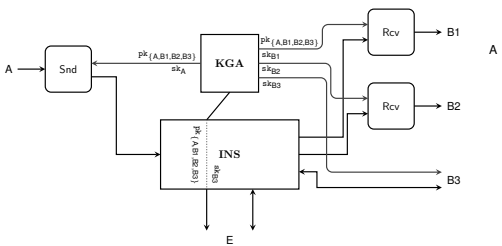


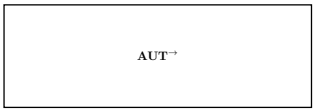
Introduction — Capturing Authenticity and Off-The-Record



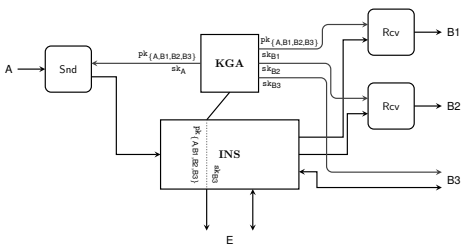
A
B1
B2
B3
E

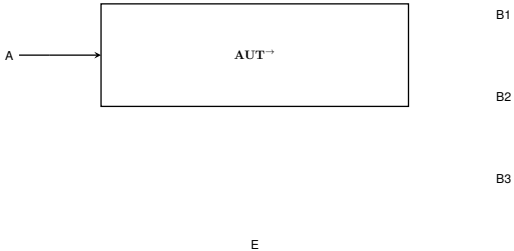
Introduction — Capturing Authenticity and Off-The-Record



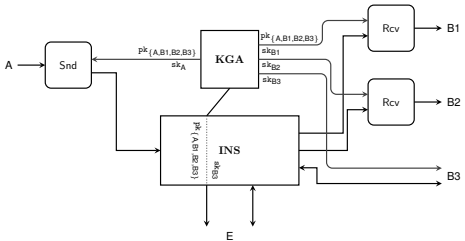


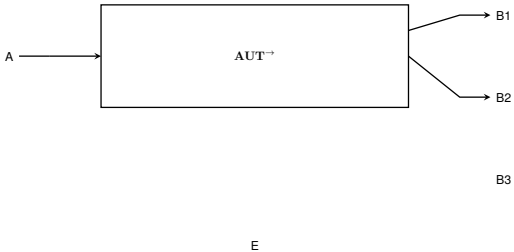
Introduction — Capturing Authenticity and Off-The-Record



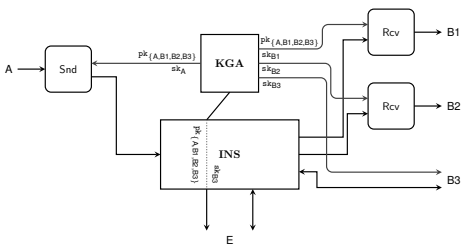


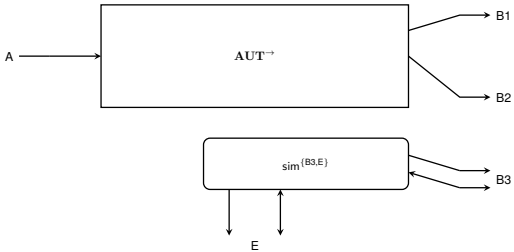
Introduction — Capturing Authenticity and Off-The-Record



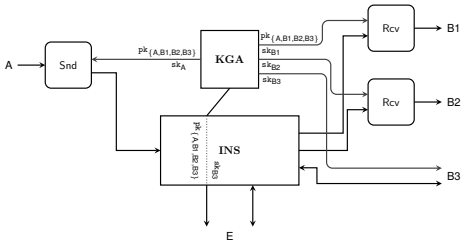


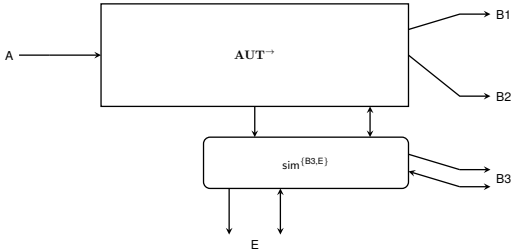
Introduction — Capturing Authenticity and Off-The-Record





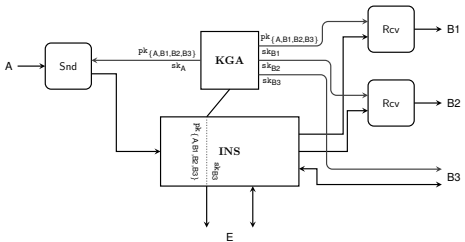
Introduction — Capturing Authenticity and Off-The-Record

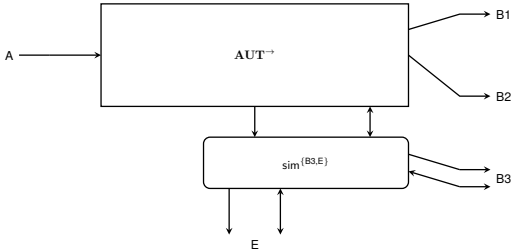




Introduction — Capturing Authenticity and Off-The-Record

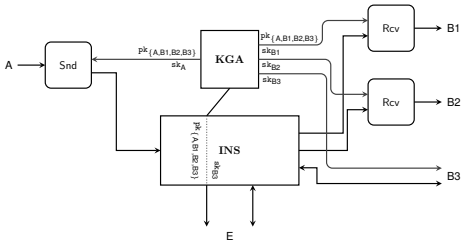
Problem: Any Unforgeable Signature Scheme satisfies this composable notion.

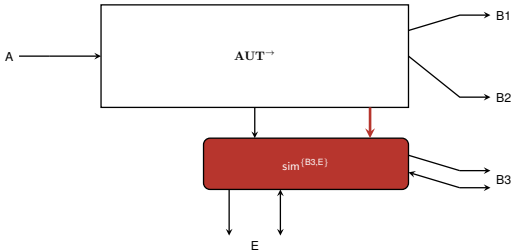




Introduction — Capturing Authenticity and Off-The-Record

Problem: Any Unforgeable Signature Scheme satisfies this composable notion.





Introduction — Problem

Introduction — Problem

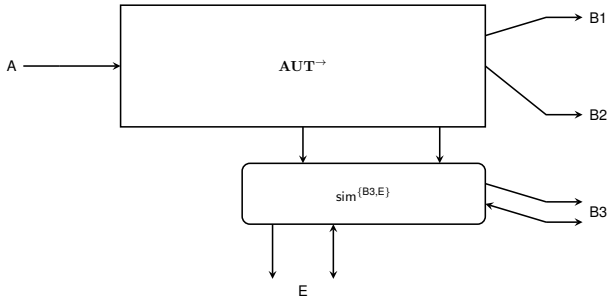
Problem: How to model that dishonest parties must have some capability?

Introduction — Problem

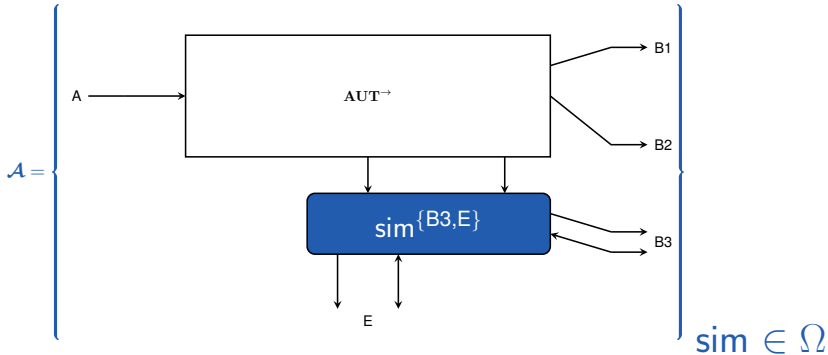
Problem: How to model that dishonest parties must have some capability?

Our approach: By using the notion of specifications (introduced by Maurer and Renner [2]).

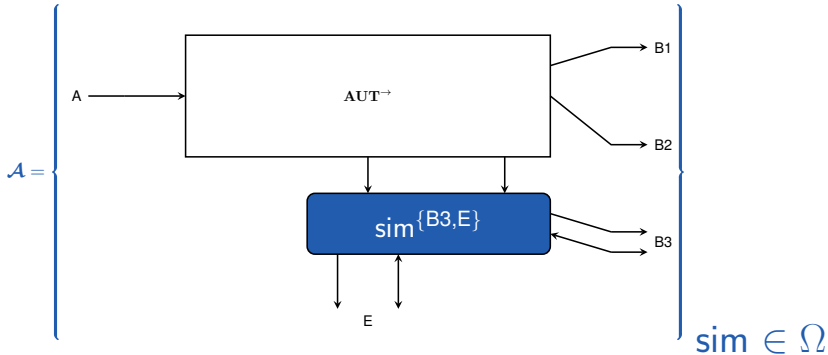
Introduction — Specifications



Introduction — Specifications



Introduction — Specifications



If an honest Bob reads a message, then Alice wrote it.

Introduction — Our approach

Introduction — Our approach

One specification restricts dishonest parties:

Introduction — Our approach

One specification restricts dishonest parties:

Authenticity: if an honest Bob reads a message, Alice wrote it;

Introduction — Our approach

One specification restricts dishonest parties:

Authenticity: if an honest Bob reads a message, Alice wrote it;

The other specification(s) gives guarantees to dishonest parties:

Introduction — Our approach

One specification restricts dishonest parties:

Authenticity: if an honest Bob reads a message, Alice wrote it;

The other specification(s) gives guarantees to dishonest parties:

Off-The-Record: dishonest parties can write too;

Introduction — Our approach

One specification restricts dishonest parties:

Authenticity: if an honest Bob reads a message, Alice wrote it;

The other specification(s) gives guarantees to dishonest parties:

Off-The-Record: dishonest parties can write too;

The ideal world is an **intersection** of specifications!

Introduction — Contributions

Introduction — Contributions

Show how to model guarantees given to dishonest parties (in Constructive Cryptography [2]);

Introduction — Contributions

Show how to model guarantees given to dishonest parties (in Constructive Cryptography [2]);

Composable notions for Multi-Designated Verifier Signature (MDVS) schemes;

Introduction — Contributions

Show how to model guarantees given to dishonest parties (in Constructive Cryptography [2]);

Composable notions for Multi-Designated Verifier Signature (MDVS) schemes;

Comparison against existing security notions for MDVS.

Introduction — Contributions

Show how to model guarantees given to dishonest parties (in Constructive Cryptography [2]);

Composable notions for Multi-Designated Verifier Signature (MDVS) schemes;

Comparison against existing security notions for MDVS. We find that:

- Only the notions introduced by Damgård et al. [1] capture the security of MDVS;

Introduction — Contributions

Show how to model guarantees given to dishonest parties (in Constructive Cryptography [2]);

Composable notions for Multi-Designated Verifier Signature (MDVS) schemes;

Comparison against existing security notions for MDVS. We find that:

- Only the notions introduced by Damgård et al. [1] capture the security of MDVS;
- Our notions are strictly weaker than Damgård et al.'s.

Outline

Constructive Cryptography

Constructive Cryptography

Resource Theory;

Constructive Cryptography

Resource Theory;

Specifications — set of resources satisfying some property

Constructive Cryptography

Resource Theory;

Specifications — set of resources satisfying some property (e.g. Authenticity);

Constructive Cryptography

Resource Theory;

Specifications — set of resources satisfying some property (e.g. Authenticity);

Construction: From (assumed) specification $\mathcal{R}$, using protocol π, construct a new specification $\mathcal{S}$:

Constructive Cryptography

Resource Theory;

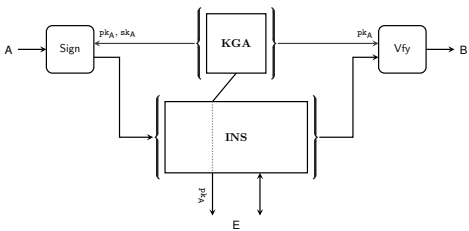
Specifications — set of resources satisfying some property (e.g. Authenticity);

Construction: From (assumed) specification $\mathcal{R}$, using protocol π, construct a new specification $\mathcal{S}$:

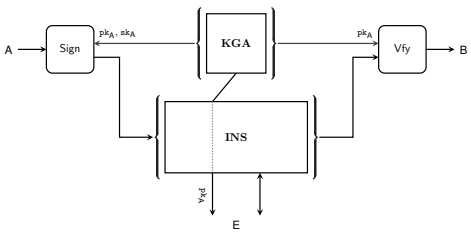
$$\pi\mathcal{R} \subseteq \mathcal{S}$$

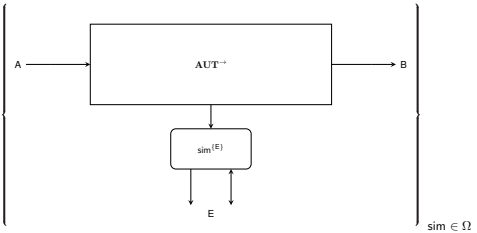
Constructive Cryptography — Construction

Constructive Cryptography — Construction

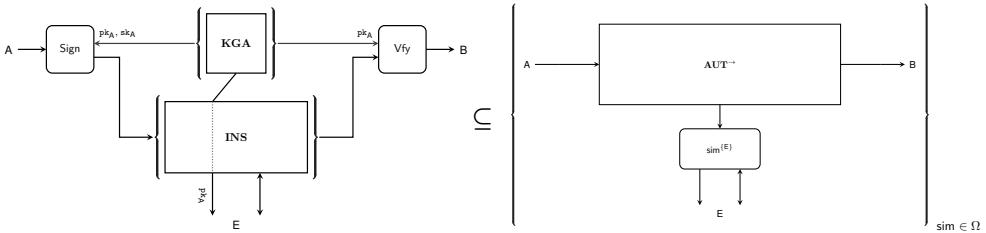


Constructive Cryptography — Construction

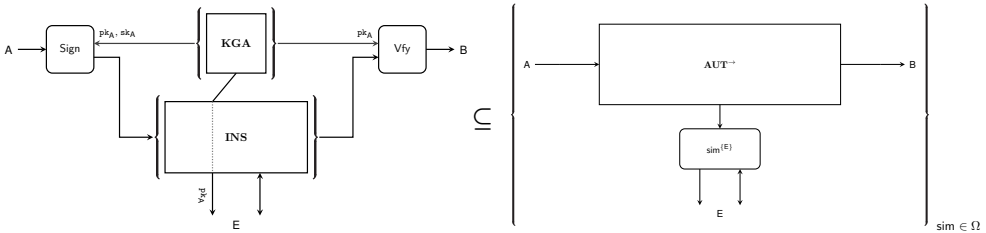




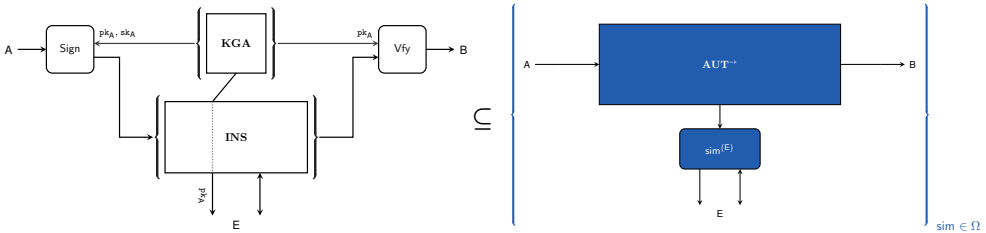
Constructive Cryptography — Construction



Constructive Cryptography — Composition



Constructive Cryptography — Composition



Constructive Cryptography — Composition

Constructive Cryptography — Composition

$$\pi\mathcal{R} \subseteq \mathcal{S}$$

Constructive Cryptography — Composition

$$\pi\mathcal{R} \subseteq \mathcal{S}$$

$$\pi'\mathcal{S} \subseteq \mathcal{T}$$

Constructive Cryptography — Composition

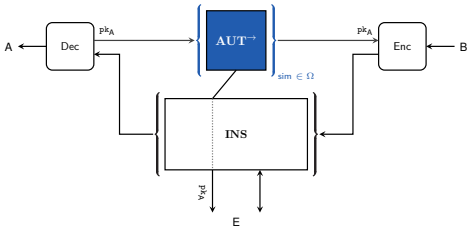
$$\pi\mathcal{R} \subseteq \mathcal{S}$$

$$\pi'\mathcal{S} \subseteq \mathcal{T}$$

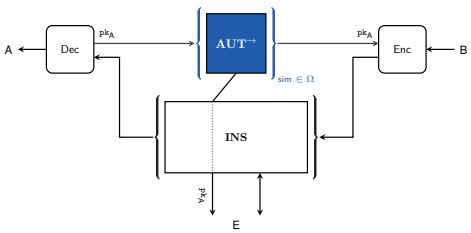
Composition: $\pi'(\pi\mathcal{R}) \subseteq \pi'\mathcal{S} \subseteq \mathcal{T}$

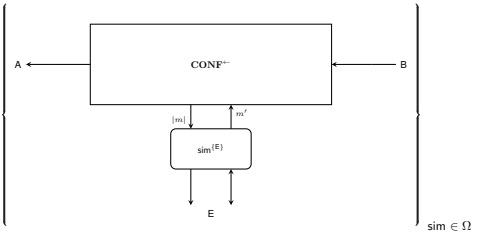
Constructive Cryptography — Composition

Constructive Cryptography — Composition

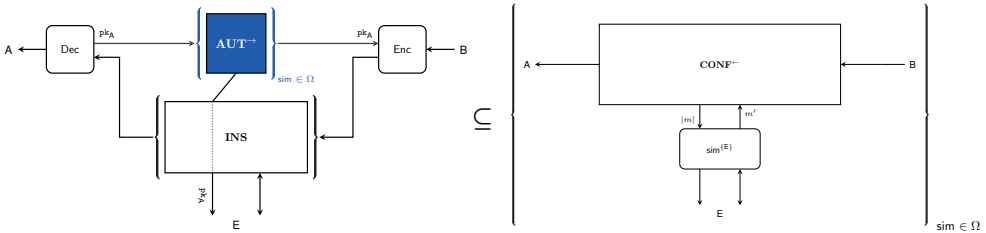


Constructive Cryptography — Composition





Constructive Cryptography — Composition



Constructive Cryptography — Specification Relaxations

Constructive Cryptography — Specification Relaxations

Often constructions do not hold unconditionally;

Constructive Cryptography — Specification Relaxations

Often constructions do not hold unconditionally;

Assumptions are needed — e.g. Discrete Log (DL) assumption;

Constructive Cryptography — Specification Relaxations

Often constructions do not hold unconditionally;
Assumptions are needed — e.g. Discrete Log (DL) assumption;

Construction statements are then bound to assumptions:

Constructive Cryptography — Specification Relaxations

Often constructions do not hold unconditionally;

Assumptions are needed — e.g. Discrete Log (DL) assumption;

Construction statements are then bound to assumptions:

One gives a reduction $\mathbf{C}_{\mathsf{DL}}$ such that:

Constructive Cryptography — Specification Relaxations

Often constructions do not hold unconditionally;

Assumptions are needed — e.g. Discrete Log (DL) assumption;

Construction statements are then bound to assumptions:

One gives a reduction $\mathbf{C}_{\mathsf{DL}}$ such that:

for any $\mathbf{D}$ and any $\mathbf{R} \in \boldsymbol{\mathcal{R}}$, there is $\mathbf{S} \in \boldsymbol{\mathcal{S}}$ such that:

$$\Delta^{\mathbf{D}}(\pi\mathbf{R}, \mathbf{S}) \leq Adv^{\mathsf{DL}}(\mathbf{D}\mathbf{C}_{\mathsf{DL}})$$

Constructive Cryptography — Specification Relaxations

Often constructions do not hold unconditionally;
Assumptions are needed — e.g. Discrete Log (DL) assumption;

Construction statements are then bound to assumptions:

One gives a reduction $\mathbf{C}_{\mathsf{DL}}$ such that:
for any $\mathbf{D}$ and any $\mathbf{R} \in \boldsymbol{\mathcal{R}}$, there is $\mathbf{S} \in \boldsymbol{\mathcal{S}}$ such that:

$$\Delta^{\mathbf{D}}(\pi\mathbf{R}, \mathbf{S}) \leq Adv^{\mathsf{DL}}(\mathbf{DC}_{\mathsf{DL}})$$

$$\boldsymbol{\mathcal{S}}^{Adv^{\mathsf{DL}}(\cdot\,\mathbf{C}_{\mathsf{DL}})} := \bigcup_{\mathbf{S}\in\boldsymbol{\mathcal{S}}} \{\mathbf{R} \mid \forall \mathbf{D} :\ \Delta^{\mathbf{D}}(\mathbf{R}, \mathbf{S}) \leq Adv^{\mathsf{DL}}(\mathbf{DC}_{\mathsf{DL}})\}$$

Constructive Cryptography — Specification Relaxations

Often constructions do not hold unconditionally;
Assumptions are needed — e.g. Discrete Log (DL) assumption;

Construction statements are then bound to assumptions:

One gives a reduction $\mathbf{C}_{\mathsf{DL}}$ such that:
for any $\mathbf{D}$ and any $\mathbf{R} \in \boldsymbol{\mathcal{R}}$, there is $\mathbf{S} \in \boldsymbol{\mathcal{S}}$ such that:

$$\Delta^{\mathbf{D}}(\pi\mathbf{R}, \mathbf{S}) \leq Adv^{\mathsf{DL}}(\mathbf{DC}_{\mathsf{DL}})$$

$$\boldsymbol{\mathcal{S}}^{Adv^{\mathsf{DL}}(\cdot\, \mathbf{C}_{\mathsf{DL}})} := \bigcup_{\mathbf{S} \in \boldsymbol{\mathcal{S}}} \{\mathbf{R} \mid \forall \mathbf{D} :\ \Delta^{\mathbf{D}}(\mathbf{R}, \mathbf{S}) \leq Adv^{\mathsf{DL}}(\mathbf{DC}_{\mathsf{DL}})\}$$

$$\pi\boldsymbol{\mathcal{R}} \subseteq \boldsymbol{\mathcal{S}}^{Adv^{\mathsf{DL}}(\cdot\, \mathbf{C}_{\mathsf{DL}})}$$

Constructive Cryptography — Specification Relaxations

Often constructions do not hold unconditionally;
Assumptions are needed — e.g. Discrete Log (DL) assumption;

Construction statements are then bound to assumptions:

One gives a reduction $\mathbf{C}_{\mathsf{DL}}$ such that:
for any $\mathbf{D}$ and any $\mathbf{R} \in \boldsymbol{\mathcal{R}}$, there is $\mathbf{S} \in \boldsymbol{\mathcal{S}}$ such that:

$$\Delta^{\mathbf{D}}(\pi\mathbf{R}, \mathbf{S}) \leq Adv^{\mathsf{DL}}(\mathbf{DC}_{\mathsf{DL}})$$

$$\boldsymbol{\mathcal{S}}^{Adv^{\mathsf{DL}}(\cdot\, \mathbf{C}_{\mathsf{DL}})} := \bigcup_{\mathbf{S} \in \boldsymbol{\mathcal{S}}} \{\mathbf{R} \mid \forall \mathbf{D} :\ \Delta^{\mathbf{D}}(\mathbf{R}, \mathbf{S}) \leq Adv^{\mathsf{DL}}(\mathbf{DC}_{\mathsf{DL}})\}$$

$$\pi\boldsymbol{\mathcal{R}} \subseteq \boldsymbol{\mathcal{S}}^{Adv^{\mathsf{DL}}(\cdot\, \mathbf{C}_{\mathsf{DL}})}$$

ε-relaxation:

Constructive Cryptography — Specification Relaxations

Often constructions do not hold unconditionally;

Assumptions are needed — e.g. Discrete Log (DL) assumption;

Construction statements are then bound to assumptions:

One gives a reduction $\mathbf{C}_{\mathsf{DL}}$ such that:

for any $\mathbf{D}$ and any $\mathbf{R} \in \boldsymbol{\mathcal{R}}$, there is $\mathbf{S} \in \boldsymbol{\mathcal{S}}$ such that:

$$\Delta^{\mathbf{D}}(\pi\mathbf{R}, \mathbf{S}) \leq Adv^{\mathsf{DL}}(\mathbf{D}\mathbf{C}_{\mathsf{DL}})$$

$$\boldsymbol{\mathcal{S}}^{Adv^{\mathsf{DL}}(\cdot\, \mathbf{C}_{\mathsf{DL}})} \coloneqq \bigcup_{\mathbf{S} \in \boldsymbol{\mathcal{S}}} \{\mathbf{R} \mid \forall \mathbf{D} :\ \Delta^{\mathbf{D}}(\mathbf{R}, \mathbf{S}) \leq Adv^{\mathsf{DL}}(\mathbf{D}\mathbf{C}_{\mathsf{DL}})\}$$

$$\pi\boldsymbol{\mathcal{R}} \subseteq \boldsymbol{\mathcal{S}}^{Adv^{\mathsf{DL}}(\cdot\, \mathbf{C}_{\mathsf{DL}})}$$

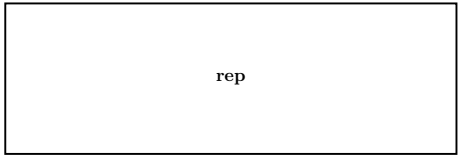
ε-relaxation:

$$\boldsymbol{\mathcal{S}}^{\varepsilon} \coloneqq \bigcup_{\mathbf{S} \in \boldsymbol{\mathcal{S}}} \{\mathbf{R} \mid \forall \mathbf{D} :\ \Delta^{\mathbf{D}}(\mathbf{R}, \mathbf{S}) \leq \varepsilon(\mathbf{D})\}.$$

Outline

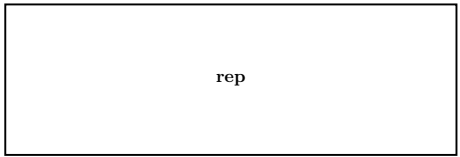
Repositories — An abstract model for communication

Repositories — An abstract model for communication



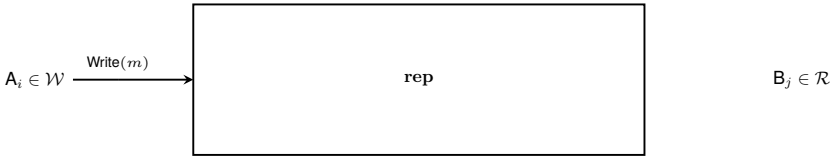
Repositories — An abstract model for communication

$\mathsf{A}_i \in \mathcal{W}$

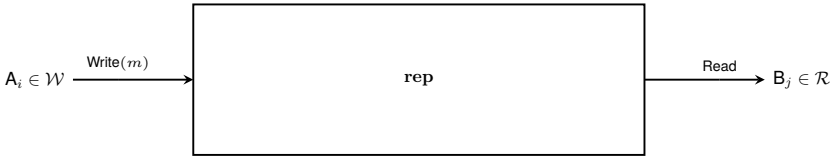


Repositories — An abstract model for communication

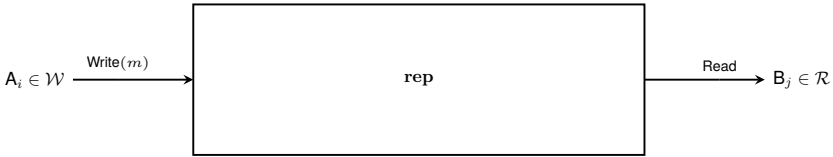
Repositories — An abstract model for communication



Repositories — An abstract model for communication

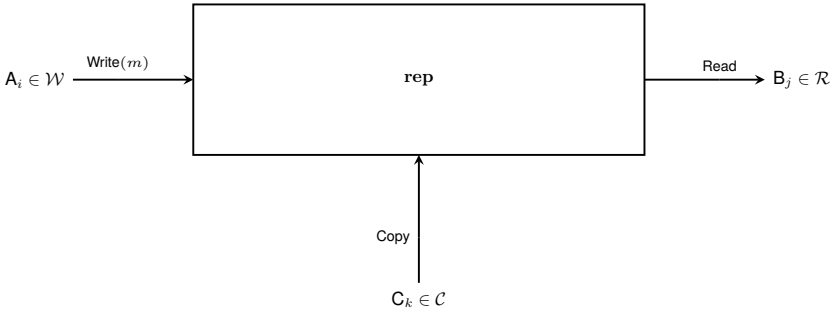


Repositories — An abstract model for communication

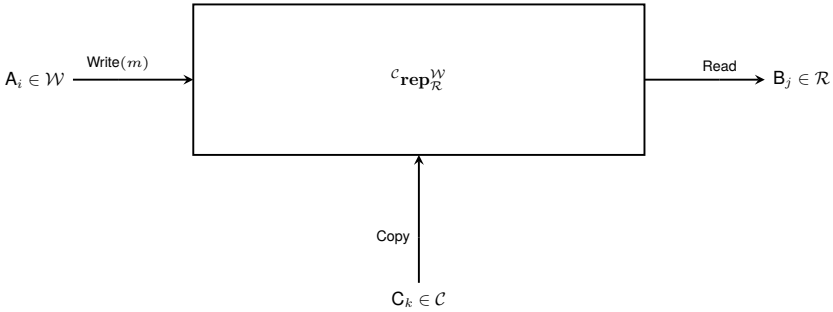


$\mathsf{C}_k \in \mathcal{C}$

Repositories — An abstract model for communication



Repositories — An abstract model for communication



Outline

Composable Notions for MDVS

Composable Notions for MDVS — Notation

Composable Notions for MDVS — Notation

Set of parties: $\mathcal{P}$

Composable Notions for MDVS — Notation

Set of parties: $\mathcal{P} = \mathcal{P}^H \uplus \overline{\mathcal{P}^H}$

Composable Notions for MDVS — Notation

Set of parties: $\mathcal{P} = \mathcal{P}^H \uplus \overline{\mathcal{P}^H}$

$\mathcal{P}^H$: Partition of honest parties

Composable Notions for MDVS — Notation

Set of parties: $\mathcal{P} = \mathcal{P}^H \uplus \overline{\mathcal{P}^H}$

- $\mathcal{P}^H$: Partition of honest parties
- $\overline{\mathcal{P}^H}$: Partition of dishonest parties

Composable Notions for MDVS — Notation

Set of parties: $\mathcal{P} = \mathcal{P}^H \uplus \overline{\mathcal{P}^H}$

- $\mathcal{P}^H$: Partition of honest parties
- $\overline{\mathcal{P}^H}$: Partition of dishonest parties

Set of parties who are senders: $\mathcal{S} \subseteq \mathcal{P}$

Composable Notions for MDVS — Notation

Set of parties: $\mathcal{P} = \mathcal{P}^H \uplus \overline{\mathcal{P}^H}$

- $\mathcal{P}^H$: Partition of honest parties
- $\overline{\mathcal{P}^H}$: Partition of dishonest parties

Set of parties who are senders: $\mathcal{S} \subseteq \mathcal{P}$

$\mathcal{S}^H \coloneqq \mathcal{S} \cap \mathcal{P}^H$
$\overline{\mathcal{S}^H} \coloneqq \mathcal{S} \cap \overline{\mathcal{P}^H}$

Composable Notions for MDVS — Notation

Set of parties: $\mathcal{P} = \mathcal{P}^H \uplus \overline{\mathcal{P}^H}$

$\mathcal{P}^H$: Partition of honest parties
$\overline{\mathcal{P}^H}$: Partition of dishonest parties

Set of parties who are senders: $\mathcal{S} \subseteq \mathcal{P}$

$\mathcal{S}^H \coloneqq \mathcal{S} \cap \mathcal{P}^H$
$\overline{\mathcal{S}^H} \coloneqq \mathcal{S} \cap \overline{\mathcal{P}^H}$

Set of parties who are receivers: $\mathcal{R} \subseteq \mathcal{P}$

Composable Notions for MDVS — Notation

Set of parties: $\mathcal{P} = \mathcal{P}^H \uplus \overline{\mathcal{P}^H}$

$\mathcal{P}^H$: Partition of honest parties
$\overline{\mathcal{P}^H}$: Partition of dishonest parties

Set of parties who are senders: $\mathcal{S} \subseteq \mathcal{P}$

$\mathcal{S}^H \coloneqq \mathcal{S} \cap \mathcal{P}^H$
$\overline{\mathcal{S}^H} \coloneqq \mathcal{S} \cap \overline{\mathcal{P}^H}$

Set of parties who are receivers: $\mathcal{R} \subseteq \mathcal{P}$

$\mathcal{R}^H \coloneqq \mathcal{R} \cap \mathcal{P}^H$
$\overline{\mathcal{R}^H} \coloneqq \mathcal{R} \cap \overline{\mathcal{P}^H}$

Composable Notions for MDVS — Setting

Composable Notions for MDVS — Setting

Fixed sender: $\mathcal{S} = \{\mathsf{A}\}$;

Composable Notions for MDVS — Setting

Fixed sender: $\mathcal{S} = \{\mathsf{A}\}$;

Fixed set of designated receivers: $\mathcal{R}$;

Composable Notions for MDVS — Setting

Fixed sender: $\mathcal{S} = \{\mathsf{A}\}$;

Fixed set of designated receivers: $\mathcal{R}$;

Non-designated receiver and dishonest party: E;

Composable Notions for MDVS — Setting

Fixed sender: $\mathcal{S} = \{\mathsf{A}\}$;

Fixed set of designated receivers: $\mathcal{R}$;

Non-designated receiver and dishonest party: E;

$$\Rightarrow \ \mathcal{P} = \{\mathsf{A},\mathsf{E}\} \cup \mathcal{R}$$

Composable Notions for MDVS — Setting

Fixed sender: $\mathcal{S} = \{\mathsf{A}\}$;

Fixed set of designated receivers: $\mathcal{R}$;

Non-designated receiver and dishonest party: E;

$$\Rightarrow \ \mathcal{P} = \{\mathsf{A},\mathsf{E}\} \cup \mathcal{R}$$

A sends messages to set $\mathcal{R}$;

Composable Notions for MDVS — Setting

Fixed sender: $\mathcal{S} = \{\mathsf{A}\}$;

Fixed set of designated receivers: $\mathcal{R}$;

Non-designated receiver and dishonest party: E;

$$\Rightarrow \ \mathcal{P} = \{\mathsf{A},\mathsf{E}\} \cup \mathcal{R}$$

A sends messages to set $\mathcal{R}$;

Static corruptions: set of dishonest parties is fixed.

Composable Notions for MDVS — Construction Statements

Composable Notions for MDVS — Construction Statements

One construction statement for each set of honest parties $\mathcal{P}^H$:

Composable Notions for MDVS — Construction Statements

One construction statement for each set of honest parties $\mathcal{P}^H$:

Real-World Specification: $\mathcal{R}^{\mathcal{P}^H}$

Composable Notions for MDVS — Construction Statements

One construction statement for each set of honest parties $\mathcal{P}^H$:

Real-World Specification: $\boldsymbol{\mathcal{R}}^{\mathcal{P}^H}$

Ideal-World Specification: $\boldsymbol{\mathcal{S}}^{\mathcal{P}^H}$

Composable Notions for MDVS — Construction Statements

One construction statement for each set of honest parties $\mathcal{P}^H$:

Real-World Specification: $\mathcal{R}^{\mathcal{P}^H}$

Ideal-World Specification: $\mathcal{S}^{\mathcal{P}^H}$

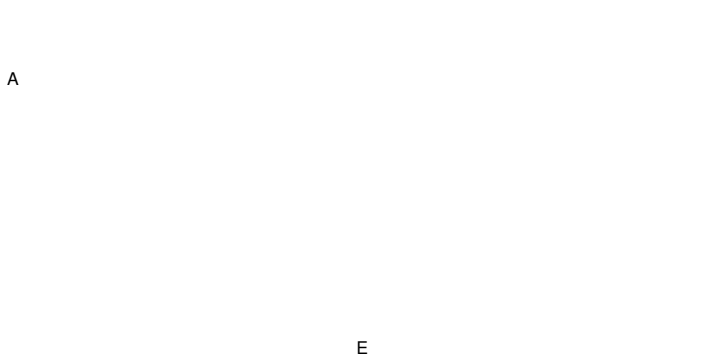
Construction statement:

$$\mathcal{R}^{\mathcal{P}^H} \subseteq \mathcal{S}^{\mathcal{P}^H}$$

Composable Notions for MDVS — The Real World

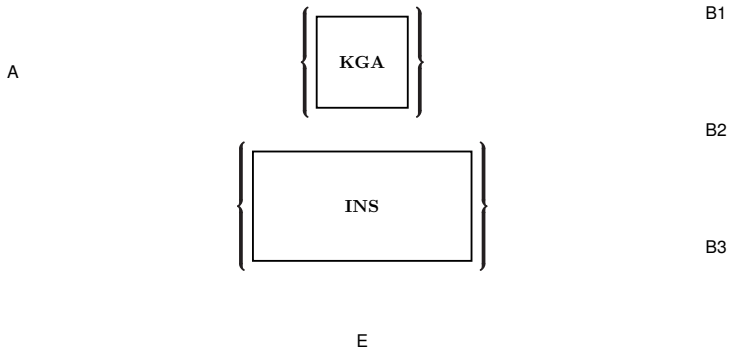
Composable Notions for MDVS — The Real World

$\mathcal{R} := \{\mathsf{B1}, \mathsf{B2}, \mathsf{B3}\}$;
$\mathcal{R}^H := \{\mathsf{B1}, \mathsf{B2}, \mathsf{B3}\}$;



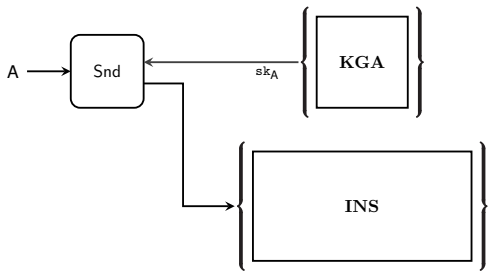
Composable Notions for MDVS — The Real World

$\mathcal{R} := \{\mathsf{B1}, \mathsf{B2}, \mathsf{B3}\}$;
$\mathcal{R}^H := \{\mathsf{B1}, \mathsf{B2}, \mathsf{B3}\}$;



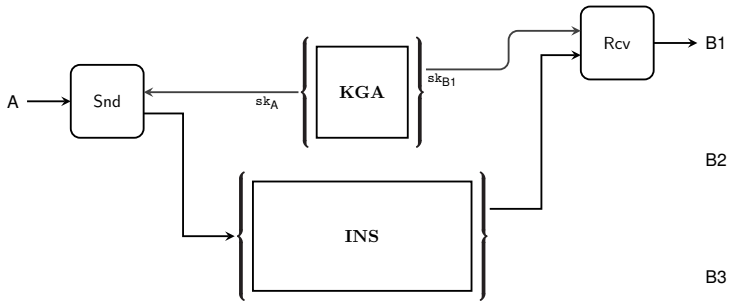
Composable Notions for MDVS — The Real World

$\mathcal{R} := \{\mathsf{B1}, \mathsf{B2}, \mathsf{B3}\}$;
$\mathcal{R}^H := \{\mathsf{B1}, \mathsf{B2}, \mathsf{B3}\}$;



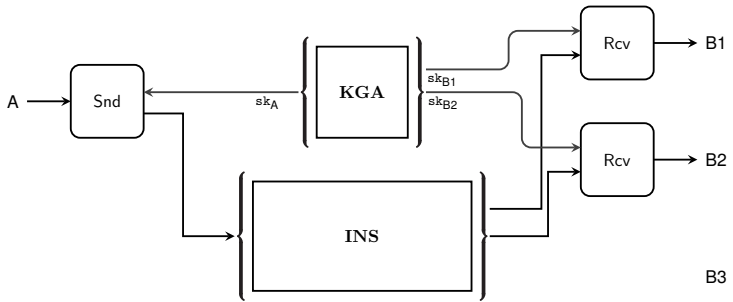
Composable Notions for MDVS — The Real World

$\mathcal{R} := \{\mathsf{B1}, \mathsf{B2}, \mathsf{B3}\}$;
$\mathcal{R}^H := \{\mathsf{B1}, \mathsf{B2}, \mathsf{B3}\}$;



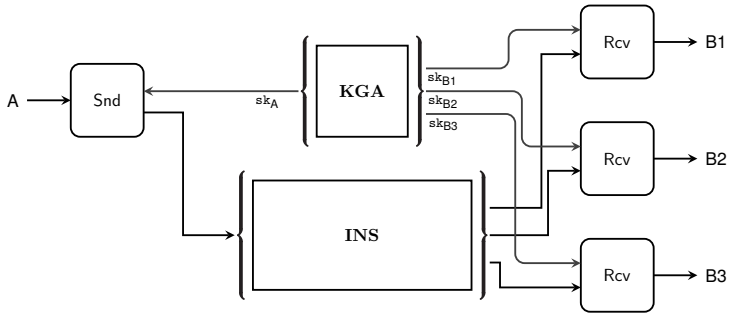
Composable Notions for MDVS — The Real World

$\mathcal{R} := \{\mathsf{B1}, \mathsf{B2}, \mathsf{B3}\};$
$\mathcal{R}^H := \{\mathsf{B1}, \mathsf{B2}, \mathsf{B3}\};$



Composable Notions for MDVS — The Real World

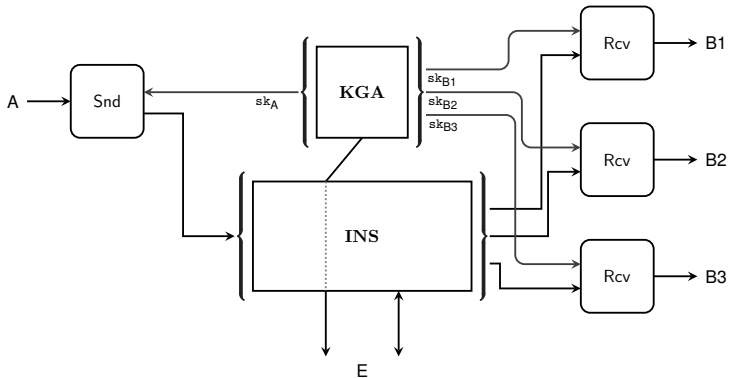
$\mathcal{R} := \{\mathsf{B1}, \mathsf{B2}, \mathsf{B3}\};$
$\mathcal{R}^H := \{\mathsf{B1}, \mathsf{B2}, \mathsf{B3}\};$



E

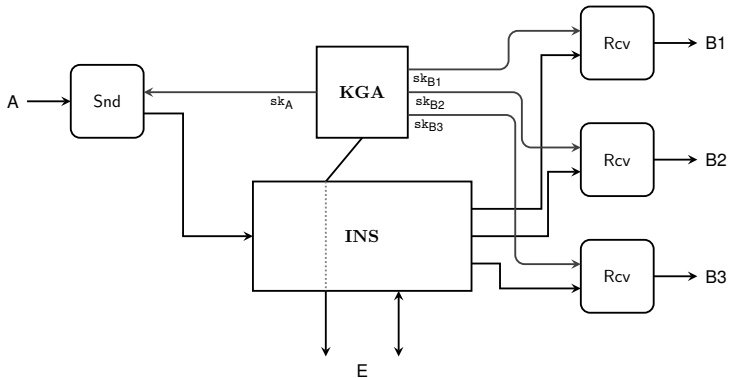
Composable Notions for MDVS — The Real World

$\mathcal{R} := \{\mathsf{B1}, \mathsf{B2}, \mathsf{B3}\}$;
$\mathcal{R}^H := \{\mathsf{B1}, \mathsf{B2}, \mathsf{B3}\}$;



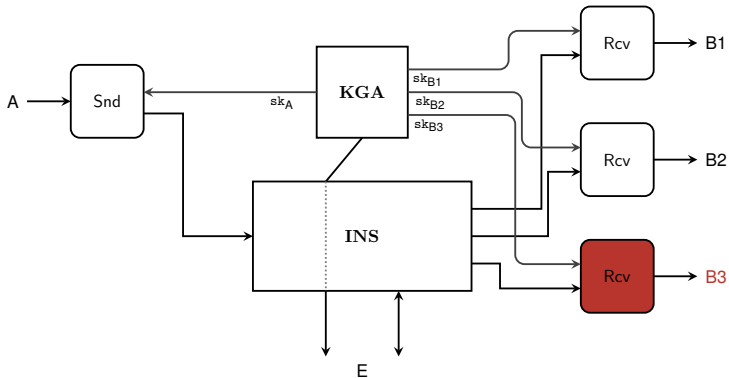
Composable Notions for MDVS — The Real World

$\mathcal{R} := \{\mathsf{B1}, \mathsf{B2}, \mathsf{B3}\}$;
$\mathcal{R}^H := \{\mathsf{B1}, \mathsf{B2}, \mathsf{B3}\}$;



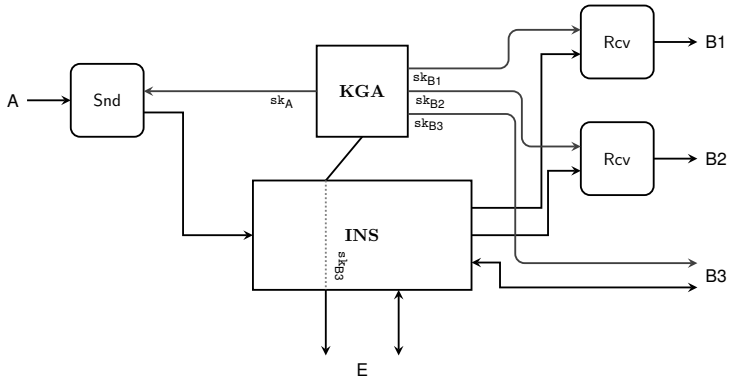
Composable Notions for MDVS — The Real World

$\mathcal{R} := \{\mathsf{B1}, \mathsf{B2}, \mathsf{B3}\};$
$\mathcal{R}^H := \{\mathsf{B1}, \mathsf{B2}, \sout{\mathsf{B3}}\};$



Composable Notions for MDVS — The Real World

$\mathcal{R} := \{\mathsf{B1}, \mathsf{B2}, \mathsf{B3}\}$;
$\mathcal{R}^H := \{\mathsf{B1}, \mathsf{B2}\}$;

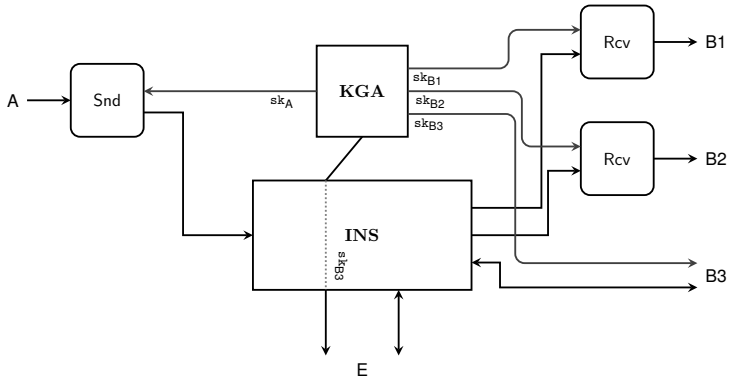


Composable Notions for MDVS — The Real World

$\mathcal{R} := \{\mathsf{B1}, \mathsf{B2}, \mathsf{B3}\}$;

$\mathcal{R}^H := \{\mathsf{B1}, \mathsf{B2}\}$;

$\boldsymbol{\mathcal{R}}$ denotes the real world specification.



Composable Notions for MDVS — Correctness and Authenticity

$\mathcal{R} \coloneqq \{\mathsf{B1}, \mathsf{B2}, \mathsf{B3}\};$

$\mathcal{R}^H \coloneqq \{\mathsf{B1}, \mathsf{B2}\};$

B1

A

B2

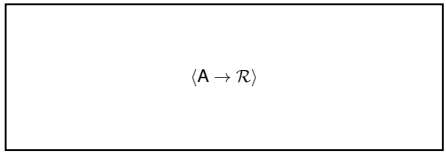
B3

E

Composable Notions for MDVS — Correctness and Authenticity

$\mathcal{R} \coloneqq \{\mathsf{B1}, \mathsf{B2}, \mathsf{B3}\};$

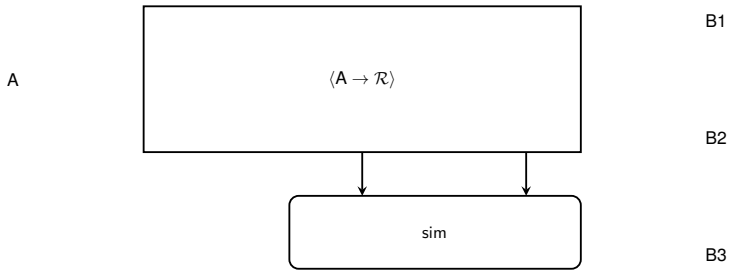
$\mathcal{R}^H \coloneqq \{\mathsf{B1}, \mathsf{B2}\};$



Composable Notions for MDVS — Correctness and Authenticity

$\mathcal{R} \coloneqq \{\mathsf{B1}, \mathsf{B2}, \mathsf{B3}\};$

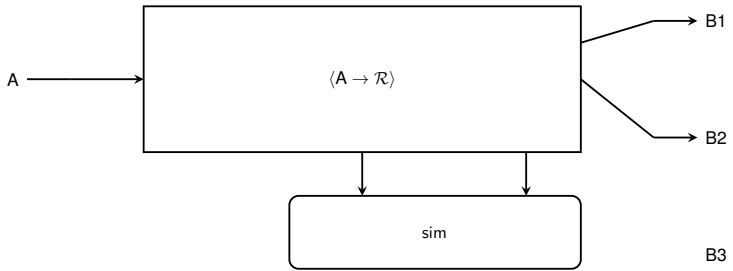
$\mathcal{R}^H \coloneqq \{\mathsf{B1}, \mathsf{B2}\};$



Composable Notions for MDVS — Correctness and Authenticity

$\mathcal{R} \coloneqq \{\mathsf{B1}, \mathsf{B2}, \mathsf{B3}\};$

$\mathcal{R}^H \coloneqq \{\mathsf{B1}, \mathsf{B2}\};$

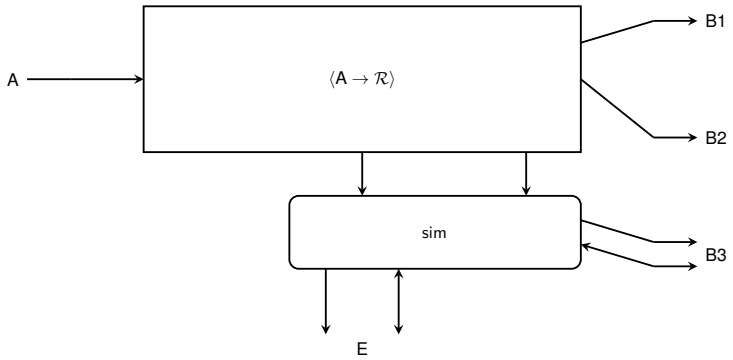


E

Composable Notions for MDVS — Correctness and Authenticity

$\mathcal{R} \coloneqq \{\mathsf{B1}, \mathsf{B2}, \mathsf{B3}\};$

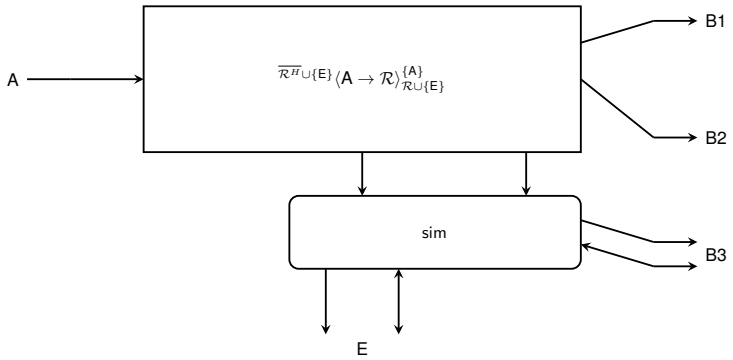
$\mathcal{R}^H \coloneqq \{\mathsf{B1}, \mathsf{B2}\};$



Composable Notions for MDVS — Correctness and Authenticity

$\mathcal{R} \coloneqq \{\mathsf{B1}, \mathsf{B2}, \mathsf{B3}\};$

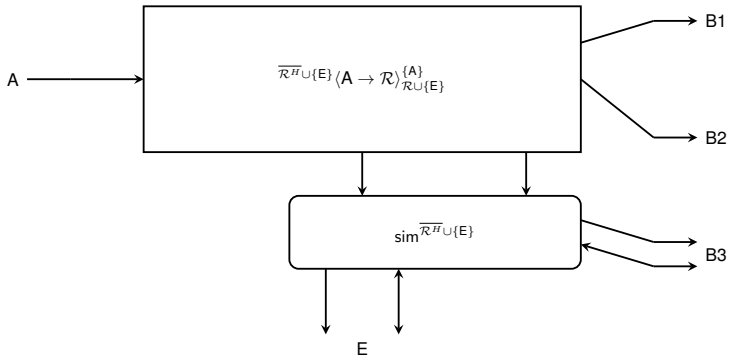
$\mathcal{R}^H \coloneqq \{\mathsf{B1}, \mathsf{B2}\};$



Composable Notions for MDVS — Correctness and Authenticity

$\mathcal{R} \coloneqq \{\mathsf{B1}, \mathsf{B2}, \mathsf{B3}\};$

$\mathcal{R}^H \coloneqq \{\mathsf{B1}, \mathsf{B2}\};$

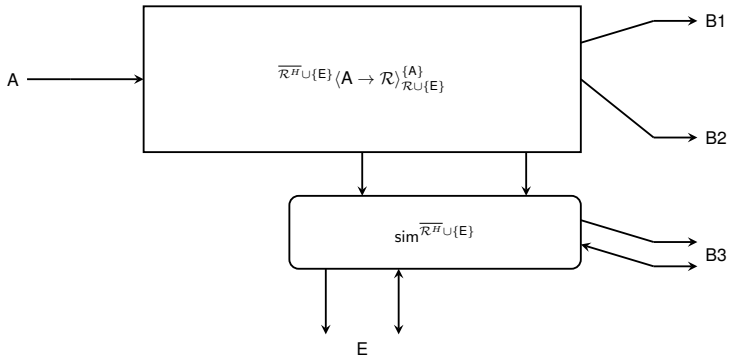


Composable Notions for MDVS — Correctness and Authenticity

$\mathcal{R} \coloneqq \{\mathsf{B1}, \mathsf{B2}, \mathsf{B3}\}$;

$\mathcal{R}^H \coloneqq \{\mathsf{B1}, \mathsf{B2}\}$;

$\boldsymbol{\mathcal{A}}$ denotes the specification capturing Correctness and Authenticity.



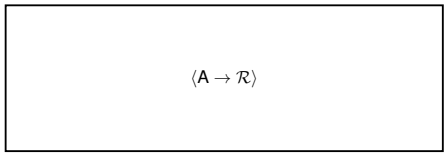
Composable Notions for MDVS — Off-The-Record

$\mathcal{R} \coloneqq \{\mathsf{B1}, \mathsf{B2}, \mathsf{B3}\}$;

$\mathcal{R}^H \coloneqq \{\mathsf{B1}, \mathsf{B2}\}$;

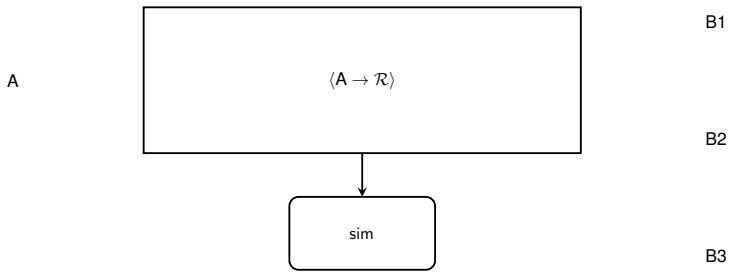
Composable Notions for MDVS — Off-The-Record

$\mathcal{R} \coloneqq \{\mathsf{B1}, \mathsf{B2}, \mathsf{B3}\}$;
$\mathcal{R}^H \coloneqq \{\mathsf{B1}, \mathsf{B2}\}$;



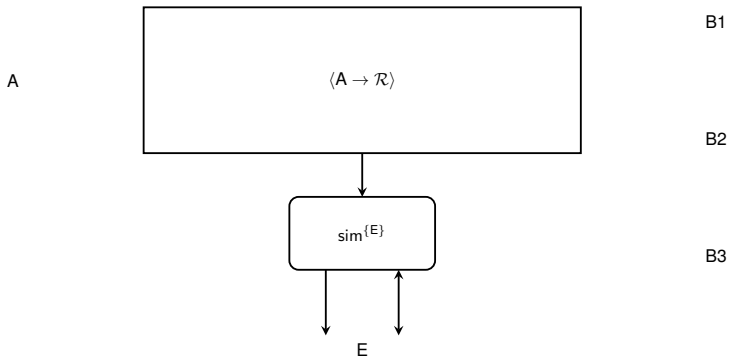
Composable Notions for MDVS — Off-The-Record

$\mathcal{R} \coloneqq \{\mathsf{B1}, \mathsf{B2}, \mathsf{B3}\};$
$\mathcal{R}^H \coloneqq \{\mathsf{B1}, \mathsf{B2}\};$



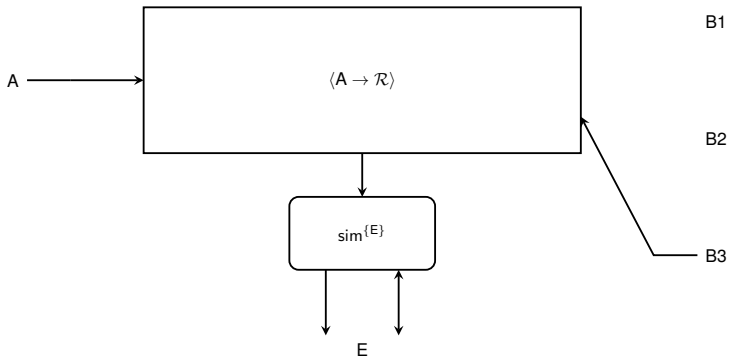
Composable Notions for MDVS — Off-The-Record

$\mathcal{R} \coloneqq \{\mathsf{B1}, \mathsf{B2}, \mathsf{B3}\};$
$\mathcal{R}^H \coloneqq \{\mathsf{B1}, \mathsf{B2}\};$



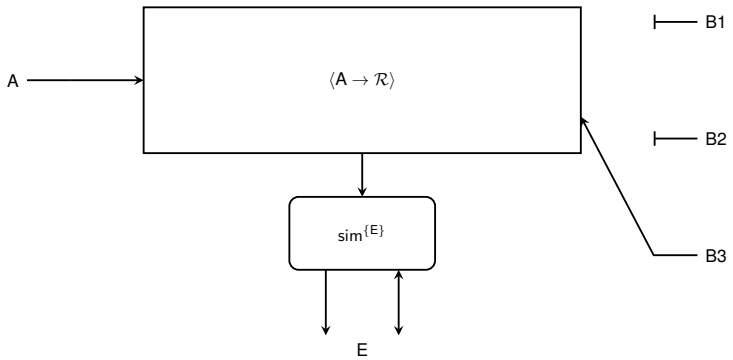
Composable Notions for MDVS — Off-The-Record

$\mathcal{R} \coloneqq \{\mathsf{B1}, \mathsf{B2}, \mathsf{B3}\}$;
$\mathcal{R}^H \coloneqq \{\mathsf{B1}, \mathsf{B2}\}$;



Composable Notions for MDVS — Off-The-Record

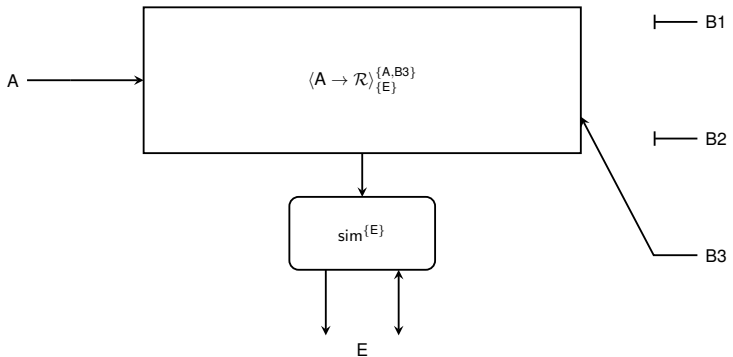
$\mathcal{R} \coloneqq \{\mathsf{B1}, \mathsf{B2}, \mathsf{B3}\}$;
$\mathcal{R}^H \coloneqq \{\mathsf{B1}, \mathsf{B2}\}$;



Composable Notions for MDVS — Off-The-Record

$\mathcal{R} \coloneqq \{\mathsf{B1}, \mathsf{B2}, \mathsf{B3}\};$

$\mathcal{R}^H \coloneqq \{\mathsf{B1}, \mathsf{B2}\};$

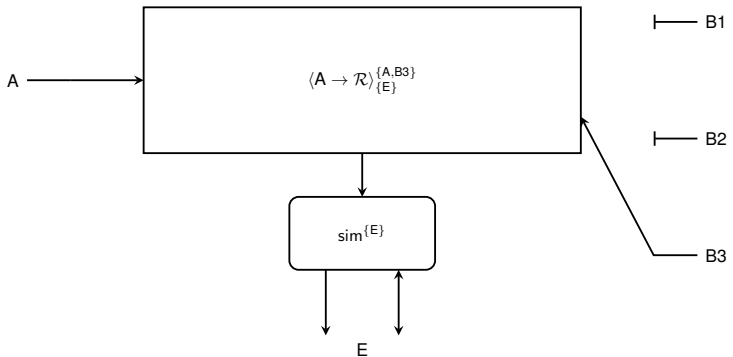


Composable Notions for MDVS — Off-The-Record

$\mathcal{R} \coloneqq \{\mathsf{B1}, \mathsf{B2}, \mathsf{B3}\}$;

$\mathcal{R}^H \coloneqq \{\mathsf{B1}, \mathsf{B2}\}$;

$\widehat{\boldsymbol{\mathcal{X}}}$ specification captures Off-The-Record.



Composable Notions for MDVS — What about the Real World?

B3 is dishonest!

Composable Notions for MDVS — What about the Real World?

B3 is dishonest!

➔ It does not run a converter. . .

Composable Notions for MDVS — What about the Real World?

B3 is dishonest!

➔ It does not run a converter…

Make a statement about what B3 **can do**!

Composable Notions for MDVS — What about the Real World?

B3 is dishonest!

➔ It does not run a converter…

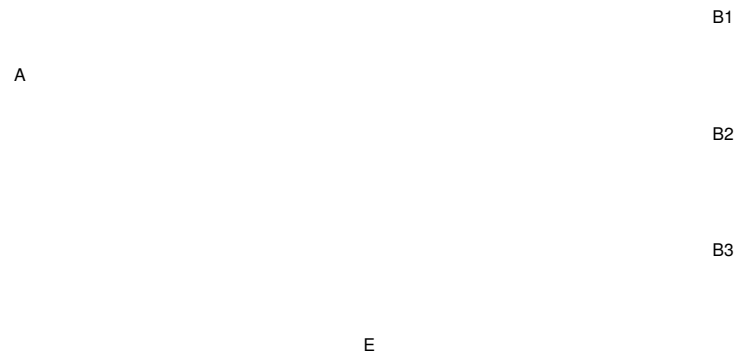
Make a statement about what B3 **can do**!

B3 **can run** a protocol π to simulate Alice writing!

Composable Notions for MDVS — B3 could have written

$\mathcal{R} := \{\mathsf{B1}, \mathsf{B2}, \mathsf{B3}\};$

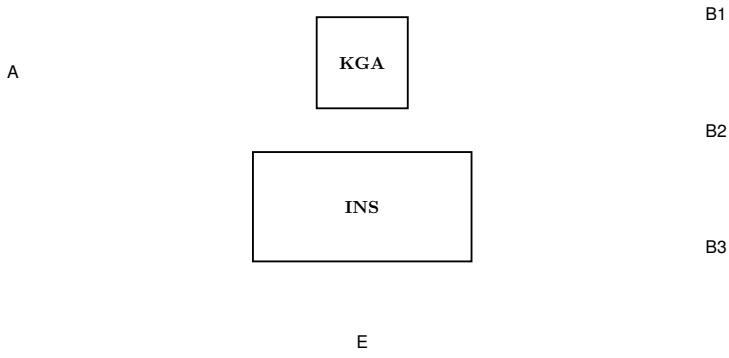
$\mathcal{R}^H := \{\mathsf{B1}, \mathsf{B2}\};$



Composable Notions for MDVS — B3 could have written

$\mathcal{R} := \{\mathsf{B1}, \mathsf{B2}, \mathsf{B3}\};$

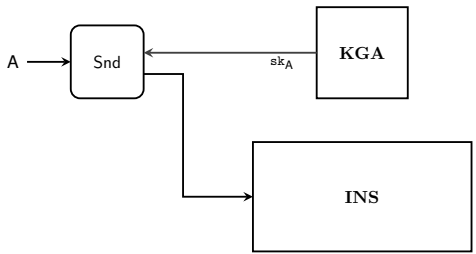
$\mathcal{R}^H := \{\mathsf{B1}, \mathsf{B2}\};$



Composable Notions for MDVS — B3 could have written

$\mathcal{R} := \{\mathsf{B1}, \mathsf{B2}, \mathsf{B3}\};$

$\mathcal{R}^H := \{\mathsf{B1}, \mathsf{B2}\};$



B1

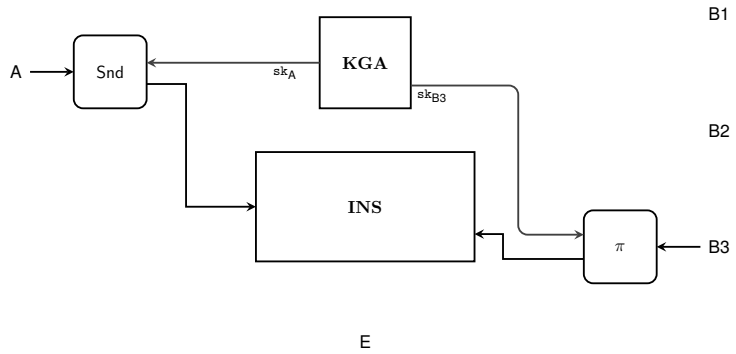
B2

B3

Composable Notions for MDVS — B3 could have written

$\mathcal{R} := \{\mathsf{B1}, \mathsf{B2}, \mathsf{B3}\};$

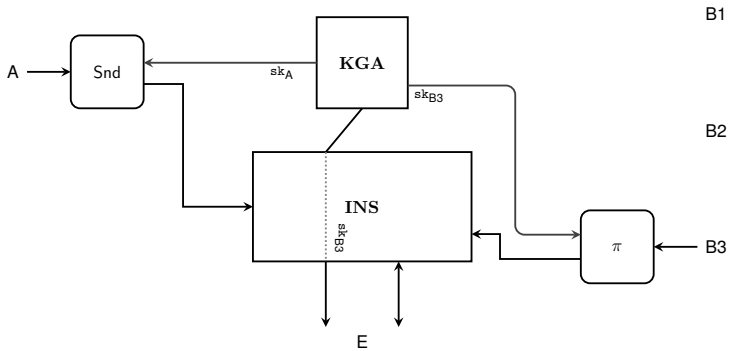
$\mathcal{R}^H := \{\mathsf{B1}, \mathsf{B2}\};$



Composable Notions for MDVS — B3 could have written

$\mathcal{R} := \{\mathsf{B1}, \mathsf{B2}, \mathsf{B3}\};$

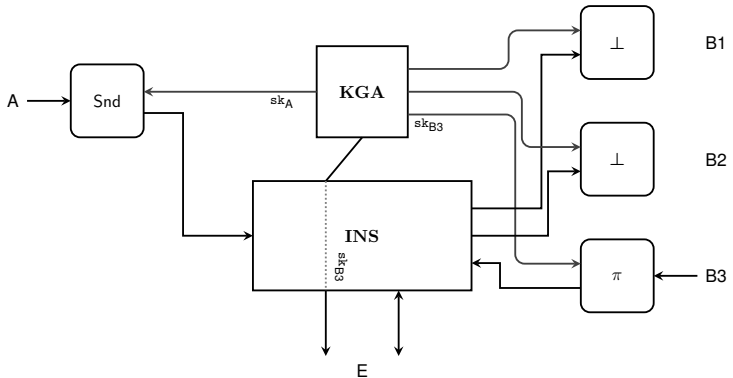
$\mathcal{R}^H := \{\mathsf{B1}, \mathsf{B2}\};$



Composable Notions for MDVS — B3 could have written

$\mathcal{R} := \{\mathsf{B1}, \mathsf{B2}, \mathsf{B3}\}$;

$\mathcal{R}^H := \{\mathsf{B1}, \mathsf{B2}\}$;



Composable Notions for MDVS — Capturing the ideal specification

Specification capturing guarantee that dishonest receivers **can write:**

$$\widehat{\boldsymbol{\mathcal{X}}} \coloneqq \left\{ \mathsf{sim}^{\{E\}} \left[\langle A \to \mathcal{R} \rangle_{\{E\}}^{\{A\} \cup \overline{\mathcal{R}^H}} \right] \right\}_{\mathsf{sim} \in \Omega}$$

Composable Notions for MDVS — Capturing the ideal specification

Specification capturing guarantee that dishonest receivers **can write:**

$$\widehat{\boldsymbol{\mathcal{X}}} := \left\{ \mathsf{sim}^{\{E\}} \left[\langle A \to \mathcal{R} \rangle_{\{E\}}^{\{A\} \cup \overline{\mathcal{R}^H}} \right] \right\}_{\mathsf{sim} \in \Omega}$$

Only consider real world systems giving this guarantee:

Composable Notions for MDVS — Capturing the ideal specification

Specification capturing guarantee that dishonest receivers **can write:**

$$\widehat{\boldsymbol{\mathcal{X}}} := \left\{ \mathsf{sim}^{\{E\}} \left[\langle A \to \mathcal{R} \rangle_{\{E\}}^{\{A\} \cup \overline{\mathcal{R}^H}} \right] \right\}_{\mathsf{sim} \in \Omega}$$

Only consider real world systems giving this guarantee:

$$\boldsymbol{\mathcal{X}}_\pi := \left\{ \mathbf{R} \mid \pi^{\overline{\mathcal{R}^H}} \perp^{\mathcal{R}^H} \mathbf{R} \in \widehat{\boldsymbol{\mathcal{X}}} \right\}$$

Composable Notions for MDVS — Capturing the ideal specification

Composable Notions for MDVS — Capturing the ideal specification

Ideal specification capturing Authenticity: $\mathcal{A}$;

Composable Notions for MDVS — Capturing the ideal specification

Ideal specification capturing Authenticity: $\mathcal{A}$;

Ideal specification capturing Off-The-Record: $\mathcal{X}_{\pi}$;

Composable Notions for MDVS — Capturing the ideal specification

Ideal specification capturing Authenticity: $\mathcal{A}$;

Ideal specification capturing Off-The-Record: $\mathcal{X}_\pi$;

Ideal specification capturing Authenticity and Off-The-Record:

$$\mathcal{A} \cap \mathcal{X}_\pi$$

Composable Notions for MDVS — Capturing the ideal specification

Ideal specification capturing Authenticity: $\mathcal{A}$;

Ideal specification capturing Off-The-Record: $\mathcal{X}_\pi$;

Ideal specification capturing Authenticity and Off-The-Record:

$$\mathcal{A} \cap \mathcal{X}_\pi$$

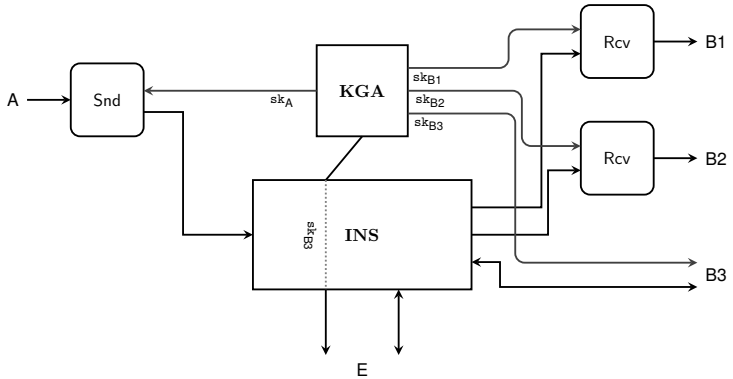
Construction statement: $\mathcal{R} \subseteq \mathcal{A} \cap \mathcal{X}_\pi$.

Composable Notions for MDVS — What if Alice is dishonest?

Composable Notions for MDVS — What if Alice is dishonest?

$\mathcal{R} := \{\mathsf{B1}, \mathsf{B2}, \mathsf{B3}\};$

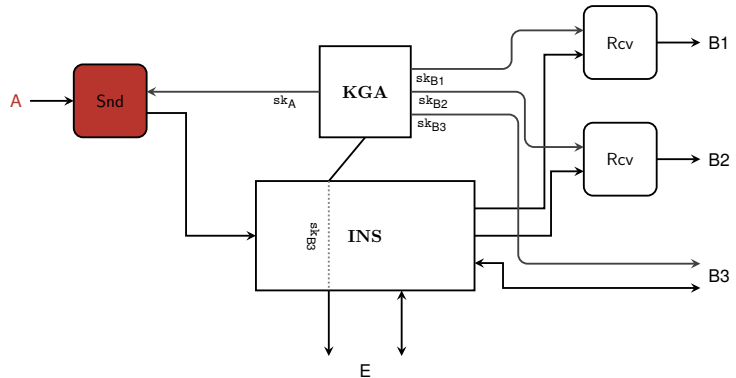
$\mathcal{R}^H := \{\mathsf{B1}, \mathsf{B2}\};$



Composable Notions for MDVS — What if Alice is dishonest?

$\mathcal{R} := \{\mathsf{B1}, \mathsf{B2}, \mathsf{B3}\};$

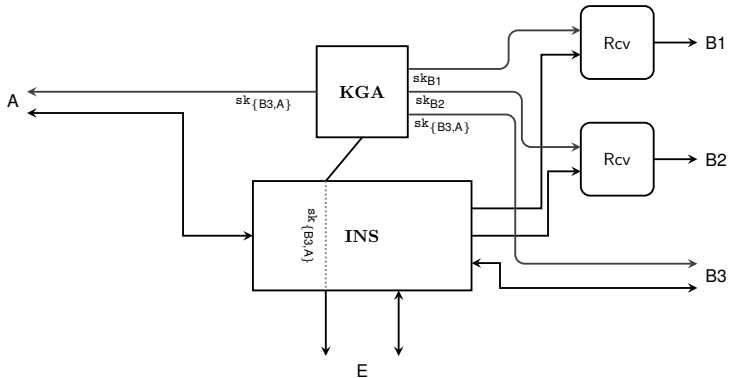
$\mathcal{R}^H := \{\mathsf{B1}, \mathsf{B2}\};$



Composable Notions for MDVS — What if Alice is dishonest?

$\mathcal{R} := \{\mathsf{B1}, \mathsf{B2}, \mathsf{B3}\};$

$\mathcal{R}^H := \{\mathsf{B1}, \mathsf{B2}\};$



Composable Notions for MDVS — What if Alice is dishonest?

Require consistency among receivers . . .

Composable Notions for MDVS — What if Alice is dishonest?

Require consistency among receivers . . .

. . . otherwise, why designating multiple receivers?

Composable Notions for MDVS — What if Alice is dishonest?

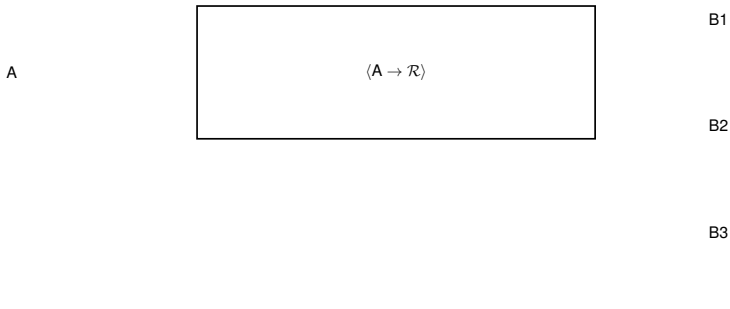
Require consistency among receivers . . .

. . . otherwise, why designating multiple receivers?

If an honest receiver gets a message m, all honest receivers get m too.

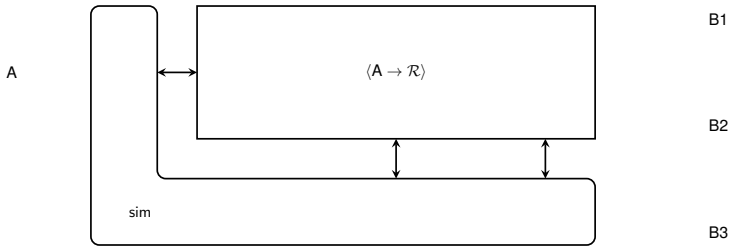
Composable Notions for MDVS — The Ideal World

$\mathcal{R} := \{\mathsf{B1}, \mathsf{B2}, \mathsf{B3}\};$
$\mathcal{R}^H := \{\mathsf{B1}, \mathsf{B2}\};$



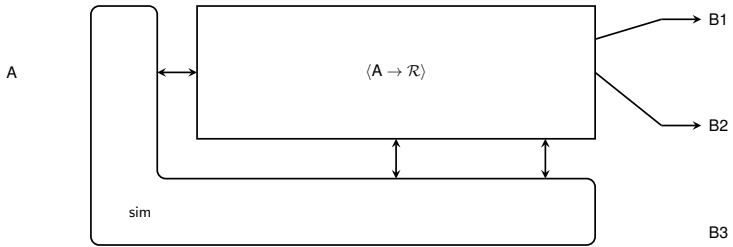
Composable Notions for MDVS — The Ideal World

$\mathcal{R} := \{\mathsf{B1}, \mathsf{B2}, \mathsf{B3}\};$
$\mathcal{R}^H := \{\mathsf{B1}, \mathsf{B2}\};$



Composable Notions for MDVS — The Ideal World

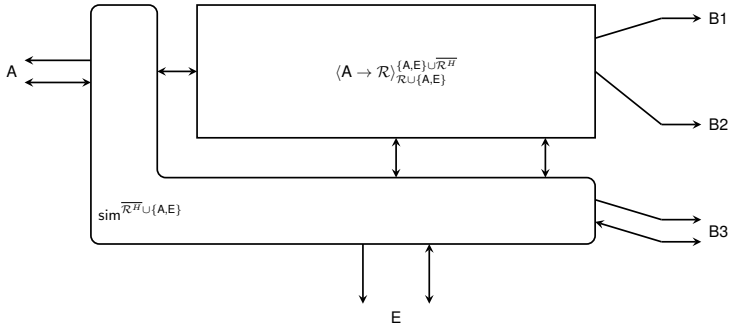
$\mathcal{R} := \{\mathsf{B1}, \mathsf{B2}, \mathsf{B3}\};$
$\mathcal{R}^H := \{\mathsf{B1}, \mathsf{B2}\};$



Composable Notions for MDVS — The Ideal World

$\mathcal{R} \coloneqq \{\mathsf{B1}, \mathsf{B2}, \mathsf{B3}\};$

$\mathcal{R}^H \coloneqq \{\mathsf{B1}, \mathsf{B2}\};$

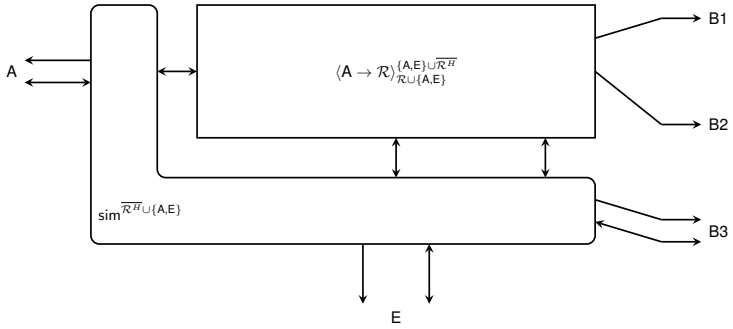


Composable Notions for MDVS — The Ideal World

$\mathcal{R} \coloneqq \{\mathsf{B1}, \mathsf{B2}, \mathsf{B3}\}$;

$\mathcal{R}^H \coloneqq \{\mathsf{B1}, \mathsf{B2}\}$;

$\mathcal{C}$ denotes the specification capturing Consistency.



Outline

1. Introduction
2. Constructive Cryptography
3. Repositories
4. Composable Notions
5. Other Contributions
6. Thank You!

Further Composable Notions for MDVS

Further Composable Notions for MDVS — Setting

Further Composable Notions for MDVS — Setting

Multiple senders: $\mathcal{S} = \{\text{A1,A2,}\dots\}$;

Further Composable Notions for MDVS — Setting

Multiple senders: $\mathcal{S} = \{\text{A1,A2,}\dots\}$;

Multiple receivers: $\mathcal{R} = \{\text{B1,B2,}\dots\}$;

Further Composable Notions for MDVS — Setting

Multiple senders: $\mathcal{S} = \{\text{A1,A2,}\dots\}$;

Multiple receivers: $\mathcal{R} = \{\text{B1,B2,}\dots\}$;

Each $A_i \in \mathcal{S}$ can send messages to any subset $\mathcal{V} \subseteq \mathcal{R}$;

Further Composable Notions for MDVS — Setting

Multiple senders: $\mathcal{S} = \{\text{A1,A2,}\dots\}$;

Multiple receivers: $\mathcal{R} = \{\text{B1,B2,}\dots\}$;

Each $A_i \in \mathcal{S}$ can send messages to any subset $\mathcal{V} \subseteq \mathcal{R}$;

Non-designated receiver and dishonest party: E;

Further Composable Notions for MDVS — Setting

Multiple senders: $\mathcal{S} = \{\text{A1,A2,}\dots\}$;

Multiple receivers: $\mathcal{R} = \{\text{B1,B2,}\dots\}$;

Each $A_i \in \mathcal{S}$ can send messages to any subset $\mathcal{V} \subseteq \mathcal{R}$;

Non-designated receiver and dishonest party: E;

$$\Rightarrow \ \mathcal{P} = \mathcal{S} \cup \mathcal{R} \cup \{\text{E}\}$$

Further Composable Notions for MDVS — Setting

Multiple senders: $\mathcal{S} = \{\text{A1,A2,}\dots\}$;

Multiple receivers: $\mathcal{R} = \{\text{B1,B2,}\dots\}$;

Each $A_i \in \mathcal{S}$ can send messages to any subset $\mathcal{V} \subseteq \mathcal{R}$;

Non-designated receiver and dishonest party: E;

$$\Rightarrow \ \mathcal{P} = \mathcal{S} \cup \mathcal{R} \cup \{\text{E}\}$$

Static corruptions: set of dishonest parties is fixed.

Further Composable Notions for MDVS

Further Composable Notions for MDVS

Stronger than notions with fixed sender and set of receivers;

Further Composable Notions for MDVS

Stronger than notions with fixed sender and set of receivers;

Only the notions introduced by Damgård et al. [1] capture the security of MDVS in this arbitrary party setting;

Further Composable Notions for MDVS

Stronger than notions with fixed sender and set of receivers;

Only the notions introduced by Damgård et al. [1] capture the security of MDVS in this arbitrary party setting;

Our notions for arbitrary party setting are strictly weaker than Damgård et al.'s.

Outline

Thank you!


Ivan Damgård, Helene Haagh, Rebekah Mercer, Anca Nitulescu, Claudio Orlandi, and Sophia Yakoubov.

Stronger security and constructions of multi-designated verifier signatures.

In Rafael Pass and Krzysztof Pietrzak, editors, *TCC 2020: 18th Theory of Cryptography Conference, Part II*, volume 12551 of *Lecture Notes in Computer Science*, pages 229–260, Durham, NC, USA, November 16–19, 2020. Springer, Heidelberg, Germany.


Ueli Maurer and Renato Renner.

From indifferentiability to constructive cryptography (and back).

In Martin Hirt and Adam D. Smith, editors, *TCC 2016-B: 14th Theory of Cryptography Conference, Part I*, volume 9985 of *Lecture Notes in Computer Science*, pages 3–24, Beijing, China, October 31 – November 3, 2016. Springer, Heidelberg, Germany.