Theory Days in Vanaõue

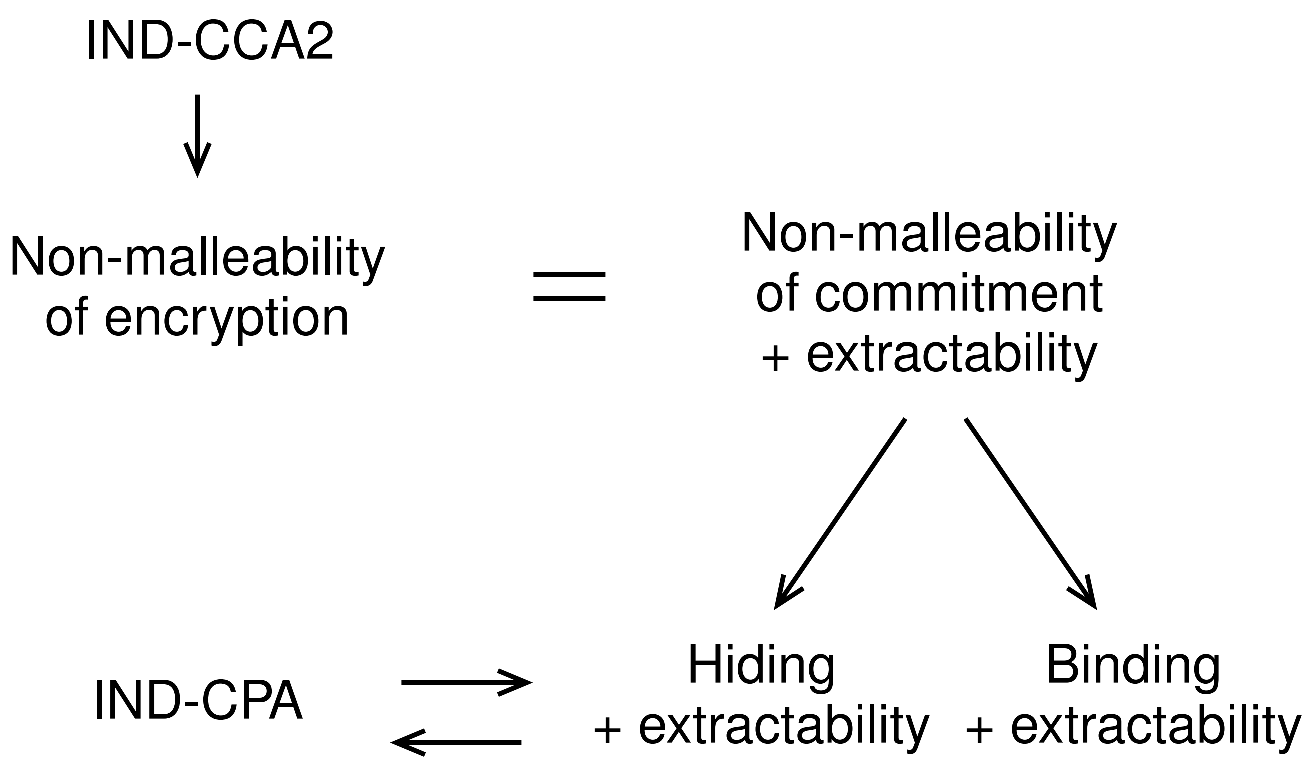
Duality Between Encryption and Commitment

Liina Kamm
University of Tartu
kamm@ut.ee

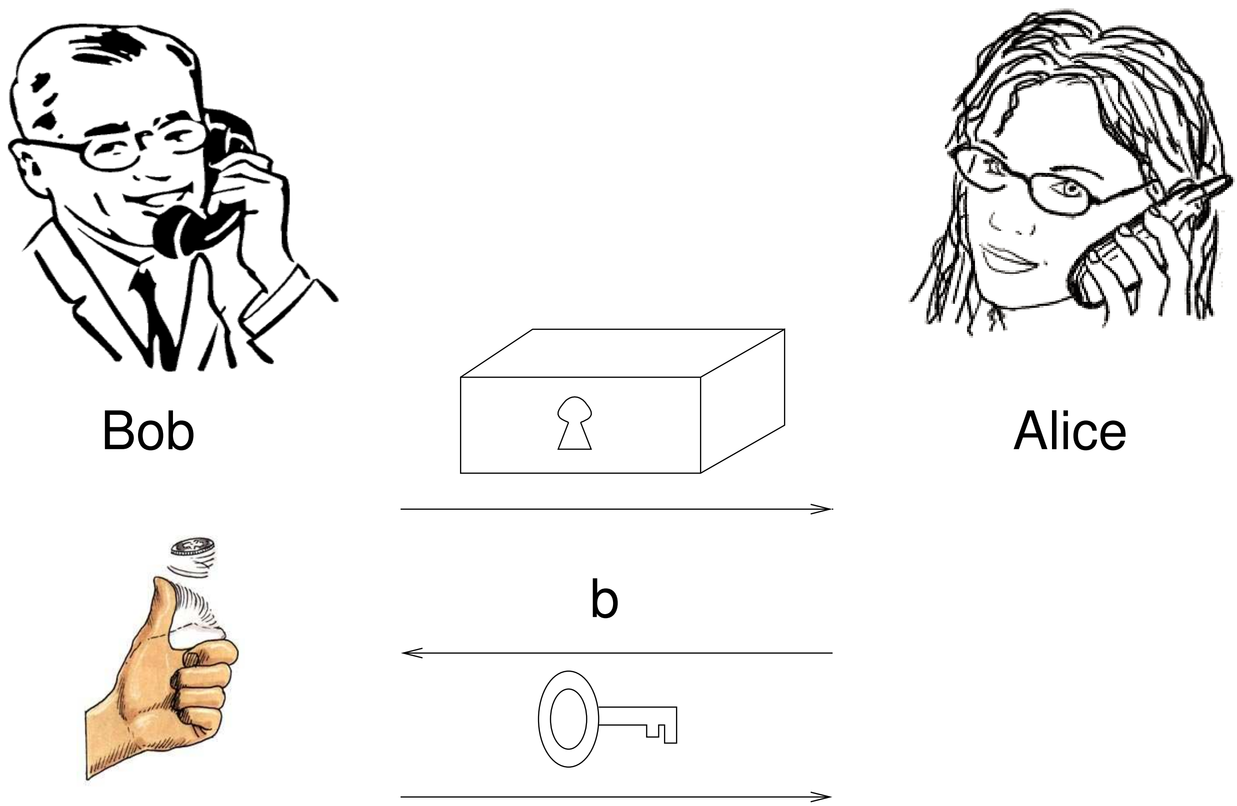
Overview

- Commitment Schemes and their basic properties
- Encryption Schemes
- Canonical correspondence between commitment and encryption

Associations Between Properties



Commitment Schemes: Basic Idea



Commitment Schemes: Applications

- Timestamping
- Secret sharing
- Electronic voting
- Secure multiparty computation
- Zero-knowledge proofs

Commitment Schemes: Construction

- Sender, receiver

- Components of a commitment scheme

  ⋆ Key generation $\mathsf{pk} \leftarrow \mathsf{Gen}$

  ⋆ Commitment $\mathsf{Com}_{\mathsf{pk}} : \mathcal{M} \times \mathcal{R} \rightarrow \mathcal{C} \times \mathcal{D}$

  ⋆ Opening $\mathsf{Open}_{\mathsf{pk}} : \mathcal{C} \times \mathcal{D} \rightarrow \mathcal{M} \cup \{\perp\}$

Commitment Schemes: Properties

- Hiding
- Binding
- Extractability
- Non-malleability

Hiding

A commitment scheme is (t, ε)-hiding, if a t-time adversary $A = (A_1, A_2)$ achieves advantage

$$\mathsf{Adv}^{\mathsf{hid}}_{\mathsf{Com}}(A) = 2 \cdot \left| \Pr \left[\begin{array}{l} \mathsf{pk} \leftarrow \mathsf{Gen}, s \leftarrow \{0,1\}, \\ (m_0, m_1, \sigma) \leftarrow A_1(\mathsf{pk}), \\ (c_s, d_s) \leftarrow \mathsf{Com}_{\mathsf{pk}}(m_s, r) : \\ A_2(\sigma, c_s) = s \end{array} \right] - \frac{1}{2} \right| \leqslant \varepsilon \ .$$

- Perfect

- Statistical

Binding

A commitment scheme is (t, ε)-binding, if a t-time adversary A achieves advantage

$$\mathsf{Adv}^{\mathsf{bind}}_{\mathsf{Com}}(A) = \Pr\left[\begin{array}{l}\mathsf{pk} \leftarrow \mathsf{Gen}, (c, d_0, d_1, \sigma) \leftarrow A(\mathsf{pk}) : \\ \perp \neq \mathsf{Open}_{\mathsf{pk}}(c, d_0) \neq \mathsf{Open}_{\mathsf{pk}}(c, d_1) \neq \perp\end{array}\right] \leqslant \varepsilon \ .$$

- Perfect
- Statistical

Hiding and Binding

- A commitment scheme cannot be both statistically hiding and binding

Challenger		Adversary
$b \leftarrow \{0, 1\}$		$(m_0, m_1) \leftarrow A_1$
	$\xleftarrow{(m_0, m_1)}$	
$c \leftarrow \mathsf{Com}(m_b)$		
	$\xrightarrow{c}$	
		$b' \leftarrow A_2(c, m_0, m_1)$

Examples of Properties

Scheme	Hiding	Binding
Canetti-Fischlin commitment scheme	computational	statistical
Halevi-Micali commitment scheme	statistical	computational
ElGamal commitment scheme	computational	perfect
Pedersen commitment scheme	perfect	computational
Fujisaki-Okamoto commitment scheme	statistical	computational
Cramer-Shoup commitment scheme	perfect	computational

Encryption Schemes

- Sender, receiver

- Components of an encryption scheme

  ⋆ Key generation $(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{Gen}$

  ⋆ Encryption $\mathsf{Enc}_{\mathsf{pk}} : \mathcal{M} \times \mathcal{R} \rightarrow \mathcal{E}$

  ⋆ Decryption $\mathsf{Dec}_{\mathsf{sk}} : \mathcal{E} \rightarrow \mathcal{M} \cup \{\perp\}$

Security of Encryption Schemes

- Indistinguishability under chosen plaintext attack (IND-CPA security)
- Indistinguishability under adaptive chosen ciphertext attack (IND-CCA2 security)

IND-CPA Security

An encryption scheme is (t, ε)-IND-CPA secure, if a t-time adversary $A = (A_1, A_2)$ achieves advantage

$$\mathsf{Adv}^{\mathsf{ind-cpa}}(A) = 2 \cdot \left| \Pr \left[\begin{array}{l} (\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{Gen}, s \leftarrow \{0,1\}, \\ (m_0, m_1, \sigma) \leftarrow A_1(\mathsf{pk}), \\ e \leftarrow \mathsf{Enc}_{\mathsf{pk}}(m_s; r) : A_2(\sigma, e) = s \end{array} \right] - \frac{1}{2} \right| \leqslant \varepsilon \ .$$

- Looks familiar?

IND-CCA2 Security

An encryption scheme is (t, ε)-IND-CCA2 secure, if a t-time adversary $A = (A_1, A_2)$ achieves advantage

$$\mathsf{Adv}^{\mathsf{ind-cca2}}(A) = 2 \cdot \left| \Pr \left[\begin{array}{l} (\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{Gen}, s \leftarrow \{0,1\}, \\ (m_0, m_1, \sigma) \leftarrow A_1^{\mathsf{Dec}_{\mathsf{sk}}(\cdot)}(\mathsf{pk}), \\ e \leftarrow \mathsf{Enc}_{\mathsf{pk}}(m_s; r) : \\ A_2^{\mathsf{Dec}_{\mathsf{sk}}(\cdot)}(\sigma, e) = s \end{array} \right] - \frac{1}{2} \right| \leqslant \varepsilon \quad ,$$

where $\mathsf{Dec}_{\mathsf{sk}}(\cdot)$ is a decryption oracle.

- It is assumed, that A_2 does not allow the oracle to decrypt e

Extractability (1)

- Two additional functions
  - ⋆ Key generation: $(\mathsf{sk}, \mathsf{pk}) \leftarrow \mathsf{Gen}^*$
  - ⋆ Message extraction: $\mathsf{Extr}_{\mathsf{sk}} : \mathcal{C} \longrightarrow \mathcal{M}$
- This kind of scheme can only be computationally hiding
- The function $\mathsf{Extr}_{\mathsf{sk}}$ cannot work for too long

Extractability (2)

- Not every commitment scheme has an extractability function
- Making an extractable scheme from a commitment scheme can be as complex as proving that $\mathcal{P} \neq \mathcal{NP}$
- It is not possible to make a sensible extractable scheme from every commitment scheme.

Canonical Correspondence

- Encryption scheme $\mathcal{E}nc = (\mathsf{Gen}_{\mathcal{E}nc}, \mathsf{Enc}, \mathsf{Dec})$
- Commitment scheme $\mathcal{C}om = (\mathsf{Gen}_{\mathcal{C}om}, \mathsf{Gen}^*_{\mathcal{C}om}, \mathsf{Com}, \mathsf{Open}, \mathsf{Extr})$
- From encryption to commitment
- From commitment to encryption

From Encryption to Commitment

- We have $\mathcal{E}nc = (\mathsf{Gen}_{\mathcal{E}nc}, \mathsf{Enc}, \mathsf{Dec})$

- What do we need?

  ⋆ Key generation

  ⋆ Commitment

  ⋆ Opening

From Commitment to Encryption

- We have $\mathcal{C}om = (\mathsf{Gen}_{\mathcal{C}om}, \mathsf{Gen}^*_{\mathcal{C}om}, \mathsf{Com}, \mathsf{Open}, \mathsf{Extr})$

- What do we need?
  - ⋆ Key generation
  - ⋆ Encryption
  - ⋆ Decryption

IND-CPA Security and Hiding

$$\mathsf{Adv}^{\mathsf{ind-cpa}}(A) = 2 \cdot \left| \Pr \left[\begin{array}{l} (\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{Gen}, s \leftarrow \{0,1\}, \\ (m_0, m_1, \sigma) \leftarrow A_1(\mathsf{pk}), \\ e \leftarrow \mathsf{Enc}_{\mathsf{pk}}(m_s; r) : A_2(\sigma, e) = s \end{array} \right] - \frac{1}{2} \right| \leqslant \varepsilon$$

and

$$\mathsf{Adv}^{\mathsf{hid}}_{\mathsf{Com}}(A) = 2 \cdot \left| \Pr \left[\begin{array}{l} \mathsf{pk} \leftarrow \mathsf{Gen}, s \leftarrow \{0,1\}, \\ (m_0, m_1, \sigma) \leftarrow A_1(\mathsf{pk}), \\ (c, d) \leftarrow \mathsf{Com}_{\mathsf{pk}}(m_s, r) : \\ A_2(\sigma, c) = s \end{array} \right] - \frac{1}{2} \right| \leqslant \varepsilon \ .$$

- Equivalent?

IND-CPA Security and Hiding

$$\mathsf{Adv}^{\mathsf{ind-cpa}}(A) = 2 \cdot \left| \Pr\left[\begin{array}{l} (\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{Gen}, s \leftarrow \{0,1\}, \\ (m_0, m_1, \sigma) \leftarrow A_1(\mathsf{pk}), \\ e \leftarrow \mathsf{Enc}_{\mathsf{pk}}(m_s; r) : A_2(\sigma, e) = s \end{array}\right] - \frac{1}{2} \right| \leqslant \varepsilon$$

and

$$\mathsf{Adv}^{\mathsf{hid}}_{\mathsf{Com}}(A) = 2 \cdot \left| \Pr\left[\begin{array}{l} \mathsf{pk} \leftarrow \mathsf{Gen}, s \leftarrow \{0,1\}, \\ (m_0, m_1, \sigma) \leftarrow A_1(\mathsf{pk}), \\ (c, d) \leftarrow \mathsf{Com}_{\mathsf{pk}}(m_s, r) : \\ A_2(\sigma, c) = s \end{array}\right] - \frac{1}{2} \right| \leqslant \varepsilon \ .$$

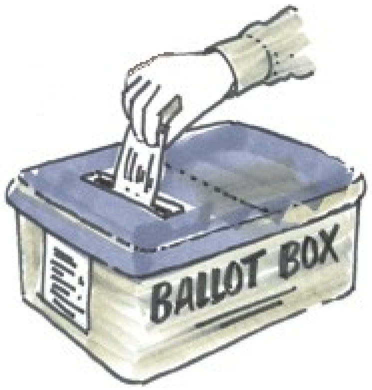
- Equivalent? Yes!

Malleability

- Possibility of making meaningful changes to the commitment

- This allows man-in-the-middle attacks

$$Alice \xrightarrow{x} Eve \xrightarrow{x+y} Bob$$



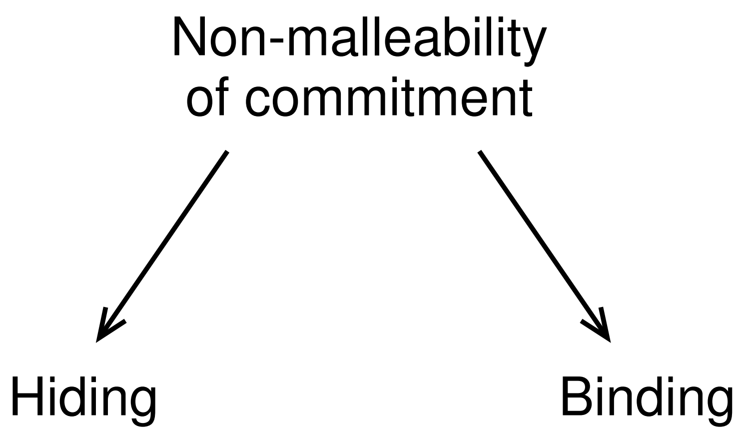
Non-Malleability

- Non-malleability w.r.t. opening
  - ⋆ The adversary cannot change the message and later be able to open it

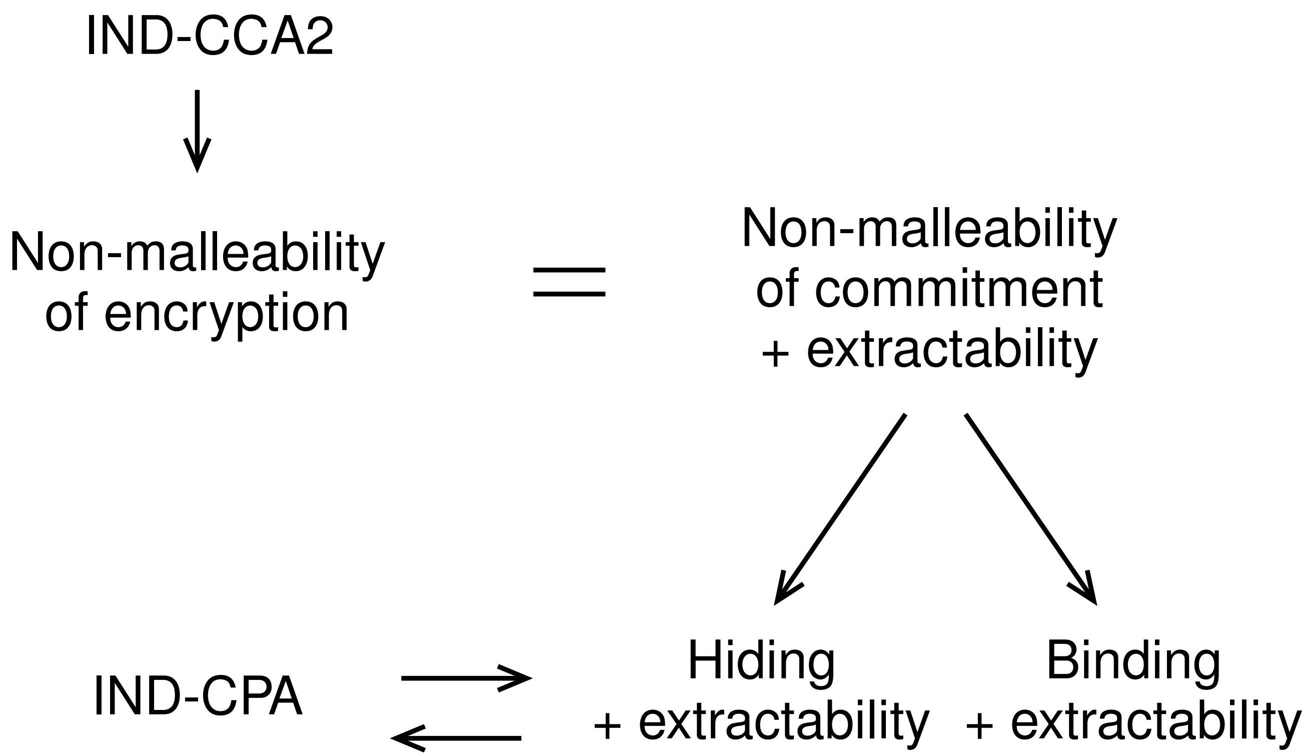
- Non-malleability w.r.t. commitment
  - ⋆ The adversary cannot create a new commitment based on an existing commitment

- Non-malleability w.r.t. commitment is stronger

Associations Between Properties (1)



Associations Between Properties (2)



Future work

- Prove, that non-malleability w.r.t. commitment implies non-malleability w.r.t. opening.

- What does IND-CCA2 mean in the context of commitments?

- How does the behaviour of the decommitment oracle change if the scheme is only computationally binding?

Thank you!