école normale supérieure paris—saclay

Analyzing KEM/DEM Hybrid Encryption in CCSA

M1 internship at LMF, CNRS, ENS Paris-Saclay

Jonathan Baumann

Supervised by Guillaume Scerri and Théo Vignon

September 5, 2024

In this Presentation

- Introduction of KEM/DEM hybrid encryption (Herranz, Hofheinz, and Kiltz [3])

In this Presentation

- Introduction of KEM/DEM hybrid encryption (Herranz, Hofheinz, and Kiltz [3])
- Introduction to CCSA (Baelde, Koutsos, and Lallemand [1])

école normale supérieure paris–saclay

In this Presentation

- Introduction of KEM/DEM hybrid encryption (Herranz, Hofheinz, and Kiltz [3])
- Introduction to CCSA (Baelde, Koutsos, and Lallemand [1])
- CCSA definitions for KEM/DEM security

In this Presentation

- Introduction of KEM/DEM hybrid encryption (Herranz, Hofheinz, and Kiltz [3])
- Introduction to CCSA (Baelde, Koutsos, and Lallemand [1])
- CCSA definitions for KEM/DEM security
- Proving KEM/DEM security in CCSA

Symmetric vs Asymmetric Encryption

Symmetric Encryption

- same key for encryption and decryption

Symmetric vs Asymmetric Encryption

Symmetric Encryption

- same key for encryption and decryption

+ typically very computationally efficient

Symmetric vs Asymmetric Encryption

Symmetric Encryption

- same key for encryption and decryption
- \+ typically very computationally efficient
- − requires establishing a shared secret key

Symmetric vs Asymmetric Encryption

Symmetric Encryption

- same key for encryption and decryption
- \+ typically very computationally efficient
- – requires establishing a shared secret key
- – one key per pair of participants

Symmetric vs Asymmetric Encryption

Symmetric Encryption

- same key for encryption and decryption

+ typically very computationally efficient

– requires establishing a shared secret key

– one key per pair of participants

Asymmetric Encryption

- different keys for encryption and decryption

Symmetric vs Asymmetric Encryption

Symmetric Encryption

- same key for encryption and decryption
- \+ typically very computationally efficient
- – requires establishing a shared secret key
- – one key per pair of participants

Asymmetric Encryption

- different keys for encryption and decryption
- \+ one key pair per participant

Symmetric vs Asymmetric Encryption

Symmetric Encryption

- same key for encryption and decryption
- \+ typically very computationally efficient
- − requires establishing a shared secret key
- − one key per pair of participants

Asymmetric Encryption

- different keys for encryption and decryption
- \+ one key pair per participant
- \+ public key can be published

Symmetric vs Asymmetric Encryption

Symmetric Encryption

- same key for encryption and decryption
- \+ typically very computationally efficient
- – requires establishing a shared secret key
- – one key per pair of participants

Asymmetric Encryption

- different keys for encryption and decryption
- \+ one key pair per participant
- \+ public key can be published
- – typically computationally expensive

Symmetric vs Asymmetric Encryption

Symmetric Encryption

- same key for encryption and decryption
- \+ typically very computationally efficient
- – requires establishing a shared secret key
- – one key per pair of participants

Asymmetric Encryption

- different keys for encryption and decryption
- \+ one key pair per participant
- \+ public key can be published
- – typically computationally expensive

Hybrid Encryption

PKE

- Generate a *single-use key* and encrypt it *asymmetrically* KEM

Symmetric vs Asymmetric Encryption

Symmetric Encryption

- same key for encryption and decryption

\+ typically very computationally efficient

– requires establishing a shared secret key

– one key per pair of participants

Asymmetric Encryption

- different keys for encryption and decryption

\+ one key pair per participant

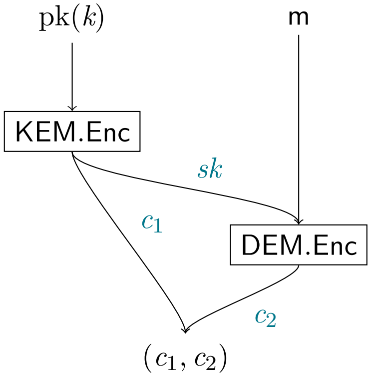
\+ public key can be published

– typically computationally expensive

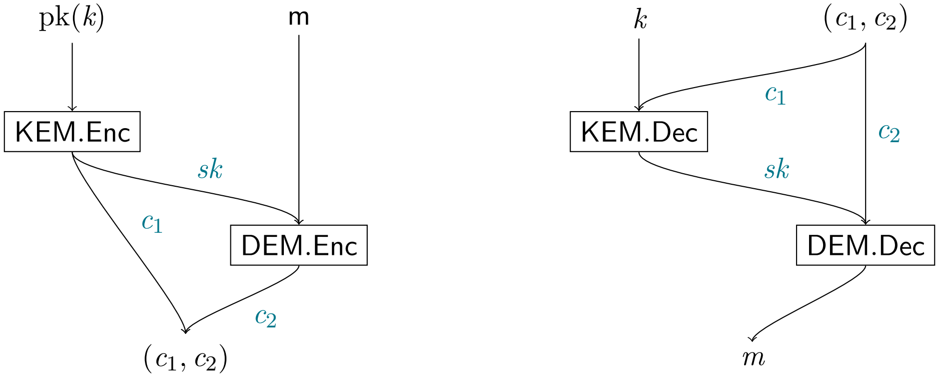
Hybrid Encryption PKE

- Generate a *single-use key* and encrypt it *asymmetrically* KEM
- Encrypt data *symmetrically* with said key DEM

KEM/DEM Construction [3]



KEM/DEM Construction [3]



PKE Security

What makes an encryption scheme secure?

- No attacker can guess what the encrypted message is? *Indistinguishability-*

PKE Security

What makes an encryption scheme secure?

- No attacker can guess what the encrypted message is? *Indistinguishability-*
- No attacker can modify the ciphertext in any meaningful way? *Nonmalleability-*

PKE Security

What makes an encryption scheme secure?

- No attacker can guess what the encrypted message is? *Indistinguishability-*
- No attacker can modify the ciphertext in any meaningful way? *Nonmalleability-*

    - if the attacker can encrypt its own messages? *-CPA*

PKE Security

What makes an encryption scheme secure?

- No attacker can guess what the encrypted message is? *Indistinguishability-*
- No attacker can modify the ciphertext in any meaningful way? *Nonmalleability-*

  - if the attacker can encrypt its own messages? *-CPA*
  - if the attacker could obtain decryptions for other ciphertexts before? *-CCA1*

PKE Security

What makes an encryption scheme secure?

- No attacker can guess what the encrypted message is? *Indistinguishability-*
- No attacker can modify the ciphertext in any meaningful way? *Nonmalleability-*

  - if the attacker can encrypt its own messages? *-CPA*
  - if the attacker could obtain decryptions for other ciphertexts before? *-CCA1*
    - even other ciphertexts derived from the one in question? *-CCA2*

PKE Indistinguishability Game [3]

$\mathbf{Exp}^{pke-ind-atk-b}_{\mathsf{PKE},\mathcal{A}}(\eta)$

$\mathcal{C}$ $\mathcal{A}$

PKE Indistinguishability Game [3]

$$\mathbf{Exp}^{pke-ind-atk-b}_{\mathsf{PKE},\mathcal{A}}(\eta)$$

$(pk, k) \leftarrow\$ \mathsf{PKE.Kg}(1^\eta)$

$\mathcal{C}$	$\mathcal{A}$
$(pk, k) \leftarrow\$ \mathsf{PKE.Kg}(1^\eta)$	

PKE Indistinguishability Game [3]

$$\mathbf{Exp}^{pke-ind-atk-b}_{\mathsf{PKE},\mathcal{A}}(\eta)$$

$(pk, k) \leftarrow\$ \mathsf{PKE.Kg}(1^\eta)$

$(St, m_0, m_1) \leftarrow\$ \mathcal{A}_1^{\mathtt{DEC}_1(\cdot)}(pk)$

$\mathcal{C}$		$\mathcal{A}$
$(pk, k) \leftarrow\$ \mathsf{PKE.Kg}(1^\eta)$		
	$\xrightarrow{pk}$	$\mathcal{A}_1$

PKE Indistinguishability Game [3]

$$\mathbf{Exp}^{pke-ind-atk-b}_{\mathsf{PKE},\mathcal{A}}(\eta)$$

$(pk, k) \leftarrow\$ \mathsf{PKE.Kg}(1^\eta)$

$(St, m_0, m_1) \leftarrow\$ \mathcal{A}_1^{\mathtt{DEC}_1(\cdot)}(pk)$

$\mathcal{C}$		$\mathcal{A}$
$(pk, k) \leftarrow\$ \mathsf{PKE.Kg}(1^\eta)$		
	pk $\longrightarrow$	$\mathcal{A}_1$
	c $\longleftarrow$	

PKE Indistinguishability Game [3]

$\mathbf{Exp}^{pke-ind-atk-b}_{\mathsf{PKE},\mathcal{A}}(\eta)$

$(pk, k) \leftarrow\$ \mathsf{PKE.Kg}(1^\eta)$

$(St, m_0, m_1) \leftarrow\$ \mathcal{A}_1^{\mathtt{DEC}_1(\cdot)}(pk)$

$\mathcal{C}$		$\mathcal{A}$
$(pk, k) \leftarrow\$ \mathsf{PKE.Kg}(1^\eta)$		
	pk $\longrightarrow$	$\mathcal{A}_1$
	c $\longleftarrow$	
	$\mathsf{PKE.Dec}(k, c)$ $\longrightarrow$	

PKE Indistinguishability Game [3]

$\mathbf{Exp}^{pke-ind-atk-b}_{\mathsf{PKE},\mathcal{A}}(\eta)$

$(pk, k) \leftarrow\$ \mathsf{PKE.Kg}(1^\eta)$

$(St, m_0, m_1) \leftarrow\$ \mathcal{A}_1^{\mathtt{DEC}_1(\cdot)}(pk)$

$\mathcal{C}$		$\mathcal{A}$
$(pk, k) \leftarrow\$ \mathsf{PKE.Kg}(1^\eta)$		
	pk $\longrightarrow$	$\mathcal{A}_1$
	m_0, m_1 $\longleftarrow$	

PKE Indistinguishability Game [3]

$$\mathbf{Exp}^{pke-ind-atk-b}_{\mathsf{PKE},\mathcal{A}}(\eta)$$

$(pk, k) \leftarrow\$ \mathsf{PKE.Kg}(1^\eta)$

$(St, m_0, m_1) \leftarrow\$ \mathcal{A}_1^{\mathtt{DEC}_1(\cdot)}(pk)$

$C^* \leftarrow\$ \mathsf{PKE.Enc}(pk, m_b)$

$\mathcal{C}$		$\mathcal{A}$
$(pk, k) \leftarrow\$ \mathsf{PKE.Kg}(1^\eta)$		
	pk $\longrightarrow$	$\mathcal{A}_1$
	$\longleftarrow$ m_0, m_1	
$C^* \leftarrow\$ \mathsf{PKE.Enc}(pk, m_b)$		

PKE Indistinguishability Game [3]

$\mathbf{Exp}^{pke-ind-atk-b}_{\mathsf{PKE},\mathcal{A}}(\eta)$

$(pk, k) \leftarrow\!\!\$\ \mathsf{PKE.Kg}(1^\eta)$

$(St, m_0, m_1) \leftarrow\!\!\$\ \mathcal{A}_1^{\mathtt{DEC}_1(\cdot)}(pk)$

$C^* \leftarrow\!\!\$\ \mathsf{PKE.Enc}(pk, m_b)$

$b' \leftarrow\!\!\$\ \mathcal{A}_2^{\mathtt{DEC}_2(\cdot)}(C^*, St)$

$\mathcal{C}$		$\mathcal{A}$
$(pk, k) \leftarrow\!\!\$\ \mathsf{PKE.Kg}(1^\eta)$		
	pk $\longrightarrow$	$\mathcal{A}_1$
	m_0, m_1 $\longleftarrow$	
$C^* \leftarrow\!\!\$\ \mathsf{PKE.Enc}(pk, m_b)$		
	C^* $\longrightarrow$	$\mathcal{A}_2$

école normale supérieure paris-saclay

PKE Indistinguishability Game [3]

$\mathbf{Exp}^{pke-ind-atk-b}_{\mathsf{PKE},\mathcal{A}}(\eta)$

$(pk, k) \leftarrow\$ \mathsf{PKE.Kg}(1^\eta)$

$(St, m_0, m_1) \leftarrow\$ \mathcal{A}_1^{\mathtt{DEC}_1(\cdot)}(pk)$

$C^* \leftarrow\$ \mathsf{PKE.Enc}(pk, m_b)$

$b' \leftarrow\$ \mathcal{A}_2^{\mathtt{DEC}_2(\cdot)}(C^*, St)$

return b'

$\mathcal{C}$		$\mathcal{A}$
$(pk, k) \leftarrow\$ \mathsf{PKE.Kg}(1^\eta)$		
	pk $\longrightarrow$	$\mathcal{A}_1$
	m_0, m_1 $\longleftarrow$	
$C^* \leftarrow\$ \mathsf{PKE.Enc}(pk, m_b)$		
	C^* $\longrightarrow$	$\mathcal{A}_2$
	b' $\longleftarrow$	

PKE Indistinguishability Game [3]

$\mathbf{Exp}^{pke-ind-atk-b}_{\mathsf{PKE},\mathcal{A}}(\eta)$

$(pk, k) \leftarrow\$ \ \mathsf{PKE.Kg}(1^\eta)$

$(St, m_0, m_1) \leftarrow\$ \ \mathcal{A}_1^{\mathtt{DEC}_1(\cdot)}(pk)$

$C^* \leftarrow\$ \ \mathsf{PKE.Enc}(pk, m_b)$

$b' \leftarrow\$ \ \mathcal{A}_2^{\mathtt{DEC}_2(\cdot)}(C^*, St)$

return b'

atk	$\mathtt{DEC}_1$	$\mathtt{DEC}_2$
CPA	/	/
CCA1	$\mathsf{PKE.Dec}(k, \cdot)$	/
CCA2	$\mathsf{PKE.Dec}(k, \cdot)$	$x \mapsto \mathsf{PKE.Dec}(k, x)$ if $x \neq C^*$

Hybrid Encryption Security

Herranz, Hofheinz, and Kiltz [3]

Composition results:

Hybrid Encryption Security

Herranz, Hofheinz, and Kiltz [3]

Composition results:

- Implications between notions of security

Hybrid Encryption Security

Herranz, Hofheinz, and Kiltz [3]

Composition results:

- Implications between notions of security
- Security of hybrid PKE based on security of KEM and DEM

CCSA

- Cryptographic proofs are typically done by reduction

CCSA

- Cryptographic proofs are typically done by reduction
  - hard to automate or machine-check

CCSA

- Cryptographic proofs are typically done by reduction
  - hard to automate or machine-check
- CCSA: Logic for cryptographic reasoning [1]

école normale supérieure paris–saclay

CCSA

- Cryptographic proofs are typically done by reduction
  - hard to automate or machine-check
- CCSA: Logic for cryptographic reasoning [1]
  - first-order logic with cryptographic predicates

CCSA

- Cryptographic proofs are typically done by reduction
  - hard to automate or machine-check
- CCSA: Logic for cryptographic reasoning [1]
  - first-order logic with cryptographic predicates
  - terms given in simply-typed lambda calculus

CCSA

- Cryptographic proofs are typically done by reduction
  - hard to automate or machine-check
- CCSA: Logic for cryptographic reasoning [1]
  - first-order logic with cryptographic predicates
  - terms given in simply-typed lambda calculus
  - *names* allow random samplings respecting a specified distribution

CCSA

- Cryptographic proofs are typically done by reduction
  - hard to automate or machine-check
- CCSA: Logic for cryptographic reasoning [1]
  - first-order logic with cryptographic predicates
  - terms given in simply-typed lambda calculus
  - *names* allow random samplings respecting a specified distribution
  - successfully used for the analysis of several protocols (e.g.[4])

école normale supérieure paris–saclay

CCSA

- Cryptographic proofs are typically done by reduction
  - hard to automate or machine-check

- CCSA: Logic for cryptographic reasoning [1]
  - first-order logic with cryptographic predicates
  - terms given in simply-typed lambda calculus
  - *names* allow random samplings respecting a specified distribution
  - successfully used for the analysis of several protocols (e.g.[4])
  - implemented in the proof assistant SQUIRREL[2]

CCSA Predicates

Def. Indistinguishability

$t_1 \sim t_2$: no efficient attacker can determine whether it was given a result of t_1 or t_2.

CCSA Predicates

Def. Indistinguishability

$t_1 \sim t_2$: no efficient attacker can determine whether it was given a result of t_1 or t_2.

Transitivity

$$\frac{\mathcal{E}; \Theta \vdash \vec{u} \sim \vec{v} \qquad \mathcal{E}; \Theta \vdash \vec{v} \sim \vec{w}}{\mathcal{E}; \Theta \vdash \vec{u} \sim \vec{w}}$$

CCSA Predicates

Def. Indistinguishability

$t_1 \sim t_2$: no efficient attacker can determine whether it was given a result of t_1 or t_2.

Transitivity

$$\frac{\mathcal{E}; \Theta \vdash \vec{u} \sim \vec{v} \qquad \mathcal{E}; \Theta \vdash \vec{v} \sim \vec{w}}{\mathcal{E}; \Theta \vdash \vec{u} \sim \vec{w}}$$

Def. Overwhelming Truth

$[\phi]$: ϕ almost always evaluates to `true`.

CCSA Predicates

Def. Indistinguishability

$t_1 \sim t_2$: no efficient attacker can determine whether it was given a result of t_1 or t_2.

$$\textsc{Transitivity}\quad \frac{\mathcal{E};\Theta \vdash \vec{u} \sim \vec{v} \qquad \mathcal{E};\Theta \vdash \vec{v} \sim \vec{w}}{\mathcal{E};\Theta \vdash \vec{u} \sim \vec{w}}$$

Def. Overwhelming Truth

$[\phi]$: ϕ almost always evaluates to `true`.

$$\textsc{Rewrite}\quad \frac{\mathcal{E};\Theta \vdash F[s] \qquad \mathcal{E};\Theta \vdash [s = t]}{\mathcal{E};\Theta \vdash F[t]}$$

$$\beta\quad \frac{}{\mathcal{E};\Theta \vdash [(\lambda(x:\tau).t)\ t_0 = t\{x \mapsto t_0\}]}$$

Why Analyze KEM/DEM in CCSA?

- CCSA so far only used for analysis of protocols

Why Analyze KEM/DEM in CCSA?

- CCSA so far only used for analysis of protocols
  - Security of primitives assumed; to be proved externally

Why Analyze KEM/DEM in CCSA?

- CCSA so far only used for analysis of protocols
  - Security of primitives assumed; to be proved externally

    $\Rightarrow$ Trust in external proof

Why Analyze KEM/DEM in CCSA?

- CCSA so far only used for analysis of protocols
  - Security of primitives assumed; to be proved externally

    $\Rightarrow$ Trust in external proof

    $\Rightarrow$ Trust in *translation* between formalizations

Why Analyze KEM/DEM in CCSA?

- CCSA so far only used for analysis of protocols
  - Security of primitives assumed; to be proved externally

    $\Rightarrow$ Trust in external proof

    $\Rightarrow$ Trust in *translation* between formalizations

$\Rightarrow$ Proving primitives in the same logic provides *better formal guarantees*

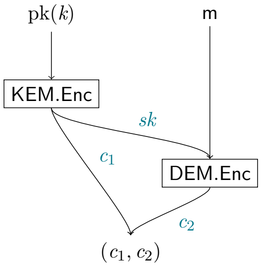
KEM/DEM Construction in CCSA

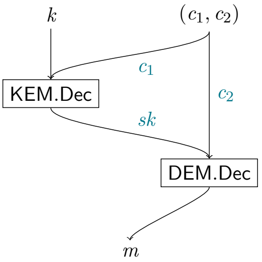
- key generation: names $\mathbf{k}_i$ and $\mathbf{sk}_j$ sample the key space

KEM/DEM Construction in CCSA

- key generation: names $\mathbf{k}_i$ and $\mathbf{sk}_j$ sample the key space
- $\mathrm{pk}(\mathbf{k}_i)$ derives the public key corresponding to $\mathbf{k}_i$

KEM/DEM Construction in CCSA





$\mathrm{PKE.Enc}(\mathrm{pk}(\mathbf{k}_i), m)$

let $(sk, c_1) = \mathrm{KEM.Enc}(\mathrm{pk}(\mathbf{k}_i))$
in $(c_1, \mathrm{DEM.Enc}(sk, m))$

$\mathrm{PKE.Dec}(\mathbf{k}_i, (c_1, c_2))$

let $sk = \mathrm{KEM.Dec}(\mathbf{k}_i, c_1)$
in $\mathrm{DEM.Dec}(sk, c_2)$

PKE Indistinguishability in CCSA

$\mathbf{Exp}^{pke-ind-atk-b}_{\mathsf{PKE},\mathcal{A}}(\eta)$

$(pk, k) \leftarrow\$ \mathsf{PKE.Kg}(1^\eta)$

$(St, m_0, m_1) \leftarrow\$ \mathcal{A}_1^{\mathtt{DEC}_1(\cdot)}(pk)$

$C^* \leftarrow\$ \mathsf{PKE.Enc}(pk, m_b)$

$b' \leftarrow\$ \mathcal{A}_2^{\mathtt{DEC}_2(\cdot)}(C^*, St)$

return b'

PKE-IND-CCA1

$$\mathcal{E}, \Theta \vdash \mathrm{PKE.Enc}(\mathrm{pk}(\mathbf{k}_{t_k}), m_0) \sim \mathrm{PKE.Enc}(\mathrm{pk}(\mathbf{k}_{t_k}), m_1)$$

PKE Indistinguishability in CCSA

$$\mathbf{Exp}^{pke-ind-atk-b}_{\mathsf{PKE},\mathcal{A}}(\eta)$$

$(pk, k) \leftarrow\$ \mathsf{PKE.Kg}(1^\eta)$

$(St, m_0, m_1) \leftarrow\$ \mathcal{A}_1^{\mathtt{DEC}_1(\cdot)}(pk)$

$C^* \leftarrow\$ \mathsf{PKE.Enc}(pk, m_b)$

$b' \leftarrow\$ \mathcal{A}_2^{\mathtt{DEC}_2(\cdot)}(C^*, St)$

return b'

PKE-IND-CCA1

$$\frac{\mathcal{E}, \Theta; \emptyset \vdash_{\mathsf{pptm}} m_0, m_1}{\mathcal{E}, \Theta \vdash \mathrm{PKE.Enc}(\mathrm{pk}(\mathbf{k}_{t_k}), m_0) \sim \mathrm{PKE.Enc}(\mathrm{pk}(\mathbf{k}_{t_k}), m_1)}$$

PKE Indistinguishability in CCSA

$$\mathbf{Exp}^{pke-ind-atk-b}_{\mathsf{PKE},\mathcal{A}}(\eta)$$

$(pk, k) \leftarrow\$ \mathsf{PKE.Kg}(1^\eta)$

$(St, m_0, m_1) \leftarrow\$ \mathcal{A}_1^{\mathtt{DEC}_1(\cdot)}(pk)$

$C^* \leftarrow\$ \mathsf{PKE.Enc}(pk, m_b)$

$b' \leftarrow\$ \mathcal{A}_2^{\mathtt{DEC}_2(\cdot)}(C^*, St)$

return b'

PKE-IND-CCA1

$$\mathcal{E}, \Theta; \emptyset \vdash_{\mathsf{pptm}} m_0, m_1, \vec{a}$$

$$\mathcal{E}, \Theta \vdash [\phi^{\text{guarded } \mathbf{k}, t_k}_{\text{pk}(\mathbf{k}_{t_k}), \text{PKE.Dec}(\mathbf{k}_{t_k}, \cdot)}(\vec{a}, m_0, m_1)]$$

$$\mathcal{E}, \Theta \vdash \vec{a}\ \text{PKE.Enc}(\text{pk}(\mathbf{k}_{t_k}), m_0) \sim \vec{a}\ \text{PKE.Enc}(\text{pk}(\mathbf{k}_{t_k}), m_1)$$

PKE Indistinguishability in CCSA

$\mathbf{Exp}^{pke-ind-atk-b}_{\mathsf{PKE},\mathcal{A}}(\eta)$
$(pk, k) \leftarrow\$ \mathsf{PKE.Kg}(1^\eta)$
$(St, m_0, m_1) \leftarrow\$ \mathcal{A}_1^{\mathtt{DEC}_1(\cdot)}(pk)$
$C^* \leftarrow\$ \mathsf{PKE.Enc}(pk, m_b)$
$b' \leftarrow\$ \mathcal{A}_2^{\mathtt{DEC}_2(\cdot)}(C^*, St)$
return b'

PKE-IND-CCA1

$$\dfrac{\mathcal{E}, \Theta; \emptyset \vdash_{\mathsf{pptm}} m_0, m_1, \vec{a}, C \qquad \mathcal{E}, \Theta \vdash [\phi^{\text{guarded } \mathbf{k}, t_k}_{\text{pk}(\mathbf{k}_{t_k}), \text{PKE.Dec}(\mathbf{k}_{t_k}, \cdot)}(\vec{a}, m_0, m_1)] \qquad \mathcal{E}, \Theta \vdash [\phi^{\text{guarded } \mathbf{k}, t_k}_{\text{pk}(\mathbf{k}_{t_k})}(C)]}{\mathcal{E}, \Theta \vdash \boxed{(\lambda\ \vec{v}\ c.C)\ \vec{a}\ \text{PKE.Enc}(\text{pk}(\mathbf{k}_{t_k}), m_0)} \sim \boxed{(\lambda\ \vec{v}\ c.C)\ \vec{a}\ \text{PKE.Enc}(\text{pk}(\mathbf{k}_{t_k}), m_1)}}$$

PKE Indistinguishability in CCSA

$$\mathbf{Exp}^{pke-ind-atk-b}_{\mathsf{PKE},\mathcal{A}}(\eta)$$

$(pk, k) \leftarrow\$ \mathsf{PKE.Kg}(1^\eta)$

$(St, m_0, m_1) \leftarrow\$ \mathcal{A}_1^{\mathtt{DEC}_1(\cdot)}(pk)$

$C^* \leftarrow\$ \mathsf{PKE.Enc}(pk, m_b)$

$b' \leftarrow\$ \mathcal{A}_2^{\mathtt{DEC}_2(\cdot)}(C^*, St)$

return b'

PKE-IND-CPA

$$\mathcal{E}, \Theta; \emptyset \vdash_{\mathsf{pptm}} m_0, m_1, \vec{a}, C$$

$$\mathcal{E}, \Theta \vdash [\phi^{\text{guarded } \mathbf{k}, t_k}_{\text{pk}(\mathbf{k}_{t_k})}(\vec{a}, m_0, m_1)]$$

$$\mathcal{E}, \Theta \vdash [\phi^{\text{guarded } \mathbf{k}, t_k}_{\text{pk}(\mathbf{k}_{t_k})}(C)]$$

$$\mathcal{E}, \Theta \vdash \boxed{(\lambda\ \vec{v}\ c.C)\ \vec{a}\ \text{PKE.Enc}(\text{pk}(\mathbf{k}_{t_k}), m_0)}$$

$$\sim \boxed{(\lambda\ \vec{v}\ c.C)\ \vec{a}\ \text{PKE.Enc}(\text{pk}(\mathbf{k}_{t_k}), m_1)}$$

PKE Indistinguishability in CCSA

$\mathbf{Exp}^{pke-ind-atk-b}_{\mathsf{PKE},\mathcal{A}}(\eta)$

$(pk, k) \leftarrow\$ \mathsf{PKE.Kg}(1^\eta)$

$(St, m_0, m_1) \leftarrow\$ \mathcal{A}_1^{\mathtt{DEC}_1(\cdot)}(pk)$

$C^* \leftarrow\$ \mathsf{PKE.Enc}(pk, m_b)$

$b' \leftarrow\$ \mathcal{A}_2^{\mathtt{DEC}_2(\cdot)}(C^*, St)$

return b'

PKE-IND-CCA2

$$\frac{\begin{array}{c}\mathcal{E}, \Theta; \emptyset \vdash_{\mathsf{pptm}} m_0, m_1, \vec{a}, C \\ \mathcal{E}, \Theta \vdash [\phi^{\text{guarded } \mathbf{k}, t_k}_{\text{pk}(\mathbf{k}_{t_k}), \text{PKE.Dec}(\mathbf{k}_{t_k}, \cdot)}(\vec{a}, m_0, m_1)] \\ \mathcal{E}, \Theta \vdash [\phi^{\text{guarded } \mathbf{k}, t_k}_{\text{pk}(\mathbf{k}_{t_k}), \mathsf{if}\ t = c\ \mathsf{then}\ \perp\ \mathsf{else}\ \text{PKE.Dec}(\mathbf{k}_{t_k}, t)}(C)]\end{array}}{\begin{array}{c}\mathcal{E}, \Theta \vdash (\lambda\ \vec{v}\ c. C)\ \vec{a}\ \text{PKE.Enc}(\text{pk}(\mathbf{k}_{t_k}), m_0) \\ \sim (\lambda\ \vec{v}\ c. C)\ \vec{a}\ \text{PKE.Enc}(\text{pk}(\mathbf{k}_{t_k}), m_1)\end{array}}$$

Guarded Occurrences

$\phi^{\text{guarded } \mathbf{k}, t_k}_{\text{pk}(\mathbf{k}_{t_k}), \text{PKE.Dec}(\mathbf{k}_{t_k}, \cdot)}(\vec{u})$

- consider all subterms $\mathbf{k}_{t_0}$ of $\vec{u}$, and the *path conditions* ψ to reach them

école normale supérieure paris-saclay

Guarded Occurrences

$\phi^{\text{guarded } \mathbf{k}, t_k}_{\text{pk}(\mathbf{k}_{t_k}), \text{PKE.Dec}(\mathbf{k}_{t_k}, \cdot)}(\vec{u})$

- consider all subterms $\mathbf{k}_{t_0}$ of $\vec{u}$, and the *path conditions* ψ to reach them
  - if it occurs as part of $\text{pk}(\mathbf{k}_{t_k})$ or $\text{PKE.Dec}(\mathbf{k}_{t_k}, \cdot)$, ignore it

école normale supérieure paris–saclay

Guarded Occurrences

$\phi^{\text{guarded } \mathbf{k}, t_k}_{\text{pk}(\mathbf{k}_{t_k}), \text{PKE.Dec}(\mathbf{k}_{t_k}, \cdot)}(\vec{u})$

- consider all subterms $\mathbf{k}_{t_0}$ of $\vec{u}$, and the *path conditions* ψ to reach them
  - if it occurs as part of $\text{pk}(\mathbf{k}_{t_k})$ or $\text{PKE.Dec}(\mathbf{k}_{t_k}, \cdot)$, ignore it
  - otherwise, make sure that $\psi \implies t_0 \neq t_k$

école normale supérieure paris–saclay

Guarded Occurrences

$\phi^{\text{guarded } \mathbf{k}, t_k}_{\text{pk}(\mathbf{k}_{t_k}), \text{PKE.Dec}(\mathbf{k}_{t_k}, \cdot)}(\vec{u})$

- consider all subterms $\mathbf{k}_{t_0}$ of $\vec{u}$, and the *path conditions* ψ to reach them
  - if it occurs as part of $\text{pk}(\mathbf{k}_{t_k})$ or $\text{PKE.Dec}(\mathbf{k}_{t_k}, \cdot)$, ignore it
  - otherwise, make sure that $\psi \implies t_0 \neq t_k$

A syntactic check is *not* sufficient:

Guarded Occurrences

$\phi^{\text{guarded } \mathbf{k}, t_k}_{\mathrm{pk}(\mathbf{k}_{t_k}), \mathrm{PKE.Dec}(\mathbf{k}_{t_k}, \cdot)}(\vec{u})$

- consider all subterms $\mathbf{k}_{t_0}$ of $\vec{u}$, and the *path conditions* ψ to reach them
  - if it occurs as part of $\mathrm{pk}(\mathbf{k}_{t_k})$ or $\mathrm{PKE.Dec}(\mathbf{k}_{t_k}, \cdot)$, ignore it
  - otherwise, make sure that $\psi \implies t_0 \neq t_k$

A syntactic check is *not* sufficient:

- $\mathbf{k}_{t_k}$ vs $\mathbf{k}_{t_k+1-1}$

Guarded Occurrences

$\phi^{\text{guarded } \mathbf{k},t_k}_{\text{pk}(\mathbf{k}_{t_k}),\text{PKE.Dec}(\mathbf{k}_{t_k},\cdot)}(\vec{u})$

- consider all subterms $\mathbf{k}_{t_0}$ of $\vec{u}$, and the *path conditions* ψ to reach them
  - if it occurs as part of $\text{pk}(\mathbf{k}_{t_k})$ or $\text{PKE.Dec}(\mathbf{k}_{t_k}, \cdot)$, ignore it
  - otherwise, make sure that $\psi \implies t_0 \neq t_k$

A syntactic check is *not* sufficient:

- $\mathbf{k}_{t_k}$ vs $\mathbf{k}_{t_k+1-1}$
- indices could be function arguments, results of if $\cdot$ then $\cdot$ else $\cdot$ expressions, etc

DEM Indistinguishability [3]

PKE Indistinguishability

$$\mathbf{Exp}^{pke-ind-atk-b}_{\mathsf{PKE},\mathcal{A}}(\eta)$$

$$(pk, k) \leftarrow\$ \ \mathsf{PKE.Kg}(1^\eta)$$
$$(St, m_0, m_1) \leftarrow\$ \ \mathcal{A}_1^{\mathtt{DEC}_1(\cdot)}(pk)$$
$$C^* \leftarrow\$ \ \mathsf{PKE.Enc}(pk, m_b)$$
$$b' \leftarrow\$ \ \mathcal{A}_2^{\mathtt{DEC}_2(\cdot)}(C^*, St)$$
$$\textbf{return } b'$$

DEM Indistinguishability

$$\mathbf{Exp}^{dem-ind-atk-b}_{\mathsf{DEM},\mathcal{A}}(\eta)$$

$$K \leftarrow\$ \ \mathsf{DEM.Kg}(1^\eta)$$
$$(St, m_0, m_1) \leftarrow\$ \ \mathcal{A}_1^{\mathtt{ENC}_1(\cdot),\mathtt{DEC}_1(\cdot)}(1^\eta)$$
$$C^* \leftarrow\$ \ \mathsf{DEM.Enc}(K, m_b)$$
$$b' \leftarrow\$ \ \mathcal{A}_2^{\mathtt{ENC}_2(\cdot),\mathtt{DEC}_2(\cdot)}(C^*, St)$$
$$\textbf{return } b'$$

DEM Indistinguishability [3]

PKE Indistinguishability

$\mathbf{Exp}^{pke-ind-atk-b}_{\mathsf{PKE},\mathcal{A}}(\eta)$

$(pk, k) \leftarrow\$ \mathsf{PKE.Kg}(1^\eta)$

$(St, m_0, m_1) \leftarrow\$ \mathcal{A}_1^{\mathtt{DEC}_1(\cdot)}(pk)$

$C^* \leftarrow\$ \mathsf{PKE.Enc}(pk, m_b)$

$b' \leftarrow\$ \mathcal{A}_2^{\mathtt{DEC}_2(\cdot)}(C^*, St)$

return b'

DEM Indistinguishability

$\mathbf{Exp}^{dem-ind-atk-b}_{\mathsf{DEM},\mathcal{A}}(\eta)$

$K \leftarrow\$ \mathsf{DEM.Kg}(1^\eta)$

$(St, m_0, m_1) \leftarrow\$ \mathcal{A}_1^{\mathtt{ENC}_1(\cdot),\mathtt{DEC}_1(\cdot)}(1^\eta)$

$C^* \leftarrow\$ \mathsf{DEM.Enc}(K, m_b)$

$b' \leftarrow\$ \mathcal{A}_2^{\mathtt{ENC}_2(\cdot),\mathtt{DEC}_2(\cdot)}(C^*, St)$

return b'

DEM Indistinguishability in CCSA

DEM-IND-CCA1

$$\frac{\mathcal{E}, \Theta; \emptyset \vdash_{\mathsf{pptm}} C, \vec{a}, m_0, m_1 \qquad \mathcal{E}, \Theta \vdash [\phi^{\text{guarded } \mathbf{sk}, t_k}_{\text{DEM.Enc}(\mathbf{sk}_{t_k}, \cdot, \cdot)}(C)] \qquad \mathcal{E}, \Theta \vdash [\phi^{\text{guarded } \mathbf{sk}, t_k}_{\text{DEM.Enc}(\mathbf{sk}_{t_k}, \cdot, \cdot), \text{DEM.Dec}(\mathbf{sk}_{t_k}, \cdot)}(\vec{a}, m)]}{\mathcal{E}, \Theta \vdash (\lambda\ \vec{v}\ c.C)\ \vec{a}\ \text{DEM.Enc}(\mathbf{sk}_{t_k}, m_0) \sim (\lambda\ \vec{v}\ c.C)\ \vec{a}\ \text{DEM.Enc}(\mathbf{sk}_{t_k}, m_1)}$$

DEM Indistinguishability in CCSA

DEM-IND-CCA1

$$\frac{\mathcal{E}, \Theta; \emptyset \vdash_{\mathsf{pptm}} C, \vec{a}, m_0, m_1 \qquad \mathcal{E}, \Theta \vdash [\phi^{\text{guarded } \mathbf{sk}, t_k}_{\text{DEM.Enc}(\mathbf{sk}_{t_k}, \cdot, \cdot)}(C)] \qquad \mathcal{E}, \Theta \vdash [\phi^{\text{guarded } \mathbf{sk}, t_k}_{\text{DEM.Enc}(\mathbf{sk}_{t_k}, \cdot, \cdot), \text{DEM.Dec}(\mathbf{sk}_{t_k}, \cdot)}(\vec{a}, m)]}{\mathcal{E}, \Theta \vdash \ (\lambda\ \vec{v}\ c. C)\ \vec{a}\ \text{DEM.Enc}(\mathbf{sk}_{t_k}, m_0) \ \sim \ (\lambda\ \vec{v}\ c. C)\ \vec{a}\ \text{DEM.Enc}(\mathbf{sk}_{t_k}, m_1)}$$

KEM Indistinguishability [3]

PKE Indistinguishability

$\mathbf{Exp}^{pke-ind-atk-b}_{\mathsf{PKE},\mathcal{A}}(\eta)$

$(pk, k) \leftarrow\$ \mathsf{PKE.Kg}(1^\eta)$

$(St, m_0, m_1) \leftarrow\$ \mathcal{A}_1^{\mathtt{DEC}_1(\cdot)}(pk)$

$C^* \leftarrow\$ \mathsf{PKE.Enc}(pk, m_b)$

$b' \leftarrow\$ \mathcal{A}_2^{\mathtt{DEC}_2(\cdot)}(C^*, St)$

return b'

KEM Indistinguishability

$\mathbf{Exp}^{kem-ind-atk-b}_{\mathsf{KEM},\mathcal{A}}(\eta)$

$(pk, k) \leftarrow\$ \mathsf{KEM.Kg}(1^\eta)$

$St \leftarrow\$ \mathcal{A}_1^{\mathtt{DEC}_1(\cdot)}(pk)$

$K_0^* \leftarrow\$ \mathsf{KeySp}(\eta)$

$(K_1^*, C^*) \leftarrow\$ \mathsf{KEM.Enc}(pk)$

$b' \leftarrow\$ \mathcal{A}_2^{\mathtt{DEC}_2(\cdot)}(C^*, St, K_b^*)$

return b'

KEM Indistinguishability in CCSA

KEM-IND-CCA1

$$\frac{\mathcal{E},\Theta;\emptyset \vdash_{\mathsf{pptm}} C,\vec{a} \qquad \mathcal{E},\Theta \vdash [\phi^{\mathbf{sk}^*,()}_{\text{fresh}}(C,\vec{a})] \qquad \mathcal{E},\Theta \vdash [\phi^{\text{guarded }\mathbf{k},t_k}_{\text{pk}(\mathbf{k}_{t_k})}(C)] \qquad \mathcal{E},\Theta \vdash [\phi^{\text{guarded }\mathbf{k},t_k}_{\text{pk}(\mathbf{k}_{t_k}),\text{KEM.Dec}(\mathbf{k}_{t_k},\cdot)}(\vec{a})]}{\mathcal{E},\Theta \vdash \begin{array}{c}(\lambda\ \vec{v}\ (sk,c).C)\ \vec{a}\\ \text{KEM.Enc}(\text{pk}(k\ t_k))\end{array} \sim \begin{array}{c}(\lambda\ \vec{v}\ (sk,c).C)\ \vec{a}\\ (\mathbf{sk}^*{}_{()},\pi_2\ \text{KEM.Enc}(\text{pk}(\mathbf{k}_{t_k})))\end{array}}$$

KEM/DEM Composition Results

Herranz, Hofheinz, and Kiltz [3]

$$\text{KEM-IND-CPA} + \text{DEM-IND-CPA} \implies \text{PKE-IND-CPA}$$
$$\text{KEM-IND-CCA1} + \text{DEM-IND-CCA1} \implies \text{PKE-IND-CCA1}$$
$$\text{KEM-IND-CCA2} + \text{DEM-IND-CCA2} \implies \text{PKE-IND-CCA2}$$

KEM/DEM Composition Results

Herranz, Hofheinz, and Kiltz [3]

$$\text{KEM-IND-CPA} + \text{DEM-IND-CPA} \implies \text{PKE-IND-CPA}$$
$$\text{KEM-IND-CCA1} + \text{DEM-IND-CCA1} \implies \text{PKE-IND-CCA1}$$
$$\text{KEM-IND-CCA2} + \text{DEM-IND-CCA2} \implies \text{PKE-IND-CCA2}$$

$$(\lambda\ \vec{v}\ c.C)\ \vec{a}\ \mathrm{PKE.Enc}(\mathrm{pk}(\mathbf{k}_{t_k}), m_0) \quad \sim \quad (\lambda\ \vec{v}\ c.C)\ \vec{a}\ \mathrm{PKE.Enc}(\mathrm{pk}(\mathbf{k}_{t_k}), m_1)$$

KEM/DEM Composition Results

$$\begin{array}{c}(\lambda\ \vec{v}\ c\ \mathsf{dec}.\,C)\ \vec{a} \\ \mathsf{let}\ (sk, c_1) = \mathrm{KEM.Enc}(\mathrm{pk}(\mathbf{k}_{t_k})) \\ \mathsf{in}\ (c_1, \mathrm{DEM.Enc}(sk, m_0))\end{array} \sim \begin{array}{c}(\lambda\ \vec{v}\ c\ \mathsf{dec}.\,C)\ \vec{a} \\ \mathsf{let}\ (sk, c_1) = \mathrm{KEM.Enc}(\mathrm{pk}(\mathbf{k}_{t_k})) \\ \mathsf{in}\ (c_1, \mathrm{DEM.Enc}(sk, m_1))\end{array}$$

KEM/DEM Composition Results

$$
\begin{array}{c}
(\lambda\ \vec{v}\ c\ \text{dec}.\,C)\ \vec{a} \\
\text{let } (sk, c_1) = \mathrm{KEM.Enc}(\mathrm{pk}(\mathbf{k}_{t_k})) \\
\text{in } (c_1, \mathrm{DEM.Enc}(sk, m_0))
\end{array}
\sim
\begin{array}{c}
(\lambda\ \vec{v}\ c\ \text{dec}.\,C)\ \vec{a} \\
\text{let } (sk, c_1) = \mathrm{KEM.Enc}(\mathrm{pk}(\mathbf{k}_{t_k})) \\
\text{in } (c_1, \mathrm{DEM.Enc}(sk, m_1))
\end{array}
$$

- DEM axioms not immediately applicable

école normale supérieure paris-saclay

KEM/DEM Composition Results

$$\begin{array}{c} (\lambda\ \vec{v}\ c\ \textsf{dec}.\,C)\ \vec{a} \\ \textsf{let}\ (\_, c_1) = \mathrm{KEM.Enc}(\mathrm{pk}(\mathbf{k}_{t_k})) \\ \textsf{in}\ (c_1, \mathrm{DEM.Enc}(\mathbf{sk}^*_{()}, m_0)) \end{array} \sim \begin{array}{c} (\lambda\ \vec{v}\ c\ \textsf{dec}.\,C)\ \vec{a} \\ \textsf{let}\ (\_, c_1) = \mathrm{KEM.Enc}(\mathrm{pk}(\mathbf{k}_{t_k})) \\ \textsf{in}\ (c_1, \mathrm{DEM.Enc}(\mathbf{sk}^*_{()}, m_1)) \end{array}$$

- DEM axioms not immediately applicable
- KEM indistinguishability allows substituting a fresh symmetric key

KEM/DEM Composition Results

$$
\begin{array}{c}
(\lambda\ \vec{v}\ c\ \textsf{dec}.\, C)\ \vec{a} \\
\textsf{let}\ (\_, c_1) = \mathrm{KEM.Enc}(\mathrm{pk}(\mathbf{k}_{t_k})) \\
\textsf{in}\ (c_1, \mathrm{DEM.Enc}(\mathbf{sk}^*{}_{()}, m_0))
\end{array}
\sim
\begin{array}{c}
(\lambda\ \vec{v}\ c\ \textsf{dec}.\, C)\ \vec{a} \\
\textsf{let}\ (\_, c_1) = \mathrm{KEM.Enc}(\mathrm{pk}(\mathbf{k}_{t_k})) \\
\textsf{in}\ (c_1, \mathrm{DEM.Enc}(\mathbf{sk}^*{}_{()}, m_1))
\end{array}
$$

- DEM axioms not immediately applicable
- KEM indistinguishability allows substituting a fresh symmetric key
- now resolvable with DEM indistinguishability

KEM/DEM Composition Results

$$\begin{array}{c}(\lambda\ \vec{v}\ c\ \mathsf{dec}.\,C)\ \vec{a}\\ \mathsf{let}\ (\_, c_1) = \mathrm{KEM.Enc}(\mathrm{pk}(\mathbf{k}_{t_k}))\\ \mathsf{in}\ (c_1, \mathrm{DEM.Enc}(\mathbf{sk}^*{}_{()}, m_0))\end{array} \sim \begin{array}{c}(\lambda\ \vec{v}\ c\ \mathsf{dec}.\,C)\ \vec{a}\\ \mathsf{let}\ (\_, c_1) = \mathrm{KEM.Enc}(\mathrm{pk}(\mathbf{k}_{t_k}))\\ \mathsf{in}\ (c_1, \mathrm{DEM.Enc}(\mathbf{sk}^*{}_{()}, m_1))\end{array}$$

- DEM axioms not immediately applicable
- KEM indistinguishability allows substituting a fresh symmetric key
- now resolvable with DEM indistinguishability

$\Rightarrow$ CPA and CCA1 provable with only minor rewriting

KEM/DEM Composition: CCA2

For CCA2, we need to take care of guarded decryption:

if $(x_1, x_2) = \mathrm{PKE.Enc}(\mathrm{pk}(\mathbf{k}_{t_k}), m)$
then $\perp$ else $\mathrm{PKE.Dec}(\mathbf{k}_{t_k}, (x_1, x_2))$

KEM/DEM Composition: CCA2

For CCA2, we need to take care of guarded decryption:

if $(x_1, x_2) =$ (let $(sk, c_1) = \mathrm{KEM.Enc}(\mathrm{pk}(\mathbf{k}_{t_k}))$ in $(c_1, \mathrm{DEM.Enc}(sk, m)))$
then $\perp$ else let $sk = \mathrm{KEM.Dec}(\mathbf{k}_{t_k}, x_1)$ in $\mathrm{DEM.Dec}(sk, x_2)$

KEM/DEM Composition: CCA2

For CCA2, we need to take care of guarded decryption:

let $(sk, c_1) = \mathrm{KEM.Enc}(\mathrm{pk}(\mathbf{k}_{t_k})); c_2 = \mathrm{DEM.Enc}(sk, m)$
in if $(x_1, x_2) = (c_1, c_2)$
then $\perp$ else $\mathrm{DEM.Dec}(\mathrm{KEM.Dec}(\mathbf{k}_{t_k}, x_1), x_2)$

KEM/DEM Composition: CCA2

For CCA2, we need to take care of guarded decryption:

let $(sk, c_1) = \mathrm{KEM.Enc}(\mathrm{pk}(\mathbf{k}_{t_k})); c_2 = \mathrm{DEM.Enc}(sk, m)$
in if $(x_1, x_2) = (c_1, c_2)$
then $\perp$ else $\mathrm{DEM.Dec}(\mathrm{KEM.Dec}(\mathbf{k}_{t_k}, x_1), x_2)$

KEM/DEM Composition: CCA2

For CCA2, we need to take care of guarded decryption:

let $(sk, c_1) = \mathrm{KEM.Enc}(\mathrm{pk}(\mathbf{k}_{t_k})); c_2 = \mathrm{DEM.Enc}(sk, m)$
in if $(x_1, x_2) = (c_1, c_2)$
then $\perp$ else if $x_1 = c_1$ then $\mathrm{DEM.Dec}(sk, x_2)$
else $\mathrm{DEM.Dec}(\mathrm{KEM.Dec}(\mathbf{k}_{t_k}, x_1), x_2)$

KEM/DEM Composition: CCA2

For CCA2, we need to take care of guarded decryption:

let $(sk, c_1) = \mathrm{KEM.Enc}(\mathrm{pk}(\mathbf{k}_{t_k})); c_2 = \mathrm{DEM.Enc}(sk, m)$
in if $(x_1, x_2) = (c_1, c_2)$

then $\perp$ else if $x_1 = c_1$ then $\mathrm{DEM.Dec}(sk, x_2)$
else $\mathrm{DEM.Dec}(\text{if } (x_1 = c_1) \text{ then } \perp \text{ else } \mathrm{KEM.Dec}(\mathbf{k}_{t_k,1}), x_2)$

KEM/DEM Composition: CCA2

For CCA2, we need to take care of guarded decryption:

$$\text{let } (sk, c_1) = \mathrm{KEM.Enc}(\mathrm{pk}(\mathbf{k}_{t_k})); c_2 = \mathrm{DEM.Enc}(sk, m)$$
$$\text{in if } (x_1, x_2) = (c_1, c_2)$$
$$\text{then } \perp \text{ else } \begin{array}{l} \text{if } x_1 = c_1 \text{ then if } x_2 = c_2 \text{ then } \perp \text{ else } \mathrm{DEM.Dec}(sk, x_2) \\ \text{else } \mathrm{DEM.Dec}(\text{if } (x_1 = c_1) \text{ then } \perp \text{ else } \mathrm{KEM.Dec}(\mathbf{k}_{t_k,1}), x_2) \end{array}$$

KEM/DEM Composition: CCA2

For CCA2, we need to take care of guarded decryption:

let $(sk, c_1) = \mathrm{KEM.Enc}(\mathrm{pk}(\mathbf{k}_{t_k})); c_2 = \mathrm{DEM.Enc}(sk, m)$
in if $(x_1, x_2) = (c_1, c_2)$
then $\perp$ else if $x_1 = c_1$ then if $x_2 = c_2$ then $\perp$ else $\mathrm{DEM.Dec}(sk, x_2)$
else $\mathrm{DEM.Dec}($if $(x_1 = c_1)$ then $\perp$ else $\mathrm{KEM.Dec}(\mathbf{k}_{t_k,1}), x_2)$

KEM-IND-CCA2 + DEM-IND-CCA2 $\implies$ PKE-IND-CCA2 is also provable in CCSA

Conclusion

Main Result

Analyzing primitives in CCSA is clearly possible, and not overly difficult

Conclusion

Main Result

Analyzing primitives in CCSA is clearly possible, and not overly difficult

Conclusion

Main Result

Analyzing primitives in CCSA is clearly possible, and not overly difficult

Other contributions:

Conclusion

Main Result

Analyzing primitives in CCSA is clearly possible, and not overly difficult

Other contributions:

- Extensive set of CCSA security definitions for KEM/DEM hybrid encryption

Conclusion

Main Result

Analyzing primitives in CCSA is clearly possible, and not overly difficult

Other contributions:

- Extensive set of CCSA security definitions for KEM/DEM hybrid encryption
- General constructions and results for "side conditions"

école normale supérieure paris–saclay

Conclusion

Main Result

Analyzing primitives in CCSA is clearly possible, and not overly difficult

Other contributions:

- Extensive set of CCSA security definitions for KEM/DEM hybrid encryption
- General constructions and results for "side conditions"
- Abstract representation in CCSA of oblivious transfer protocols

école normale supérieure paris–saclay

Conclusion

Main Result

Analyzing primitives in CCSA is clearly possible, and not overly difficult

Other contributions:

- Extensive set of CCSA security definitions for KEM/DEM hybrid encryption
- General constructions and results for "side conditions"
- Abstract representation in CCSA of oblivious transfer protocols
- Analysis of two oblivious transfer protocols

Conclusion

Main Result

Analyzing primitives in CCSA is clearly possible, and not overly difficult

Other contributions:

- Extensive set of CCSA security definitions for KEM/DEM hybrid encryption
- General constructions and results for "side conditions"
- Abstract representation in CCSA of oblivious transfer protocols
- Analysis of two oblivious transfer protocols

Future work:

Conclusion

Main Result

Analyzing primitives in CCSA is clearly possible, and not overly difficult

Other contributions:

- Extensive set of CCSA security definitions for KEM/DEM hybrid encryption
- General constructions and results for "side conditions"
- Abstract representation in CCSA of oblivious transfer protocols
- Analysis of two oblivious transfer protocols

Future work:

- Analyze concrete KEM and DEM

école normale supérieure paris-saclay

Conclusion

Main Result

Analyzing primitives in CCSA is clearly possible, and not overly difficult

Other contributions:

- Extensive set of CCSA security definitions for KEM/DEM hybrid encryption
- General constructions and results for "side conditions"
- Abstract representation in CCSA of oblivious transfer protocols
- Analysis of two oblivious transfer protocols

Future work:

- Analyze concrete KEM and DEM
- Proof of a protocol using abstract OT

Conclusion

Main Result

Analyzing primitives in CCSA is clearly possible, and not overly difficult

Other contributions:

- Extensive set of CCSA security definitions for KEM/DEM hybrid encryption
- General constructions and results for "side conditions"
- Abstract representation in CCSA of oblivious transfer protocols
- Analysis of two oblivious transfer protocols

Future work:

- Analyze concrete KEM and DEM
- Proof of a protocol using abstract OT
- Implementation in SQUIRREL

Bibliography

[1] David Baelde, Adrien Koutsos, and Joseph Lallemand. "A Higher-Order Indistinguishability Logic for Cryptographic Reasoning". In: *LICS*. Boston, United States: IEEE, June 2023, pp. 1–13. DOI: 10.1109/LICS56636.2023.10175781. URL: https://inria.hal.science/hal-03981949.

[2] David Baelde et al. "An Interactive Prover for Protocol Verification in the Computational Model". In: *42nd IEEE Symposium on Security and Privacy, SP 2021, San Francisco, CA, USA, 24-27 May 2021*. IEEE, 2021, pp. 537–554. DOI: 10.1109/SP40001.2021.00078. URL: https://doi.org/10.1109/SP40001.2021.00078.

[3] Javier Herranz, Dennis Hofheinz, and Eike Kiltz. "Some (in)sufficient conditions for secure hybrid encryption". In: *IACR Cryptol. ePrint Arch.* (2006), p. 265. URL: http://eprint.iacr.org/2006/265.

[4] Adrien Koutsos. "The 5G-AKA Authentication Protocol Privacy". In: *2019 IEEE European Symposium on Security and Privacy (EuroS&P)*. 2019, pp. 464–479. DOI: 10.1109/EuroSP.2019.00041.

CCSA: Indistinguishability [1]

Def. CCSA indistinguishability

$t_1 \sim t_2$ if no polynomial-time attacker can distinguish between t_1 and t_2:

$$[\![t_1 \sim t_2]\!]_{\mathbb{M}:\mathcal{E}} := \forall \mathcal{A} \in \mathrm{PPTM}, \mathrm{Adv}^{\eta}_{\mathbb{M}:\mathcal{E}}(\mathcal{A} : t_1 \sim t_2) \in \mathsf{negl}(\eta)$$

$$\mathrm{Adv}^{\eta}_{\mathbb{M}:\mathcal{E}}(\mathcal{A} : t_1 \sim t_2) := |\mathtt{Pr}_{\rho \in \mathbb{T}_{\mathbb{M},\eta}}[\mathcal{A}(1^{\eta}, [\![t_1]\!]^{\eta,\rho}_{\mathbb{M}:\mathcal{E}}, \rho_a)] - \mathtt{Pr}_{\rho \in \mathbb{T}_{\mathbb{M},\eta}}[\mathcal{A}(1^{\eta}, [\![t_2]\!]^{\eta,\rho}_{\mathbb{M}:\mathcal{E}}, \rho_a)]|$$

$\mathsf{negl}(\eta)$ denotes that the advantage grows slower than the inverse of any polynomial.

Symmetry

$$\frac{\mathcal{E}; \Theta \vdash \vec{u} \sim \vec{v}}{\mathcal{E}; \Theta \vdash \vec{v} \sim \vec{u}}$$

Transitivity

$$\frac{\mathcal{E}; \Theta \vdash \vec{u} \sim \vec{v} \qquad \mathcal{E}; \Theta \vdash \vec{v} \sim \vec{w}}{\mathcal{E}; \Theta \vdash \vec{u} \sim \vec{w}}$$

CCSA: Overwhelming Truth [1]

Def. Overwhelming Truth

$[\phi]$: Formula ϕ almost always evaluates to `true`

$$[\![[\phi]]\!]_{\mathbb{M}:\mathcal{E}} := \mathtt{Pr}_{\rho \in \mathbb{T}_{\mathbb{M},\eta}}[\neg [\![\phi]\!]^{\eta,\rho}_{\mathbb{M}:\mathcal{E}}] \in \mathsf{negl}(\eta)$$

Rewrite

$$\frac{\mathcal{E};\Theta \vdash F[s] \qquad \mathcal{E};\Theta \vdash [s = t]}{\mathcal{E};\Theta \vdash F[t]}$$

β

$$\frac{}{\mathcal{E};\Theta \vdash [(\lambda(x:\tau).t)\ t_0 = t\{x \mapsto t_0\}]}$$

KEM/DEM Security Results

Herranz, Hofheinz, and Kiltz [3]:
KEM-IND-CCA2 + DEM-IND-CCA2 $\implies$ PKE-IND-CCA2

$$\begin{array}{c}(\lambda\ \vec{v}\ c.C)\ \vec{a} \\ \mathrm{PKE.Enc}(\mathrm{pk}(k\ \ t_k), m, (r_1\ \ t_r, r_2\ \ t_r))\end{array} \sim \begin{array}{c}(\lambda\ \vec{v}\ c.C)\ \vec{a} \\ \mathrm{PKE.Enc}(\mathrm{pk}(k\ \ t_k), 0^{|m|}, (r_1\ \ t_r, r_2\ \ t_r))\end{array}$$

KEM/DEM Security Results

Herranz, Hofheinz, and Kiltz [3]:
KEM-IND-CCA2 + DEM-IND-CCA2 $\implies$ PKE-IND-CCA2

$$\begin{array}{c} (\lambda\ \vec{v}\ c\ \mathsf{dec}.\,C)\ \vec{a} \\ \mathrm{PKE.Enc}(\mathrm{pk}(k\ t_k), m, (r_1\ t_r, r_2\ t_r)) \\ (\lambda x.\mathsf{if}\ x = \\ \mathrm{PKE.Enc}(\mathrm{pk}(k\ t_k), m, (r_1\ t_r, r_2\ t_r)) \\ \mathsf{then}\ \bot\ \mathsf{else}\ \mathrm{PKE.Dec}(k\ t_k, x)) \end{array} \sim \begin{array}{c} (\lambda\ \vec{v}\ c\ \mathsf{dec}.\,C)\ \vec{a} \\ \mathrm{PKE.Enc}(\mathrm{pk}(k\ t_k), 0^{|m|}, (r_1\ t_r, r_2\ t_r)) \\ (\lambda x.\mathsf{if}\ x = \\ \mathrm{PKE.Enc}(\mathrm{pk}(k\ t_k), 0^{|m|}, (r_1\ t_r, r_2\ t_r)) \\ \mathsf{then}\ \bot\ \mathsf{else}\ \mathrm{PKE.Dec}(k\ t_k, x)) \end{array}$$

KEM/DEM Security Results

Herranz, Hofheinz, and Kiltz [3]:
KEM-IND-CCA2 + DEM-IND-CCA2 $\implies$ PKE-IND-CCA2

$$
\begin{array}{c}
(\lambda\ \vec{v}\ c\ \text{dec}.\, C)\ \vec{a}\ \text{let}\ (sk, c_1) = \\
\mathrm{KEM.Enc}(\mathrm{pk}(k\ t_k), r_1\ \ t_r) \\
\text{in}\ (c_1, \mathrm{DEM.Enc}(sk, m, r_2\ \ t_r)) \\
(\lambda(x_1, x_2).\text{if}\ (x_1, x_2) = \text{let}\ (sk, c_1) = \\
\mathrm{KEM.Enc}(\mathrm{pk}(k\ t_k), r_1\ \ t_r) \\
\text{in}\ (c_1, \mathrm{DEM.Enc}(sk, m, r_2\ \ t_r)) \\
\text{then}\ \perp \\
\text{else let}\ sk = \mathrm{KEM.Dec}(k\ t_k, x_1) \\
\text{in}\ \mathrm{DEM.Dec}(sk, x_2))
\end{array}
\sim
\begin{array}{c}
(\lambda\ \vec{v}\ c\ \text{dec}.\, C)\ \vec{a}\ \text{let}\ (sk, c_1) = \\
\mathrm{KEM.Enc}(\mathrm{pk}(k\ t_k), r_1\ \ t_r) \\
\text{in}\ (c_1, \mathrm{DEM.Enc}(sk, 0^{|m|}, r_2\ \ t_r)) \\
(\lambda(c_1, c_2).\text{if}\ (c_1, c_2) = \text{let}\ (sk, c_1) = \\
\mathrm{KEM.Enc}(\mathrm{pk}(k\ t_k), r_1\ \ t_r) \\
\text{in}\ (c_1, \mathrm{DEM.Enc}(sk, 0^{|m|}, r_2\ \ t_r)) \\
\text{then}\ \perp \\
\text{else let}\ sk = \mathrm{KEM.Dec}(k\ t_k, x_1) \\
\text{in}\ \mathrm{DEM.Dec}(sk, x_2))
\end{array}
$$

KEM/DEM Security Results

Herranz, Hofheinz, and Kiltz [3]:
KEM-IND-CCA2 + DEM-IND-CCA2 $\implies$ PKE-IND-CCA2

$$\begin{array}{c}\text{let } (sk, c_1) = \\ \mathrm{KEM.Enc}(\mathrm{pk}(k\ t_k), r_1\ t_r) \\ \text{in } (\lambda\ \vec{v}\ c\ \text{dec}.\, C)\ \vec{a} \\ (c_1, \mathrm{DEM.Enc}(sk, m, r_2\ t_r)) \\ (\lambda(x_1, x_2).\text{if } (x_1, x_2) = \\ (c_1, \mathrm{DEM.Enc}(sk, m, r_2\ t_r)) \text{ then } \bot \\ \text{else let } sk' = \mathrm{KEM.Dec}(k\ t_k, x_1) \\ \text{in } \mathrm{DEM.Dec}(sk', x_2))\end{array} \sim \begin{array}{c}\text{let } (sk, c_1) = \\ \mathrm{KEM.Enc}(\mathrm{pk}(k\ t_k), r_1\ t_r) \\ \text{in } (\lambda\ \vec{v}\ c\ \text{dec}.\, C)\ \vec{a} \\ (c_1, \mathrm{DEM.Enc}(sk, 0^{|m|}, r_2\ t_r)) \\ (\lambda(x_1, x_2).\text{if } (x_1, x_2) = \\ (c_1, \mathrm{DEM.Enc}(sk, 0^{|m|}, r_2\ t_r)) \text{ then } \bot \\ \text{else let } sk' = \mathrm{KEM.Dec}(k\ t_k, x_1) \\ \text{in } \mathrm{DEM.Dec}(sk', x_2))\end{array}$$

KEM/DEM Security Results

Herranz, Hofheinz, and Kiltz [3]:
KEM-IND-CCA2 + DEM-IND-CCA2 $\implies$ PKE-IND-CCA2

$$\begin{array}{c} \text{let } (sk, c_1) = \\ \mathrm{KEM.Enc}(\mathrm{pk}(k\ t_k), r_1\ t_r) \\ \text{in } (\lambda\ \vec{v}\ c\ \text{dec}.\ C)\ \vec{a} \\ (c_1, \mathrm{DEM.Enc}(sk, m, r_2\ t_r)) \\ (\lambda(x_1, x_2).\text{if } (x_1, x_2) = \\ (c_1, \mathrm{DEM.Enc}(sk, m, r_2\ t_r)) \text{ then } \bot \\ \text{else let } sk' = \text{if } x_1 = c_1 \text{ then } sk \\ \text{else } \mathrm{KEM.Dec}(k\ t_k, x_1) \\ \text{in } \mathrm{DEM.Dec}(sk', x_2)) \end{array} \sim \begin{array}{c} \text{let } (sk, c_1) = \\ \mathrm{KEM.Enc}(\mathrm{pk}(k\ t_k), r_1\ t_r) \\ \text{in } (\lambda\ \vec{v}\ c\ \text{dec}.\ C)\ \vec{a} \\ (c_1, \mathrm{DEM.Enc}(sk, 0^{|m|}, r_2\ t_r)) \\ (\lambda(x_1, x_2).\text{if } (x_1, x_2) = \\ (c_1, \mathrm{DEM.Enc}(sk, 0^{|m|}, r_2\ t_r)) \text{ then } \bot \\ \text{else let } sk' = \text{if } x_1 = c_1 \text{ then } sk \\ \text{else } \mathrm{KEM.Dec}(k\ t_k, x_1) \\ \text{in } \mathrm{DEM.Dec}(sk', x_2)) \end{array}$$

KEM/DEM Security Results

Herranz, Hofheinz, and Kiltz [3]:
KEM-IND-CCA2 + DEM-IND-CCA2 $\implies$ PKE-IND-CCA2

$$
\begin{array}{c}
\text{let } (sk, c_1) = \\
\mathrm{KEM.Enc}(\mathrm{pk}(k\ t_k), r_1\ t_r) \\
\text{in } (\lambda\ \vec{v}\ c\ \text{dec}.\ C)\ \vec{a} \\
(c_1, \mathrm{DEM.Enc}(sk, m, r_2\ t_r)) \\
(\lambda(x_1, x_2).\text{if } (x_1, x_2) = \\
(c_1, \mathrm{DEM.Enc}(sk, m, r_2\ t_r)) \text{ then } \bot \\
\text{else let } sk' = \text{if } x_1 = c_1 \text{ then } sk \\
\text{else if } x_1 = c_1 \text{ then } \bot \\
\text{else } \mathrm{KEM.Dec}(k\ t_k, x_1) \\
\text{in } \mathrm{DEM.Dec}(sk', x_2))
\end{array}
\sim
\begin{array}{c}
\text{let } (sk, c_1) = \\
\mathrm{KEM.Enc}(\mathrm{pk}(k\ t_k), r_1\ t_r) \\
\text{in } (\lambda\ \vec{v}\ c\ \text{dec}.\ C)\ \vec{a} \\
(c_1, \mathrm{DEM.Enc}(sk, 0^{|m|}, r_2\ t_r)) \\
(\lambda(x_1, x_2).\text{if } (x_1, x_2) = \\
(c_1, \mathrm{DEM.Enc}(sk, 0^{|m|}, r_2\ t_r)) \text{ then } \bot \\
\text{else let } sk' = \text{if } x_1 = c_1 \text{ then } sk \\
\text{else if } x_1 = c_1 \text{ then } \bot \\
\text{else } \mathrm{KEM.Dec}(k\ t_k, x_1) \\
\text{in } \mathrm{DEM.Dec}(sk', x_2))
\end{array}
$$

KEM/DEM Security Results

Herranz, Hofheinz, and Kiltz [3]:
KEM-IND-CCA2 + DEM-IND-CCA2 $\implies$ PKE-IND-CCA2

$$\begin{array}{c}
\text{let } (sk, c_1) = \\
\mathrm{KEM.Enc}(\mathrm{pk}(k\ t_k), r_1\ t_r) \\
\text{in } (\lambda\ \vec{v}\ c\ \text{dec}.\, C)\ \vec{a} \\
(c_1, \mathrm{DEM.Enc}(sk, m, r_2\ t_r)) \\
(\lambda(x_1, x_2).\text{if } (x_1, x_2) = \\
(c_1, \mathrm{DEM.Enc}(sk, m, r_2\ t_r)) \text{ then } \bot \\
\text{else let } sk' = \text{if } x_1 = c_1 \text{ then } sk \\
\text{else if } x_1 = c_1 \text{ then } \bot \\
\text{else } \mathrm{KEM.Dec}(k\ t_k, x_1) \\
\text{in } \mathrm{DEM.Dec}(sk', x_2))
\end{array}
\sim
\begin{array}{c}
\text{let } (sk, c_1) = \\
\mathrm{KEM.Enc}(\mathrm{pk}(k\ t_k), r_1\ t_r) \\
\text{in } (\lambda\ \vec{v}\ c\ \text{dec}.\, C)\ \vec{a} \\
(c_1, \mathrm{DEM.Enc}(sk, 0^{|m|}, r_2\ t_r)) \\
(\lambda(x_1, x_2).\text{if } (x_1, x_2) = \\
(c_1, \mathrm{DEM.Enc}(sk, 0^{|m|}, r_2\ t_r)) \text{ then } \bot \\
\text{else let } sk' = \text{if } x_1 = c_1 \text{ then } sk \\
\text{else if } x_1 = c_1 \text{ then } \bot \\
\text{else } \mathrm{KEM.Dec}(k\ t_k, x_1) \\
\text{in } \mathrm{DEM.Dec}(sk', x_2))
\end{array}$$

KEM/DEM Security Results

Herranz, Hofheinz, and Kiltz [3]:
KEM-IND-CCA2 + DEM-IND-CCA2 $\implies$ PKE-IND-CCA2

$$
\begin{array}{c}
\text{let } (sk, c_1) = \\
(sk^*\ (), \pi_2 \mathrm{KEM.Enc}(\mathrm{pk}(k\ t_k), r_1\ t_r)) \\
\text{in } (\lambda\ \vec{v}\ c\ \text{dec.}\, C)\ \vec{a} \\
(c_1, \mathrm{DEM.Enc}(sk, m, r_2\ t_r)) \\
(\lambda(x_1, x_2).\text{if } (x_1, x_2) = \\
(c_1, \mathrm{DEM.Enc}(sk, m, r_2\ t_r)) \text{ then } \bot \\
\text{else let } sk' = \text{if } x_1 = c_1 \text{ then } sk \\
\text{else if } x_1 = c_1 \text{ then } \bot \\
\text{else } \mathrm{KEM.Dec}(k\ t_k, x_1) \\
\text{in } \mathrm{DEM.Dec}(sk', x_2))
\end{array}
\sim
\begin{array}{c}
\text{let } (sk, c_1) = \\
(sk^*\ (), \pi_2 \mathrm{KEM.Enc}(\mathrm{pk}(k\ t_k), r_1\ t_r)) \\
\text{in } (\lambda\ \vec{v}\ c\ \text{dec.}\, C)\ \vec{a} \\
(c_1, \mathrm{DEM.Enc}(sk, 0^{|m|}, r_2\ t_r)) \\
(\lambda(x_1, x_2).\text{if } (x_1, x_2) = \\
(c_1, \mathrm{DEM.Enc}(sk, 0^{|m|}, r_2\ t_r)) \text{ then } \bot \\
\text{else let } sk' = \text{if } x_1 = c_1 \text{ then } sk \\
\text{else if } x_1 = c_1 \text{ then } \bot \\
\text{else } \mathrm{KEM.Dec}(k\ t_k, x_1) \\
\text{in } \mathrm{DEM.Dec}(sk', x_2))
\end{array}
$$

KEM/DEM Security Results

Herranz, Hofheinz, and Kiltz [3]:
KEM-IND-CCA2 + DEM-IND-CCA2 $\implies$ PKE-IND-CCA2

$$
\begin{array}{c}
\text{let } c_1 = \pi_2 \mathrm{KEM.Enc}(\mathrm{pk}(k\ t_k), r_1\ t_r) \\
\text{in } (\lambda\ \vec{v}\ c\ \text{dec.}C)\ \vec{a} \\
(c_1, \mathrm{DEM.Enc}(sk^*\ (), m, r_2\ t_r)) \\
(\lambda(x_1, x_2).\text{if } (x_1, x_2) = \\
(c_1, \mathrm{DEM.Enc}(sk^*\ (), m, r_2\ t_r)) \\
\text{then } \bot \text{ else let } sk' = \text{if } x_1 = c_1 \\
\text{then } sk^*\ () \text{ else if } x_1 = c_1 \text{ then } \bot \\
\text{else } \mathrm{KEM.Dec}(k\ t_k, x_1) \\
\text{in } \mathrm{DEM.Dec}(sk', x_2))
\end{array}
\sim
\begin{array}{c}
\text{let } c_1 = \pi_2 \mathrm{KEM.Enc}(\mathrm{pk}(k\ t_k), r_1\ t_r) \\
\text{in } (\lambda\ \vec{v}\ c\ \text{dec.}C)\ \vec{a} \\
(c_1, \mathrm{DEM.Enc}(sk^*\ (), 0^{|m|}, r_2\ t_r)) \\
(\lambda(x_1, x_2).\text{if } (x_1, x_2) = \\
(c_1, \mathrm{DEM.Enc}(sk^*\ (), 0^{|m|}, r_2\ t_r)) \\
\text{then } \bot \text{ else let } sk' = \text{if } x_1 = c_1 \\
\text{then } sk^*\ () \text{ else if } x_1 = c_1 \text{ then } \bot \\
\text{else } \mathrm{KEM.Dec}(k\ t_k, x_1) \\
\text{in } \mathrm{DEM.Dec}(sk', x_2))
\end{array}
$$

KEM/DEM Security Results

Herranz, Hofheinz, and Kiltz [3]:

KEM-IND-CCA2 + DEM-IND-CCA2 $\implies$ PKE-IND-CCA2

$$\begin{array}{c}\text{let } c_1 = \pi_2 \mathrm{KEM.Enc}(\mathrm{pk}(k\ t_k), r_1\ t_r) \\ \text{in } (\lambda\ \vec{v}\ c\ \text{dec.}\,C)\ \vec{a} \\ (c_1, \mathrm{DEM.Enc}(sk^*\ (), m, r_2\ t_r)) \\ (\lambda(x_1, x_2).\text{if } (x_1, x_2) = \\ (c_1, \mathrm{DEM.Enc}(sk^*\ (), m, r_2\ t_r)) \\ \text{then } \bot \text{ else if } x_1 = c_1 \text{ then if } x_2 = c_2 \\ \text{then } \bot \text{ else } \mathrm{DEM.Dec}(sk^*\ (), x_2) \\ \text{else } \mathrm{DEM.Dec}(\mathrm{KEM.Dec}(k\ t_k, x_1), x_2))\end{array} \sim \begin{array}{c}\text{let } c_1 = \pi_2 \mathrm{KEM.Enc}(\mathrm{pk}(k\ t_k), r_1\ t_r) \\ \text{in } (\lambda\ \vec{v}\ c\ \text{dec.}\,C)\ \vec{a} \\ (c_1, \mathrm{DEM.Enc}(sk^*\ (), 0^{|m|}, r_2\ t_r)) \\ (\lambda(x_1, x_2).\text{if } (x_1, x_2) = \\ (c_1, \mathrm{DEM.Enc}(sk^*\ (), 0^{|m|}, r_2\ t_r)) \\ \text{then } \bot \text{ else if } x_1 = c_1 \text{ then if } x_2 = c_2 \\ \text{then } \bot \text{ else } \mathrm{DEM.Dec}(sk^*\ (), x_2) \\ \text{else } \mathrm{DEM.Dec}(\mathrm{KEM.Dec}(k\ t_k, x_1), x_2))\end{array}$$

KEM/DEM Security Results

Herranz, Hofheinz, and Kiltz [3]:
KEM-IND-CCA2 + DEM-IND-CCA2 $\implies$ PKE-IND-CCA2

$$\begin{array}{c} \text{let } c_1 = \pi_2 \mathrm{KEM.Enc}(\mathrm{pk}(k\ t_k), r_1\ t_r) \\ \text{in } (\lambda\ \vec{v}\ c\ \text{dec.}\, C)\ \vec{a} \\ (c_1, \mathrm{DEM.Enc}(sk^*\ (), m, r_2\ t_r)) \\ (\lambda(x_1, x_2).\text{if } (x_1, x_2) = \\ (c_1, \mathrm{DEM.Enc}(sk^*\ (), m, r_2\ t_r)) \\ \text{then } \bot \text{ else if } x_1 = c_1 \text{ then if } x_2 = c_2 \\ \text{then } \bot \text{ else } \mathrm{DEM.Dec}(sk^*\ (), x_2) \\ \text{else } \mathrm{DEM.Dec}(\mathrm{KEM.Dec}(k\ t_k, x_1), x_2)) \end{array} \sim \begin{array}{c} \text{let } c_1 = \pi_2 \mathrm{KEM.Enc}(\mathrm{pk}(k\ t_k), r_1\ t_r) \\ \text{in } (\lambda\ \vec{v}\ c\ \text{dec.}\, C)\ \vec{a} \\ (c_1, \mathrm{DEM.Enc}(sk^*\ (), 0^{|m|}, r_2\ t_r)) \\ (\lambda(x_1, x_2).\text{if } (x_1, x_2) = \\ (c_1, \mathrm{DEM.Enc}(sk^*\ (), 0^{|m|}, r_2\ t_r)) \\ \text{then } \bot \text{ else if } x_1 = c_1 \text{ then if } x_2 = c_2 \\ \text{then } \bot \text{ else } \mathrm{DEM.Dec}(sk^*\ (), x_2) \\ \text{else } \mathrm{DEM.Dec}(\mathrm{KEM.Dec}(k\ t_k, x_1), x_2)) \end{array}$$