Composable and Finite Computational Security of Quantum Message Transmission

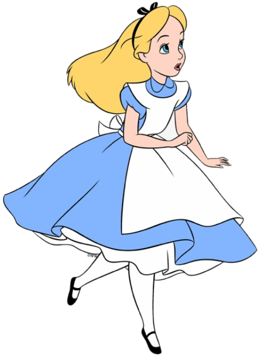
Fabio Banfi, Ueli Maurer, Christopher Portmann, Jiamin Zhu

ETH Zurich, Switzerland

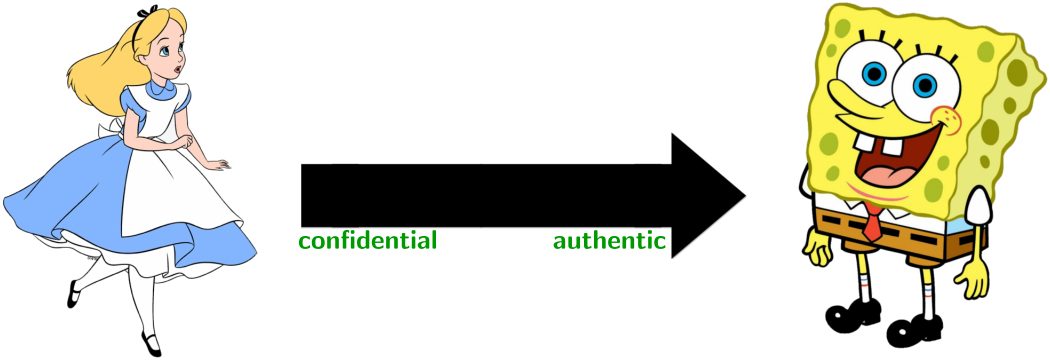
Theory of Cryptography Conference
December 1-5, 2019, Nuremberg, Germany

Background: communication channels

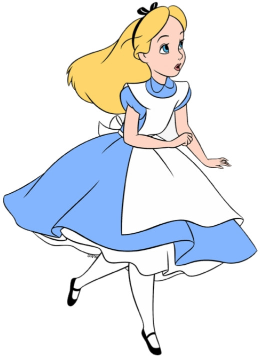
Background: communication channels

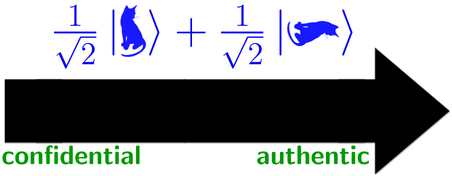


Background: communication channels

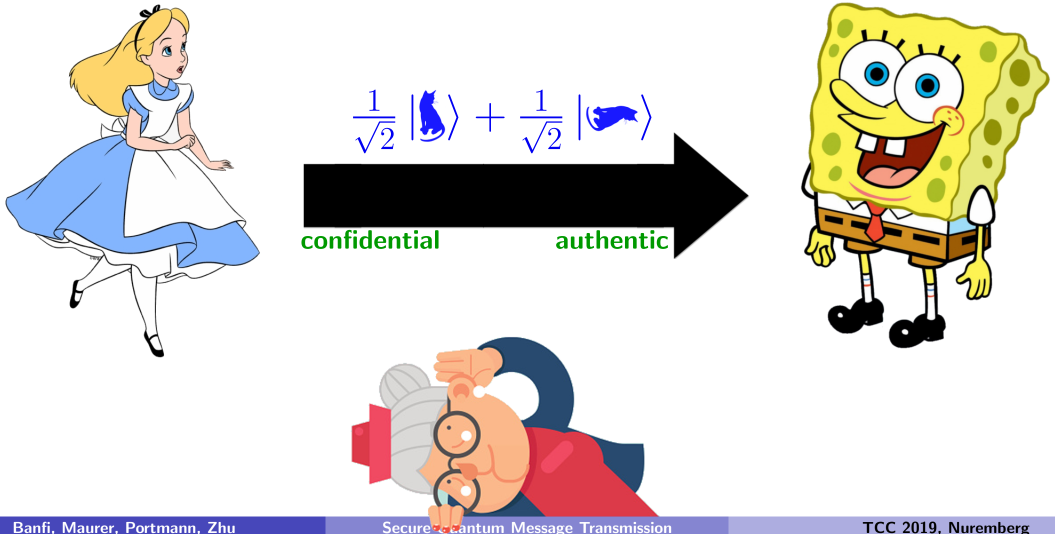


Background: quantum communication channels

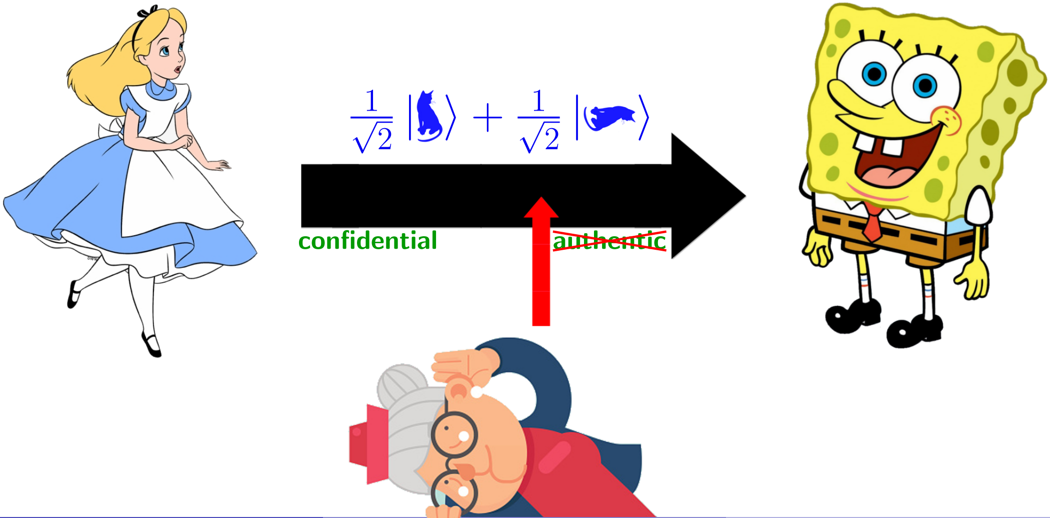




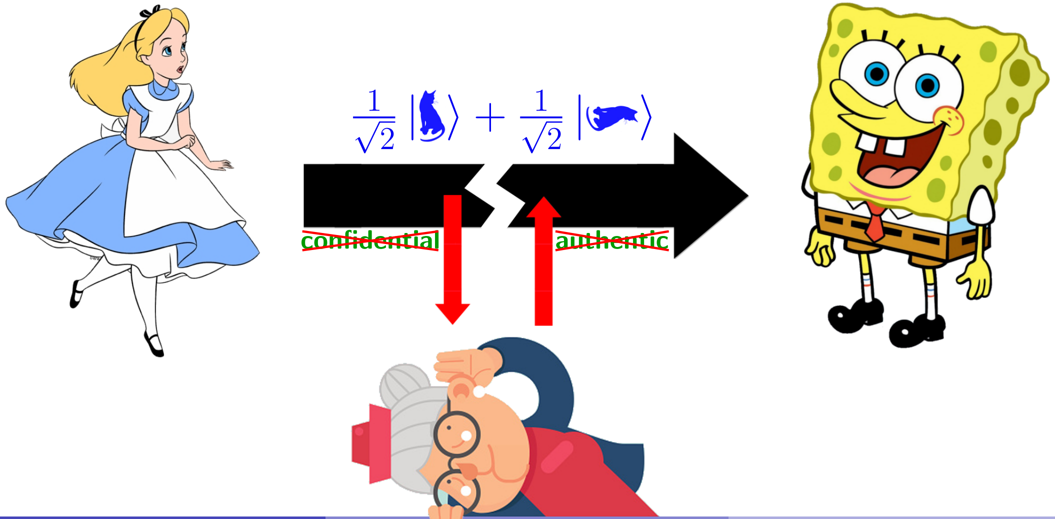
Background: quantum communication channels



Background: quantum communication channels



Background: quantum communication channels



Background: quantum symmetric encryption

Background: quantum symmetric encryption

Alice and Bob might use *Quantum Symmetric Encryption* (QSE):

Background: quantum symmetric encryption

Alice and Bob might use *Quantum Symmetric Encryption* (QSE):

- Shared classical secret key: K (e.g., $K \in \{0,1\}^n$)

Background: quantum symmetric encryption

Alice and Bob might use *Quantum Symmetric Encryption* (QSE):

- Shared classical secret key: K (e.g., $K \in \{0,1\}^n$)
- Plaintexts (ρ) and ciphertexts (σ) are *mixed quantum states*

Background: quantum symmetric encryption

Alice and Bob might use *Quantum Symmetric Encryption* (QSE):

- Shared classical secret key: K (e.g., $K \in \{0,1\}^n$)
- Plaintexts (ρ) and ciphertexts (σ) are *mixed quantum states*
- Encryption: $\sigma \leftarrow \texttt{Enc}_K(\rho)$; Decryption: $\rho \leftarrow \texttt{Dec}_K(\sigma)$ (if σ invalid, $\rho = |\bot\rangle\langle\bot|$)

Background: quantum symmetric encryption

Alice and Bob might use *Quantum Symmetric Encryption* (QSE):

- Shared classical secret key: K (e.g., $K \in \{0,1\}^n$)
- Plaintexts (ρ) and ciphertexts (σ) are *mixed quantum states*
- Encryption: $\sigma \leftarrow \mathtt{Enc}_K(\rho)$; Decryption: $\rho \leftarrow \mathtt{Dec}_K(\sigma)$ (if σ invalid, $\rho = |\bot\rangle\langle\bot|$)

How to define security of QSE?

Background: quantum symmetric encryption

Alice and Bob might use *Quantum Symmetric Encryption* (QSE):

- Shared classical secret key: K (e.g., $K \in \{0,1\}^n$)
- Plaintexts (ρ) and ciphertexts (σ) are *mixed quantum states*
- Encryption: $\sigma \leftarrow \texttt{Enc}_K(\rho)$; Decryption: $\rho \leftarrow \texttt{Dec}_K(\sigma)$ (if σ invalid, $\rho = |\bot\rangle\langle\bot|$)

How to define security of QSE? E.g., can we “adapt” the classical **IND-CCA2** notion?

Background: quantum symmetric encryption

Alice and Bob might use *Quantum Symmetric Encryption* (QSE):

- Shared classical secret key: K (e.g., $K \in \{0,1\}^n$)
- Plaintexts (ρ) and ciphertexts (σ) are *mixed quantum states*
- Encryption: $\sigma \leftarrow \texttt{Enc}_K(\rho)$; Decryption: $\rho \leftarrow \texttt{Dec}_K(\sigma)$ (if σ invalid, $\rho = |\bot\rangle\langle\bot|$)

How to define security of QSE? E.g., can we "adapt" the classical **IND-CCA2** notion?

Challenging: *No-cloning Theorem*

Background: quantum symmetric encryption

Alice and Bob might use *Quantum Symmetric Encryption* (QSE):

- Shared classical secret key: K (e.g., $K \in \{0,1\}^n$)
- Plaintexts (ρ) and ciphertexts (σ) are *mixed quantum states*
- Encryption: $\sigma \leftarrow \texttt{Enc}_K(\rho)$; Decryption: $\rho \leftarrow \texttt{Dec}_K(\sigma)$ (if σ invalid, $\rho = |\bot\rangle\langle\bot|$)

How to define security of QSE? E.g., can we "adapt" the classical **IND-CCA2** notion?

Challenging: *No-cloning Theorem* $\implies$ cannot "save copies of ciphertext to compare"

Background: security of QSE

Background: security of QSE

[Alagic, Gagliardoni, Majenz, 2018] provide *(asymptotic) game-based* definitions of:

Background: security of QSE

[Alagic, Gagliardoni, Majenz, 2018] provide *(asymptotic) game-based* definitions of:

- Confidentiality: *quantum adaptive chosen-ciphertext indistinguishability* (**QIND-CCA2**)

Background: security of QSE

[Alagic, Gagliardoni, Majenz, 2018] provide *(asymptotic) game-based* definitions of:

- Confidentiality: *quantum adaptive chosen-ciphertext indistinguishability* (**QIND-CCA2**)
- Confidentiality + authenticity: *quantum authenticated encryption* (**QAE**)

Background: security of QSE

[Alagic, Gagliardoni, Majenz, 2018] provide *(asymptotic) game-based* definitions of:

- Confidentiality: *quantum adaptive chosen-ciphertext indistinguishability* (**QIND-CCA2**)
- Confidentiality + authenticity: *quantum authenticated encryption* (**QAE**)

QAE: any *efficient* adversary must have *negligible* advantage in distinguishing between:

Background: security of QSE

[Alagic, Gagliardoni, Majenz, 2018] provide *(asymptotic) game-based* definitions of:

- Confidentiality: *quantum adaptive chosen-ciphertext indistinguishability* (**QIND-CCA2**)
- Confidentiality + authenticity: *quantum authenticated encryption* (**QAE**)

QAE: any *efficient* adversary must have *negligible* advantage in distinguishing between:

- Real encryption ($\mathbf{RealEnc}_K \equiv \mathtt{Enc}_K$) and decryption ($\mathbf{RealDec}_K \equiv \mathtt{Dec}_K$) oracles

Background: security of QSE

[Alagic, Gagliardoni, Majenz, 2018] provide *(asymptotic) game-based* definitions of:

- Confidentiality: *quantum adaptive chosen-ciphertext indistinguishability* (**QIND-CCA2**)
- Confidentiality + authenticity: *quantum authenticated encryption* (**QAE**)

QAE: any *efficient* adversary must have *negligible* advantage in distinguishing between:

- Real encryption ($\mathbf{RealEnc}_K \equiv \mathtt{Enc}_K$) and decryption ($\mathbf{RealDec}_K \equiv \mathtt{Dec}_K$) oracles
- Ideal encryption ($\mathbf{IdealEnc}_K$) and decryption ($\mathbf{IdealDec}_K$) oracles

Background: QAE security of QSE

Background: QAE security of QSE

Defining the **ideal** oracles (simplified for 1 message):

registers P, C

---

oracle $\mathbf{IdealEnc}_K(\rho)$
 $P \leftarrow \rho$
 $C \leftarrow \mathbf{Enc}_K(|\mathbf{0}\rangle)$
 return [copy of] C

Background: QAE security of QSE

Defining the **ideal** oracles (simplified for 1 message):

registers P, C

---

oracle $\mathbf{IdealEnc}_K(\rho)$
  $P \leftarrow \rho$
  $C \leftarrow \mathbf{Enc}_K(|\mathbf{0}\rangle)$
  return [copy of] C

---

oracle $\mathbf{IdealDec}_K(\sigma)$
  if $\sigma \equiv C$ **then**
    return P
  return $|\bot\rangle$

Background: QAE security of QSE

Defining the **ideal** oracles (simplified for 1 message):

registers P, C

---

oracle $\mathbf{IdealEnc}_K(\rho)$
  $P \leftarrow \rho$
  $C \leftarrow \mathbf{Enc}_K(|\mathbf{0}\rangle)$
  return [copy of] C

---

oracle $\mathbf{IdealDec}_K(\sigma)$
  if $\sigma \equiv C$ **then**
    return P
  return $|\bot\rangle$

$\Longrightarrow$ **This breaks no-cloning!**

Background: QAE security of QSE

Defining the **ideal** oracles (simplified for 1 message):

registers P, C

oracle $\mathbf{IdealEnc}_K(\rho)$
  $P \leftarrow \rho$
  $C \leftarrow \mathbf{Enc}_K(|\mathbf{0}\rangle)$
  return [copy of] C

oracle $\mathbf{IdealDec}_K(\sigma)$
  if $\sigma \equiv C$ **then**
    return P
  return $|\bot\rangle$

$\Longrightarrow$ **This breaks no-cloning!**

$\Longrightarrow$

registers P, M_0, M_1

oracle $\mathbf{IdealEnc}_K(\rho)$
  $P \leftarrow \rho$
  $[M_0, M_1] \leftarrow |\mathbf{\Phi}^+\rangle$
  return $\mathbf{Enc}_K(M_0)$

Background: QAE security of QSE

Defining the **ideal** oracles (simplified for 1 message):

registers P, C

---

oracle $\mathbf{IdealEnc}_K(\rho)$
  $P \leftarrow \rho$
  $C \leftarrow \mathbf{Enc}_K(|\mathbf{0}\rangle)$
  return [copy of] C

---

oracle $\mathbf{IdealDec}_K(\sigma)$
  if $\sigma \equiv C$ **then**
    return P
  return $|\bot\rangle$

$\Longrightarrow$ **This breaks no-cloning!**

$\Longrightarrow$

registers P, M_0, M_1

---

oracle $\mathbf{IdealEnc}_K(\rho)$
  $P \leftarrow \rho$
  $[M_0, M_1] \leftarrow |\mathbf{\Phi}^+\rangle$
  return $\mathbf{Enc}_K(M_0)$

---

oracle $\mathbf{IdealDec}_K(\sigma)$
  register $\tilde{M}_0 \leftarrow \mathbf{Dec}_K(\sigma)$
  if $[\tilde{M}_0, M_1] \equiv |\mathbf{\Phi}^+\rangle$ **then**
    return P
  return $|\bot\rangle$

Background: QIND-CCA2 security of QSE

Background: QIND-CCA2 security of QSE

[Alagic et al. 2018]: compare the performance of adversary in two different games:

Background: QIND-CCA2 security of QSE

[Alagic et al. 2018]: compare the performance of adversary in two different games:

- **Test**: quantum version of single-challenge **IND-CCA2**, but w/o checks upon decryption

Background: QIND-CCA2 security of QSE

[Alagic et al. 2018]: compare the performance of adversary in two different games:

- **Test**: quantum version of single-challenge **IND-CCA2**, but w/o checks upon decryption
- **Fake**: same but always encrypt a fixed plaintext; lose if cheat, win with prob. $\frac{1}{2}$ o/w

Background: QIND-CCA2 security of QSE

[Alagic et al. 2018]: compare the performance of adversary in two different games:

- **Test**: quantum version of single-challenge **IND-CCA2**, but w/o checks upon decryption
- **Fake**: same but always encrypt a fixed plaintext; lose if cheat, win with prob. $\frac{1}{2}$ o/w

We introduce a **new formulation** of **QIND-CCA2**: like **QAE**, but for ideal decryption:

Background: QIND-CCA2 security of QSE

[Alagic et al. 2018]: compare the performance of adversary in two different games:

- **Test**: quantum version of single-challenge **IND-CCA2**, but w/o checks upon decryption
- **Fake**: same but always encrypt a fixed plaintext; lose if cheat, win with prob. $\frac{1}{2}$ o/w

We introduce a new formulation of **QIND-CCA2**: like **QAE**, but for ideal decryption:

```
oracle IdealDec_K(σ)
    register M̃_0 ← Dec_K(σ)
    if [M̃_0, M_1] ≡ |Φ+⟩ then
        return P
    return |⊥⟩
```

$$\begin{aligned}&\textbf{oracle } \mathbf{IdealDec}_K(\sigma)\\&\quad \textbf{register } \tilde{M}_0 \leftarrow \mathbf{Dec}_K(\sigma)\\&\quad \textbf{if } [\tilde{M}_0, M_1] \equiv |\mathbf{\Phi}^+\rangle \textbf{ then}\\&\qquad \textbf{return } P\\&\quad \textbf{return } |\bot\rangle\end{aligned}$$

(Simplified for 1 message)

Background: QIND-CCA2 security of QSE

[Alagic et al. 2018]: compare the performance of adversary in two different games:

- **Test**: quantum version of single-challenge **IND-CCA2**, but w/o checks upon decryption
- **Fake**: same but always encrypt a fixed plaintext; lose if cheat, win with prob. $\frac{1}{2}$ o/w

We introduce a **new formulation** of **QIND-CCA2**: like **QAE**, but for ideal decryption:

oracle $\mathbf{IdealDec}_K(\sigma)$
  register $\tilde{M}_0 \leftarrow \mathbf{Dec}_K(\sigma)$
  if $[\tilde{M}_0, M_1] \equiv |\mathbf{\Phi}^+\rangle$ **then**
    return P
  ~~**return** $|\bot\rangle$~~
  return $\tilde{M}_0$

(Simplified for 1 message)

Background: QIND-CCA2 security of QSE

[Alagic et al. 2018]: compare the performance of adversary in two different games:

- **Test**: quantum version of single-challenge **IND-CCA2**, but w/o checks upon decryption
- **Fake**: same but always encrypt a fixed plaintext; lose if cheat, win with prob. $\frac{1}{2}$ o/w

We introduce a **new formulation** of **QIND-CCA2**: like **QAE**, but for ideal decryption:

oracle $\mathbf{IdealDec}_K(\sigma)$
  register $\tilde{M}_0 \leftarrow \mathbf{Dec}_K(\sigma)$
  if $[\tilde{M}_0, M_1] \equiv |\mathbf{\Phi}^+\rangle$ **then**
    return P
  ~~**return** $|\bot\rangle$~~
  return $\tilde{M}_0$

(Simplified for 1 message)

$\Longrightarrow$ This is **QROR-CCA2** (**ROR** = real-or-random)

Background: QIND-CCA2 security of QSE

[Alagic et al. 2018]: compare the performance of adversary in two different games:

- **Test**: quantum version of single-challenge **IND-CCA2**, but w/o checks upon decryption
- **Fake**: same but always encrypt a fixed plaintext; lose if cheat, win with prob. $\frac{1}{2}$ o/w

We introduce a **new formulation** of **QIND-CCA2**: like **QAE**, but for ideal decryption:

oracle $\mathbf{IdealDec}_K(\sigma)$
  register $\tilde{M}_0 \leftarrow \mathbf{Dec}_K(\sigma)$
  if $[\tilde{M}_0, M_1] \equiv |\mathbf{\Phi}^+\rangle$ **then**
    return P
  ~~**return** $|\perp\rangle$~~
  return $\tilde{M}_0$

(Simplified for 1 message)

$\Longrightarrow$ This is **QROR-CCA2** (**ROR** = real-or-random)

$\Longrightarrow$ It is possible to relate the two notions

Our contribution

Our contribution

But this notions are not composable! We use the **Constructive Cryptography** framework [Maurer and Renner, 2011].

Our contribution

But this notions are not composable! We use the **Constructive Cryptography** framework [Maurer and Renner, 2011].

This provides:

Our contribution

But this notions are not composable! We use the **Constructive Cryptography** framework [Maurer and Renner, 2011].

This provides:

- **Operational interpretation**: define right scope of use of a primitive

Our contribution

But this notions are not composable! We use the **Constructive Cryptography** framework [Maurer and Renner, 2011].

This provides:

- **Operational interpretation**: define right scope of use of a primitive
- **Abstraction:** security/confidentiality definitions for arbitrary protocols, not only QSE!

Our contribution

But this notions are not composable! We use the **Constructive Cryptography** framework [Maurer and Renner, 2011].

This provides:

- **Operational interpretation**: define right scope of use of a primitive
- **Abstraction:** security/confidentiality definitions for arbitrary protocols, not only QSE!
- **Composability**: prove different components security in isolation, reuse in any context

Our contribution

But this notions are not composable! We use the **Constructive Cryptography** framework [Maurer and Renner, 2011].

This provides:

- **Operational interpretation**: define right scope of use of a primitive
- **Abstraction:** security/confidentiality definitions for arbitrary protocols, not only QSE!
- **Composability**: prove different components security in isolation, reuse in any context
- **Finite statements:** concrete reductions to hardness assumptions

Our contribution

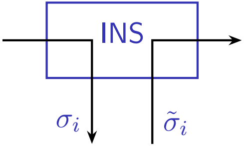
But this notions are not composable! We use the **Constructive Cryptography** framework [Maurer and Renner, 2011].

This provides:

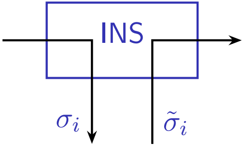
- **Operational interpretation**: define right scope of use of a primitive
- **Abstraction:** security/confidentiality definitions for arbitrary protocols, not only QSE!
- **Composability**: prove different components security in isolation, reuse in any context
- **Finite statements:** concrete reductions to hardness assumptions
    - Crucial for real-world implementations, appreciated by the Experimental QCrypt community

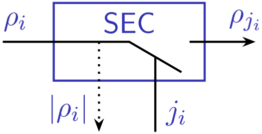
Composable security (= confidentiality + authenticity)

Composable security (= confidentiality + authenticity)

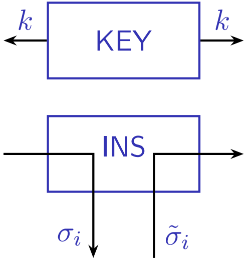


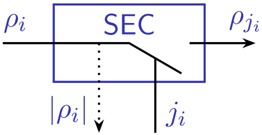
Composable security (= confidentiality + authenticity)



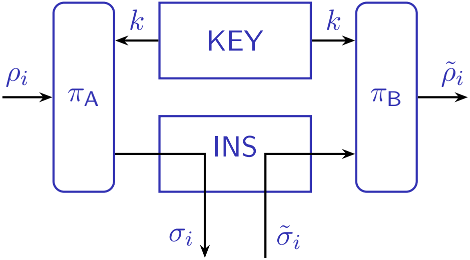


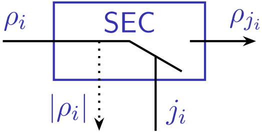
Composable security (= confidentiality + authenticity)



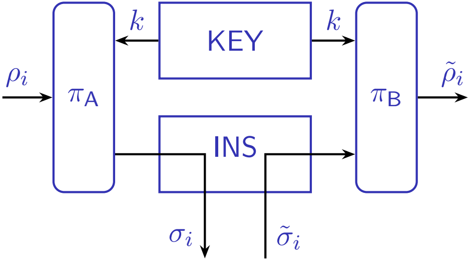


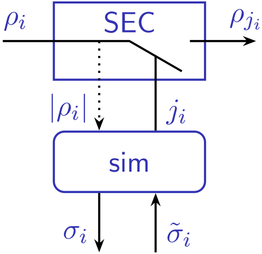
Composable security (= confidentiality + authenticity)



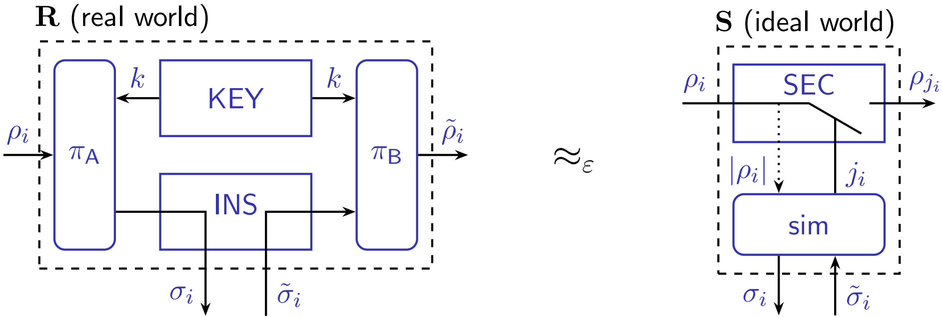


Composable security (= confidentiality + authenticity)

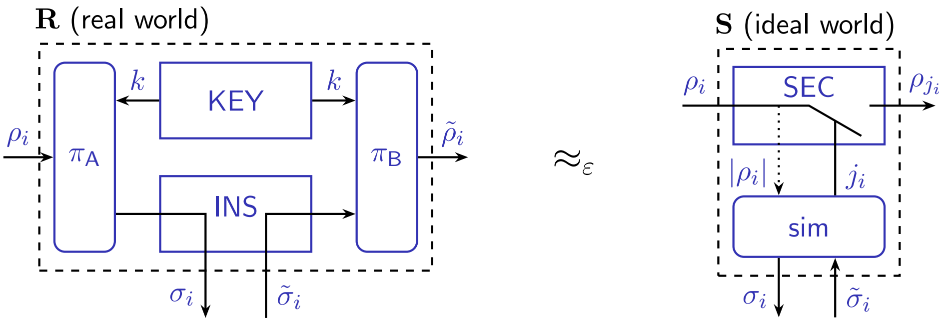




Composable security (= confidentiality + authenticity)



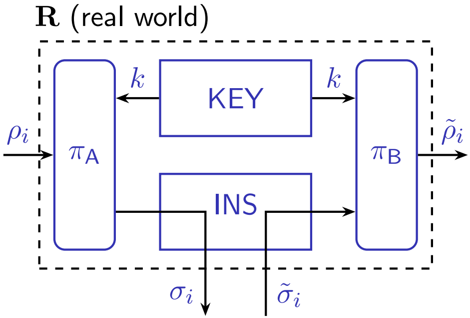
Composable security (= confidentiality + authenticity)



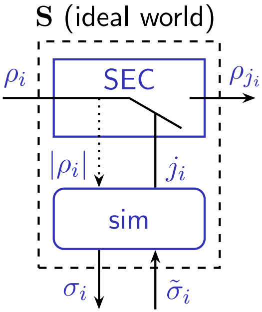
Definition

$\boldsymbol{\pi} := (\pi_A, \pi_B)$ *ε-secure*

Composable security (= confidentiality + authenticity)



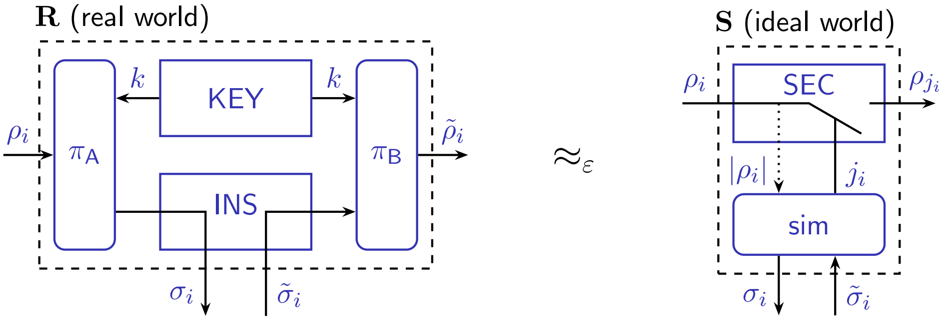
$\approx_\varepsilon$



Definition

$$\boldsymbol{\pi} := (\pi_A, \pi_B)\ \varepsilon\text{-secure} \quad :\Longleftrightarrow \quad [\text{KEY}, \text{INS}] \xrightarrow{\boldsymbol{\pi}, \varepsilon} \text{SEC}$$

Composable security (= confidentiality + authenticity)

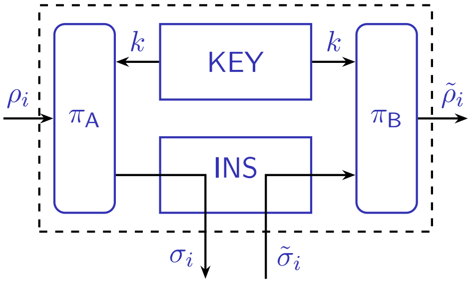


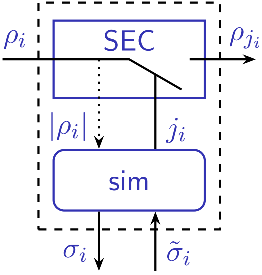
Definition

$\boldsymbol{\pi} := (\pi_A, \pi_B)$ *ε-secure* $\quad :\Longleftrightarrow \quad [\text{KEY}, \text{INS}] \xrightarrow{\boldsymbol{\pi},\varepsilon} \text{SEC} \quad :\Longleftrightarrow \quad \exists\,\text{sim} : \mathbf{R} \approx_\varepsilon \mathbf{S}$

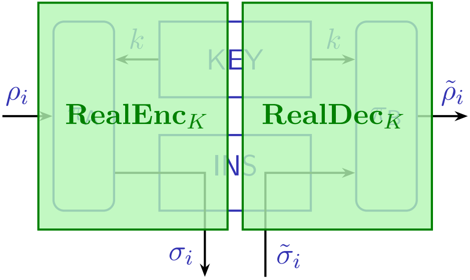
Comparing QAE and composable security of QSE

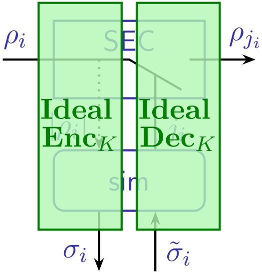
Comparing QAE and composable security of QSE



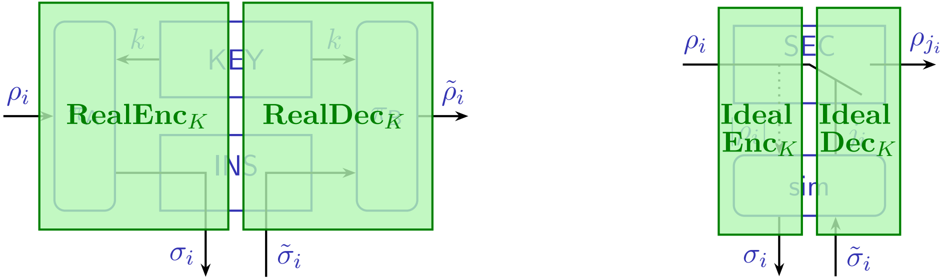


Comparing QAE and composable security of QSE





Comparing QAE and composable security of QSE



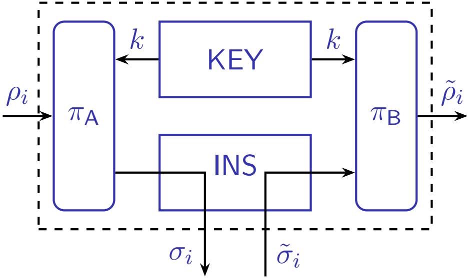
Theorem

QAE is *composable security (conf. + auth.)* with a simulator hard-coded.

Recall: composable security (= confidentiality + authenticity)

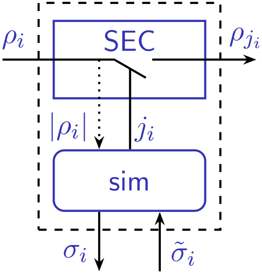
Recall: composable security (= confidentiality + authenticity)

$\mathbf{R}$ (real world)



$\approx_\varepsilon$

$\mathbf{S}$ (ideal world)

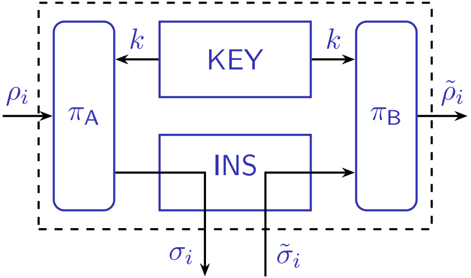


Definition

$$\boldsymbol{\pi} := (\pi_{\mathsf{A}}, \pi_{\mathsf{B}}) \ \varepsilon\text{-secure} \quad :\Longleftrightarrow \quad [\mathsf{KEY}, \mathsf{INS}] \xrightarrow{\boldsymbol{\pi},\varepsilon} \mathsf{SEC} \quad :\Longleftrightarrow \quad \exists\, \mathsf{sim} : \mathbf{R} \approx_\varepsilon \mathbf{S}$$

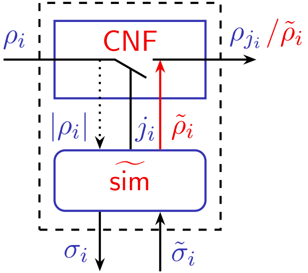
Recall: **composable** security (= **confidentiality** + authenticity)

$\mathbf{R}$ (real world)



$\approx_\varepsilon$

$\widetilde{\mathbf{S}}$ (ideal world)

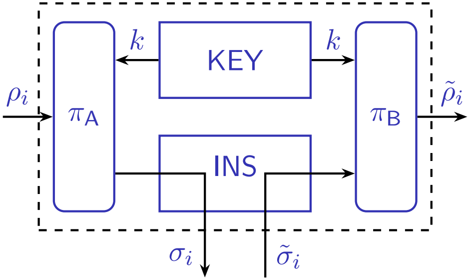


Definition

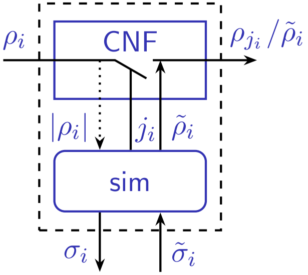
$$\boldsymbol{\pi} := (\pi_A, \pi_B)\ \varepsilon\text{-conf.} \quad :\Longleftrightarrow \quad [\text{KEY}, \text{INS}] \xrightarrow{\boldsymbol{\pi},\varepsilon} \text{CNF} \quad :\Longleftrightarrow \quad \exists\, \widetilde{\text{sim}} : \mathbf{R} \approx_\varepsilon \widetilde{\mathbf{S}}$$

Comparing QROR-CCA2 and composable confidentiality of QSE

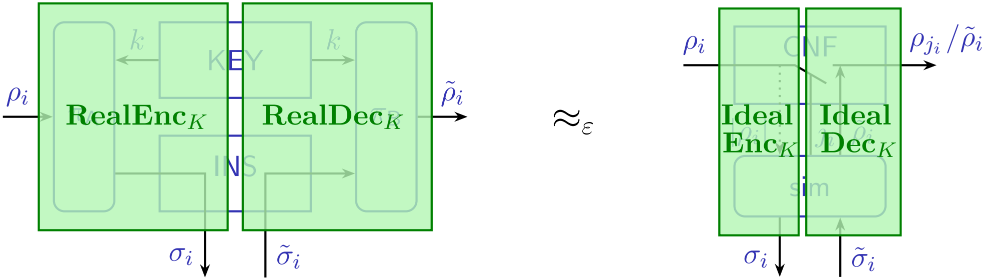
Comparing QROR-CCA2 and composable confidentiality of QSE



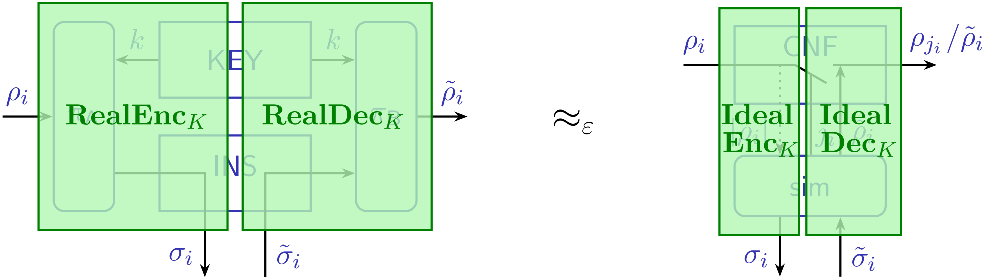
$\approx_\varepsilon$



Comparing QROR-CCA2 and composable confidentiality of QSE



Comparing QROR-CCA2 and composable confidentiality of QSE



Theorem

QCCA2 is *composable confidentiality* with a simulator hard-coded.

The End