Computational Security of Quantum Encryption

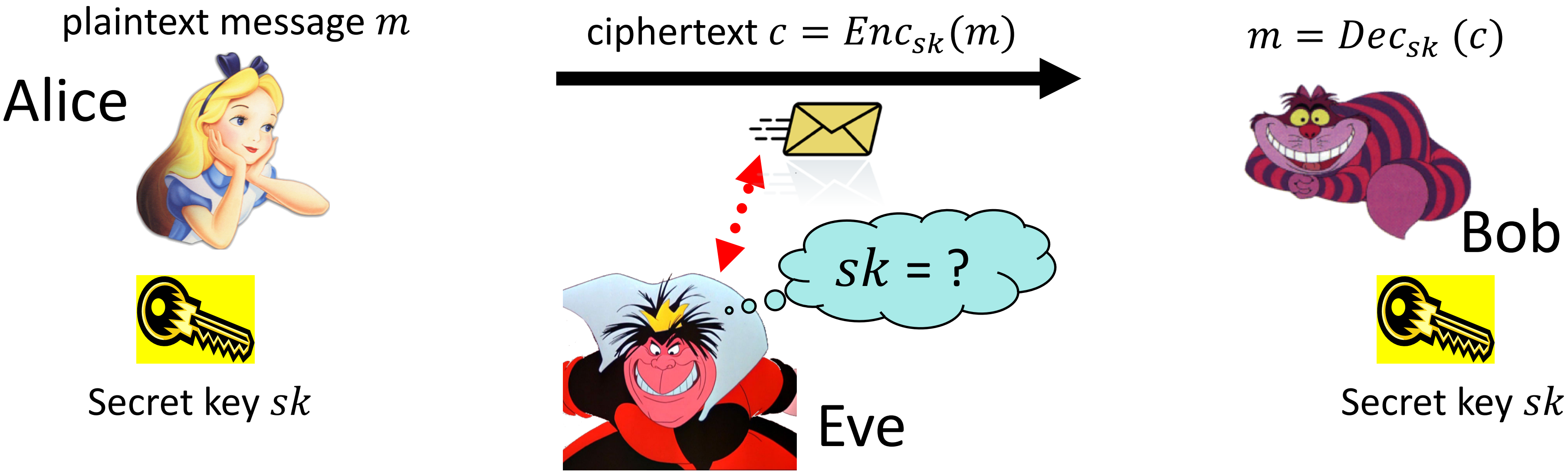
http://arxiv.org/abs/1602.01441

GORJAN ALAGIC, COPENHAGEN
ANNE BROADBENT, OTTAWA
BILL FEFFERMAN, MARYLAND
TOMMASO GAGLIARDONI, DARMSTADT
MICHAEL ST JULES, OTTAWA

CHRISTIAN SCHAFFNER,
AMSTERDAM

QCrypt 2016. Friday, September 16, 2016. Washington DC, USA

Secure Encryption



plaintext message m

Alice

Secret key sk

ciphertext $c = Enc_{sk}(m)$

sk = ?

Eve

$m = Dec_{sk}(c)$

Bob

Secret key sk

One-Time Pad:

- Classical: $c = Enc_{sk}(m) := m \oplus sk$, $Dec_{sk}(c) := c \oplus sk$
- Quantum: $Enc_{a,b}(\rho_M) := X^a Z^b \rho_M Z^b X^a$,
  $Dec_{a,b}(\rho_C) := X^a Z^b \rho_C Z^b X^a$

SECURE

QOTP

End of Talk

Thank you for your attention!

TECHNISCHE
UNIVERSITÄT
DARMSTADT

Cryptoplexity
Cryptography & Complexity Theory
Technische Universität Darmstadt
www.cryptoplexity.de

cost
EUROPEAN COOPERATION IN SCIENCE AND TECHNOLOGY

NWO
Nederlandse Organisatie voor
Wetenschappelijk Onderzoek

CWI

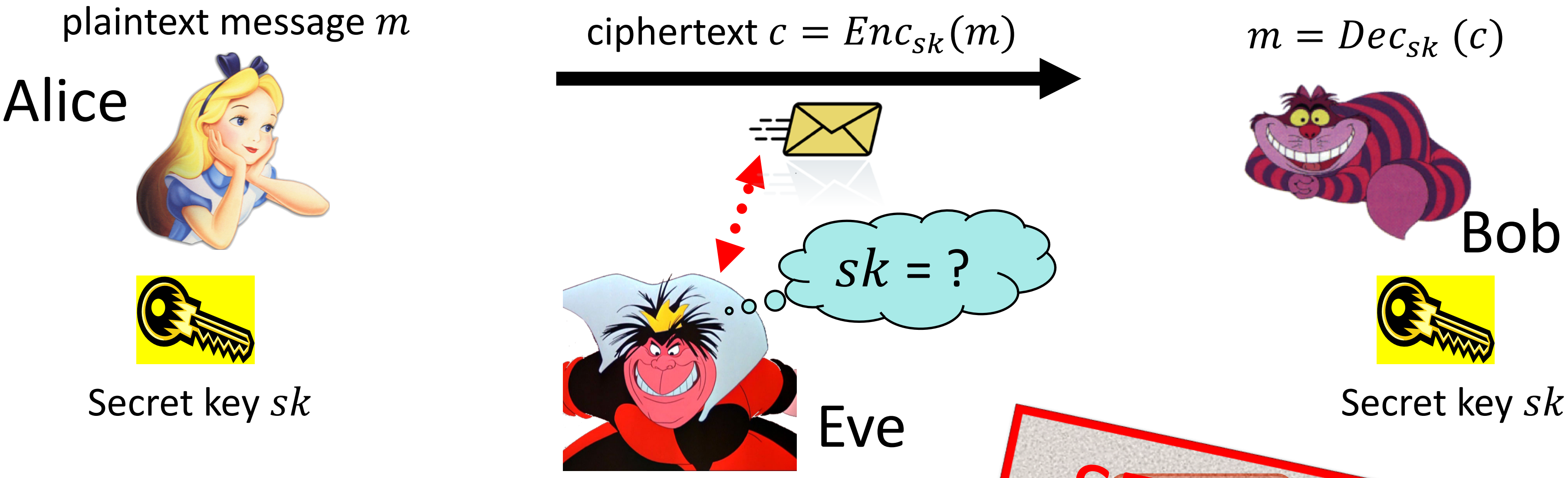
KØBENHAVNS
UNIVERSITET

uOttawa

UNIVERSITY OF
MARYLAND

QuSoft

Information-Theoretic Security



plaintext message m

Alice

ciphertext $c = Enc_{sk}(m)$

$m = Dec_{sk}\ (c)$

Bob

sk = ?

Eve

Secret key sk

Secret key sk

SECURE

OTP

Perfect / information-theoretic security:

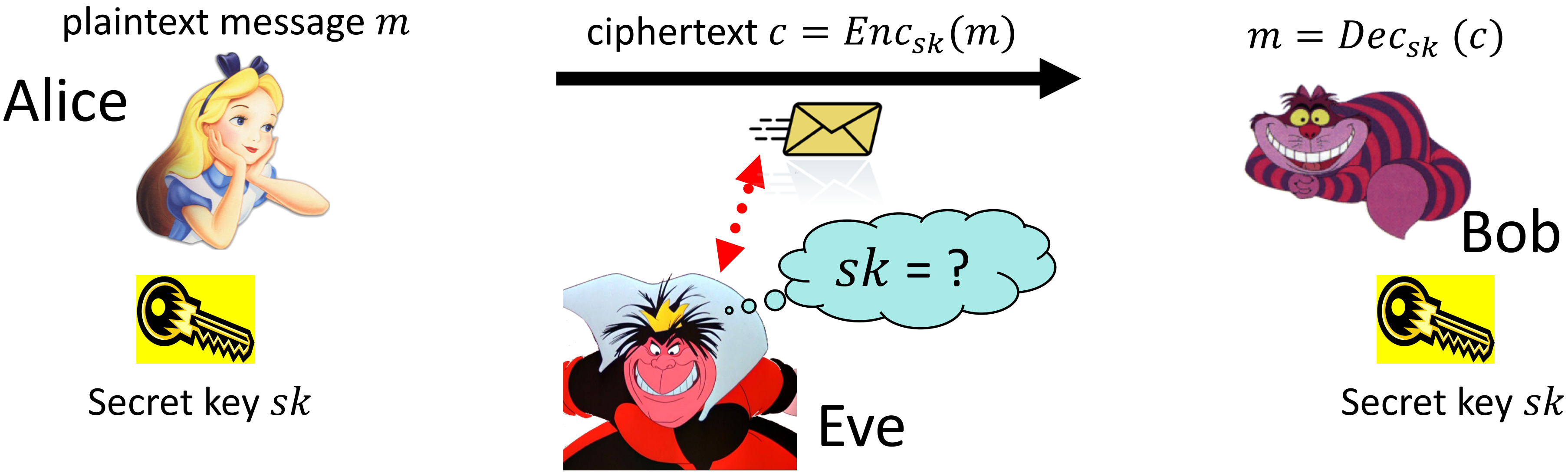
- Ciphertext distribution P_C is statistically independent of message distribution P_M.

Theorem: Secret key has to be as large as the message.

Highly impractical, e.g. for encrypting a video stream…

[Shannon 48, Dodis 12, Boykin Roychowdhury 03]

Computational Security



plaintext message m

Alice

Secret key sk

ciphertext $c = Enc_{sk}(m)$

sk = ?

Eve

$m = Dec_{sk}(c)$

Bob

Secret key sk

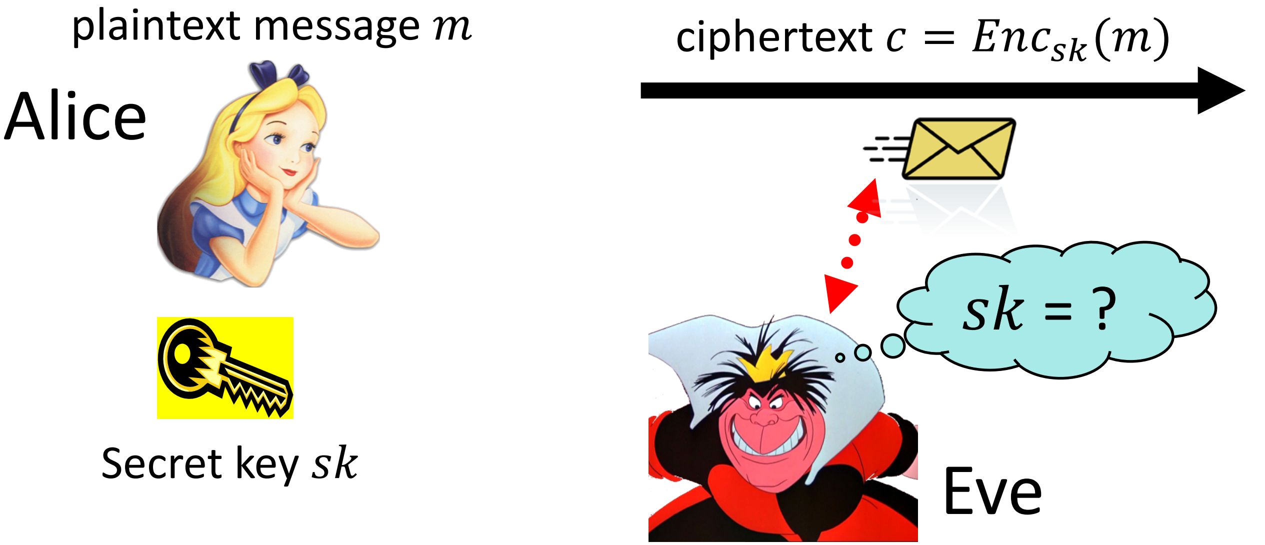
Threat model:

- Eve sees ciphertexts (eavesdropper)
- Eve knows plaintext/ciphertext pairs
- Eve chooses plaintexts to be encrypted
- Eve can decrypt ciphertexts

Security guarantee:

- c does not reveal sk
- c does not reveal the whole m
- c does not reveal any bit of m
- c does not reveal “anything” about m

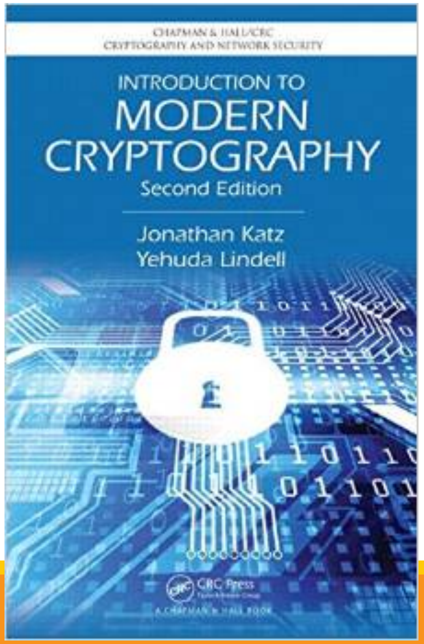
Semantic Security



DEFINITION 3.12 *A private-key encryption scheme* (Enc, Dec) *is* semantically secure in the presence of an eavesdropper *if for every* PPT *algorithm $\mathcal{A}$ there exists a* PPT *algorithm $\mathcal{A}'$ such that for any* PPT *algorithm* Samp *and polynomial-time computable functions f and h, the following is negligible:*

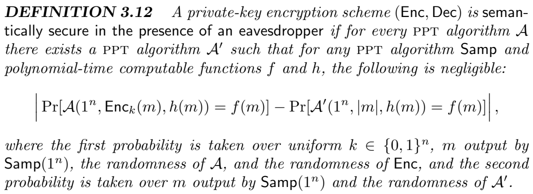
$$\left| \Pr[\mathcal{A}(1^n, \mathsf{Enc}_k(m), h(m)) = f(m)] - \Pr[\mathcal{A}'(1^n, |m|, h(m)) = f(m)] \right|,$$

where the first probability is taken over uniform $k \in \{0,1\}^n$, m output by $\mathsf{Samp}(1^n)$*, the randomness of $\mathcal{A}$, and the randomness of* Enc*, and the second probability is taken over m output by* $\mathsf{Samp}(1^n)$ *and the randomness of $\mathcal{A}'$.*



[Goldwasser Micali 84]

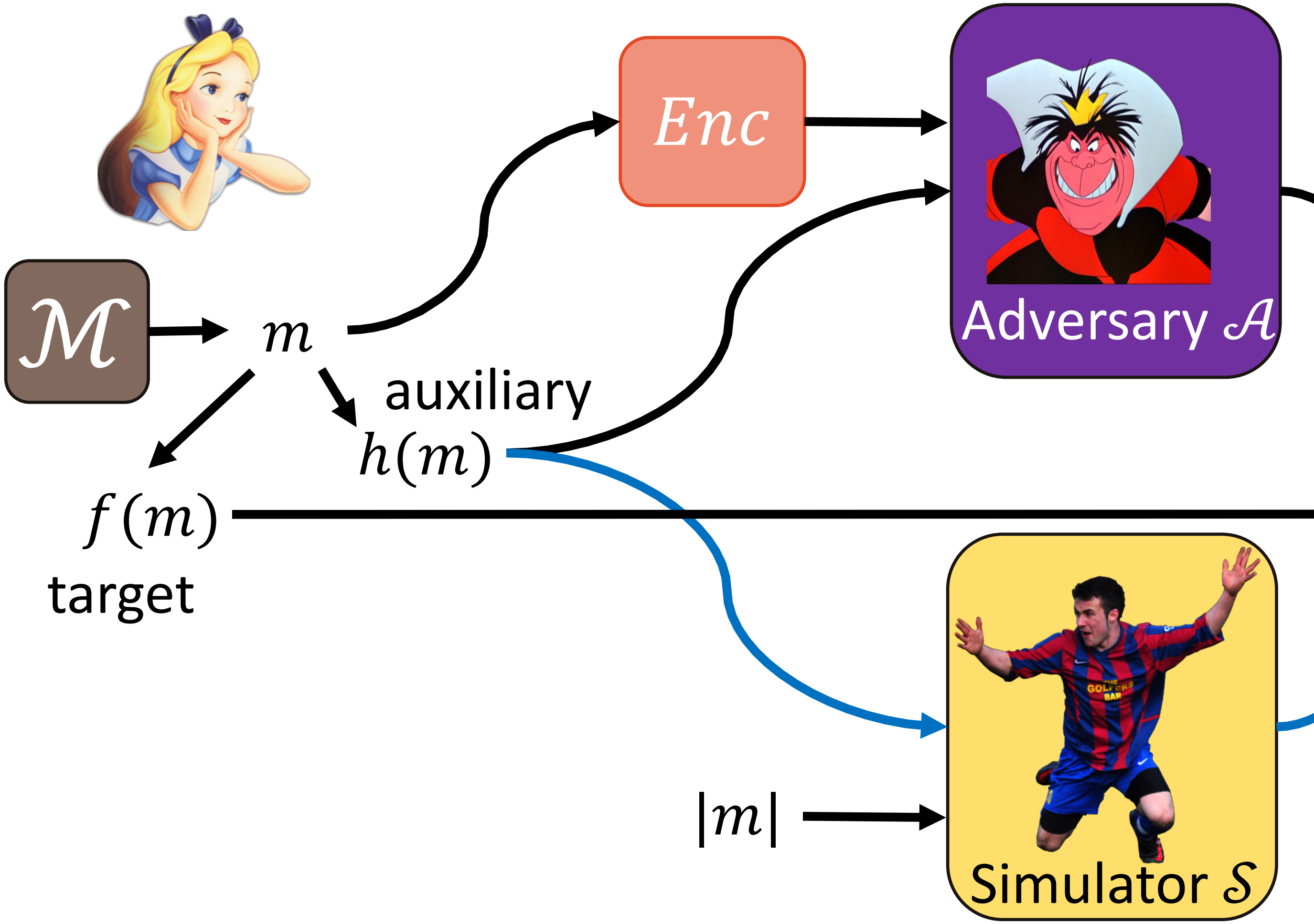
Classical Semantic Security

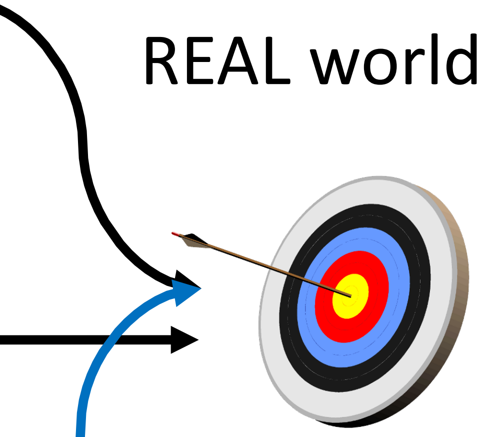


DEFINITION 3.12 *A private-key encryption scheme* (Enc, Dec) *is* semantically secure in the presence of an eavesdropper *if for every* PPT *algorithm $\mathcal{A}$ there exists a* PPT *algorithm $\mathcal{A}'$ such that for any* PPT *algorithm* Samp *and polynomial-time computable functions f and h, the following is negligible:*

$$\left|\Pr[\mathcal{A}(1^n, \mathsf{Enc}_k(m), h(m)) = f(m)] - \Pr[\mathcal{A}'(1^n, |m|, h(m)) = f(m)]\right|,$$

where the first probability is taken over uniform $k \in \{0,1\}^n$, m output by Samp(1^n)*, the randomness of $\mathcal{A}$, and the randomness of* Enc*, and the second probability is taken over m output by* Samp(1^n) *and the randomness of $\mathcal{A}'$.*





REAL world

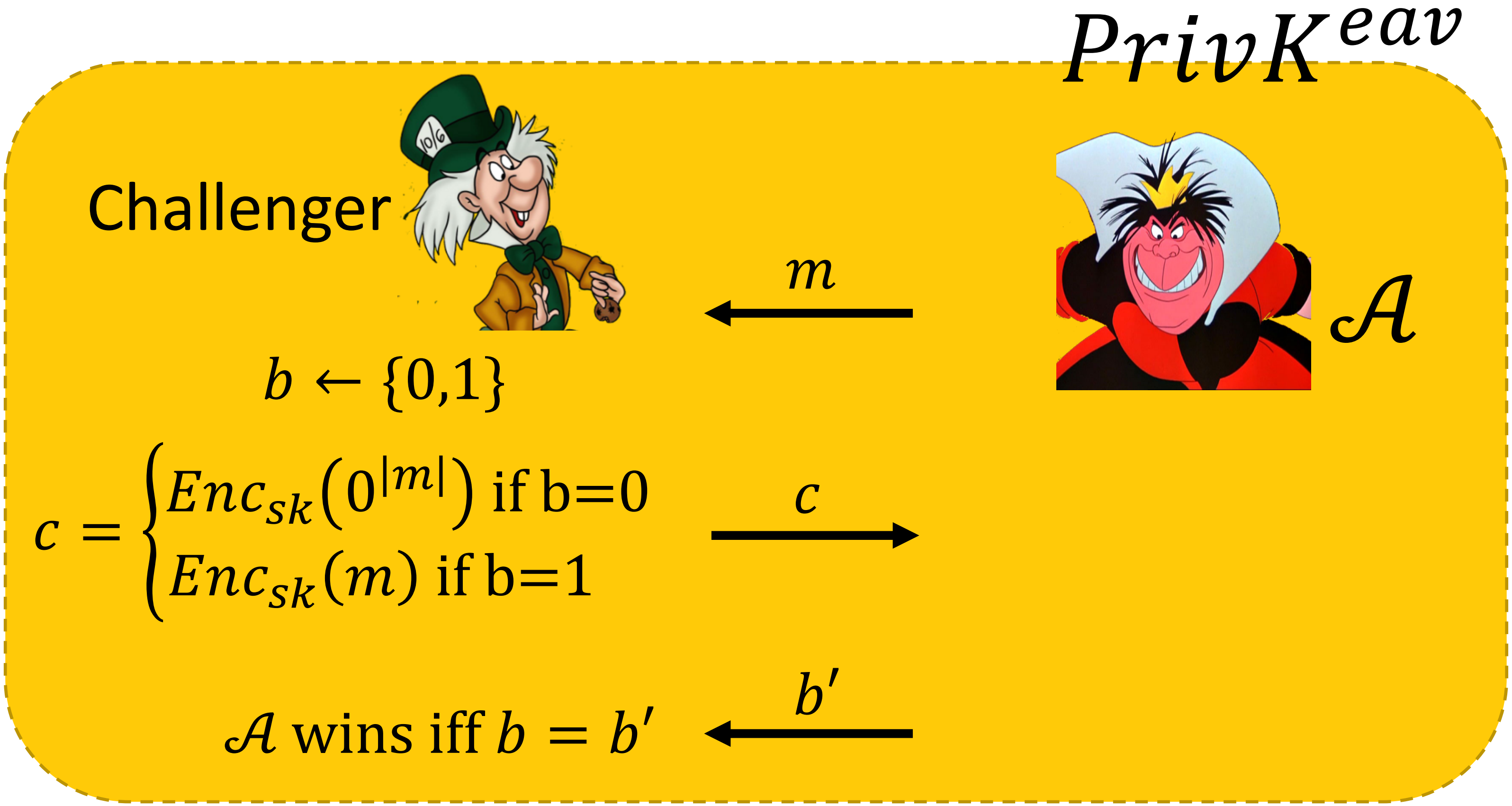
IDEAL world

Definition (SEM): $\forall \mathcal{A}\ \exists \mathcal{S} : \forall (\mathcal{M}, h, f)$

$$\Pr[\mathcal{A}(Enc_k(m), h(m)) = f(m)] \approx \Pr[\mathcal{S}(|m|, h(m)) = f(m)]$$

[Goldwasser Micali 84]

Classical Indistinguishability



$PrivK^{eav}$

Challenger

$\xleftarrow{m}$

$\mathcal{A}$

$b \leftarrow \{0,1\}$

$$c = \begin{cases} Enc_{sk}\left(0^{|m|}\right) \text{ if b=0} \\ Enc_{sk}(m) \text{ if b=1} \end{cases}$$

$\xrightarrow{c}$

$\mathcal{A}$ wins iff $b = b'$

$\xleftarrow{b'}$

Definition (IND): $\forall \mathcal{A}\colon\ \Pr[\mathcal{A} \text{ wins } PrivK^{eav}] \leq \frac{1}{2} + \ negl(n)$

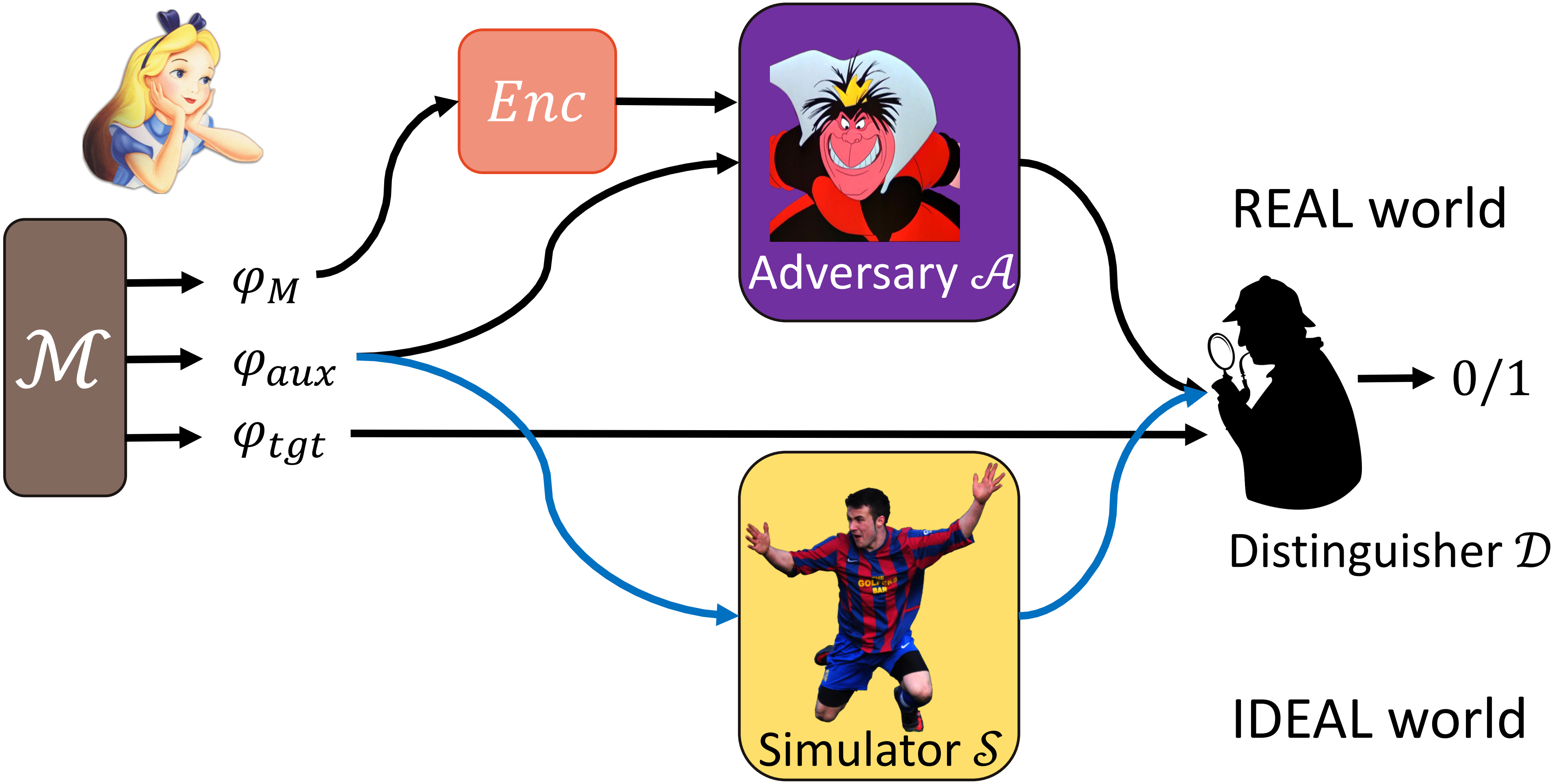
Theorem: SEM ⇔ IND

[Goldwasser Micali 84]

Our Contributions

1. Formal definition of Quantum Semantic Security
2. Equivalence to Quantum Indistinguishability
3. Extension to CPA and CCA1 scenarios
4. Construction of IND-CCA1 Quantum Secret-Key Encryption from Post-Quantum One-Way Functions
5. Construction of Quantum Public-Key Encryption from Post-Quantum One-Way Trapdoor Permutations

Quantum Semantic Security



Enc

Adversary $\mathcal{A}$

REAL world

$\mathcal{M}$

φ_M

φ_{aux}

φ_{tgt}

0/1

Distinguisher $\mathcal{D}$

Simulator $\mathcal{S}$

IDEAL world

Definition (QSEM): $\forall \mathcal{A}\ \exists \mathcal{S}\ \forall (\mathcal{M}, \mathcal{D})$:

$$\Pr[\mathcal{D}(\mathrm{REAL}) = 1] \approx \Pr[\mathcal{D}(\mathrm{IDEAL}) = 1]$$

Quantum Indistinguishability

$QPrivK^{eav}$

Challenger

$\xleftarrow{\rho_M}$

$\mathcal{A}$

$b \leftarrow \{0,1\}$

$$\rho_C = \begin{cases} Enc_{sk}(|0\rangle) \text{ if b=0} \\ Enc_{sk}(\rho_M) \text{ if b=1} \end{cases} \xrightarrow{\rho_C}$$

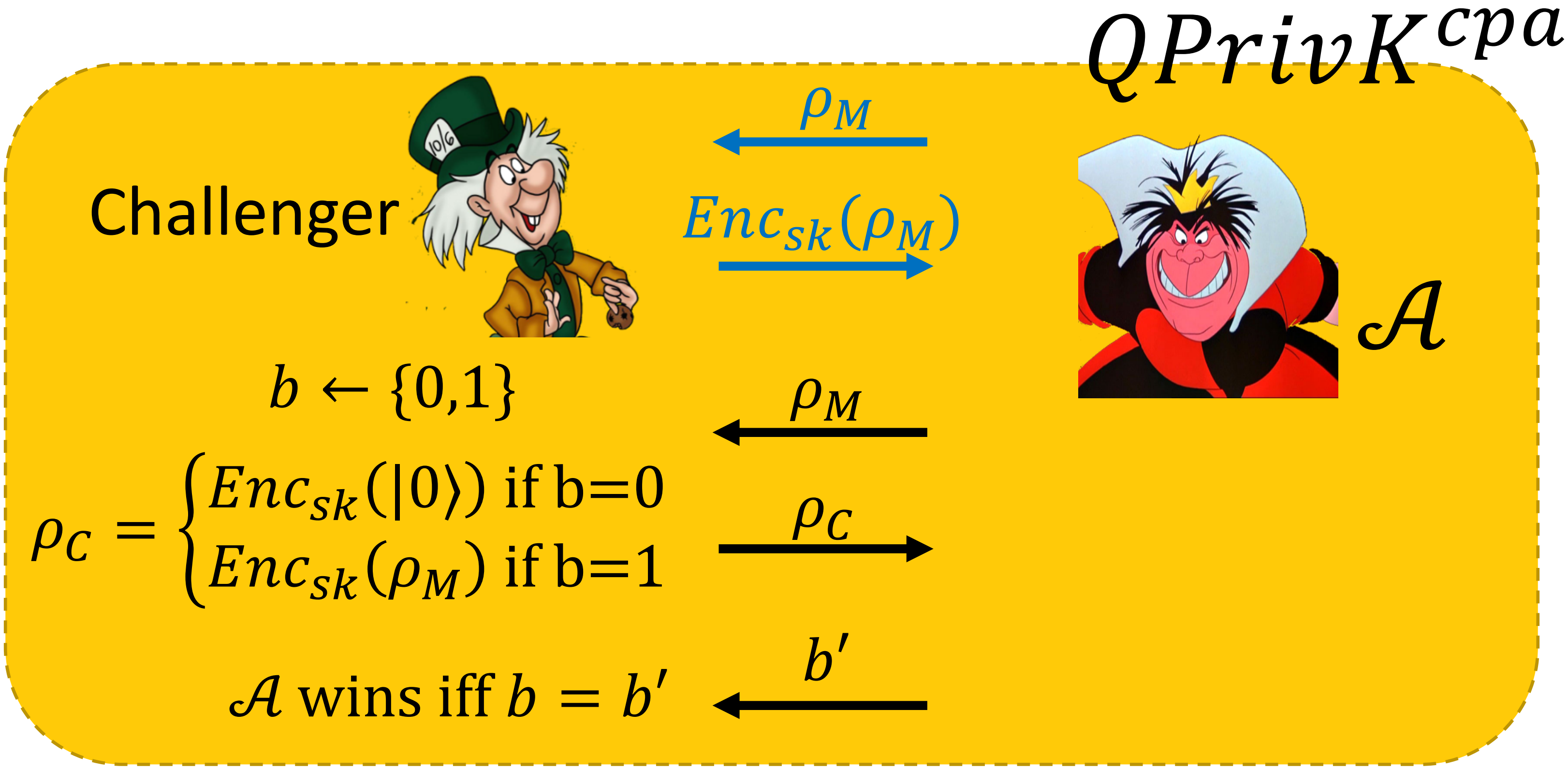
$\mathcal{A}$ wins iff $b = b'$ $\xleftarrow{b'}$

Definition (QIND): $\forall \mathcal{A}\text{:}\ \Pr[\mathcal{A} \text{ wins } QPrivK^{eav}] \leq \frac{1}{2} + negl(n)$

Theorem: QSEM ⇔ QIND

QIND: [Broadbent Jeffery 15, Gagliardoni Huelsing Schaffner 16]

Chosen-Plaintext Attacks (CPA)



$QPrivK^{cpa}$

Challenger

$\xleftarrow{\rho_M}$

$\xrightarrow{Enc_{sk}(\rho_M)}$

$\mathcal{A}$

$b \leftarrow \{0,1\}$

$\xleftarrow{\rho_M}$

$$\rho_C = \begin{cases} Enc_{sk}(|0\rangle) \text{ if b=0} \\ Enc_{sk}(\rho_M) \text{ if b=1} \end{cases}$$

$\xrightarrow{\rho_C}$

$\xleftarrow{b'}$

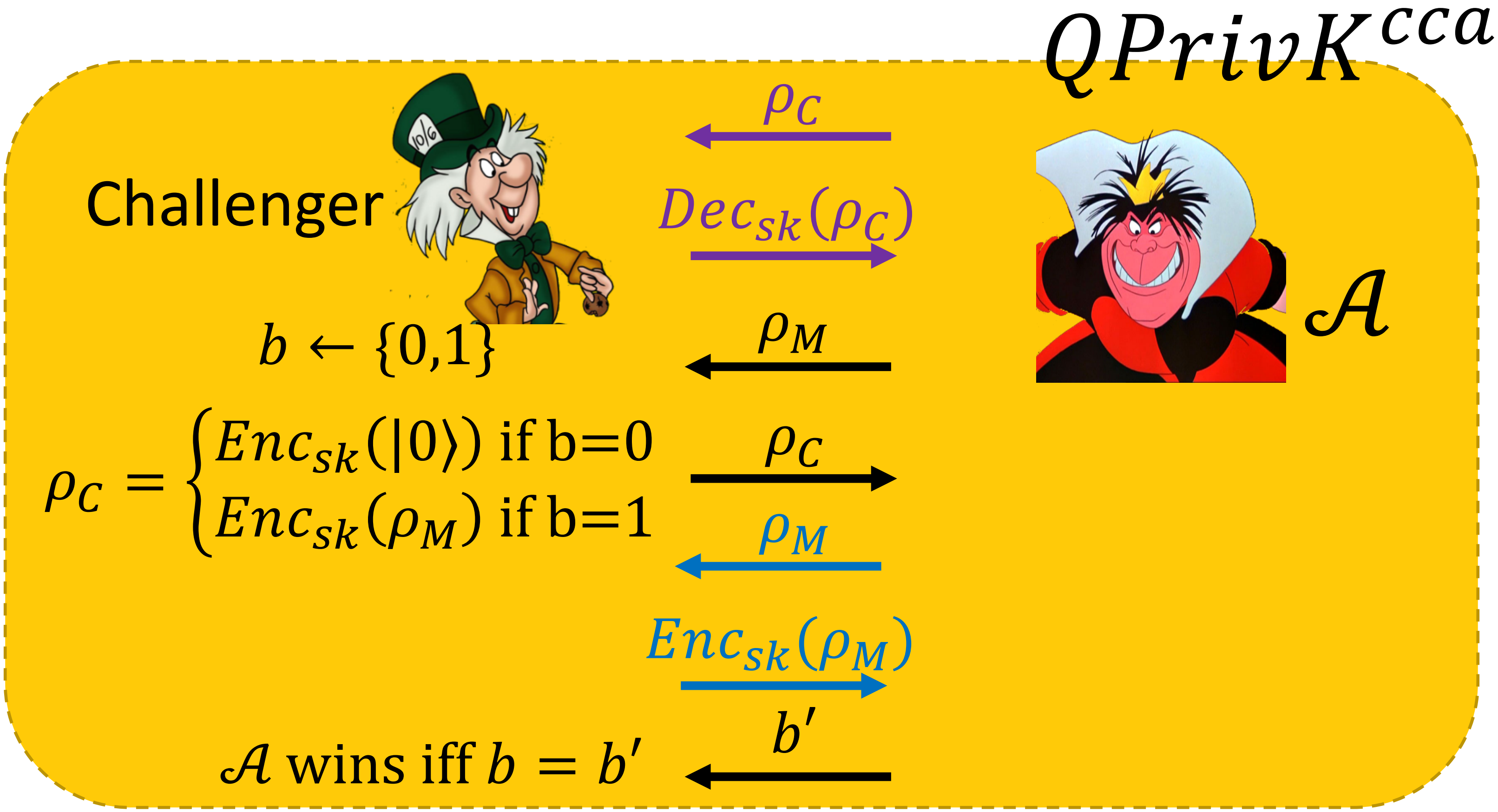
$\mathcal{A}$ wins iff $b = b'$

Definition (QIND-CPA): $\forall \mathcal{A}\colon \Pr[\mathcal{A} \text{ wins } QPrivK^{cpa}] \leq \frac{1}{2} + negl(n)$

Theorem: QSEM-CPA ⇔ QIND-CPA

Fact: CPA security requires **randomized encryption**

Chosen-Ciphertext Attacks (CCA1)



$QPrivK^{cca}$

Challenger

$\mathcal{A}$

$\xleftarrow{\rho_C}$

$\xrightarrow{Dec_{sk}(\rho_C)}$

$b \leftarrow \{0,1\}$

$\xleftarrow{\rho_M}$

$$\rho_C = \begin{cases} Enc_{sk}(|0\rangle) \text{ if b=0} \\ Enc_{sk}(\rho_M) \text{ if b=1} \end{cases}$$

$\xrightarrow{\rho_C}$

$\xleftarrow{\rho_M}$

$\xrightarrow{Enc_{sk}(\rho_M)}$

$\mathcal{A}$ wins iff $b = b'$ $\xleftarrow{b'}$

Definition (QIND-CCA1): $\forall \mathcal{A}\colon \ \Pr[\mathcal{A} \text{ wins } QPrivK^{cca}] \leq \frac{1}{2} + \ negl(n)$

Theorem: QSEM-CCA1 $\Leftrightarrow$ QIND-CCA1

Fact: QSEM-CCA1 $\overset{\neq}{\Rightarrow}$ QIND-CPA $\overset{\neq}{\Rightarrow}$ QIND

Our Contributions

✓Formal definition of Quantum Semantic Security

✓Equivalence to Quantum Indistinguishability

✓Extension to CPA and CCA1 scenarios

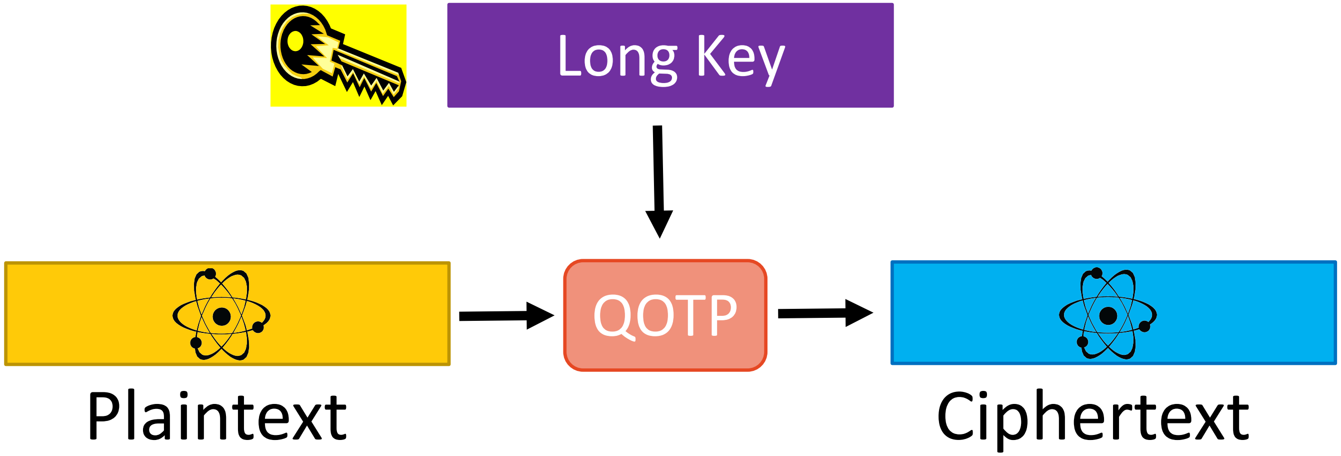
4. Construction of IND-CCA1 Quantum Secret-Key Encryption from Post-Quantum One-Way Functions
5. Construction of Quantum Public-Key Encryption from Post-Quantum One-Way Trapdoor Permutations

Quantum Secret-Key Encryption

Goal: build CCA1-secure quantum secret-key encryption

Ingredients:

- quantum one-time pad (QOTP)



Long Key

QOTP

Plaintext

Ciphertext

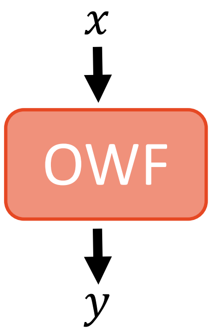
Not even CPA secure, scheme is not randomized!

Quantum Secret-Key Encryption

Goal: build CCA1-secure quantum secret-key encryption

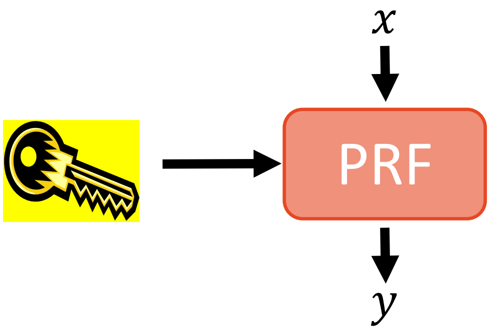
Ingredients:

- quantum one-time pad (QOTP)
- quantum-secure one-way function (OWF)

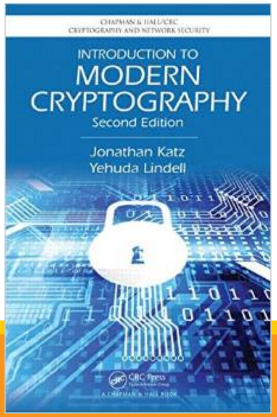


$f: x \mapsto y$ easy to compute, but hard to invert even for quantum adversaries, e.g. lattice-problems, …

Theorem: One-Way Function $\Longrightarrow$ Pseudo-Random Function



$\{f_k: x \mapsto y\}_k$ is indistinguishable from random function if key k is unknown


CHAPMAN & HALL/CRC
CRYPTOGRAPHY AND NETWORK SECURITY
INTRODUCTION TO
MODERN
CRYPTOGRAPHY
Second Edition
Jonathan Katz
Yehuda Lindell

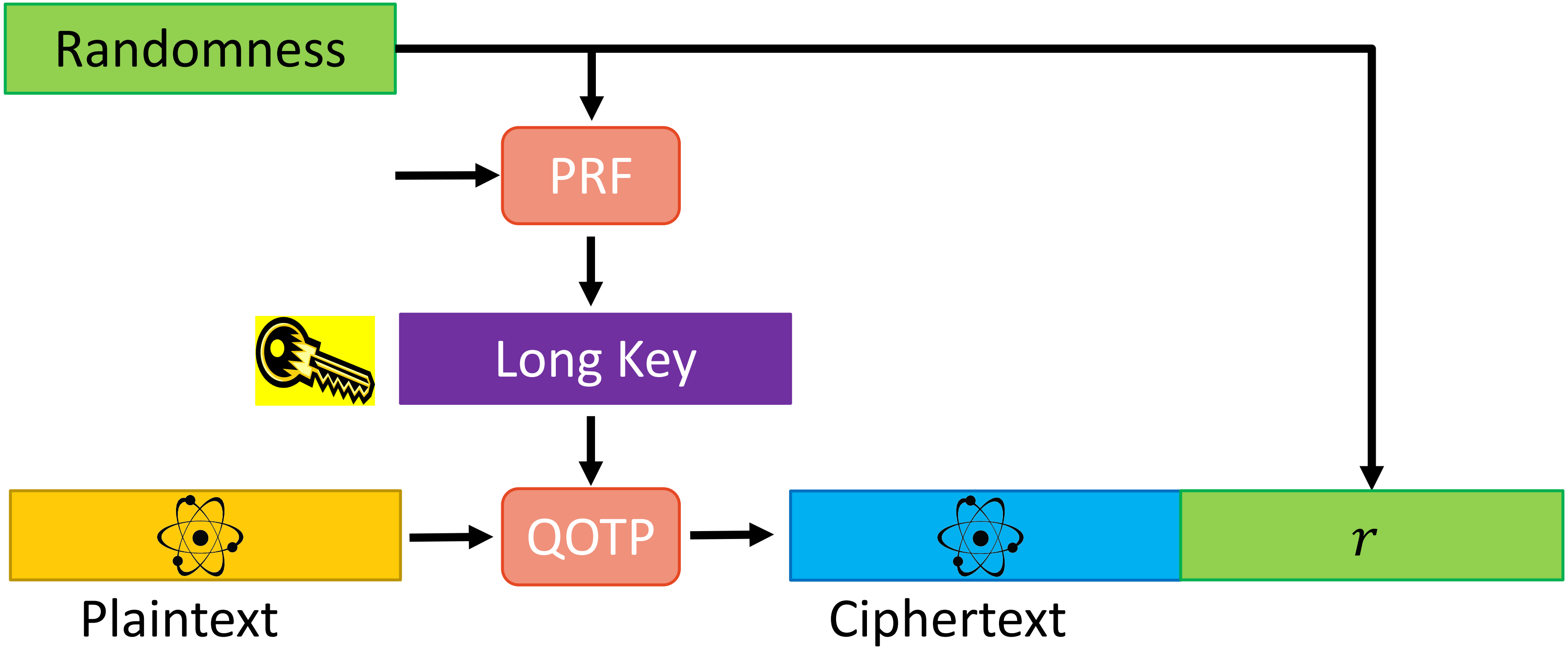
[Hastad Impagliazzo Levin Luby 99]

Quantum Secret-Key Encryption

Goal: build CCA1-secure quantum secret-key encryption

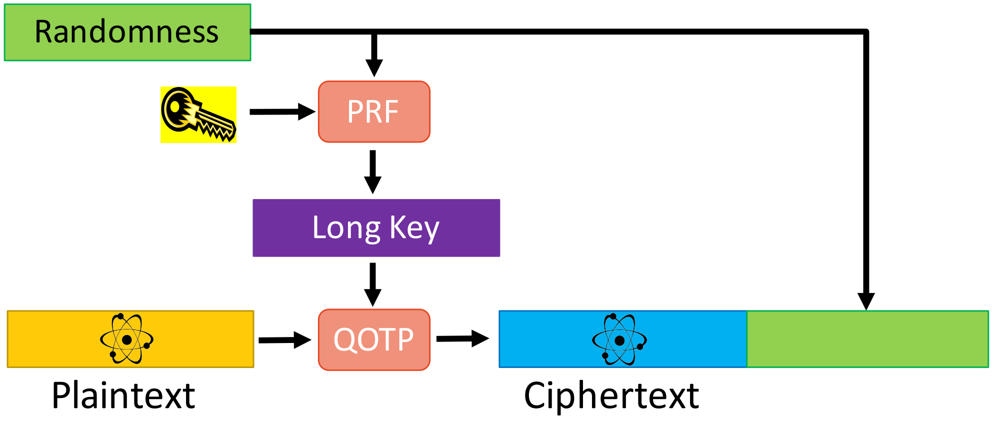
Ingredients:

- quantum one-time pad (QOTP)
- quantum-secure one-way function (OWF) $\Longrightarrow$ PRF



Classical version: [Goldreich Goldwasser Micali 85]

Intuition of CCA1 security


Randomness

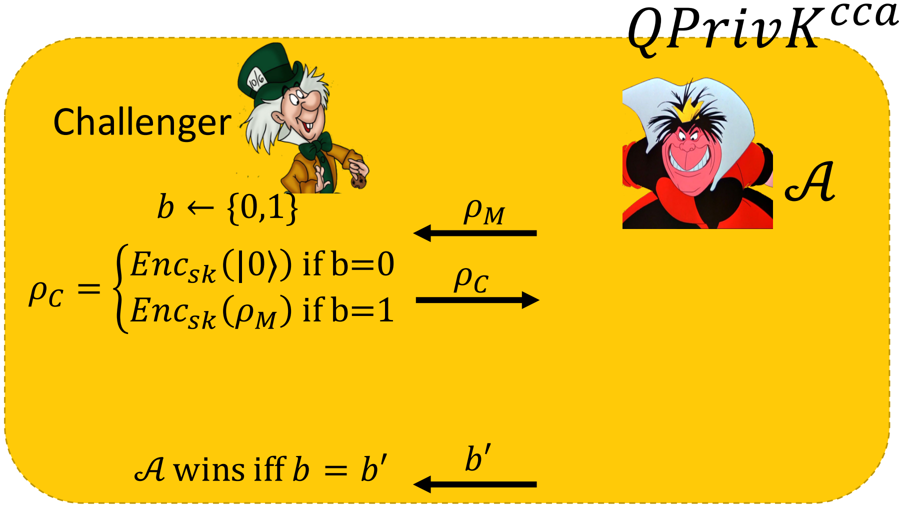
PRF

Long Key

QOTP

Plaintext

Ciphertext


$QPrivK^{cca}$

Challenger

$\mathcal{A}$

$b \leftarrow \{0,1\}$

ρ_M

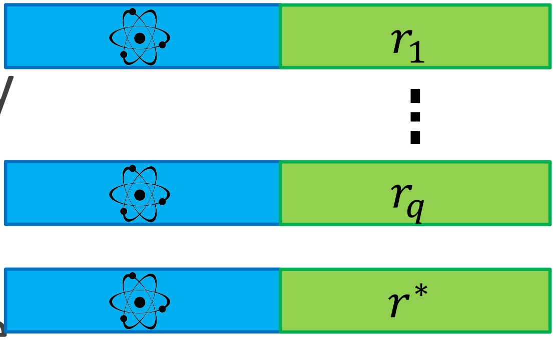
$\rho_C = \begin{cases} Enc_{sk}(|0\rangle) \text{ if b=0} \\ Enc_{sk}(\rho_M) \text{ if b=1} \end{cases}$

ρ_C

$\mathcal{A}$ wins iff $b = b'$

b'

1. Replace pseudo-random function with totally random function
2. Encryption queries result in polynomially many ciphertexts with different randomness:
3. With overwhelming probability the randomness of the challenge ciphertext will be different from previous r’s.


r_1

⋮

r_q

r^*

Conclusion and Open Questions

- ✓ Formal definition of Quantum Semantic Security
- ✓ Equivalence to Quantum Indistinguishability
- ✓ Extension to CPA and CCA1 scenarios
- ✓ Construction of IND-CCA1 Quantum Secret-Key Encryption from Post-Quantum One-Way Functions
- ✓ Construction of Quantum Public-Key Encryption from Post-Quantum One-Way Trapdoor Permutations

- How to define quantum CCA2 security?

Thank you!

http://arxiv.org/abs/1602.01441

TECHNISCHE
UNIVERSITÄT
DARMSTADT

Cryptoplexity
Cryptography & Complexity Theory
Technische Universität Darmstadt
www.cryptoplexity.de

cost
EUROPEAN COOPERATION IN SCIENCE AND TECHNOLOGY

NWO
Nederlandse Organisatie voor
Wetenschappelijk Onderzoek

CWI

KØBENHAVNS
UNIVERSITET

uOttawa

UNIVERSITY OF
MARYLAND

QuSoft

Questions

Quantum Public-Key Encryption