On Quantum Ciphertext Indistinguishability, Recoverability, and OAEP

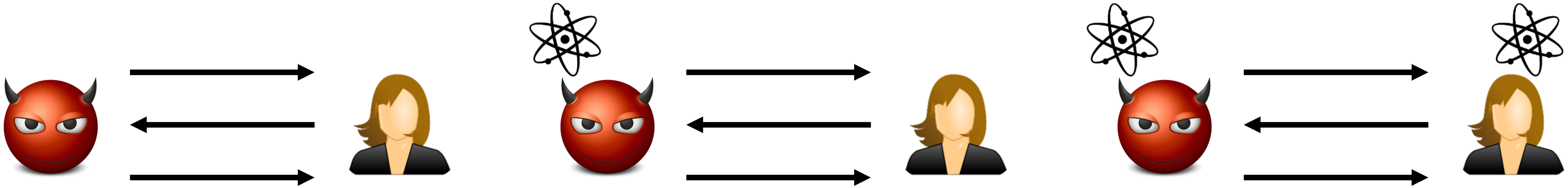
Juliane Krämer and Patrick Struck

PQCrypto 2022

Universität Regensburg

The Setting

weak → strong



Classical Security

- Only classical access to oracles

Post-Quantum Security

- Quantum access to “offline” oracles
- Classical access to “online” oracles

Quantum Security

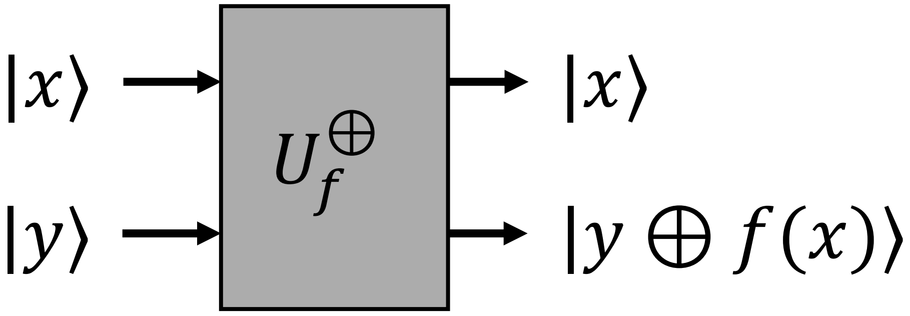
- Quantum access to “offline” oracles
- Quantum access to “online” oracles

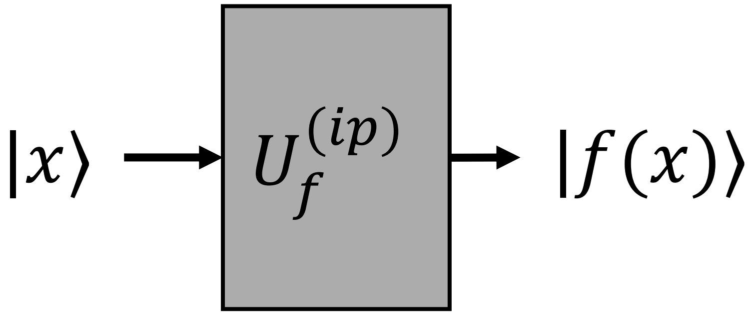
Quantum Security Notions for PKE

- 3 different security notions:
  1. INDqCCA [BZ13]
     - Classical challenges and quantum access to decryption
     - Left-or-Right
     - Always applicable
  2. qINDqCPA [CEV20]
     1. Quantum challenges
     2. Real-or-Random
     3. Always applicable
  3. qINDqCPA [GKS21]
     1. Quantum challenges
     2. Left-or-Right
     3. Not always applicable ← **Scope of this work**

[BZ13] Boneh, Zhandry. Secure signatures and chosen ciphertext security in a quantum computing world. CRYPTO 2013
[CEV20] Chevalier, Ebrahimi, Vu. On security notion for encryption in a quantum world. ePrint 2020
[GKS21] Gagliardoni, Krämer, Struck. Quantum indistinguishability for public key encryption. PQCrypto 2021

Quantum Operators



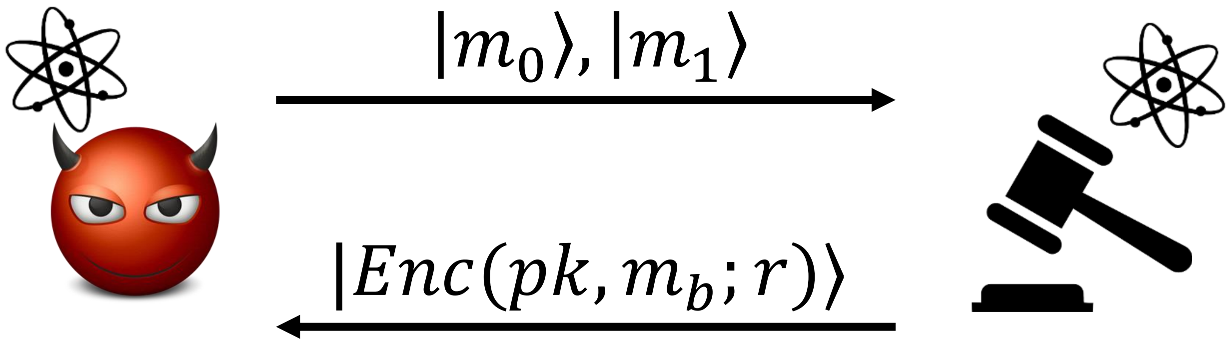


- XOR operator
  - Realisable for any f [NC16]
  - Creates entanglement

- In-place operator [KKVB02]
  - Realisable only for reversible f
  - Not always efficiently realisable

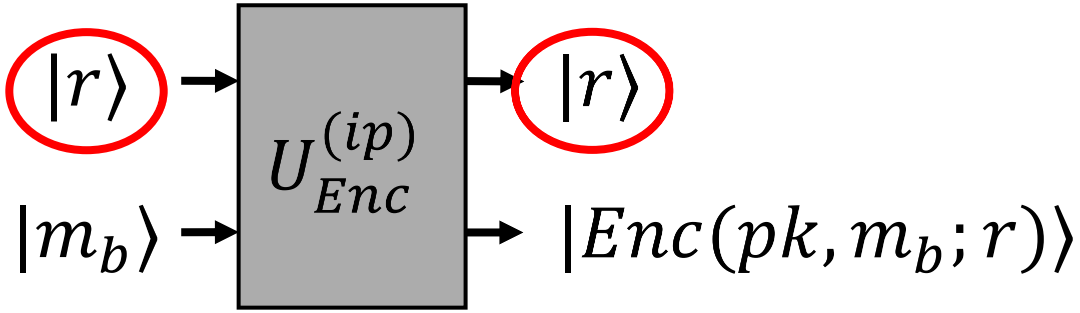
[NC16] Nielsen, Chuang. Quantum computation and quantum information. Cambridge University Press 2016
[KKVB02] Kashefi, Kent, Vedral, Banaszek. Comparison of quantum oracles. Physical Review A 2002

The qINDqCPA Security Notion [GKS21]



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

Discard $|m_{1-b}\rangle$

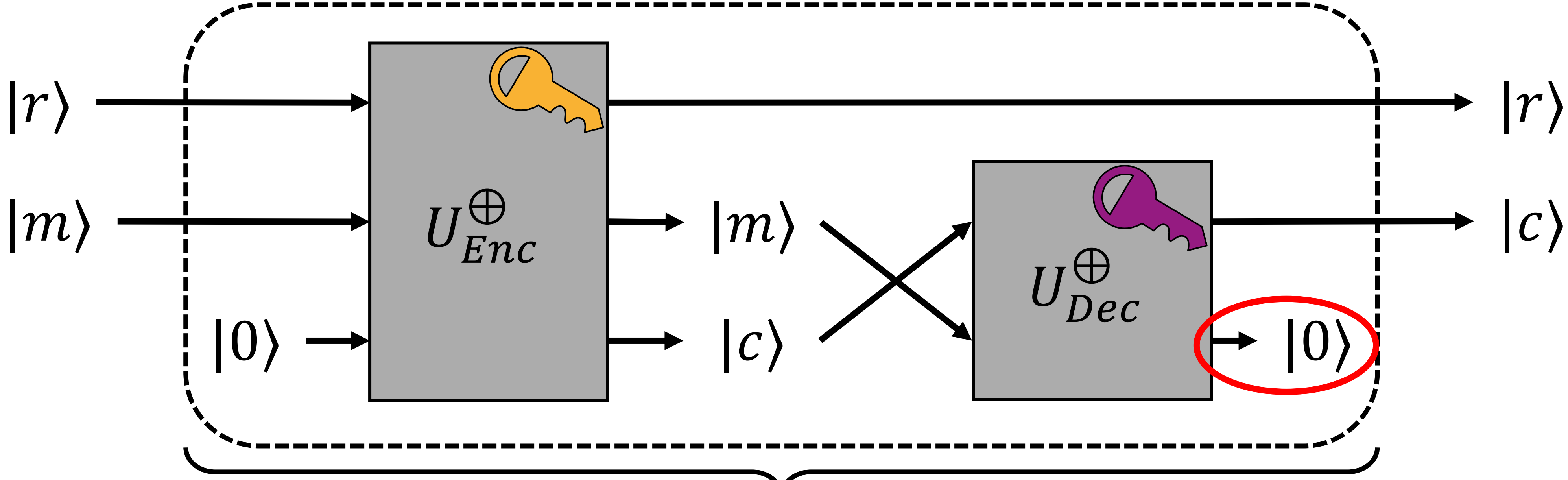


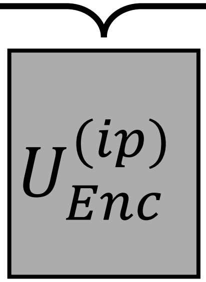
- Randomness is classical, hence unentangled
  - Challenger can simply withhold it
- Question: can we (efficiently) build $U_{Enc}^{(ip)}$?

- Explicitly de-randomise the operator
  - Randomness is often implicit in other notions
  - Required to ensure reversibility

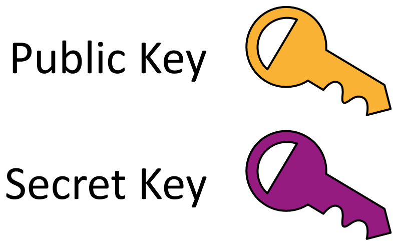
[GKS21] Gagliardoni, Krämer, Struck. Quantum indistinguishability for public key encryption. PQCrypto 2021

In-Place Operator for Perfectly Correct PKE

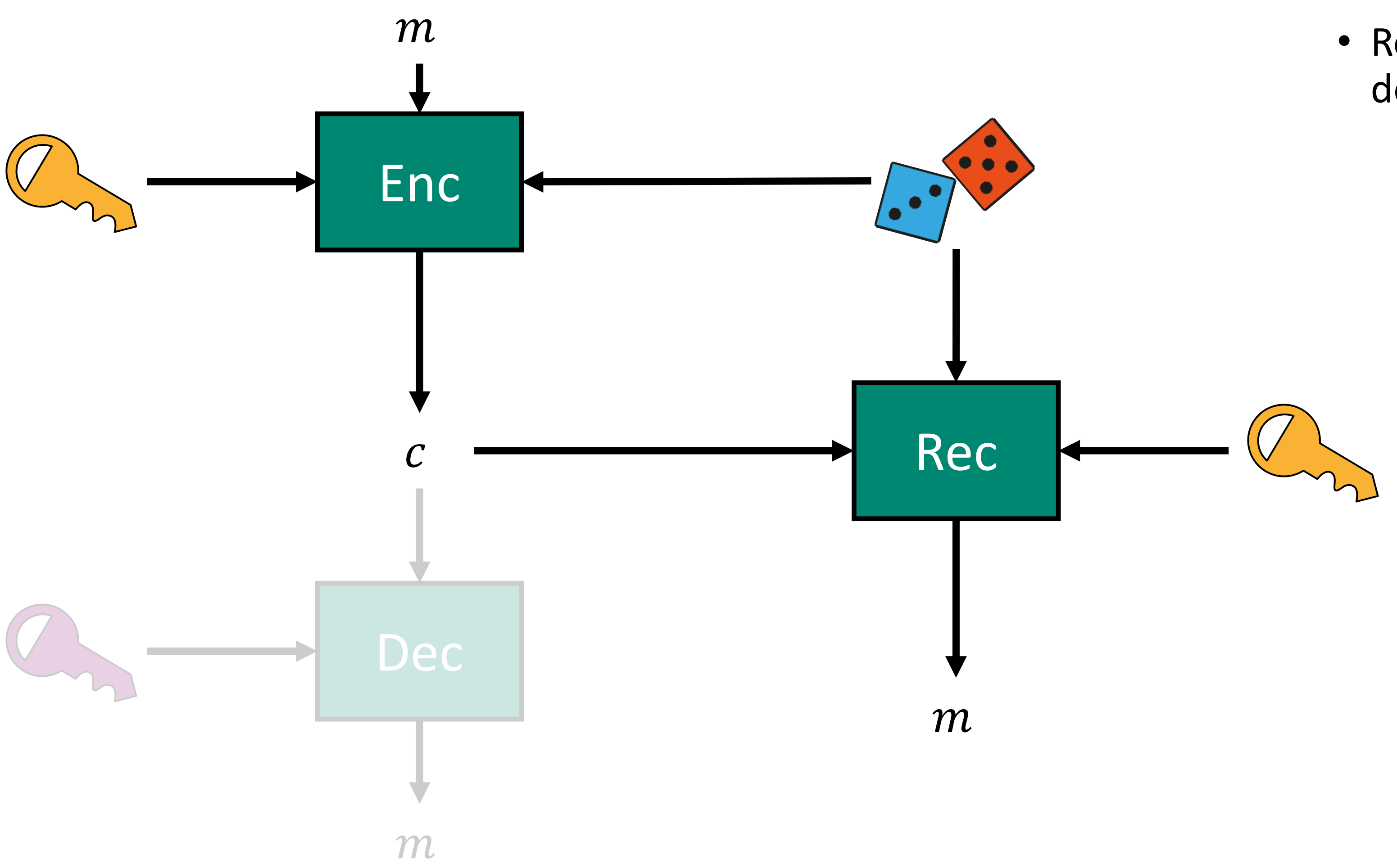




- Two drawbacks:
  1. In-place encryption operator requires knowledge of the secret key
  2. Does not work for schemes with decryption failures

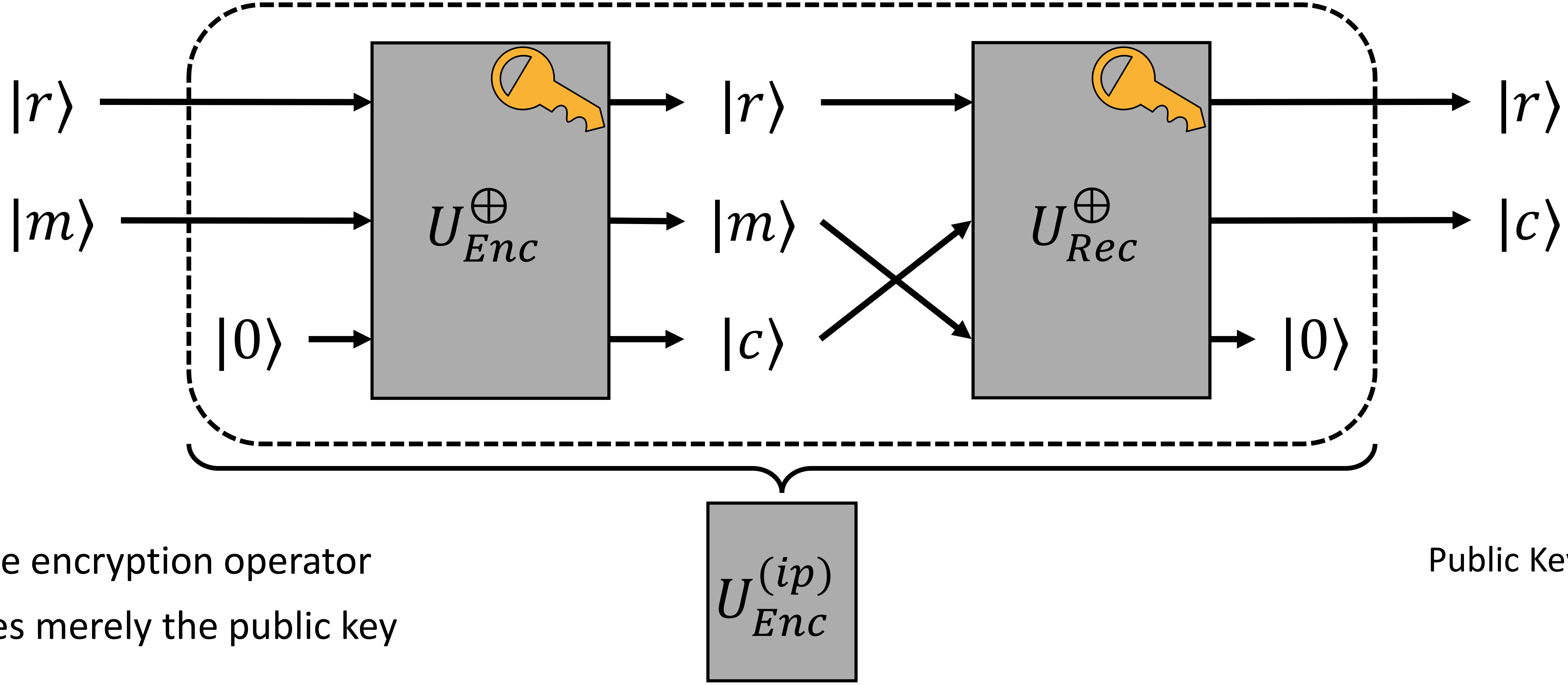


Recoverable Public Key Encryption



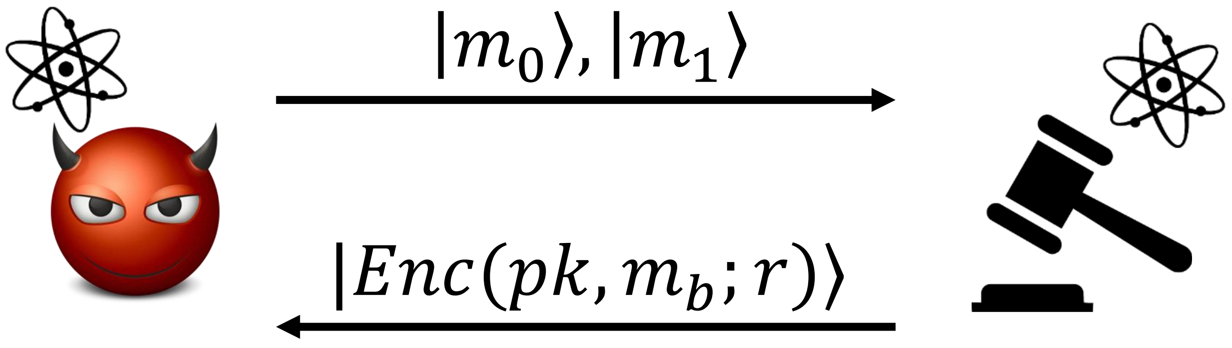
- Recoverable PKE schemes allow decryption using the randomness
  - Most PKE schemes are recoverable

In-Place Operator for Recoverable PKE



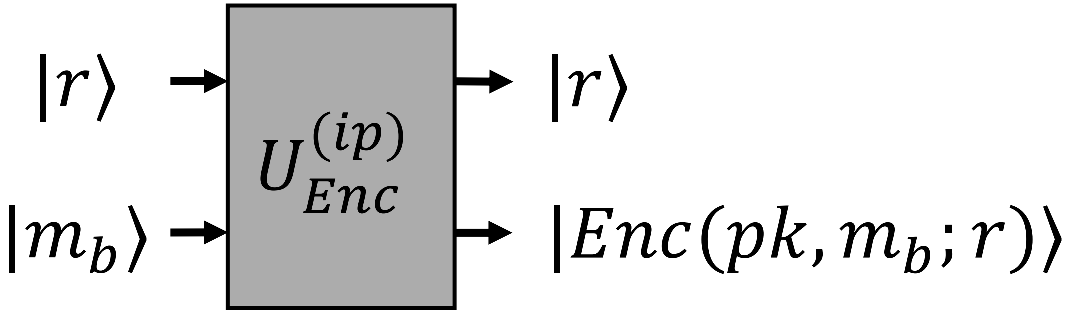
- In-place encryption operator requires merely the public key

The qINDqCPA Security Notion



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

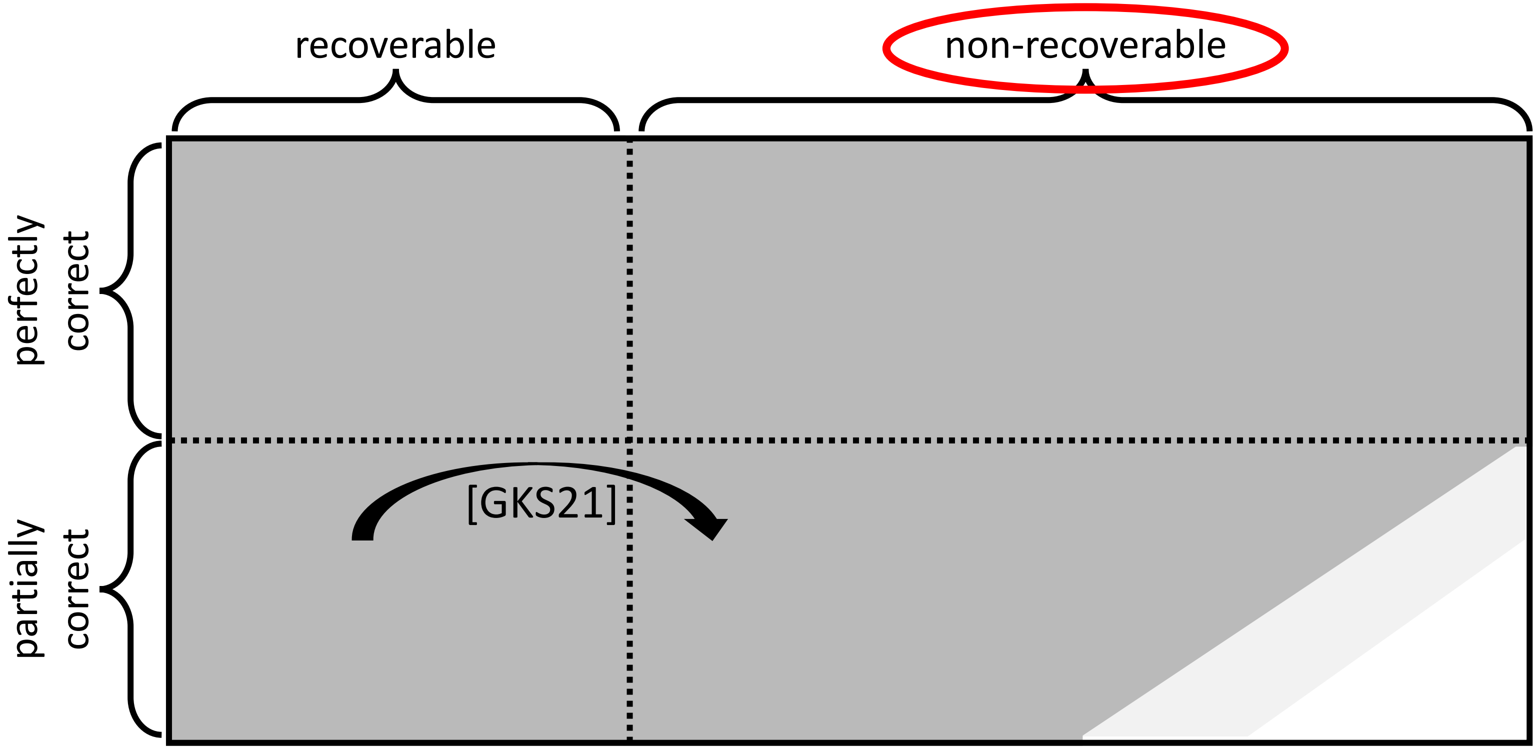
Discard $|m_{1-b}\rangle$



- Challenger models the encrypting party
  - Standard communication setting: only public key known
  - Other settings possible

Are there public key encryption schemes for which qINDqCPA security cannot be defined for challengers knowing only the public key?

Classification of PKE Schemes [GKS21]



Are there non-recoverable public key encryption schemes?

[GKS21] Gagliardoni, Krämer, Struck. Quantum indistinguishability for public key encryption. PQCrypto 2021

Universität Regensburg

Trapdoor Transformation [GKS21]

- PKE scheme $\Sigma = (KGen^{\Sigma}, Enc^{\Sigma}, Dec^{\Sigma})$
- Trapdoor permutation $\Pi = (KGen^{\Pi}, F, F^{-1})$

$KGen()$	$Enc(pk, m; r)$	$Dec(sk, c)$
$(pk_{\Sigma}, sk_{\Sigma}) \leftarrow KGen^{\Sigma}()$	Parse pk as (pk_{Σ}, pk_{Π})	Parse sk as (sk_{Σ}, sk_{Π})
$(pk_{\Pi}, sk_{\Pi}) \leftarrow KGen^{\Pi}()$	$y \leftarrow F(pk_{\Pi}, m)$	$y \leftarrow Dec^{\Sigma}(sk_{\Sigma}, c)$
$pk \leftarrow (pk_{\Sigma}, pk_{\Pi})$	c $\leftarrow Enc^{\Sigma}(pk_{\Sigma}, y; r)$	$m \leftarrow F^{-1}(sk_{\Pi}, y)$
$sk \leftarrow (sk_{\Sigma}, sk_{\Pi})$	Return c	Return m
Return (pk, sk)		

- Trapdoor permutation prevents recoverability
  - Trapdoor permutation does not affect the security
  - Can be transformed into a recoverable PKE scheme

[GKS21] Gagliardoni, Krämer, Struck. Quantum indistinguishability for public key encryption. PQCrypto 2021

Equivalent Recoverable PKE

$KGen()$
- $(pk_\Sigma, sk_\Sigma) \leftarrow KGen^\Sigma()$
- $(pk_\Pi, sk_\Pi) \leftarrow KGen^\Pi()$
- $pk \leftarrow (pk_\Sigma, pk_\Pi)$
- $sk \leftarrow (sk_\Sigma, sk_\Pi)$
- Return (pk, sk)

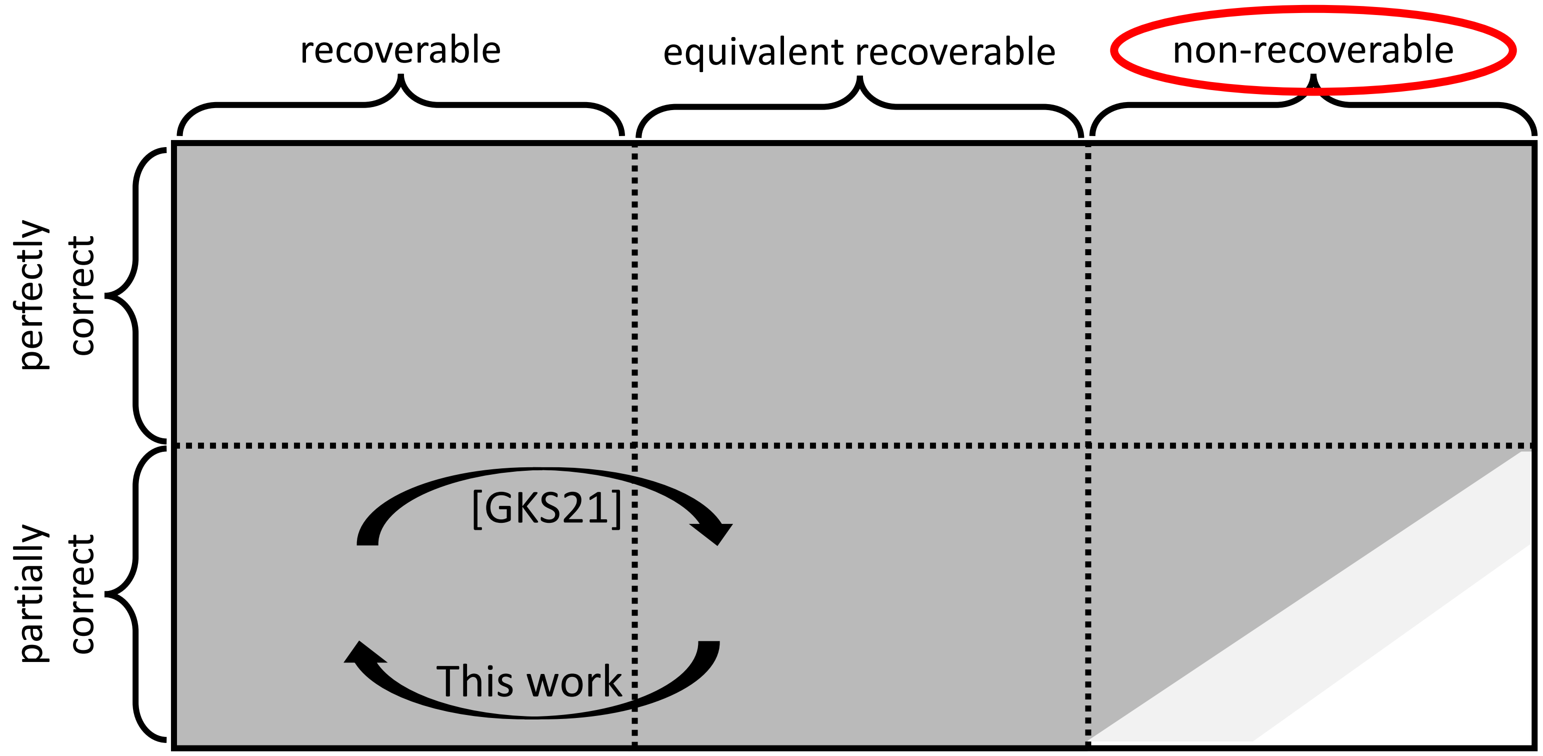
$KGen'()$
- $(pk_\Sigma, sk_\Sigma) \leftarrow KGen^\Sigma()$
- $(pk_\Pi, sk_\Pi) \leftarrow KGen^\Pi()$
- $pk \leftarrow (pk_\Sigma, pk_\Pi, sk_\Pi)$
- $sk \leftarrow sk_\Sigma$
- Return (pk, sk)

$Enc(pk, m; r)$
- Parse pk as $(pk_\Sigma, pk_\Pi, sk_\Pi)$
- $y \leftarrow F(pk_\Pi, m)$
- c $\leftarrow Enc^\Sigma(pk_\Sigma, y; r)$
- Return c

$Dec(sk, c)$
- Parse sk as sk_Σ
- $y \leftarrow Dec^\Sigma(sk_\Sigma, c)$
- $m \leftarrow F^{-1}(sk_\Pi, y)$
- Return m

Can be done with the public key

Refined Classification of PKE Schemes

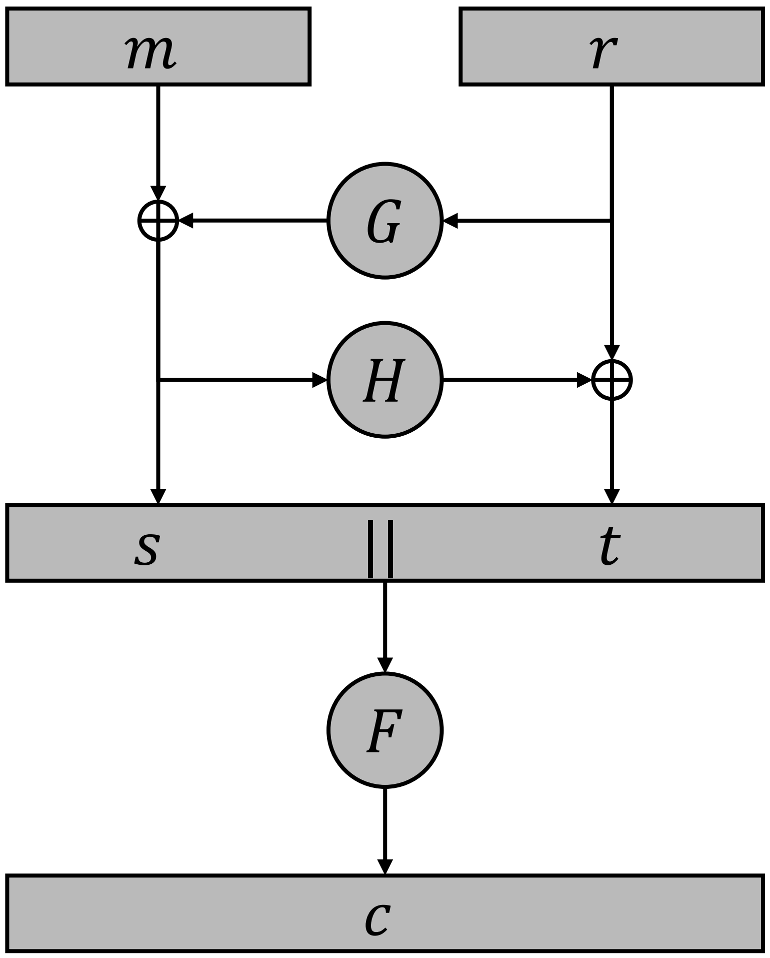


Are there non-recoverable public key encryption schemes?

The OAEP Construction

- Transforms a trapdoor permutation into a public key encryption scheme

- Secure if F is partial-domain one-way:
  - Given c, it is hard to find s

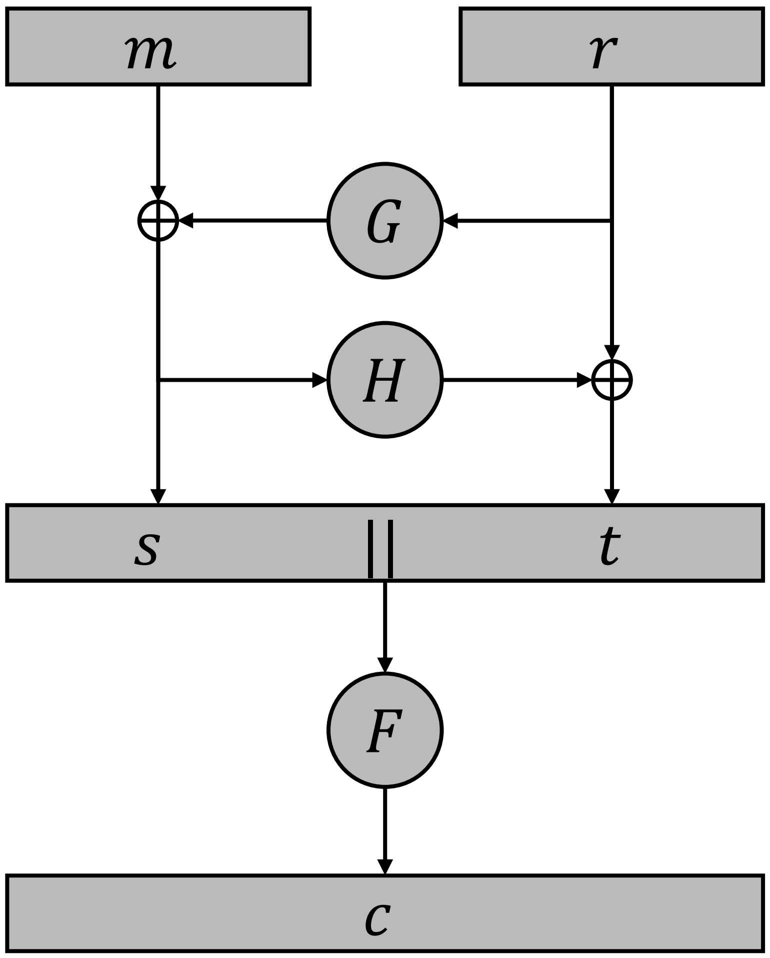


Recoverability of OAEP

- Assuming that if F is partial-domain one-way, OAEP is not recoverable
  - Knowledge of the randomness r does not help
  - $m = s \oplus G(r)$

- Assuming that F is one-way is not enough
  - Consider $F(s||t) = s||F^*(t)$
  - From $F(s||t) = s||F^*(t)$ and r, one can easily recover the message $m = s \oplus G(r)$

- This rules out only the construction based on the recoverable property but not the quantum operator



Universität Regensburg

In-Place Operator for OAEP

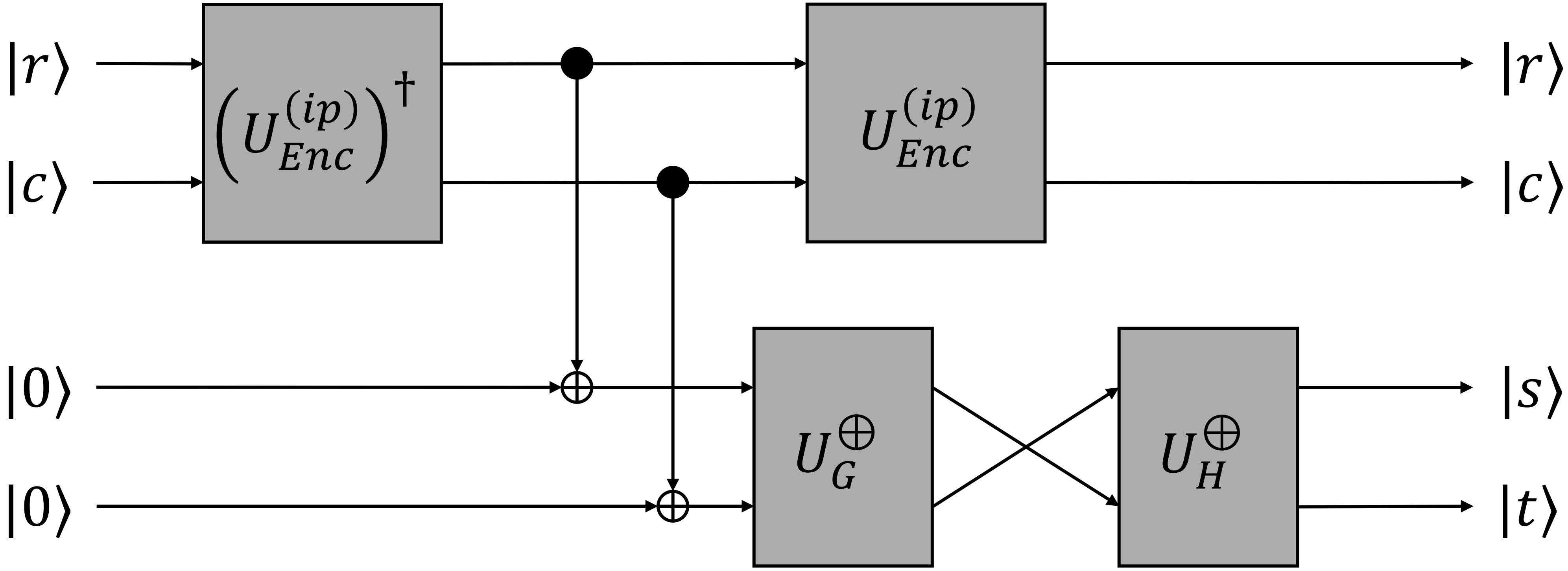
Game $pdOW$
$(pk_\Pi, sk_\Pi) \leftarrow KGen^\Pi()$
$s, t \leftarrow_\$ \{0,1\}^n$
$c \leftarrow F(pk_\Pi, s||t)$
$s' \leftarrow A(pk_\Pi, c)$
Return $s' = s$

Game $pdOW^*$
$(pk_\Pi, sk_\Pi) \leftarrow KGen^\Pi()$
$s, t \leftarrow_\$ \{0,1\}^n$
$c \leftarrow F(pk_\Pi, s||t)$
$r \leftarrow H(s) \oplus t$
$s' \leftarrow A(pk_\Pi, c, r)$
Return $s' = s$

- Hardness of $pdOW$ implies hardness of $pdOW^*$
    - Extra information r does not help

In-Place Operator for OAEP

- Assumption: $U_{Enc}^{(ip)}$ can be constructed solely from the public key and F is $pdOW^*$ secure



- This construction breaks $pdOW^*$, hence contradicting the assumption

Summary/Open Problems

- Applicability of the qINDqCPA security notion
  - Challengers knowing only the public key
  - The OAEP construction is non-recoverable
  - Mandatory in-place operator cannot be constructed solely from the public key for the OAEP construction

- Are there more non-recoverable PKE schemes?

- Unified quantum security notion for public key encryption
  - Combining [GKS21] and [CEV[20]

Thank You!

patrick.struck@ur.de

ePrint 2022/1074

[CEV20] Chevalier, Ebrahimi, Vu. On security notion for encryption in a quantum world. ePrint 2020
[GKS21] Gagliardoni, Krämer, Struck. Quantum indistinguishability for public key encryption. PQCrypto 2021