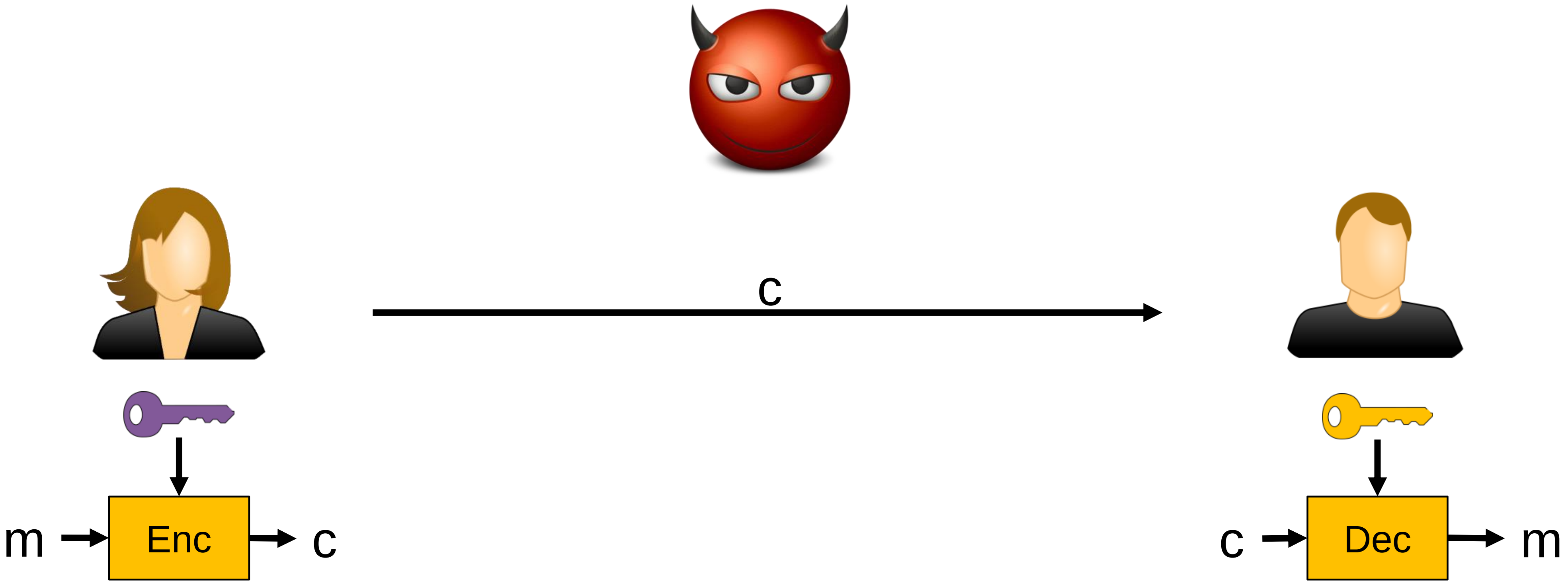
PQCrypto 2021

Quantum Indistinguishability for Public Key Encryption

Tommaso Gagliardoni, Juliane Krämer, and Patrick Struck

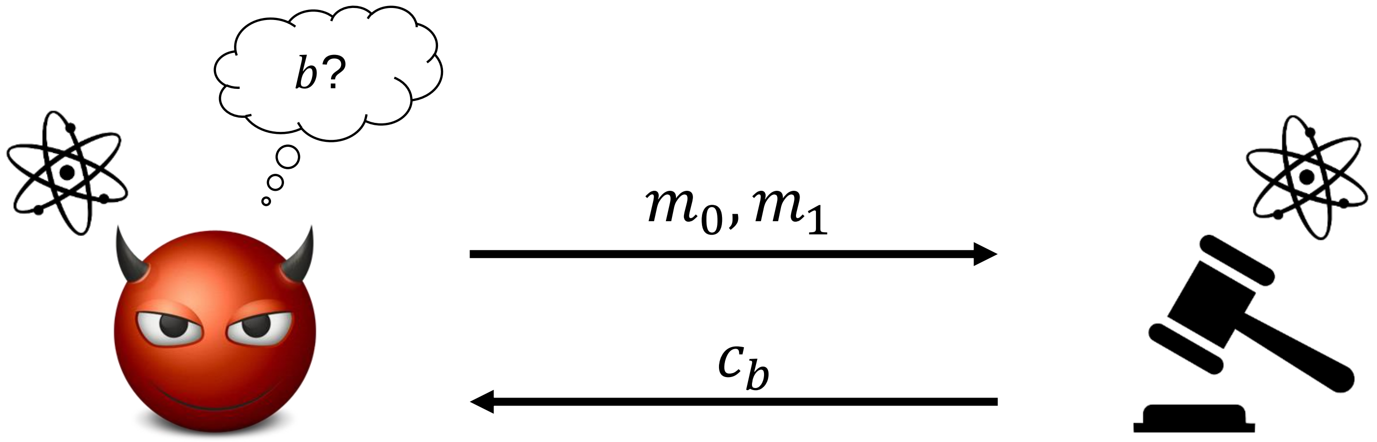
MOTIVATION AND BACKGROUND

Motivation



- Adversary should not learn anything about m from c

INDCPA Security

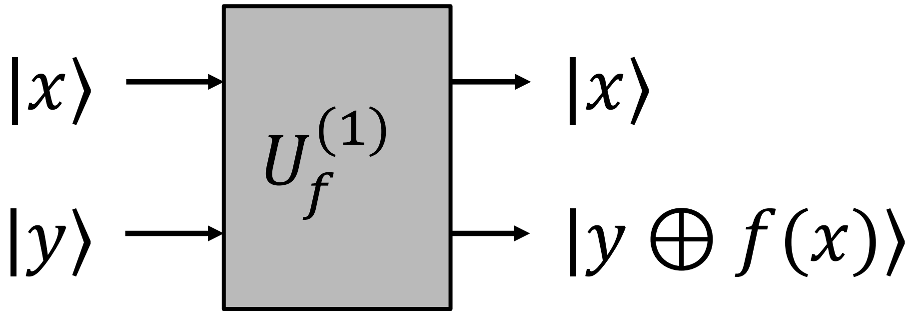


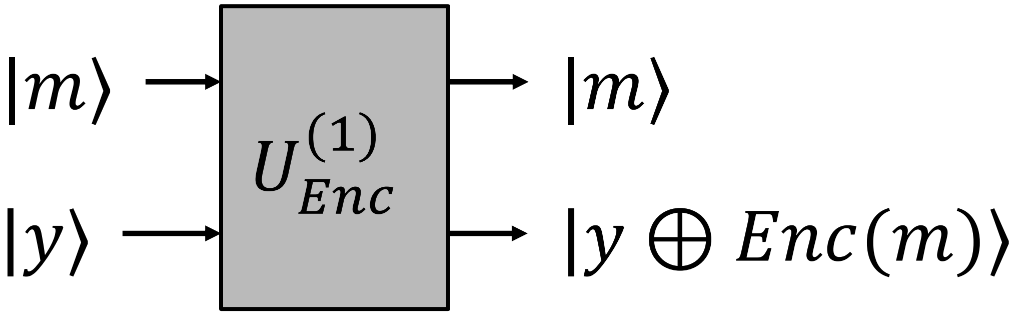
$b \leftarrow_{\$} \{0,1\}$

- Classical security (QS0): both adversary and challenger are classical
- Post-quantum security (QS1): quantum adversary and classical challenger
- Quantum security (QS2): both adversary and challenger are quantum

Focus of this work

Quantum Operators

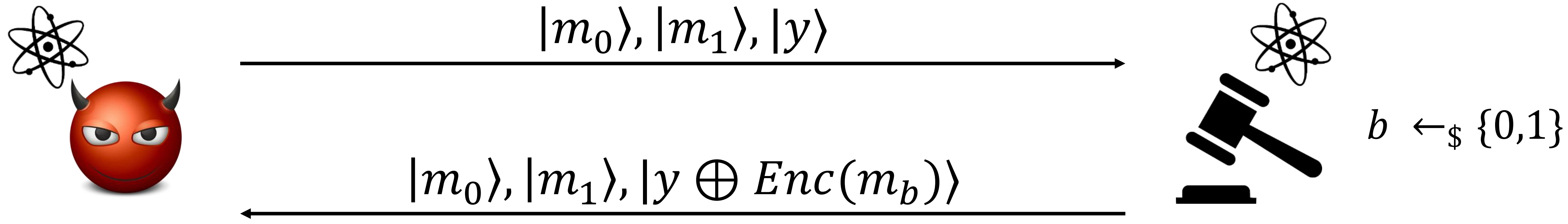




- Type-1 operator
  - Realisable for any f
  - Efficiently realisable if f is efficient
  - E.g. used in the QROM [BDFLSZ11]
- Type-1 operator of an encryption scheme
  - Fixed public key
  - Randomness is implicit

[BDFLSZ11] Boneh, Dagdelen, Fischlin, Lehmann, Schaffner, Zhandry. Random Oracles in a Quantum World. ASIACRYPT 2011

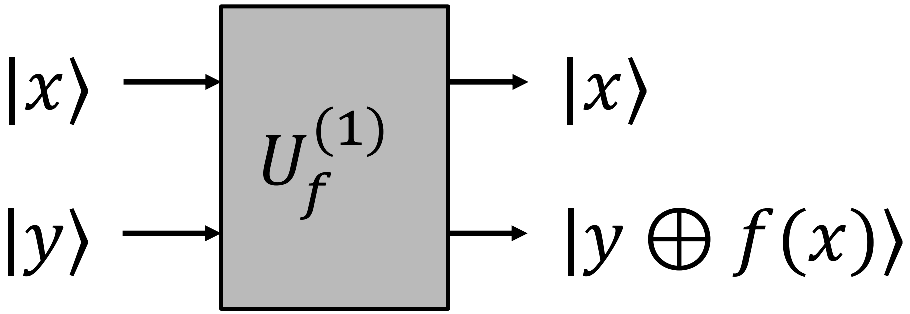
Fully-quantum INDCPA [BZ13]

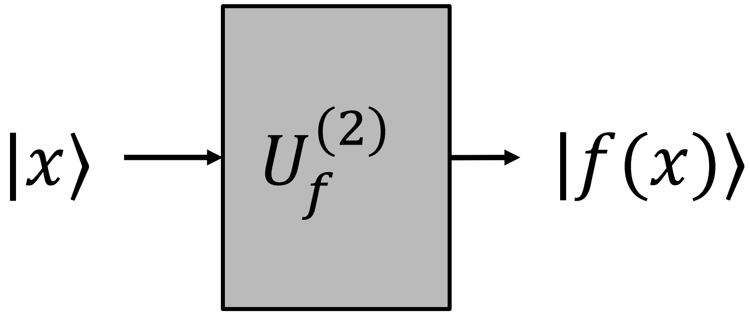


- Obervation: $|y \oplus Enc(m_b)\rangle$ will be entangled with $|m_b\rangle$ while $|m_{1-b}\rangle$ remains unentangled
  - Adversary can detect this entanglement
  - Unachievable for any encryption scheme
- Withholding the message registers makes the notion equivalent to classical messages
- No security notion with a quantum indistinguishability phase exists (concurrent work: [CEV20])

[BZ13] Boneh, Zhandry. Secure signatures and chosen ciphertext security in a quantum computing world. CRYPTO 2013
[CEV20] Chevalier, Ebrahimi, Vu. On Security Notions for Encryption in a Quantum World. ePrint 2020/237

Quantum Operators





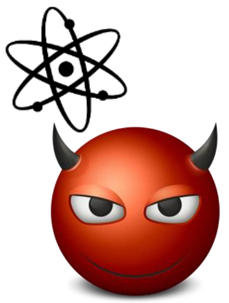
- Type-1 operator
  - Realisable for any f
  - Efficiently realisable if f is efficient

- Type-2 operator [KKVB02]
  - Realisable only for reversible f
  - Not always efficiently realisable

[KKVB02] Kashefi, Kent, Vedral, Banaszek. Comparison of quantum oracles. Physical Review A 2002

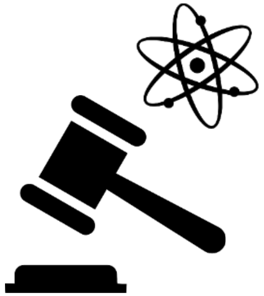
NEW SECURITY NOTION

The qINDqCPA Security Notion



$$\xrightarrow{\quad |m_0\rangle, |m_1\rangle \quad}$$

$$\xleftarrow{\quad |Enc(pk, m_b; r)\rangle \quad}$$



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

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

$$|r\rangle \rightarrow U^{(2)}_{Enc} \rightarrow |r\rangle$$

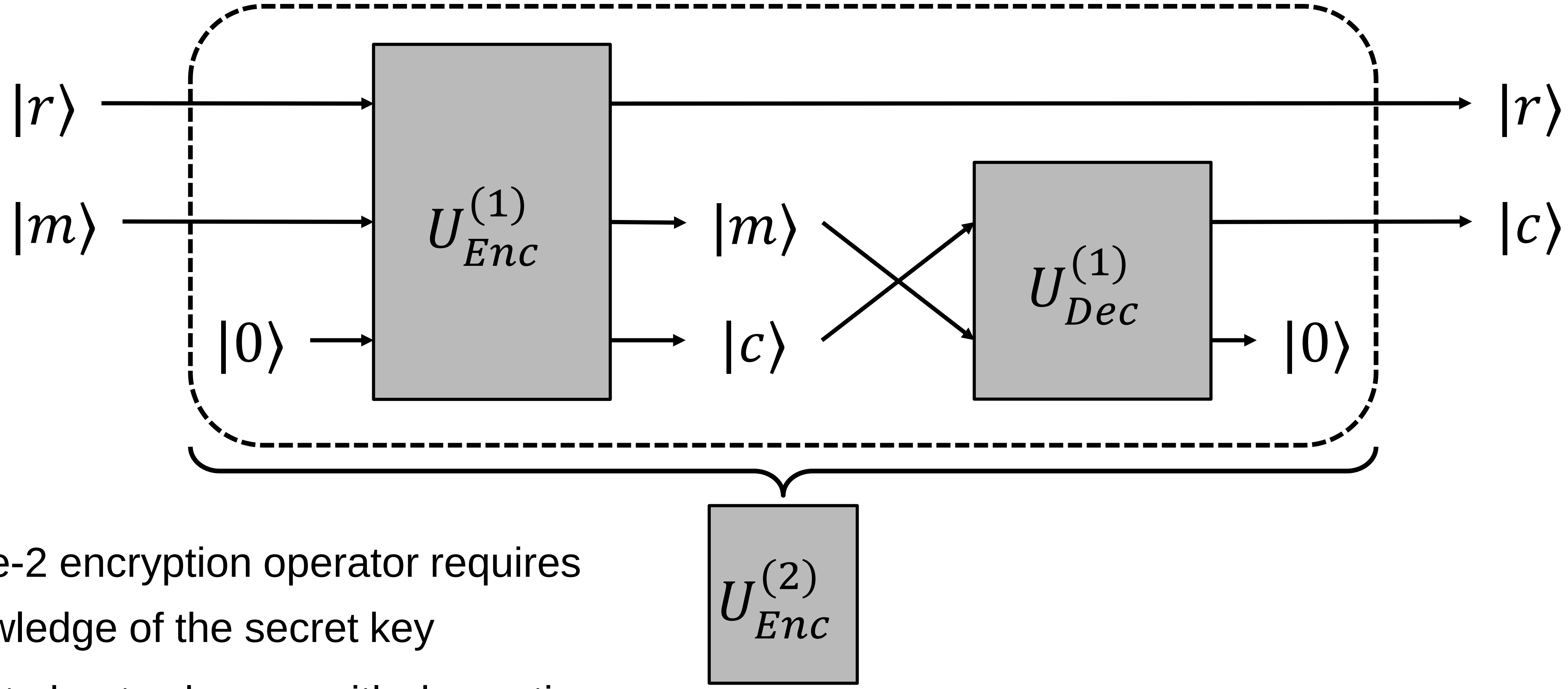
$$|m_b\rangle \rightarrow U^{(2)}_{Enc} \rightarrow |Enc(pk, m_b; r)\rangle$$

- Adversary does not get entangled registers
  - Avoids the Boneh-Zhandry impossibility result
- Randomness is classical, hence unentangled
  - Challenger can simply withhold it
- Question: can we efficiently build $U^{(2)}_{Enc}$?

- Explicitly de-randomise the operator
  - Randomness is implicit in [BZ13]
  - Required to ensure reversibility

[BZ13] Boneh, Zhandry. Secure signatures and chosen ciphertext security in a quantum computing world. CRYPTO 2013

Type-2 Operator for perfectly correct PKE

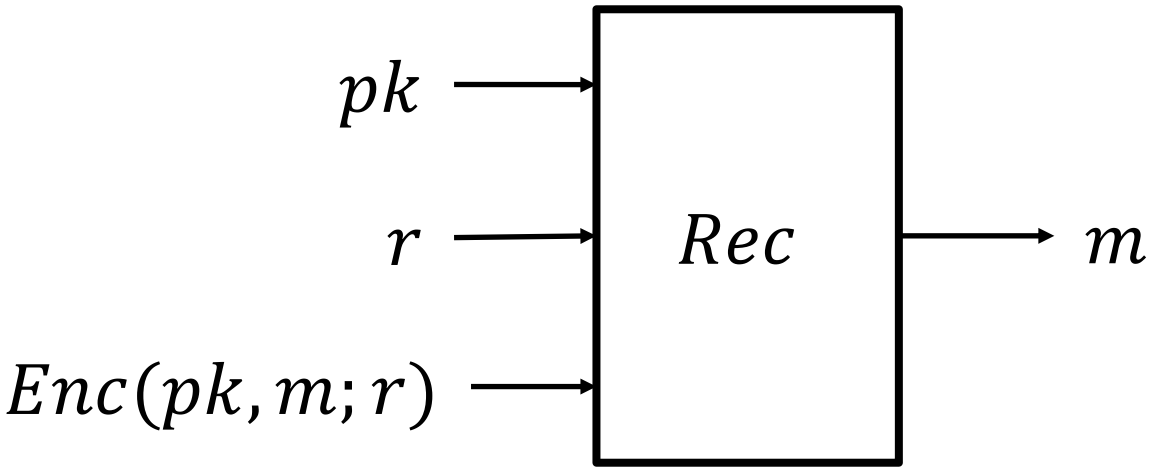


- Type-2 encryption operator requires knowledge of the secret key
- What about schemes with decryption failures?

Recoverable PKE

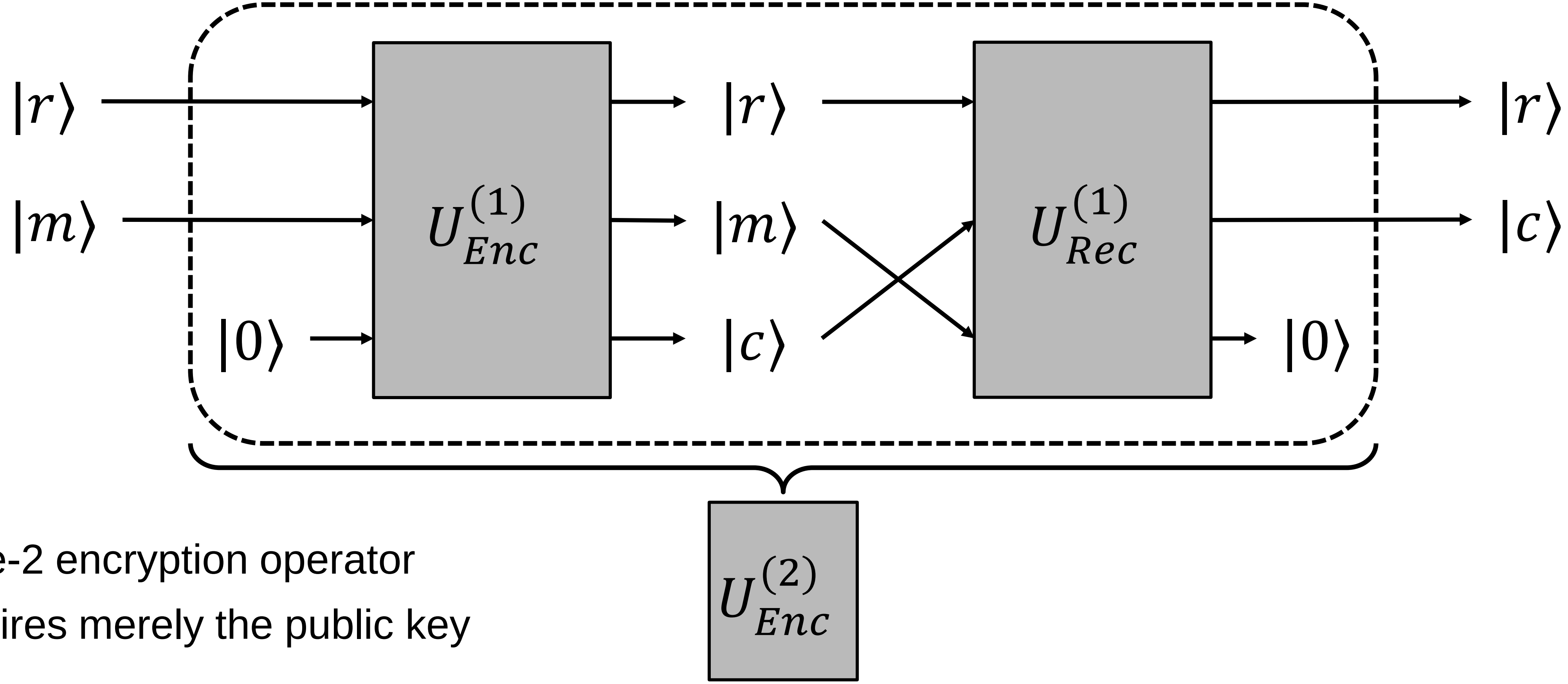
TECHNISCHE UNIVERSITÄT DARMSTADT

- Idea: knowledge of the randomness allows to perfectly decrypt ciphertexts (without the secret key)



- Examples: Most lattice-based and code-based PKE schemes

Type-2 Operator for Recoverable PKE



- Type-2 encryption operator requires merely the public key

APPLICATION

qINDqCPA Security of Real-World PKE Schemes

- Code-based PKE ROLLO-II
- Canonical LWE-based PKE
- Hybrid Encryption
- All schemes are recoverable
  - Allow realisation of type-2 operators using merely the public key

qINDqCPA Security of ROLLO-II

$\mathtt{KGen}(\lambda; r)$	$\mathtt{Enc}(\mathsf{pk}, m; r)$
$\mathbf{x}, \mathbf{y} := r$	$\mathbf{e}_1, \mathbf{e}_2 := r$
$\mathbf{h} := \mathbf{x}^{-1}\mathbf{y} \bmod \mathsf{P}$	$\mathsf{E} := \mathsf{Supp}(\mathbf{e}_1, \mathbf{e}_2)$
$\mathsf{sk} := (\mathbf{x}, \mathbf{y})$	$c_1 := m \oplus \mathsf{O}(\mathsf{E})$
$\mathsf{pk} := \mathbf{h}$	$c_2 := \mathbf{e}_1 + \mathbf{e}_2\mathbf{h} \bmod \mathsf{P}$
$\mathbf{return}\ (\mathsf{pk}, \mathsf{sk})$	$\mathbf{return}\ c := (c_1, c_2)$

Message is encrypted using a One-Time Pad

- Equal superposition of all messages for $|m_0\rangle$ and a random classical message for $|m_1\rangle$
  - If $b = 0$: $|c_1\rangle$ will be an equal superposition
  - If $b = 1$: $|c_1\rangle$ will be a random classical ciphertext
  - Can be distinguished almost perfectly by measuring in the Hadamard basis

qINDqCPA Security of Hybrid Encryption

TECHNISCHE UNIVERSITÄT DARMSTADT

$\mathtt{KGen}(\lambda)$	$\mathtt{Enc}_{\mathsf{pk}}(m; r)$
$(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathtt{KGen}^P(\lambda)$	**parse** r **as** (r_1, r_2, r_3)
return $(\mathsf{pk}, \mathsf{sk})$	$\mathsf{k} := \mathtt{KGen}^S(\lambda; r_1)$
	$c_1 := \mathtt{Enc}^S_{\mathsf{k}}(m; r_2)$
	$c_2 := \mathtt{Enc}^P_{\mathsf{pk}}(\mathsf{k}; r_3)$
	return (c_1, c_2)

Message m is encrypted using Symmetric Key Encryption Σ^S

Symmetric key k is encrypted using Public Key Encryption Σ^P

- Post-quantum (QS1) secure Σ^P + quantum (QS2) secure Σ^S [GHS16] $\Rightarrow$ quantum (QS2) secure Σ
  - Σ^P used to encrypt the symmetric key which is classical
  - Σ^S used to encrypt the message which is quantum

[GHS16] Gagliardoni, Hülsing, Schaffner. Semantic Security and Indistinguishability in the Quantum World. CRYPTO 2016

qINDqCPA Security of Real-World PKE Schemes

- ROLLO-II
  - qINDqCPA insecure as a stand-alone PKE scheme
  - qINDqCPA secure in conjunction with a quantum secure SKE scheme
- Security depends on the use case
  - For the NIST standardization, post-quantum (QS1) security is sufficient
  - Potential problem when used in larger protocols

Summary

- Novel quantum security notion for public key encryption schemes based on type-2 operators

- Efficient realisation of type-2 operators for schemes that are perfectly correct or recoverable

- Positive and negative results for existing public key encryption schemes

Thank You!

IACR ePrint archive 2020/266

patrick@qpc.tu-darmstadt.de