qIND-qCPA (In)security of CBC, CFB, OFB and CTR

PQCrypto 2023

Tristan Nemoz, Zoé Amblard, Aurélien Dupin
tristan.nemoz@telecom-paris.fr
August 17, 2023

Reminders on modes of operation

Problem

Being given a long message and a secure block cipher (e.g. AES), how to encrypt the message?

Reminders on modes of operation

Problem

Being given a long message and a secure block cipher (e.g. AES), how to encrypt the message?

What if we simply encrypt each block?

Reminders on modes of operation

Problem

Being given a long message and a secure block cipher (e.g. AES), how to encrypt the message?

What if we simply encrypt each block?

Figure: Original image

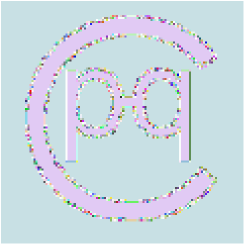


Figure: Encrypted image

Reminders on modes of operation

Problem

Being given a long message and a secure block cipher (e.g. AES), how to encrypt the message?

What if we simply encrypt each block?

Figure: Original image

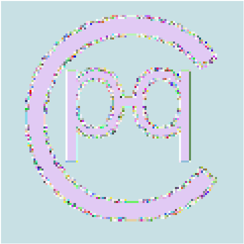
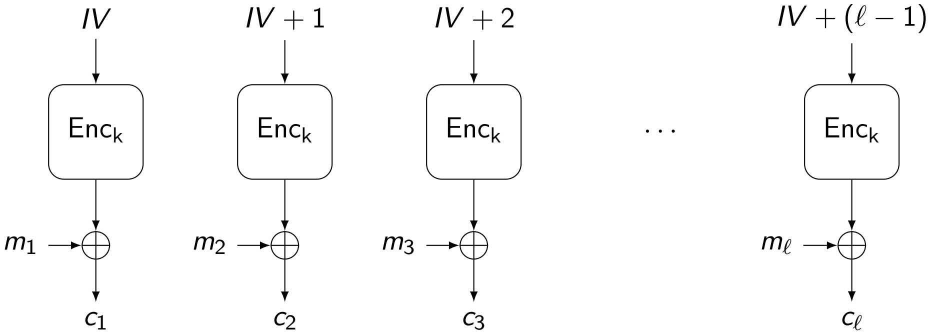


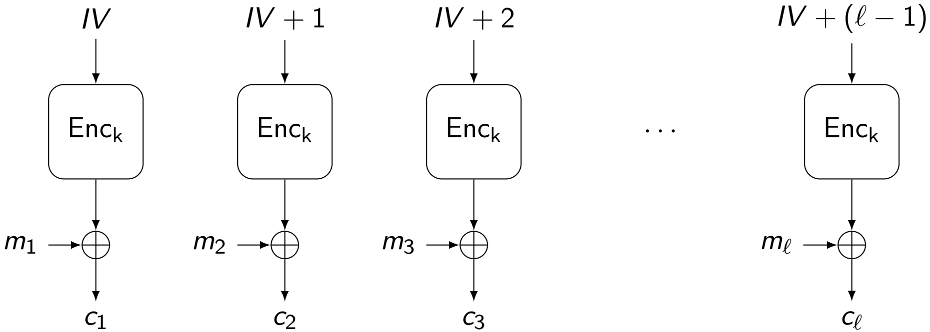
Figure: Encrypted image

Modes of operation allow us to securely encrypt long messages.

Example: CTR mode



Example: CTR mode



In particular, it acts as a stream cipher: $\mathsf{Enc}_\mathsf{k}^{\mathsf{CTR}}(m) = m \oplus s$ for a (pseudo)random s.

History of the security of these modes

	CTR/OFB	CBC/OFB with PRP	CBC/OFB with qPRP
IND-CPA			

IND-CPA Classical learning queries, Classical challenge queries

History of the security of these modes

	CTR/OFB	CBC/OFB with PRP	CBC/OFB with qPRP
IND-CPA	✓	✓	✓

IND-CPA Classical learning queries, Classical challenge queries

History of the security of these modes

	CTR/OFB	CBC/OFB with PRP	CBC/OFB with qPRP
IND-CPA	✓	✓	✓
IND-qCPA[1]			

IND-CPA Classical learning queries, Classical challenge queries

IND-qCPA **Quantum** learning queries, Classical challenge queries

[1] Boneh and Zhandry, "Secure Signatures and Chosen Ciphertext Security in a Quantu Computing World", In: CRYPTO 2013.

History of the security of these modes

	CTR/OFB	CBC/OFB with PRP	CBC/OFB with qPRP
IND-CPA	✓	✓	✓
IND-qCPA[1]	✓[2]	◆[2]	✓[2]

IND-CPA Classical learning queries, Classical challenge queries

IND-qCPA **Quantum** learning queries, Classical challenge queries

[1] Boneh and Zhandry, "Secure Signatures and Chosen Ciphertext Security in a Quantum Computing World", In: CRYPTO 2013.

[2] Anand et al., "Post-Quantum Security of the CBC, CFB, OFB, CTR, and XTS Modes of Operation", In: PQCrypto 2016.

History of the security of these modes

	CTR/OFB	CBC/OFB with PRP	CBC/OFB with qPRP
IND-CPA	✓	✓	✓
IND-qCPA[1]	✓[2]	◆[2]	✓[2]
qIND-qCPA[3]			

IND-CPA Classical learning queries, Classical challenge queries

IND-qCPA Quantum learning queries, Classical challenge queries

qIND-qCPA **Quantum**/**Classical** learning queries, **Quantum** challenge queries

[1] Boneh and Zhandry, "Secure Signatures and Chosen Ciphertext Security in a Quantum Computing World", In: CRYPTO 2013.

[2] Anand et al., "Post-Quantum Security of the CBC, CFB, OFB, CTR, and XTS Modes of Operation", In: PQCrypto 2016.

[3] Carstens et al., "Relationships Between Quantum IND-CPA Notions", In: TCC 2021.

History of the security of these modes

	CTR/OFB	CBC/OFB with PRP	CBC/OFB with qPRP
IND-CPA	✓	✓	✓
IND-qCPA[1]	✓[2]	◆[2]	✓[2]
qIND-qCPA[3]	This work	This work	This work

IND-CPA Classical learning queries, Classical challenge queries

IND-qCPA Quantum learning queries, Classical challenge queries

qIND-qCPA **Quantum**/**Classical** learning queries, **Quantum** challenge queries

[1] Boneh and Zhandry, "Secure Signatures and Chosen Ciphertext Security in a Quantum Computing World", In: CRYPTO 2013.

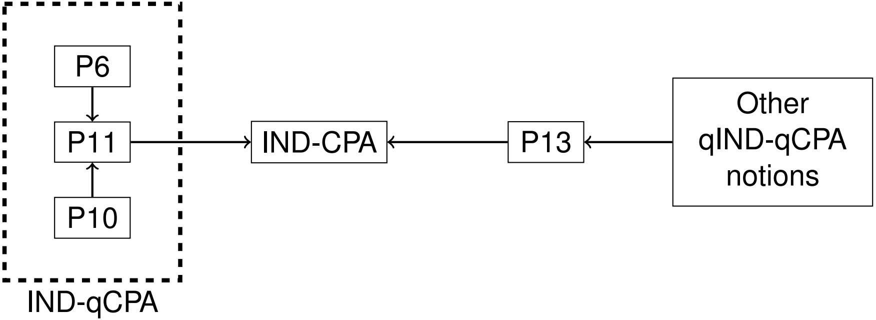
[2] Anand et al., "Post-Quantum Security of the CBC, CFB, OFB, CTR, and XTS Modes of Operation", In: PQCrypto 2016.

[3] Carstens et al., "Relationships Between Quantum IND-CPA Notions", In: TCC 2021.

TELECOM Paris

IP PARIS

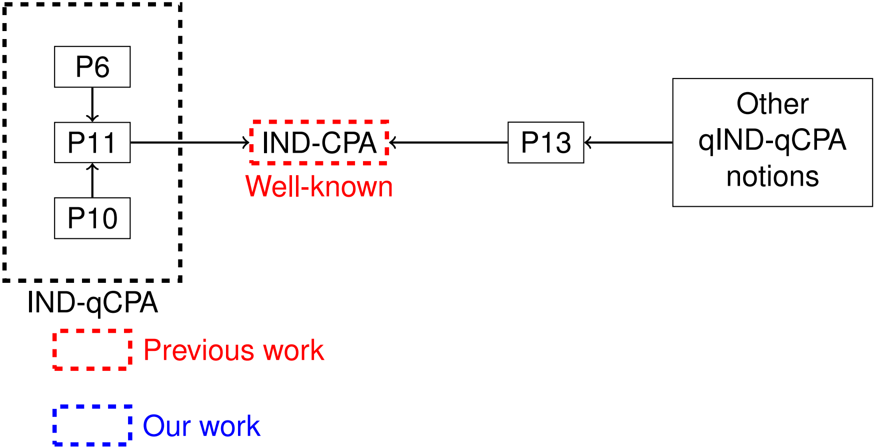
qIND-qCPA security of CBC, CFB, CTR and OFB



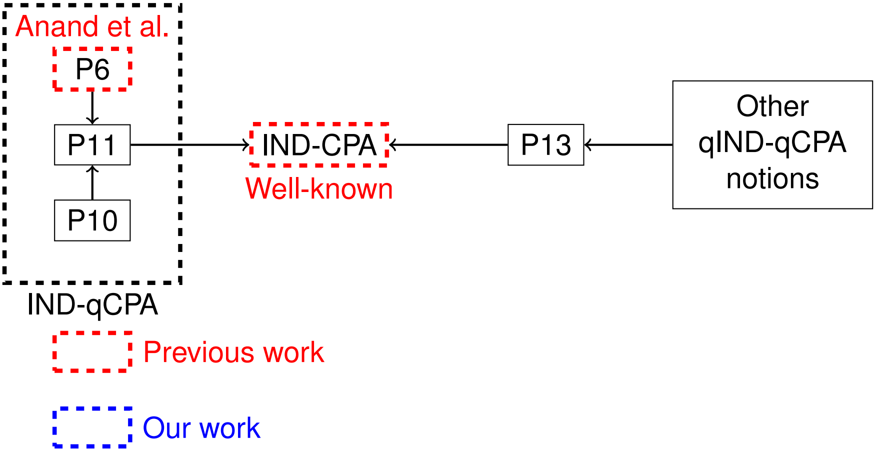
Previous work

Our work

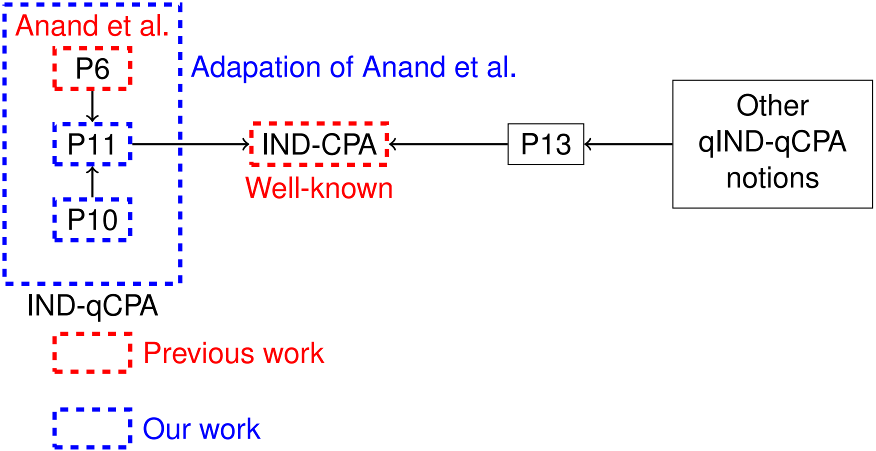
qIND-qCPA security of CBC, CFB, CTR and OFB



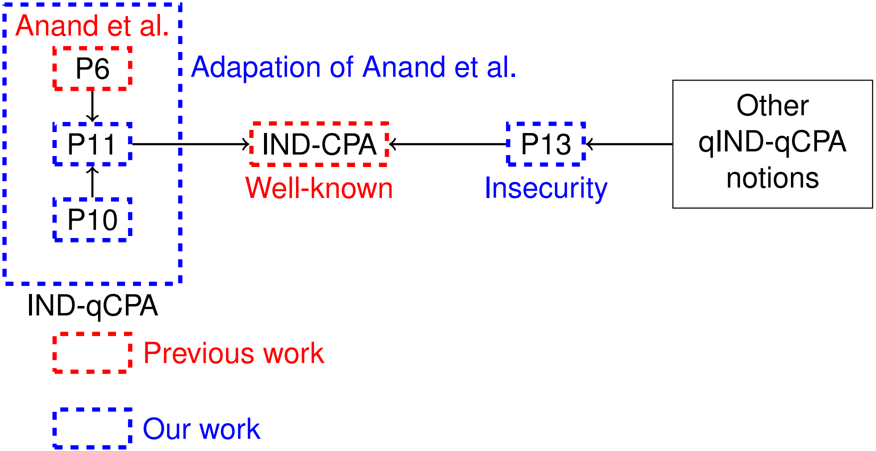
qIND-qCPA security of CBC, CFB, CTR and OFB



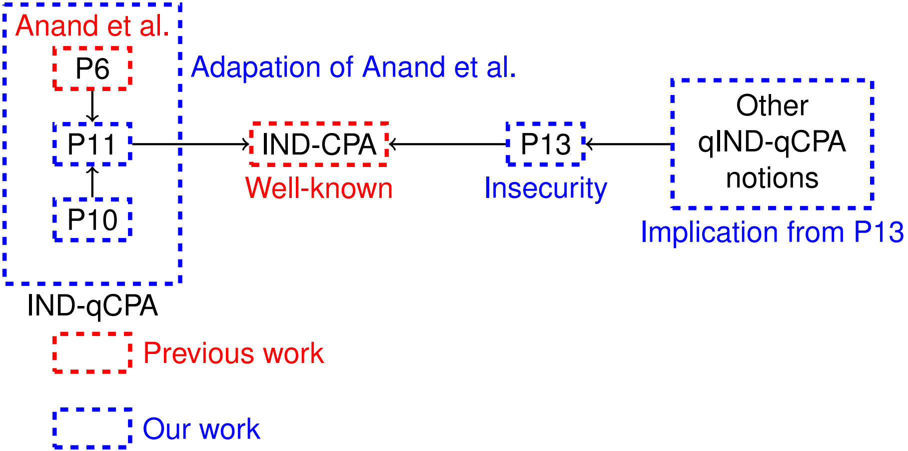
qIND-qCPA security of CBC, CFB, CTR and OFB



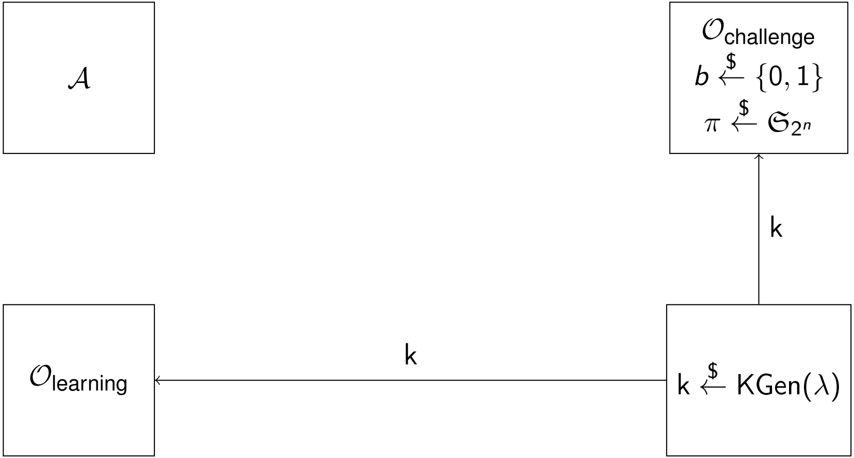
qIND-qCPA security of CBC, CFB, CTR and OFB



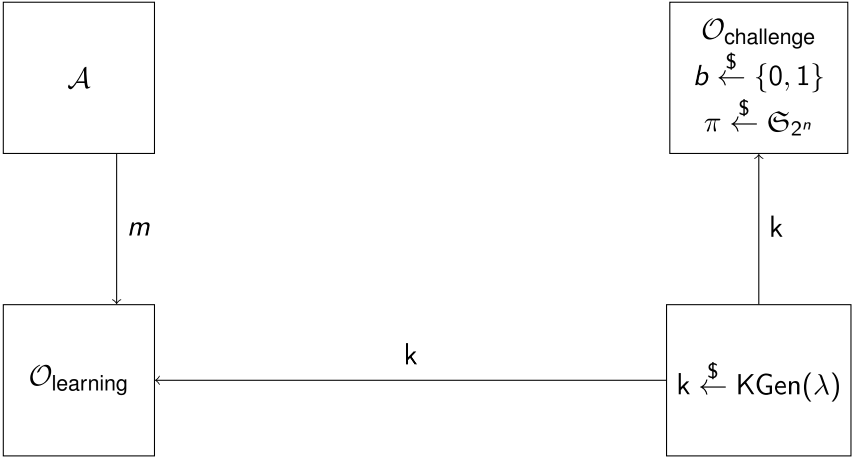
qIND-qCPA security of CBC, CFB, CTR and OFB



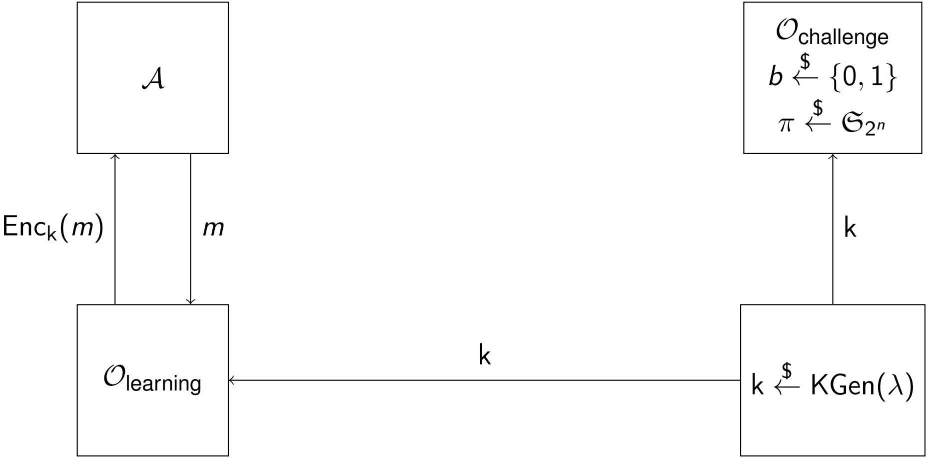
qIND-qCPA-P13 security notion



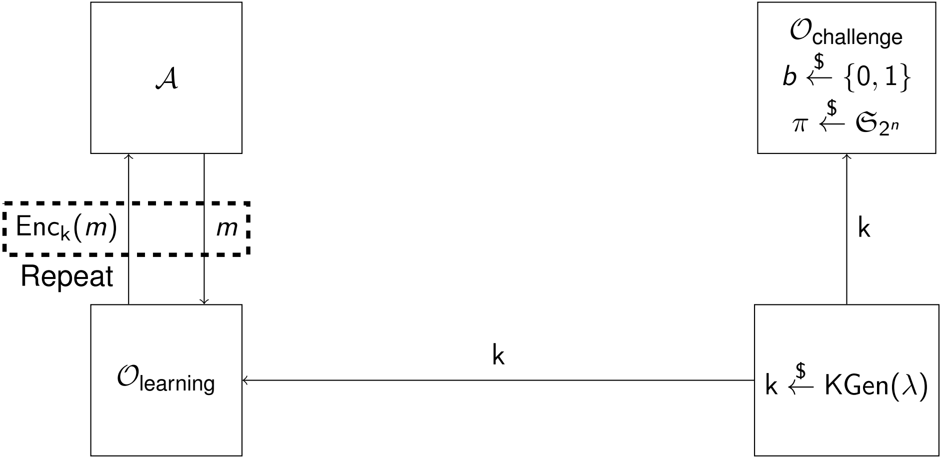
qIND-qCPA-P13 security notion



qIND-qCPA-P13 security notion

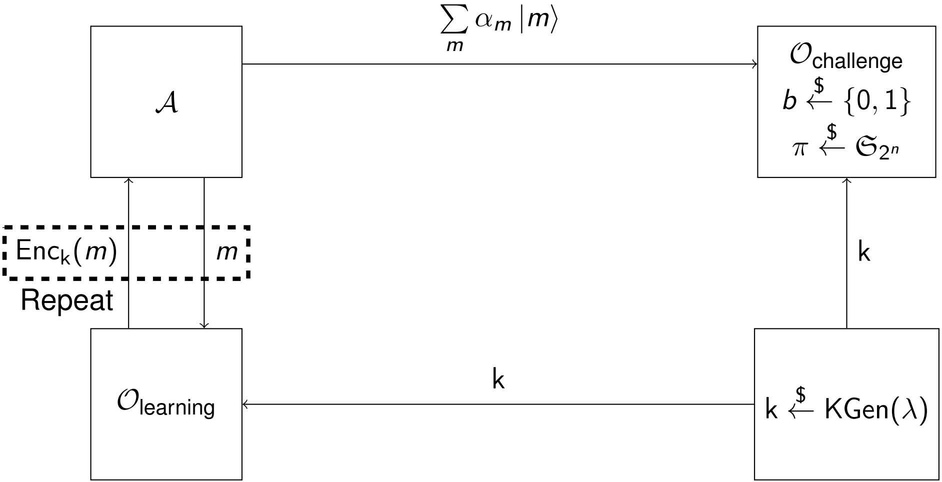


qIND-qCPA-P13 security notion

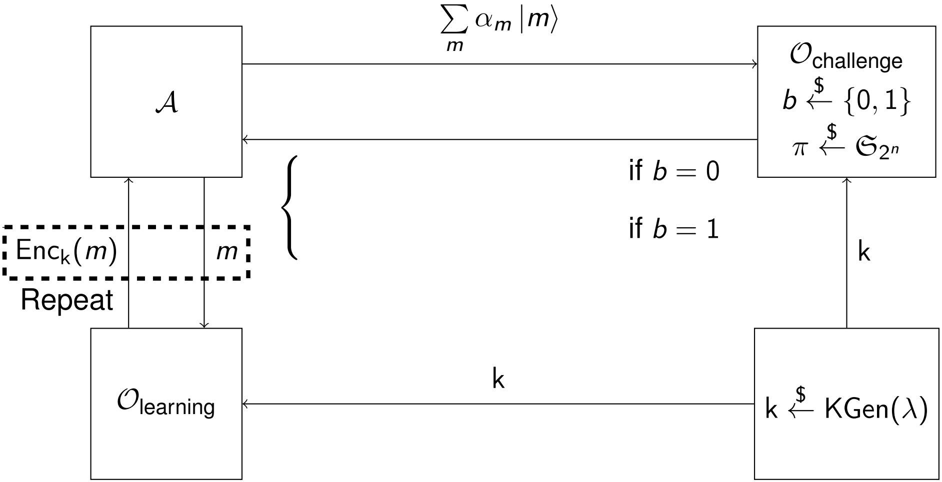


TELECOM Paris IP PARIS

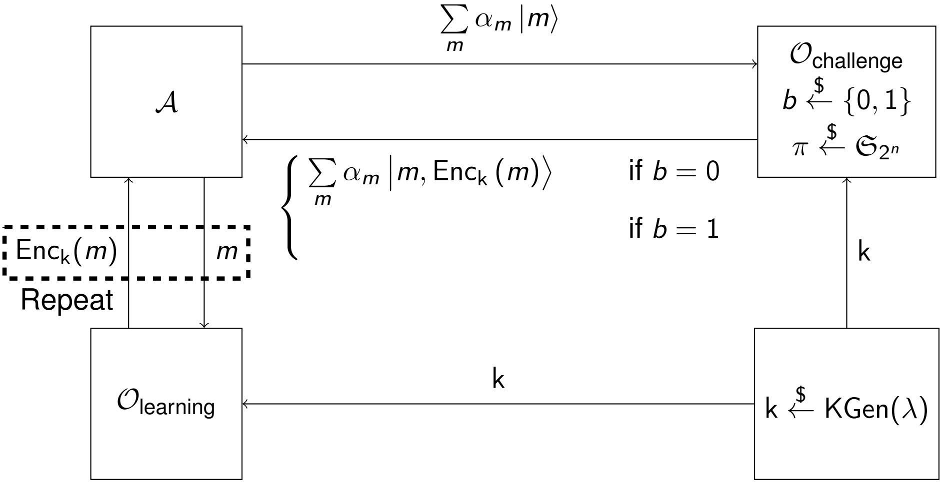
qIND-qCPA-P13 security notion



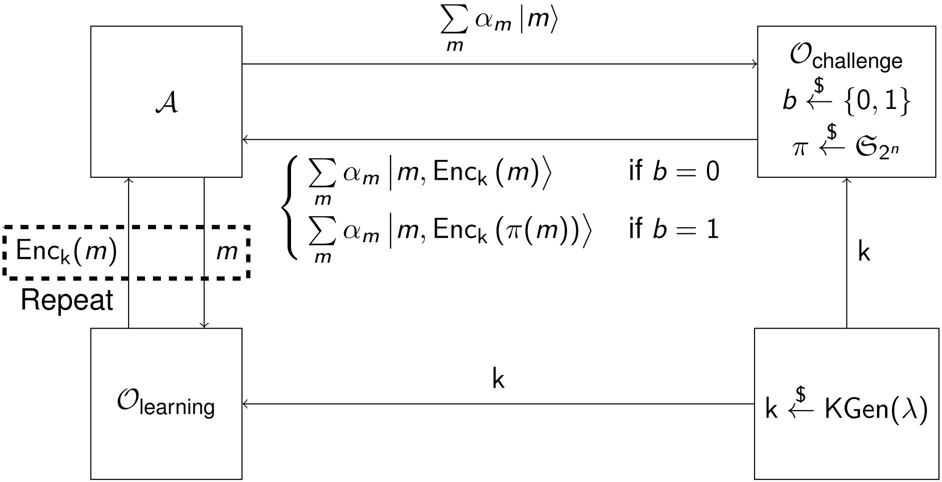
qIND-qCPA-P13 security notion



qIND-qCPA-P13 security notion



qIND-qCPA-P13 security notion



Example: qIND-qCPA-P13 insecurity of a stream cipher

$$\mathsf{Enc}_\mathsf{k}(m) = m \oplus s$$

TELECOM Paris

IP PARIS

Example: qIND-qCPA-P13 insecurity of a stream cipher

$$\mathsf{Enc_k}(m) = m \oplus s$$

$\mathcal{A}$ sends $\frac{1}{\sqrt{2^n}} \sum_m |m\rangle$ to the challenge oracle.

Example: qIND-qCPA-P13 insecurity of a stream cipher

$$\mathsf{Enc}_{\mathsf{k}}(m) = m \oplus s$$

$\mathcal{A}$ sends $\frac{1}{\sqrt{2^n}} \sum_m |m\rangle$ to the challenge oracle.

If $b = 0$ $\frac{1}{\sqrt{2^n}} \sum_m |m, m \oplus s\rangle$

Example: qIND-qCPA-P13 insecurity of a stream cipher

$$\mathrm{Enc_k}(m) = m \oplus s$$

$\mathcal{A}$ sends $\frac{1}{\sqrt{2^n}} \sum_m |m\rangle$ to the challenge oracle.

If $b = 0$ $\frac{1}{\sqrt{2^n}} \sum_m |m, m \oplus s\rangle$

If $b = 1$ $\frac{1}{\sqrt{2^n}} \sum_m |m, \pi(m) \oplus s\rangle$

Example: qIND-qCPA-P13 insecurity of a stream cipher

$$\mathrm{Enc_k}(m) = m \oplus s$$

$\mathcal{A}$ sends $\frac{1}{\sqrt{2^n}} \sum_m |m\rangle$ to the challenge oracle.

If $b = 0$ $\quad \frac{1}{\sqrt{2^n}} \sum_m |m, m \oplus s\rangle$

If $b = 1$ $\quad \frac{1}{\sqrt{2^n}} \sum_m |m, \pi(m) \oplus s\rangle$

$|x, y\rangle \rightarrow |x, y \oplus x\rangle$ is a valid transformation.

Example: qIND-qCPA-P13 insecurity of a stream cipher

$$\mathrm{Enc_k}(m) = m \oplus s$$

$\mathcal{A}$ sends $\frac{1}{\sqrt{2^n}} \sum_m |m\rangle$ to the challenge oracle.

If $b = 0$ $\frac{1}{\sqrt{2^n}} \sum_m |m, m \oplus s\rangle$

If $b = 1$ $\frac{1}{\sqrt{2^n}} \sum_m |m, \pi(m) \oplus s\rangle$

$|x, y\rangle \rightarrow |x, y \oplus x\rangle$ is a valid transformation.

If $b = 0$ $\frac{1}{\sqrt{2^n}} \sum_m |m, s\rangle$

TELECOM Paris

IP PARIS

Example: qIND-qCPA-P13 insecurity of a stream cipher

$$\mathrm{Enc_k}(m) = m \oplus s$$

$\mathcal{A}$ sends $\frac{1}{\sqrt{2^n}} \sum_m |m\rangle$ to the challenge oracle.

If $b = 0$ $\frac{1}{\sqrt{2^n}} \sum_m |m, m \oplus s\rangle$

If $b = 1$ $\frac{1}{\sqrt{2^n}} \sum_m |m, \pi(m) \oplus s\rangle$

$|x, y\rangle \to |x, y \oplus x\rangle$ is a valid transformation.

If $b = 0$ $\frac{1}{\sqrt{2^n}} \sum_m |m, s\rangle$

If $b = 1$ $\frac{1}{\sqrt{2^n}} \sum_m |m, m \oplus \pi(m) \oplus s\rangle$

TELECOM Paris

IP PARIS

Example: qIND-qCPA-P13 insecurity of a stream cipher

$$\mathrm{Enc_k}(m) = m \oplus s$$

$\mathcal{A}$ sends $\frac{1}{\sqrt{2^n}} \sum_m |m\rangle$ to the challenge oracle.

If $b = 0$ $\frac{1}{\sqrt{2^n}} \sum_m |m, m \oplus s\rangle$

If $b = 1$ $\frac{1}{\sqrt{2^n}} \sum_m |m, \pi(m) \oplus s\rangle$

$|x, y\rangle \to |x, y \oplus x\rangle$ is a valid transformation.

If $b = 0$ $\frac{1}{\sqrt{2^n}} \sum_m |m, s\rangle$

If $b = 1$ $\frac{1}{\sqrt{2^n}} \sum_m |m, m \oplus \pi(m) \oplus s\rangle$

In the Hadamard basis: $\mathbb{P}[|0\rangle] = 1$ if $b = 0$, $\frac{1}{2^{n-1}}$ otherwise.

TELECOM Paris

IP PARIS

Example: qIND-qCPA-P13 insecurity of a stream cipher

$$\mathsf{Enc}_\mathsf{k}(m) = m \oplus s$$

$\mathcal{A}$ sends $\frac{1}{\sqrt{2^n}} \sum_m |m\rangle$ to the challenge oracle.

If $b = 0$ $\quad \frac{1}{\sqrt{2^n}} \sum_m |m, m \oplus s\rangle$

If $b = 1$ $\quad \frac{1}{\sqrt{2^n}} \sum_m |m, \pi(m) \oplus s\rangle$

$|x, y\rangle \to |x, y \oplus x\rangle$ is a valid transformation.

If $b = 0$ $\quad \frac{1}{\sqrt{2^n}} \sum_m |m, s\rangle$

If $b = 1$ $\quad \frac{1}{\sqrt{2^n}} \sum_m |m, m \oplus \pi(m) \oplus s\rangle$

In the Hadamard basis: $\mathbb{P}[|0\rangle] = 1$ if $b = 0$, $\frac{1}{2^{n-1}}$ otherwise. No (other) property of Enc has been used!

TELECOM Paris

IP PARIS

Public randomization is qIND-qCPA-P5-insecure

Public randomization is qIND-qCPA-P5-insecure

Suppose:

Public randomization is qIND-qCPA-P5-insecure

Suppose:

- $\mathsf{Enc}_{\mathsf{k}}(x, r) = f_{\mathsf{k}}(g(x, r))$ with g being public (e.g. $\texttt{XOR}$)

Public randomization is qIND-qCPA-P5-insecure

Suppose:

- $\mathsf{Enc}_\mathsf{k}(x, r) = f_\mathsf{k}(g(x, r))$ with g being public (e.g. $\mathtt{XOR}$)
- r is known by the adversary

Public randomization is qIND-qCPA-P5-insecure

Suppose:

- $\mathsf{Enc}_\mathsf{k}(x, r) = f_\mathsf{k}(g(x, r))$ with g being public (e.g. $\mathtt{XOR}$)
- r is known by the adversary

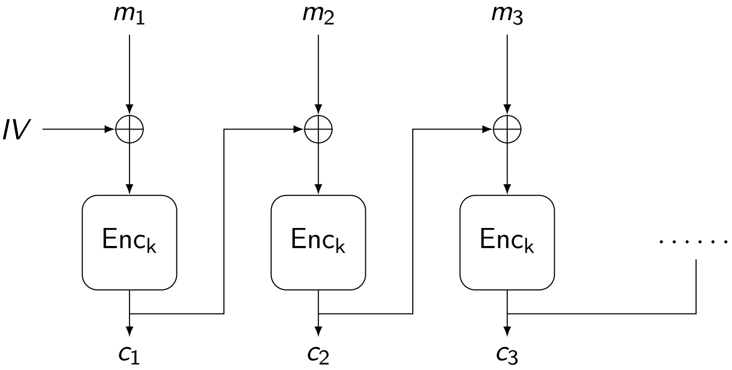
Then Enc is qIND-qCPA-P5-insecure.

Public randomization is qIND-qCPA-P5-insecure

Suppose:

- $\mathsf{Enc}_\mathsf{k}(x, r) = f_\mathsf{k}(g(x, r))$ with g being public (e.g. $\mathtt{XOR}$)
- r is known by the adversary

Then Enc is qIND-qCPA-P5-insecure.



One-to-one encryption is qIND-qCPA-P8-insecure

One-to-one encryption is qIND-qCPA-P8-insecure

Suppose:

- $\mathsf{Enc}_\mathsf{k} : \{0,1\}^m \times \{0,1\}^p \to \{0,1\}^n$, with m being the message length

One-to-one encryption is qIND-qCPA-P8-insecure

Suppose:

- $\mathsf{Enc_k} : \{0,1\}^m \times \{0,1\}^p \to \{0,1\}^n$, with m being the message length

Then there is an adversary with advantage $\frac{2^m}{2^n}$ in the qIND-qCPA-P8 game of Enc.

One-to-one encryption is qIND-qCPA-P8-insecure

Suppose:

- $\mathsf{Enc}_\mathsf{k} : \{0,1\}^m \times \{0,1\}^p \rightarrow \{0,1\}^n$, with m being the message length

Then there is an adversary with advantage $\frac{2^m}{2^n}$ in the qIND-qCPA-P8 game of Enc.

Invalidates most modes of operation. . .

One-to-one encryption is qIND-qCPA-P8-insecure

Suppose:

- $\mathsf{Enc}_k : \{0,1\}^m \times \{0,1\}^p \to \{0,1\}^n$, with m being the message length

Then there is an adversary with advantage $\frac{2^m}{2^n}$ in the qIND-qCPA-P8 game of Enc.

Invalidates most modes of operation. . . **without authenticity tag.**

TELECOM Paris IP PARIS

Conclusion

Shown results

- Adapted Anand et al.'s results to all IND-qCPA notions

Conclusion

Shown results

- Adapted Anand et al.'s results to all IND-qCPA notions
- qIND-qCPA-P13-insecurity of CBC, CTR, OFB and CFB

Conclusion

Shown results

- Adapted Anand et al.'s results to all IND-qCPA notions
- qIND-qCPA-P13-insecurity of CBC, CTR, OFB and CFB
- Two general results on qIND-qCPA-P5 and qIND-qCPA-P8 security

Conclusion

Shown results

- Adapted Anand et al.'s results to all IND-qCPA notions
- qIND-qCPA-P13-insecurity of CBC, CTR, OFB and CFB
- Two general results on qIND-qCPA-P5 and qIND-qCPA-P8 security

Relevance of the qIND-qCPA security notions

- Attacks are generic: how bad is it for a scheme to be qIND-qCPA-P13-insecure?

Conclusion

Shown results

- Adapted Anand et al.'s results to all IND-qCPA notions
- qIND-qCPA-P13-insecurity of CBC, CTR, OFB and CFB
- Two general results on qIND-qCPA-P5 and qIND-qCPA-P8 security

Relevance of the qIND-qCPA security notions

- Attacks are generic: how bad is it for a scheme to be qIND-qCPA-P13-insecure?
- No equivalent semantic security notion for most qIND-qCPA notions

Conclusion

Shown results

- Adapted Anand et al.'s results to all IND-qCPA notions
- qIND-qCPA-P13-insecurity of CBC, CTR, OFB and CFB
- Two general results on qIND-qCPA-P5 and qIND-qCPA-P8 security

Relevance of the qIND-qCPA security notions

- Attacks are generic: how bad is it for a scheme to be qIND-qCPA-P13-insecure?
- No equivalent semantic security notion for most qIND-qCPA notions

Takeaway: we need to perform more research to define a useful qIND-qCPA notion.

Thank you!

What are the qIND-qCPA security notions?

Two oracles for the IND-CPA game:

$$\begin{aligned} \textbf{Query} &\quad m \rightarrow \mathsf{Enc}_{\mathsf{k}}(m) \\ \textbf{Challenge} &\quad m_0, m_1 \rightarrow \mathsf{Enc}_{\mathsf{k}}\left(m_b\right) \end{aligned}$$

What are the qIND-qCPA security notions?

Two oracles for the IND-CPA game:

Query $m \to \mathrm{Enc}_k(m)$

Challenge $m_0, m_1 \to \mathrm{Enc}_k(m_b)$

Challenge type To choose from:

- Left-or-Right

What are the qIND-qCPA security notions?

Two oracles for the IND-CPA game:

Query $m \to \mathrm{Enc_k}(m)$

Challenge $m_0, m_1 \to$
$\mathrm{Enc_k}\left(m_b\right), \mathrm{Enc_k}\left(m_{\overline{b}}\right)$

Challenge type To choose from:

- Left-or-Right
- 2-ciphertexts

What are the qIND-qCPA security notions?

Two oracles for the IND-CPA game:

Query $m \rightarrow \mathsf{Enc}_{\mathsf{k}}(m)$

Challenge $m \rightarrow \mathsf{Enc}_{\mathsf{k}}\left(\pi^{b}(m)\right)$

Challenge type To choose from:

- Left-or-Right
- 2-ciphertexts
- Real-or-Random

What are the qIND-qCPA security notions?

Two oracles for the IND-CPA game:

Query $m \to \mathsf{Enc_k}(m)$

Challenge $m \to \mathsf{Enc_k}\left(\pi^b(m)\right)$

Challenge type To choose from:

- Left-or-Right
- 2-ciphertexts
- Real-or-Random

Number of challenge queries A single or $\mathsf{poly}(\lambda)$

What are the qIND-qCPA security notions?

Two oracles for the IND-CPA game:

Query $m \rightarrow \mathsf{Enc}_{\mathsf{k}}(m)$

Challenge $m \rightarrow \mathsf{Enc}_{\mathsf{k}}\left(\pi^{b}(m)\right)$

Challenge type To choose from:

- Left-or-Right
- 2-ciphertexts
- Real-or-Random

Number of challenge queries A single or $\mathsf{poly}(\lambda)$

Oracle type To choose from:

- Classical

What are the qIND-qCPA security notions?

Two oracles for the IND-CPA game:

Query $|x, y\rangle \to |x, y \oplus \mathsf{Enc_k}(x)\rangle$

Challenge $|x, y\rangle \to |x, y \oplus \mathsf{Enc_k}\left(\pi^b(x)\right)\rangle$

Challenge type To choose from:

- Left-or-Right
- 2-ciphertexts
- Real-or-Random

Number of challenge queries A single or $\mathsf{poly}(\lambda)$

Oracle type To choose from:

- Classical
- Standard

What are the qIND-qCPA security notions?

Two oracles for the IND-CPA game:

Query $|x\rangle \to \left|x, \mathsf{Enc_k}(x)\right\rangle$

Challenge $|x\rangle \to \left|x, \mathsf{Enc_k}\left(\pi^b(x)\right)\right\rangle$

Challenge type To choose from:

- Left-or-Right
- 2-ciphertexts
- Real-or-Random

Number of challenge queries A single or $\mathsf{poly}(\lambda)$

Oracle type To choose from:

- Classical
- Standard
- Embedding

What are the qIND-qCPA security notions?

Two oracles for the IND-CPA game:

Query $|x\rangle \to \left|\mathsf{Enc}_\mathsf{k}(x)\right\rangle$

Challenge $|x\rangle \to \left|\mathsf{Enc}_\mathsf{k}\left(\pi^b(x)\right)\right\rangle$

Challenge type To choose from:
- Left-or-Right
- 2-ciphertexts
- Real-or-Random

Number of challenge queries A single or $\mathsf{poly}(\lambda)$

Oracle type To choose from:
- Classical
- Standard
- Embedding
- Erasing

What are the qIND-qCPA security notions?

Two oracles for the IND-CPA game:

Query $|x\rangle \to |\mathsf{Enc}_\mathsf{k}(x)\rangle$

Challenge $|x\rangle \to |\mathsf{Enc}_\mathsf{k}(\pi^b(x))\rangle$

Challenge type To choose from:

- Left-or-Right
- 2-ciphertexts
- Real-or-Random

Number of challenge queries A single or $\mathsf{poly}(\lambda)$

Oracle type To choose from:

- Classical
- Standard
- Embedding
- Erasing

$\Longrightarrow$ Many notions, some of them being equivalent.

What are the qIND-qCPA security notions?

Two oracles for the IND-CPA game:

Query $|x\rangle \to |\mathsf{Enc_k}(x)\rangle$

Challenge $|x\rangle \to |\mathsf{Enc_k}(\pi^b(x))\rangle$

Challenge type To choose from:

- Left-or-Right
- 2-ciphertexts
- Real-or-Random

Number of challenge queries A single or $\mathsf{poly}(\lambda)$

Oracle type To choose from:

- Classical
- Standard
- Embedding
- Erasing

$\implies$ Many notions, some of them being equivalent.

$\implies$ 14 different qIND-qCPA notions

Bibliography I

Anand, Mayuresh Vivekanand et al. “Post-Quantum Security of the CBC, CFB, OFB, CTR, and XTS Modes of Operation”. In: *Post-Quantum Cryptography - 7th International Workshop, PQCrypto 2016*. Ed. by Tsuyoshi Takagi. Fukuoka, Japan: Springer, Heidelberg, Germany, Feb. 2016, pp. 44–63. DOI: 10.1007/978-3-319-29360-8_4.

Boneh, Dan and Mark Zhandry. “Secure Signatures and Chosen Ciphertext Security in a Quantum Computing World”. In: *Advances in Cryptology – CRYPTO 2013, Part II*. Ed. by Ran Canetti and Juan A. Garay. Vol. 8043. Lecture Notes in Computer Science. Santa Barbara, CA, USA: Springer, Heidelberg, Germany, Aug. 2013, pp. 361–379. DOI: 10.1007/978-3-642-40084-1_21.

Bibliography II

Carstens, Tore Vincent et al. "Relationships Between Quantum IND-CPA Notions". In: *TCC 2021: 19th Theory of Cryptography Conference, Part I*. Ed. by Kobbi Nissim and Brent Waters. Vol. 13042. Lecture Notes in Computer Science. Raleigh, NC, USA: Springer, Heidelberg, Germany, Nov. 2021, pp. 273–298. DOI: 10.1007/978-3-030-90459-3_9.