Lightweight FHE-based Protocols Achieving Results Consistency for Data Encrypted under Different Keys

Marina Checri, Jean-Paul Bultel, Renaud Sirdey, Aymen Boudguiga

Université Paris-Saclay, CEA, List, F-91120, Palaiseau, France
{marina.checri, jean-paul.bultel, renaud.sirdey, aymen.boudguiga}@cea.fr

October 17, 2023

The Need for Homomorphic Encryption Protocols

The Need for Homomorphic Encryption Protocols

What are we talking about?

The Need for Homomorphic Encryption Protocols

What are we talking about?

$$[x] + [y] \rightarrow [x + y]$$
$$[x] \times [y] \rightarrow [x \times y]$$

The Need for Homomorphic Encryption Protocols

What are we talking about?

$$m \xrightarrow{\quad f \quad} f(m)$$

$$[x] + [y] \rightarrow [x + y]$$
$$[x] \times [y] \rightarrow [x \times y]$$

The Need for Homomorphic Encryption Protocols

What are we talking about?

$$m \xrightarrow{\quad f \quad} f(m)$$

$$[x] + [y] \rightarrow [x + y]$$
$$[x] \times [y] \rightarrow [x \times y]$$

$$[m] \qquad\qquad [f(m)]$$

The Need for Homomorphic Encryption Protocols

What are we talking about?

$$m \xrightarrow{\quad f \quad} f(m)$$

$$[x] + [y] \rightarrow [x + y]$$
$$[x] \times [y] \rightarrow [x \times y]$$

$$[m] \xrightarrow[\mathrm{Eval}(f,\,[m])]{} [f(m)]$$

The Need for Homomorphic Encryption Protocols

What are we talking about?

$$[x] + [y] \rightarrow [x + y]$$
$$[x] \times [y] \rightarrow [x \times y]$$

$$\begin{tikzcd}
m \arrow[r, "f"] \arrow[d, bend left, "\mathrm{Enc}(m)"] & f(m) \\
{[m]} \arrow[u, bend left, "\mathrm{Dec}([m])"] \arrow[r, "\mathrm{Eval}(f,\,[m])"'] & {[f(m)]}
\end{tikzcd}$$

The Need for Homomorphic Encryption Protocols

What are we talking about?

$$[x] + [y] \rightarrow [x + y]$$
$$[x] \times [y] \rightarrow [x \times y]$$

$$\begin{tikzcd}
m \arrow[r, "f"] \arrow[d, bend left, "\mathrm{Enc}(m)"] & f(m) \\
{[m]} \arrow[r, "\mathrm{Eval}(f,\,[m])"'] \arrow[u, bend left, "\mathrm{Dec}([m])"] & {[f(m)]} \arrow[u, "\mathrm{Dec}([f(m)])"']
\end{tikzcd}$$

The Need for Homomorphic Encryption Protocols

What are we talking about?

$$[x] + [y] \rightarrow [x + y]$$
$$[x] \times [y] \rightarrow [x \times y]$$

$$\begin{tikzcd}
m \arrow[r, "f"] \arrow[d, bend left, "\mathrm{Enc}(m)"] & f(m) \\
{[m]} \arrow[u, bend left, "\mathrm{Dec}([m])"] \arrow[r, "\mathrm{Eval}(f,\,[m])"'] & {[f(m)]} \arrow[u, "\mathrm{Dec}([f(m)])"']
\end{tikzcd}$$

What for?

The Need for Homomorphic Encryption Protocols

What are we talking about?

$$[x] + [y] \rightarrow [x + y]$$
$$[x] \times [y] \rightarrow [x \times y]$$

$$\begin{tikzcd}
m \arrow[r, "f"] \arrow[d, bend left, "\mathrm{Enc}(m)"] & f(m) \\
{[m]} \arrow[u, bend left, "\mathrm{Dec}([m])"] \arrow[r, "\mathrm{Eval}(f,\,[m])"'] & {[f(m)]} \arrow[u, "\mathrm{Dec}([f(m)])"']
\end{tikzcd}$$

What for?

Data confidentiality *during* calculations

Typically, for Cloud Computing

A Multi-user / Multi-key Framework

Did you say multi-user?

A Multi-user / Multi-key Framework

Did you say multi-user?

- Real context → several data from different contributors
- A user cannot trust the other users
- One key-pair per user ⇒ Multiple keys
- Need of multi-user settings based on FHE
- Medical secrecy, analysis of sensitive data, ...

A Multi-user / Multi-key Framework

Did you say multi-user?

- Real context → several data from different contributors
- A user cannot trust the other users
- One key-pair per user ⇒ Multiple keys
- Need of multi-user settings based on FHE
- Medical secrecy, analysis of sensitive data, ...

Medical secrecy

A Multi-user / Multi-key Framework

Did you say multi-user?

- Real context → several data from different contributors
- A user cannot trust the other users
- One key-pair per user ⇒ Multiple keys
- Need of multi-user settings based on FHE
- Medical secrecy, analysis of sensitive data, ...

Medical secrecy

Financial domain

A Multi-user / Multi-key Framework

Did you say multi-user?

- Real context → several data from different contributors
- A user cannot trust the other users
- One key-pair per user ⇒ Multiple keys
- Need of multi-user settings based on FHE
- Medical secrecy, analysis of sensitive data, ...

Medical secrecy

Financial domain

Analysis of sensitive data

A Multi-user / Multi-key Framework

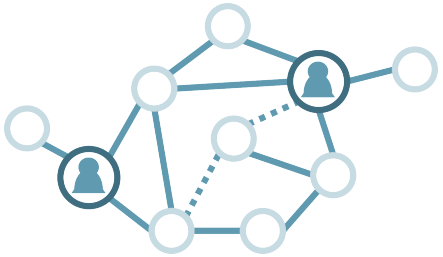
Did you say multi-user?

- Real context → several data from different contributors
- A user cannot trust the other users
- One key-pair per user ⇒ Multiple keys
- Need of multi-user settings based on FHE
- Medical secrecy, analysis of sensitive data, ...

Medical secrecy

Financial domain

Analysis of sensitive data



Secure discovery of friends in social networks

Prerequisite: Ensure Results Consistency

How can users detect those encrypted messages intended for them?

Prerequisite: Ensure Results Consistency

🤔 How can users detect those encrypted messages intended for them?

👉 Detect key inconsistency with a padding of zeroes

Prerequisite: Ensure Results Consistency

How can users detect those encrypted messages intended for them?

Detect key inconsistency with a padding of zeroes

$\hookrightarrow$ Decrypting zero with a wrong key yields a random number

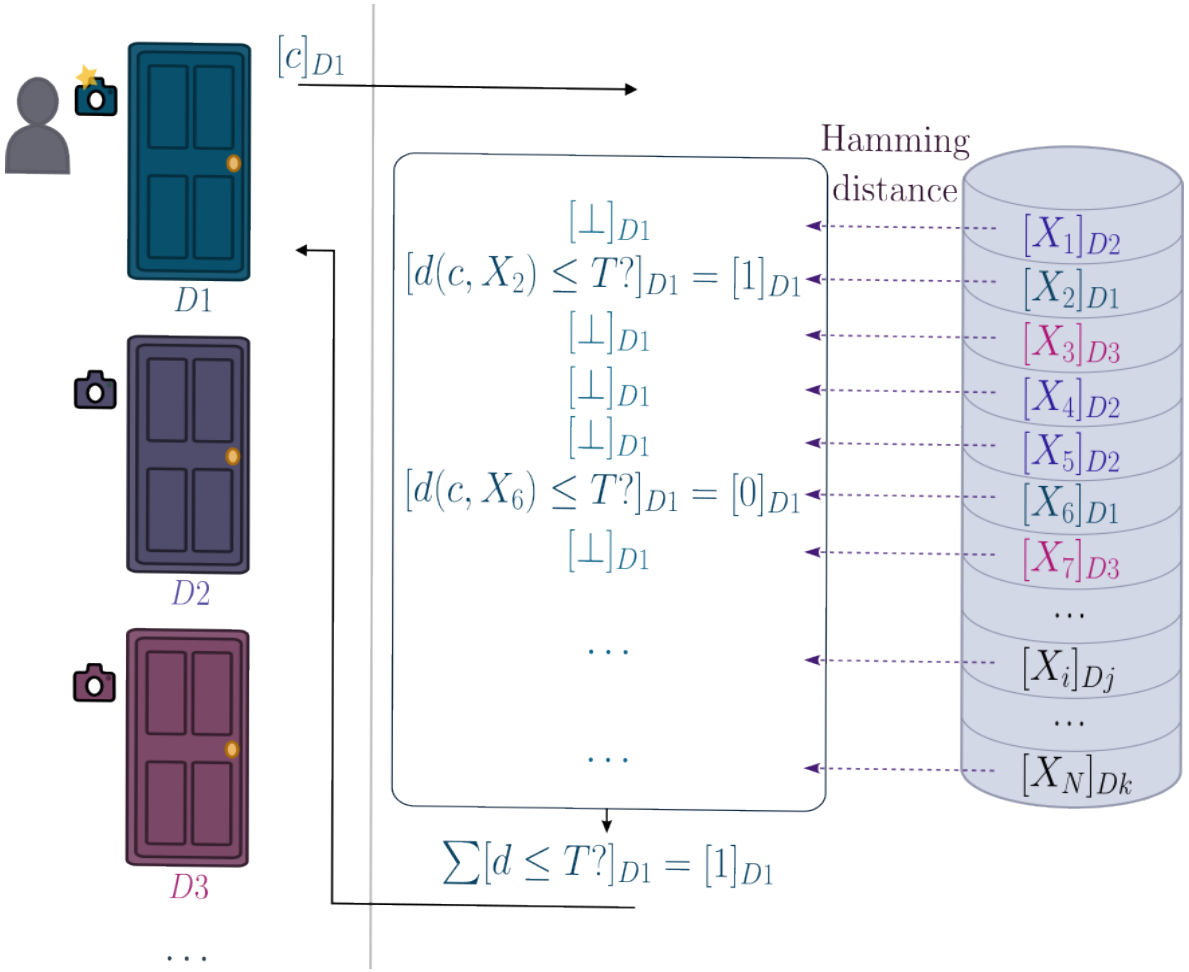
$\hookrightarrow$ Zero padding makes it possible to sort valid results from random ones

$\hookrightarrow$ Assuming a uniform distribution over $\mathbb{F}_q$
$\Rightarrow$ When decrypting $[\underbrace{00\cdots0}_{\ell}]$, the probability of a false positive is $1/q^\ell$

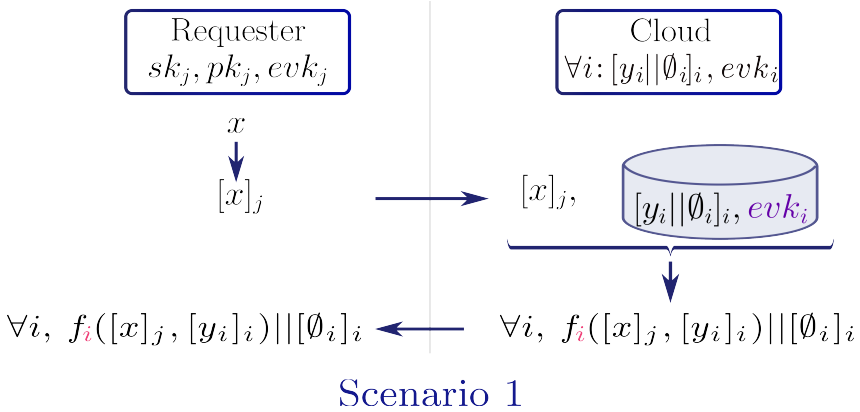
A Use Case: Regulate Accesses to Secured Rooms

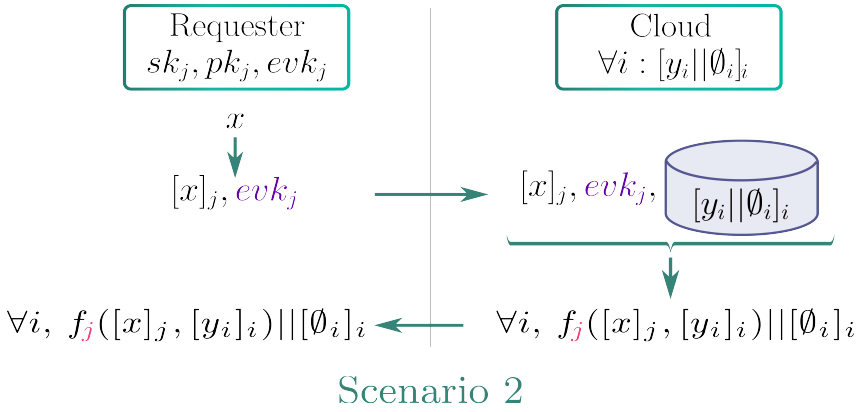
The server:

- ↪ grants or denies room access, according to user's accreditation.
- ↪ must learn nothing about the admission policy or room attendance.



An Incremental Approach: Scenarii 1 and 2

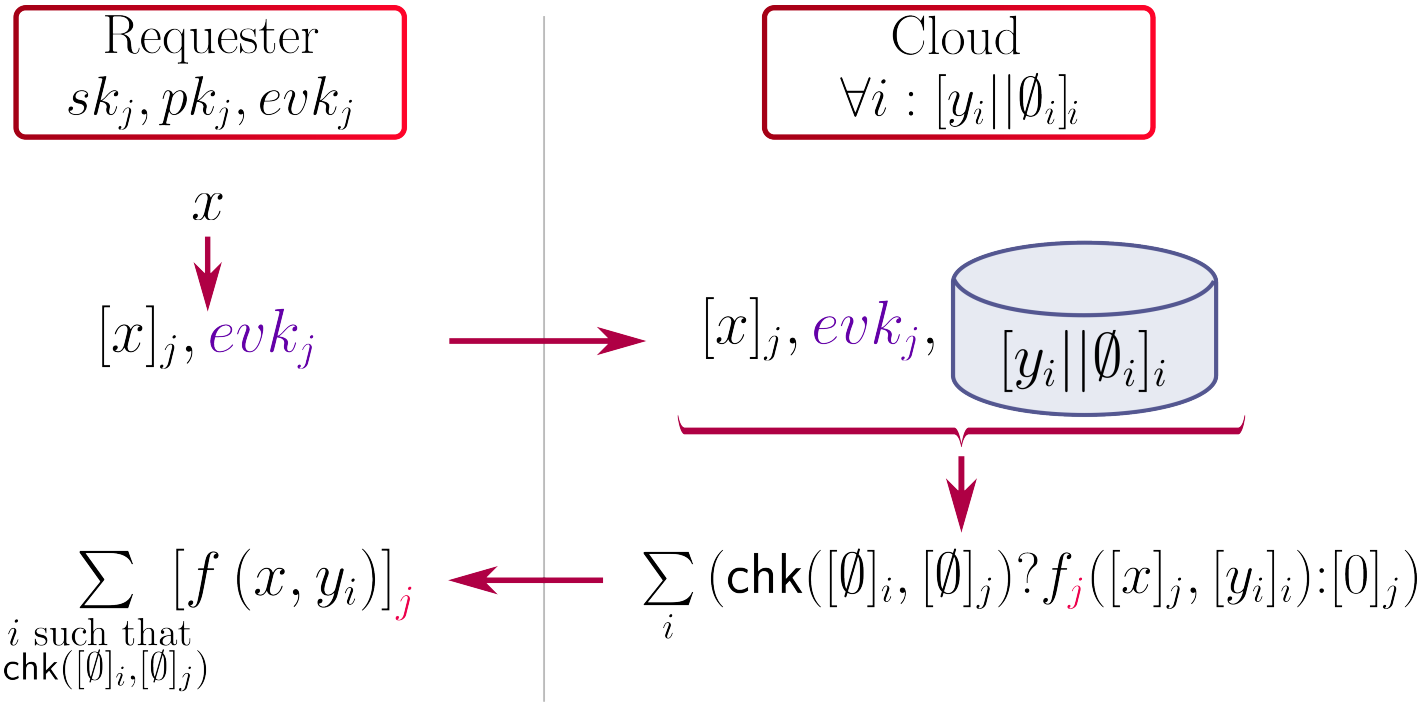




☑ Produce consistent results derived only from data encrypted under the requester's key.

☑ Avoid transmissions of evks by the contributors

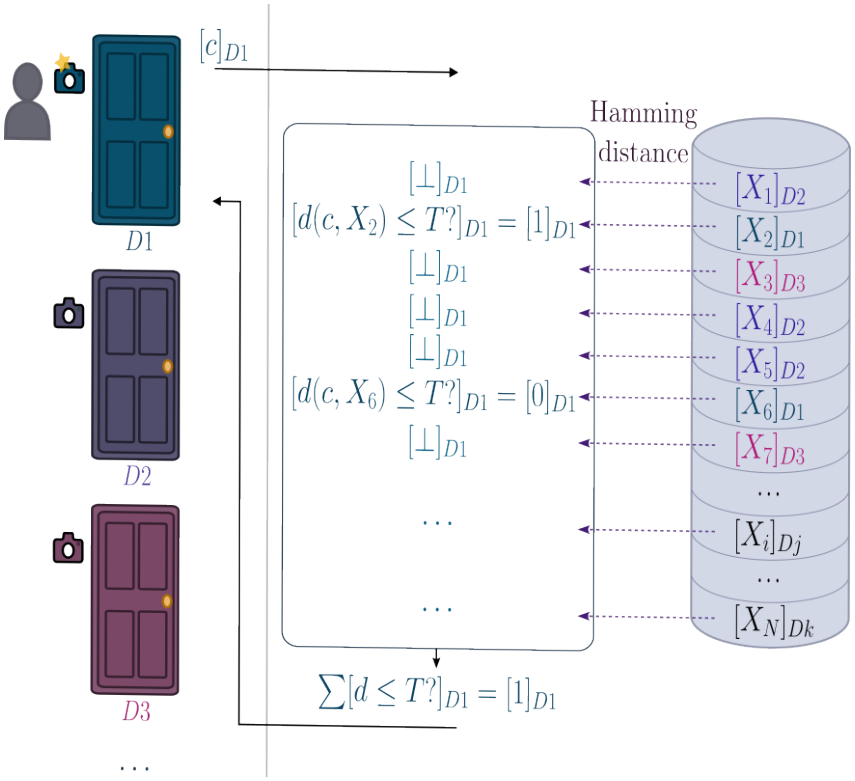
An Incremental Approach: Scenario 3



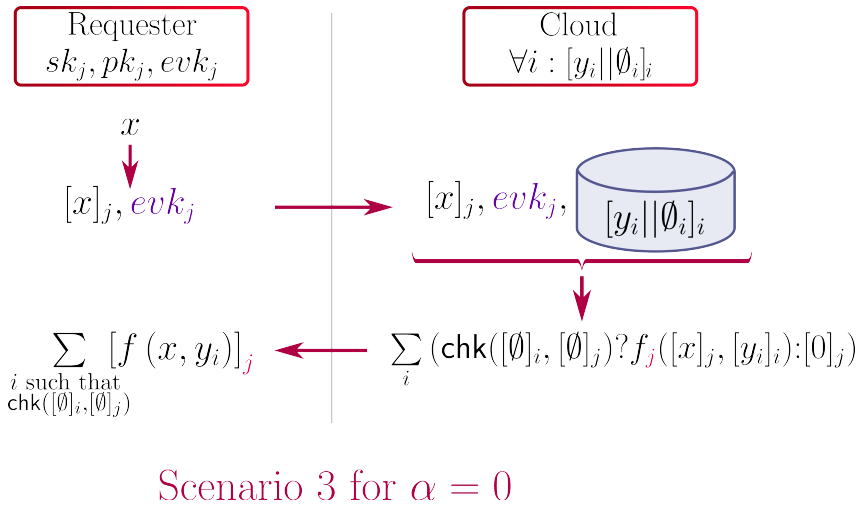
Scenario 3 for $\alpha = 0$

- ☑ Result compactness
- ☑ No need for post-decryption padding verification for the requester

Our Use Case is Addressed by Scenario 3



(a) Use case



(b) Scenario 3 - last scenario

$$[b] ? [m] : [\alpha] \iff ([m] - [\alpha]) \cdot [b] + [\alpha] = \begin{cases} [m] & \text{if } b = 1 \\ [\alpha] & \text{if } b = 0 \end{cases}$$

Key Forcing Subtility with TFHE

Key Forcing Subtility with TFHE

TFHE is not natively designed for multi-user operations

Key Forcing Subtility with TFHE

FHE and noise

FHE encryption	$\rightarrow$	add noise for security
Homomorphic operations	$\rightarrow$	increase the noise
Bootstrapping	$\rightarrow$	to reduce the noise
		= homomorphic decryption

Key Forcing Subtility with TFHE

FHE and noise

FHE encryption	$\rightarrow$	add noise for security
Homomorphic operations	$\rightarrow$	increase the noise
Bootstrapping	$\rightarrow$	to reduce the noise
		= homomorphic decryption

TFHE Bootstrapping key

Bootstrapping key = evaluation key

Bootstrapping key = encryption of the private key

Key Forcing Subtility with TFHE

FHE and noise

FHE encryption	$\rightarrow$	add noise for security
Homomorphic operations	$\rightarrow$	increase the noise
Bootstrapping	$\rightarrow$	to reduce the noise
		= homomorphic decryption

TFHE Bootstrapping key

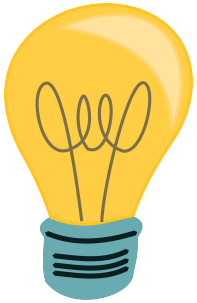
Bootstrapping key = evaluation key

Bootstrapping key = encryption of the private key

Multi-user framework

$\hookrightarrow$ The encryption key used does not always match the bootstrapping key.

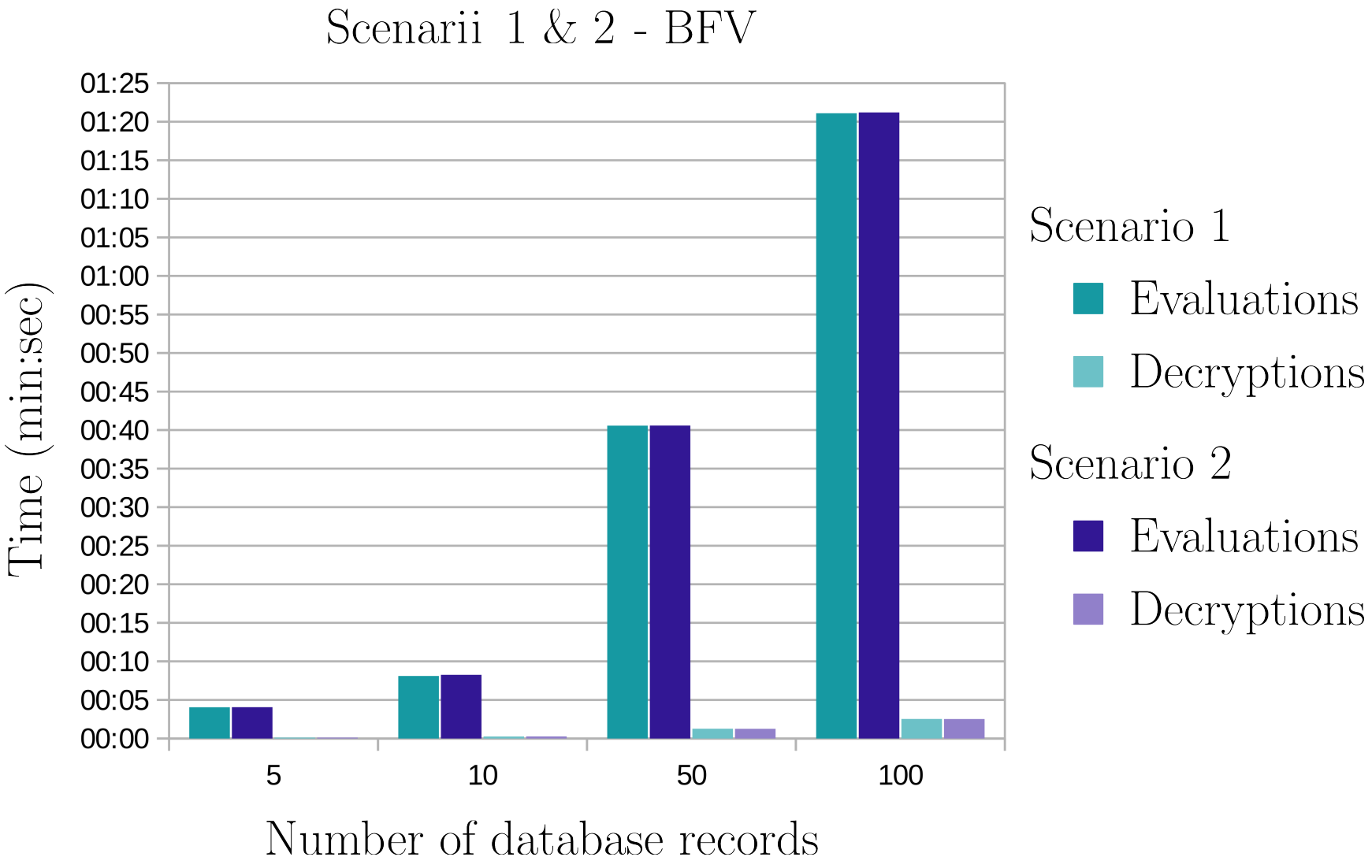
Key Forcing Subtility with TFHE



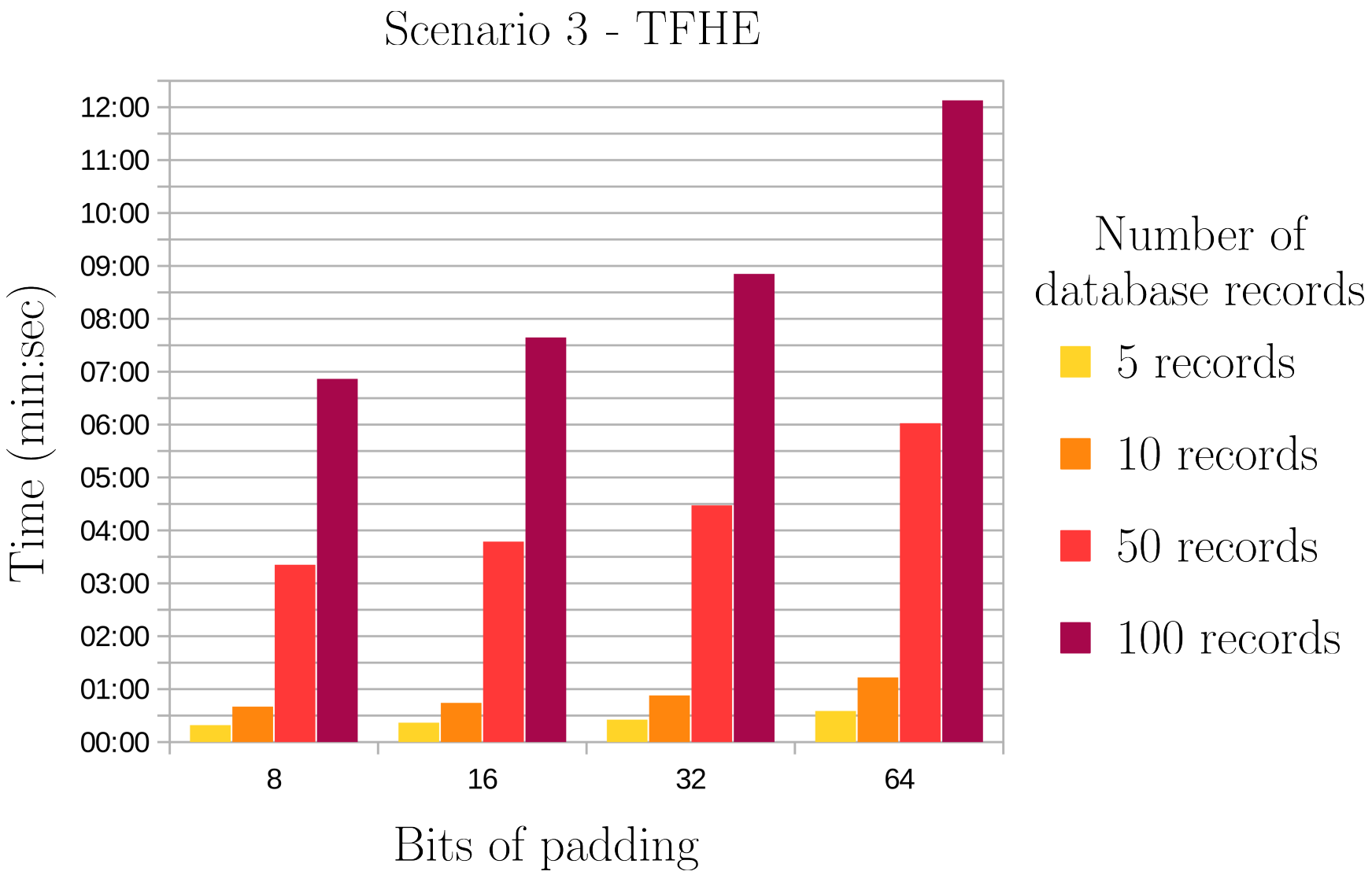
$$
\begin{aligned}
& \mathrm{JFK}(\varkappa_{\mathrm{bk}_{RK}}, [a]_{\mathrm{pk}_{RK}}, [b]_{\mathrm{pk}_{RK}}) \\
= \; & [a]_{\mathrm{pk}_{RK}} \; \varkappa_{\mathrm{bk}_{RK}} \; \underbrace{([1]_{\mathrm{pk}_{RK}} \; \&_{\mathrm{bk}_{RK}} \; [b]_{\mathrm{pk}_{RK}})}_{[b]_{\mathrm{pk}_{RK}}} \\
= \; & [a]_{\mathrm{pk}_{RK}} \; \varkappa_{\mathrm{bk}_{RK}} \; [b]_{\mathrm{pk}_{RK}} \\
= \; & [a \varkappa b]_{\mathrm{pk}_{RK}}
\end{aligned}
$$

$$
\begin{aligned}
& \mathrm{JFK}(\varkappa_{\mathrm{bk}_{RK}}, [a]_{\mathrm{pk}_{RK}}, [b]_{\mathrm{pk}_{WK}}) \\
= \; & [a]_{\mathrm{pk}_{RK}} \; \varkappa_{\mathrm{bk}_{RK}} \; \underbrace{([1]_{\mathrm{pk}_{RK}} \; \&_{\mathrm{bk}_{RK}} \; [b]_{\mathrm{pk}_{WK}})}_{[\$]_{\mathrm{pk}_{RK}}} \\
= \; & [a]_{\mathrm{pk}_{RK}} \; \varkappa_{\mathrm{bk}_{RK}} \; [\$]_{\mathrm{pk}_{RK}} \\
= \; & [\$]_{\mathrm{pk}_{RK}}
\end{aligned}
$$

Time Analysis of Scenarii 1 and 2



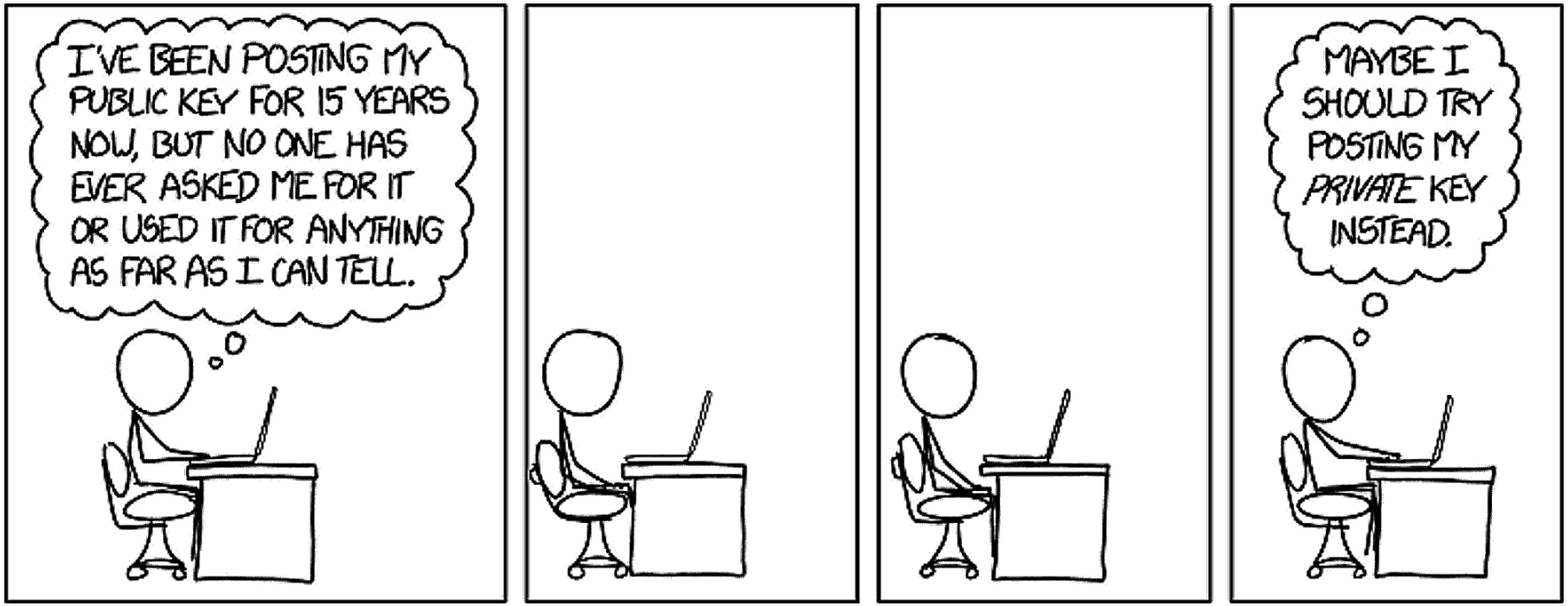
Time Analysis of Scenario 3



Key Takeaways

- Scenarii of increasing practical relevance and usefulness
- Lightweight multi-user setting (one requester per request)
- Calculations on data from different contributors under different keys
- Data and results confidentiality
- Results consistency
- Untraceability of contributors by requesters

Thank you for your kind attention!



credit: xkcd.com