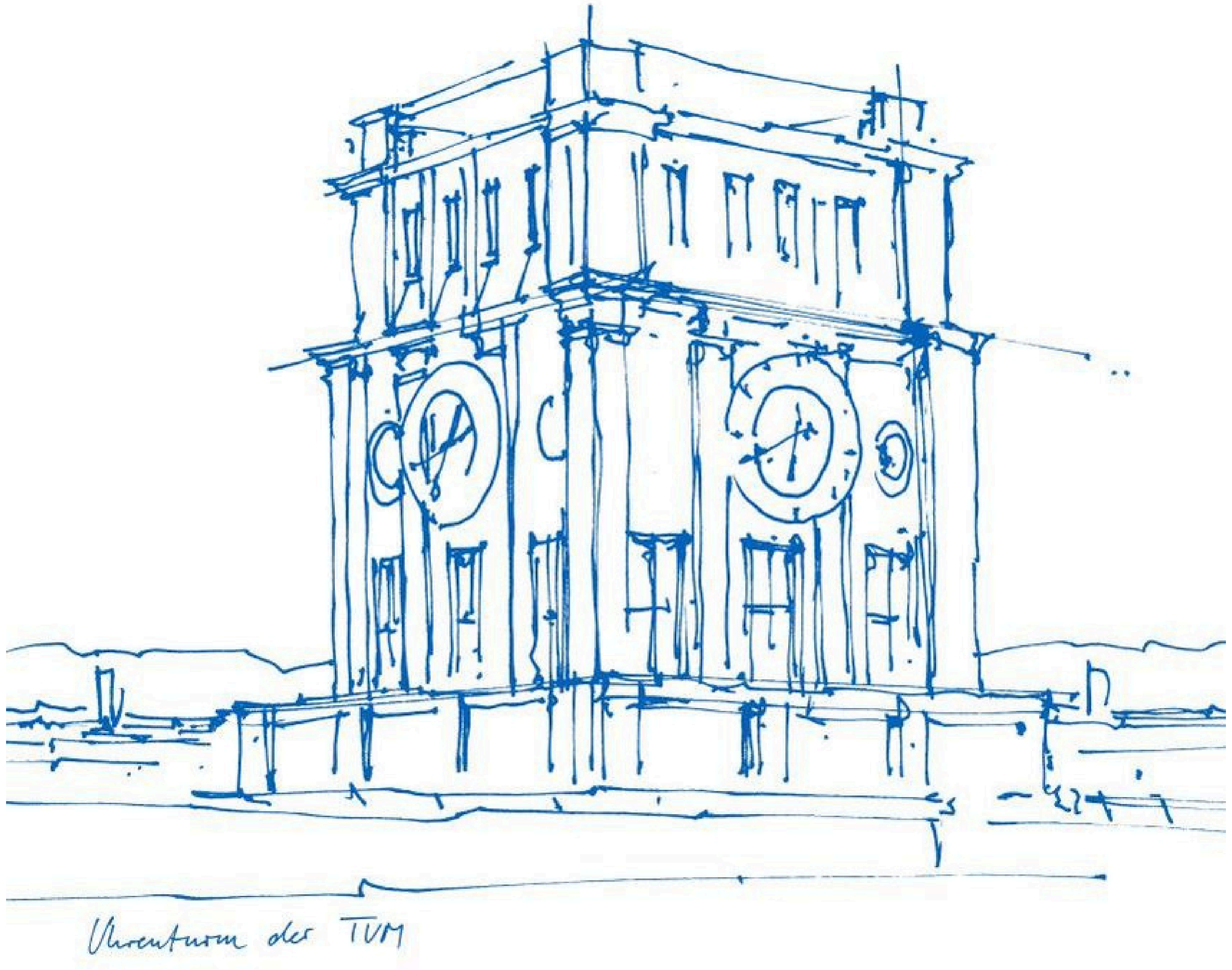
School of Computation, Information and Technology
http://www.ce.cit.tum.de/lti
Technical University of Munich

Information Theoretic Analysis of a Quantum PUF



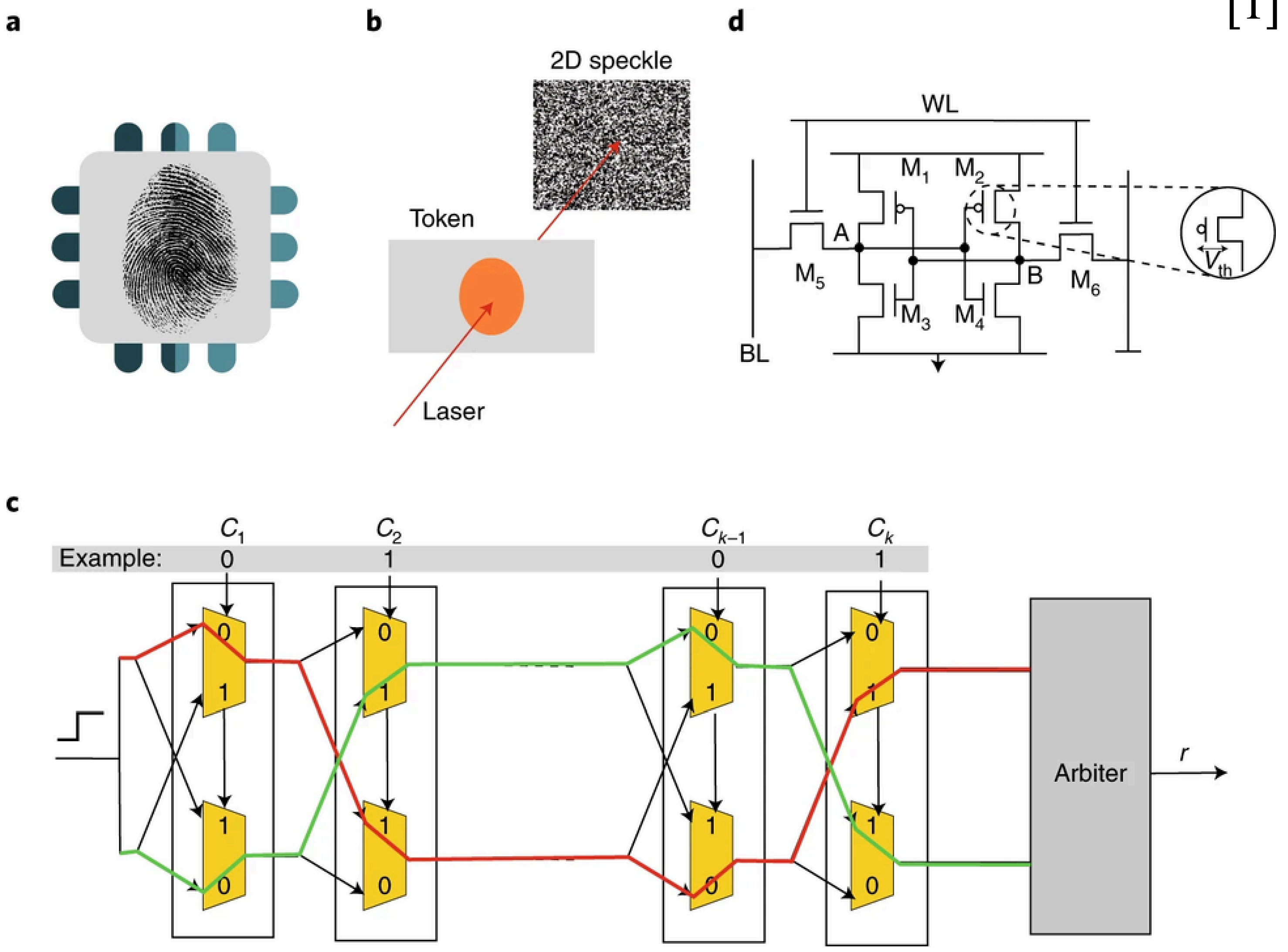
Kumar Nilesh, Christian Deppe and Holger Boche
Chair of Theoretical Information Technology
Technical University of Munich

ISIT July 2024

PUFs
Definition

PUF, is a **physical object** whose operation **cannot be reproduced** ("cloned") in **physical way** (by making another system using the same technology), that for a given input and conditions (challenge), provides a physically defined "**digital fingerprint**" output (response), that serves as a unique identifier.[2]

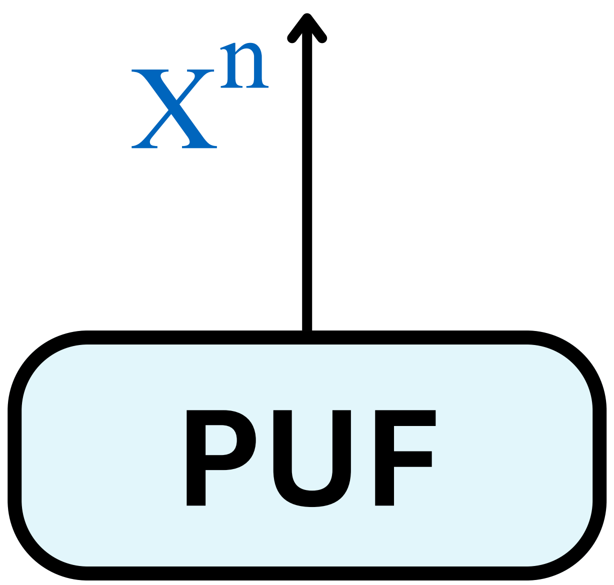
[1]



A PUF is a physical entity embodied in a physical structure.

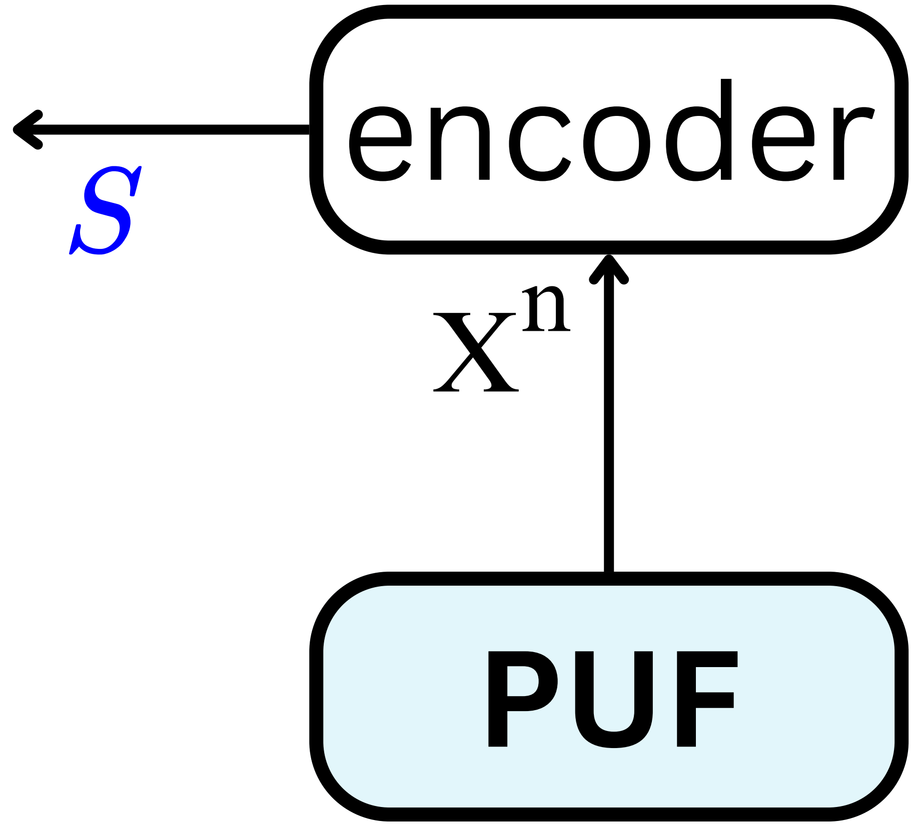
[1] Gao, et al. "Physical unclonable functions." Nature Electronics 3.2 (2020): 81-91.
[2] Wikipedia.org : "Physical unclonable functions."

PUFs
Source Model



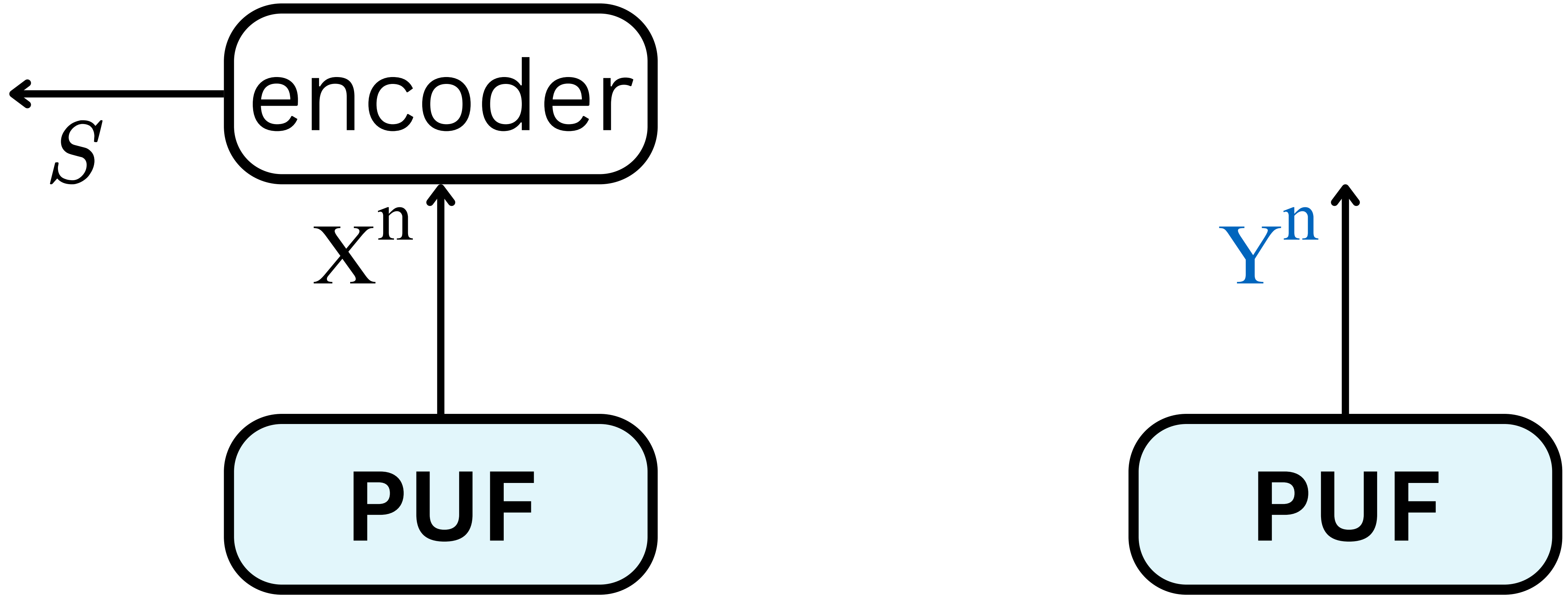
PUFs

Source Model



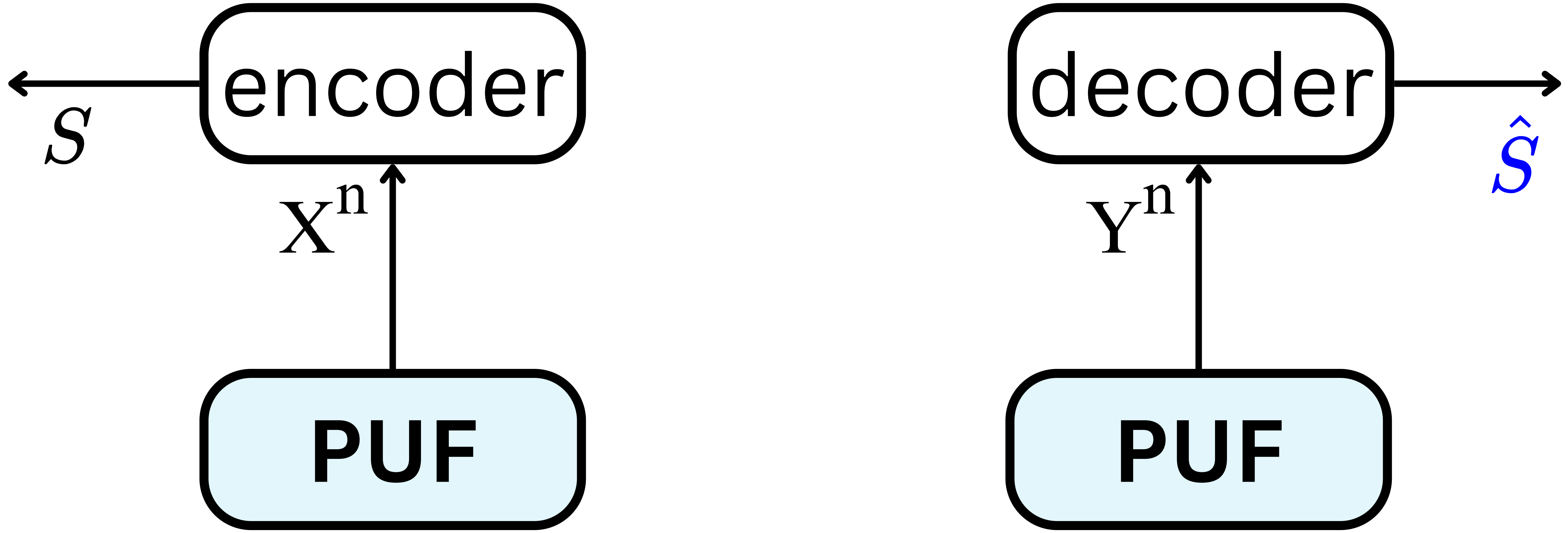
PUFs

Source Model

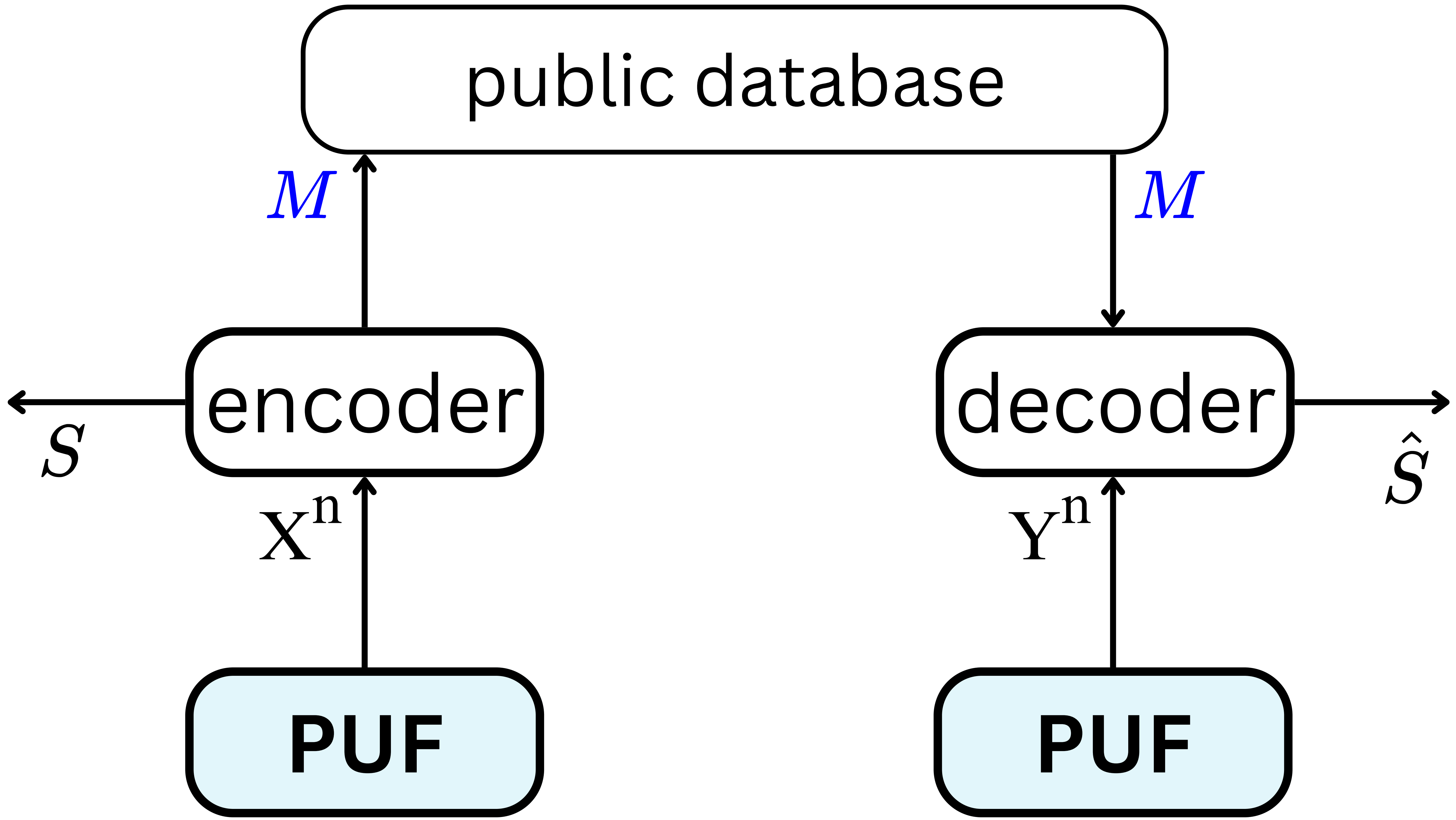


PUFs

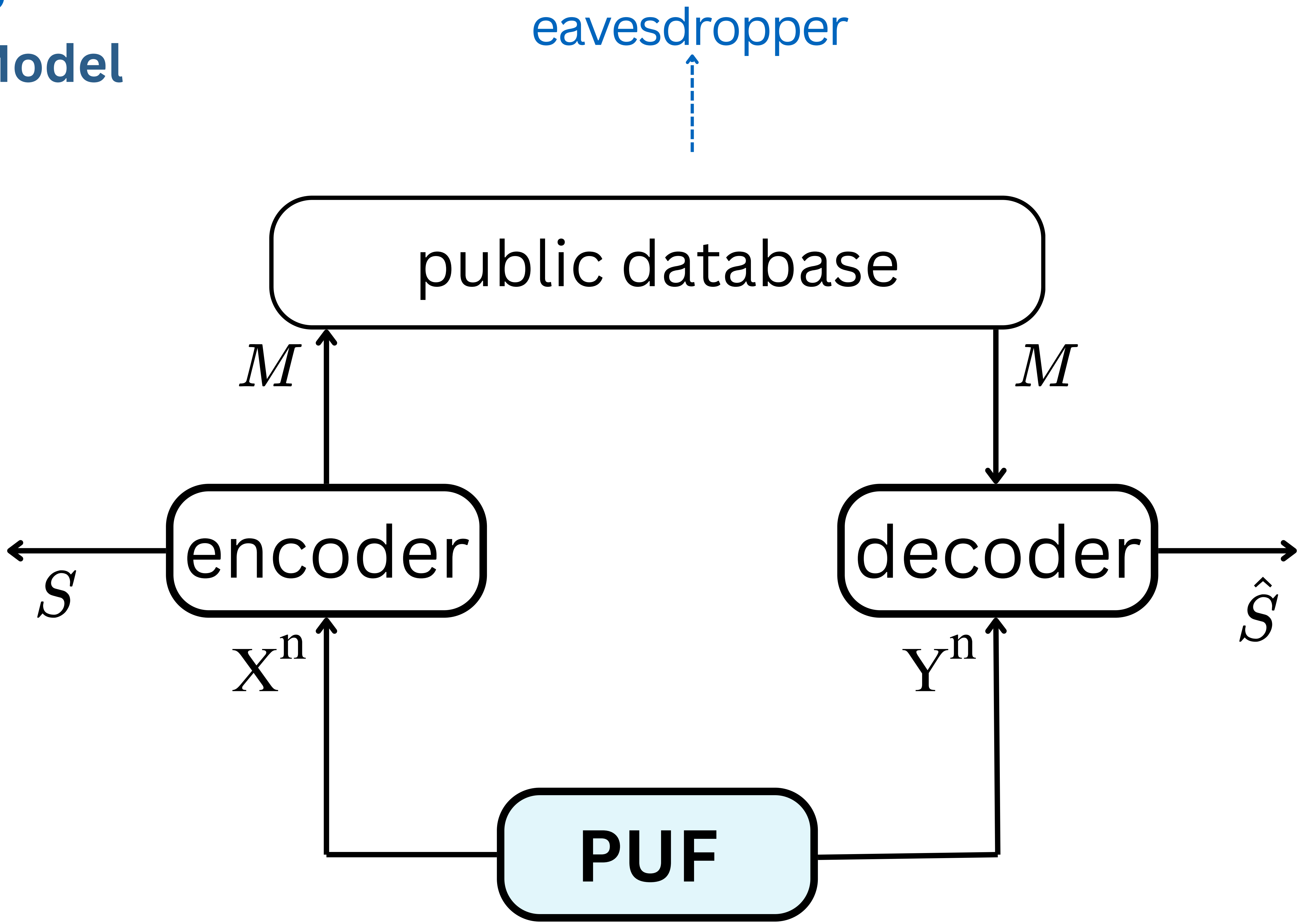
Source Model



PUFs
Source Model



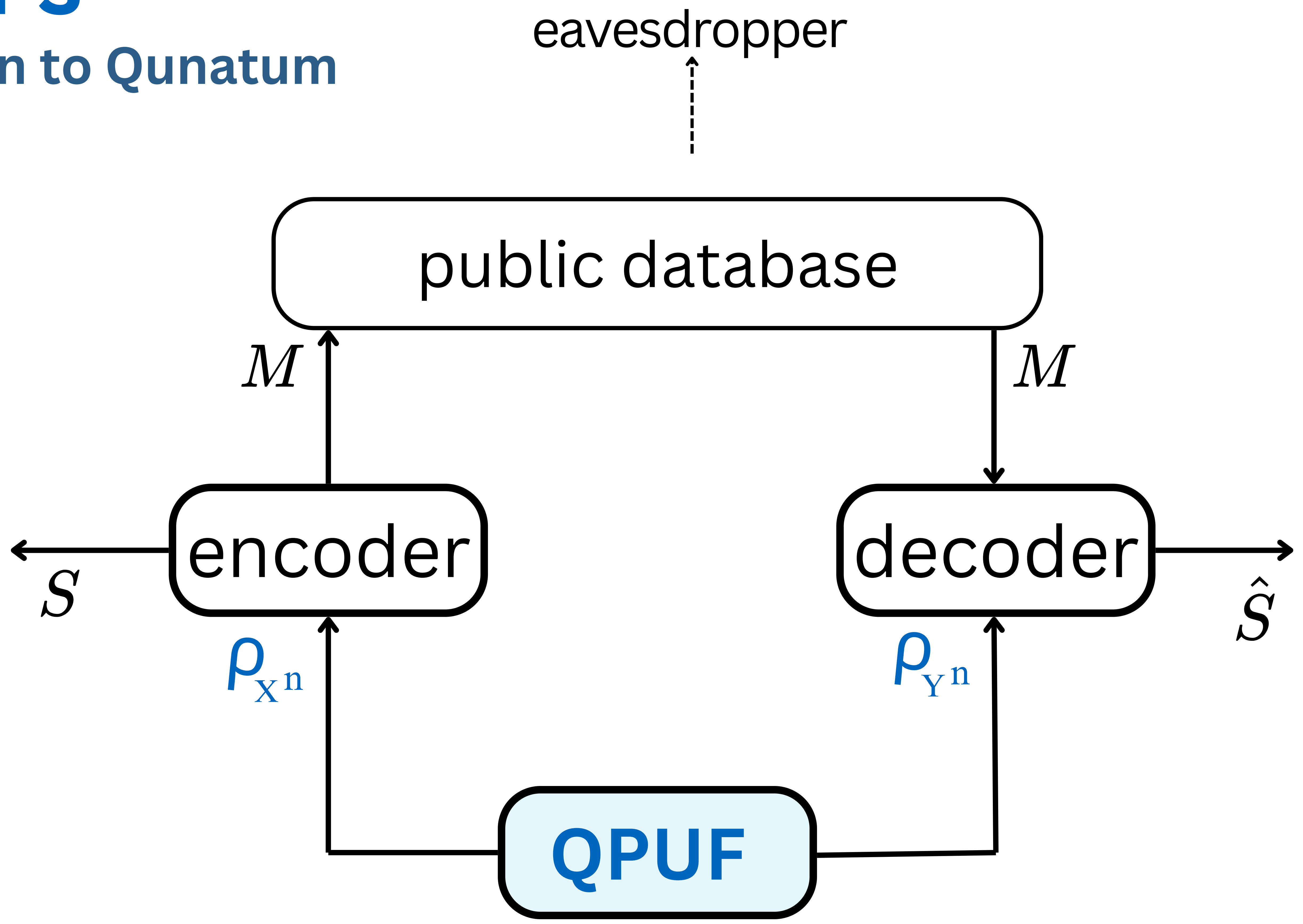
PUFs
Source Model



[1] Ignatenko, et al. "Biometric security from an information-theoretical perspective." FTCIT 7.2–3 (2012): 135-316
[2] Baur, “Secret Key Generation with Perfect Secrecy...” PhD diss., T. U. München, 2021.

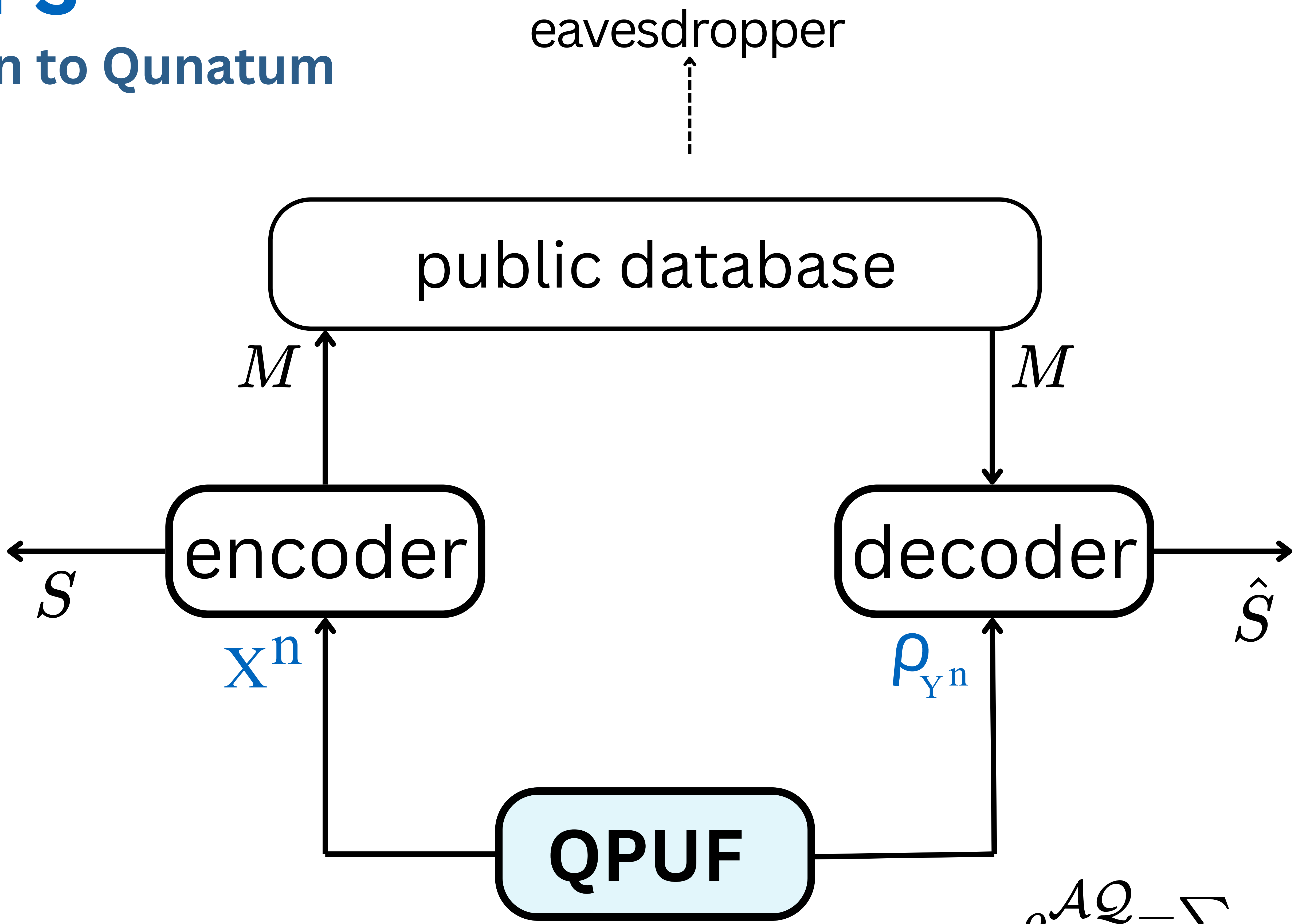
QPUFs

Extension to Qunatum



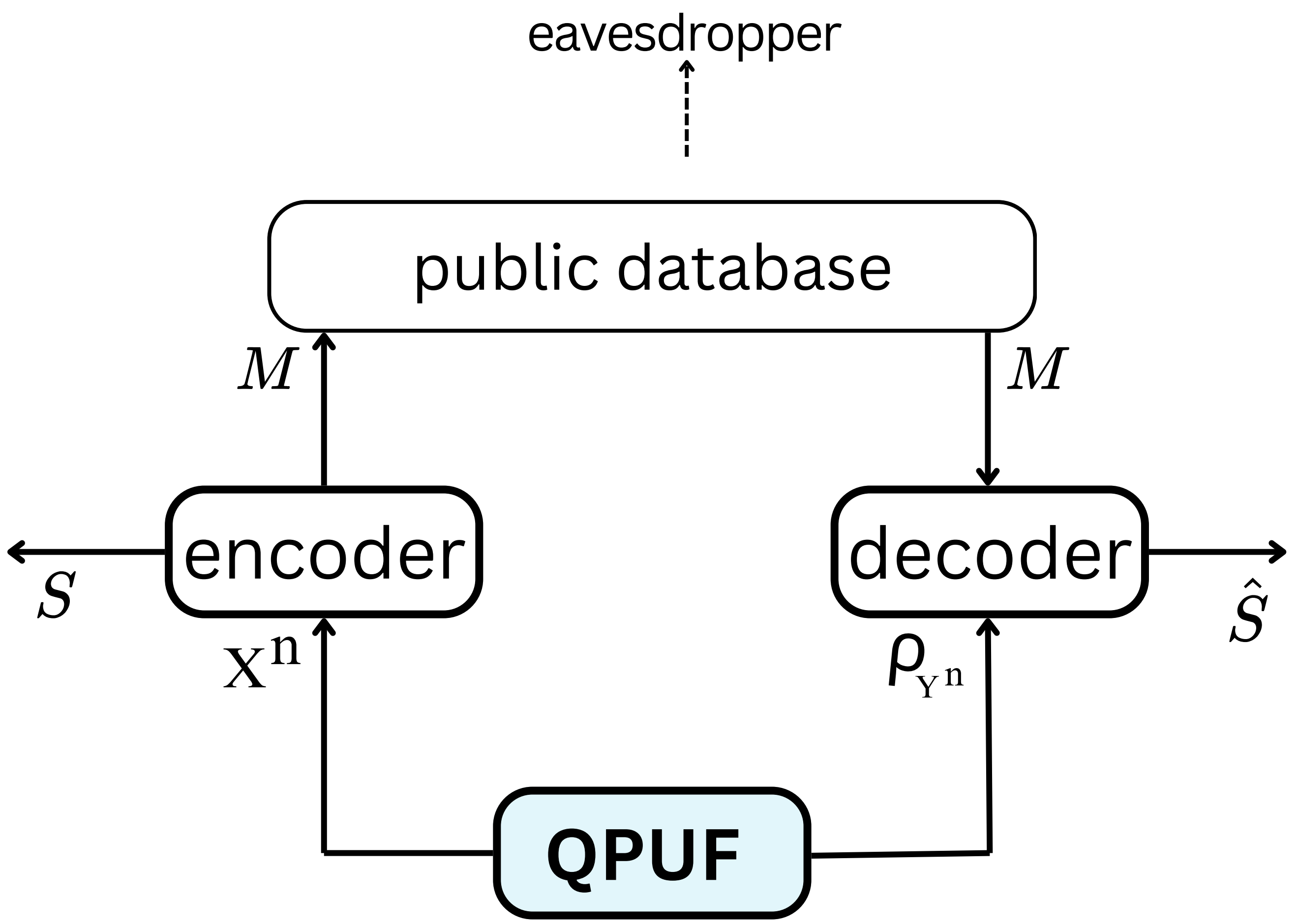
QPUFs

Extension to Qunatum



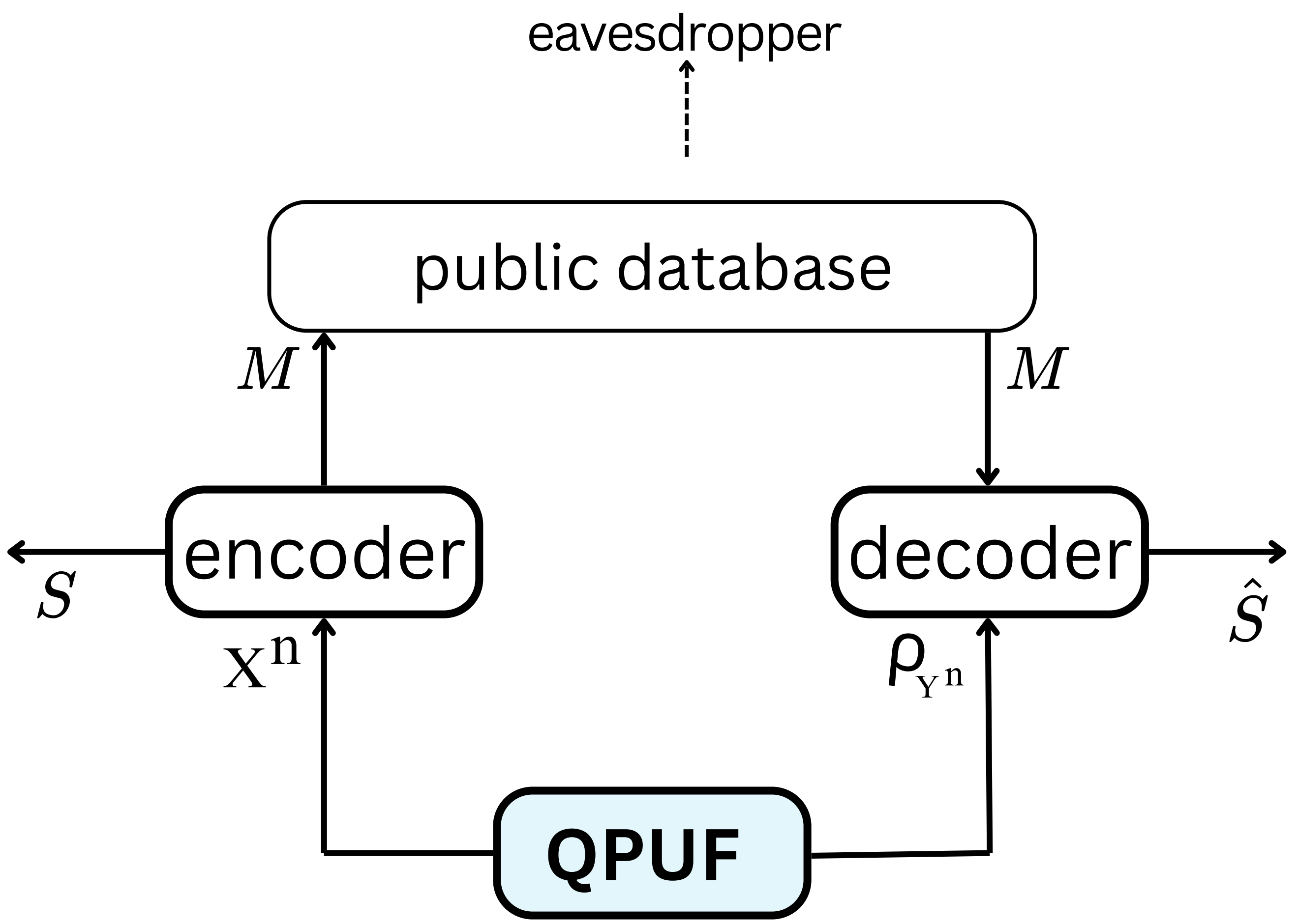
$$\rho^{\mathcal{AQ}} = \sum_{x,y} p(x,y) |x\rangle\langle x| \otimes \pi_y$$

Secret Key
Constraints



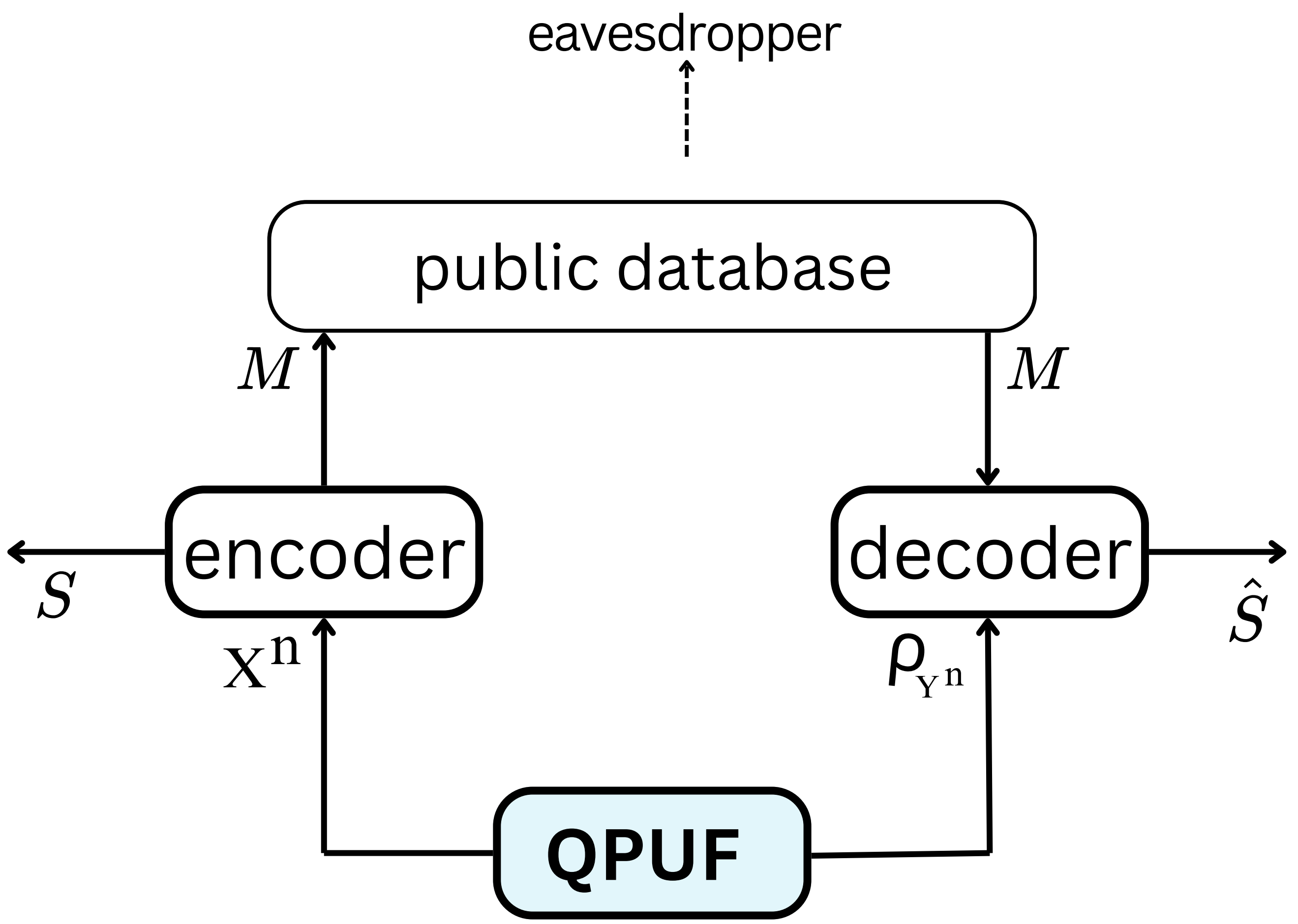
Secret Key
Constraints

$$\Pr(S \neq \widehat{S}) \leqslant \epsilon$$



Secret Key

Constraints

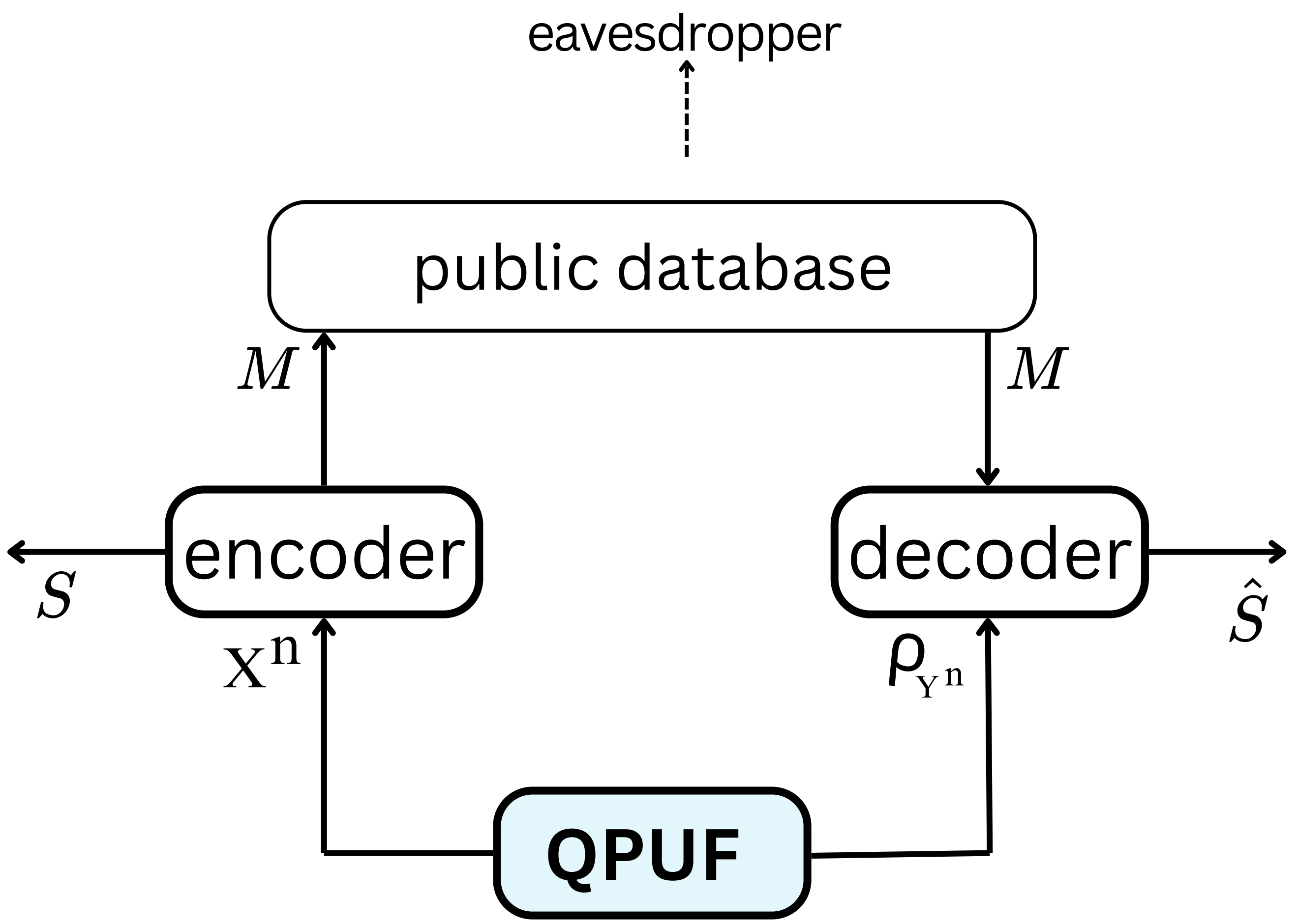


$$\Pr(S \neq \widehat{S}) \leqslant \epsilon$$

$$\frac{1}{n} I(S \wedge M) \leqslant \epsilon$$

Secret Key

Constraints

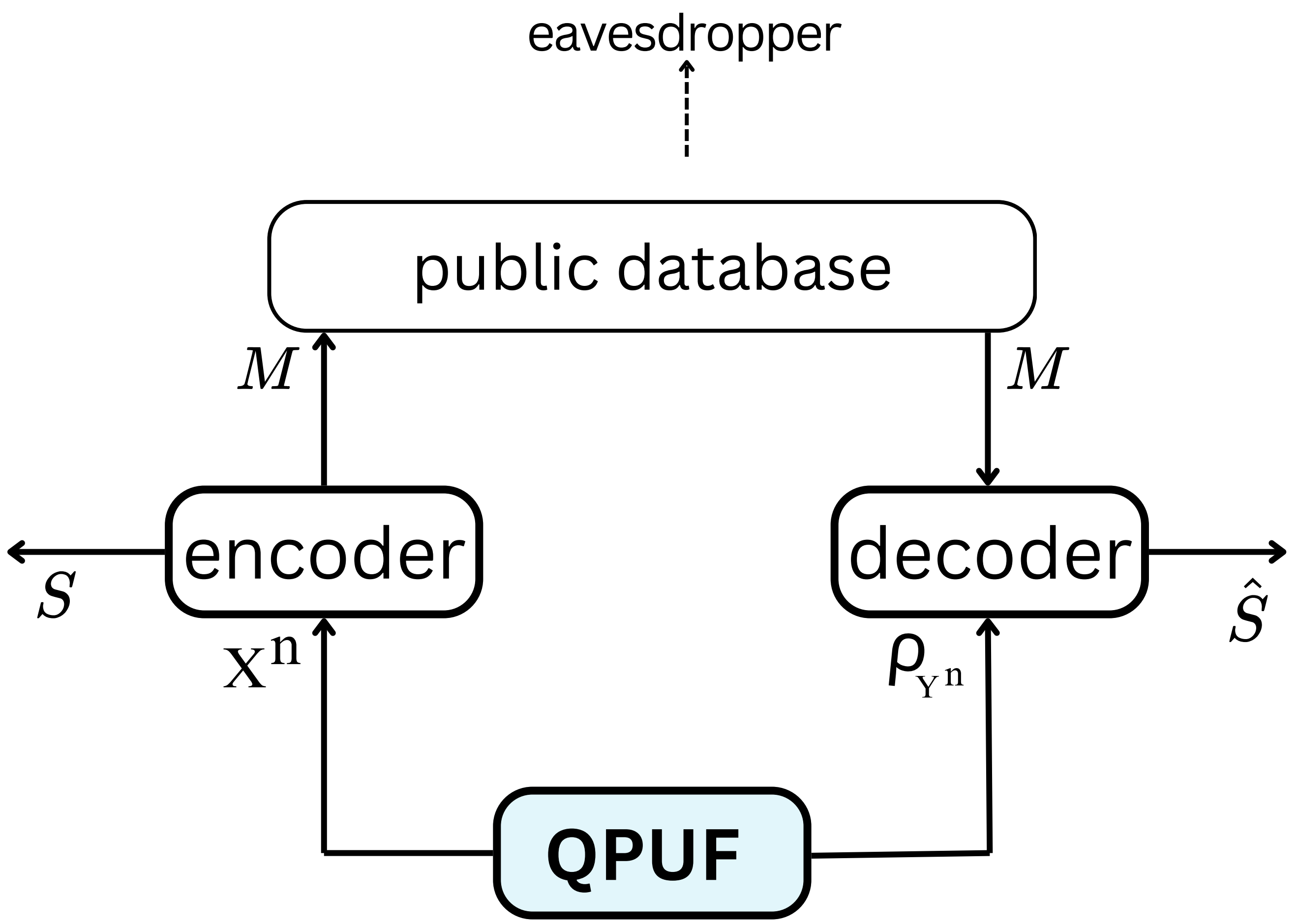


$$\Pr(S \neq \widehat{S}) \leqslant \epsilon$$

$$\frac{1}{n} I(S \wedge M) = 0$$

Secret Key

Constraints



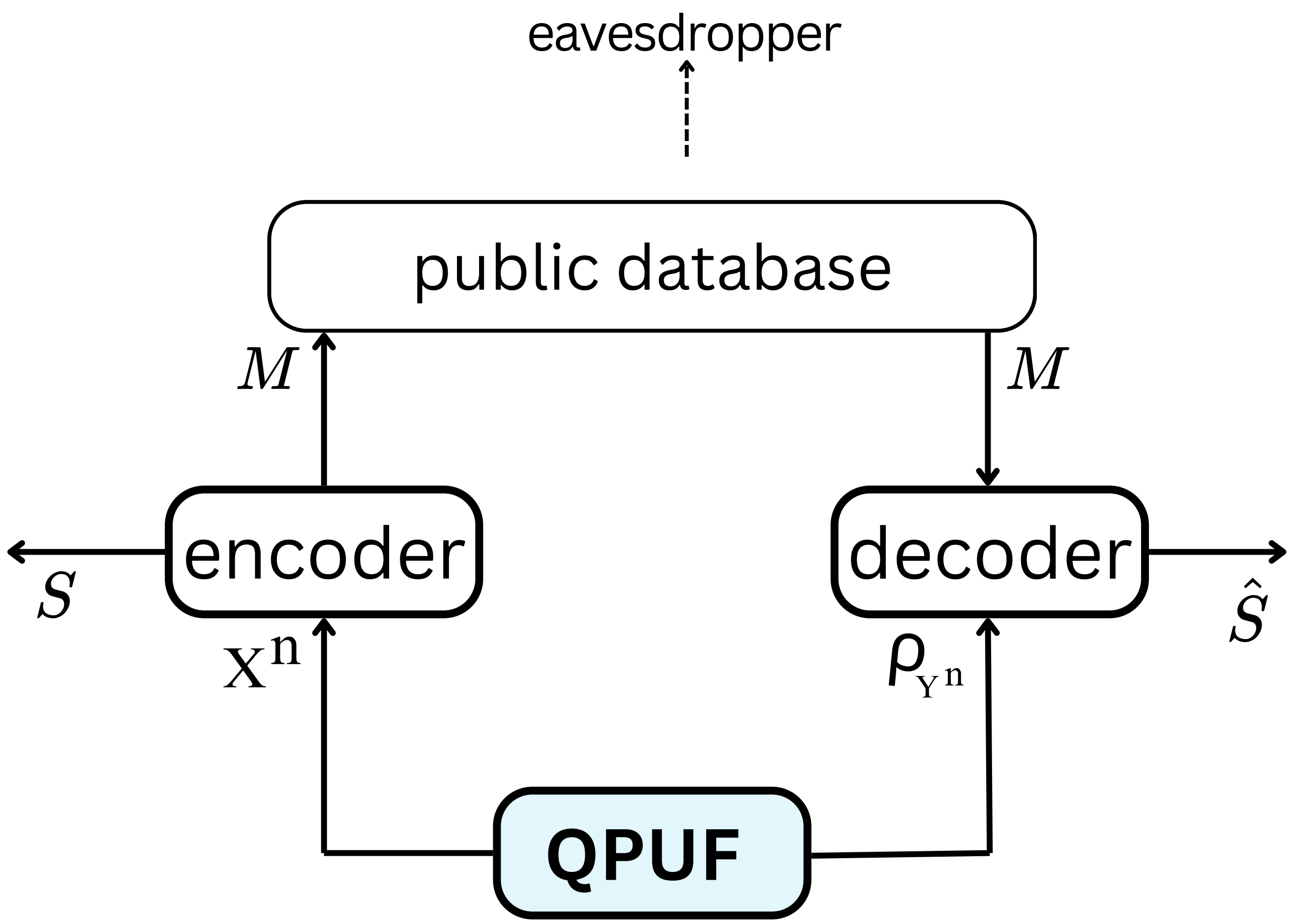
$$\Pr(S \neq \widehat{S}) \leqslant \epsilon$$

$$\frac{1}{n} I(S \wedge M) = 0$$

$$\frac{1}{n} H(S) \geqslant \frac{1}{n} \log |\mathcal{S}| - \epsilon$$

Secret Key

Constraints



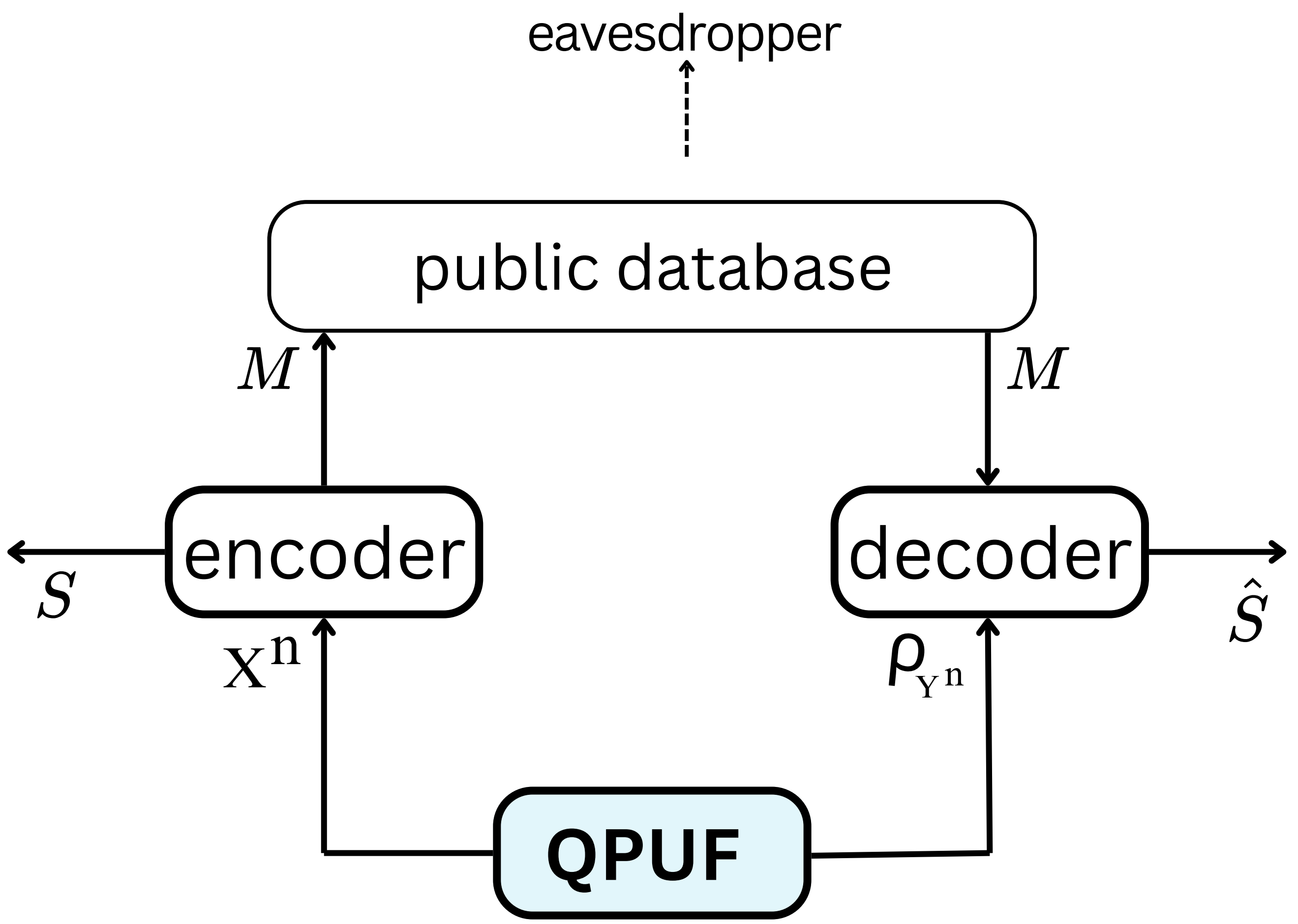
$$\Pr(S \neq \widehat{S}) \leqslant \epsilon$$

$$\frac{1}{n} I(S \wedge M) = 0$$

$$\frac{1}{n} H(S) = \frac{1}{n} \log |\mathcal{S}|$$

Secret Key

Constraints



$$\Pr(S \neq \widehat{S}) \leqslant \epsilon$$

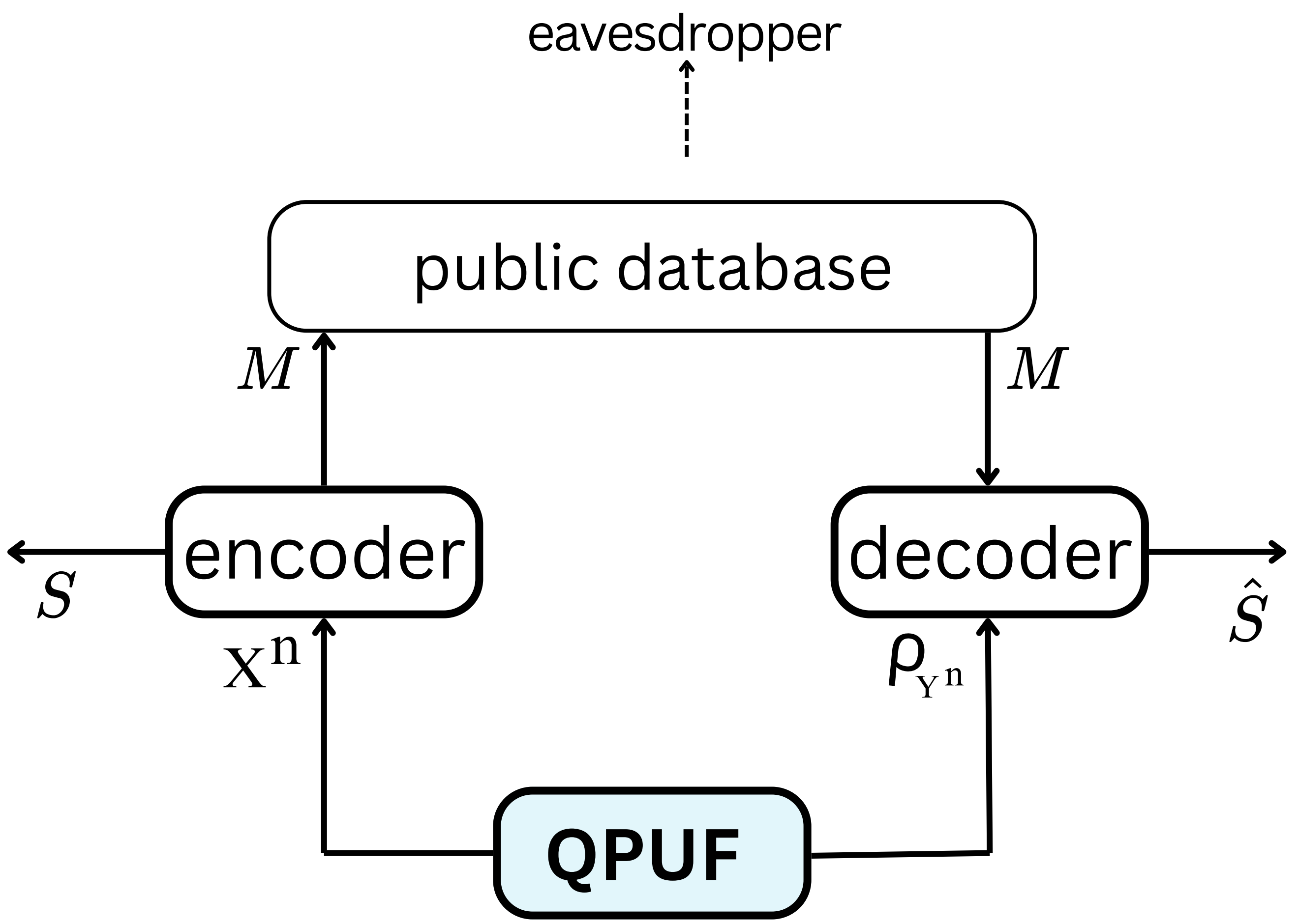
$$\frac{1}{n} I(S \wedge M) = 0$$

$$\frac{1}{n} H(S) = \frac{1}{n} \log |\mathcal{S}|$$

$$\frac{1}{n} \log |\mathcal{S}| \geqslant K - \epsilon$$

Secret Key

Constraints



$$\Pr(S \neq \widehat{S}) \leqslant \epsilon$$

$$\frac{1}{n} I(S \wedge M) = 0$$

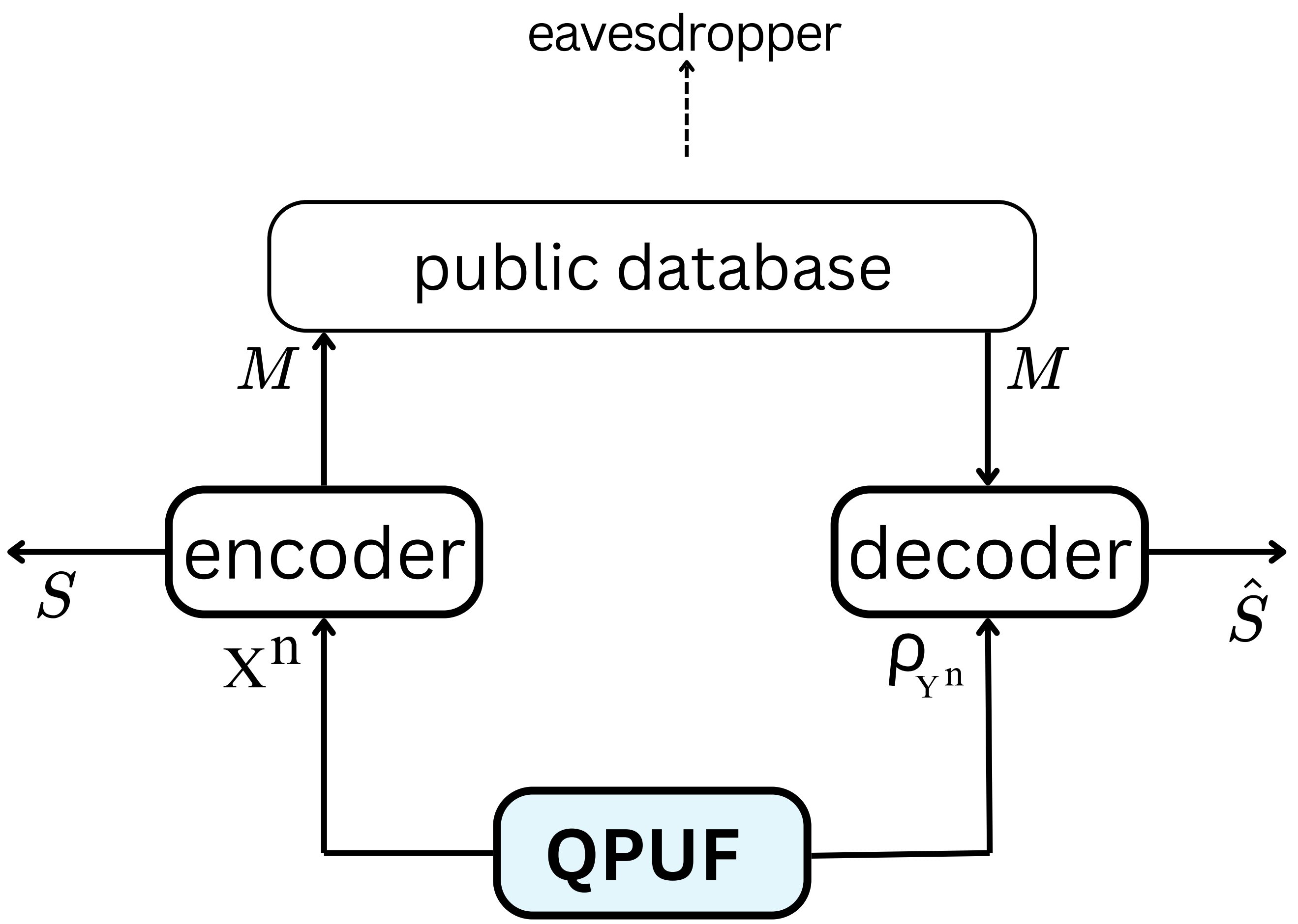
$$\frac{1}{n} H(S) = \frac{1}{n} \log |\mathcal{S}|$$

$$\frac{1}{n} \log |\mathcal{S}| \geqslant K - \epsilon$$

$$\frac{1}{n} I(M \wedge X^n) \leqslant L$$

Secret Key

Constraints



$$\Pr(S \neq \widehat{S}) \leqslant \epsilon$$

$$\frac{1}{n} I(S \wedge M) = 0$$

$$\frac{1}{n} H(S) = \frac{1}{n} \log |\mathcal{S}|$$

$$\frac{1}{n} \log |\mathcal{S}| \geqslant K - \epsilon$$

$$\frac{1}{n} I(M \wedge X^n) \leqslant L$$

$$\frac{1}{n} \log |\mathcal{M}| \leqslant R$$

Results

Simple Model

$$\Pr(S \neq \widehat{S}) \leqslant \epsilon$$

$$\frac{1}{n} I(S \wedge M) = 0$$

$$\frac{1}{n} H(S) = \frac{1}{n} \log |\mathcal{S}|$$

$$\frac{1}{n} \log |\mathcal{S}| \geqslant K - \epsilon$$

Results

Simple Model

$$\Pr(S \neq \widehat{S}) \leqslant \epsilon$$

$$\frac{1}{n} I(S \wedge M) = 0$$

$$\frac{1}{n} H(S) = \frac{1}{n} \log |\mathcal{S}|$$

$$\frac{1}{n} \log |\mathcal{S}| \geqslant K - \epsilon$$

Theorem 1

The SK capacity is given by

$$C_{SK} = \max_{T|X} I\left(T; \mathcal{Y}\right)$$

$\mathcal{Y}^n$ is the quantum system observed at the 2nd terminal for the classical output X^n observed at the 1st terminal.

[1] Nilesh, K., et al. "Information Theoretic Analysis of a Quantum PUF." ISIT (2024)

Results

Simple Model

$$\Pr(S \neq \widehat{S}) \leqslant \epsilon$$

$$\cancel{\frac{1}{n} I(S \wedge M) = 0}$$

$$\frac{1}{n} H(S) = \frac{1}{n} \log |\mathcal{S}|$$

$$\frac{1}{n} \log |\mathcal{S}| \geqslant K - \epsilon$$

Theorem 1'

The Distillable CR capacity is given by

$$C_{SK} = \max_{T|X} I\left(T; \mathcal{Y}\right)$$

$\mathcal{Y}^n$ is the quantum system observed at the 2nd terminal for the classical output X^n observed at the 1st terminal.

Proof Theorem 1

Converse

$$
\begin{aligned}
nK &\overset{a}{\leqslant} H(S) \\
&= I(S;\hat{S}) + H(S \mid \hat{S}) \\
&\overset{b}{\leqslant} I(S;\hat{S}) + 1 + n\varepsilon \log|\mathcal{S}| \\
&\overset{c}{\leqslant} I\left(S; M\mathcal{Y}^n\right) + 1 + n\varepsilon \log|\mathcal{S}| \\
&\overset{d}{\leqslant} I(S;M) + I\left(S;\mathcal{Y}^n \mid M\right) + 1 + n\varepsilon \log|\mathcal{S}| \\
&\leqslant I\left(S;\mathcal{Y}^n \mid M\right) + \varepsilon + 1 + n\varepsilon \log|\mathcal{S}| \\
&= I\left(SM;\mathcal{Y}^n \mid M\right) + \varepsilon + 1 + n\varepsilon \log|\mathcal{S}|
\end{aligned}
$$

$$
\begin{aligned}
\Longrightarrow \quad K - \delta &\leqslant \lim_{n\to\infty} \frac{1}{n} I\left(T;\mathcal{Y}^n \mid M\right) \leqslant \lim_{n\to\infty} \max_{T|X^n} \frac{1}{n} I\left(T;\mathcal{Y}^n\right) \\
&\overset{e}{=} \max_{T|X} I\left(T;\mathcal{Y}\right).
\end{aligned}
$$

a) Definition; b) Fano's inequality; c) data processing inequality; d) chain rule for mutual information

e) Devetak, et al. "Distilling common randomness from bipartite quantum states." IEEE TIT 50.12 (2004): 3183-3196

Proof Theorem 1

Direct

- The achievability part follows directly using the Classical-Quantum Slepian-Wolf (CQSW) protocol [1].
- We just need to consider the codewords of each such channel code to be almost of the same type.
    - This can be achieved by considering the largest subcode with codewords of constant type. This gives the conditional distribution of S uniform.

[1] Devetak, et al. "Classical data compression with quantum side information." Physical Review A 68.4 (2003): 042301.
[2] Ahlswede, et al. "Common randomness in information theory and cryptography. I." IEEE TIT 39.4 (1993): 1121-1132.

Remarks for Theorem 1

Storage rate & Disturbance

1. $$R = \frac{1}{n}\log M \approx H(X \mid \mathcal{Y}) + \delta.$$

2. $$\sum_{X^n} P\left(X^n\right)\left\|\hat{\rho}_{X^n} - \rho_{X^n}\right\|_1 \leqslant \sqrt{8\varepsilon} + \varepsilon.$$

[1] Devetak, et al. "Classical data compression with quantum side information." Physical Review A 68.4 (2003): 042301.

Results

Storage rate Constraint

$$\Pr(S \neq \widehat{S}) \leqslant \epsilon$$

$$\frac{1}{n} I(S \wedge M) = 0$$

$$\frac{1}{n} H(S) = \frac{1}{n} \log |\mathcal{S}|$$

$$\frac{1}{n} \log |\mathcal{S}| \geqslant K - \epsilon$$

$$\frac{1}{n} \log |\mathcal{M}| \leqslant R$$

Results

Storage rate Constraint

$$\Pr(S \neq \widehat{S}) \leqslant \epsilon$$

$$\frac{1}{n} I(S \wedge M) = 0$$

$$\frac{1}{n} H(S) = \frac{1}{n} \log |\mathcal{S}|$$

$$\frac{1}{n} \log |\mathcal{S}| \geqslant K - \epsilon$$

$$\frac{1}{n} \log |\mathcal{M}| \leqslant R$$

Theorem 2

For a QPUF with CQ output at the two terminals, the SK capacity as a function of storage rate is given by

$$C_{SK}^{RC}(R) = \sup_{T|X} \{ I(T; \mathcal{Y}) \mid I(T; X) - I(T; \mathcal{Y}) \leqslant R \}$$

R is the bound on the unsecured non-volatile memory.

[1] Nilesh, K., et al. "Information Theoretic Analysis of a Quantum PUF." ISIT (2024)

Results

Storage rate Constraint

$$\Pr(S \neq \widehat{S}) \leqslant \epsilon$$

$$\cancel{\frac{1}{n} I(S \wedge M) = 0}$$

$$\frac{1}{n} H(S) = \frac{1}{n} \log |\mathcal{S}|$$

$$\frac{1}{n} \log |\mathcal{S}| \geqslant K - \epsilon$$

$$\frac{1}{n} \log |\mathcal{M}| \leqslant R$$

Theorem 2'

For a QPUF with CQ output, the Distillable CR capacity as a function of storage rate is given by

$$C_{SK}^{RC}(R) = \sup_{T|X} \{ I(T;\mathcal{Y}) \mid I(T;X) - I(T;\mathcal{Y}) \leqslant R \}$$

R is the bound on the unsecured non-volatile memory.

[1] Devetak, et al. "Distilling common randomness from bipartite quantum states." IEEE TIT 50.12 (2004): 3183-3196.

Proof of Theorem 2

Converse

- The converse directly follows from the converse of [1].

- as the secret key rate cannot be larger than the common randomness rate generated through the same system.

[1] Devetak, et al. "Distilling common randomness from bipartite quantum states." IEEE TIT 50.12 (2004): 3183-3196.

Proof of Theorem 2

Direct

From Theorem 1, with $S = S(X^n)$, we have the achievability of

$$(K, R) = \left(\frac{1}{n} I(S; \mathcal{Y}^n), \frac{1}{n} H(S \mid \mathcal{Y}^n)\right).$$

Proof of Theorem 2

Direct

From Theorem 1, with $S = S(X^n)$, we have the achievability of

$$(K, R) = \left(\frac{1}{n} I(S; \mathcal{Y}^n), \frac{1}{n} H(S \mid \mathcal{Y}^n)\right).$$

We estimate these quantities using Lemma:

[1]**Lemma 1:** For every $\epsilon, \delta > 0$ and $n \geq n_2(|\mathcal{T}|, |\mathcal{X}|, d, \delta, \epsilon)$, there exists a function $\mathcal{E} : \mathcal{X}^n \to \mathcal{T}^n$ such that

$$\frac{1}{n} H(\mathcal{Y}^n \mid \mathcal{E}(X^n)) \leq H(\mathcal{Y} \mid T) + \delta,$$

$$\left| \frac{1}{n} H(X^n \mid \mathcal{E}(X^n)) - H(X \mid T) \right| \leq \delta.$$

[1] Devetak, et al. "Distilling common randomness from bipartite quantum states." IEEE TIT 50.12 (2004): 3183-3196.

Proof of Theorem 2

Direct

- $\frac{1}{n} H\left(S \mid \mathcal{Y}^n\right) \leqslant I(T;X) - I(T;\mathcal{Y}) + \delta.$

- $\frac{1}{n} I\left(S;\mathcal{Y}^n\right) = \frac{1}{n}\left[H(S) - H\left(S \mid \mathcal{Y}^n\right)\right] \geqslant I(T;\mathcal{Y}) - \delta$

This gives the achievability of

$$(K,R) = (I(T;\mathcal{Y}), I(T;X) - I(T;\mathcal{Y}))$$

Results

Privacy Leakage Constraint

$$\Pr(S \neq \widehat{S}) \leqslant \epsilon$$

$$\frac{1}{n} I(S \wedge M) = 0$$

$$\frac{1}{n} H(S) = \frac{1}{n} \log |\mathcal{S}|$$

$$\frac{1}{n} \log |\mathcal{S}| \geqslant K - \epsilon$$

$$\frac{1}{n} I(M \wedge X^n) \leqslant L$$

Results

Privacy Leakage

$$\Pr(S \neq \widehat{S}) \leqslant \epsilon$$

$$\frac{1}{n} I(S \wedge M) = 0$$

$$\frac{1}{n} H(S) = \frac{1}{n} \log |\mathcal{S}|$$

$$\frac{1}{n} \log |\mathcal{S}| \geqslant K - \epsilon$$

$$\frac{1}{n} I(M \wedge X^n) \leqslant L$$

Theorem 3

$$C_{SK}^{PL}(L) = C_{SK}^{RC}(L)$$
$$= \sup_{T|X} \{ I(T;\mathcal{Y}) \mid I(T;X) - I(T;\mathcal{Y}) \leqslant L \}$$

The SK capacity with privacy leakage constraint is equivalent to the SK capacity with storage constraint when the bound on these two constraints are the same.

[1] Nilesh, K., et al. "Information Theoretic Analysis of a Quantum PUF." ISIT (2024)

Proof of Theorem 3

Direct

- The basic idea is to construct a code that achieves the SK capacity with storage rate constraint given in Theorem 2.

  - Particularly $\frac{1}{n} \log |\mathcal{M}| \leqslant L.$

Proof of Theorem 3

Direct

- The basic idea is to construct a code that achieves the SK capacity with storage rate constraint given in Theorem 2.
  - Particularly $\frac{1}{n}\log|\mathcal{M}| \leqslant L.$
- Now using the fact that $I(X^n \wedge M) \leqslant \log|\mathcal{M}|$
  - we observe that the same code achieves the SK capacity with privacy leakage constraint.

Proof of Theorem 3

Converse

- For a given fixed blocklength n, we perform a quantum measurement on the second terminal that collapses the classical-quantum system to a classical-classical system.
  - After measurement, we represent the terminal $\mathcal{Y}^n$ by the mea- -surement outcome given by the classical random variable Y^n.

Proof of Theorem 3

Converse

- For a given fixed blocklength n, we perform a quantum measurement on the second terminal that collapses the classical-quantum system to a classical-classical system.
  - After measurement, we represent the terminal $\mathcal{Y}^n$ by the mea- -surement outcome given by the classical random variable Y^n.
- The classical converse [1] can then be applied to the system (X^n, Y^n)
  - $C_{SK}^{PL}(L) \leq \sup_{T|X}\{I(T;Y) \mid I(T;X) - I(T;Y) \leq L\}$

[1] Ignatenko, et al. "Biometric security from an information-theoretical perspective." FTCIT 7.2–3 (2012): 135-316

Proof of Theorem 3

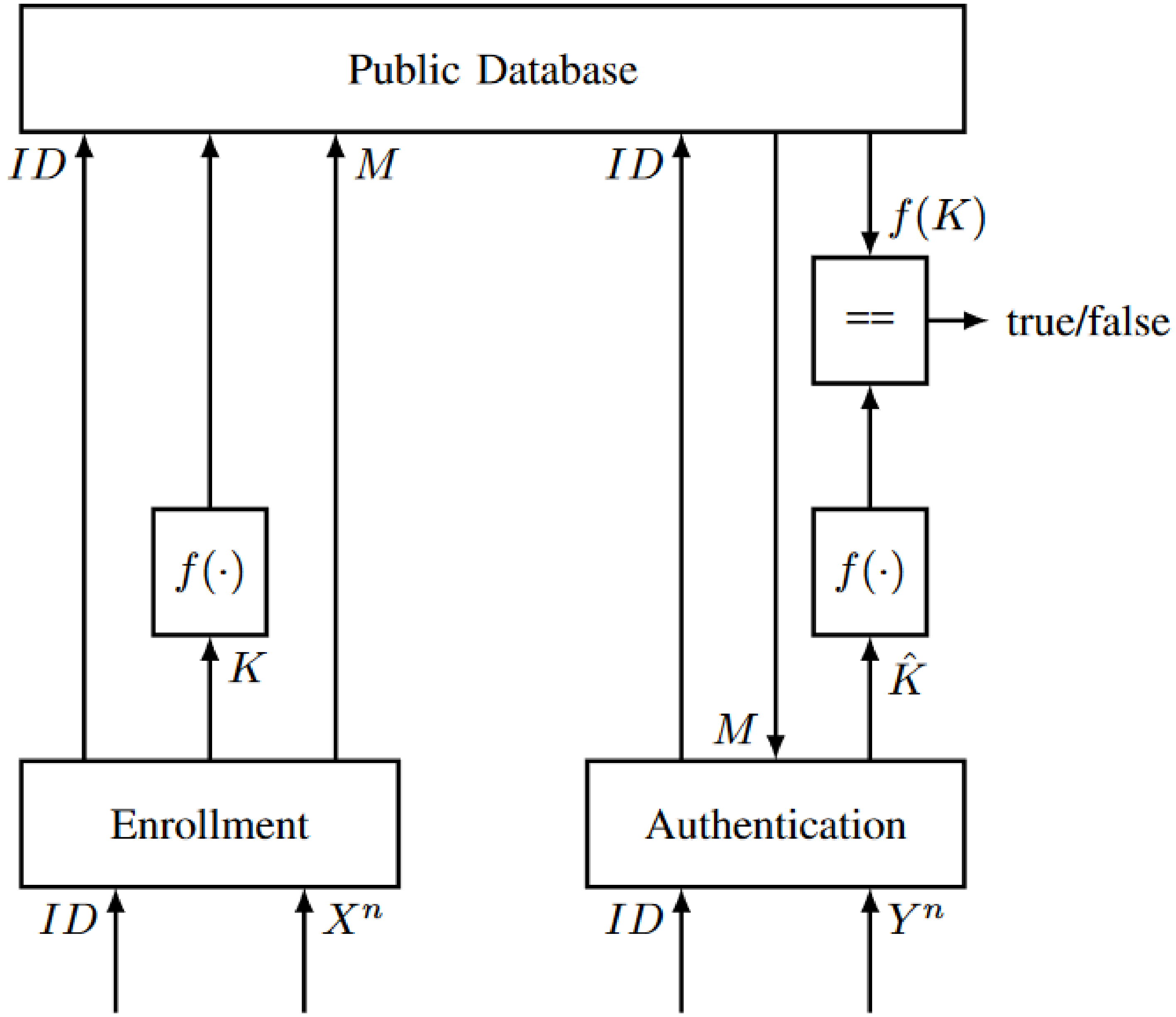
Converse

- For a given fixed blocklength n, we perform a quantum measurement on the second terminal that collapses the classical-quantum system to a classical-classical system.
  - After measurement, we represent the terminal $\mathcal{Y}^n$ by the mea- -surement outcome given by the classical random variable Y^n.
- The classical converse [1] can then be applied to the system (X^n, Y^n)
  - $C_{SK}^{PL}(L) \leq \sup_{T|X}\{I(T;Y) \mid I(T;X) - I(T;Y) \leq L\}$
  - $C_{SK}^{PL}(L) \leq \sup_{T|X}\{I(T;\mathcal{Y}) \mid I(T;X) - I(T;\mathcal{Y}) \leq L\}.$

[1] Ignatenko, et al. "Biometric security from an information-theoretical perspective." FTCIT 7.2–3 (2012): 135-316

Applications

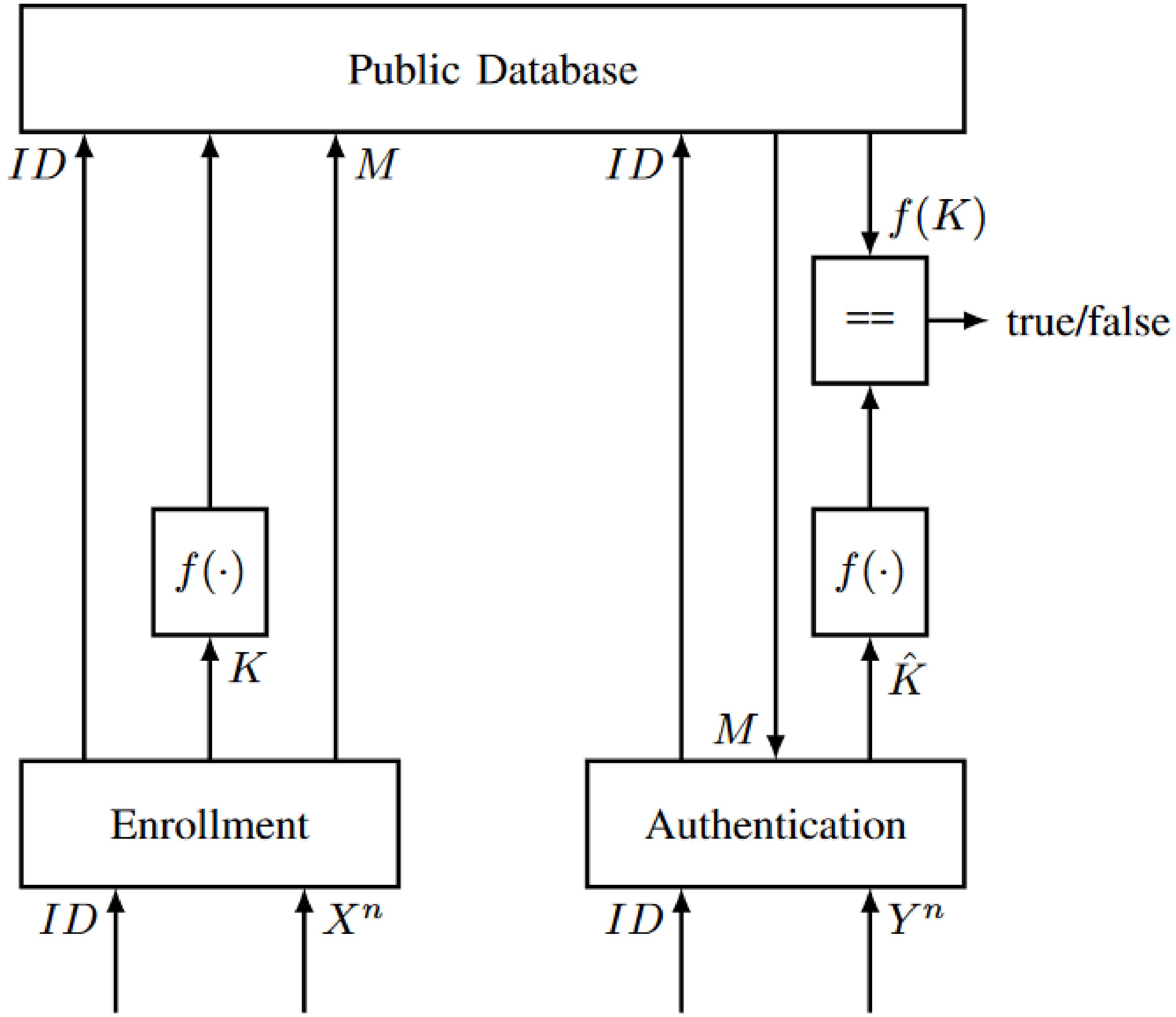
Authentication



$$\mathrm{FRR} \triangleq \Pr\left\{\hat{s}_y \neq s\right\}$$

$$\mathrm{mFAR} = \sum_{m=1}^{|\mathcal{M}|} P_M(m) \max_{\rho_{z^n} \in \mathcal{H}_{\mathcal{Y}}^{\otimes n}} P_{S|M}\left(\mathcal{D}_m\left(\rho_{z^n}\right) \mid m\right)$$

Applications
Authentication

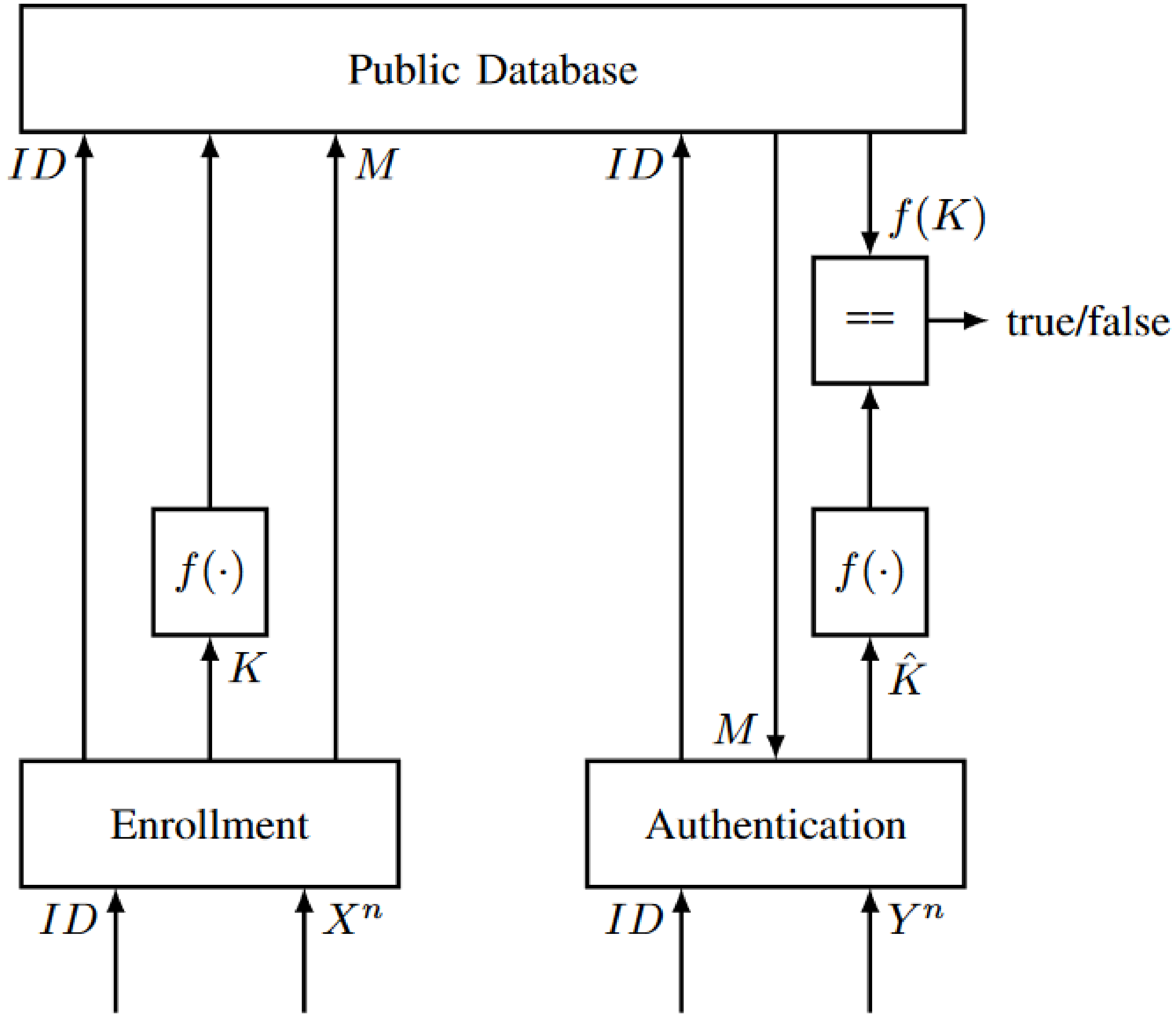


Definition: For a QPUF $(\mathcal{E}, \mathcal{D})$, We call $E \geqslant 0$ an achievable false acc- -eptance exponent with secret key rate K, if for any $\epsilon > 0$ there is an $n_0 \in \mathbb{N}$ such that for all $n \geqslant n_0$ there is a QPUF protocol $(\mathcal{E}, \mathcal{D})$ such that $\frac{1}{n}\log|\mathcal{S}| \geqslant K - \epsilon$, and the following conditions are satisfied :

$$\mathrm{FRR} \leqslant \epsilon$$
$$\frac{1}{n}\log\frac{1}{\mathrm{mFAR}} \geqslant E - \epsilon$$

We denote the capacity region by $\mathcal{R}_{mFAR}(K, E) = \{(K, E) \text{ is achievable}\}$.

Applications
Authentication



Theorem 4

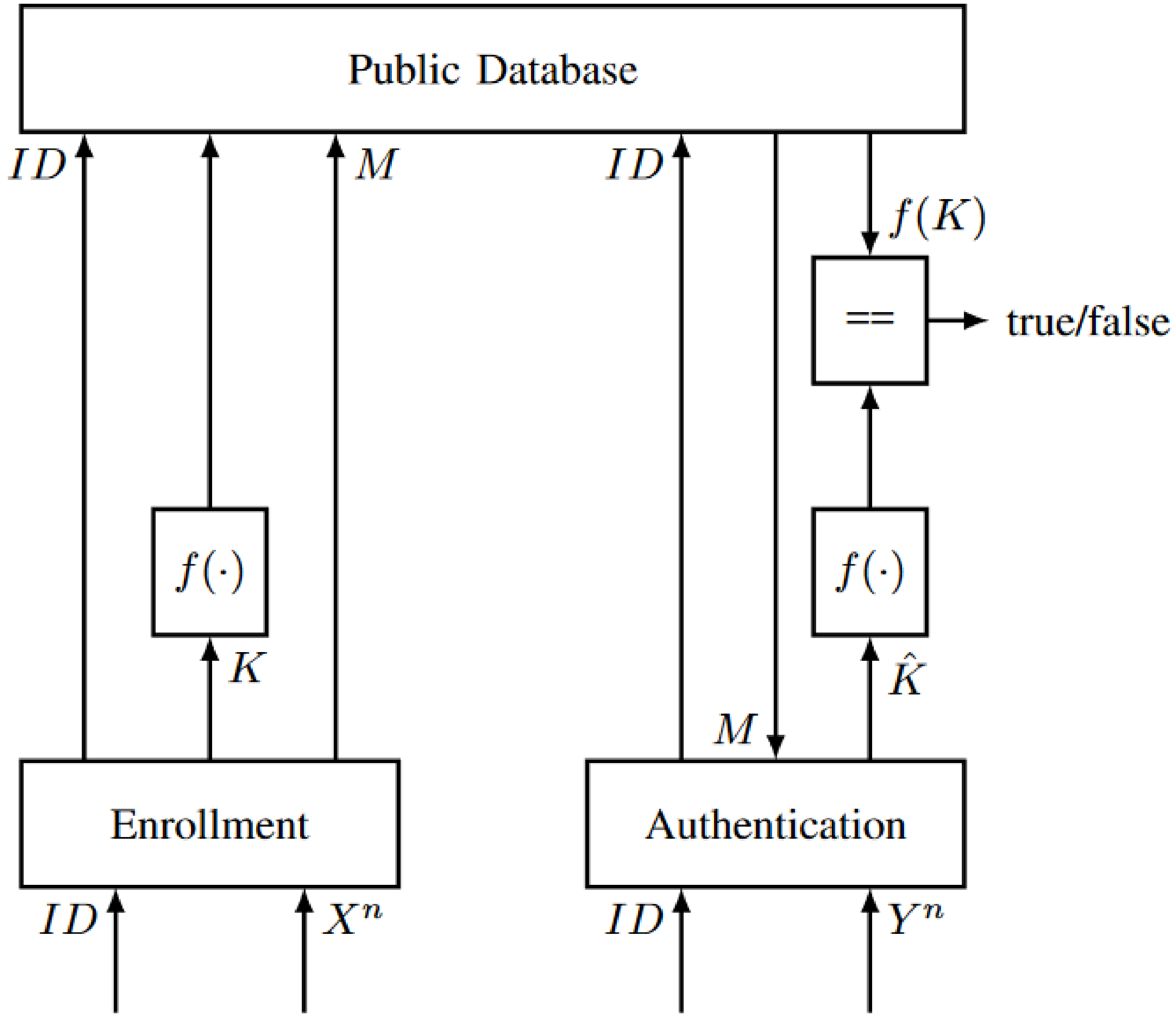
The capacity region in terms of false acce- -ptance exponent and SK rate is given by

$$\mathcal{R}_{mFAR}(K,E) =$$
$$\{(K,E) \mid 0 \leqslant K \leqslant I\,(X;\mathcal{Y}) \text{ and } 0 \leqslant E \leqslant I\,(X;\mathcal{Y})\}$$

[1] Nilesh, K., et al. "Authentication based on Quantum PUF." submitted

Applications

Authentication



Theorem 5

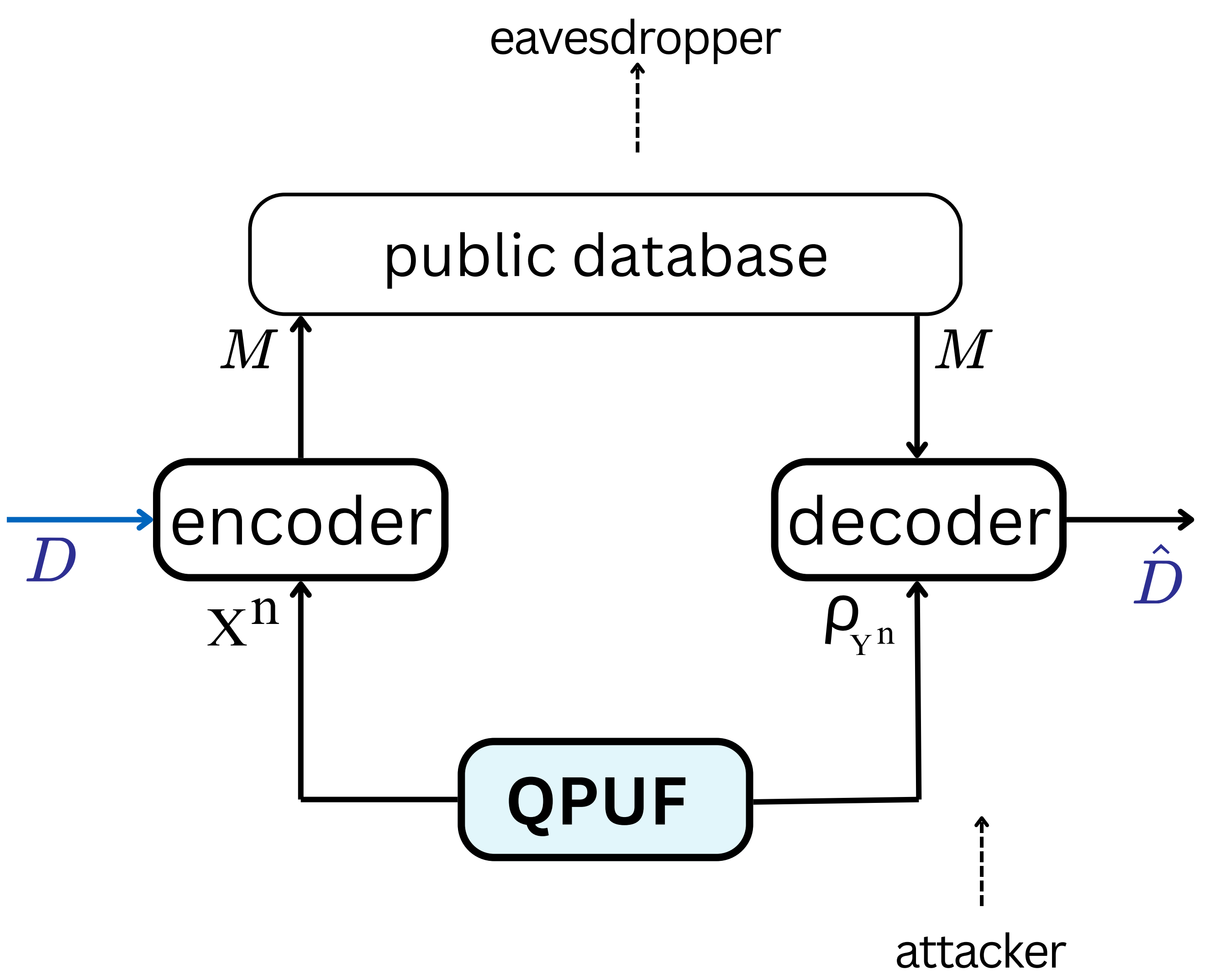
The following bound holds for any $\delta_1, \delta_2 > 0$

$$K - \delta_1 \leqslant \frac{1}{n} \log \frac{1}{\mathrm{mFAR}} \leqslant K + \delta_2$$

where K is the secret key rate and

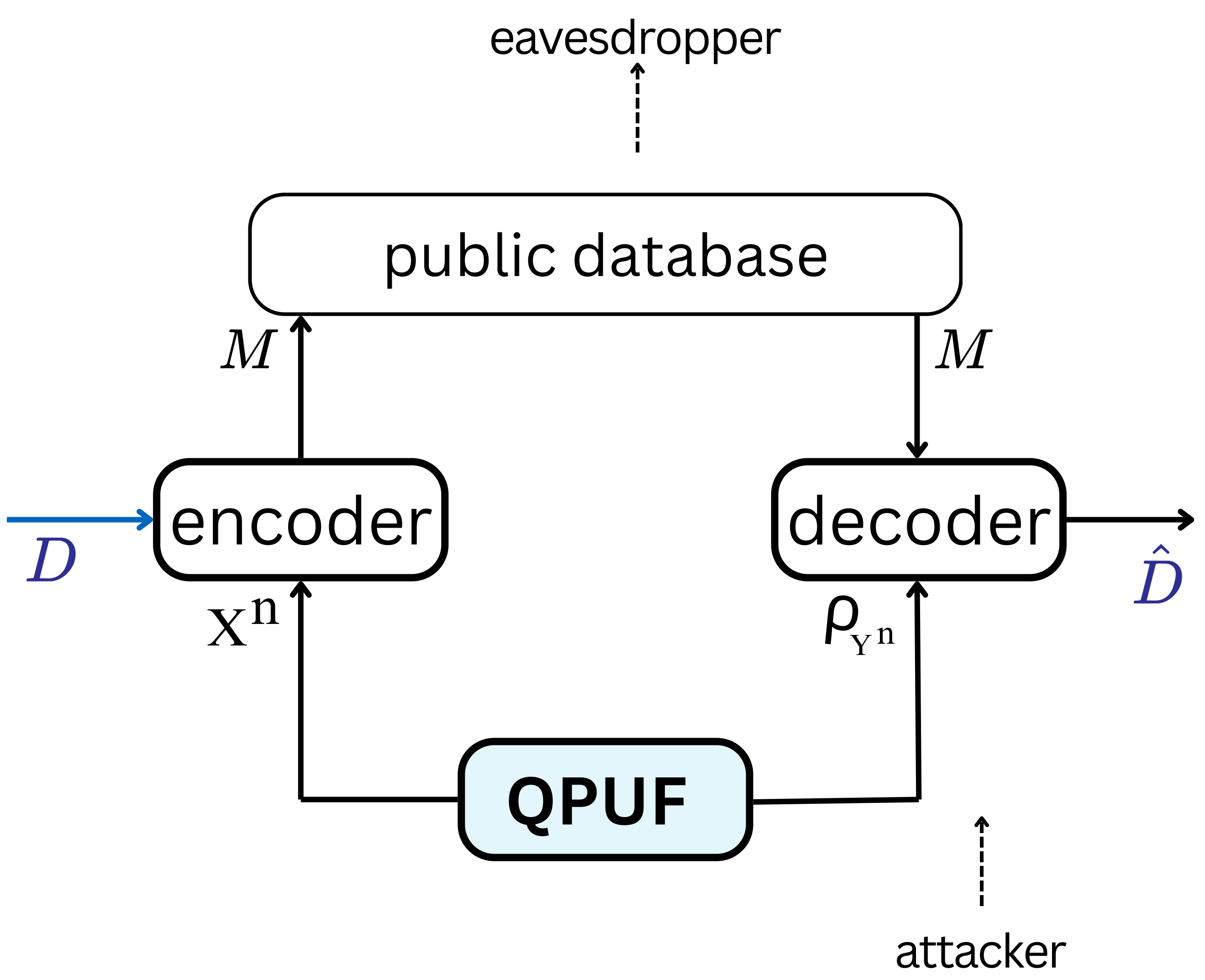
mFARis the maximum false acceptance rate

Applications
Secure Storage



Applications

Secure Storage



$$\Pr(D \neq \hat{D}) \leqslant \varepsilon$$

$$\mathrm{I}\left(M; D\right) = 0$$

$$\frac{1}{n}\log|\mathcal{D}| \geqslant R_s - \varepsilon$$

$$\frac{1}{n} I\left(M; X^n\right) \leq L$$

Applications

Secure Storage

$$\Pr(D \neq \hat{D}) \leqslant \varepsilon$$

$$\mathrm{I}\left(M; D\right) = 0$$

$$\frac{1}{n}\log|\mathcal{D}| \geqslant R_s - \varepsilon$$

$$\frac{1}{n} I\left(M; X^n\right) \leq L$$

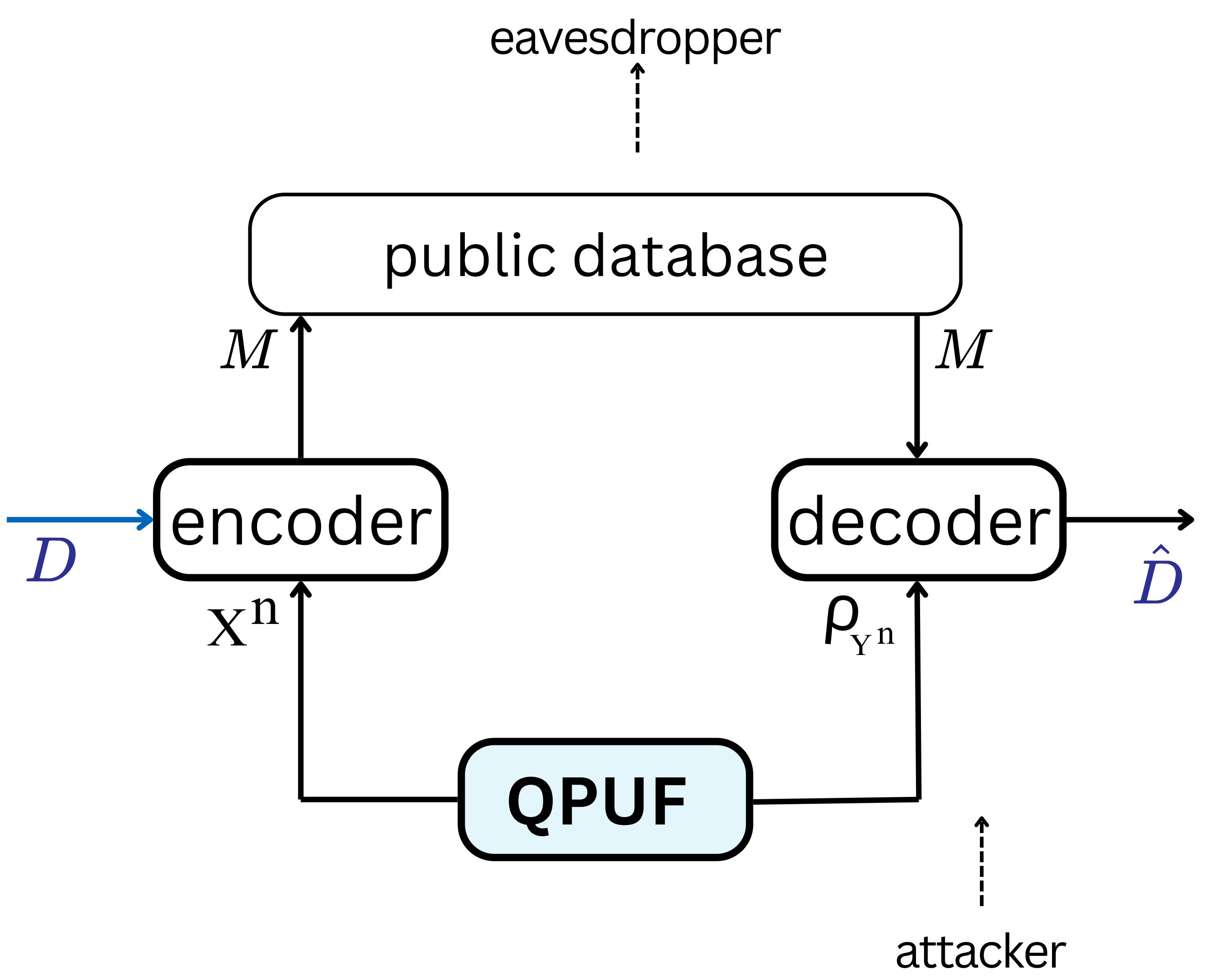
Theorem 5

$$C_{PL}(L) = \sup_{T|X}\{I(T;\mathcal{Y}) \mid I(T;X) - I(T;\mathcal{Y}) \leq L\}$$

[1] Nilesh, K., et al. "Secure Storage and Identification based on Quantum PUF." submitted

Applications

Secure Storage



Theorem 6

$$\mathcal{R}_{mFAR}(D,E) =$$
$$\{(D,E) \mid 0 \leqslant D \leqslant I\,(X;\mathcal{Y}) \text{ and } 0 \leqslant E \leqslant I\,(X;\mathcal{Y})\}$$

Kumar Nilesh
kumar.nilesh@tum.de

THANK YOU

ISIT-2024