ApPLIED 2023 Workshop, PODC 2023

Invited Paper: Oblivious Transfer Protocol without Physical Transfer of Hardware Root-of-Trust

Harishma Boyapally†*, **Chandan Kumar Chaudhary†**, Debdeep Mukhopadhyay†

† Secure Embedded Architecture Laboratory (SEAL),

Indian Institute of Technology Kharagpur, India

*Temasek Laboratories, Nanyang Technological University, Singapore

Contents

Era of Internet of Things (IoT)

SECURITY ?

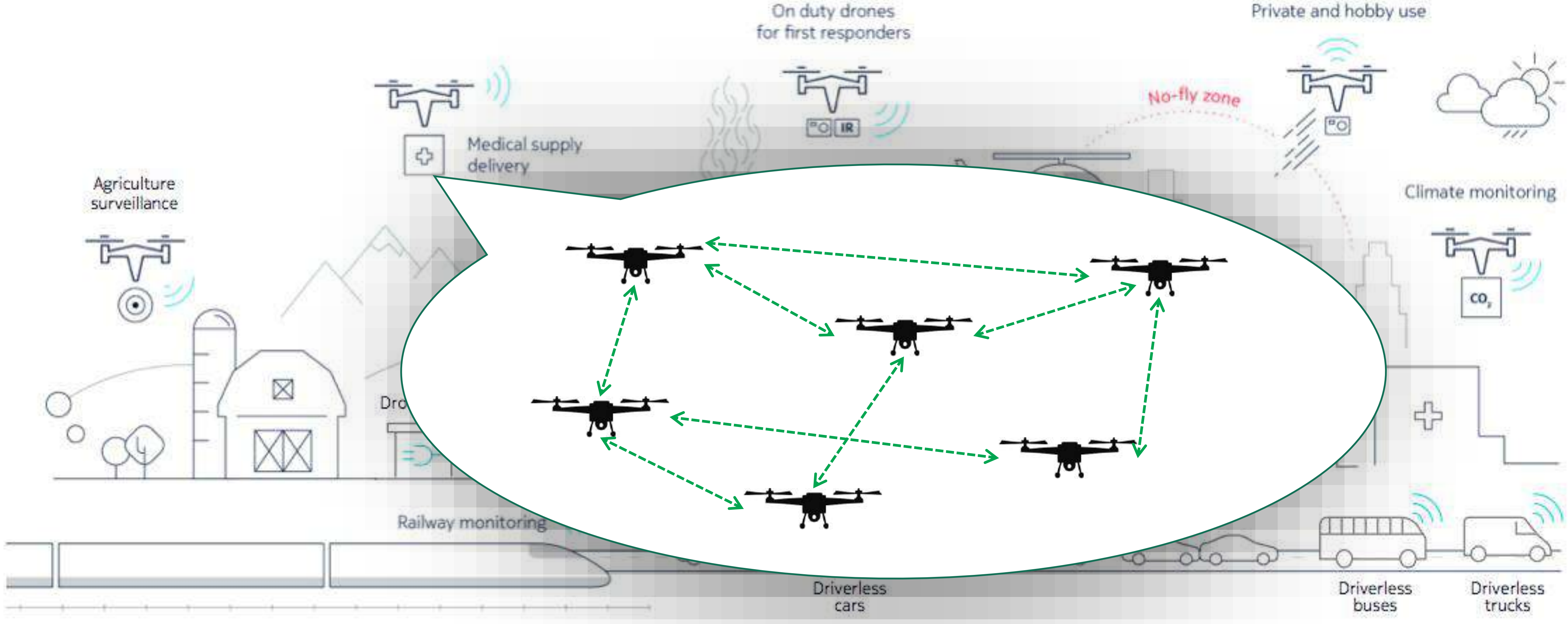
CNBC

Amazon debuts its new delivery drone

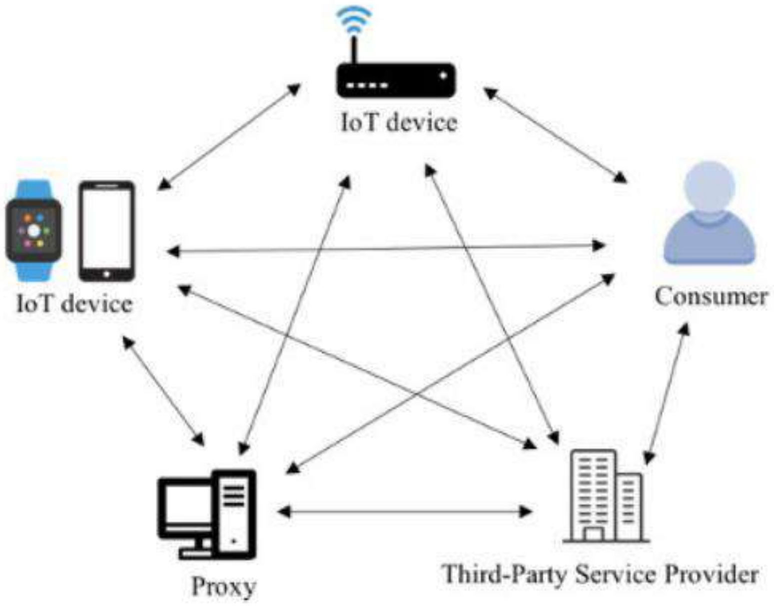
Amazon's head of worldwide consumer Jeff Wilke unveiled its latest delivery drone at the re:MARS conference in Las Vegas on June 5, 2019.

05-Jun-2019

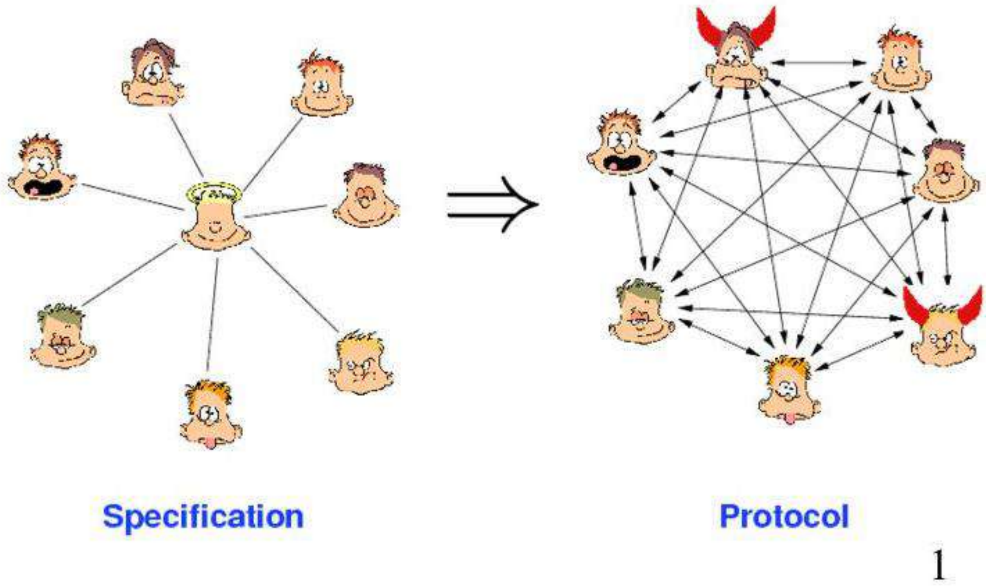
Distributed Computing in IoTs



From Distributed Computing to Multi-Party Computation



Distributed IoT System

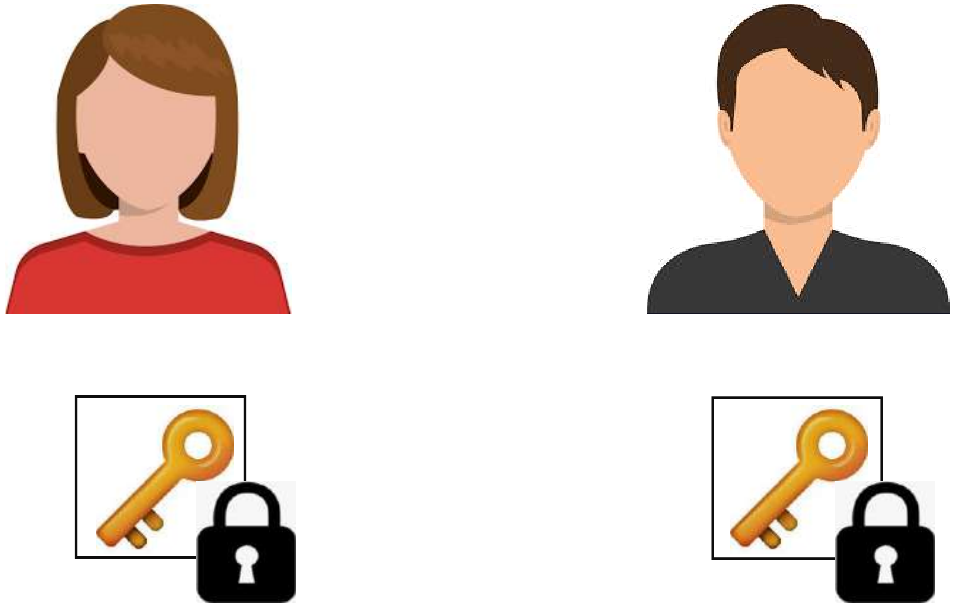


Secure Multi-Party Computation

Image Source: Google.com

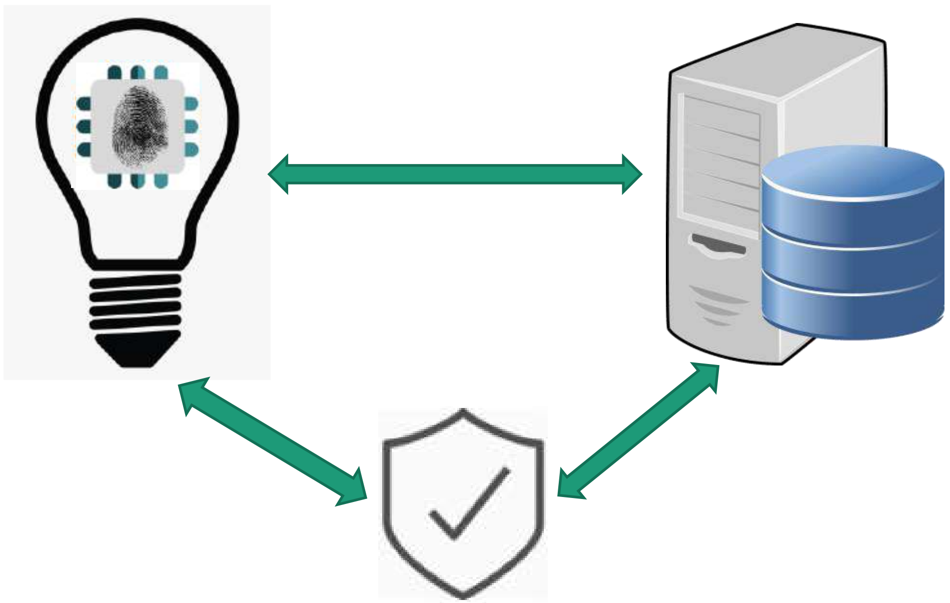
Cryptographic Primitives

Classical Cryptography



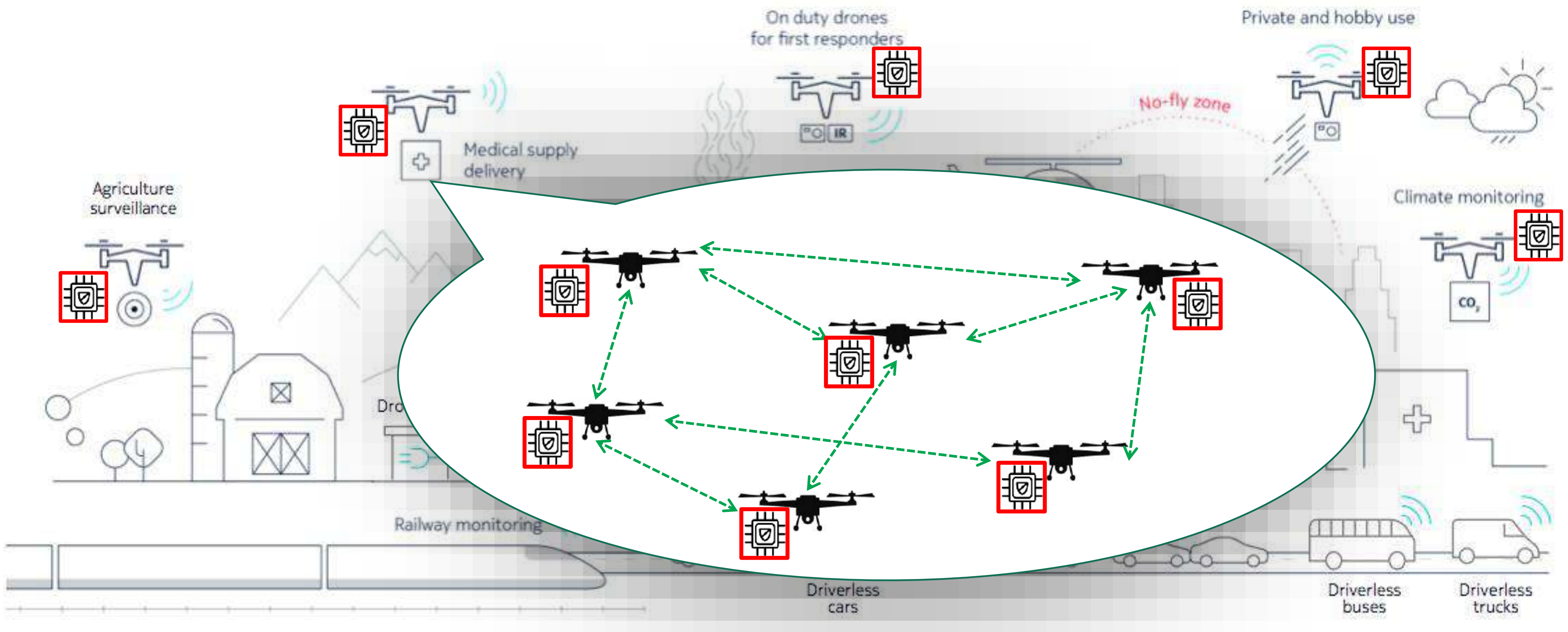
Requires Secure Storage of Secret Keys

Hardware-based Solutions



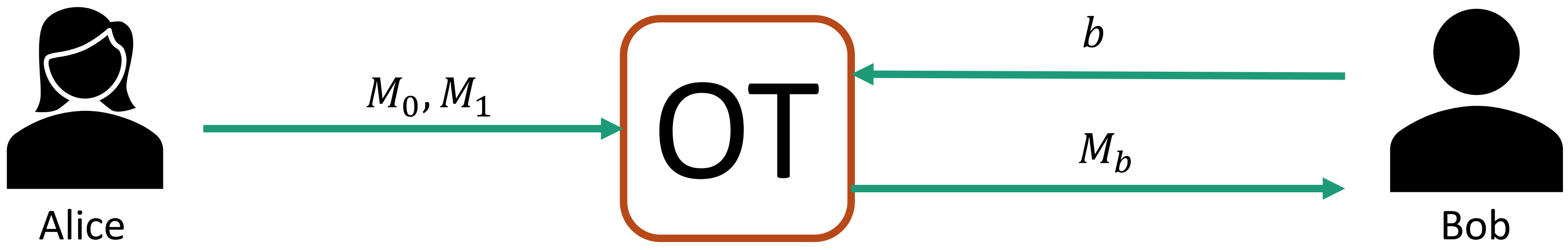
Requires Trusted Third Party & Heavy Computation on Server

Solution: Physically Related Functions (PReFs)



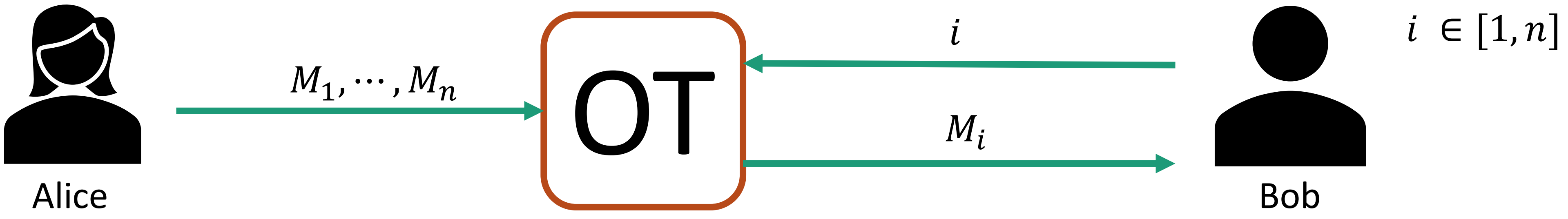
Oblivious Transfer (OT): A Building Block of MPC

1-out-of-2 OT Protocol



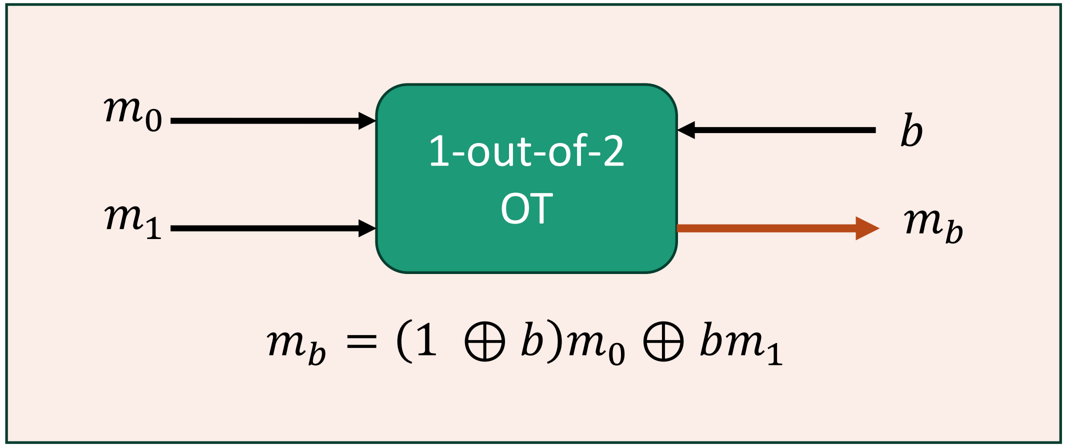
1. Alice know nothing about b.
2. Bob can only know message (M_b) and remains clueless about M_{1-b}.

1-out-of-n OT Protocol

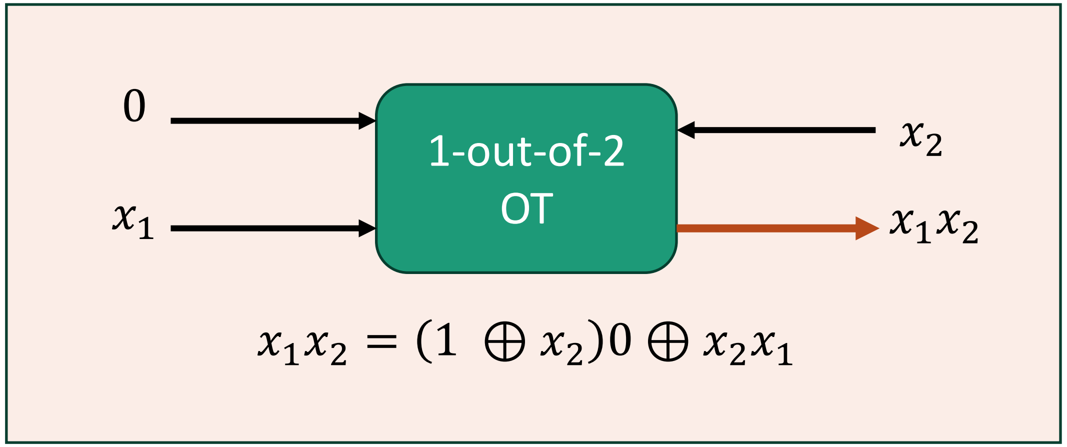


Oblivious Transfer (OT): Building Block of MPC

Let us consider a particular case of 2-parties.



1-out-of-2 OT Functionality

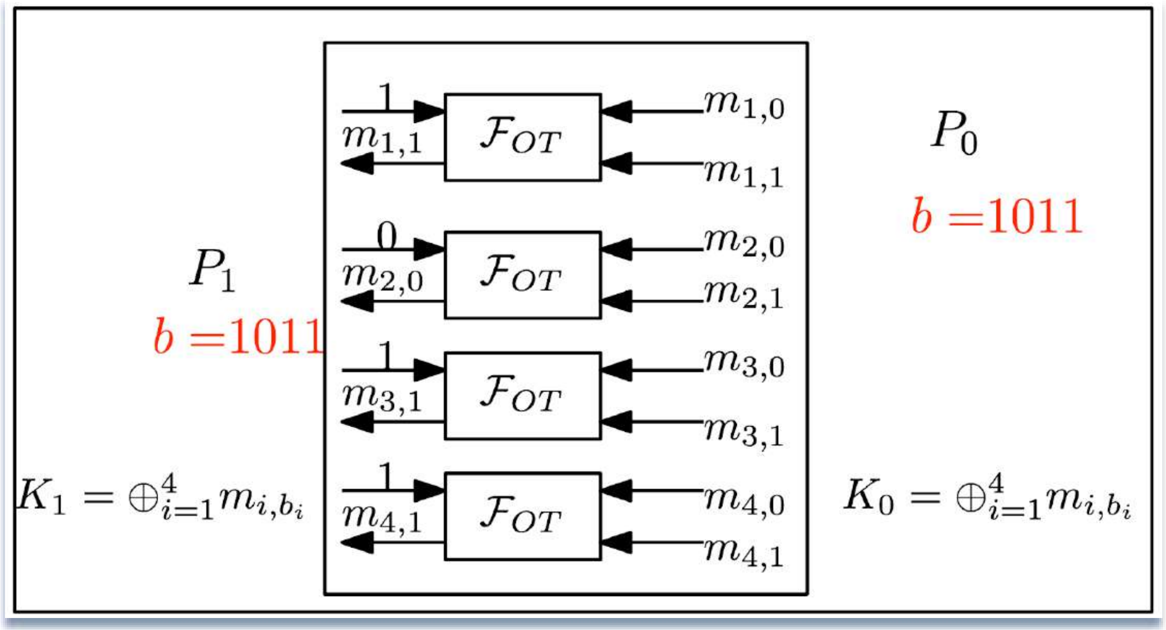


2-party AND protocol

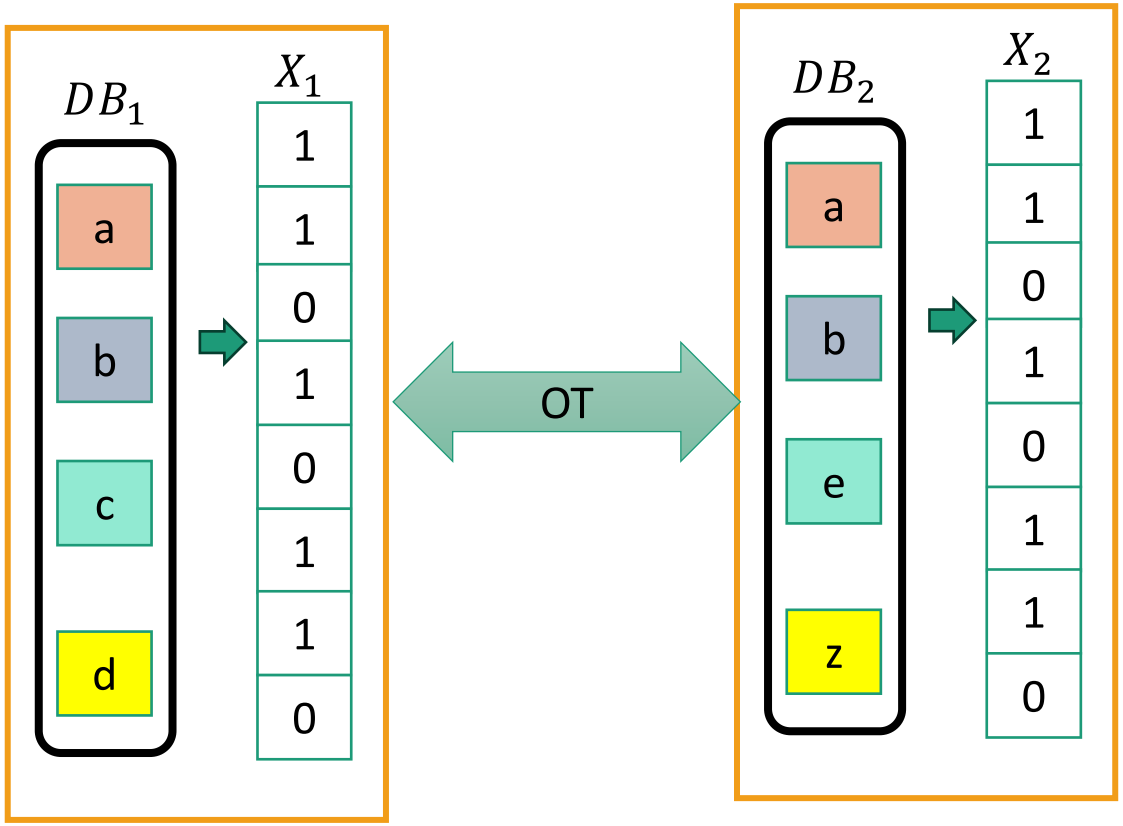
- ❑ Correctness of OT → Correctness of the AND protocol
- ❑ Privacy of OT → privacy of the AND Protocol

Oblivious Transfer (OT): For PAKE, PSI and others

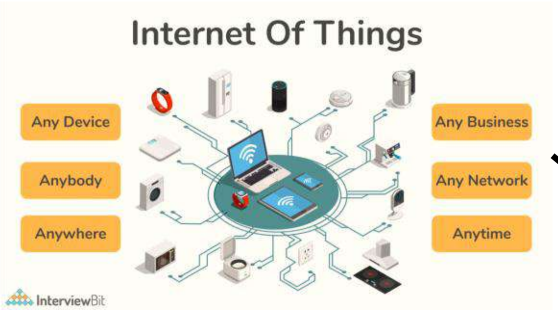
Password Authenticated Key Exchange (PAKE)



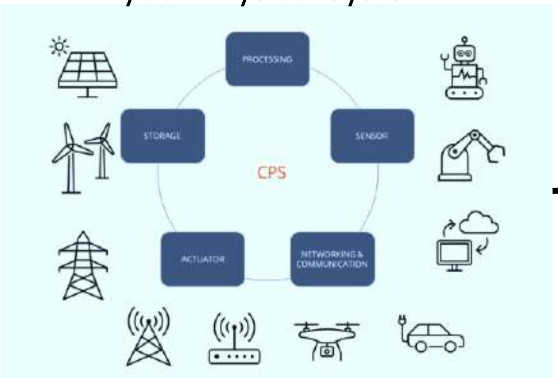
Private Set Intersection (PSI)

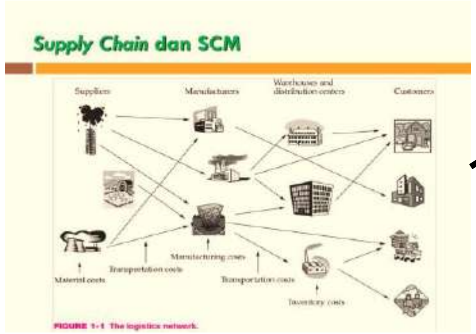


Oblivious Transfer in Resource Constrained IoT



Cyber Physical System





Resource Constrained
- Low computation
- Low storage

- Computation complexity
- Secure storage requirement
- Countermeasures against physical attacks

OT using Public Key Cryptography

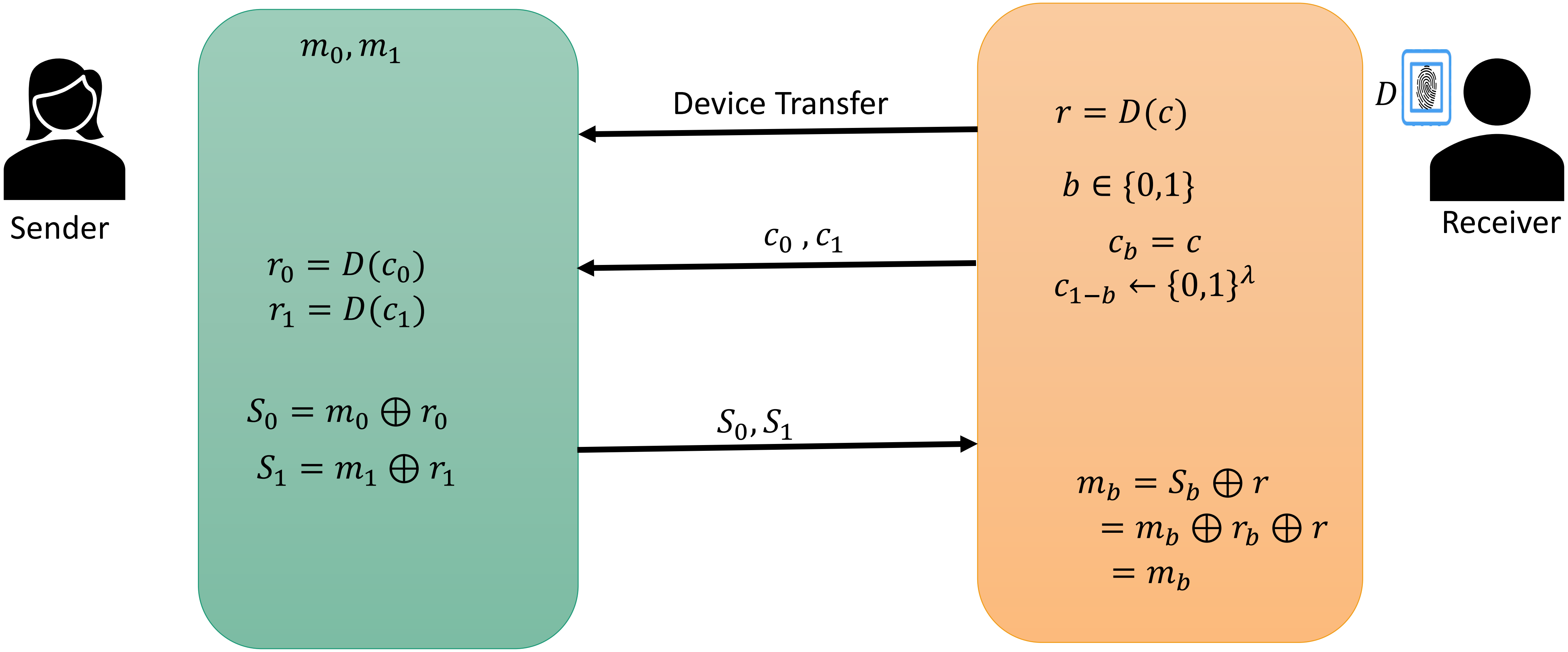
OT using Hardware Primitives

Physically Unclonable Functions (PUFs)

- Hardware intrinsic primitive.
- Due to inherent physical variations in electronic devices.
- Generates **unique** and **unpredictable** responses.
- Digital Fingerprint of a chip.

$$y_1 \neq y_2$$

Oblivious Transfer using PUFs



Oblivious Transfer using PUFs: SOTA

2010

Oblivious Transfer Based on Physical Unclonable Functions: Ulrich Ruhrmair proposed OT protocol implemented on Strong PUFs. In this paper, for the first time, PUFs are used beyond the known schemes for identification and Key Exchange.

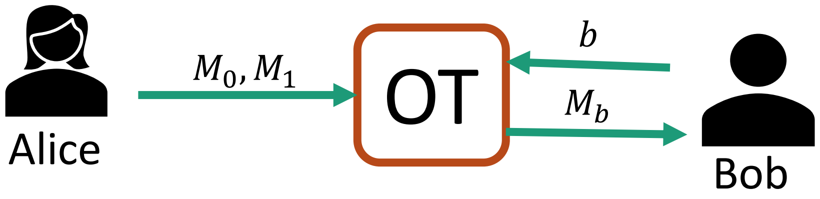
2011

Physically Unclonable Functions in the Universal Composition Framework: Brzuska, Fischin, Schroder, and Katzenbeisser augmented the PUF based protocol like oblivious transfer, commitments, and key exchange in universal composability (UC) framework.

2013

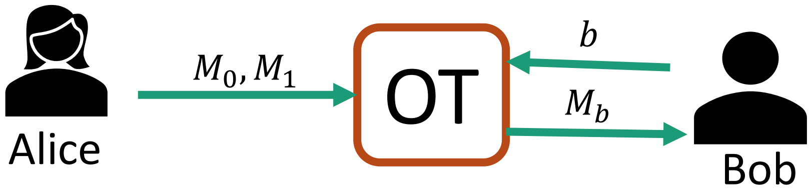
On the practical use of physical unclonable functions in oblivious transfer and bit commitment protocol: Ruhrmair Ulrich and Dijk Van Marten presented an attack on OT and BC protocol by Brzuska et al. and proposed a new OT protocol with better security.

Oblivious Transfer: State-of-the-art

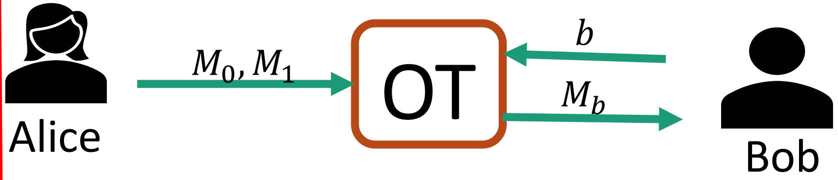


Public Key Primitives
- Heavy Computation
- DDH or ECDDH uses exponentiation

OT Extensions
- Lighter than public key
- Still not suitable for distributed systems like IoTs.

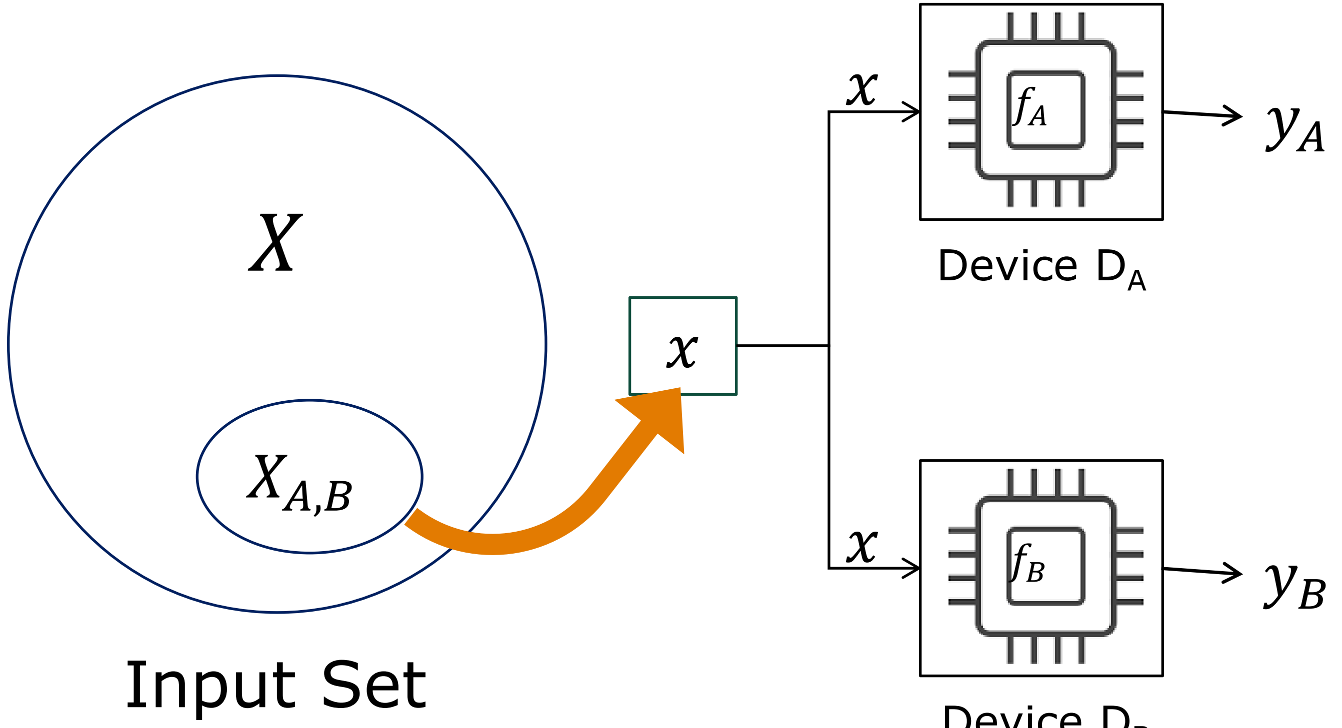


Hardware based primitives
- Physically Unclonable functions (PUF)
- Lighter than Previous setting
- Need storage for Challenge-Response Pair.
- Device Need to be transferred to other party



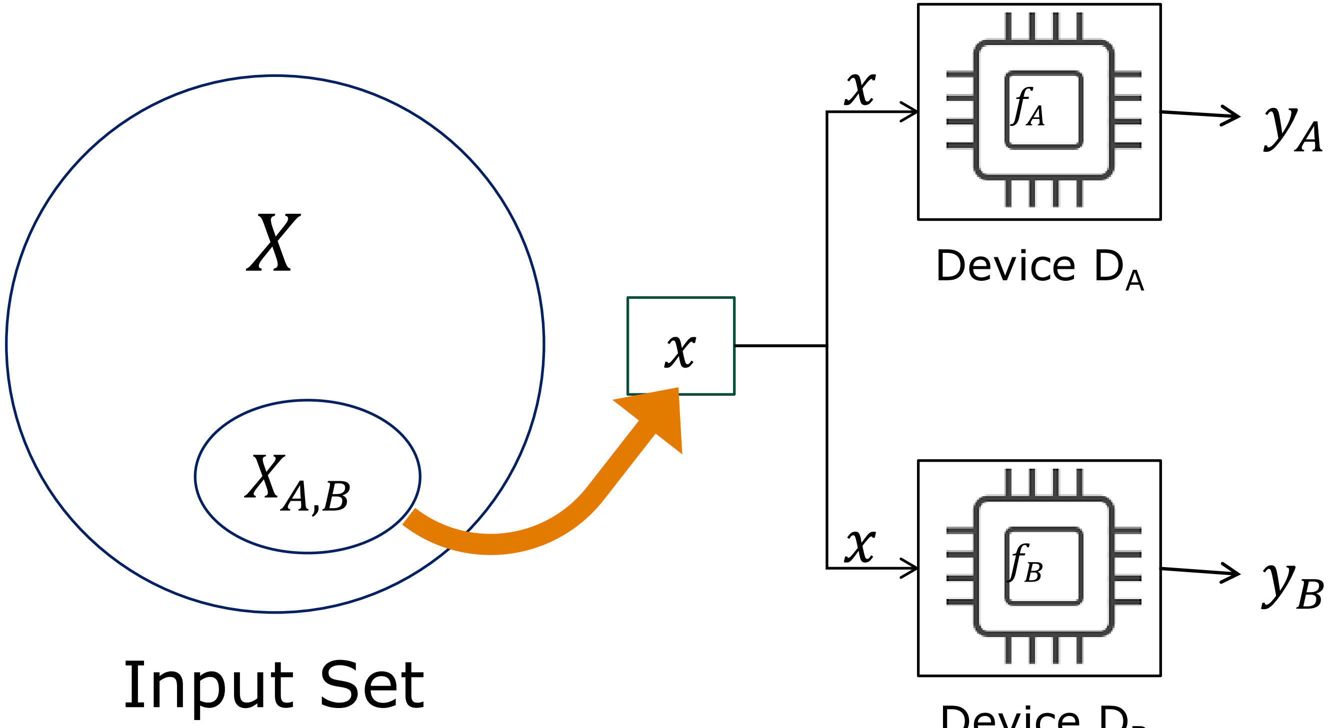
Hardware based primitives
- Physically Related functions (PReFs)
- Lighter computation
- Need least storage for Related input storage
- No need to transfer the device to other party

Physically Relatable Functions (PReFs): In Nut Shell



$$HD(y_A, y_B) \leq \delta$$

Physically Related Functions (PReFs): In Nut Shell



$x \in X_{A,B} \quad \delta = 3$

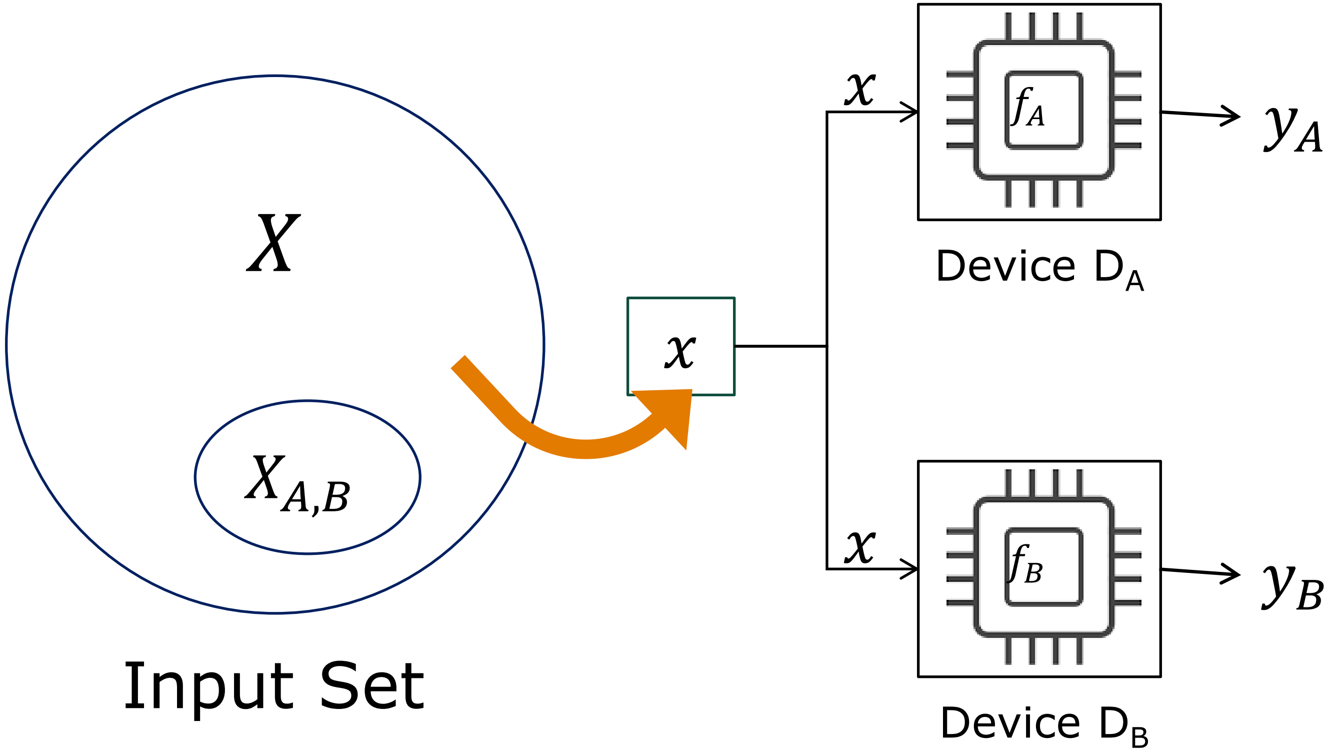
$y_A = 10110101$

$y_B = 10010111$

$HD(y_A, y_B) = 2 \leq \delta$

$$HD(y_A, y_B) \leq \delta$$

Physically Related Functions (PReFs): Properies



y_A, y_B are uncorrelated

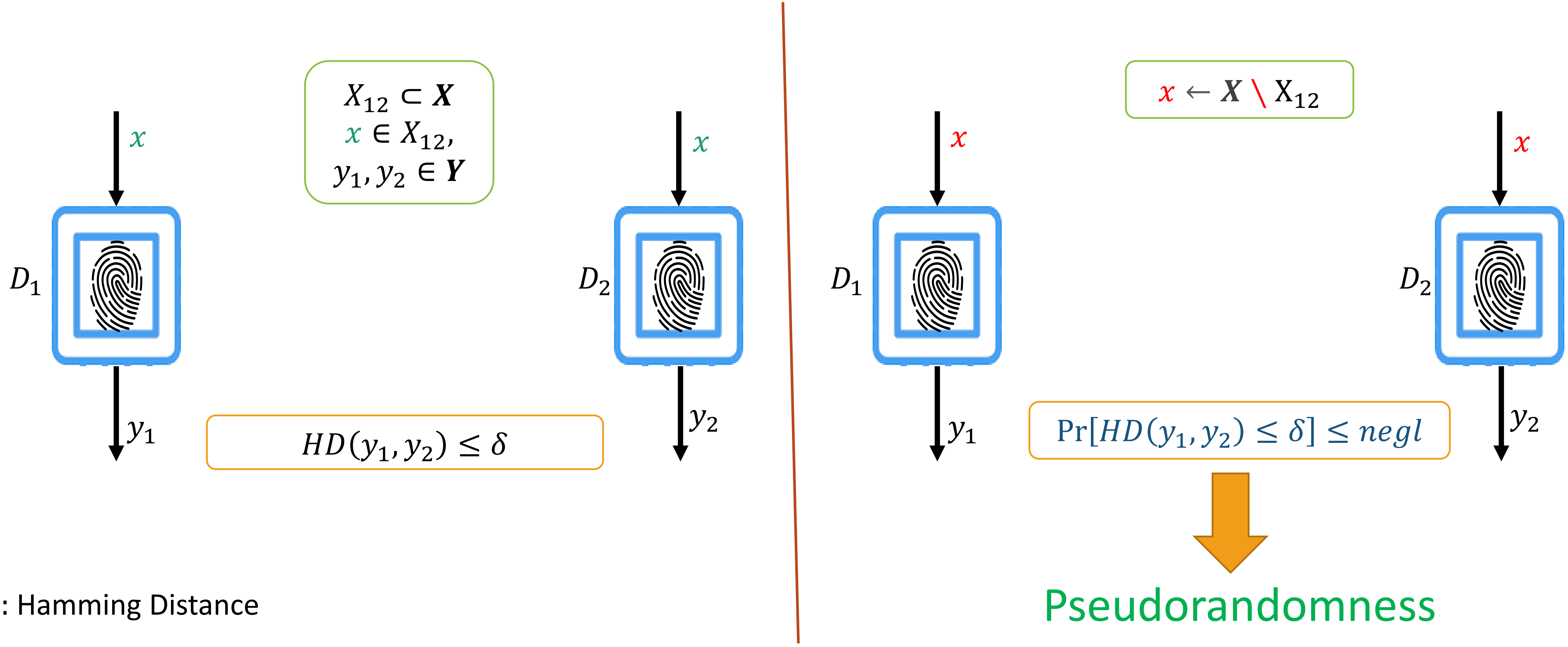
$x \notin X_{A,B}$

$y_A = 10110101$
$y_B = ?$

Pseudorandomness

Physically Related Functions (PReFs): Properties

Let D_1 and D_2 are two devices with input space $\boldsymbol{X}$ and output space $\boldsymbol{Y}$.



HD: Hamming Distance

Physically Relatable Functions (PReFs): Properties

Decisional Relation Hiding:

Given: $x \in X_{12}$ and $x' \leftarrow \boldsymbol{X}$

Difficult for adversary A to **distinguish between $\boldsymbol{x}$ and $\boldsymbol{x'}$,** without (knowing the functionalities) having physical access to D_1 and D_2.

Computational Relation Hiding:

Given: related input set X_{12}

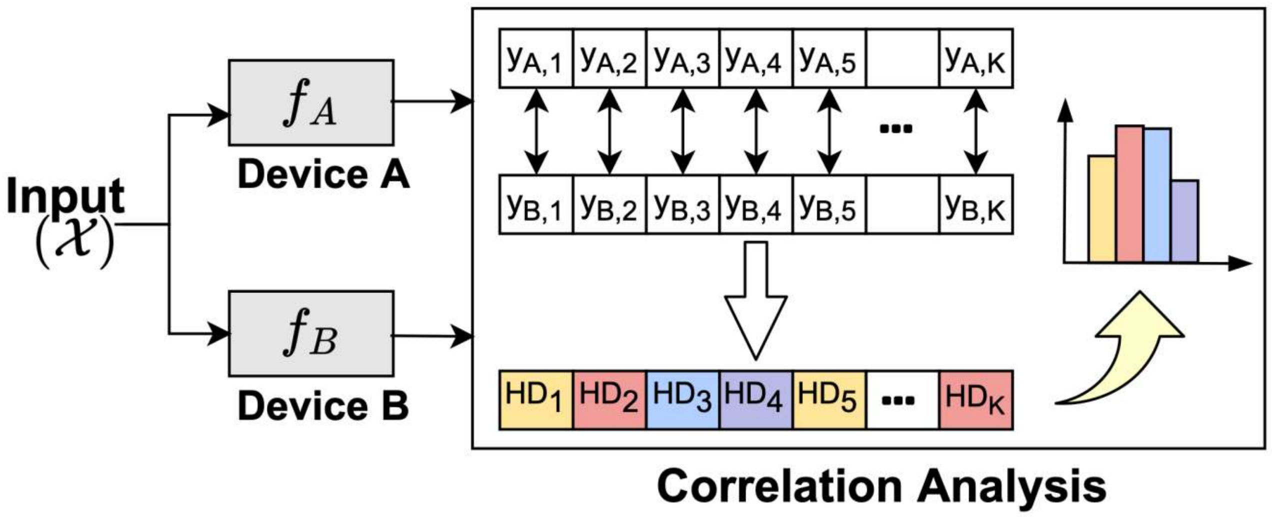
Difficult for adversary A to **generate related input x'** such that $\boldsymbol{HD(y_1, y_2) \leq \delta}$, without (knowing the functionalities) having physical access to D_1 and D_2.

Universality:

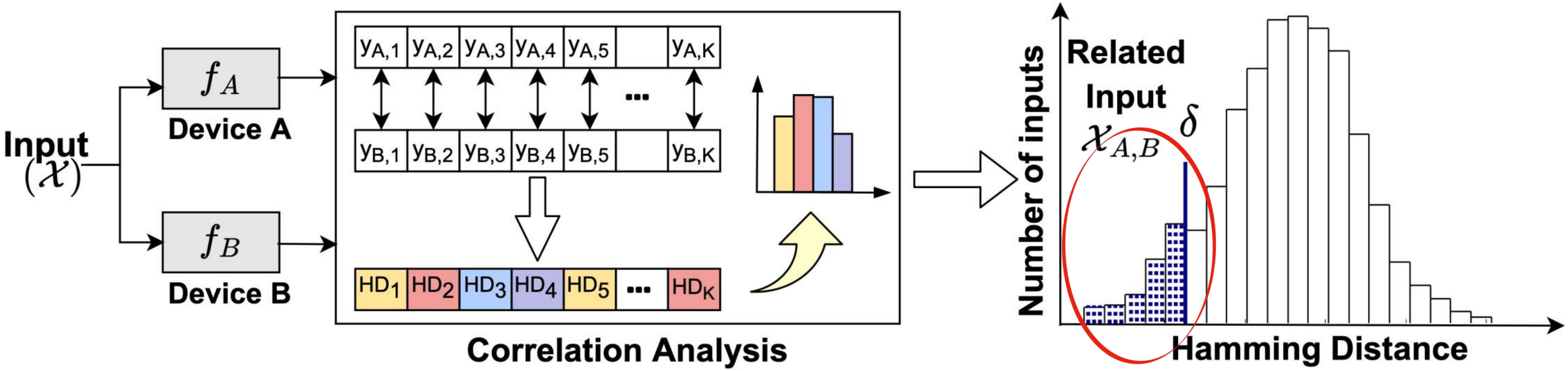
Given: $x \in X_{12}$

Difficult for adversary A to **distinguish between $\boldsymbol{D_1(x)}$ and $\boldsymbol{y}$** such that $\boldsymbol{y} \leftarrow \boldsymbol{Y}$.

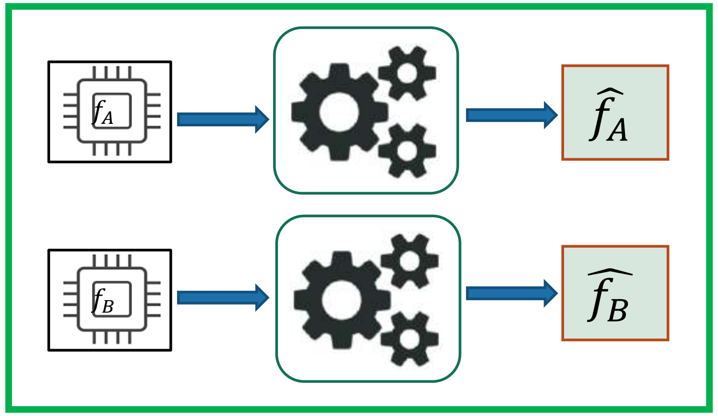
PReFs from PUFs: An Instance



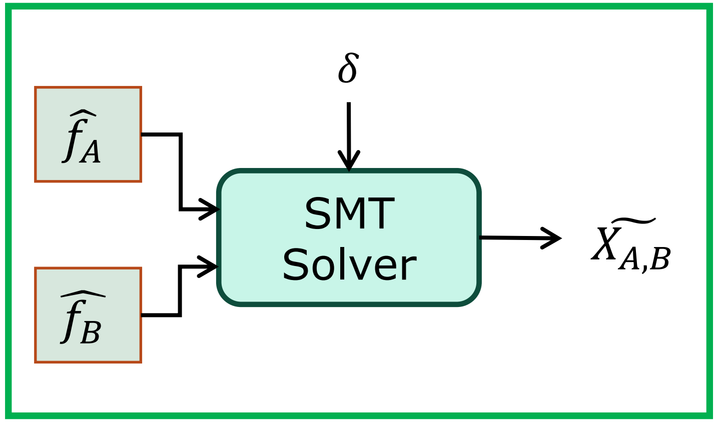
Existence of a unique and small input set over which two PUFs (f_A, f_B) output correlated responses



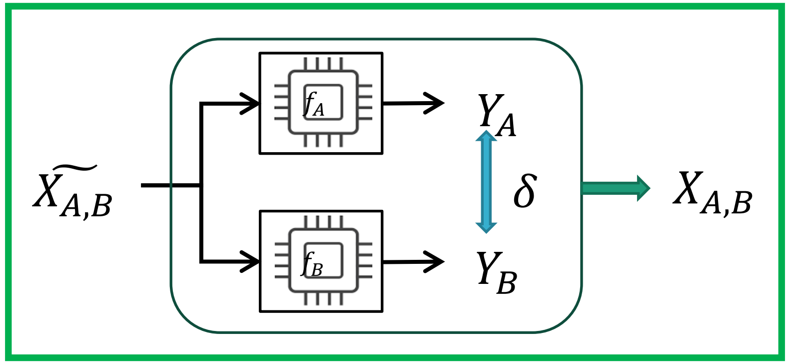
Identifying and Generating Related Inputs



Modeling before deployment



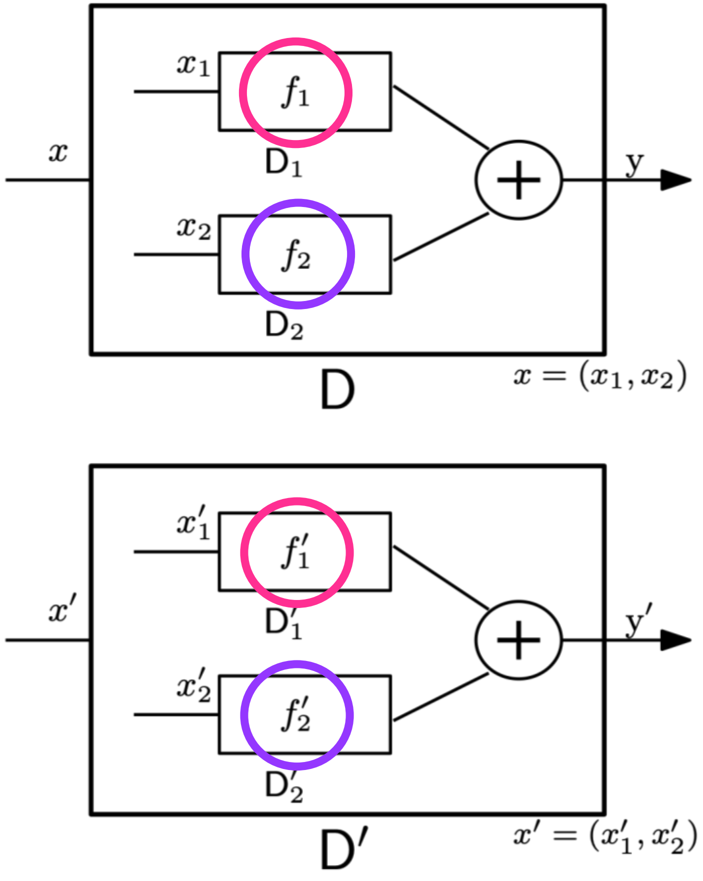
Sampling Related inputs

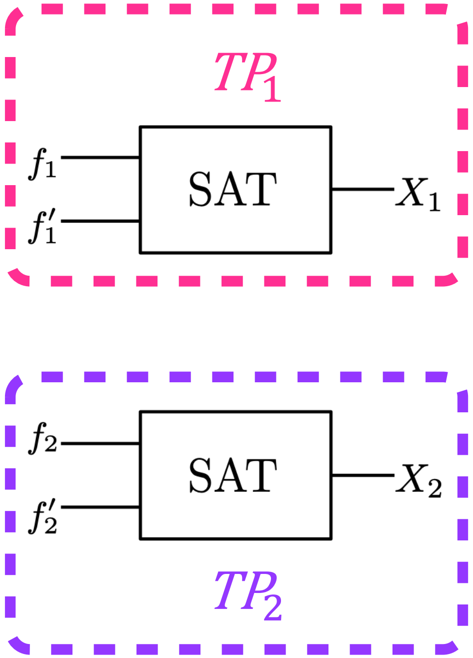


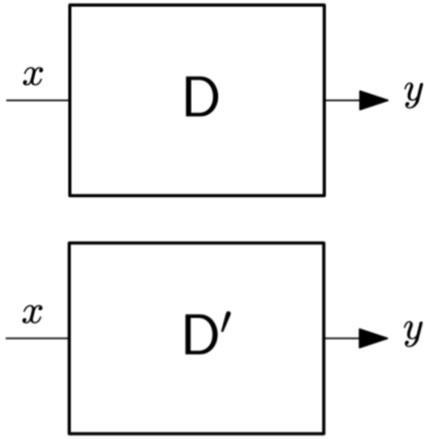
Filtering Inputs

Related Input has to be generated by a **Trusted Third Party.**

XOR-PReF: Removing Third Party







$x = (u, v)$, where $u \in X_1$, $v \in X_2$

$$f_1(u) = f_1'(u)$$
$$f_2(v) = f_2'(v)$$

$$\mathsf{D}(x) = f_1(u) \oplus f_2(v)$$
$$\mathsf{D}'(x) = f_1'(u) \oplus f_2'(v)$$

(D_1, D_1') – PReF Device Pair
(D_2, D_2') – PReF Device Pair

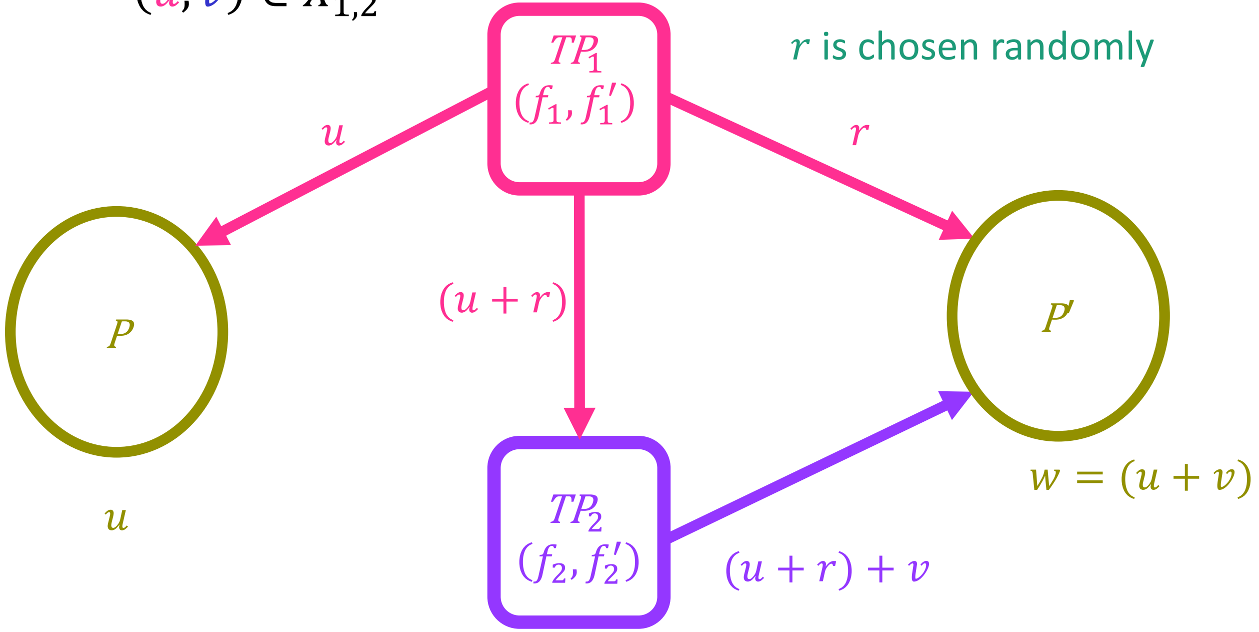
→

(D, D') – PReF Device Pair

XOR-PREF based OT: Setup Phase

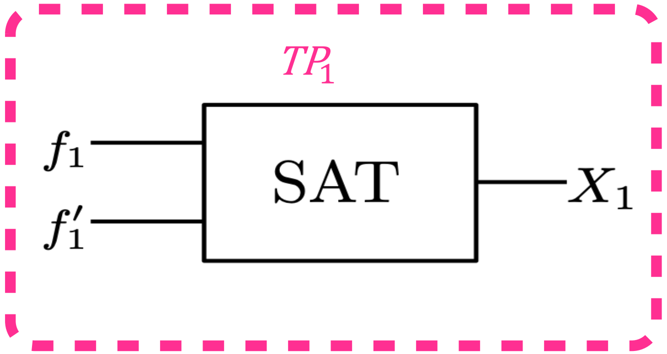
Input Format for Device D and D’

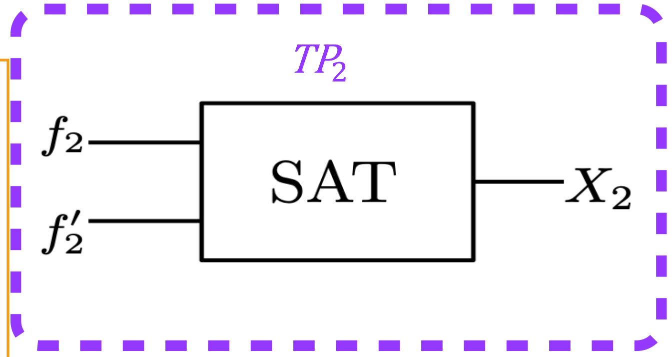
$(u, v) \in X_{1,2}$



$TP_1 : u \in X_1$

$TP_2 : v \in X_2$

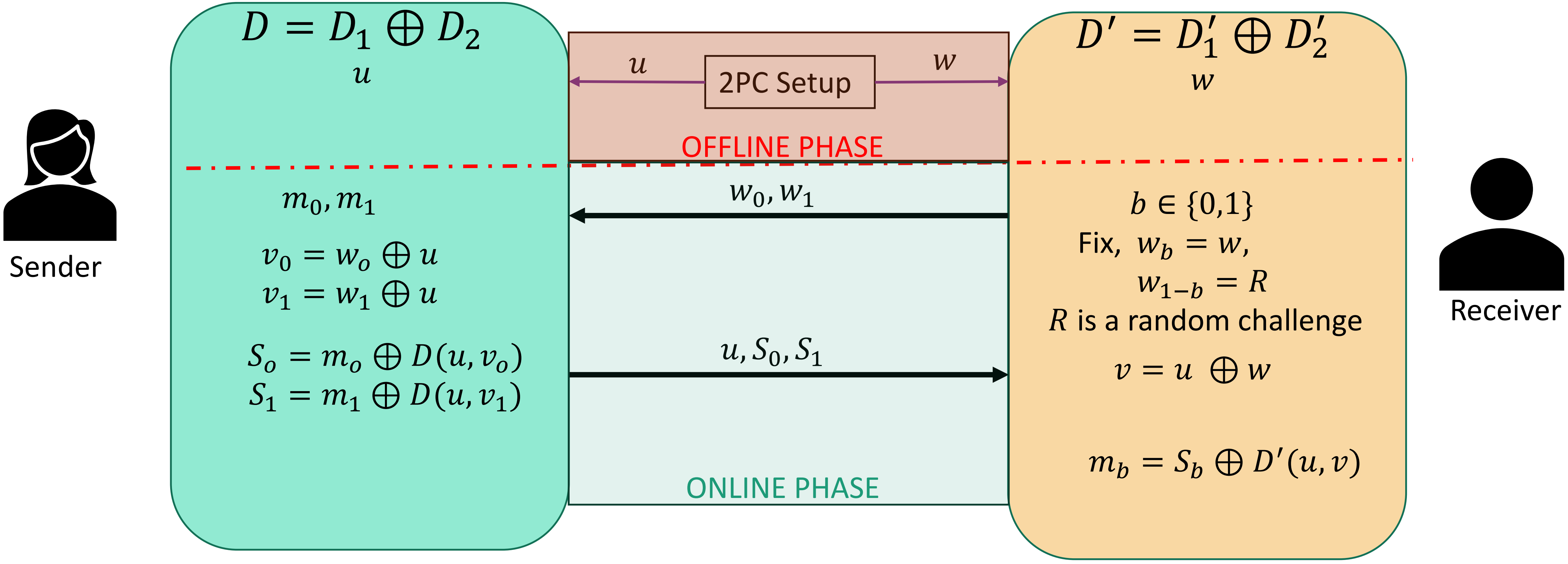




Four Points:

1. TP1 and TP2 are semi-honest and non-colluding.
2. Party P does not know v, w.
3. D(u,v) and D' (u,v) is indistinguishable from a random tuple (**relation hiding**).
4. D(u, v) + r is indistinguishable from s where r,s are chosen uniformly at random.

1. Oblivious Transfer using PReFs: Semi-malicious Receiver

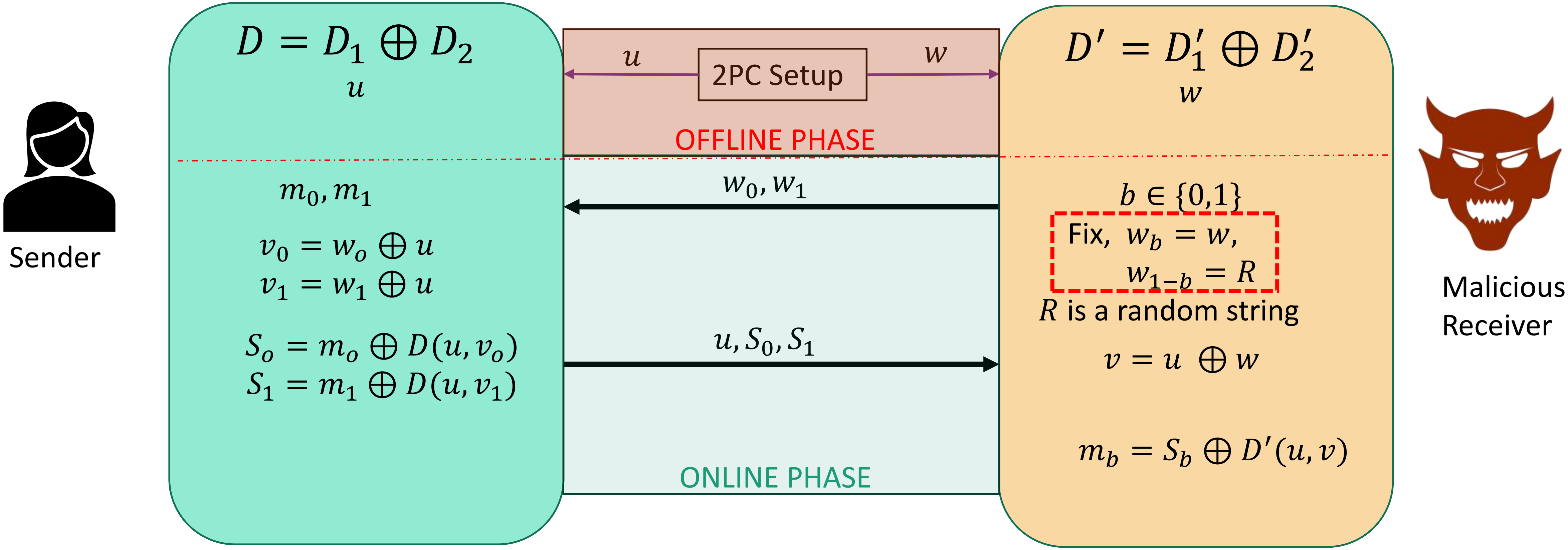


Proof of correctness:

$$S_b \oplus D'(u,v) = S_b \oplus D'(u, u \oplus w) = m_b \oplus D(u, v_b) \oplus D'(u, u \oplus w) = m_b \oplus \cancel{D(u, u \oplus w_b) \oplus D'(u, u \oplus w)}$$

$$= m_b$$

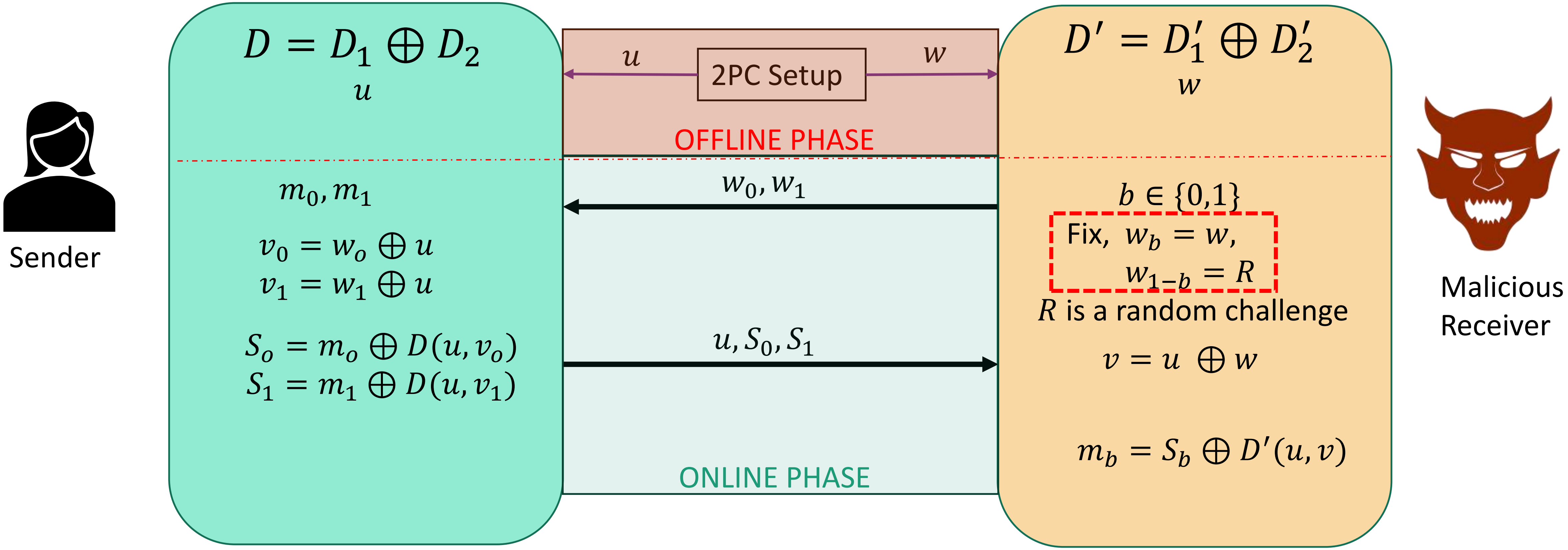
1. Oblivious Transfer using PReFs: Malicious Receiver



Possible Malicious Behaviour:

- **Case1:** Both w_0 and w_1 are chosen s.t. $D(u, v_0) = D'(u, v_1)$ and $D(u, v_1) = D'(u, v_1)$
  meaning, $D(u, u \oplus w_0) = D'(u, u \oplus w_0)$ and $D(u, u \oplus w_1) = D'(u, u \oplus w_1)$
  Which is, knowing only input $w \in X$, the malicious receiver can generate two inputs w_0 , $w_1 \in X$
  Breaking **Computational relation hiding property**.

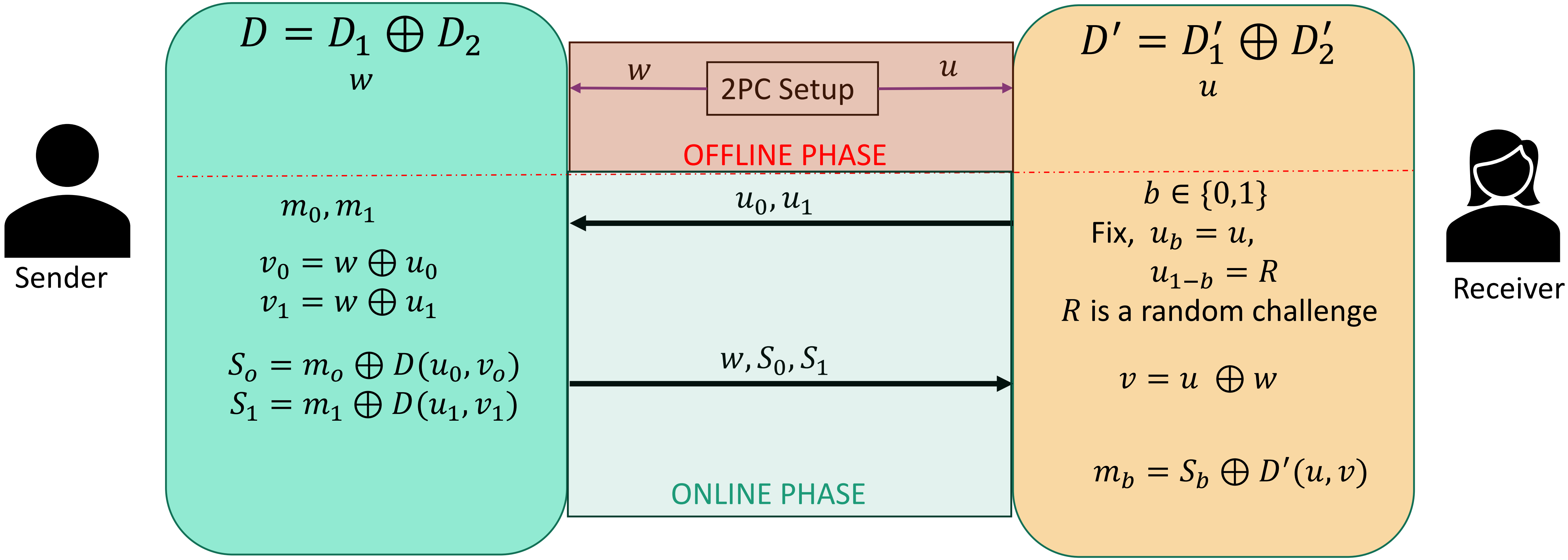
1. Oblivious Transfer using PReFs: Malicious Receiver



Possible Malicious Behaviour:

- **Case2:** Both w_0 and w_1 are chosen s.t. $D(u, v_0) = D'(u, v_1)$ and $D(u, v_1) \neq D'(u, v_1)$
  meaning, $D(u, u \oplus w_0) = D'(u, u \oplus w_0)$ and $D(u, u \oplus w_1) \neq D'(u, u \oplus w_1)$
  Which is, knowing only input $w \in X$ and without having access to device D, the malicious receiver can distinguish two outputs $\mathrm{D}(\mathrm{u}, \mathrm{v}_0)$ and $\mathrm{y} \in Y$, breaking **Conditional Pseudorandomness property**.

2. Oblivious Transfer using PReFs: Semi-malicious Receiver

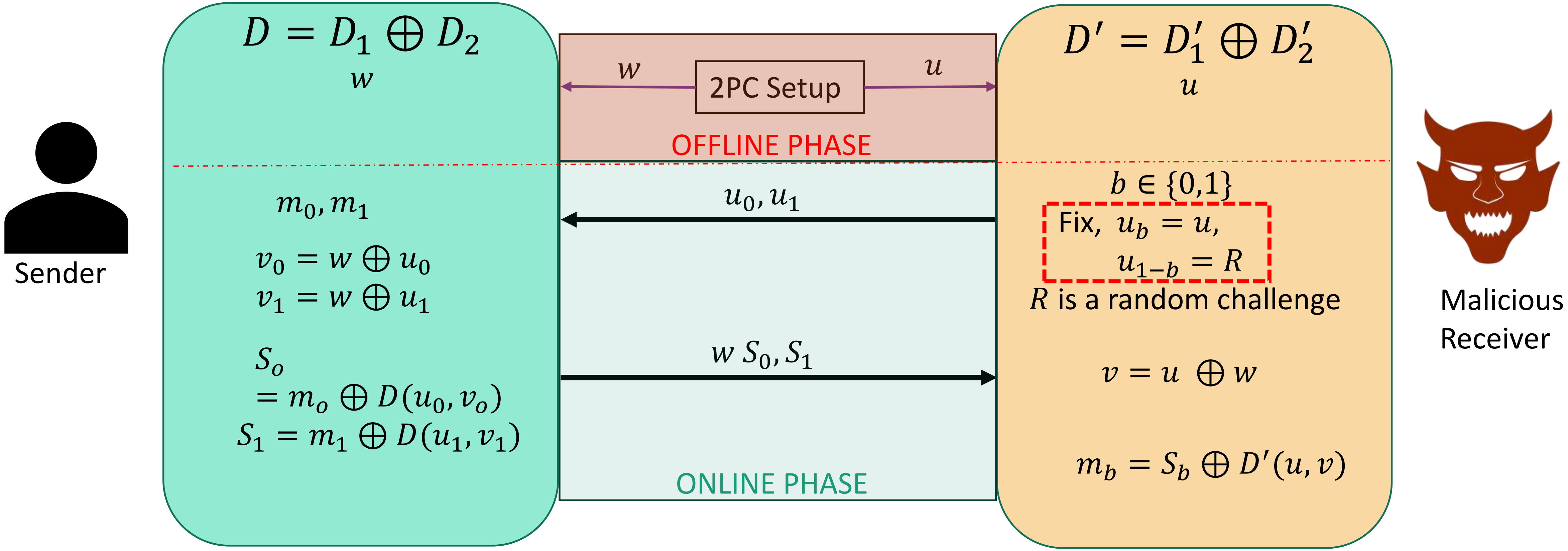


Proof of correctness:

$S_b \oplus D'(u,v) = S_b \oplus D'(u, u \oplus w) = m_b \oplus D(u, v_b) \oplus D'(u, u \oplus w) = m_b \oplus$ ~~$D(u, u_b \oplus w) \oplus D'(u, u \oplus w)$~~

$= m_b$

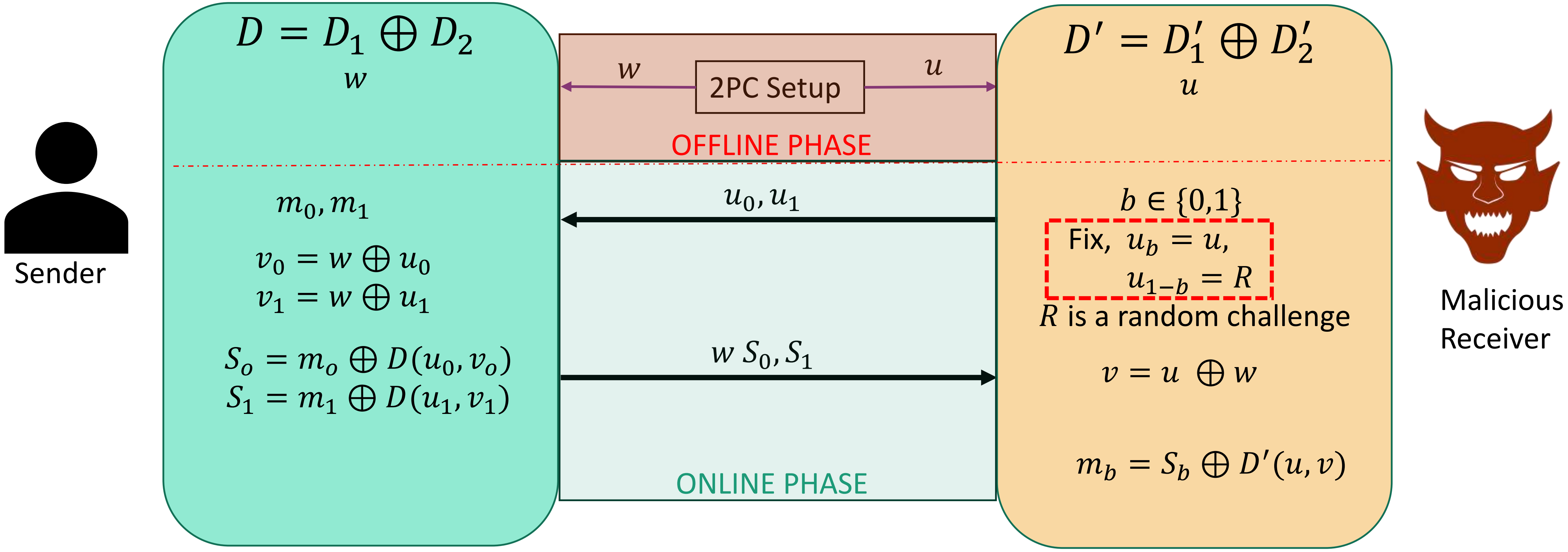
2. Oblivious Transfer using PReFs: Malicious Receiver



Possible Malicious Behaviour:

- **Case1:** Both u_0 and u_1 are chosen s.t. $D(u_0, v_0) = D'(u_0, v_0)$ and $D(u_1, v_1) = D'(u_{,1}\ v_1)$
  meaning, $D(u_0, u_0 \oplus w) = D'(u_0, u_0 \oplus w)$ and $D(u_1, u_1 \oplus w) = D'(u_1, u_1 \oplus w)$
  Which is, knowing only input $w \in X$, the malicious receiver can generate two inputs $u_0, u_1 \in X$
  Breaking **Computational relation hiding property**.

2. Oblivious Transfer using PReFs: Malicious Receiver

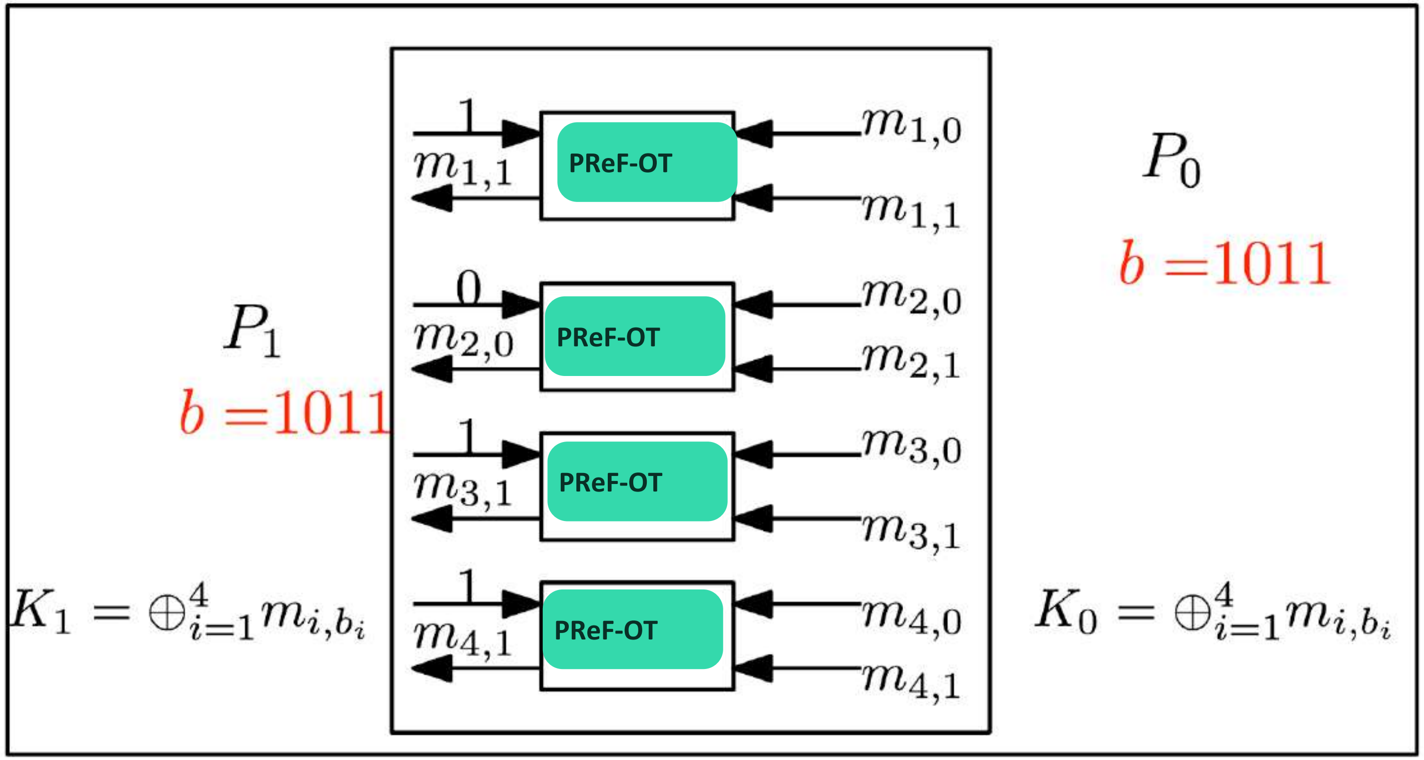


Possible Malicious Behaviour:

- **Case2:** Both w_0 and w_1 are chosen s.t. $D(u, v_0) = D'(u, v_1)$ and $D(u, v_1) \neq D'(u, v_1)$
  meaning, $D(u_0, u_0 \oplus w) = D'(u_0, u_0 \oplus w)$ and $D(u_1, u_1 \oplus w_1) \neq D'(u_{,1}\ u_1 \oplus w_1)$
  Which is, knowing only input $w \in X$ and without having access to device D, the malicious receiver can distinguish two outputs $\mathrm{D}(\mathrm{u}, \mathrm{v}_0)$ and $\mathrm{y} \in Y$, breaking **Conditional Pseudorandomness property**.

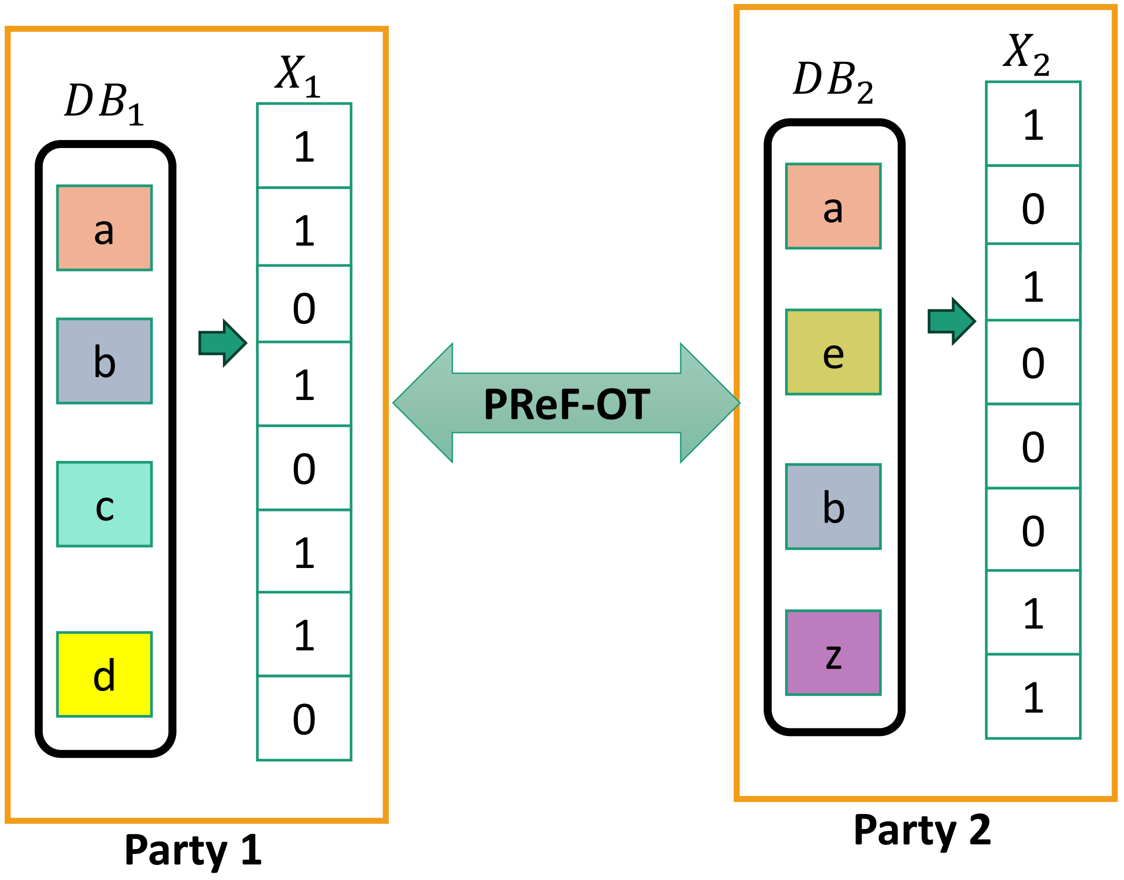
Applications: PAKE using **OT-PReF**

PAKE: Password Authenticated Key Exchange



Applications: PSI using **OT-PReF**

PSI: Private Set Intersection



Advantages of PReFs based OT protocol

1. Secure against malicious receiver and security depends on one's own primitive.

2. Pseudorandomness property helps honest party maintain security if the inputs are honestly generated.

3. No physical transfer of device can assist in adopting to build complex MPC protocols.

4. The protocol is Lightweight and does not require any other cryptographic blocks. It need only 2 message communication requirement.

Conclusion

1. MPC helps in achieving security and privacy in distributed computing.
2. We build lightweight OT protocols from XOR_PReFs, a fundamental building block for MPC.
3. We eliminate the long-standing physical transfer requirement of hardware primitive.
4. We additionally show new applications like PSI and PAKE


THANK YOU

Questions