Statistically-Sender-Private Oblivious-Transfer from LPN and Derandomization

Nir Bitansky, **Sapir Freizeit**

Tel Aviv University

The work in a nutsheel 

Goal

To expand the reach of Learning Parity with Noise (LPN).

The work in a nutsheel 

Goal

To expand the reach of Learning Parity with Noise (LPN).

Focus

2-message Statistically-Sender-Private Oblivious-Transfer (SSP-OT)

- OT where we take round complexity and security to the extreme

The work in a nutsheel 

Goal

To expand the reach of Learning Parity with Noise (LPN).

Focus

2-message Statistically-Sender-Private Oblivious-Transfer (SSP-OT)

- OT where we take round complexity and security to the extreme

Results:

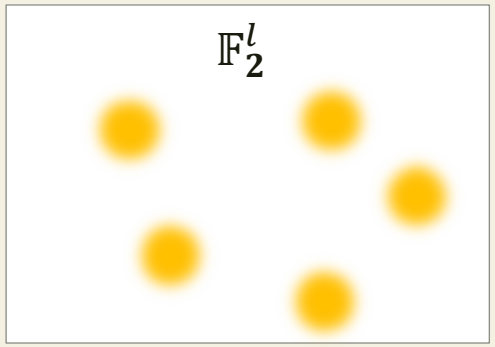
1. Construct SSP-OT in the common random string model from LPN.
2. Remove the crs using a standard derandomization assumption.

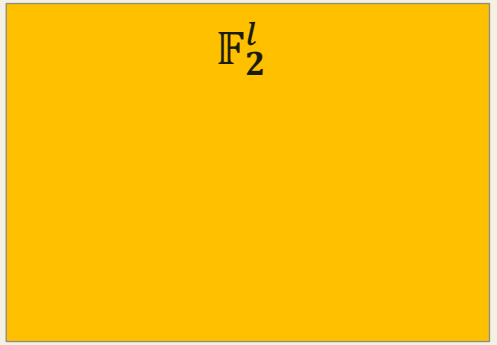
Learning Parity With Noise (LPN_{ε})

Noise rate: $\varepsilon = \varepsilon(n)$

$$\boldsymbol{A} \leftarrow \mathbb{F}_2^{l \times n}, \boldsymbol{s} \leftarrow \mathbb{F}_2^{n}, \boldsymbol{e} \leftarrow Bern(\boldsymbol{\varepsilon})^{l}, \boldsymbol{r} \leftarrow \mathbb{F}_2^{l}$$

$$\left(\underset{l}{\boldsymbol{A}}, \underset{n}{\boldsymbol{A}} \boldsymbol{s} + \boldsymbol{e} \right) \overset{c}{\approx} \left(\boldsymbol{A}, \boldsymbol{r} \right)$$





LWE vs LPN

- Learning With Errors (LWE): $\mathbb{F}_q$ for large q, Gaussian error.

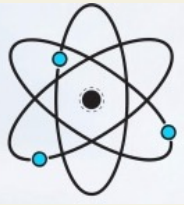
LWE vs LPN

- Learning With Errors (LWE): $\mathbb{F}_q$ for large q, Gaussian error.

- Both are plausibly hard, resilient to quantum attacks.

LWE vs LPN

- Learning With Errors (LWE): $\mathbb{F}_q$ for large q, Gaussian error.
- Both are plausibly hard, resilient to quantum attacks.
- Similar in flavor – but different: LPN is far behind LWE.



LWE vs LPN

- Learning With Errors (LWE): $\mathbb{F}_q$ for large q, Gaussian error.

- Both are plausibly hard, resilient to quantum attacks.

- Similar in flavor – but different: LPN is far behind LWE.

- **Known Applications**:
  - LPN ⇒ mostly basic primitives:
    secret-key encryption [Gilbert et al. 08], PKE [Alekhnovich 03], commitments [JPT 11], CRH [BLVW19, YZW+17]…
  - LWE ⇒ advanced primitives:
    Fully Homomorphic Encryption [Gen09, BV11], ABE [BV16], NIZK [PS19] and much more…

LWE vs LPN

- Learning With Errors (LWE): $\mathbb{F}_q$ for large q, Gaussian error.

- Both are plausibly hard, resilient to quantum attacks.

- Similar in flavor – but different: LPN is far behind LWE.

- **Known Applications**:
  - LPN ⇒ mostly basic primitives:
    secret-key encryption [Gilbert et al. 08], PKE [Alekhnovich 03], commitments [JPT 11], CRH [BLVW19, YZW+17]…
  - LWE ⇒ advanced primitives:
    Fully Homomorphic Encryption [Gen09, BV11], ABE [BV16], NIZK [PS19] and much more…

- **Hardness Results**:
  LWE [Regev05, Peikert09…] is better understood than LPN [BKW00, BLVW19].

So why LPN?

- **Efficiency:** simple bit operations.

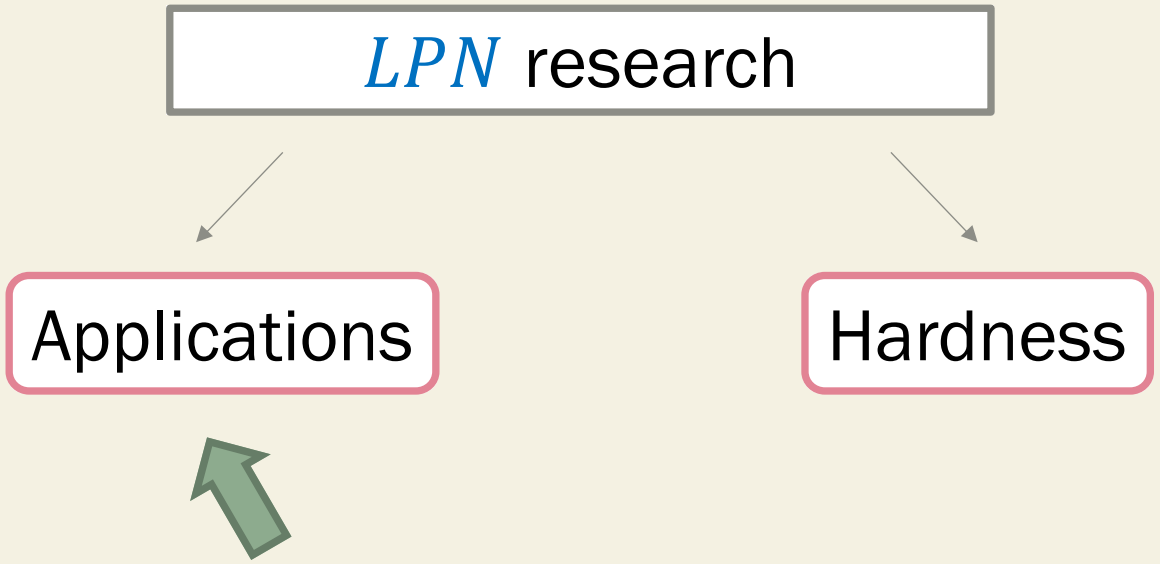
So why LPN?

- **Efficiency:** simple bit operations.
- **Robustness:** basing crypto on a variety of assumptions.

So why LPN?

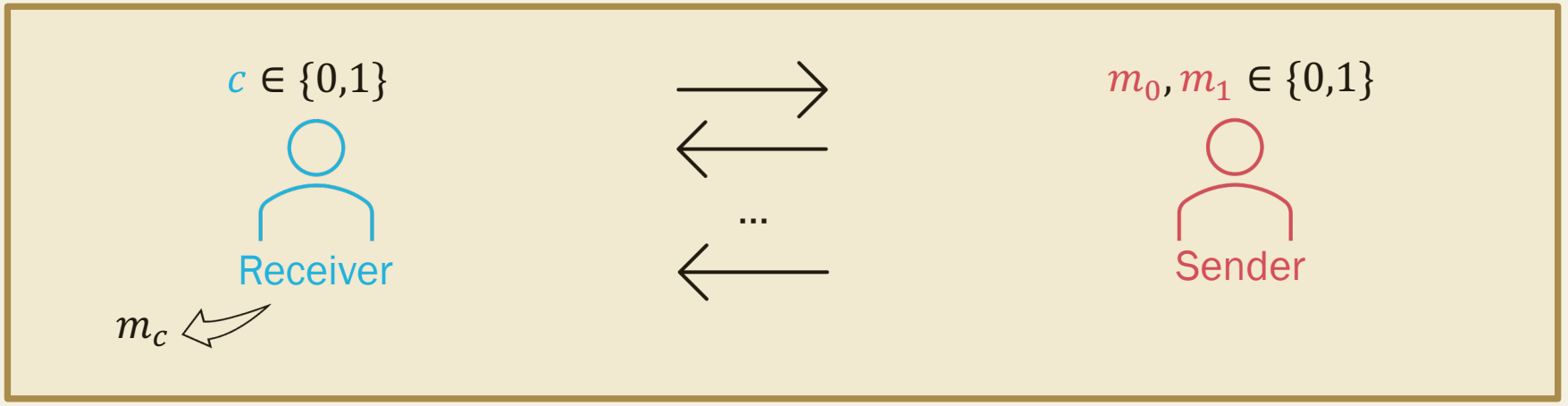
- **Efficiency:** simple bit operations.
- **Robustness:** basing crypto on a variety of assumptions.
- **Theoretical:** fundamental problem.

Our Contribution



This work:
Statistically-Sender-Private Oblivious-Transfer (SSP-OT) from LPN and derandomization

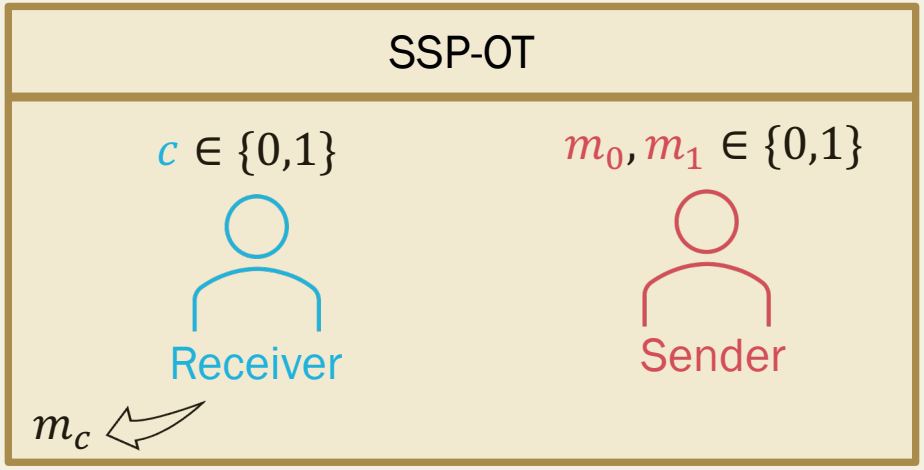
Oblivious Transfer (OT)



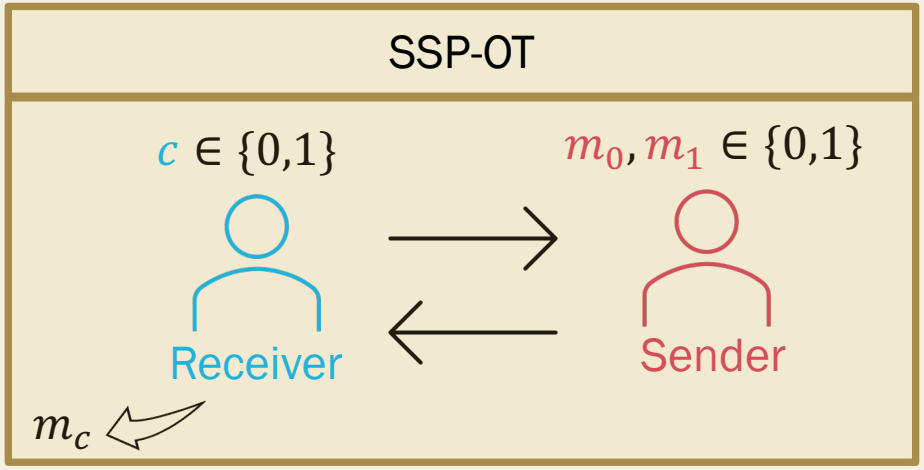
Common Goal	Security
Receiver should learn m_c.	• Sender doesn't learn c. • Receiver doesn't learn m_{1-c}.

Features of interest:
round complexity, communication complexity, security level...

Statistically-Sender Private OT (SSP-OT) [Naor-Pinkas 01], [Aiello et al. 01]

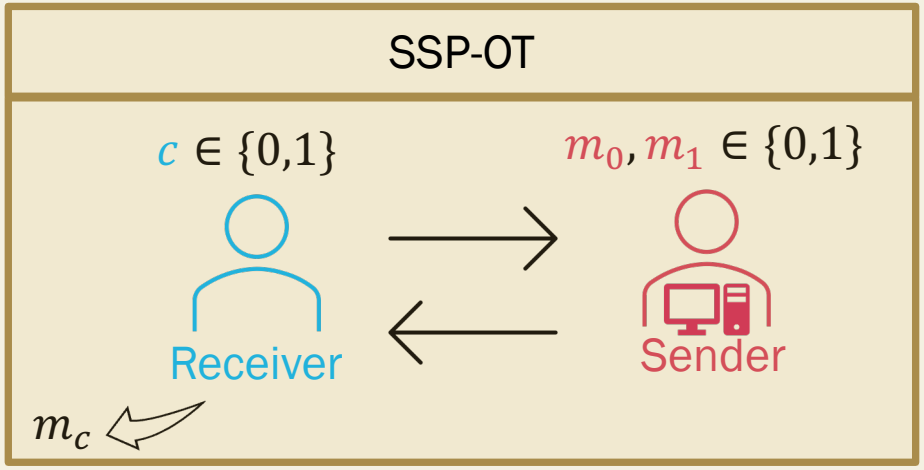


Statistically-Sender Private OT (SSP-OT) [Naor-Pinkas 01], [Aiello et al. 01]



Minimal Round Complexity
Minimal **2-message** protocol.

Statistically-Sender Private OT (SSP-OT) [Naor-Pinkas 01], [Aiello et al. 01]



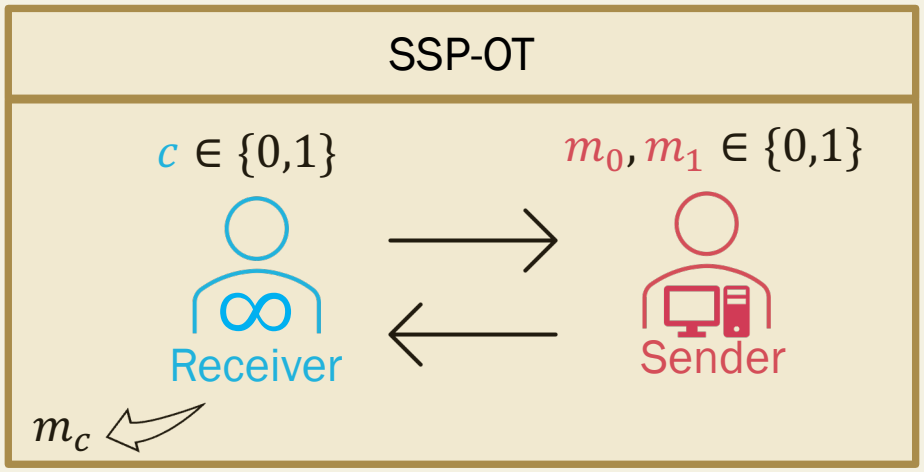
Minimal Round Complexity

Minimal **2-message** protocol.

Computational Receiver Security

Comp-bounded Sender doesn't learn c.

Statistically-Sender Private OT (SSP-OT) [Naor-Pinkas 01], [Aiello et al. 01]



Minimal Round Complexity

Minimal **2-message** protocol.

Computational Receiver Security

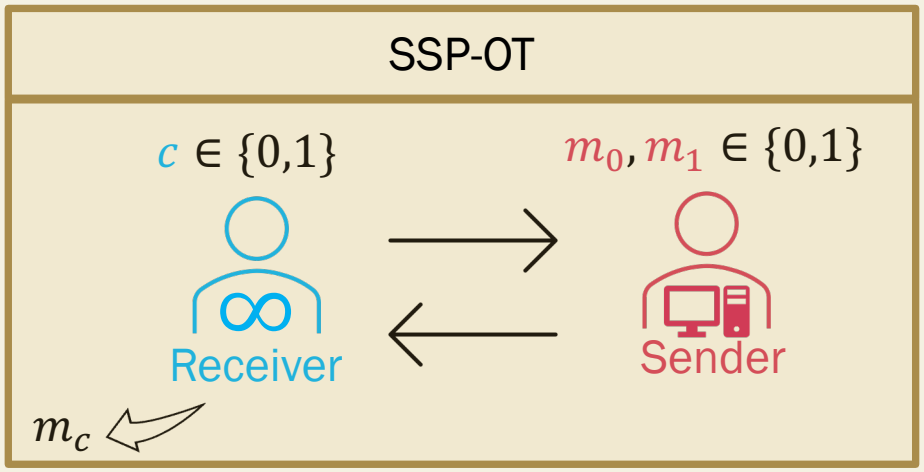
Comp-bounded Sender doesn't learn c.

Statistical Sender Security

Unbounded Receiver doesn't learn m_{1-c}.

1st msg information-theoretically fixes $c^* \in \{0,1\}$ s.t. m_{1-c^*} is **statistically** hidden.

Statistically-Sender Private OT (SSP-OT) [Naor-Pinkas 01], [Aiello et al. 01]



Minimal Round Complexity

Minimal **2-message** protocol.

Computational Receiver Security

Comp-bounded Sender doesn't learn c.

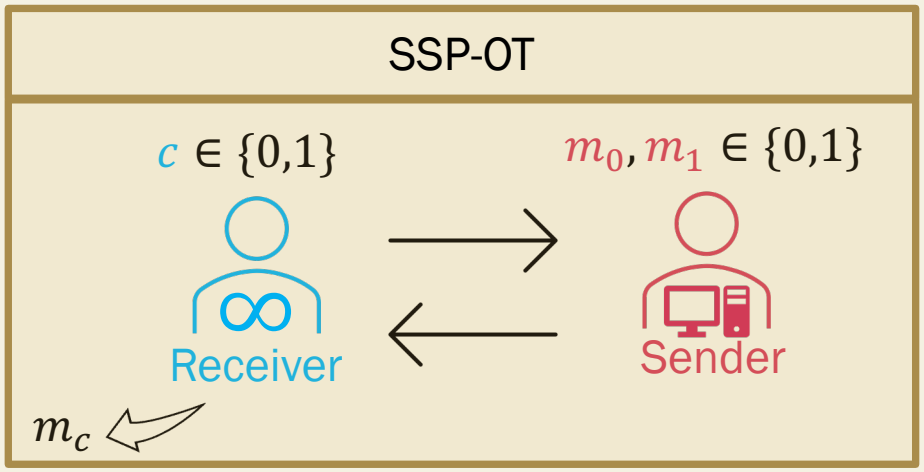
Statistical Sender Security

Unbounded Receiver doesn't learn m_{1-c}.

1st msg information-theoretically fixes $c^* \in \{0,1\}$ s.t. m_{1-c^*} is **statistically** hidden.

- Taking round-complexity and security to the extreme.

Statistically-Sender Private OT (SSP-OT) [Naor-Pinkas 01], [Aiello et al. 01]



Minimal Round Complexity

Minimal **2-message** protocol.

Computational Receiver Security

Comp-bounded Sender doesn't learn c.

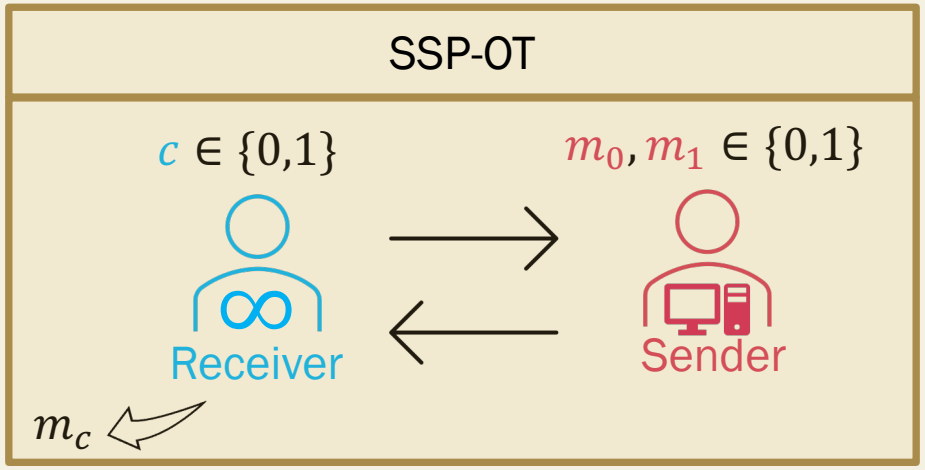
Statistical Sender Security

Unbounded Receiver doesn't learn m_{1-c}.

1st msg information-theoretically fixes $c^* \in \{0,1\}$ s.t. m_{1-c^*} is **statistically** hidden.

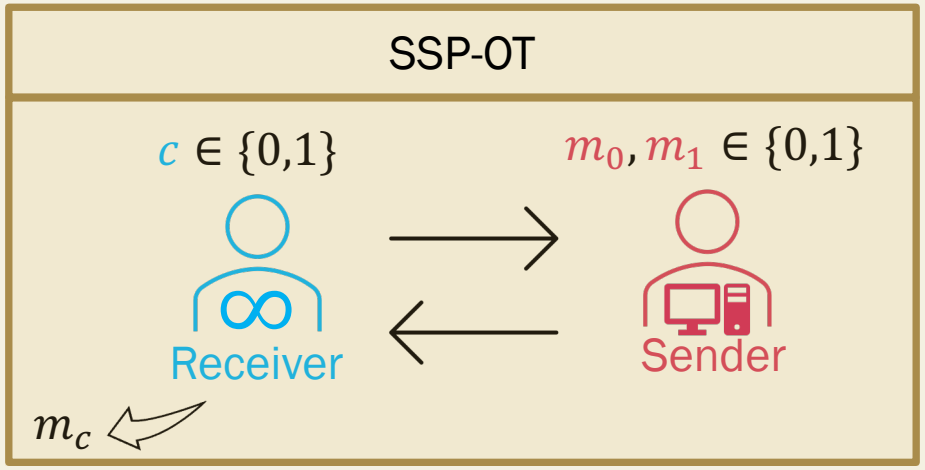
- Taking round-complexity and security to the extreme.
- Highly useful, reducing interaction: 2-msg statistically-WI [BGI+17], [KKS18], weak zero-knowledge [JKKR17], [BKP19], MPC with min round complexity [AJ17], [BGJ+18], Correctness amplification for iO [BV16] …

Prior work



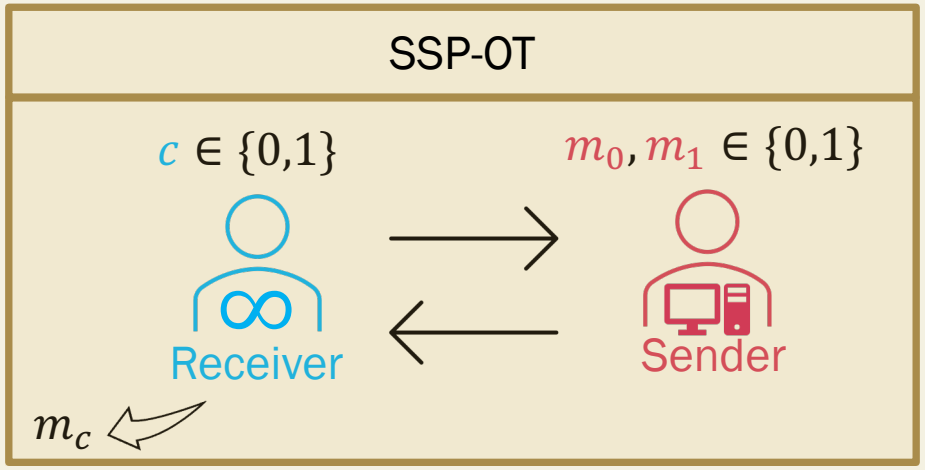
- Up until recently, SSP-OT only from number-theoretic assumptions (quantunly broken) [NP01, AIR01, HK12…].

Prior work



- Up until recently, SSP-OT only from number-theoretic assumptions (quantunly broken) [NP01, AIR01, HK12…].
- Post quantum SSP-OT: from LWE [Brakerski - Dottling 18], [DGI+19], [ADD+22].

Prior work

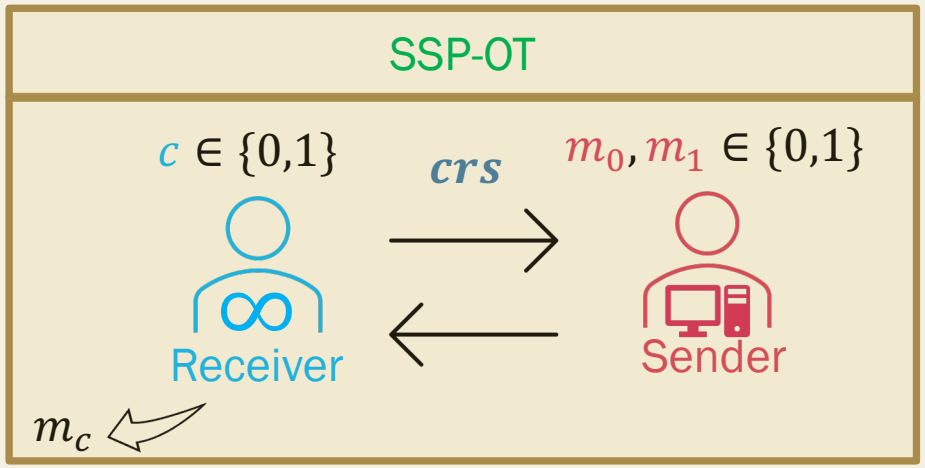


- Up until recently, SSP-OT only from number-theoretic assumptions (quantunly broken) [NP01, AIR01, HK12…].
- Post quantum SSP-OT: from LWE [Brakerski - Dottling 18], [DGI+19], [ADD+22].
- From LPN: (both sides) computationally private OT in the crs model [Dottling et al. 19].

Results

1. Construct a 2-message statistically-sender-private OT (SSP-OT) in the common random string (crs) model from LPN.

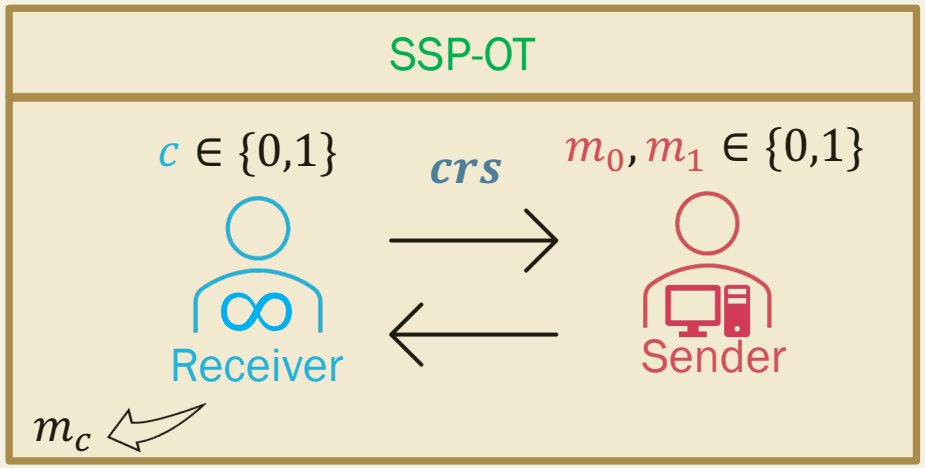
$LPN \Rightarrow$



Results

1. Construct a 2-message statistically-sender-private OT (SSP-OT) in the common random string (crs) model from LPN.
2. Remove the crs using standard Nisan-Wigderson style derandomization.

$LPN \Rightarrow$



Derandomization $\Rightarrow$ can remove the crs

Low noise LPN

Low noise: $LPN_{\log^2 n/n}$ is breakable in quasi-poly time [BKW00].

Low noise LPN

Low noise: $LPN_{\log^2 n/n}$ is breakable in quasi-poly time [BKW00].

- Other basic primitives are only known from $LPN_{\log^2 n/n}$.
  E.g., collision resistant hashing [BLVW19, YZW+17].

Low noise LPN

Low noise: $LPN_{\log^2 n/n}$ is breakable in quasi-poly time [BKW00].

- Other basic primitives are only known from $LPN_{\log^2 n/n}$.
  E.g., collision resistant hashing [BLVW19, YZW+17].

- Potential Complexity Barrier:

  1. LPN_{ε} implies SSP-OT $\Rightarrow LPN_{\varepsilon} \in BPP^{SZK}$,

Low noise LPN

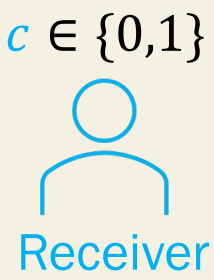
Low noise: $LPN_{\log^2 n/n}$ is breakable in quasi-poly time [BKW00].

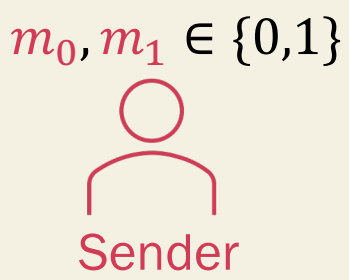
- Other basic primitives are only known from $LPN_{\log^2 n/n}$.
  E.g., collision resistant hashing [BLVW19, YZW+17].

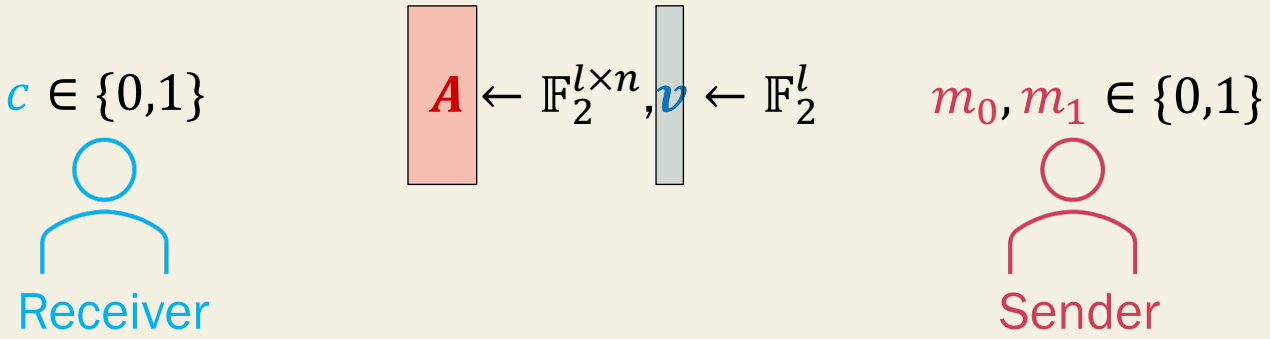
- Potential Complexity Barrier:

  1. LPN_{ε} implies SSP-OT $\Rightarrow LPN_{\varepsilon} \in BPP^{SZK}$,
  2. currently known only for $\varepsilon \approx \log^2 n\,/n$ [BLVW19] .

AND NOW FOR THE CONSTRUCTION...


$c \in \{0,1\}$
Receiver


$m_0, m_1 \in \{0,1\}$
Sender


$c \in \{0,1\}$
$\boldsymbol{A} \leftarrow \mathbb{F}_2^{l \times n}, \boldsymbol{v} \leftarrow \mathbb{F}_2^{l}$
$m_0, m_1 \in \{0,1\}$
Receiver
Sender

$c \in \{0,1\}$

Receiver

$\boldsymbol{A} \leftarrow \mathbb{F}_2^{l \times n}, \boldsymbol{v} \leftarrow \mathbb{F}_2^{l}$

$m_0, m_1 \in \{0,1\}$

Sender

$\boldsymbol{s} \leftarrow \mathbb{F}_2^{n}, \boldsymbol{e} \leftarrow Bern(\varepsilon)^{l}$

$\boldsymbol{v}_0 \coloneqq \boldsymbol{A}\boldsymbol{s} + \boldsymbol{e} + c \cdot \boldsymbol{v}$ $\xrightarrow{\quad \boldsymbol{v}_0 \quad}$

$c \in \{0,1\}$

Receiver

$\boldsymbol{A} \leftarrow \mathbb{F}_2^{l \times n}, \boldsymbol{v} \leftarrow \mathbb{F}_2^{l}$

$m_0, m_1 \in \{0,1\}$

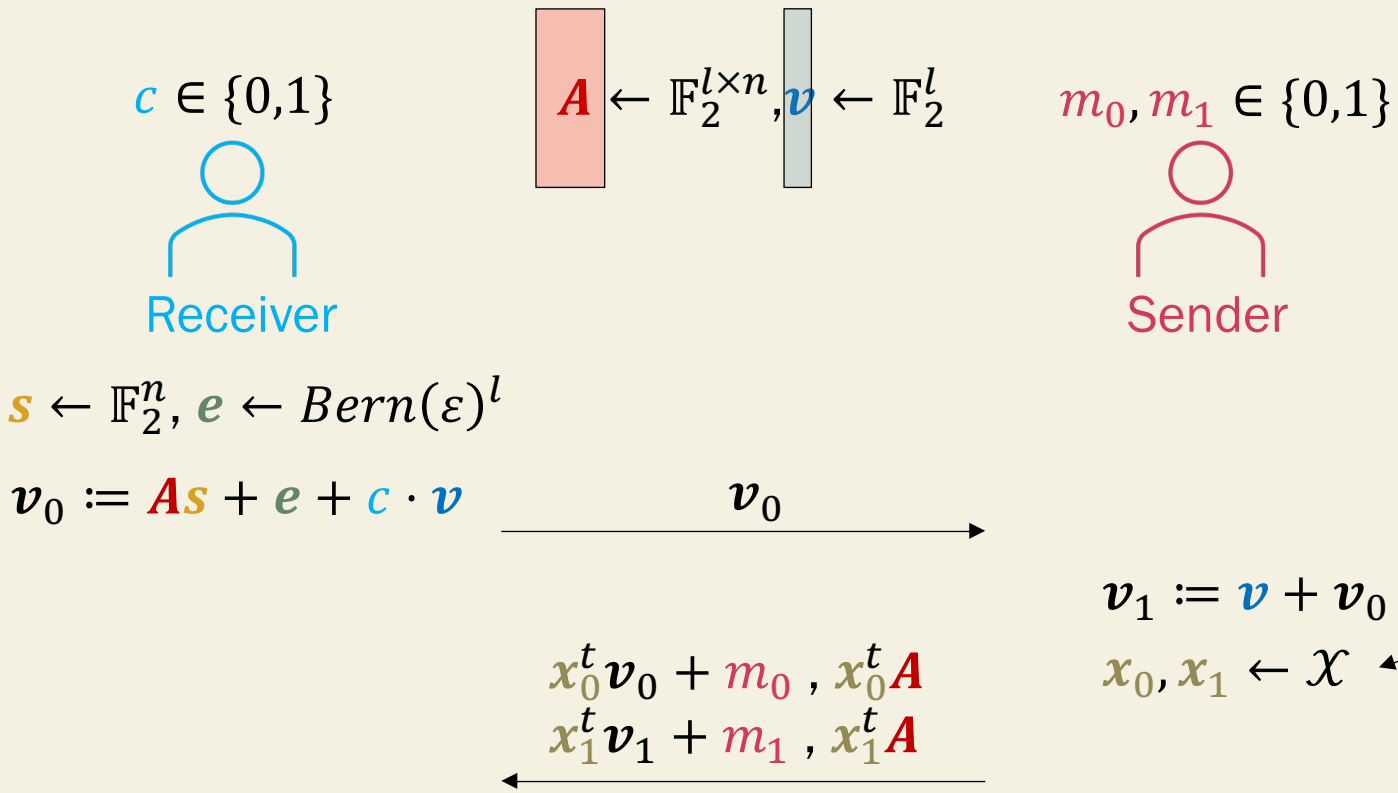
Sender

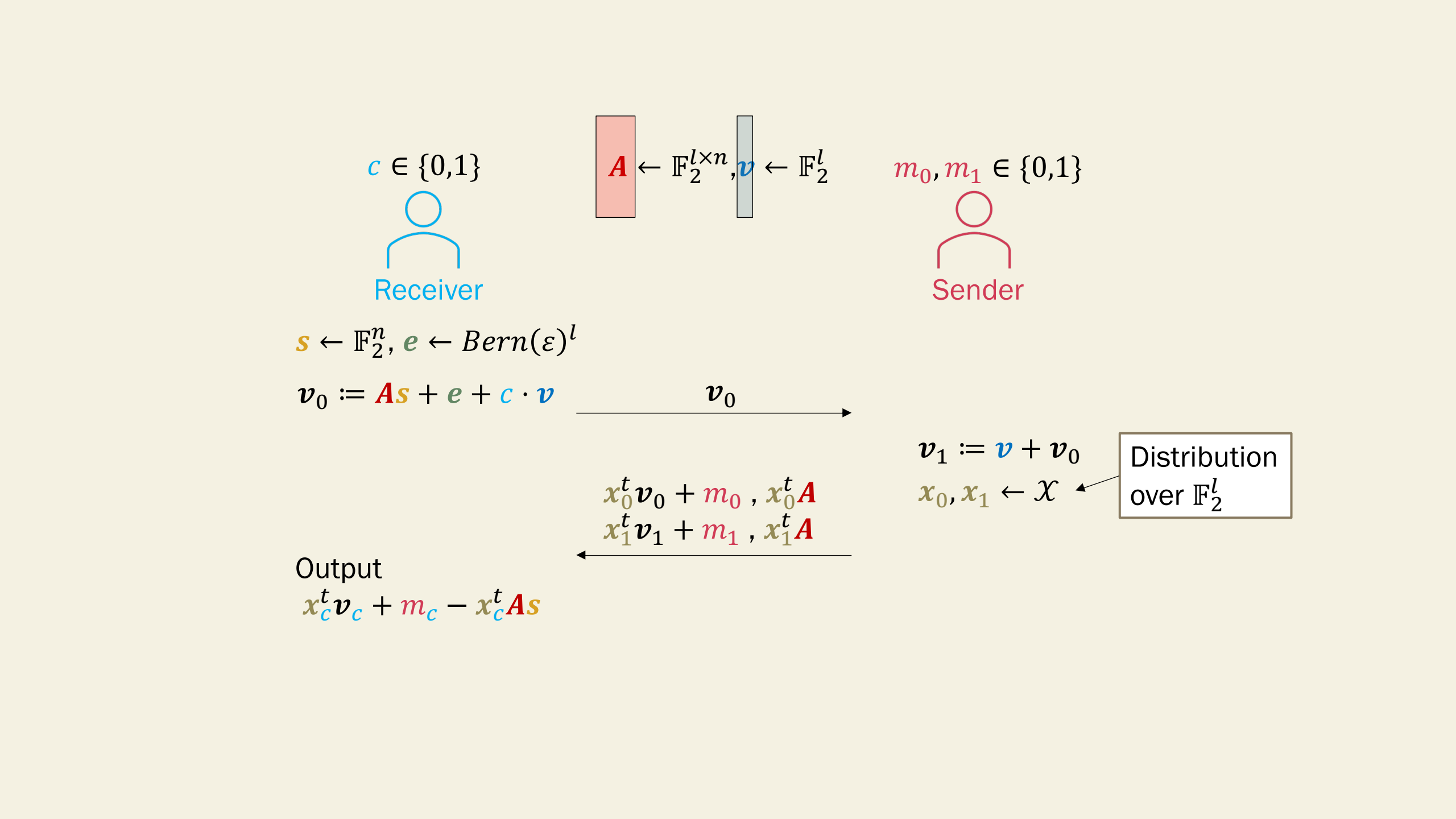
$\boldsymbol{s} \leftarrow \mathbb{F}_2^{n}, \boldsymbol{e} \leftarrow Bern(\varepsilon)^{l}$

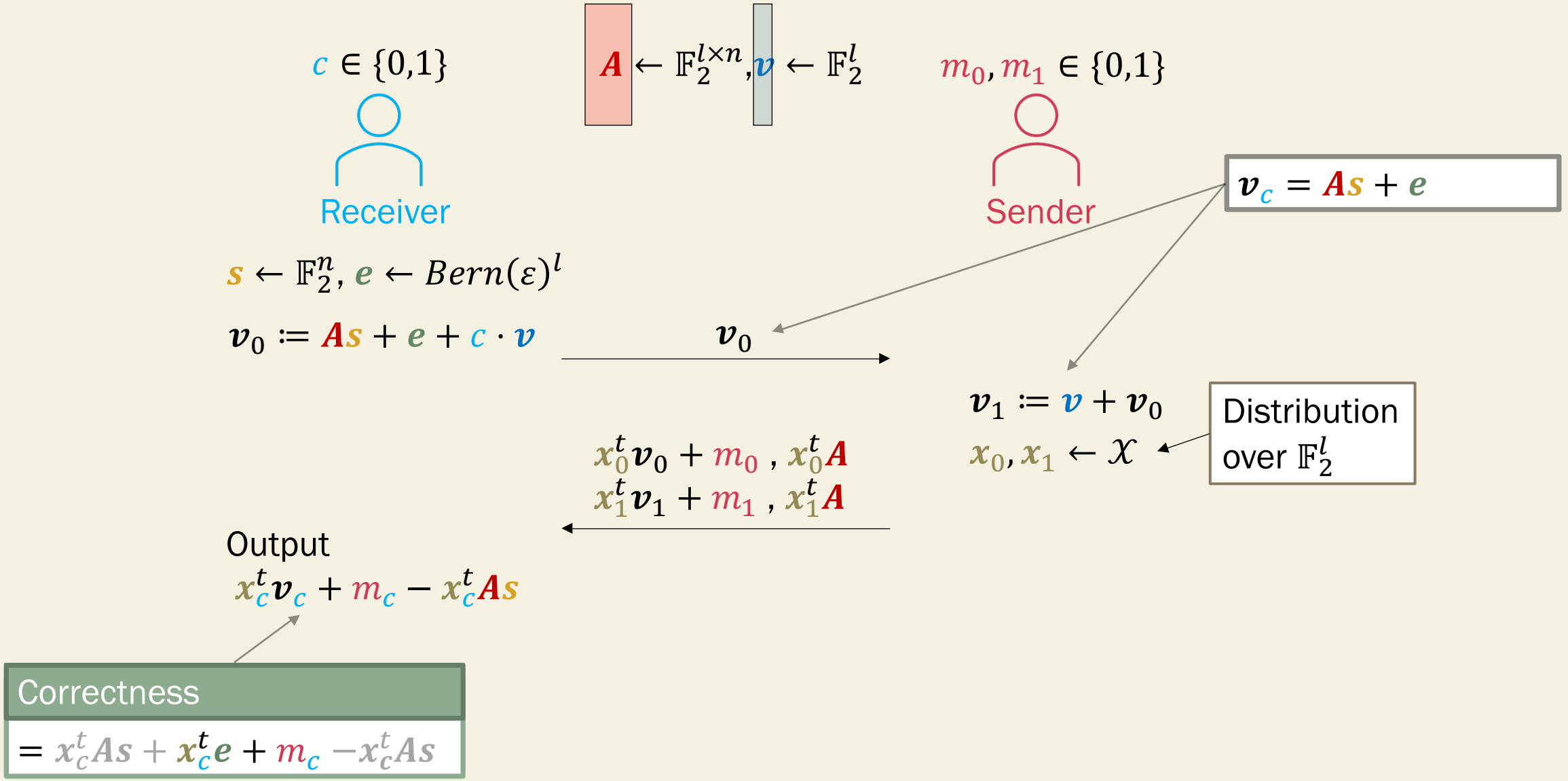
$\boldsymbol{v}_0 \coloneqq \boldsymbol{A}\boldsymbol{s} + \boldsymbol{e} + c \cdot \boldsymbol{v}$

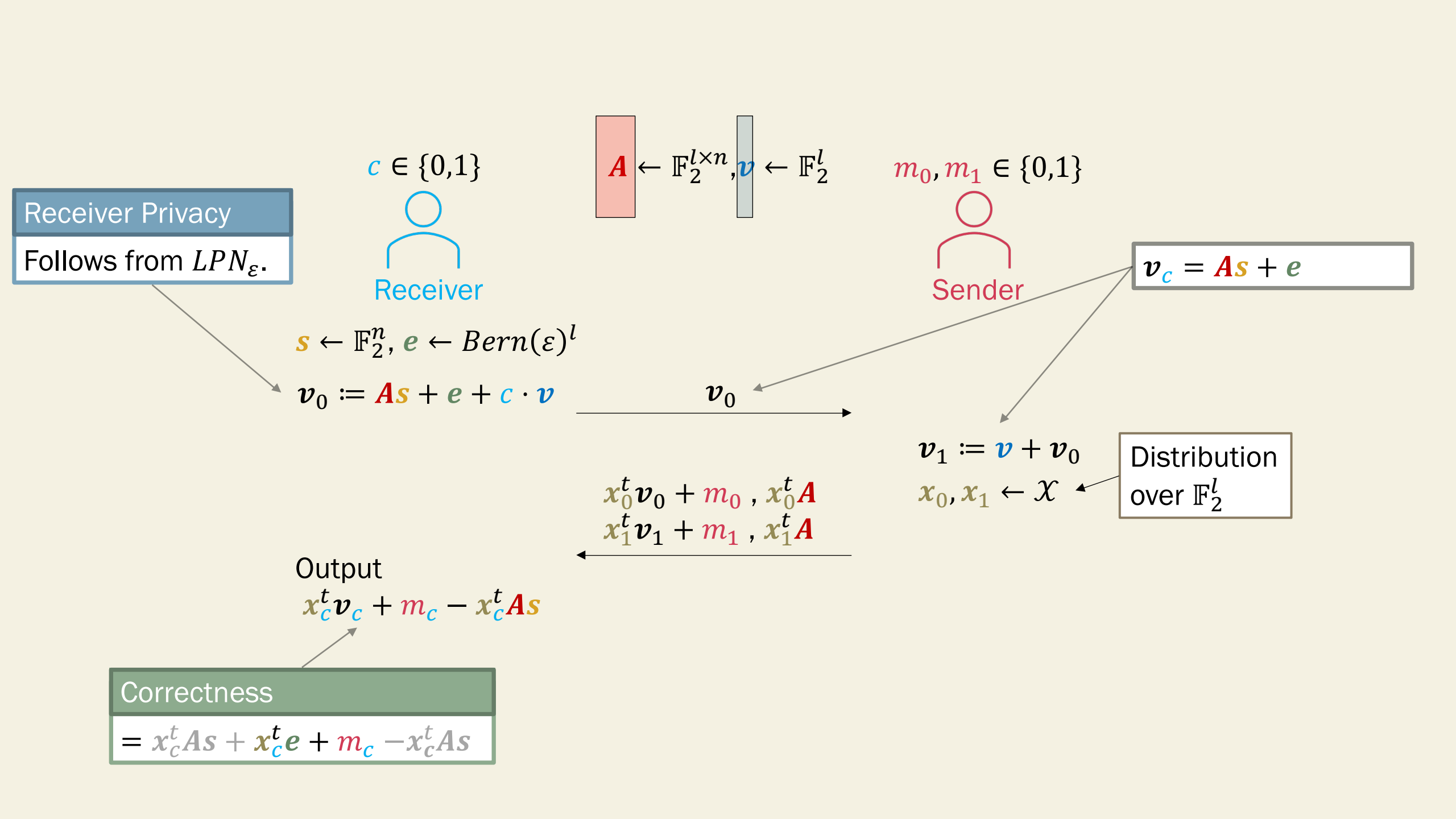
$\boldsymbol{v}_0$

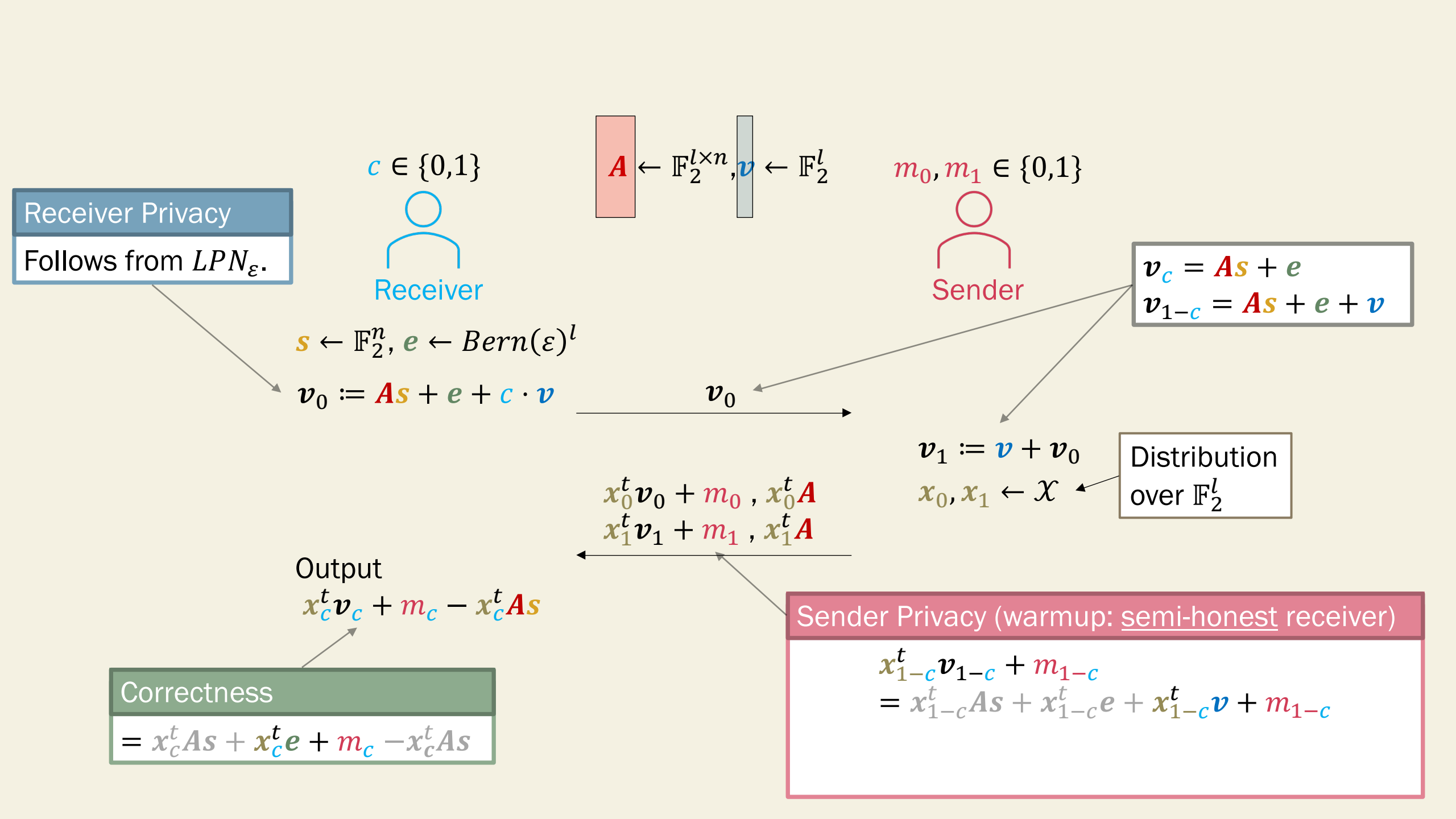
$\boldsymbol{v}_1 \coloneqq \boldsymbol{v} + \boldsymbol{v}_0$

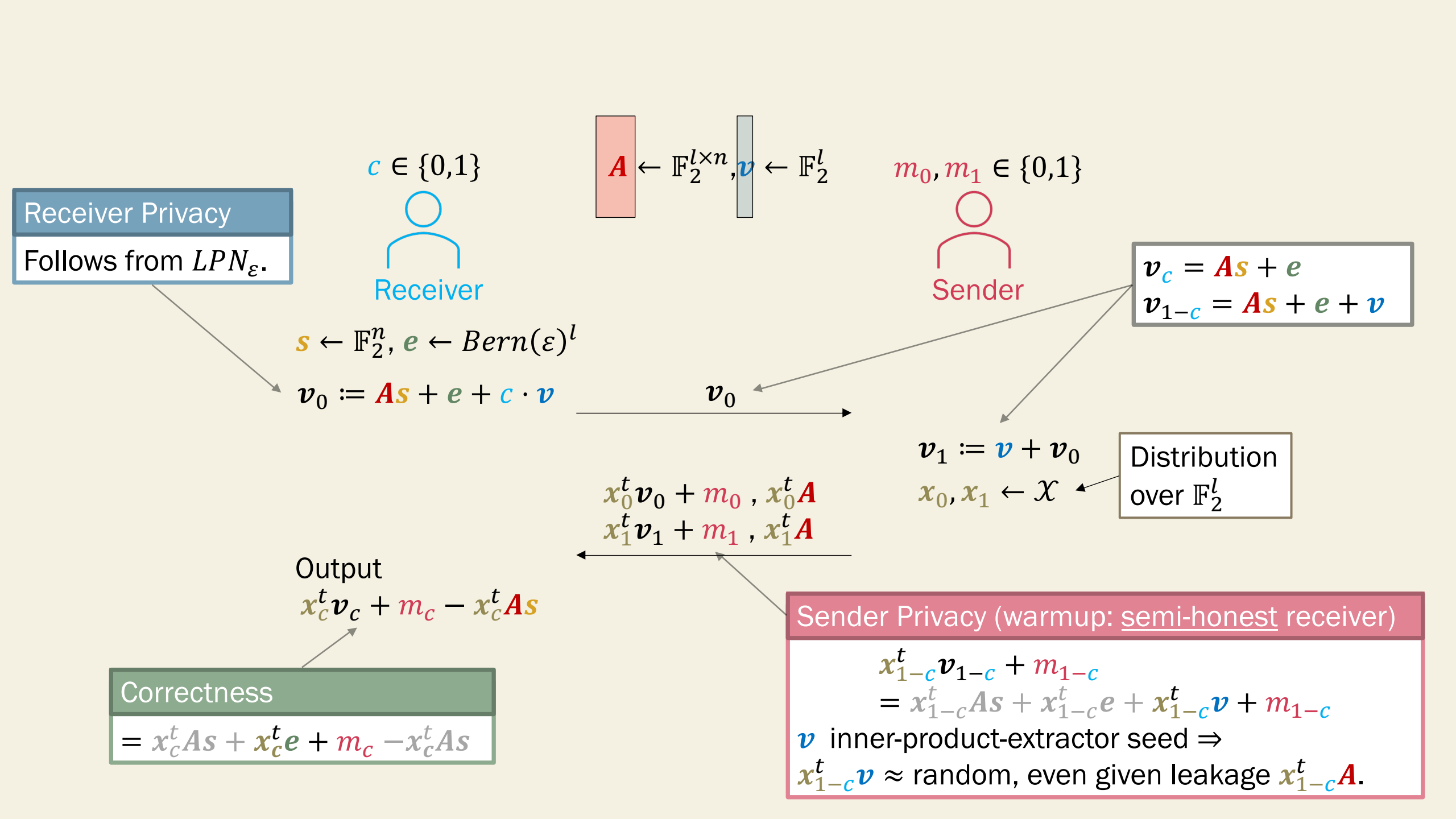

$c \in \{0,1\}$
$\boldsymbol{A} \leftarrow \mathbb{F}_2^{l \times n}, \boldsymbol{v} \leftarrow \mathbb{F}_2^{l}$
$m_0, m_1 \in \{0,1\}$
Receiver
Sender
$\boldsymbol{s} \leftarrow \mathbb{F}_2^{n}, \boldsymbol{e} \leftarrow Bern(\varepsilon)^{l}$
$\boldsymbol{v}_0 := \boldsymbol{A}\boldsymbol{s} + \boldsymbol{e} + c \cdot \boldsymbol{v}$
$\boldsymbol{v}_0$
$\boldsymbol{v}_1 := \boldsymbol{v} + \boldsymbol{v}_0$
$\boldsymbol{x}_0, \boldsymbol{x}_1 \leftarrow \mathcal{X}$
Distribution over $\mathbb{F}_2^{l}$
$\boldsymbol{x}_0^t \boldsymbol{v}_0 + m_0 \; , \; \boldsymbol{x}_0^t \boldsymbol{A}$
$\boldsymbol{x}_1^t \boldsymbol{v}_1 + m_1 \; , \; \boldsymbol{x}_1^t \boldsymbol{A}$


$c \in \{0,1\}$
$\boldsymbol{A} \leftarrow \mathbb{F}_2^{l \times n}, \boldsymbol{v} \leftarrow \mathbb{F}_2^{l}$
$m_0, m_1 \in \{0,1\}$
Receiver
Sender
$\boldsymbol{s} \leftarrow \mathbb{F}_2^{n}, \boldsymbol{e} \leftarrow Bern(\varepsilon)^{l}$
$\boldsymbol{v}_0 := \boldsymbol{A}\boldsymbol{s} + \boldsymbol{e} + c \cdot \boldsymbol{v}$
$\boldsymbol{v}_0$
$\boldsymbol{v}_1 := \boldsymbol{v} + \boldsymbol{v}_0$
$\boldsymbol{x}_0, \boldsymbol{x}_1 \leftarrow \mathcal{X}$
Distribution over $\mathbb{F}_2^{l}$
$\boldsymbol{x}_0^t \boldsymbol{v}_0 + m_0 \; , \; \boldsymbol{x}_0^t \boldsymbol{A}$
$\boldsymbol{x}_1^t \boldsymbol{v}_1 + m_1 \; , \; \boldsymbol{x}_1^t \boldsymbol{A}$
Output
$\boldsymbol{x}_c^t \boldsymbol{v}_c + m_c - \boldsymbol{x}_c^t \boldsymbol{A}\boldsymbol{s}$


$c \in \{0,1\}$
$\boldsymbol{A} \leftarrow \mathbb{F}_2^{l \times n}, \boldsymbol{v} \leftarrow \mathbb{F}_2^l$
$m_0, m_1 \in \{0,1\}$
Receiver
Sender
$\boldsymbol{v}_c = \boldsymbol{A}\boldsymbol{s} + \boldsymbol{e}$
$\boldsymbol{s} \leftarrow \mathbb{F}_2^n, \boldsymbol{e} \leftarrow Bern(\varepsilon)^l$
$\boldsymbol{v}_0 := \boldsymbol{A}\boldsymbol{s} + \boldsymbol{e} + c \cdot \boldsymbol{v}$
$\boldsymbol{v}_0$
$\boldsymbol{v}_1 := \boldsymbol{v} + \boldsymbol{v}_0$
$x_0, x_1 \leftarrow \mathcal{X}$
Distribution over $\mathbb{F}_2^l$
$x_0^t \boldsymbol{v}_0 + m_0 \; , \; x_0^t \boldsymbol{A}$
$x_1^t \boldsymbol{v}_1 + m_1 \; , \; x_1^t \boldsymbol{A}$
Output
$x_c^t \boldsymbol{v}_c + m_c - x_c^t \boldsymbol{A}\boldsymbol{s}$
Correctness
$= x_c^t \boldsymbol{A}\boldsymbol{s} + x_c^t \boldsymbol{e} + m_c - x_c^t \boldsymbol{A}\boldsymbol{s}$


$c \in \{0,1\}$
$\boldsymbol{A} \leftarrow \mathbb{F}_2^{l \times n}, \boldsymbol{v} \leftarrow \mathbb{F}_2^l$
$m_0, m_1 \in \{0,1\}$
Receiver Privacy
Follows from LPN_ε.
Receiver
Sender
$\boldsymbol{v}_c = \boldsymbol{A}\boldsymbol{s} + \boldsymbol{e}$
$\boldsymbol{s} \leftarrow \mathbb{F}_2^n, \boldsymbol{e} \leftarrow Bern(\varepsilon)^l$
$\boldsymbol{v}_0 := \boldsymbol{A}\boldsymbol{s} + \boldsymbol{e} + c \cdot \boldsymbol{v}$
$\boldsymbol{v}_0$
$\boldsymbol{v}_1 := \boldsymbol{v} + \boldsymbol{v}_0$
$\boldsymbol{x}_0, \boldsymbol{x}_1 \leftarrow \mathcal{X}$
Distribution over $\mathbb{F}_2^l$
$\boldsymbol{x}_0^t \boldsymbol{v}_0 + m_0 \; , \; \boldsymbol{x}_0^t \boldsymbol{A}$
$\boldsymbol{x}_1^t \boldsymbol{v}_1 + m_1 \; , \; \boldsymbol{x}_1^t \boldsymbol{A}$
Output
$\boldsymbol{x}_c^t \boldsymbol{v}_c + m_c - \boldsymbol{x}_c^t \boldsymbol{A}\boldsymbol{s}$
Correctness
$= \boldsymbol{x}_c^t \boldsymbol{A}\boldsymbol{s} + \boldsymbol{x}_c^t \boldsymbol{e} + m_c - \boldsymbol{x}_c^t \boldsymbol{A}\boldsymbol{s}$

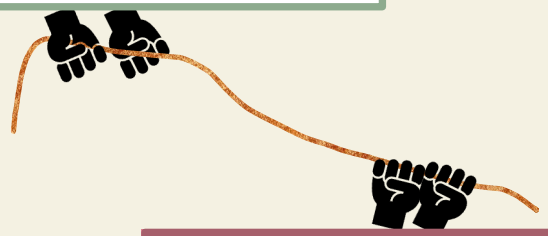

$c \in \{0,1\}$
$\boldsymbol{A} \leftarrow \mathbb{F}_2^{l \times n}, \boldsymbol{v} \leftarrow \mathbb{F}_2^l$
$m_0, m_1 \in \{0,1\}$
Receiver
Sender
Receiver Privacy
Follows from LPN_ε.
$\boldsymbol{v}_c = \boldsymbol{As} + \boldsymbol{e}$
$\boldsymbol{v}_{1-c} = \boldsymbol{As} + \boldsymbol{e} + \boldsymbol{v}$
$\boldsymbol{s} \leftarrow \mathbb{F}_2^n, \boldsymbol{e} \leftarrow Bern(\varepsilon)^l$
$\boldsymbol{v}_0 := \boldsymbol{As} + \boldsymbol{e} + c \cdot \boldsymbol{v}$
$\boldsymbol{v}_0$
$\boldsymbol{v}_1 := \boldsymbol{v} + \boldsymbol{v}_0$
$\boldsymbol{x}_0, \boldsymbol{x}_1 \leftarrow \mathcal{X}$
Distribution over $\mathbb{F}_2^l$
$\boldsymbol{x}_0^t \boldsymbol{v}_0 + m_0 , \boldsymbol{x}_0^t \boldsymbol{A}$
$\boldsymbol{x}_1^t \boldsymbol{v}_1 + m_1 , \boldsymbol{x}_1^t \boldsymbol{A}$
Output
$\boldsymbol{x}_c^t \boldsymbol{v}_c + m_c - \boldsymbol{x}_c^t \boldsymbol{As}$
Correctness
$= \boldsymbol{x}_c^t \boldsymbol{As} + \boldsymbol{x}_c^t \boldsymbol{e} + m_c - \boldsymbol{x}_c^t \boldsymbol{As}$
Sender Privacy (warmup: semi-honest receiver)
$\boldsymbol{x}_{1-c}^t \boldsymbol{v}_{1-c} + m_{1-c}$
$= \boldsymbol{x}_{1-c}^t \boldsymbol{As} + \boldsymbol{x}_{1-c}^t \boldsymbol{e} + \boldsymbol{x}_{1-c}^t \boldsymbol{v} + m_{1-c}$


$c \in \{0,1\}$
$\boldsymbol{A} \leftarrow \mathbb{F}_2^{l \times n}, \boldsymbol{v} \leftarrow \mathbb{F}_2^l$
$m_0, m_1 \in \{0,1\}$
Receiver
Sender
Receiver Privacy
Follows from LPN_ε.
$\boldsymbol{v}_c = \boldsymbol{As} + \boldsymbol{e}$
$\boldsymbol{v}_{1-c} = \boldsymbol{As} + \boldsymbol{e} + \boldsymbol{v}$
$\boldsymbol{s} \leftarrow \mathbb{F}_2^n, \boldsymbol{e} \leftarrow Bern(\varepsilon)^l$
$\boldsymbol{v}_0 := \boldsymbol{As} + \boldsymbol{e} + c \cdot \boldsymbol{v}$
$\boldsymbol{v}_0$
$\boldsymbol{v}_1 := \boldsymbol{v} + \boldsymbol{v}_0$
$x_0, x_1 \leftarrow \mathcal{X}$
Distribution over $\mathbb{F}_2^l$
$x_0^t \boldsymbol{v}_0 + m_0 \; , \; x_0^t \boldsymbol{A}$
$x_1^t \boldsymbol{v}_1 + m_1 \; , \; x_1^t \boldsymbol{A}$
Output
$x_c^t \boldsymbol{v}_c + m_c - x_c^t \boldsymbol{As}$
Correctness
$= x_c^t \boldsymbol{As} + x_c^t \boldsymbol{e} + m_c - x_c^t \boldsymbol{As}$
Sender Privacy (warmup: semi-honest receiver)
$x_{1-c}^t \boldsymbol{v}_{1-c} + m_{1-c}$
$= x_{1-c}^t \boldsymbol{As} + x_{1-c}^t \boldsymbol{e} + x_{1-c}^t \boldsymbol{v} + m_{1-c}$
$\boldsymbol{v}$ inner-product-extractor seed ⇒
$x_{1-c}^t \boldsymbol{v} \approx$ random, even given leakage $x_{1-c}^t \boldsymbol{A}$.

Tradeoff (why small noise)

Correctness

Need $\boldsymbol{x}^t \boldsymbol{e} = 0$ w.h.p.

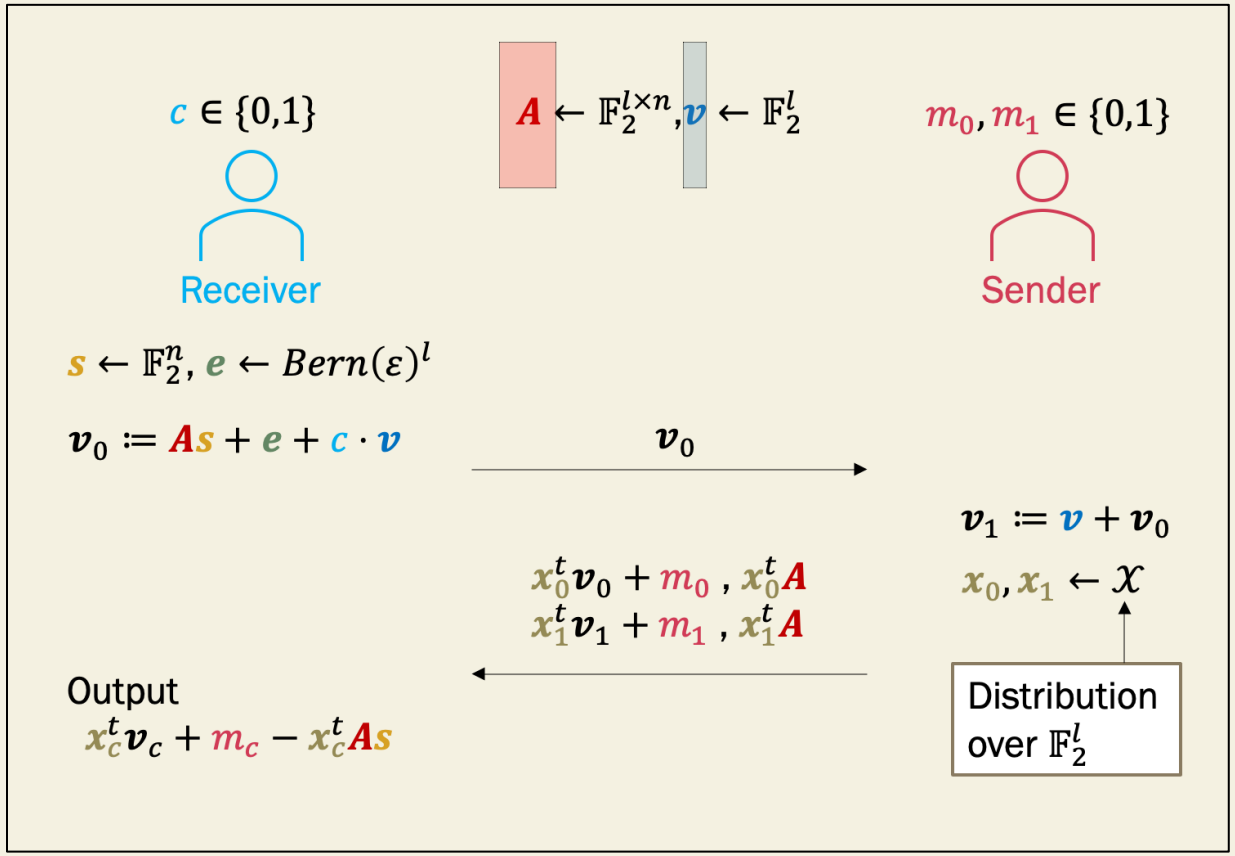


Sender Privacy

Need $\boldsymbol{x} \leftarrow \mathcal{X}$ to have **high** entropy

$$\Rightarrow \quad \varepsilon = O\left(\frac{\log^2 n}{n}\right)$$

The Challenge: Malicious Receiver

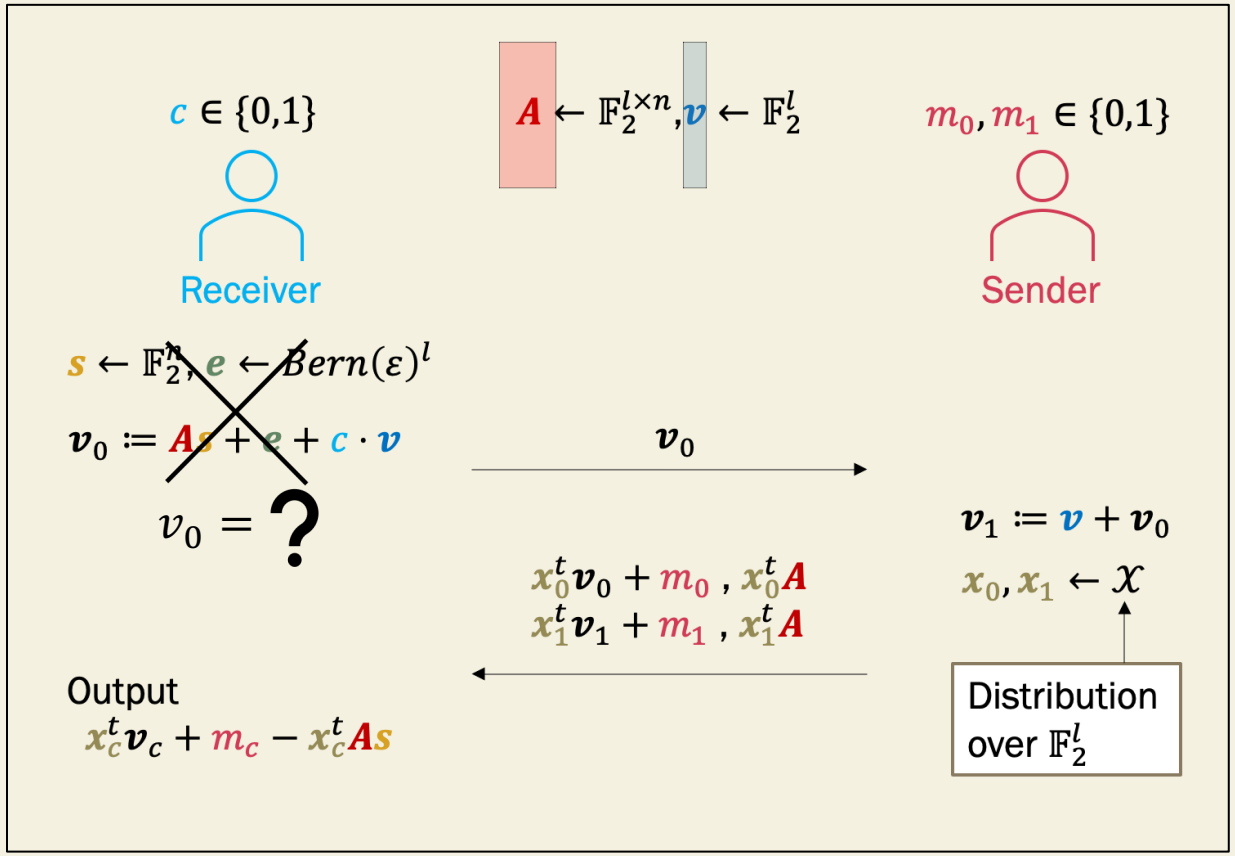


The Challenge: Malicious Receiver

Where is the challenge?

Now, receiver may choose v_0 **adaptively** depending on the seed v.

Extractor argument no longer works.



The Challenge: Malicious Receiver

Where is the challenge?

Now, receiver may choose v_0 **adaptively** depending on the seed v.

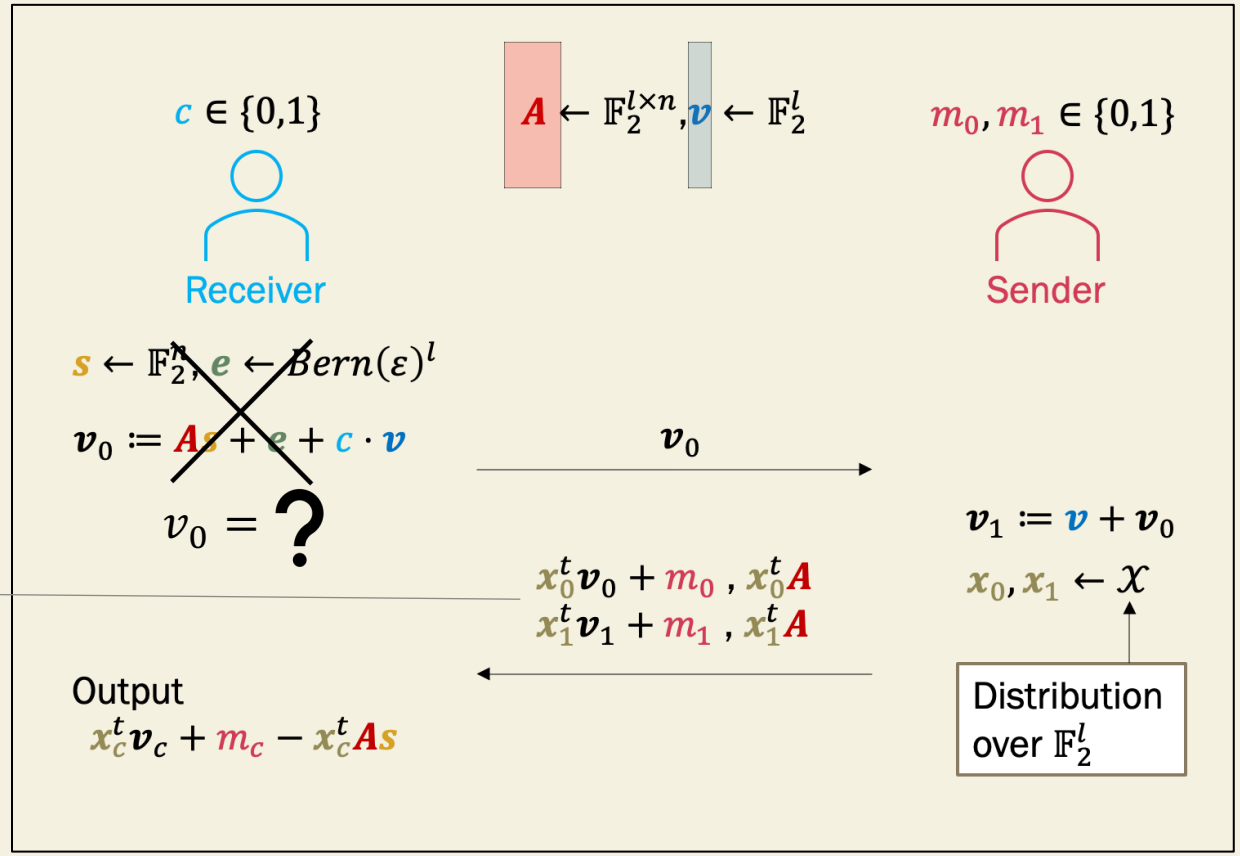
Extractor argument no longer works.

Question

Does any (adaptively) split of v to 2 seeds:

$$v = v_0 + v_1$$

contains good extractor v_i?



The Challenge: Malicious Receiver

Where is the challenge?

Now, receiver may choose v_0 **adaptively** depending on the seed v.

Extractor argument no longer works.

Question

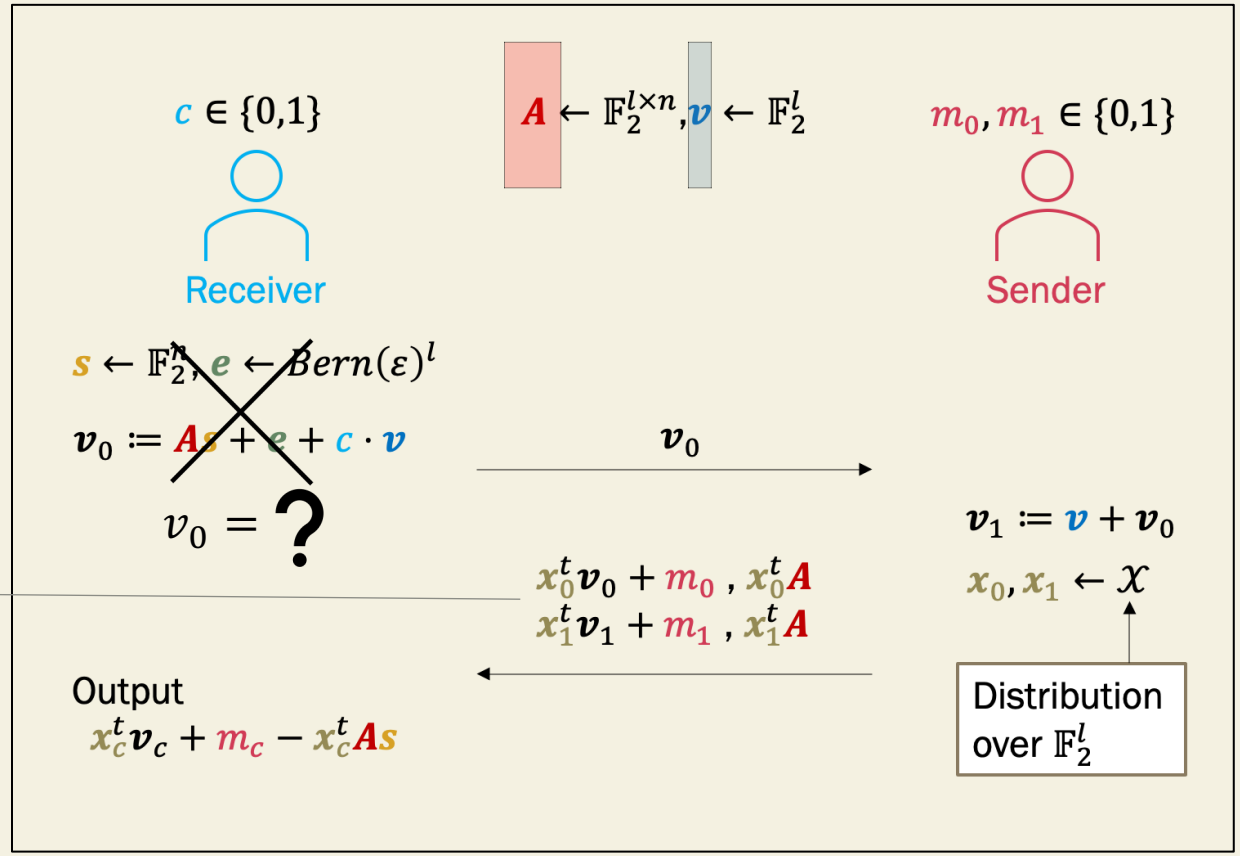
Does any (adaptively) split of v to 2 seeds:

$$v = v_0 + v_1$$

contains good extractor v_i?

Answer

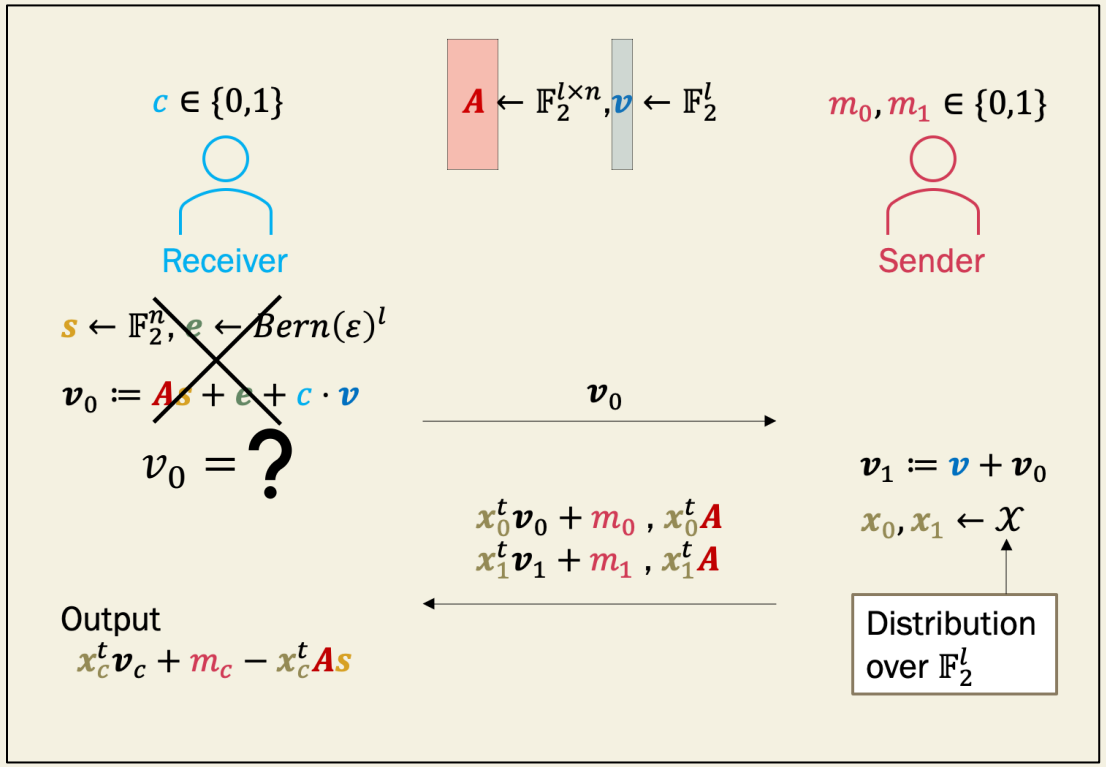
Inner-product-extractor is generally NOT resilient to such "linear splitting attacks".
(counter example in the paper)



Fortunately…

In Our Case

1. Specific leakage form: $x^t A$
2. Can choose the entropy source $\mathcal{X}$.



Fortunately…

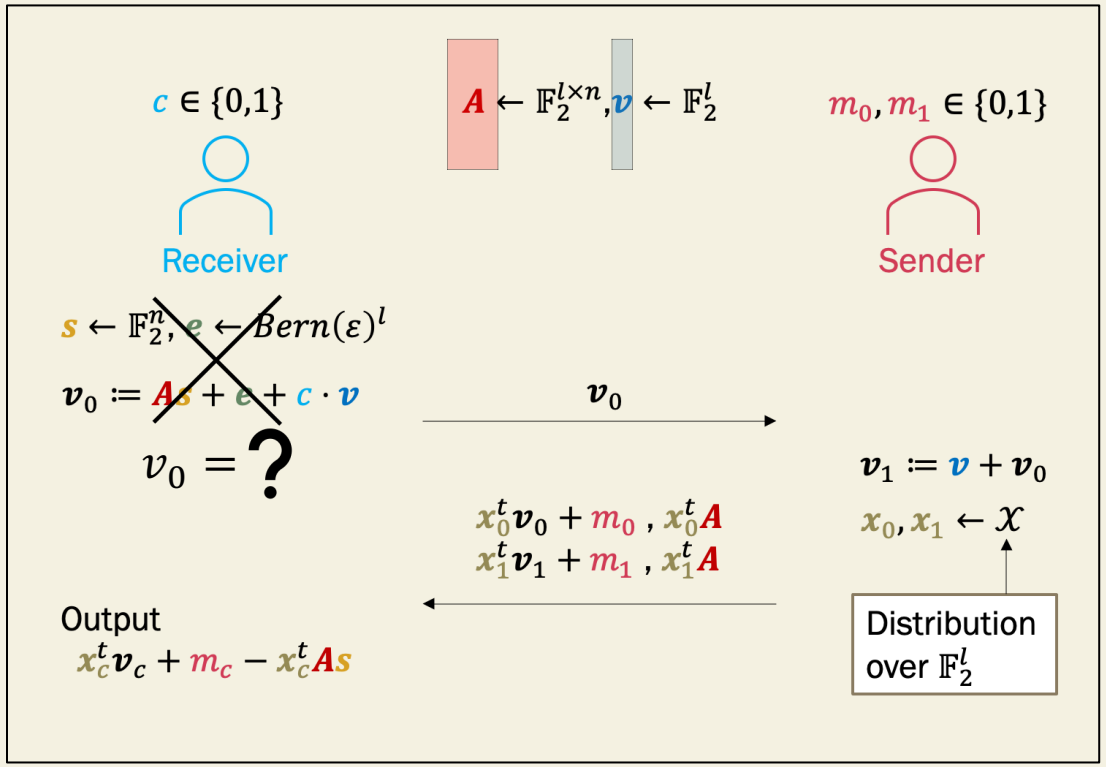
In Our Case

1. Specific leakage form: $x^t A$
2. Can choose the entropy source $\mathcal{X}$.

Choosing $\mathcal{X}$

$\mathcal{X} := \sum_{i=1}^{k} U\{e_1, \ldots, e_l\}$
The sum (over $\mathbb{F}_2$) of k random unit vectors.

- Correctness $\Rightarrow k \approx n/\log(n)$.
- $\mathcal{X}$ behaves nicely with Fourier analysis [BLVW19]



Fortunately…

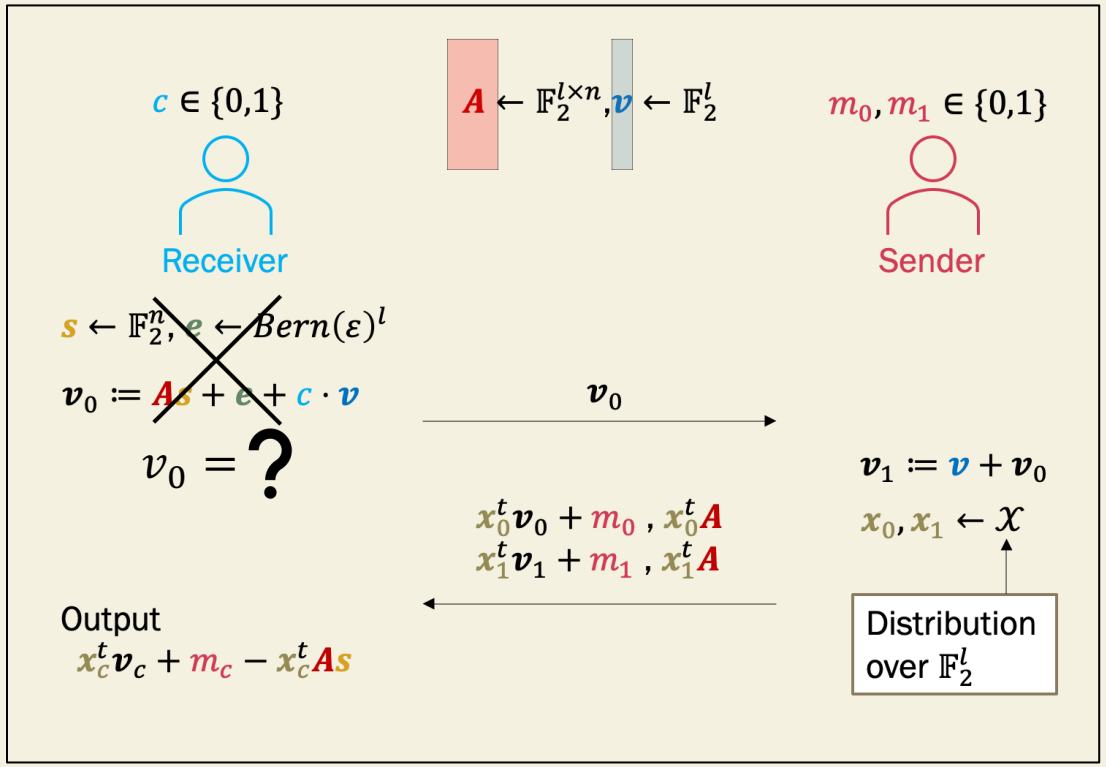
In Our Case

1. Specific leakage form: $x^t A$
2. Can choose the entropy source $\mathcal{X}$.

Choosing $\mathcal{X}$

$\mathcal{X} := \sum_{i=1}^{k} U\{e_1, \ldots, e_l\}$
The sum (over $\mathbb{F}_2$) of k random unit vectors.

- Correctness $\Rightarrow k \approx n/\log(n)$.
- $\mathcal{X}$ behaves nicely with Fourier analysis [BLVW19]



Goal

w.h.p over $(A, v) \leftarrow \mathbb{F}_2^{l\times n} \times \mathbb{F}_2^l$,

Fortunately…

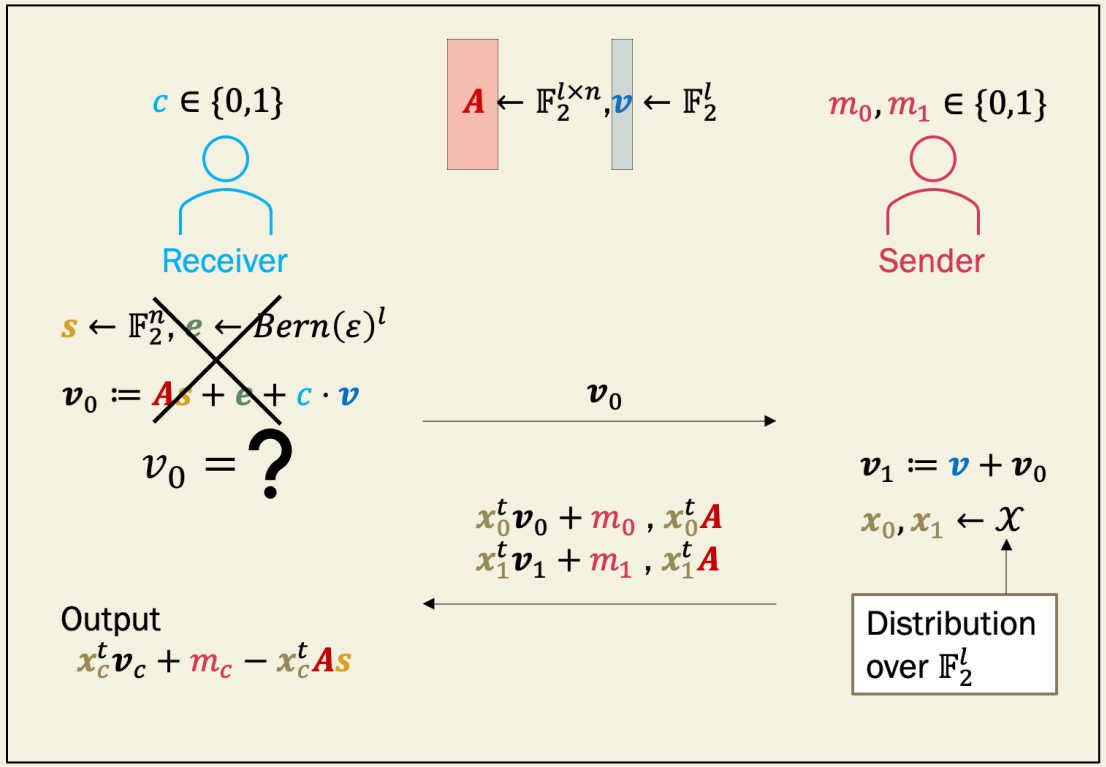
In Our Case

1. Specific leakage form: $x^t A$
2. Can choose the entropy source $\mathcal{X}$.

Choosing $\mathcal{X}$

$\mathcal{X} := \sum_{i=1}^{k} U\{e_1, \ldots, e_l\}$
The sum (over $\mathbb{F}_2$) of k random unit vectors.

- Correctness $\Rightarrow k \approx n/\log(n)$.
- $\mathcal{X}$ behaves nicely with Fourier analysis [BLVW19]



Goal

w.h.p over $(A, v) \leftarrow \mathbb{F}_2^{l \times n} \times \mathbb{F}_2^l$,
$\forall$ split $v = v_0 + v_1, \exists v_i \in \{v_0, v_1\}$:

Fortunately…

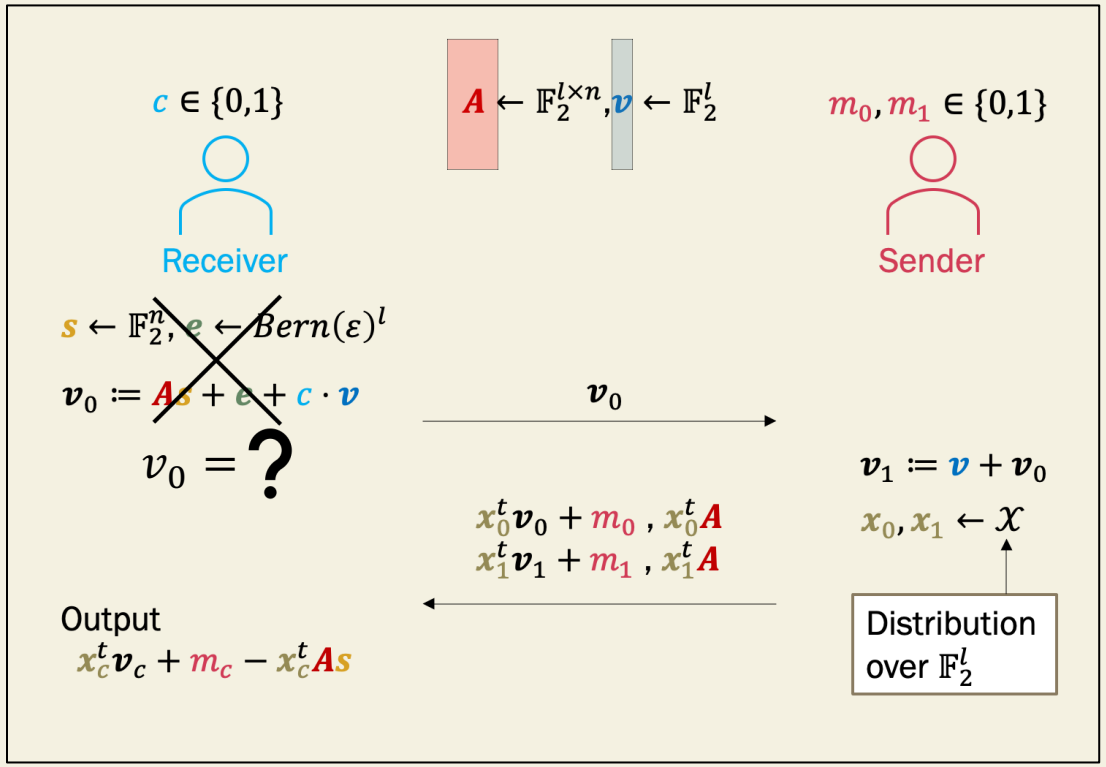
In Our Case

1. Specific leakage form: $x^t A$
2. Can choose the entropy source $\mathcal{X}$.

Choosing $\mathcal{X}$

$\mathcal{X} := \sum_{i=1}^{k} U\{e_1, \dots, e_l\}$
The sum (over $\mathbb{F}_2$) of k random unit vectors.

- Correctness $\Rightarrow k \approx n/\log(n)$.
- $\mathcal{X}$ behaves nicely with Fourier analysis [BLVW19]



Goal

w.h.p over $(A, v) \leftarrow \mathbb{F}_2^{l \times n} \times \mathbb{F}_2^l$,
$\forall$ split $v = v_0 + v_1, \exists v_i \in \{v_0, v_1\}$:

$$(x^t A, x^t v_i) \overset{s}{\approx} (x^t A, Bern(1/2))$$

$x^t v_i$ looks random, given $x^t A$

But how are we going to prove this?

Goal

w.h.p over $(\boldsymbol{A}, \boldsymbol{v}) \leftarrow \mathbb{F}_2^{l \times n} \times \mathbb{F}_2^{l}$,

$\forall$ split $\boldsymbol{v} = \boldsymbol{v}_0 + \boldsymbol{v}_1, \exists \boldsymbol{v}_i \in \{\boldsymbol{v}_0, \boldsymbol{v}_1\}$:

$$(\boldsymbol{x}^t \boldsymbol{A}, \boldsymbol{x}^t \boldsymbol{v}_i) \overset{s}{\approx} (\boldsymbol{x}^t \boldsymbol{A}, Bern(1/2))$$

$\boldsymbol{x}^t \boldsymbol{v}_i$ looks random, given $\boldsymbol{x}^t \boldsymbol{A}$

Step 1 – Relate to coset balance

$x \leftarrow \mathcal{X} := \sum^k U\{e_1, \ldots, e_l\}$

Goal (reminder)

w.h.p over $(\boldsymbol{A}, \boldsymbol{v}) \leftarrow \mathbb{F}_2^{l \times n} \times \mathbb{F}_2^l$,

$\forall$ split $\boldsymbol{v} = \boldsymbol{v}_0 + \boldsymbol{v}_1, \exists \boldsymbol{v}_i \in \{\boldsymbol{v}_0, \boldsymbol{v}_1\}$:

$$(x^t \boldsymbol{A}, x^t \boldsymbol{v}_i) \overset{s}{\approx} (x^t \boldsymbol{A}, Bern(1/2))$$

$x^t \boldsymbol{v}_i$ looks random, given $x^t \boldsymbol{A}$

Step 1 – Relate to coset balance

$x \leftarrow \mathcal{X} := \sum^k U\{e_1, \ldots, e_l\}$

Goal (reminder)

w.h.p over $(\boldsymbol{A}, \boldsymbol{v}) \leftarrow \mathbb{F}_2^{l \times n} \times \mathbb{F}_2^l$,
$\forall$ split $\boldsymbol{v} = \boldsymbol{v}_0 + \boldsymbol{v}_1, \exists \boldsymbol{v}_i \in \{\boldsymbol{v}_0, \boldsymbol{v}_1\}$:

$$(x^t \boldsymbol{A}, x^t \boldsymbol{v}_i) \overset{s}{\approx} (x^t \boldsymbol{A}, Bern(1/2))$$

$x^t \boldsymbol{v}_i$ looks random, given $x^t \boldsymbol{A}$

Lemma

$\forall \boldsymbol{A} \in \mathbb{F}_2^{l \times n}, \boldsymbol{w} \in \mathbb{F}_2^l$:

$$SD_{x \leftarrow \mathcal{X}}\left((x^t \boldsymbol{A}, x^t \boldsymbol{w}), (x^t \boldsymbol{A}, bern(1/2))\right) \leq$$

"How balanced are all vectors in coset $\boldsymbol{A} + \boldsymbol{w}$ "

(proof: Fourier analysis)

Step 1 – Relate to coset balance

$x \leftarrow \mathcal{X} := \sum^k U\{e_1, \ldots, e_l\}$

Goal (reminder)

w.h.p over $(\boldsymbol{A}, \boldsymbol{v}) \leftarrow \mathbb{F}_2^{l \times n} \times \mathbb{F}_2^l$,
$\forall$ split $\boldsymbol{v} = \boldsymbol{v}_0 + \boldsymbol{v}_1, \exists \boldsymbol{v}_i \in \{\boldsymbol{v}_0, \boldsymbol{v}_1\}$:

$$(x^t \boldsymbol{A}, x^t \boldsymbol{v}_i) \overset{s}{\approx} (x^t \boldsymbol{A}, Bern(1/2))$$

$x^t \boldsymbol{v}_i$ looks random, given $x^t \boldsymbol{A}$

Lemma

$\forall \boldsymbol{A} \in \mathbb{F}_2^{l \times n}, \boldsymbol{w} \in \mathbb{F}_2^l$:

$$SD_{x \leftarrow \mathcal{X}}\left((x^t \boldsymbol{A}, x^t \boldsymbol{w}), (x^t \boldsymbol{A}, bern(1/2))\right) \leq$$

"How balanced are all vectors in coset $\boldsymbol{A} + \boldsymbol{w}$ "

Formally:

$$\sum_{\boldsymbol{s} \in \mathbb{F}_2^n} |\beta_{\boldsymbol{A}\boldsymbol{s}+\boldsymbol{w}}|^k$$

(proof: Fourier analysis)

Balance parameter

$$(\beta_{\boldsymbol{u}} + 1)\frac{len(\boldsymbol{u})}{2} := weight(\boldsymbol{u})$$

Step 1 – Relate to coset balance

$x \leftarrow \mathcal{X} := \sum^k U\{e_1, \ldots, e_l\}$

Goal (reminder)

w.h.p over $(\boldsymbol{A}, \boldsymbol{v}) \leftarrow \mathbb{F}_2^{l \times n} \times \mathbb{F}_2^l$,
$\forall$ split $\boldsymbol{v} = \boldsymbol{v}_0 + \boldsymbol{v}_1, \exists \boldsymbol{v}_i \in \{\boldsymbol{v}_0, \boldsymbol{v}_1\}$:

$$(x^t \boldsymbol{A}, x^t \boldsymbol{v}_i) \overset{s}{\approx} (x^t \boldsymbol{A}, Bern(1/2))$$

$x^t \boldsymbol{v}_i$ looks random, given $x^t \boldsymbol{A}$

Lemma

$\forall \boldsymbol{A} \in \mathbb{F}_2^{l \times n}, \boldsymbol{w} \in \mathbb{F}_2^l$:

$$SD_{x \leftarrow \mathcal{X}}\left((x^t \boldsymbol{A}, x^t \boldsymbol{w}), (x^t \boldsymbol{A}, bern(1/2))\right) \leq$$

"How balanced are all vectors in coset $\boldsymbol{A} + \boldsymbol{w}$ "

Formally:

$$\sum_{\boldsymbol{s} \in \mathbb{F}_2^n} |\beta_{\boldsymbol{A}\boldsymbol{s}+\boldsymbol{w}}|^k$$

(proof: Fourier analysis)

Balance parameter

$$(\beta_{\boldsymbol{u}} + 1)\frac{len(\boldsymbol{u})}{2} := weight(\boldsymbol{u})$$

$x^t \boldsymbol{w}$ predictable, given $x^t \boldsymbol{A}$?

Step 1 – Relate to coset balance

$x \leftarrow \mathcal{X} := \sum^k U\{e_1, \ldots, e_l\}$

Goal (reminder)

w.h.p over $(\boldsymbol{A}, \boldsymbol{v}) \leftarrow \mathbb{F}_2^{l \times n} \times \mathbb{F}_2^l$,
$\forall$ split $\boldsymbol{v} = \boldsymbol{v}_0 + \boldsymbol{v}_1, \exists \boldsymbol{v}_i \in \{\boldsymbol{v}_0, \boldsymbol{v}_1\}$:

$$(x^t \boldsymbol{A}, x^t \boldsymbol{v}_i) \overset{s}{\approx} (x^t \boldsymbol{A}, Bern(1/2))$$

$x^t \boldsymbol{v}_i$ looks random, given $x^t \boldsymbol{A}$

Lemma

$\forall \boldsymbol{A} \in \mathbb{F}_2^{l \times n}, \boldsymbol{w} \in \mathbb{F}_2^l$:

$$SD_{x \leftarrow \mathcal{X}}\left((x^t \boldsymbol{A}, x^t \boldsymbol{w}), (x^t \boldsymbol{A}, bern(1/2))\right) \leq$$

"How balanced are all vectors in coset $\boldsymbol{A} + \boldsymbol{w}$ "

Formally:

$$\sum_{\boldsymbol{s} \in \mathbb{F}_2^n} |\beta_{\boldsymbol{A}\boldsymbol{s}+\boldsymbol{w}}|^k$$

(proof: Fourier analysis)

Balance parameter

$$(\beta_{\boldsymbol{u}} + 1)\frac{len(\boldsymbol{u})}{2} := weight(\boldsymbol{u})$$

small $\boldsymbol{e}^*$

$x^t \boldsymbol{w}$ predictable, given $x^t \boldsymbol{A}$?
$\exists$ small vector: $\boldsymbol{A}\boldsymbol{s}^* + \boldsymbol{w} = \boldsymbol{e}^* \quad \Rightarrow x^t \boldsymbol{w} \approx x^t \boldsymbol{A}\boldsymbol{s}^*$

Step 1 – Relate to coset balance

$x \leftarrow \mathcal{X} := \sum^k U\{e_1, \ldots, e_l\}$

Goal (reminder)

w.h.p over $(\boldsymbol{A}, \boldsymbol{v}) \leftarrow \mathbb{F}_2^{l \times n} \times \mathbb{F}_2^l$,
$\forall$ split $\boldsymbol{v} = \boldsymbol{v}_0 + \boldsymbol{v}_1, \exists \boldsymbol{v}_i \in \{\boldsymbol{v}_0, \boldsymbol{v}_1\}$:

$$(x^t \boldsymbol{A}, x^t \boldsymbol{v}_i) \overset{s}{\approx} (x^t \boldsymbol{A}, Bern(1/2))$$

$x^t \boldsymbol{v}_i$ looks random, given $x^t \boldsymbol{A}$

Lemma

$\forall \boldsymbol{A} \in \mathbb{F}_2^{l \times n}, \boldsymbol{w} \in \mathbb{F}_2^l$:

$$SD_{x \leftarrow \mathcal{X}}\left((x^t \boldsymbol{A}, x^t \boldsymbol{w}), (x^t \boldsymbol{A}, bern(1/2))\right) \leq$$

"How balanced are all vectors in coset $\boldsymbol{A} + \boldsymbol{w}$ "

Formally: $\sum_{\boldsymbol{s} \in \mathbb{F}_2^n} |\beta_{\boldsymbol{A}\boldsymbol{s}+\boldsymbol{w}}|^k$

(proof: Fourier analysis)

Balance parameter $(\beta_{\boldsymbol{u}} + 1)\frac{len(\boldsymbol{u})}{2} := weight(\boldsymbol{u})$

small $\boldsymbol{e}^*$

$x^t \boldsymbol{w}$ predictable, given $x^t \boldsymbol{A}$?

$\exists$ small vector: $\boldsymbol{A}\boldsymbol{s}^* + \boldsymbol{w} = \boldsymbol{e}^* \quad \Rightarrow x^t \boldsymbol{w} \approx x^t \boldsymbol{A}\boldsymbol{s}^*$

$\exists$ large vector: $\boldsymbol{A}\boldsymbol{s}^* + \boldsymbol{w} = \boldsymbol{e}^* + \vec{\boldsymbol{1}} \quad \Rightarrow x^t \boldsymbol{w} \approx x^t \boldsymbol{A}\boldsymbol{s}^* + k \bmod 2$

$x^t \vec{\boldsymbol{1}} \equiv k \bmod 2$

Step 2 – one of the cosets is balanced

Goal (reminder)

w.h.p over $(\boldsymbol{A}, \boldsymbol{v}) \leftarrow \mathbb{F}_2^{l \times n} \times \mathbb{F}_2^{l}$,

$\forall$ split $\boldsymbol{v} = \boldsymbol{v}_0 + \boldsymbol{v}_1, \exists \boldsymbol{v}_i \in \{\boldsymbol{v}_0, \boldsymbol{v}_1\}$:

"All vectors in coset $\boldsymbol{A} + \boldsymbol{v}_i$ are balanced"

Formally:

$$\sum_{\boldsymbol{s} \in \mathbb{F}_2^n} |\beta_{\boldsymbol{A}\boldsymbol{s}+\boldsymbol{w}}|^k = neg(n)$$

Balance parameter

$$(\beta_{\boldsymbol{u}} + 1)\frac{len(\boldsymbol{u})}{2} \coloneqq weight(\boldsymbol{u})$$

Step 2 – one of the cosets is balanced

Goal (reminder)

w.h.p over $(\boldsymbol{A}, \boldsymbol{v}) \leftarrow \mathbb{F}_2^{l \times n} \times \mathbb{F}_2^{l}$,
$\forall$ split $\boldsymbol{v} = \boldsymbol{v}_0 + \boldsymbol{v}_1, \exists \boldsymbol{v}_i \in \{\boldsymbol{v}_0, \boldsymbol{v}_1\}$:

"All vectors in coset $\boldsymbol{A} + \boldsymbol{v}_i$ are balanced"

Formally:

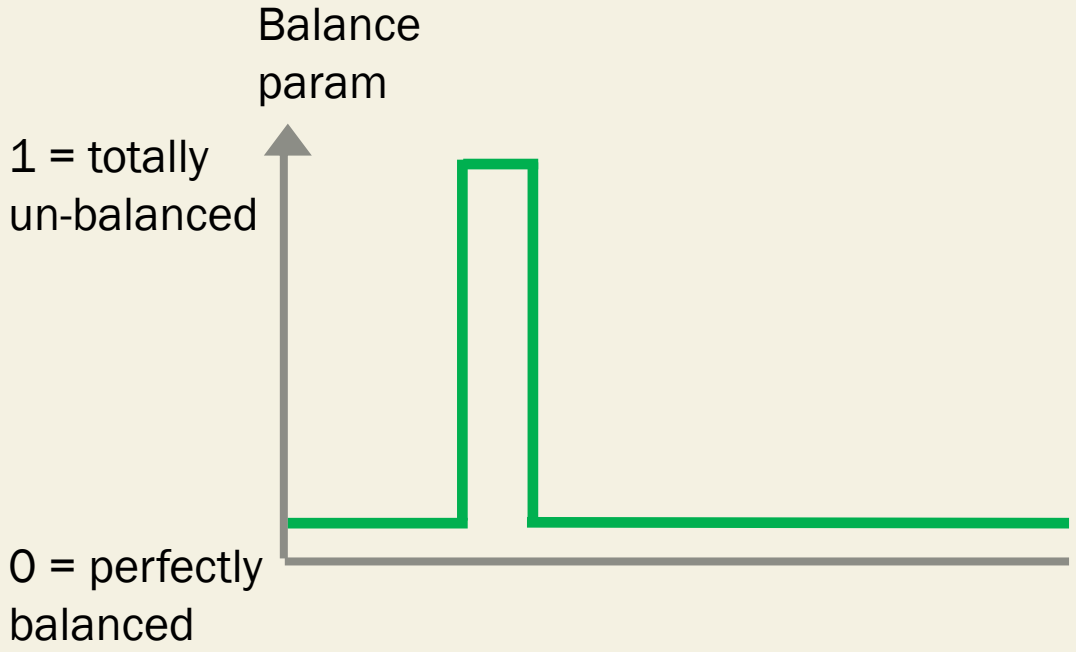
$$\sum_{\boldsymbol{s} \in \mathbb{F}_2^n} |\beta_{\boldsymbol{A}\boldsymbol{s}+\boldsymbol{w}}|^k = neg(n)$$

Balance parameter

$$(\beta_{\boldsymbol{u}} + 1)\frac{len(\boldsymbol{u})}{2} \coloneqq weight(\boldsymbol{u})$$

w.h.p $\boldsymbol{A}$ is affinely-balanced

For any $\boldsymbol{w} \in \mathbb{F}_2^l$, in the coset $\boldsymbol{A} + \boldsymbol{w}$ most members are well balanced.



Step 2 – one of the cosets is balanced

Goal (reminder)

w.h.p over $(\boldsymbol{A}, \boldsymbol{v}) \leftarrow \mathbb{F}_2^{l \times n} \times \mathbb{F}_2^{l}$,
$\forall$ split $\boldsymbol{v} = \boldsymbol{v}_0 + \boldsymbol{v}_1, \exists \boldsymbol{v}_i \in \{\boldsymbol{v}_0, \boldsymbol{v}_1\}$:

"All vectors in coset $\boldsymbol{A} + \boldsymbol{v}_i$ are balanced"

Formally:

$$\sum_{\boldsymbol{s} \in \mathbb{F}_2^n} |\beta_{\boldsymbol{A}\boldsymbol{s}+\boldsymbol{w}}|^k = neg(n)$$

Balance parameter

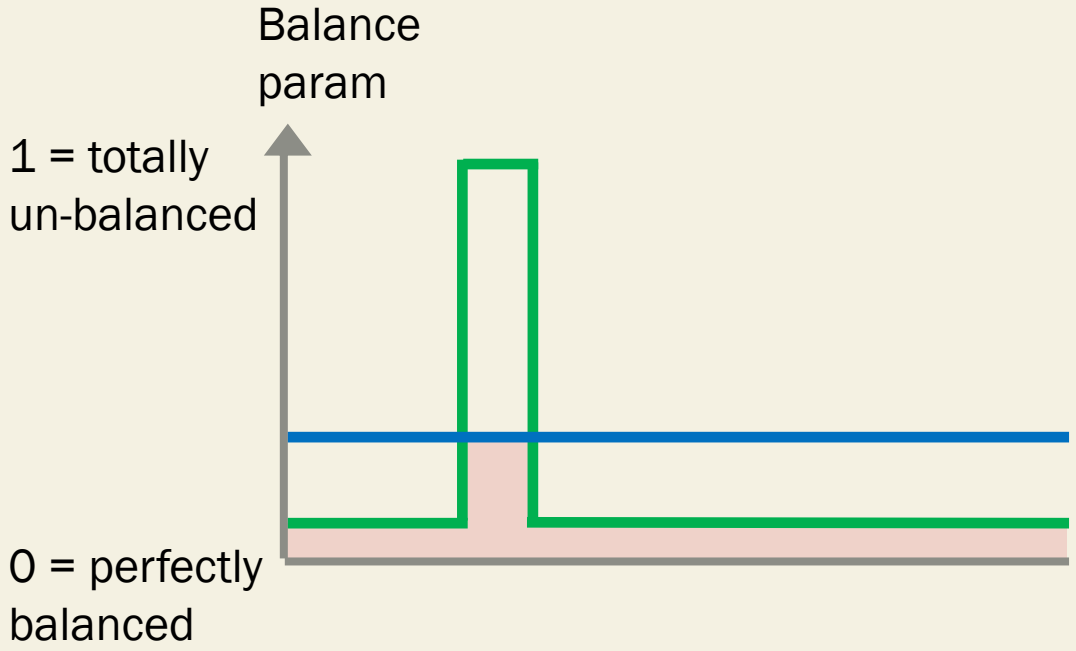
$$(\beta_{\boldsymbol{u}} + 1)\frac{len(\boldsymbol{u})}{2} \coloneqq weight(\boldsymbol{u})$$

w.h.p $\boldsymbol{A}$ is affinely-balanced

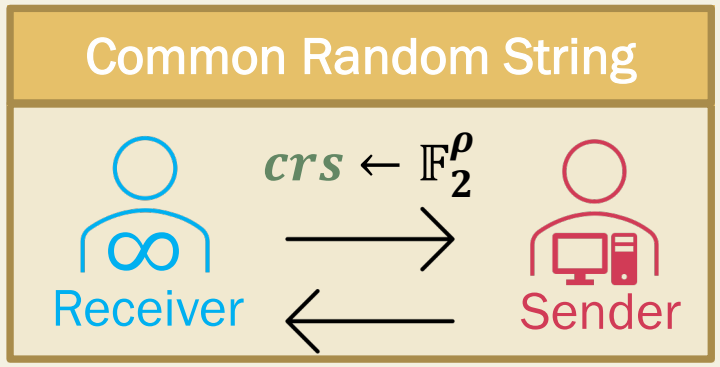
For any $\boldsymbol{w} \in \mathbb{F}_2^{l}$, in the coset $\boldsymbol{A} + \boldsymbol{w}$ most members are well balanced.

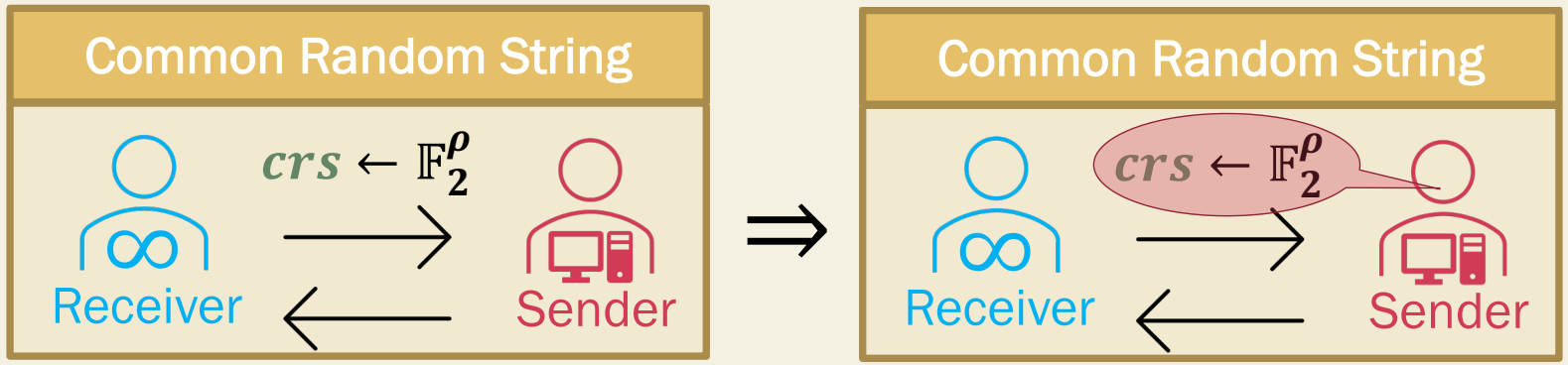
w.h.p $\boldsymbol{v}$ is $\boldsymbol{A}$-balanced for sums

$\forall \boldsymbol{v} = \boldsymbol{v}_0 + \boldsymbol{v}_1, \exists \boldsymbol{v}_i \in \{\boldsymbol{v}_0, \boldsymbol{v}_1\}$ s.t. in the coset $\boldsymbol{A} + \boldsymbol{v}_i$ all members are somewhat balanced.

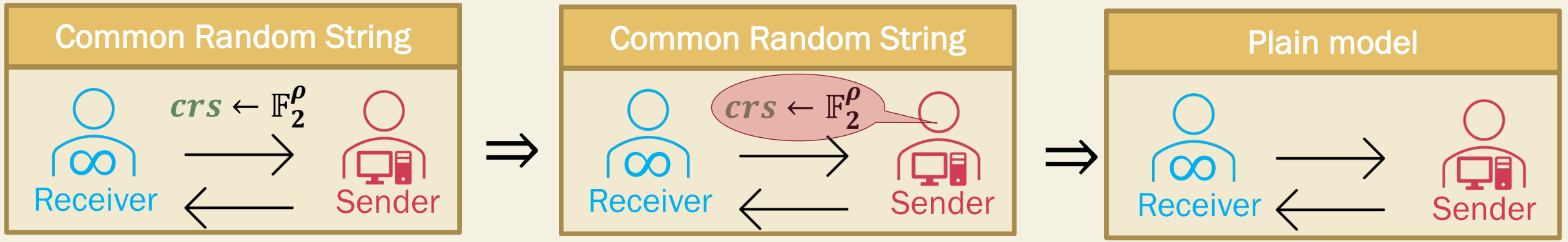


Now, let's remove the crs...


Common Random String
$crs \leftarrow \mathbb{F}_2^{\rho}$
Receiver
Sender

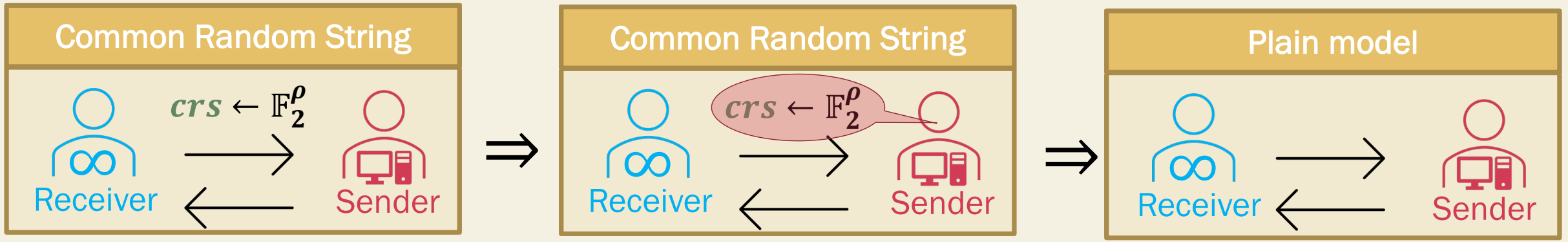


1. Reverse - randomization [Dwork-Naor: NIZK to ZAP 00].
   ⇒ Receiver security holds $\forall crs$



1. Reverse - randomization [Dwork-Naor: NIZK to ZAP 00].
   ⇒ Receiver security holds ∀crs

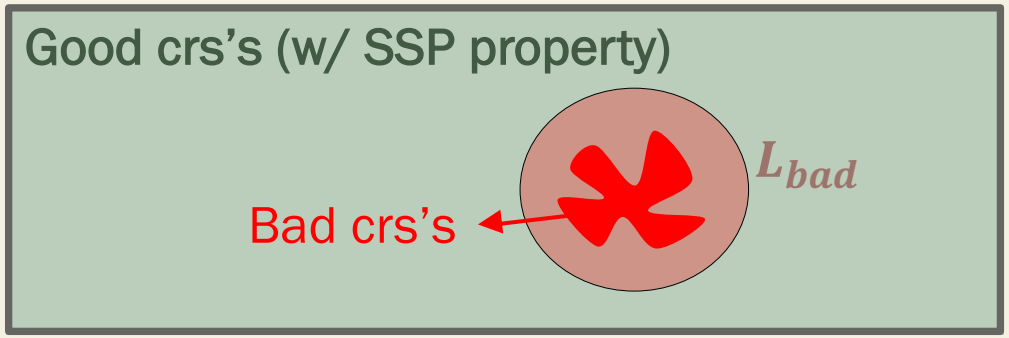
2. Derandomize crs [Barak-Ong-Vadhan Zaps 07].
   NW style worst-case assumption ⇒ ∃PRG that "fools" non-deterministic distinguishers



1. Reverse - randomization [Dwork-Naor: NIZK to ZAP 00].
   ⇒ Receiver security holds ∀crs

2. Derandomize crs [Barak-Ong-Vadhan Zaps 07].
   NW style worst-case assumption ⇒ ∃PRG that "fools" non-deterministic distinguishers

Challenge: need an algebraic characterization that capture bad crs's



Open Questions:

1. Can we achieve SSP-OT from LPN with better noise?

2. How expressive is LPN in the $n^{-\varepsilon}$ noise regime? (CRH, hardness in SZK, …)

3. How far can we push LPN (PIR, HE, ABE,…)?

Open Questions:

1. Can we achieve SSP-OT from LPN with better noise?

2. How expressive is LPN in the $n^{-\varepsilon}$ noise regime? (CRH, hardness in SZK, …)

3. How far can we push LPN (PIR, HE, ABE,…)?

Thanks!

eprint.iacr.org/2022/185