Secure Computation with Constant Communication Overhead using Multiplication Embeddings

Alexander R. Block[1], Hemanta K. Maji[1], **Hai H. Nguyen**[1]

[1]Purdue University, {block9,hmaji,nguye245}@purdue.edu

Multiplication Embedding Problem

$\mathbf{a} \in \mathbb{F}^m$ $\mathbf{b} \in \mathbb{F}^m$

Multiplication Embedding Problem

$$\mathbf{a} \in \mathbb{F}^m \xrightarrow{\mathsf{Enc}} A \in \mathbb{K} \qquad B \in \mathbb{K} \xleftarrow{\mathsf{Enc}} \mathbf{b} \in \mathbb{F}^m$$

$\mathbb{K}$ is the degree-n extension field of some finite field $\mathbb{F}$

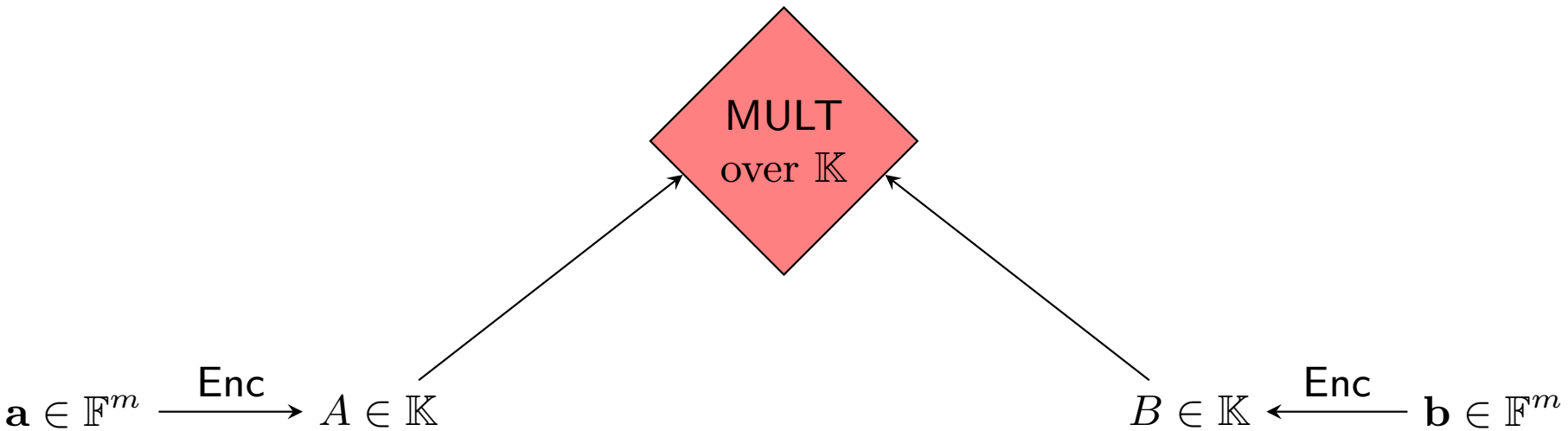
Multiplication Embedding Problem

$\mathbf{a} \in \mathbb{F}^m \xrightarrow{\mathsf{Enc}} A \in \mathbb{K}$

$B \in \mathbb{K} \xleftarrow{\mathsf{Enc}} \mathbf{b} \in \mathbb{F}^m$

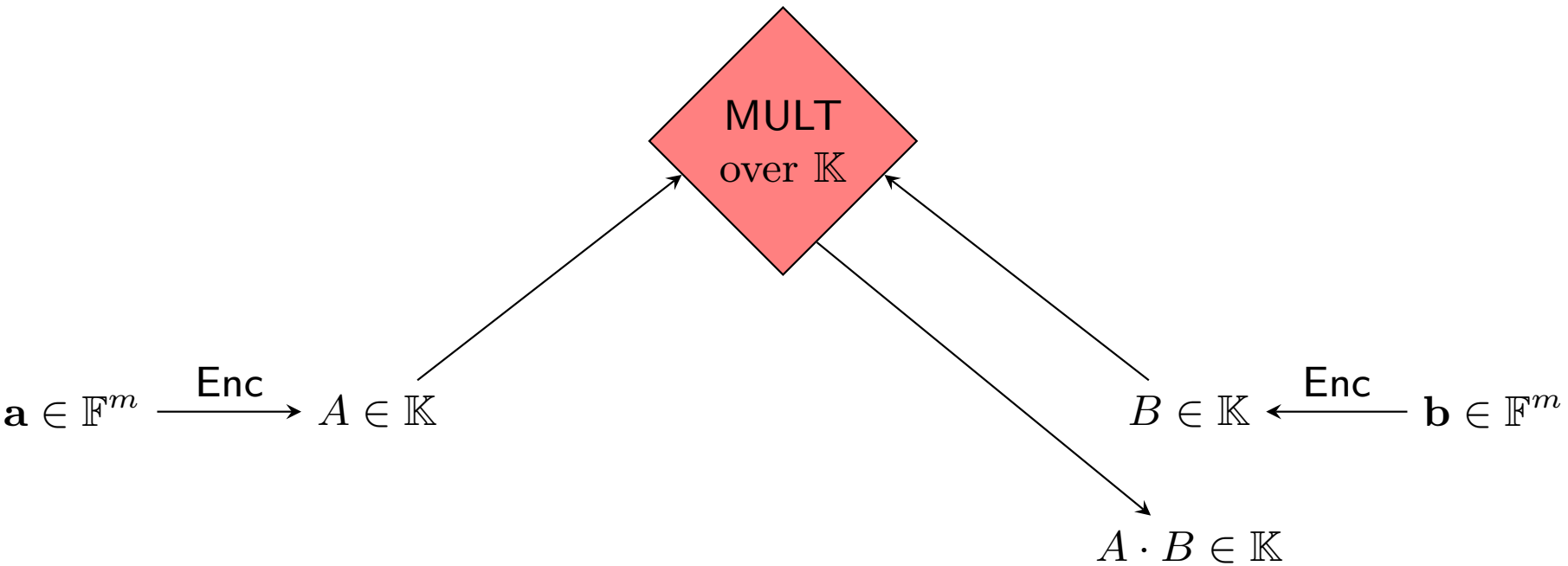
$\mathbb{K}$ is the degree-n extension field of some finite field $\mathbb{F}$

Multiplication Embedding Problem



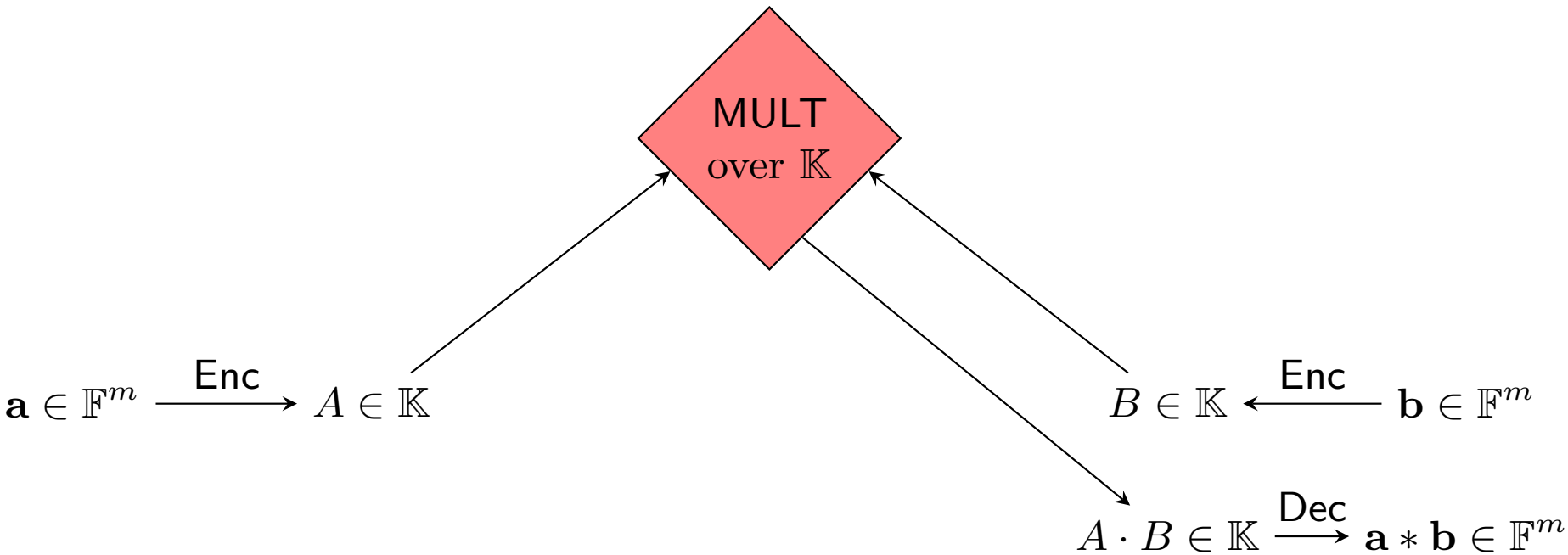
$\mathbb{K}$ is the degree-n extension field of some finite field $\mathbb{F}$

Multiplication Embedding Problem



$\mathbb{K}$ is the degree-n extension field of some finite field $\mathbb{F}$

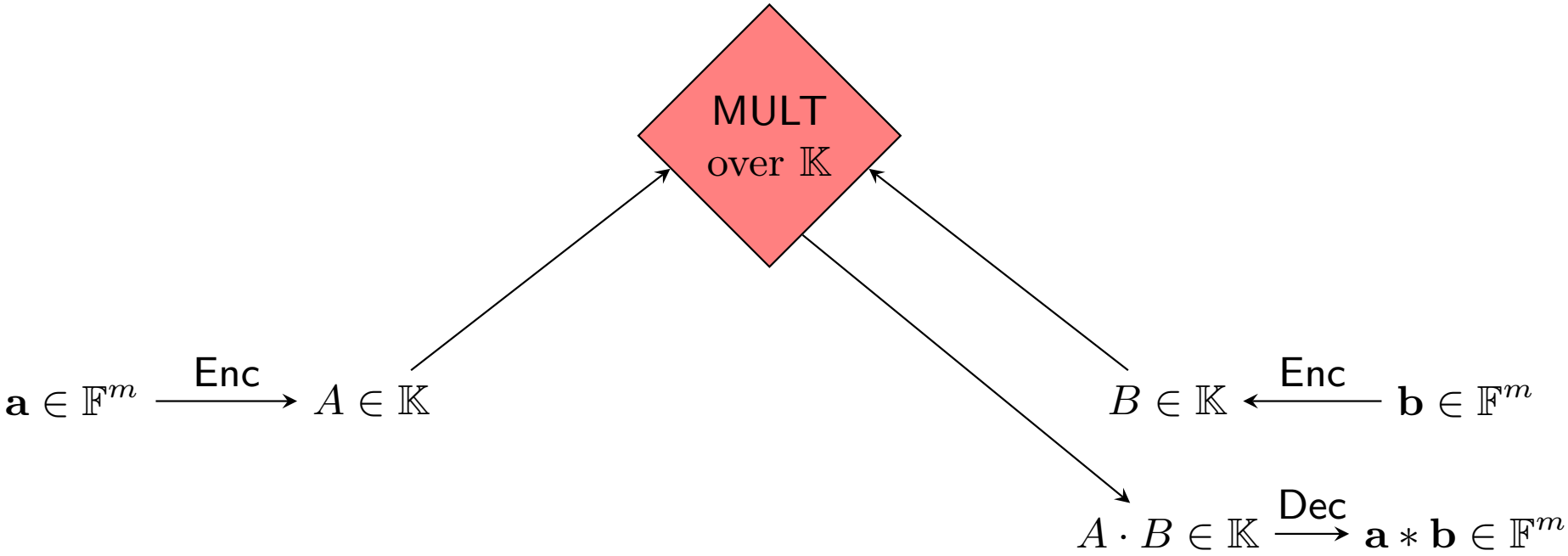
Multiplication Embedding Problem



$\mathbb{K}$ is the degree-n extension field of some finite field $\mathbb{F}$

The operator $*$ is coordinate-wise multiplication of the vectors $\mathbf{a}, \mathbf{b} \in \mathbb{F}^m$
For example $(a_1, \ldots, a_m) * (b_1, \ldots, b_m) = (a_1 b_1, \ldots, a_m b_m)$

Multiplication Embedding Problem



$\mathbb{K}$ is the degree-n extension field of some finite field $\mathbb{F}$

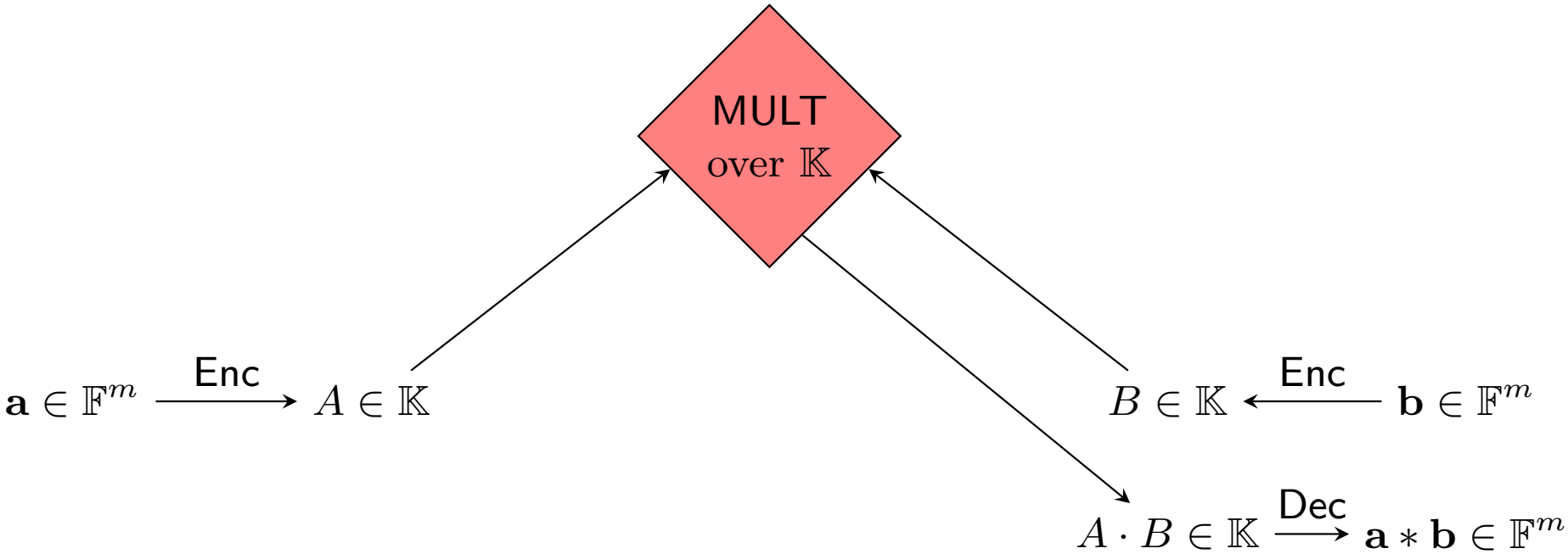
The operator $*$ is coordinate-wise multiplication of the vectors $\mathbf{a}, \mathbf{b} \in \mathbb{F}^m$
For example $(a_1, \ldots, a_m) * (b_1, \ldots, b_m) = (a_1 b_1, \ldots, a_m b_m)$

Question

Given n and a field $\mathbb{F}$, find the largest m such that there exist two mappings $\mathsf{Enc} : \mathbb{F}^m \to \mathbb{K}$ and $\mathsf{Dec} : \mathbb{K} \to \mathbb{F}^m$ and

$$\forall\, \mathbf{a}, \mathbf{b} \in \mathbb{F}^m \text{ we have } \mathsf{Dec}(\mathsf{Enc}(\mathbf{a}) \cdot \mathsf{Enc}(\mathbf{b})) = \mathbf{a} * \mathbf{b}$$

Multiplication Embedding Problem



$\mathbb{K}$ is the degree-n extension field of some finite field $\mathbb{F}$

The operator $*$ is coordinate-wise multiplication of the vectors $\mathbf{a}, \mathbf{b} \in \mathbb{F}^m$
For example $(a_1, \ldots, a_m) * (b_1, \ldots, b_m) = (a_1 b_1, \ldots, a_m b_m)$

Note

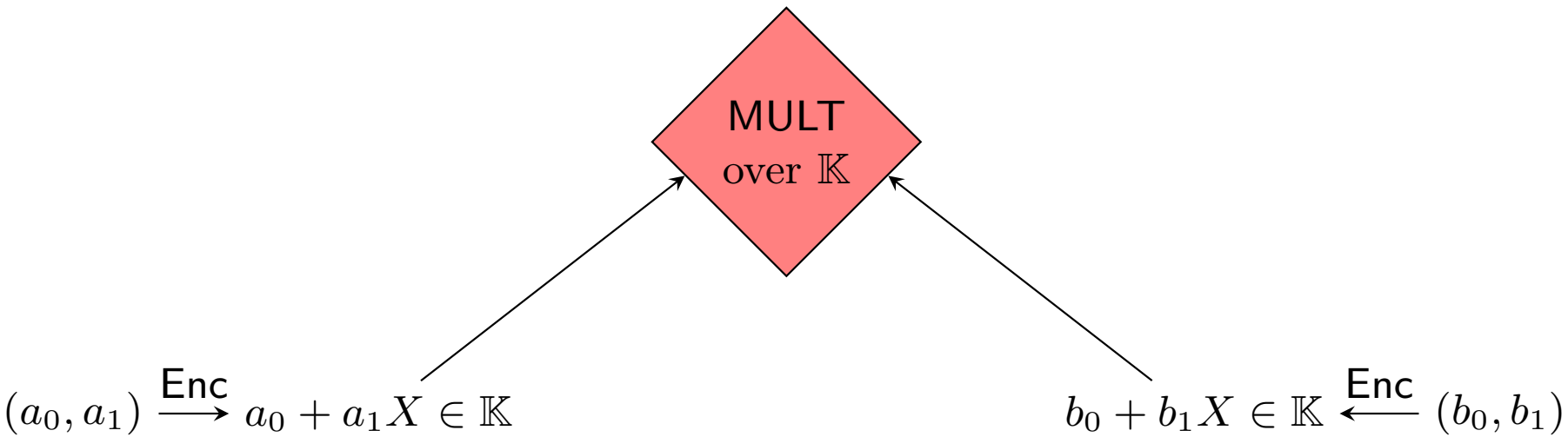
- Intuitively, we perform m multiplications over the base field $\mathbb{F}$ using one multiplication over the degree-n extension field $\mathbb{K}$
- For intuition, consider $\mathbb{K} = \mathbb{GF}[2^n]$ and $\mathbb{F} = \mathbb{GF}[2]$. However, our results hold for any degree-n extension field $\mathbb{K}$ of any base field $\mathbb{F}$.

Multiplication Embedding Problem: An Example

Suppose $\mathbb{K} = \mathbb{GF}[2^3]$ and $\mathbb{F} = \mathbb{GF}[2]$.
We interpret $\mathbb{K}$ as degree $\leqslant 2$ polynomials in X over $\mathbb{F}$.
The multiplication over $\mathbb{K}$ is defined using polynomial multiplication (modulo an irreducible degree-3 polynomial)

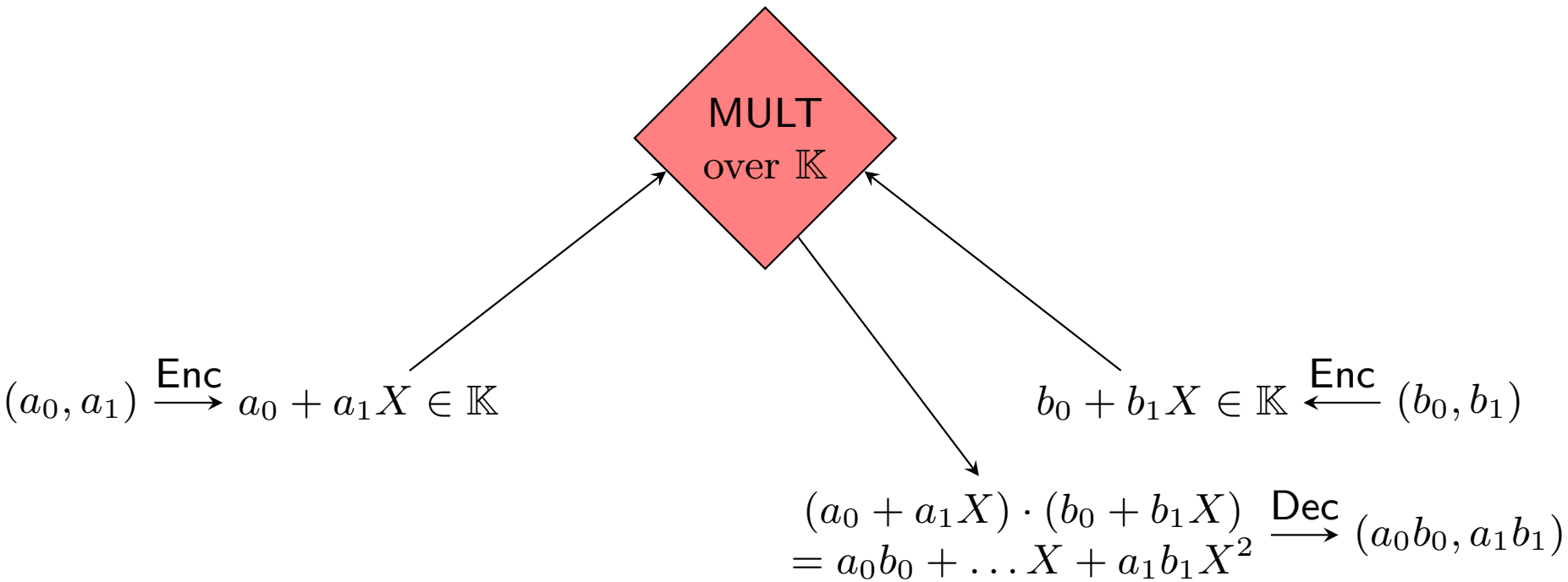
Multiplication Embedding Problem: An Example

Suppose $\mathbb{K} = \mathbb{GF}[2^3]$ and $\mathbb{F} = \mathbb{GF}[2]$.
We interpret $\mathbb{K}$ as degree $\leqslant 2$ polynomials in X over $\mathbb{F}$.
The multiplication over $\mathbb{K}$ is defined using polynomial multiplication (modulo an irreducible degree-3 polynomial)



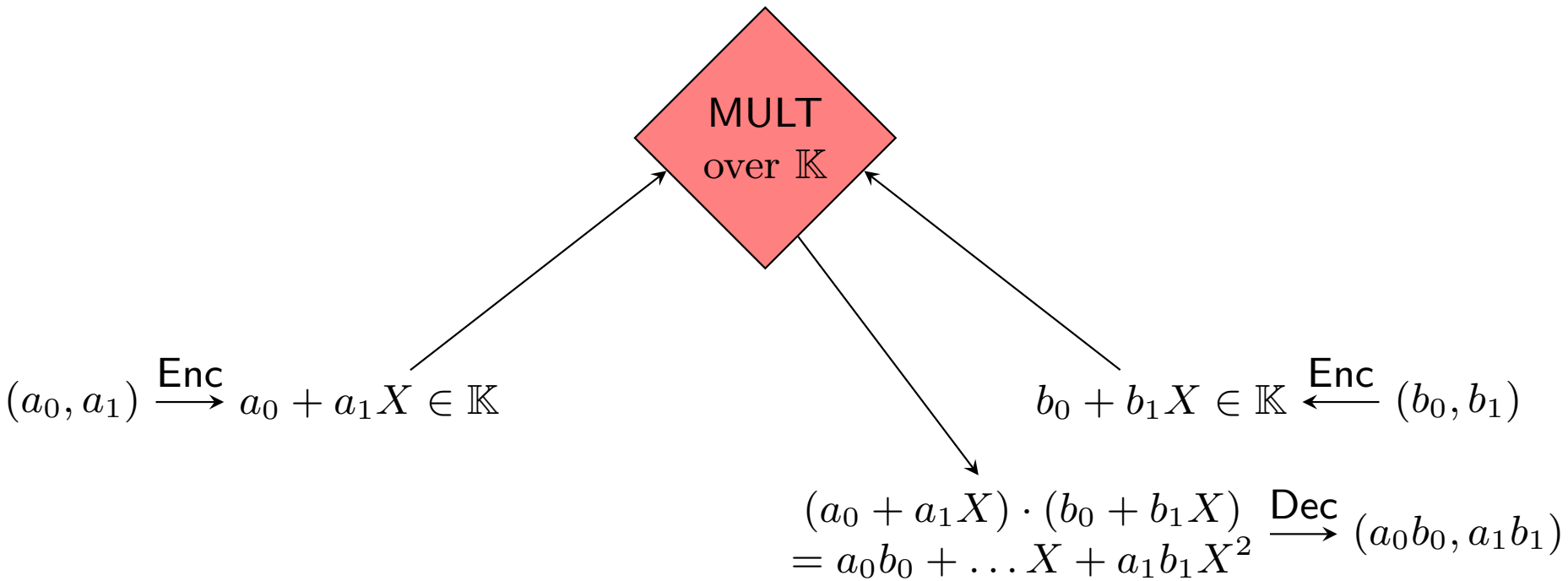
Multiplication Embedding Problem: An Example

Suppose $\mathbb{K} = \mathbb{GF}[2^3]$ and $\mathbb{F} = \mathbb{GF}[2]$.
We interpret $\mathbb{K}$ as degree $\leqslant 2$ polynomials in X over $\mathbb{F}$.
The multiplication over $\mathbb{K}$ is defined using polynomial multiplication (modulo an irreducible degree-3 polynomial)



Multiplication Embedding Problem: An Example

Suppose $\mathbb{K} = \mathbb{GF}[2^3]$ and $\mathbb{F} = \mathbb{GF}[2]$.
We interpret $\mathbb{K}$ as degree $\leqslant 2$ polynomials in X over $\mathbb{F}$.
The multiplication over $\mathbb{K}$ is defined using polynomial multiplication (modulo an irreducible degree-3 polynomial)



Note

Any element of the degree-n extension field $\mathbb{K}$ of a base field $\mathbb{F}$ can be represented as a polynomial of degree less than n with coefficients in $\mathbb{F}$.

Related Problem: Bi-linear Multiplication

$A \in \mathbb{K}$ $B \in \mathbb{K}$

$\mathbb{K}$ is the degree-n extension field of some finite field $\mathbb{F}$

Related Problem: Bi-linear Multiplication

$$A \in \mathbb{K} \xrightarrow{\mathsf{Enc}'} \mathbf{a} \in \mathbb{F}^m \qquad \mathbf{b} \in \mathbb{F}^m \xleftarrow{\mathsf{Enc}'} B \in \mathbb{K}$$

$\mathbb{K}$ is the degree-n extension field of some finite field $\mathbb{F}$

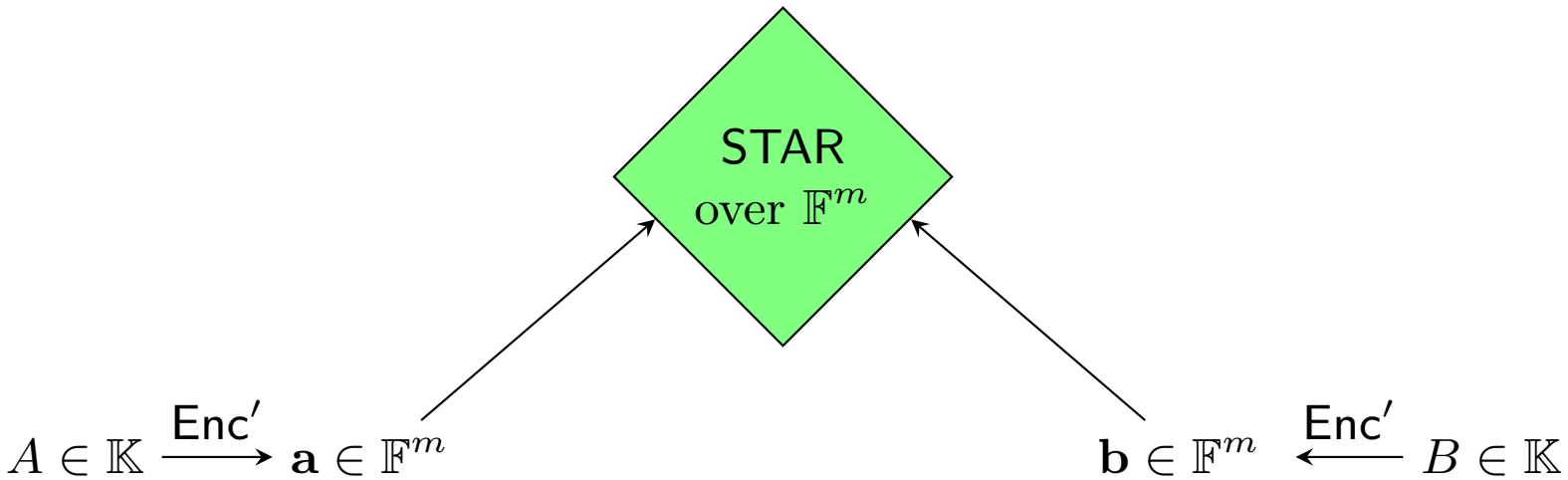
Related Problem: Bi-linear Multiplication

$A \in \mathbb{K} \xrightarrow{\mathsf{Enc}'} \mathbf{a} \in \mathbb{F}^m$ $\qquad$ $\mathbf{b} \in \mathbb{F}^m \xleftarrow{\mathsf{Enc}'} B \in \mathbb{K}$

$\mathbb{K}$ is the degree-n extension field of some finite field $\mathbb{F}$

The operator $*$ (STAR) is coordinate-wise multiplication of the vectors $\mathbf{a}, \mathbf{b} \in \mathbb{F}^m$

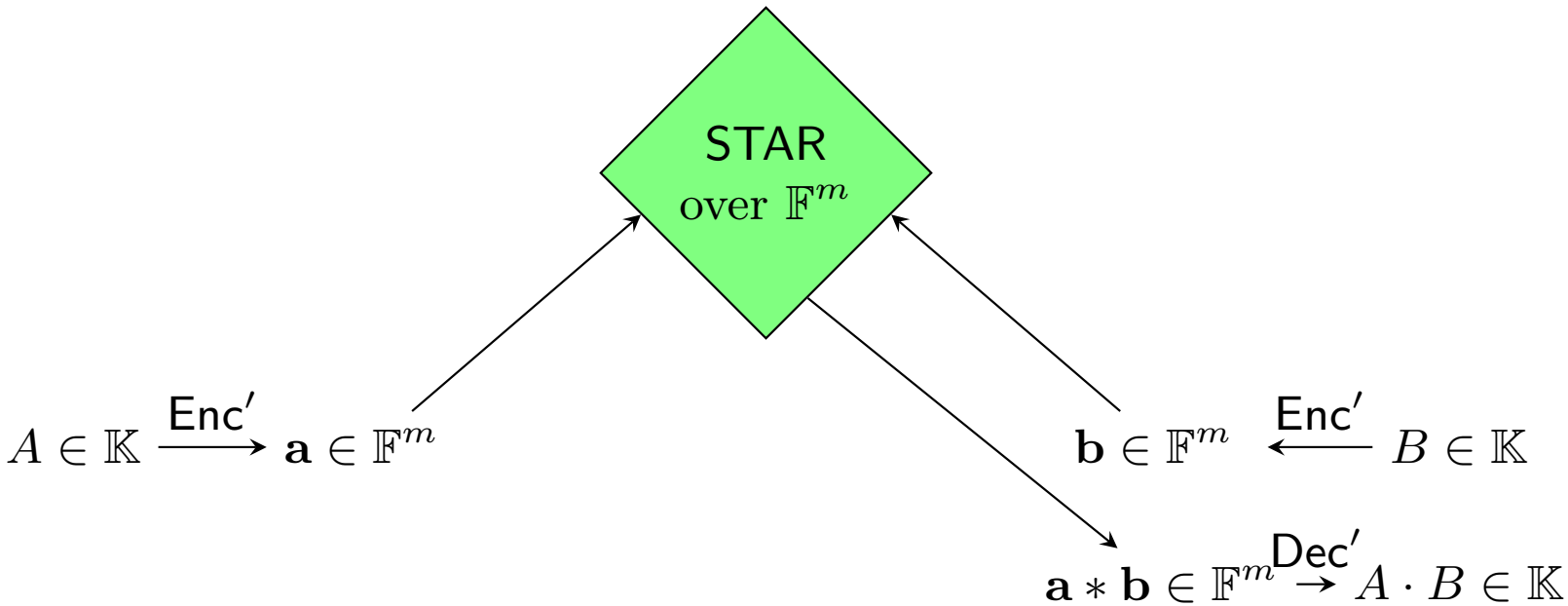
Related Problem: Bi-linear Multiplication



$\mathbb{K}$ is the degree-n extension field of some finite field $\mathbb{F}$

The operator $*$ (STAR) is coordinate-wise multiplication of the vectors $\mathbf{a}, \mathbf{b} \in \mathbb{F}^m$

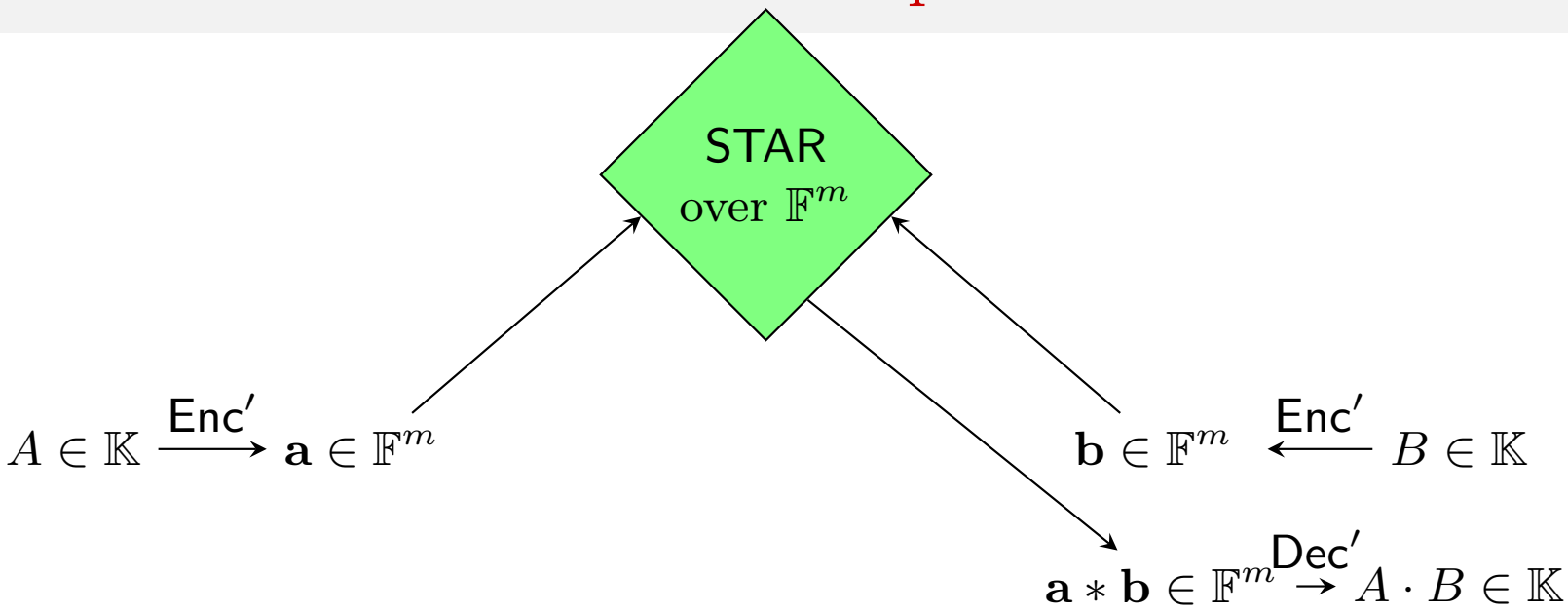
Related Problem: Bi-linear Multiplication



$\mathbb{K}$ is the degree-n extension field of some finite field $\mathbb{F}$

The operator $*$ (STAR) is coordinate-wise multiplication of the vectors $\mathbf{a}, \mathbf{b} \in \mathbb{F}^m$

Related Problem: Bi-linear Multiplication



$\mathbb{K}$ is the degree-n extension field of some finite field $\mathbb{F}$

The operator $*$ (STAR) is coordinate-wise multiplication of the vectors $\mathbf{a}, \mathbf{b} \in \mathbb{F}^m$

Question

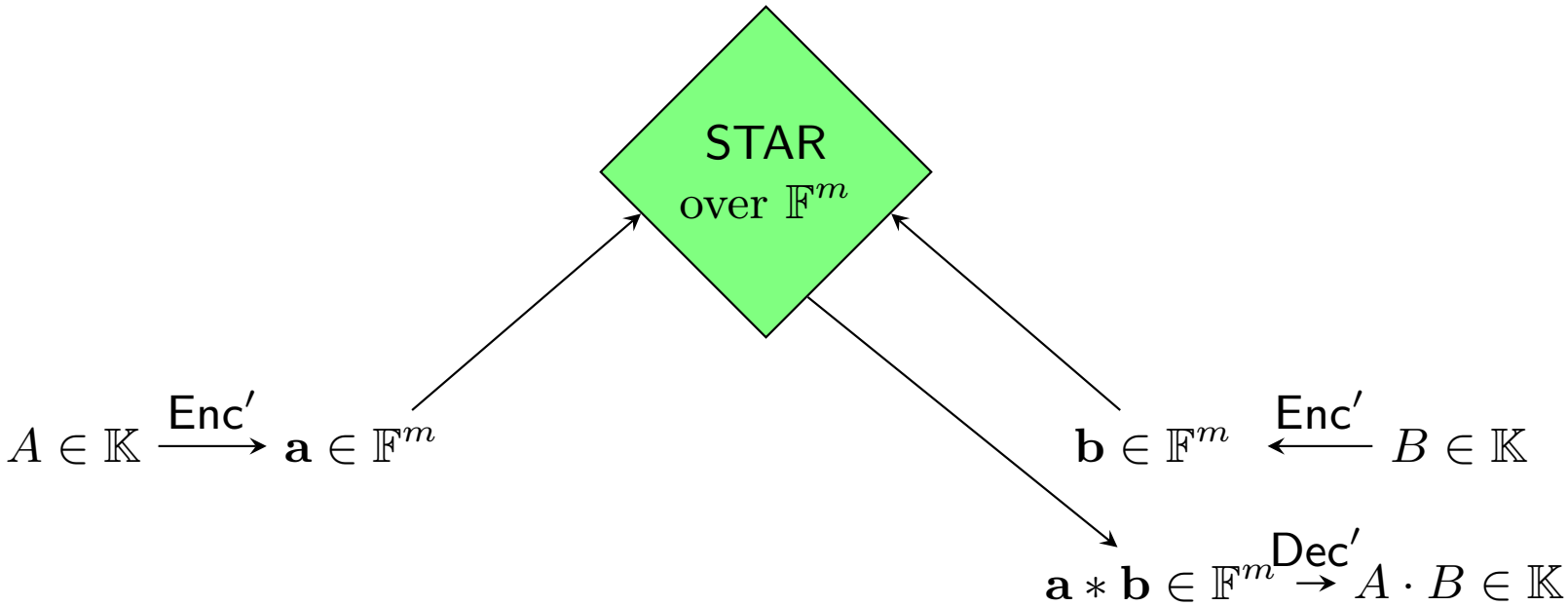
Given n and a field $\mathbb{F}$, find smallest m such that there exist Enc' and Dec' satisfying

$$\mathsf{Dec}'(\mathsf{Enc}'(A) * \mathsf{Enc}'(B)) = A \cdot B \text{ for all } A, B \in \mathbb{F}^m$$

Intuition

We can perform one multiplication over the degree-n extension field $\mathbb{K}$ using m multiplications over the base field $\mathbb{F}$.

Related Problem: Bi-linear Multiplication



$\mathbb{K}$ is the degree-n extension field of some finite field $\mathbb{F}$

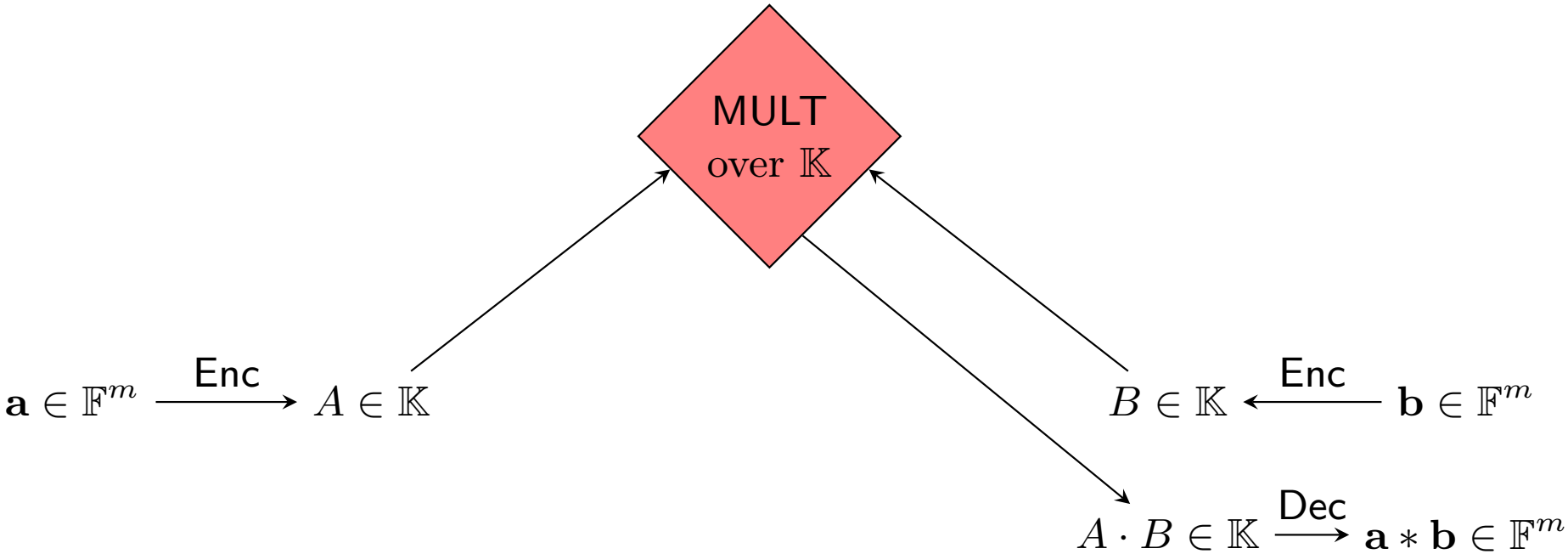
The operator $*$ (STAR) is coordinate-wise multiplication of the vectors $\mathbf{a}, \mathbf{b} \in \mathbb{F}^m$

Theorem (Chudnovsky-Chudnovsky [CC87])

There exist mappings $\mathsf{Enc}' : \mathbb{K} \to \mathbb{F}^m$ *and* $\mathsf{Dec}' : \mathbb{F}^m \to \mathbb{K}$ *such that*

- m *is linear in* n
- $\mathsf{Dec}'(\mathsf{Enc}'(A) * \mathsf{Enc}'(B)) = A \cdot B$ *for all* $A, B \in \mathbb{F}^m$

Our Main Result



$\mathbb{K}$ is the degree-n extension field of some finite field $\mathbb{F}$
The operator $*$ is coordinate-wise multiplication of the vectors $\mathbf{a}, \mathbf{b} \in \mathbb{F}^m$
For example $(a_1, \ldots, a_m) * (b_1, \ldots, b_m) = (a_1 b_1, \ldots, a_m b_m)$

Theorem (Multiplication Embedding)

There exist two linear maps $E : \mathbb{F}^m \to \mathbb{K}$ and $D : \mathbb{K} \to \mathbb{F}^m$ such that

- *m is linear in n*
- *$D(E(\mathbf{a}) \cdot E(\mathbf{b})) = \mathbf{a} * \mathbf{b}$ for all $\mathbf{a}, \mathbf{b} \in \mathbb{F}^m$*

Our Main Result

Theorem (Multiplication Embedding)

There exist two linear maps $E : \mathbb{F}^m \to \mathbb{K}$ *and* $D : \mathbb{K} \to \mathbb{F}^m$ *such that*

- m *is* *linear* *in* n
- $D(E(\mathbf{a}) \cdot E(\mathbf{b})) = \mathbf{a} * \mathbf{b}$ *for all* $\mathbf{a}, \mathbf{b} \in \mathbb{F}^m$

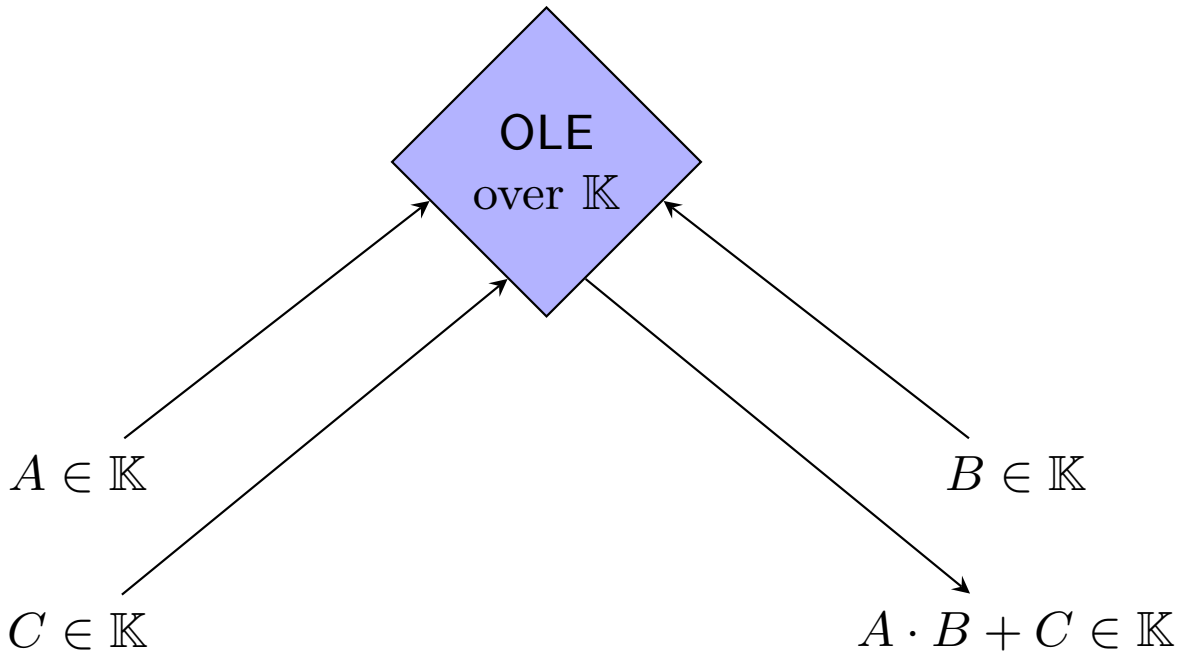
Recent Independent Work

Cascudo et al. [CCXY18] (CRYPTO–2018) studied this embedding problem (referred to as the "Reverse Multiplication-Friendly Embeddings" (RMFE))

- Provide a linear-rate construction.
- Use this result to achieve new amortization results in MPC.

Assuming Linear-rate Solution for the Embedding Problem: Consequences for MPC

Oblivious Linear-function Evaluation over a field $\mathbb{K}$:



Note

1-out-of-2-OT $\equiv$ OLE($\mathbb{GF}[2]$) since $x_b = (x_1 + x_0)b + x_0$.

Assuming Linear-rate Solution for the Embedding Problem: Consequences for MPC

Theorem

There exists a 2-party semi-honest secure protocol that

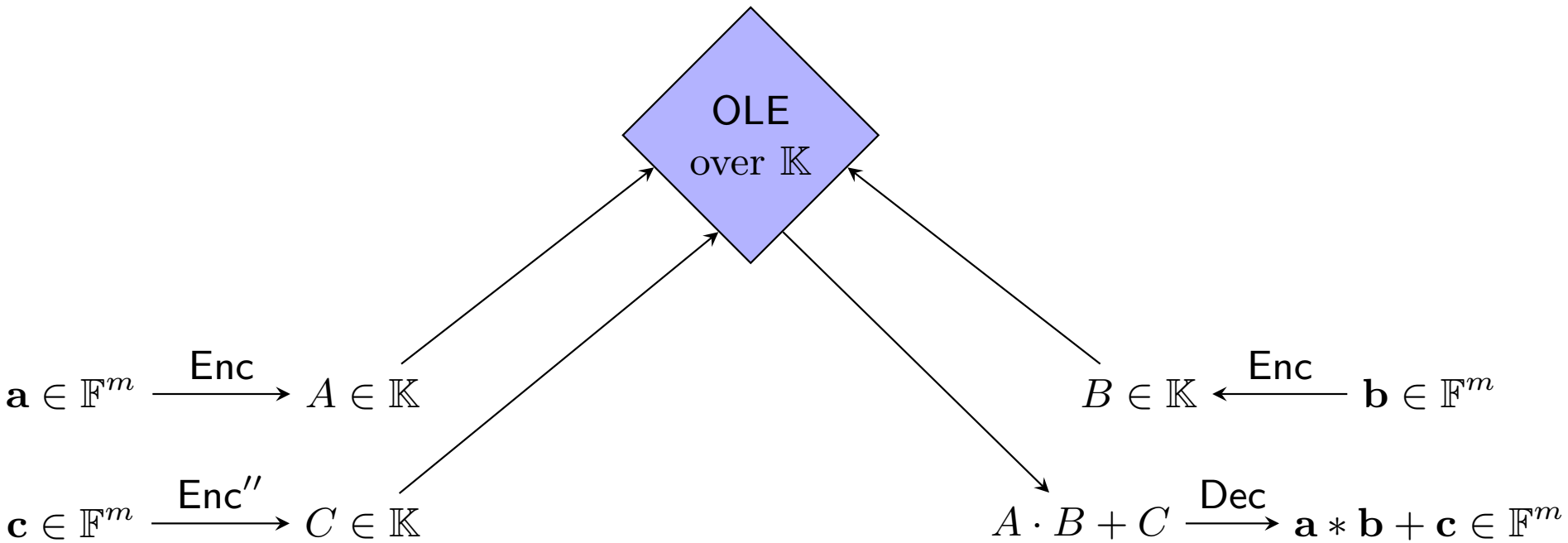
- *performs only one call to* $\mathsf{OLE}(\mathbb{K})$ *(no additional communication)*
- *produces* $m = \Theta(n)$ *samples of* $\mathsf{OLE}(\mathbb{F})$

Assuming Linear-rate Solution for the Embedding Problem: Consequences for MPC

Theorem

There exists a 2-party semi-honest secure protocol that

- *performs only one call to* $\mathsf{OLE}(\mathbb{K})$ *(no additional communication)*
- *produces* $m = \Theta(n)$ *samples of* $\mathsf{OLE}(\mathbb{F})$



Assuming Linear-rate Solution for the Embedding Problem: Consequences for MPC (Corollary 1)

Corollary

There exists a computationally secure protocol that is

- *Based on any computational hardness assumption that helps construct one* OLE *over an extension field, and*
- *Implements a linear number of* OT*s with linear communication complexity*

Assuming Linear-rate Solution for the Embedding Problem: Consequences for MPC (Corollary 1)

Corollary

There exists a computationally secure protocol that is

- *Based on any computational hardness assumption that helps construct one* OLE *over an extension field, and*
- *Implements a linear number of* OT*s with linear communication complexity*

Example (Computational Hardness Assumption)

- Ishai-Prabhakaran-Sahai [IPS09] and Naor-Pinkas [NP06]: Pseudorandomness of noisy random RS codewords $\Rightarrow \mathsf{OLE}(\mathbb{K})$.
- Applebaum et al. [ADI+17]: Arithmetic analogues of well-studied cryptographic assumptions $\Rightarrow \mathsf{OLE}(\mathbb{K})$.

Assuming Linear-rate Solution for the Embedding Problem: Consequences for MPC (Corollary 2)

Corollary

For all $\varepsilon \in [0, 1/2)$, there exists an n-bit correlated private randomness such that

- *Despite $t = (1/2 - \varepsilon)n$ bits of leakage*
- *We can securely compute a linear number of independent and secure OTs from the leaky correlated private randomness*

Prior Best Solution to the Embedding Problem: BMN Embedding

Theorem (Block-Maji-Nguyen [BMN17])

There exist two mappings $\mathsf{Enc} : \mathbb{F}^m \to \mathbb{K}$ *and* $\mathsf{Dec} : \mathbb{K} \to \mathbb{F}^m$ *satisfying*

- $m = n^{1-o(1)}$
- $\mathsf{Dec}(\mathsf{Enc}(\mathbf{a}) \cdot \mathsf{Enc}(\mathbf{b})) = \mathbf{a} * \mathbf{b}$ *for all* $\mathbf{a}, \mathbf{b} \in \mathbb{F}^m$

Prior Best Solution to the Embedding Problem: BMN Embedding

Theorem (Block-Maji-Nguyen [BMN17])

There exist two mappings $\mathsf{Enc} : \mathbb{F}^m \to \mathbb{K}$ *and* $\mathsf{Dec} : \mathbb{K} \to \mathbb{F}^m$ *satisfying*

- $m = n^{1-o(1)}$
- $\mathsf{Dec}(\mathsf{Enc}(\mathbf{a}) \cdot \mathsf{Enc}(\mathbf{b})) = \mathbf{a} * \mathbf{b}$ *for all* $\mathbf{a}, \mathbf{b} \in \mathbb{F}^m$

Note

Reduces the construction to the famous "Tri-colored Sum-free Set" problem in combinatorics (Kleinberg [Kle16], Blasiak et.al. [BCC+17], Kleinberg-Speyer-Sawin [KSS18]).

Let Us Try to Solve the Embedding Multiplication Problem

Principal Observation: Two equivalent ways to multiply polynomials

- Direct technique: compute the convolution of the two polynomials

$$\mathbb{F}_{q^n} \times \mathbb{F}_{q^n} \xrightarrow{\text{mult.}} \mathbb{F}_{q^n}$$

Let Us Try to Solve the Embedding Multiplication Problem

Principal Observation: Two equivalent ways to multiply polynomials

- Direct technique: compute the convolution of the two polynomials
- Indirect technique:
  - Evaluate both polynomials at sufficiently many points

$$\begin{array}{c} \mathbb{F}_{q^n} \times \mathbb{F}_{q^n} \\ \Big\downarrow \beta \times \beta \\ \mathbb{F}_q^m \times \mathbb{F}_q^m \end{array}$$

Here β is the "evaluation map"

Let Us Try to Solve the Embedding Multiplication Problem

Principal Observation: Two equivalent ways to multiply polynomials

- Direct technique: compute the convolution of the two polynomials
- Indirect technique:
  - Evaluate both polynomials at sufficiently many points
  - Compute the coordinate-wise product of each evaluation

$$\begin{array}{ccc} \mathbb{F}_{q^n} \times \mathbb{F}_{q^n} & & \\ \Big\downarrow \beta \times \beta & & \\ \mathbb{F}_q^m \times \mathbb{F}_q^m & \xrightarrow{\quad * \quad} & \mathbb{F}_q^m \end{array}$$

Here β is the "evaluation map"

Let Us Try to Solve the Embedding Multiplication Problem

Principal Observation: Two equivalent ways to multiply polynomials

- Direct technique: compute the convolution of the two polynomials
- Indirect technique:
  - Evaluate both polynomials at sufficiently many points
  - Compute the coordinate-wise product of each evaluation
  - Lagrange interpolate to reconstruct the "product polynomial"

$$\begin{array}{ccc} \mathbb{F}_{q^n} \times \mathbb{F}_{q^n} & & \mathbb{F}_{q^n} \\ \downarrow{\scriptstyle \beta \times \beta} & & \downarrow{\scriptstyle \beta} \\ \mathbb{F}_q^m \times \mathbb{F}_q^m & \xrightarrow{\quad * \quad} & \mathbb{F}_q^m \end{array}$$

Here β is the "evaluation map"

Let Us Try to Solve the Embedding Multiplication Problem

Principal Observation: Two equivalent ways to multiply polynomials

- Direct technique: compute the convolution of the two polynomials
- Indirect technique:
  - Evaluate both polynomials at sufficiently many points
  - Compute the coordinate-wise product of each evaluation
  - Lagrange interpolate to reconstruct the "product polynomial"

$$\begin{array}{ccc} \mathbb{F}_{q^n} \times \mathbb{F}_{q^n} & \xrightarrow{\text{mult.}} & \mathbb{F}_{q^n} \\ \downarrow \beta \times \beta & & \downarrow \beta \\ \mathbb{F}_q^m \times \mathbb{F}_q^m & \xrightarrow{*} & \mathbb{F}_q^m \end{array}$$

Here β is the "evaluation map"

Implications

There are also 2 ways to perform coordinate-wise product.

First Attempt: Reed-Solomon Codes + BMN Embeddings

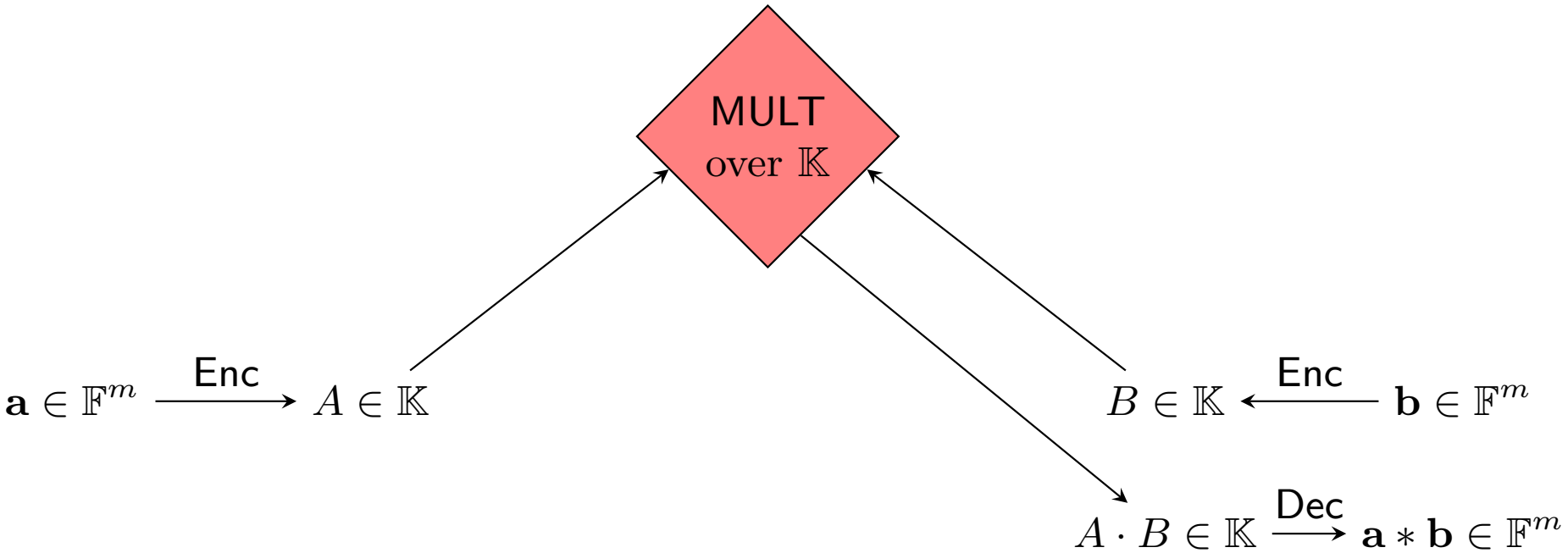
Reed-Solomon Codes

- For a field $\mathbb{F}$ of size $|\mathbb{F}| \geqslant \eta$, and $S = \{\alpha_1, \alpha_2, \ldots, \alpha_\eta\} \subseteq \mathbb{F}$, the Reed-Solomon code with block length η and dimension k is defined as

$$\mathsf{RS}_{\mathbb{F},S}(\eta, k) = \{(p(\alpha_1), \ldots, p(\alpha_\eta)) \in \mathbb{F}^\eta \mid \deg p(X) \text{ is less than } k\}.$$

First Attempt: Reed-Solomon Codes + BMN Embeddings

Recall that we want to do:



$\mathbb{K}$ is the degree-n extension field of some finite field $\mathbb{F}$
The operator $*$ is coordinate-wise multiplication of the vectors $\mathbf{a}, \mathbf{b} \in \mathbb{F}^m$
For example $(a_1, \ldots, a_m) * (b_1, \ldots, b_m) = (a_1 b_1, \ldots, a_m b_m)$

Think about $\mathbf{a}, \mathbf{b}$ as codewords in $\mathsf{RS}_{\mathbb{F},S}(m, m)$.

First Attempt: Reed-Solomon Codes + BMN Embeddings

If $|\mathbb{F}| \geqslant m = n/2$, let $\alpha_0, \alpha_1, \ldots, \alpha_{m-1}$ be distinct elements of $\mathbb{F}$.

$$\mathbf{a} \in \mathbb{F}^m \xrightarrow[\text{L.I.}]{\mathsf{Enc}} \begin{array}{l} A(X) \in \mathbb{K} \\ \deg A < m \\ A(\alpha_i) = a_i \end{array}$$

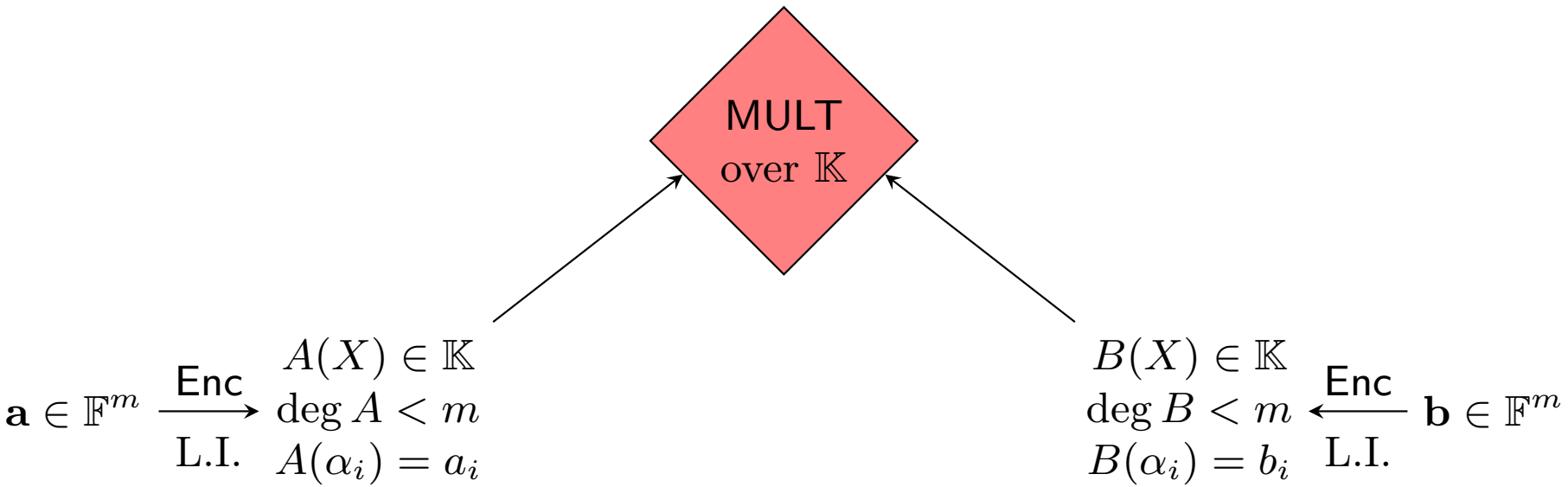
$$\begin{array}{l} B(X) \in \mathbb{K} \\ \deg B < m \\ B(\alpha_i) = b_i \end{array} \xleftarrow[\text{L.I.}]{\mathsf{Enc}} \mathbf{b} \in \mathbb{F}^m$$

Note

- Enc is Largrange Interpolation (LI).

First Attempt: Reed-Solomon Codes + BMN Embeddings

If $|\mathbb{F}| \geqslant m = n/2$, let $\alpha_0, \alpha_1, \ldots, \alpha_{m-1}$ be distinct elements of $\mathbb{F}$.

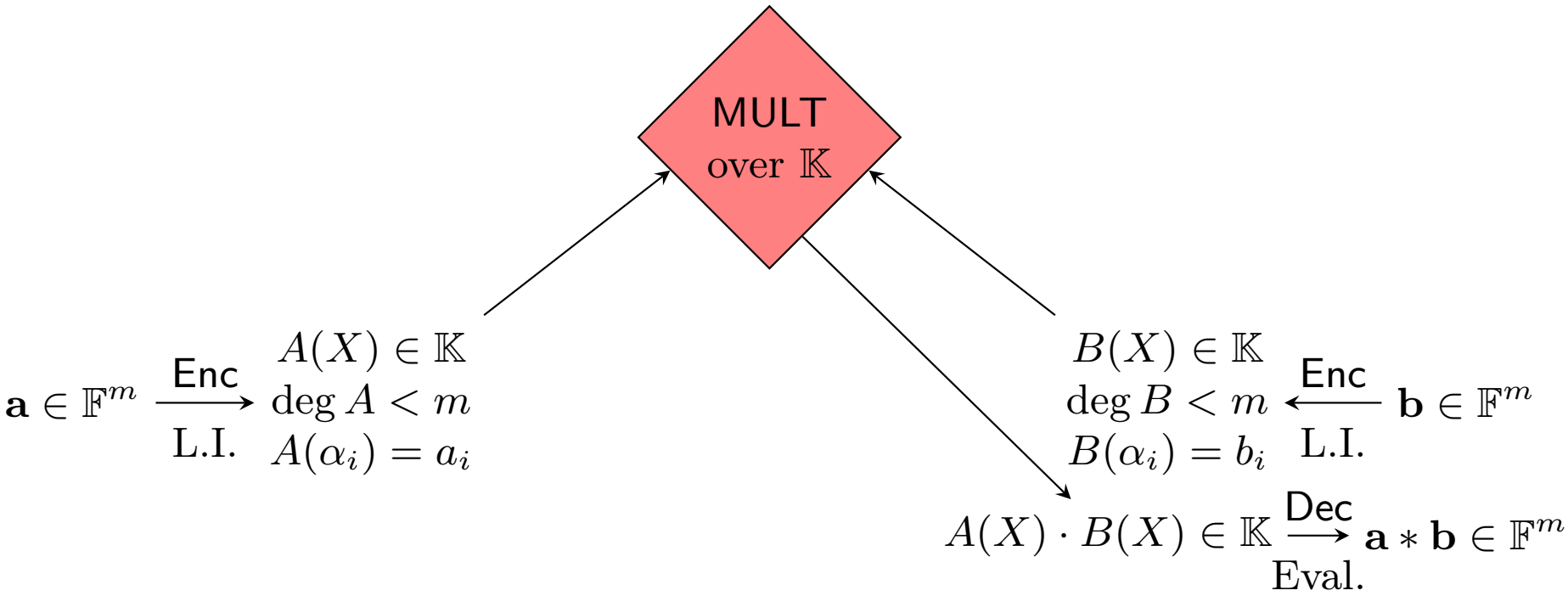


Note

- Enc is Largrange Interpolation (LI).
- Multiplication of two polynomials of degree $< n/2$ is the same as multiplication over degree-n extension field $\mathbb{K}$.

First Attempt: Reed-Solomon Codes + BMN Embeddings

If $|\mathbb{F}| \geqslant m = n/2$, let $\alpha_0, \alpha_1, \ldots, \alpha_{m-1}$ be distinct elements of $\mathbb{F}$.

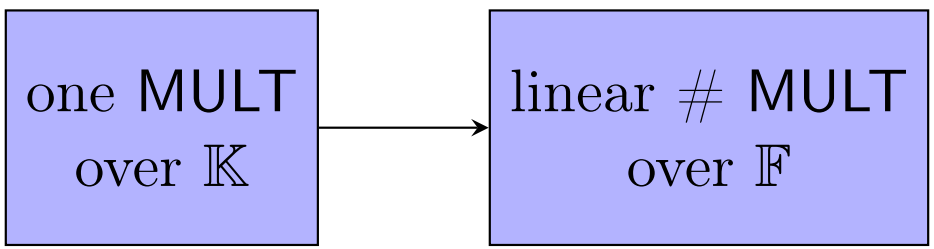


Note

- Enc is Largrange Interpolation (LI).
- Multiplication of two polynomials of degree $< n/2$ is the same as multiplication over degree-n extension field $\mathbb{K}$.
- Dec is an evaluation (Eval.) map such that $A(\alpha_i) \cdot B(\alpha_i) = a_i \cdot b_i$.

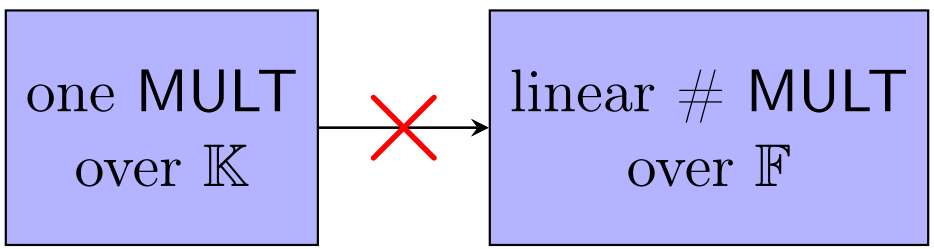
First Attempt: Reed-Solomon Codes + BMN Embeddings

If $\mathbb{F}$ has sufficiently many places ($|\mathbb{F}|$ is linear in n)



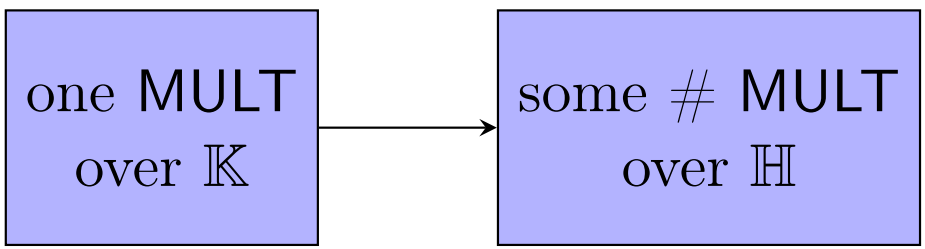
First Attempt: Reed-Solomon Codes + BMN Embeddings

What if $\mathbb{F}$ does not have enough places ($|\mathbb{F}|$ is constant)?



First Attempt: Reed-Solomon Codes + BMN Embeddings

What if $\mathbb{F}$ does not have enough places ($|\mathbb{F}|$ is constant)?

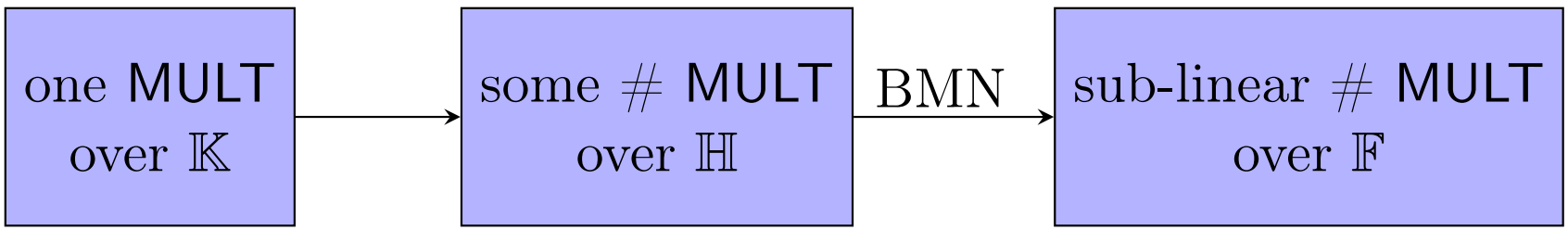


Note

- $\mathbb{K} = \mathbb{GF}[2^n], \mathbb{H} = \mathbb{GF}[2^s], \mathbb{F} = \mathbb{GF}[2]$, where $s \approx \lg n$
- RS encoding: n/s copies of $\mathsf{OLE}(\mathbb{H})$

First Attempt: Reed-Solomon Codes + BMN Embeddings

What if $\mathbb{F}$ does not have enough places ($|\mathbb{F}|$ is constant)?



Note

- $\mathbb{K} = \mathbb{GF}[2^n], \mathbb{H} = \mathbb{GF}[2^s], \mathbb{F} = \mathbb{GF}[2]$, where $s \approx \lg n$
- RS encoding: n/s copies of $\mathsf{OLE}(\mathbb{H})$
- BMN embedding: each $\mathsf{OLE}(\mathbb{H})$ gives $s^{1-o(1)}$ copies of OTs
- $\#\mathsf{OT} = n \cdot \dfrac{1}{(\lg n)^{o(1)}}$

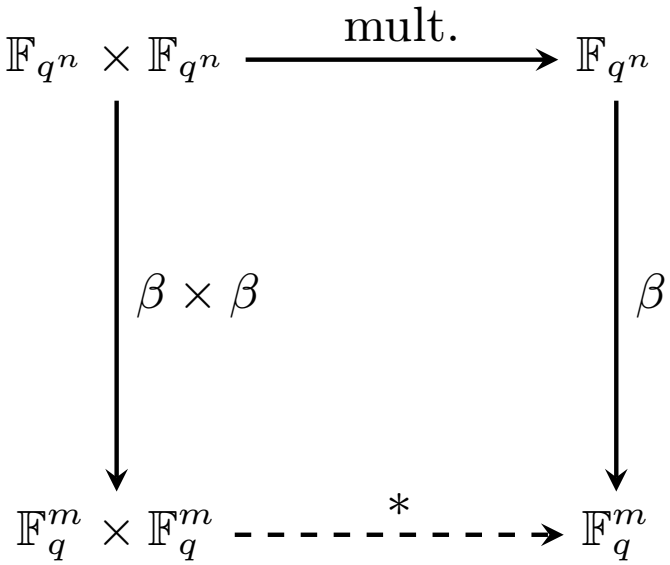
Getting to Multiplication Embeddings with a Linear Rate

Note

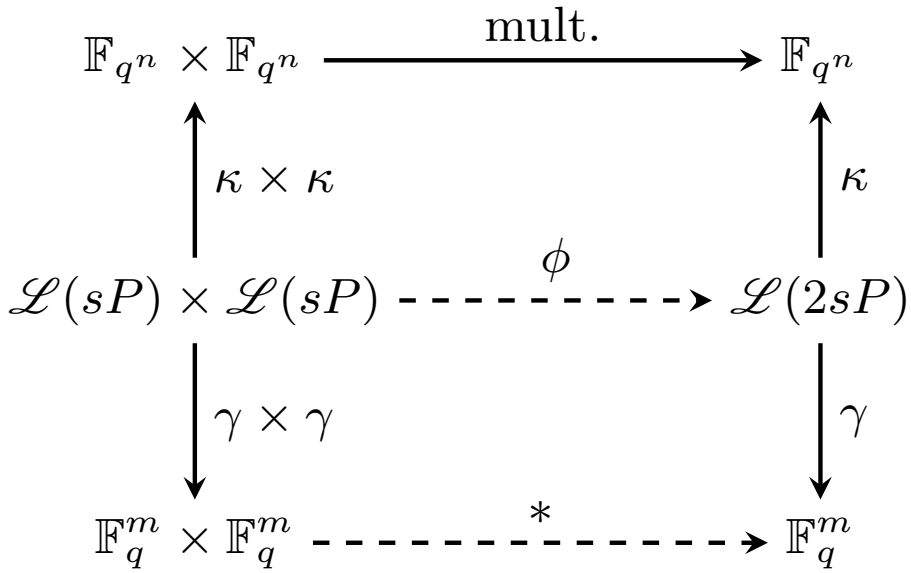
- Reed-Solomon codes: Maximum Distance Separable (MDS) over large-size fields.
- Algebraic Geometry codes (Goppa [Gop81]): near MDS with multiplicative property just like RS but over constant-size fields.

Getting to Multiplication Embeddings with a Linear Rate

Commutative diagrams for multiplication embedding:



Using RS codes



Using AG codes

Note

- $\gamma : z \mapsto (z(P_1), \ldots, z(P_m))$, where P_i's is prime divisors of degree one.
- $\kappa : z \mapsto z(Q)$, where Q is a prime divisor of degree n.
- κ must be surjective to make our embedding work.

Getting to Multiplication Embeddings with a Linear Rate

Note

We use algebraic function fields (Burgisser-Clausen-Shokrollahi [BCS97], Garcia-Stichtenoth [GS96]) to construct the multiplication embeddings for every base field $\mathbb{F}$.

Theorem

There exist two mappings $\mathsf{Enc} : \mathbb{F}^m \to \mathbb{K}$ *and* $\mathsf{Dec} : \mathbb{K} \to \mathbb{F}^m$ *satisfying*

- m *is* *linear* *in* n
- $\mathsf{Dec}(\mathsf{Enc}(\mathbf{a}) \cdot \mathsf{Enc}(\mathbf{b})) = \mathbf{a} * \mathbf{b}$ *for all* $\mathbf{a}, \mathbf{b} \in \mathbb{F}^m$.

Getting to Multiplication Embeddings with a Linear Rate

Note

We use algebraic function fields (Burgisser-Clausen-Shokrollahi [BCS97], Garcia-Stichtenoth [GS96]) to construct the multiplication embeddings for every base field $\mathbb{F}$.

Theorem

There exist two mappings $\mathsf{Enc} : \mathbb{F}^m \to \mathbb{K}$ *and* $\mathsf{Dec} : \mathbb{K} \to \mathbb{F}^m$ *satisfying*

- m *is* *linear* *in* n
- $\mathsf{Dec}(\mathsf{Enc}(\mathbf{a}) \cdot \mathsf{Enc}(\mathbf{b})) = \mathbf{a} * \mathbf{b}$ *for all* $\mathbf{a}, \mathbf{b} \in \mathbb{F}^m$.

Thank You!