Slicing Boolean Functions with Inner Products

Pierrick Méaux **Tim Seuré**

University of Luxembourg

Selected Areas in Cryptography
Ottawa, Canada

August 28, 2026

Motivation

Within symmetric cryptography, we choose Boolean functions with:

- Strong cryptographic properties, *e.g.*:
  - High algebraic degree
  - High nonlinearity
  - High algebraic immunity

Motivation

Within symmetric cryptography, we choose Boolean functions with:

- Strong cryptographic properties, *e.g.*:
  - High algebraic degree
  - High nonlinearity
  - High algebraic immunity
- Some extra structure to enable efficient evaluation (*e.g.*, in the context of HHE [NLV11]).

Hamming-Weight Decompositions

Here is one recent source for obtaining such Boolean functions:

Definition [GM22, MO24]

We call $f \in \mathcal{B}_n$ *weightwise degree-d if there are* $f_k \in \mathcal{B}_n$ *with* $\deg(f_k) \leqslant d$ *such that:*

$$\forall \boldsymbol{x} \in \mathbb{F}_2^n : \; f(\boldsymbol{x}) = \sum_k \mathbb{1}_{w(\boldsymbol{x})=k} \cdot f_k(\boldsymbol{x}).$$

Hamming-Weight Decompositions

Here is one recent source for obtaining such Boolean functions:

Definition [GM22, MO24]

We call $f \in \mathcal{B}_n$ *weightwise degree-d if there are* $f_k \in \mathcal{B}_n$ *with* $\deg(f_k) \leqslant d$ *such that:*

$$\forall \boldsymbol{x} \in \mathbb{F}_2^n : \; f(\boldsymbol{x}) = \sum_k \mathbb{1}_{w(\boldsymbol{x})=k} \cdot f_k(\boldsymbol{x}).$$

Notice that:

$$w(\boldsymbol{x}) = \langle \boldsymbol{v}, \boldsymbol{x} \rangle = \sum_i v_i x_i, \qquad \boldsymbol{v} = (1, \ldots, 1) \in \mathbb{Z}^n.$$

Vector-Slice Decompositions

This naturally leads to the following generalization to any $\boldsymbol{v} \in \mathbb{Z}^n$:

Definition

We call $f \in \mathcal{B}_n$ *degree-d on* $\boldsymbol{v}$*-slices if there are* $f_k \in \mathcal{B}_n$ *with* $\deg(f_k) \leqslant d$ *such that:*

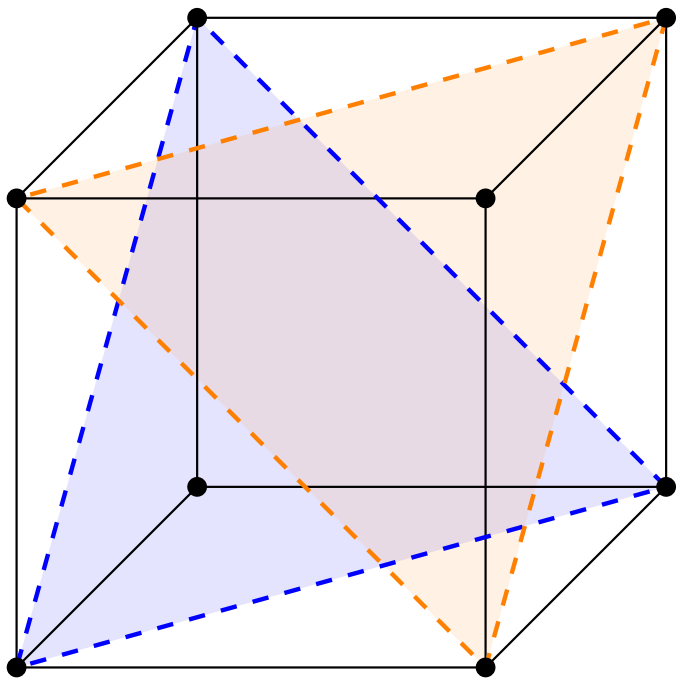
$$\forall \boldsymbol{x} \in \mathbb{F}_2^n : \; f(\boldsymbol{x}) = \sum_k \mathbb{1}_{\langle \boldsymbol{v}, \boldsymbol{x} \rangle = k} \cdot f_k(\boldsymbol{x}).$$

We denote the number of terms in this decomposition by:

$$\kappa(\boldsymbol{v}) \coloneqq \#\{\langle \boldsymbol{v}, \boldsymbol{x} \rangle \mid \boldsymbol{x} \in \mathbb{F}_2^n\}.$$

Vector-Slice Decompositions

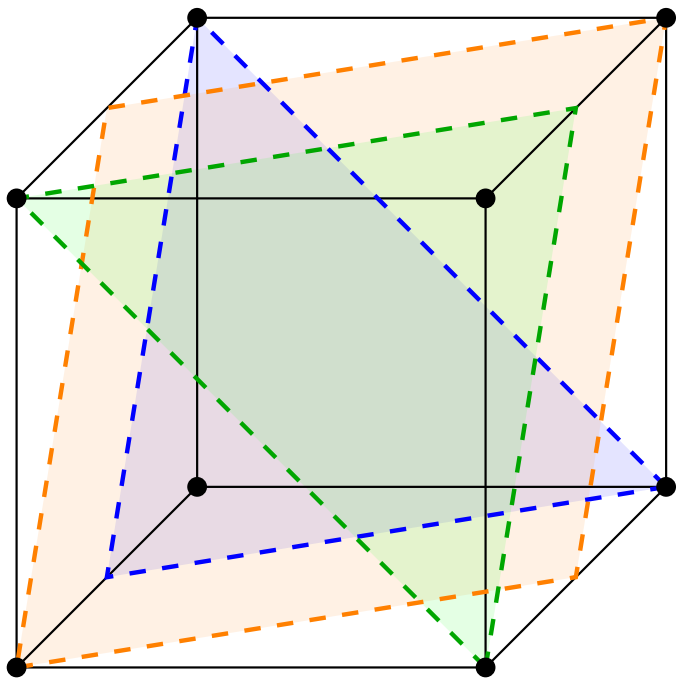
Decomposition of $\mathbb{F}_2^3$ according to $\boldsymbol{v} = (1, 1, 1)$:



$$\{(0,0,0)\}$$
$$\{(0,0,1),(0,1,0),(1,0,0)\}$$
$$\{(1,1,0),(1,0,1),(0,1,1)\}$$
$$\{(1,1,1)\}$$

Vector-Slice Decompositions

Decomposition of $\mathbb{F}_2^3$ according to $\boldsymbol{v} = (1, 1, 2)$:



$$\{(0,0,0)\}$$
$$\{(0,1,0),(1,0,0)\}$$
$$\{(0,0,1),(1,1,0)\}$$
$$\{(0,1,1),(1,0,1)\}$$
$$\{(1,1,1)\}$$

Slice Complexities

We want to minimize the number of terms in the decomposition of f:

Definition

The degree-d slice complexity of $f \in \mathcal{B}_n$ is:

$$\kappa_d(f) := \min\{\kappa(\boldsymbol{v}) \mid \boldsymbol{v} \in \mathbb{Z}^n \text{ and } f \text{ is degree-}d \text{ on } \boldsymbol{v}\text{-slices}\}.$$

Slice Complexities

We want to minimize the number of terms in the decomposition of f:

Definition

The degree-d slice complexity of $f \in \mathcal{B}_n$ is:

$$\kappa_d(f) \coloneqq \min\{\kappa(\boldsymbol{v}) \mid \boldsymbol{v} \in \mathbb{Z}^n \text{ and } f \text{ is degree-}d \text{ on } \boldsymbol{v}\text{-slices}\}.$$

Every $f \in \mathcal{B}_n$ is degree-d on $\boldsymbol{v}$-slices for $\boldsymbol{v} = \left(1, 2, 4, \ldots, 2^{n-1}\right) \in \mathbb{Z}^n$, so $\kappa_d(f)$ is well-defined.

First Results

Proposition

Every $f \in \mathcal{B}_n$ satisfies the following:

- $\kappa_d(f) = 1 \iff \deg(f) \leqslant d$
- $\kappa_d(f) \leqslant 2^{n-d}$
- $2^n - 1 \geqslant \kappa_0(f) \geqslant \kappa_1(f) \geqslant \cdots \geqslant \kappa_n(f) = 1$

Proposition

If $f \in \mathcal{B}_n$ depends on all n variables, then $\kappa_0(f) \geqslant n + 1$, with equality if and only if f is translation-equivalent to a symmetric function.

Many more results are in the paper!

Homomorphic Evaluation

- Consider a GSW-like FHE scheme [GSW13] handling encrypted bits.

Homomorphic Evaluation

- Consider a GSW-like FHE scheme [GSW13] handling encrypted bits.
- In the paper, we provide a circuit to homomorphically compute:

$$\mathsf{Enc}(x_1), \ldots, \mathsf{Enc}(x_n) \mapsto \mathsf{Enc}(f(\boldsymbol{x})).$$

Homomorphic Evaluation

- Consider a GSW-like FHE scheme [GSW13] handling encrypted bits.
- In the paper, we provide a circuit to homomorphically compute:

$$\mathsf{Enc}(x_1), \ldots, \mathsf{Enc}(x_n) \mapsto \mathsf{Enc}(f(\boldsymbol{x})).$$

- For fixed scheme parameters, this circuit increases the error variance by a factor of $\mathcal{O}\big(\kappa_d(f) \cdot n^d\big)$.

Homomorphic Evaluation

- Consider a GSW-like FHE scheme [GSW13] handling encrypted bits.
- In the paper, we provide a circuit to homomorphically compute:

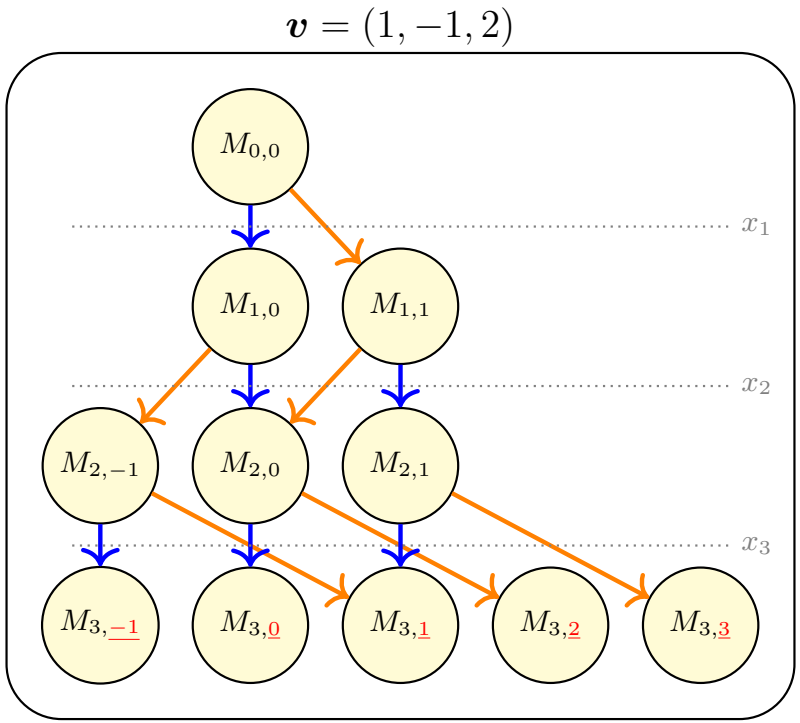
$$\mathsf{Enc}(x_1), \ldots, \mathsf{Enc}(x_n) \mapsto \mathsf{Enc}(f(\boldsymbol{x})).$$

- For fixed scheme parameters, this circuit increases the error variance by a factor of $\mathcal{O}\big(\kappa_d(f) \cdot n^d\big)$.
- The essential part is how we homomorphically compute the indicators:

$$\mathsf{Enc}(x_1), \ldots, \mathsf{Enc}(x_n) \overset{?}{\mapsto} \mathsf{Enc}(\mathbb{1}_{\langle \boldsymbol{v}, \boldsymbol{x} \rangle = k}).$$

Homomorphic Computation of Indicators

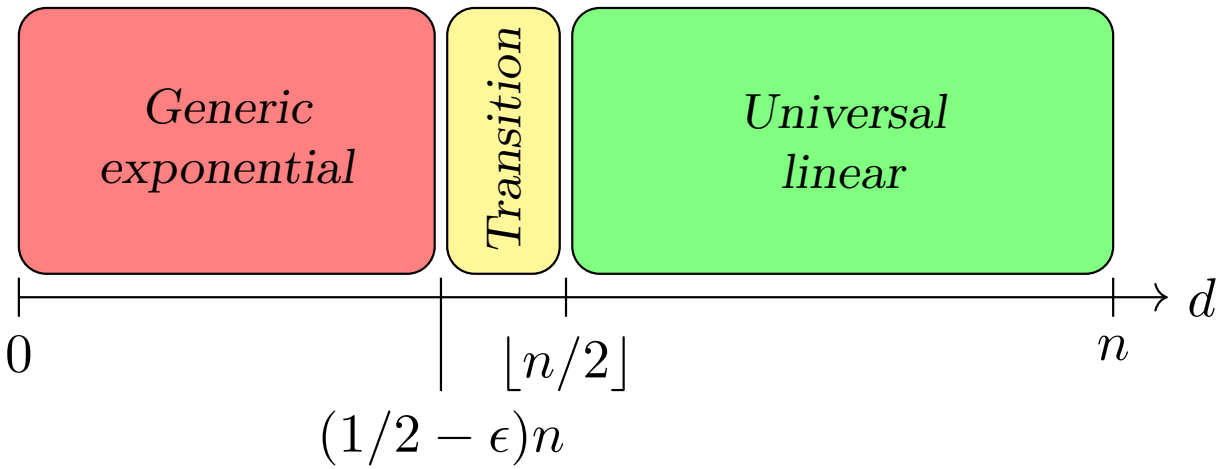
The indicators are homomorphically computed as follows (adapted from [HMR20]):



$$\left.\begin{aligned} M_{0,0} &= 1 \\ M_{i,k} &= \mathsf{MUX}\big(x_i, M_{i-1,k}, M_{i-1,k-v_i}\big) \end{aligned}\right\} \implies M_{n,k} = \mathbb{1}_{\langle \boldsymbol{v}, \boldsymbol{x} \rangle = k}$$

Generic Behavior

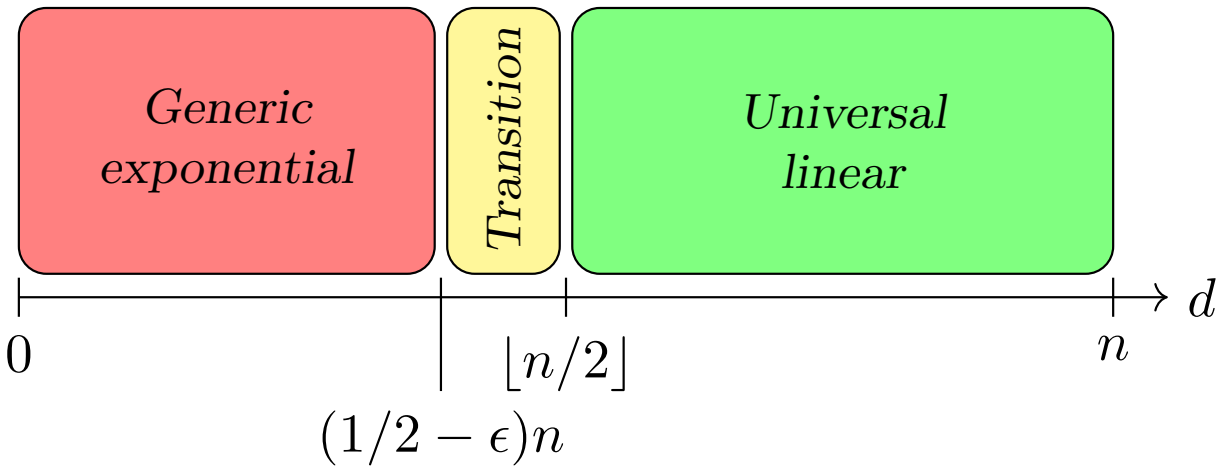
Theorem



- $d \leqslant (1/2 - \epsilon)n$: *Almost all* $f \in \mathcal{B}_n$ *have* $\kappa_d(f) = 2^{\Omega(n)}$.
- $d \geqslant \lfloor n/2 \rfloor$: *All* $f \in \mathcal{B}_n$ *have* $\kappa_d(f) \leqslant n + 1$.

Generic Behavior

Theorem



- $d \leqslant (1/2-\epsilon)n$: *Almost all* $f \in \mathcal{B}_n$ *have* $\kappa_d(f) = 2^{\Omega(n)}$.
- $d \geqslant \lfloor n/2 \rfloor$: *All* $f \in \mathcal{B}_n$ *have* $\kappa_d(f) \leqslant n+1$.

- The proposed decomposition is thus not useful for generic $f \in \mathcal{B}_n$.
- Instead, we should aim to *construct* special Boolean functions.

Generalizing Weightwise Degree-d Functions

Definition [Bry91]

The hidden-weight-bit function is the function $\mathsf{HWBF}_n \in \mathcal{B}_n$ *given by:*

$$\mathsf{HWBF}_n(\boldsymbol{x}) \coloneqq \sum_k \mathbb{1}_{w(\boldsymbol{x})=k} \cdot x_{k \bmod n}.$$

Generalizing Weightwise Degree-d Functions

Definition [Bry91]

The hidden-weight-bit function is the function $\mathsf{HWBF}_n \in \mathcal{B}_n$ *given by:*

$$\mathsf{HWBF}_n(\boldsymbol{x}) \coloneqq \sum_k \mathbb{1}_{w(\boldsymbol{x})=k} \cdot x_{k \bmod n}.$$

Definition

The hidden-weight-bit function on $\boldsymbol{v}$*-slices is the function* $\mathsf{HWBF}_n^{\boldsymbol{v}} \in \mathcal{B}_n$ *given by:*

$$\mathsf{HWBF}_n^{\boldsymbol{v}}(\boldsymbol{x}) \coloneqq \sum_k \mathbb{1}_{\langle \boldsymbol{v},\boldsymbol{x} \rangle=k} \cdot x_{k \bmod n}.$$

Parameters for Small n

Small-dimensional parameters for $\mathsf{HWBF}_n^{\boldsymbol{v}}$:

Param.	$\boldsymbol{v}$	n = 10	11	12	13	14	15	16
deg	$(1,\ldots,1)$	9	10	11	12	13	14	15
	$(1,\ldots,1,2)$	10	11	12	13	14	15	16
	$(1,2,\ldots,n)$	8	10	10	11	13	13	12
AI	$(1,\ldots,1)$	4	5	5	5	5	6	6
	$(1,\ldots,1,2)$	4	5	5	5	6	6	6
	$(1,2,\ldots,n)$	4	4	5	5	6	6	7
NL	$(1,\ldots,1)$	372	772	1 544	3 172	6 344	12 952	25 904
	$(1,\ldots,1,2)$	399	799	1 627	3 255	6 607	13 215	26 761
	$(1,2,\ldots,n)$	396	874	1 620	3 716	7 486	13 784	30 584

Takeaways & Outlook

- ***Beyond Hamming Weight:***
  Replacing $(1, \ldots, 1) \in \mathbb{Z}^n$ by a general $\boldsymbol{v} \in \mathbb{Z}^n$ yields more freedom in slicing up $\mathbb{F}_2^n$.
- ***Rich Structure:***
  The slice complexity $\kappa_d(f)$ leads to interesting new combinatorial questions, structural results, and bounds.
- ***Generic Limitation:***
  Unfortunately, almost all functions require exponentially many slices in the low-degree regime.

Takeaways & Outlook

- ***Beyond Hamming Weight:***
  Replacing $(1, \ldots, 1) \in \mathbb{Z}^n$ by a general $\boldsymbol{v} \in \mathbb{Z}^n$ yields more freedom in slicing up $\mathbb{F}_2^n$.
- ***Rich Structure:***
  The slice complexity $\kappa_d(f)$ leads to interesting new combinatorial questions, structural results, and bounds.
- ***Generic Limitation:***
  Unfortunately, almost all functions require exponentially many slices in the low-degree regime.
- ***Outlook:***
  Study how the cryptographic parameters of known weightwise degree-d functions change when $(1, \ldots, 1) \in \mathbb{Z}^n$ is replaced by a general $\boldsymbol{v} \in \mathbb{Z}^n$.

Questions?

References

[Bry91] Randal E. Bryant.
On the Complexity of VLSI Implementations and Graph Representations of Boolean Functions with Application to Integer Multiplication.
IEEE Trans. Computers, pages 205–213, 1991.

[GM22] Agnese Gini and Pierrick Méaux.
On the Weightwise Nonlinearity of Weightwise Perfectly Balanced Functions.
Discrete Applied Mathematics, 322:320–341, 2022.

[GSW13] Craig Gentry, Amit Sahai, and Brent Waters.
Homomorphic Encryption from Learning with Errors: Conceptually-Simpler, Asymptotically-Faster, Attribute-Based.
In Ran Canetti and Juan A. Garay, editors, *Advances in Cryptology - CRYPTO 2013 - 33rd Annual Cryptology Conference, Santa Barbara, CA, USA, August 18-22, 2013. Proceedings, Part I*, volume 8042 of *Lecture Notes in Computer Science*, pages 75–92. Springer, 2013.

[HMR20] Clément Hoffmann, Pierrick Méaux, and Thomas Ricosset.
Transciphering, Using FiLIP and TFHE for an Efficient Delegation of Computation.
In Karthikeyan Bhargavan, Elisabeth Oswald, and Manoj Prabhakaran, editors, *Progress in Cryptology - INDOCRYPT 2020 - 21st International Conference on Cryptology in India, Bangalore, India, December 13-16, 2020, Proceedings*, volume 12578 of *Lecture Notes in Computer Science*, pages 39–61. Springer, 2020.

[MO24] Pierrick Méaux and Yassine Ozaim.
On the Cryptographic Properties of Weightwise Affine and Weightwise Quadratic Functions.
Discret. Appl. Math., 355:13–29, 2024.

[NLV11] Michael Naehrig, Kristin Lauter, and Vinod Vaikuntanathan.
Can Homomorphic Encryption Be Practical?
In *Proceedings of the 3rd ACM Workshop on Cloud Computing Security Workshop*, CCSW '11, page 113–124, New York, NY, USA, 2011. Association for Computing Machinery.