The Revisited Hidden Weight Bit Function

Pierrick Méaux[1] **Tim Seuré**[1] Deng Tang[2]

[1]University of Luxembourg
[2]Shanghai Jiao Tong University

August 14, 2025

Motivation

- *Boolean functions* are simply maps $f : \mathbb{F}_2^n \to \mathbb{F}_2$.

Motivation

- *Boolean functions* are simply maps $f : \mathbb{F}_2^n \to \mathbb{F}_2$.
- They are crucial in symmetric cryptography.

Motivation

- *Boolean functions* are simply maps $f : \mathbb{F}_2^n \to \mathbb{F}_2$.
- They are crucial in symmetric cryptography.
- For instance, in the context of *stream ciphers*, they can be used as *filter functions* (depending on many variables).

Motivation

- *Boolean functions* are simply maps $f : \mathbb{F}_2^n \to \mathbb{F}_2$.
- They are crucial in symmetric cryptography.
- For instance, in the context of *stream ciphers*, they can be used as *filter functions* (depending on many variables).
- In that context, their cryptographic strength is linked to properties like:
  - *algebraic degree*;
  - *algebraic immunity*;
  - *balancedness*;
  - *nonlinearity*.

Motivation

- *Boolean functions* are simply maps $f : \mathbb{F}_2^n \to \mathbb{F}_2$.
- They are crucial in symmetric cryptography.
- For instance, in the context of *stream ciphers*, they can be used as *filter functions* (depending on many variables).
- In that context, their cryptographic strength is linked to properties like:
  - *algebraic degree*;
  - *algebraic immunity*;
  - *balancedness*;
  - *nonlinearity*.
- For applications in *Hybrid Homomorphic Encryption (HHE)*, the filter function should further be easy to evaluate.

The **HWBF** & our contribution

- The *Hidden Weight Bit Function (HWBF)* has been introduced in [Bry91].

The HWBF & our contribution

- The *Hidden Weight Bit Function (HWBF)* has been introduced in [Bry91].
- It is easy to evaluate (homomorphically) and has good cryptographic properties, except for its nonlinearity [WCST14].

The HWBF & our contribution

- The *Hidden Weight Bit Function (HWBF)* has been introduced in [Bry91].
- It is easy to evaluate (homomorphically) and has good cryptographic properties, except for its nonlinearity [WCST14].
- Various works have tried to alter the function to enhance its nonlinearity while preserving the other properties [Car22, CS24, MO24].

The HWBF & our contribution

- The *Hidden Weight Bit Function (HWBF)* has been introduced in [Bry91].
- It is easy to evaluate (homomorphically) and has good cryptographic properties, except for its nonlinearity [WCST14].
- Various works have tried to alter the function to enhance its nonlinearity while preserving the other properties [Car22, CS24, MO24].
- We follow a similar route and propose an excellent candidate for a new filter function in the context of HHE.

The HWBF & our contribution

- The *Hidden Weight Bit Function (HWBF)* has been introduced in [Bry91].
- It is easy to evaluate (homomorphically) and has good cryptographic properties, except for its nonlinearity [WCST14].
- Various works have tried to alter the function to enhance its nonlinearity while preserving the other properties [Car22, CS24, MO24].
- We follow a similar route and propose an excellent candidate for a new filter function in the context of HHE.
- In particular, our function has high nonlinearity, and we prove this with tools from complex analysis.

Introducing the Revisited HWBF

The *HWBF* is the function $h : \mathbb{F}_2^n \to \mathbb{F}_2$ defined by:

$$h(\boldsymbol{x}) := \sum_{i=1}^{n} x_i \cdot \mathbb{1}_{w_{\mathsf{H}}(\boldsymbol{x})=i}.$$

Introducing the Revisited HWBF

The *HWBF* is the function $h : \mathbb{F}_2^n \to \mathbb{F}_2$ defined by:

$$h(\boldsymbol{x}) \coloneqq \sum_{i=1}^{n} x_i \cdot \mathbb{1}_{w_{\mathsf{H}}(\boldsymbol{x})=i}.$$

The *Revisited HWBF* is the function $\tilde{h} : \mathbb{F}_2^n \to \mathbb{F}_2$ defined by:

$$\tilde{h}(\boldsymbol{x}) \coloneqq h(\boldsymbol{x}) + \sum_{i=1}^{n/2} (x_i + 1) x_{i+n/2}.$$

Introducing the Revisited HWBF

The *HWBF* is the function $h : \mathbb{F}_2^n \to \mathbb{F}_2$ defined by:

$$h(\boldsymbol{x}) \coloneqq \sum_{i=1}^{n} x_i \cdot \mathbb{1}_{w_{\mathsf{H}}(\boldsymbol{x})=i}.$$

The *Revisited HWBF* is the function $\tilde{h} : \mathbb{F}_2^n \to \mathbb{F}_2$ defined by:

$$\tilde{h}(\boldsymbol{x}) \coloneqq h(\boldsymbol{x}) + \sum_{i=1}^{n/2} (x_i + 1) x_{i+n/2}.$$

Therefore $\tilde{h} = h + d \circ \pi + g$, where:

- $d : \mathbb{F}_2^n \to \mathbb{F}_2$ is defined by $d(\boldsymbol{x}) \coloneqq \sum_{i=1}^{n/2} x_{2i-1} \cdot x_{2i}$;
- $\pi : \mathbb{F}_2^n \to \mathbb{F}_2^n$ permutes the indices;
- $g : \mathbb{F}_2^n \to \mathbb{F}_2$ is a sum of linear terms.

Algebraic degree & algebraic immunity

The Revisited HWBF satisfies:

- $\mathsf{deg}(\tilde{h}) = \mathsf{deg}(h) = n - 1$ if $n \geqslant 4$

Algebraic degree & algebraic immunity

The Revisited HWBF satisfies:

- $\mathsf{deg}(\tilde{h}) = \mathsf{deg}(h) = n - 1$ if $n \geqslant 4$;
- $\mathsf{AI}(\tilde{h}) \geqslant \mathsf{AI}(h) - 2$.

Algebraic degree & algebraic immunity

The Revisited HWBF satisfies:

- $\mathsf{deg}(\tilde{h}) = \mathsf{deg}(h) = n - 1$ if $n \geqslant 4$;
- $\mathsf{AI}(\tilde{h}) \geqslant \mathsf{AI}(h) - 2$.

What about balancedness and nonlinearity?

Walsh transform

The *Walsh transform* of weight $k \in [0, n]$ of a function $f : \mathbb{F}_2^n \to \mathbb{F}_2$ at $\boldsymbol{a} \in \mathbb{F}_2^n$ is defined by:

$$\mathcal{W}_{f,k}(\boldsymbol{a}) \coloneqq \sum_{w_{\mathsf{H}}(\boldsymbol{x})=k} (-1)^{f(\boldsymbol{x})+\langle \boldsymbol{a},\boldsymbol{x} \rangle}.$$

Walsh transform

The *Walsh transform* of weight $k \in [0, n]$ of a function $f : \mathbb{F}_2^n \to \mathbb{F}_2$ at $\boldsymbol{a} \in \mathbb{F}_2^n$ is defined by:

$$\mathcal{W}_{f,k}(\boldsymbol{a}) \coloneqq \sum_{w_{\mathsf{H}}(\boldsymbol{x})=k} (-1)^{f(\boldsymbol{x})+\langle \boldsymbol{a},\boldsymbol{x}\rangle}.$$

The *unrestricted Walsh transform* is defined by:

$$\mathcal{W}_{f}(\boldsymbol{a}) \coloneqq \sum_{k=0}^{n} \mathcal{W}_{f,k}(\boldsymbol{a}).$$

Walsh transform

The *Walsh transform* of weight $k \in [0, n]$ of a function $f : \mathbb{F}_2^n \to \mathbb{F}_2$ at $\boldsymbol{a} \in \mathbb{F}_2^n$ is defined by:

$$\mathcal{W}_{f,k}(\boldsymbol{a}) \coloneqq \sum_{w_{\mathsf{H}}(\boldsymbol{x})=k} (-1)^{f(\boldsymbol{x})+\langle \boldsymbol{a},\boldsymbol{x}\rangle}.$$

The *unrestricted Walsh transform* is defined by:

$$\mathcal{W}_f(\boldsymbol{a}) \coloneqq \sum_{k=0}^{n} \mathcal{W}_{f,k}(\boldsymbol{a}).$$

Properties

- *f is balanced if and only if $\mathcal{W}_f(\mathbf{0}) = 0$.*
- *The nonlinearity of f can be computed as:*

$$\mathsf{NL}(f) = 2^{n-1} - \frac{1}{2} \max_{\boldsymbol{a} \in \mathbb{F}_2^n} |\mathcal{W}_f(\boldsymbol{a})|.$$

Balancedness

For the Revisited HWBF:

Theorem

- *If* $n = 4m + 2$, *then* $\mathcal{W}_{\tilde{h}}(\mathbf{0}) = -2\binom{2m}{m}$.
- *If* $n = 4m$, *then* $\mathcal{W}_{\tilde{h}}(\mathbf{0}) = 0$.

Therefore, $\tilde{h}$ *is balanced if and only if* $n \equiv 0 \bmod 4$.

Balancedness

For the Revisited HWBF:

Theorem

- *If* $n = 4m + 2$, *then* $\mathcal{W}_{\tilde{h}}(\mathbf{0}) = -2\binom{2m}{m}$.
- *If* $n = 4m$, *then* $\mathcal{W}_{\tilde{h}}(\mathbf{0}) = 0$.

Therefore, $\tilde{h}$ *is balanced if and only if* $n \equiv 0 \bmod 4$.

We proved this by relating $\mathcal{W}_{\tilde{h},k}$ to $\mathcal{W}_{d,k}$.

From $\tilde{h}$ to d

Lemma

For every $\boldsymbol{a} \in \mathbb{F}_2^n$ *and every* k*, there exists a* $\boldsymbol{b} \in \mathbb{F}_2^n$ *such that:*

$$\mathcal{W}_{\tilde{h},k}(\boldsymbol{a}) = \mathcal{W}_{d,k}(\boldsymbol{b}).$$

The result remains true if we replace $\tilde{h}$ *by a function which is weightwise quadratic with* $n/2$ *quadratic terms in direct sum on each slice.*

From $\tilde{h}$ to d

Lemma

For every $\boldsymbol{a} \in \mathbb{F}_2^n$ and every k, there exists a $\boldsymbol{b} \in \mathbb{F}_2^n$ such that:

$$\mathcal{W}_{\tilde{h},k}(\boldsymbol{a}) = \mathcal{W}_{d,k}(\boldsymbol{b}).$$

The result remains true if we replace $\tilde{h}$ by a function which is weightwise quadratic with $n/2$ quadratic terms in direct sum on each slice.

Let us find a bound $|\mathcal{W}_{d,k}(\boldsymbol{b})| \leqslant B_n$ that works for every $\boldsymbol{b} \in \mathbb{F}_2^n$ and every k.

From $\tilde{h}$ to d

Lemma

For every $\boldsymbol{a} \in \mathbb{F}_2^n$ and every k, there exists a $\boldsymbol{b} \in \mathbb{F}_2^n$ such that:

$$\mathcal{W}_{\tilde{h},k}(\boldsymbol{a}) = \mathcal{W}_{d,k}(\boldsymbol{b}).$$

The result remains true if we replace $\tilde{h}$ by a function which is weightwise quadratic with $n/2$ quadratic terms in direct sum on each slice.

Let us find a bound $|\mathcal{W}_{d,k}(\boldsymbol{b})| \leqslant B_n$ that works for every $\boldsymbol{b} \in \mathbb{F}_2^n$ and every k. Then:

$$|\mathcal{W}_{\tilde{h}}(\boldsymbol{a})| \leqslant \sum_{k=0}^{n} |\mathcal{W}_{\tilde{h},k}(\boldsymbol{a})| \leqslant (n+1)B_n.$$

Generating function

For this, we study the following generating function, with $\boldsymbol{a} \in \mathbb{F}_2^n$:

$$P_{\boldsymbol{a}}(z) := \sum_{k \geqslant 0} \mathcal{W}_{d,k}(\boldsymbol{a}) z^k.$$

Generating function

For this, we study the following generating function, with $\boldsymbol{a} \in \mathbb{F}_2^n$:

$$P_{\boldsymbol{a}}(z) := \sum_{k \geqslant 0} \mathcal{W}_{d,k}(\boldsymbol{a}) z^k.$$

We can express it in terms of three integers:

$$\begin{aligned} p &:= \#\{i \in [1, n/2] \mid (a_{2i-1}, a_{2i}) = (1,1)\}, \\ q &:= \#\{i \in [1, n/2] \mid (a_{2i-1}, a_{2i}) = (0,0)\}, \\ r &:= \#\{i \in [1, n/2] \mid (a_{2i-1}, a_{2i}) = (0,1) \text{ or } (1,0)\}. \end{aligned}$$

Generating function

For this, we study the following generating function, with $\boldsymbol{a} \in \mathbb{F}_2^n$:

$$P_{\boldsymbol{a}}(z) := \sum_{k \geqslant 0} \mathcal{W}_{d,k}(\boldsymbol{a}) z^k.$$

We can express it in terms of three integers:

$$\begin{aligned} p &:= \#\{i \in [1, n/2] \mid (a_{2i-1}, a_{2i}) = (1,1)\}, \\ q &:= \#\{i \in [1, n/2] \mid (a_{2i-1}, a_{2i}) = (0,0)\}, \\ r &:= \#\{i \in [1, n/2] \mid (a_{2i-1}, a_{2i}) = (0,1) \text{ or } (1,0)\}. \end{aligned}$$

Proposition

$$P_{\boldsymbol{a}}(z) = \left(-z^2 + 2z + 1\right)^p \left(-z^2 - 2z + 1\right)^q \left(z^2 + 1\right)^r$$

Cauchy's estimate

- Recall that $\sum_{k \geqslant 0} \mathcal{W}_{d,k}(\boldsymbol{a}) z^k = P_{\boldsymbol{a}}(z)$.

Cauchy's estimate

- Recall that $\sum_{k\geqslant 0} \mathcal{W}_{d,k}(\boldsymbol{a}) z^k = P_{\boldsymbol{a}}(z)$.
- Therefore:

$$k! \cdot \mathcal{W}_{d,k}(\boldsymbol{a}) = \frac{\mathrm{d}^k}{\mathrm{d}^k z} P_{\boldsymbol{a}}(z)|_{z=0}.$$

Cauchy's estimate

- Recall that $\sum_{k \geqslant 0} \mathcal{W}_{d,k}(\boldsymbol{a}) z^k = P_{\boldsymbol{a}}(z)$.
- Therefore:

$$k! \cdot \mathcal{W}_{d,k}(\boldsymbol{a}) = \frac{\mathrm{d}^k}{\mathrm{d}^k z} P_{\boldsymbol{a}}(z)|_{z=0}.$$

- On the other hand, by Cauchy's estimate:

$$\left| \frac{\mathrm{d}^k}{\mathrm{d}^k z} P_{\boldsymbol{a}}(z)|_{z=0} \right| \leqslant k! \cdot \max_{|z|=1} |P_{\boldsymbol{a}}(z)| \leqslant k! \cdot 2^{3n/4}.$$

Cauchy's estimate

- Recall that $\sum_{k \geqslant 0} \mathcal{W}_{d,k}(\boldsymbol{a}) z^k = P_{\boldsymbol{a}}(z)$.
- Therefore:

$$k! \cdot \mathcal{W}_{d,k}(\boldsymbol{a}) = \frac{\mathrm{d}^k}{\mathrm{d}^k z} P_{\boldsymbol{a}}(z)|_{z=0}.$$

- On the other hand, by Cauchy's estimate:

$$\left| \frac{\mathrm{d}^k}{\mathrm{d}^k z} P_{\boldsymbol{a}}(z)|_{z=0} \right| \leqslant k! \cdot \max_{|z|=1} |P_{\boldsymbol{a}}(z)| \leqslant k! \cdot 2^{3n/4}.$$

Theorem

For every $\boldsymbol{a} \in \mathbb{F}_2^n$ and every k, we have:

$$|\mathcal{W}_{d,k}(\boldsymbol{a})| \leqslant 2^{3n/4}.$$

Bounds on the Walsh transform of $\tilde{h}$

Corollary

$$\max_{\boldsymbol{a}\in\mathbb{F}_2^n} |\mathcal{W}_{\tilde{h}}(\boldsymbol{a})| \leqslant (n+1)\cdot 2^{3n/4}$$

Bounds on the Walsh transform of $\tilde{h}$

Corollary

$$\max_{\boldsymbol{a} \in \mathbb{F}_2^n} |\mathcal{W}_{\tilde{h}}(\boldsymbol{a})| \leqslant (n+1) \cdot 2^{3n/4}$$

$f : \mathbb{F}_2^n \to \mathbb{F}_2$	$\frac{1}{n} \log_2(\max_{\boldsymbol{a}} \lvert\mathcal{W}_f(\boldsymbol{a})\rvert)$
$\tilde{h}$	$\frac{3}{4} + o(1)$
h	$1 + o(1)$
Maj	$1 + o(1)$
Bent functions	$\frac{1}{2} + o(1)$

Generalization

Theorem

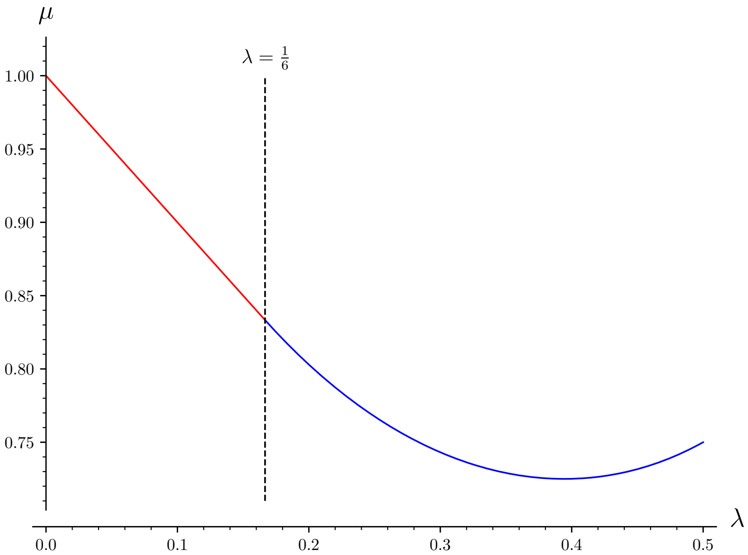
For a function $f : \mathbb{F}_2^n \to \mathbb{F}_2$ which is weightwise quadratic with $t \in [0, n/2]$ quadratic terms in direct sum on each slice, we have:

$$\frac{1}{n} \log_2(\max_{\boldsymbol{a} \in \mathbb{F}_2^n} |\mathcal{W}_f(\boldsymbol{a})|) \leqslant \mu + o(1),$$

where μ only depends on $\lambda \coloneqq t/n$:

$$\mu \coloneqq \begin{cases} \frac{\lambda+1}{2} + \frac{1}{2} \log_2\left(\frac{\left(-\lambda^2+2\lambda+\lambda\sqrt{\lambda^2-4\lambda+2}\right)^{\lambda}}{\left(1-\lambda+\sqrt{\lambda^2-4\lambda+2}\right)^{2\lambda-1}} \right) & \text{if } \lambda > \frac{1}{6}, \\ 1-\lambda & \text{if } \lambda \leqslant \frac{1}{6}. \end{cases}$$

Generalization



And more

The paper also contains:

- tighter nonlinearity bounds for $\tilde{h}$, for small n;

And more

The paper also contains:

- tighter nonlinearity bounds for $\tilde{h}$, for small n;
- some curiosities about $\mathcal{W}_{d,k}$;

And more

The paper also contains:

- tighter nonlinearity bounds for $\tilde{h}$, for small n;
- some curiosities about $\mathcal{W}_{d,k}$;
- ...

Takeaways

- Nonlinearity bounds for a wide variety of weightwise quadratic functions have been found.

Takeaways

- Nonlinearity bounds for a wide variety of weightwise quadratic functions have been found.
- Techniques from complex analysis can be used to study Boolean functions.

Takeaways

- Nonlinearity bounds for a wide variety of weightwise quadratic functions have been found.
- Techniques from complex analysis can be used to study Boolean functions.
- It's a lot of fun!

Questions?

References

[Bry91] Randal Bryant.
On the Complexity of VLSI Implementations and Graph Representations of Boolean Functions with Application to Integer Multiplication.
IEEE Transactions on Computers, 40, 1991.

[Car22] Claude Carlet.
A Wide Class of Boolean Functions Generalizing the Hidden Weight Bit Function.
IEEE Transactions on Information Theory, 68, 2022.

[CS24] Claude Carlet and Palash Sarkar.
Constructions of Efficiently Implementable Boolean Functions Possessing High Nonlinearity and Good Resistance to Algebraic Attacks, 2024.
https://eprint.iacr.org/2024/1305.

[MO24] Pierrick Méaux and Yassine Ozaim.
On the Cryptographic Properties of Weightwise Affine and Weightwise Quadratic Functions.
Discrete Applied Mathematics, 355, 2024.

[WCST14] Qichun Wang, Claude Carlet, Pante Stănică, and Chik How Tan.
Cryptographic Properties of the Hidden Weighted Bit Function.
Discrete Applied Mathematics, 174, 2014.