

On the Differential Uniformity of Polynomials over Galois Rings

Sondre Rønjom and Arne Sandrib



Table of contents

- 1 Overview**
- 2 Motivation
- 3 Preliminaries
- 4 Differential Uniformity in $GR(p^k, m)$
- 5 Differential Uniformity of Non-polynomial Functions**
- 6 References



Motivation



Motivation

- Growing interest in ring based technologies:



Motivation

- Growing interest in ring based technologies:
 - Used in high function crypto: MPC, FHE, and zk proofs.
 - Compatibility with lattice based cryptography.
 - Elisabeth for FHE [Cos+22]



Motivation

- Growing interest in ring based technologies:
 - Used in high function crypto: MPC, FHE, and zk proofs.
 - Compatibility with lattice based cryptography.
 - Elisabeth for FHE [Cos+22]
 - 'More Efficient Zero-Knowledge Protocols over \mathbb{Z}_{2^k} via Galois Rings' [LXY23]



Motivation

- Growing interest in ring based technologies:
 - Used in high function crypto: MPC, FHE, and zk proofs.
 - Compatibility with lattice based cryptography.
 - Elisabeth for FHE [Cos+22]
 - 'More Efficient Zero-Knowledge Protocols over \mathbb{Z}_{2^k} via Galois Rings' [LXY23]
 - 'Transparent SNARKs using Galois rings' [WZD25].



Motivation

- Growing interest in ring based technologies:
 - Used in high function crypto: MPC, FHE, and zk proofs.
 - Compatibility with lattice based cryptography.
 - Elisabeth for FHE [Cos+22]
 - 'More Efficient Zero-Knowledge Protocols over \mathbb{Z}_{2^k} via Galois Rings' [LXY23]
 - 'Transparent SNARKs using Galois rings' [WZD25].
- Universal hash functions over Galois fields and Galois rings [HJ96]



Motivation

- Growing interest in ring based technologies:
 - Used in high function crypto: MPC, FHE, and zk proofs.
 - Compatibility with lattice based cryptography.
 - Elisabeth for FHE [Cos+22]
 - 'More Efficient Zero-Knowledge Protocols over \mathbb{Z}_{2^k} via Galois Rings' [LXY23]
 - 'Transparent SNARKs using Galois rings' [WZD25].
- Universal hash functions over Galois fields and Galois rings [HJ96]
- Not an active area of research



Motivation

- Growing interest in ring based technologies:
 - Used in high function crypto: MPC, FHE, and zk proofs.
 - Compatibility with lattice based cryptography.
 - Elisabeth for FHE [Cos+22]
 - 'More Efficient Zero-Knowledge Protocols over \mathbb{Z}_{2^k} via Galois Rings' [LXY23]
 - 'Transparent SNARKs using Galois rings' [WZD25].
- Universal hash functions over Galois fields and Galois rings [HJ96]
- Not an active area of research
- Finite rings have a different algebraic structure than finite fields



Motivation

- Growing interest in ring based technologies:
 - Used in high function crypto: MPC, FHE, and zk proofs.
 - Compatibility with lattice based cryptography.
 - Elisabeth for FHE [Cos+22]
 - 'More Efficient Zero-Knowledge Protocols over \mathbb{Z}_{2^k} via Galois Rings' [LXY23]
 - 'Transparent SNARKs using Galois rings' [WZD25].
- Universal hash functions over Galois fields and Galois rings [HJ96]
- Not an active area of research
- Finite rings have a different algebraic structure than finite fields
- There are less known attacks against ring ciphers



Motivation

- Growing interest in ring based technologies:
 - Used in high function crypto: MPC, FHE, and zk proofs.
 - Compatibility with lattice based cryptography.
 - Elisabeth for FHE [Cos+22]
 - 'More Efficient Zero-Knowledge Protocols over \mathbb{Z}_{2^k} via Galois Rings' [LXY23]
 - 'Transparent SNARKs using Galois rings' [WZD25].
- Universal hash functions over Galois fields and Galois rings [HJ96]
- Not an active area of research
- Finite rings have a different algebraic structure than finite fields
- There are less known attacks against ring ciphers
- More versatility in future designs. One specification for both $GF(p^k, m)$ and $GR(p^k, m)$?



Motivation

- Growing interest in ring based technologies:
 - Used in high function crypto: MPC, FHE, and zk proofs.
 - Compatibility with lattice based cryptography.
 - Elisabeth for FHE [Cos+22]
 - 'More Efficient Zero-Knowledge Protocols over \mathbb{Z}_{2^k} via Galois Rings' [LXY23]
 - 'Transparent SNARKs using Galois rings' [WZD25].
- Universal hash functions over Galois fields and Galois rings [HJ96]
- Not an active area of research
- Finite rings have a different algebraic structure than finite fields
- There are less known attacks against ring ciphers
- More versatility in future designs. One specification for both $GF(p^k, m)$ and $GR(p^k, m)$?
- Possibly better resistance against differential cryptanalysis?



Preliminaries

Galois Rings



Galois Rings

Definition

Let p be prime and $k, m \geq 1$, $g(x)$ a monic irreducible polynomial over \mathbb{Z}_p of degree m . Define

$$R_{q^m} := \text{GR}(p^k, m) = \mathbb{Z}_{p^k}[z]/(g(z)).$$



Galois Rings

Definition

Let p be prime and $k, m \geq 1$, $g(x)$ a monic irreducible polynomial over \mathbb{Z}_p of degree m . Define

$$R_{q^m} := \text{GR}(p^k, m) = \mathbb{Z}_{p^k}[z]/(g(z)).$$

Remark

- Setting $k = 1$ gives the usual Galois field $\text{GR}(p, m) = \text{GF}(p^m)$.
- The ideal (p) is the only maximal ideal in R_{q^m} , hence for any k , $\text{GR}(p^k, m)/(p) \cong \text{GF}(p^m)$.
- Setting $m = 1$ gives \mathbb{Z}_{p^k}



Permutation Polynomials

Definition

A polynomial $f(x) \in R_{q^m}[x]$ is called a *permutation polynomial* if the induced function is a permutation of R_{q^m} .



Differential Uniformity

Definition

For a function $f(x)$ over a finite field \mathbb{F}_{p^m} , define

$$\delta_f(a, b) = |\{x \in \mathbb{F}_{p^m} \mid f(x+a) - f(x) = b\}|.$$

The differential uniformity of f is $\Delta_f = \max_{a \neq 0, b} \delta_f(a, b)$.



Differential Uniformity

Definition

For a function $f(x)$ over a finite field \mathbb{F}_{p^m} , define

$$\delta_f(a, b) = |\{x \in \mathbb{F}_{p^m} \mid f(x+a) - f(x) = b\}|.$$

The differential uniformity of f is $\Delta_f = \max_{a \neq 0, b} \delta_f(a, b)$.

- Measures resistance against differential attacks.



Differential Uniformity

Definition

For a function $f(x)$ over a finite field \mathbb{F}_{p^m} , define

$$\delta_f(a, b) = |\{x \in \mathbb{F}_{p^m} \mid f(x+a) - f(x) = b\}|.$$

The differential uniformity of f is $\Delta_f = \max_{a \neq 0, b} \delta_f(a, b)$.

- Measures resistance against differential attacks.
- In binary finite fields, $\Delta_f \geq 2$. If $\Delta_f = 2$, then f is called Almost perfect nonlinear (APN).



Differential Uniformity

Definition

For a function $f(x)$ over a finite field \mathbb{F}_{p^m} , define

$$\delta_f(a, b) = |\{x \in \mathbb{F}_{p^m} \mid f(x+a) - f(x) = b\}|.$$

The differential uniformity of f is $\Delta_f = \max_{a \neq 0, b} \delta_f(a, b)$.

- Measures resistance against differential attacks.
- In binary finite fields, $\Delta_f \geq 2$. If $\Delta_f = 2$, then f is called Almost perfect nonlinear (APN).
- Defined analogously for Galois rings.



Differential Uniformity

Definition

For a function $f(x)$ over a finite field \mathbb{F}_{p^m} , define

$$\delta_f(a, b) = |\{x \in \mathbb{F}_{p^m} \mid f(x+a) - f(x) = b\}|.$$

The differential uniformity of f is $\Delta_f = \max_{a \neq 0, b} \delta_f(a, b)$.

- Measures resistance against differential attacks.
- In binary finite fields, $\Delta_f \geq 2$. If $\Delta_f = 2$, then f is called Almost perfect nonlinear (APN).
- Defined analogously for Galois rings.
- In Galois rings, we may have $\delta_f(a, b) = 1$, giving trivial bound $\Delta_f \geq 1$. If $\Delta_f = 1$, then f is called perfect nonlinear (PN).



Differential Uniformity in $\text{GR}(p^k, m)$

Lower Bound on Differential Uniformity for Polynomial Functions



Lower Bound on Differential Uniformity for Polynomial Functions

Proposition

Suppose that $f(x) \in R_{q^m}[x]$ with $k > 1$. Then $\Delta_f \geq |(p)| = p^{m(k-1)}$.



Lower Bound on Differential Uniformity for Polynomial Functions

Proposition

Suppose that $f(x) \in R_{q^m}[x]$ with $k > 1$. Then $\Delta_f \geq |(p)| = p^{m(k-1)}$.

Proposition

Suppose that $f(x) \in R_{q^m}[x]$ is a permutation polynomial and $k > 1$. Then $\Delta_f \geq 2|(p)| = 2p^{m(k-1)}$.



Lower Bound on Differential Uniformity for Polynomial Functions

Proposition

Suppose that $f(x) \in R_{q^m}[x]$ with $k > 1$. Then $\Delta_f \geq |(p)| = p^{m(k-1)}$.

Proposition

Suppose that $f(x) \in R_{q^m}[x]$ is a permutation polynomial and $k > 1$. Then $\Delta_f \geq 2|(p)| = 2p^{m(k-1)}$.

Definition

Let f be a polynomial function over a Galois ring $R_{q^m}[x]$. We say that

- 1 f is *poly-APN* if $\Delta_f = p^{m(k-1)}$;
- 2 f is *permutation-poly-APN* (*ppoly-APN*) if $\Delta_f = 2p^{m(k-1)}$ and f is a permutation.

Consequence of Bounds



Consequence of Bounds

Proposition

Suppose that $f(x) \in R_{q^m}[x]$ is a permutation polynomial and $k > 1$. Then $\Delta_f \geq 2|(p)| = 2p^{m(k-1)}$.



Consequence of Bounds

Proposition

Suppose that $f(x) \in R_{q^m}[x]$ is a permutation polynomial and $k > 1$. Then $\Delta_f \geq 2|(p)| = 2p^{m(k-1)}$.

- The differential probability of $f(x)$ becomes independent of k in the Galois ring setting, where $\max_{a \neq 0, b} DP(a, b) = 2p^{-m}$.



Consequence of Bounds

Proposition

Suppose that $f(x) \in R_{q^m}[x]$ is a permutation polynomial and $k > 1$. Then $\Delta_f \geq 2|(p)| = 2p^{m(k-1)}$.

- The differential probability of $f(x)$ becomes independent of k in the Galois ring setting, where $\max_{a \neq 0, b} DP(a, b) = 2p^{-m}$.
- In contrast, the maximal differential probability generally decreases when the field size increases for finite fields.



Differential Uniformity of Non-polynomial Functions

APN Permutations over R_{4^2}



APN Permutations over R_{4^2}

- Most functions over R_{q^m} do not admit polynomial representation.



APN Permutations over R_{4^2}

- Most functions over R_{q^m} do not admit polynomial representation.
- For cryptographic applications requiring low differential uniformity this may be the right path forward.



APN Permutations over R_{4^2}

- Most functions over R_{q^m} do not admit polynomial representation.
- For cryptographic applications requiring low differential uniformity this may be the right path forward.

Order R_{4^2} by $0, 1, \dots, 3z + 2, 3z + 3$. Consider the function $S = [6, 0, 5, 14, 12, 13, 7, 9, 3, 4, 11, 2, 15, 8, 10, 1]$ which is APN, as it has DDT

16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	1	2	0	0	2	1	1	2	1	1	0	2	1	2
0	1	0	1	1	1	2	0	2	2	0	2	1	0	2	1
0	2	1	0	0	2	1	2	1	1	1	2	0	1	2	0
0	2	1	0	1	2	0	2	1	2	1	1	2	1	0	0
0	0	1	0	0	1	1	2	1	1	2	1	2	1	1	2
0	2	0	1	2	2	0	1	0	2	2	1	1	0	1	1
0	1	2	2	1	0	1	0	2	1	1	1	1	1	2	0
0	1	0	1	2	1	1	2	2	0	0	0	2	2	1	1
0	1	2	2	1	2	1	2	0	1	0	0	1	1	1	1
0	1	2	1	1	1	2	0	2	0	2	0	1	0	2	1
0	2	2	1	1	1	1	1	0	0	0	1	1	2	1	2
0	0	1	2	2	0	0	1	1	1	1	2	1	2	0	2
0	2	2	1	1	0	2	1	2	1	1	1	1	0	1	0
0	1	0	2	1	1	1	0	0	1	2	2	2	1	0	2
0	0	1	0	2	2	1	1	1	1	2	1	0	2	1	1

Table: The DDT of S



Conclusion



Conclusion

- One should avoid univariate Galois Ring polynomials when striving for low differential uniformity.



Conclusion

- One should avoid univariate Galois Ring polynomials when striving for low differential uniformity.
- Table-based permutations may result in highly nonlinear functions



Conclusion

- One should avoid univariate Galois Ring polynomials when striving for low differential uniformity.
- Table-based permutations may result in highly nonlinear functions
- Open questions



Conclusion

- One should avoid univariate Galois Ring polynomials when striving for low differential uniformity.
- Table-based permutations may result in highly nonlinear functions
- Open questions
 - Can we identify classes of APN functions?



Conclusion

- One should avoid univariate Galois Ring polynomials when striving for low differential uniformity.
- Table-based permutations may result in highly nonlinear functions
- Open questions
 - Can we identify classes of APN functions?
 - Do PN functions exist over Galois rings?



Conclusion

- One should avoid univariate Galois Ring polynomials when striving for low differential uniformity.
- Table-based permutations may result in highly nonlinear functions
- Open questions
 - Can we identify classes of APN functions?
 - Do PN functions exist over Galois rings?
 - What technologies may benefit from transitioning to Galois rings?



References I

- [Cos+22] Orel Cosseron et al. *Towards Globally Optimized Hybrid Homomorphic Encryption - Featuring the Elisabeth Stream Cipher*. Cryptology ePrint Archive, Paper 2022/180. 2022. URL: <https://eprint.iacr.org/2022/180>.
- [HJ96] Tor Helleseth and Thomas Johansson. 'Universal Hash Functions from Exponential Sums over Finite Fields and Galois Rings'. In: *Advances in Cryptology — CRYPTO '96*. Ed. by Neal Koblitz. Berlin, Heidelberg: Springer Berlin Heidelberg, 1996, pp. 31–44. ISBN: 978-3-540-68697-2.
- [LXY23] Fuchun Lin, Chaoping Xing and Yizhou Yao. *More Efficient Zero-Knowledge Protocols over \mathbb{Z}_{2^k} via Galois Rings*. Cryptology ePrint Archive, Paper 2023/150. 2023. URL: <https://eprint.iacr.org/2023/150>.



References II

- [WZD25] Yuanju Wei, Xinxuan Zhang and Yi Deng. *Transparent SNARKs over Galois Rings*. *Cryptology ePrint Archive*, Paper 2025/263. 2025. URL: <https://eprint.iacr.org/2025/263>.

