The Role of Permutations in Cryptographic Hash Functions

Liljana Babinkostova, Dmitriy Khripkov, Nicholas Lacasse, Bai Lin, Michelle Mastrianni

REU 2015: Complexity Across Disciplines

November 16, 2015

Overview

What is a Hash Function?

A *hash function* takes digital data of arbitrary length and outputs data of a fixed length. (The output is called the *hash value*.)

What is a Hash Function?

A *hash function* takes digital data of arbitrary length and outputs data of a fixed length. (The output is called the *hash value*.)

A good hash function is *collision resistant*, meaning it is hard to find two inputs that hash to the same output.

What is a Hash Function?

A *hash function* takes digital data of arbitrary length and outputs data of a fixed length. (The output is called the *hash value*.)

A good hash function is *collision resistant*, meaning it is hard to find two inputs that hash to the same output.

A good *cryptographic hash function* is practically impossible to invert.

Permutations

$$\begin{pmatrix} 0 & 1 & 2 & 3 & 4 \\ 3 & 4 & 0 & 1 & 2 \end{pmatrix}$$

Permutations

$$\begin{pmatrix} 0 & 1 & 2 & 3 & 4 \\ 3 & 4 & 0 & 1 & 2 \end{pmatrix}$$

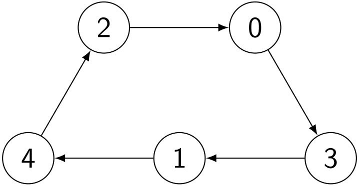
$$\begin{pmatrix} \cancel{0\ 1\ 2\ 3\ 4} \\ 3\ 4\ 0\ 1\ 2 \end{pmatrix}$$

Permutations

Three different representations

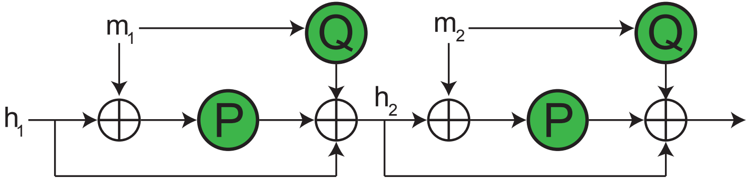
$$\begin{pmatrix} 0 & 1 & 2 & 3 & 4 \\ 3 & 4 & 0 & 1 & 2 \end{pmatrix}$$

$$\begin{pmatrix} 3 & 4 & 0 & 1 & 2 \end{pmatrix}$$

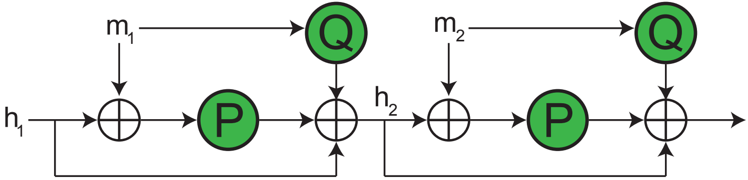


The Grøstl Hash Function

The Grøstl Hash Function

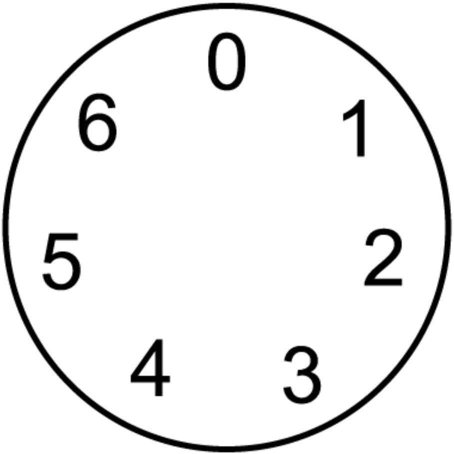


The Grøstl Hash Function



The Question: When is $P \oplus Q$ a Permutation?

Modular (Clock) Arithmetic



Sums of Permutations

$$
\begin{array}{r}
\begin{pmatrix} 1 & 0 & 2 & 4 & 3 \end{pmatrix} \\
+\begin{pmatrix} 2 & 1 & 0 & 4 & 3 \end{pmatrix} \\
\hline
\Big(\qquad\qquad\qquad\qquad
\end{array}
$$

Sums of Permutations

$$
\begin{array}{r}
\left(\begin{array}{ccccc} 1 & 0 & 2 & 4 & 3 \end{array}\right) \\
+\left(\begin{array}{ccccc} 2 & 1 & 0 & 4 & 3 \end{array}\right) \\
\hline
\left(\begin{array}{ccccc} 3 & & & & \end{array}\right.
\end{array}
$$

Sums of Permutations

$$
\begin{array}{r}
\begin{pmatrix} 1 & 0 & 2 & 4 & 3 \end{pmatrix} \\
+\begin{pmatrix} 2 & 1 & 0 & 4 & 3 \end{pmatrix} \\
\hline
\left(3 \; 1 \right.
\end{array}
$$

Sums of Permutations

$$
\begin{array}{r}
\begin{pmatrix} 1 & 0 & 2 & 4 & 3 \end{pmatrix} \\
+ \begin{pmatrix} 2 & 1 & 0 & 4 & 3 \end{pmatrix} \\
\hline
\left(\begin{matrix} 3 & 1 & 2 & & \end{matrix} \right.
\end{array}
$$

Sums of Permutations

$$
\begin{array}{r}
(\,1\ 0\ 2\ 4\ 3\,) \\
+\,(\,2\ 1\ 0\ 4\ 3\,) \\
\hline
(\,3\ 1\ 2\ 3\ \,
\end{array}
$$

Sums of Permutations

$$
\begin{array}{r}
\begin{pmatrix} 1 & 0 & 2 & 4 & 3 \end{pmatrix} \\
+\begin{pmatrix} 2 & 1 & 0 & 4 & 3 \end{pmatrix} \\
\hline
\begin{pmatrix} 3 & 1 & 2 & 3 & 1 \end{pmatrix}
\end{array}
$$

Research Questions

Research Questions

- When is the sum of two permutations a permutation?

Research Questions

- When is the sum of two permutations a permutation?
- Do they exist?

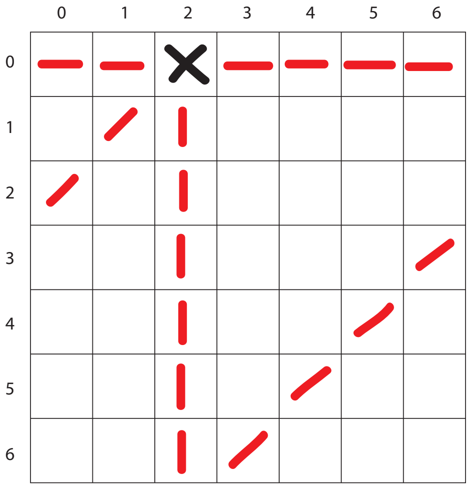
Research Questions

- When is the sum of two permutations a permutation?
- Do they exist?
- If they exist, can we count them?

Research Questions

- When is the sum of two permutations a permutation?
- Do they exist?
- If they exist, can we count them?
- How can we construct them?

Toroidal Chessboard Construction Tool



Near Permutations

$$
\begin{array}{rcccccccccccc}
 & (6 & 5 & 7 & 3 & 2 & 0 & 11 & 4 & 10 & 9 & 8 & 1) \\
\oplus & (7 & 9 & 8 & 1 & 3 & 5 & 6 & 4 & 11 & 0 & 2 & 10) \\
\hline
\end{array}
$$

Near Permutations

$$
\begin{array}{cc}
 & (6 \quad 5 \quad 7 \quad 3 \quad 2 \quad 0 \quad 11 \quad 4 \quad 10 \quad 9 \quad 8 \quad 1) \\
\oplus & (7 \quad 9 \quad 8 \quad 1 \quad 3 \quad 5 \quad 6 \quad 4 \quad 11 \quad 0 \quad 2 \quad 10) \\
\hline
 & (1 \quad 2 \quad 3 \quad 4 \quad 5 \quad 5 \quad 5 \quad 8 \quad 9 \quad 9 \quad 10 \quad 11)
\end{array}
$$

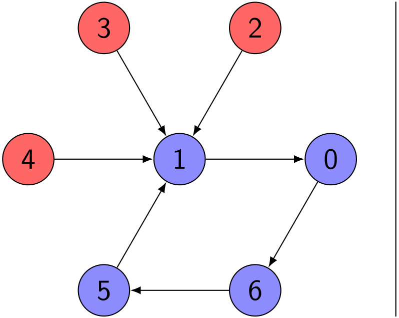
Near Permutations

Near Permutations

(6011115) vs. (0234560)

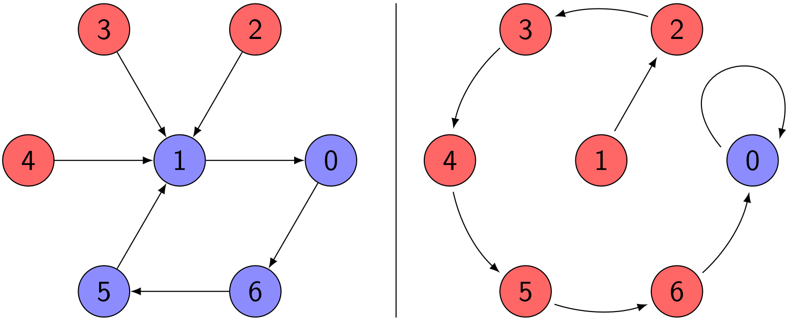
Near Permutations

(6011115) vs. (0234560)



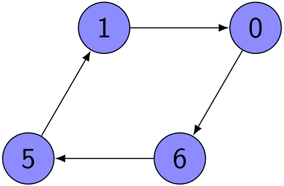
Near Permutations

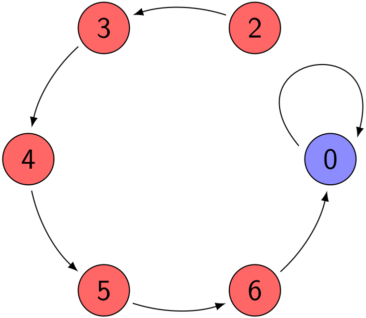
(6011115) vs. (0234560)



Near Permutations

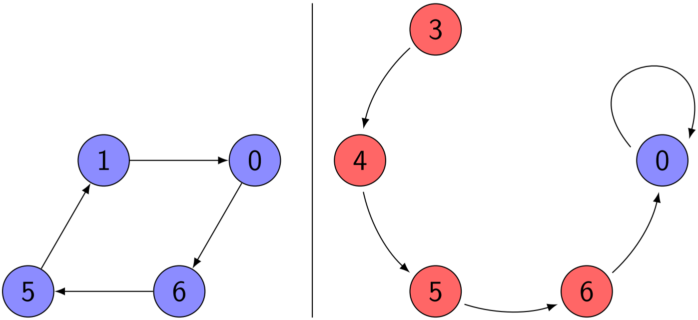
(6011115) vs. (0234560)





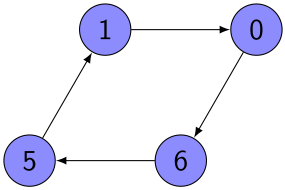
Near Permutations

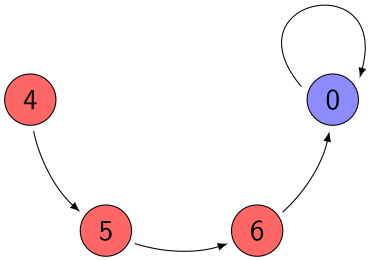
(6011115) vs. (0234560)



Near Permutations

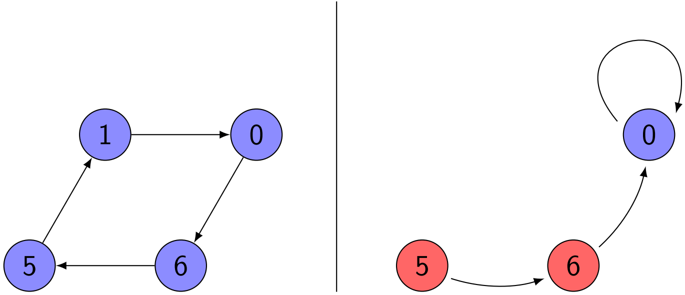
(6011115) vs. (0234560)





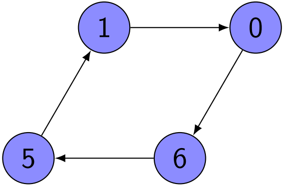
Near Permutations

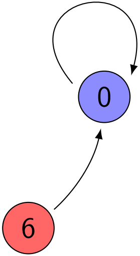
(6011115) vs. (0234560)



Near Permutations

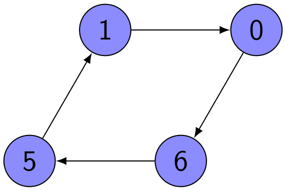
(6011115) vs. (0234560)

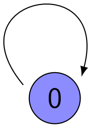




Near Permutations

(6011115) vs. (0234560)





Coining some language

Coining some language

Definition

The **size** of a function, f, is equal to the number of distinct elements in its one-line notation.

Coining some language

Definition

The **size** of a function, f, is equal to the number of distinct elements in its one-line notation.

Example

(122340) has **size 5**

Coining some language

Definition

The **size** of a function, f, is equal to the number of distinct elements in its one-line notation.

Example

(122340) has **size 5**

Definition

Let f be a function. The **k**th**-step** of f, is f iterated k times.

Coining some language

Definition

The **size** of a function, f, is equal to the number of distinct elements in its one-line notation.

Example

(122340) has **size 5**

Definition

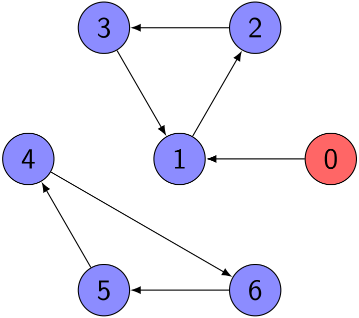
Let f be a function. The **kth-step** of f, is f iterated k times.

Definition

A function's **terminal size** is the number of vertices that are in cycles.

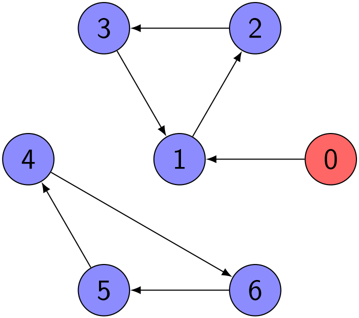
Examples

$$\begin{pmatrix} 1 & 2 & 3 & 1 & 6 & 4 & 5 \end{pmatrix}$$

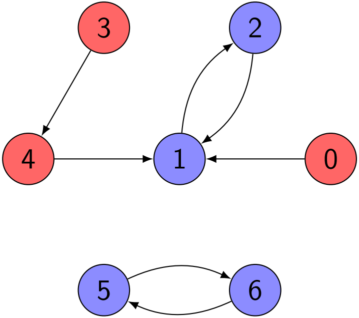


Examples

$$\begin{pmatrix} 1 & 2 & 3 & 1 & 6 & 4 & 5 \end{pmatrix}$$



$$\begin{pmatrix} 1 & 2 & 1 & 4 & 1 & 6 & 5 \end{pmatrix}$$



Data

$n = 4$

		Size			
		1	2	3	4
Step	1	1	1	4	0
	2	2	2	2	0
	3	4	0	2	0

Data

$n = 4$

		Size			
		1	2	3	4
Step	1	1	1	4	0
	2	2	2	2	0
	3	4	0	2	0

$n = 5$

		1	2	...	4	5
Step	1	1	0	...	0	3
	2	3	8	...	0	3
	3	11	0	...	0	3
	4	11	0	...	0	3

Data

$n = 4$

		Size			
		1	2	3	4
Step	1	1	1	4	0
	2	2	2	2	0
	3	4	0	2	0

$n = 5$

		1	2	...	4	5
Step	1	1	0	...	0	3
	2	3	8	...	0	3
	3	11	0	...	0	3
	4	11	0	...	0	3

$n = 6$

		1	2	...	5	6
Step	1	1	5	...	24	0
	2	11	21	...	8	0
	3	32	12	...	8	0
	4	44	4	...	8	0
	5	48	0	...	8	0

Data

$n = 4$

		Size			
		1	2	3	4
Step	1	1	1	4	0
	2	2	2	2	0
	3	4	0	2	0

$n = 5$

		1	2	...	4	5
Step	1	1	0	...	0	3
	2	3	8	...	0	3
	3	11	0	...	0	3
	4	11	0	...	0	3

$n = 6$

		1	2	...	5	6
Step	1	1	5	...	24	0
	2	11	21	...	8	0
	3	32	12	...	8	0
	4	44	4	...	8	0
	5	48	0	...	8	0

$n = 7$

		1	2	...	6	7
Step	1	1	0	...	0	19
	2	21	84	...	0	19
	3	117	78	...	0	19
	4	195	72	...	0	19
	5	267	0	...	0	19
	6	267	0	...	0	19

Periodicity in Permutation Sums

Theorem

Let π be a permutation of the cyclic group of n elements, and let f denote $\pi \oplus \theta$. Then if the size of f is 2, the one line representation of f is periodic.

Periodicity in Permutation Sums

Theorem

Let π be a permutation of the cyclic group of n elements, and let f denote $\pi \oplus \theta$. Then if the size of f is 2, the one line representation of f is periodic.

$$(2, 4, 2, 4, 2, 4)$$
$$(2, 5, 5, 2, 5, 5)$$
$$(2, 5, 2, 2, 5, 2)$$
$$(2, 6, 2, 6, 2, 6)$$
$$(2, 2, 5, 2, 2, 5)$$

Periodicity in Permutation Sums

Theorem

Let π be a permutation of the cyclic group of n elements, and let f denote $\pi \oplus \theta$. Then if the size of f is 2, the one line representation of f is periodic.

$$(2,\ 4,\ 2,\ 4,\ 2,\ 4)$$
$$(2,\ 5,\ 5,\ 2,\ 5,\ 5)$$
$$(2,\ 5,\ 2,\ 2,\ 5,\ 2)$$
$$(2,\ 6,\ 2,\ 6,\ 2,\ 6)$$
$$(2,\ 2,\ 5,\ 2,\ 2,\ 5)$$

Permutations over Galois Fields

In Grøstl, and in other hash functions, we are working with *bytes*, which are binary strings of length 8.

Permutations over Galois Fields

In Grøstl, and in other hash functions, we are working with *bytes*, which are binary strings of length 8.

The set of all binary strings of a given length corresponds directly to an algebraic structure called a *Galois field*.

Permutations over Galois Fields

In Grøstl, and in other hash functions, we are working with *bytes*, which are binary strings of length 8.

The set of all binary strings of a given length corresponds directly to an algebraic structure called a *Galois field*.

Bytes correspond to the Galois Field of size 2^8.

Permutations over Galois Fields

Sums of permutations behave differently over Galois Fields.

Permutations over Galois Fields

Sums of permutations behave differently over Galois Fields.

For example, while there is no pair of permutations P, Q on the elements $\{0, 1, 2, 3\}$ such that $P + Q$ is a permutation, the Galois Field of size 2^2 does have such permutations:

Permutations over Galois Fields

Sums of permutations behave differently over Galois Fields.

For example, while there is no pair of permutations P, Q on the elements $\{0, 1, 2, 3\}$ such that $P + Q$ is a permutation, the Galois Field of size 2^2 does have such permutations:

$$\begin{array}{cccccc} & (& 00 & 01 & 10 & 11 &) \\ + & (& 01 & 10 & 00 & 11 &) \end{array}$$

Permutations over Galois Fields

Sums of permutations behave differently over Galois Fields.

For example, while there is no pair of permutations P, Q on the elements $\{0, 1, 2, 3\}$ such that $P + Q$ is a permutation, the Galois Field of size 2^2 does have such permutations:

$$\begin{array}{cc} & (\ 00 \quad 01 \quad 10 \quad 11\ ) \\ + & (\ 01 \quad 10 \quad 00 \quad 11\ ) \\ \hline = & (\ 01 \quad 11 \quad 10 \quad 00\ ) \end{array}$$

Counting Sums of Permutations Over Galois Fields $GF(p^r)$

Theorem

If a is the identity permutation, the number of pairs of permutations (a, b) of the elements in $GF(p^r)$ with the size of $a+b$ equal to 2 is

$$(2^{p^{r-1}} - 2)\binom{p^r}{2}$$

Research Questions

Research Questions

- When is the sum of two permutations a permutation?

Research Questions

- When is the sum of two permutations a permutation?
- Do they exist?

Research Questions

- When is the sum of two permutations a permutation?
- Do they exist?
- If they exist, can we count them?

Research Questions

- When is the sum of two permutations a permutation?
- Do they exist?
- If they exist, can we count them?
- How can we construct them?

Acknowledgments

Supported by the National Science Foundation grant DMS-1359425 and Boise State University.
Thank you to Samuel Simon, REU CAD 2014 Alum (Simon Fraser University, Canada) for providing valuable comments.

BOISE STATE UNIVERSITY

References

- L. Babinkostova, K.W. Bombardier, M. C. Cole, T. A. Morrell, C. B. Scott, *Algebraic properties of generalized Rijndael-like ciphers*, **Groups, Complexity, Cryptology** Vol. 6, (2014), 37–54.
- B.D. McKay, J.C. McLeod and I.M. Wanless, The number of transversals in a latin square, *Des. Codes Cryptogr.* **40** (2006), 269-284.
- Martin Schlaffer, 2011. *Cryptanalysis of AES-Based Hash Functions*. PhD Thesis, Graz University of Technology, Austria.
- L. Sunil Chandran, Deepak Rajendraprasad, Nitin Singh. *On Additive Combinatorics of Permutations of* $\mathbb{Z}_n$. **Discrete Mathematics and Theoretical Computer Science**, Vol. 16:2 (2014),3540.