- *Preimage resistance:* For a given hash value h, it is computationally infeasible to find

The set of all even permutations is a group under functional composition and is called the *alternating group* on X. The symbol A

3.2. The SubBytes-like function (λ-function).

Definition 3. Let $\lambda : M_{m,n}(\mathrm{GF}(p^r)) \to M_{m,n}(\mathrm{GF}(p^r))$ denotes the mapping defined as a parallel application of $m \cdot n$ bijective S-box-mappings $\lambda_{ij} : \mathrm{GF}(p^r) \to \mathrm{GF}(p^r)$ and defined by $\lambda(a) = b$ if and only if $b_{ij} = \lambda_{ij}(a_{ij})$ for all $0 \leq i < m, 0 \leq j < n$.

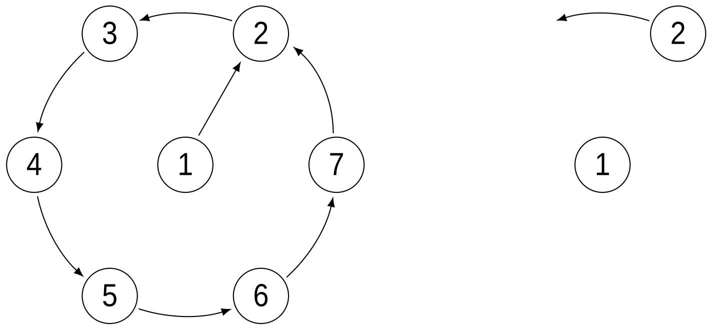
Each S-box mapping consists of an inversion, multiplication by a fixed A $\quad \mathrm{GF}(p^r)$, and addition of a fixed element B $\quad \mathrm{GF}(p^r)$ i.e. it is a mapping of the form $Ax^{-1} + B$ where A, B $\quad \mathrm{GF}(p^r)$ are fixed. For convenience we define this map on all of $\mathrm{GF}(p^r)$ so that it maps 0 to B, and any nonzero x to $Ax^{-1} + B$.

3.3. The ShiftBytes-like function (π-function).

Definition 4.

Definition 6. The function f is said to be *k-near* if $|\mathrm{Domain}(f)| - |\mathrm{Range}(f)| = k$.[2]

Definition 7. The k



π_1

Definition 12. A *transversal* of a Latin square is a set of n

Definition 16 (k-Transversals)**.** A k-transversal of a Latin square L of order n, where $1 \le k \le n$, is a list of n entries of L such that no two entries are in the same row, no two entries are in the same column, and there are k distinct symbols in the list.

5.3. Results in $\mathbb{Z}_n$.

Lemma 17. *If f is a permutation over $\mathbb{Z}_n$ that is the sum of the identity with another permutation then f has a fixed point.*

Proof. The identity maps every element to itself. Because the function we are adding to the identity is a permutation, it must be true that the additive identity will be added to some element in the identity permutation. For this element, the identity mapping will remain unchanged and yield a fixed point. □

Theorem 18. *Let f be a function defined over $\mathbb{Z}_n$ be the sum of the identity permutation with another permutation. Then $|range(f^{(n-1)})| = 2$.*

Proof. For a function to have a terminal range of 2 it is required that the total number of elements that are a part of some cycle is 2. This can manifest in two ways: two 1-cycles or one 2-cycle.

Case 1: Two 1-Cycles

Suppose f does contain two 1-cycles. A 1-cycle is a fixed point in our function. If we have two 1-cycles then there are two elements, i and j, such that $i \to i$ and $j \to j$. If f is the sum of the identity with some other permutation then when we subtract the identity we should be left with a permutation. However, if we subtract the identity from a function that maps i to itself and

(a)

by pigeon-hole principle, we know that there are exactly two of c_i's that are the same, say $c_k = c_l = h \quad (h = t)$, and the rest of c_i's are some arrangement of $\{1, 2, \cdots, n\}/\{t, h\}$. By summing up the quality $a_i + b_i = c_i$ over all i's, we have

$$\sum_{i=1}^{n}(a_i + b_i) \equiv \sum_{i=1}^{n} c_i \quad mod(n),$$

$$\sum_{i=1}^{n} a_i + \sum_{i=1}^{n} b_i \equiv \sum_{i=1}^{n} c_i \quad mod(n),$$

n

Lemma 21. *If* $f(i) = 2$*, then* $f(i + k(e - 2)) = 2$

elements in the range of $(\pi + id)$ sending to them, since all the $a_1, a_2, \cdots, a_t$ have already disappeared from the i^{th} step to $(i+1)^{th}$ step and Thus $b_1, b_2, \cdots, b_l$ will vanish at this time. By the fact that $l \leq t$, we are confirmed that the inequality holds. □

Definition 25. Let $\#(k, s)$ denote the number of permutations π that has size s after composing $\pi + id$ with itself k times, where id is the identity permutation.

Corollary 26. *If n is odd, then $\#(n-2, 2) = \#(n-1, 2) = 0$.*

Proof. It su□ces to show that $\#(n-2, 2) = 0$. Suppose not, then the size decreases at least 1 from the step $n-2$ to step $n-1$. By Theorem 24, we know that the size decreases at least 1 from the i^{th} step to $(i+1)^{th}$ step, where $i = 1, 2, \cdots, n-3$. This will imply that the function f with $|range(f^{(n-2)})| = 2$ is initially from a function $(\pi + id)$ that has size at least $2 + 1 \times (n-3) = n-1$. But according to the Theorem 19 d) the range cannot be $n-1$ since n is odd, neither could it be n as in this case $(\pi + id)$ will be a permutation and arbitrary times of composition of permutation result in permutation rather than function of size 2.

missing from the one-line notation, otherwise the size is $\leq n -$

And let's call the possible size of $(\pi + id)$ in this case the *initial size* for convenience.

Case 1: When n is even, we deduce from the previous statement that the y-step function $(\pi+id)^y$ might be initially degenerated from a 1-step function has at least size $n-1$. However, by Theorem 27 this is impossible since it only loses size by 1 at the first time of composition rather than 2. Also, the initial size cannot be n because if $(\pi + id)$ is of size n then it's a permutation, and so is $(\pi + id)^y$.

Case 2: When n is odd, the initial size is n, which means that $(\pi + id)$ is a permutation.

Consequently, either case yields contradiction. So there's no such function $(\pi + id)^y$ of size 1 that previously comes from $(\pi$

Corollary 31. *The number of terminally 1-near permutations is even.*

5.4. All the stu□

Proof. Let $f \in F_{1t}$. Consider the graph representing f. Since f is terminally one near, the graph necessarily contains a subset A of size $|A| = n-1$ on which f acts as a permutation, as well as an excluded element which is mapped into A. There are n choices for the excluded element, $n-1$ choices for its target (if it were a fixed point then it wouldn't be excluded), and $(n-1)!$ configurations for the permutation on A. Taking the product yields $n(n-1)(n-1)!$ possible functions f, which simplifies to the result. ▫

Theorem 34. $F_1(n)$ *has n-1 equivalence classes determined by* $\left(\sum_{i=1}^{n} f(i)\right)$ *mod n.*

Proof. $F_1(n)$ is the set of 1-near permutations on n elements. It is known that $\left(\sum_{i=1}^{n} i\right)$ *mod* $n = \frac{n}{2}$. To find the sum of an arbitary 1-near permutation we consider the following sum for $x, y \in \{1, 2, \cdots, n\}$ and $x = y$:

$$1 + 2 + 3 + \cdots + n - x + y.$$

The first n elements will sum to $\frac{n}{2}$ *mod* n. So we have

$$\frac{n}{2} - x + y.$$

From the constraints on x and y we have that $1 \leq |-x+y| \leq n-1$. Therefore, we have

$$\frac{n}{2} + 1 \leq \left(\frac{n}{2} - x + y\right) \text{ mod } n \leq \frac{n}{2} + n - 1.$$

This allows for every value on the range [1,n] with the exception of $\frac{n}{2}$. ▫

Theorem 35. *The n-1 equivalence classes of* $F_1(n)$ *are determined by* $\left(\sum_{i=1}^{n} f(i)\right)$ *mod n are the same size.*

Proof. We know that the sum of a 1-near permutation mod n is $\frac{n}{2} - x + y$ for some $x, y \in \{1, 2, \cdots, n\}$ with $x = y$. The $n-1$ equivalence classes are determined by the value of this sum. Let $c = \frac{n}{2} - x + y$. Then, rewriting, we see that for a given c, x is determined by y. So, in a particular class, c, there are n choices for an x, y pair that will satisfy the equation.

Each pair will result in a distinct function with a different repeated element. For each of

Consider $M_{n,n}(GF(p^r))$ $(n \geq 2)$ and the group formed by all the invertible matrices in it, namely $GL(n, GF(p^r))$.

In addition, an immediate consequence is that the number of the transversals over the

[11]

[28] T. Van Le, R. Sparr, R. Wernsdorf, and Y. Desmedt, *Complementation-like and cyclic properties of AES round functions*, Proceedings of the 4th International Conference on the Advanced Encryption Standard, Vol. 3373 (2005), 128-141.

[29] W. Mao, *Modern Cryptography: Theory and Practice*, Prentice Hall, (2003).

[30] S. Mattarei, *Inverse-closed additive subgroups of fields*, Israel Journal of Mathematics Vol. 159 (2007), 343–348.

[31] 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.

[32] L. Miller,*Generators of the Symmetric and Alternating Group*, The American Mathematical Monthly, Vol. 48, (1941), 43 – 44.

[33] S. Murphy, K.G. Paterson, P. Wild, *A weak cipher that generates the symmetric group*, Journal of Cryptology 7 (1994), 61–65.

[34] S. Murphy, M.J.B. Robshaw, *Essential algebraic structure within the AES*, Proceedings of CRYPTO 2002 Vol. 2442 (2002), 1–16.

[35] National Institute of Standards and Technology (US), *Advanced Encryption Standard (AES)*, FIPS Publication 197, (2001).

[36] National Institute of Standards and Technology (US), *Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher*, Special Publication 800-67 (2004).

[37] K.G. Paterson, *Imprimitive permutation groups and trapdoors in iterated block ciphers*, Lecture Notes in Computer Science, Vol. 1636 (1999), 201– 214.

[38] S. Patel, Z. Ramzan, G. S. Sundaram, *Luby-Rackof Ciphers: Why XOR Is Not So Exclusive*, Lecture Notes in Computer Science, Vol. 2595 (2003), 271–290.

[39] D. M. Rodgers, *Generating and Covering the Alternating or Symmetric group*, Communications in Algebra, 30 (2002), 425–435.

[40] P. Rogaway and T. Shrimpton, *Cryptographic Hash-Function Basics: Definitions, Implications, and Separations for Preimage Resistance, Second-Preimage Resistance, and Collision Resistance*, Fast Software Encryption, Lecture Notes in Computer Science , Vol. 3017 (2004), 371–388.

[41] Martin Schla□er, 2011. *Cryptanalysis o(i)*

[43] R. Sparr and R. Wernsdorf, *Group theoretic properties of Rijndael-like ciphers*, Discrete Applied Mathematics, Vol. 156 (2008), 3139–3149.

[44] W. Trappe and L. C. Washington, *Introduction to Cryptography with Coding Theory*, Pearson Education, (2006).

[45] R. Wernsdorf, *The round functions of Rijndael generate the alternating group*, Lecture Notes in Computer Science, Vol. 2365, Springer-Verlag (2002), 143–148.

[46] A. Williamson, *On Primitive Permutation Groups Containing a Cycle*, Mathematische Zeitschrift, 130 (1973), 159–162.

[47] I. M. Wanless, *Transversals in Latin squares: A survey*, Surveys in Combinatorics 2011, London Math. Soc. Lecture Note Series 392, Cambridge University Press, (2011) 403–437.