On the Use of GF-Inversion as a Cryptographic Primitive

Kazumaro Aoki[1] and Serge Vaudenay[2]*

[1] NTT Laboratories
maro@isl.ntt.co.jp
[2] Swiss Federal Institute of Technology (EPFL)
Serge.Vaudenay@epfl.ch

Abstract. Inversion in Galois Fields is a famous primitive permutation for designing cryptographic algorithms e.g. for Rijndael because it has suitable differential and linear properties. Inputs and outputs are usually transformed by addition (e.g. XOR) to key bits. We call this construction the APA (Add-Permute-Add) scheme. In this paper we study its pseudorandomness in terms of k-wise independence.
We show that the pairwise independence of the APA construction is related to the impossible differentials properties. We notice that inversion has many impossible differentials, so $x \mapsto \frac{1}{x+a} + b$ is not pairwise independent.
In 1998, Vaudenay proposed the random harmonic permutation $h : x \mapsto \frac{a}{x-b} + c$. Although it is not perfectly 3-wise independent (despite what was originally claimed), we demonstrate in this paper that it is *almost* 3-wise independent. In particular we show that any distinguisher limited to three queries between this permutation and a perfect one has an advantage limited to $\frac{3}{q}$ where q is the field order. This holds even if the distinguisher has access to h^{-1}.
Finally, we investigate 4-wise independence and we suggest the cross-ratio as a new tool for cryptanalysis of designs involving inversion.

Inversion in Galois fields is quite a popular primitive permutation for making block ciphers. This comes from nice properties with respect to differential and linear cryptanalysis (see Nyberg [10]). It has been used e.g. in Rijndael [5]. Inversion is also known to have bad algebraic properties which can lead to interpolation attacks (see Jakobsen-Knudsen [7]) or quadratic equations (see Murphy-Robshaw [9] and Courtois-Pieprzyk [4]). In this paper we study randomness in terms of k-wise independence of constructions with inversion.

Since Carter and Wegman introduced the notion of universal hash function, a wide spectrum of extensions, including ε-almost k-wise independent functions, and constructions have been proposed. In cryptography, pairwise independent hash functions ($k = 2$) can be used in order to construct secure message authentication codes. (See Wegman-Carter [19].)

* This work started while this author was visiting NTT Labs.

The k-wise independent *permutations* are also well suited properties of encryption functions. The perfect $k = 1$ case corresponds to the perfect secrecy in a Shannon sense [14]. This is however limited to one-time usage. More generally, perfect k-wise independence is linked to randomness when limited to k-time usage. The result is even quantitative in non perfect cases: for an ε-almost k-wise independent permutation, the best distinguisher between the permutation and an ideal one which is limited to k oracle calls has an advantage of $\frac{\varepsilon}{2}$. (When adopting an appropriate metrics, see Vaudenay [17,18].) Furthermore, almost pairwise independence ($k = 2$) has application to block ciphers since there is an upper bound of the best differential and linear characteristics in terms of pairwise independence. (See Vaudenay [16,18].) The 3-wise independent permutations recently found an application for strengthening short encryption keys (See Russel-Wang [13].)

Constructing k-wise independent functions over any finite field $\mathbf{K}$ is quite easy. Actually, a random polynomial of degree at most $k-1$ is perfectly k-wise independent. However constructing k-wise independent *permutations* is not so easy but for the $k = 1$ and $k = 2$ cases. For $k = 1$, one notices that $h(x) = x + a$ with $a \in_U \mathbf{K}$ is perfectly 1-wise independent. For $k = 2$, the $h(x) = ax + b$ function with $(a, b) \in_U \mathbf{K}^* \times \mathbf{K}$ is perfectly 2-wise independent. In Rees [11] a nice perfect 3-wise independent permutation construction was proposed in $P_2(\mathbf{K})$ using $\mathrm{PGL}_2(\mathbf{K})$. This means that we can define the permutation family for a projective plane over $\mathbf{K}$ which is a set of cardinality $\#\mathbf{K}+1$. This can never be equal to 2^{4n} since $15 = 2^4 - 1$ divides $2^{4n} - 1$ and is not a prime power. So this cannot help us in order to construct a 3-wise independent permutation over, for instance, a set of byte strings. In this paper we study the following construction over any finite field $\mathbf{K}$.

$$h(x) = a.\mathrm{inv}(x - b) + c$$

for $(a, b, c) \in_U \mathbf{K}^* \times \mathbf{K} \times \mathbf{K}$ where $\mathrm{inv}(t)$ is defined as being $1/t$ it $t \neq 0$ and 0 otherwise. We call it the *random harmonic permutation* construction. This construction was suggested in [16]. This paper claimed perfect 3-wise independence without proof. We show that this is not the case, but we still have almost independence. This provides a simple construction for almost 3-wise independent permutation over any finite field $\mathbf{K}$.

We also outline that the cross-ratio

$$R(t, u, v, w) = \left(\frac{t-u}{t-w}\right) / \left(\frac{v-u}{v-w}\right)$$

(for pairwise different t, u, v, w) is quite interesting from a cryptanalytic viewpoint since it is invariant under translation, multiplication, and inversion. We can distinguish the random harmonic permutation from an ideal one with only four queries t, u, v, w, so it is not 4-wise independent. We discuss about potential applications related to Rijndael.

We also study the pairwise independence of $h(x) = \mathrm{inv}(x - a) + b$ which is a kind of Even-Mansour [6] extension of the inversion. We show that for any permutation S, the pairwise independence of $h(x) = S(x + a) + b$ is related to impossible differentials for S. More precisely, we define a new measurement IDP (as for *Impossible Differential Probability*) by

$$\mathrm{IDP}^S = \max_{\delta \neq 0} \frac{1}{q} \#\{\Delta; \mathrm{DP}^S(\delta, \Delta) = 0\}$$

where q is the output range size and DP is the regular differential probability, i.e.

$$\mathrm{DP}^S(\delta, \Delta) = \frac{1}{q} \#\{x; S(x+\delta) = S(x) + \Delta\}.$$

We demonstrate that the best advantage for distinguishing h from a random permutation with two queries is close to IDP^S. We also show that this quantity is quite bad for the inversion since we have IDP $\approx \frac{1}{2}$ in this case. This is however not a specific weakness of the inversion in characteristic 2: it is indeed linked to the choice of the XOR as the addition.

1 Previous Work and Definitions

There is a wide menagerie of universal functions. We recall here a few definitions. First of all, here are definitions related to perfect functions.

Definition 1 (Carter-Wegman [3], Wegman-Carter [19]). *Let A and B be two finite sets. Let $\mathcal{F}(A, B)$ denote the set of all functions from A to B. Let H be a subset of $\mathcal{F}(A, B)$.*

1. *H is universal$_2$ if*

$$\forall x, y \in A \quad (x \neq y) \quad \Pr_{h \in_U H}[h(x) = h(y)] \leq \frac{1}{\#B}.$$

2. *H is strongly universal$_k$, or (perfect) k-wise independent function, if*

$$\forall x_1, \ldots, x_k \in A,\ \forall y_1, \ldots, y_k \in B, \quad (x_i \neq x_j \text{ for } i \neq j),$$
$$\Pr_{h \in_U H}[h(x_1) = y_1, \ldots, h(x_k) = y_k] = \frac{1}{\#B^k}.$$

3. *for $A = B$ when all functions of H are permutations, we say that H is a (perfect) k-wise independent permutation if*

$$\forall x_1, \ldots, x_k \in A,\ \forall y_1, \ldots, y_k \in B, \quad (x_i \neq x_j, y_i \neq y_j \text{ for } i \neq j),$$
$$\Pr_{h \in_U H}[h(x_1) = y_1, \ldots, h(x_k) = y_k] = \prod_{i=0}^{k-1} \frac{1}{\#B - i}.$$

Here are definitions related to imperfect functions.

Definition 2 (Stinson [15]). *Let A and B be two finite sets. Let $\mathcal{F}(A, B)$ denote the set of all functions from A to B. Let H be a subset of $\mathcal{F}(A, B)$.*

1. *H is ε-almost universal$_2$ if*

$$\forall x, y \in A \quad (x \neq y) \quad \Pr_{h \in_U H}[h(x) = h(y)] \leq \varepsilon.$$

2. *H is ε-almost strongly universal$_2$ if*

$$\forall x_1 \in A,\ \forall y_1 \in B, \quad \Pr_{h \in_U H}[h(x_1) = y_1] = \frac{1}{\#B}$$
$$\forall x_1, x_2 \in A,\ \forall y_1, y_2 \in B, \quad (x_1 \neq x_2),$$
$$\Pr_{h \in_U H}[h(x_1) = y_1, h(x_2) = y_2] \leq \frac{\varepsilon}{\#B}.$$

Almost k-wise independence is well known to be harder to define since it depends on the metric choice.

In order to measure k-wise independence for cryptography, we take the following general definition.

Definition 3 (Vaudenay [16,18]). *Let A and B be two finite sets. Let $\mathcal{F}(A, B)$ denote the set of all functions from A to B. Let $\mathcal{S}(A)$ denote the set of all permutations over A. Let H be a subset of $\mathcal{F}(A, B)$. Let $\mathcal{M}_k(A, B)$ be the set of all functions from $A^k \times B^k$ to the field $\mathbf{R}$ of real numbers. Let d be a distance over $\mathcal{M}_k(A, B)$. Let $k > 0$ be an integer. We define $[H]^k \in \mathcal{M}_k(A, B)$ by*

$$[H]^k(x_1, \ldots, x_k, y_1, \ldots, y_k) = \Pr_{h \in_U H}[h(x_1) = y_1, \ldots, h(x_k) = y_k].$$

1. *We say that H is an ε-d-almost k-wise independent function if $d([H]^k, [H^*]^k) \leq \varepsilon$ where $H^* = \mathcal{F}(A, B)$.*
2. *For $A = B$ and when H is a subset of $\mathcal{S}(A)$, we say that H is an ε-d-almost k-wise independent permutation if $d([H]^k, [H^*]^k) \leq \varepsilon$ where $H^* = \mathcal{S}(A)$.*

Several distances are quite significant in cryptography, including metrics induced by the $|||.|||_\infty$, $||.||_a$ and $||.||_s$ norms as defined in [16,17,18]:

$$|||f|||_\infty = \max_{(x_1,\ldots,x_k) \in A^k} \sum_{(y_1,\ldots,y_k) \in B^k} |f(x_1, \ldots, x_k, y_1, \ldots, y_k)|$$
$$||f||_a = \max_{x_1 \in A} \sum_{y_1 \in B} \ldots \max_{x_k \in A} \sum_{y_k \in B} |f(x_1, \ldots, x_k, y_1, \ldots, y_k)|$$

for $f \in \mathcal{M}_k(A, B)$. Obviously, $|||f|||_\infty \leq ||f||_a$. The $||.||_s$ norm is defined by

$$||f||_s = \max_{b_1 \in \{0,1\}} \max_{z_1^0 \in A} \sum_{z_1^1 \in A} \ldots \max_{b_k \in \{0,1\}} \max_{z_k^0 \in A} \sum_{z_k^1 \in A} |f(z_1^{b_1}, \ldots, z_k^{b_k}, z_1^{1-b_1}, \ldots, z_k^{1-b_k})|$$

for $f \in \mathcal{M}_k(A, A)$. Obviously, $|||f|||_\infty \leq ||f||_a \leq ||f||_s$. Here are some important properties which motivate these choices for cryptography.

Theorem 4 (Vaudenay [16,17,18]). *Let A and B be two finite sets. Let $\mathcal{F}(A, B)$ denote the set of all functions from A to B. Let $\mathcal{S}(A)$ denote the set of all permutations over A. Let H and H' be subsets of $\mathcal{F}(A, B)$.*

1. *The best distinguisher between H and H' limited to k queries has an advantage of* $\frac{1}{2}||[H]^k - [H']^k||_a$. *It is* $\frac{1}{2}|||[H]^k - [H']^k|||_\infty$ *when we restrict to non adaptive attacks.*
2. *For $A = B$ and H and H' subsets of $\mathcal{S}(A)$, the best distinguisher between $h \in_U H$ and $h \in_U H'$ limited to k queries with access to both h and h^{-1} has an advantage of* $\frac{1}{2}||[H]^k - [H']^k||_s$.
3. *When $A = B = \{0,1\}^n$ and H is an ε-$|||.|||_\infty$-almost pairwise independent permutation, differential and linear probabilities are bounded as follows.*

$$\forall b \quad \forall a \neq 0 \qquad \mathop{E}_{h \in_U H}(\mathrm{DP}^h(a,b)) \leq \frac{1}{2^n - 1} + \varepsilon$$
$$\forall a \quad \forall b \neq 0 \qquad \mathop{E}_{h \in_U H}(\mathrm{LP}^h(a,b)) \leq \frac{1}{2^n - 1} + 4\varepsilon$$

where

$$\mathrm{DP}^h(a,b) = \Pr_{X \in_U A}[h(X \oplus a) = h(X) \oplus b]$$
$$\mathrm{LP}^h(a,b) = \left(2 \Pr_{X \in_U A}[a \cdot X = b \cdot h(X)] - 1\right)^2.$$

Therefore k-wise independence has nice interpretations in terms of randomness when limited to k uses. k-wise independence for $k \geq 2$ leads to upper bounds for the best differential and linear probabilities.

Given a finite field $\mathbf{K} = \mathrm{GF}(q)$, we let inv be the permutation defined by $\mathrm{inv}(x) = \frac{1}{x}$ for $x \neq 0$ and $\mathrm{inv}(0) = 0$. Note that $\mathrm{inv}(x) = x^{q-2}$ for all $x \in \mathbf{K}$ when $q > 2$. This permutation is widely used in cryptography, e.g. in the design of the substitution boxes of Rijndael [1,5]. It is known to have nice differential properties. In particular Nyberg [10] proved that

$$\mathrm{DP}^{\mathrm{inv}}(a,b) \leq \tfrac{4}{q} \text{ for all } a \neq 0 \text{ and all } b$$
$$\mathrm{LP}^{\mathrm{inv}}(a,b) \leq \tfrac{4}{q} \text{ for all } b \neq 0 \text{ and all } a.$$

2 The Random Harmonic Permutation Construction

2.1 Our Result

Theorem 5. *Let $\mathbf{K}$ be a finite field of cardinality q. For any $a, b, c \in \mathbf{K}$ such that $a \neq 0$ we define $h_{a,b,c}(x) = a.\mathrm{inv}(x - b) + c$. Let H be the set of all $h_{a,b,c}$.*

1. *H is a perfect 2-wise independent permutation.*
2. *H is not a perfect 3-wise independent permutation for $q > 3$.*
3. *H is a $\frac{6}{q}$-$||.||_s$-almost 3-wise independent permutation.*
4. *H is not a $(2 - \frac{13}{q})$-$|||.|||_\infty$-almost 4-wise independent permutation for $q > 4$.*

The proof is achieved over the following subsections.

As a corollary H is also a $\frac{6}{q}$-$||.||_a$-almost 3-wise independent permutation and a $\frac{6}{q}$-$|||.|||_\infty$-almost 3-wise independent permutation as well.

This result means that any distinguisher limited to two queries has no chance at all for distinguishing H from a random permutation. Its advantage is limited to $\frac{3}{q}$ when limited to three queries (even adaptive, even with access to the inverse of H). Its advantage can be pretty close to 1 when four queries are allowed.

2.2 On the Perfect 3-wise Independence

One can wonder whether H is perfect 3-wise independent.

The $q = 2$ and $q = 3$ cases are particular. For $q = 2$ or $q = 3$ we have $\mathrm{inv}(x) = x$ for all $x \in \mathbf{K}$. Hence

$$a.\mathrm{inv}(x - b) + c = a.(x - b) + c = ax + (-ab + c).$$

Therefore H has the same distribution as $H' = \{h_{a,b}; (a, b) \in \mathbf{K}^* \times \mathbf{K}\}$ defined by $h_{a,b}(x) = ax + b$. We further notice that all permutations are indeed affine in these fields. Therefore H is perfectly 3-wise independent for $q = 2$ or $q = 3$.

Next, we check that H is never perfectly 3-wise independent for $q > 3$. Actually if we take any x_1, x_2, x_3 pairwise different elements of $\mathbf{K}$ we can consider $(h(x_1), h(x_2), h(x_3))$ for $h \in H$. This triplet must take values among all $q(q - 1)(q - 2)$ triplets with pairwise different coordinates in a uniform way. But we have $q^2(q - 1)$ elements h in H. Therefore this cannot be uniformly distributed unless $q - 2$ divides q which leads to $q = 3$ or $q = 4$. The $q = 4$ is also special since $\mathrm{inv}(x) = x^2$ which is GF(2)-linear for all $x \in \mathbf{K}$. Hence

$$a.\mathrm{inv}(x - b) + c = a.(x - b)^2 + c = ax^2 + (ab^2 + c).$$

We thus notice that H defines the same distribution than the set of all $h_{a,b}$ defined by $h_{a,b}(x) = ax^2 + b$ for $(a, b) \in \mathbf{K}^* \times \mathbf{K}$. This cannot be perfectly 3-wise independent since two (x_i, y_i) points offer no freedom for any third one. This proves Theorem 5 item 2.

We can manually compute $\varepsilon = |||[H]^3 - [H^*]^3|||_\infty$ for small q. We found

q	2	3	4	5	7	8	9	11	13	16	17	19	23	25	27	29	31	32
ε	0	0	1	$\frac{4}{15}$	$\frac{26}{35}$	$\frac{1}{2}$	$\frac{10}{21}$	$\frac{14}{33}$	$\frac{62}{143}$	$\frac{5}{14}$	$\frac{26}{85}$	$\frac{98}{323}$	$\frac{38}{161}$	$\frac{134}{575}$	$\frac{46}{225}$	$\frac{50}{261}$	$\frac{170}{899}$	$\frac{7}{40}$

We can notice that these numbers get closer to $\frac{6}{q}$ which seems to mean that our bound is tight.

2.3 Pairwise Independence

We notice that for any permutation S the set of all $a.S(x)+c$ for $(a, c) \in \mathbf{K}^* \times \mathbf{K}$ is perfectly pairwise independent. Hence H is a disjoint union of perfectly pairwise independent permutations. Therefore H is a perfect pairwise independent permutation. This proves Theorem 5 item 1.

2.4 Four-wise Independence

We construct a distinguisher which uses four input-output pairs (x_i, y_i) for $i = 1, 2, 3, 4$ by using the cross-ratio: let

$$R(t,u,v,w) = \frac{\frac{t-u}{t-w}}{\frac{v-u}{v-w}}$$

when t, u, v, w are pairwise different. We notice that R is invariant under translation, scalar multiplication, and inversion:

1. $R(t+\alpha, u+\alpha, v+\alpha, w+\alpha) = R(t,u,v,w)$ for any α,
2. $R(t.\beta, u.\beta, v.\beta, w.\beta) = R(t,u,v,w)$ for any $\beta \neq 0$,
3. $R(\mathrm{inv}(t), \mathrm{inv}(u), \mathrm{inv}(v), \mathrm{inv}(w)) = R(t,u,v,w)$ when t, u, v, w are nonzero.

Hence R is almost invariant under any h in H. The distinguisher works as follows: if $R(x_1, x_2, x_3, x_4) = R(y_1, y_2, y_3, y_4)$, yield 1, otherwise yield 0. The probability that the distinguisher yields 1 for $h \in H$ is at least than $1 - \frac{4}{q}$ since none of the inv input is zero with this probability. When y_1 takes all values but y_2, y_3, y_4, then $R(y_1, y_2, y_3, y_4)$ takes all but three values. So the probability that the distinguisher yields 1 for a random permutation is at most $\frac{1}{q-3}$. The advantage of the distinguisher is thus greater than $1 - \frac{4}{q} - \frac{1}{q-3}$. This is greater than $1 - \frac{13}{2q}$ for $q \geq 5$. The best non-adaptive distinguisher has thus an advantage greater than $1 - \frac{13}{2q}$. For the $|||.|||_\infty$-almost 4-wise independence we just need to multiply by 2 due to Theorem 4 item 1. This proves Theorem 5 item 4.

For $q = 4$ we notice that 4-wise independence is just like 3-wise independence for permutations: once three different input-output pairs are known, the fourth one is known as well. Thus H is 1-almost 4-wise independent for $q = 4$. For $q < 4$ the notion of 4-wise independence does not make sense.

Note that we can see Rijndael [1,5] as parallel applications and mixtures of $h_{a,b,c}$ functions as was shown by Murphy and Robshaw [9].[3] The distinguisher above shows that if we reduce this scheme to a single branch then it is totally insecure when having only four known plaintexts.

2.5 Three-wise Independence

Let us now prove Theorem 5 item 3. Let $x = (x_1, x_2, x_3)$, $y = (y_1, y_2, y_3)$. Let $p(x, y)$ be as follows.

$$p(x,y) = \Pr_{(a,b,c) \in_U \mathbf{K}^* \times \mathbf{K} \times \mathbf{K}} [h_{a,b,c}(x_1) = y_1, h_{a,b,c}(x_2) = y_2, h_{a,b,c}(x_3) = y_3]$$

Similarly we let $p^*(x, y)$ be as follows.

$$p^*(x,y) = \Pr_{h \in_U \mathcal{S}(\mathbf{K})} [h(x_1) = y_1, h(x_2) = y_2, h(x_3) = y_3]$$

[3] This is also equivalent to the simple SHARK [12] that was studied by using interpolation attacks by Jakobsen and Knudsen [7].

We define $d(x,y) = p(x,y) - p^*(x,y)$. We want to compute

$$D^3_{|||\cdot|||_\infty} = \max_x \sum_y |d(x,y)|$$
$$D^3_{||\cdot||_a} = \max_{x_1} \sum_{y_1} \max_{x_2} \sum_{y_2} \max_{x_3} \sum_{y_3} |d(x,y)|$$
$$D^3_{||\cdot||_s} = \max_{b_1,z_1^0} \sum_{z_1^1} \max_{b_2,z_2^0} \sum_{z_2^1} \max_{b_3,z_3^0} \sum_{z_3^1} |d(x,y)|$$

with $x_i = z_i^{b_i}$ and $y_i = z_i^{1-b_i}$. According to the definition of 3-wise independent permutation (see Def. 3), we should prove that $D^3_{.} \leq \frac{6}{q}$ for the three norms.

First, we notice that both $p(x,y)$ and $p^*(x,y)$ are zero when $x_i = x_j$ is not equivalent to $y_i = y_j$ since $h_{a,b,c}$ and h are permutations. Therefore the sums can be restricted to all y for which the equivalence holds. Second, we notice that terms in $D^3_{.}$ for which $x_i = x_j$ for some $i < j$ are already in the maximum defined for the pairwise independence. Since H is a perfect pairwise independent permutation these terms are all zero. We can thus focus on x terms for which we have $x_1 \neq x_2, x_2 \neq x_3, x_3 \neq x_1$. This means that we have

$$D^3_{|||\cdot|||_\infty} = \max_{\substack{x \\ x_1\neq x_2, x_2\neq x_3, x_3\neq x_1}} \sum_{\substack{y \\ y_1\neq y_2, y_2\neq y_3, y_3\neq y_1}} |d(x,y)|$$
$$D^3_{||\cdot||_a} = \max_{x_1} \sum_{y_1} \max_{\substack{x_2 \\ x_2\neq x_1}} \sum_{\substack{y_2 \\ y_2\neq y_1}} \max_{\substack{x_3 \\ x_3\neq x_1, x_3\neq x_2}} \sum_{\substack{y_3 \\ y_3\neq y_1, y_3\neq y_2}} |d(x,y)|.$$

We also consider

$$D = q(q-1) \max_{\substack{x_1,x_2,x_3,y_1,y_2 \\ x_1\neq x_2, x_2\neq x_3, x_3\neq x_1, y_2\neq y_1}} \sum_{\substack{y_3 \\ y_3\neq y_1, y_3\neq y_2}} |d(x,y)|.$$

Obviously we have $D^3_{|||\cdot|||_\infty} \leq D^3_{||\cdot||_a} \leq D$ so it is sufficient to prove that $D \leq \frac{6}{q}$. For the $||.||_s$ norm we also have $D^3_{||\cdot||_s} \leq \max(D, D')$ with D' defined by

$$D' = q(q-1) \max_{\substack{x_1,x_2,y_1,y_2,y_3 \\ y_1\neq y_2, y_2\neq y_3, y_3\neq y_1, x_2\neq x_1}} \sum_{\substack{x_3 \\ x_3\neq x_1, x_3\neq x_2}} |d(x,y)|.$$

So it is sufficient to prove that $D \leq \frac{6}{q}$ and $D' \leq \frac{6}{q}$. Since the treatment for D' is similar to that for D, we focus on the $D \leq \frac{6}{q}$ inequality.

By the definition of $p(x,y)$, we are interested in the number of solutions $(a,b,c) \in \mathbf{K}^* \times \mathbf{K} \times \mathbf{K}$ of

$$\begin{cases} a.\mathrm{inv}(x_1 - b) + c = y_1 \\ a.\mathrm{inv}(x_2 - b) + c = y_2 \\ a.\mathrm{inv}(x_3 - b) + c = y_3 \end{cases} \tag{1}$$

By linear combination of those equations, we obtain.

$$\mathrm{inv}(x_1-b)(y_3-y_2)+\mathrm{inv}(x_2-b)(y_1-y_3)+\mathrm{inv}(x_3-b)(y_2-y_1)=0 \qquad (2)$$

as a necessary condition. Then we realize that once a fixed b satisfies this equation, then, thanks to the hypothesis on x that $x_1 \neq x_2, x_2 \neq x_3, x_3 \neq x_1$, at least two out of the three equations of (1) are independent linear equations in a and c which leads to a unique solution (a,b,c). Therefore (1) and Eq. (2) have the same number of solutions. It is thus sufficient to count the number of solutions of Eq. (2).

Let $x=(x_1,x_2,x_3)$ be fixed and such that $x_1 \neq x_2, x_2 \neq x_3, x_3 \neq x_1$. Let y_1, y_2 be fixed and such that $y_1 \neq y_2$. We let $n_i(x,y_1,y_2)$ be the number of y_3 such that $y_2 \neq y_3, y_3 \neq y_1$ and such that the number of solutions b for (2) is exactly i. We also define

$$d_i=\frac{i}{q^2(q-1)}-\frac{1}{q(q-1)(q-2)}.$$

We notice that for $q>3$ then d_0 and d_1 are the only negative terms. We have

$$D=q(q-1)\max_{x,y_1,y_2}\sum_{i=0}^{q} n_i(x,y_1,y_2)|d_i|.$$

Obviously, for any x_1,x_2,x_3,y_1,y_2 with x_1,x_2,x_3 pairwise different and $y_1 \neq y_2$, we have

$$\sum_{\substack{y_3\\ y_3\neq y_1,y_3\neq y_2}} p(x,y)=\Pr_{(a,b,c)\in_U \mathbf{K}^*\times\mathbf{K}\times\mathbf{K}}[h_{a,b,c}(x_1)=y_1,h_{a,b,c}(x_2)=y_2]$$

and

$$\sum_{\substack{y_3\\ y_3\neq y_1,y_3\neq y_2}} p^*(x,y)=\Pr_{h\in_U \mathcal{S}(\mathbf{K})}[h(x_1)=y_1,h(x_2)=y_2]$$

and both are equal since H is perfectly pairwise independent. Hence the sum for D without absolute values is zero thus

$$n_0(x,y_1,y_2)|d_0|+n_1(x,y_1,y_2)|d_1|=\sum_{i=2}^{q} n_i(x,y_1,y_2)|d_i|$$

thus

$$D=2q(q-1)\max_{x,y_1,y_2}(n_0(x,y_1,y_2)|d_0|+n_1(x,y_1,y_2)|d_1|).$$

Let $n_{\leq 1}$ be n_0+n_1. We now have

$$D=2q(q-1)\max_{x,y_1,y_2}(n_0(x,y_1,y_2)(|d_0|-|d_1|)+n_{\leq 1}(x,y_1,y_2)|d_1|)$$

which expands into

$$D=2\max_{x,y_1,y_2}\left(\frac{n_0(x,y_1,y_2)}{q}+\frac{2n_{\leq 1}(x,y_1,y_2)}{q(q-2)}\right)$$

Since we have $n_{\leq 1}(x, y_1, y_2) \leq q - 2$, we have

$$D \leq \frac{4}{q} + \frac{2}{q} \max_{\substack{x_1, x_2, x_3, y_1, y_2 \\ x_1 \neq x_2, x_2 \neq x_3, x_3 \neq x_1, y_2 \neq y_1}} n_0(x, y_1, y_2).$$

Therefore we only have to show that we have no more than one y_3 for which we have no solution for b in Eq. (2).

Under the assumption that $b \notin \{x_1, x_2, x_3\}$ Eq. (2) is equivalent to

$$\begin{aligned} 0 = & \, b\,(y_1(x_3 - x_2) + y_2(x_1 - x_3) + y_3(x_2 - x_1)) \\ & - ((x_3 - x_2)x_1y_1 + (x_1 - x_3)x_2y_2 + (x_2 - x_1)x_3y_3) \end{aligned}$$

When we have no solution at all we must have

$$y_1(x_3 - x_2) + y_2(x_1 - x_3) + y_3(x_2 - x_1) = 0. \tag{3}$$

For any choice of x, y_1, y_2 (with $x_1 \neq x_2$) there is at most one y_3 which verifies this condition. Similarly for any choice of x_1, x_2, y (with $y_1 \neq y_2$) there is at most one x_3 which verifies this condition. This concludes the proof. □

3 The APA Construction

In this section we investigate $h_{a,b}(x) = \mathrm{inv}(x + a) + b$. This kind of primitive is used in several block ciphers, e.g. Rijndael since inv is one substitution-box application and a and b are key additions. Interestingly, we can also consider $h_{a,b}$ as the Even-Mansour [6] extension of inv, like for DESX [8]. We first study the problem with fixed permutations in a more general context that we call the Add-Permute-Add (APA) construction.

Note that one may also like to investigate $x \mapsto a.\mathrm{inv}(x)+c$ or $x \mapsto a.\mathrm{inv}(x+b)$. We notice that the latter family is the inverse of the former one. We also notice that the former family is equivalent to $y \mapsto a.y + c$ which is a perfect pairwise independent permutation.

3.1 Pairwise Independence of the APA Construction

The following lemma provides an interesting link between pairwise independence and the number of impossible differentials.

Lemma 6. *Let G be a finite group of order $q \geq 2$. Let S be a (fixed) permutation over G. For $(a, b) \in G \times G$, we consider the permutation $h_{a,b}$ defined by $h_{a,b}(x) = a + S(x + b)$. We let H denote the set of all $h_{a,b}$.*

Given a nonzero input difference δ in G, we let $\mathrm{IDP}^S(\delta)$ be the fraction of the number of nonzero Δ values in G such that the $S(x+\delta) = S(x)+\Delta$ equation has no solution, i.e.

$$\mathrm{IDP}^S(\delta) = \frac{\#\{\Delta \in G; \mathrm{DP}^S(\delta, \Delta) = 0\}}{\#G}$$

We further let IDP^S *be the maximum of* $\mathrm{IDP}^S(\delta)$ *for all nonzero* δ.

The best advantage Adv of a non-adaptive distinguisher between H *and a random permutation limited to two queries is such that*

$$\frac{q-2}{2q(q-1)} \leq \mathrm{Adv} - \mathrm{IDP}^S \leq \frac{1}{q}.$$

Note that $\mathrm{IDP}^S(\delta)$ denotes the number of impossible differentials (δ, Δ) in the sense of Biham et al. [2] with a fixed δ. Hence we have a nice link between pairwise independence and impossible differentials.

Due to the link between differential probabilities and pairwise independence (see Theorem 4), we notice the consequence that we have

$$\max_{a \neq 0, b} \mathop{E}_{h \in_U H} (\mathrm{DP}^h(a,b)) \leq \frac{1}{q-1} + \frac{2}{q} + 2.\mathrm{IDP}^S$$

where $E_{h \in_U H}(\mathrm{DP}^h(a,b))$ denotes the expected value of $\mathrm{DP}^h(a,b)$ for a random h uniformly distributed in H. Therefore we also have a nice link between differential probabilities and impossible differentials for the APA construction.

Proof. As in previous sections, and with similar notations, we observe that

$$D^2_{|||.|||_\infty} = \max_{\substack{x_1, x_2 \\ x_1 \neq x_2}} \sum_{\substack{y_1, y_2 \\ y_1 \neq y_2}} |d(x,y)|.$$

We let

$$d_i = \frac{i}{q^2} - \frac{1}{q(q-1)}$$

and $n_i(x)$ be the number of y for which $d(x,y) = d_i$. We have

$$D^2_{|||.|||_\infty} = \max_{\substack{x_1, x_2 \\ x_1 \neq x_2}} \sum_{i=0}^{q(q-1)} n_i(x)|d_i|.$$

The sum without absolute values is zero and d_0 and d_1 are the only negative terms we obtain

$$D^2_{|||.|||_\infty} = 2 \max_{\substack{x_1, x_2 \\ x_1 \neq x_2}} (n_0(x)(|d_0| - |d_1|) + n_{\leq 1}(x)|d_1|)$$

where $n_{\leq 1}(x) = n_0(x) + n_1(x)$. Since $\sum_{i \geq 2} n_i(x) = q(q-1) - n_{\leq 1}(x)$ and $d_i \geq d_2$ for $i \geq 2$, we have

$$(q(q-1) - n_{\leq 1}(x))d_2 \leq \sum_{i=2}^{q(q-1)} n_i(x) d_i = n_0(x)|d_0| + n_1(x)|d_1| \leq n_{\leq 1}(x)|d_0|$$

thus

$$n_{\leq 1}(x) \geq q(q-1)\frac{d_2/|d_0|}{1 + d_2/|d_0|} = \frac{1}{2}q(q-2).$$

Furthermore $n_{\leq 1} \leq q(q-1)$, thus we obtain

$$\frac{q-2}{q(q-1)} \leq D^2_{|||.|||_\infty} - \frac{2}{q^2} \max_{\substack{x_1,x_2\\x_1\neq x_2}} n_0(x) \leq \frac{2}{q}.$$

Now we notice that $n_0(x)$ counts the number of unreached (y_1,y_2) pairs by $h_{a,b}$. Since a perfectly randomizes the outputs $(h_{a,b}(x_1), h_{a,b}(x_2))$ up to a fixed difference, $n_0(x)$ is equal to q times the number of unreached differences. Since b perfectly randomizes the inputs (x_1+b, x_2+b) of S, $n_0(x)$ is simply equal to $q^2.\mathrm{IDP}^S(x_2-x_1)$. Hence we obtain the claimed inequalities. □

The lemma bounds the best advantage of a distinguisher (regardless of the complexity). We describe here a distinguisher whose advantage is very close to the best one.

1. Pick a random x_1, x_2 $(x_1 \neq x_2)$ such that $\mathrm{IDP}^S(x_2-x_1)$ is maximal.
2. Send x_1, x_2 to the oracle, get y_1, y_2 respectively.
3. If $y_2 - y_1$ is in the set of all $S(x+x_2) - S(x+x_1)$ when $x \in G$, then output 1, otherwise, output 0.

Obviously the advantage is IDP^S.

3.2 Application to inv

With notations of the previous lemma, we notice that $\mathrm{IDP}^{\mathrm{inv}}$ is pretty bad. Actually, $\mathrm{inv}(x+\delta) = \mathrm{inv}(x) + \Delta$ has no solution if, and only if the following conditions are satisfied

1. $\Delta \neq \mathrm{inv}(\delta)$.
2. The $x^2 + \delta x + \frac{\delta}{\Delta}$ polynomial has no root.

These conditions hold for half of all possible Δs hence $\mathrm{IDP}^{\mathrm{inv}} = \frac{1}{2}$ for q even and $\mathrm{IDP}^{\mathrm{inv}} = \frac{1}{2}(1-q^{-1})$ for q odd. This suggests that $h_{a,b}$ has a pretty bad pairwise independence. With two samples $x_1 \mapsto y_1$ and $x_2 \mapsto y_2$, we can actually distinguish $h_{a,b}$ from a random permutation with high advantage by checking whether the above conditions hold for $\delta = x_1 - x_2$ and $\Delta = y_1 - y_2$. (This is the distinguisher of the previous section.) Since $\mathrm{IDP}^{\mathrm{inv}}$ is close to $\frac{1}{2}$, the advantage is close to $\frac{1}{2}$.

3.3 On the Choice of XOR as a Group Operation

The bad performance if inv in the previous construction is actually not exceptional when the group operation is equivalent to the XOR. Indeed, given a fixed $\delta \neq 0$ we know that $\mathrm{DP}^S(\delta, \Delta)$ is always an even multiple of q^{-1} (since x is a solution of $S(x+\delta) = S(x) + \Delta$ implies that $x+\delta$ is also a solution). It sums to 1 over all of the q choices of Δ, so at least half of them are zero. This means that $\mathrm{IDP}^S \geq \frac{1}{2}$ for all S. So inv does not perform so bad in the characteristic 2 case: it is just the maximum we can get from the the APA construction with the XOR addition and a fixed permutation.

4 Conclusion

We investigated properties of the random harmonic permutation construction. We demonstrated that it is perfect pairwise independent, and almost 3-wise independent. It implies that any distinguisher between those permutations and perfect ones which is limited to three queries has an advantage bounded by $\frac{3}{q}$ where q is the field order.

We also have shown that it is not 4-wise independent and can actually be easily distinguished from random permutations by using the cross-ratio. This suggests the cross-ratio as a new tool for cryptanalysis.

We investigated the pairwise independence of the APA construction. We have shown it relates to the impossible differentials. In particular, this construction used together with the inversion is not a good one since we can easily distinguish it with two oracle accesses, despite the good properties of inversion with respect to differential and linear cryptanalysis.

References

1. Advanced Encryption Standard (AES). *Federal Information Processing Standards* Publication #197. U.S. Department of Commerce, National Institute of Standards and Technology, 2001.
2. E. Biham, A. Biryukov, A. Shamir. Cryptanalysis of Skipjack Reduced to 31 Rounds using Impossible Differentials. In *Advances in Cryptology EUROCRYPT'99*, Prague, Czech Republic, Lectures Notes in Computer Science 1592, pp. 12–23, Springer-Verlag, 1999.
3. J.L. Carter, M.N. Wegman. Universal Classes of Hash Functions. *Journal of Computer and System Sciences*, vol. 18, pp. 143–154, 1979.
4. N. T. Courtois, J. Pieprzyk. Cryptanalysis of Block Ciphers with Overdefined Systems of Equations. In *Advances in Cryptology ASIACRYPT'02*, Queenstwon, New Zeland, Lectures Notes in Computer Science 2501, pp. 267–287, Springer-Verlag, 2002.
5. J. Daemen, V. Rijmen. *The Design of Rijndael*, Information Security and Cryptography, 2002.
6. S. Even, Y. Mansour. A Construction of a Cipher from a Single Pseudorandom Permutation. In *Advances in Cryptology ASIACRYPT'91*, Fujiyoshida, Japan, Lectures Notes in Computer Science 739, pp. 210–224, Springer-Verlag, 1993. Also in *Journal of Cryptology*, vol. 10, pp. 151–161, 1997.
7. T. Jakobsen, L. R. Knudsen. The Interpolation Attack on Block Ciphers. In *Fast Software Encryption'97*, Haifa, Israel, Lectures Notes in Computer Science 1267, pp. 28–40, Springer-Verlag, 1997.
8. J. Kilian, P. Rogaway. How to Protect DES Against Exhaustive Key Search. *Journal of Cryptology*, vol. 14, pp. 17–35, 2001.
9. S. Murphy, M.J.B. Robshaw. Essential Algebraic Structure within the AES. In *Advances in Cryptology CRYPTO'02*, Santa Barbara, California, U.S.A., Lectures Notes in Computer Science 2442, pp. 1–16, Springer-Verlag, 2002.
10. K. Nyberg. Differentially Uniform Mappings for Cryptography. In *Advances in Cryptology EUROCRYPT'93*, Lofthus, Norway, Lectures Notes in Computer Science 765, pp. 55–64, Springer-Verlag, 1994.

11. E.G. Rees. *Notes on Geometry*, Springer-Verlag, 1983.
12. V. Rijmen, J. Daemen, B. Preneel, A. Bosselaers, E. De Win. The Cipher SHARK. In *Fast Software Encryption'96*, Cambridge, United Kingdom, Lectures Notes in Computer Science 1039, pp. 99–112, Springer-Verlag, 1996.
13. A. Russel, H. Wang. How to Fool an Unbounded Adversary with a Short Key. In *Advances in Cryptology EUROCRYPT'02*, Amsterdam, Netherland, Lectures Notes in Computer Science 2332, pp. 133–148, Springer-Verlag, 2002.
14. C.E. Shannon. Communication Theory of Secrecy Systems. *Bell system technical journal*, vol. 28, pp. 656–715, 1949.
15. D.R. Stinson. Universal Hashing and Authentication Codes. In *Advances in Cryptology CRYPTO'91*, Santa Barbara, California, U.S.A., Lectures Notes in Computer Science 576, pp. 74–85, Springer-Verlag, 1992.
16. S. Vaudenay. Provable Security for Block Ciphers by Decorrelation. In *STACS 98*, Paris, France, Lectures Notes in Computer Science 1373, pp. 249–275, Springer-Verlag, 1998.
17. S. Vaudenay. Adaptive-Attack Norm for Decorrelation and Super-Pseudorandomness. In *Selected Areas in Cryptography'99*, Kingston, Ontario, Canada, Lectures Notes in Computer Science 1758, pp. 49–61, Springer-Verlag, 2000.
18. S. Vaudenay. Decorrelation: a Theory for Block Cipher Security. To appear in the Journal of Cryptology.
19. M.N. Wegman, J.L. Carter. New Hash Functions and their Use in Authentication and Set Equality. *Journal of Computer and System Sciences*, vol. 22, pp. 265–279, 1981.