# On Differential Properties of Pseudo-Hadamard Transform and Related Mappings (Extended Abstract)

Helger Lipmaa

Laboratory for Theoretical Computer Science
Department of Computer Science and Engineering
Helsinki University of Technology
P.O.Box 5400, FI-02015 Espoo, Finland
helger@tcs.hut.fi

**Abstract.** In FSE 2001, Lipmaa and Moriai proposed efficient log-time algorithms for computing some functions that are related to the differential probability of modular addition. They posed it as an open question whether their algorithms can be generalized to more complex functions. In this paper, we will give a fundamentally different proof of their main result by using a more scalable linear-algebraic approach. Our proof technique enables us to easily derive differential probabilities of some other related mappings like the subtraction and the Pseudo-Hadamard Transform. Finally, we show how to apply the derived formulas to analyse partial round mapping of Twofish.

**Keywords:** differential probability, linear functions, Pseudo-Hadamard Transform, Twofish.

## 1 Introduction

To measure the success of first-order differential cryptanalysis [BS91] against cryptographic primitives like block ciphers, one must be able to efficiently calculate the differential probability of various functions. For example, one might need to bound the maximum differential probability, or the percentage of impossible differentials.

Several well-known block ciphers were constructed so as their differential probabilities are easy to compute. This has enabled to bound the relevant maximum differential probabilities and prove the security against the impossible differential cryptanalysis. While this design methodology has been very productive (for example, AES and KASUMI are based on such an approach), practice has shown that ciphers that are specifically constructed to thwart the differential attacks are sometimes "simple enough" to be attackable by other cryptanalytic methods [JK97].

By this reason, the majority of modern block ciphers are still designed in a way that makes it rather difficult to estimate their security against differential cryptanalysis. This difficulty is mostly caused by the hardness of computing differential probabilities of corresponding ciphers, not even talking about the maximum differential probabilities or many other differential properties. This situation is may be best demonstrated by the fact that until lately it was still not known how to efficiently compute exact differential probabilities of very simple and widely used mappings like the addition modulo $2^n$.

Only recently Lipmaa and Moriai made a breakthrough in the last respect, by showing in [LM01] how to compute the differential probability of addition modulo $2^n$, for $n > 1$. Their algorithms are surprisingly efficient, working in worst-case time $\Theta(\log n)$ when a RAM model of computation is assumed. By contrast, the best previous algorithms for related problems worked often in time $2^{\Omega(n)}$. In the same paper, Lipmaa and Moriai suggested the next "bottom-up" cryptanalysis principle: start with exhaustive analysis of the simplest primitives and then gradually work upwards toward the analysis of the whole ciphers.

The current paper is a further extension of the methods from [LM01]. We compute differential probabilities of a special class of practically important mappings. All such mappings can be represented as $F(x_1, x_2) = (x_1{}^{\lll\kappa_{11}} \pm x_2{}^{\lll\kappa_{12}}, x_1{}^{\lll\kappa_{21}} \pm x_2{}^{\lll\kappa_{22}})$ with $\kappa_{jk} \geq 0$. Here, $x^{\lll k}$ denotes the left shift of $x$ by $k$ bits (i.e., $x^{\lll k} = 2^k \cdot x \mod 2^n$), and $\pm$ denotes either addition or subtraction in $\mathbb{Z}_{2^n}$, where $n \geq 1$. We call the class of such mappings *Quasi-Hadamard Transforms*. We show that for all Quasi-Hadamard Transforms, the formula for differential probability $\mathsf{dp}^F$ of $F$ can be transformed to a simple matrix equation in the inputs $x$ and the carries $c$ that occur in additions $x_1{}^{\lll\kappa_{j1}} \pm x_2{}^{\lll\kappa_{j2}}$.

It is valid to assume that $c$ is a constant in the special case when $\kappa_{11} = \kappa_{21}$, $\kappa_{12} = \kappa_{22}$ and $\kappa_{11} \leq \kappa_{12} + 1$. This gives us a matrix equation in $x$, with $2^{2n} \cdot \mathsf{dp}^F(\Delta x \mapsto \Delta y)$ being equal to the number of solutions to this matrix equation, which can be found by using standard methods from linear algebra. This results, in particular, in a closed form formula and log-time algorithms for the differential probability of all functions that have the form $F(x_1, x_2) = 2^{\kappa_1}x_1 \pm 2^{\kappa_2}x_2$. Our formula for addition is equivalent to the formula from [LM01] but our proof technique is very different and allows to obtain us a more general result after a relatively compact proof.

Apart from addition and subtraction, only a few Quasi-Hadamard Transforms are used in real block ciphers. The most important one, the PHT (*Pseudo-Hadamard Transform*) is employed in SAFER [Mas93] and Twofish [SKW+99]. The PHT is defined as $\mathrm{PHT}(x_1, x_2) = (2x_1 + x_2, x_1 + x_2)$. Another example is Schnorr's FFT-hash [Sch92] that employs several functions $F$ of type $F(x_1, x_2) = (4^j x_1 + x_2, x_1 + x_2)$. The mappings of both type are invertible.

In the current paper, we present a formula for $\mathsf{dp}^{\mathrm{PHT}}$. We show that a differential $\delta = (\Delta x_1, \Delta x_2 \to \Delta y_1, \Delta y_2)$ is PHT-possible iff corresponding projections of $\delta$ are possible under both coordinate mappings of both PHT and $\mathrm{PHT}^{-1}$. We also describe a log-time algorithm for $\mathsf{dp}^{\mathrm{PHT}}$. Therefore, this paper first solves completely the case when $F(x_1, x_2) = x_1{}^{\lll\kappa_{11}} \pm x_2{}^{\lll\kappa_{12}}$ for $\kappa_1 \leq \kappa_2 + 1$, and second, solves the important case of the Pseudo-Hadamard Transform.

We conclude the current paper with some applications of our results to Twofish [SKW+99] that was one of the leading AES candidates. In particular, we present a short proof that certain differentials described by Robshaw and Murphy in [MR02] (that were originally obtained by extensive computer experiments) are optimal under their conditions. Our proof only needs an exhaustive search over $\leq 2^{10}$ differentials. We present a few new differentials that are optimal under some more general conditions and might result in other applications of the methods from [MR02].

*Road-Map.* In Section 2, we introduce preliminaries and notation that are necessary for reading the rest of this paper. In Section 3, we present a linear-algebraic framework for computing the differential probability of a large class of interesting mappings. In particular, in Section 3.2 we derive a formula for the differential probability of any mapping of the form $F(x_1, x_2) = x_1^{\lll \kappa_{11}} \pm x_2^{\lll \kappa_{12}}$. In Section 4, we present a formula for the differential probability of Pseudo-Hadamard Transform. In Section 5, we apply our results to the partial round function of Twofish. We end the paper with conclusions.

## 2 Preliminaries and Notation

*Notation.* Throughout this paper, we will denote by $n$ the bit-length of basic variables. We will equivalently consider these variables as bit-strings of length $n$, members of group $(\mathbb{Z}_{2^n}, +)$ or members of ring $(\mathbb{Z}_2^n, \cdot, \oplus)$. The variables $x$ (the *input variable*) and $y$ (the *output variable*) will have a special meaning.

For any bit-vector $\alpha \in \mathbb{Z}_2^{2n}$, let $\alpha_1$ (resp., $\alpha_2$) denote its least significant (resp., most significant) half. For any bit-vector $\alpha \in \mathbb{Z}_2^m$ , $m \geq 1$, let $\alpha = \langle\alpha\rangle_0 2^0 + \cdots + \langle\alpha\rangle_{m-1} 2^{m-1}$ be the binary representation of corresponding integer, with $\langle\alpha\rangle_i \in \{0, 1\}$ being the $i$th bit of $\alpha$. That is, we start counting bits from zero. We use the special notation $\langle\alpha\rangle_i$ to distinguish individual bits of $\alpha$ from $n$-bit sub-vectors of a $2n$-bit vector.We assume that $\langle\alpha\rangle_i = 0$ when $i \notin [0, m-1]$.

Let $w_h(\alpha)$ be the Hamming weight of $\alpha$, that is, if $\alpha \in \mathbb{Z}_2^m$ then $w_h(\alpha) = \langle\alpha\rangle_0 + \cdots + \langle\alpha\rangle_{m-1}$. Hamming weight of an $\alpha \in \mathbb{Z}_2^m$ can be computed in time $\Theta(\log m)$ in a RAM model. Let $\mathsf{ntz}(x)$ be the number of trailing zeros of $x$; that is, $\mathsf{ntz}(x) = k$ iff $2^k \mid x$ but $2^{k+1} \nmid x$. For example, $\mathsf{ntz}(48) = 4$ and $\mathsf{ntz}(0) = n$. The function $\mathsf{ntz}$ can then be computed in time $O(\log_2 n)$ as $\mathsf{ntz}(x) := w_h(x - (x \wedge (x - 1)) - 1)$.

Let $\alpha \cdot \beta$ denote the component-wise multiplication in $\mathbb{Z}_2^m$. Let $\mathsf{maj}(\alpha, \beta, \gamma) := \alpha \cdot \beta \oplus \alpha \cdot \gamma \oplus \beta \cdot \gamma$ be the bitwise majority function, $\mathsf{xor}(\alpha_1, \ldots, \alpha_m) := \alpha_1 \oplus \cdots \oplus \alpha_m$ and $\mathsf{eq}(\alpha, \beta, \gamma) := (1 \oplus \alpha \oplus \beta) \cdot (1 \oplus \alpha \oplus \gamma)$ be the bitwise equality function. (The $\mathsf{xor}$ function is solely introduced to make some formulas more readable.) Clearly, $\langle\mathsf{maj}(\alpha, \beta, \gamma)\rangle_i = 1$ iff $\langle\alpha\rangle_i + \langle\beta\rangle_i + \langle\gamma\rangle_i \geq 2$ and $\langle\mathsf{eq}(\alpha, \beta, \gamma)\rangle_i = 1$ iff $\langle\alpha\rangle_i = \langle\beta\rangle_i = \langle\gamma\rangle_i$. Observe that matrix indexes (denoted as $A_{ij}$) start with 1, while vector indexes (denoted as $\langle\alpha\rangle_i$) start with 0.

*Differential cryptanalysis.* Let $\partial x = x \oplus x^*$ be the difference between two inputs $x, x^* \in \mathbb{Z}_2^{m_1 n}$ to a fixed mapping $F : \mathbb{Z}_2^{m_1 n} \to \mathbb{Z}_2^{m_2 n}$. For every intermediate node $Q$ in the computation graph of $F$, let $q$ (or $q^*$) denote the value in this node when the input was $x$ (or $x^*$). Let $\partial q = q \oplus q^*$ be the corresponding difference with concrete inputs $x$ and $x^*$ usually understood from the context. In particular, let $\partial F(x) = F(x) \oplus F(x^*)$ be the output difference. With $\Delta q$ we will denote the "desired" difference in node $Q$. That is, this is the difference the cryptanalyst is "aiming for", but which is not necessarily the actual difference for every choice of $x$ and $x^*$ with $\partial x = \Delta x$. The cryptanalyst is successful when the probability $\Pr_x[\partial F = \Delta F]$ is high. We always assume that $\Delta x = \partial x$ since $\partial x$ can be controlled by the adversary in all relevant attack models. The pair $(\Delta x, \Delta F)$ is usually denoted as $(\Delta x \rightarrow \Delta F)$.

For any mapping $F : \mathbb{Z}_{2^n}^{m_1 n} \rightarrow \mathbb{Z}_2^{m_2 n}$, the *differential probability* $\mathsf{dp}^F : \mathbb{Z}_2^{m_1 n} \times \mathbb{Z}_2^{m_2 n} \rightarrow [0,1]$ *of* $F$ is defined as $\mathsf{dp}^F(\delta) := \Pr_x[F(x) \oplus F(x \oplus \Delta x) = \Delta y]$, where $x$ is chosen uniformly and randomly from $\mathbb{Z}_{2^n}^{m_1 n}$. Equivalently, $\mathsf{dp}^F(\delta) = \sharp\{x \in \mathbb{Z}_2^{m_1 n} : F(x) \oplus F(x \oplus \Delta x) = \Delta y\}/\sharp\mathbb{Z}_2^{m_1 n}$. We say that $\delta$ is $F$*-possible* if $\mathsf{dp}^F(\delta) \neq 0$.

*Linear algebra.* Let $\mathrm{Mat}_{k\times\ell}(R)$ be the group of $k\times\ell$ matrices over a commutative ring $R$. Let $\mathrm{Mat}_k(R) := \mathrm{Mat}_{k\times\ell}(R)$ when $k = \ell$. We will mostly need $n \times n$ and $2n \times 2n$ matrices. In the latter case, let $A_{ij}$, $i, j \in \{0, 1\}$, denote the $n \times n$ sub-matrix in $A$ that starts from the row $i \cdot n + 1$ and the column $j \cdot n + 1$. For any binary matrix (or vector) $A$, let $\neg A$ denote the bit-inverse of $A$, that is, $\neg A_{ij} = 1 \oplus A_{ij}$ where $A_{ij} \in \mathbb{Z}_2$. To simplify reading, we will denote matrices with capital letters, while we denote vectors with lower-case letters.

Let $J$ be the binary $m \times m$ Toeplitz matrix with $J_{ij} = 1$ iff $i = j + 1$; $m$ is usually understood from the context. Clearly, for any $k$ and $\alpha \in \mathbb{Z}_2^m$, $\langle J^k \cdot \alpha\rangle_i = \langle\alpha\rangle_{i-k}$. Thus, $J^k \cdot \alpha$ corresponds to the shifting the bits of $\alpha$ to left $k$ times (when $\alpha$ is seen as a bit-string), or to the modular multiplication $2^k \cdot \alpha$ in the ring $\mathbb{Z}_{2^n}$.

For any $\alpha \in \mathbb{Z}_2^m$, let $[\![\alpha]\!]$ be the unique diagonal matrix, such that $[\![\alpha]\!]_{ii} = \langle\alpha\rangle_{i-1}$. (Recall that by our convention, the matrix indexes start from 1 but the vector indexes start from 0.) Note that $[\![\alpha]\!]\cdot\beta = \alpha\cdot\beta$, where on the right hand side "$\cdot$" denotes component-wise multiplication in $\mathbb{Z}_2^n$. That is, $\langle\alpha \cdot \beta\rangle_i = \langle\alpha\rangle_i \cdot \langle\beta\rangle_i$. Also, $J \cdot [\![\alpha]\!] \cdot \beta = \sum_{i=1}^{m-1} \langle\alpha\rangle_{i-1}\langle\beta\rangle_i = [\![J\alpha]\!] \cdot \beta = (J\alpha) \cdot \beta$ for any $\alpha, \beta \in \mathbb{Z}_2^m$.

Now, let $A \cdot \alpha = \beta$ be an arbitrary non-homogeneous matrix equation with $A \in \mathrm{Mat}_m(\mathbb{Z}_2)$ and $\alpha, \beta \in \mathbb{Z}_2^m$. This equation has a solution in $\alpha \in \mathbb{Z}_2^m$ iff $\mathrm{rank}(A) = \mathrm{rank}\begin{pmatrix}A\ \beta\end{pmatrix}$, where $\begin{pmatrix}A\ \beta\end{pmatrix}$ is a $m \times (m + 1)$ matrix. If there is at least one solution, the solution space is a subspace of $\mathbb{Z}_2^m$ of dimension $m - \mathrm{rank}(A)$. Hence, it has $2^{m-\mathrm{rank}(A)}$ elements. As an example, if $A$ is the identity matrix then $A \cdot \alpha = \beta$ has a solution iff $m = \mathrm{rank}(A) = \mathrm{rank}\begin{pmatrix}A\ \beta\end{pmatrix} = m$. (I.e., always.) Since $2^{m-\mathrm{rank}(A)} = 2^{m-m} = 2^0 = 1$, there is only one solution $\alpha \leftarrow \beta$.

*Bit-level operations.* Let $\alpha^{\ll k} := 2^k\alpha \mod 2^n$ be the left shift of $\alpha$ by $k$ bits. If the variables are seen as bit-vectors of length $m$ then the next operations have natural Boolean analogues: $\alpha\cdot\beta = \alpha\wedge\beta$ (multiplication in $\mathbb{Z}_2^m$ corresponds to the Boolean AND), $J^k\alpha = \alpha^{\ll k}$ (multiplication by $J^k$ corresponds to the left shift by $k$ positions) and $\neg\alpha$ corresponds to bit-negation. While we use the algebraic

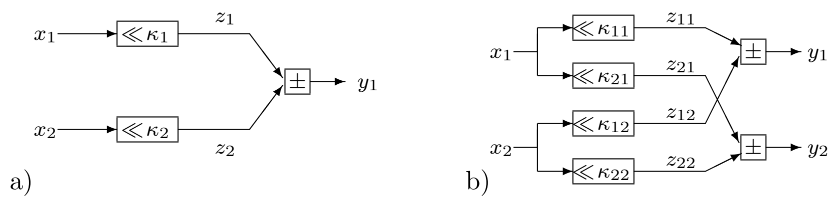


**Fig. 1.** Computational graph of a function a) $F \in \mathcal{L}_1$ with three internal nodes and of a function b) $F \in \mathcal{L}_2$ with 6 internal nodes

notation during this paper, keeping these few equivalences in mind should make it fairly simple to transform our formulas to efficient algorithms in any modern computer language.

*Carry and borrow.* For any $\alpha, \beta \in \mathbb{Z}_2^n$, let $\mathsf{carry}(\alpha, \beta) := \alpha \oplus \beta \oplus (\alpha + \beta)$ be the *carry* and $\mathsf{borrow}(\alpha, \beta) := \alpha \oplus \beta \oplus (\alpha - \beta)$ be the *borrow* of $\alpha$ and $\beta$. We often denote carry by $\mathsf{carry}^1$ and borrow by $\mathsf{carry}^0$.

*Differential Probability of Addition.* Let $\delta = (\Delta x_1, \Delta x_2 \to \Delta y)$ and $e = \mathsf{eq}(J\Delta x_1, J\Delta x_2, J\Delta y)$. In [LM01], Lipmaa and Moriai showed that, reformulated in our notation, $\mathsf{dp}^+(\delta) = 0$ when $e \cdot (\mathsf{xor}(\Delta x_1, \Delta x_2, \Delta y) \oplus J\Delta x_2) \neq 0$, and $\mathsf{dp}^+(\delta) = 2^{-w_h(\neg e)}$, otherwise.

# 3 Linear-Algebraic Viewpoint to Differential Probability

## 3.1 Differential Probability in Language of Matrix Equations

We proceed with computing the differential probabilities of some mappings of form $(x_1{}^{\lll \kappa_{11}} \pm x_2{}^{\lll \kappa_{12}}, x_1{}^{\lll \kappa_{21}} \pm x_2{}^{\lll \kappa_{22}})$. We call such functions *Quasi-Hadamard Transforms*. In this section, we develop a general framework for handling all mappings of form $F(x_1, x_2) = x_1{}^{\lll \kappa_1} + x_2{}^{\lll \kappa_2}$. In particular, we show that the differential probability of such a mapping is equal to $2^{-2n}$ times the number of solutions to a certain matrix equation. (The next section will concentrate on other mappings.)

For $\sigma \in \{0, 1\}$, let $z_1 \pm^{\sigma} z_2 := z_1 + (-1)^{\sigma} z_2$, and $\partial c^{\sigma} = \partial c^{\sigma}(z_1, z_2) := \mathsf{carry}^{\sigma}(z_1, z_2) \oplus \mathsf{carry}^{\sigma}(z_1^*, z_2^*)$. Consider the set $\mathfrak{A} := \{J^k : 0 \leq k < n\} \subset \mathrm{Mat}_n(\mathbb{Z}_2)$. Let $x = \begin{pmatrix} x_1 & x_2 \end{pmatrix}^T$. Let $\mathcal{L}_1 \subset \mathrm{Mat}_{1 \times 2}(\mathbb{Z}_{2^n})$ be such that $F \in \mathcal{L}_1$ iff for some $\sigma \in \{0, 1\}$, $F_1 \in \mathfrak{A}$ and $F_2 \in (-1)^{\sigma}\mathfrak{A}$. Equivalently, $F(x) = 2^{\kappa_1} x_1 \pm 2^{\kappa_2} x_2$. Such a function $F$ can alternatively be seen as a $\pm$-operation applied to the results of some left shift operations, with $z_1 = x_1{}^{\lll \kappa_1}$, $z_2 = x_2{}^{\lll \kappa_2}$ and $y = z_1 \pm^{\sigma} z_2$. (See Fig. 1.)

With this representation in mind, we will consistently denote $\Delta z_k := x_k{}^{\lll \kappa_k} \oplus (x_k^*)^{\lll \kappa_k}$ and $\partial y := y \oplus y^*$. Since the differential $x_k \xrightarrow{\lll \kappa_k} z_k$ has probability 1 then $\Delta z_k = \Delta x_k{}^{\lll \kappa_k}$ and $z_k^* = z_k \oplus \partial z_k$. As usual, we denote $x := (x_1, x_2)$ and

$\Delta x := (\Delta x_1, \Delta x_2)$. Let $F \in \mathcal{L}_1$. By definition, $\mathsf{dp}^F(\delta) = \Pr_x[(x_1{}^{\lll \kappa_1} \boxplus^{\sigma} x_2{}^{\lll \kappa_2}) \oplus ((x_1^*)^{\lll \kappa_1} \boxplus^{\sigma} (x_2^*)^{\lll \kappa_2}) = \Delta y] = \Pr_x[(z_1 \boxplus^{\sigma} z_2) \oplus (z_1^* \boxplus^{\sigma} z_2^*) = \Delta y] = \Pr_x[\partial y = \Delta y]$. Let $\boldsymbol{\sigma} \in \mathbb{Z}_{2^n}$ be the vector of $\sigma$-s, that is, $\boldsymbol{\sigma}_i = \sigma$, $\forall i$. The main result of this subsection is the following:

**Theorem 1.** *Fix a function $F \in \mathcal{L}_1$, and a differential $\delta = (\Delta x_1, \Delta x_2 \to \Delta y)$. For fixed $z = (z_1, z_2)$, let $c^\sigma := \mathsf{carry}^\sigma(z_1, z_2)$. Let $\omega = \omega(\delta), a = a(\delta, x) \in \mathbb{Z}_2^n$, $M = M(\delta) \in \mathrm{Mat}_{n \times 2n}(\mathbb{Z}_2)$ be defined as follows:*

$$\begin{aligned} \omega :=& J(\boldsymbol{\sigma} \cdot (\Delta z_1 \oplus \Delta y) \oplus \Delta z_1 \oplus \mathbf{1} \oplus \mathsf{eq}(\Delta z_1, \Delta z_2, \Delta y)) \oplus \\ & \mathsf{xor}(\Delta z_1, \Delta z_2, \Delta y) \ , \\ M :=& \left( J \cdot [\![\Delta z_1 \oplus \Delta y]\!] \cdot J^{\kappa_1} \ \ J \cdot [\![\Delta z_2 \oplus \Delta y]\!] \cdot J^{\kappa_2} \right) \ , \\ a :=& \omega \oplus J \cdot (\Delta z_1 \oplus \Delta z_2) \cdot c^\sigma \ . \end{aligned} \tag{1}$$

*Then $\mathsf{dp}^F(\delta) = \Pr_x[M \cdot x = a]$. Equivalently, $2^{2n} \cdot \mathsf{dp}^F(\delta)$ is equal to the number of solutions to the matrix equation $M \cdot x = a$ in ring $\mathbb{Z}_2$.*

Since $a$ depends on $c^\sigma$ and hence in a nontrivial manner on $x$, we must first get rid of the variable $c^\sigma$ in $a$ to find the number of solutions to the matrix equation $M \cdot x = a$. We will deal with this in the next subsection. Rest of the current subsection will give a proof of Theorem 1. First,

**Lemma 1.** *Let $F \in \mathcal{L}_1$ and let $x \in \mathbb{Z}_2^{2n}$ be such that $F(x) \oplus F(x \oplus \Delta x) = \Delta y$. Denote $q(\alpha, \beta, \gamma) := (\partial\beta \oplus \partial\gamma) \cdot \alpha \oplus (\partial\alpha \oplus \partial\gamma) \cdot \beta \oplus (\partial\alpha \oplus \partial\beta) \cdot \gamma$ and $\mathsf{desired}(\delta, x) := J \cdot (\neg\boldsymbol{\sigma} \cdot (\Delta z_2 \oplus \partial c^\sigma) \oplus \mathsf{maj}(\Delta z_1, \Delta z_2, \partial c^\sigma) \oplus q(z_1, z_2, c^\sigma)) \oplus \mathsf{xor}(\Delta z_1, \Delta z_2, \Delta y)$. Then*

$$\mathsf{desired}(\delta, x) = \mathbf{0} \ . \tag{2}$$

*In general, let $D$ be the event that (2) holds for an uniformly random $x$. Then $\mathsf{dp}^F(\delta) = \Pr[D]$.*

*Proof.* Let $c^1 = c = \mathsf{carry}(z_1, z_2)$ and $c^0 = b = \mathsf{borrow}(z_1, z_2)$. By definitions of carry and borrow, $\langle c \rangle_{i+1} = 1$ iff $\langle z_1 \rangle_i + \langle z_2 \rangle_i + \langle c \rangle_i \geq 2$ and $\langle b \rangle_{i+1} = 1$ iff $\langle z_1 \rangle_i < \langle z_2 \rangle_i + \langle b \rangle_i$. That is, $c^1 = c = J \cdot \mathsf{maj}(z_1, z_2, c)$ and $c^0 = b = J \cdot (z_2 \oplus b \oplus \mathsf{maj}(z_1, z_2, b))$. Thus, $c^\sigma = J \cdot (\neg\boldsymbol{\sigma} \cdot (z_2 \oplus c^\sigma) \oplus \mathsf{maj}(z_1, z_2, c^\sigma))$ and $\partial c^\sigma = J \cdot (\neg\boldsymbol{\sigma} \cdot (\Delta z_2 \oplus \partial c^\sigma) \oplus \mathsf{maj}(z_1, z_2, c^\sigma) \oplus \mathsf{maj}(z_1 \oplus \partial z_2, z_2 \oplus \partial z_2, c^\sigma \oplus \partial c^\sigma)) = J \cdot (\neg\boldsymbol{\sigma} \cdot (\Delta z_2 \oplus \partial c^\sigma) \oplus \mathsf{maj}(\Delta z_1, \Delta z_2, \partial c^\sigma) \oplus q(z_1, z_2, c^\sigma))$. But $F(x) \oplus F(x \oplus \Delta x) = \Delta y$ iff $\partial c^\sigma = \mathsf{xor}(\Delta z_1, \Delta z_2, \Delta y)$ and therefore $F(x) \oplus F(x \oplus \Delta x) = \Delta y$ iff $\mathsf{desired}(\delta, x) = \mathbf{0}$. Thus, $\mathsf{dp}^F(\delta) = \Pr[D]$. □

Our next step is to eliminate the auxiliary variable $\partial c^\sigma = c^\sigma \oplus (c^*)^\sigma$ that introduces non-linearity to the equation (2).

*Proof (Proof of Thm. 1.).* Define $r(\delta, x) := \prod_{i=0}^{n-1}(1 - \langle \mathsf{desired}(\delta, x) \rangle_i)$. By Lemma 1, $\mathsf{dp}^F(\delta) = \Pr[D]$, or equivalently, $2^{2n} \cdot \mathsf{dp}^F(\delta) = \sharp\{x : r(\delta, x) = 1\}$. Observe that $\mathsf{desired}(\delta, x) \neq \mathbf{0}$ iff there is a (minimal) $\ell_0$, such that $\langle \mathsf{desired}(\delta, x) \rangle_{\ell_0} = 1$. Hence, for any $\lambda(\delta, x)$, $r(\delta, x) = \prod_{i=0}^{n-1}(1 - \langle \lambda(\delta, x) \rangle_i)$, given that $\lambda(\delta, x) \equiv \mathsf{desired}(\delta, x) \pmod{2^{\ell_0+1}}$.

Now, $r(\delta, x) = 1$ iff $F(x) \oplus F(x \oplus \Delta x) = \Delta y$ iff $\partial c^\sigma = \mathsf{xor}(\Delta z_1, \Delta z_2, \Delta y)$. The same holds also for word lengths $n' < n$ with the variables that have been reduced modulo $2^{n'}$. Thus, when $\prod_{\ell=0}^{i-1}(1 - \langle \mathsf{desired}(\delta, x)\rangle_\ell) = 1$ then $\mathsf{desired}(\delta, x) \equiv 0 \pmod{2^i}$ and thus $J \cdot \partial c^\sigma \equiv J \cdot \mathsf{xor}(\Delta z_1, \Delta z_2, \Delta y) \pmod{2^{i+1}}$. Therefore, we set $\langle \lambda \rangle_i$ to be equal to $\langle \mathsf{desired}(\delta, x)\rangle_i$, except that we substitute every occurrence of $\langle J \cdot \partial c^\sigma \rangle_i$ in $\langle \mathsf{desired}(\delta, x)\rangle_i$ with an occurrence of $\langle J \cdot \mathsf{xor}(\Delta z_1, \Delta z_2, \Delta y)\rangle_i$. Since this applies for *every* $i$, what we do is that we substitute $J \cdot \partial c^\sigma$ with $J \cdot \mathsf{xor}(\Delta z_1, \Delta z_2, \Delta y)$ in $\mathsf{desired}(\delta, x)$.

Denote $\alpha = (\Delta z_1 \oplus \Delta y) \cdot z_1 \oplus (\Delta z_2 \oplus \Delta y) \cdot z_2 \oplus (\Delta z_1 \oplus \Delta z_2) \cdot c^\sigma$. By the previous discussion, $x$ is $\delta$-possible iff $\partial c^\sigma = \mathsf{desired}(\delta, x) \oplus \mathsf{xor}(\Delta z_1, \Delta z_2, \Delta y) = J \cdot (\neg \boldsymbol{\sigma} \cdot (\Delta z_2 \oplus \partial c^\sigma) \oplus \mathsf{maj}(\Delta z_1, \Delta z_2, \partial c^\sigma) \oplus q(z_1, z_2, c^\sigma)) = J \cdot (\boldsymbol{\sigma} \cdot (\Delta z_1 \oplus \Delta y) \oplus \mathbf{1} \oplus \Delta z_1 \oplus \mathsf{eq}(\Delta z_1, \Delta z_2, \Delta y) \oplus \alpha)$ is equal to $\mathsf{xor}(\Delta z_1, \Delta z_2, \Delta y)$. Therefore, $\mathsf{dp}^F(\delta) = \Pr_x[J \cdot \alpha = \omega] = \Pr_x[J \cdot \alpha = \omega] = \Pr_x[J \cdot ((\Delta z_1 \oplus \Delta y) \cdot J^{\kappa_1} x_1 \oplus (\Delta z_2 \oplus \Delta y) \cdot J^{\kappa_2} x_2) = a]$. The claim follows. □

### 3.2 Algorithm for $\mathsf{dp}^F$ for $F \in \mathcal{L}_1$

In the previous subsection we established that $2^{2n} \cdot \mathsf{dp}^F$ is equal to the number of solutions to a certain matrix equation $M \cdot x = a$. Initially, this matrix equation depended on both $\partial c^\sigma$ and $c^\sigma$. While we thereafter showed how to eliminate the dependency on $\partial c^\sigma$, we still have a matrix equation that depends on the carry $c^\sigma$. However, it is easy to show that this problem is not severe.

Let again $\sigma \in \{0, 1\}$ and let $F \in \mathcal{L}_1$, $F(x_1, x_2) = 2^{\kappa_1} x_1 \overset{\sigma}{+} 2^{\kappa_2} x_2$. As in the proof of Thm. 1, we can consider the matrix equation $M \cdot x = a$ as a system of equations in $\mathbb{Z}_2$, starting with bit $i = 0$. Now, for every $i$, $\langle c^\sigma \rangle_i$ is already fixed and known when we look at the row $i$, since it is a function of the "previous" bits of $x_1$ and $x_2$. Hence, $J \cdot [\![\Delta z_1 \oplus \Delta z_2]\!] \cdot c^\sigma = J \cdot (\Delta z_1 \oplus \Delta z_2) \cdot c^\sigma$ is a constant (although, an a priori unknown) vector and therefore, $a$ is a constant vector. Therefore, we have proven that

$$\mathsf{dp}^F(\delta) = \begin{cases} 0 \ , & \operatorname{rank}(M) \neq \operatorname{rank}\begin{pmatrix} M & a \end{pmatrix} \ , \\ 2^{-\operatorname{rank}(M)} \ , & \text{otherwise} \ . \end{cases} \tag{3}$$

Next we will compute the ranks of associated matrices $M$ and $\begin{pmatrix} M & a \end{pmatrix}$. (Note that here $a = a(\delta)$ does not depend on $x$ anymore.) For this, we must introduce an additional assumption $\kappa_1 \leq \kappa_2 + 1$. The reasoning behind this assumption will become obvious from the proof of Thm. 2.

**Theorem 2.** *Let $E_k \in \mathbb{Z}_2^n$ be the vector with $\langle E_k \rangle_i = 1$ iff $i \geq k$. (That is, $E_k = \neg(2^k - 1)$ when seen as an element of $\mathbb{Z}_{2^n}$.) Let us denote $e_j := J((\Delta z_j \oplus \Delta y) \cdot E_{\kappa_j})$ and $e := e_1 \vee e_2$. Let $F(x_1, x_2) = z_1 \overset{\sigma}{+} z_2 \in \mathcal{L}_1$ be such that $\kappa_1 \leq \kappa_2 + 1$. Then*

$$\mathsf{dp}^F(\delta) = \begin{cases} 0 \ , & \neg e \cdot (J(\neg \boldsymbol{\sigma} \cdot (\Delta z_1 \oplus \Delta y) \oplus \Delta z_2) \oplus \mathsf{xor}(\Delta z_1, \Delta z_2, \Delta y)) \neq 0 \ , \\ 2^{-w_h(e)} \ , & \textit{otherwise.} \end{cases}$$

*Equivalently, Algorithm 1 computes $\mathsf{dp}^F(\delta)$ in time $O(\log n)$, given a RAM model of computation.*

**Algorithm 1** An $O(\log n)$-time algorithm for computing $\mathsf{dp}^F(\Delta x_1, \Delta x_2 \to \Delta y)$ where $F(x_1, x_2) = 2^{\kappa_1} x_2 \pm^{\sigma} 2^{\kappa_2} x_2$. Here we assume that $\kappa_1 \le \kappa_2 + 1$

INPUT: $(\Delta x_1, \Delta x_2 \to \Delta y)$ and $F$ as represented by $\kappa_j$ and $\sigma \in \{0, 1\}$
OUTPUT: $\mathsf{dp}^F(\Delta x_1, \Delta x_2 \to \Delta y)$

1. Let $\Delta z_j \leftarrow \Delta x_j{}^{\lll \kappa_j}$ for $j \in \{1, 2\}$;
2. Let $e_j \leftarrow ((\Delta z_j \oplus \Delta y) \wedge \neg(2^{\kappa_j} - 1))^{\lll 1}$ for $j \in \{1, 2\}$;
3. Let $e \leftarrow e_1 \vee e_2$;
4. If $\neg e \wedge (((\neg \boldsymbol{\sigma} \wedge (\Delta z_1 \oplus \Delta y)) \oplus \Delta z_2)^{\lll 1} \oplus \Delta z_1 \oplus \Delta z_2 \oplus \Delta y)$ then return 0 ;
5. Return $2^{-w_h(e)}$.

(Algorithm 1 works in time $O(\log n)$ since the Hamming weight $w_h$ can be computed in time $O(\log n)$ when working in the RAM model [LM01].)

*Proof.* Recall that by Thm. 1, $\mathsf{dp}^F(\delta) = \Pr_x[M \cdot x = a]$. Therefore, $\mathsf{dp}^F(\delta) = 0$ if $\operatorname{rank}(M) \neq \operatorname{rank}\begin{pmatrix} M & a \end{pmatrix}$, and $\mathsf{dp}^F(\delta) = 2^{-\operatorname{rank}(M)}$, otherwise. Next, for any vector $v$, $(J[\![v]\!]J^{\kappa_k})_{ij} = \langle v \rangle_{i-2}$ when $j = i - 1 - \kappa_k$ and $i > \kappa_k + 1$, and $(J[\![v]\!]J^{\kappa_k})_{ij} = 0$, otherwise. (Recall that the bits $\langle v \rangle_i$ are counted from $i = 0$ to $i = n - 1$.) Therefore, $\operatorname{rank}(M) = \operatorname{rank}\begin{pmatrix} J[\![\Delta z_1 \oplus \Delta y]\!]J^{\kappa_1} & J[\![\Delta z_2 \oplus \Delta y]\!]J^{\kappa_2} \end{pmatrix} = \sharp\{i \in [1, n] : (J[\![\Delta z_1 \oplus \Delta y]\!]J^{\kappa_1})_{i,i-\kappa_1-1} = 1 \vee (J[\![\Delta z_2 \oplus \Delta y]\!]J^{\kappa_2})_{i,i-\kappa_2-1} = 1\} = \sharp\{i \in [0, n-1] : \langle E_{\kappa_1} \cdot J(\Delta z_1 \oplus \Delta y) \rangle_i = 1 \vee \langle E_{\kappa_2} J(\Delta z_2 \oplus \Delta y) \rangle_i = 1\} = w_h(E_{\kappa_1} \vee E_{\kappa_2}) = w_h(e)$. That is, if $\delta$ is $F$-possible, then $\mathsf{dp}^F(\delta) = 2^{-w_h(e)}$.

Let us next establish when the equation $M \cdot x = a$ does not have any solutions. Since $M$ is an echelon matrix up to the permutation of rows, then $\operatorname{rank}\begin{pmatrix} M & a \end{pmatrix} \neq \operatorname{rank}(M)$ only if for some $i \in [0, n-1]$, $(M_1)_{i+1,i-\kappa_1} = (M_2)_{i+1,i-\kappa_2} = 0$ but $\langle a \rangle_i = 1$. This happens iff for some $i \in [0, n-1]$, $\langle e_1 \rangle_i = \langle e_2 \rangle_i = 0$ (i.e., $\langle e_1 \vee e_2 \rangle_i = 0$) but $\langle a \rangle_i = \langle \omega \oplus J(\Delta z_1 \oplus \Delta z_2) \cdot c^\sigma \rangle_i = 1$. Thus, $\delta$ is $F$-impossible iff $\neg(e_1 \vee e_2) \cdot (\omega \oplus J(\Delta z_1 \oplus \Delta z_2) \cdot c^\sigma) \neq 0$. (Recall that $\omega = J(\boldsymbol{\sigma} \cdot (\Delta z_1 \oplus \Delta y) \oplus \Delta z_1 \oplus \mathbf{1} \oplus \mathsf{eq}(\Delta z_1, \Delta z_2, \Delta y)) \oplus \mathsf{xor}(\Delta z_1, \Delta z_2, \Delta y)$.)

We are only left to prove that the next two facts hold in the case $\langle e_1 \vee e_2 \rangle_i = 0$, or equivalently, in the case $\langle e_1 \rangle_i = \langle e_2 \rangle_i = 0$. First, $\langle J(\Delta z_1 \oplus \mathbf{1} \oplus \mathsf{eq}(\Delta z_1, \Delta z_2, \Delta y)) \rangle_i = \langle J \cdot \mathsf{xor}(\Delta z_1, \Delta z_2, \Delta y) \rangle_i$. Really, if $i \ge \kappa_1$ then $\langle e_1 \rangle_i = 0 \Rightarrow \langle \Delta z_1 \rangle_{i-1} = \langle \Delta y \rangle_{i-1}$ and therefore $\langle \Delta z_1 \oplus \mathbf{1} \oplus \mathsf{eq}(\Delta z_1, \Delta z_2, \Delta y) \rangle_i = \langle \mathsf{xor}(\Delta z_1, \Delta z_2, \Delta y) \rangle_i$. Otherwise, if $i \ge \kappa_2$ then $\langle \Delta z_2 \rangle_{i-1} = \langle \Delta y \rangle_{i-1}$ and thus $\langle \Delta z_1 \oplus \mathbf{1} \oplus \mathsf{eq}(\Delta z_1, \Delta z_2, \Delta y) \rangle_i = \langle \Delta y \rangle_i$. (Since $\kappa_1 \le \kappa_2 + 1$ we can ignore this case.) Finally, let $i \le \min(\kappa_1, \kappa_2)$. Then $\langle \Delta z_1 \rangle_{i-1} = \langle \Delta z_2 \rangle_{i-1} = 0$ and therefore $\langle \Delta z_1 \oplus \mathbf{1} \oplus \mathsf{eq}(\Delta z_1, \Delta z_2, \Delta y) \rangle_i = \langle \mathbf{1} \oplus \mathsf{eq}(0, 0, \Delta y) \rangle_i = \langle \mathsf{xor}(\Delta z_1, \Delta z_2, \Delta y) \rangle_i$.

Second, $\langle J(\Delta z_1 \oplus \Delta z_2) \cdot c^\sigma \rangle_i = 0$. Really, first assume $\sigma = 1$. If $i \le \kappa_1$ then $\langle J^{\kappa_1} x_1 \rangle_{i-1} = \langle x_1 \rangle_{i-\kappa_1-1} = 0$ and hence $\langle c^1 \rangle_i = 0$, and therefore $\langle J(\Delta z_1 \oplus \Delta z_2) \cdot c^1 \rangle_i = 0$. The case $i \le \kappa_2$ is dual. On the other hand, when $i > \max(\kappa_1, \kappa_2)$ then $\langle J \cdot (\Delta z_1 \oplus \Delta z_2) \cdot c^\sigma \rangle_i = \langle (e_1 \oplus e_2) \cdot c^\sigma \rangle_i = 0$.

Let us now consider the case $\sigma = 0$. If $i \le \kappa_2$ then $\langle c^0 \rangle_i = \langle (\mathbf{1} \oplus z_1) \cdot c^0 \rangle_{i-1}$, which means that $c^0 \equiv 0 \pmod{2^{\kappa_2}}$. Otherwise, if $i \le \kappa_1$ then $\langle c^0 \rangle_i = 1 \iff \langle z_2 \oplus c^0 \rangle_{i-1} = 1$, which means that $c^0 \equiv \overline{(2^{\mathsf{ntz}(z_2)+1} - 1)} \pmod{2^{\kappa_1}}$. (Since $\kappa_1 \le$

$\kappa_2 + 1$ we can ignore this case.) If $i \geq \max(\kappa_1, \kappa_2)$ then $\langle J(\Delta z_1 \oplus \Delta z_2)c^0\rangle_i = 0$ due to $\langle J(e_1 \oplus e_2)\rangle_i = 0$. □

**Corollary 1.** *Let $+(x_1, x_2) = x_1 + x_2$ be the $\mathbb{Z}_{2^n}$-addition mapping and let $-(x_1, x_2) = x_1 - x_2$ be the $\mathbb{Z}_{2^n}$-subtraction mapping. Recall that $\alpha \vee \beta = \alpha \oplus \beta \oplus \alpha \cdot \beta$. First, the differential $\delta$ is $+$-impossible if $\neg(J \cdot (\Delta x_1 \oplus \Delta y) \vee J \cdot (\Delta x_2 \oplus \Delta y)) \cdot (\mathsf{xor}(\Delta x_1, \Delta x_2, \Delta y) \oplus J \cdot \Delta x_2) \neq 0$. Otherwise, $\mathsf{dp}^{+}(\delta) = 2^{-w_h(J \cdot (\Delta x_1 \oplus \Delta y) \vee J \cdot (\Delta x_2 \oplus \Delta y))}$. Second, $\mathsf{dp}^{-}(\delta) = \mathsf{dp}^{+}(\delta)$ for any $\delta$.*

*Proof.* First claim is trivial. For the proof of the second claim it is sufficient to observe that in this case, $\kappa_1 = \kappa_2 = 0$, and that in the third paragraph of the proof of Theorem 2, if $\langle e_1\rangle_i = \langle e_2\rangle_i = 0$ then $\langle \omega\rangle_i = \langle J \cdot (\Delta x_1 \oplus \mathbf{1} \oplus \mathsf{eq}(\Delta x_1, \Delta x_2, \Delta y)) \oplus \mathsf{xor}(\Delta x_1, \Delta x_2, \Delta y)\rangle_i = \langle J \cdot \Delta x_1 \oplus \mathsf{xor}(\Delta x_1, \Delta x_2, \Delta y)\rangle_i = \langle J \cdot \Delta x_2 \oplus \mathsf{xor}(\Delta x_1, \Delta x_2, \Delta y)\rangle_i$ for $i > \max(\kappa_1, \kappa_2) = 0$. □

The formula for $\mathsf{dp}^{+}$, presented in Corollary 1, is equivalent to the formula from [LM01]. Its complete proof is somewhat longer than the one in [LM01]. However, our proof is based on a more scalable approach, that allows us to find similar formulas for other related mappings like subtraction, without having to write down yet another, somewhat different, proofs.

**Corollary 2.** *Let $x, \Delta x, \Delta y \in \mathbb{Z}_{2^n}$. Let $F = +_\alpha$ be the unary operation that adds the constant $\alpha$ to its single argument, $F(x) = x + \alpha$. Let $\delta = (\Delta x \to \Delta y)$. Then, by definition, $\mathsf{dp}^{+_\alpha}(\delta) = \Pr_x[(x + \alpha) \oplus ((x \oplus \Delta x) + \alpha)]$. Then $\delta$ is $+_\alpha$-impossible iff $\neg(J \cdot (\Delta x_1 \oplus \Delta y)) \cdot \neg(J \cdot \Delta y) \cdot (\Delta x_1 \oplus \Delta y) \neq 0$. Otherwise, $\mathsf{dp}^{+}(\delta) = 2^{-w_h((J \cdot (\Delta x_1 \oplus \Delta y) \vee J \cdot \Delta y))}$.*

*Proof.* Straightforward from Corollary 1. □

## 4 The Pseudo-Hadamard Transform

### 4.1 Generalization to 2 × 2 Matrices

Next, we will look at a slightly more general case. Namely, assume that $\mathcal{L}_2 \subset \mathrm{Mat}_2(\mathbb{Z}_{2^n})$ is such that

$$F = \begin{pmatrix} F_{11} & F_{12} \\ F_{21} & F_{22} \end{pmatrix} \in \mathcal{L}_2$$

iff for some $\sigma \in \{0, 1\}$, $F_{j1} \in \mathfrak{A}$ and $F_{j2} \in (-1)^\sigma \mathfrak{A}$. Then $F(x) = (2^{\kappa_{12}} x_1 +^{\sigma} 2^{\kappa_{12}} x_2, 2^{\kappa_{22}} x_1 +^{\sigma} 2^{\kappa_{22}} x_2)$, for some $\kappa_{jk} \geq 0$. Alternatively, such mappings $F$ can be described by using a computation graph with $z_{ij} = x_j^{\ll \kappa_{ij}}$ and $y_i = z_{i1} \pm z_{i2}$. (See Figure 1.) We call the mappings from $\mathcal{L}_2$ the *Quasi-Hadamard Transforms*. Next, let us state some generalizations of previous results.

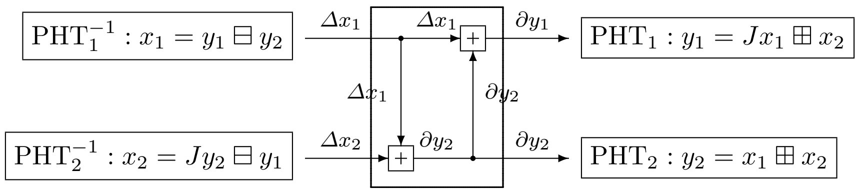


**Fig. 2.** Propagation of differences during the Pseudo-Hadamard Transform

**Lemma 2.** *[Generalization of Thm 1.] Let* $\delta = (\Delta x \to \Delta y)$ *with* $\Delta x, \Delta y \in \mathbb{Z}_2^{2n}$. *For* $j \in \{1, 2\}$, *let* $\omega_j := J \cdot (\boldsymbol{\sigma} \cdot (\Delta z_{j1} \oplus \Delta y_j) \oplus \Delta z_{j1} \oplus \mathbf{1} \oplus \mathsf{eq}(\Delta z_{j1}, \Delta z_{j2}, \Delta y_j)) \oplus \mathsf{xor}(\Delta z_{j1}, \Delta z_{j2}, \Delta y_j)$. *Let*

$$M = M(\delta) := \begin{pmatrix} J \cdot [\![\Delta z_{11} + \Delta y_1]\!] J^{\kappa_{11}} & J \cdot [\![\Delta z_{12} + \Delta y_1]\!] J^{\kappa_{12}} \\ J \cdot [\![\Delta z_{21} + \Delta y_2]\!] J^{\kappa_{21}} & J \cdot [\![\Delta z_{22} + \Delta y_2]\!] J^{\kappa_{22}} \end{pmatrix} ,$$

$$a = a(\delta, x) := \begin{pmatrix} \omega_1 \oplus J \cdot (\Delta z_{11} \oplus \Delta z_{12}) \cdot c_1^{\sigma} \\ \omega_2 \oplus J \cdot (\Delta z_{21} \oplus \Delta z_{22}) \cdot c_2^{\sigma} \end{pmatrix} .$$

*Then* $\mathsf{dp}^F(\delta) = \Pr_x[M \cdot x = a]$.

*Proof.* Straightforward corollary of Theorem 1. □

Note that Thm. 1 can additionally be generalized to more than 2-dimensional matrices.

### 4.2 Analysis of PHT

While Lemma 2 is a simple generalization of our previous result for $F \in \mathcal{L}_1$, we cannot proceed by using exactly the same methodology as in Thm. 2. The reason is that here we cannot assume that the carries are constant so as to use simple linear algebra to derive the number of solutions to $M \cdot x = a$. However, it comes out that at least in some special cases the value of $\mathsf{dp}^F$ will depend on the values of $\mathsf{dp}^{F'}$ for some functions $F'$ in class $\mathcal{L}_1$.

If $F \in \mathcal{L}_2$ is an invertible mapping then $\det F = (-1)^{\sigma} 2^{\kappa_{11}} 2^{\kappa_{22}} - (-1)^{\sigma} 2^{\kappa_{12}} 2^{\kappa_{22}} \neq 0$ and

$$F^{-1} = \frac{1}{\det F} \begin{pmatrix} (-1)^{\sigma} 2^{\kappa_{22}} & -(-1)^{\sigma} 2^{\kappa_{12}} \\ -2^{\kappa_{21}} & 2^{\kappa_{11}} \end{pmatrix} ,$$

or $F^{-1}(y_1, y_2) = \frac{1}{\det F}((-1)^{\sigma} 2^{\kappa_{22}} y_1 - (-1)^{\sigma} 2^{\kappa_{12}} y_2, 2^{\kappa_{11}} y_2 - 2^{\kappa_{21}} y_1)$. Let $\Delta x, \Delta y \in \mathbb{Z}_{2^{2n}}$. Clearly, $\delta = (\Delta x \to \Delta y)$ is $F$-possible iff $\delta^{-1} = (\Delta y \to \Delta x)$ is $F^{-1}$-possible. The most important of invertible mapping $F \in \mathcal{L}_2$ from a cryptographic viewpoint,

$$F = \mathrm{PHT} = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix} \quad \text{with} \quad \mathrm{PHT}^{-1} = \begin{pmatrix} 1 & -1 \\ -1 & 2 \end{pmatrix} ,$$

is called the *Pseudo-Hadamard Transform* (PHT, [Mas93]). The PHT is employed in block ciphers like SAFER [Mas93] and Twofish [SKW+99] for achieving better diffusion. (See Figure 2.)

For $j \in \{0,1\}$, let $F_j(x)$ denote the projection of $F(x)$ to the $j$th coordinate. That is, $F_j(x_1, x_2) = 2^{\kappa_{j1}} x_1 \stackrel{\sigma}{+} 2^{\kappa_{j2}} x_2$. By definition, $\mathsf{dp}^{F_j}(\Delta x_1, \Delta x_2 \to \Delta y_1) = \Pr_x[(2^{\kappa_{j1}} x_1 \stackrel{\sigma}{+} 2^{\kappa_{j2}} x_2) \oplus ((2^{\kappa_{j1}} x_1 \oplus \Delta x_1) \stackrel{\sigma}{+} (2^{\kappa_{j2}} x_2 \oplus \Delta x_2)) = \Delta y_1]$. In particular, $\mathrm{PHT}_1(x_1, x_2) = 2x_1 + x_2$ and $\mathrm{PHT}_2(x_1, x_2) = x_1 + x_2$.

**Theorem 3.** *Let us denote* $e_{kj} := J((\Delta z_{kj} \oplus \Delta y_k) \cdot E_{\kappa_{kj}})$. *Let* $e_j := e_{j1} \vee e_{j2}$. *(1)* $\delta$ *is PHT-possible iff all next four differential probabilities are positive:* $\mathsf{dp}^{\mathrm{PHT}_1}(\Delta x_1, \Delta x_2 \to \Delta y_1)$, $\mathsf{dp}^{\mathrm{PHT}_2}(\Delta x_1, \Delta x_2 \to \Delta y_2)$, $\mathsf{dp}^{\mathrm{PHT}_1^{-1}}(\Delta y_1, \Delta y_2 \to \Delta x_1)$, $\mathsf{dp}^{\mathrm{PHT}_2^{-1}}(\Delta y_2, \Delta y_1 \to \Delta x_2)$. *(2) If* $\delta$ *is* PHT*-possible, then* $\mathsf{dp}^{\mathrm{PHT}}(\delta) = \mathsf{dp}^{+}(\Delta x_1, \Delta x_2 \to \Delta y_2) \cdot 2^{-w_h(e_1 \cdot J(\neg(\mathsf{eq}(\Delta x_1, \Delta y_1, \Delta y_2))) \cdot J(\neg(\mathsf{eq}(\Delta x_2, \Delta y_1, J\Delta y_2))))}$.

*Proof (Sketch.).* $(1, \Rightarrow)$ Straightforward: since PHT is invertible then $\delta = (\Delta x \to \Delta y)$ is PHT-possible iff $\delta^{-1} = (\Delta y \to \Delta x)$ is $\mathrm{PHT}^{-1}$-possible. Rest of the proof is omitted from the extended abstract. □

Equivalently, $\delta$ is PHT-possible iff $\langle J\Delta x_1 \oplus \Delta x_2 \oplus \Delta y_1 \rangle_i = 0$ and the next four differential probabilities are positive: $\mathsf{dp}^{+}(\Delta x_1, \Delta x_2 \to \Delta y_1)$, $\mathsf{dp}^{+}(\Delta x_1, \Delta x_2 \to \Delta y_2)$, $\mathsf{dp}^{+}(\Delta y_1, \Delta y_2 \to \Delta x_1)$, $\mathsf{dp}^{+}(J\Delta y_2, \Delta y_1, \Delta x_2)$. (Note that all four differential probabilities can be computed by using Algorithm 1.) Moreover, a computationally slightly less expensive formula for $\mathsf{dp}^{\mathrm{PHT}}$ is $\mathsf{dp}^{\mathrm{PHT}}(\delta) = 2^{-w_h(e_2)} \cdot 2^{-w_h(e_1) \cdot J(\neg(\mathsf{eq}(\Delta x_1, \Delta y_1, \Delta y_2))) \cdot J(\neg(\mathsf{eq}(\Delta x_2, \Delta y_1, J\Delta y_2))))}$.

Based on Theorem 3 one can build a $\Theta(\log n)$-time algorithm for computing the value of $\mathsf{dp}^{\mathrm{PHT}}$ in the RAM model by using the same ideas as in [LM01].

## 5 Application to Twofish

In their paper [MR02], Murphy and Robshaw proposed an interesting new methodology for attacking Twofish by first finding a good characteristic and then fixing such key-dependent S-boxes that satisfy this characteristic. However, their concrete approach is somewhat heuristic and based on computer experiments. For example, in [MR02, Section 4.1] they choose a differential $(0, \Delta z_2)$, such that the differential probability of $(0, \Delta z_2 \to \Delta z_2, \Delta z_2)$ w.r.t. the PHT and averaged sub-key additions (see Fig. 3) would be large. As they established experimentally, choosing $\Delta z_2 =$ `A0E080A0` results in a probability $p = 2^{-14}$, where $p$ was determined experimentally averaged over random inputs and random additive round keys. No motivation was given in their paper why this concrete differential was chosen instead of some others.

Based on our formula for $\mathsf{dp}^{\mathrm{PHT}}$ we are able to determine that

**Theorem 4.** *Let* $F$ *be the part of the Twofish's round that contains S-boxes, MDS-s and the PHT. Let the input-to-*$F$ *difference* $\Delta x = \begin{pmatrix}\Delta x_1 & 0\end{pmatrix}^T$ *be chosen such that only one of the four S-boxes becomes active. Then* $\mathsf{dp}^{F}(0, \Delta z_2 \to$

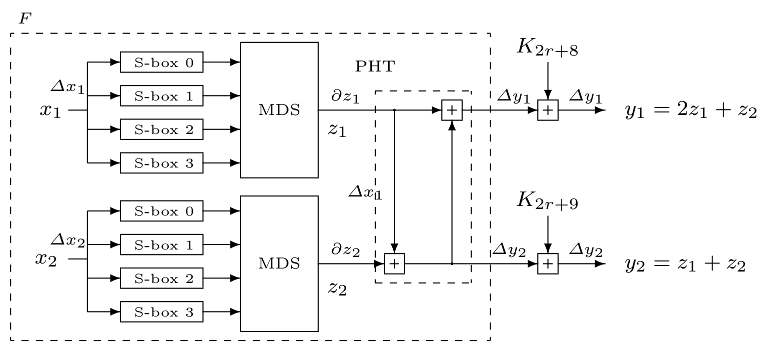


**Fig. 3.** Propagation of differences within a partial round of Twofish

**Table 1.** Optimal differences for the partial Twofish round function

| $(\Delta x_1, \Delta x_2)$ | $\delta = (0, \Delta z_2 \to \Delta z_2, \Delta z_2)$ | $\mathsf{dp}^F(\delta)$ |
|---|---|---|
| 1 active S-box | | |
| (00000000, 00000080) | (00000000, e0e0a080 → e0e0a080, e0e0a080) | $2^{-13}$ |
| (00000000, 00000400) | (00000000, 04050707 → 04050707, 04050707) | $2^{-13}$ |
| (00000000, 00008000) | (00000000, 80a0e0e0 → 80a0e0e0, 80a0e0e0) | $2^{-12}$ |
| (00000000, 00008900) | (00000000, 89f10101 → 89f10101, 89f10101) | $2^{-13}$ |
| (00000000, 00040000) | (00000000, 07040705 → 07040705, 07040705) | $2^{-13}$ |
| (00000000, 00800000) | (00000000, e080e0a0 → e080e0a0, e080e0a0) | $2^{-13}$ |
| (00000000, 04000000) | (00000000, 05070405 → 05070405, 05070405) | $2^{-13}$ |
| (00000000, 80000000) | (00000000, a0e080a0 → a0e080a0, a0e080a0) | $2^{-12}$ |
| Two active S-boxes | | |
| (00000000, 00040004) | (00000000, 00030201 → 00030201, 00030201) | $2^{-6}$ |
| (00000000, 004e00ed) | (00000000, 80004204 → 80004204, 80004204) | $2^{-6}$ |
| (00000000, 00696900) | (00000000, c0400080 → c0400080, c0400080) | $2^{-6}$ |
| (00000000, 04000004) | (00000000, 02000101 → 02000101, 02000101) | $2^{-5}$ |
| (00000000, 08000008) | (00000000, 04000202 → 04000202, 04000202) | $2^{-6}$ |
| (00000000, 10000010) | (00000000, 08000404 → 08000404, 08000404) | $2^{-6}$ |
| (00000000, 20000020) | (00000000, 10000808 → 10000808, 10000808) | $2^{-6}$ |
| (00000000, 40000040) | (00000000, 20001010 → 20001010, 20001010) | $2^{-6}$ |
| (00000000, 69000069) | (00000000, 80004040 → 80004040, 80004040) | $2^{-4}$ |
| (00000000, 80000080) | (00000000, 40002020 → 40002020, 40002020) | $2^{-6}$ |
| (00000000, 69690000) | (00000000, 80c0c000 → 80c0c000, 80c0c000) | $2^{-6}$ |
| Three active S-boxes | | |
| (00000000, 0017eb43) | (00000000, 80000041 → 80000041, 80000041) | $2^{-3}$ |
| (00000000, 3a00a6e8) | (00000000, 80008000 → 80008000, 80008000) | $2^{-2}$ |
| (00000000, 53001d53) | (00000000, 80400000 → 80400000, 80400000) | $2^{-2}$ |
| (00000000, 25a61f00) | (00000000, 01800000 → 01800000, 01800000) | $2^{-3}$ |

*$\Delta z_2, \Delta z_2) \geq 2^{-13}$ only in the 8 cases, depicted in Table 1. Therefore, the differential with $\Delta z_2 =$ `A0E080A0` chosen in [MR02] is optimal for $F$ under the given constraints, and there is only one another differential with $\Delta z_2 =$ `80A0E0E0` that has the same differential probability. Analogously, if two S-boxes are allowed to be active then there are 11 different differentials $(0, \Delta z_2)$, such that $\mathsf{dp}^F(0, \Delta z_2 \to \Delta z_2, \Delta z_2) \geq 2^{-6}$. If three S-boxes are active then there are 4 differentials $(0, \Delta z_2)$, such that $\mathsf{dp}^F(0, \Delta z_2 \to \Delta z_2, \Delta z_2) \geq 2^{-3}$.*

*Proof.* One can prove this by doing by exhaustive search over $2^{10} = 1024$ (in the one active S-box case), $3 \cdot 2^{17}$ (in the two active S-boxes case) or $3^2 \cdot 2^{26}$ (in three active S-boxes case) differentials. □

In all cases, one spends $\Theta(\log n)$ steps for computing the corresponding differential probability. Thus, our method is still efficient with 3 active S-boxes.

One of the conclusions of this lemma is that if two active S-boxes can be tolerated then it is possible to find a differential that is $2^8$ times more probable—this sharp growth might, in some situations, compensate the need for the second active S-box, and therefore potentially lead to some attack against Twofish.

## 6 Conclusions

We extended the previous results of Lipmaa and Moriai [LM01] by developing a linear-algebraic framework for proving the differential properties for addition (in $\mathbb{Z}_{2^n}$) and related functions w.r.t. the XOR (or addition in $\mathbb{Z}_2^n$). While [LM01] exhaustively analysed the addition itself but gave no guidelines for how to analyse related functions, we were able to compute differential probabilities of different functions like the subtraction and the Pseudo-Hadamard transformation as the special cases of our general approach. Our proof methods might be of independent interest. For example, we showed that the differential probability of $2^\alpha x \pm 2^\beta y$, $\alpha \leq \beta + 1$, is equal to the number of solutions to a certain matrix equation. Due to the lack of space, this extended abstract has been shortened by omitting the complete solution for $\mathsf{dp}^F$ for *any* $F \in \mathcal{L}_2$ and several proofs. Corresponding formulas will appear in the full version.

We ended the paper by presenting optimal differentials for the partial Twofish round function. In particular, we were able to prove formally that a certain differential found by Murphy and Robshaw is really optimal under given conditions. We also presented other differentials that are optimal under somewhat general conditions. These results show that the results of the current paper are not only theoretical but might be directly applicable in practical cryptanalysis.

Together with [LM01], the current paper presents a positive step forward in helping to construct ciphers that are secure against differential cryptanalysis. While until now, the differential properties of ciphers that include both modular addition and exclusive OR-s have only found experimentally by heuristic methods, our results make it possible to prove rigorously lower bounds on differential attacks of at least some ciphers. As compared to [LM01], our paper stepped significantly closer to the reality, since we were able to prove that some differentials used in an actual attack are optimal.

Finally, all results of this paper have been implemented in the C language and verified by using a computer. In particular, it took about 30 seconds for a 1.4 GHz Athlon to produce the numbers in Table 1.

### Acknowledgments and Further Work

This work was partially supported by the Finnish Defense Forces Research Institute of Technology. We would like to thank Stefan Lucks, Markku-Juhani Olavi Saarinen and anonymous referees for useful comments.

An interesting open question is whether our methods can be applied to a more general class of mappings than $\mathcal{L}_2$. We hope that more applications of our results to the real ciphers will be found in the future.

The need for partial exhaustive search in Thm. 4 was caused by the nontrivial preconditions on the inputs. When there are no such preconditions (that is, all $2^{32}$ values $\Delta z_2$ are allowed), we hope that an analytic formula can be derived for optimal differentials, akin to the ones presented in [LM01] for optimal differentials of additions. It might even be true that there is a closed-form formula for optimal differentials when $\Delta z_2$ is restricted.

## References

[BS91] Eli Biham and Adi Shamir. Differential Cryptanalysis of DES-like Cryptosystems. *Journal of Cryptology*, 4(1):3–72, 1991.

[JK97] Thomas Jakobsen and Lars Knudsen. The Interpolation Attack on Block Ciphers. In Eli Biham, editor, *Fast Software Encryption '97*, volume 1267 of *Lecture Notes in Computer Science*, pages 28–40, Haifa, Israel, January 1997. Springer-Verlag.

[LM01] Helger Lipmaa and Shiho Moriai. Efficient Algorithms for Computing Differential Properties of Addition. In Mitsuru Matsui, editor, *Fast Software Encryption '2001*, volume 2355 of *Lecture Notes in Computer Science*, pages 336–350, Yokohama, Japan, 2–4 April 2001. Springer-Verlag, 2002.

[Mas93] James L. Massey. SAFER K-64: A Byte-Oriented Block-Ciphering Algorithm. In Ross Anderson, editor, *Fast Software Encryption '93*, volume 809 of *Lecture Notes in Computer Science*, pages 1–17, Cambridge, UK, 9–11 December 1993. Springer-Verlag.

[MR02] S. Murphy and M. J. B. Robshaw. Key-dependent S-boxes and Differential Cryptanalysis. *Designs, Codes and Cryptography*, 27(3):229–255, 2002.

[Sch92] Claus-Peter Schnorr. FFT-Hash II, Efficient Cryptographic Hashing. In Rainer A. Rueppel, editor, *Advances in Cryptology — EUROCRYPT '92*, volume 658 of *Lecture Notes in Computer Science*, pages 45–54, Balatonfüred, Hungary, 24–28 May 1992. Springer-Verlag. ISBN 3-540-56413-6.

[SKW+99] Bruce Schneier, John Kelsey, Doug Whiting, David Wagner, Chris Hall, and Niels Ferguson. *The Twofish Encryption Algorithm: A 128-Bit Block Cipher*. John Wiley & Sons, April 1999. ISBN: 0471353817.