A Way Reduce Signed Bitwise Differences that Transformed Into Same Modular Differences

Xu ZiJie and Xu Ke

xuzijiewz@gmail.com
xukezp@gmail.com

Abstract. We study signed bitwise differences and modular differences. We find a way to reduce signed bitwise differences that can be transformed into same modular differences. In this way, it needs arithmetic difference. We establish one-one relationship between modular differences and arithmetic difference. And establish one-one relationship between signed bitwise differences and arithmetic difference. Then it will reduce signed bitwise differences that can be transformed into same arithmetic difference. In this paper, we design a construction with ways we find. Given modular differences, some signed bitwise difference is uniquely determined.

Keywords: Modular difference, Arithmetic difference, Signed Bitwise difference

1 Introduction

Biham and Shamir[1,2] proposed differential cryptanalysis, and differential cryptanalysis was success applied on some cryptosystems. Afterwards some different differences are proposed. The main differences include modular difference, signed bitwise difference[3], xor-difference. These differences have different advantage. They are used in different scheme.

In this paper, we will focus on modular difference and signed bitwise difference. By theorem 4.3 of Daum's paper 'Cryptanalysis of Hash Functions of the MD4-Family' [5], to given signed bitwise difference the modular difference is uniquely determined. At the same time, there are some signed bitwise differences will be transformed into same modular difference. For example, signed bitwise differences (0,…,0,1) and (0,…,1,-1) will be transformed into modular difference 1. So the relationship of modular difference and signed bitwise difference is one-many relationship.

There are some constructions or functions have more feasible variable pairs satisfy given modular difference than satisfy given signed bitwise difference. Usual the feasible variable pairs satisfy given modular difference include feasible variable pairs satisfy signed bitwise differences transformed into given modular difference. Thus if it can reduce signed bitwise differences transformed into given modular difference, it will strong construction or function under modular difference.

When we study arithmetic difference, we find that there are some ways to establish one-one relationship between signed bitwise differences and arithmetic differences

and establish one-one relationship between arithmetic differences and modular differences. And we build a construction with these ways. Given modular difference, some signed bitwise difference will be uniquely determined.

In this paper, we will explain ways establish one-one relationship between different differences in section 2 and section 3, and then we will build a construction with these ways in section 4.

We will use follow notation:

Modular difference: $\Delta^{+}x:=\Delta^{+}(x,x'):=(x-x'+2^n) \bmod 2^n$ (1.1)

Arithmetic difference: $\Delta x:=\Delta(x,x'):=x-x'$ (1.2)

Signed Bitwise difference:

$$\Delta^{\pm}x:=\Delta^{\pm}(x,x'):=(\Delta^{\pm}x_{n-1},\ldots,\Delta^{\pm}x_0):=(x_{n-1}-x'_{n-1},\ldots,x_0-x'_0) \quad (1.3)$$

The + and - operation in section 2 and section 3 is normal addition and subtraction. And the + operation in section 4 is modular addition.

2 Arithmetic Differences and Modular Differences

In this section we will discuss transition between arithmetic difference and modular difference, and then we will show the way establish one-one relationship between arithmetic difference and modular difference.

2.1 Transform Arithmetic Difference into Modular Difference

By (1.1)(1.2), there exists:

$$\Delta^{+}x=(x-x'+2^n) \bmod 2^n=(\Delta x+2^n) \bmod 2^n \quad (2.1)$$

Because there exists $-2^n<\Delta x<2^n$ and $0<\Delta^{+}x<2^n$, thus:

$$\begin{cases}\Delta^{+}x=\Delta x & if \quad \Delta x\geq 0\\ \Delta^{+}x=\Delta x+2^n & if \quad \Delta x<0\end{cases} \quad (2.1.a)$$

By (2.1), it can transform given arithmetic difference into the sole modular difference. So there exists follow theorem

Theorem 2.1: *Given arithmetic difference, the modular difference is uniquely determined.*

2.2 Transform Modular Difference into Arithmetic Difference

To a given modular difference, by (2.1), it is known there are many arithmetic differences will satisfy (2.1). Because there exists $-2^n<\Delta x<2^n$ and $0<\Delta^{+}x<2^n$. So the follow arithmetic differences can be transformed into given modular difference:

$$\begin{cases}\Delta x=\Delta^{+}x+k\times 2^n & k=-1,0 \quad if \quad \Delta^{+}x\neq 0\\ \Delta x=0 & if \quad \Delta^{+}x=0\end{cases} \quad (2.2)$$

By (2.2), it can transform given modular difference into two arithmetic differences. One is bigger than 0, the other less than 0.

2.3 Establish one-one relationship between arithmetic difference and modular difference

When we study the transition of arithmetic difference and modular difference, we find that if change arithmetic difference, the change of modular difference will depend on arithmetic difference bigger than 0 or not. By (2.2), the modular difference can transform into the arithmetic difference bigger than 0 or less than 0. So it can change the arithmetic difference, and then determine the sign of arithmetic difference by how modular difference change, and then compute out the arithmetic difference by (2.2).

It can use shift right operation (SHR) to change arithmetic difference. Let there are two variable x, x1 satisfy:

$$x1= SHR^r(x)=x>>r \tag{2.3}$$

We just discuss the case r=1. If there is arithmetic difference $\Delta x\neq 0$, then there exists:

$$\Delta x1=x1-x1'=x>>1-x'>>1=(x-x')/2=\Delta x/2 \tag{2.4}$$

By (2.4), if $\Delta x1\neq 0$, $\Delta x1$ will has same sign with Δx. So it can be divided into three cases:

1. $\Delta x1=0$ and $\Delta x\neq 0$ ==>$\Delta {}^{+}x1=0$ $\Delta x=\pm 1$
2. $\Delta x1>0$ and $\Delta x\neq 0$ ==>$\Delta x>0$ ==> $\Delta {}^{+}x=\Delta x$ and $\Delta {}^{+}x1=\Delta x1$
3. $\Delta x1<0$ and $\Delta x\neq 0$ ==>$\Delta x<0\neq 0$==> $\Delta {}^{+}x=\Delta x+2^n$ and $\Delta {}^{+}x1=\Delta x1+2^n$

Case 1: $\Delta x1=0$ and $\Delta x\neq 0$

By (2.1) and $\Delta x1=0$, there exists $\Delta {}^{+}x1=0$

If $\Delta x>1$, there exists:

$$\Delta x1\geq 1 \tag{2.5}$$

If $\Delta x<1$, there exists:

$$\Delta x1\leq -1 \tag{2.6}$$

By (2.5), (2.6) and $\Delta x\neq 0$, there exists:

$$\Delta x\in\{1,\ -1\} \tag{2.7}$$

By (2.1.a), there exists:

$$\Delta {}^{+}x\in\{1,\ 2^n-1\} \tag{2.8}$$

Thus if $\Delta {}^{+}x=1$, by (2.2), there exists $\Delta x\in\{1,\ 1-2^n\}$. Thus by (2.7), if $\Delta {}^{+}x1=0$ and $\Delta {}^{+}x=1$, there exist:

$$\Delta x\in\{1,\ -1\}\cap\{1,\ 1-2^n\}=\{1\} \tag{2.9}$$

If $\Delta {}^{+}x=2^n-1$, by (2.2), there exists $\Delta x\in\{-1,2^n-1\}$. Thus by (2.7), if $\Delta {}^{+}x1=0$ and $\Delta {}^{+}x=2^n-1$, there exist:

$$\Delta x\in\{1,\ -1\}\cap\{-1,2^n-1\}=\{-1\} \tag{2.10}$$

Case 2: $\Delta x1>0$ and $\Delta x\neq 0$

By (2.1) and $\Delta x1>0$, there exists $\Delta {}^{+}x1\neq 0$.

By (2.4) and $\Delta x1>0$,there exists $\Delta x>0$.

By (2.1.a), there exists:

$$(\Delta {}^{+}x-\Delta {}^{+}x1)\times\Delta x=(\Delta x-\Delta x1)\times\Delta x=(\Delta x)^2-\Delta x/2\times\Delta x\ >0 \tag{2.11}$$

Case 3: $\Delta x1<0$ and $\Delta x\neq 0$

By (2.1) and $\Delta x1<0$, there exists $\Delta^{+}x1\neq 0$.

By (2.4) and $\Delta x1<0$,there exists $\Delta x<0$.

By (2.1.a), there exists:

$$(\Delta^{+}x-\Delta^{+}x1)\times\Delta x=(\Delta x+2^{n}-\Delta x1-2^{n})\times\Delta x=(\Delta x)^{2}-\Delta x/2\times\Delta x>0 \quad (2.12)$$

So to given modular difference $(\Delta^{+}x,\Delta^{+}x1)$, by(2.9), (2.10), (2.11) and (2.12), it can compute Δx follow:

$$\Delta x=\begin{cases}-1 & if \quad (\Delta^{+}x1=0)and(\Delta^{+}x=2^{n}-1)\\ 1 & if \quad (\Delta^{+}x1=0)and(\Delta^{+}x=1)\\ \Delta^{+}x & if \quad (\Delta^{+}x1\neq 0)and((\Delta^{+}x-\Delta^{+}x1)>0)\\ \Delta^{+}x-2^{n} & if \quad (\Delta^{+}x1\neq 0)and((\Delta^{+}x-\Delta^{+}x1)<0)\end{cases} \quad (2.13)$$

By (2.13), there exists follow theorem:

Theorem 2.2: *If variable x1, x satisfy (2.3), Given modular difference ($\Delta^{+}x,\Delta^{+}x1$), the arithmetic difference Δx is uniquely determined.*

3 Arithmetic Difference and Singed Bitwise Difference

In this section, we will discuss some characters about signed bitwise difference, and then we will expound a way establish one-one relationship between arithmetic difference and signed bitwise difference.

3.1 Singed Bitwise Difference

Let there are two different signed bitwise difference $\Delta^{\pm}xa$, $\Delta^{\pm}xb$ satisfy:

$$\Delta^{\pm}xa_{2\times k+1}=\Delta^{\pm}xb_{2\times k+1} \qquad k=0,1,\ldots,n/2-1 \quad (3.1)$$

There exists follow lemma:

Lemma 3.1: *Given two signed bitwise difference $\Delta^{\pm}xa$, $\Delta^{\pm}xb$. There exists $\Delta^{\pm}xa_i-\Delta^{\pm}xb_i\in\{-2,-1,0,1,2\}$*

Proof:

Because $\Delta^{\pm}xa_i,\Delta^{\pm}xb_i\in\{-1,0,1\}$, so there exists:

$$\Delta^{\pm}xa_i-\Delta^{\pm}xb_i\in\{-2,-1,0,1,2\}$$ □

Then there exists follow corollary:

Corollary 3.1: *Given different signed bitwise differences $\Delta^{\pm}xa$, $\Delta^{\pm}xb$ satisfy (3.1). If $\Delta^{\pm}xa\neq\Delta^{\pm}xb$. Then there exists $\Delta xa\neq\Delta xb$.*

Proof:

To two different signed bitwise difference $\Delta^{\pm}xa$, $\Delta^{\pm}xb$ there exists index I make:

$$\Delta^{\pm}xa_I\neq\Delta^{\pm}xb_I$$

Let I_{MAX} is the maximum index: $I_{MAX}=\max\{|\Delta^{\pm}xa_i\neq\Delta^{\pm}xb_i\}$

By (3.1), there exists: $I_{MAX} \bmod 2=0$

And $\Delta^{\pm} xa_{I_{MAX}-1} = \Delta^{\pm} xb_{I_{MAX}-1}$

If $I_{MAX}=0$, there exists:

$$\sum_{i=0}^{n-1} \Delta^{\pm} xa_i \times 2^i - \sum_{i=0}^{n-1} \Delta^{\pm} xb_i \times 2^i = \Delta^{\pm} xa_0 - \Delta^{\pm} xb_0 \neq 0$$

$$\sum_{i=0}^{n-1} \Delta^{\pm} xa_i \times 2^i \neq \sum_{i=0}^{n-1} \Delta^{\pm} xb_i \times 2^i \tag{3.2}$$

If $I_{MAX}>0$, there exists:

$$\sum_{i=0}^{n-1} \Delta^{\pm} xa_i \times 2^i - \sum_{i=0}^{n-1} \Delta^{\pm} xb_i \times 2^i$$

$$= \sum_{i=0}^{I_{MAX}} (\Delta^{\pm} xa_i - \Delta^{\pm} xb_i) \times 2^i$$

$$= (\Delta^{\pm} xa_{I_{MAX}} - \Delta^{\pm} xb_{I_{MAX}}) \times 2^{I_{MAX}} + \sum_{i=0}^{I_{MAX}-2} (\Delta^{\pm} xa_i - \Delta^{\pm} xb_i) \times 2^i$$

Let:

$$\Delta 1 = (\Delta^{\pm} xa_{I_{MAX}} - \Delta^{\pm} xb_{I_{MAX}}) \times 2^{I_{MAX}}$$

$$\Delta 2 = \sum_{i=0}^{I_{MAX}-2} (\Delta^{\pm} xa_i - \Delta^{\pm} xb_i) \times 2^i$$

By lemma 3.1 and $\Delta^{\pm} xa_{I_{MAX}} \neq \Delta^{\pm} xb_{I_{MAX}}$, there exists:

$$\Delta 1 \in \{-2^{I_{MAX}+1}, -2^{I_{MAX}}, 2^{I_{MAX}}, 2^{I_{MAX}+1}\}$$

$$-\Delta 1 \in \{2^{I_{MAX}+1}, 2^{I_{MAX}}, -2^{I_{MAX}}, -2^{I_{MAX}+1}\}$$

By lemma 3.1, there exists:

$$\sum_{i=0}^{I_{MAX}-2} -2 \times 2^i = \sum_{i=1}^{I_{MAX}-1} -2^i = (-2^{I_{MAX}} + 1)$$

$$\leq \Delta 2$$

$$\leq \sum_{i=0}^{I_{MAX}-2} 2 \times 2^i = \sum_{i=1}^{I_{MAX}-1} 2^i = (2^{I_{MAX}} - 1)$$

Thus: $\Delta 2 \in \{-2^{I_{MAX}} + 1, ..., 0, ..., 2^{I_{MAX}} - 1\}$

Because there exists:

$$\{2^{I_{MAX}+1}, 2^{I_{MAX}}, -2^{I_{MAX}}, -2^{I_{MAX}+1}\} \cap \{-2^{I_{MAX}} + 1, ..., 0, ..., 2^{I_{MAX}} - 1\} = \phi$$

Thus there do not exists $\Delta 2$ make $\Delta 1 + \Delta 2 = 0$. So there exists:

$$\sum_{i=0}^{n-1} \Delta^{\pm} xa_i \times 2^i - \sum_{i=0}^{n-1} \Delta^{\pm} xb_i \times 2^i = \Delta 1 + \Delta 2 \neq 0$$

Thus: $$\sum_{i=0}^{n-1} \Delta^{\pm} xa_i \times 2^i \neq \sum_{i=0}^{n-1} \Delta^{\pm} xb_i \times 2^i \tag{3.3}$$

By (3.2)(3.3), there exists: $\sum_{i=0}^{n-1} \Delta^{\pm} xa_i \times 2^i \neq \sum_{i=0}^{n-1} \Delta^{\pm} xb_i \times 2^i$

Thus: $\Delta xa \neq \Delta xb$ □

Corollary 3.1 show it can transform two different signed bitwise difference satisfy (3.1) into same arithmetic difference. Similarly, if two different signed bitwise difference $\Delta^{\pm}$xa, $\Delta^{\pm}$xb satisfy:

$$\Delta^{\pm}xa_{2\times k}=\Delta^{\pm}xb_{2\times k} \qquad k=0,1,\ldots,n/2-1 \tag{3.4}$$

There exists corollary:

Corollary 3.2: *Given different signed bitwise differences $\Delta^{\pm}xa$, $\Delta^{\pm}xb$ satisfy (3.4). If $\Delta^{\pm}xa\neq\Delta^{\pm}xb$. Then there exists $\Delta xa\neq\Delta xb$.*

3.2 Establish one-one relationship between Arithmetic difference and Singed Bitwise Difference

Corollary 3.1 and 3.2 show it can transform two signed bitwise differences satisfy (3.1) or (3.4) into same arithmetic difference. We find some ways to create signed bitwise difference satisfy (3.1) or (3.4), we give out a way as follow:

$$x1 = x \wedge \sum_{i=0}^{n/2} 2^{2\times i} \tag{3.5}$$

Then there exists follow corollary:

Corollary 3.3: *Let x, x1 satisfy (3.5), to two given difference pair $(\Delta^{\pm}x,\Delta^{\pm}x1)$ and $(\Delta^{\pm}x',\Delta^{\pm}x1')$. If $(\Delta^{\pm}x,\Delta^{\pm}x1)\neq(\Delta^{\pm}x',\Delta^{\pm}x1')$, there exists:*

$$(\Delta x,\Delta x1)\neq(\Delta x',\Delta x1')$$

Proof:

x, x1 satisfy (3.5), then there exists:

$$x1_{2\times k+1}=0 \qquad k=0,1,\ldots,n/2-1$$

Then there exists:

$$\Delta^{\pm}x1_{2\times k+1}\neq\Delta^{\pm}x1'_{2\times k+1}=0 \qquad k=0,1,\ldots,n/2-1$$

By corollary 3.1, it can divide this into two cases :

Case 1: $\Delta^{\pm}x1\neq\Delta^{\pm}x1' \Rightarrow \Delta x1\neq\Delta x1'$

Case 2: $\Delta^{\pm}x1=\Delta^{\pm}x1' \Rightarrow \Delta x1=\Delta x1'$

Case 1: $\Delta^{\pm}x1\neq\Delta^{\pm}x1'$

By corollary 3.1, there exists $\Delta x1\neq\Delta x1'$, thus:

$$(\Delta x,\Delta x1)\neq(\Delta x',\Delta x1') \tag{3.6}$$

Case 2: $\Delta^{\pm}x1=\Delta^{\pm}x1'$

Because x, x1 satisfy (3.5), thus there exists:

$$x1_{2\times k}\neq x_{2\times k}$$

Thus:

$$\Delta^{\pm}x1_{2\times k}=\Delta^{\pm}x_{2\times k} \qquad k=0,1,\ldots,n/2-1$$
$$\Delta^{\pm}x1'_{2\times k}=\Delta^{\pm}x'_{2\times k} \qquad k=0,1,\ldots,n/2-1$$

By $\Delta^{\pm}x1=\Delta^{\pm}x1'$, thus:

$$\Delta^{\pm}x1'_{2\times k}=\Delta^{\pm}x'_{2\times k}=\Delta^{\pm}x1_{2\times k}=\Delta^{\pm}x_{2\times k} \qquad k=0,1,\ldots,n/2-1 \tag{3.7}$$

By $(\Delta^{\pm}x,\Delta^{\pm}x1)\neq(\Delta^{\pm}x',\Delta^{\pm}x1')$, $\Delta^{\pm}x1=\Delta^{\pm}x1'$, there exists:

$$\Delta^{\pm}x\neq\Delta^{\pm}x' \tag{3.8}$$

By (3.7), (3.8), corollary 3.2, there exists $\Delta x\neq\Delta x'$, thus:

$$(\Delta x,\Delta x1)\neq(\Delta x',\Delta x1') \tag{3.9}$$

By (3.6) and (3.9), if x, x1 satisfy (3.5) and $(\Delta^{\pm}x,\Delta^{\pm}x1)\neq(\Delta^{\pm}x',\Delta^{\pm}x1')$, there exists:

$$(\Delta x,\Delta x1)\neq(\Delta x',\Delta x1')$$ □

By corollary 3.3, if x, x1 satisfy (3.5), it can not transform different signed bitwise difference pair into same arithmetic difference pair. Thus the relationship between $(\Delta^{\pm}x,\Delta^{\pm}x1)$ and $(\Delta x,\Delta x1)$ is one-one relationship.

4. A Construction

In this section, we will build a construction that use ways that explained in section 2 and section 3. In the construction, given modular differences, some signed bitwise difference will be uniquely determined.

In this section, we will use addition model 2^n. And the construction as follow:

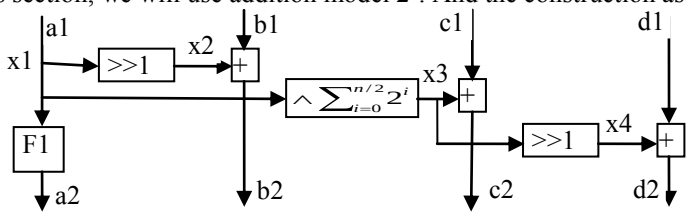

Fig 4.1 Construction I

The function F1 is some function be well analyzed. The construction take 4 n-bit words a1,b1,c1,d1 as input, and produce 4 n-bit words a2,b2,c2,d2 as output. To simplify analysis, we use variable x1,x2,x3,x4, and let:

$$\begin{cases} x1 = a1 \\ x2 = b2 - b1 \\ x3 = c2 - c1 \\ x4 = d2 - d1 \end{cases}$$

By fig 4.1, there exists:

$$\begin{cases} x3 = x1 \wedge \sum_{i=0}^{n/2} 2^i \\ x2 = x1 >> 1 \\ x4 = x3 >> 1 \end{cases}$$

When given modular difference $\Delta^+a1,\Delta^+b1,\Delta^+b2,\Delta^+c1,\Delta^+c2,\Delta^+d1,\Delta^+d2$, there exists:

$\Delta^+x1=\Delta^+a1$

$\Delta^+x2=\Delta^+c1-\Delta^+c2$

$\Delta^+x3=\Delta^+b1-\Delta^+b2$

$\Delta^+x4=\Delta^+d1-\Delta^+d2$

By theorem 2.2 and x1,x2 satisfy (2.3), given modular differences Δ^+x1,Δ^+x2, the arithmetic differences $\Delta x1$ is uniquely determined. By theorem 2.2 and x3,x4 satisfy (2.3), given modular differences Δ^+x3,Δ^+x4, the arithmetic differences $\Delta x3$ is uniquely determined. By corollary 3.3 and x1,x3 satisfy (3.5), given arithmetic differences $\Delta x3,\Delta x1$, the signed bitwise difference $\Delta^{\pm}x1,\Delta^{\pm}x3$ are uniquely determined. Thus in the construction I, given the modular difference, the input signed bitwise difference of function F1 is uniquely determined.

When design a construction, there maybe some functions strong under arithmetic difference or signed bitwise difference, but weak under modular difference. Then it can use ways showed in fig 4.1 to strengthen the construction under modular difference.

5. Conclusion

In this paper, we study some characters about modular difference, arithmetic difference, and signed bitwise difference. Then we give out the ways (2.3) and (3.5) to establish one-one relationship between arithmetic difference and singed bitwise difference and one-one relationship between arithmetic difference and modular difference. At section 4, we build a construction with (2.3) and (3.5). Given modular difference, some signed bitwise difference is uniquely determined. So it can use (2.3) and (3.5) to reduce some signed bitwise difference transformed into given modular difference in some construction.

References

[1] Eli Biham and Adi Shamir, Differential Cryptanalysis of DES-like Cryptosystems.in advances in Cryptology-Crypto'90, pp.2-21

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

[3] Xiaoyun Wang; Hongbo Yu (2005). "How to Break MD5 and Other Hash Functions". EUROCRYPT. ISBN 3-540-25910-4.

[4] Berson, Thomas A. (1992). "Differential Cryptanalysis Mod 2^{32} with Applications to MD5". EUROCRYPT. pp. 71–80. ISBN 3-540-56413-6.

[5]M. Daum. Cryptanalysis of Hash Functions of the MD4-Family. PhD thesis, Ruhr-University of Bochum, 2005.