Finding Zero Correlation Linear Hulls Using Quantum Bernstein-vazirani Algorithm

Huiqin Xie and Zhangmei Zhao*

Beijing Electronic Science and Technology Institute, Beijing 100070, China
Email: zmzhao@mail.ustc.edu.cn

Abstract. Facing the threat of quantum computing to cryptography schemes, it is urgent to study the applications of quantum algorithms to cryptanalysis and evaluate the security of cryptographic schemes in a quantum computing environment. To do this, it is necessary to analyze the ability of cryptanalysis methods, such as integral and linear attacks, when combined with quantum algorithms. In this article, we investigate the properties of block ciphers with SPN structure and their security against a quantum adversary and apply the Bernstein-Vazirani algorithm to zero correlation linear attacks. Based on the relation between linear approximates of SPN ciphers and the dual cipher's linear structures, we proposed a quantum algorithm that can find linear hulls with zero correlation of SPN ciphers. We show the validity of the proposed quantum algorithm and estimate the corresponding computational complexity. Implementing our quantum algorithm only costs polynomial qubits and quantum gates.

Keywords: Symmetric cryptanalysis, Quantum algorithm, Linear cryptanalysis

1. Introduction

The burgeon of quantum information and quantum computers has seriously threatened the security of traditional cryptographic primitives. For example, for public-key schemes, any adversary with quantum computers can break an arbitrary public-key primitive whose security is based on discrete logarithm or factorization problem via Shor's algorithm [1] . For symmetric cryptographic schemes, using Grover's algorithm [2] quantum attackers can get a square order speed-up when searching the key. By Simon's algorithm [3] a quantum adversary can attack Feistel schemes [4] and Even-Mansour block cipher [5], whose security has been proved against classical adversaries. In terms of cryptographic protocols, any security protocols based on the discrete logarithm problem, such as Chaum protocol [6] and Pedersen commitment [7], will no longer be secure in quantum computing environments. Therefore, It is significant to investigate the accurate security of widely used classical cryptographic protocols in quantun setting.

In recent years, quantum algorithms have been widely used to attack symmetric ciphers and there are many remarkable results. Kuwakado *et al.* designed a quantum algorithm that can distinguish Feistel structure from random functions, which uses Simon's algorithm and has only polynomial complexity [4]. Subsequently, they also used the similar method to solve the subkey of Even-Mansour cipher [5]. These two examples fully demonstrate the superiority of quantum algorithms in symmetric cryptanalysis. Santoli improved the results in the research [4] by proving the fact that, even when the round function is not a permutation, there still exists an effective quantum distinguisher [8]. Kaplan *et. al.* almost simultaneously proved the same results by different method [9]. Leander and Alexander uses the quantum distinguisher to present a quantum circuit that recovered the key of FX structure [10]. Dong et.

al. combined the distinguisher proposed by Kuwakado and Grover's algorithm, then executed a quantum attack that recovered the key of Feistel schemes[11]. They then also attack the generalized Feistel structure using the same same idea [12].

Although these results is remarkable, they are still not enough to measure the accurate security of symmetric primitives when facing quantum attackers. It is also indispensable to analyze the ability of cryptanalysis methods when they are assisted by quantum algorithms. Some work has already applied quantum algorithms to differential cryptanalysis [13,14]. Bonnetain studied the quantum slide attack [15]. Chen and Gao proposed quantum algebraic attack [16]. ZHANG *et. al.* proposed quantum differential collision distinguishing attacks [17]. Schrottenloher *et. al.* uesd Grover's algorithm to meet-in-the-middle cryptanalysis [18]. In this work, we focus on zero correlation linear cryptanalytic tool [19] and design quantum algorithms that can find linear hulls whose correlation is zero.

2. Preliminaries

In this paper, $Enc_k(x)$**:** $\{0,1\}^n \to \{0,1\}^n$ represents a SPN block cipher. the length of its inputs is n bits. If a quantum circuit can execute the unitary operator

$$U_{Enc_k} : |x\rangle|y\rangle \to |x\rangle|y \oplus Enc_k(x)\rangle,$$

we say that this circuit realizes $Enc_k(x)$ quantumly. All quantum circuits of Boolean functions can be composed of quantum universal gates [20]. We use $|Enc_k|_Q$ to represent the amount of quantum universal gates used in this quantum circuit. Since the computational complexity of encryption of an arbitrary block ciphers is a polynomial of n, the value $|Enc_k|_Q$ is always a polynomial of the parameter n.

2.1. Linear Structures

Let the set of Boolean functions from $\{0,1\}^n$ to $\{0,1\}$ be B_n. Linear structure notion was proposed for cryptanalytic applications [21].

Definition 1. *For any* f *in* B_n*, if* $a \in \{0,1\}^n$ *satisfies that*

$$f(x) \oplus f(x \oplus a) = f(\vec{0}) \oplus f(a), \quad \forall x \in \{0,1\}^n,$$

where the notation $\oplus$ is exclusive-or and $\vec{0}$ is the n-dimension zero vector, then a is said to be f's linear structure.

Suppose linear structures of f forms the set Ω_f. Define the sets

$$\Omega_f^i = \{a \in \{0,1\}^n \mid f(x) \oplus f(x \oplus a) = i, \forall x \in \{0,1\}^n\},$$

for $i = 0$ or 1. Obviously it is correct that $\Omega_f = \Omega_f^0 \bigcup \Omega_f^1$. Each vector in Ω_f^0 are called the 0-linear structure of the fuction f while the vectors in Ω_f^1 are called the 1-linear structure of f. It has been proved that the linear structures are related closely to the concept of Walsh spectrum.

Definition 2. *If* f *is in* B_n*,* its Walsh spectrum is also a Boolean function in B_n*:*

$$S_f : \{0,1\}^n \to \{0,1\}$$

$$\omega \quad \to S_f(\omega) = \frac{1}{2^n} \sum_{x \in \{0,1\}^n} (-1)^{f(x) \oplus \omega \cdot x}.$$

For each function f in B_n, let $Q_f = \{x \mid S_f(x) \neq 0\}$. Lemma 1 presents the connection between f's Walsh spectrum and f's linear structures.

Lemma 1. [21] For each single-output Boolean function f in B_n, any $i = 0,1$,

$$\Omega_f^i = \{a \in \{0,1\}^n \mid \omega \cdot a = i, \forall \omega \in Q_f\}.$$

According to the above lemma, one method to obtain the sets Ω_f^i is to first get a sufficiently big subset S of the set Q_f, then solve the linear equation system $\{x \cdot \upsilon \mid \upsilon \in S\}$.

2.2. Bernstein-Vazirani Algorithm and its applications

Bernstein-Vazirani (BV) algorithm [22] proposed in 1997 solves the question: given the access to execute the quantum oracle of $f_\tau(x) = \tau \cdot x$, with $\tau \in \{0,1\}^n$ being a secret vector, how to get the value of s. BV algorithm is presented below:

(1) Execute the Hadamard operation H^{n+1} on $|\varphi_0\rangle = |0\rangle^{\otimes n}|1\rangle$ to get

$$|\varphi_1\rangle = \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle \cdot \frac{|0\rangle - |1\rangle}{\sqrt{2}}.$$

(2) Executing the unitary operator U_{f_τ}, getting the state

$$|\varphi_2\rangle = \sum_{x \in \{0,1\}^n} \frac{(-1)^{f_\tau(x)}|x\rangle}{\sqrt{2^n}} \cdot \frac{|0\rangle - |1\rangle}{\sqrt{2}}.$$

(3) Omit the rightmost qubit, then execute the Hadamard operation H^n to get

$$|\varphi_3\rangle = \sum_{y \in \{0,1\}^n} \left(\frac{1}{2^n} \sum_{x \in \{0,1\}^n} (-1)^{f_\tau(x) \oplus y \cdot x}\right)|y\rangle. \quad (1)$$

Because $f_\tau(x) = \tau \cdot x$, it holds that

$$|\varphi_3\rangle = \sum_{y \in \{0,1\}^n} \left(\frac{1}{2^n} \sum_{x \in \{0,1\}^n} (-1)^{(\tau \oplus y) \cdot x}\right)|y\rangle = |\tau\rangle.$$

Thus, measuring the above state $|\varphi_3\rangle$ the probability of the output being τ is 1.

The detailed circuit construction of the above algorithm is showed in figure 1. Considering the equation (1), if we implement the above algorithm on a arbitrary Boolean function f in the set B_n, the obtained quantum state without the final measurement should be

$$\sum_{y \in \{0,1\}^n} S_f(y)|y\rangle.$$

Here $S_f(\cdot)$ denotes the function f 's Walsh spectrum. If this state is measured, the probability that we get the vector y is $S_f(y)^2$. As a result the output of BV algorithm running on f must be in Q_f.

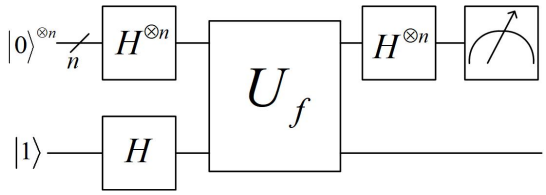

Figure 1. Quantum circuit diagram of BV algorithm.

Applying BV algorithm to f needs totally $2n+|f|_Q+1$ universal quantum gates. Executing BV algorithm needs $n+1$ qubits. Since the outputs of BV algorithm when applied to f gives vectors in Q_f, based on Lemma 1, Li proposed algorithm 1 for finding linear structures [23].

Algorithm 1
Input: Quantum circuit of function $f \in \mathrm{B}_n$
Output: linear structures of function f
1: Initialize set $S = \Phi$;
2: **For** $l = 1, 2, ..., n$ **do**
3: Execute BV algorithm on the Boolean function f, getting an output $\upsilon \in Q_f$;
4: Compute $S = S \bigcup \{\upsilon\}$;
5: **End for**
6: Compute the equation $\{\upsilon \cdot x = i \mid \upsilon \in S\}$, getting the solution set A^i for $i = 0,1$;
7: **If** $A^0 \bigcup A^1 = \{\vec{0}\}$ **then**
8: Output "No";
9: **else**
10: Output the sets A^0 and A^1;
11: **End if**

Theorem 1 indicates the effectiveness of the above algorithm.

Theorem 1. [24] $f \in \mathrm{B}_n$. If implementing the algorithm 1 on function f outputs A^0 and A^1, then $\Omega_f^i \subseteq A^i$ and for $\forall a \notin \Omega_f^i$ ($i = 0,1$), it must hold that $a \notin A^i$ except a negligible probability.

Theorem 1 indicates that the probability of the vectors in A^i ($i = 0,1$) being the i-linear structures of the function f is almost equal to 1.

3. Quantum Tool for Searching Linear Hulls with Zero Correlation

We first converse the goal of finding hulls with zero correlation of SPN block ciphers to the goal of searching linear structures. Afterwards, we applying BV algorithm to find linear hulls with zero correlation.

3.1. The Attack Idea

Zero correlation linear attack was proposed as an significant cryptanalytic tool of block ciphers and was introduced by the cryptographers Bogdanov and Rijmen [19]. For any $f \in \mathrm{B}_n$, its correlation is

$$c(f(x)) = \frac{1}{2^n} \sum_{x \in \{0,1\}^n} (-1)^{f(x)}.$$

Suppose $Enc_k(x): \{0,1\}^n \to \{0,1\}^n$ is a SPN block cipher. (a,b) is a linear approximate of $Enc_k(x)$. If $c(b \cdot f(x) \oplus a \cdot x) = 0$, then (a,b) is called a linear hull of $Enc_k(x)$ with correlation zero. Here "$\cdot$" is the common inner product operation. The most important step for zero correlation linear attack is to find linear approximates with correlation zero.

According to the relation of zero correlation approximates and impossible differentials [25], (a,b) is $Enc_k(x)$'s linear approximate with zero correlation if and only if it is the impossible differential of its dual cipher $Enc_k^{\perp}(x)$, which means for each $x \in \{0,1\}^n$ and $k \in \{0,1\}^m$, it hols that

$$Enc_k^{\perp}(x) \oplus Enc_k^{\perp}(x \oplus a) \neq b .$$

Suppose $Enc_k(x)$ has a linear layer P, then its dual structure is defined as a block cipher the same as $Enc_k(x)$ except for replacing P with $(P^{-1})^T$. We present a comparison between an SPN cipher and its dual structure in figures 2 and 3, where S is the substitution layer, and x_{i-1} is the input while x_i is the output in round i.

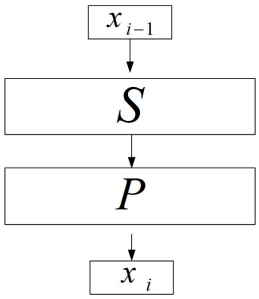

Figure 2. One round of a SPN cipher.

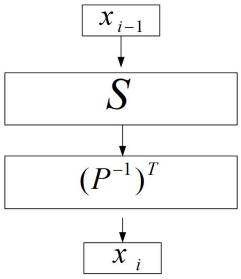

Figure 3. One round of SPN dual structure.

Define

$$G : \{0,1\}^m \times \{0,1\}^n \rightarrow \{0,1\}^n$$
$$(k \quad , \quad x) \quad \rightarrow Enc_k^{\perp}(x).$$

Let $G = (G_1, G_2, ..., G_n)$. Theorem 2 shows a method to search linear structures using the constructed function G.

Theorem 2. If there exists $i \in \{1,2,...,n\}, a \in \{0,1\}^n$ and $u \in \{0,1\}$ *such that* $(\vec{0},a)$ *is a* u *-linear structure of* G_i, where $\vec{0}$ is the m-dimension zero vector, then for any vector $b \in \{0,1\}^n$, as long as the i-th bit of b is not equal to u, then (a,b) will be a linear hull of the SPN cipher $Enc_k(x)$ with zero correlation .

Proof. Since $(\vec{0},a)$ is a u-linear structure of G_i, then

$$G_i(k,x) \oplus G_i(k \oplus \vec{0}, x \oplus a) = u, \forall x, \forall k.$$

Therefore

$$Enc_k^{\perp}[i](x) \oplus Enc_k^{\perp}[i](x \oplus a) = u, \ \forall k, \ \forall x.$$

Here $Enc_k^{\perp}[i](x)$ is the i-th component function of $Enc_k^{\perp}(x)$. Since the i-th bit of b is unequal to u, $Enc_k^{\perp}[i](x) \oplus Enc_k^{\perp}[i](x \oplus a)$ is not equal to b. Therefore, we have

$$Enc_k^{\perp}(x) \oplus Enc_k^{\perp}(x \oplus a) \neq b, \ \forall k, \forall x,$$

which indicates (a,b) must be an impossible differential of $Enc_k^{\perp}(x)$. According to theorem 2 of [23], (a,b) must be a linear hull of $Enc_k(x)$ whose correlation is zero.

3.2. The Proposed Quantum Algorithm

Due to theorem 2, algorithm 1 can be executed on each G_i for $i=1,2,...,n$ to obtain zero correlation linear hulls of $Enc_k(x)$. The only problem is that linear structures output by algorithm 1 are required to have m zeros at the beginning. We can achieve this requirement by adding linear equations in the sixth step of algorithm 1. Considering the above analysis, we propose algorithm 2 for finding linear hull of SPN ciphers with zero correlation.

Algorithm 2

Input: quantum circuit of the function $G=(G_1,G_2,...,G_n)$

Output: zero correlation linear hulls of the SPN cipher $Enc_k(x)$

1: **For** $i=1,2,...,n$ **do**

2: Execute BV algorithm on G_i for $m+n$ times to get outputs $\upsilon^{(1)},...,\upsilon^{(m+n)}\in\{0,1\}^{m+n}$;

3: Solve the linear equations

$$\begin{cases} x\cdot(\upsilon_{m+1}^{(1)},\upsilon_{m+2}^{(1)},...,\upsilon_{m+n}^{(1)})=0 \\ x\cdot(\upsilon_{m+1}^{(2)},\upsilon_{m+2}^{(2)},...,\upsilon_{m+n}^{(2)})=0 \\ \vdots \\ x\cdot(\upsilon_{m+1}^{(m+n)},v_{m+2}^{(m+n)},...,v_{m+n}^{(m+n)})=0 \end{cases} \tag{2}$$

to get solution set A_0^i. Here x is the unknown, $\upsilon_t^{(j)}$ is its t-th bit;

4: Solve the linear equations

$$\begin{cases} x\cdot(\upsilon_{m+1}^{(1)},\upsilon_{m+2}^{(1)},...,v_{m+n}^{(1)})=1 \\ x\cdot(v_{m+1}^{(2)},\upsilon_{m+2}^{(2)},...,\upsilon_{m+n}^{(2)})=1 \\ \vdots \\ x\cdot(v_{m+1}^{(m+n)},v_{m+2}^{(m+n)},...,v_{m+n}^{(m+n)})=1 \end{cases} \tag{3}$$

to get solution set A_1^i;

5: **For** any $a\in A_0^i$ **do**

6: **If** $a\neq\vec{0}$ **then**

7: Output $(a,'b_i\neq 0')$;

8: **End if**

9: **End for**

10: **For** any $a\in A_1^i$ **do**

11: **If** $a\neq\vec{0}$ **then**

12: Output $(a,'b_i\neq 1')$;

13: **End if**

14: **End for**

15: **End for**

In algorithm 2, $a\in A_0^i$ means that a is the 0-linear structure of G_i, then according to theorems1 and 2, for any $b\in\{0,1\}^n$ such that $b_i\neq 0$, (a,b) is a linear approximate of $Enc_k(x)$ with zero correlation except a negligible probability. Similarly, for any $a\in A_1^i$ and any $b\in\{0,1\}^n$ such that $b_i\neq 1$, (a,b) is a linear hull of $Enc_k(x)$

with zero correlation except a negligible probability. Each nonzero vector in a in A_0^i or A_1^i results in 2^{n-1} linear hulls with zero correlation of $Enc_k(x)$. It should be noted that, because the encryption construction of the block cipher is completely public, attackers can obtain the quantum circuit of $Enc_k(x)$ by themselves, and therefore the quantum circuit of each G_i is available. Theorem 3 illustrates the correctness of the above algorithm.

Theorem 3. If the algorithm 2 outputs $(a,'b_i \neq 0')$, then for any $b \in \{0,1\}^n$ such that $b_i \neq 0$, (a,b) must be a linear hull whose correlation is zero to $Enc_k(x)$. If algorithm 2 outputs $(a,'b_i \neq 1')$, then for any $b \in \{0,1\}^n$ such that $b_i \neq 1$, (a,b) is a linear hull of $Enc_k(x)$ whose correlation is zero.

Proof. We only prove the first part of the theorem, and the second part can be proved similarly. If algorithm 2 outputs $(a,'b_i \neq 0')$, then $a \in A_0^i$. Thus a is a solution of equation (2), then $(\vec{0},a)$ is a solution of

$$\begin{cases} (y,x)\cdot(\upsilon_1^{(1)},\upsilon_2^{(1)},...,\upsilon_{m+n}^{(1)})=0 \\ (y,x)\cdot(\upsilon_1^{(2)},\upsilon_2^{(2)},...,\upsilon_{m+n}^{(2)})=0 \\ \vdots \\ (y,x)\cdot(\upsilon_1^{(m+n)},\upsilon_2^{(m+n)},...,\upsilon_{m+n}^{(m+n)})=0 \end{cases}$$

where $\vec{0}$ is m-dimension zero vector, $(y,x) \in \{0,1\}^m \times \{0,1\}^n$ are the unknowns. This means $(\vec{0},a)$ is also an output when running algorithm 1 on G_i, thus except a negligible probability, $(\vec{0},a)$ is a 0-linear structure of G_i. Then by theorem 2, for any $b \in \{0,1\}^n$ such that $b_i \neq 0$, (a,b) must be a linear hull whose correlation is zero to $Enc_k(x)$, which draws the conclusion.

3.3. Complexity

We estimate the quantum complexity of the proposed algorithm 2. Its main computational complexity includes two parts: (I) execute BV algorithm on each G_i for $m+n$ times; (ii) compute the equation (2) and equation (3) for n times respectively.

Running BV algorithm on each G_i needs $2m+2n+1$ Hadamard gates and one quantum execution of G_i. Since the cost of performing all G_i is equal to the cost of performing $Enc_k(x)$, the cost of the first part includes $n(m+n)(2m+2n+1)$ Hadamard gates and $m+n$ quantum executions of $Enc_k(x)$.

The second part only needs classical computational. The complexity of computing equation (2) or (3) is $O(n^2(m+n))$. Therefore, the classical computational complexity is $O(n^3(m+n))$. Algorithm 2 needs $m+n+1$ qubits. We list the resources, including the gates and qubits, required by algorithm 2 in table 1.

Table 1. Resources required to execute algorithm 2.

The number of Hadamard gates	The number of $U_{Enc_k(x)}$	The number of qubits	The classical computational complexity
$n(m+n)(2m+2n+1)$	$m+n$	$m+n+1$	$O(n^3(m+n))$

4. Conclusions

In this work, we investigate the applications of the BV algorithm to symmetric cryptanalysis. Based on the relation between linear approximates of SPN ciphers and the SPN dual cipher's impossible differentials, we design a quantum tool for linear hulls of SPN ciphers with zero correlation. We show

the effectiveness of the algorithm proposed, then estimate the quantum complexity. Executing our quantum algorithm only needs polynomial qubits and quantum gates.

Acknowledgments
This work was supported by the Fundamental Research Funds for the Central Universities (No.328202202).

References

[1] Shor P W 1994 Algorithms for quantum computation: Discrete logarithms and factoring *Proceedings 35th Annual Symposium on Foundations of Computer Science* pp 124–134
[2] Grover L K 1996 A fast quantum mechanical algorithm for database search *Proceedings of the Twenty-eighth Annual ACM symposium on Theory of computing* pp 212-219
[3] Simon D R 1997 On the power of quantum computation *SIAM J Comput* 26 pp 1474-148
[4] Kuwakado H and Morii M 2010 Quantum distinguisher between the 3-round Feistel cipher and the random permutation *IEEE International Symposium on Information Theory* pp 2682-2685
[5] Kuwakado H and Morii M 2012 Security on the quantum-type Even-Mansour cipher *International Symposium on Information Theory and its Applications* pp 312-316
[6] Chaum D and Van Heyst E 1991 Group signatures *EUROCRYPT'91* pp 257-265
[7] Pedersen T P 1991 Non-interactive and information-theoretic secure verifiable secret sharing *Annual international cryptology conference* pp 129-140
[8] Santoli T and Schaffner C 2017 Using Simon's algorithm to attack symmetric-key cryptographic primitives *Quantum Information & Computation* **17** pp 65-78
[9] Kaplan M, Leurent G and Leverrier A 2016 Breaking symmetric cryptosystems using quantum period finding *CRYPTO'16* pp 207-237
[10] Leander G and May A 2017 Grover meets simom--quantumly attacking the FX-construction *ASIACRYPT'17* pp 161-178
[11] Dong X and Wang X 2018 Quantum key-recovery attack on Feistel structures *Science China Information Sciences* **61**(10) pp 102501
[12] Dong X, Li Z and Wang X 2019 Quantum cryptanalysis on some generalized Feistel scheme *Science China Information Sciences* **62**(2) 22501
[13] Kaplan M, Leurent G, Leverrier A and Naya-Plasencia M 2016 Quantum differential and linear cryptanalysis *IACR Transactions on Symmetric Cryptology* pp 71-94
[14] Xie H and Yang L 2019 Using Bernstein-Vazirani algorithm to attack block ciphers *Designs, Codes and Cryptography* **87** pp 1161-1182
[15] Bonnetain X, Naya-Plasencia M and Schrottenloher A 2019 On quantum slide attacks *International Conference on Selected Areas in Cryptography* pp 492-519
[16] CHEN Y A and GAO X S 2021 Quantum algorithms for Boolean equation solving and quantum algebraic attack on cryptosystems *Journal of Systems Science and Complexity* **35**(1) pp 373-412
[17] Zhongya Z, Wenling W U and Bolin W 2021 Quantum Differential Collision Distinguishing Attacks on Feistel Schemes *Chinese Journal of Electronics* **30**(6) pp 1030-1037
[18] Hosoyamada A And Sasaki Y 2018 Cryptanalysis against symmetric-key schemes with online classical queries and offline quantum computations *Topics in Cryptology* pp 198-218
[19] Bogdanov A and Rijmen V 2014 Linear hulls with correlation zero and linear cryptanalysis of block ciphers *Designs, Codes and Cryptography* **70**(3) pp 369-383
[20] Nielsen M and Chuang I 2000 *Quantum Computation and Quantum Information* Cambridge University Press chapter 4 pp 171-211
[21] Dubuc S 2001 Characterization of linear structures *Designs, Codes and Cryptography* **22**(1) pp 33-45
[22] Bernstein E and Vazirani U 1997 Quantum complexity theory *SIAM Journal on Computing* **26**(5) pp 1411-1473

[23] Li H and Yang L 2018 A quantum algorithm to approximate the linear structures of Boolean functions *Math. Struct. Comput. Sci* **28** pp 1-13
[24] Xie H and Yang L 2019 Using Bernstein-Vazirani algorithm to attack block ciphers *Designs, Codes and Cryptography* **87** pp 1161-1182
[25] Bing S, Zhiqiang L and Vincent R 2015 Links Among Impossible Differential, Integral and Zero Correlation Linear Cryptanalysis *CRYPTO'15* pp 95-115