About the Tu-Deng Conjecture for $\mathrm{w}(t)$ Less Than or Equal to 10

Yindong Chen, Limin Lin, and Chuliang Wei

***Abstract*—Let $k \geq 2$ be an integer, define**

$$S_t^k := \left\{ (a,b) \in \mathbb{Z}^2 \middle| \begin{array}{c} 0 \leq a, b \leq 2^k - 2 \\ a + b \equiv t \ (\mathbf{mod}\ 2^k - 1) \\ \mathrm{w}(a) + \mathrm{w}(b) \leq k - 1 \end{array} \right\},$$

where $t \in \mathbb{Z}, 1 \leq t \leq 2^k - 2$. This paper gives the upper bound of cardinality of S_t^k when $\mathrm{w}(t) \leq 10$, proving that a conjecture proposed by Tu and Deng in the case.

***Index Terms*—Tu-Deng Conjecture, algebraic immunity, Boolean function, Hamming weight**

I. Introduction

In the design of almost every modern symmetric cipher, an imperative part is a good Boolean function, which is immune to some cryptographic attack. Boolean functions used in some cryptosystems should satisfy various cryptographic properties to resist many attacks, mainly including balancedness, large algebraic degree and high nonlinearity. In 2003, Courtois and Meier successfully proposed algebraic attacks on several stream ciphers [1]. As a result, a new criterion called algebraic immunity was imposed on cryptographic Boolean functions. Since then, several classes of Boolean functions with optimal algebraic immunity have been investigated and constructed [2]–[6]. However, the nonlinearities of most such functions are not high enough to resist fast correlation attacks. In 2008, Carlet and Feng proposed an infinite class of balanced Boolean functions with optimal algebraic immunity [7], of which the algebraic degree is optimal and nonlinearity is the highest at that time. Hence, such functions are the first class to closely satisfying practical requirements.

In 2011, in Tu and Deng's construction, a conjecture [8] was created, which is presented in Conjecture 1. The $k \leq 29$ situation was at that time brute-forcedly validated. Based on the conjecture, some potentially good functions are constructed [8], [9]. Yet there is still no complete proof on the conjecture.

Here, for easy discussion, we define

Definition 1. *For non-negative integer x and i, we define x_i as the i-th bit of x in its binary representation, i.e.,*

$$x_i \equiv \left\lfloor \frac{x}{2^i} \right\rfloor (\mathrm{mod}\, 2),$$

$$x_i \in \{0, 1\},$$

and the Hamming weight of x, $\mathrm{w}(x)$ is the amount of ones in its binary representation, i.e.,

$$\mathrm{w}(x) = \sum_{i=0}^{\infty} x_i.$$

Meanwhile, the length of x, $\mathrm{len}(x)$ is the smallest integer L such that $2^L > x$.

Definition 2. *We define $[x]_m$ as the smallest non-negative value that congruence with x modulo m, i.e.,*

$$[x]_m \equiv x \ (\mathrm{mod}\, m),$$

$$0 \leq [x]_m < m.$$

When $m = 2^k - 1$, we can omit the value of m, and claim $[x] = [x]_{2^k-1}$.

Conjecture 1. *(Tu-Deng Conjecture [8]) Assume $k \in \mathbb{Z}$, $k \geq 2$. For any $t \in \mathbb{Z}$, $1 \leq t \leq 2^k - 2$, let*

$$S_t^k := \left\{ (a,b) \in \mathbb{Z}^2 \middle| \begin{array}{c} 0 \leq a, b \leq 2^k - 2, \\ [a + b] = t, \\ \mathrm{w}(a) + \mathrm{w}(b) \leq k - 1 \end{array} \right\}.$$

Then $|S_t^k| \leq 2^{k-1}$.

Lots of works are done to try to get near to the conjecture [10]–[15]. In 2011, Cusick et al. proved the correction of Tu-Deng Conjecture when $\mathrm{w}(t) = 1, 2$; $t = 2^k - t', \mathrm{w}(t') \leq 2$ and t' is even; $t = 2^k - t', \mathrm{w}(t') \leq 4$ and t' is odd [11]. In 2012, Huang et al. presented a paper which proved the Tu-Deng Conjecture in the case of $\mathrm{w}(t) = 3$ as well as the case of $\mathrm{w}(t) = k - 3$ [12]. In 2015, Cheng et al. gave a proof of the conjecture in case of $\mathrm{w}(t) = 4$ [13]. In 2016, Chen et al. proved the case $\mathrm{w}(t) = 5$ [15].

This paper optimizes the method and go on with the conjecture, and make the amount of cases to check reasonable for a computer when $\mathrm{w}(t) \leq 10$. The reminder of the paper is organized as follows. Section II introduces some notations and existing results. Section III explores the upper bound of $|S_t^k|$ in the case $\mathrm{w}(t) \leq 10$. Section IV concludes this paper.

II. Preliminaries

In this section, we provide some definitions and some lemmas.

Definition 3. *Given $a_k \cdots a_3 a_2 a_1 a_0$ and $b_k \cdots b_3 b_2 b_1 b_0$ that $2^k \leq a + b < 2^{k+1}$, we define its carrying chains as*

$$\begin{array}{cccc} a_k \cdots a_{u_{h-1}} & a_{u_{h-1}-1} \cdots a_{u_{h-2}} & \cdots & a_{u_1 - 1} \cdots a_{u_0} \\ b_k \cdots b_{u_{h-1}} & b_{u_{h-1}-1} \cdots b_{u_{h-2}} & \cdots & b_{u_1 - 1} \cdots b_{u_0} \end{array}$$

, and $u_h = k + 1, u_0 = 0$, where u_i contains all positions i such that $a_{i-1} \cdots a_1 a_0 + b_{i-1} \cdots b_1 b_0 < 2^i$.

We use $H(a, b)$ to represent the h we just used.

Lemma 1. $\mathrm{w}(a)+\mathrm{w}(b)\ge \mathrm{w}(a+b)$.

Proof: Let $x_i=a_i+b_i$. Since $a=\sum_{i=0}^{\infty}a_i2^i, b=\sum_{i=0}^{\infty}b_i2^i$, we know that

$$a+b=\sum_{i=0}^{\infty}x_i2^i$$

and

$$\sum_{i=0}^{\infty}x_i=\mathrm{w}(a)+\mathrm{w}(b).$$

To make $x_i\in\{0,1\}$ for each i, whenever an x_i reaches or goes beyond 2, we decrease x_i by 2, and increase x_{i+1} by 1. In this way, $\sum_{i=0}^{\infty}x_i2^i$ remains its previous value, and $\sum_{i=0}^{\infty}x_i$ decreases by 1.

Since $\sum_{i=0}^{\infty}x_i$ can't decrease infinitely, there's time when we can no longer do any move, and every x_i is in range $\{0,1\}$, and it's the binary expression of $a+b$, and $\mathrm{w}(a+b)=\sum_{i=0}^{\infty}x_i\le \mathrm{w}(a)+\mathrm{w}(b)$ since $\sum_{i=0}^{\infty}x_i$ decreases from $\mathrm{w}(a)+\mathrm{w}(b)$. ∎

Lemma 2. *[13] Let i,t,k be positive integers, and $0\le t<2^k-1$, then* $\mathrm{w}([2^it])=\mathrm{w}(t)$.

Proof: If $i=1$, then $2t=\sum_{i=0}^{k-1}t_i2^{t+1}$ as $\mathrm{len}(t)<k$, and since $[2^k]=1$, $2t\equiv\left(\sum_{i=0}^{k-2}t_i2^{t+1}\right)+t_{k-1}$, which is a valid binary expression and just a rearrangement of the binary expression of t.

In general case,

$$\mathrm{w}(t)=\mathrm{w}([2t])=\mathrm{w}([4t])=\cdots=\mathrm{w}([2^it]).$$

∎

Lemma 3. *[13] Let i,t,k be positive integers, and $0\le t<2^k-1$, then* $\left|S_t^k\right|=\left|S_{[t2^i]}^k\right|$

Proof: Since $[a+b]=t$ means $[(a2^i)+(b2^i)]=[t2^i]$, the lemma obviously satisfies. ∎

Lemma 4. *If $a+b=t$, then*

$$\mathrm{w}(a)+\mathrm{w}(b)=\mathrm{len}(t)+\mathrm{w}(t)-H(a,b).$$

Proof: Since we can directly connect $a_k\cdots a_{u_1}+b_k\cdots b_{u_1}$ and $a_{u_1-1}\cdots a_0+b_{u_1}\cdots b_0$ when $H(a,b)>1$, we only prove the situation when $H(a,b)=1$.

Since there's no carry to t_0, but some carry is made from t_0, we know that $a_0+b_0=t_0+2$, i.e., $a_0=b_0=1,t_0=0$. Similarly, there's carry to $t_{\mathrm{len}(t)-1}$, but there's no carry from $t_{\mathrm{len}(t)-1}$, so $a_0+b_0+1=t_0$, i.e., $a_0=b_0=0,t_0=1$. For other positions i, there's carry to and from t_i, so $a_i+b_i+1=t_i+2$, i.e., $t_i+1=a_i+b_i$. Now sum up all a_i's and b_i's, resulting in

$$\begin{aligned}&(a_0{+}b_0)+(a_1{+}b_1)+(a_2{+}b_2)+\cdots+(a_{\mathrm{len}(t)-1}{+}b_{\mathrm{len}(t)-1})\\&=(1+1+t_0)+(1+t_1)+(1+t_2)+\cdots+(1+t_{\mathrm{len}(t)-2})\\&=\mathrm{w}(t)+\mathrm{len}(t)-1\\&=\mathrm{w}(t)+\mathrm{len}(t)-H(a,b).\end{aligned}$$

∎

III. Main Results

Lemma 5. *If $\mathrm{len}(t)+\mathrm{w}(t)\le k+1,\mathrm{len}(t)>1,t_0=1$, then* $2\left|S_t^k\right|>\left|S_t^{k+1}\right|$.

Proof: If $[a+b]_{2^{k+1}-1}=t$, then we have either $a+b=t$ or $a+b=t+2^{k+1}-1$.

If $a_k+b_k=1$, then $a+b\ge 2^k$, meaning that it's impossible that $a+b=t$, so $a+b=t+2^{k+1}-1$. Therefore, $a_{k-1}\cdots a_1a_0+b_{k-1}\cdots b_1b_0=t+2^{k+1}-1-2^k=t+2^k$.

If $a_k=b_k=0$, then $a+b<2^{k+1}$ and $a+b=t$. If $a_k=b_k=1$, then $a+b=t+2^{k+1}-1$. Either way, $a_{k-1}\cdots a_1a_0+b_{k-1}\cdots b_1b_0=t-a_k$.

Notice that $2\left|S_t^k\right|>\left|S_t^{k+1}\right|$ means that

$$\begin{aligned}&2\left|\left\{(a,b)\middle|\begin{array}{c}a+b=t\\ \mathrm{w}(a)+\mathrm{w}(b)<k\end{array}\right\}\right|\\&+2\left|\left\{(a,b)\middle|\begin{array}{c}a+b=t+2^k-1\\ \mathrm{w}(a)+\mathrm{w}(b)<k\end{array}\right\}\right|\\&>\left|\left\{(a,b)\middle|\begin{array}{c}a+b\equiv t \pmod{2^{k+1}-1}\\ \mathrm{w}(a)+\mathrm{w}(b)\le k\end{array}\right\}\right|\\&+\left|\left\{(a,b)\middle|\begin{array}{c}(2^k+a)+(2^k+b)\equiv t \pmod{2^{k+1}-1}\\ \mathrm{w}(a)+\mathrm{w}(b)\le k-2\end{array}\right\}\right|\\&+2\left|\left\{(a,b)\middle|\begin{array}{c}a+b+2^k\equiv t \pmod{2^{k+1}-1}\\ \mathrm{w}(a)+\mathrm{w}(b)<k\end{array}\right\}\right|,\end{aligned}$$

where $0\le a,b<2^k$, which is shown to have the same meaning as

$$\begin{aligned}&2\left|\left\{(a,b)\middle|\begin{array}{c}a+b=t\\ \mathrm{w}(a)+\mathrm{w}(b)<k\end{array}\right\}\right|\\&>\left|\left\{(a,b)\middle|\begin{array}{c}a+b=t\\ \mathrm{w}(a)+\mathrm{w}(b)\le k\end{array}\right\}\right|\\&+\left|\left\{(a,b)\middle|\begin{array}{c}a+b=t-1\\ \mathrm{w}(a)+\mathrm{w}(b)\le k-2\end{array}\right\}\right|,\end{aligned}$$

and can be converted into

$$\begin{aligned}&1+\left|\left\{(a,b)\middle|\begin{array}{c}a+b=t-1\\ \mathrm{w}(a)+\mathrm{w}(b+1)<k\end{array}\right\}\right|\\&>\left|\left\{(a,b)\middle|\begin{array}{c}a+b=t\\ \mathrm{w}(a)+\mathrm{w}(b)=k\end{array}\right\}\right|\\&+\left|\left\{(a,b)\middle|\begin{array}{c}a+b=t-1\\ \mathrm{w}(a)+\mathrm{w}(b)\le k-2\end{array}\right\}\right|,\end{aligned}$$

where the 1 moved outside comes from situation $(t, 0)$ in the first element, which is excluded after the conversion because there's no non-negative integer b such that $b + 1 = 0$. Since $\mathrm{w}(b) + 1 \geq \mathrm{w}(b + 1)$, we know that

$$\left\{ (a, b) \middle| \begin{matrix} a + b + 1 = t \\ \mathrm{w}(a) + \mathrm{w}(b + 1) < k \end{matrix} \right\} \supseteq \left\{ (a, b) \middle| \begin{matrix} a + b = t - 1 \\ \mathrm{w}(a) + \mathrm{w}(b) \leq k - 2 \end{matrix} \right\},$$

and the equation has the same meaning as

$$1 + \left| \left\{ (a, b) \middle| \begin{matrix} a + b = t - 1 \\ \mathrm{w}(a) + \mathrm{w}(b + 1) < k \\ \mathrm{w}(a) + \mathrm{w}(b) > k - 2 \end{matrix} \right\} \right| > \left| \left\{ (a, b) \middle| \begin{matrix} a + b = t \\ \mathrm{w}(a) + \mathrm{w}(b) = k \end{matrix} \right\} \right|.$$

If there is a pair of integers (a, b) satisfying that $a + b = t, \mathrm{w}(a) + \mathrm{w}(b) = k$, then by Lemma 4, $\mathrm{len}(t) + \mathrm{w}(t) = \mathrm{w}(a) + \mathrm{w}(b) + H(a, b)$. Also, since $t_0 = 1$ and $\mathrm{len}(t) > 1$, we know that $H(a, b) \geq 2$, and $\mathrm{len}(t) + \mathrm{w}(t) \geq \mathrm{w}(a) + \mathrm{w}(b) + 2 = k + 2$, which is a conflict to requirement, and therefore

$$\left| \left\{ (a, b) \middle| \begin{matrix} a + b = t \\ \mathrm{w}(a) + \mathrm{w}(b) = k \end{matrix} \right\} \right| = 0,$$

and the inequality obviously apply. ■

Therefore, we can get that

Lemma 6. *Given $n > 1$, if for every integers reading*

$$\underbrace{00 \cdots 0}_{z_n} 1 \cdots \underbrace{00 \cdots 0}_{z_2} 1 \underbrace{00 \cdots 0}_{z_1} 1, \tag{1}$$

where $z_i < n$, Conjecture 1 with $k = 1 + z_1 + 1 + z_2 + \cdots + 1 + z_n$ holds, then this conjecture also holds for all non-negative integers t weighted n.

Proof: Given any integer t weighted n, we can write it as

$$\underbrace{00 \cdots 0}_{z_n} 1 \cdots \underbrace{00 \cdots 0}_{z_2} 1 \underbrace{00 \cdots 0}_{z_1} 1 \underbrace{00 \cdots 0}_{z_0}.$$

i) If $z_0 > 0$, then by lemma 3 $\left| S_t^k \right| = \left| S_{[t2^{n - z_0}]}^k \right|$, and we can replace the t with $[t2^{n - z_0}]$. It clears z_0.

ii) If $z_n \geq n$, then $\mathrm{len}(t) + \mathrm{w}(t) = k - z_n + n \leq k$, making $2 \left| S_t^{k-1} \right| < \left| S_t^k \right|$, and we can reduce k by one.

iii) If $z_0 = 0, z_i \geq n$ for some $i \neq n$, then we can replace the t with $[t2^{z_n + 1}]$, making $z_{i+1} \geq n$ and remaining $z_0 = 0$. We can just repeat till $z_n \geq n$ and apply operation ii).

Since k can't reduce infinitely, sooner or later t reads as the format in Expression (1) and it is known that the conjecture holds. ■

Lemma 5 reduces the range we need to test from an infinite class of pairs (k, t) with $\mathrm{w}(t) = n$ to n^n small instances. With a computer, we can easily work out all such instances for $2 \leq \mathrm{w}(t) \leq 10$, and some result can be found in the appendix. Since the case that $\mathrm{w}(t) < 2$ is proved [11], we can get that

Theorem 1. *Conjecture 1 holds when $\mathrm{w}(t) \leq 10$.*

For further researching, it's likely that we need the exact value of cases not listed in Lemma 6. Therefore, we need to know the exact relationship between operation ii).

Lemma 7. *If $\mathrm{len}(t) + \mathrm{w}(t) > k + 1, \mathrm{len}(t) > 1, t_0 = 1$, then $2 \left| S_t^k \right| = \left| S_t^{k+1} \right| + 1$. If $\mathrm{len}(t) + \mathrm{w}(t) = k + 1, \mathrm{len}(t) > 1, t_0 = 1$, then $2 \left| S_t^k \right| = \left| S_t^{k+1} \right| + 1 + 2^{k + 1 - 2\,\mathrm{w}(t)}$.*

Proof: Remind the proof for Lemma 5. We can get that

$$\begin{aligned} & 2 \left| S_t^k \right| - \left| S_t^{k+1} \right| \\ = & 1 + \left| \left\{ (a, b) \middle| \begin{matrix} a + b = t - 1 \\ \mathrm{w}(a) + \mathrm{w}(b + 1) < k \\ \mathrm{w}(a) + \mathrm{w}(b) > k - 2 \end{matrix} \right\} \right| \\ & - \left| \left\{ (a, b) \middle| \begin{matrix} a + b = t \\ \mathrm{w}(a) + \mathrm{w}(b) = k \end{matrix} \right\} \right| \\ = & 1 + \left| \left\{ (a, b) \middle| \begin{matrix} a + b = t - 1 \\ \mathrm{w}(a) + \mathrm{w}(b + 1) < k \\ \mathrm{w}(a) + \mathrm{w}(b) > k - 2 \end{matrix} \right\} \right|. \end{aligned} \tag{2}$$

By Lemma 4, $\mathrm{len}(t - 1) + \mathrm{w}(t - 1) = \mathrm{w}(a) + \mathrm{w}(b) + H(a, b)$. Since $s_0 = 1$, we can easily see that $\mathrm{len}(t - 1) = \mathrm{len}(t), \mathrm{w}(t - 1) = \mathrm{w}(t) - 1, H(a, b) \geq 1$, and therefore $\mathrm{len}(t) + \mathrm{w}(t) \leq \mathrm{w}(a) + \mathrm{w}(b) + 2$.

If $\mathrm{len}(t) + \mathrm{w}(t) > k + 1$, then it's a direct contrary, and Equation (2) equals to 1. If $\mathrm{len}(t) + \mathrm{w}(t) = k + 1$, then to make $\mathrm{len}(t - 1) + \mathrm{w}(t - 1) = \mathrm{w}(a) + \mathrm{w}(b) + H(a, b)$ we have to let $H(a, b) = 1$ and $\mathrm{w}(a) + \mathrm{w}(b) = k - 1$.

Since carry applies everywhere, we know that

$$a_0 + b_0 = 2,$$

$$a_i + b_i = 1 + t_i \text{ for } 0 < i < \mathrm{len}(t) - 1,$$

$$a_{\mathrm{len}(t)-1} + b_{\mathrm{len}(t)-1} = 0,$$

and now we're going to get the amount of elements.

Since $a_0 + b_0 = 2$, there's no choice but $a_0 = b_0 = 1$. Similarly, since $a_{\mathrm{len}(t)-1} + b_{\mathrm{len}(t)-1} = 0$, we're forced to have $a_{\mathrm{len}(t)-1} = b_{\mathrm{len}(t)-1} = 0$. For the rest positions, if $t_i = 0$, then $a_i + b_i = 1$, meaning there are two choices $a_i = 0, b_i = 1$ and $a_i = 1, b_i = 0$; If $t_i = 1$, then $a_i + b_i = 2$, and we only have $a_i = b_i = 1$. It's easily shown that all numbers constructed here matches all conditions.

Therefore, there are $2^{\mathrm{len}(t) - \mathrm{w}(t)}$ possible pairs of (a, b), where $\mathrm{len}(t) - \mathrm{w}(t)$ is the appearances of zeros in t. As given, $\mathrm{len}(t) + \mathrm{w}(t) = k + 1$, and thus there are $2^{k + 1 - 2\,\mathrm{w}(t)}$ possibilities. ■

TABLE I
t FOR LARGEST $\left|S_t^k\right|$ WHEN k IS LARGE ENOUGH

$\mathrm{w}(t)$	$\max \frac{\left|S_t^k\right|-1}{2^{k-1}}$ [1]	Beginning k	A possible t[1]
2	.9	5	5
3	.D	7	D
4	.DC	9	1B
5	.E	12	6B
6	.E48	14	DB
7	.E82	16	1DB
8	.EBC8	18	3B7
9	.ECBA	20	777
10	.EE17	23	1DB7

1 Numbers are represented in hexadecimal.

With such result, we can further list the maximum size of the set with given k and $\mathrm{w}(t)$. We find that when k goes to infinity, a same t always make $\left|S_t^k\right|$ largest, which is listed in Table I. Another fact is that when k is smaller, to reach the largest $\left|S_t^k\right|$, it's possible to match the format as Expression (1), and the exact maximum size can be found in the appendix.

IV. Conclusion

Boolean functions constructed based on Tu-Deng Conjecture perform very well in some cryptographic properties. It is a quite meaningful task to complete the proof of the conjecture. With the help of computer, we calculate all kinds of results we need. From the results, we proved that Tu-Deng Conjecture is correct under the condition $\mathrm{w}(t) \leq 10$, and furthermore we get the upper bound for candinality of S_t when $\mathrm{w}(t) \leq 10$.

References

[1] N. Courtois, W. Meier, "Algebraic attacks on stream ciphers with linear feedback," in Advances in Cryptology-EUROCRYPT 2003 (Lecture Notes in Computer Science), Berlin, Germany: Springer-Verlag, 2003, vol. 2656, pp. 345-359.

[2] C. Carlet, D.K. Dalai, K.C. Gupta, S. Maitra, "Algebraic immunity for cryptographically significant Boolean functions: analysis and construction," IEEE Transactions on Information Theory, vol. 52, no. 7, pp. 3105-3121, 2016.

[3] C. Carlet, X.Y. Zeng, C.L. Li, L. Hu, "Further properties of several classes of Boolean functions with optimum algebraic immunity," Designs, Codes and Cryptography, vol. 52, no. 3, pp. 303-338, 2009.

[4] D.K. Dalai, S. Maitra, S. Sarkar, "Basic theory in construction of Boolean functions with maximum possible annihilator immunity," Designs, Codes and Cryptography, vol. 40, no. 1, pp. 41-58, 2006.

[5] L.J. Qu, K.Q. Feng, F. Liu, L. Wang, "Constructing symmetric Boolean functions with maximum algebraic immunity," IEEE Transactions on Information Theory, vol. 55, no. 5, pp. 2406-2412, 2009.

[6] Y. Chen and P. Lu, "Two classes of symmetric Boolean functions with optimum algebraic immunity: Construction and analysis," IEEE Trans. Inf. Theory, vol.57, no.4, pp.2522-2538, 2011.

[7] C. Carlet and K.Q. Feng, "An infinite class of balanced functions with optimal algebraic immunity, good immunity to fast algebraic attacks and good nonlinearity," in Proc. Advances in Cryptology-ASIACRYPT, Berlin, Germany, 2008, vol. 5350, Lecture Notes in Computer Science, pp. 425-440.

[8] Z.R. Tu , Y.P. Deng, "A conjecture about binary strings and its applications on constructing Boolean function with optimal algebraic immunity," Designs, Codes and Cryptography, vol. 60, pp. 1-14, 2011.

[9] Z. Liu , B. Wu, "Recent Results on Constructing Boolean Functions with(Potentially) Optimal Algebraic Immunity Based onDecompositions of Finite Fields," J Syst Sci Complex, vol. 32, pp. 356-374, 2019.

[10] G. Cohen, J.P. Flori, "On a generalized combinatorial conjecture involving addition mod $2^k - 1$," 2011/400. [Online]. Available: http://eprint.iacr.org/, Cryptology ePrint Archive.

[11] T.W. Cusick, Y. Li, P. Stanic, "On a combinatorial conjecture," Integers, vol. 11, no. 2, pp. 185-203, 2011.

[12] K. Huang, C. Li, S.J. Fu, "Note on the Tu-Deng Conjecture," Computer Science, vol. 39, no. B06, pp. 6-8, 2012.

[13] K.M. Cheng, S.F. Hong, Y.M. Zhong, "A Note on the Tu-Deng Conjecture," Journal of Systems Science and Complexity, vol. 28, pp. 702-724, 2015.

[14] S. Qarboua, J. Schrek, C. Fontaine, "New results about Tu-Deng's conjecture," IEEE International Symposium on Information Theory, pp. 485-489, 2016.

[15] Y. Chen, F. Guo, Z. Gong, W. Cai, "One Note About the Tu-Deng Conjecture in Case $\mathrm{w}(t) = 5$," IEEE Access, vol. 7, pp. 13799-13802, 2019.

Yindong Chen was born in Jieyang, Guangdong province of China in 1983. He received the B.S. degree in mathematics from South China University of Technology in 2005, and the Ph.D. degree in computer science from the Fudan University in 2010. Currently he is an Associate Professor at Shantou University, China. His research interest is in Cryptology and Information Security.

Liming Lin was born in Jieyang, Guangdong province of China in 1997. He received the B.S. degree in mathematics from South China Normal University in 2018. Now he is a Master candidate of Shantou University, China. His research interest is in Cryptology and Information Security.

Chuliang Wei received the B.Sc. and Ph.D. degrees in electrical engineering and electronics from the University of Liverpool, Liverpool, U.K., in 2003 and 2006, respectively. He was a Research Fellow with the Department of Electrical Engineering, the Hong Kong Polytechnic University. He is currently an Associate Professor with Shantou University, Shantou, China, and he also serves as the Deputy Head of the Department of Electronic Engineering. His research interests include intelligent control and robotic system, FPGA-based applications, fiber optical sensor system, information security, image processing, and machine learning.

Appendix

Appendix: Largest $\left|S_t^k\right|$ with t matches Expression (1)

w(t)	k	max $\left\|S_t^k\right\|$	a t	w(t)	k	max $\left\|S_t^k\right\|$	a t	w(t)	k	max $\left\|S_t^k\right\|$	a t
2	3	4	10	6	23	342001	511145	8	9	100	10000000
2	4	8	11	6	24	681001	511155	8	10	200	10000001
3	4	8	100	6	25	CE4001	511255	8	11	400	10001010
3	5	10	101	6	26	19B8001	521255	8	12	7A0	20001100
3	6	1C	201	6	27	3328001	521355	8	13	F00	30010100
3	7	33	211	6	28	65D0001	511555	8	14	1DA8	40010100
3	8	65	212	6	29	CB40001	512555	8	15	3B10	50010100
3	9	C9	222	6	30	19540001	522555	8	16	75EE	60010100
4	5	10	1000	6	31	3041042	505555	8	17	EBCB	70010100
4	6	20	1001	6	32	A082084	515555	8	18	1CBA5	70010101
4	7	3C	2010	6	33	11E82085	525555	8	19	39009	70101101
4	8	70	3010	6	34	21C82087	535555	8	20	70E11	70101102
4	9	D7	2021	6	35	4188208B	545555	8	21	E0021	70110103
4	10	1A5	3111	6	36	81082093	555555	8	22	1BE041	70101104
4	11	341	3202	7	8	80	1000000	8	23	37A781	70101105
4	12	661	3113	7	9	100	1000001	8	24	6F4001	70101106
4	13	C81	3222	7	10	200	1001010	8	25	DE7401	70101107
4	14	18C1	3223	7	11	3D0	2001100	8	26	1B9C801	71011017
4	15	3101	3233	7	12	768	3001100	8	27	36EB001	70111027
4	16	6101	3333	7	13	E9C	4001100	8	28	6D82001	71111117
5	6	20	10000	7	14	1D0E	5001010	8	29	DA04001	71111127
5	7	40	10001	7	15	3A0B	6001010	8	30	1B248001	70111057
5	8	78	10101	7	16	70A5	6010101	8	31	7AD1112	32333333
5	9	EC	20110	7	17	E089	6011101	8	32	1CAA2224	33333333
5	10	1CA	30110	7	18	1BB91	6011102	8	33	2F6D0845	40144444
5	11	383	40110	7	19	37221	6011103	8	34	5A5D0847	40244444
5	12	6C5	41011	7	20	6DBC1	6011104	8	35	B091084B	40344444
5	13	D49	40112	7	21	DB201	6011105	8	36	AF408x13	40444444
5	14	1A71	41103	7	22	1B5E01	6011106	8	37	94C84x14	41444444
5	15	3441	40114	7	23	362401	6101116	8	38	840C2x15	42444444
5	16	6781	41114	7	24	6C0801	6111116	8	39	F6F42x15	43444444
5	17	CD81	42123	7	25	D69001	6111126	8	40	EEB21x16	44444444
5	18	19901	42124	7	26	1AB2001	6111136	8	41	BBF04x17	50355555
5	19	32801	41144	7	27	3538001	6111146	8	42	B9F82x18	50455555
5	20	64801	41244	7	28	6A4C001	6111156	8	43	B9741x19	50555555
5	21	C7801	42244	7	29	D478001	6111166	8	44	9C020x20	51555555
5	22	18D001	42344	7	30	1A690001	6111266	8	45	8AE10x21	52555555
5	23	316001	42444	7	31	5B88422	4044444	8	46	82708x22	53555555
5	24	624001	43444	7	32	13210844	4144444	8	47	FCA08x22	54555555
5	25	C38001	44444	7	33	21D90845	4244444	8	48	F8B04x23	55555555
6	7	40	100000	7	34	3F510847	4344444	8	49	BEE20x24	60566666
6	8	80	100001	7	35	7A81084B	4444444	8	50	BE610x25	60666666
6	9	100	101010	7	36	BE082093	5045555	8	51	9E808x26	61666666
6	10	1E0	200110	7	37	BD441x13	5055555	8	52	8E804x27	62666666
6	11	3A4	300110	7	38	9E820x14	5155555	8	53	87102x28	63666666
6	12	72E	401010	7	39	8D410x15	5255555	8	54	82681x29	64666666
6	13	E4B	501010	7	40	84E08x16	5355555	8	55	80440x30	65666666
6	14	1BE5	510101	7	41	80D04x17	5455555	8	56	FE840x30	66666666
6	15	3709	501102	7	42	FD904x17	5555555	8	57	C0004x31	70777777
6	16	6C91	501103	7	43	C0010x18	6066666	8	58	9FE02x32	71777777
6	17	D861	501104	7	44	9FC08x19	6166666	8	59	8FD01x33	72777777
6	18	1AF81	501105	7	45	8FA04x20	6266666	8	60	87C80x34	73777777
6	19	35301	501115	7	46	88102x21	6366666	8	61	83C40x35	74777777
6	20	6A201	511115	7	47	83881x22	6466666	8	62	81C20x36	75777777
6	21	D2C01	511125	7	48	81840x23	6566666	8	63	81010x37	76777777
6	22	1A2801	511135	7	49	80820x24	6666666	8	64	80808x38	77777777

w(t)	k	max $\left\lvert S_t^k \right\rvert$	a t	w(t)	k	max $\left\lvert S_t^k \right\rvert$	a t	w(t)	k	max $\left\lvert S_t^k \right\rvert$	a t
9	10	200	100000000	9	64	C0008x38	706777777	10	47	8D844x24	4144444444
9	11	400	100000001	9	65	BF304x39	707777777	10	48	FCB04x24	4244444444
9	12	800	100001010	9	66	9F302x40	717777777	10	49	EC932x25	4344444444
9	13	F80	200100100	9	67	8F201x41	727777777	10	50	E47A1x26	4444444444
9	14	1E20	200101100	9	68	87180x42	737777777	10	51	C0B30x27	5015555555
9	15	3B90	400010100	9	69	83140x43	747777777	10	52	B84A8x28	5025555555
9	16	7698	500010100	9	70	81120x44	757777777	10	53	B4164x29	5035555555
9	17	ECD8	600100100	9	71	80210x45	767777777	10	54	B22F2x30	5045555555
9	18	1D97E	700100100	9	72	80008x46	777777777	10	55	B1AA1x31	5055555555
9	19	3B2EB	800100100	9	73	C0201x46	808888888	10	56	96420x32	5155555555
9	20	749E5	800101010	9	74	9FF00x47	818888888	10	57	861B0x33	5255555555
9	21	E6A09	801011001	9	75	8FE80x48	828888888	10	58	FBAD0x33	5355555555
9	22	1C9611	801011002	9	76	87E40x49	838888888	10	59	F36A8x34	5455555555
9	23	38B821	810111101	9	77	83E20x50	848888888	10	60	EF824x35	5555555555
9	24	70FE41	801010104	9	78	81E10x51	858888888	10	61	BD081x36	6036666666
9	25	E1B081	801010105	9	79	80E08x52	868888888	10	62	BAAC0x37	6046666666
9	26	1C31F01	801010106	9	80	80604x53	878888888	10	63	B9440x38	6056666666
9	27	3861801	801010107	9	81	80202x54	888888888	10	64	BA810x39	6066666666
9	28	70C1801	801010108	10	11	400	1000000000	10	65	9B288x40	6166666666
9	29	DFC9001	801011018	10	12	800	1000000001	10	66	8B1E4x41	6266666666
9	30	1BE92001	810111018	10	13	1000	1000001010	10	67	83062x42	6366666666
9	31	A881112	301333333	10	14	1F00	1001001001	10	68	FDFC2x42	6466666666
9	32	28542224	302333333	10	15	3D40	2001010100	10	69	FA101x43	6566666666
9	33	4E472225	303333333	10	16	78C0	3001010100	10	70	F8780x44	6666666666
9	34	84D72227	313333333	10	17	EF50	4001010100	10	71	BEC08x45	7067777776
9	35	EE9A222B	323333333	10	18	1DD20	5001010100	10	72	BEC08x46	7067777777
9	36	DFF91x13	333333333	10	19	3B8E8	6001010100	10	73	BDD04x47	7077777777
9	37	C7A84x14	400444444	10	20	77100	7001010100	10	74	9E2C2x48	7177777777
9	38	B8662x15	401444444	10	21	EE185	8001010100	10	75	8E241x49	7277777777
9	39	AFFE1x16	402444444	10	22	1DC2E5	9001010100	10	76	861C0x50	7377777777
9	40	ABDB0x17	403444444	10	23	3A2F89	9010101001	10	77	82180x51	7477777777
9	41	AA5E8x18	404444444	10	24	738691	9010101002	10	78	801A0x52	7577777777
9	42	90E84x19	414444444	10	25	E57821	9101011101	10	79	FE6A0x52	7677777777
9	43	81062x20	424444444	10	26	1C91641	9010101004	10	80	FE410x53	7777777777
9	44	F16C2x20	434444444	10	27	390D881	9010101005	10	81	BFE01x54	8088888878
9	45	E9361x21	444444444	10	28	7207901	9010101006	10	82	BFE01x55	8088888888
9	46	BC0C8x22	502555555	10	29	E404E01	9010101007	10	83	9F980x56	8188888888
9	47	B7D84x23	503555555	10	30	1C801001	9001010108	10	84	8F880x57	8288888888
9	48	B5F02x24	504555555	10	31	BAEB112	3000333333	10	85	87840x58	8388888888
9	49	B5741x25	505555555	10	32	2D502224	3001333333	10	86	83820x59	8488888888
9	50	99220x26	515555555	10	33	58544225	3002333333	10	87	81810x60	8588888888
9	51	88750x27	525555555	10	34	AE322227	3003333333	10	88	80808x61	8688888888
9	52	80108x28	535555555	10	35	A3AE9x13	3013333333	10	89	80004x62	8788888888
9	53	F7D88x28	545555555	10	36	9D878x14	3023333333	10	90	FF904x62	8888888888
9	54	F3F04x29	555555555	10	37	992F4x15	3033333333	10	91	C0000x63	9099999999
9	55	BD6C0x30	604666666	10	38	820B2x16	3133333333	10	92	9FF80x64	9199999999
9	56	BC620x31	605666666	10	39	E9C6Ax16	3233333333	10	93	8FF40x65	9299999999
9	57	BBE10x32	606666666	10	40	DB7D1x17	3333333333	10	94	88020x66	9399999999
9	58	9CD88x33	616666666	10	41	C1D64x18	4004444443	10	95	83B0Ax67	9499999999
9	59	8D004x34	626666666	10	42	C1C44x19	4004444444	10	96	82008x68	9599999999
9	60	85902x35	636666666	10	43	B3C22x20	4014444444	10	97	80F04x69	9699999999
9	61	80E81x36	646666666	10	44	ABDC1x21	4024444444	10	98	80702x70	9799999999
9	62	FD681x36	656666666	10	45	A7D98x22	4034444444	10	99	80301x71	9899999999
9	63	FAB40x37	666666666	10	46	A63F0x23	4044444444	10	100	80100x72	9999999999

Numbers in columns max $\left\lvert S_t^k \right\rvert$ are represented in hexadecimal, where ”x” with a decimal number r means multiply by 2^r, and maybe plus a positive integer smaller than 2^r.
Numbers in columns t are represented as a string $z_n \cdots z_2 z_1$.