The Range of Reasonable Parameters for Cryptanalytic Tradeoff Algorithms: Focusing on the Rainbow Tradeoff Algorithm

by

Taehwan Kim

A DISSERTATION

Submitted to the faculty of the Graduate School
in partial fulfillment of the requirements
for the degree Master of Science
in the Department of Mathematical Sciences
Seoul National University
February 2013

Abstract

We suggest a new terminology, *reasonable tradeoff parameters* in a fixed tradeoff algorithm. In brief, if there is no other set of parameters which is a comparative advantage in terms all of the tradeoff efficiency, the cost of pre-computation and the probability of success, we call it a reasonable set of parameters. And the criterion for tradeoff parameters being reasonable is also obtained.

As an additional corollary, it is showed that if one of the tradeoff efficiency, the cost of pre-computation and the probability of success is given with the table count l in the rainbow tradeoff (instead, with the matrix stopping constant in the Hellman and the DP case), the remaining ones are uniquely determined and tradeoff parameters implementing these values always exist.

The concept of reasonable tradeoff parameters is extended to the case of comparing two sets of parameters from two different tradeoff algorithms respectively. Under assumptions typically considered in theoretical discussions, we conclude that in the range of the high value of the probability of success, we get reasonable tradeoff parameters by selecting the rainbow tradeoff only. And the method to get these reasonable tradeoff parameters is obtained.

Keywords : Hellman tradeoff, DP tradeoff, Rainbow tradeoff, optimal tradeoff parameters, reasonable tradeoff parameters
Student number : 2011–20267

Contents

1 Introduction

Historically, the time memory tradeoff algorithm was described as the method to attack the 64-bit block cipher DES in 1980 [4]. As a modification, the Distinguished Point (DP) method was introduced in the book [3]. Afterwards, Oechslin designed another modified tradeoff algorithm, the rainbow table method [9]. While there are many other modified tradeoff algorithms, we only concentrate on these three tradeoff algorithms which are called the Hellman tradeoff, the DP tradeoff and the rainbow tradeoff, respectively. And for the readers familiar to the time-memory tradeoff algorithms, it is made clear that we treat non-perfect table versions of the three tradeoff algorithms (the explanation about the perfect table method will not be provided in this paper).

When a new modified tradeoff algorithm is introduced, one should research its advantages and disadvantages compared with existing tradeoff algorithms. However, the comparison of tradeoff algorithms has been controversial for some reasons. First of all, it is a hard work to find the accurate expected values of online time, probability of success and so on. Second, to compare their tradeoff efficiencies, the unit of memory and time should be unified between tradeoff algorithms. And tradeoff algorithms could be estimated in a variety of view such as not only tradeoff efficiency, but also the cost of pre-computation, the probability of success and so on. So, assessing the comparative advantage of them only in terms of tradeoff efficiency could not be a fair comparison.

In [6], authors obtained the condition of tradeoff parameters providing the best tradeoff efficiency under circumstances where the probability of success is fixed. This paper is a follow-up study on this subject. We suggest a new terminology, *reasonable tradeoff parameters*. The precise mathematical definition is in Section 4.1. In brief, for a set of parameters, if there is no other set of parameters which is a comparative advantage in terms all of the tradeoff efficiency, the cost of pre-computation and the probability of success, we call it a reasonable set of parameters (or reasonable tradeoff parameters). Here, it should be noted that the notion of being reasonable is confined to the case of comparison between sets of parameters in the *same* tradeoff algorithm (the reason is explained in Section 4.1 and 4.8). The main interest of this paper is to obtain the criterion for tradeoff parameters being reasonable.

The remainder of this paper is organized as follows. In Section 2, we explain how the three tradeoff algorithms are processed. In Section 3, analyses on the probability of success, the tradeoff curve and the cost of pre-computation are introduced from early rough analyses to recent accurate analyses. Section 4 is the main part of this paper. In Section 4.1, the new terminology, reasonable tradeoff parameters is strictly defined. In Section

4.2–4.6, the study is focused on the case of the rainbow tradeoff only. In Section 4.2, the research in [6] to obtain the best tradeoff efficiency under circumstances where the probability of success is fixed is introduced. In Section 4.3–4.5, it is studied how to search out unreasonable tradeoff parameters under circumstances where one of the tradeoff efficiency, the cost of pre-computation and the probability of success is fixed. In Section 4.6, a method to find all reasonable tradeoff parameters is studied not fixing any of the tradeoff efficiency, the cost of pre-computation and the probability of success. And the results of Section 4.2–4.5 are reinterpreted in the united point of view. In Section 4.7, the result of Section 4.6 is extended to the Hellman and the DP tradeoff. Lastly, in Section 4.8, the concept of reasonable tradeoff parameters is extended to the case of comparing two sets of parameters from two different tradeoff algorithms respectively.

2 Inversion Problem and Time Memory Tradeoff Algorithms

2.1 Inversion problem

Let $f : \mathcal{N} \to \mathcal{H}$ be a one-way function. The inversion problem is to find x when the target $y = f(x)$ is given. In cryptanalysis, to find any $x' \in \mathcal{N}$ satisfying $f(x') = y$ is occasionally sufficient instead of the correct answer $x \in \mathcal{N}$. So we could think of two versions of the inversion problem: One is to find the correct answer $x \in \mathcal{N}$, which is called *the version* of the inversion problem. The other is to find any answer $x' \in \mathcal{N}$ that satisfies $f(x') = y$, which is called *any version* of the inversion problem. Analyses of tradeoff algorithm depends on what we choose between the version and any version, so we have to make it clear. In this paper, we will deal with *the version* of the inversion problem.

2.2 Hellman, DP and rainbow time memory tradeoff algorithms

The tradeoff algorithm comprises of two phases. One is the pre-computation phase, where images of f on elements of $\mathcal{N}$ are calculated and some of them are stored in the memory. The other is the online phase, where the target $y = f(x)$ is given and the process for finding the correct answer x using the stored information is assigned.

2.2.1 Hellman tradeoff

Let N be the size of the domain $\mathcal{N}$ of the one-way function $f : \mathcal{N} \to \mathcal{H}$. Tradeoff parameters m, t, l should be set to satisfy $1 \ll m, t \ll N, l \approx t$ and *the matrix stopping rule* $mt^2 \approx N$. Matrices are made in the pre-computation phase. Here, l, m and $t+1$ denote the number of matrices, rows in each matrix and columns in each matrix respectively. For k $(1 \leq k \leq l)$, reduction functions $R_k : \mathcal{H} \to \mathcal{N}$ which is easily calculated are selected, and $f_k : \mathcal{N} \to \mathcal{N}$ is defined with $f_k = R_k \circ f$ which is used in the k-th matrix.

Next, k-th matrix is constructed as follows. First, we choose randomly $sp_1^k, \cdots, sp_m^k \in \mathcal{N}$. We set sp_i^k as the element of the i-th row $(1 \leq i \leq m)$ and the 0-th column of the k-th matrix $(1 \leq k \leq l)$. Let $sp_i^k = x_{i,0}^k$ be the starting point of the i-th row, then we obtain $x_{i,j}^k$ iteratively from $x_{i,j}^k = f_k(x_{i,j-1}^k)$ $(1 \leq j \leq t)$. Then, $x_{i,j}^k$ $(0 \leq j \leq t)$ is set to be the element of the i-th row and the j-th column of the k-th matrix. Since $x_{i,t}^k$ can be regarded as the end point of the i-th row, we denote this as $x_{i,t}^k = ep_i^k$.

The $m \times (t+1)$ matrix made by these processes is called a *Hellman matrix* of size $m \times t$ which is usually visualized as follows.

$$\begin{aligned}
sp_1^k = x_{1,0}^k &\xrightarrow{f_k} x_{1,1}^k \xrightarrow{f_k} \cdots \xrightarrow{f_k} x_{1,t-1}^k \xrightarrow{f_k} x_{1,t}^k = ep_1^k \\
sp_2^k = x_{2,0}^k &\xrightarrow{f_k} x_{2,1}^k \xrightarrow{f_k} \cdots \xrightarrow{f_k} x_{2,t-1}^k \xrightarrow{f_k} x_{2,t}^k = ep_2^k \\
&\vdots \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \vdots \\
sp_m^k = x_{m,0}^k &\xrightarrow{f_k} x_{m,1}^k \xrightarrow{f_k} \cdots \xrightarrow{f_k} x_{m,t-1}^k \xrightarrow{f_k} x_{m,t}^k = ep_m^k
\end{aligned}$$

The sequence which is generated by acting f_k iteratively is called a *Hellman chain*. Each row of the matrix which is a Hellman chain is called *pre-computation chain* and the length of it is defined as t.

In the memory, not all elements of the Hellman matrices but only the ordered pairs $\{(sp_i^k, ep_i^k)\}_{i=1}^m$ are stored after sorted by ending points. For a fixed k, the set $\{(sp_i^k, ep_i^k)\}_{i=1}^m$ is called the k-th *Hellman table*. This is the end of the pre-computation phase of the Hellman tradeoff.

The online phase begins when a target $y = f(x)$ is given. The online phase is processed for each fixed k $(1 \leq k \leq l)$. A Hellman chain which is made by acting f_k iteratively starting with $R_k(y) = R_k \circ f(x) = f_k(x)$ is called the k-th *online chain*. The k-th online chain is visualized as below.

$$\left(x \xrightarrow{f_k}\right) y_1^k \xrightarrow{f_k} \cdots \xrightarrow{f_k} y_j^k$$

When an y_j^k $(1 \leq j \leq t)$ is generated, the element ep_i^k satisfying $y_j^k = ep_i^k$ is searched out among the stored elements $\{ep_i^k\}_{i=1}^m$ by table lookups. If there exists the element ep_i^k satisfying $y_j^k = ep_i^k$, then the pre-computation chain starting with the sp_i^k is regenerated up to $x_{i,t-j}^k$. However, if f_k is not injective, $x_{i,t-j}^k$ is not guaranteed to be the correct answer x. The case of $x_{i,t-j}^k \neq x$ is called a *false alarm*. If there is no ep_i^k satisfying $y_j^k = ep_i^k$ or a false alarm occurs, then the next element y_{j+1}^k $(1 \leq j \leq t-1)$ is generated, so that the same process is repeated. If the correct answer is not found with the k-th online chain, the same process is repeated using $(k+1)$-th online chain.

2.2.2 DP tradeoff

The entire process of the DP tradeoff is similar with the Hellman tradeoff. So the process of the DP tradeoff will be explained focusing on the differences between them.

Tradeoff parameters m, t, l are to be set to satisfy the same condition in the case of the Hellman tradeoff. However, the parameter t does not denote the exact length of the pre-computation chain. It will denote the expected value of the length of the DP chain.

The most distinct feature is that a property which is satisfied by a random element of $\mathcal{N}$ with probability $1/t$ is chosen. We call this property a *distinguishing property* and an element satisfying this property a *distinguished point* (DP). The distinguishing property should be very easy to be checked. For example, when $\mathcal{N}$ is the set of n-bit integers, if we set $t = 2^s$ and choose the distinguishing property as the last s-bit is zero, then this property can readily be checked.

Reduction functions $R_k : \mathcal{H} \to \mathcal{N}$ are selected and we define $f_k : \mathcal{N} \to \mathcal{N}$ with $f_k = R_k \circ f$ which is used in the k-th matrix. A sequence of elements of $\mathcal{N}$ which is generated by acting f_k iteratively until a DP appears is called a *DP chain*.

Choosing $sp_1^k, \cdots, sp_m^k \in \mathcal{N}$ randomly, a DP chain starting with sp_i^k is set to be the i-th row and the 0-th column of the k-th *DP matrix*. We call a DP chain in the DP matrix as the row a pre-computation chain. Strictly, the length of a DP chain is not fixed, so what we make is not a matrix. But it will be allowed to use the name a DP matrix.

Note that when we make the pre-computation chain, it is possible that a DP does not appear forever. To prevent this, we set the chain length bound $\hat{t}$. If a DP does not appear until the length of the chain reaches $\hat{t}$, then this chain is discarded and another chain is tried. In this paper, we only treat the case that $\hat{t}$ is sufficiently larger than t. In this case, the number of discarded chains is minimized and most of the pre-computation is put to use.

When l DP matrices are made, $\{(sp_i^k, ep_i^k)\}_{i=1}^m$ is stored in the memory after sorted by ending points. For a fixed k, the set $\{(sp_i^k, ep_i^k)\}_{i=1}^m$ is called the k-th *DP table*. This is the end of the pre-computation phase of the DP tradeoff.

In the online phase, the differences from the Hellman tradeoff are as follows. Table lookups are needed only when the online chain reaches a DP because the ending points in the DP table are consist only of DPs. And when the pre-computation chain is regenerated to resolve an alarm the pre-computation chain is to be generated entirely until the DP appears because the length of the pre-computation chain is not known. To avoid this, we can think of storing the chain length in the memory. But this gives rise to the side effect of increasing the pre-computation table size. And when a false alarm occurs, the online chain should be discarded because the pre-computation chain do not have another DP in the middle of it.

2.2.3 Rainbow tradeoff

The entire process is similar with that of the Hellman tradeoff, so the process of the rainbow tradeoff is explained focusing on the differences.

Tradeoff parameters m, t are set to satisfy $1 \ll m, t \ll N$ and the matrix

stopping rule $mt \approx N$. Note that the matrix stopping rule is different from the ones for the previous two tradeoff algorithms. And the parameter l is to be set not to satisfy $l \approx t$, but to be a small positive integer.

The most distinct feature is that t reduction functions are selected for each *rainbow matrix*, Thus, we should use double indices to denote reduction functions such as $R_{k,i} : \mathcal{H} \to \mathcal{N}$ $(1 \leq i \leq t,\ 1 \leq k \leq l)$. And then $f_{k,i} : \mathcal{H} \to \mathcal{N}$ is defined by $f_{k,i} = R_{k,i} \circ f$.

A sequence of $t+1$ elements of $\mathcal{N}$ which is generated by acting $f_{k,1}, \cdots, f_{k,t}$ iteratively in turn is called a *rainbow chain*. We choose randomly sp_1^k, $\cdots$, $sp_m^k \in \mathcal{N}$ randomly. A rainbow chain starting with sp_i^k is set to be the i-th row of the k-th rainbow matrix. We call a rainbow chain as the row in the rainbow matrix a pre-computation chain.

When l rainbow matrices are made, $\{(sp_i^k, ep_i^k)\}_{i=1}^m$ is stored in the memory after sorted by ending points. For a fixed k, the set $\{(sp_i^k, ep_i^k)\}_{i=1}^m$ is called the k-th *rainbow table*. This is the end of the pre-computation phase of the rainbow tradeoff.

The j-th online chain in k-th rainbow table $(1 \leq j \leq t, 1 \leq k \leq l)$ is made as follows.

$$\left(x \xrightarrow{f_{k,t-j+1}}\right) y_{t-j+1}^{k,j} \xrightarrow{f_{k,t-j+2}} y_{t-j+2}^{k,j} \xrightarrow{f_{k,t-j+3}} \cdots \xrightarrow{f_{k,t}} y_t^{k,j}$$

For a fixed j, searching an ep_i^k satisfying $y_t^{k,j} = ep_i^k$ is tried for all $1 \leq k \leq l$. If there is no such an ending point or a false alarm occurs for all $1 \leq k \leq l$, then the next procedure for the fixed $j+1$ is processed. This is another distinct feature of the rainbow tradeoff, which is called the parallel processing of the rainbow tradeoff. According to [9], this parallel approach is more efficient in the sense of the expected number of one-way function iterations.

3 Analyses of Time Memory Tradeoff Algorithms

In this section, we introduce analyses of the probability of success, the tradeoff curve and so forth from early rough analyses to recent accurate ones. Rough analyses in this section can be found in [6]. And the reader who wonders where these analyses are originated may also get the answer in [6]. In the case of recent accurate analyses, justifications will be omitted because long and detailed discussions are needed.

Terminologies such as the matrix stopping constant, the pre-computation coefficient, the probability of success and the tradeoff coefficient will be used frequently in Section 4. For emphasis, the title of each subsection is named according to these terminologies.

3.1 Hellman tradeoff

3.1.1 Matrix stopping constant

In the Hellman tradeoff, parameters m, t is set to satisfy the matrix stopping rule $mt^2 \approx N$. The basis of it is as follows.

Suppose a Hellman matrix of size $m \times t$ has not too many duplicates. Using the randomness of f and the well-known fact

$$\Big(1 - \frac{1}{b}\Big)^a \approx 1 - \exp\Big(-\frac{a}{b}\Big) \text{ if } a = O(b),$$

we are led to a conclusion that when one chain of length t is added to the matrix, the probability of occurrence of duplicates between the matrix and the chain is

$$1 - \Big(1 - \frac{mt}{N}\Big)^t \approx 1 - \exp\Big(-\frac{mt^2}{N}\Big).$$

Thus, when $mt^2 \approx N$, duplicates occur in the high probability of $1 - 1/e \approx 63.2\%$, so that it is better to make a next matrix rather than to enlarge the size of the matrix. So, it is recommended to set parameters m, t to satisfy $mt^2 \approx N$. We can express this as

$$mt^2 = \mathrm{H}_{msc} N \tag{3.1}$$

where $\mathrm{H}_{msc} = \Theta(1)$ is called the *matrix stopping constant* of the Hellman tradeoff.

3.1.2 Probability of success and pre-computation coefficient

In one Hellman matrix, the success in finding the correct answer x depends on whether there exists the correct answer x in the matrix excluding ending points. Thus, the probability of success to find the correct answer x in one Hellman matrix is $|HM|/N$. Because the probability of success to find the correct answer x in the Hellman tradeoff is equal to the probability of existence of the correct answer x in l Hellman matrices excluding ending points, it is obtained as

$$1 - \Big(1 - \frac{|HM|}{N}\Big)^l \approx 1 - \exp\Big(-\frac{l|HM|}{N}\Big).$$

So, if we apply $|HM| \approx mt$. $l \approx t$ and the matrix stopping rule, we can roughly analyse that the probability of success of the Hellman tradeoff is

$$1 - \frac{1}{e} \approx 63.2\%.$$

Next, we introduce more accurate analyses. In [4], a lower bound of $|HM|/N$ was obtained as

$$\frac{|HM|}{N} \geq \frac{1}{N}\sum_{i=1}^{m}\sum_{j=1}^{t}\Big(1 - \frac{it}{N}\Big)^j.$$

Later, in [7], the above was approximated as

$$\frac{|HM|}{N} \geq \frac{mt}{N}\frac{1}{\mathrm{H}_{msc}}\int_0^{\mathrm{H}_{msc}}\frac{1-e^{-x}}{x}dx.$$

When we take $\mathrm{H}_{msc} = 1$, we get the right hand side of the formula above to be $0.80mt/N$. But according to the experiments in [7], we get $|HM|/N = 0.85mt/N$. This means that the above inequality can not be considered as being tight.

Recently, in [2] and [8], $|HM|/N$ is accurately calculated not as the lower bound but as the expected value. Using these results, in [6], the probability of success of the Hellman tradeoff accurately calculated as the expected value. The summary of the long story is as follows. Since the number of one-way function iterations needed in the pre-computation phase of the Hellman tradeoff is mtl, it is natural to define the *pre-computation coefficient* H_{pc} as

$$\mathrm{H}_{pc} = \frac{mtl}{N}. \tag{3.2}$$

If we define the coverage rate H_{cr} as the expected value of $|HM|/N$, then

$$H_{cr} = \frac{\sqrt{2}}{\sqrt{\mathrm{H}_{msc}}}\frac{e^{\sqrt{2\mathrm{H}_{msc}}}-1}{e^{\sqrt{2\mathrm{H}_{msc}}}+1}. \tag{3.3}$$

Thus, the probability of failure to find the correct answer x in one Hellman matrix is $1-H_{cr}mt/N$ and the probability of success of the Hellman tradeoff, H_{ps} is

$$\begin{aligned}\mathrm{H}_{ps} = 1 - \Big(1 - \frac{H_{cr}mt}{N}\Big)^{l} &\approx 1 - \exp\Big(-H_{cr}\frac{mt}{N}\Big) \\ &= 1 - \exp(-H_{cr}\mathrm{H}_{pc}).\end{aligned} \tag{3.4}$$

3.1.3 Cost of resolving alarms

This subsection is for the next subsection on the tradeoff coefficient.

When an alarm $y_j^k = ep_i^k$ occurs in the online phase, $t-j$ times of one-way function iterations for regenerating the pre-computation chain is processed to resolve the alarm. Then it is checked whether it is a false alarm or not. So, to resolve alarms in the online process for one Hellman table, the number of one-way function iterations is

$$t + (t-1) + \cdots + 1 \approx \frac{t^2}{2},$$

which is the worst case complexity. In [6], the number of one-way function iterations to resolve alarms in the online process for one table is calculated as

$$\frac{\mathrm{H}_{msc}}{6}t,$$

which is the expected value.

3.1.4 Tradeoff coefficient

In this subsection, we deal with the tradeoff curve which is the equation denoting the relations between the online time and the storage.

Define M as the number of ordered pairs (sp_i^k, ep_i^k) to be stored. It is easily calculated as $M = ml$. And define T as the number of one-way function iterations in the online process. Ignoring the cost of resolving alarms, it can be roughly analysed as $T = tl$, because the length of the online chain is t as the worst case complexity. Thus, applying $l \approx t$ and the matrix stopping rule, we obtain the following relation

$$TM^2 \approx N^2$$

which is called the *tradeoff curve* of the Hellman tradeoff.

Note that if we set tradeoff parameters m, t, l as $m = M/\sqrt{T}, t = \sqrt{T}, l \approx t$, then they satisfy $1 \ll m, t \ll N$, the matrix stopping rule, $l \approx t$ and the tradeoff curve. That is, any value (T, M) in the range of satisfying the tradeoff curve can always be implemented.

However, $T = tl$ is a very rough analysis. It does not reflect the cost of resolving alarms and it is not the expected value but the worst case complexity. In [6], the expected value reflecting the cost of resolving alarms was calculated and the tradeoff curve was obtained accurately as

$$TM^2 = \mathrm{H}_{tc}N^2,$$

where

$$\mathrm{H}_{tc} = \Big(\frac{1}{\mathrm{H}_{msc}} + \frac{1}{6}\Big)\frac{1}{H_{cr}^3}\mathrm{H}_{ps}\{(\ln(1-\mathrm{H}_{ps})\}^2. \tag{3.5}$$

Here, H_{tc} is called the *tradeoff coefficient* of the Hellman tradeoff.

Note that H_{tc} does not reflect the time required for table lookups, so that the number of table lookups should be calculated separately to treat the real physical time in the online phase. In [6], the expected value of the number of table lookups in the online process for one Hellman table was calculated as

$$t^2\frac{\mathrm{H}_{ps}}{H_{\mathrm{cr}}\mathrm{H}_{msc}}.$$

3.2 DP tradeoff

3.2.1 Matrix stopping constant

In the DP tradeoff, parameters m, t are set to satisfy the matrix stopping rule $mt^2 \approx N$ which is same with that of the Hellman tradeoff. And the basis of it is similar to the case of the Hellman tradeoff. So, we will omit it. We can express this as

$$mt^2 = \mathrm{D}_{msc}N \tag{3.6}$$

where $\mathrm{D}_{msc} = \Theta(1)$ is called the matrix stopping constant of the DP matrix.

3.2.2 Probability of success and pre-computation coefficient

By the similar argument with the Hellman tradeoff, the probability of the existence of the correct answer x in l DP matrices excluding ending points is

$$1 - \Big(1 - \frac{|DM|}{N}\Big)^l \approx 1 - \exp\Big(-\frac{l|DM|}{N}\Big).$$

So, if we apply $|DM| \approx mt$, $l \approx t$ and the matrix stopping rule, we can roughly analyse that the probability of success of the DP tradeoff is

$$1 - \frac{1}{e} \approx 63.2\%.$$

In [6], the probability of success of DP tradeoff was accurately calculated. The summary of the long story is as follows. When $\hat{t}$ is sufficiently large, the expected value of the length of one pre-computation chain can be approximated as t. Thus, the number of one-way function iterations needed in the pre-computation phase of the Hellman tradeoff is mtl. It is natural to define the pre-computation coefficient D_{pc} as

$$\mathrm{D}_{pc} = \frac{mtl}{N}. \tag{3.7}$$

And if we define the coverage rate D_{cr} as the expected value of $|DM|/mt$, then

$$D_{cr} = \frac{|DM|}{mt} = \frac{2}{\sqrt{1 + 2\mathrm{D}_{msc}} + 1}, \tag{3.8}$$

when $\hat{t}$ is sufficiently large. Thus, the probability of failure to find the correct answer x in one DP matrix is $1 - D_{cr}mt/N$ and the probability of success of DP tradeoff, D_{ps} is

$$\begin{aligned} \mathrm{D}_{ps} = 1 - \Big(1 - \frac{D_{\mathrm{cr}}mt}{N}\Big)^{l} &\approx 1 - \exp\Big(-D_{\mathrm{cr}}\frac{mt}{N}\Big) \\ &= 1 - \exp(-D_{\mathrm{cr}}\mathrm{D}_{pc}). \end{aligned} \tag{3.9}$$

3.2.3 Tradeoff coefficient

In the DP tradeoff, $M = ml$. And, ignoring the cost of resolving alarms, the value of T can be roughly analysed as $T = tl$, because the expected value of the length of the online chain can be approximated as t when $\hat{t}$ is sufficiently large. Thus, applying $l \approx t$ and the matrix stopping rule, we obtain the tradeoff curve

$$TM^2 \approx N^2,$$

which is the same with the Hellman tradeoff.

However, $T = tl$ is a very rough analysis. It does not reflect the cost of resolving alarm and the assumption that all of l table is used means that what we calculate is not the expected value. In [6], the expected value reflecting the cost of resolving alarms was calculated and the tradeoff curve was obtained accurately as follows.

$$TM^2 = \mathrm{D}_{tc}N^2,$$

where

$$\mathrm{D}_{tc} = \Big(2 + \frac{1}{\mathrm{D}_{msc}}\Big)\frac{1}{D_{\mathrm{cr}}^3}\mathrm{D}_{ps}\{(\ln(1 - \mathrm{D}_{ps})\}^2. \tag{3.10}$$

Here, D_{tc} is called the tradeoff coefficient of the DP tradeoff.

And, the expected value of the number of table lookups in the online process for one DP table was calculated as

$$t\frac{\mathrm{D}_{ps}}{D_{cr}\mathrm{D}_{msc}}.$$

3.3 Rainbow tradeoff

3.3.1 Matrix stopping constant

In the rainbow tradeoff, parameters m, t are set to satisfy the matrix stopping rule. The basis of it is as below.

In contrast to the Hellman and the DP tradeoff, merging chain in one rainbow matrix occurs only when a collision occurs in the same column. Suppose a rainbow matrix of size $m \times t$ has not too many collisions in each columns. Using the randomness of f, we obtain that when one chain of length t is added to the matrix, the probability of the occurrence of collisions in a column between the matrix and the chain is as follows.

$$1 - \Big(1 - \frac{m}{N}\Big)^t \approx 1 - \exp\Big(-\frac{mt}{N}\Big)$$

Thus, when $mt \approx N$, a merging chain occurs in high probability of $1 - 1/e \approx 63.2\%$, so it is better to make a next matrix rather than to enlarge the size of the matrix. So, it is recommended to set parameters m, t to satisfy $mt \approx N$. We can express this as

$$mt = \mathrm{R}_{msc}N, \tag{3.11}$$

where $\mathrm{R}_{msc} = \Theta(1)$ is called the matrix stopping constant of the rainbow tradeoff.

3.3.2 Probability of success and pre-computation coefficient

First of all, let us discuss the cost of pre-computation. Because the length of one pre-computation chain is t, the number of one-way function iterations needed in the pre-computation phase of the Hellman tradeoff is mtl. So, to define the pre-computation coefficient R_{pc} as

$$\mathrm{R}_{pc} = \frac{mtl}{N} \tag{3.12}$$

is natural.

In the second place, let us consider the probability of success. Assume $l = 1$ and there is no collision in each column of the rainbow matrix . By the

similar argument with the Hellman tradeoff, the probability of the existence of the correct answer in the rainbow matrix excluding ending points is

$$1-\Big(1-\frac{m}{N}\Big)^t \approx 1-\exp\Big(-\frac{mt}{N}\Big) \approx 1-\frac{1}{e} \approx 63.2\%.$$

Next, we introduce accurate analyses on the probability of success. In [9], with the assumption $l=1$, the probability of success was calculated as $1-\prod_{j=0}^{t-1}\big(1-\frac{m_j}{N}\big)$. In [1], with additional assumptions $m=N$ and using perfect table, the above term was approximated as $1-\prod_{j=t-i}^{t-1}\big(1-\frac{m_j}{N}\big) \approx \frac{t-i}{t}\frac{t-i+1}{t+1}$. In [5], the probability of failure of the first k times iteration in the online phase was approximated as $1-\prod_{i=1}^{k}\big(1-\frac{m_{t-i}}{N}\big)^l \approx \big(1-\frac{\mathrm{R}_{msc}}{2+\mathrm{R}_{msc}}\frac{k+1}{t}\big)^{2l}$. In the basis of these arguments, in [6], the probability of success of the rainbow tradeoff was accurately calculated as

$$\mathrm{R}_{ps} = 1-\Big(\frac{2}{2+\mathrm{R}_{msc}}\Big)^{2l}. \tag{3.13}$$

3.3.3 Tradeoff coefficient

In the rainbow tradeoff, with assumptions $l=1$, $M=m$ and ignoring the cost of resolving alarms, the value of T can be roughly analysed as $T = 0+1+\cdots+(t-1) \approx \frac{t^2}{2}$. Applying the matrix stopping rule, we obtain the tradeoff curve

$$TM^2 \approx \frac{1}{2}N^2,$$

which is the different from that of the Hellman and DP tradeoff.

However, $T \approx t^2/2$ is a very rough analysis. It does not reflect the cost of resolving alarms, it is calculated as the worst case complexity and it is the specific result for the case of when $l=1$. In [6], the expected value reflecting the cost of resolving alarms was calculated and the tradeoff curve could be obtained accurately as

$$TM^2 = \mathrm{R}_{tc}N^2,$$

where

$$\begin{aligned}\mathrm{R}_{tc} =& \frac{l^3}{(2l+1)(2l+2)(2l+3)}\Bigg[\{(2l-1)+(2l+1)\,\mathrm{R}_{msc}\}\,(2+\mathrm{R}_{msc})^2 \\ &-4\Bigg\{(2l-1)+l\,(2l+3)\,\mathrm{R}_{msc}\Big(\frac{2}{2+\mathrm{R}_{msc}}\Big)^{2l}\Bigg\}\Bigg].\end{aligned} \tag{3.14}$$

Here, R_{tc} is called the tradeoff coefficient of the rainbow tradeoff.

Finally, the expected value of the number of table lookups in the online process for one rainbow table was calculated as

$$tl\frac{2+\mathrm{R}_{msc}-2\left(\frac{2}{2+\mathrm{R}_{msc}}\right)^{2l}}{(2l+1)\mathrm{R}_{msc}}.$$

4 Reasonable Tradeoff Parameters

4.1 Reasonable tradeoff parameters

As we can confirm in Section 3, tradeoff parameters m, t, l in a fixed tradeoff algorithm completely determine the tradeoff coefficient, the pre-computation coefficient and the probability of success of the tradeoff algorithm. When it is clear or of no importance which tradeoff algorithm we concerned, we admit the notation tc, pc and ps for the tradeoff coefficient, the pre-computation coefficient and the probability of success respectively. For exaple, we can use the notation tc, pc and ps instead of R_{tc}, R_{pc} and R_{ps} in the rainbow tradeoff. On the contrary, users of tradeoff algorithms want to know weather tradeoff parameters m, t, l that yield tc, pc and ps exist or not and how to find those tradeoff parameters.

Needless to say, the values of tc and pc are preferable as close to 0 as possible and the value of ps is preferable as close to 1 as possible. However, it is clear that tradeoff parameters which implement any values of tc, pc and ps do not always exist.

In [6], authors pointed out if ps is sacrificed then any value of tc could be implemented. For this reason, they were concerned with the lowest value of tc which could be implemented when ps is fixed. In this paper, when a set of parameters implement the lowest tc in the circumstances where ps is fixed, it is called an *optimal set of parameters* (or *optimal tradeoff parameters*).

However, when ps is fixed, we need to sacrifice pc to obtain the lowest tc as pointed out in [6]. And, upon user environments, a higher value of tc could be preferred to get lower value of pc rather than to get the lowest value of tc. That is, it should be noted that the notion of optimality ignores the cost of pre-computation and the optimal set of parameters found in [6] is not the parameters recommended regardless of user environments.

In this paper we will treat tc, pc and ps on an equal footing, not concerning only on obtaining the lowest tc. So, we need another terminology. When we compare two sets of parameters in terms all of tc, pc and ps, the comparative advantage could be said only in the case as follows: $tc_1 \leq tc_2, pc_1 \leq pc_2, ps_1 \geq ps_2$ are satisfied for $[tc_1, pc_1, ps_1]$ and $[tc_2, pc_2, ps_2]$ which corresponds to sets of parameters $[m_1, t_1, l_1]$ and $[m_2, t_2, l_2]$ respectively. We will say that two sets of parameters are *comparable* only if the condition above is satisfied. For a set of parameters, if there exist another set of parameters which has a comparative advantage in this sense, it will be called an *unreasonable set of parameters* (or *unreasonable tradeoff parameters*). And a set of parameters which is not unreasonable is called a *reasonable set of parameters* (or *reasonable tradeoff parameters*).

Here, it should be noted that the values of pc from two different tradeoff

algorithms can be compared directly and the values of ps are also, but the values of tc can not be compared directly. This will is discussed in detail in Section 4.8. Thus, the notion of optimality and being reasonable can be used only when we compare two set of parameters which are from the *same* tradeoff algorithms. We will discuss the method to compare the values of tc from two differnt tradeoff algorithms in Section 4.8, and then the notion of being reasonable will be extended to the comparison of two set of parameters from different tradeoff parameters.

The main interest of this paper is that: First, under what conditions on tc, pc and ps, does there exist tradeoff parameters implementing these tc, pc and ps. Second, what is the criterion for tradeoff parameters being reasonable. Researches on these subjects will be processed focusing on the rainbow tradeoff (in Section 4.3-4.6) and the results will be extended to the Hellman and the DP tradeoff (in Section 4.7).

4.2 Criterion for optimal parameters of rainbow tradeoff

In this subsection, we introduce the result of researches in [6] about the optimal tradeoff parameters in the case of the rainbow tradeoff. Remind again the purpose of the research was to get the lowest tc when ps is fixed.

If $[\mathrm{R}_{ps}, l]$ is fixed, R_{msc} is totally determined by $\mathrm{R}_{msc} = 2\{(1-\mathrm{R}_{ps})^{-1/2l} - 1\}$, which is from (3.13). And R_{tc} and R_{pc} are also determined uniquely because each could be expressed as a function of $[\mathrm{R}_{msc}, l]$ only by (3.11), (3.12), (3.13) and (3.14). Thus, tradeoff parameters m, t, l always exist by setting parameters m, t to satisfy $mt = \mathrm{R}_{msc}N$ where R_{msc} is the value determined uniquely from the fixed $[\mathrm{R}_{msc}, l]$. In brief, by fixing $[\mathrm{R}_{msc}, l]$, R_{tc} and R_{pc} are determined uniquely and tradeoff parameters m, t, l implementing these values of R_{ps}, R_{tc} and R_{pc} always exist. The graph in Figure 1 [6] are the one in R_{ps}-R_{tc} plane for fixed $l = 1, 2, 3$ (When x and y axes represent R_{ps} and R_{tc} respectively, the XY-plane will be expressed as R_{ps}-R_{tc} plane).

These graphs show that if the value of ps is low, the lowest tc could be obtained by taking $l = 1$. Thus, when the value of ps is low, a set of parameters $[m, t, l]$ corresponding to $[\mathrm{R}_{ps}, l] = [\mathrm{R}_{ps}, 1]$ is the optimal tradeoff parameters. And, as R_{ps} increases, the value of l giving the lowest R_{tc} increases.

The set of parameters implementing the lowest tc could be obtained by determining the value of l only. One can get the value of l giving the lowest R_{tc} for a fixed value of R_{ps} using Table 1 [6]. For example, when users want to set $\mathrm{R}_{ps} = 0.8$, they could get the optimal tradeoff parameters by setting $l = 2$.

For reference, although the information about R_{pc} does not appear explicitly in the graph of the Figure 1, authors of [6] pointed out that users are

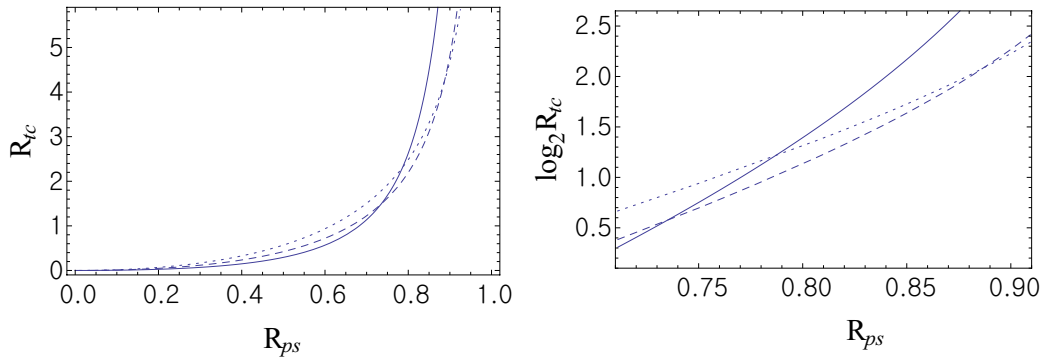

Figure 1: Graphs for fixed values of l in R_{ps}-R_{tc} plane ($l = 1$(solid), $l = 2$(dased) and $l = 3$(dotted))

l	R_{ps}	$\log_2(1-R_{ps})$	$\log_2 R_{tc}$	$R_{msc}[R_{ps}, l\uparrow]$	$R_{msc}[R_{ps}, l\uparrow]$
1	0	0	$-\infty$	None	0
2	0.734166	-1.91140	0.565848	1.87905	0.785335
3	0.886651	-3.14116	2.08082	1.44688	0.874929
4	0.946562	-4.22600	2.88968	1.25878	0.884357
5	0.973305	-5.22729	3.41666	1.14577	0.873341
6	0.986146	-6.17353	3.79818	1.06812	0.856920
7	0.992618	-7.08171	4.09387	1.01079	0.839893
8	0.995992	-7.96295	4.33425	0.966542	0.823891
9	0.997795	-8.82486	4.03663	0.931326	0.809415
10	0.998775	-9.67274	4.71157	0.902658	0.796529
11	0.999314	-10.5104	4.86585	0.878902	0.785129
12	0.999614	-11.3404	5.00406	0.858929	0.775059
13	0.999782	-12.1649	5.12941	0.841927	0.766150
14	0.999877	-12.9850	5.24421	0.827299	0.758246
15	0.999930	-13.8020	5.35019	0.814594	0.751208
	0.999960	-14.6163	5.44869	0.803466	0.744914

Table 1: Range of R_{ps} for which each table count l is optimal

sometimes recommended to use bigger value of l to get lower value of R_{pc} rather than to use the value of l to get the optimal tradeoff parameters.

4.3 Criterion for unreasonable parameters of rainbow tradeoff: where tradeoff coefficient is fixed

From Section 4.3 to 4.5, we will study the criterion for removing unreasonable tradeoff parameters in circumstances where one of R_{tc}, R_{pc} and R_{ps} is fixed. It should be noted that even if some unreasonable tradeoff parameters are removed by the criterion in circumstances where one of R_{tc}, R_{pc} and R_{ps} is fixed, remaining tradeoff parameters could be still unreasonable tradeoff parameters. In Section 4.6, we will discuss how to remove *all* the unreasonable tradeoff parameters and compare the results with the ones in Section 4.3–4.5.

In this subsection, we analyse the (R_{pc}, R_{ps}) which could be implemented in circumstances where R_{tc} is fixed and suggest the criterion for removing *some* unreasonable tradeoff parameters.

First, let us show that if [R_{tc}, l] is fixed to any value in their own range, (R_{pc} ,R_{ps}) is uniquely determined and tradeoff parameters implementing these R_{tc}, R_{pc} and R_{ps} exist. From (3.14), for the fixed $[\mathrm{R}_{tc}, l]$, an equation on R_{msc} of order $2l+3$ is obtained as follows.

$$l^3[\{(2l-1)+(2l+1)\mathrm{R}_{msc}\}(2+\mathrm{R}_{msc})^{2l+2}-\{(2l-1)+l(2l+3)\mathrm{R}_{msc}\}2^{2l+2}] \\ -\mathrm{R}_{tc}(2l+1)(2l+2)(2l+3)(2+\mathrm{R}_{msc})^{2l}=0$$

Lemma 4.1. *For fixed $l \in \mathbb{N}$ and $\mathrm{R}_{tc} \in \mathbb{R}^+$, define $f(x)$ as below.*

$$l^3[\{(2l-1)+(2l+1)x\}(2+x)^{2l+2}-\{(2l-1)+l(2l+3)x\}2^{2l+2}] \\ -\mathrm{R}_{tc}(2l+1)(2l+2)(2l+3)(2+x)^{2l}=0$$

Then, $f(x)=0$, the equation on x of order $2l+3$, has unique solution in positive real numbers.

Proof. It suffices to show that $(i) f^{2l+3}(0)>0$, $(ii) f(0)<0$ and $(iii) f^{k+1}(0)<0$ implies $f^k(0)<0$ (for $0 \le k \le 2l+2$).

From $f^{2l+3}(0)=(2l+3)!l^3(2l+1)$ and $f(0)=-\mathrm{R}_{tc}2^{2l}(2l+1)(2l+2)(2l+3)$, (i) and (ii) are easily checked. (iii) could be shown as follows.

Case 1. $0 \le k \le 1$ (iii) is true because

$$f(0)=-\mathrm{R}_{tc}2^{2l}(2l+1)(2l+2)(2l+3)<0, \\ f^1(0)=-\mathrm{R}_{tc}2^{2l-1}(2l)(2l+1)(2l+2)(2l+3)<0.$$

Case 2. $2l \leq k \leq 2l+2$ (iii) is true because

$$f^{2l+1}(0) = (2l+1)!\{2l^3(2l-1)(2l+2) + 2l^3(2l+1)^2(2l+2)\} > 0,$$
$$f^{2l+2}(0) = (2l+2)!\{l^3(2l-1) + 2l^3(2l+1)(2l+2)\} > 0,$$
$$f^{2l+3}(0) = (2l+3)!2l^3(2l+1) > 0$$

Case 3. $2 \leq k \leq 2l-1$

For $2 \leq k \leq 2l$, the following is true.

$$\begin{aligned} f^k(0) =& 2^{2l-k}(2l+2)(2l+1)\cdots(2l+4-k) \times [4l^3(2l-1)(2l+3-k) \\ &+ 8l^3(2l+1)k - \mathrm{R}_{tc}(2l+3)(2l+3-k)(2l+2-k)(2l+1-k)] \end{aligned}$$

Therefore, the sign of $f^k(0)$ is same with the sign of

$$\begin{aligned} f^k(0) :=& 4l^3(2l-1)(2l+3-k) + 8l^3(2l+1)k \\ &- \mathrm{R}_{tc}(2l+3)(2l+3-k)(2l+2-k)(2l+1-k) \end{aligned}$$

So, it is enough to show that $f(k+1) < 0$ implies $f(k) < 0$. Let us regard $f(k)$ as the function defined on real numbers, then from

$$\begin{aligned} \frac{d}{dk}f(k) =& 4l^3(2l+3) + \mathrm{R}_{tc}(2l+3)(2l+2-k)(2l+1-k) + \mathrm{R}_{tc}(2l+3) \\ & (2l+3-k)(2l+1-k) + \mathrm{R}_{tc}(2l+3)(2l+3-k)(2l+2-k) > 0, \end{aligned}$$

$f(k)$ is strictly increasing function and the proof is completed.

□

From Lemma 4.1, it follows that R_{msc} is uniquely determined when $[\mathrm{R}_{tc}, l]$ is fixed. And then, R_{pc} and R_{ps} are uniquely determined because those can be expressed as the functions of variables $[\mathrm{R}_{msc}, l]$ only from (3.11), (3.12) and (3.13). In addition, tradeoff parameters m, t, l which implement the fixed $[\mathrm{R}_{tc}, l]$ always exist by setting m and t to satisfy the relation $\mathrm{R}_{msc} = mt/N$.

The graphs in Figure2 are the ones in R_{pc}-R_{ps} plane for several fixed values of R_{tc}.

See Figure3. Each point of the graph corresponds to a fixed value of l. For arbitrary point, points on the right and below mean higher value of R_{pc} and lower value of R_{ps}. So, the tradeoff parameters corresponding to these points are recommended not to be used. For this reason, we should remove all of these points.

Under circumstances where R_{tc} is fixed, we could search out unreasonable tradeoff parameters by determining the value of l only. See (c) in Figure2. If the slope of two points corresponding to $l = k+1$ and $l = k$ has plus

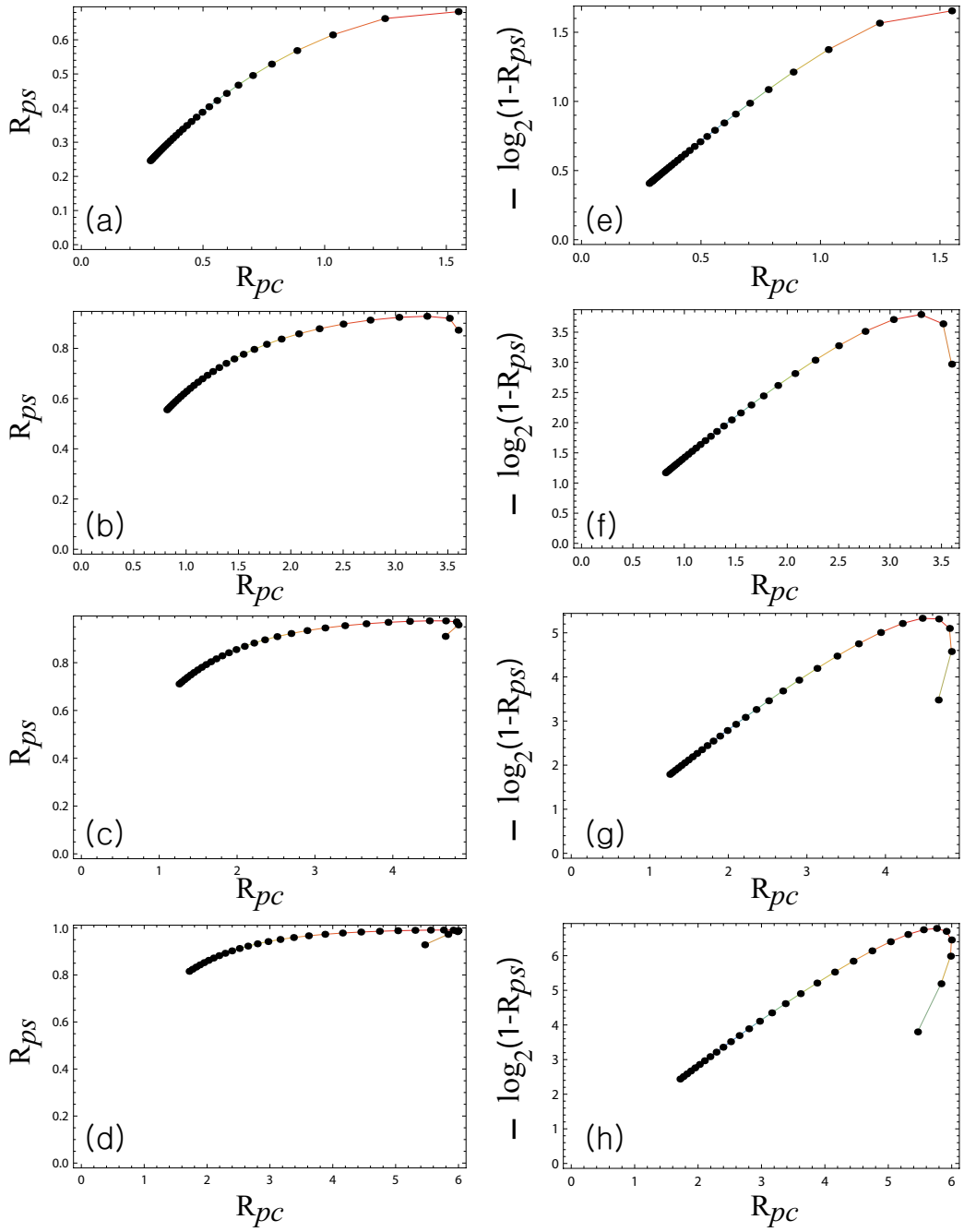

Figure 2: Graphs in R_{pc}-R_{ps} plane for fixed values of R_{tc} ((a): $R_{tc} = 1$, (b): $R_{tc} = 6$, (c): $R_{tc} = 11$, (d): $R_{tc} = 16$). Each points in graph is for $l = 1, 2, \cdots, 30$. Each graphs in right is magnified view of left graph in logarithmic scale.

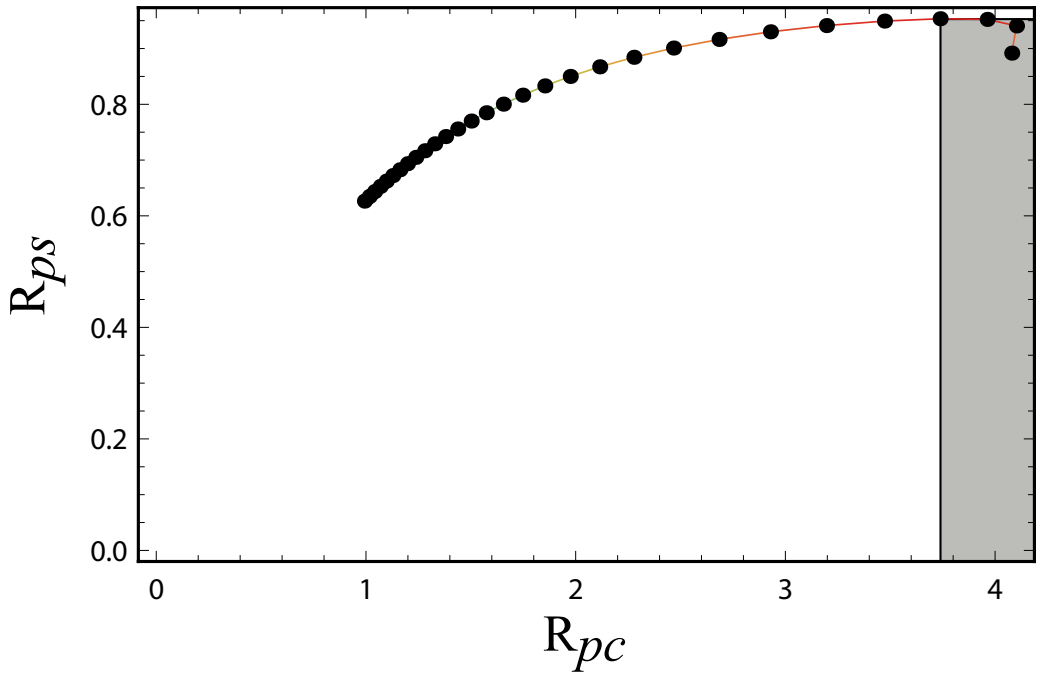

Figure 3: Graph in R_{pc}-R_{ps} plane for fixed values of $R_{tc} = 8$. Each points in graph is for $l = 1, 2, \cdots, 30$.

sign and the slope of two points corresponding to $l = k$ and $l = k - 1$ has minus sign, then we can conclude that tradeoff parameters corresponding to $l \leq k - 1$ are unreasonable. Thus, by finding out the value of R_{tc} where the slope of two points corresponding to $l = k + 1$ and $l = k$ becomes zero for fixed value of k, we can obtain the value of R_{tc} at the moment when the range of l for unreasonable tradeoff parameters is changed. The results are in Table 2. For example, $l \geq 4$ is recommended for $R_{tc} = 10$. That is, $l \leq 3$ means unreasonable tradeoff parameters.

Note that two sets of parameters for different values of R_{tc} could be comparable. What we remove might not be *all* the unreasonable tradeoff parameters.

4.4 Criterion for unreasonable parameters of rainbow tradeoff: where pre-computation coefficient is fixed

In this subsection, we analyse the (R_{tc}, R_{ps}) which could be implemented in circumstances where R_{pc} is fixed and suggest the criterion for removing *some* unreasonable tradeoff parameters.

First, let us show that if $[R_{pc}, l]$ is fixed to any value in their own range, (R_{tc}, R_{ps}) is uniquely determined and tradeoff parameters implementing these

l	R_{tc}	R_{ps}	R_{pc}	R_{msc}
1-	0	0	0	0
2-	1.48026	0.734167	1.57067	0.785336
3-	4.23048	0.886651	2.62479	0.874930
4-	7.41105	0.946562	3.53743	0.884357
5-	10.6787	0.973305	4.36669	0.873338
6-	13.9112	0.986146	5.14151	0.856918
7-	17.0756	0.992618	5.87924	0.839891
8-	20.1715	0.995992	6.59111	0.823889
9-	23.2093	0.997795	7.28472	0.809414
10-	26.2013	0.998775	7.96528	0.796528
11-	29.1586	0.999314	8.63641	0.785129
12-	32.0902	0.999614	9.30070	0.775058
13-	35.0030	0.999782	9.95994	0.766150
14-	37.9022	0.999877	10.6155	0.758246
15-	40.7914	0.999930	11.2681	0.751207
	43.6735	0.999960	11.9186	0.744914

Table 2: Range of R_{tc} for which each ranges of table count l denotes remaining tradeoff parameters after removing unreasonable tradeoff parameters by method in Section 4.3

R_{pc}, R_{tc} and R_{ps} exist. From $R_{msc} = R_{pc}/l$, it follows that R_{msc} is uniquely determined when $[R_{pc}, l]$ is fixed. Thus, R_{tc} and R_{ps} are uniquely determined because those can be expressed as the functions of variables $[R_{msc}, l]$ only by (3.13) and (3.14). In addition, tradeoff parameters m, t, l which implement the fixed $[R_{pc}, l]$ always exist by setting m and t to satisfy the relation $R_{msc} = mt/N$.

The graphs in Figure4 are the ones in R_{tc}-R_{ps} plane for several fixed values of R_{pc}.

See Figure5. Each point of the graph corresponds to a fixed value of l. For arbitrary point, points on the right or below mean higher value of R_{tc} and lower value of R_{ps}. So, the tradeoff parameters corresponding to these point is recommended not to use. For this reason, we should remove all of these points.

Under circumstances where R_{pc} is fixed, we could search out unreasonable tradeoff parameters by determining the value of l only. See (b) in Figure4. If the slope of two points corresponding to $l = k + 1$ and $l = k$ has plus sign and the slope of two points corresponding to $l = k$ and $l = k - 1$ has minus sign, then we can conclude that tradeoff parameters corresponding to $l \leq k - 1$ are unreasonable. Thus, by finding out the value of R_{pc} where the slope of two points corresponding to $l = k+1$ and $l = k$ becomes ∞ for fixed value of k, we can obtain the value of R_{pc} at the moment when the range of l for unreasonable tradeoff parameters is changed. The results are in Table 3. For example, $l \geq 6$ is recommended for $R_{pc} = 8$. That is, $l \leq 5$ means unreasonable tradeoff parameters.

Note that two sets of parameters for different values of R_{pc} could be comparable. What we remove might not be *all* the unreasonable tradeoff parameters.

4.5 Criterion for unreasonable parameters of rainbow tradeoff: where probability of success is fixed

In this subsection, we analyse the (R_{tc}, R_{pc}) which could be implemented in circumstances where R_{ps} is fixed and suggest the criterion for removing *some* unreasonable tradeoff parameters.

First, let us show that if $[R_{ps}, l]$ is fixed to any value in their own range, (R_{tc}, R_{pc}) is uniquely determined and tradeoff parameters implementing these R_{tc}, R_{pc} and R_{ps} exist. From (3.13), we get $R_{msc} = 2\{(1 - R_{ps})^{-1/2l}\}$. And $R_{msc} = 2\{(1 - x)^{-1/2l}\}$ is a strictly increasing function in the range of $0 < x < 1$. So, R_{msc} is uniquely determined from fixed $[R_{ps}, l]$. As a result, R_{tc} and R_{pc} are uniquely determined because those can be expressed as the functions of variables $[R_{msc}, l]$ only by (3.11), (3.12) and (3.14). In addition, tradeoff parameters m, t, l which implement the fixed $[R_{ps}, l]$ are always exist

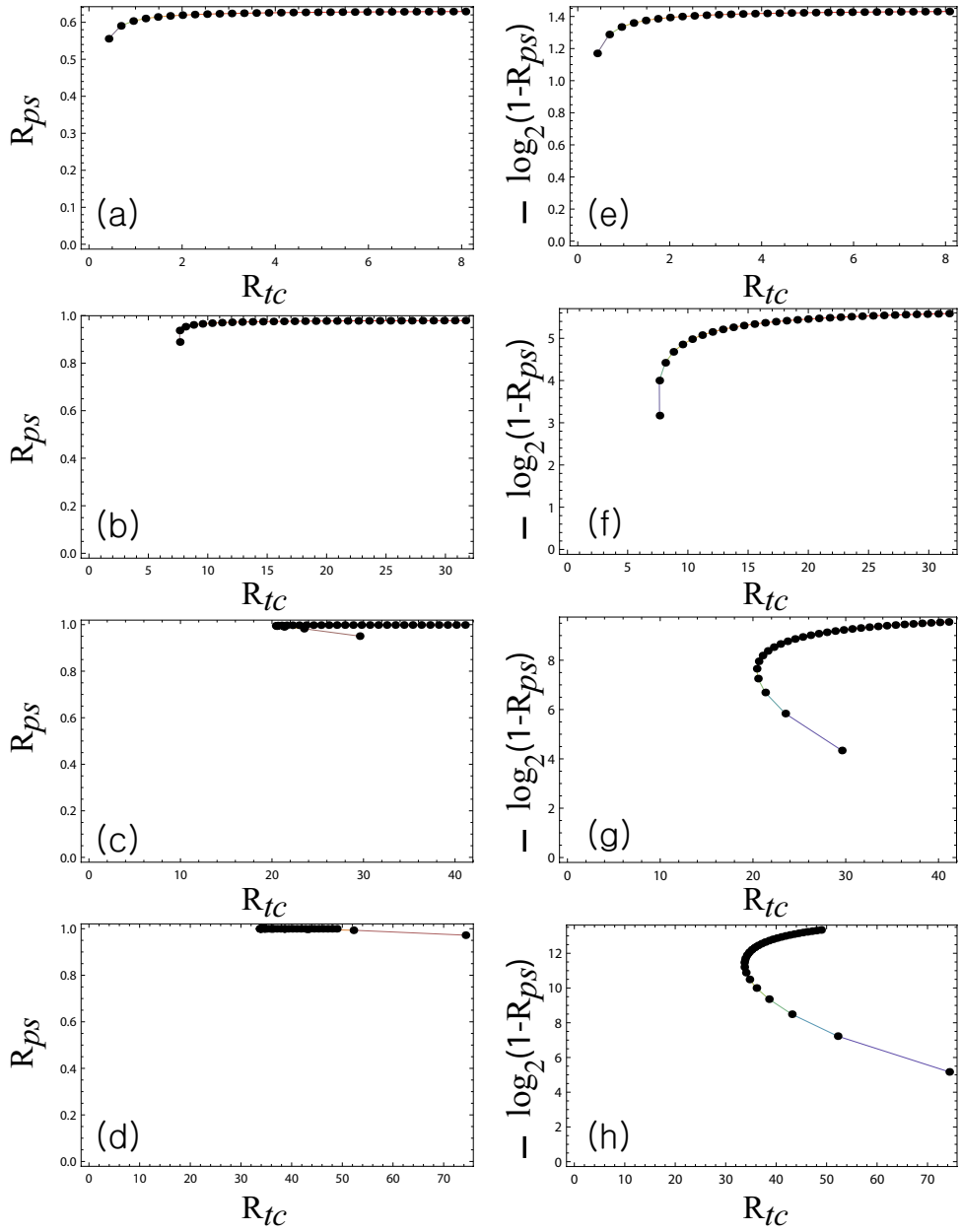

Figure 4: Graphs in R_{tc}-R_{ps} plane for fixed values of R_{pc} ((a): $R_{pc} = 1$, (b): $R_{pc} = 4$, (c): $R_{pc} = 7$, (d): $R_{pc} = 10$). Each points in graph is for $l = 1, 2, \cdots, 30$. Each graphs in right is magnified view of left graph in logarithmic scale.

l	R_{pc}	R_{ps}	R_{tc}	R_{msc}
1-	0	0	0	0
2-	3.98071	0.936894	7.55959	1.99036
3-	4.98607	0.973463	11.6666	1.66202
4-	5.88160	0.987832	15.5279	1.47047
5-	6.72638	0.994166	19.2359	1.34528
6-	7.54470	0.997130	22.8463	1.25745
7-	8.34858	0.998567	26.3953	1.19265
8-	9.14439	0.999277	29.9061	1.14305
9-	9.93563	0.999634	33.3937	1.10396
10-	10.7242	0.999813	36.8670	1.07242
11-	11.5112	0.999905	40.3318	1.04647
12-	12.2971	0.999951	43.7911	1.02476
13-	13.0823	0.999975	47.2471	1.00633
14-	13.8669	0.999987	50.7006	0.990493
15-	14.6511	0.999993	54.1526	0.976740
	15.4349	0.999997	57.6033	0.964681

Table 3: Range of R_{pc} for which each ranges of table count l denotes remaining tradeoff parameters after removing unreasonable tradeoff parameters by method in Section 4.4

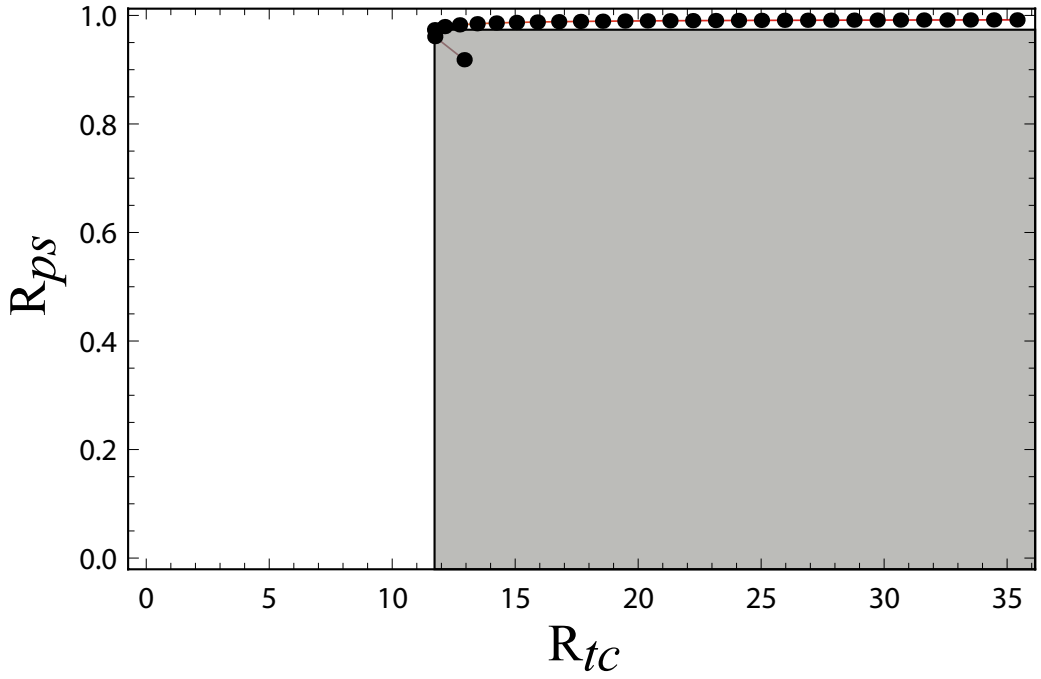

Figure 5: Graph in R_{tc}-R_{ps} plane for fixed values of $R_{pc} = 5$. Each points in graph is for $l = 1, 2, \cdots, 30$.

by setting m and t to satisfy the relation $R_{msc} = mt/N$.

The graphs in Figure 6 are the ones in R_{tc}-R_{pc} plane for several fixed values of R_{ps}.

See Figure 7. Each point of the graph corresponds to a fixed value of l. For arbitrary point, points on the right and above mean higher value of R_{tc} and higher value of R_{pc}. So, the tradeoff parameters corresponding to these points are recommended not to use. For this reason, we should remove all of these points.

Under circumstances where R_{ps} is fixed, we could search out unreasonable tradeoff parameters by determining the value of l only. See (d) in Figure 6. If the slope of two points corresponding to $l = k + 1$ and $l = k$ has minus sign and the slope of two points corresponding to $l = k$ and $l = k - 1$ has plus sign, then we can conclude that tradeoff parameters corresponding to $l \leq k - 1$ are unreasonable. Thus, by finding out the value of R_{ps} where the slope of two points corresponding to $l = k+1$ and $l = k$ becomes ∞ for fixed value of k, we can obtain the value of R_{ps} at the moment when the range of l for unreasonable tradeoff parameters is changed. The results are in Table 4. For example, $l \geq 4$ is recommended for $R_{ps} = 0.95$. That is, $l \leq 3$ means unreasonable tradeoff parameters.

Note that two sets of parameters for different values of R_{ps} could be

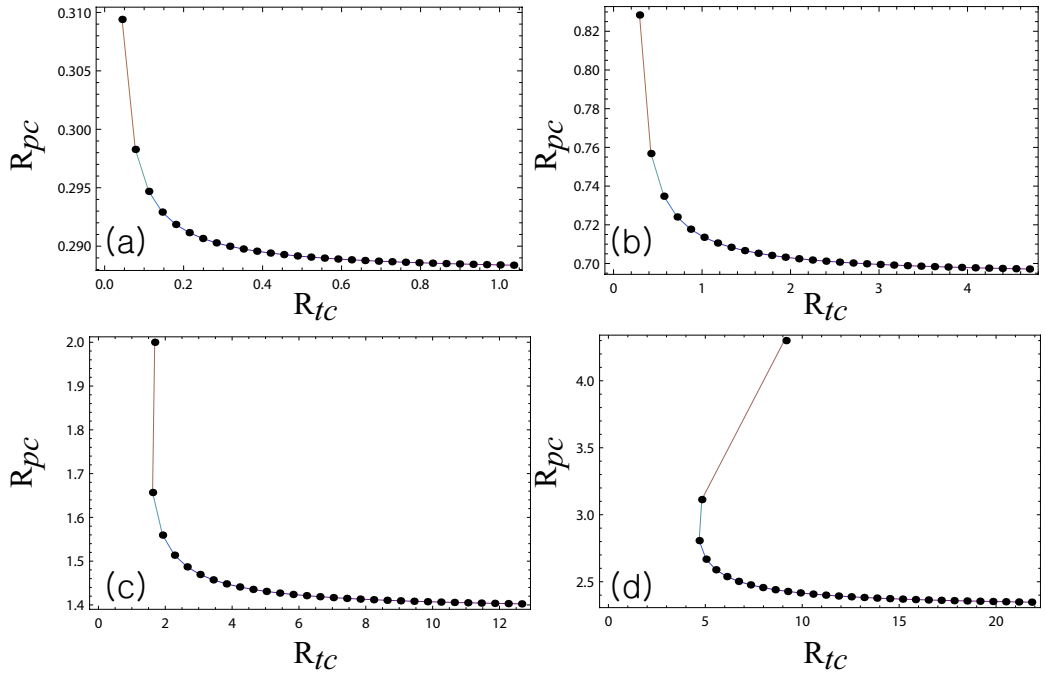

Figure 6: Graphs in R_{tc}-R_{pc} plane for fixed values of R_{ps} ((a): $R_{ps} = 0.25$, (b): $R_{ps} = 0.5$, (c): $R_{ps} = 0.75$, (d): $R_{pc} = 0.9$). Each points in graph is for $l = 1, 2, \cdots, 30$.

l	R_{ps}	R_{tc}	R_{pc}	R_{msc}
1-	0	0	0	0
2-	0.734166	1.48025	1.57067	0.785335
3-	0.886651	4.23047	2.62479	0.874928
4-	0.946562	7.41103	3.53742	0.884355
5-	0.973305	10.6786	4.36670	0.873340
6-	0.986146	13.9113	5.14155	0.856924
7-	0.992618	17.0759	5.87931	0.839902
8-	0.995992	20.1714	6.59108	0.823885
9-	0.997795	23.2098	7.28488	0.809431
10-	0.998775	26.2022	7.96554	0.796554
11-	0.999314	29.1557	8.63558	0.785053
12-	0.999614	32.0857	9.29943	0.774952
13-	0.999782	34.9980	9.95853	0.766041
14-	0.999877	37.9159	10.6193	0.758521
15-	0.999930	40.7926	11.2684	0.751229
	0.999960	43.6504	11.9122	0.744515

Table 4: Range of R_{ps} for which each ranges of table count l denotes remaining tradeoff parameters after removing unreasonable tradeoff parameters by method in Section 4.5

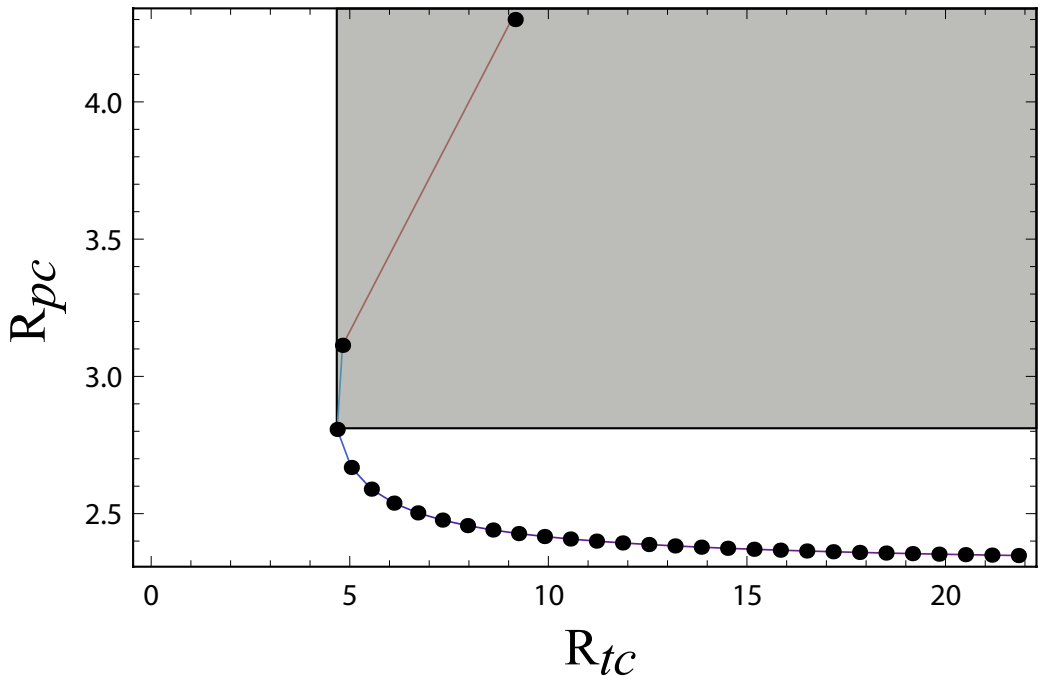

Figure 7: Graph in R_{tc}-R_{pc} plane for fixed values of $R_{ps} = 0.9$. Each points in graph is for $l = 1, 2, \cdots, 30$.

comparable. What we remove might not be *all* the unreasonable tradeoff parameters.

4.6 Criterion for reasonable parameters of rainbow tradeoff

To sum up, in Section 4.3–4.5, we have shown that if we fix one of R_{tc}, R_{pc} and R_{ps} and fix the value of l, the remaining two values are determined uniquely. And the tradeoff parameters implementing these values are always exist. We have also shown it can be judged by the value of l weather tradeoff parameters are unreasonable or not in circumstances where one of R_{tc}, R_{pc} and R_{ps} is fixed. And we obtained tables as the criterion for removing unreasonable tradeoff parameters in circumstances where one of R_{tc}, R_{pc} and R_{ps} is fixed. However, as it noted at the end of Section 4.3–4.5, we do not obtain the criterion for determining *all* the unreasonable tradeoff parameters. In this subsection, we discuss how to remove all the unreasonable tradeoff parameters and compare this result with the ones in Section 4.3–4.5.

The graphs in Figure 8 are the ones in R_{tc}-R_{pc}-R_{ps} space for fixed l. For convenience, x, y, z axes will always denote R_{tc}, R_{pc}, R_{ps} respectively.

First, let us analyse the shape of the graphs.

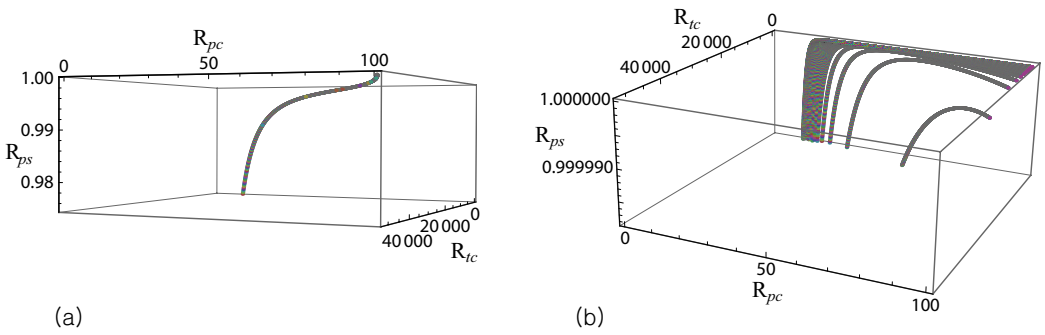

Figure 8: Graphs in R_{tc}-R_{pc}-R_{ps} space for fixed values of l ((a): $l = 1$, (b): $l = 1, 2, \cdots, 50$)

Lemma 4.2. *A graph in* R_{tc}-R_{pc}-R_{ps} *space for a fixed* l *starts at* $(0, 0, 0)$ *and is drawn in a continuous curve. As* R_{pc} *increases,* R_{tc} *and* R_{ps} *also increases.*

Proof. From (3.11), (3.12), (3.13) and (3.14), we can conclude that $\mathrm{R}_{pc} = 0$ implies $\mathrm{R}_{msc} = 0$ and so $\mathrm{R}_{ps} = 0$ and $\mathrm{R}_{tc} = 0$. Thus, the graph for a fixed l starts at $(0, 0, 0)$.

From $\mathrm{R}_{ps} = 1 - \left(\frac{2}{2+\mathrm{R}_{pc}/l}\right)^{2l}$, it is implied that R_{ps} is a continuous and strictly increasing function of R_{pc}. So, if we project the graph onto YZ-plane, it draws a continuous curve moving to the plus direction of z axis as it moves to the plus direction of y axis.

By (3.14) and $\mathrm{R}_{msc} = \mathrm{R}_{pc}/l$, R_{tc} is a continuous function of R_{pc}. And remind that R_{pc} is uniquely determined when $[\mathrm{R}_{tc}, l]$ is fixed (See Lemma 4.1). Thus, R_{tc} is a continuous and strictly increasing function of R_{pc}. □

For reference, Proposition 4.3 below could be obtained as a corollary of Lemma 4.2. This result was obtained already in each Section 4.3–4.5, but now we can see each results in the united point of view.

Proposition 4.3. *When fixing* l*, if one of* R_{tc}*,* R_{pc} *and* R_{ps} *is fixed in its own range, the other two are determined uniquely. And tradeoff parameters implementing these* R_{tc}*,* R_{pc} *and* R_{ps} *exist.*

Proof. The first part of this proposition is the direct result of Lemma 4.2.

By the determined value of R_{pc}, R_{msc} is uniquely determined by $\mathrm{R}_{msc} = \mathrm{R}_{pc}/l$. As a result, we see the existence of tradeoff parameters implementing these R_{tc}, R_{pc} and R_{ps} by setting parameters m, t to satisfy $\mathrm{R}_{msc} = mt/N$. □

Now, we discuss how to remove all the unreasonable tradeoff parameters using graphs in R_{tc}-R_{pc}-R_{ps} space.

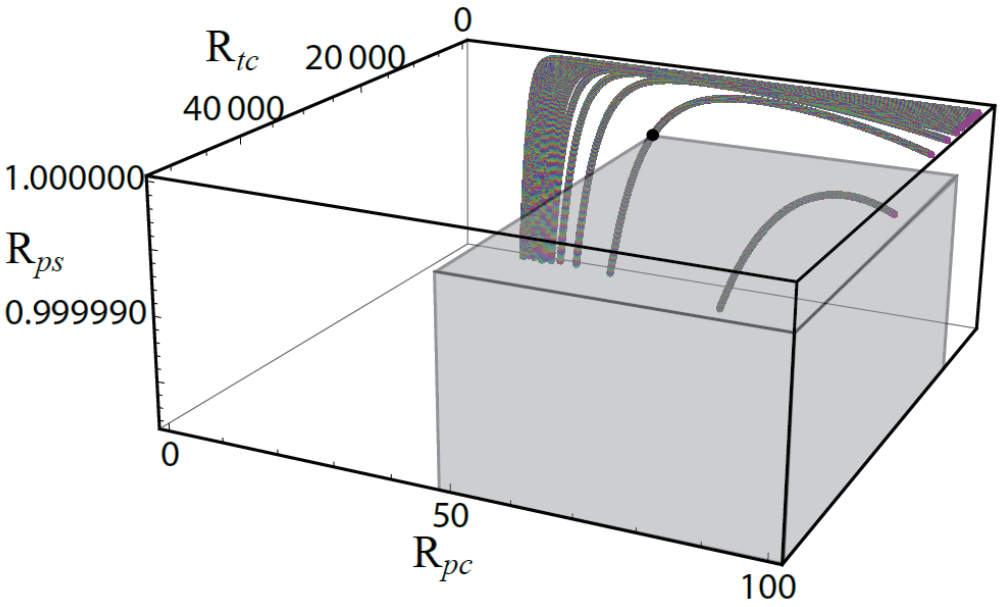

Figure 9: Graphs in R_{tc}-R_{pc}-R_{ps} space for fixed values of $l = 1, 2, \cdots, 50$

See Figure9. Each curve of graphs corresponds to a fixed value of l. For arbitrary point, points on the plus direction of x axis, the plus direction of y axis and the minus direction of z axis mean higher value of R_{tc}, higher value of R_{pc} and lower value of R_{ps} each. So, the tradeoff parameters corresponding to these points are recommended not to be used. For this reason, we should remove all of these points.

Note that, unlike the discussions in Section 4.3–4.5, by removing unreasonable tradeoff parameters using this method, we can remove *all* the unreasonable tradeoff parameters because this method considers all of R_{tc}, R_{pc} and R_{ps}. Thus, the remaining points must be *reasonable* tradeoff parameters. For the convenience, we call this method which removes unreasonable tradeoff parameters the R criterion.

Reinterpreting the discussions of Section 4.3–4.5, each graph of Figure 2, Figure 4 and Figure 6 is the graph in the plane perpendicular x, y and z axis respectively. For convenience, we call each criterion for removing unreasonable tradeoff parameters in Section 4.3–4.5 the R_{tc}, R_{pc} and R_{ps} criterion respectively.

Proposition 4.4. *To judge a set of parameters weather it is unreasonable or not by the R criterion is same with to judge it by the R_{ps} criterion.*

Proof. Let us show that if the point (R_{tc}, R_{pc}, R_{ps}; l)=(tc_1, pc_1, ps_1; l_1) in R_{tc}-R_{pc}-R_{ps} space is removed by the R criterion, then it is removed by the R_{ps} criterion and let us show the converse.

Suppose that based on the criterion, the point (R_{tc}, R_{pc}, R_{ps}; l)=(tc_1, pc_1, ps_1; l_1) is removed by the point (R_{tc}, R_{pc}, R_{ps}; l)=(tc_2, pc_2, ps_2; l_2). Then, $tc_2 \leq tc_1$, $pc_2 \leq pc_1$, $ps_2 \geq ps_1$. Let ϵ=$ps_2 - ps_1$. Denote the points corresponding to (R_{ps}; l)=($ps_2 - \epsilon$; l_2)=(ps_1; l_2) as (R_{tc}, R_{pc}, R_{ps}; l)=(tc'_2, pc'_2, ps_1; l_2). Then, by Lemma 4.2, $tc'_2 \leq tc_2$, $pc'_2 \leq pc_2$. Thus, based on the R_{ps} criterion, (R_{ps}; l)=(ps_1; l_1) is removed by (R_{ps}; l)=(ps_1; l_2).

For the converse, suppose that based on the R_{ps} criterion, (R_{ps}; l)=(ps; l_1) is removed by (R_{ps}; l)=(ps; l_2). And denote each point corresponding to (R_{ps}; l)=(ps; l_1) and (R_{ps}; l)=(ps; l_2) as (R_{tc}, R_{pc}, R_{ps}; l)=(tc_1, pc_1, ps; l_1) and (R_{tc}, R_{pc}, R_{ps}; l)=(tc_2, pc_2, ps; l_2) respectively. Then, $tc_2 \leq tc_1$, $pc_2 \leq pc_1$ because of the rule of the R_{ps} criterion. Thus based on the R criterion, (R_{ps}; l)=(ps_1; l_2) is removed. □

By Proposition 4.4, we see that the remaining tradeoff parameters after removing unreasonable tradeoff parameters by the R_{ps} criterion are reasonable tradeoff parameters. Therefore, Table 4 can be used to search out all the reasonable tradeoff parameters.

Proposition 4.5. *To judge a set of parameters weather it is unreasonable or not by the* R_{tc} *criterion together with the* R_{pc} *criterion is same with to judge it by the* R_{ps} *criterion.*

Proof. Similar discussion with the proof of Proposition 4.4. □

By Proposition 4.5, after removing unreasonable tradeoff parameters using the R_{tc} criterion together with the R_{pc} criterion, the remaining tradeoff parameters are reasonable tradeoff parameters. We could confirm this with the tables in Section 4.3–4.5. That is, the set of remaining parameters based on Table 2 together with Table 3 should be same with the set of remaining parameters based on Table 4.

First, let us compare Table 2 with Table 3 in terms of the value of R_{ps}. We can confirm that the set of remaining parameters based on Table 2 together with Table 3 is same with the set of remaining parameters based on Table 2 only. For example, $[R_{ps}, l] = [0.95, 2]$ is not removed based on Table 3, but is removed based on Table 2. In addition, comparing Table 2 with Table 4 in terms of the value of R_{ps}, we can confirm that Table 2 is same with Table 4. In summary, the set of remaining parameters based on Table 2 together with Table 3 is same with the set of remaining parameters based on Table 2 only and this is same with the set of remaining parameters based on Table 4.

We have confirmed Proposition 4.4 and Proposition 4.5 agree with the results of Section 4.3–4.5. But, it is an unexpected result that the set of

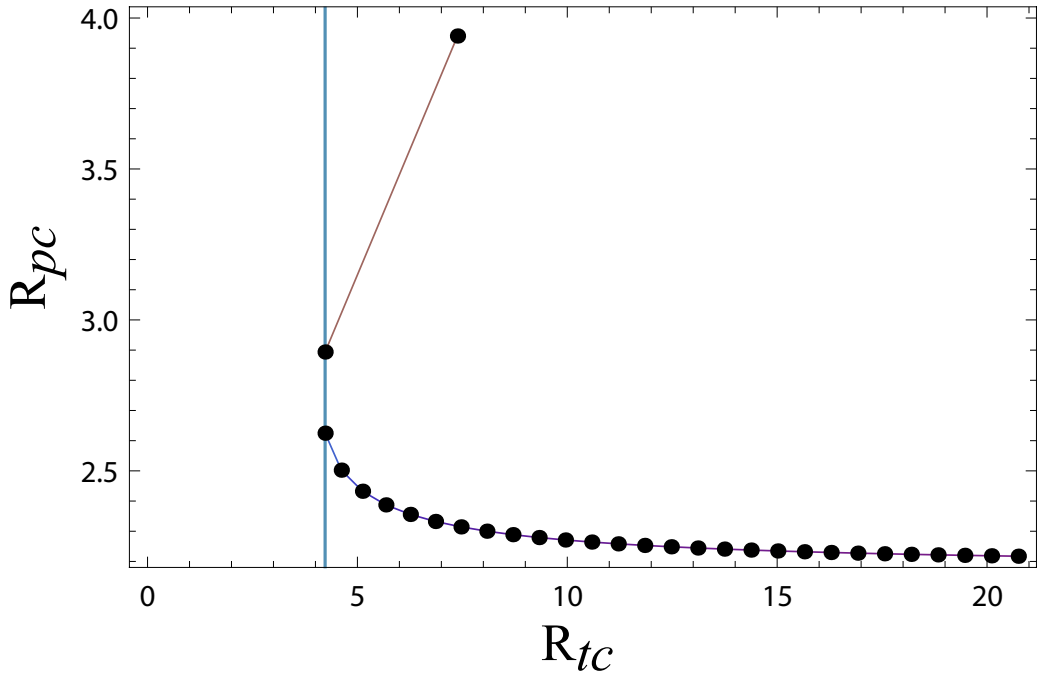

Figure 10: Graph in R_{tc}-R_{pc} plane for $R_{ps} = 0.886651$. Slope of two points corresponding to $l = 2$ and $l = 3$ is ∞.

remaining parameters based on Table 2 and together with Table 3 is same with the set of remaining parameters based on Table 2 only. This cannot be derived by using only Lemma 4.2, Proposition 4.4 and Proposition 4.5. To explain this, another discussion about the shape of graphs in R_{tc}-R_{pc}-R_{ps} space is needed. Let us take a close look.

As we see in Section 4.5, the shape of a graph in R_{tc}-R_{pc} plane which is a plane perpendicular to z axis is as Figure 10. As we see in Section 4.3, the shape of a graph in R_{pc}-R_{ps} plane which is a plane perpendicular to x axis is as Figure 11. Note that the shape of the graph in Figure 11 could be predicted by applying Lemma 4.2 to the shape of the graph in Figure 11.

When we obtained Table 2 and Table 4, we calculated the values of R_{tc} and R_{ps} for a fixed k where the slope of two points corresponding to $l = k+1$ and $l = k$ is zero and ∞ respectively. Imagine two curves in R_{tc}-R_{pc}-R_{pc} space for $l = k$ and $l = k + 1$ each. What we calculated in Section 4.3 and 4.5 are the values of R_{tc} and R_{ps} where (R_{tc}, R_{ps}) corresponding to $l = k + 1$ and $l = k$ respectively are same with each other. Thus the result of the R_{tc} criterion should be same with the R_{ps} criterion.

On contrary, if the shape of a graph in R_{tc}-R_{pc} plane which is a plane perpendicular to z axis, is as Figure12, the result of the R_{ps} criterion would be the same with that of the R_{pc} criterion.

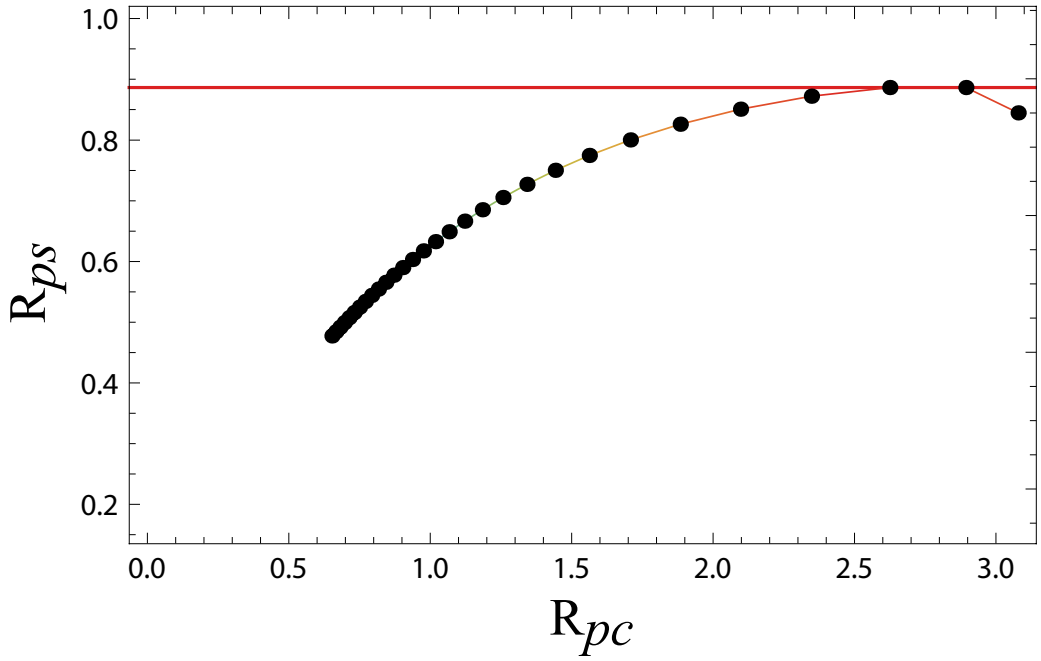

Figure 11: Graph in R_{pc}-R_{ps} plane for $R_{tc} = 0.423047$. Slope of two points corresponding to $l = 2$ and $l = 3$ is zero.

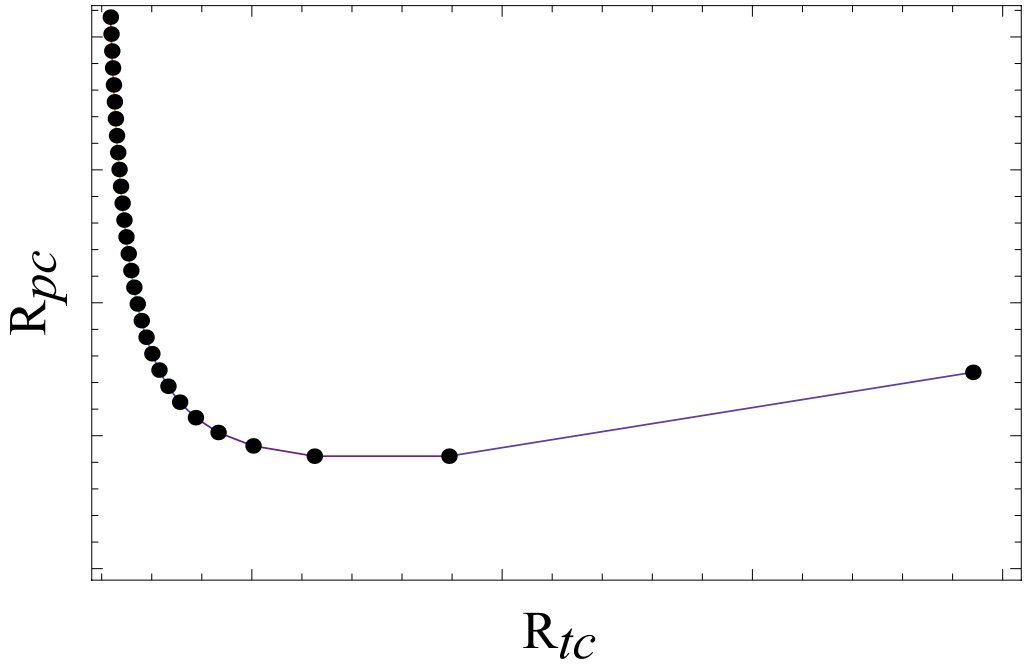

Figure 12: Symmetric image of Figure 10

Thus, from the shape of graphs in R_{tc}-R_{pc} plane which is a plane perpendicular to z axis, we can get the remark below.

Remark 4.6. To judge a set of parameters weather it is unreasonable or not by the R_{tc} criterion is same with to judge it by the R_{ps} criterion.

Let us summarize arguments from the beginning of this subsection. First, in R_{tc}-R_{pc}-R_{ps} space, imagine one curve corresponding to a fixed l. The criterion for tradeoff parameters being reasonable for this fixed value l is expressed as $0 \leq R_{ps} \leq ps(l)$ (of course, it can be expressed as $0 \leq R_{tc} \leq tc(l)$ or $0 \leq R_{pc} \leq pc(l)$). Here, $ps(l)$ becomes a strictly increasing function of l. Second, in R_{tc}-R_{pc}-R_{ps} space, imagine two curves corresponding to fixed values $l = k$ and $l = k+1$ respectively. Let us focus on two points in R_{tc}-R_{pc}-R_{ps} space; one is the *ending* point $[R_{tc}, R_{pc}, R_{ps}; l] = [tc(k), pc(k), ps(k); k]$ of the curve for $l = k$ and the other is the middle point $[R_{ps}; l] = [ps(k); k+1]$ of the curve for $l = k+1$.

The values of (R_{tc}, R_{ps}) corresponding to these two points are coincide initially when one moves starting from the origin according to two curves. So, if we project two curves into the XZ-plane, two curves meet initially at the moment. And there, the value of R_{pc} of the curve for $l = k+1$ is smaller than the one of the curve for $l = k$.

Now, we can discuss the relation of the criterion for the optimality in Section 4.2 and the criterion for tradeoff parameters being reasonble. In fact, Figure 1 is the projected images of the curves for $l = 1, 2, 3$ in R_{tc}-R_{pc}-R_{ps} space into XZ-plane.

When R_{ps} is fixed, $R_{pc} = R_{msc} l = 2l\{(1 - R_{ps})^{-1/2l} - 1\}$ is a decreasing function of l. With this fact, by the arguments in the previous paragraph, the shape of the graph in Figure 1 could be predicted and we can conclude that the end point of a curve for a fixed l in R_{tc}-R_{pc}-R_{ps} space corresponds to the optimal set of parameters. And this is confirmed by comparing Table 4 with Table1 in terms of the value of R_{ps}. We write this result as the remark below.

Remark 4.7. For a fixed value of l, the criterion for tradeoff parameters being reasonable is expressed as $0 \leq R_{ps} < ps(l)$, where $ps(l)$ is a increasing function of l. And, the criterion for the optimality for the fixed value of l is $ps(l-1) \leq R_{ps} \leq ps(l)$.

4.7 Criterion for reasonable parameters of Hellman and DP tradeoff

In this subsection, we discuss the criterion for tradeoff parameters being reasonable in the case of the Hellman and the DP tradeoff.

Lemma 4.8. *A graph in* H_{tc}-H_{pc}-H_{ps} *space for a fixed* H_{msc} *starts at* $(0,0,0)$ *and is drawn in a continuous curve. As* H_{pc} *increases,* H_{ps} *and* H_{tc} *also increases.*

Proof. For the convenience, x, y and z axes denote H_{tc}, H_{pc} and H_{ps} respectively.

From (3.1), (3.2), (3.3), (3.4) and (3.5), we can conclude that $\mathrm{H}_{pc} = 0$ implies $\mathrm{H}_{ps} = 0$ and $\mathrm{H}_{tc} = 0$. Thus, the graph for a fixed H_{msc} starts at $(0,0,0)$.

From (3.3) and (3.4), it is easily checked that H_{cr} is fixed when H_{msc} is fixed and H_{ps} is a continuous and strictly increasing function of H_{pc}. So, if we project the graph onto YZ-plane, it draws a continuous curve moving to the plus direction of z axis as it moves to the plus direction of y axis.

Lastly, when H_{msc} is fixed,

$$\mathrm{H}_{tc} = \Big(\frac{1}{\mathrm{H}_{msc}} + \frac{1}{6}\Big)\frac{1}{\mathrm{H}_{msc}^3}\mathrm{H}_{ps}\{\ln(1-\mathrm{H}_{ps})\}^2$$

is a function of H_{ps} whose derivative

$$\frac{d}{d\mathrm{H}_{ps}}\mathrm{H}_{tc} = \Big(\frac{1}{\mathrm{H}_{msc}} + \frac{1}{6}\Big)\frac{1}{\mathrm{H}_{msc}^3}\Big[\{\ln(1-\mathrm{H}_{ps})\}^2 - 2\mathrm{H}_{ps}\ln(1-\mathrm{H}_{ps})\frac{1}{1-\mathrm{H}_{ps}}\Big]$$

has positive value excluding at $\mathrm{H}_{ps} = 0$. So it is a continuous and strictly increasing function. Thus, the proof is completed. □

Proposition 4.9. *When fixing* H_{msc}*, if one of* H_{tc}*,* H_{pc} *and* H_{ps} *is fixed in their own range, the other two are determined uniquely. And tradeoff parameters implementing these* H_{tc}*,* H_{pc} *and* H_{ps} *exist.*

Proof. The first part of this proposition is the direct result of Lemma 4.8.

By setting parameters m, t to satisfy $\mathrm{H}_{msc} = mt^2/N$, $\mathrm{H}_{pc} = mtl/N$, we see the existence of tradeoff parameters implementing these H_{tc}, H_{pc} and H_{ps}. □

Lemma 4.10. *When* $\hat{t}$ *is sufficiently large, a graph in* D_{tc}-D_{pc}-D_{ps} *space for a fixed* D_{msc} *starts at* $(0,0,0)$ *and is drawn in a continuous curve. As* D_{pc} *increases,* D_{ps} *and* D_{tc} *also increases.*

Proof. Using (3.6), (3.7), (3.8), (3.9) and (3.10), this lemma can be proved by similar arguments in Lemma 4.8. □

Proposition 4.11. *When* $\hat{t}$ *is sufficiently large, if one of* D_{tc}*,* D_{pc} *and* D_{ps} *is fixed in their own range with fixed* D_{msc}*, the other two are determined uniquely. And tradeoff parameters implementing these* D_{tc}*,* D_{pc} *and* D_{ps} *exist.*

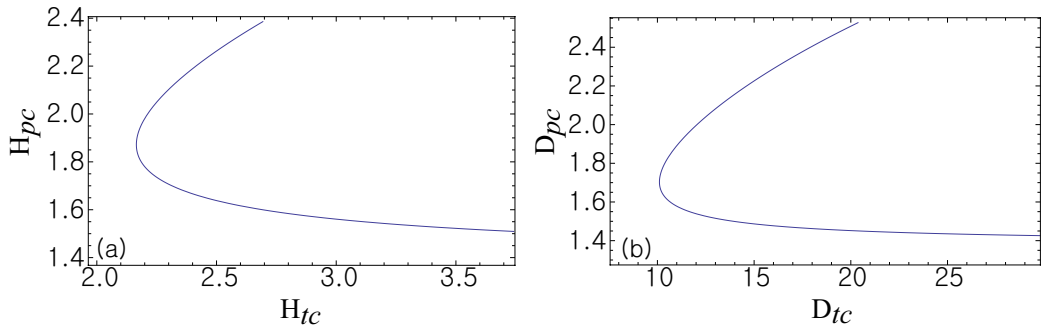

Figure 13: Graph in *tc-pc* plane for fixed value of $ps = 0.75$ ((a): Hellman tradeoff, (b): DP tradeoff)

Proof. The first part of this proposition is the result of Lemma 4.10.

By setting parameters m, t to satisfy $\mathrm{D}_{msc} = mt^2/N$, $\mathrm{D}_{pc} = mtl/N$, we see the existence of tradeoff parameters implementing these D_{tc}, D_{pc} and D_{ps}. □

Similar to the R, R_{tc}, R_{pc} and R_{ps} criteria in case of the Rainbow tradeoff, let us define the H, H_{tc}, H_{pc} and H_{ps} criteria and the D, D_{tc}, D_{pc} and D_{ps} criteria in the case of the Hellman and the DP tradeoff respectively.

Using Lemma 4.8, we get the next two results by arguments similar to the ones in the rainbow case.

Proposition 4.12. *To judge a set of parameters weather it is unreasonable or not by the* H *criterion is same with to judge it by the* H_{ps} *criterion.*

Proposition 4.13. *To judge a set of parameters weather it is unreasonable or not by the* H_{tc} *criterion together with the* H_{pc} *criterion is same with to judge it by the* H_{ps} *criterion.*

Likewise, using Lemma 4.10, we get the next two results by arguments similar to the ones in the rainbow case.

Proposition 4.14. *When* $\hat{t}$ *is suffice large, to judge a set of parameters weather it is unreasonable or not by the* D *criterion is same with to judge it by the* D_{ps} *criterion.*

Proposition 4.15. *When* $\hat{t}$ *is suffice large, to judge a set of parameters weather it is unreasonable or not by the* D_{tc} *criterion together with the* D_{pc} *criterion is same with to judge it by the* D_{ps} *criterion.*

In addition, when we fix *ps*, the shape of graphs in *tc-pc* plane is as Figure 13.

Thus, we get the next remarks by arguments similar to Remark 4.6.

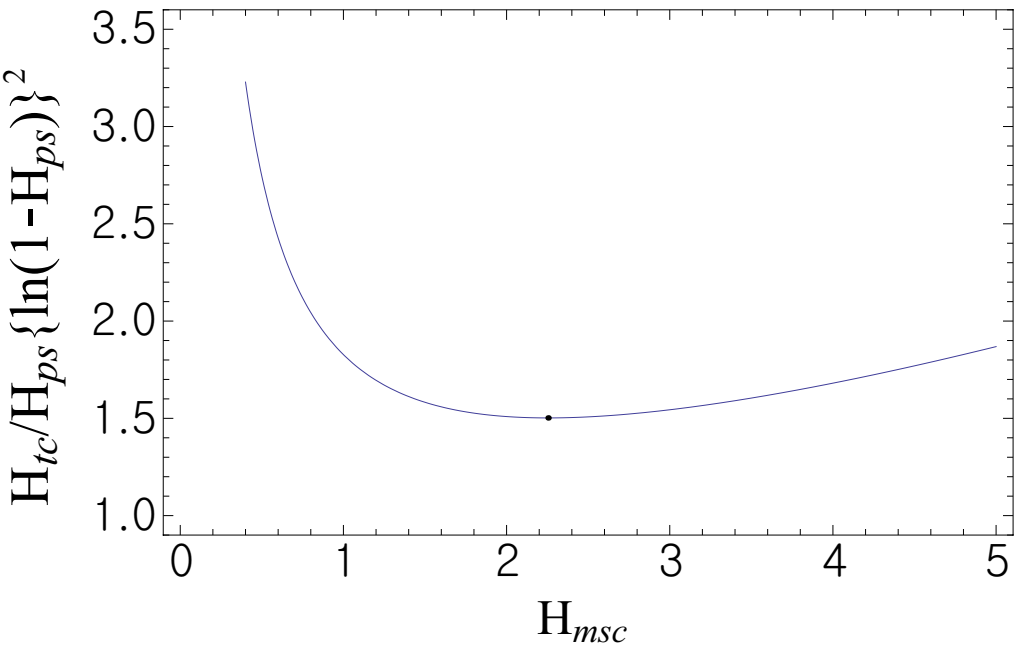

Figure 14: Graph for fixed value of H_{ps} in Hellman tradeoff

Remark 4.16. To judge a set of parameters weather it is unreasonable or not by the H_{tc} criterion is same with to judge it by the H_{ps} criterion.

Remark 4.17. When $\hat{t}$ is sufficiently large, to judge a set of parameters weather it is unreasonable or not by the D_{tc} criterion is same with to judge it by the D_{ps} criterion.

From (3.3) and (3.5), H_{tc} can be analysed as a function of H_{msc} only in circumstances where H_{ps} is fixed. In [6], the value of H_{msc} which implements the lowest H_{tc} was obtained as H_{msc}=2.25433 (See Figure 14).

As a result, regardless of the fixed value of H_{ps}, the criterion for the optimality is $H_{msc} = 2.25433$. From (3.3) and (3.4), we get

$$H_{pc} = \frac{\sqrt{H_{msc}}}{\sqrt{2}} \frac{e^{\sqrt{2H_{msc}}} + 1}{e^{\sqrt{2H_{msc}}} - 1} \{-\ln(1 - H_{ps})\}.$$

Thus, H_{pc} is a increasing function of H_{msc}. By this reason, any value in the range of $H_{msc} \leq 2.25433$ was recommended depending on the user circumstances.

In fact, because H_{pc} is a strictly increasing function of H_{msc} where H_{ps} is fixed, the shape of a graph in H_{tc}-H_{msc} space is similar to the shape of a graph in H_{tc}-H_{pc} space. Thus, by Remark 4.16 and Proposition 4.12 the next remark follows.

H_{tc}	H_{pc}	highest H_{ps}
1	1.38	0.639503
2	1.81	0.73879
3	2.14	0.795036
5	2.66	0.860145
10	3.61	0.931024

Table 5: Highest value of H_{ps} under fixed value of H_{tc}

Remark 4.18. Where one of H_{tc}, H_{pc} and H_{ps} is fixed, the necessary and sufficient condition for tradeoff parameters being reasonable is $H_{msc} \leq 2.25433$.

From the above remark, we can find a big difference on the shape of graphs in *tc-pc-ps* space between the rainbow tradeoff and the Hellman tradeoff. Remind that in the rainbow tradeoff, when we imagine one curve for a fixed l in R_{tc}-R_{pc}-R_{ps} space, the criterion for tradeoff parameters being reasonable for this fixed value is expressed as $0 \leq R_{ps} \leq ps(l)$. But, in the Hellman tradeoff, when we imagine one curve for a fixed H_{msc} in H_{tc}-H_{pc}-H_{ps} space, a point of this curve corresponds to reasonable tradeoff parameters iff all the points of this curve corresponds to reasonable tradeoff parameters. In H_{tc}-H_{pc}-H_{ps} space all the curve for fixed H_{msc} in the range of $H_{msc} > 2.25433$ are removed by the curve for fixed $H_{msc} = 2.25433$. And the curve for the fixed $H_{msc} = 2.25433$ denotes all of optimal tradeoff parameters.

For reference, in [10], under circumstances where H_{tc} is fixed, the value of implementing the highest value of H_{tc} was calculated as Table 5.

By arguments so far, however, it is anticipated that the values in Table 5 could be obtained by applying $H_{msc} = 2.25433$ to the fixed value of H_{tc}. And this is confirmed in Table 6.

By arguments similar to Remark 4.18 with the result in [6] on the criteria for optimal tradeoff parameters in the DP tradeoff, the remark below can be obtained.

Remark 4.19. When $\hat{t}$ is sufficiently large, where one of D_{tc}, D_{pc}, D_{ps} is fixed, the necessary and sufficient condition for tradeoff parameters being reasonable is $D_{msc} \leq 0.562047$.

4.8 Extension of concept of reasonable tradeoff parameters

In this subsection, we will extend the concept of reasonable tradeoff parameters to the case of comparing two sets of parameters from two different

H_{tc}	H_{msc}	H_{pc}	H_{ps}
1	2.25433	1.37759	0.639505
2	2.25433	1.81258	0.738792
3	2.25433	2.13998	0.795036
5	2.25433	2.65608	0.860146
10	2.25433	3.61046	0.931024

Table 6: Values of H_{pc} and H_{ps} determined by each fixed values of H_{tc} with $\mathrm{H}_{msc} = 2.25433$

tradeoff algorithms respectively. The comparison of three tradeoff algorithms was studied in [6] under circumstances where ps is fixed. In this subsection, those results will be reused in removing unreasonable tradeoff parameters in the extended sense.

In [6], it is pointed out that comparing tradeoff efficiencies of the three tradeoff algorithms by the rates

$$\mathrm{D}_{tc} : \mathrm{H}_{tc} : \mathrm{R}_{tc}$$

is not fair.

Note that M in the tradeoff curve is not the real physical storage needed in the pre-computation phase. It is just the number of ordered pairs (sp_i^k, ep_i^k) to be stored. The number of bits needed to store one (sp_i^k, ep_i^k) can be different for each tradeoff. Likewise, T in the tradeoff curve is not the real physical time needed in the online phase. It is just the number of one-way function iterations in the online phase, and T does not contain the time necessary for table lookups. The time necessary for a one-way function iteration and a table lookup can also be different for each tradeoff. Therefore, it is needed to unify two units of the three tradeoff algorithms.

In [6], it is pointed out that it is suitable to assume that the tradeoff parameters that would be chosen for each algorithm would be related through $\log t_D \approx \log t_H \approx \log t_R$, $\log m_D \approx \log m_H$ and $\log m_R \approx \log m_H + \log t_H$. Under this assumption, [6] showed thattradeoff efficiency should be compared by the ratio

$$\left(\frac{\log m_D}{\log m_R}\right)^2 \mathrm{D}_{tc} : \mathrm{H}_{tc} : \mathrm{R}_{tc}$$

to reflect the real physical storage.

Next, let us define $|\mathrm{TL} - \mathrm{H}|$, $|\mathrm{TL} - \mathrm{D}|$ and $|\mathrm{TL} - \mathrm{R}|$ as the time necessary for one table lookup in case of the Hellman, the DP and the rainbow tradeoff respectively, and $|\mathrm{Itr}|$ as the time necessary for a one-way function iteration in the three tradeoffs. Then, it is suitable to assume that $|\mathrm{Itr}| \approx |\mathrm{TL} - \mathrm{D}| \approx$

$|\mathrm{TL}-\mathrm{H}| \leq |\mathrm{TL}-\mathrm{R}| \ll t_D|\mathrm{Itr}| \approx t_R|\mathrm{Itr}|$. Under this assumption, [6] showed that tradeoff efficiency should be compared by the ratio

$$\mathrm{D}_{tc} : \left(1 + \frac{6}{6+\mathrm{H}_{msc}} \frac{|\mathrm{TL}-\mathrm{H}|}{|\mathrm{Itr}|}\right)\mathrm{H}_{tc} : \mathrm{R}_{tc}$$

to reflect the real physical time.

From above two arguments, tradeoff efficiency of three tradeoff can be compared fairly by the ratio

$$\left(\frac{\log m_D}{\log m_R}\right)^2 \mathrm{D}_{tc} : \left(1 + \frac{6}{6+\mathrm{H}_{msc}} \frac{|\mathrm{TL}-\mathrm{H}|}{|\mathrm{Itr}|}\right)\mathrm{H}_{tc} : \mathrm{R}_{tc}$$

With assumptions in the above two arguments, the following assumptions are called *the typical situation* : $\log m_D \approx \log m_H \approx \log t_D \approx \log t_H \approx \log t_R \approx \frac{1}{3}\log N$, $\log m_R \approx \frac{2}{3}\log N$ and a single table lookup is negligible in comparison to that required for a single one-way function computation. Under the typical situation, tradeoff efficiency of the three tradeoff can be compared fairly by the ratio

$$\frac{1}{4}\mathrm{D}_{tc} : \mathrm{H}_{tc} : \mathrm{R}_{tc}.$$

Here, we use the notation tc^u for the tradeoff coefficient after the unification of units. That is, tc^u means H_{tc}, $\frac{1}{4}\mathrm{D}_{tc}$ or R_{tc} in the case of the Hellman, the DP or the rainbow tradeoff respectively.

In [6], the three tradeoffs are compared by analysing graphs of

$$\{(\mathrm{H}_{pc}[\mathrm{H}_{msc}], \mathrm{H}_{tc}[\mathrm{H}_{msc}])|\mathrm{H}_{msc} \leq 2.25433\},$$
$$\{(\mathrm{D}_{pc}[\mathrm{D}_{msc}], \frac{1}{4}\mathrm{D}_{tc}[\mathrm{D}_{msc}])|\mathrm{D}_{msc} \leq 0.562047\},$$
$$\{(\mathrm{R}_{pc}[l], \mathrm{R}_{tc}[l])|l \geq \textit{optimal table count for } \mathrm{R}_{ps}\}$$

in circumstances where ps is fixed. From graphs in Figure 15 [6], when the fixed value of ps is equal to or greater than 75%, we can confirm that tradeoff parameters which is a comparative advantage in terms of tc^u and pc exist only in the rainbow tradeoff. Thus, in the typical situation, [6] concluded that the use of rainbow tradeoff is advisable for high success rate requirements.

Now, we can compare the values of tc from two different tradeoff algorithms. Thus, the concept of reasonable tradeoff parameters can be extended to the case of comparing two sets of parameters from two different tradeoff algorithms respectively. And, we can think of the method removing unreasonable tradeoff parameters in the extended sense by analysing the graphs in tc^u-pc plane for a fixed ps after the unification of units. We call this method as the *ps criterion*. Then, using Lemma 4.2, 4.8 and 4.10, we get the next proposition which unifies Proposition 4.4, 4.12 and 4.14. This can be easily proved by similar argument in Proposition 4.4.

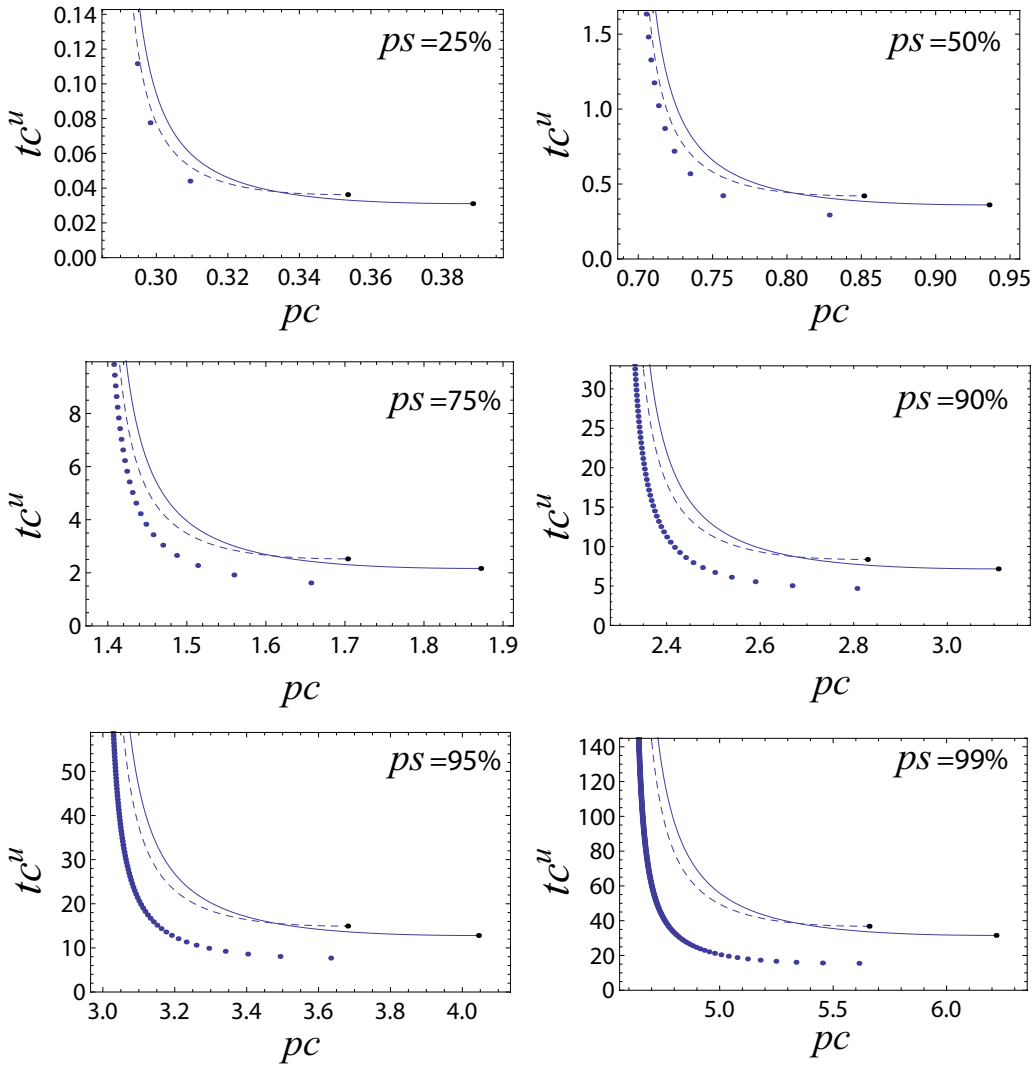

Figure 15: Graphs in pc-tc^u plane for fixed values of ps (Hellman tradeoff: solid, DP tradeoff: dashed, Rainbow tradeoff: large dots)

Proposition 4.20. *To judge a set of parameters of the three tradeoff algorithms weather it is reasonable or not in the extended sense can be done by the ps criterion.*

Reinterpreting the graphs in Figure 15 by Proposition 4.20, all the points of the Hellman and the DP tradeoff correspond to unreasonable tradeoff parameters in the extended sense in the range of $ps \geq 75\%$. In conclusion, when we consider the typical situation and high success rate requirements, reasonable tradeoff parameters in the extended sense exist only in the case of the rainbow tradeoff. And these reasonable tradeoff algorithm could be found using the R_{ps} criterion.

5 Conclusion

In [6], tradeoff parameters implementing the best tradeoff efficiency in the circumstances where the probability of success is fixed was called optimal tradeoff parameters. And the criterion for optimality of tradeoff parameters was obtained. In this paper, we have treated the tradeoff efficiency(or the tradeoff coefficient(tc)), the cost of pre-computation(or the pre-compatation coefficient(pc)) and the probability of success(ps) all equally, not concerning only on obtaining the lowest tc. For this, we have defined new terminology, so called reasonable tradeoff parameters. We have studied how to decide whether a set of parameters is reasonable or not. As a result, we have proved that all of reasonable tradeoff parameters could be searched out by analysing the graph in tc-pc plane under circumstances where ps is fixed. In addition, we have shown that reasonable tradeoff parameters could be also searched out by analysing the graphs in pc-ps plane in circumstances where tc is fixed. And we have determined the relations between the optimal tradeoff parameters and the reasonable tradeoff parameters.

We have also proven that if one of tc, pc and ps is fixed in its own range, the other two are determined uniquely when fixing the table count l in the case of the rainbow tradeoff (instead, when fixing the matrix stopping constant(msc) in the case of the Hellman and the DP tradeoff). The existence of tradeoff parameters implementing these tc, pc and ps have also been shown. This conclusion was deduced from the result of one lemma about the shape of graphs in tc-pc-ps space for a fixed l or msc depending on the kind of the tradeoff.

Finally, we have extended the concept of reasonable tradeoff parameters to the case of comparing two sets of parameters from two different tradeoff algorithms respectively. It has been shown that, when we consider the typical situation and high success rate requirements, reasonable tradeoff parameters exist only in the rainbow tradeoff. And these reasonable tradeoff algorithm could be get using the so-called R_{ps} criterion.

Bibliography

[1] G.Avoine, P.Junod, P.Oechslin, Characterization and improvement of time-memory trade-off based on perfect tables. ACM *Trans. Inform. Syst. Secur.,* 11(4), 17:1–17:22 (2008). Preliminary version in INDOCRYPT 2005

[2] C.Calik, *How to Invert One-way Functions: Time-Memory Trade-off Method.* M.S.Thesis, Middle East Technical University, January 2007

[3] D.E.Denning, *Cryptography and Data Security* (Addison-Wesley, 1982)

[4] M.E.Hellman, A cryptanalytic time-memory trade-off. *IEEE Trans. on Infor. Theory*, 26, pp. 401–406 (1980)

[5] J.Hong, The cost of false alarms in Hellman and rainbow tradeoffs. *Des. Codes Cryptogr.,* 57, pp. 293–327 (2010)

[6] J.Hong, S.Moon, *A comparison of cryptanalytic tradeoff algorithms.* Cryptology ePrint Archive. Report 2010/176

[7] K.Kusuda, T.Matsumoto, Optimization of time-memory trade-off cryptanalysis and its application to DES, FEAL-32, and Skipjack. *IEICE Trans. Fundamentals*, E79-A(1), pp. 35–48 (1996)

[8] D.Ma, J.Hong, Success probability of the Hellman trade-off. *Inf. Process. Lett.,* 109(7), pp. 345-351 (2009)

[9] P.Oechslin, Making a faster cryptanalytic time-memory trade-off. In *Advances in Cryptology—CRYPTO 2003*, LNCS 2729, (Springer, 2003), pp. 617-630

[10] C.Paeon, *Optimal Success Probability of the Hellman Time Memory Tradeoff,* M.S.Thesis, Seoul National University, August 2012