Analysis of the Parallel Distinguished Point Tradeoff

Jin Hong, *Ga Won Lee, Daegun Ma

Seoul National University

13/12/2011

The Inversion Problem

$\mathcal{N}$: key space with size N.

$F : \mathcal{N} \to \mathcal{N}$: one-way function

The inversion problem

For a given inversion target $F(x) = y$, Find x.

The Inversion Problem

$\mathcal{N}$: key space with size N.

$F : \mathcal{N} \to \mathcal{N}$: one-way function

The inversion problem

For a given inversion target $F(x) = y$, Find x.

The Inversion Problem

$\mathcal{N}$: key space with size N.

$F : \mathcal{N} \to \mathcal{N}$: one-way function

The inversion problem

For a given inversion target $F(x) = y$, Find x.

Two extreme methods

- Exhaustive search : T=N, M=1,
- Dictionary attack : T=1, M=N,

where T is total online time, M is storage size.

The Inversion Problem

Time Memory Tradeoff(Hellman)

- *Pre-computation phase :*

  pre-compute sufficiently many $(a, F(a))$ pairs, and

  store a digest of the computation in a table **smaller than the complete dictionary.**

- *Online phase :*

  given an inversion target, using the table, find the answer in time **shorter than required by exhaustive search.**

The DP Tradeoff : pre-computation phase

R. Rivest

- Choose parameters $m,\ t$ satisfying $mt^2 = N$.

The DP Tradeoff : pre-computation phase

R. Rivest

- Choose parameters $m, \ t$ satisfying $mt^2 = N$.
- **DP**(distinguished point) is an element satisfying a certain pre-set property. Here, the prob. of DP occurrence is set to $\frac{1}{t}$.
(ex. $X \equiv 0 \mod t$)

The DP Tradeoff : pre-computation phase

R. Rivest

- Choose parameters $m,\ t$ satisfying $mt^2 = N$.
- **DP**(distinguished point) is an element satisfying a certain pre-set property. Here, the prob. of DP occurrence is set to $\frac{1}{t}$. (ex. $X \equiv 0 \mod t$)

1. Construct t many DP matrices using F.
   - each chain is set to end on a DP.

$$m \begin{cases} \mathrm{SP}_1 = \circ \xrightarrow{F} \circ \xrightarrow{F} \cdots\cdots \quad \xrightarrow{F} \circ = \mathrm{EP}_1 \ : \ \mathrm{DP} \\ \mathrm{SP}_2 = \circ \xrightarrow{F} \circ \xrightarrow{F} \cdots\cdots \quad \xrightarrow{F} \cdots\cdots \xrightarrow{F} \circ = \mathrm{EP}_2 \ : \ \mathrm{DP} \\ \vdots \\ \mathrm{SP}_m = \circ \xrightarrow{F} \cdots\cdots \xrightarrow{F} \circ \quad = \mathrm{EP}_m : \ \mathrm{DP} \end{cases}$$

: A single DP matrix

The DP Tradeoff : pre-computation phase

R. Rivest

- Choose parameters $m,\ t$ satisfying $mt^2 = N$.
- **DP**(distinguished point) is an element satisfying a certain pre-set property. Here, the prob. of DP occurrence is set to $\frac{1}{t}$. (ex. $X \equiv 0 \mod t$)

1. Construct t many DP matrices using F.
   - each chain is set to end on a DP.

$$m \begin{cases} \mathrm{SP}_1 = \circ \xrightarrow{F} \circ \xrightarrow{F} \cdots\cdots \quad \xrightarrow{F} \circ = \mathrm{EP}_1 \ : \ \mathrm{DP} \\ \mathrm{SP}_2 = \circ \xrightarrow{F} \circ \xrightarrow{F} \cdots\cdots \quad \xrightarrow{F} \cdots\cdots \xrightarrow{F} \circ = \mathrm{EP}_2 \ : \ \mathrm{DP} \\ \vdots \\ \mathrm{SP}_m = \circ \xrightarrow{F} \cdots\cdots \xrightarrow{F} \circ \quad = \mathrm{EP}_m : \ \mathrm{DP} \end{cases}$$

: A single DP matrix

2. Store $\{(SP_j, EP_j)\}_{j=1}^{m}$ only, throwing the rest out.

The DP Tradeoff : online phase

Given an inversion target $y = F(x)$

1. **Online chian creation**

Create *online chain* from y.

$$y \xrightarrow{F} \circ \xrightarrow{F} \circ \xrightarrow{F} \cdots\cdots \xrightarrow{F} \bullet : \mathrm{DP}$$

The DP Tradeoff : online phase

Given an inversion target $y = F(x)$

1. **Online chian creation**

Create *online chain* from y.

$$y \xrightarrow{F} \circ \xrightarrow{F} \circ \xrightarrow{F} \cdots\cdots \xrightarrow{F} \bullet : \mathrm{DP}$$

Check if it matches an ending point in $\{EP_j\}$.

The DP Tradeoff : online phase

Given an inversion target $y = F(x)$

1. **Online chian creation**

Create *online chain* from y.

$$y \xrightarrow{F} \circ \xrightarrow{F} \circ \xrightarrow{F} \cdots\cdots \xrightarrow{F} \color{red}{\bullet} : \mathrm{DP}$$

Check if it matches an ending point in $\{EP_j\}$.

$$m \begin{cases} \mathrm{SP}_1 = \circ \xrightarrow{F} \circ \xrightarrow{F} \cdots\cdots \quad \xrightarrow{F} \circ = \mathrm{EP}_1 \ : \ \mathrm{DP} \\ \mathrm{SP}_2 = \circ \xrightarrow{F} \circ \xrightarrow{F} \cdots\cdots \quad \xrightarrow{F} \cdots\cdots \xrightarrow{F} \overset{\color{red}{\text{alarm!!}}}{\color{red}{\bullet}} = \mathrm{EP}_2 \ : \ \mathrm{DP} \\ \qquad \vdots \\ \mathrm{SP}_m = \circ \xrightarrow{F} \cdots\cdots \xrightarrow{F} \circ \ = \mathrm{EP}_m : \ \mathrm{DP} \end{cases}$$

The DP Tradeoff : online phase

2. **pre-computed chain regeneration**

Expectation :

$$\mathrm{SP}_2 = \circ \xrightarrow{F} \circ \xrightarrow{F} \cdots\cdots \quad {\color{red}x} \xrightarrow{F} y \xrightarrow{F} \circ \cdots\cdots \xrightarrow{F} \overset{\color{red}\text{alarm!!}}{\color{red}\bullet} = \mathrm{EP}_2$$

$$ {\color{red}x} \xrightarrow{F} y \xrightarrow{F} \circ \cdots\cdots \xrightarrow{F} {\color{red}\bullet}$$

The DP Tradeoff : online phase

2. **pre-computed chain regeneration**

Expectation :

$$\mathrm{SP}_2 = \circ \xrightarrow{F} \circ \xrightarrow{F} \cdots\cdots \quad x \xrightarrow{F} y \xrightarrow{F} \circ \cdots\cdots \xrightarrow{F} \overset{\text{alarm!!}}{\bullet} = \mathrm{EP}_2$$

$$x \xrightarrow{F} y \xrightarrow{F} \circ \cdots\cdots \xrightarrow{F} \bullet$$

pre-computed chain regeneration :

$$\mathrm{SP}_2 = \circ$$

The DP Tradeoff : online phase

2. **pre-computed chain regeneration**

Expectation :

$$\mathrm{SP}_2 = \circ \xrightarrow{F} \circ \xrightarrow{F} \cdots\cdots \quad x \xrightarrow{F} y \xrightarrow{F} \circ \cdots\cdots \xrightarrow{F} \overset{\text{alarm!!}}{\bullet} = \mathrm{EP}_2$$

$$x \xrightarrow{F} y \xrightarrow{F} \circ \cdots\cdots \xrightarrow{F} \bullet$$

pre-computed chain regeneration :

$$\mathrm{SP}_2 = \circ \xrightarrow{F} \circ$$

The DP Tradeoff : online phase

2. **pre-computed chain regeneration**

Expectation :

$$\begin{array}{l} \mathrm{SP}_2 = \circ \xrightarrow{F} \circ \xrightarrow{F} \cdots\cdots \quad {\color{red}x} \xrightarrow{F} y \xrightarrow{F} \circ \cdots\cdots \xrightarrow{F} \overset{\color{red}\text{alarm!!}}{\color{red}\bullet} = \mathrm{EP}_2 \\ \qquad\qquad\qquad\qquad\qquad\quad {\color{red}x} \xrightarrow{F} y \xrightarrow{F} \circ \cdots\cdots \xrightarrow{F} {\color{red}\bullet} \end{array}$$

pre-computed chain regeneration :

$$\mathrm{SP}_2 = \circ \xrightarrow{F} \circ \xrightarrow{F}$$

The DP Tradeoff : online phase

2. **pre-computed chain regeneration**

Expectation :

$$\mathrm{SP}_2 = \circ \xrightarrow{F} \circ \xrightarrow{F} \cdots\cdots \quad x \xrightarrow{F} y \xrightarrow{F} \circ \cdots\cdots \xrightarrow{F} \overset{\text{alarm!!}}{\bullet} = \mathrm{EP}_2$$

$$x \xrightarrow{F} y \xrightarrow{F} \circ \cdots\cdots \xrightarrow{F} \bullet$$

pre-computed chain regeneration :

$$\mathrm{SP}_2 = \circ \xrightarrow{F} \circ \xrightarrow{F} \cdots\cdots \xrightarrow{F}$$

The DP Tradeoff : online phase

2. **pre-computed chain regeneration**

Expectation :

$$\begin{array}{l} \mathrm{SP}_2 = \circ \xrightarrow{F} \circ \xrightarrow{F} \cdots\cdots \quad {\color{red}x} \xrightarrow{F} y \xrightarrow{F} \circ \cdots\cdots \xrightarrow{F} \overset{\color{red}\text{alarm!!}}{\color{red}\bullet} = \mathrm{EP}_2 \\ \qquad\qquad\qquad\qquad\qquad\quad {\color{red}x} \xrightarrow{F} y \xrightarrow{F} \circ \cdots\cdots \xrightarrow{F} {\color{red}\bullet} \end{array}$$

pre-computed chain regeneration :

$$\mathrm{SP}_2 = \circ \xrightarrow{F} \circ \xrightarrow{F} \cdots\cdots \xrightarrow{F} {\color{red}x}$$

The DP Tradeoff : online phase

2. **pre-computed chain regeneration**

Expectation :

$$\mathrm{SP}_2 = \circ \xrightarrow{F} \circ \xrightarrow{F} \cdots\cdots \quad {\color{red}x} \xrightarrow{F} y \xrightarrow{F} \circ \cdots\cdots \xrightarrow{F} \overset{\color{red}\text{alarm!!}}{\color{red}\bullet} = \mathrm{EP}_2$$

$$\qquad\qquad\qquad\qquad {\color{red}x} \xrightarrow{F} y \xrightarrow{F} \circ \cdots\cdots \xrightarrow{F} {\color{red}\bullet}$$

pre-computed chain regeneration :

$$\mathrm{SP}_2 = \circ \xrightarrow{F} \circ \xrightarrow{F} \cdots\cdots \xrightarrow{F} {\color{red}x} \xrightarrow{F} y$$

The DP Tradeoff : online phase

2. **pre-computed chain regeneration**

Expectation :

$$\begin{array}{llll} \mathrm{SP}_2 = \circ \xrightarrow{F} \circ \xrightarrow{F} \cdots\cdots & x \xrightarrow{F} y \xrightarrow{F} \circ \cdots\cdots \xrightarrow{F} & \overset{\text{alarm!!}}{\bullet} & = \mathrm{EP}_2 \\ & x \xrightarrow{F} y \xrightarrow{F} \circ \cdots\cdots \xrightarrow{F} & \bullet & \end{array}$$

pre-computed chain regeneration :

$$\mathrm{SP}_2 = \circ \xrightarrow{F} \circ \xrightarrow{F} \cdots\cdots \xrightarrow{F} x \xrightarrow{F} y$$

'x' is just found!!!

The DP Tradeoff : online phase

However,

Most case : Since F is not injective, $\acute{x} \neq x$

$$\mathrm{SP}_2 = \circ \xrightarrow{F} \cdots \quad \acute{x} \xrightarrow{F} \circ \xrightarrow{F} \circ \quad \cdots \quad \xrightarrow{F} \bullet \cdots \xrightarrow{F} \overset{\text{alarm!!}}{\bullet} = \mathrm{EP}_2$$

$$\nearrow$$

$$x \xrightarrow{F} y \xrightarrow{F} \circ \quad \cdots$$

The DP Tradeoff : online phase

However,

Most case : Since F is not injective, $\acute{x} \neq x$

$$\mathrm{SP}_2 = \circ \xrightarrow{F} \cdots \quad \acute{x} \xrightarrow{F} \circ \xrightarrow{F} \circ \quad \cdots \quad \xrightarrow{F} \bullet \cdots \xrightarrow{F} \overset{\text{alarm!!}}{\bullet} = \mathrm{EP}_2$$

$$\nearrow$$

$$x \xrightarrow{F} y \xrightarrow{F} \circ \quad \cdots$$

- It is called a *false alarm*.

The DP Tradeoff : online phase

However,

Most case : Since F is not injective, $\acute{x} \neq x$

$$\mathrm{SP}_2 = \circ \xrightarrow{F} \cdots \quad \acute{x} \xrightarrow{F} \circ \xrightarrow{F} \circ \quad \cdots \quad \xrightarrow{F} \bullet \cdots \xrightarrow{F} \overset{\text{alarm!!}}{\bullet} = \mathrm{EP}_2$$

$$\nearrow$$

$$x \xrightarrow{F} y \xrightarrow{F} \circ \quad \cdots$$

- It is called a *false alarm*.

pre-computed chain regeneration :

$$\mathrm{SP}_2 = \circ \xrightarrow{F} \cdots$$

The DP Tradeoff : online phase

However,

Most case : Since F is not injective, $\acute{x} \neq x$

$$\mathrm{SP}_2 = \circ \xrightarrow{F} \cdots \quad \acute{x} \xrightarrow{F} \circ \xrightarrow{F} \circ \quad \cdots \quad \xrightarrow{F} \bullet \cdots \xrightarrow{F} \overset{\text{alarm!!}}{\bullet} = \mathrm{EP}_2$$

$$\nearrow$$

$$x \xrightarrow{F} y \xrightarrow{F} \circ \quad \cdots$$

- It is called a *false alarm*.

pre-computed chain regeneration :

$$\mathrm{SP}_2 = \circ \xrightarrow{F} \cdots \quad \acute{x} \xrightarrow{F} \circ \xrightarrow{F} \circ \cdots$$

The DP Tradeoff : online phase

However,

Most case : Since F is not injective, $\acute{x} \neq x$

$$\mathrm{SP}_2 = \circ \xrightarrow{F} \cdots \quad \acute{x} \xrightarrow{F} \circ \xrightarrow{F} \circ \quad \cdots \quad \xrightarrow{F} \bullet \cdots \xrightarrow{F} \overset{\text{alarm!!}}{\bullet} = \mathrm{EP}_2$$

$$\nearrow$$

$$x \xrightarrow{F} y \xrightarrow{F} \circ \quad \cdots$$

- It is called a *false alarm*.

pre-computed chain regeneration :

$$\mathrm{SP}_2 = \circ \xrightarrow{F} \cdots \quad \acute{x} \xrightarrow{F} \circ \xrightarrow{F} \circ \cdots \xrightarrow{F} \bullet \cdots$$

The DP Tradeoff : online phase

However,

Most case : Since F is not injective, $\acute{x} \neq x$

$$\mathrm{SP}_2 = \circ \xrightarrow{F} \cdots \quad \acute{x} \xrightarrow{F} \circ \xrightarrow{F} \circ \quad \cdots \quad \xrightarrow{F} \bullet \cdots \xrightarrow{F} \overset{\text{alarm!!}}{\bullet} = \mathrm{EP}_2$$

$$\nearrow$$

$$x \xrightarrow{F} y \xrightarrow{F} \circ \quad \cdots$$

- It is called a *false alarm*.

pre-computed chain regeneration :

$$\mathrm{SP}_2 = \circ \xrightarrow{F} \cdots \quad \acute{x} \xrightarrow{F} \circ \xrightarrow{F} \circ \cdots \xrightarrow{F} \bullet \cdots \xrightarrow{F} \quad \bullet \quad = \mathrm{EP}_2$$

The DP Tradeoff : online phase

However,

Most case : Since F is not injective, $\acute{x} \neq x$

$$\mathrm{SP}_2 = \circ \xrightarrow{F} \cdots \quad \acute{x} \xrightarrow{F} \circ \xrightarrow{F} \circ \quad \cdots \quad \xrightarrow{F} \bullet \cdots \xrightarrow{F} \overset{\text{alarm!!}}{\bullet} = \mathrm{EP}_2$$

$$\nearrow$$

$$x \xrightarrow{F} y \xrightarrow{F} \circ \quad \cdots$$

- It is called a *false alarm*.

pre-computed chain regeneration :

$$\mathrm{SP}_2 = \circ \xrightarrow{F} \cdots \quad \acute{x} \xrightarrow{F} \circ \xrightarrow{F} \circ \cdots \xrightarrow{F} \bullet \cdots \xrightarrow{F} \quad \bullet \quad = \mathrm{EP}_2$$

• Whole pre-computed chain is re-generated, but 'x' cannot be found.

The Rainbow Method : the rainbow matrix

Oechslin

- Choose parameters m, t satisfying $mt = N$.(Recall. In DP, $m_D t_D^2 = N$)

The Rainbow Method : the rainbow matrix

Oechslin

- Choose parameters m, t satisfying $mt = N$.(Recall. In DP, $m_D t_D^2 = N$)

1. Create one big $m \times t$ matrix using F and reduction functions r_i.

$$\mathrm{SP}_1 = \circ \xrightarrow{F_1} \circ \xrightarrow{F_2} \cdots\cdots \xrightarrow{F_t} \circ = \mathrm{EP}_1$$
$$\mathrm{SP}_2 = \circ \xrightarrow{F_1} \circ \xrightarrow{F_2} \cdots\cdots \xrightarrow{F_t} \circ = \mathrm{EP}_2$$
$$\vdots$$
$$\vdots$$
$$\vdots$$
$$\mathrm{SP}_m = \circ \xrightarrow{F_1} \circ \xrightarrow{F_2} \cdots\cdots \xrightarrow{F_t} \circ = \mathrm{EP}_m$$

: A single rainbow matrix

,where $F_i = r_i \circ F$.

The Rainbow Method : the rainbow matrix

Oechslin

- Choose parameters m, t satisfying $mt = N$.(Recall. In DP, $m_D t_D^2 = N$)

1. Create one big $m \times t$ matrix using F and reduction functions r_i.

$$\mathrm{SP}_1 = \circ \xrightarrow{F_1} \circ \xrightarrow{F_2} \cdots\cdots \xrightarrow{F_t} \circ = \mathrm{EP}_1$$
$$\mathrm{SP}_2 = \circ \xrightarrow{F_1} \circ \xrightarrow{F_2} \cdots\cdots \xrightarrow{F_t} \circ = \mathrm{EP}_2$$
$$\vdots$$
$$\vdots$$
$$\vdots$$
$$\mathrm{SP}_m = \circ \xrightarrow{F_1} \circ \xrightarrow{F_2} \cdots\cdots \xrightarrow{F_t} \circ = \mathrm{EP}_m$$

: A single rainbow matrix

,where $F_i = r_i \circ F$.

2. Store $\{(SP_j, EP_j)\}_{j=1}^{m}$ only, throwing the rest out.

Previous Results : online time complexity [HM10]

The DP tradeoff, $mt^2 = \mathtt{D}_{msc}N$

Previous Results : online time complexity [HM10]

The DP tradeoff, $mt^2 = \mathtt{D}_{msc}N$

- The expected number of distinct points in a single DP matrix is $\mathtt{D}_{cr}mt$, where

$$\mathtt{D}_{cr} = \frac{2}{\sqrt{1 + 2\mathtt{D}_{msc}} + 1}.$$

Previous Results : online time complexity [HM10]

The DP tradeoff, $mt^2 = \mathtt{D}_{msc}N$

- The expected number of distinct points in a single DP matrix is $\mathtt{D}_{cr}mt$, where

$$\mathtt{D}_{cr} = \frac{2}{\sqrt{1+2\mathtt{D}_{msc}}+1}.$$

- The *success probability* of the DP tradeoff is

$$\mathtt{D}_{ps} = 1 - e^{-\mathtt{D}_{cr}\mathtt{D}_{pc}},$$

with pre-computation cost $\mathtt{D}_{pc}N$.

Previous Results : online time complexity [HM10]

The DP tradeoff, $mt^2 = \mathtt{D}_{msc}N$

- The expected number of distinct points in a single DP matrix is $\mathtt{D}_{cr}mt$, where

$$\mathtt{D}_{cr} = \frac{2}{\sqrt{1+2\mathtt{D}_{msc}}+1}.$$

- The *success probability* of the DP tradeoff is

$$\mathtt{D}_{ps} = 1 - e^{-\mathtt{D}_{cr}\mathtt{D}_{pc}},$$

  with pre-computation cost $\mathtt{D}_{pc}N$.

- The *time memory tradeoff curve* for the DP tradeoff is $\mathrm{TM}^2 = \mathtt{D}_{tc}N^2$, where

$$\mathtt{D}_{tc} = (2+\frac{1}{\mathtt{D}_{msc}})\frac{1}{\mathtt{D}_{cr}^3}\mathtt{D}_{ps}\{\ln(1-\mathtt{D}_{ps})\}^2.$$

Previous Results : online time complexity [HM10]

The rainbow method, $mt = \mathtt{R}_{msc}N$, l tables

Previous Results : online time complexity [HM10]

The rainbow method, $mt = \mathtt{R}_{msc}N$, l tables

- The *success probability* of the rainbow method is

$$\mathtt{R}_{ps} = 1 - \left(\frac{2}{2 + \mathtt{R}_{msc}}\right)^{2l}.$$

Previous Results : online time complexity [HM10]

The rainbow method, $mt = \mathtt{R}_{msc}N$, l tables

- The *success probability* of the rainbow method is

$$\mathtt{R}_{ps} = 1 - \left(\frac{2}{2+\mathtt{R}_{msc}}\right)^{2l}.$$

- The *time memory tradeoff curve* for the rainbow method is $\mathrm{TM}^2 = \mathtt{R}_{tc}N^2$, where

$$\mathtt{R}_{tc} = \frac{l^3}{(2l+1)(2l+2)(2l+3)}\bigg(\{(2l-1)+(2l+1)\mathtt{R}_{msc}\}(2+\mathtt{R}_{msc})^2 \\ -4\{(2l-1)+l(2l+3)\mathtt{R}_{msc}\}\left(\tfrac{2}{2+\mathtt{R}_{msc}}\right)^{2l}\bigg).$$

Previous Results : efficient use of storage [HM10]

$$\boxed{m_D {t_D}^2 = N = m_R t_R}$$

Previous Results : efficient use of storage [HM10]

$$\boxed{m_D {t_D}^2 = N = m_R t_R}$$

For each entry (SP_i, EP_i) in the DP tradeoff and the rainbow method,

- $\log m$ bits for the starting point,
- very small bits for the ending point.

are required.

Previous Results : efficient use of storage [HM10]

$$\boxed{m_D {t_D}^2 = N = m_R t_R}$$

For each entry (SP_i, EP_i) in the DP tradeoff and the rainbow method,

- $\log m$ bits for the starting point,
- very small bits for the ending point.

are required.

Typically, $\log m_R \approx \log m_D + \log t_D$ and $\log t_R \approx \log t_D$

So,

$$\frac{\log m_R}{\log m_D} \approx \frac{\log m_D + \log t_D}{\log m_D} \approx 2$$

Previous Results : efficient use of storage [HM10]

$$\boxed{m_D {t_D}^2 = N = m_R t_R}$$

For each entry (SP_i, EP_i) in the DP tradeoff and the rainbow method,

- $\log m$ bits for the starting point,
- very small bits for the ending point.

are required.

Typically, $\log m_R \approx \log m_D + \log t_D$ and $\log t_R \approx \log t_D$

So,

$$\frac{\log m_R}{\log m_D} \approx \frac{\log m_D + \log t_D}{\log m_D} \approx 2 \text{ and } M_R = 2\ M_D$$

The Parallel DP Tradeoff(The pD Tradeoff)

Variant of the DP tradeoff (Hoch, Shamir 09),

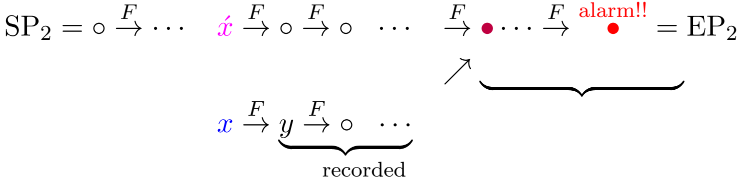
- A full record of the online chain is maintained during the online phase,
- The DP tables processed in parallel, rather than serially.

The Parallel DP Tradeoff(The pD Tradeoff)

Variant of the DP tradeoff (Hoch, Shamir 09),

- A full record of the online chain is maintained during the online phase,
- The DP tables processed in parallel, rather than serially.

Most case : false alarm



The Parallel DP Tradeoff(The pD Tradeoff)

Variant of the DP tradeoff (Hoch, Shamir 09),

- A full record of the online chain is maintained during the online phase,
- The DP tables processed in parallel, rather than serially.

Most case : false alarm

$$\mathrm{SP}_2 = \circ \xrightarrow{F} \cdots \quad \acute{x} \xrightarrow{F} \circ \xrightarrow{F} \circ \quad \cdots \quad \xrightarrow{F} \bullet \cdots \xrightarrow{F} \overset{\text{alarm!!}}{\bullet} = \mathrm{EP}_2$$

$$x \xrightarrow{F} \underbrace{y \xrightarrow{F} \circ \quad \cdots}_{\text{recorded}} \nearrow$$

pre-computed chain regeneration :

$$\mathrm{SP}_2 = \circ$$

The Parallel DP Tradeoff(The pD Tradeoff)

Variant of the DP tradeoff (Hoch, Shamir 09),

- A full record of the online chain is maintained during the online phase,
- The DP tables processed in parallel, rather than serially.

Most case : false alarm

$$\mathrm{SP}_2 = \circ \xrightarrow{F} \cdots \quad \acute{x} \xrightarrow{F} \circ \xrightarrow{F} \circ \quad \cdots \quad \xrightarrow{F} \bullet \cdots \xrightarrow{F} \overset{\text{alarm!!}}{\bullet} = \mathrm{EP}_2$$

$$x \xrightarrow{F} \underbrace{y \xrightarrow{F} \circ \quad \cdots}_{\text{recorded}} \nearrow$$

pre-computed chain regeneration :

$$\mathrm{SP}_2 = \circ \xrightarrow{F} \circ$$

The Parallel DP Tradeoff(The pD Tradeoff)

Variant of the DP tradeoff (Hoch, Shamir 09),

- A full record of the online chain is maintained during the online phase,
- The DP tables processed in parallel, rather than serially.

Most case : false alarm

$$\mathrm{SP}_2 = \circ \xrightarrow{F} \cdots \quad \acute{x} \xrightarrow{F} \circ \xrightarrow{F} \circ \quad \cdots \quad \xrightarrow{F} \bullet \cdots \xrightarrow{F} \overset{\text{alarm!!}}{\bullet} = \mathrm{EP}_2$$

$$x \xrightarrow{F} \underbrace{y \xrightarrow{F} \circ \quad \cdots}_{\text{recorded}}$$

pre-computed chain regeneration :

$$\mathrm{SP}_2 = \circ \xrightarrow{F} \circ \cdots \ \acute{x}$$

The Parallel DP Tradeoff(The pD Tradeoff)

Variant of the DP tradeoff (Hoch, Shamir 09),

- A full record of the online chain is maintained during the online phase,
- The DP tables processed in parallel, rather than serially.

Most case : false alarm

$$\mathrm{SP}_2 = \circ \xrightarrow{F} \cdots \quad \acute{x} \xrightarrow{F} \circ \xrightarrow{F} \circ \quad \cdots \quad \xrightarrow{F} \bullet \cdots \xrightarrow{F} \overset{\text{alarm!!}}{\bullet} = \mathrm{EP}_2$$

$$x \xrightarrow{F} \underbrace{y \xrightarrow{F} \circ \quad \cdots}_{\text{recorded}} \nearrow$$

pre-computed chain regeneration :

$$\mathrm{SP}_2 = \circ \xrightarrow{F} \circ \cdots \acute{x} \xrightarrow{F} \circ$$

The Parallel DP Tradeoff(The pD Tradeoff)

Variant of the DP tradeoff (Hoch, Shamir 09),

- A full record of the online chain is maintained during the online phase,
- The DP tables processed in parallel, rather than serially.

Most case : false alarm

$$\mathrm{SP}_2 = \circ \xrightarrow{F} \cdots \quad \acute{x} \xrightarrow{F} \circ \xrightarrow{F} \circ \quad \cdots \quad \xrightarrow{F} \bullet \cdots \xrightarrow{F} \overset{\text{alarm!!}}{\bullet} = \mathrm{EP}_2$$

$$x \xrightarrow{F} \underbrace{y \xrightarrow{F} \circ \quad \cdots}_{\text{recorded}} \nearrow$$

pre-computed chain regeneration :

$$\mathrm{SP}_2 = \circ \xrightarrow{F} \circ \cdots \acute{x} \xrightarrow{F} \circ \xrightarrow{F} \circ$$

The Parallel DP Tradeoff(The pD Tradeoff)

Variant of the DP tradeoff (Hoch, Shamir 09),

- A full record of the online chain is maintained during the online phase,
- The DP tables processed in parallel, rather than serially.

Most case : false alarm

$$\mathrm{SP}_2 = \circ \xrightarrow{F} \cdots \quad \acute{x} \xrightarrow{F} \circ \xrightarrow{F} \circ \quad \cdots \quad \xrightarrow{F} \bullet \cdots \xrightarrow{F} \overset{\text{alarm!!}}{\bullet} = \mathrm{EP}_2$$

$$x \xrightarrow{F} \underbrace{y \xrightarrow{F} \circ \quad \cdots}_{\text{recorded}} \nearrow$$

pre-computed chain regeneration :

$$\mathrm{SP}_2 = \circ \xrightarrow{F} \circ \cdots \acute{x} \xrightarrow{F} \circ \xrightarrow{F} \circ \cdots \xrightarrow{F}$$

The Parallel DP Tradeoff(The pD Tradeoff)

Variant of the DP tradeoff (Hoch, Shamir 09),

- A full record of the online chain is maintained during the online phase,
- The DP tables processed in parallel, rather than serially.

Most case : false alarm

$$\mathrm{SP}_2 = \circ \xrightarrow{F} \cdots \quad \acute{x} \xrightarrow{F} \circ \xrightarrow{F} \circ \quad \cdots \quad \xrightarrow{F} \bullet \cdots \xrightarrow{F} \overset{\text{alarm!!}}{\bullet} = \mathrm{EP}_2$$

$$x \xrightarrow{F} \underbrace{y \xrightarrow{F} \circ \quad \cdots}_{\text{recorded}}$$

pre-computed chain regeneration :

$$\mathrm{SP}_2 = \circ \xrightarrow{F} \circ \cdots \acute{x} \xrightarrow{F} \circ \xrightarrow{F} \circ \cdots \xrightarrow{F} \bullet$$

The Parallel DP Tradeoff(The pD Tradeoff)

Variant of the DP tradeoff (Hoch, Shamir 09),

- A full record of the online chain is maintained during the online phase,
- The DP tables processed in parallel, rather than serially.

Most case : false alarm

$$\mathrm{SP}_2 = \circ \xrightarrow{F} \cdots \quad \acute{x} \xrightarrow{F} \circ \xrightarrow{F} \circ \quad \cdots \quad \xrightarrow{F} \bullet \cdots \xrightarrow{F} \overset{\text{alarm!!}}{\bullet} = \mathrm{EP}_2$$

$$x \xrightarrow{F} \underbrace{y \xrightarrow{F} \circ \quad \cdots}_{\text{recorded}}$$

pre-computed chain regeneration :

$$\mathrm{SP}_2 = \circ \xrightarrow{F} \circ \cdots \; \acute{x} \xrightarrow{F} \circ \xrightarrow{F} \circ \cdots \xrightarrow{F} \bullet$$

(Recall : In the original DP tradeoff,

$$\mathrm{SP}_2 = \circ \xrightarrow{F} \cdots \quad \acute{x} \xrightarrow{F} \circ \xrightarrow{F} \circ \cdots \xrightarrow{F} \bullet \cdots \xrightarrow{F} \quad \bullet \quad = \mathrm{EP}_2 \;)$$

The Parallel DP Tradeoff(The pD Tradeoff)

Variant of the DP tradeoff (Hoch, Shamir 09),

- A full record of the online chain is maintained during the online phase,
- The DP tables processed in parallel, rather than serially.

[the original DP tradeoff] In the online phase,

The Parallel DP Tradeoff(The pD Tradeoff)

Variant of the DP tradeoff (Hoch, Shamir 09),

- A full record of the online chain is maintained during the online phase,
- The DP tables processed in parallel, rather than serially.

[the original DP tradeoff] In the online phase,

- 1st DP table

$$y \xrightarrow{1} \circ \xrightarrow{2} \circ \xrightarrow{3} \circ \xrightarrow{4} \cdots \xrightarrow{s} \text{DP}$$

- 2nd DP table

$$y \xrightarrow{s+1} \circ \xrightarrow{s+2} \cdots$$

- 3rd DP table

$$\vdots$$

- t-th DP table

The Parallel DP Tradeoff(The pD Tradeoff)

Variant of the DP tradeoff (Hoch, Shamir 09),

- A full record of the online chain is maintained during the online phase,
- The DP tables processed in parallel, rather than serially.

[the original DP tradeoff] In the online phase,

- 1st DP table

$$y \xrightarrow{1} \circ \xrightarrow{2} \circ \xrightarrow{3} \circ \xrightarrow{4} \cdots \xrightarrow{s} \text{DP}$$

- 2nd DP table

$$y \xrightarrow{s+1} \circ \xrightarrow{s+2} \cdots$$

- 3rd DP table

$$\vdots$$

- t-th DP table

The Parallel DP Tradeoff(The pD Tradeoff)

Variant of the DP tradeoff (Hoch, Shamir 09),

- A full record of the online chain is maintained during the online phase,
- The DP tables processed in parallel, rather than serially.

[the original DP tradeoff] In the online phase,

- 1st DP table

$$y \xrightarrow{1} \circ \xrightarrow{2} \circ \xrightarrow{3} \circ \xrightarrow{4} \cdots \xrightarrow{s} \text{DP}$$

- 2nd DP table

$$y \xrightarrow{s+1} \circ \xrightarrow{s+2} \cdots$$

- 3rd DP table

$$\vdots$$

- t-th DP table

The Parallel DP Tradeoff(The pD Tradeoff)

Variant of the DP tradeoff (Hoch, Shamir 09),

- A full record of the online chain is maintained during the online phase,
- The DP tables processed in parallel, rather than serially.

[the original DP tradeoff] In the online phase,

- 1st DP table

$$y \xrightarrow{1} \circ \xrightarrow{2} \circ \xrightarrow{3} \circ \xrightarrow{4} \cdots \xrightarrow{s} \text{DP}$$

- 2nd DP table

$$y \xrightarrow{s+1} \circ \xrightarrow{s+2} \cdots$$

- 3rd DP table

$$\vdots$$

- t-th DP table

The Parallel DP Tradeoff(The pD Tradeoff)

Variant of the DP tradeoff (Hoch, Shamir 09),

- A full record of the online chain is maintained during the online phase,
- The DP tables processed in parallel, rather than serially.

[the parallel DP tradeoff] In the online phase,

The Parallel DP Tradeoff(The pD Tradeoff)

Variant of the DP tradeoff (Hoch, Shamir 09),

- A full record of the online chain is maintained during the online phase,
- The DP tables processed in parallel, rather than serially.

[the parallel DP tradeoff] In the online phase,

- 1st DP table

$$y \xrightarrow{1} \circ \xrightarrow{t+1} \circ \cdots$$

- 2nd DP table

$$y \xrightarrow{2} \circ \xrightarrow{t+2} \circ \cdots$$

- 3rd DP table

$$y \xrightarrow{3} \circ \xrightarrow{t+3} \circ \cdots$$

$$\vdots$$

- t-th DP table

$$y \xrightarrow{t} \circ \xrightarrow{t+t} \circ \cdots$$

The Parallel DP Tradeoff(The pD Tradeoff)

Variant of the DP tradeoff (Hoch, Shamir 09),

- A full record of the online chain is maintained during the online phase,
- The DP tables processed in parallel, rather than serially.

[the parallel DP tradeoff] In the online phase,

- 1st DP table

$$y \xrightarrow{1} \circ \xrightarrow{t+1} \circ \cdots$$

- 2nd DP table

$$y \xrightarrow{2} \circ \xrightarrow{t+2} \circ \cdots$$

- 3rd DP table

$$y \xrightarrow{3} \circ \xrightarrow{t+3} \circ \cdots$$

$$\vdots$$

- t-th DP table

$$y \xrightarrow{t} \circ \xrightarrow{t+t} \circ \cdots$$

The Parallel DP Tradeoff(The pD Tradeoff)

Variant of the DP tradeoff (Hoch, Shamir 09),

- A full record of the online chain is maintained during the online phase,
- The DP tables processed in parallel, rather than serially.

[the parallel DP tradeoff] In the online phase,

- 1st DP table

$$y \stackrel{1}{\to} \circ \stackrel{t+1}{\to} \circ \cdots$$

- 2nd DP table

$$y \stackrel{2}{\to} \circ \stackrel{t+2}{\to} \circ \cdots$$

- 3rd DP table

$$y \stackrel{3}{\to} \circ \stackrel{t+3}{\to} \circ \cdots$$

$$\vdots$$

- t-th DP table

$$y \stackrel{t}{\to} \circ \stackrel{t+t}{\to} \circ \cdots$$

The Parallel DP Tradeoff(The pD Tradeoff)

Variant of the DP tradeoff (Hoch, Shamir 09),

- A full record of the online chain is maintained during the online phase,
- The DP tables processed in parallel, rather than serially.

[the parallel DP tradeoff] In the online phase,

- 1st DP table

$$y \xrightarrow{1} \circ \xrightarrow{t+1} \circ \cdots$$

- 2nd DP table

$$y \xrightarrow{2} \circ \xrightarrow{t+2} \circ \cdots$$

- 3rd DP table

$$y \xrightarrow{3} \circ \xrightarrow{t+3} \circ \cdots$$

$$\vdots$$

- t-th DP table

$$y \xrightarrow{t} \circ \xrightarrow{t+t} \circ \cdots$$

The Parallel DP Tradeoff(The pD Tradeoff)

Variant of the DP tradeoff (Hoch, Shamir 09),

- A full record of the online chain is maintained during the online phase,
- The DP tables processed in parallel, rather than serially.

[the parallel DP tradeoff] In the online phase,

- 1st DP table

$$y \xrightarrow{1} \circ \xrightarrow{t+1} \circ \cdots$$

- 2nd DP table

$$y \xrightarrow{2} \circ \xrightarrow{t+2} \circ \cdots$$

- 3rd DP table

$$y \xrightarrow{3} \circ \xrightarrow{t+3} \circ \cdots$$

$$\vdots$$

- t-th DP table

$$y \xrightarrow{t} \circ \xrightarrow{t+t} \circ \cdots$$

The Parallel DP Tradeoff(The pD Tradeoff)

Variant of the DP tradeoff (Hoch, Shamir 09),

- A full record of the online chain is maintained during the online phase,
- The DP tables processed in parallel, rather than serially.

[the parallel DP tradeoff] In the online phase,

- 1st DP table

$$y \xrightarrow{1} \circ \xrightarrow{t+1} \circ \cdots$$

- 2nd DP table

$$y \xrightarrow{2} \circ \xrightarrow{t+2} \circ \cdots$$

- 3rd DP table

$$y \xrightarrow{3} \circ \xrightarrow{t+3} \circ \cdots$$

$$\vdots$$

- t-th DP table

$$y \xrightarrow{t} \circ \xrightarrow{t+t} \circ \cdots$$

The Parallel DP Tradeoff(The pD Tradeoff)

Variant of the DP tradeoff (Hoch, Shamir 09),

- A full record of the online chain is maintained during the online phase,
- The DP tables processed in parallel, rather than serially.

[the parallel DP tradeoff] In the online phase,

- 1st DP table

$$y \xrightarrow{1} \circ \xrightarrow{t+1} \circ \cdots$$

- 2nd DP table

$$y \xrightarrow{2} \circ \xrightarrow{t+2} \circ \cdots$$

- 3rd DP table

$$y \xrightarrow{3} \circ \xrightarrow{t+3} \circ \cdots$$

$$\vdots$$

- t-th DP table

$$y \xrightarrow{t} \circ \xrightarrow{t+t} \circ \cdots$$

The Parallel DP Tradeoff(The pD Tradeoff)

Variant of the DP tradeoff (Hoch, Shamir 09),

- A full record of the online chain is maintained during the online phase,
- The DP tables processed in parallel, rather than serially.

[the parallel DP tradeoff] In the online phase,

- 1st DP table

$$y \stackrel{1}{\to} \circ \stackrel{t+1}{\to} \circ \cdots$$

- 2nd DP table

$$y \stackrel{2}{\to} \circ \stackrel{t+2}{\to} \circ \cdots$$

- 3rd DP table

$$y \stackrel{3}{\to} \circ \stackrel{t+3}{\to} \circ \cdots$$

$$\vdots$$

- t-th DP table

$$y \stackrel{t}{\to} \circ \stackrel{t+t}{\to} \circ \cdots$$

The pD Tradeoff : the online time complexity

$$\boxed{mt^2 = \mathtt{D}_{msc} N}$$

The pD Tradeoff : the online time complexity

$$\boxed{mt^2 = \mathtt{D}_{msc} N}$$

- The **online chain creation** of the pD Tradeoff require

$$t^2 \frac{\mathtt{D}_{ps}}{\mathtt{D}_{msc}\mathtt{D}_{cr}}$$

invocations of F.

The pD Tradeoff : the online time complexity

$$\boxed{mt^2 = \mathtt{D}_{msc}N}$$

- The **online chain creation** of the pD Tradeoff require

  $$t^2 \frac{\mathtt{D}_{ps}}{\mathtt{D}_{msc}\mathtt{D}_{cr}}$$

  invocations of F.

- The number of iterations required by the pD tradeoff in **dealing with alarms** is

  $$t^2 \frac{\ln(1-\mathtt{D}_{ps})}{\mathtt{D}_{cr}} \int_0^1 (1-\mathtt{D}_{ps})^{1-u} \ln u \; du.$$

The pD Tradeoff : the tradeoff curve

$$\boxed{mt^2 = \mathtt{D}_{msc}N}$$

T=the total online time complexity

M= storage size

The pD Tradeoff : the tradeoff curve

$$\boxed{mt^2 = \mathtt{D}_{msc} N}$$

T=the total online time complexity

M= storage size

The *time memory tradeoff curve* for the pD tradeoff is $\mathrm{TM}^2 = \mathtt{pD}_{tc} N^2$,

where

$$\mathtt{pD}_{tc} = \Big(\frac{\ln(1-\mathtt{D}_{ps})}{\mathtt{D}_{ps}} \int_0^1 (1-\mathtt{D}_{ps})^{1-u} \ln u \; du + \frac{1}{\mathtt{D}_{msc}}\Big) \frac{1}{\mathtt{D}_{cr}^3} \mathtt{D}_{ps} \{\ln(1-\mathtt{D}_{ps})\}^2.$$

The pD Tradeoff : the tradeoff curve

$$\boxed{mt^2 = \mathtt{D}_{msc} N}$$

T=the total online time complexity

M= storage size

The *time memory tradeoff curve* for the pD tradeoff is $\mathrm{TM}^2 = \mathtt{pD}_{tc} N^2$,

where

$$\mathtt{pD}_{tc} = \Big(\frac{\ln(1-\mathtt{D}_{ps})}{\mathtt{D}_{ps}} \int_0^1 (1-\mathtt{D}_{ps})^{1-u} \ln u \; du + \frac{1}{\mathtt{D}_{msc}} \Big) \frac{1}{\mathtt{D}_{cr}^3} \mathtt{D}_{ps} \{\ln(1-\mathtt{D}_{ps})\}^2.$$

- Recall : In the original DP tradeoff,

$$\mathtt{D}_{tc} = (\qquad 2 \qquad + \frac{1}{\mathtt{D}_{msc}}) \frac{1}{\mathtt{D}_{cr}^3} \mathtt{D}_{ps} \{\ln(1-\mathtt{D}_{ps})\}^2.$$

pD versus DP

Since

$$\frac{\ln(1-\mathtt{D}_{ps})}{\mathtt{D}_{ps}} \int_0^1 (1-\mathtt{D}_{ps})^{1-u} \ln u \; du < 1 < 2,$$

$$\text{DP} < \text{pD}$$

the pD tradeoff will outperform the original DP tradeoff.

pD versus Rainbow

- $\mathtt{X}_{tc} = \frac{TM^2}{N^2}$ is a measure of how efficiently the algorithm balances online time against storage requirements.
  - A smaller $\mathtt{X}_{tc}$ implies a more efficient tradeoff.
- However, a better tradeoff efficiency usually requires a higher pre-computation cost and is not always desirable in practice.

$\Rightarrow$ We have to consider both $\mathtt{X}_{tc}$ and $\mathtt{X}_{pc}$ for comparison.

pD versus Rainbow

- $\mathtt{X}_{tc} = \frac{TM^2}{N^2}$ is a measure of how efficiently the algorithm balances online time against storage requirements.
  - A smaller $\mathtt{X}_{tc}$ implies a more efficient tradeoff.
- However, a better tradeoff efficiency usually requires a higher pre-computation cost and is not always desirable in practice.

$\Rightarrow$ We have to consider both $\mathtt{X}_{tc}$ and $\mathtt{X}_{pc}$ for comparison.

- In a fair manner, compare $\mathtt{D}_{tc}$ with $4\mathtt{R}_{tc}$, since $M_R = 2M_D$.

pD versus Rainbow

The pD tradeoff

$$\mathtt{pD}_{tc} = \Big(\frac{\ln(1-\mathtt{D}_{ps})}{\mathtt{D}_{ps}}\int_0^1 (1-\mathtt{D}_{ps})^{1-u}\ln u\ du + \frac{1}{\mathtt{D}_{msc}}\Big)\frac{1}{\mathtt{D}_{cr}^3}\mathtt{D}_{ps}\{\ln(1-\mathtt{D}_{ps})\}^2$$

The rainbow method[HM10]

$$\mathtt{R}_{tc} = \tfrac{l^3}{(2l+1)(2l+2)(2l+3)}\Big(\{(2l-1)+(2l+1)\mathtt{R}_{msc}\}(2+\mathtt{R}_{msc})^2$$
$$-4\{(2l-1)+l(2l+3)\mathtt{R}_{msc}\}\big(\tfrac{2}{2+\mathtt{R}_{msc}}\big)^{2l}\Big)$$

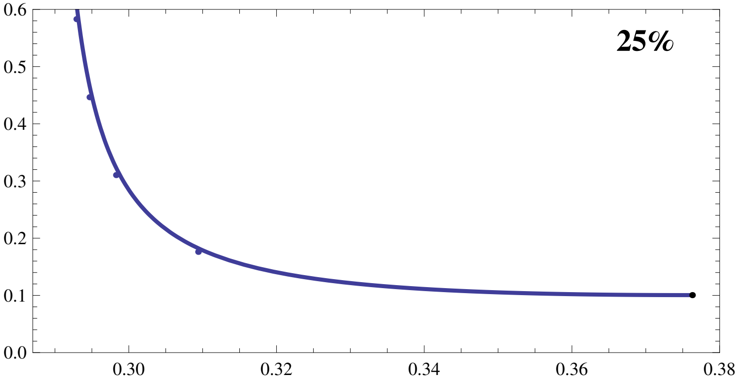
,where

$$\mathtt{R}_{ps} = 1-\Big(\frac{2}{2+\mathtt{R}_{msc}}\Big)^{2l},\ \mathtt{D}_{ps} = 1-e^{-\mathtt{D}_{cr}\mathtt{D}_{pc}}.$$

pD versus Rainbow

$\boxed{\mathtt{D}_{pc} : \mathtt{pD}_{tc} \,,\, \mathtt{R}_{pc} : 4\mathtt{R}_{tc}}$

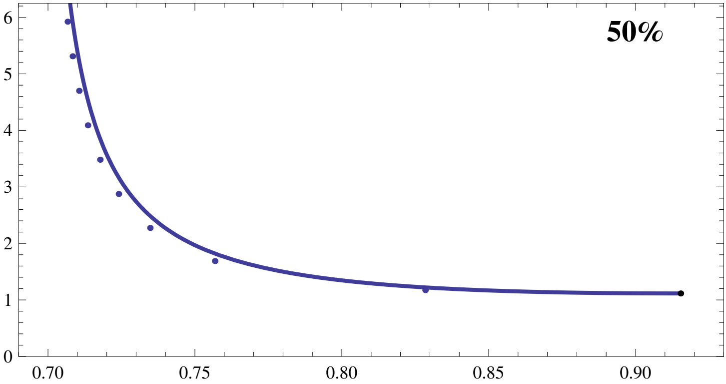
Figure: the pD(line) and the rainbow(bullet)



pD versus Rainbow

$\mathtt{D}_{pc} : \mathtt{pD}_{tc}$, $\mathtt{R}_{pc} : 4\mathtt{R}_{tc}$

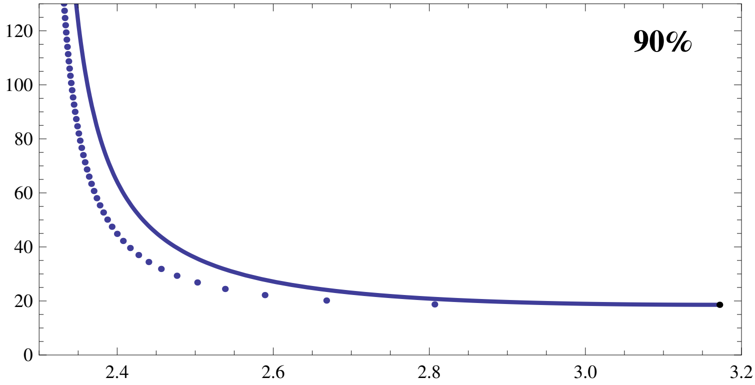
Figure: the pD(line) and the rainbow(bullet)



pD versus Rainbow

$\mathtt{D}_{pc} : \mathtt{pD}_{tc}$, $\mathtt{R}_{pc} : 4\mathtt{R}_{tc}$

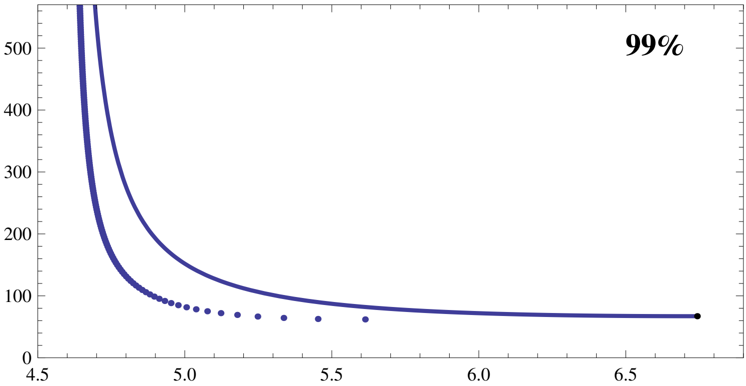
Figure: the pD(line) and the rainbow(bullet)



pD versus Rainbow

D_{pc} : pD_{tc} , R_{pc} : $4R_{tc}$

Figure: the pD(line) and the rainbow(bullet)



Conclusion

- There are two added conditions in the pD in comparison with the DP.
  - online chain record
  - parallel processing

  $\Rightarrow$ In the online phase, cost for resolving alarms is reduced more than half.
- The pD tradeoff is not likely to be preferable over the rainbow method under most situations.
- The only exception is when the success rate requirement is very low.
  - example. multi-target time memory tradeoff