dC d Dff s
g h s f v s dd s s

National University of Singapore, School of o p ting
S5322 Databases Sec rity - 2009/2010 (Se ester 2) - Project eport

attanak UN
00 2 0N
NUS - So , Singapore
S pélec, rance
a00 2 0 n s e sg

Da ien S
00 2
NUS - So , Singapore
S pélec, rance
a00 2 n s e sg

onika
00 2
NUS - So , Singapore
a00 2 n s e sg

Yann-Lo p P N
V N S N
00 23
NUS - So , Singapore
S pélec, rance
a00 23 n s e sg

ABSTRACT

or the Dat abases Sec rity project, e choose to ake a Java i ple entation of the sol tions sho e in [ ] he context of this paper is the classic para ig of atabase o tso rcing an privacy threats r paper provi es so e explanations of [ ] an of o r choices of i ple entation

atabase, sec rity, privacy, encryption, q ery, in ex, java, ery- pti al- cketi ation, ontrolle -Diff sion, attack

1. THE ORIGINAL PAPER

n this section e ill q ickly intro ce the notions presente in [ ] e a vice the rea er to refer at least to the *table 1: Notation o Bucket* of [4] 722. mor r n *ection 3* r our m m n on.

1.1

[3, 1], v cy c y v . [4] . c

paper a e on e work of [4].
paper a 9 page .
Ver on of pr 12, 2010.

n [1, 3, 4] e n e e o ake a opera on on en r p e pe .

par on an en e e of ke a are repre en e e n e e . e o rea e prva on an en ve o n of e rea on w are e o ake e a opera on a ee on . n e a pe g ven e ow:

Example 1. [1] *table 1* 1)

d	*Name*		*One*	*wo*
23			70	0
860			60	80
320			50	50
875			55	110

1: **f h**

f m w . yp (f. *table 2*

upl		*O*	*wo*
100101010..		1	
101101110..			
101010010..			
111101100..			

2: **f h**

When you look he en y e le he only h n h you n u e e he u on of he u le n o he ffe

h ex m le e l ely n e f om he *example 1* [4] nd *e* 2 [3] nd

o m o s

s o os w os of
o m s.

1.2

Two o e e e w e e o o e T e
-*Op* - *ck* (*O*) c .
c
.
[3], w w ,
y *O* c
[1].

c w cy
, c y w y c w
. - ( ) c
c
. c
c c ( ).

1.3

[4]
w
(q y v y. F
y
v y.

v y *5.2* 5) dis-
c v r ur v rsi n f s ri n s

2.

Today o a o oa a o o
a d o y o a y a a o d a o o d d a a a
o o a d o a a a y w d a a
a a d d o a y a o o a
o a a a a o o d o o o
d a a o a o

y o a y o d o o d a a a d
d o o y d o a o
o w a a a a o d a o a y y
o o a o a A a o d a a a
w a y a d y

2.1

T o o o a w o d

y Mo a o

T o o o a a a y z a o w a a
o o d a a a o y o o a
a a d a Fo a a w
o o o o wo a od
a y a z a o o a O o a d
o a o d o a [4]
y o d a a o d a a o o
a y a d y a

O o a o d a a a o H w a
a a a y o a o a o a
o a d a d o o a
d a a o wo a d a a T a a w
o d y z H o d w a
o o d d o o a y a o o
d o a d a a a

2.2

O o a o o o a o a a a
od o a d a a a a d o o wo
a o d [4] w y o o d a a
o a d [4]

a o w a o o a y a a a o
o y d a A o d o a o o
a a [4] w w d o
a d d w o d o a
o a o d a o w wo
a o d o o o a o w o a a

A o a a a o o a a z a o
o *QOB* for o r y lo o r
l r c r v .

3. OUR O

3.1

J
k
(f [2]) k M f
f
k (f [6]) k k
J [5] J
f f [2]

3.1.1

a a p
p k a a f a
f a a p k a f f
a 5 p f f a a
p f [6]

p a p f p f [7] ak a
f a a : a
p a f a
k p a a a p a a
a a k

3.1.2 JU t

a f a k f a a a
a a a k
f k a a p f a
p p p a p
a f *A.2* pa 9 f f a
a a a

3.2 a a a a

3.2.1

to t t your u r t r r to *1*[4]
3) r r t r r o our

you obj t-or t ro r , you y o
b uty our o , t t o.
[3]our SVN t)
tt r . roj to r. o 3
[4] r o t r b t
t , t o t br ry.

o
m o s

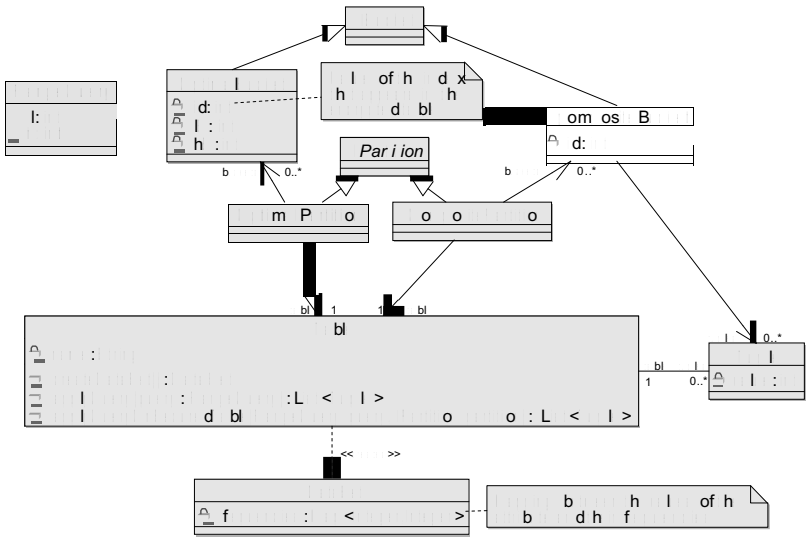


Figure 1: Our ir i e e i : i g e ri u e

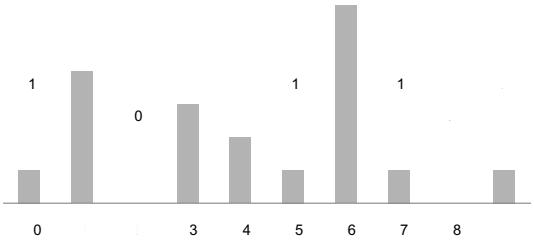


Figure 2: e for our e

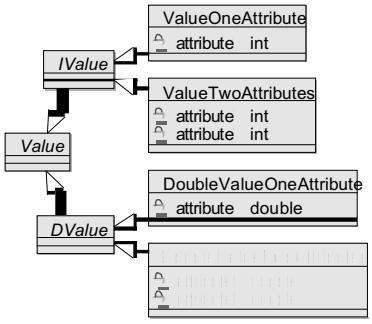


Figure 3: e u gr e f r ri u e

frs model of e d se d of e e o e rre model s more omplex e se of e m l r e poss l es

3.2.2

m y f y 2[5] 3) f f

3.2.3 M l - b

f m m y f m m m f 3 3) m f m m y f m F y f m

Ex mpl 2. f f my =

[5] m f m f

s s

s f s ss s f 1)

3.3

order o perform ome me re o e e d o e p r o e e mpeme ed e d or rod ed [4]. o o r J p e d or e e e e d or d d or o e fo o me od . For more form o o e mpeme o of me od p e e refer o e J o of o r pro e or d re o o r ode.

o m o s

3.3.1 f

1. *3.2* o

TFP

$_T$ −

w ere

- *Q*: of ov *R*, o
- *R* : of f
- $_T$: of *R* d d z d o f *T* , d
- : d o o

TFP m fo of f o v , d v o f o

Fo m m o of o F o v , o m od o d o f f om d f om do d :

- e
- e n e e e

3.3.2 n ( )

n *2.* efne n *n 3.2* f [4], n e e e

P ——————1 − ——————
$_S$ $_S$

our o of *FP*, u r for r u r r o .

o o r o o *AQP* r u o ro u *Q* or *3.2* *3.3* of [4] 723

3.3.3 *Vara*

a r 3. f [10], r of r o r b k u , *n*] with corre-

, *n*] g ven

)^n
) × −))

e e) ^{n} ×

ed en n X e ne e e e lden n gene l e e d n e e een nd). g ve

)^n
) × −)

) a , *n*] are vectors.

A cass c way to wr te t s

E −E

o , o mod of d , o d v of dom v o fo m , ’ o , d m o o dom v o o dm o o dom v o o d o m o

3.3.4 *Devi io*

Fo m o d d *e io 5.2* 5 , d d d v o

i o 4. d f d d d v o *σ* of dom v oo of v :

σ

3.3.5 E opy

i o 5. d f d *e io 4.3* of [4], o of dom v d v o o d o *p*$_i$, *i* *n*] g ven

n ^{n} *p* × g$_2$ *p*

3.3.6 *E fE n (EE)* m en e ev e e - e me

6. *4.1* o *4.2* of [4]:

ASEE f b for ro o r of r bu o of u bu k B f r r N u o B, for u of *ASEE* b f :

) ^{t}) ×) × −)

n X nd v le ll e e d n e ele en e B P den e X l d n X g e ed v l e X

X nd v le n e n l e e en l n) P l d n X X g e ed v l e X

l dve e e e v l e nd ele en en e e B.

n e g l ng e e l l ve e *4.2* de ned n [4].

o m o s

1. a a
a a a d a f a d a a
)))) –

3.4 lg r hms

3.4.1 ( )
n

3.4.2 ( )

4. CONFRONTATION OF THE O UCK-ETI ATION

[4], ,
f f QOB
f x).
f , .

4.1 A

x . .
f).

f
x .
)
x
f f) f .

4.2 O r A A r (AA)

4.2.1 Principle

4.2.2 P e e

4.3 Our u u r ( )

4.3.1 Origin of n

Su oku k o u
w y w foun n u k u
Su oku . y w u u n of f nk
w n n x n u k o n o y on
n of o n x n u k .

You n njoy u oku n 3 5) you n
y n n 3 n o o
33 qu ... o you o u f .
f you y o u f you wo o
. . 0.5 o y o . o
n x fo u oku w know
ou on n foun .

You nfn ou on of u oku n
).

4.3.2 Principl

T o fo [9]

		8						
8								
			8					
							8	
				8				

T 3: r y, r

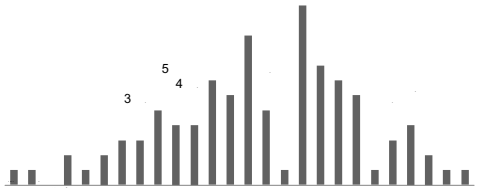


Figure 4: e genered n r r nd

4.3.3

5.

5.1

To conduct o xp ri nt n d data to i uat in or ation For our xp ri nt con id r t o ourc o in or ation hich ar od d by t o rando ariab o o in r p cti y

- Uniformly i ri
- orm lly i ri

2. f no *N* norm l i ri ion i m n n ri n ,

$$N \quad N\ 0\ 1$$

Wi i propri y, ily impl m n om f n ion r l i r n om l On fig r 4 p g 5 for 100 pl follo ing *N* 100 30 g n r l n p ion of 100 4 n ri n of 8 6 An on fig r 5 p g 6 for 1000 pl follo ing niform i ri ion for 0 99]

5.2

5.2.1

To of [4] o of
o o o of q :

Fo o fo o o o o o o
f o [8].

o
m o s

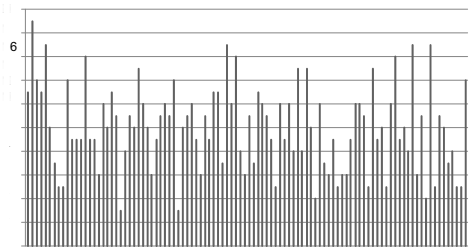


Figure 5: e genered uni r r nd

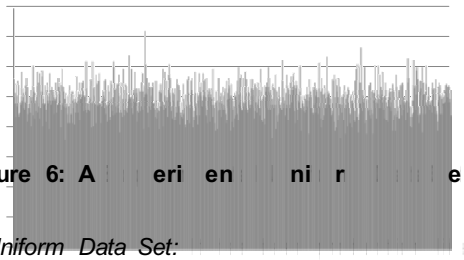


Figure 6: A eri en ni r e

. *Uniform Data Set:* 7.1 f [4] 728). 10^5 f [0 999]. Y - f f 6 6). f 500 f 83333.5.

2. *orma Data Set:* 10^5 f - w 500 83333.5). Y f f 7 6) [759 1880].

3. *Random Range Query Sets:* w ff f 100000 f). E f w f - .

4. *ist of arameters:* F w *QOB CD* f
   - *M* 100 150 200 250 300 350 400}
   - 2 4 6 8 10}

   f w w 7 35 .

5.2.2 ro edure

, w w , w . [4].

ff f *OutOfMemory rror*, w . A

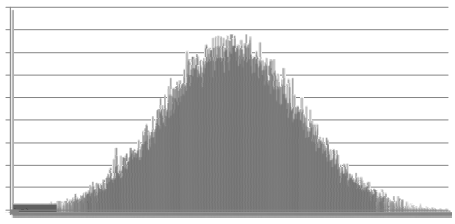


Figure 7: A eri e r e

problem e e o l l e e *AQP* fo o

o (fo o f o fo o o (O (fo o o o o o *O* (*M* 2

o o o o o f of o f q - of q of oo o w o w *O* (*M* o of *AQP*, w o o o

o o o

A m 1. o

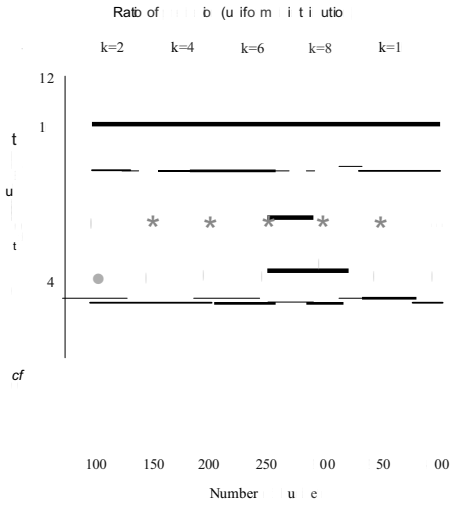
o of o of o of o q o o of B fo QOB o o of o - every *QOB*(M) on on of on every on on of on Co po

---

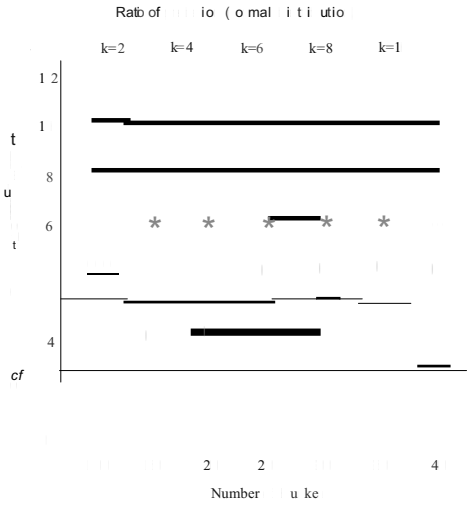
ur u r r

5.2.3

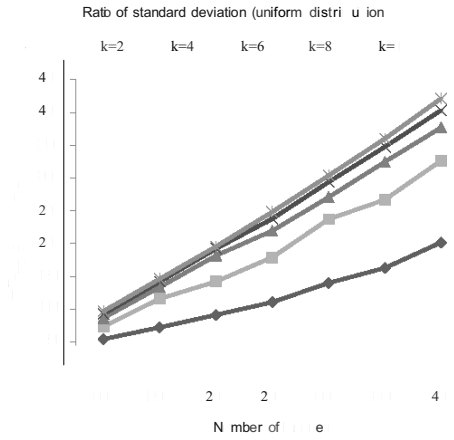
You may find our r u in a a d fi ma ri m n

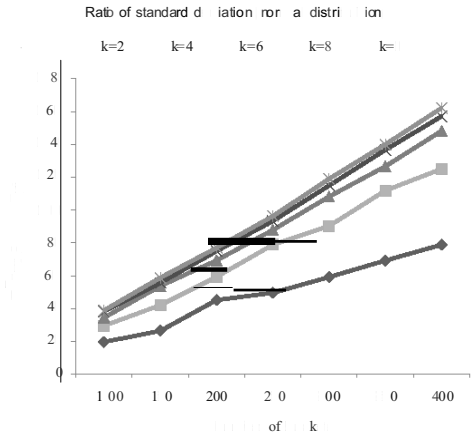


ure

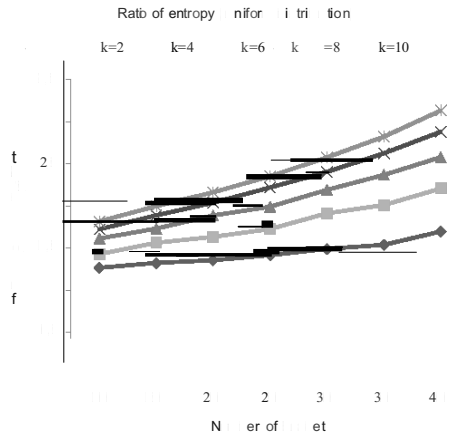


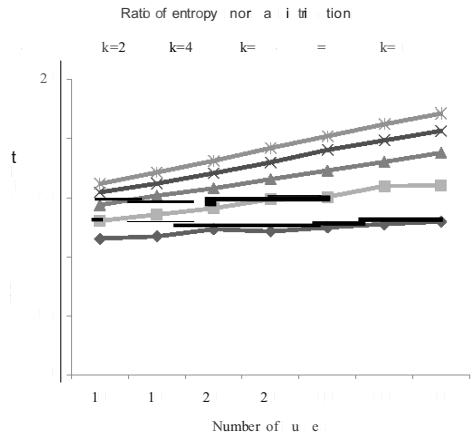
ure





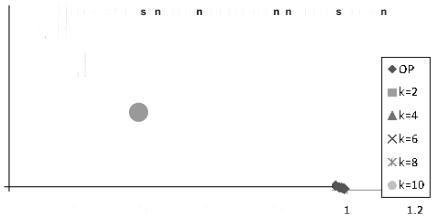
12



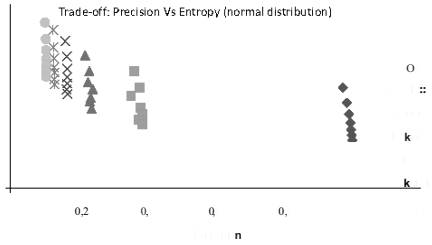


ure 1

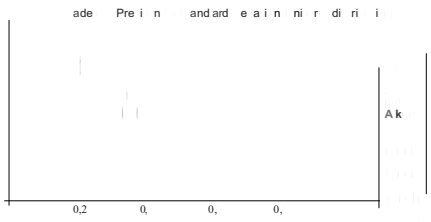
R S
R C U



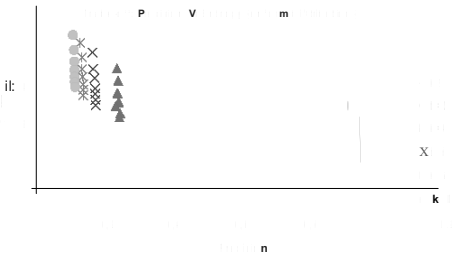
14:



15:



16:



17:

Trade-off

Time taken. *table* (pag s ows t o spo of t tim fo pa t of ou p im t fo t o ma ist i ut ta tota tim to u t u 57

f h	1 2 s
f s	68 s
f h B	45 s
f h s	18 s
f h s	12 s
f h 35 s	2.1
s s h	316 s
f s	1. s
f	1. s
s s f	45 s

4:

f h	s
f s	s
f h B	s
f h s	s
f h s	s
f h 35 s	
s s h	s
f s	s
f	s
s s f	s

5:

5.3

6. OU SOLU ION I N

7. CONCLUSIONS

pipo pipo ou p s c r nous ont est up ec on it p s ce u on dit et surtout on ne dit p s ce u on it En in re ceci c est un peu de contenu pour tester ise en p e *CQFD*, not t oo

8. REFERENCES

[1] E. S. . C. S. S. . S . C y y U

In *CCS f th Oth C f C t a at* N w N U A A www

H. H B. . L . . QL v

R S R C U

s Po Mo l. *SIGMOD f th ACM SIGMOD t t f M m t f t*, 216–227, N w York, NY, USA, 2 2 A
[4] B Hor , S hrotr , nd G d k A Pr v cy-Pr rv n nd for n Q r n *D f th h t th t t f y t*, 72 –7 1 VLDB ndow nt, 2 4
[5] Un t htt www nt or
[6] Pro ct Lock r htt www ro ct ock r co
[7] S c htt c t r or
[8] G n d tr t on htt nwk d or wk G n-d tr t on
[9] S dok htt nwk d or wk S dok
[1] V r nc - D cr t c htt nwk d or wk V r nc D cr t -c

APPENDIX

A. IN A A I N

[2] you m y f om b c uc o o l you u g ou J v o c f you v om ff cul you c co c u u g o o w kw y

A.1 P

To ll cl l f o [2]

To m o o c o cl

- *File New Java e*
- *eae e e i i e*: f r
- Write t e e rit in t e *Nam* (if ne - e r
- i on

f o re onfort e it i e nd i e o i t nt to do n o d t e ro e t dire t fro o r if o nt to do o e e e to o r ro e t o er o nt on [6].

A.2 JUnit

nit . . . yo can ownloa on [5] a a yo wan o

- on o *Path ath*
- on *a*
- C on *A t a JAR* nd on n do n o d d

Now you ou o run n or r o o o r on w you w n o run our o r or v n n *Run n*

B. SOLUTION OF THE SUDOKU

Here e f e d k e e 3 e

		4	6		8	9		
6				9			4	8
	9	8		4			6	
8		9		6		4		
4		6	8				9	
			9		4	8		6
9	6						8	4
	8		4		9	6		
	4			8	6			9

T 6: Th f h

k
D e re
k
Y -L P V