Pots de miel et Machine Virtuelle

Cédric Lauradoux

21 novembre 2005

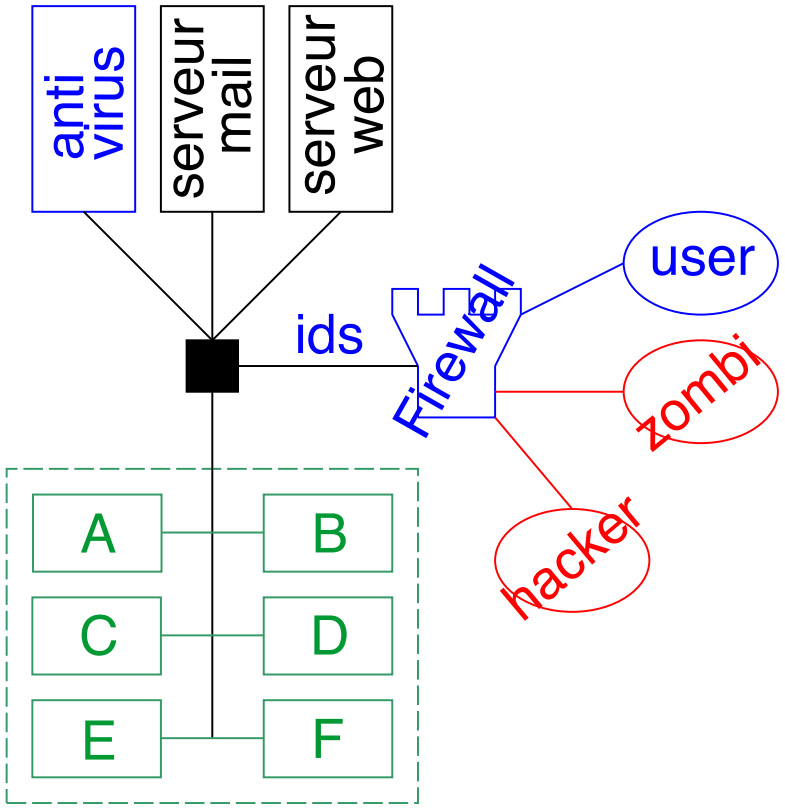
ACI UNIHAVEGE

Plan

- Introduction aux pots de miel
- Réalisation
- Détection
  - Processeur
  - Changement de contexte
- Conclusion

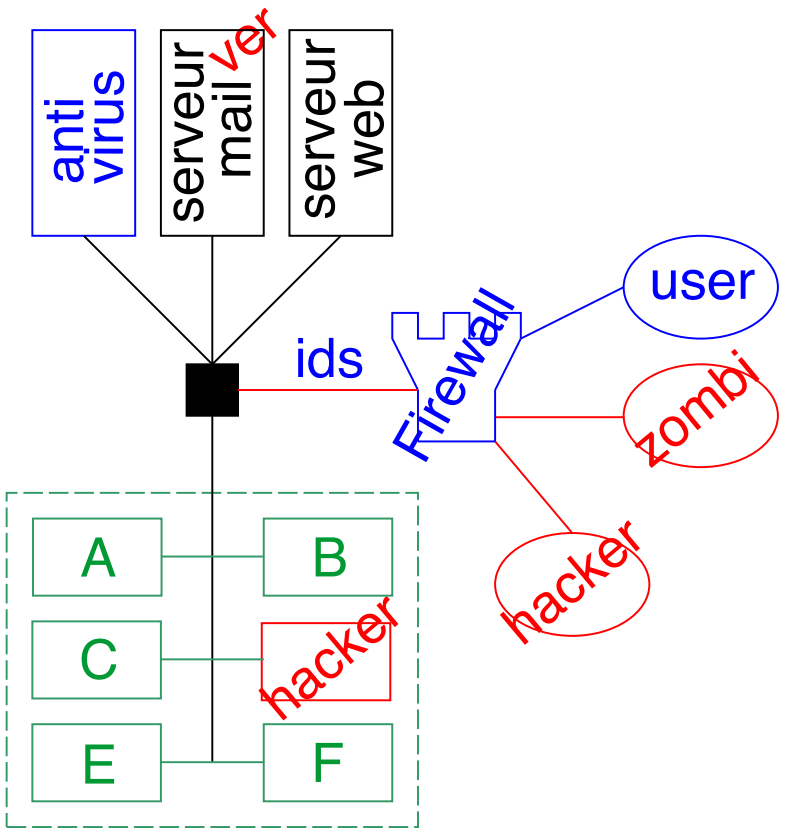
Introduction aux pots de miel

Sécurité



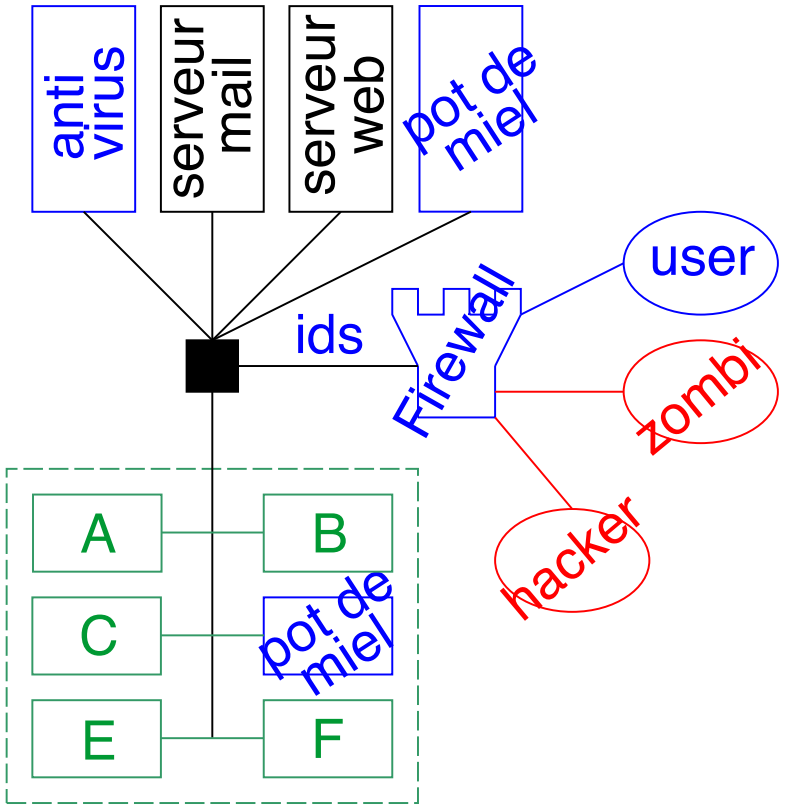
Introduction aux pots de miel

Intrusion



Introduction aux pots de miel

Intrusion



Introduction aux pots de miel

Fonctions

- Sonde de détection d'intrusion (aider ids)
- Observation de l'attaquant
- Test de logiciel

- 2 Familles **[SPIT 04]** :
  - Haut niveau d'interaction (HNI)
  - Bas niveau d'interaction (BNI)

Introduction aux pots de miel
HNI

- Pot de miel BNI : l'attaquant accède seulement à un service

Détection d'intrusion = Signal d'activité

- Pot de miel HNI : l'attaquant accède à une machine complète

Observation = Espionnage

Réalisation
Choix

- Machine physique
  - Ajouter des services espion [SEBEK]
  - Attaquant devient root = ROOTKIT
- Isolateur
  - Cloisonne les processus = impossiblité d'atteindre les droits de root
  - Pas de produits
- Virtualisation

Réalisation
Virtualisation

- Définition : création d'environnements indépendants sur une même machine
- Chaque environnement a son mode privilégié :

• une machine virtuelle émule le mode privilévigié d'un processeur

Réalisation
Virtualisation

- 2 familles :
  - processeur totalement émulé
  - processeur partiellement émulé

Détection
Objectif

Trouver ce qui ne va pas sur la machine.

- Processeur totalement émulé : chercher le processeur hôte
- Processeur partiellement émulé : chercher l'activité anormale

Processeur totalement émulé

Caractéristiques

Informations sur le processeur : *less /proc/cpuinfo*

```
processor       : 0
vendor_id       : GenuineIntel
cpu family      : 15
model            : 2
model name      : Intel(R) Pentium(R) 4 CPU 2.60GHz
stepping        : 9
cpu MHz         : 2593.533
cache size      : 512 KB
```

Existe t'il d'autres sources d'information ?

Processeur totalement émulé

Caractéristiques

- Jeu d'instructions
- Gestion mémoire
- Gestion interruption

} Emulation

- Antémémoires
- Branchements
- Latence

} Optimisation

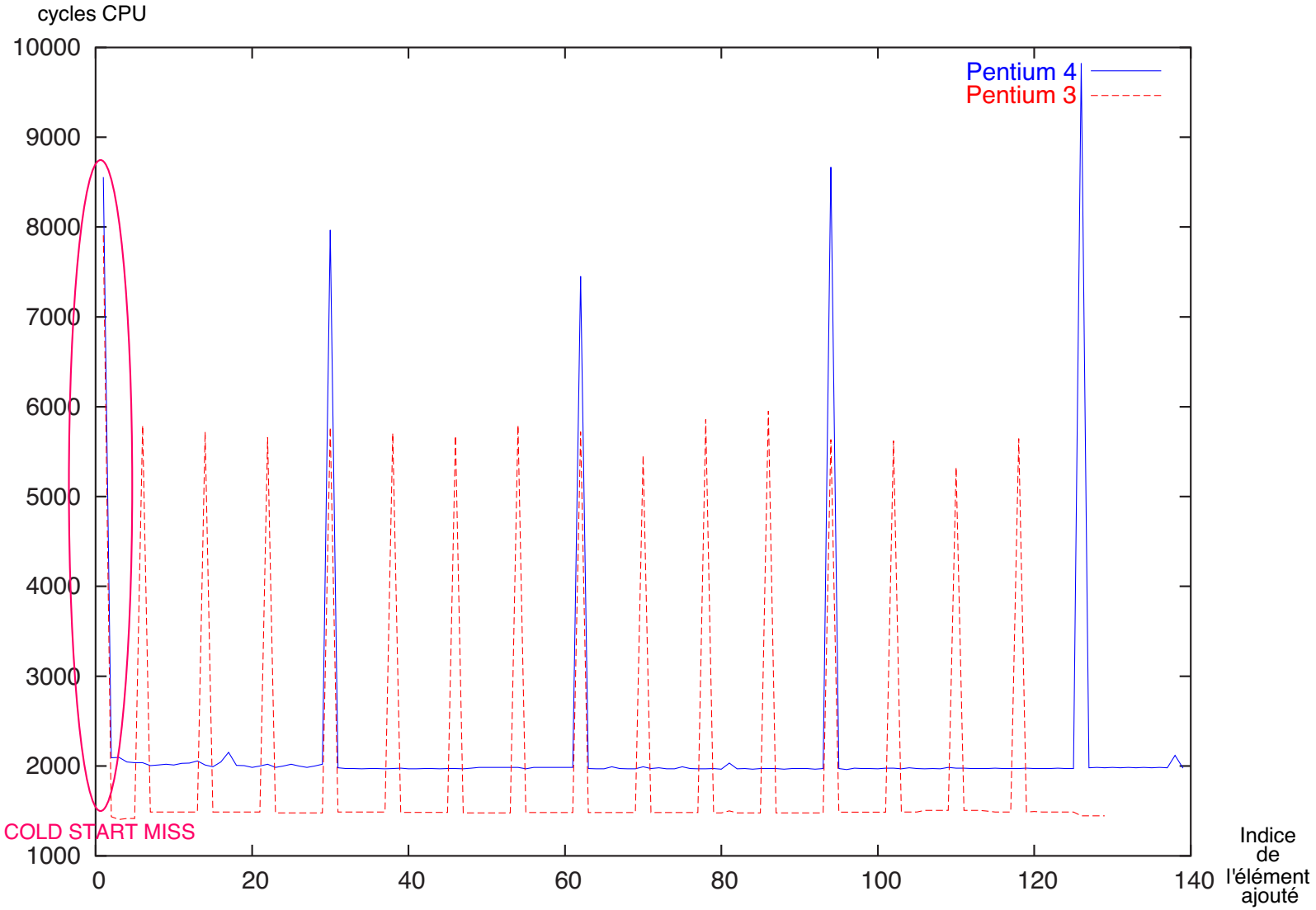
} Simulation

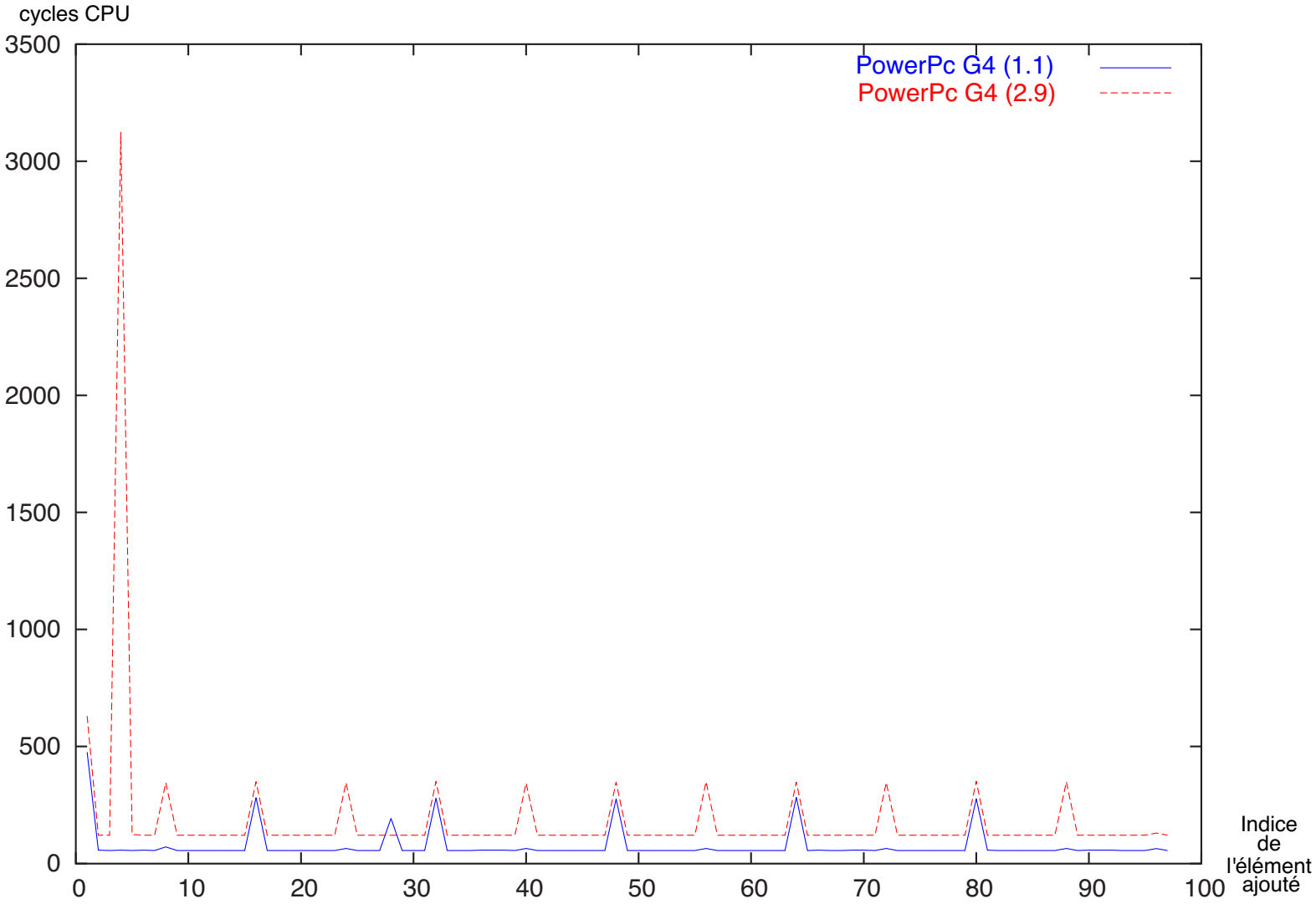
Processeur totalement émulé

Antémémoires

- Taille et taille des blocs
- Algorithme de placement
- Algorithme d'insertion (LRU)

} Rétro-ingénierie

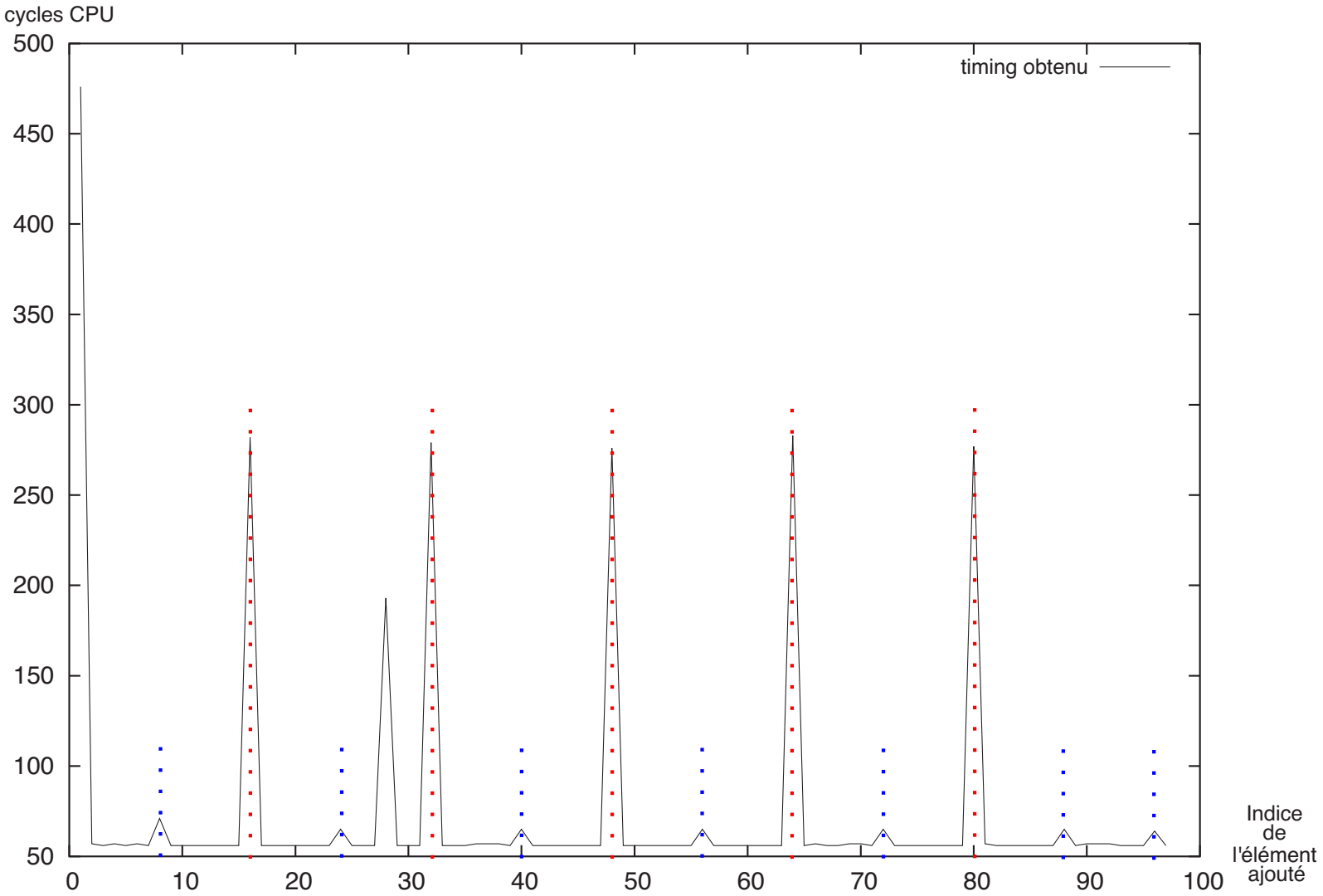

cycles CPU
10000
9000
8000
7000
6000
5000
4000
3000
2000
1000
0
20
40
60
80
100
120
140
Pentium 4
Pentium 3
COLD START MISS
Indice
de
l'élément
ajouté

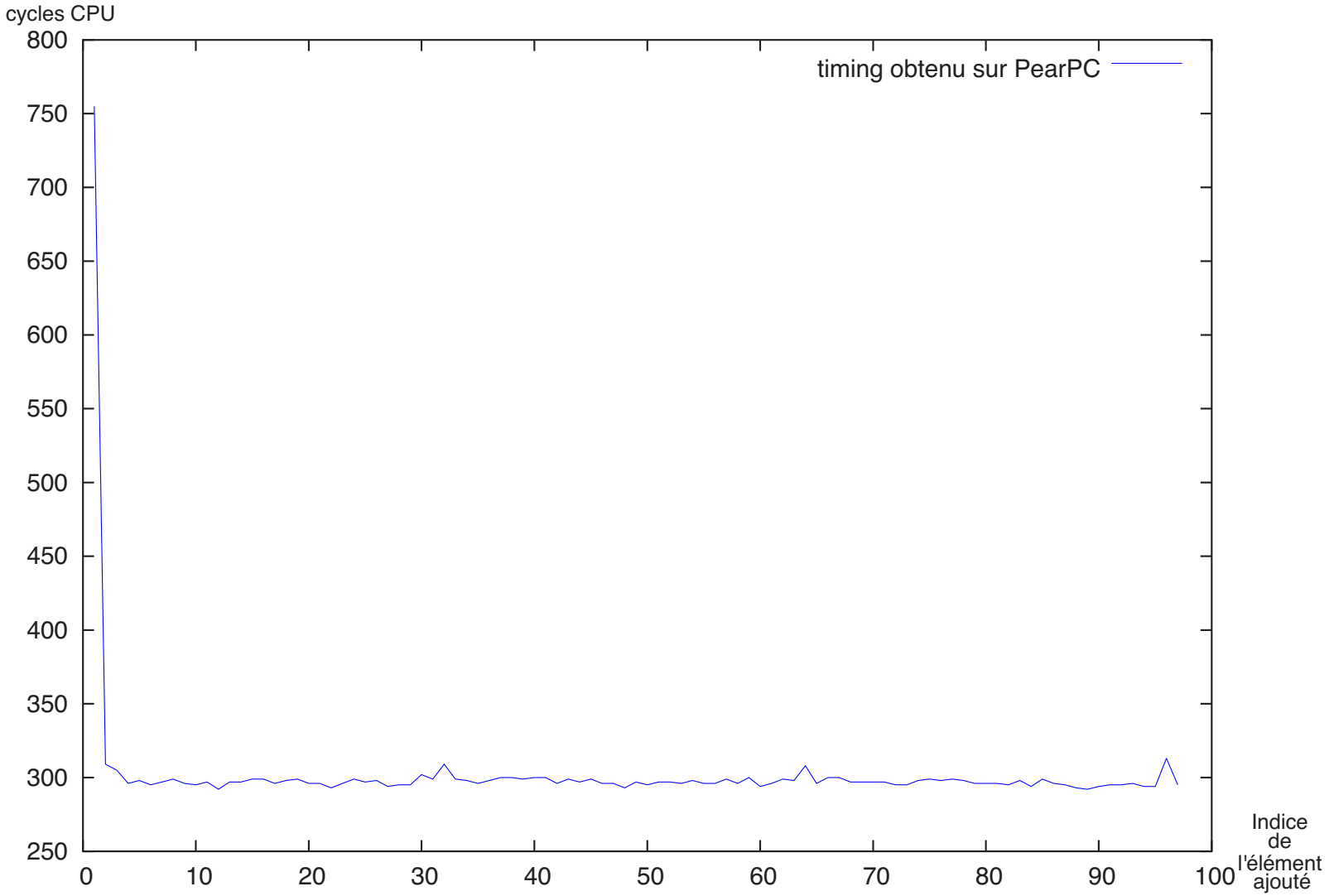

cycles CPU
3500
3000
2500
2000
1500
1000
500
0
0
10
20
30
40
50
60
70
80
90
100
Indice de l'élément ajouté
PowerPc G4 (1.1)
PowerPc G4 (2.9)

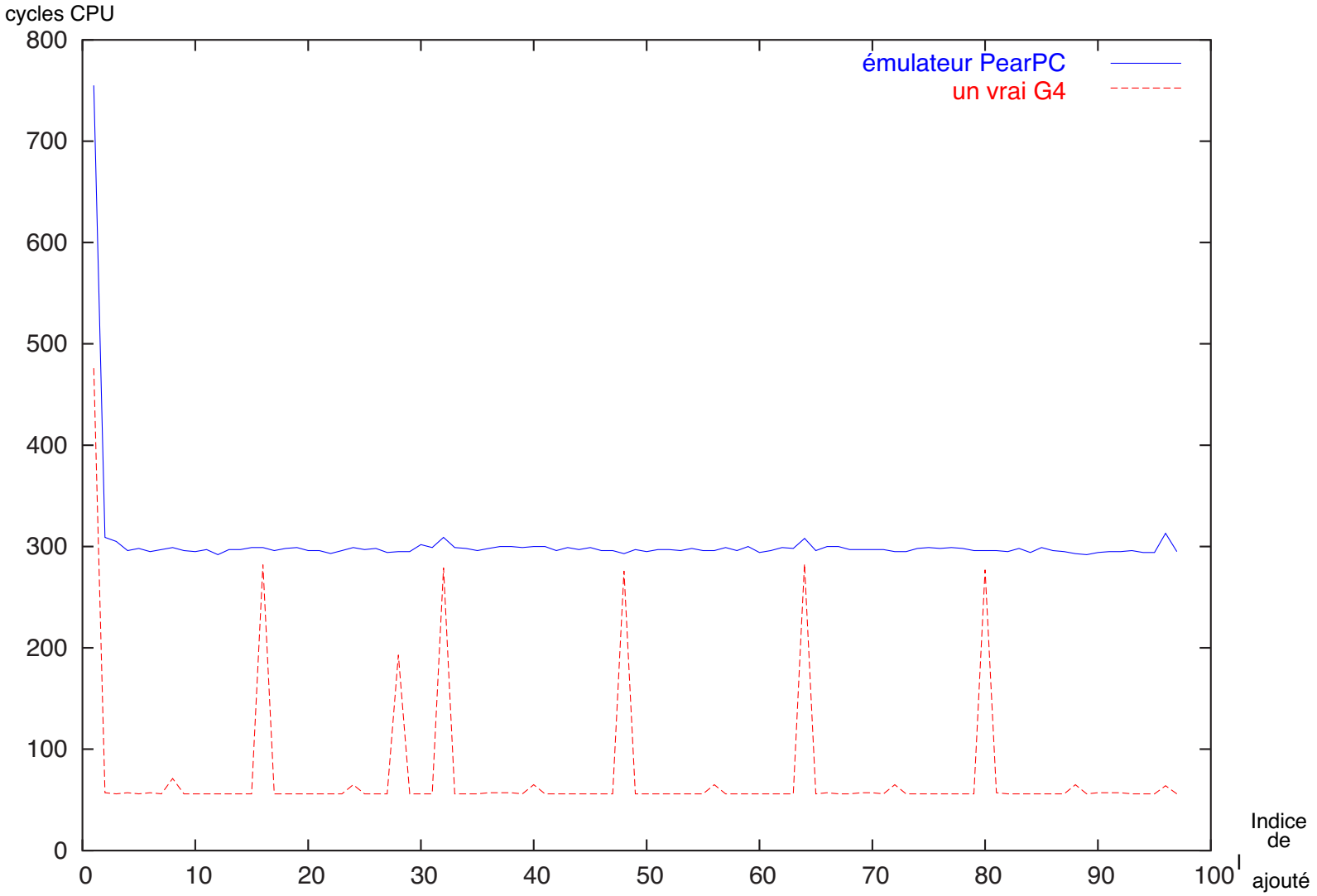
Processeur totalement émulé

Machine virtuelle et détection

Les paramêtres entre machine émulée et machine d'exécution sont souvent (toujours) différents.


cycles CPU
500
450
400
350
300
250
200
150
100
50
0
10
20
30
40
50
60
70
80
90
100
timing obtenu
Indice
de
l'élément
ajouté


cycles CPU
800
750
700
650
600
550
500
450
400
350
300
250
0
10
20
30
40
50
60
70
80
90
100
timing obtenu sur PearPC
Indice de l'élément ajouté


cycles CPU
800
700
600
500
400
300
200
100
0
émulateur PearPC
un vrai G4
0
10
20
30
40
50
60
70
80
90
100
Indice de l ajouté

Processeur totalement émulé
Conclusion

- On est capable de voir le processeur enfoui derrière l'émulateur
- Besoin de décorréler le compteur de cycle du processeur hôte et des processeurs émulés : difficile

Processeur partiellement émulé
Ordonnancement

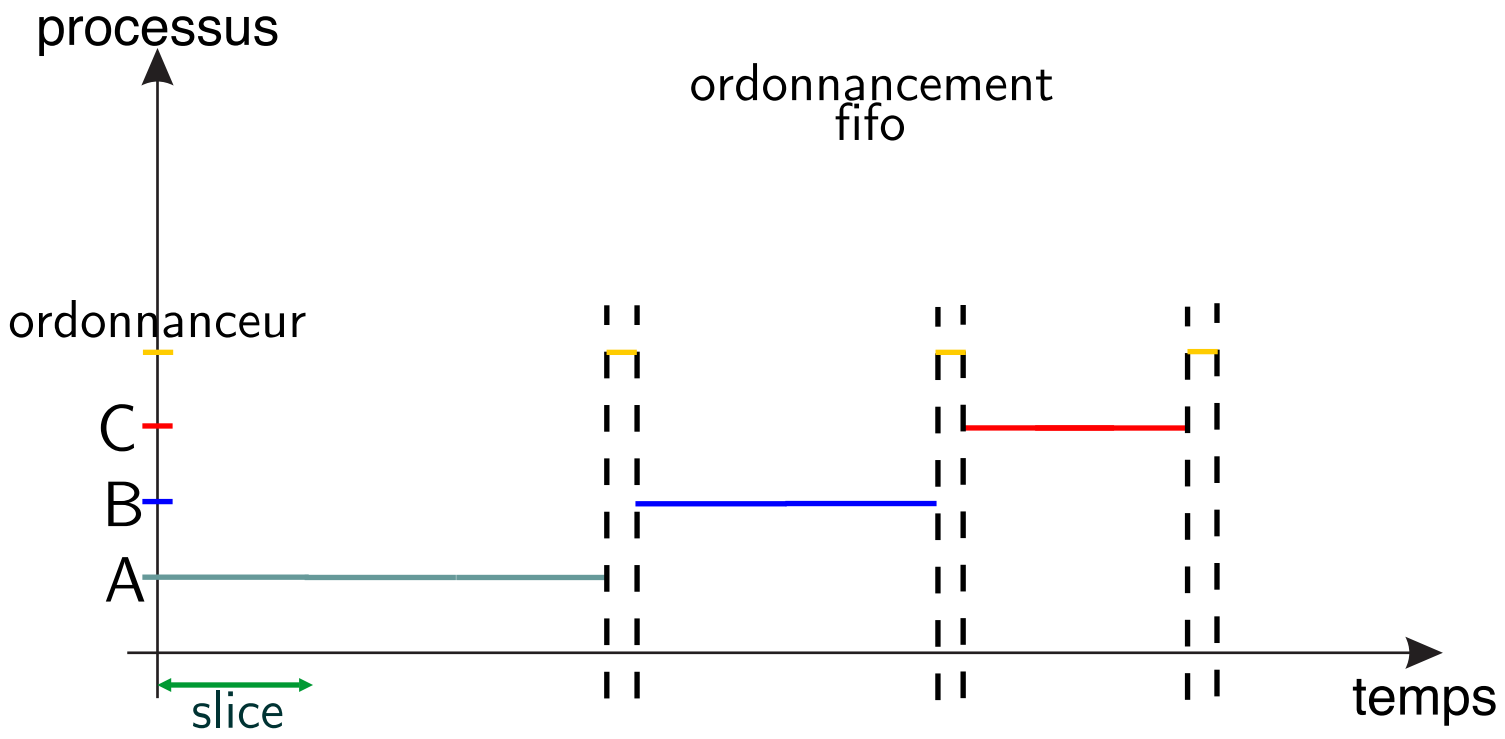
- Système réactif
- Impression simultanéité

- Problème un seul processeur

- Ordonnancement - Préemption
- Interruptions

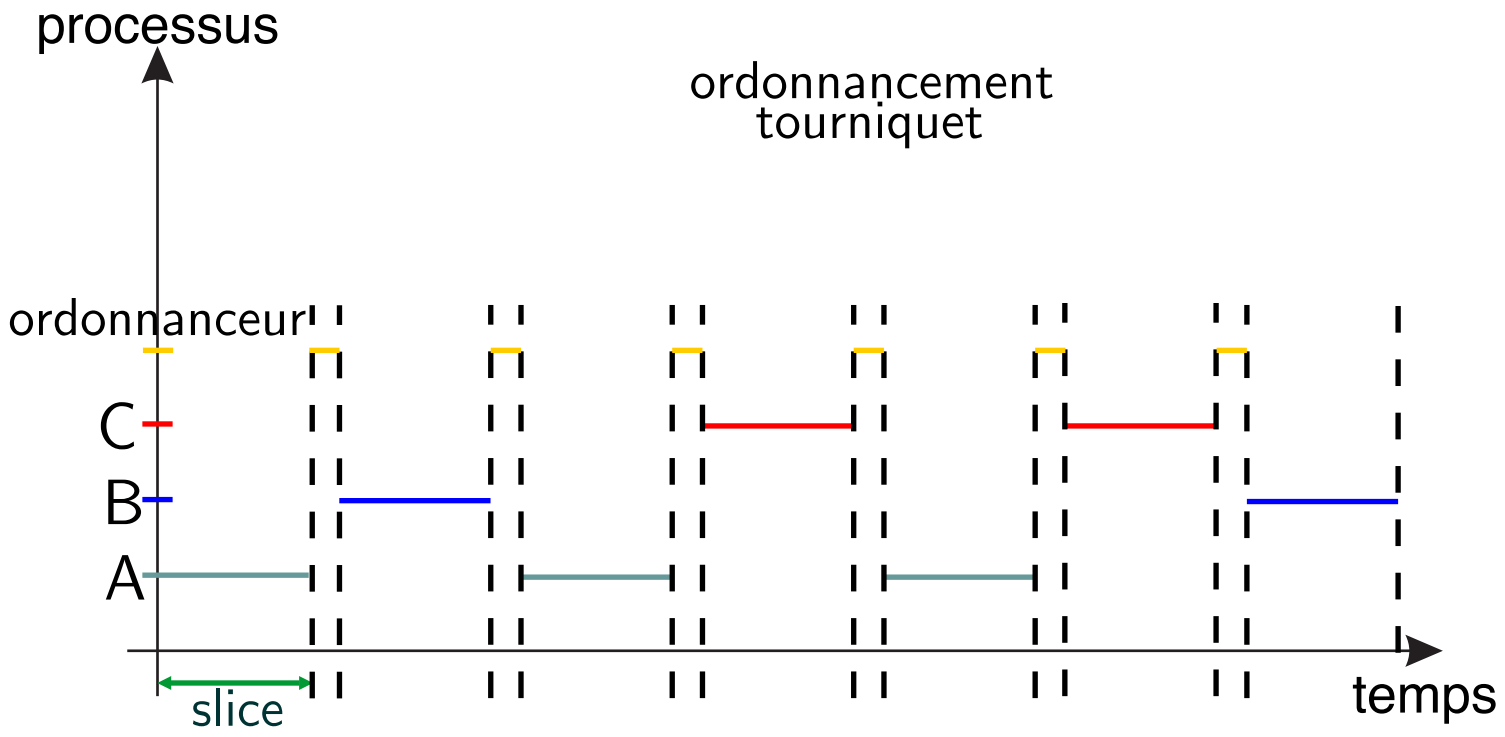
Système d'exploitation

Ordonnancement



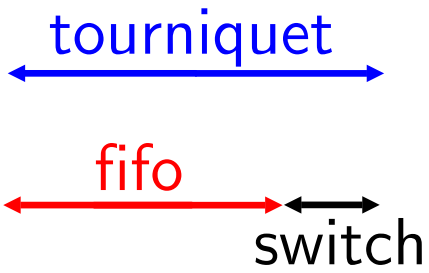
Processeur partiellement émulé

Ordonnancement



Processeur partiellement émulé
Ordonnancement

- Le coût caché du tourniquet ?



Communication entre les processus

Processeur partiellement émulé
Interruptions

- **R**eal **T**ime **C**lock (**RTC**) 1Hz-8192Hz
- **T**ime **S**tamp **C**ounter (**TSC**) 3.5Ghz
- **P**rogrammable **I**nterval **T**imer (**PIT**) 10Mhz

- Oscillateur (**PIT** sous **X86** : 82C54)
- Compteur 64 bits (**TSC** : **X86**)

Processeur partiellement émulé
HAVEGE

- Un outil : HAVEGE et ses dérivées (SEZNEC et SENDRIER 2003).

HArdware Volatile Entropy Gathering and Expansion

http ://www.irisa.fr/caps/projects/hipsor/HAVEGE.html

Processeur partiellement émulé
HAVEGE

```
i=SAMPLING_SIZE;
start=hardClock();
while(i>0)
{
    end=HardClock();
    printf("%llu\n",end-start);
    start=end;
    i--;
}
```

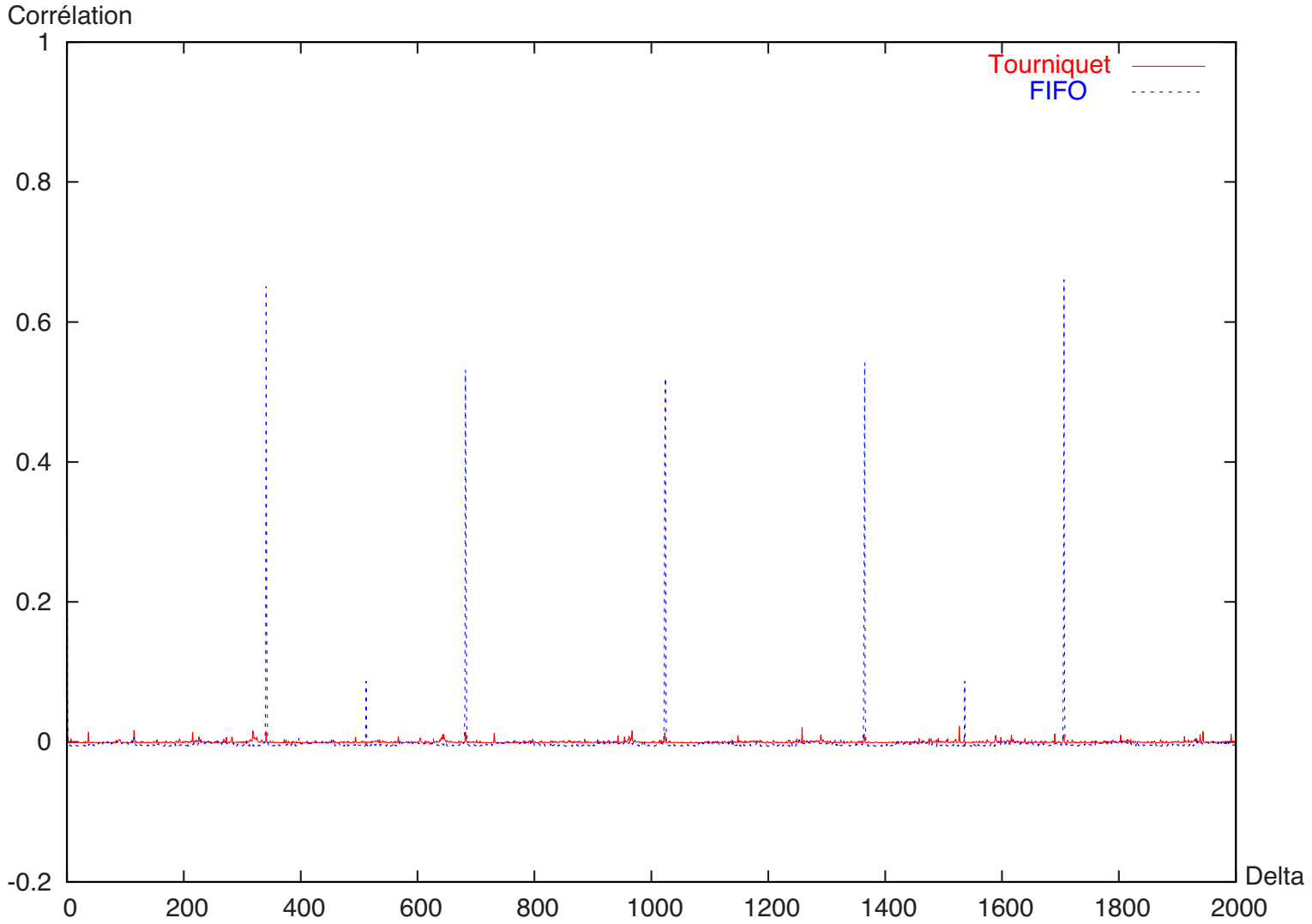
Processeur partiellement émulé

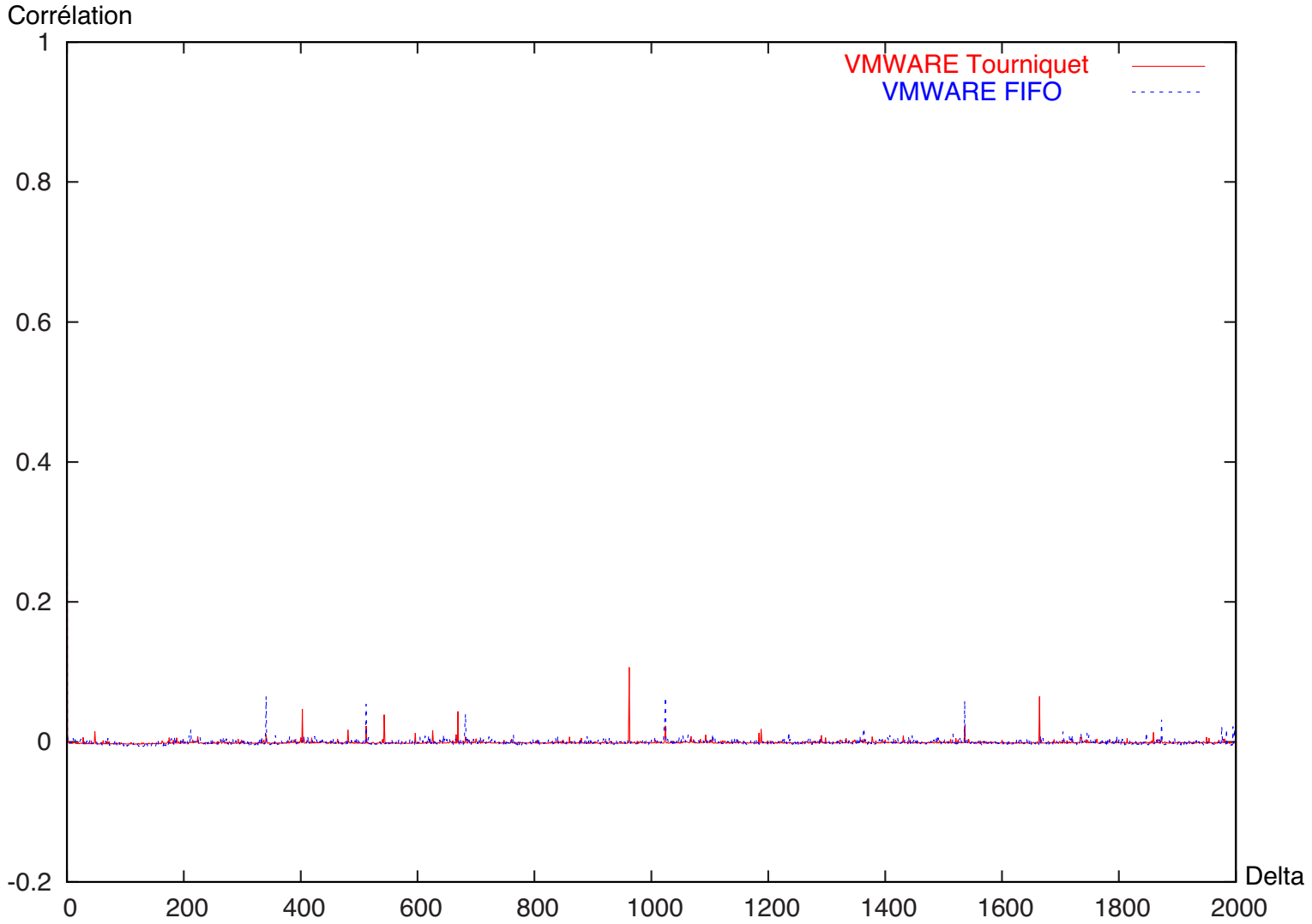
Trace suivant l'ordonnancement

- Mesure de la régularité de la boucle : auto-corrélogramme

$$C_h = \frac{1}{n} \sum_{t=1}^{n-h} (Y_t - \overline{Y})(Y_{t+h} - \overline{Y})$$

  - pour une machine réelle
  - pour vmware


Corrélation
1
0.8
0.6
0.4
0.2
0
-0.2
0
200
400
600
800
1000
1200
1400
1600
1800
2000
Delta
Tourniquet
FIFO


Corrélation
1
0.8
0.6
0.4
0.2
0
-0.2
0
200
400
600
800
1000
1200
1400
1600
1800
2000
Delta
VMWARE Tourniquet
VMWARE FIFO

Conclusions

- La réalisation des pots de miel reste un problème ouvert.
- La latence des opérations sur le processeur est cruciale.
- Le compteur de cycle est le point sensible