HArdware Volatile Entropy Gathering and Expansion

Cédric Lauradoux

1er juin 2006

Ces hommes sont dangereux

André Seznec - Nicolas Sendrier

- Ce sont mes directeurs de thèse ! Ils peuvent avancer ma date de soutenance. . . Bref je leur fais de la pub. . . enfin je crois ?

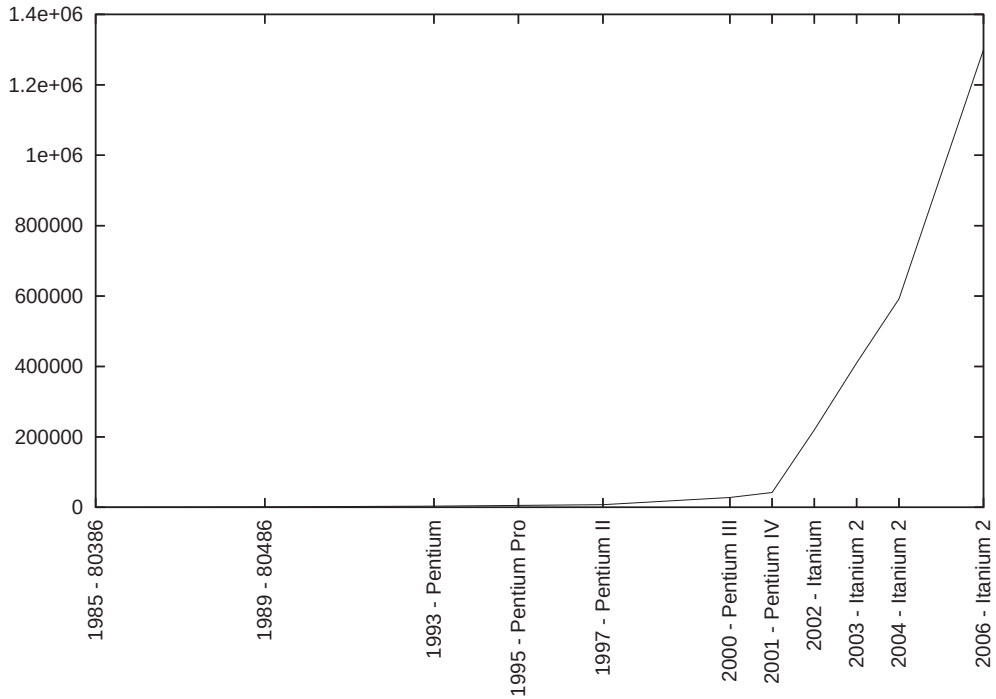
INRIA

Processeur
Compliqué ?

- Un processeur scalaire c'est simple !
- Un processeur superscalaire c'est moins simple, voire c'est très compliqué : pipeliné, à exécution out-of-order, hyperthreadé, à prédiction de branchement, à prefetch hardware, avec plusieurs niveaux de cache, avec des tlbs, avec différents bancs, avec des bugs, avec une pile L/S . . .
- L'état interne des processeurs va être de plus en plus compliqué

Processeur

Moore



HAVEG

Sans l'expansion

```
while (INTERRUPT < min)
{
  if(A==0) A++; else A--;
  Entrop[K]= (Entrop[K]<<5) ^ HardTick () ^ (Entrop[K]>>27)
  ^ (Entrop[(K+1) & (SIZEENTROPY-1)] >>31;
  K= (K+1) & (SIZEENTROPY-1);
  .... ITERER N FOIS (depend de la taille du cache L1) ....
}
```

HAVEGE

Avec l'expansion

- Post Processing : Bayes-Carter = Table = Cache = Entropy
- Bref lisez la bible - lisez les Knuth

Plus d'informations sur

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

HAVEGE

La vitesse vous manque ?

- /dev/random : 10-100 Kbits par secondes
- HAVEGE : 10-100 Mbits par secondes