

Bonus: Meltdown



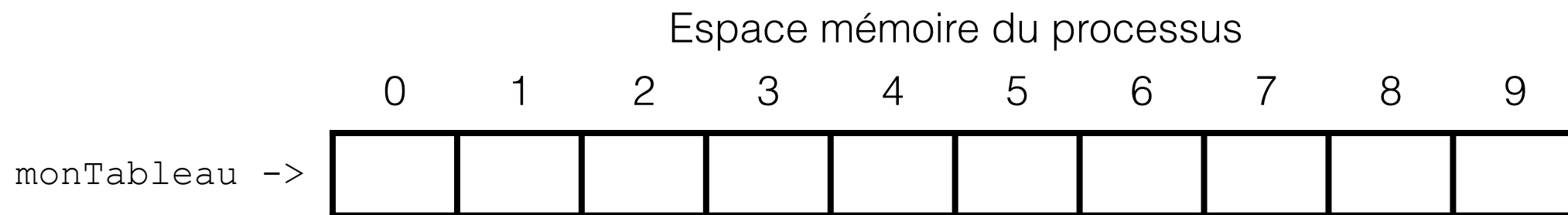
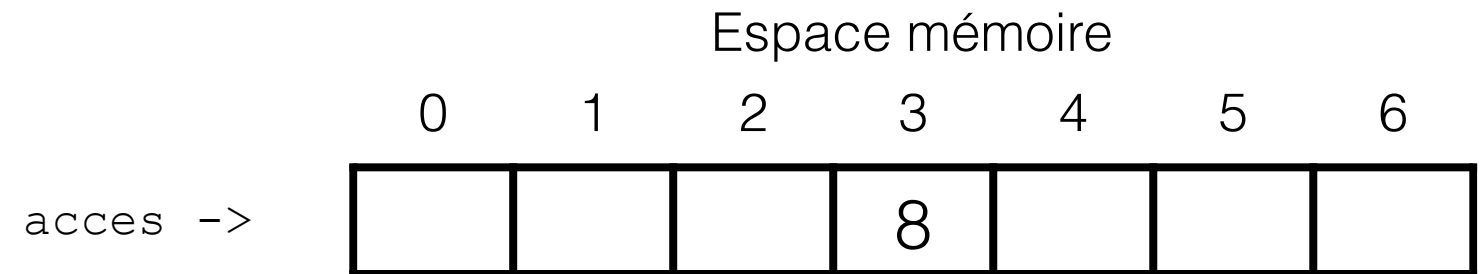
GIF-1001 Ordinateurs: Structure et Applications
Jean-François Lalonde

Meltdown

- Façon d'exploiter un ordinateur
 - prendre contrôle
 - copier des données protégées
- Exploite la façon dont les microprocesseurs sont conçus.
- Deux concepts clés pour en comprendre son fonctionnement:
 - les pipelines
 - les caches



Meltdown

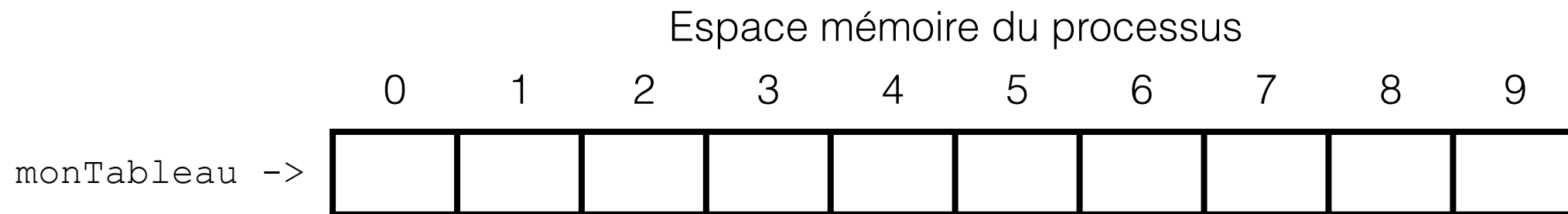
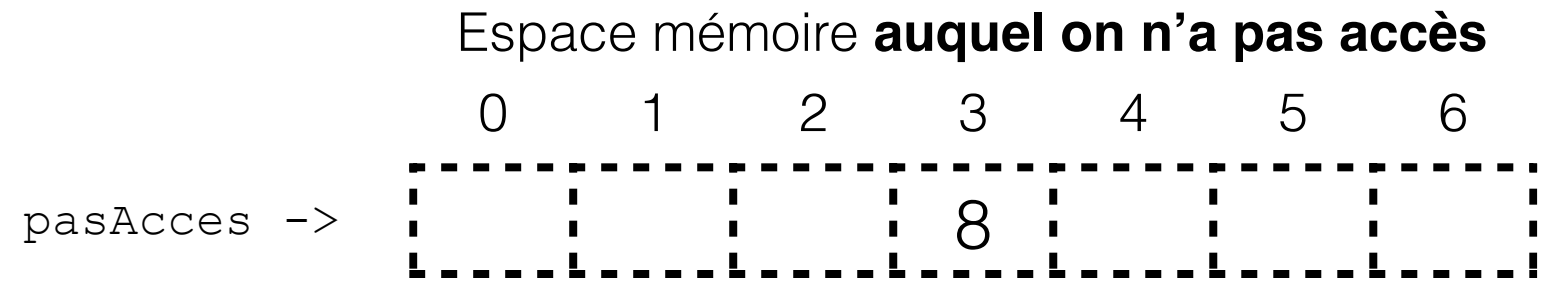


Code à exécuter

```
a = monTableau[accès[3]]
```

Ce code place le 8e élément de `monTableau` dans la variable `a` (car le 3e élément de `accès` est 8).

Meltdown

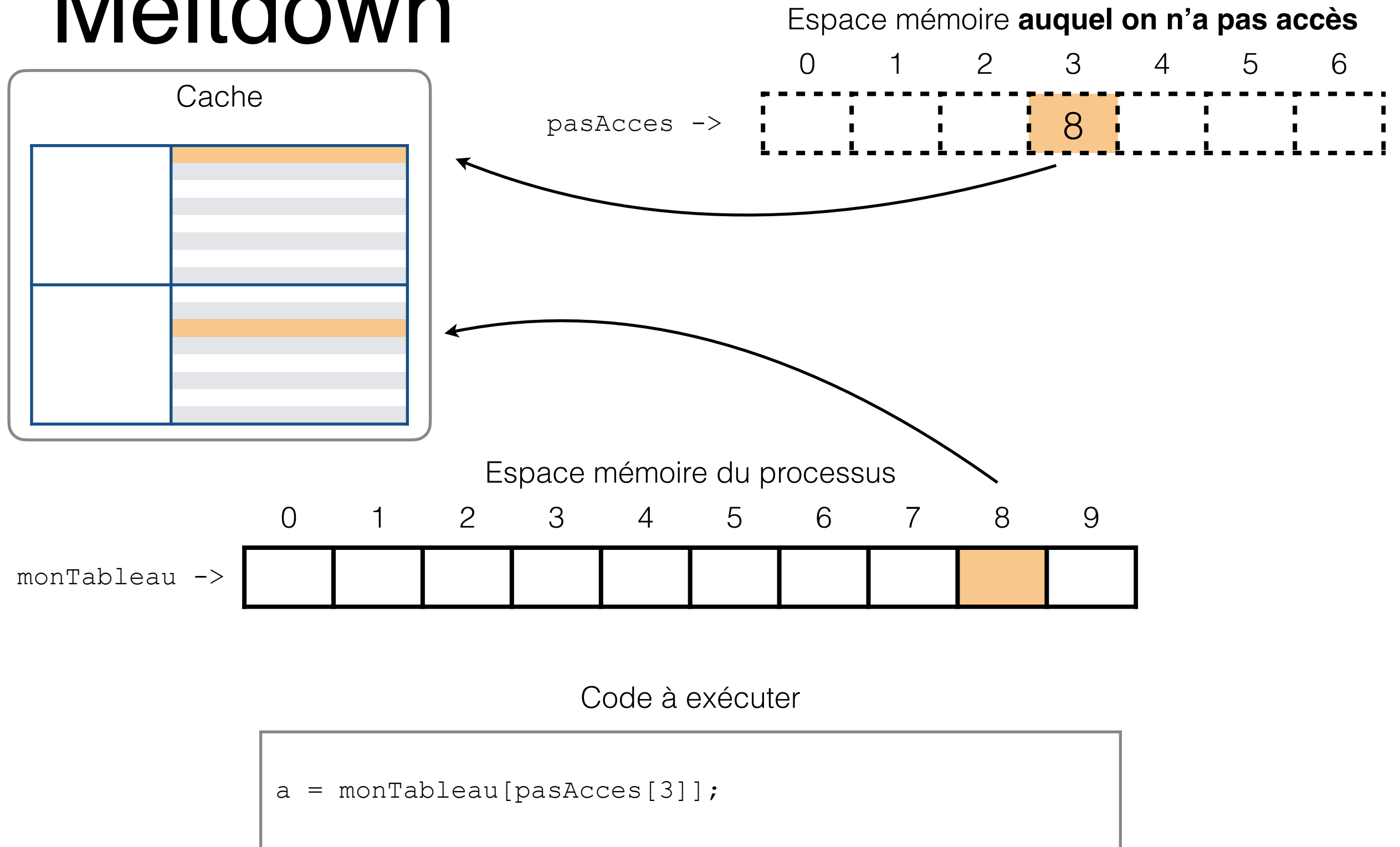


Code à exécuter

```
a = monTableau[pasAcces[3]];
```

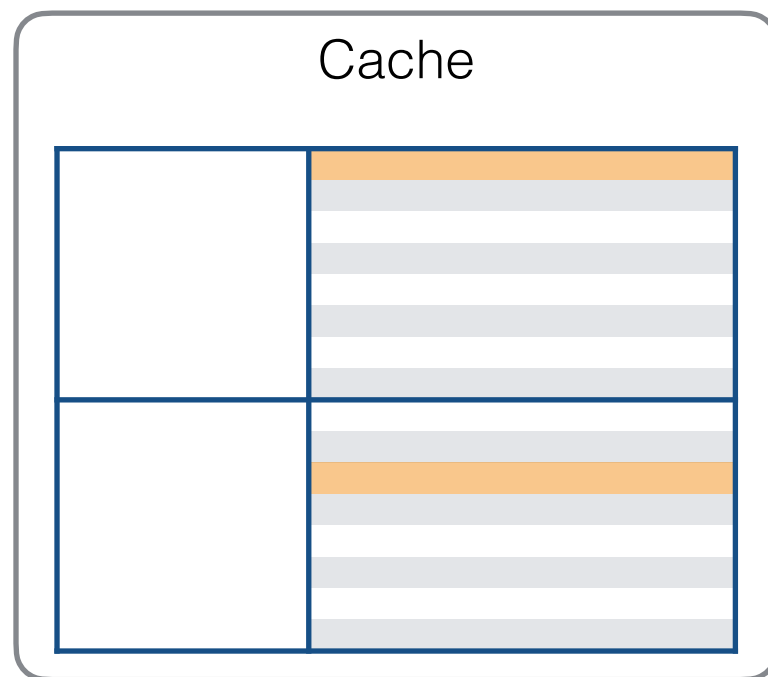
Ce code soulève une exception! Nous n'avons pas accès au 3e élément de `pasAcces`...

Meltdown

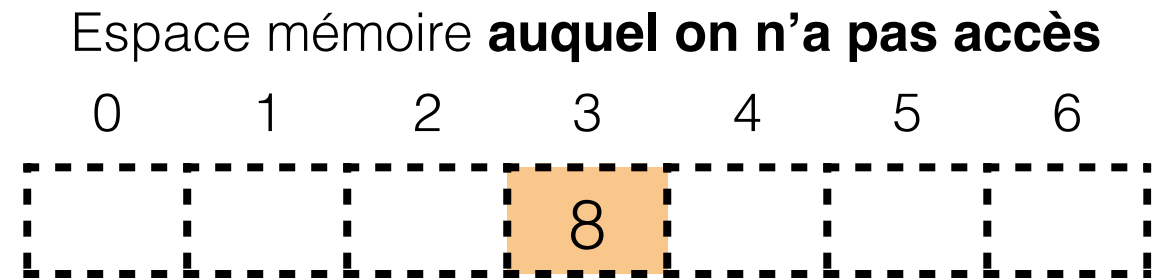


Avant de soulever l'exception, la donnée (inaccessible) **et l'élément correspondant de monTableau** ont été mises en cache (lors de l'étape « pre-fetch » du pipeline)

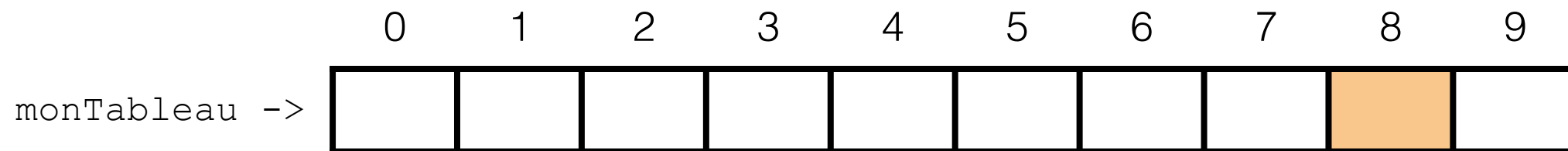
Meltdown



pasAcces ->



Espace mémoire du processus



Il ne reste plus qu'à boucler sur chaque élément de monTableau, et de compter le temps que ça prend pour les accéder.

Quelle est la valeur de l'espace mémoire (supposément) inaccessible?

L'indice de monTableau qui est dans la cache, donc qui est accessible le plus rapidement!