

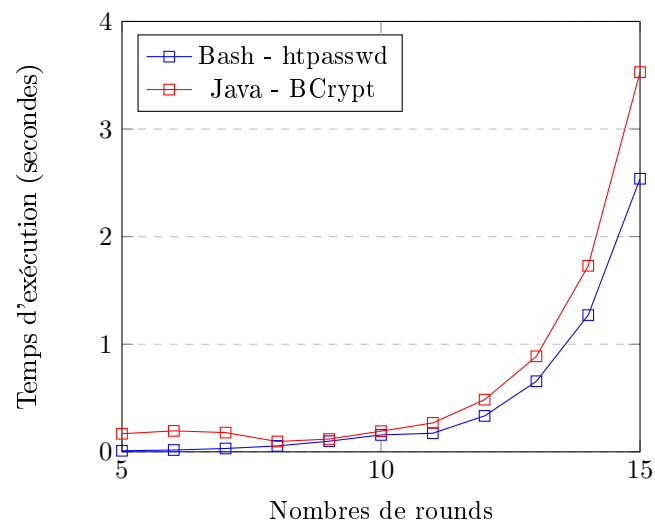
Bcrypt

Evaluation des performances

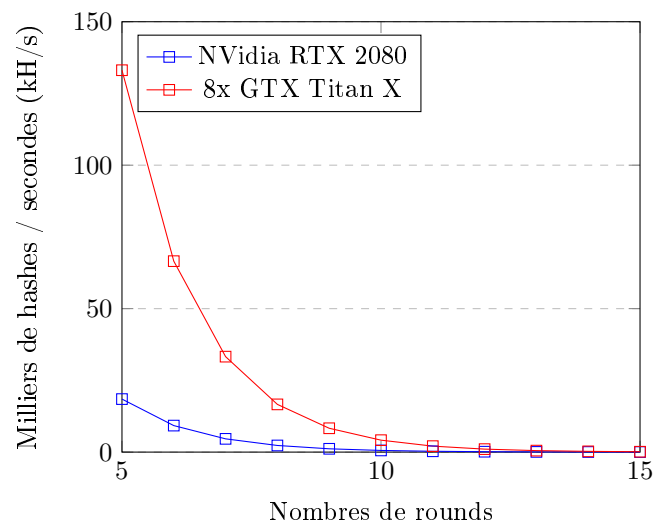
Louka Boivin

22 janvier 2022

Temps d'exécution en fonction du nombre de rounds (i5-8250U CPU @ 1.60GHz)



Temps estimé de calcul de hashes en fonction du nombre de rounds (calcul GPU avec Hashcat)



Détails :

Pour 15 rounds :

- NVidia RTX 2080 : 18 H/s
- 8x GTX Titan X : 130 H/s

Comparaison avec SHA-512 :

- NVidia RTX 2080 : 1556.2 MH/s
- 8x GTX Titan X : 5898.1 MH/s

Source :

- 8x GTX NVidia Titan X - *Hashcat Benchmark*
<https://gist.github.com/epixoip/63c2ad11baf7bbd57544>
- NVidia RTX 2080 - *Hashcat Benchmark*
<https://gist.github.com/epixoip/23068f4bc81db505115c43e7751522f2>
- Post StackExchange - Estimate the time to crack passwords using bcrypt
[https://security.stackexchange.com/questions/139721/estimate-the-time-to-crack-\passwords-using-bcrypt](https://security.stackexchange.com/questions/139721/estimate-the-time-to-crack-passwords-using-bcrypt)
- Source BCrypt Java - <https://www.mindrot.org/projects/jBCrypt/>