Lámání hesel pomocí Rainbow Tables na GPU

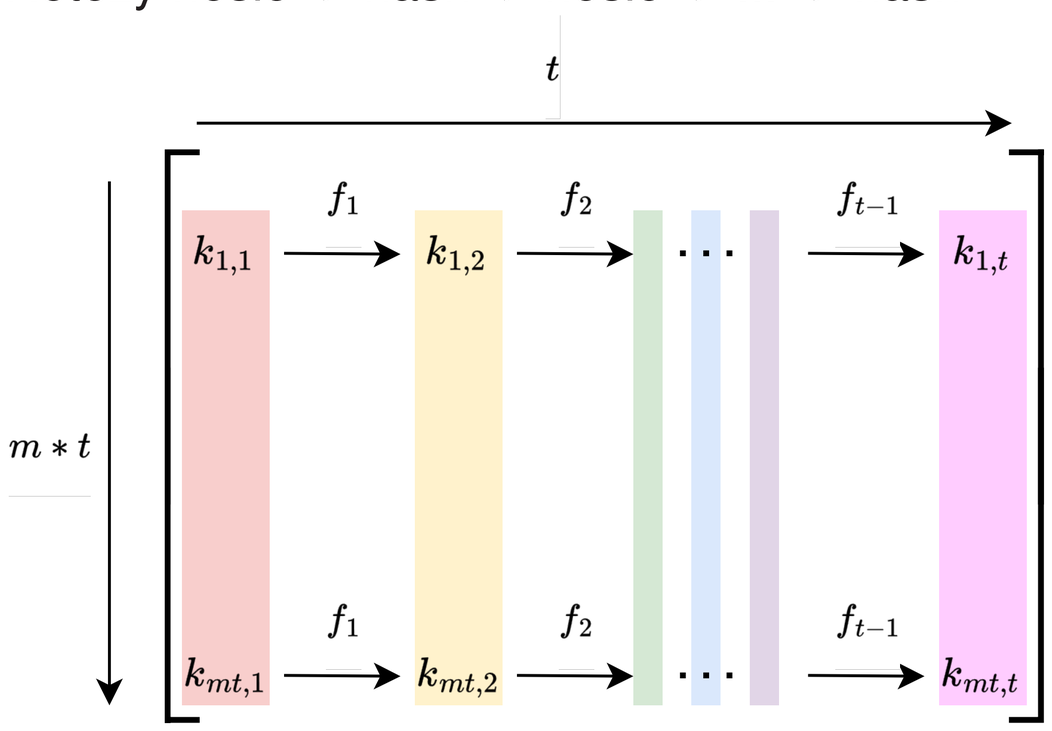
Autor: Bc. David Jahoda
Vedoucí: Mgr. Kamil Malinka, Ph.D.

Motivace

- Autentizace heslem je u mnoha systémů stále jedinou překážkou od kompromitování účtu
- I bez kompromitování hesla uživatelem stále hrozí útok na poskytovatele služby a jeho databázi hesel
- A nad takto zcizenou databází mohou být následně vedeny útoky na jednotlivé hashe hesel

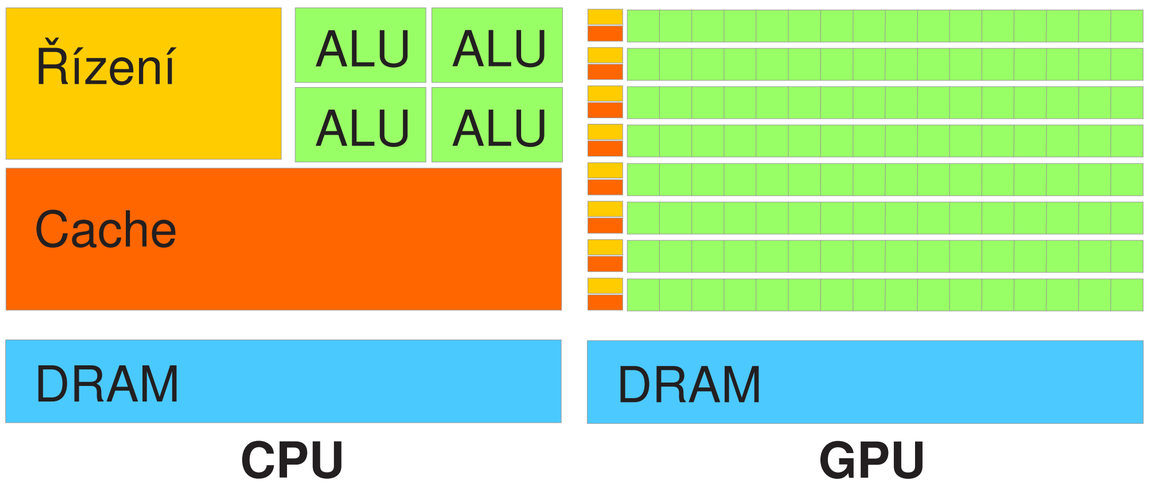
Útok pomocí duhových tabulek [2]

- Rainbow tables = duhové tabulky
- Technika výměny času za prostor [1]
- Tabulka duhových řetězů (záznam: heslo + hash)
- Řetězy heslo -> hash -> heslo -> ... -> hash

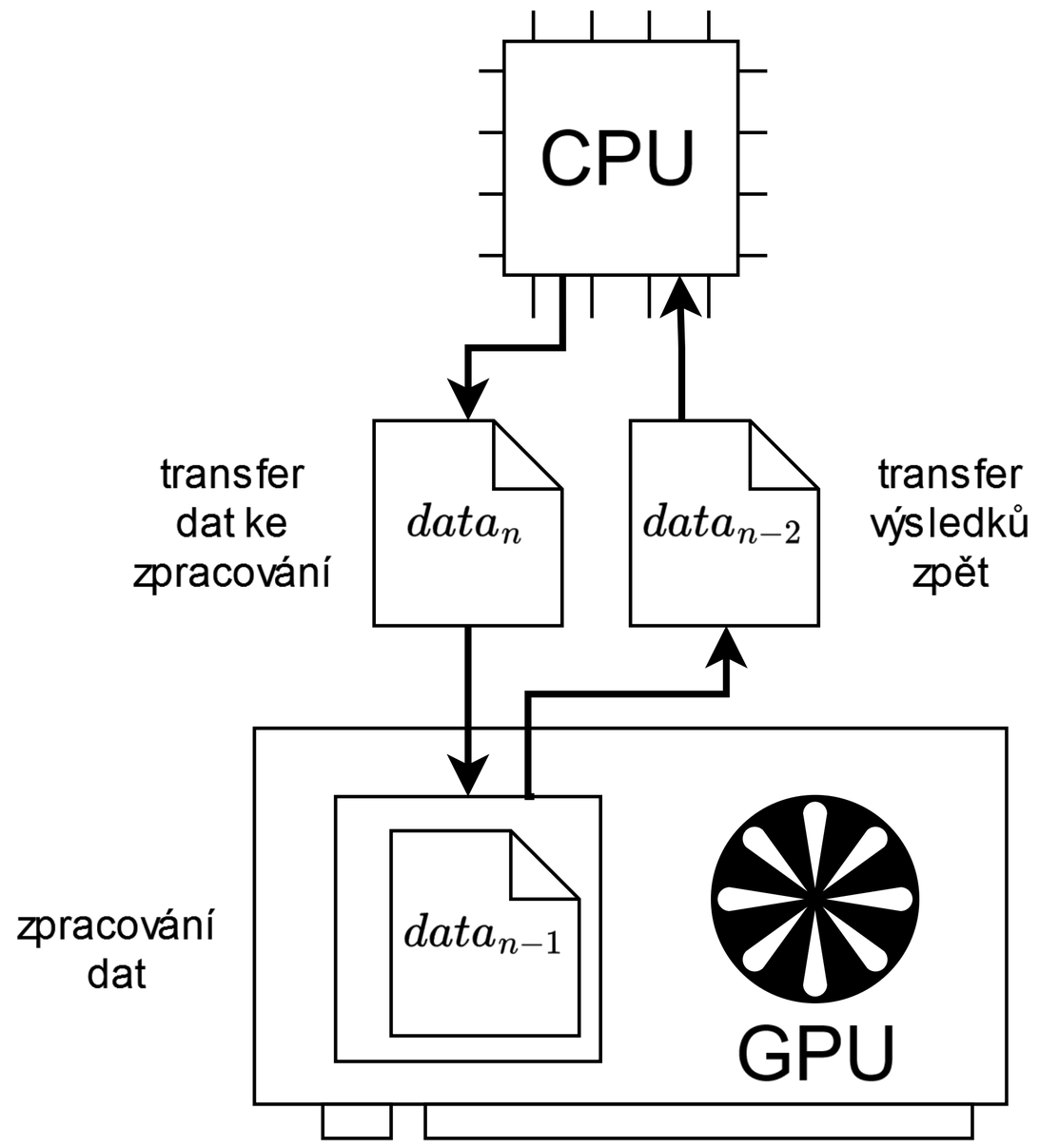


GPU akcelerace duhových tabulek [3]

- SIMT zpracování:



- Překrývání transférů prací:



Výhled

- Rozšiřitelnost: multi-GPU, distribuovaná verze pro výpočetní cluster, statistické redukční funkce, port další GPU platformy, ...

REFERENCE

[1] M. Hellman. A cryptanalytic time-memory trade-off. IEEE transactions on information theory, 26(4):401–406, 1980.

[2] Philippe Oechslin. Making a faster cryptana-lytic time-memory trade-off. In ADVANCES IN CRYPTOLOGY-CRYPTO 2003, PROCEEDINGS, volume 2729 of Lecture Notes in Computer Science, pages 617–630. Springer Berlin Heidelberg, Berlin, Heidelberg, 2003.

[3] R.E. Graves. High performance password cracking by implementing rainbow tables on nvidia graphics cards (isecrack). Master's thesis, Iowa State University, 2008

PODĚKOVÁNÍ

- Computational resources were provided by the e-INFRA CZ project (ID:90254), supported by the Ministry of Education, Youth and Sports of the Czech Republic.
- "Cyber security". This cover has been designed using assets from Freepik.com "Designed by slidesgo / Freepik"
- DALL-E 3 - náhled

Excel@FIT 2024

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ FAKULTA INFORMAČNÍCH TECHNOLOGIÍ