



# GPU Architectures – Password Cracking

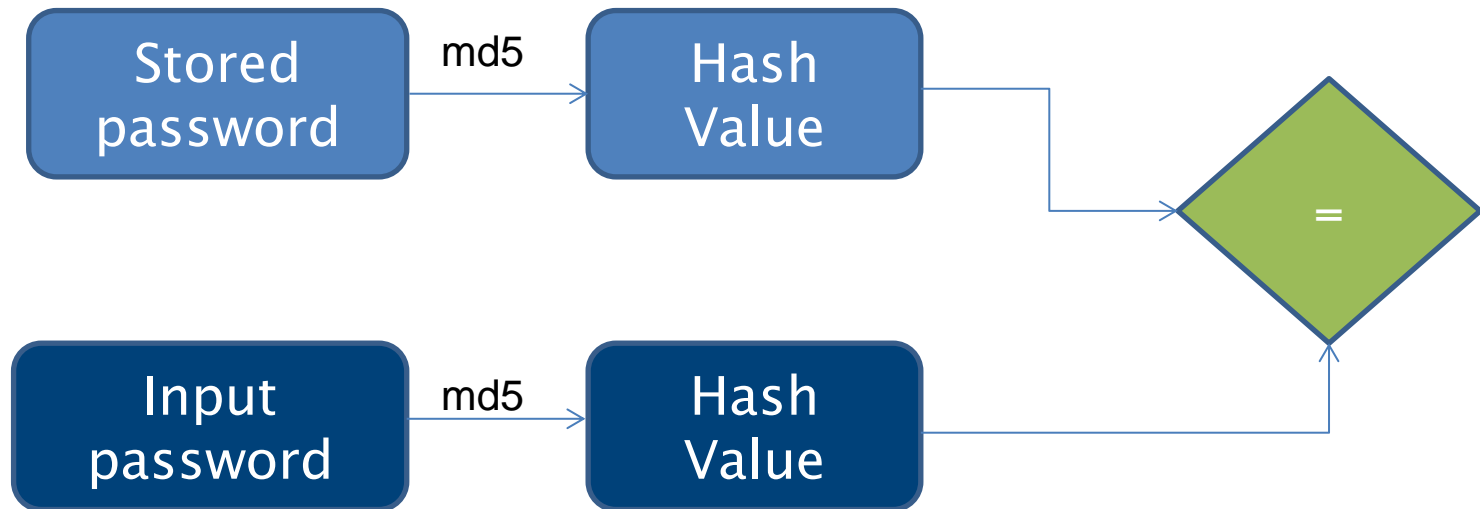
Prof. Dr.-Ing. Sohan Lal

Institute of Massively Parallel Systems

School of Electrical Engineering, Computer Science and Mathematics

Technische Universität Hamburg

- Passwords are stored as hash values
- Checking passwords by checking has values



- Check hash value of every possible combination of N letters
- MD5 calculation is independent for very possible password
- Constrain for the password:
  - 4 letters
  - Lower case only
  - Number of possible passwords:  $26 \times 26 \times 26 \times 26$
- Example:

f	a	s	t
---	---	---	---

- The C code file is named as md5.c