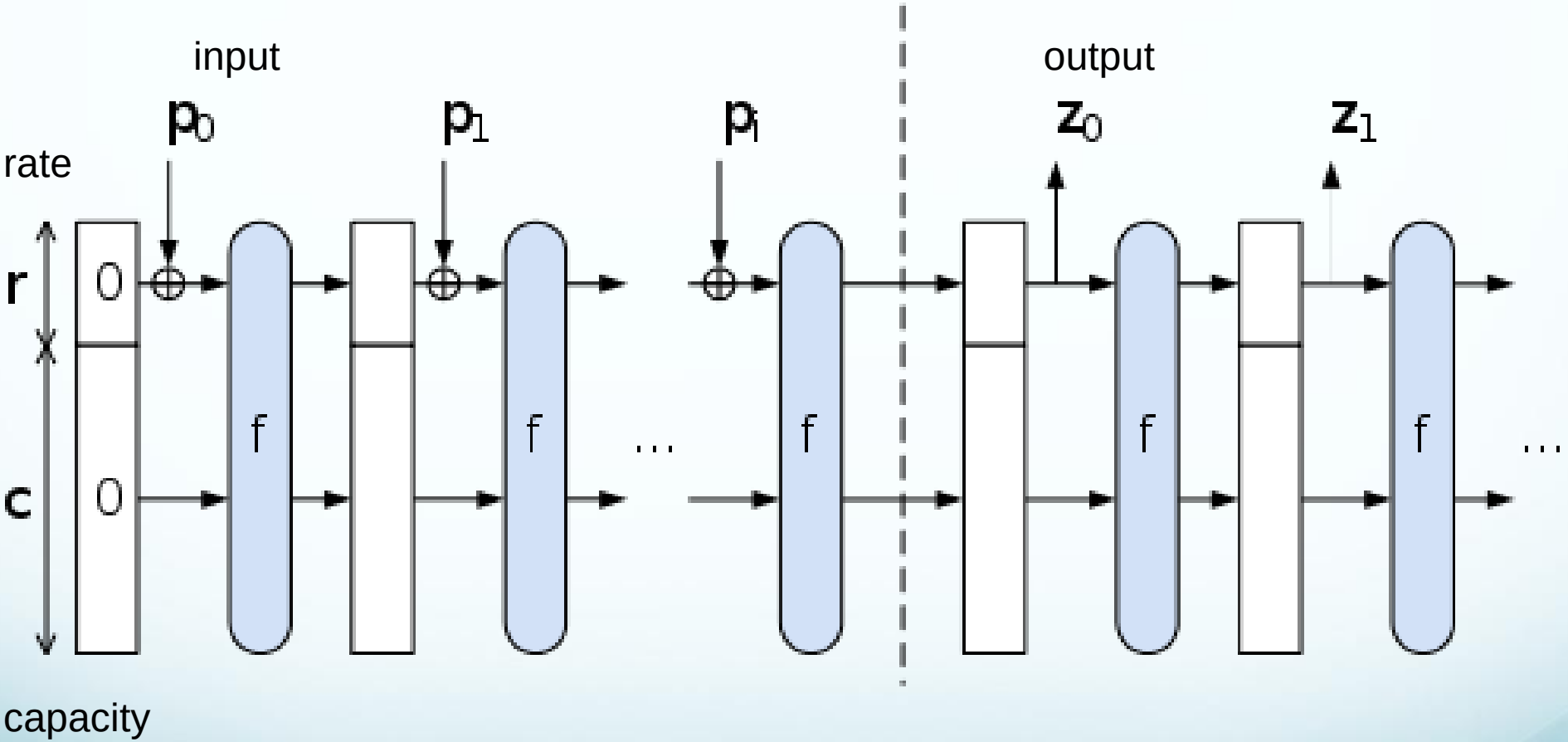
# Moderní hashovací funkce

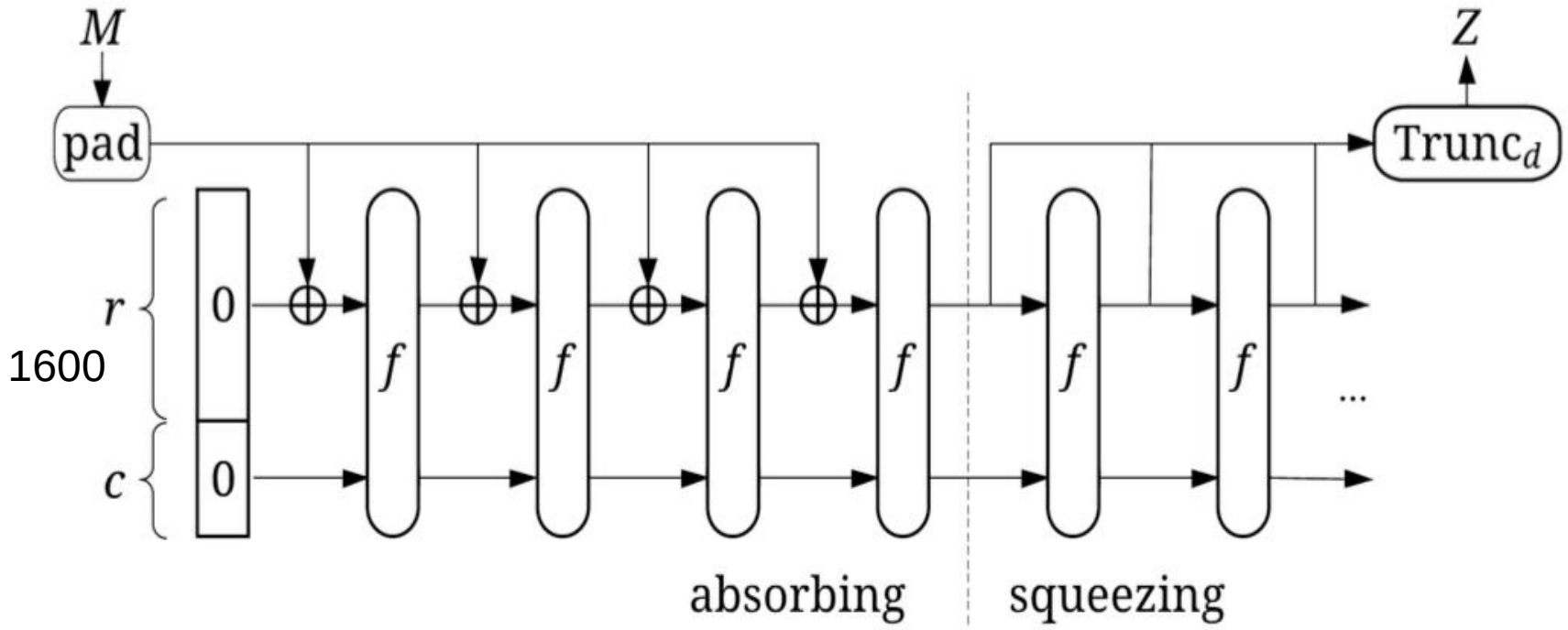
Milan Juřička

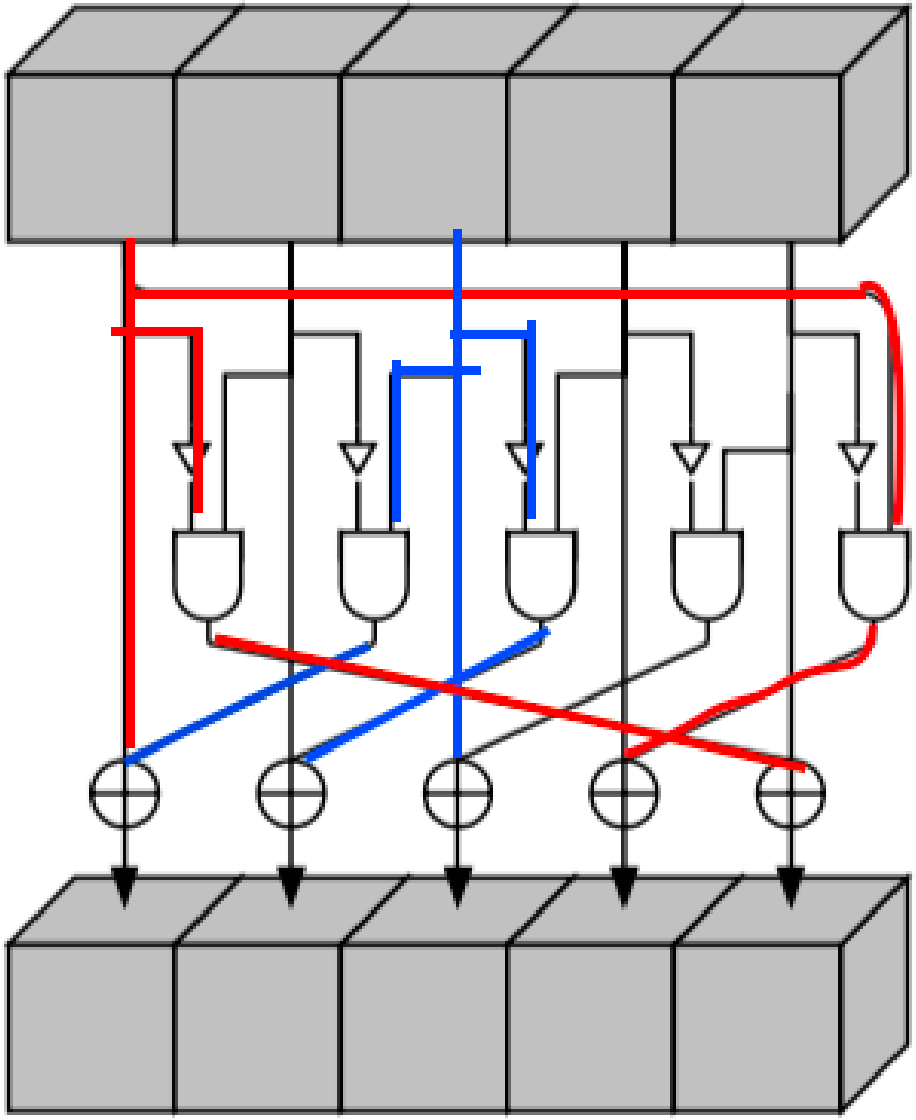
# SHA-3

- 2006 NIST
- Keccak
- 5.8.2015
- Počet round vzrostl z 12 + ℓ na 12 + 2ℓ
- Sponge construction
- Markantní rozdíl architekury mezi sha-2
- 2x softwarově a 1/4x hardwarově pomalejší oproti SHA-2


input
output
$p_0$
$p_1$
$p_i$
$z_0$
$z_1$
rate
r
c
0
0
f
f
f
f
f
...
...
capacity

1. SHA3-224: $\lfloor \text{KECCAK}[r = 1152, c = 448, d = 28] \rfloor_{224}$
2. SHA3-256: $\lfloor \text{KECCAK}[r = 1088, c = 512, d = 32] \rfloor_{256}$
3. SHA3-384: $\lfloor \text{KECCAK}[r = 832, c = 768, d = 48] \rfloor_{384}$
4. SHA3-512: $\lfloor \text{KECCAK}[r = 576, c = 1024, d = 64] \rfloor_{512}$





# Děkuji za pozornost

# zdroje


- http://csrc.nist.gov/publications/drafts/fips-202/fips_202_draft.pdf
- http://citeseerx.ist.psu.edu/viewdoc/download;jsessionid=97D08DBBAD6E39034805E629C9662AE5?doi=10.1.1.184.3037&rep=rep1&type=pdf
- https://en.wikipedia.org/wiki/SHA-3
- http://www.drdobbs.com/security/keccak-the-new-sha-3-encryption-standard/240154037