

Slide attack je útok proti blokovým šifrám, které mají všechny rundy stejné. Úspěch a složitost nezávisí na počtu rund. Původní slide attack se zaměřoval převážně na Feistlovo schéma a jen velmi zřídka na substitučně permutační sítě, protože substitučně permutační sítě mají obecně poslední rundu odlišnou. Kvůli této jejich vlastnosti není možné použít původní slide attack. V článku *New slide attacks on almost self-similar ciphers* od autorů Orr Dunkelman, Nathan Keller, Noam Lasry, and Adi Shamir jsou představeny nové slide attacky, které se zaměřují na substitučně permutační sítě a řeší problém poslední rundy.

V této práci vysvětlíme hlavní myšlenku původního slide attacku a hlavní myšlenku dvou nových slide attacků – slid sets attack a slide attack using a hypercube of slid pairs. V obou těchto útocích tvoříme speciální struktury otevřených textů a šifrových textů, abychom získali speciální páry otevřených textů, tzv. slid páry. Navíc v práci vysvětlujeme vybrané části obou nových útoků a počítáme jejich složitost.