

Tato práce se zabývá možným spojením mezi výsledky článkem Léo Perrina z roku 2019 a článkem Faruka Gologlu z roku 2022. Perrin se zabývá S-boxem π , který se používá v šifře Kuznyechik a hashovací funkci Streebog, a především představuje strukturu TKlog, kterou v něm našel. Výsledkem článku Gologlu je klasifikace lomených q -projektivních funkcí, které se zdají podobné struktuře TKlog. V práci je popsána šifra Kuznyechik i hashovací funkce Streebog. Dále jsou shrnuty výsledky Perrinova článku včetně popisu kryptografických vlastností S-boxu π . Jako hlavní přínos je zde popsán experiment, během kterého se snažíme najít nějakou lomenou q -projektivní funkci, nebo jí podobnou funkci, se stejnými nebo podobnými invarianty jako S-box π . Pokud taková funkce existuje, mohla by být použita jako základ pro útok na S-box π .