

Hledání nových APN funkcí je v symetrické kryptografii důležitým tématem. V roce 2014 popsali Y. Yu, M. Wang a Y. Li maticový přístup ke konstrukci kvadratických APN funkcí. Tento přístup využívá jednoznačné korespondence mezi kvadratickými homogenními APN funkcemi a kvadratickými APN maticemi. Cílem této práce je představit matice používané v původním článku a ukázat, že podobné matice se dají zkonstruovat přímo z algebraické normální formy dané APN funkce. Ve druhé kapitole vysvětlíme původní metodu a pro snazší pochopení přidáme některá tvrzení a kroky důkazů. Ve třetí kapitole definujeme matice získané čistě z algebraické normální formy dané funkce. Ve čtvrté kapitole spočítáme matice pro konkrétní APN funkce a ukážeme, jak spolu souvisí.