

Abstrakt: V této práci zkoumáme rodinu vektorových boolovských funkcí na $\mathbb{F}_{2^{2m}}$, která je inspirována Kimovou funkcí, s cílem najít nové APN permutace na $\mathbb{F}_{2^{2m}}$ pro $m > 2$. Funkce této rodiny jsou definované jako $F(X) = X^3 + bX^{3q} + cX^{2q+1} + dX^{q+2}$, kde parametry b, c a d jsou z \mathbb{F}_{2^m} . V této práci jsou prezentovány nutné a postačující podmínky, které zaručují, že tyto funkce jsou APN nebo ekvivalentní permutaci. K nalezení podmínek na APN byla použita metoda využívající Trace-0/Trace-1 rozklad. Metoda využívající exponenciální sumy byla použita k odvození podmínek, za kterých je funkce z této rodiny ekvivalentní permutaci určitého typu. Získané podmínky pak byly použity k hledání APN permutací v tělesech \mathbb{F}_{2^6} a $\mathbb{F}_{2^{10}}$.