研究テーマ：GAPN関数の暗号理論，符号理論を含む他分野への応用に関する基礎研究

研　究　者：　黒田　匡迪
KURODA Masamichi
（工学部　准教授）

【研究・開発の目的】
Almost Perfect Nonlinear (APN) 関数とは，有限体上で定義された高い非線形性を有する関数である。標数2の場合は，暗号理論における研究対象の1つであり，符号理論などへの応用も知られている。一方で，奇標数の場合では，これらの分野への応用が知られていない。このことは，標数2の場合の代数的な性質が奇標数の場合では成立しないことに起因しているのではないかと考える。そのため，標数2のAPN関数の代数的な性質を保つ奇標数への一般化であるGeneralized APN (GAPN) 関数を暗号理論，符号理論を含む他分野へ応用できないかと考え，研究を行っている。

【研究のきっかけ】
Web通信の暗号化などのデータ暗号化で広く用いられる暗号方式として，ブロック暗号が知られている。差分解読法や線形解読法といった攻撃方法に対して高い耐性を有するブロック暗号アルゴリズムを構築する上で，重要な部品の1つとして，標数2の有限体上で高い非線形性を有するAPN関数が必要であるとされ，盛んに研究されてきた。研究が進められてきた中で，このAPN関数は暗号理論のみならず他分野の研究でも用いられるようになった。例えば，符号理論における例外的数の分類に関するDillonの予想の解決にも寄与している。一方で，奇標数への一般化であるGAPN関数については，暗号理論や符号理論への上記のような応用が知られていない。そのため，GAPN関数の他分野への応用を見込んだ基礎研究を行っている。

【研究・開発の特色】
奇標数の有限体上のGAPN関数も高い非線形性を有すると言えるので，特に暗号理論への応用について期待できる。また，上記の標数2の場合と同様に，GAPN関数を符号理論の言葉で言い換えることで，例外的数の奇標数の場合への一般化を構成できると考えており，符号理論への応用も期待できる。このように，他分野への応用を見込める点が本研究の特色である。

【今後の展開】
GAPN関数の暗号理論や符号理論を含む他分野への応用を見込んでいるが，基礎研究は未だ不十分である。そのため，まずは最も基本的な単項関数の場合に深く研究し，その性質を明らかにするべきである。また，実用上では，単項APN関数が多く用いられているため，単項GAPN関数から始めるのは自然である。現在までに，主に標数3の場合に単項GAPN関数の分類についての研究を行ってきた。標数3においては，多くの場合に分類を進めることができている。

【今後の課題】
標数3の単項GAPN関数の分類については，技術的な条件を仮定した場合にのみ完了している。1つ目の課題として，この技術的な条件を仮定しない場合に分類を与えることが挙げられる。2つ目の課題として，標数5以上の場合の単項GAPN関数の分類についての研究が挙げられる。上記2点の課題について，継続して研究を進めていく。

【地域・企業へのメッセージ】
専門は代数幾何学ですが，上記のような暗号理論を始めとした応用的な内容にも興味を持って研究を進めています．未だ基礎研究の段階であり，具体的な実用が可能かどうかも解らない状況ですが，本研究に興味をお持ちでしたらお気軽にお声がけいただけますと幸甚です。