【論文題目】Study on permutation polynomials over a ring of modulo 2^w and their applications to cryptography　（2 冪剰余環上置換多項式とその暗号技術への応用に関する研究）

【著者】岩崎淳

【論文内容の要旨】整数係数多項式 $F(X)$ が 2 冪剰余環上置換多項式であるとは,

$$\forall w,\ \{F(X) \mod 2^w | X \in \mathbb{Z}/2^w\mathbb{Z}\} = \mathbb{Z}/2^w\mathbb{Z}$$

を満たすことをいう.「2 冪剰余環」とは 2 の冪乗を法とする環 ($\coloneqq$ 集合 $\{0, 1, 2, \cdots, 2^w - 1\}$) で,「2 冪剰余環上置換多項式」は 2 冪剰余環上で全単射となる多項式のことである．2 の冪乗を法とする剰余演算はデジタルコンピュータ上では実質的に無視出来る．そのため, 2 冪剰余環上置換多項式は多項式値を非常に高速に計算可能である．暗号・乱数生成では, 同様の計算を繰り返し行うことから，一つの演算の速度向上は全体の速度向上に有効である．また，デジタルコンピュータとの相性の良さから，ソフトウェア・ハードウェアどちらでも実装を軽量に出来る．これらの性質から，近い将来実現される IoT (Internet of Things) で求められる暗号技術に「2 冪剰余環上置換多項式」は活かされうる．その一方で,「2 冪剰余環上置換多項式」はこれまであまり研究されておらず，応用例も非常に少ない. 本論文では，2 冪剰余環上置換多項式を用いた数少ない既存暗号の解析・改良を行うとともに，将来的な暗号技術開発のための基礎について議論する．具体的には，以下の 4 項目である.

1. 奇数次 Chebyshev 多項式は 2 冪剰余環上置換多項式になることが知られており，それを用いた鍵交換法が提案されていた．本論文では，Chebyshev 多項式が 2 冪剰余環上でもつ周期性を完全に明らかにし，それを基に提案されていた鍵交換法を多項式時間で解読するアルゴリズムを開発する．また，結果を一般化し，一定の条件を満たす一般の 2 冪剰余環上置換多項式を用いて同様の鍵交換法を構成しても，多項式時間で解読可能であることを示す.
2. 2 冪剰余環上置換多項式を用いたストリーム暗号 (共通鍵暗号の一種) として，Vector Stream Cipher(VSC) が提案されていた．VSC は高速性・軽量性で優れていたものの，いくつかの攻撃が成立する．本論文では，VSC に改良を加え，安全性を向上させた VSC2.0 と VSC2.1 を提案する．改良後の暗号は，線形マスクを用いた識別攻撃に対する証明可能な安全性を有する．この結果は，2 冪剰余環上置換多項式のストリーム 暗号・乱数生成の分野での有用性を示唆する.
3. ストリーム暗号・乱数生成の分野では，一般に，用いられる写像の周期は長いほうが良い．2 冪剰余環上置換多項式が最大周期となる (一本の軌道が 2 冪剰余環をくまなく巡る) 必要十分条件は，多項式の次数が低い場合を除き，知られていなかった. 本論文では，その必要十分条件を導出する．また，条件を満たす多項式の性質について議論する.
4. 前項の周期が最大の 2 冪剰余環上置換多項式は，単体ではあまりに単純すぎ，そのままストリーム暗号・乱数生成に用いることはできない．そこで，最大周期となる多項式を複数組み合わせ，より複雑な挙動をさせることが考えられる．最大周期となる多項式を用いる利点は，その長い周期性であるので，組み合わせることによって周期性が壊れないような組み合わせ方を提案する．また，組み合わせることでさらに周期を伸ばす方法も提示する.