L-001

量子鍵配布プロトコルへの強化のためのベント関数の検討

Investigation of vent functions for quantum key distribution protocols

松本　大輝† 森下　航† 三重野　凌† 馬場　優作† 荒木　智行†

Hiroki Matsumoto Koh Morishita Ryo Mieno Yusaku Baba Tomoyuki Araki

1. まえがき

社会インフラとしての IT ネットワークの普及に伴いセキュリティへの要求が高まっている中、量子力学理論によって物理的に安全性が保証される暗号通信技術が注目されている。しかし、実用性や信頼性の向上に関する技術的な課題が残されている。[1][2]

本研究の目的は暗号通信技術の実用性と信頼性向上のために、新しい手法を提案することである。

2. 諸準備

新手法の提案にあたり、従来の手法を概観する。

2.1 アフィン関数

アフィン関数は、2 元体$\mathbb{F}_2$上で定義される基本的な関数であり、線形関数に定数項を加えた形で構成される。この関数は、暗号理論や情報理論のさまざまな分野で利用され、特に線形的な構造を解析する際に役立つ。アフィン関数は以下の式(1)のように定義される。

$$l_{a,b}(x) = \langle a, x \rangle \oplus b \tag{1}$$

ここで、$\langle a, x \rangle$ は n -次元ベクトルa とxの内積を意味し、以下の式(2)で計算される。

$$l_{a,b}(x) = a_1 x_1 \oplus a_2 x_2 \oplus \ldots \oplus a_n x_n \tag{2}$$

また、bは定数項であり、アフィン関数に非対称性を導入する役割を果たす。この定義により、アフィン関数は入力ベクトル xを線形的に変換しつつ、定数bによって追加の変化を加えることができる。

暗号理論では、アフィン関数は特にブール関数や非線形性の評価において基本的な役割を果たす。例えば、線形近似攻撃では、暗号化関数をアフィン関数に近似し、その特性を利用して暗号の内部構造を解析する。

2.2 ハミング距離

ハミング距離は、同じ長さの 2 つのビット列間で異なるビットの数を表す指標であり、暗号理論や誤り訂正符号の設計において重要な役割を果たす。この距離は、データの類似性を測定したり、誤りを検出したりする際の基礎的な指標である。

たとえば、以下の 2 つのビット列を考える。

ビット列 1: 1 0 1 1 0, ビット列 2: 1 0 0 1 1

この場合、異なるビットは 2 箇所存在するため、ハミング距離は 2 であると計算される。

一般的に、2 つの n-ビット列 x, y のハミング距離 $dist(x, y)$ は以下の式(3)のように定義される。

$$dist(x, y) = \sum_{i=1}^{n} \delta(x_i, y_i) \tag{3}$$

この場合、異なるビットは 2 箇所存在するため、ハミング距離は 2 であると式(4)のように計算される。

$$\delta(x_i, y_i) = \begin{cases} 0 & (x_i = y_i) \\ 1 & (x_i \neq y_i) \end{cases} \tag{4}$$

ハミング距離は、特にブール関数や暗号通信において重要な役割を持つ。暗号理論では、ハミング距離を利用して鍵やビット列間の差異を評価し、攻撃への耐性や誤り訂正能力を向上させることが求められる。

2.3 非線形性

具体的に、非線形性はブール関数 f と最も近いアフィン関数とのハミング距離として定義される。n 変数ブール関数f の非線形性N_fは次の式(5)で表される。

$$N_f = \min_{a \in F_2^n, b \in F_2^n} dist\left(f, l_{a,b}\right) \tag{5}$$

この式は、ブール関数 f の出力と全てのアフィン関数の出力を比較し、最も近いアフィン関数とのハミング距離を求めるものである。この値が大きいほど、関数は非線形であると評価される。

さらに、ウォルシュスペクトルを用いることで非線形性を次の式(6)で計算することもできる。

$$N_f = 2^{n-1} - \frac{1}{2} \max_{\omega \in F_2^n} \left| W_f(\omega) \right| \tag{6}$$

ここで$W_f(\omega)$はウォルシュ変換によって得られる値であり、ブール関数の周波数特性を示している。この計算により、暗号理論で用いる関数が攻撃に対してどの程度の強度を持つかを評価することができる。

2.4 ウォルシュ変換

ウォルシュ変換[3]は、ブール関数の特性を周波数領域で解析するための重要な手法である。この変換を用いることで、関数の線形性や非線形性を効率的に評価することが可能となる。定義を以下式(7)に示す。

$$W_f(\omega) = \sum_{x \in F_2^n} (-1)^{f(x) \oplus \langle \omega, x \rangle}, \omega \in F_2^n \tag{7}$$

†広島工業大学　Hiroshima Institute of Technology

ここで、$f(x)$ブール関数、xはnビットの入力ベクトル、ωは周波数ベクトルを表し、$\langle \omega, x \rangle$ は内積を意味し、式(8)のように計算される。

$$\langle \omega, x \rangle = \omega_1 x_1 \oplus \omega_2 x_2 \oplus \ldots \oplus \omega_n x_n \quad (8)$$

この変換によって得られる$W_f(\omega)$ は、入力ベクトルxに対するブール関数 $f(x)$ の特性を示す値であり、周波数領域での関数の振る舞いを解析するのに用いられる。特に、ウォルシュスペクトル$\{W_f(\omega) | \omega \in F_2^n\}$ は、ブール関数が持つ周波数成分を全体的に把握することを可能にする。

ウォルシュ変換は、暗号システムの解析や設計において非常に有用である。たとえば、関数の線形性を評価したり、攻撃に対する耐性を確認するために利用される。

2.5 ウォルシュ変換による非線形性

ブール関数の非線形性は、その関数が線形関数またはアフィン関数からどれだけ離れているかを示す指標である。この非線形性を評価する際に、ウォルシュ変換を利用する方法が非常に有効である。

n変数ブール関数 $f(x)$ の非線形性 N_f は、次の式(9)で計算される。

$$N_f = 2^{n-1} - \frac{1}{2} \max_{\omega \in F_2^n} |W_f(\omega)| \quad (9)$$

ここで、$max_{\omega \in F_2^n} |W_f(\omega)|$はウォルシュスペクトルの最大値を意味する。この最大値が小さいほど、ブール関数は高い非線形性を持つことを示している。

この評価方法では、ブール関数のウォルシュスペクトルを計算し、その中で最も大きな値を見つけることで非線形性を定量化する。

2.4 ベント関数

ベント関数[4]は、非線形性が理論上最大値を持つ特殊なブール関数であり、暗号理論において重要な役割を果たす。この関数は、入力変数の数nが偶数の場合にのみ存在し、その際の非線形性は次の式(10)で表される。

$$N_f = 2^{n-1} - 2^{\frac{n}{2}-1} \quad (10)$$

ここでN_fはブール関数の非線形性を示す。この最大非線形性を持つことで、ベント関数は線形攻撃や差分攻撃に対する強い耐性を提供する。

3. 新手法の提案

本研究では、ベント関数により最大の非線形性を持つ S-Box を構成し、安全性の高い疑似乱数の生成を目指す。手法として、S-Box を構成し、バランス化を行う。

3.1 S-Box

S-Box（Substitution Box）は、ブロック暗号において非線形性を導入するための重要な構成要素であり、入力ビット列を出力ビット列へと変換する置換写像として定義される。S-Box の設計においては、差分均一性、非線形性、バランス性、固定点の存在などが安全性を左右する要素となる。特に、線形攻撃や差分攻撃といった代表的な解析手法に対抗するためには、S-Box の非線形性の確保が不可欠である。ビット列間の関係性を複雑にし、情報の拡散を促進することで、暗号全体としての強度を高める役割を担う。

3.2 バランス化

バランス化は、暗号における S-Box やブール関数に求められる基本的な性質の一つであり、全ての入力値に対して出力のビットが 0 と 1 を等しく取る状態を指す。出力に偏りがあると、統計的な分析から入力の情報が漏洩しやすくなり、暗号全体の安全性が損なわれる。そのため、バランス化は、非線形性や差分均一性と並び、暗号設計における重要な設計基準の一つとされる。情報の拡散と均等性を確保し、暗号解析への耐性を高める役割を担っている。

4. むすび

本研究では、量子鍵交換プロトコルの強化を目的として、ベント関数を用いた S-Box の生成とそのバランス化手法の検討を行った。今後はビット長や使用するベント関数などの条件を変えて生成した疑似乱数でも実行を行い、どのような条件下でもランダム性が高く解読されにくい疑似乱数を生成できるのかを検証する。加えて、疑似乱数生成器の更なるランダム性の向上を目指す。

謝辞

本研究をまとめるにあたり江田英雄教授にご指導をいただきました.心より感謝をいたします.

参考文献

[1] 杉本幹太，方穆湧，荒木智行，“ベント関数の量子鍵交換プロトコルへの適用について”，多値論理研究会，第 46 回多値論理フォーラム研究ノート，Vol.46, No.4, pp. 3-5, (2023).
[2] 方穆湧，杉本幹太，荒木智行，“ベント関数を使った量子鍵交換プロトコルの評価について”，多値論理研究会，第 46 回多値論理フォーラム研究ノート，Vol. 46, No.5, pp. 1-4, (2023).
[3] 遠藤靖, “数理科学セミナー ウォルシュ解析”, pp. 75-79, (1993).
[4] Natalia Tokareva, “Bent Functions~~Results and Applications to Cryptography”, pp. 17-24, Academic Press, Boston, (2015).