連の検定と Non-overlapping template matching test を用いた暗号解読に関する検討

神奈川工科大　竹田　裕一　　中央大・理工　藤井　光昭
中央大・理工　渡邉　則生　　中央大・理工　鎌倉　稔成

1. はじめに

暗号は情報の保護やセキュリティの観点から欠かせない技術となっており、暗号の種類についても数多くの考案がなされており、代数的方法や乱数を用いる方法など様々な手法が提案されている。本研究では乱数を用いる方法について焦点をあてる。本発表では、連の検定や Non-overlapping template matching test を用いた暗号の解読を行う立場に立った検討を行う。

乱数を用いた暗号の方法については、次のような表現を用いることとする。

> メッセージはある文字により表現されているとし、各文字を 0 と 1 の組合せのパターン（各要素が 0 か 1 かである m 次元ベクトル）$\mathbf{\Xi}$ で表し、これに各要素が 0 か 1 の乱数ベクトル $\mathbf{Z}$ を要素毎に加えて送信信号 $\mathbf{X}$ を作る。これは、各要素を 2 進法での和を用いて $\mathbf{X} = \mathbf{\Xi} + \mathbf{Z}$ と表すことができる。

2. 暗号解読に関する検討

セキュリティの分野では、乱数 $\mathbf{Z}$ に関する議論が行われ、米国国立標準技術研究所 (NIST) では 15 個の検定法が提案され、実際に用いられている。NIST ではこの検定の帰無仮説として「0 と 1 がそれぞれ確率 1/2 で出現し、さらに各ビットの値は独立に出現する $0-1$ 数列」を用いている。しかしながら暗号の観点から見た本来の帰無仮説は「暗号文を第三者が得たときに解読されない $0-1$ 数列」とすべきである。実際に NIST が用いる帰無仮説を満たす乱数の場合「解読されない $0-1$ 数列」であることを証明できるが、２つの仮説が同値であると証明されていない。

そこで本研究では、連の検定とこれまで研究を行ってきた Non-overlapping template matching test を用い、乱数を加えた場合の暗号解読の問題を議論する。特に NIST で提案されている検定に関して、精密分布を導出することによって、NIST とは異なる検定の検討を行う。

参考文献

[1] Rukhin, A. et al.(2010) A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications. NIST Special Publication 800-22.

[2] Takeda,Y., Huzii, M., Watanabe, N. and Kamakura, T. (2017) An improved method for identification of patterns in the non-overlapping template matching test. Journal of the Japanese Society of Computational Statistics, **30**, 15-25.