暗号に用いる乱数列の性質と暗号解読に関する検討

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

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。本論文では、メッセージに乱数を加える方法に対して、暗号の解読可能性について議論し、加える乱数に対しての統計的仮説検定法の検討を行う。

2. 統計的解読不可能と仮説検定の検討

乱数を用いた暗号の方法については次の通りとする。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）ξ 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 $\mathbf{X} = \xi + \mathbf{Z}$ と表すことができる。このとき

$$P(\mathbf{X} = \mathbf{x}) = \sum_{\mathbf{a}} P(\xi = \mathbf{a}) P(\mathbf{Z} = \mathbf{x} - \mathbf{a})$$

が成立しており、解読を行う第三者は $P(\mathbf{X} = \mathbf{x})$ のみを知ることができ、$P(\xi = \mathbf{a})$ と $P(\mathbf{Z} = \mathbf{x} - \mathbf{a})$ は未知である。過去の学会において、統計的解読不可能の定義を次のように表現した。

「$P(\mathbf{X} = \mathbf{x})$ が得られたとき、$\forall \mathbf{a}$ について $P(\xi = \mathbf{a})$ として 0 も 1 も取り得て、
さらに無限個の値を取る可能性もある」

この定義のもとで、暗号の分野において一般に $\mathbf{Z}$ が持つべき条件としている「$\mathbf{Z}$ は独立に 0 と 1 が確率 $\frac{1}{2}$ で出現する」を満たす場合、統計的解読不可能な条件も満たしている。また、$\mathbf{Z}$ が強い周期をもつ場合や、0 または 1 が長く続くことが頻繁に生じる傾向を持つ場合、統計的解読不可能な条件を満たさない。このように、統計的解読不可能な条件を満たさない $\mathbf{Z}$ については、暗号解読の手掛かりを得ることができるため、使用を避けるべきである。NIST などにおいて、いくつかの乱数検定方が提案されているが、本研究では一つの検定法として、統計的仮説検定論に従う形で検定法の検討を行っている。発表当日は、シミュレーション実験を踏まえた上で、報告を行う。

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.