古賀　弘樹
筑波大学大学院システム情報工学研究科　准教授

ユニバーサルな一様乱数生成に関する研究

本研究では、ユニバーサル乱数生成に関する 2 つの成果を得た。

1 つ目の成果は、近年注目を集めている情報理論的なステガノグラフィをに関するものである。本研究では情報理論的なステガノグラフィのモデルを一般化し、送信者から受信者に対して送ることができる最大の情報量の公式を導出することに成功した。本研究で考えたステゴシステムは、微小な復号誤りを許し、カバーテキストの確率分布と、秘密の情報を埋め込んだステゴテキストの確率分布間の変動距離が漸近的に 0 になるという特徴をもっている。また、カバーテキストと相関をもつ副情報が復号器に与えられれば、復号器は高い確率でステゴテキストとカバーテキスト区別することができることが示された。送信者から受信者に送ることができる最大の情報量の公式を導出するにあたり、送信者は単位区間[0,1]上の一様乱数を用いて、秘密の情報を埋め込んだ符号語を受信者に送信する必要があり、この成果は一様乱数生成の１１つのアプリケーションとしての意味をもつ。

もう一つの成果は情報ハイディングに関してである。gzip は 特に UNIX 系の OS で広く普及しているデータ圧縮のためのソフトウェアであり、Lempel-Ziv77 符号を原型としている。本研究では gzip で圧縮したファイルに秘密のデータを埋め込むという手法を 4 種類提案する。提案手法を計算機ファイルに適用した場合、いずれの方法も、情報が埋め込まれたファイルから通常の gzip 復号器によってもとファイルが得られる。本研究では、情報が埋め込まれたファイルのサイズと、埋め込むことができる情報の量を実験的に調べる。また gzip で圧縮されたファイルのサイズと、情報が埋め込まれたファイルのサイズが完全に一致するような情報埋め込みの方法が実現できることも示す。提案した手法は本質的にユニバーサルであり、圧縮されるデータがどのようなものであっても適用可能である。提案手法は、gzip の原形である Lempel-Ziv 77 符号の性質というよりはむしろ gzip の実装上の特徴を利用しており、特定のソフトウェアの実装に踏み込むことによって秘密情報の埋め込みができることを(特に圧縮後のファイルサイズを全く変化させることなく)、世界に先駆けて示した。

研究成果

Coding Theorems for General Stegosystems

Proc. 2007 IEEE Int. Symp. Inform. Theory, 2456—2460 2007

gzip のアルゴリズムに基づく情報ハイディング

電子情報通信学会技術研究報告 IT2006-119 2007

情報源符号化およびシャノンの暗号システムに対する一般的な
符号化定理の別形式

電子情報通信学会技術研究報告 IT2006-108 2007