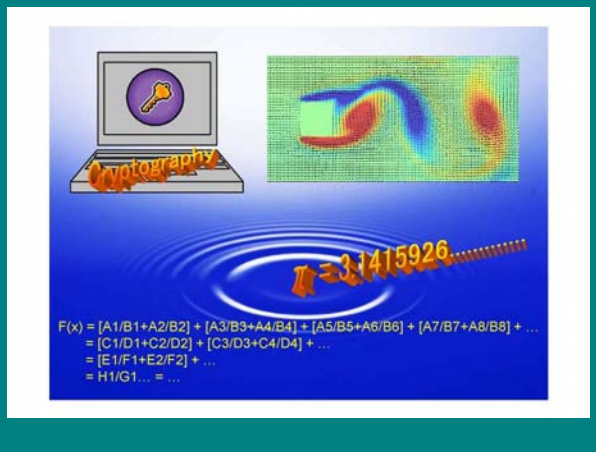
コンピュータとインターネット時代に
数値シュミレーションと暗号技術で
未来を拓く



コンピュータ応用学科

数値シミュレーション研究室

研究内容

テーマ 1　**物理現象の数値シミュレーション**

物理現象をモデル化(偏微分方程式で表現)し、コンピュータの中で模擬実験(数値シミュレーション)します。
地震の多い日本に超高層ビルが建つのは、数値シミュレーションにより耐震設計が可能になったためです。
一方、天気予報はまだまだ 100%的中していません。これは、天気予報の中心となる流れがカオス現象(微小な乱れが全体の様子を大きく変える)を発生させるために予測が難しいためです。
本研究室では、この流れの振る舞い(対称性が崩れる現象など)の原因を数値計算で追究しています。

テーマ 2　**電子社会の安全を保つ暗号技術**

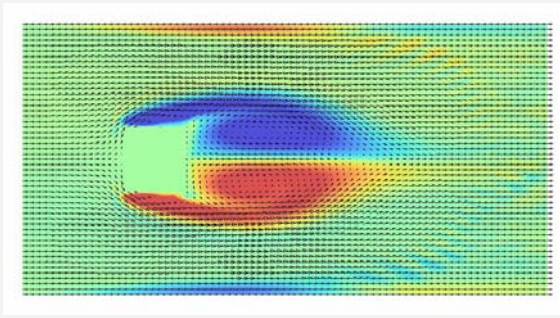
インターネットで情報を送るとき、情報の盗み見を完全に防ぐことはできません。
そのため、途中で見られても内容が分からないように暗号化します。
暗号化の方法として、共通鍵暗号と公開鍵暗号が使用されます。
共通鍵暗号はローマ皇帝シーザーが使用したという、歴史のある暗号方式です。
公開鍵暗号(RSA 暗号)はインターネット時代に考案され、暗号化した鍵では復号(元に戻すこと)はできません。
RSA 暗号は多数桁(1024 ビット、309 桁)の因数分解が困難(スーパーコンで 1000 年)なことを利用しています。
この研究では、RSA 暗号の強度(因数分解の手法と計算時間)に関する研究をしています。

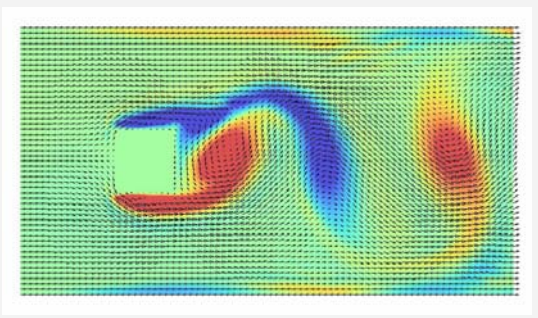
テーマ 3　**数学的手法を用いた投資分析**

過去の株価のデータからより確率の高い投資の基準値を求める方法などを研究しています。

研究テーマ

テーマ 1　**対称な流れの中でおこるカルマン渦の発生原因の究明**





テーマ 2　**RSA 暗号解読(多数桁因数分解)の高速計算方式の研究**

46784543299299809600231907781019994097303462500039946417909378970611300044943
→ 279239975251862285228108683583004507721×167542427466204260138359702876428892183
現在使用されている RSA 暗号は 1024 ビットです。154 桁と 155 桁の素数を掛けて 309 桁(1024 ビット)の数にします。この掛け算は PC(パソコン)で 1 秒間に約 100 万回できます。
しかし、この数を 154 桁と 155 桁の素数に分解するには PC で約 100 万年かかります。

テーマ 3　**多数桁高速計算手法の研究(円周率計算世界記録)**

$\pi = 16\arctan(1/5) - 4\arctan(1/239)$、 DRM 法(分割有理数化法)を考案し、π世界記録に使用しました。

$$\arctan(1/5) = 1/5 - 1/(3\cdot5^3) + 1/(5\cdot5^5) - 1/(7\cdot5^7) + 1/(9\cdot5^9) - 1/(11\cdot5^{11}) + 1/(13\cdot5^{13}) - \cdots$$
$$= (3\cdot5^2-1)/(3\cdot5^3) + (7\cdot5^2-5)/(35\cdot5^7) + (11\cdot5^2-9)/(99\cdot5^{11}) + (15\cdot5^2-13)/(195\cdot5^{15}) + \cdots$$
$$= a_1/(3\cdot5^3) + a_2/(35\cdot5^7) + a_3/(99\cdot5^{11}) + a_4/(195\cdot5^{15}) + \cdots$$
$$= (35\cdot5^4a_1+3a_2)/(3\cdot35\cdot5^7) + (195\cdot5^4a_1+99a_3)/(99\cdot195\cdot5^{15}) + \cdots = \cdots = A/B$$

テーマ 4　**乱数理論による株式の短期投資基準の設定と評価**

株価を中、長期変動(月、年)と短期変動(日、週)に分け、短期変動の大部分を乱数変動と仮定して、数学的仮説を用いて、売り買いの投資判断価格を算出し、評価します

スタッフ

後　保範　　コンピュータ応用学科　教授

情報処理学会 会員
1967 年 早稲田大学理工学部卒、2005 年 博士(工学)
2002 年 11 月 πの 1 兆 2411 億桁計算の世界記録達成
スパーコン出現(1976 年)からスパーコンを使用した大規模数値計算の高速化に取り組む