豊泉　洋　研究室
(応用確率/オペレーションズリサーチ研究)

確率的な事象の本質を捉え、具体的なシステムのより良い使い方を提案

早稲田大学基幹理工学部 応用数理学科
早稲田大学院 会計研究科
http://www.f.waseda.jp/toyoizumi

確率をどんなことに応用するのか？

どんなシステムであってもなんらかの不確実性が存在するものです。ありとあらゆるシステムが対象となり得ます。例えば、

- 遺伝子発見手法
- 量子通信の性能評価
- グループでの暗号通信の最適化
- ストリーミング通信の帯域削減手法
- コンピュータウィルスの撃退法
- 株価の形成理論
- option 価格の評価

などが今までの研究対象です。

グループ暗号通信

確率的な考え方がどのように生かされるかを、グループ暗号通信を題材に検証してみましょう。現在、もっとも日常で使われている暗号通信のひとつとして、公開鍵暗号方式があげられます。しかし、この手順は大規模なグループ通信には不向きです。

スポーツリアルタイム社（架空）

スポーツリアルタイム社は１万人の顧客に向かってスポーツ番組を有料でインターネット生中継しようと計画しています。
１万人に一対一の暗号通信をするためには、一つのデータパケットを１万回（！）も各ユーザー別の公開鍵で暗号化する必要があり、リアルタイムで行うことは、事実上不可能です。スポーツリアルタイム社はインターネットビジネスから撤退するべきなのでしょうか？

グループ鍵を使った暗号化、サブグループ鍵を使った暗号化

スポーツリアルタイム社のエンジニアはこう考えるかもしれません。

「グループ全体が一つの暗号鍵を共有すればいいんだ。そうすれば、ひとつのパケットは一回だけ暗号化すれば良い。」

しかし、セキュリティーを確保するには、グループ鍵の更新が必要です。さらに、グループ内にサブグループの階層を作り、複数のグループ鍵を使うことによって、顧客が脱退や参加した場合のグループ鍵の暗号化回数を削減できるということが提案されている。しかし、

- どの程度暗号回数を減らせるのか？
- 最適なサブグループ数は？

といった疑問に答えるためには、顧客の加入や脱退に伴いランダムに移り変わる顧客数をモデル化しなければなりません。

グループ暗号通信の確率モデル（待ち行列モデル）

そのためのモデル化の手段が下図のような確率モデルです。

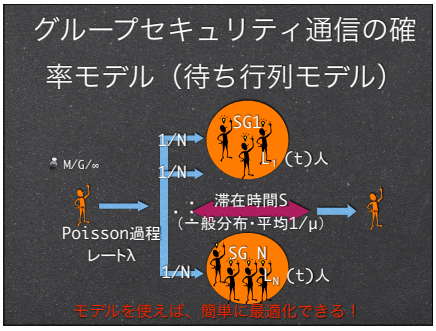

図１：確率モデル

最適なサブグループ数

この確率モデルを使うことにより、最適な暗号化回数を評価することができます。この場合には、１万人の顧客を１００個のグループに分けることによって暗号化回数が最小になることが示されます。

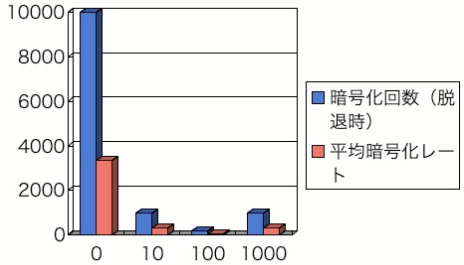

図２：暗号化回数