BitTorrent型分散システムと使い捨てパッドを用いた通信システムの開発

―原理的に完全に安全な暗号システム―

1. 背景

使い捨てパッドとは、平文データと暗号化の鍵とが同じ長さである暗号化方式で、解読が不可能であることが数学的に証明されている。しかしながら、暗号化の鍵が平文データと同じであるために、鍵の配送問題を容易に解決することができず、これまでほとんど使われてこなかった。

2. 目的

使い捨てパッドにおける鍵の配送問題を解決するために、

- BitTorrent 型分散システムによる鍵配信
- 専用ドライバーを用意し、Diffie-Hellman を用いて、通信するマシン間で使い捨てパッドを同時に生成する

という手法を用いた。

3. 開発の内容

開発したソフトはいずれも WindowsXP 上で開発を行ったものである。したがって、WindowsXP での動作が保証されている。

開発したソフトは、組織内特に LAN 内にあるか否かで使われ方が異なる。

LAN 外のマシン同士で通信を行う場合には、使い捨てパッドを分割配信するのが有用である。分割配信にあたっては、配信を中継するサーバーが必要となるが、これを PKI を用いて認証し、なりすましへの対策をおこなっている。

各サーバーは、自身が配信･受信サーバーであると同時に、他のサーバーの中継機能をも持つようになっている。すなわち、本システムは、サーバー同士が互いに強調して、配信を行うようになっている。配信サーバーは、Web サーバー･SMTP サーバーの機能をも併せ持っており、このソフトを起動するだけですべての機能を実現できる。

図 1 にその構成を示す。

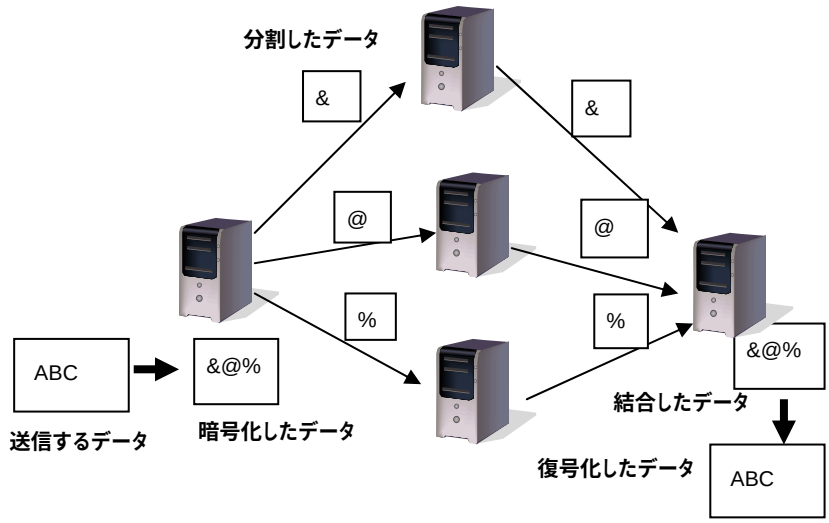

図 1　LAN 外で使用する場合の本システム

一方、LAN 内で使用する場合においては、各マシンにドライバーを導入することにより、全てのパケットを使い捨てパッドで暗号化することが可能になる。この場合、使い捨てパッド自体は Diffie-Hellman によって共有鍵を生成し、それを種とする乱数列を用いるので、通信における鍵配信問題は生じない。

図 2 にその構成を示す。

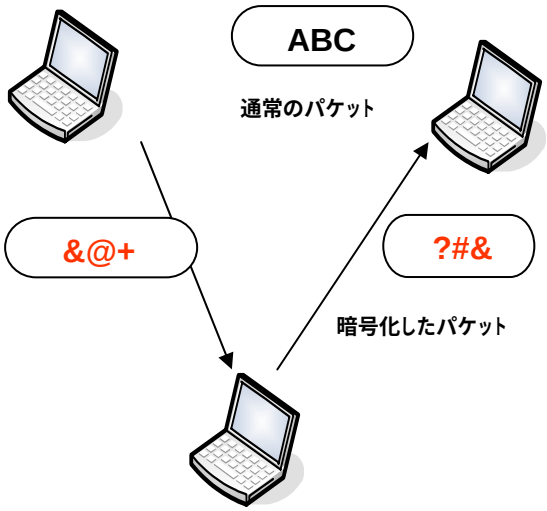

図 2　LAN 内ではパケット単位で暗号化する

4．従来の技術（または機能）との相違

従来の暗号化方式は、基本的には、その時点での計算機の計算能力の範囲内では解読か困難であるというものであったが、本システムでは、原理的に解読が不可能である。

また、暗号化に要する時間も、本システムでは既存の暗号化システムと比較すると高速である。

これらの特徴をそなえつつも、従来の暗号化システムと両立可能であり、既存の暗号化システムの上に本システムを重ねて使用することが可能である。その際に、既存のシステムでのクライアントの変更は必要なく、SMTP サーバーなどの外部に本システムを導入するだけでよい。

5．期待される効果

既存のシステムだけではセキュリティ上の不安がある場合などに、本システムを導入することによって、原理的に安全なシステムの構築が可能となる。

6．普及（または活用）の見通し

具体的な普及に向けた取り組みはまだ始まったばかりである。

7．開発者名（所属）

石井充　（アペイロン）

（参考）開発者ＵＲＬ

http://www.a-peiron.com/tech.html