

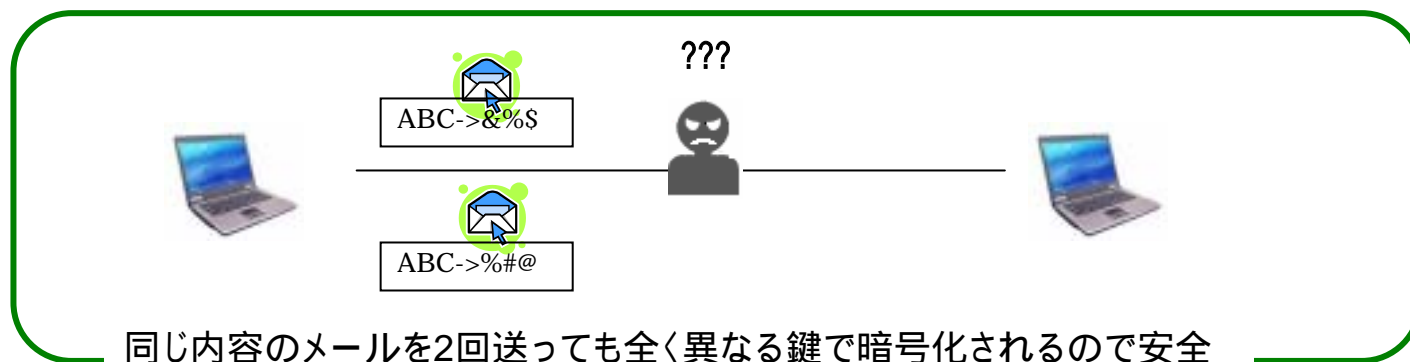
# BitTorrent型分散システムと使い捨てパッドを用いた通信システムの開発

石井 充

使い捨てパッド: **絶対に解読できない**ことが数学的に証明されている暗号



**既存の暗号と異なり100%安全な暗号**



## 既存の問題点

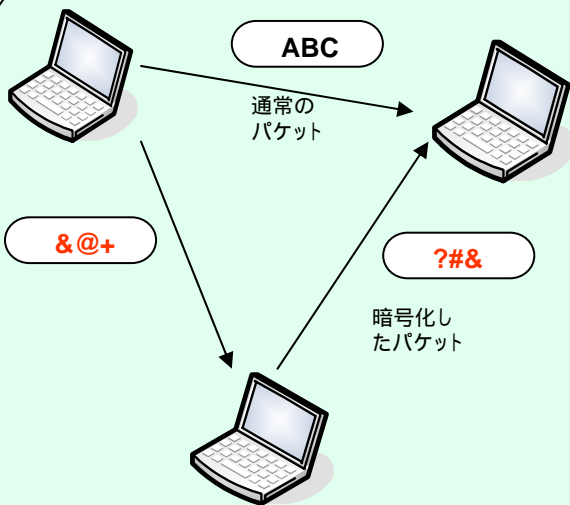
- 使い捨てパッドでは鍵の長さが平文データと同じ
- 鍵を安全に配信する方法がない



## 解決方法

- BitTorrent方式の分散システムを利用
- Diffie-Hellmanを用いて鍵を共有

## 社内LANの場合



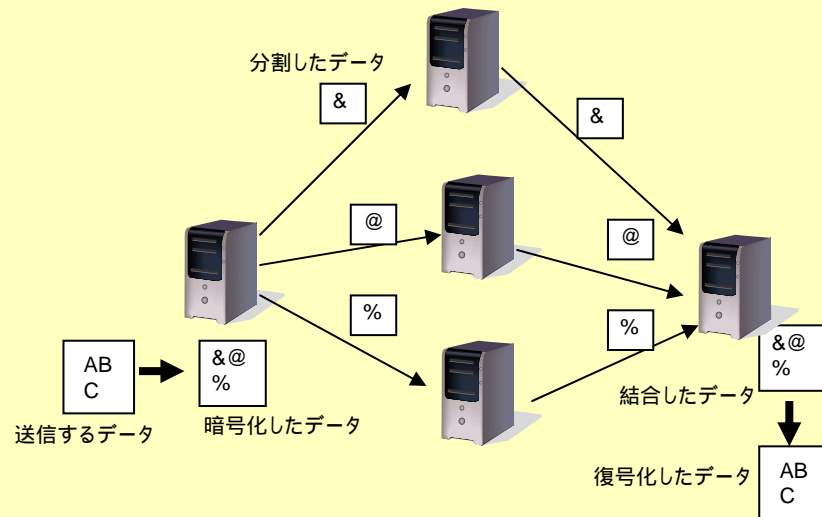
### パケット単位で暗号化

- Diffie-Hellmanによる鍵共有
- TCP/IPのヘッダーまで暗号化
- 暗号化される対象PCを自由に設定可能
- ドライバーをインストールするだけで、特別なソフトは必要なし

```

1  0.C0B00080 01 83 5c ra 0E 1a 57 aa
2  0.C0B02179 0a e4 7c 42 13 14 58 05
3  0.C0B04187 4b 2a 06 76 80 a7 41 01
4  0.C0B06284 aa 32 89 68 23 67 4a 85
5  0.C0B08374 2c 8a 94 89 67 82 8a 02
6  0.C0B0A465 c8 e3 86 5a a3 86 78 8a
7  0.C0B0C556 07 2a b1 08 5a 48 af aa
8  0.C0B0E647 4b 97 da 80 52 89 0c 01
9  0.C0B10738 28 17 43 5a 69 40 79 70
10 0.C0B12829 c7 24 d7 80 07 82 76 04
11 0.C0B14920 bc a7 48 b5 14 c1 a2 80
12 0.C0B17011 0a a9 41 57 a5 78 c8 89
13 0.C0B19102 08 71 54 5a a9 06 9a 03
14 0.C0B1B193 04 87 4b 28 8a e7 86 a2
    
```

## 社外ネットの場合



### 暗号化して分割配信

使い捨てパスワードは毎回  
変わるので盗まれても安全

- 分割して送信・障害対応可能
- 異なる経路で配信して安全を確保
- ハッシュ値を確認し、改ざん対策



両手法を用いて、全通信で使い捨てパッドによる暗号化が可能