

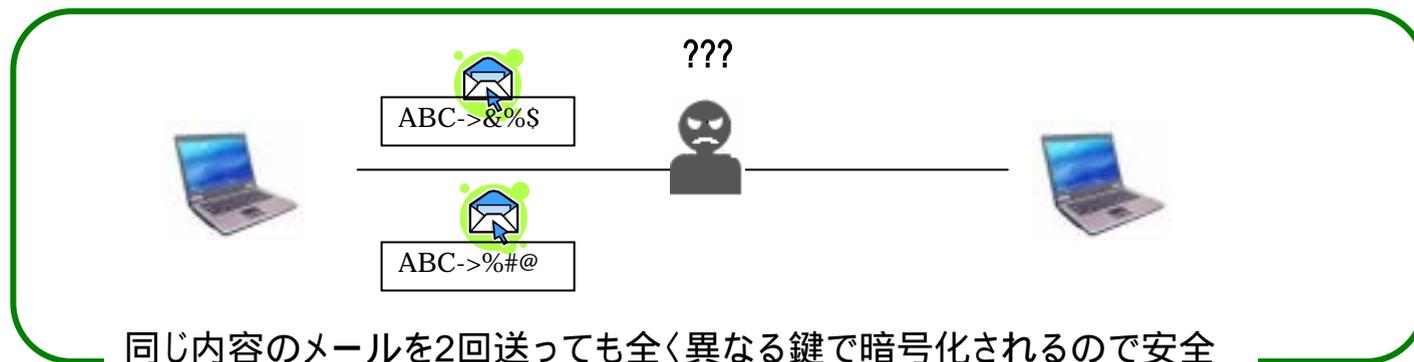
# BitTorrent型分散システムと使い捨てパッドを用いた通信システムの開発

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

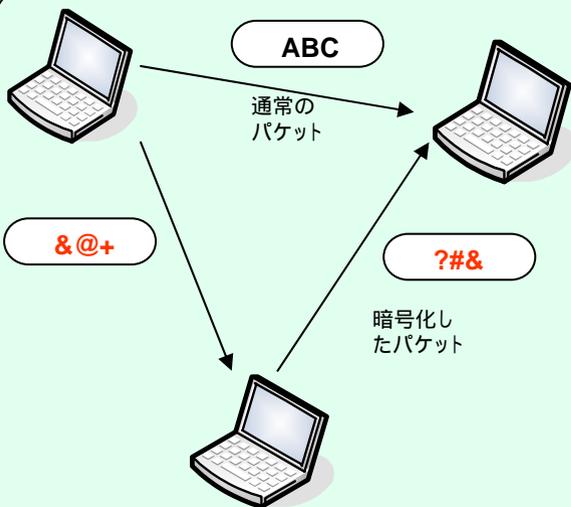
- 使い捨てパッドでは鍵の長さが平文データと同じ
- 鍵を安全に配信する方法がない



## 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

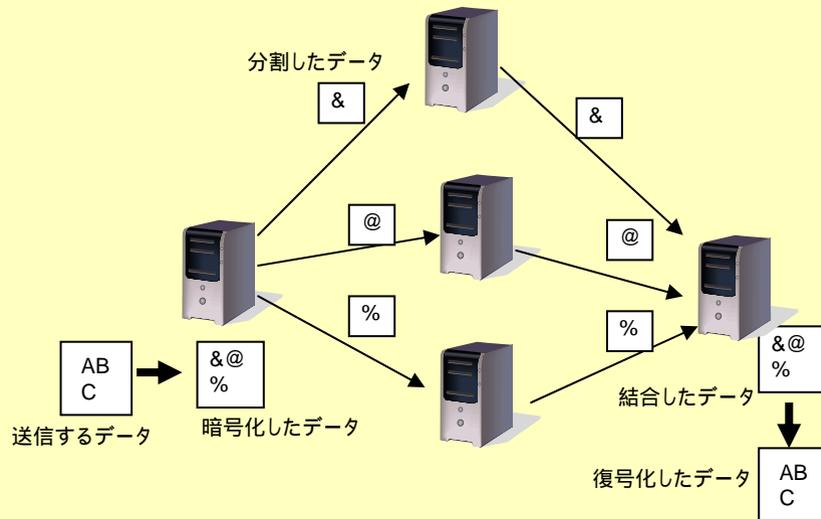


### パケット単位で暗号化

- 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

```
0  0.00000000  01 83 5c 7a 02 1a 57 aa
1  0.00001792  0a e4 7d 42 13 14 58 05
2  0.00003584  4b 2a 06 7b 30 a7 41 01
3  0.00005376  aa 32 69 68 23 67 4a 05
4  0.00007168  2c 9a 94 69 67 62 5a 02
5  0.00008960  c8 e3 98 5a a3 98 78 8c
6  0.00010752  07 2a b1 08 5a 48 af aa
7  0.00012544  4b 97 da 80 52 69 0c 01
8  0.00014336  28 17 43 5a 69 60 79 70
9  0.00016128  c7 24 d7 90 07 82 76 04
10 0.00017920  5c a7 48 b5 14 c1 a2 80
11 0.00019712  0a 69 41 57 a5 78 c8 89
12 0.00021504  08 71 54 5a a9 06 9a 03
13 0.00023296  04 87 4b 28 8c a7 16 a2
```

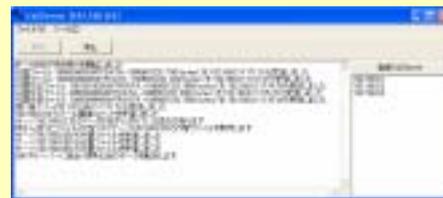
## 社外ネットの場合



### 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