METEORA SYSTEM

Post-BB84 コンセプト

数学的な防衛

メテオーラ・システム株式会社（神奈川県伊勢原市，代表渡邊栄治）は，1970 年代から情報理論の研究とその実装技術の開発を進めてきました．今後は，ゼロトラスト・ソリューションを開発されている企業様への技術提供等を模索して参ります．協業，共創に関するお問合せをお待ちしております．

Contents

1．はじめに

最近の研究開発に依れば，量子鍵配送が数十キロから数百キロに延びたといいます．どちらも実用にならない話です．当社の発明を活用すると，BB84 の特色を全て引き継いで，それ以上の利便性をもたらす，言わば Post-BB84 を実現することができます．本リリースでは，その存在を情報理論の視点で紹介します．

C．E．Shannon が情報を数学に乗せて以来，「ビット」という言葉が常識用語になりました．他方，**データと情報は違います**．データの流れは目に見えますが，情報の流れは目に見えません．だから，一つの問題にデータと情報が行う評価は異なります．事例がいくつかあります．”A Mathematical Theory of Communication” の 20 ページはその一つです（1948 年）．そして，Polar 符号もその一つです．

プログラマが目に見えるデータを追いかけるのは当然そう有るべきことですが，IT の研究者が全員プログラマになってしまったのは一体どうしたことでしょうか？プログラマは BB84 フォトンをデータの流れとして見ます．だから雑音チャネルが見えません．プログラマは誤り訂正チャネルが雑音チャネルのインラインに無いことに疑問を感じません．

BB84 は中間者攻撃に対して量子現象が働くので，そこに魅力を感じている人が多いと思いますが，Post-BB84 の Mod2 演算雑音チャネルを知るようになれば，感動を覚えるかも知れません．このチャネルは，Shannon の通信ライン，当社の発明，それと物理乱数 256[bit]/ブロックから成ります．

このチャネルに盗聴を仕掛けるとどうなるでしょう？盗聴者が観測をしていない時，1）Mod2 演算雑音チャネルはセッション鍵の消費と生成を繰り返します．これは鍵配送の実行を意味します．2）観測が始まると，つまり，盗聴者が通信ラインから情報を盗む時，それは必然的に Mod2 演算雑音チャネルの時間積分です．3）その時

間積分の最中にセッション鍵は自らを消去します．4）セッション鍵が消えた後，情報チャネルは，特定の情報エントロピー，512[bit] に収縮します．

このように，観測していない時，セッション鍵は消費と生成を繰り返し，観測が始まると，観測時点から現在に至るセッション鍵は自らを消去し，結果チャネルは必ず特定の情報エントロピーに収縮します．この情報チャネルの観測と情報チャネルの収縮，これは驚くべきことか量子力学における観測と確率波の収縮の解釈に対応しています．当社はこのコンセプトを，BB84 を引き継ぐ Post-BB84 として名付けています．

Post-BB84 は現状の BB84 の欠点を克服しています．なぜなら，鍵の消費と生成を繰り返している間 = ウイルスが鍵を悪用していない間，”A Mathematical Theory of Communication” に示された伝送レート R は理論上の最大値を達成するからです．

2．Post-BB84 の利便性

1．乱数がフォトンを符号化するのではなく，乱数が乱数を符号化するので，特殊な Fiber に頼る必要はありません．
2．利用距離の制限がありません．ネットワークは End - End 通信です．
3．今の軍事用の通信設備は固定の拠点に限られます．この制限が外れます．
4．通信プロトコル TCP/IP のトポロジーと互換です．
5．特別の中継設備を開発する必要がありません．
6．量子コンピュータは脅威になりません．
7．物理乱数 ASIC を利用することで，超小型衛星やドローンにも搭載可能です．
8．特定の運用技術に頼る必要はありません．
9．マンパワーが不要です．運用コストがインターネット並みです．

3．第五の戦場を制する“数学的な防衛線”

通常，以下の 5 項目には対策技術がありません．今の TCP/IP は「IP アドレスとポート番号」を指定すればどこともコネクションを張るので，ウイルスやバックドアには都合の良いプロトコルです．が，Post-BB84 はサイバー攻撃の時代を終わらせることができます．Post-BB84 はサブネットの境界に「数学的な防衛線」を提供します．すなわち「The CeanNet」が実現します．アルゴリズムは驚くほどシンプルです．

1. While cyberattacks are a way of fighting in favor of the weak, cyber defense is impossible even for the strong.
2. The targeted tissue is unaware of the virus infection.
3. By the time you notice, the virus operation has already ended.
4. The virus begins its operation without a declaration of war.
5. There are always backdoor concerns.

4．Inquiries about this release

METEORA SYSTEM Co., Ltd

https://www.meteora-system.com

