平成 22 年 11 月 29 日

資料

超高速クラウド・コンピューテイング・システムのニーズの高まりに合わせて、超高速暗号技術の開発が望まれている。ストリーム暗号は高速な暗号通信に適しているが、現状のストリーム暗号はいくつかの重要な問題点が存在する。特に典型的なストリーム暗号は、平文と秘密鍵から伸長された鍵ストリームとの排他的論理和により暗号文を生成している。正規受信者は暗号文から平文を得るには単に逆算を実行すればよい。ところが攻撃者が暗号文を傍受して、それを改ざんして置き換える“改ざん攻撃”が実施された場合、正規受信者は確実に改ざんされた平文を受け取ることになる。このような改ざんは既知平文攻撃の場合に特に深刻であり、たとえ真性乱数を鍵に用いる鍵使い捨て暗号でも防げない。すなわち通常のストリーム暗号では、改ざんの危険性は常に存在する。以上のように、安全性の保証と改ざんへの耐性、あるいは検知は暗号学においては重い課題である。

【Y-00 光通信量子暗号の実現方式の比較】

物理暗号である Y-00 光通信量子暗号は正規受信者と盗聴者の受信特性が異なる状態を意図的に構成できるため、改ざんに対してある程度の耐性があることが期待できる。Y-00 光通信量子暗号の実現法には、現在 2 種類の方式がある。

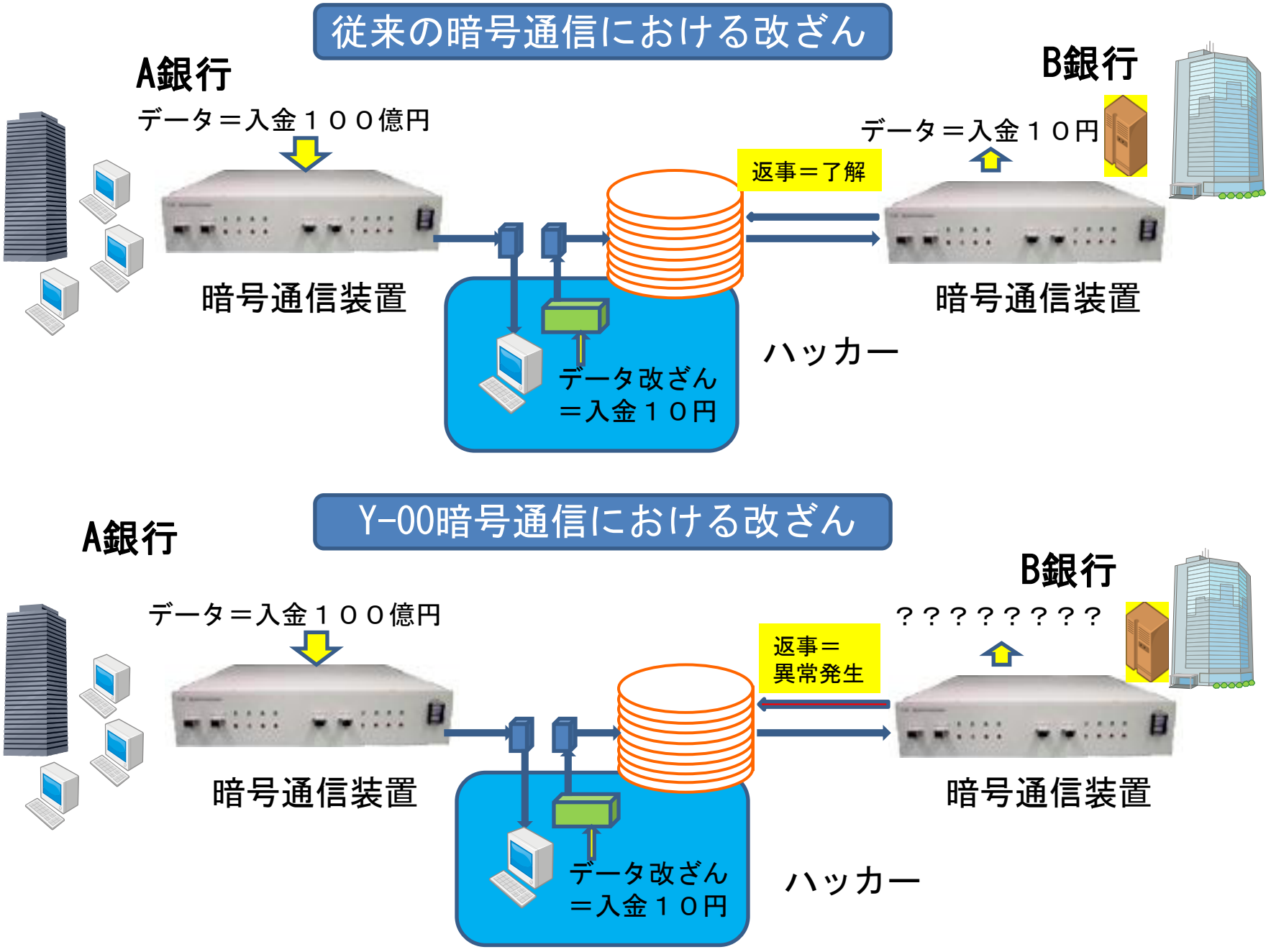
一つは光の位相を変調パラメータとして利用する位相変調方式 Y-00 であり、アメリカのノースウエスタン大学とベンチャー企業である Nucrypt 社によって開発がすすめられている。現在、2.5Gbit/sec で 500km 伝送可能なシステムが実現されている。もう一方は、光の強度を変調パラメータとして利用する強度変調方式 Y-00 であり、玉川大学と日立情報通信エンジニアリングによって開発がすすめられている。これも、2.5Gbit/sec では 500km, 10Gbit/sec では 300km 伝送可能なシステムが実現されている。位相変調などの光のコヒーレンスを応用する場合には、量子雑音が極めて小さいため、通信データのスクランブルへの量子効果も小さい。それに比べて、強度変調方式では、量子雑音はショット雑音としてスクランブルに寄与するため、量子効果が大きい。その結果、改ざん耐性は強度変調方式のみが持つことが示された。

１．鍵使い捨て暗号（One time pad、あるいはバーナム暗号と呼ばれる）

擬似乱数の代わりに、真正乱数を利用するストリーム暗号の一種である。Y-00 量子暗号は擬似乱数と量子雑音を併用するストリーム暗号の一種

２．ストリーム暗号

通信データは一般に１と０の系列で表現される。このデータ系列を暗号化するために、ひとつの鍵を擬似乱数生成器によって伸長した乱数系列によって、その通信データ系列をスクランブルする暗号形式


従来の暗号通信における改ざん
A銀行
データ＝入金１００億円
暗号通信装置
B銀行
データ＝入金１０円
返事＝了解
暗号通信装置
ハッカー
データ改ざん
＝入金１０円
Y-00暗号通信における改ざん
A銀行
データ＝入金１００億円
暗号通信装置
B銀行
？？？？？？？？
返事＝
異常発生
暗号通信装置
ハッカー
データ改ざん
＝入金１０円