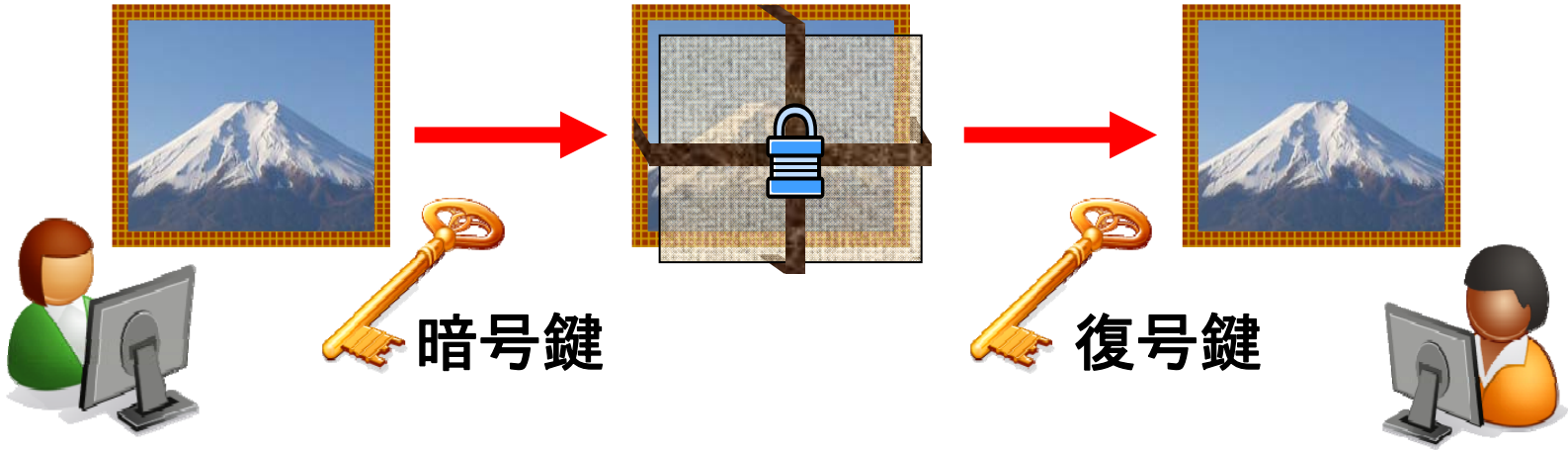
量子暗号とは

量子暗号の必要性

・インターネット上での安全な商取引や個人情報の保護、機密情報の流出防止など、情報の安全性確保への要求は日々高まっています。現在の光ファイバー回線では、悪意のある第3者が敷設管にアクセスし、漏れ光から情報を盗みることは難しいことではありません。そこで、光伝送路の安全性を守る暗号技術が必要となってきます。

暗号とは



・暗号とは、メッセージを暗号鍵と呼ばれる秘密の文字列で変換し、他人に盗み見られないようにする方法です。共通鍵暗号（付録参照）と呼ばれるものは、受け手は、送り手と同じ鍵を使ってメッセージを復元します。従って事前に送り手と受け手の間で鍵を安全に渡す手段が必要となります。暗号鍵が分からない盗聴者は、暗号文の文字パターンの偏りなどから、メッセージを解読しようとしますが、一般に暗号鍵を長くすると、解読は指数関数的に困難になります。現在安全とされている共通鍵暗号は鍵の長さが128ビット以上のものです。

研究開発の背景

一方、公開鍵暗号(付録参照)という方式も現在広く利用されています。特に1970年代後半に開発されたRSA(Rivest, Shamir, Adleman)暗号と呼ばれる暗号は、現在のインターネットを使った商取引に革命をもたらしました。整数論に基づくこの暗号技術は、非常に大きな数の素因数分解の難しさを利用し、共通鍵暗号の鍵配布の問題を解決しました。例えば、

191207＝X×Y？

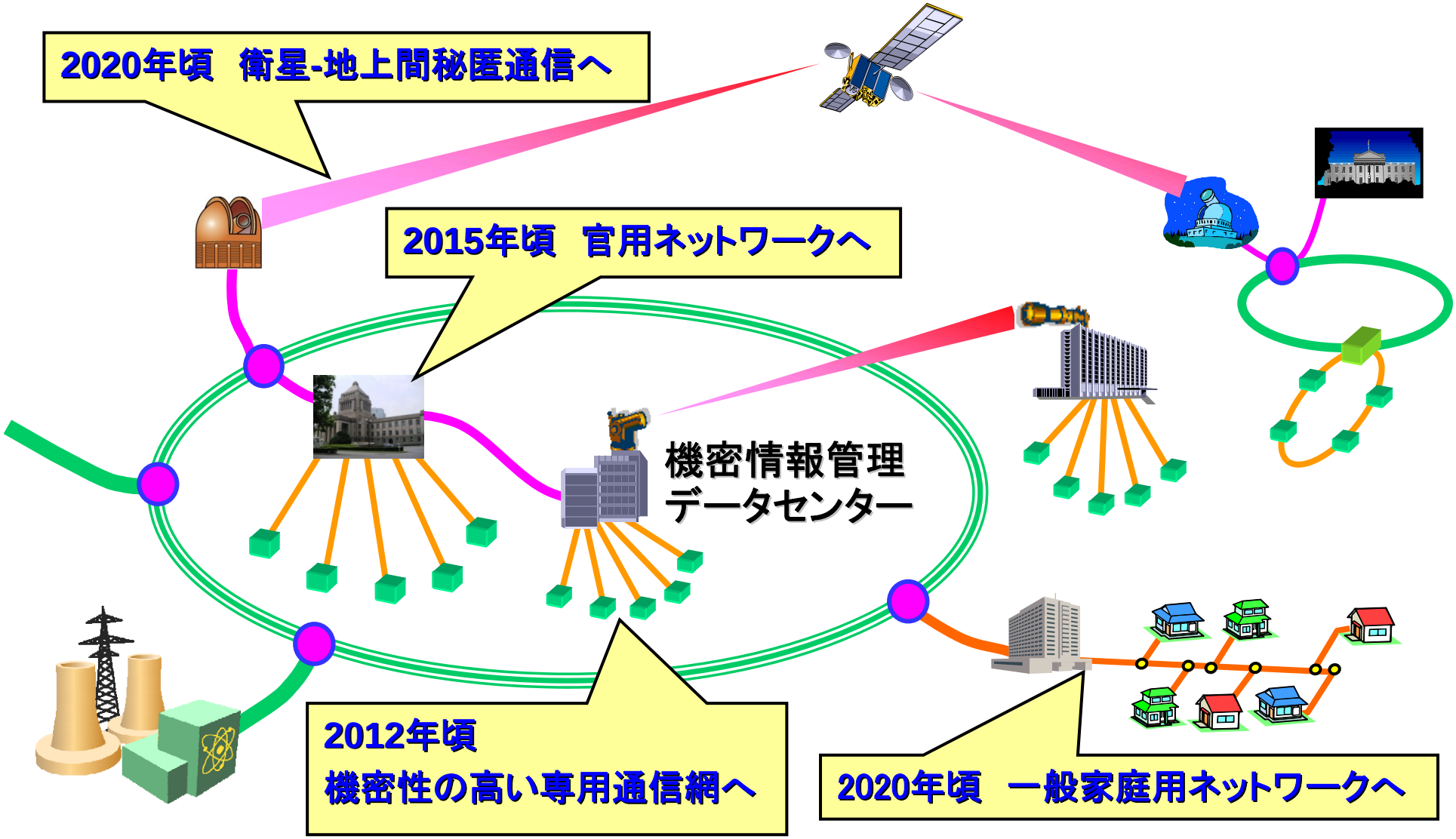
のような素因数分解で、受け手は、367×521であることをあらかじめ知っていて、これから公開鍵と秘密鍵の2つの鍵を作り、電話帳のようなものに公開鍵を公開します。送り手は、公開情報から相手を探し、その公開鍵で送りたい情報を暗号化し送ります。復号は受け手の秘密鍵でしか行えません。

盗聴はこの素因数分解を解く必要がありますが、素因数分解すべき数字の桁数が増えると、計算量は莫大になり、実質的に解読できません。しかし、この方法も、そして先に紹介した共通鍵暗号も、将来、新しい解読法が発見されたり、コンピュータの能力が飛躍的に向上すると、短時間で解読されてしまうという危険性をはらんでいます。これを計算量的な安全性と言います。

量子暗号

これに対して量子暗号は、***将来的に技術が進歩しても絶対に破られることのない***次世代暗号技術として、注目されています。

量子暗号の実用化イメージ



量子暗号とは（1）

量子暗号は、アルゴリズムの複雑さではなく、量子力学理論と単一光子の組み合わせを用いた物理学で安全性を実現する技術です。量子暗号は正確には、量子鍵配送と、Shannonにより情報理論的な安全性が証明されたOne-Time Pad暗号法を組み合わせてできた、誰にも破ることのできない究極の暗号法です。

（1982年にCharles Bennett氏とGiles Brassard氏が発明しました。）

量子暗号　≈　量子鍵配送（QKD）　＋　One-Time Pad暗号

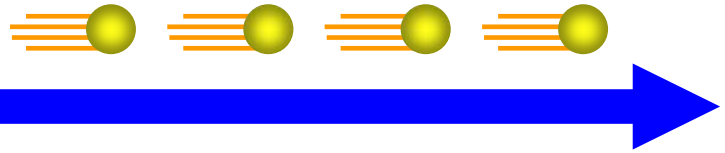
その方法は次の3つのステップから成ります。

（1）暗号鍵（乱数表（列））の伝送＜量子鍵配送＞

乱数列

0101101

光子で乱数列を配送



乱数列

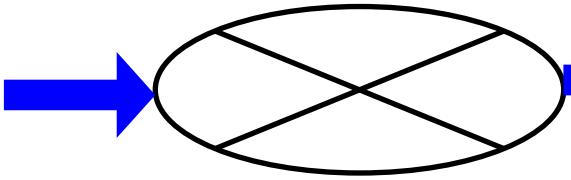
0101101

量子暗号とは(2)

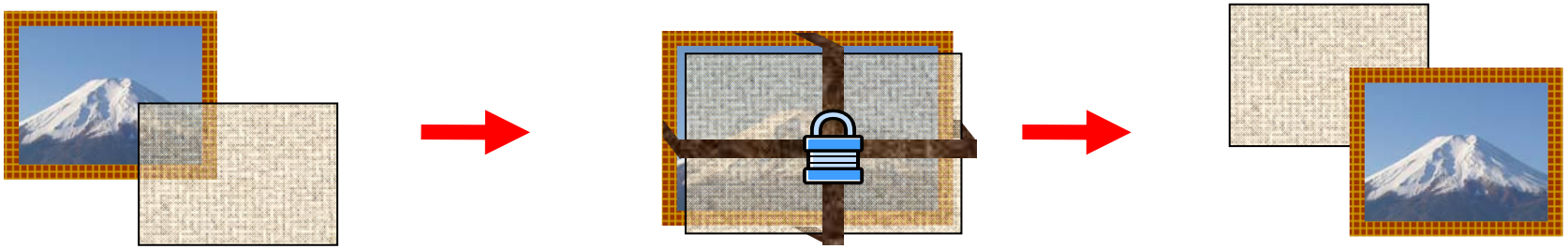
(2)(1)で共有した乱数列に、同じ情報量(長さ)の送信したい文(平文という)を其々のビット毎、足し算*して公衆回線で送信<One-Time Pad>。
逆に、受信者は(1)で共有した乱数列を引き算して平文を取り出す。

＊桁上がりが面倒なので
2の剰余系上で計算。

平　文	1001001
＋)乱数列	0101101
暗号文	1100100



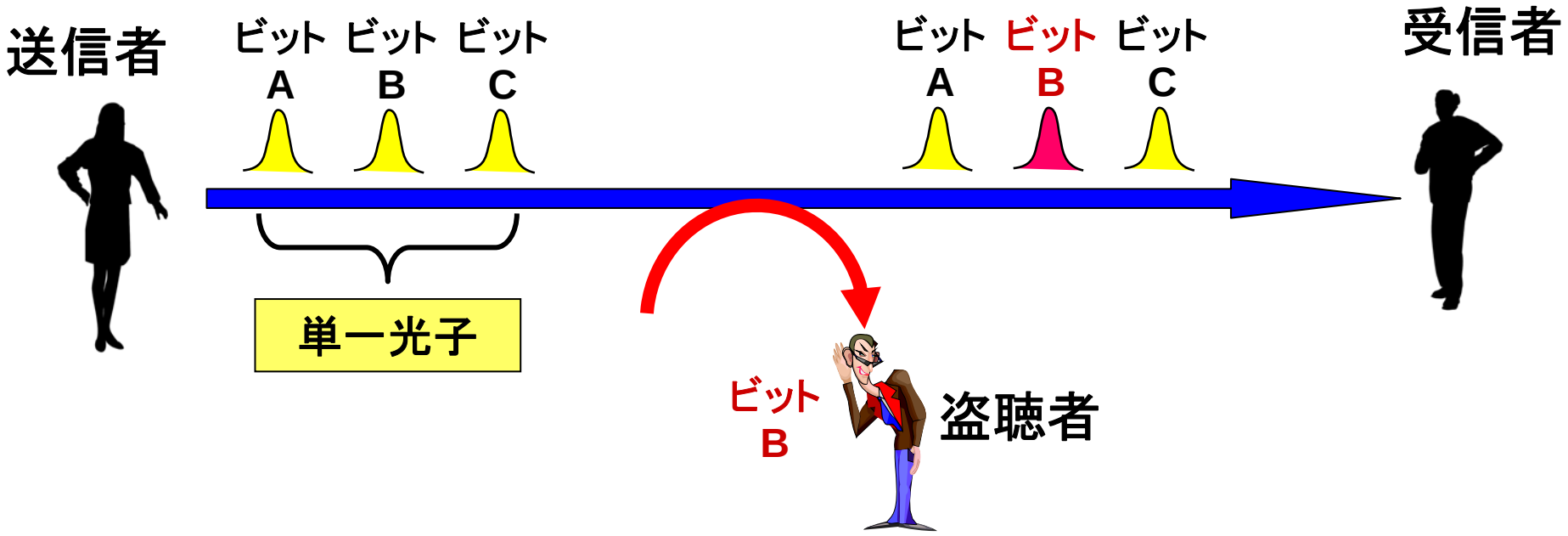
暗号文	1100100
－) 乱数列	0101101
平　文	1001001



(3)(2)で使用した乱数列を破棄し、2度と使用しない<One-Time Pad>。
追加の暗号通信は、量子鍵配送(1)から新たに行います。こうすることで
量子鍵配送で作られた乱数列が解らなければ、盗聴者は解読できません。

量子鍵配送

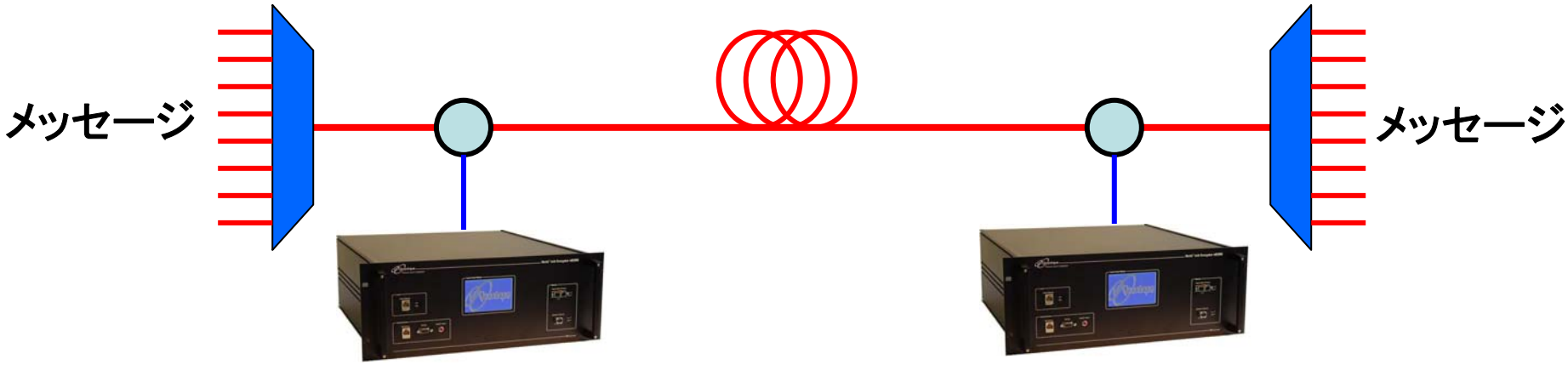
量子暗号の最大の特徴である、量子鍵配送について説明します。量子鍵配送は、微弱な光が持つ粒子（光子）の物理的性質を利用します。暗号鍵の共有作業の途中で誰かが鍵を盗むと、光子の状態に必ず痕跡が残り、受け手は盗聴を必ず検知できます（量子力学の不確定性原理）。



量子暗号の安全性は解読の計算量には依存しないため、将来どんなに科学技術が進歩しても、絶対に盗み見られることのない安全な暗号通信が可能になります。

量子暗号の研究開発の現状

都市圏内における量子暗号の実用化に向けて、世界で活発な研究開発が進んでいます。



・欧米ベンチャーによる製品化
（伝送距離～25km、鍵生成速度～1万ビット/秒）
・id Quantique社（スイス）
・MagiQ Technologies社（米国）

・ヨーロッパでは、2008年10月に、研究所と企業が共同でウィーン市内において量子暗号ネットワークの野外実証実験を実施(SECOQC project)

・国内では、総務省・NICTが2001年より、量子暗号技術の研究開発の支援を始め、 NEC、三菱電機、NTTなどが商用に向けた技術を開発中。

（付録）共通鍵暗号と公開鍵暗号の特徴

（1）共通鍵暗号は、暗号と復号で同じ鍵（共通の鍵）を使う暗号化方式

- 古代より利用されている
- 基本的にはアルゴリズムを含め巨大な乱数表を共有していることに相当する。
- 共通鍵をどのように暗号通信相手に安全に渡すか（鍵配送）が課題
- 代表的なブロック暗号など、高速な処理が特徴（但し、安全性は計算量に依存）
- 唯一、情報理論的に安全性が証明されたOne-time pad暗号もこれに含まれるが、やはり安全な鍵配送が課題　⇒　量子鍵配送

（2）公開鍵暗号は、暗号と復号で異なる鍵を使う暗号化方式

- 1976年以降登場した新しい暗号方式
- 公開鍵と秘密鍵の2つの鍵を使う。公開鍵で暗号化されたものは秘密鍵でしか復号できないし、逆に秘密鍵で暗号化されたものは公開鍵でしか復号できない
- その公開されている鍵を使えば、誰とでも暗号通信ができる
- 公開鍵や暗号文から、秘密鍵を取り出すことは、計算量的に困難（情報理論的×）
- 処理は共通鍵暗号に比べ非常に遅い。従って多くの場合、高速な共通鍵暗号の共通鍵を公開鍵暗号の公開鍵で暗号化して送り、受信者は公開鍵暗号のもう一方の鍵である秘密鍵で解き、共通鍵暗号の鍵を抽出。以降は、高速な共通鍵暗号で暗号化通信を行う、ハイブリッドとしての利用が一般的
- 公開鍵暗号は、秘匿通信のみならず、デジタル署名や第三者認証、ゼロ知識証明などの現代の暗号プロトコルの主役
- 数千ビット以上の量子計算機が登場したら、現在の公開鍵暗号基盤は崩壊