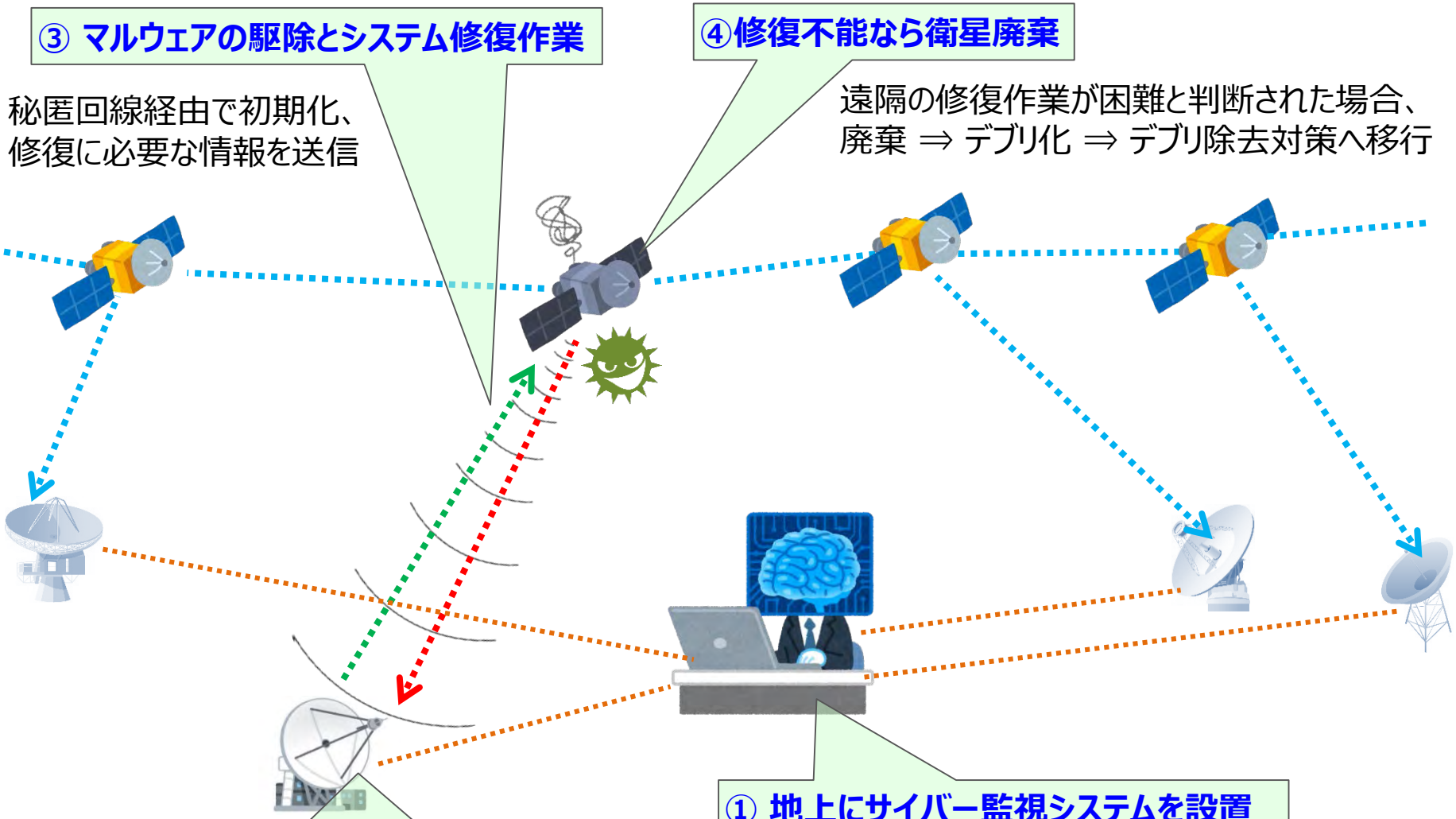
サイバー攻撃への対策（マルウェアの監視と駆除）



秘匿回線で地上局から即座に衛星通信
停止を指令、感染拡大を未然に防止

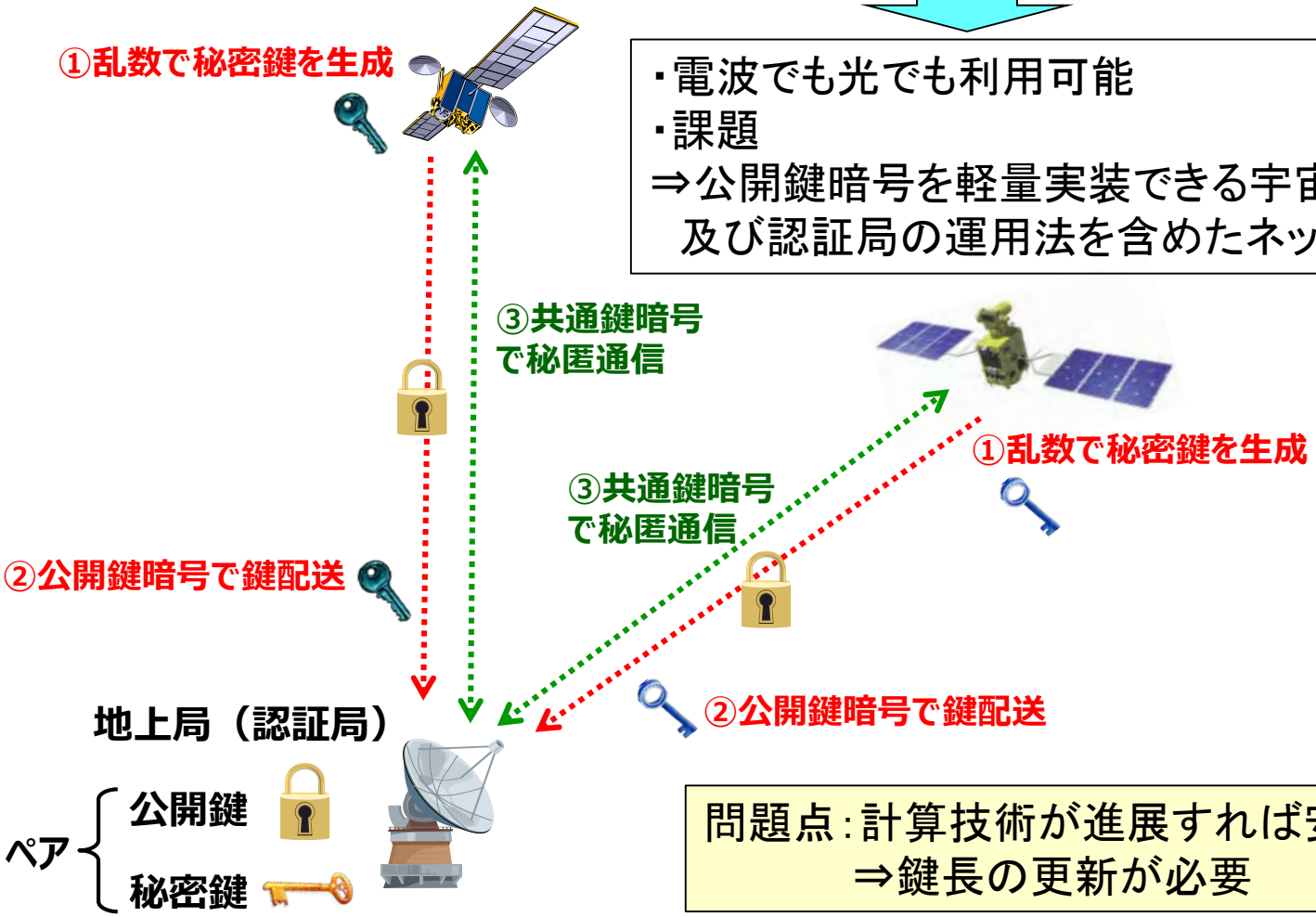
通信パケットのメタデータを収集
⇒AIで通信トラフィックを監視
⇒マルウェア感染をいち早く検知

盗聴、改竄への対策：現代暗号

地上インターネットで使われている暗号技術を衛星通信網に実装

・公開鍵暗号による鍵配送（1対多、多対1）
・共通鍵暗号による通信の暗号化

・電波でも光でも利用可能
・課題
⇒公開鍵暗号を軽量実装できる宇宙仕様のチップ開発、
及び認証局の運用法を含めたネットワーク設計

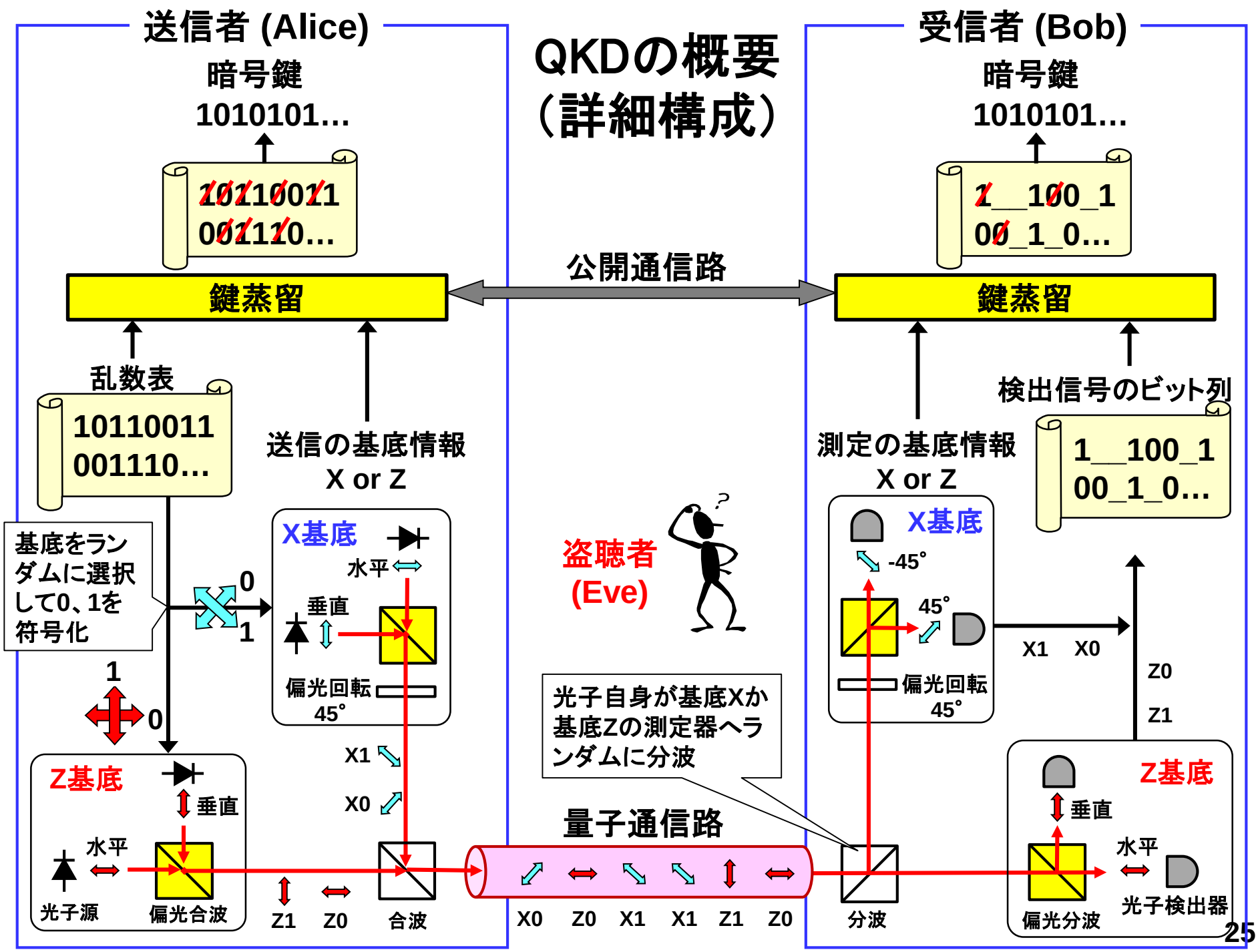


問題点：計算技術が進展すれば安全性は危殆化
⇒鍵長の更新が必要

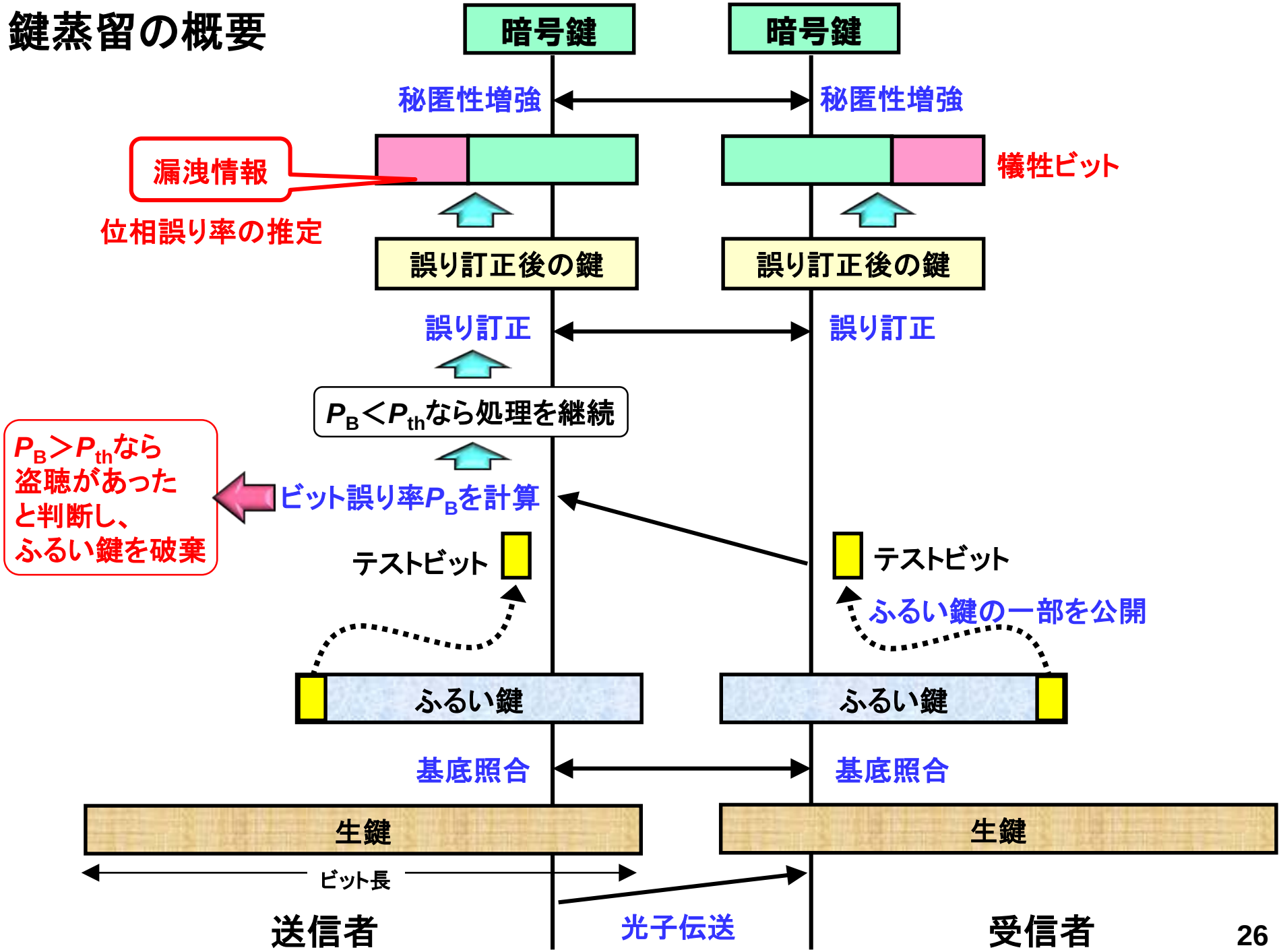
補足資料2

量子鍵配送（QKD）の仕組み

QKDの概要（詳細構成）


送信者 (Alice)
暗号鍵
1010101…
10110011
001110…
鍵蒸留
乱数表
10110011
001110…
送信の基底情報
X or Z
基底をランダムに選択して0、1を符号化
0
1
1
0
X基底
水平
垂直
偏光回転
45°
Z基底
垂直
水平
光子源
偏光合波
X1
X0
Z1
Z0
合波
公開通信路
盗聴者
(Eve)
光子自身が基底Xか基底Zの測定器へランダムに分波
量子通信路
X0
Z0
X1
X1
Z1
Z0
分波
受信者 (Bob)
暗号鍵
1010101…
1__100_1
00_1_0…
鍵蒸留
検出信号のビット列
1__100_1
00_1_0…
測定の基底情報
X or Z
X基底
-45°
45°
偏光回転
45°
X1
X0
Z0
Z1
Z基底
垂直
水平
偏光分波
光子検出器

鍵蒸留の概要


暗号鍵
暗号鍵
秘匿性増強
秘匿性増強
漏洩情報
犠牲ビット
位相誤り率の推定
誤り訂正後の鍵
誤り訂正後の鍵
誤り訂正
誤り訂正
$P_B < P_{th}$なら処理を継続
$P_B > P_{th}$なら
盗聴があった
と判断し、
ふるい鍵を破棄
ビット誤り率P_Bを計算
テストビット
テストビット
ふるい鍵の一部を公開
ふるい鍵
ふるい鍵
基底照合
基底照合
生鍵
生鍵
ビット長
送信者
光子伝送
受信者

基底照合、誤り率評価のイメージ

		1	0	1	1	0	0	1	1	0	0	1	1	1	0	1	0	0	0
送信者 Alice	送信基底	✚	⊠	✚	✚	⊠	⊠	✚	✚	⊠	✚	⊠	⊠	✚	✚	✚	⊠	✚	⊠
	送信信号	↕	↗	↕	↕	↗	↗	↕	↕	↗	↔	↘	↘	↕	↔			↔	↗
受信者 Bob	測定基底	✚	✚	⊠	✚	⊠	⊠	⊠	✚	⊠	✚	✚	⊠	⊠	✚	⊠	✚	✚	⊠
	検出信号	↕	—	—	↕	↗	↘	—	↕	↗	↔	—	↘	—	↔	—	—	↔	↗
	検出ビット	1	—	—	1	0	1	—	1	0	0	—	1	—	1	—	—	0	0

基底照合：送受信者の基底が一致するスロットのみを選択 ⇒ ふるい鍵

双方でチェック	テストビット	○					x				○						
	ふるい鍵				1	0			1	0			1		1			0	0

誤り率を評価

鍵蒸留処理

安全な乱数列を生成　11010…