電波の4次元的ゆらぎと伝播相反性を利用した秘密鍵共有技術

工学部　情報工学系
教授　大平　孝

新技術の概要

情報を無線で交換する機会が増えてきた

一方で情報セキュリティの重要性も増している

データの暗号化は有効な手段であるが鍵配信が問題

そこで鍵を配信せずに共有する方法はないか

電波伝播の相反性を利用して鍵を共有

電波が４次元的にゆらぐことを利用して盗聴防止

いつでもどこでも鍵を自動生成

パスワード・暗証番号覚えなくても

鍵サーバ不要　鍵束不要　使い捨ての秘密鍵

デジタルデバイド解消　安全安心の情報交換

研究背景(1)

背景A	背景B	背景C
企業情報	個人情報	情報通信手段
⇩	⇩	⇩
コンプライアンス	保護	ワイヤレス化

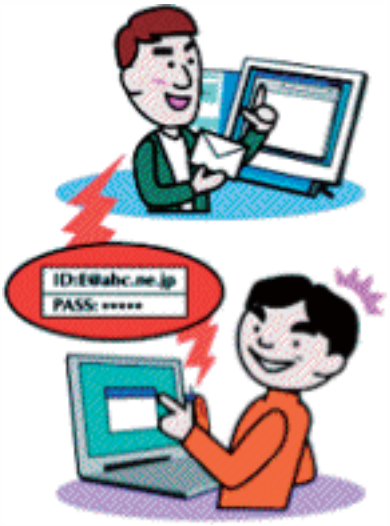
無線＝
　　便利・当然、コードからの人類開放
暗号化＝
　　有効な盗聴対策、鍵の発行共有が必要

研究背景(2)

無線＝どこでも使えて便利

しかし

・・無防備で送ると・・



盗聴　踏み台　漏洩　侵入　破壊　改ざん　ウィルス

想定される用途(1)

乱数性／ランダム性

数学的手法でない、自然環境の時空間的な複雑性を利用

⇩

用途：全く不規則な鍵、信号、数列、符号の生成

相反性／可逆性

離れた場所で同時に鍵生成すると同じ鍵となる

⇩

用途：合い言葉、パスワード発行、相手確認

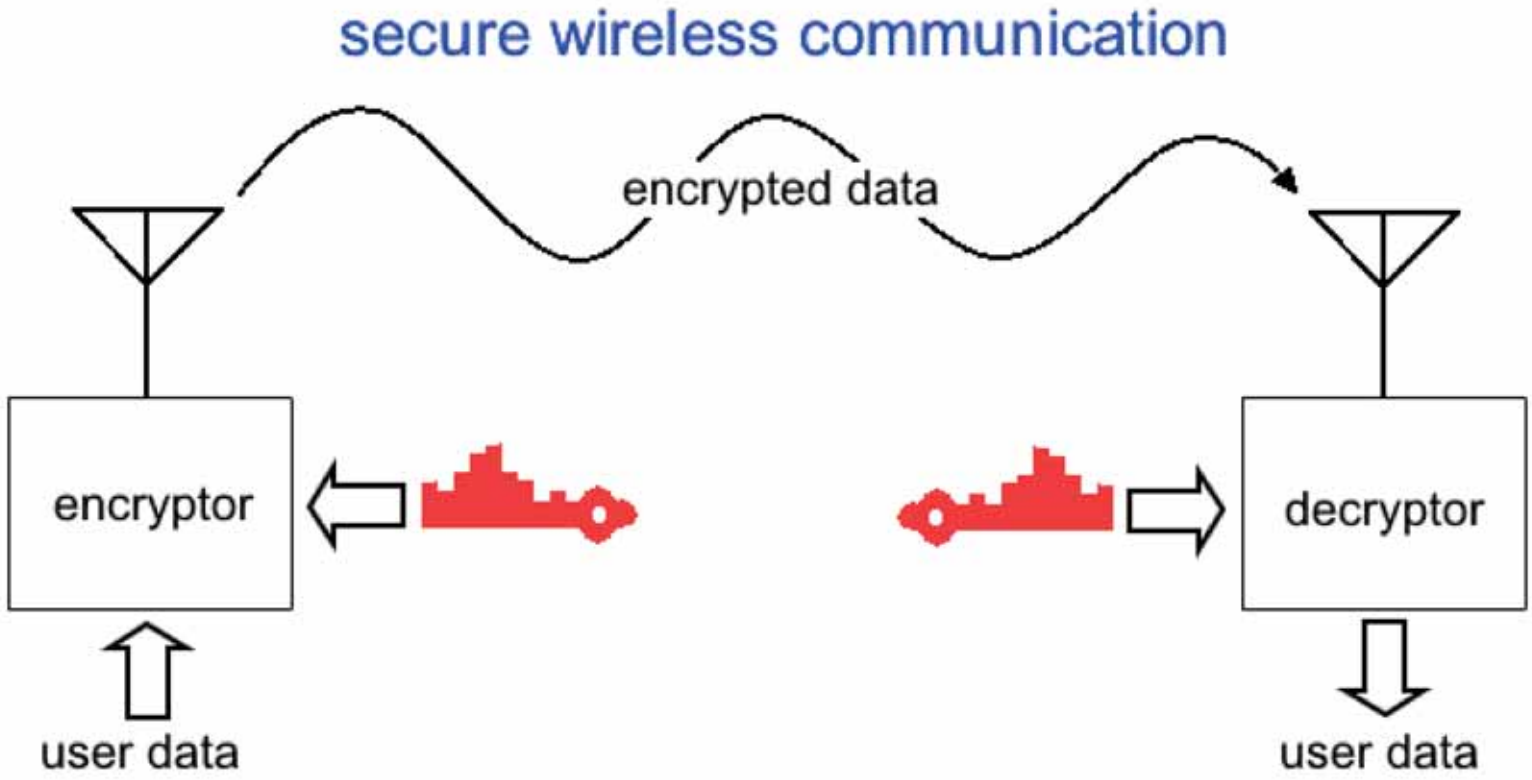
汎用性／万人性

人為的手法でない、人手を介さない、覚えなくてよい

⇩

用途： 操作不要、種が不要、鍵束不要
鍵サーバ不要、デジタルデバイド解消

想定される用途(2)



共通鍵ができると
頑強な無線リンクが実現

想定される用途(3)

共通鍵が応用できる
2種類の無線シナリオ

不特定多数アクセス

ホテルロビー、カフェ
ラウンジ、無線スポット

認証なしの利用

限定利用アクセス

オフィス、工場、学校

認証を伴う利用

想定される業界

盗聴されたくない個人情報交換

高い秘匿性を必要とする企業通信

不特定多数の利用者がアクセスする無線サーバ

高額商取引決済

防衛指揮系統無線通信

防犯警備無線指令

高エネルギー施設制御通信

危険物制御通信

従来技術とその問題点

熱雑音を用いた乱数発生

○ 自然現象を用いているため不規則性が高い

× 離れた場所へ送る手段ではない

鍵情報を紙またはメモリなどのメディアで手渡し

○ 情報量的（物理的）に安全性を担保

× 人手を介する

公開鍵方式

○ 広く使われている

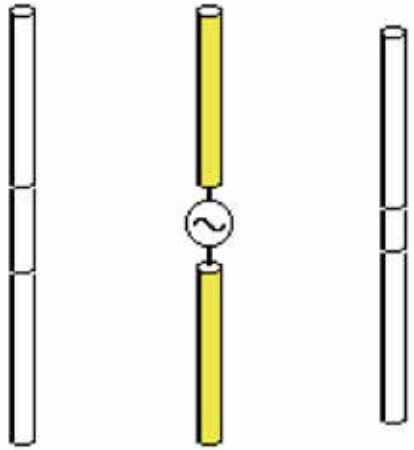
× 計算量的（数学的）に安全性を担保

量子暗号

○ 情報量的（物理的）に安全性を担保

× ハードウェアが高価

八木宇田アンテナ



H. Yagi and S. Uda, "Projector of the sharpest beam of electric waves",
Proc. Imperial Academy Japan, 2, 2, pp.49-52, Feb. 1926.

- 日本からの発明（昭和元年）
- 主素子の近傍にパラサイト素子を配置
- パラサイト素子の長さを少し変えるだけで「導波器」が「反射器」に

新技術の基となる研究成果・技術（2）

電波伝播の相反定理

upLink P_{T1} → $P_{R2} = A_{21} P_{T1}$

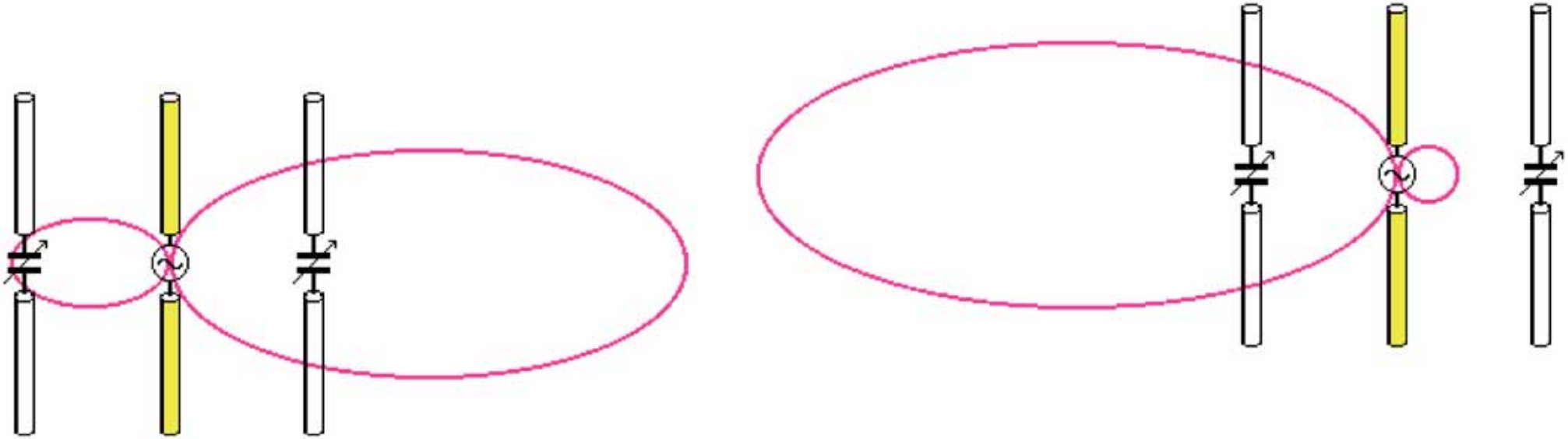
$P_{R1} = A_{12} P_{T2}$ ← P_{T2} dnLink

$$A_{21} = A_{12}$$

伝播路が非対称形状であっても
アンテナ１と２が異なる性能であっても
見通し外であっても
多重反射があっても

新技術の内容(1)

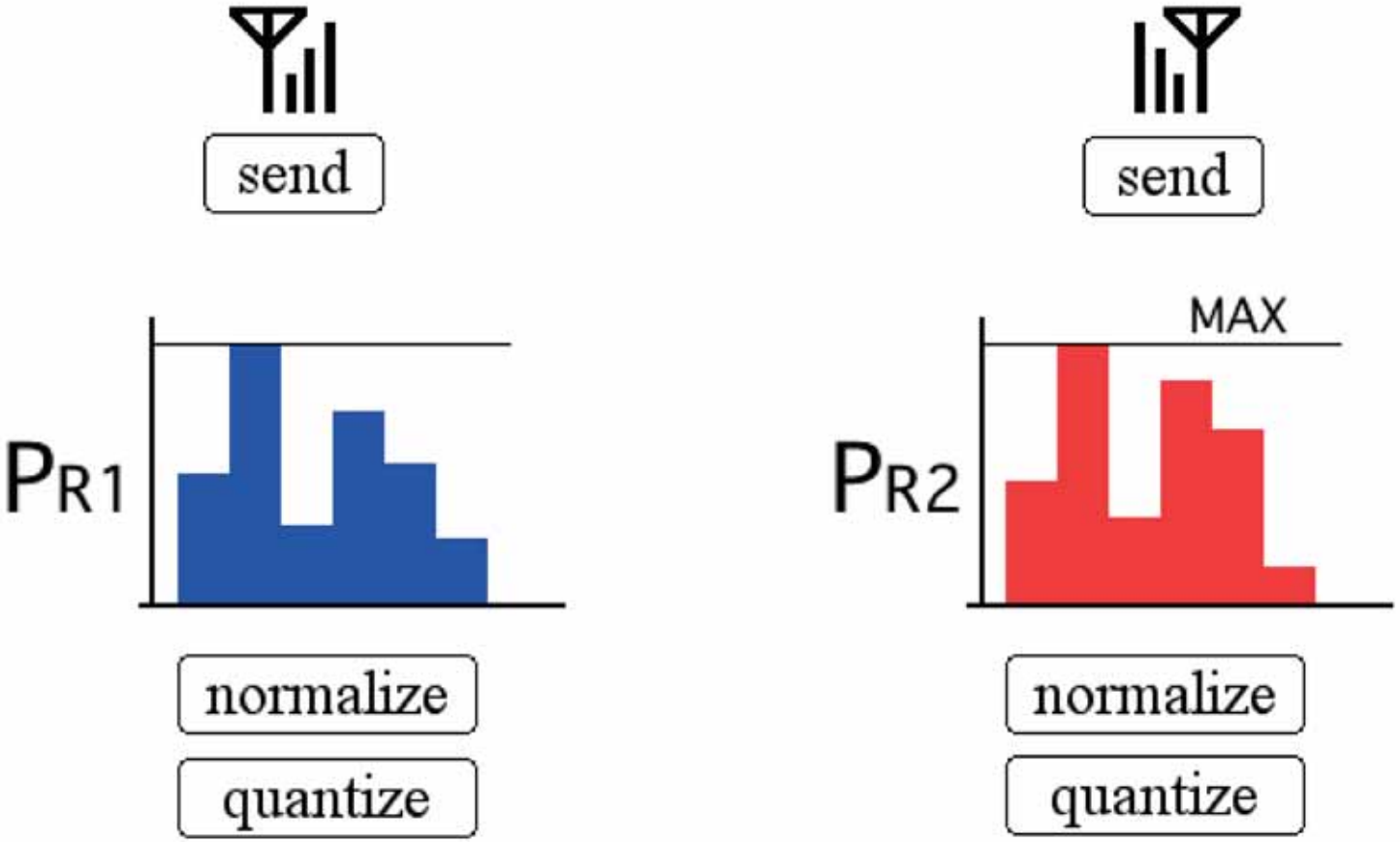
パラサイト素子で電波を「かき混ぜる」



環境変化が穏やかな場合でも
任意のタイミングに鍵を生成

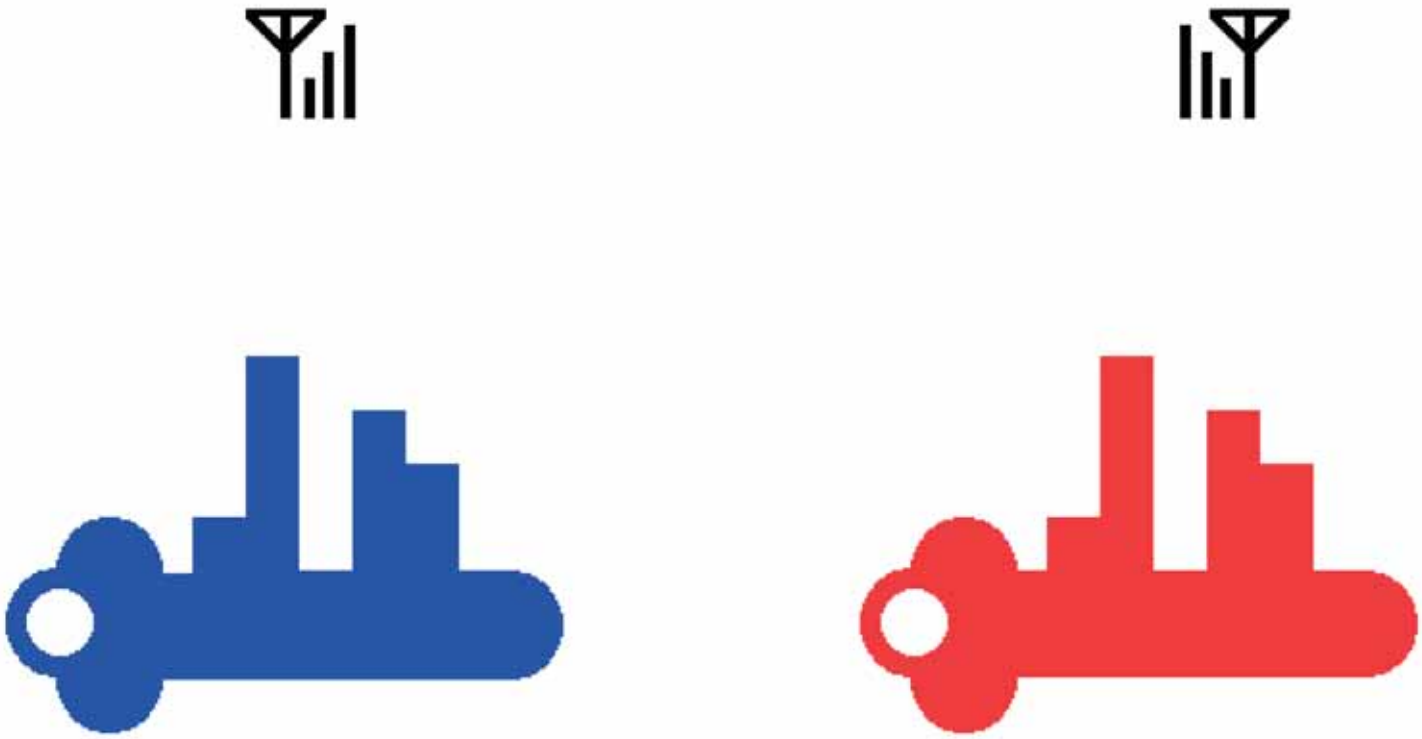
新技術の内容(2)

鍵を配送しないで共有する方法



新技術の内容(3)

鍵を配送しないで共有する方法



離れた場所で全く同じ鍵が生成できた

新技術の特徴・従来技術との比較

- 空間的に離れた２点間で鍵情報を無線で共有
- 数学的安全性ではなく、電波という自然現象による物理的安全性
- 鍵情報を送るのではなく、電波が上りと下りで同じ伝播特性（減衰量・遅延量）となることを利用
- 電波が４次元的（時間的・空間的）にゆらいでいるので第３者は電波を受けても鍵を盗聴できない
- 鍵はランダムに生成され、ユーザの手を介する必要がない
- 一旦共有した鍵は場所が変わっても使い続けられるし、毎回使い捨ても可
- ハードウェアは通常の無線送受信回路と可変指向性アンテナ

実用化に向けた課題

現状達成レベル

試作品で原理確認が可能なところまで開発済

今後の課題

様々な環境で鍵共有を実証

能動的攻撃に対する耐性を検証

具体的利用シーンを想定し実用化課題を抽出

可変指向性アンテナをさらに小型化

企業への期待

- 今後の課題のうち、アンテナ小型化については、本学にて電磁界シミュレーションとアンテナ試作・電波暗室でのアンテナ基本性能測定により達成できると考えている。
- 本共有鍵方式をシステムへ応用する技術を持つ企業との共同研究を希望。
- 秘匿情報交換、盗聴防止、セキュリティ分野などへの展開を考えている企業には、利用方法・利用モデルについて共同考案出願を希望。

本技術に関する知的財産権

- 発明の名称：秘密鍵共有通信システム及び通信方法
- 出願番号　：特願2009-5563
- 出願人　：国立大学法人豊橋技術科学大学
- 発明者　：大平　孝、成田譲二、長谷川　拓

お問合せ先：（株）豊橋キャンパスイノベーション（とよはしTLO）
Phone: 0532 - 44 - 6975　FAX: 0532 - 44 - 6980
Mail: ttlo-iten@kktci.co.jp　担当: 科学技術コーディネータ　白川正知