新技術説明会
New Technology Presentation Meetings!

ポーラ符号に基づいた無線通信における新しい物理層セキュリティ技術

横浜国立大学　大学院工学研究院
知的構造の創生部門　教授
落合　秀樹

2023年6月6日

背景：無線通信における盗聴問題

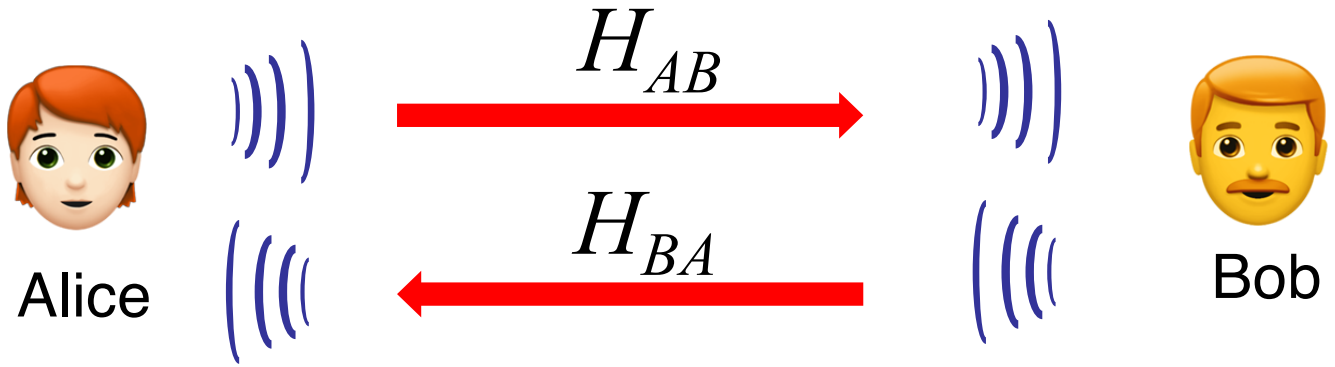
公開鍵暗号は計算面で実装困難 → 共通鍵暗号が主流

盗聴に対する秘匿性を保つには送信者(Alice)と正規受信者(Bob)間で事前に暗号化鍵(復号鍵)の共有が必要

物理層セキュリティ技術

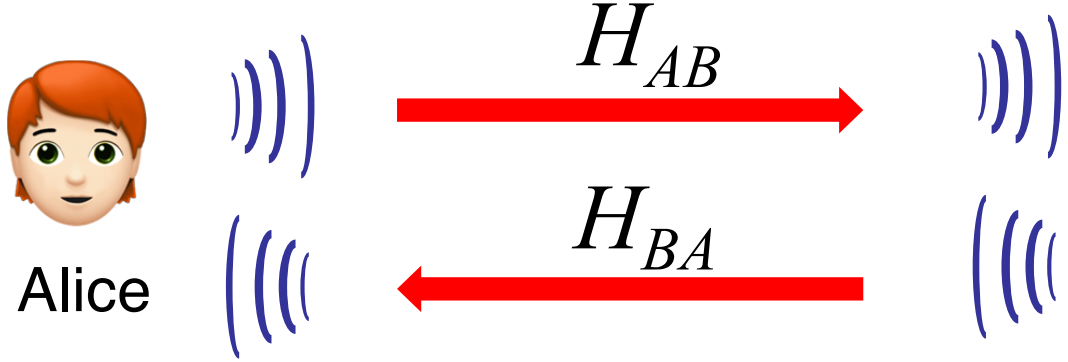
- 従来の上位層における暗号化によらず、物理層において通信の安全性や秘匿性を担保する技術
- 物理層セキュリティの代表的な技術
  - 無線伝搬路のランダム性を利用して秘密鍵を生成、さらに伝搬路の可逆性を利用して秘密鍵を共有
  - 正規受信者と盗聴者の信号対雑音電力比（SNR）の違いによる通信路容量の差に着目して情報伝送
  - 正規受信者の物理的位置においてのみ送信信号を高SNRで受信できるビームフォーミング技術

既存技術①：可逆性を利用した鍵生成・共有



- 時間分割多重（TDD）においては、送受信機間で伝搬路情報（CSI）に可逆性が成り立つことに着目（CSIから鍵を生成）

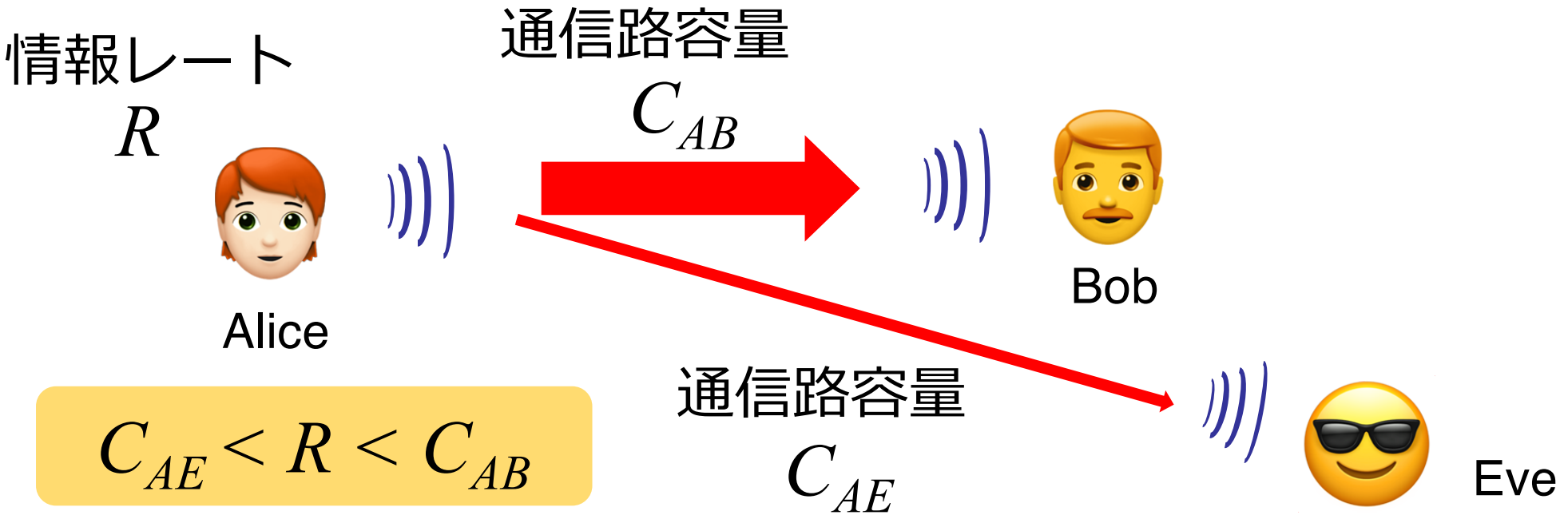
既存技術①:可逆性を利用した鍵生成・共有



$$H_{AB} \fallingdotseq H_{BA}$$

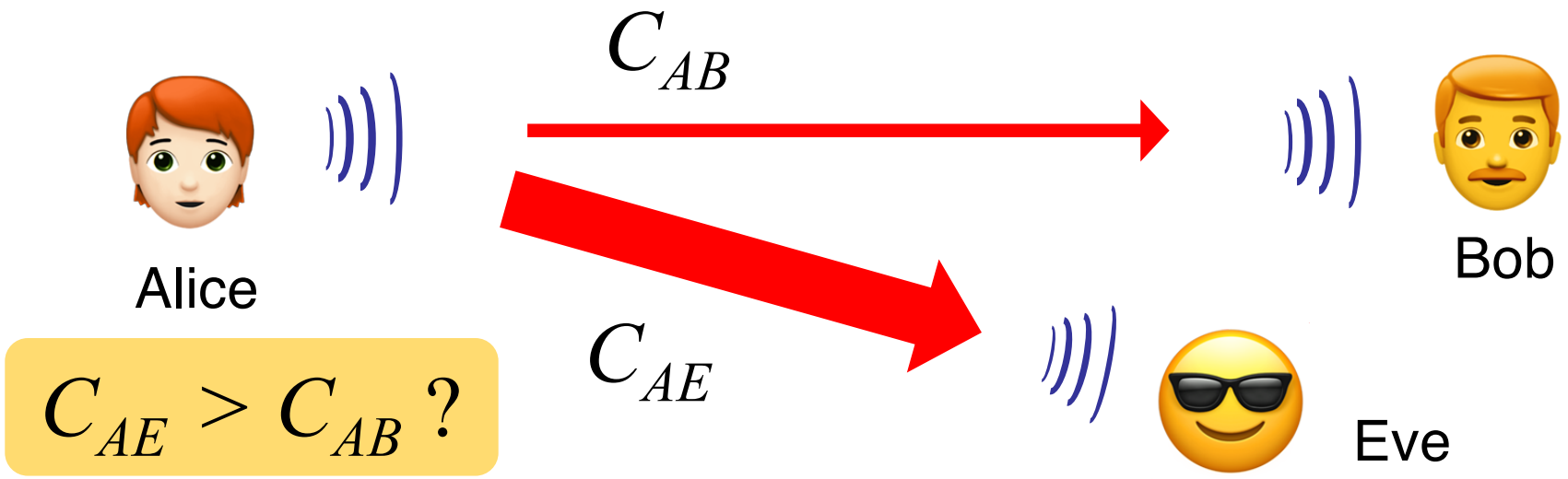
- 技術課題：
  - 一般にTDDでなければ可逆性が成立しない
  - 鍵のランダム性は伝搬路特性に依存(保証できない)
  - 雑音や推定誤差、またその他のハードウェアの影響により高精度な伝搬路情報(CSI)が共有できない
  - CSIの適切な量子化処理と情報整合などの後処理により、生成した鍵の一致率を確保する必要がある

既存技術②：正規受信者と盗聴者の受信電力比（SNR）の差に着目



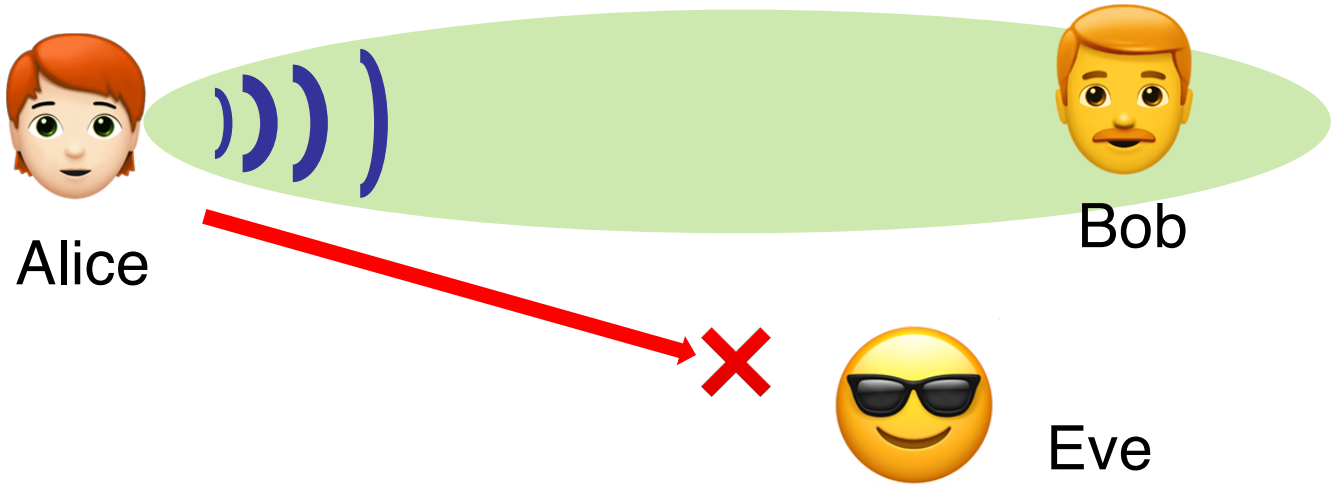
- 正規受信者（Bob）と比べて盗聴者（Eve）の受信電力が相対的に低ければ、Bobのみが情報を復号できるようにAliceが情報レートを設定して送信

既存技術②:正規受信者と盗聴者の受信電力比(SNR)の差に着目



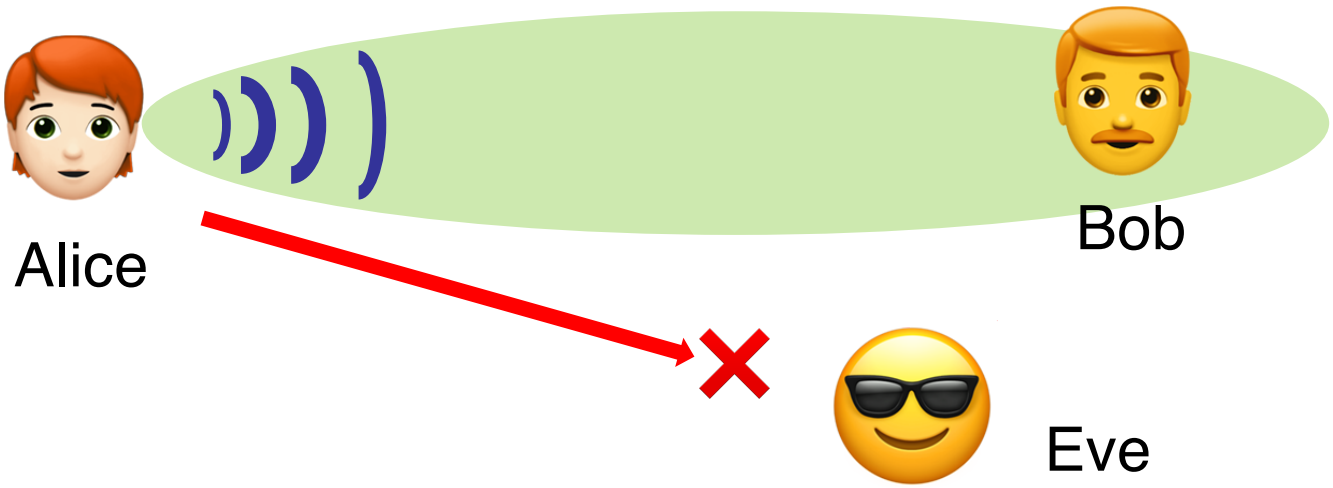
- 技術課題:
  - (送信を行わない)受動的な盗聴者(Eve)のSNRは正規の送受信者(AliceとBob)にとって未知
  - EveがBobよりAliceに近ければ秘匿性担保が困難

既存技術③:ビームフォーミングによる情報伝送



- 複数送信アンテナを用いたビームフォーミングにより、正規受信者の物理的な位置においてのみ十分なSNRが達成できる状況をつくり出す

既存技術③:ビームフォーミングによる情報伝送

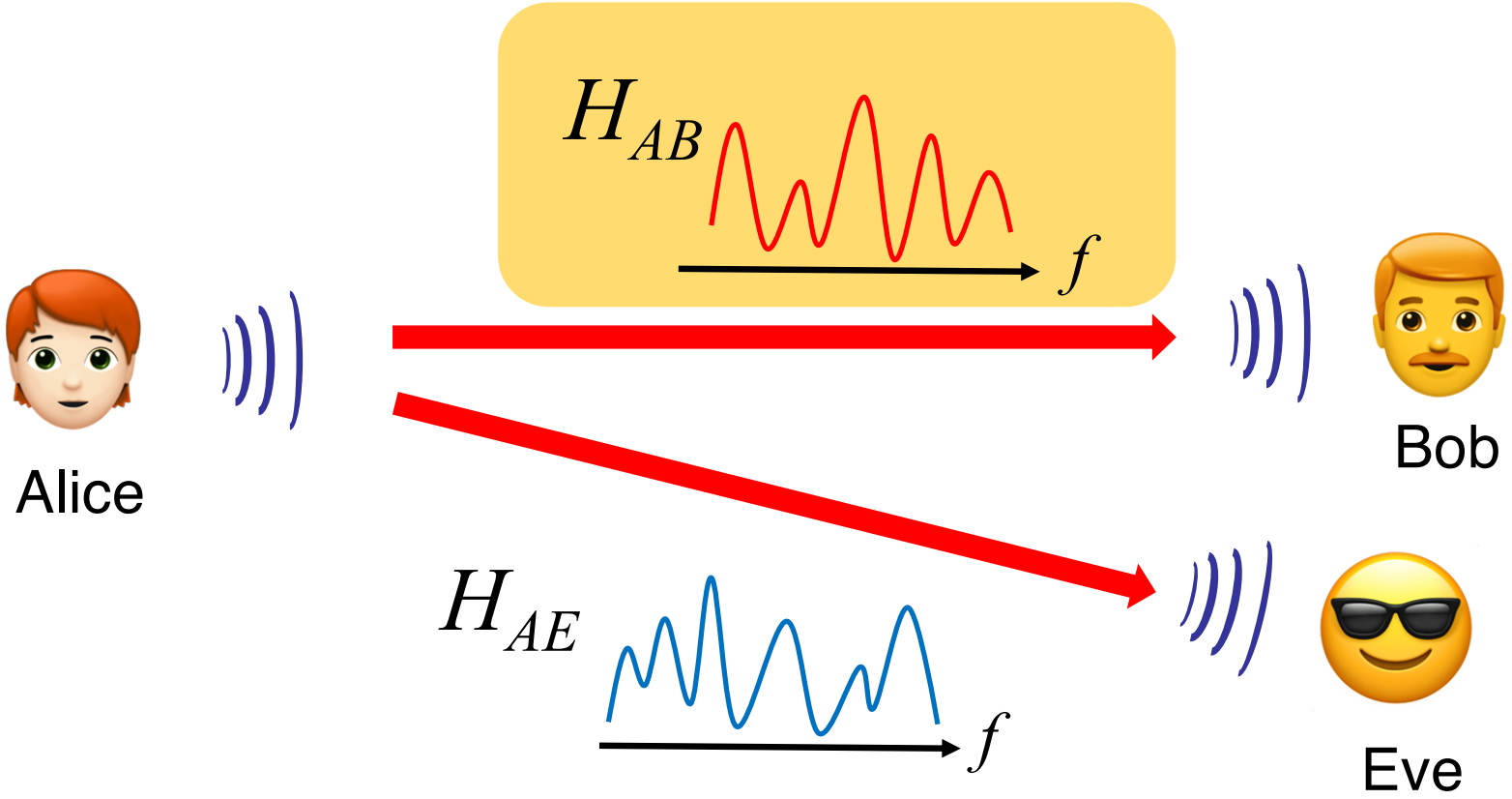


- 技術課題：
  - 送信側に複数送信アンテナが必要
  - 送信側で正規受信者に対する伝搬路情報（CSI）を精度良く推定する必要があり、一般に技術的なハードルが高い

提案技術：新しい物理層セキュリティ技術

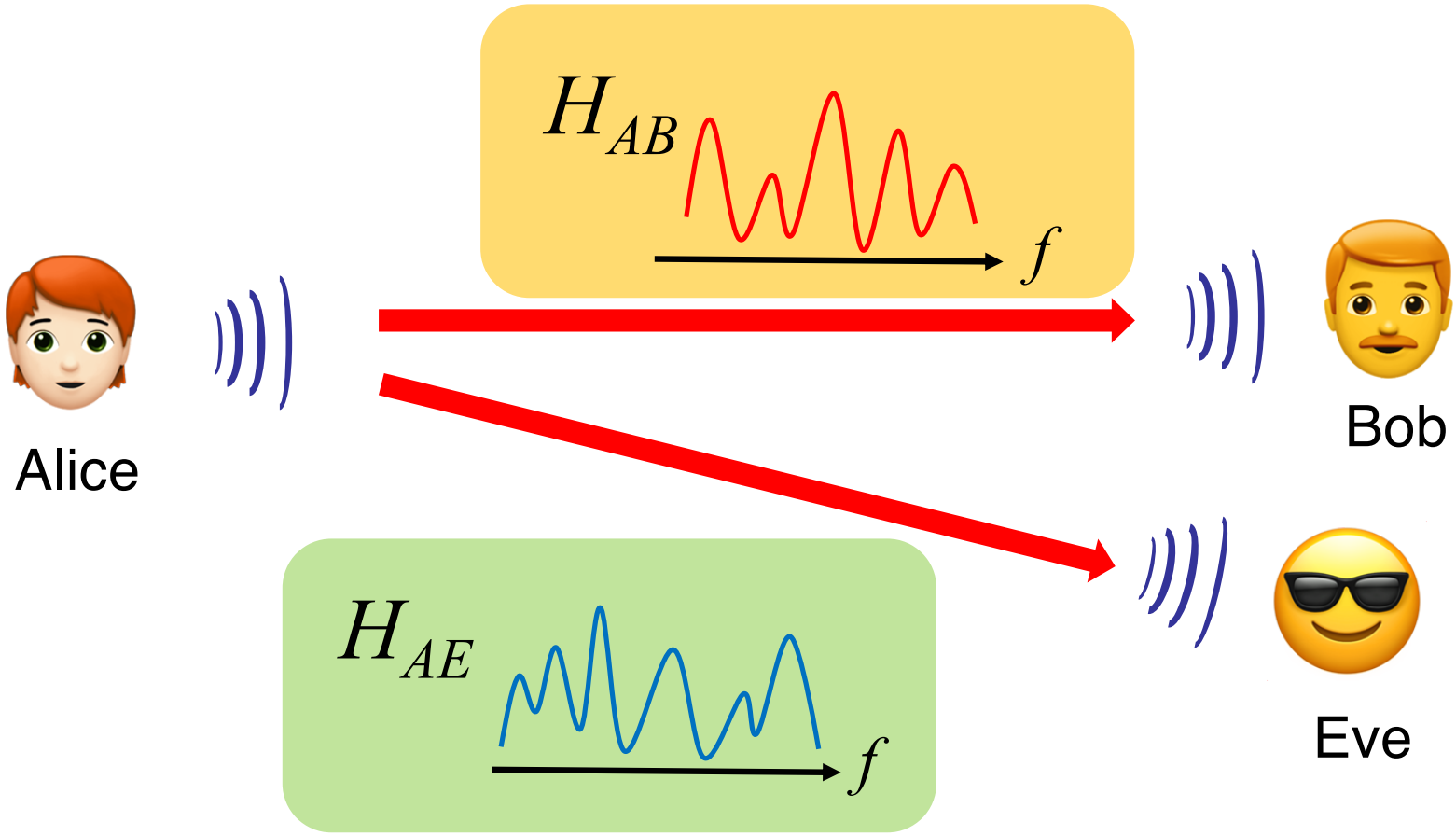
- 基本概念
  - 送信に用いる誤り訂正符号を正規受信者の伝搬路状況に合わせて設計する
  - 正規受信者は受信した符号を高い確率で復号できるが、それ以外の受信者にとっては復号が困難
- 利点
  - 可逆性を仮定しないため、多重方式（TDDやFDD等）によらず適用可能
  - 伝搬路情報（CSI）を送信側で推定不要
  - 送信に用いる符号自体は、公知としても問題ない

提案技術の基本原理①



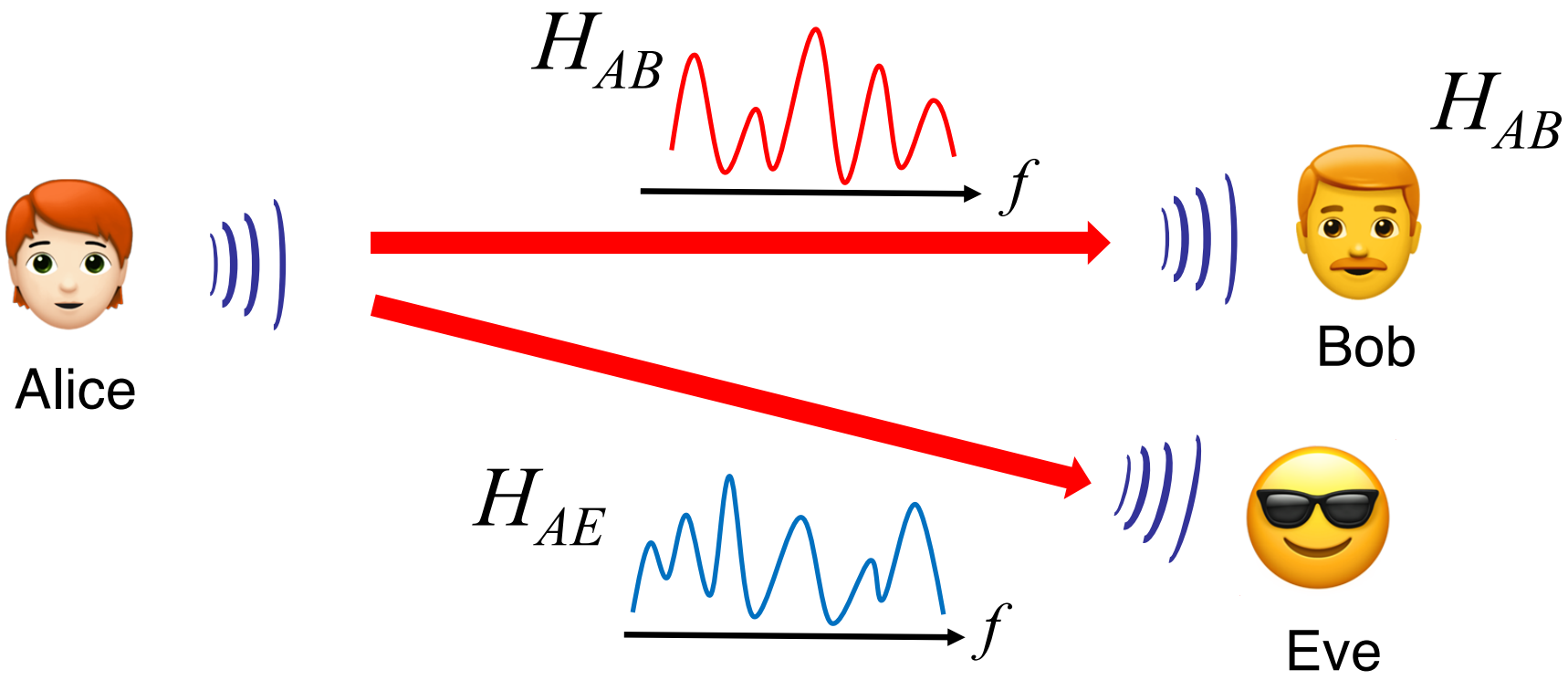
Alice-Bobの伝搬路に合わせてBobが符号を決定し、Aliceに符号を周知する（Bob自身が復号できるように自ら符号を選択する）

提案技術の基本原理②



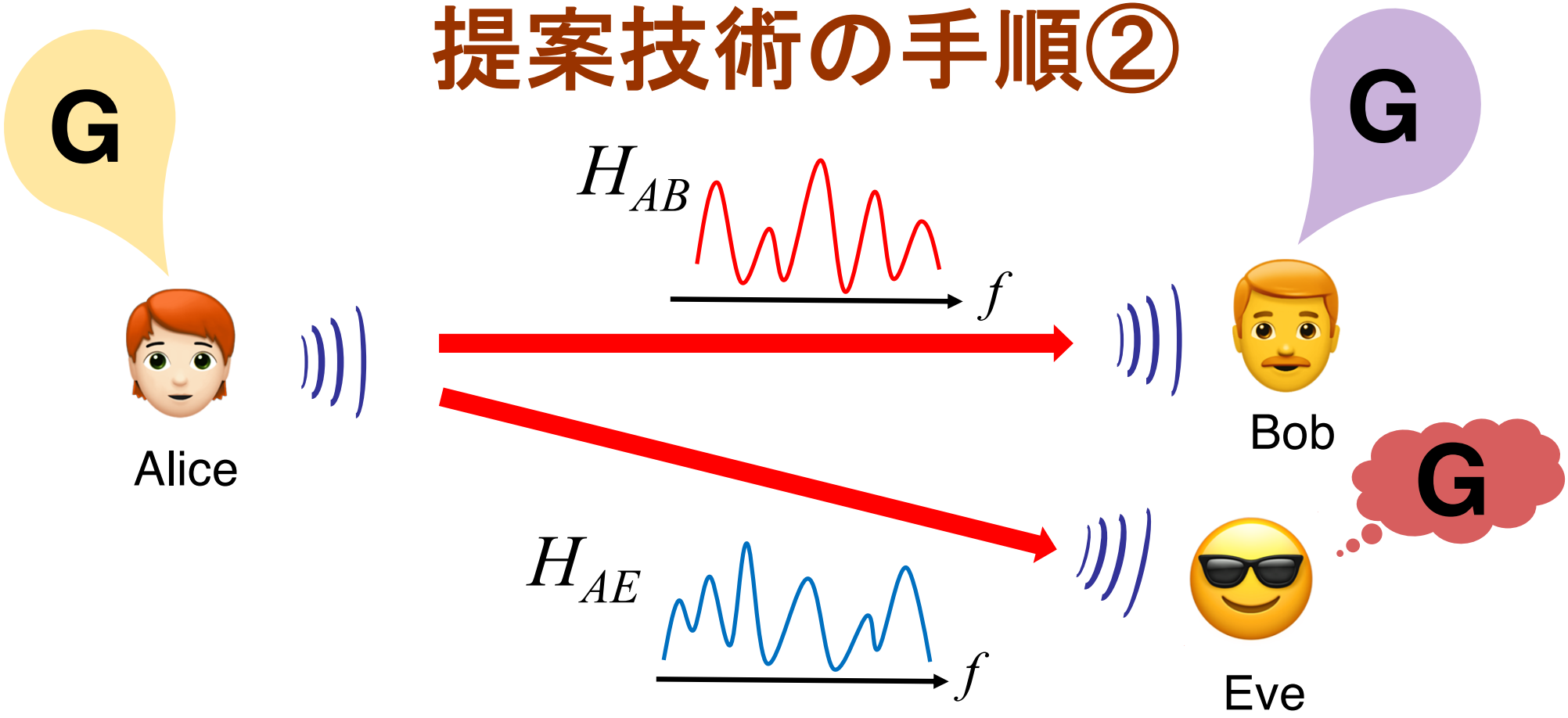
Aliceが送る符号はEveの伝搬路にマッチしないため、
Bobと同等の通信環境においてもEveによる復号は困難

提案技術の手順①



① Aliceがパイロットを送信、Bobは伝搬路H_{AB}を推定

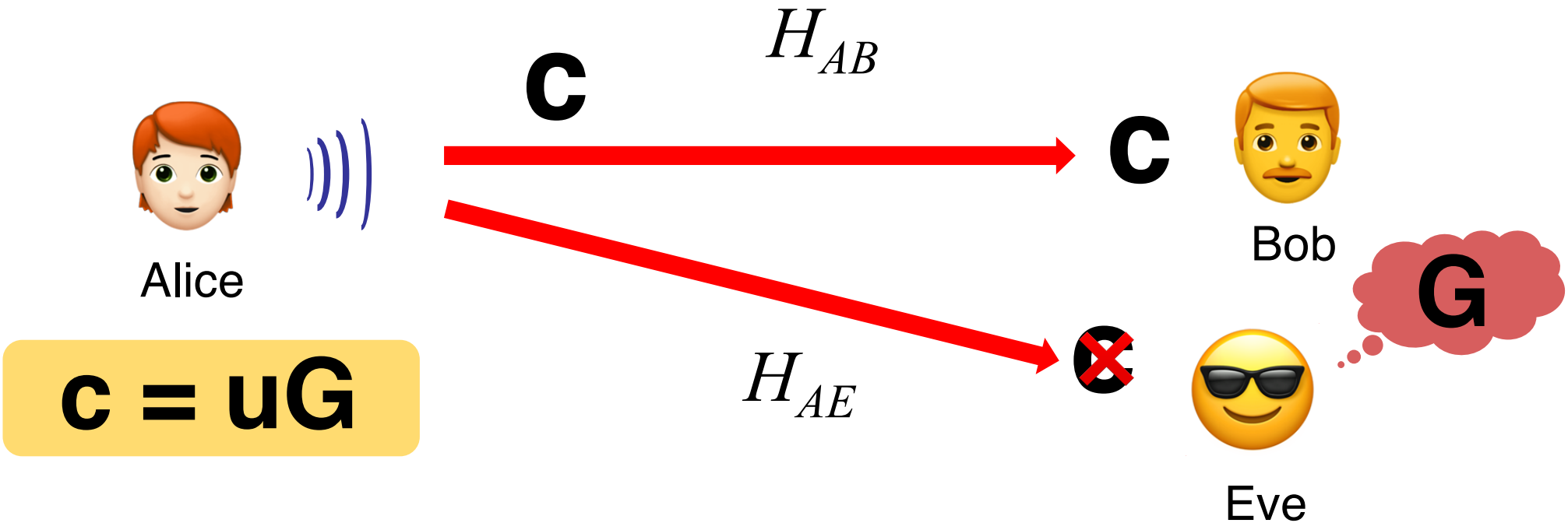
提案技術の手順②



① Aliceがパイロットを送信、Bobは伝搬路H_{AB}を推定

② Bobは伝搬路H_{AB}に適した符号を設計、Aliceに周知

提案技術の手順③



① Aliceがパイロットを送信、Bobは伝搬路H_{AB}を推定

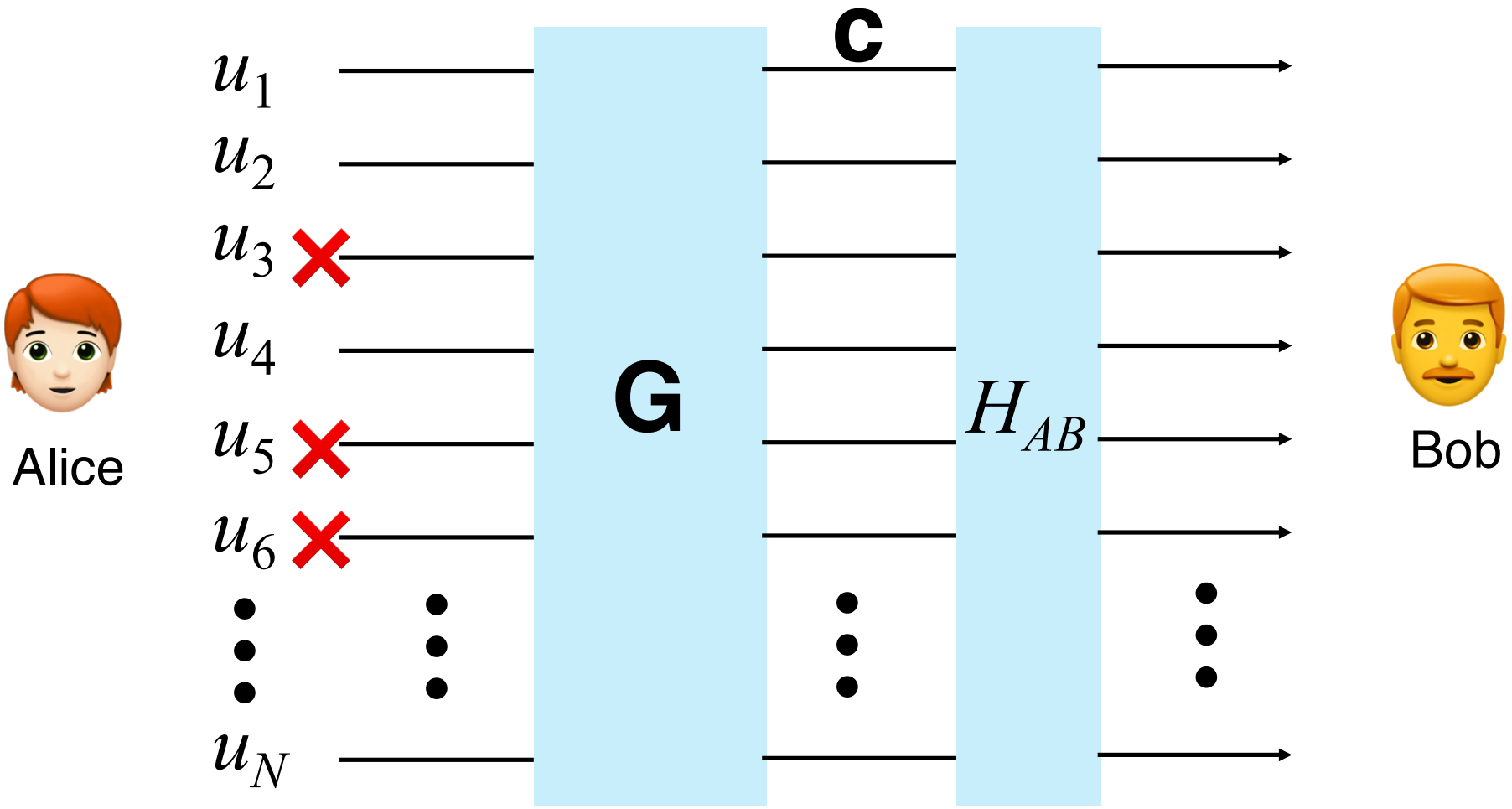
② Bobは伝搬路H_{AB}に適した符号を設計、Aliceに周知

③ Aliceは周知された符号を用いて情報を伝送

提案技術の具体的な実現方法①

- 直交周波数分割多重（OFDM）伝送
  - 移動体通信（4G/5G）や無線LAN(IEEE802.11)で広く利用されている伝送方式
  - 周波数選択性伝搬路の性質を符号設計に利用
- ポーラ符号
  - 移動体通信（5G）で採用された比較的新しい符号
  - 通信路分極の概念により「凍結ビット」を決定することで符号構造が決まる
  - 情報レートの柔軟な設計が可能

提案技術の具体的な実現方法②



受信信号よりBobにおいて最も信頼度の低い N-K ビットを判定して凍結ビットとし、これをAliceに周知

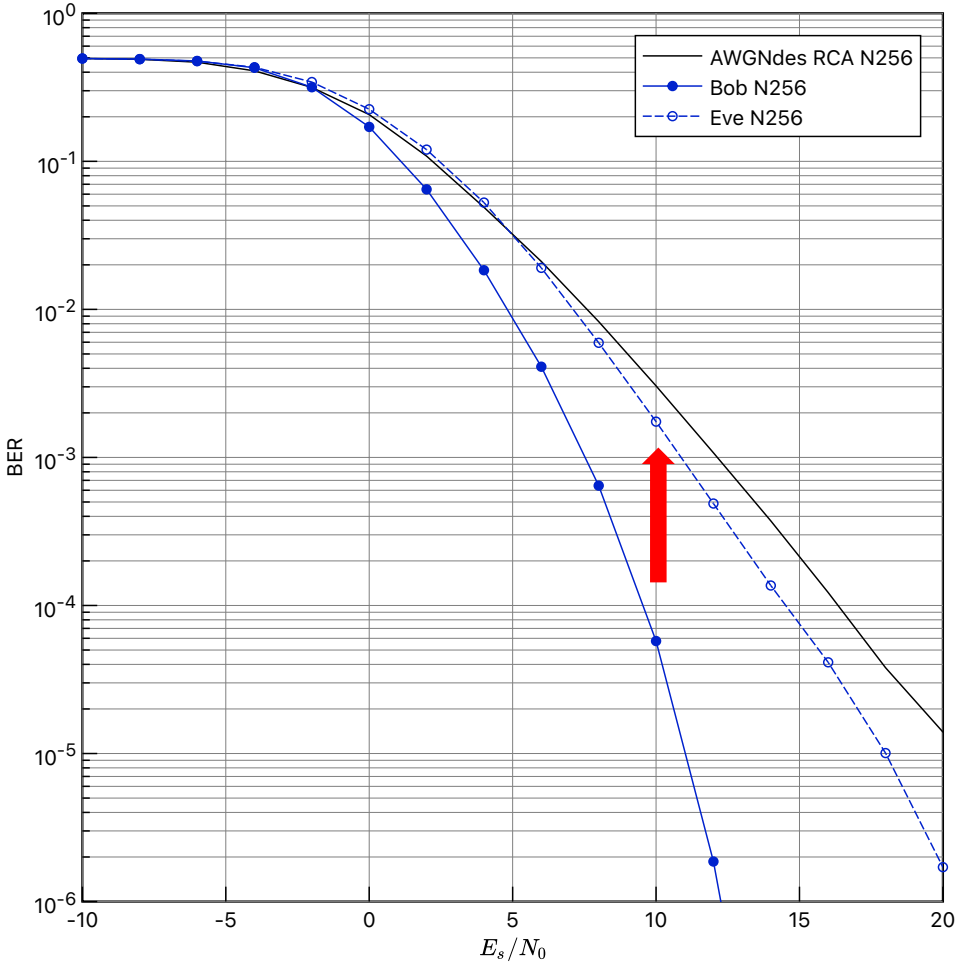
シミュレーション実装例

変調方式	QPSK / 64-サブキャリア OFDM
伝搬路	周波数選択性レイリーフェージング（パス数 5）
符号化率 R	0.5
符号長 N	256 or 2048 ビット

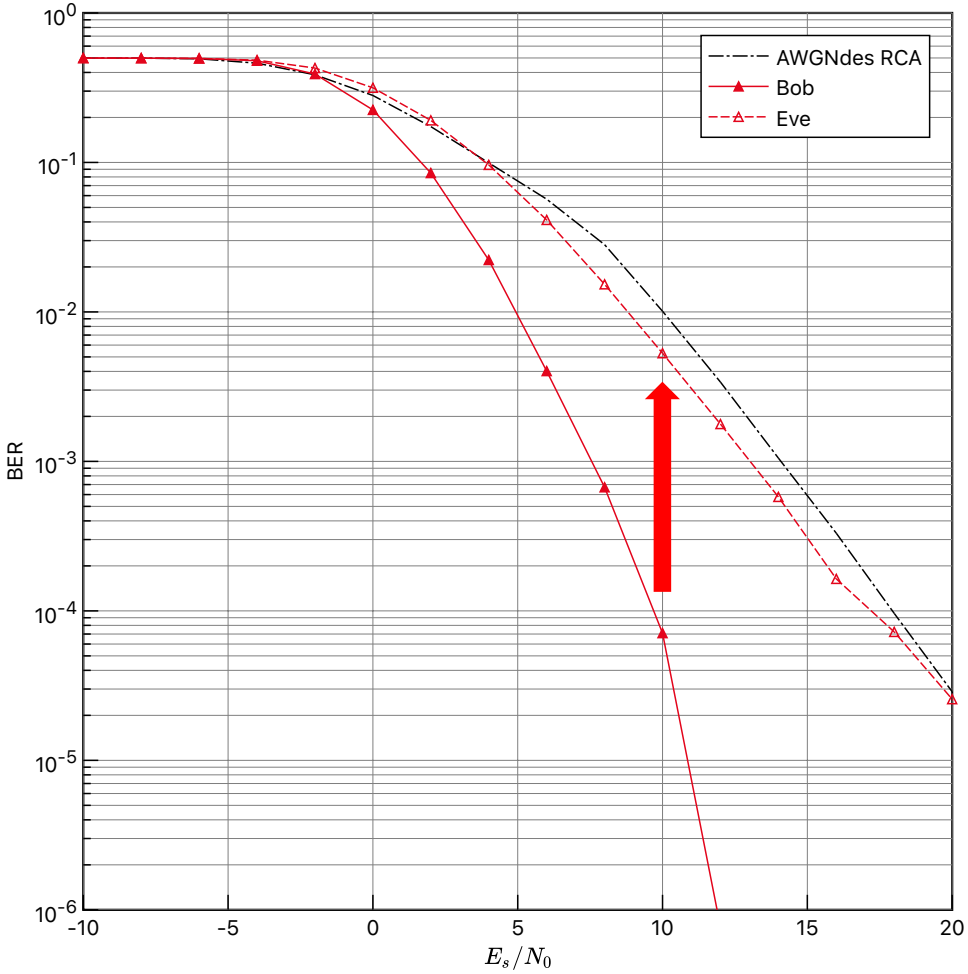
新技術説明会
New Technology Presentation Meetings!

ビット誤り率特性の比較

N = 256



N = 2048



BobとEveが同じSNR環境下においても

Eveのビット誤り率特性はBobに比べて大きく劣化

新技術の特徴･従来技術との比較

- ポーラ符号とOFDM方式を組み合わせることで、伝搬路の可逆性によらない新しい物理層セキュリティ技術を提案
- ポーラ符号の構造を正規受信者の伝搬路にマッチさせることで、正規受信者以外の受信機では復号を困難とする
- 正規通信者間で用いる符号の構造自体が盗聴者に知られても、盗聴者の復号特性の改善にはつながらない

想定される用途

- OFDMを採用する広帯域無線通信方式において、初期の秘密鍵配送に適する
- 物理層セキュリティが求められる上記以外のシステムへも適用可

実用化に向けた課題

- 現時点では計算機シミュレーションによる評価の段階
- ソフトウェア無線等を用いた実験により提案方式の実用性を示すことが求められるが、実験局免許の取得が必要であるなど、大学で行う研究開発としてはハードルが高い

企業への期待①

- 物理層セキュリティ技術自体、研究は広く行われているが、実用化されるに至っていない
  - 今後実用化が高く期待される研究分野である
- 多くの無線通信システムにおいては、標準規格に採用されなければ実用化されない
- 実用化に向けては、標準化に参画する企業、もしくは独自の通信方式の導入を検討している企業との連携が必要

企業への期待②

- 物理層セキュリティ技術以外においても、有線および無線通信技術の低消費電力化のための符号化・変調技術に研究実績を有する
- 6Gでは超低消費電力の無線通信もユースケースとして挙げられる
- これらについても技術連携や共同研究等のニーズがあれば応えたい

本技術に関する知的財産権

- 発明の名称：通信システム、通信装置、通信方法およびプログラム
- 出願番号　　：特願2022－117363
- 出願人　　：横浜国立大学
- 発明者　　：倉谷 悠希、落合 秀樹

お問い合わせ先

横浜国立大学
研究推進機構　産学官連携推進部門
産学官連携支援室

ＴＥＬ：045－339－4450
ＦＡＸ：045－339－3057
e-mail：sangaku-cd@ynu.ac.jp