Enforcing End-to-end Security for Remote Conference Applications

Yuelin Liu
ShanghaiTech University
liuyl5@shanghaitech.edu.cn

Huangxun Chen
Hong Kong University of Science and Technology (Guangzhou)
huangxunchen@hkust-gz.edu.cn

Zhice Yang
ShanghaiTech University
yangzhc@shanghaitech.edu.cn

上海科技大学
ShanghaiTech University

THE HONG KONG UNIVERSITY OF SCIENCE AND TECHNOLOGY (GUANGZHOU)

Remote Conference Applications

腾讯会议 Tencent Meeting

Signal

zoom

jitsi

webex by cisco

Microsoft Teams

Online learning

Business

eHealth

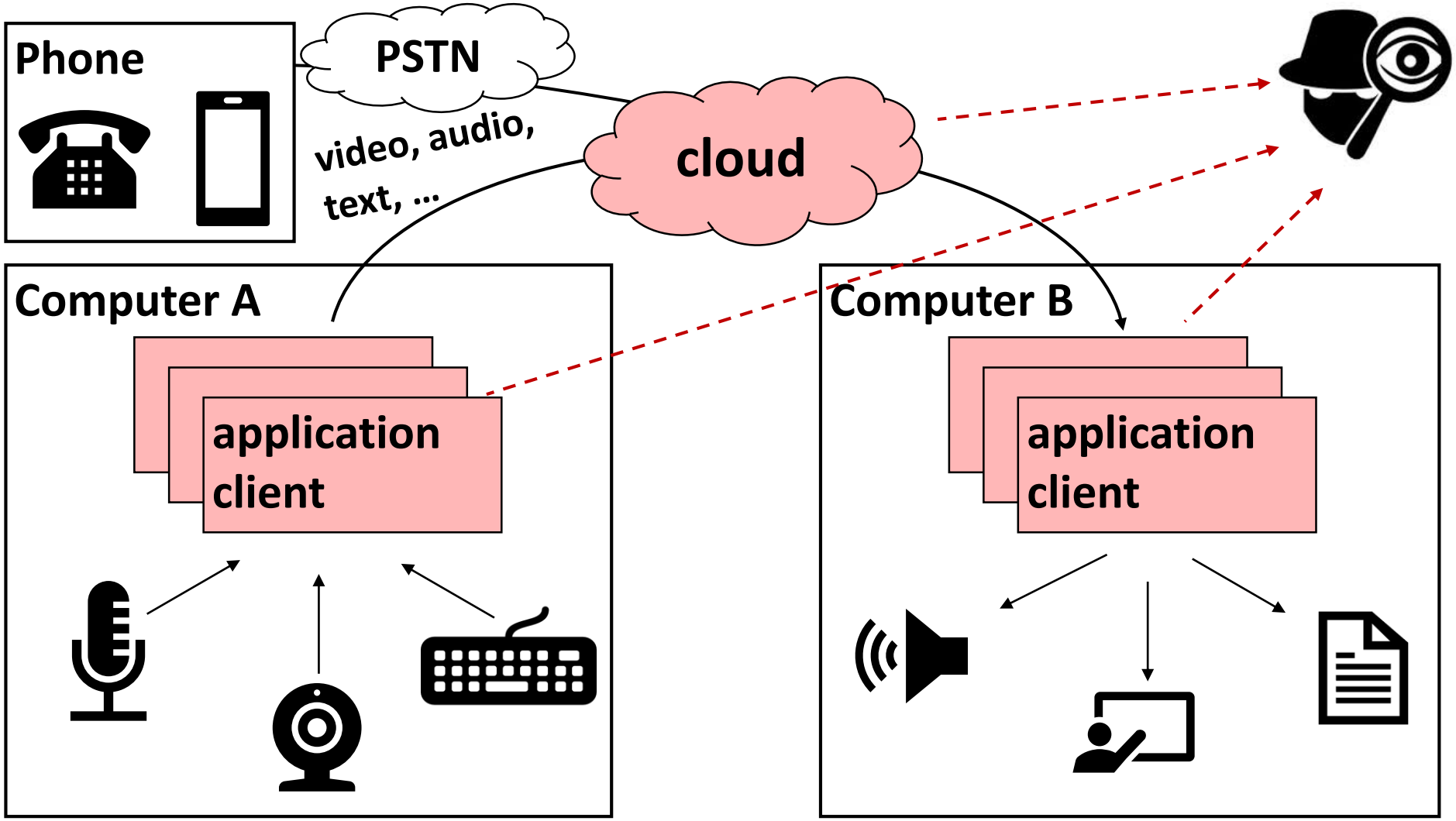
Photo Sources: Microsoft Copilot and pexels.com with CC license

Threats in Conference Applications

- In 2020, Zoom gave user data to Facebook and Google without user's consent[1]
- In 2022, an ex-Amazon employee was convicted of hacking Capital One and stealing data of over 100 million people[2]

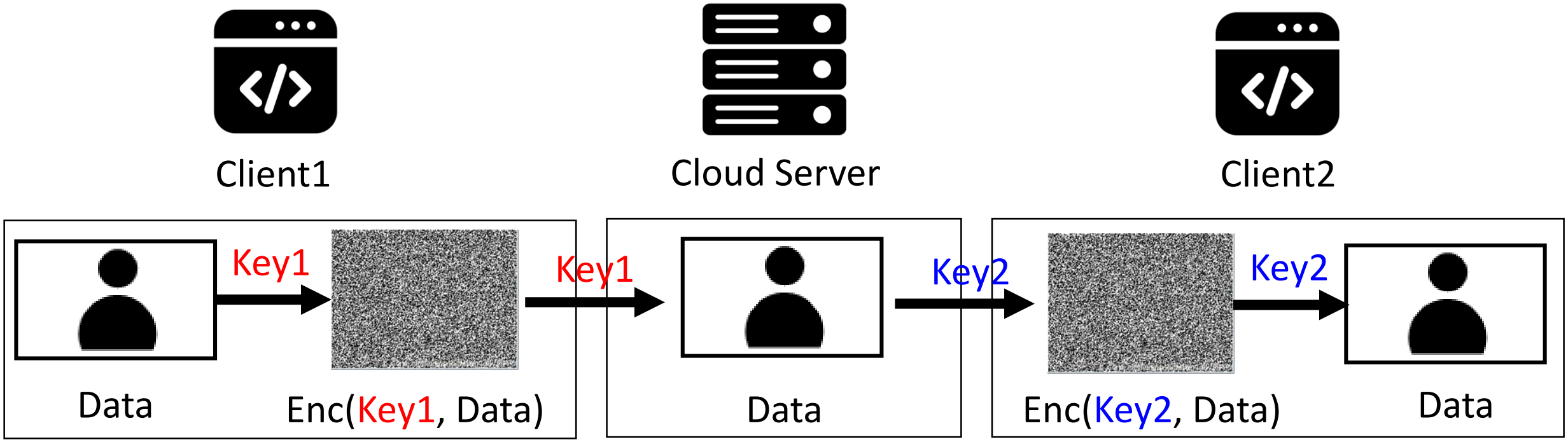
[1] "Zoom is being sued for allegedly handing over data to Facebook," https://www.businessinsider.com/zoom-sued-allegedly-sharing-data-with-facebook-2020-3, Business Insider. 2020.
[2] "Ex-Amazon employee convicted of hacking Capital One and stealing data of over 100 million people," https://www.insider.com/ex-amazon-worker-convicted-of-hacking-capital-one-and-stealing-data-2022-6, Insider. 2022.

Threats in Conference Applications



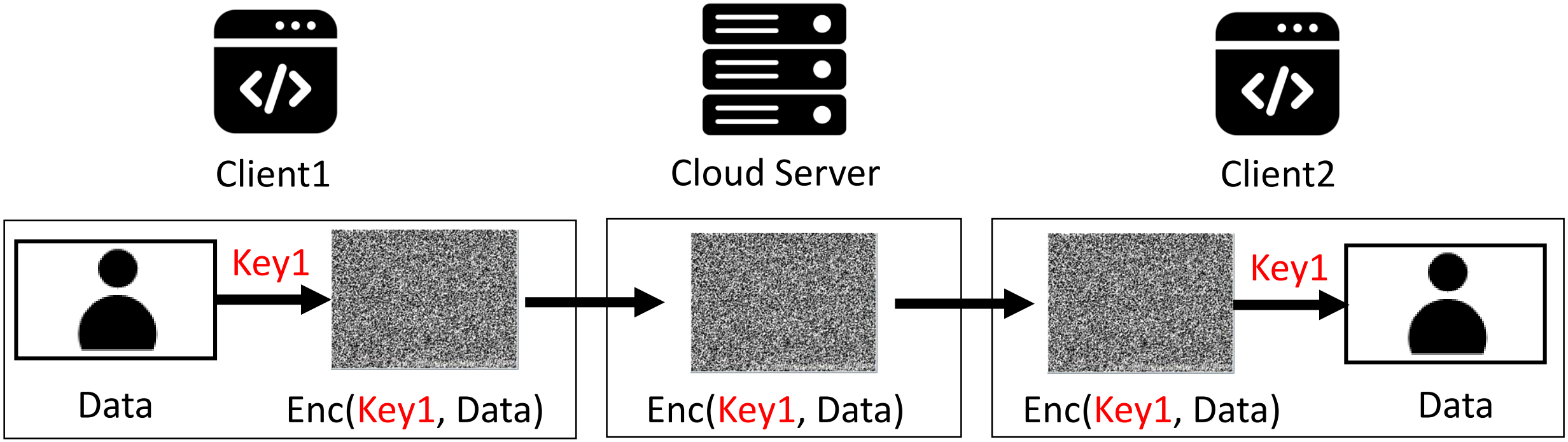
Background - Secure Transmission Schemes

- Point-to-point encryption (P2PE)
  - Encryption keys are negotiated with the cloud
  - User data is transparent to the cloud



Background - Secure Transmission Schemes

- End-to-end encryption (E2EE)
  - Encryption keys are negotiated among clients
  - User data is confidential to the cloud



Limitations of Current E2EE Solutions

- Proprietary Implementations
  - Lack of effective auditing methods
  - Lack of trust from the general public[1]
- Open-source Implementations
  - Lack of rich features
  - Limited market share
- Lack of support for dial-in access

[1] R. Abu-Salma, E. M. Redmiles, B. Ur, and M. Wei, “Exploring user mental models of End-to-End encrypted communication tools,” in 8th USENIX Workshop on Free and Open Communications on the Internet (FOCI 18). Baltimore, MD: USENIX Association, Aug. 2018.

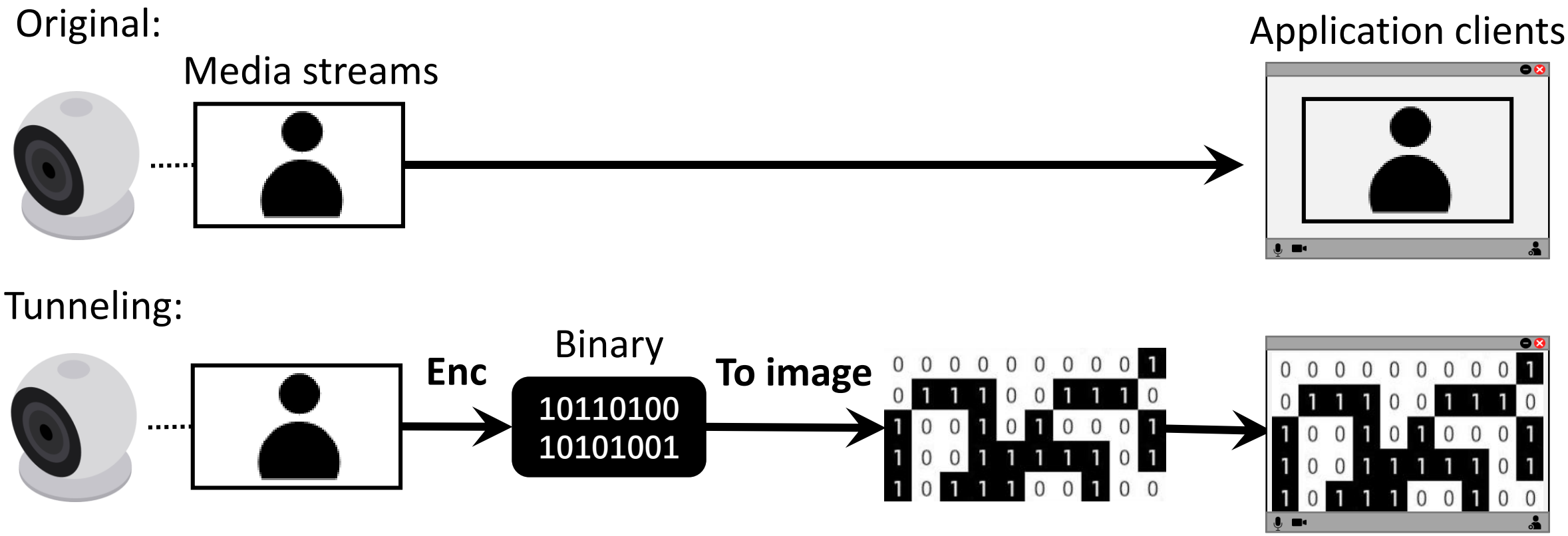
Design Goals

- Threat model: the adversary is a network attacker who can access, replay, and generate arbitrary on-path data and key information
  - *e.g.* Malicious insider, cloud service provider, external adversary

- We want to design a tool to enhance conference applications
  - Achieve E2EE security
  - Ensure compatibility
  - Preserve functionality

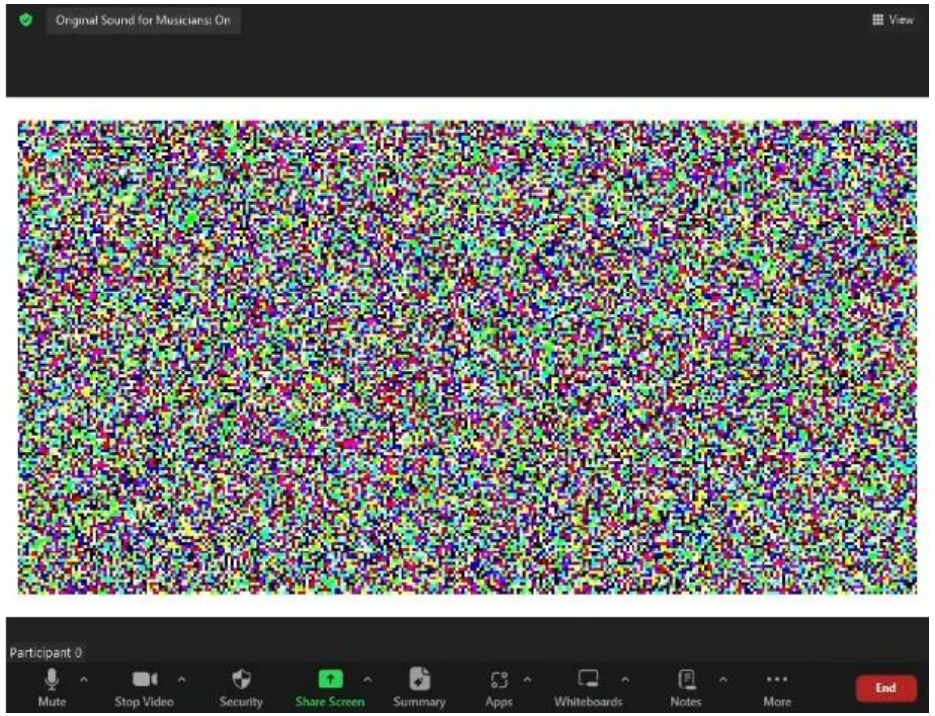
Approach - Media Tunneling

- Basic idea: use E2EE key to encrypt the media streams before they are acquired by the application clients



Demo

Original / Recovered Client UI



Client UI under Protection

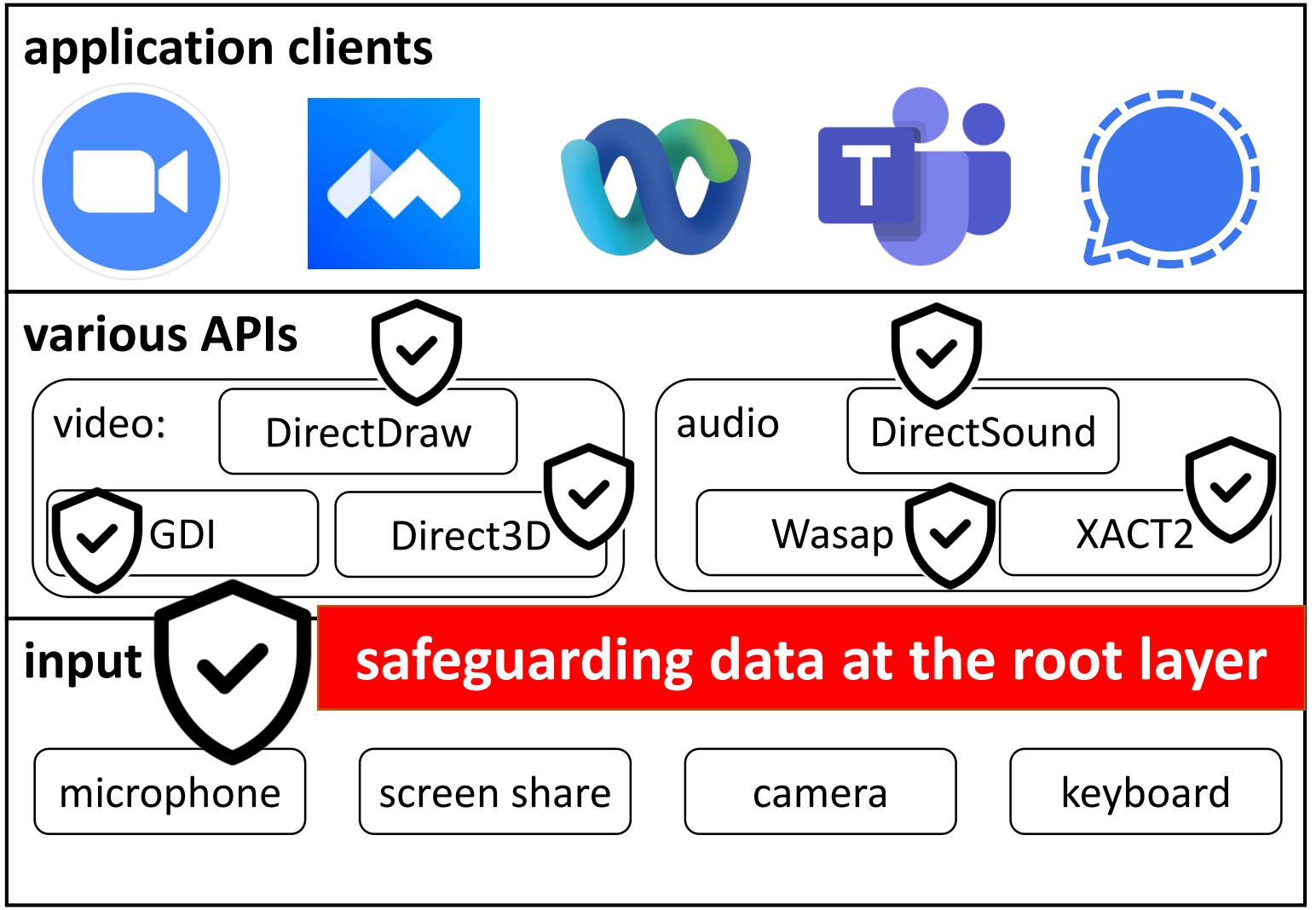
Challenges - E2EE Media Tunneling

1. Be compatible for various clients
   - Conference applications utilize distinct I/O interfaces for data retrieval

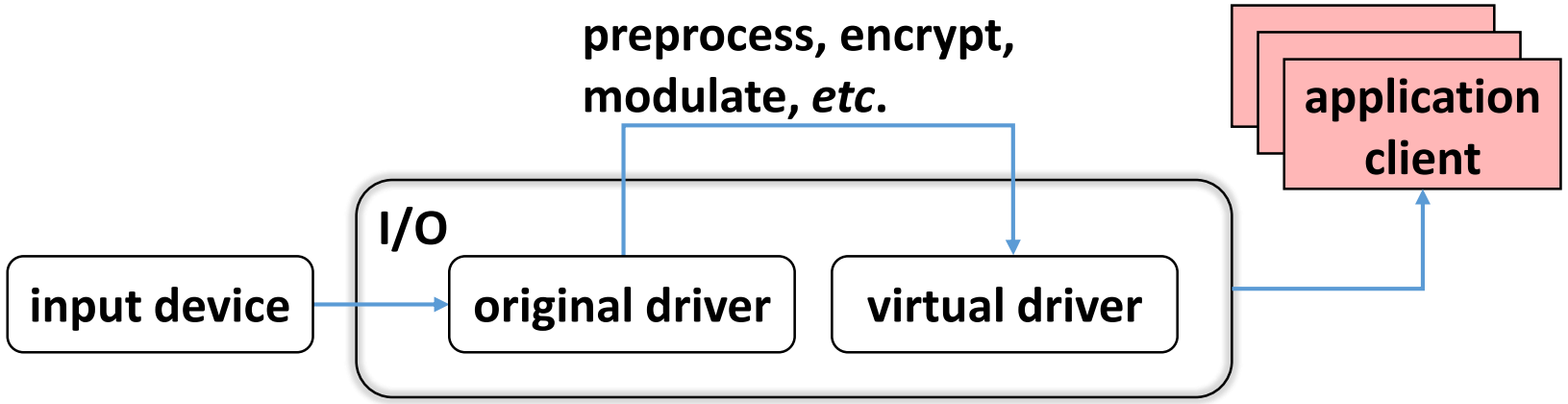
2. Resist lossy compression
   - Conference applications perform lossy compression on transmitted data, corrupting the decryption of ciphertext

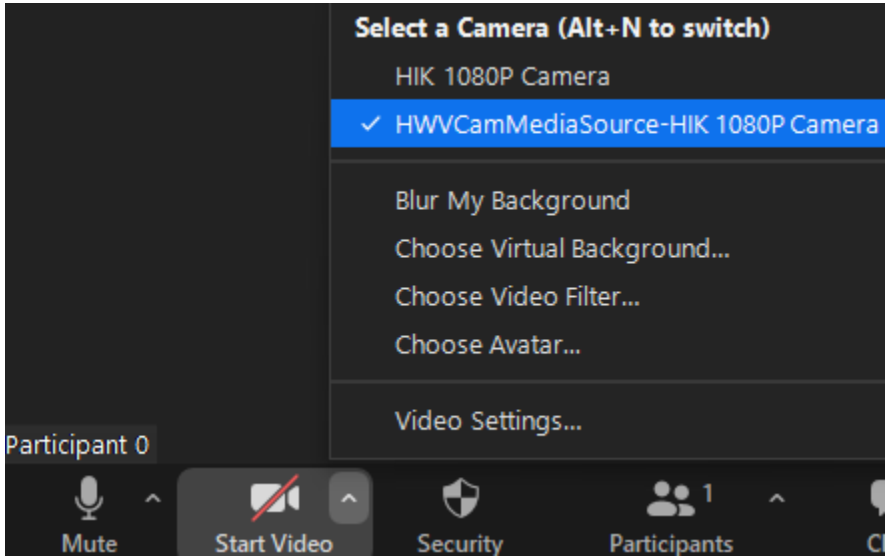
3. Support dial-in access
   - No generic data links to phone clients

Challenge 1 - Be Compatible for Various Clients



Solution - Virtualization





- Virtual device:
  - Virtual camera
  - Virtual display buffer
  - Virtual microphone
  - Virtual speaker

Challenge 2 - Resist Lossy Compression

Left: original

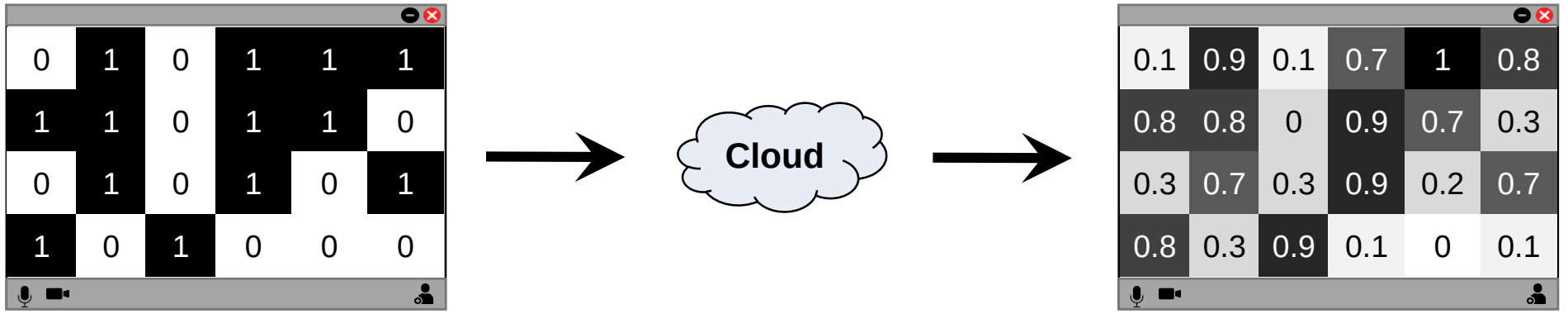
Right: compressed

Photo Sources: dreamstime.com with RF license

Challenge 2 - Resist Lossy Compression

Lossy channel: the media data will be lossy compressed before being transmitted to the remote side

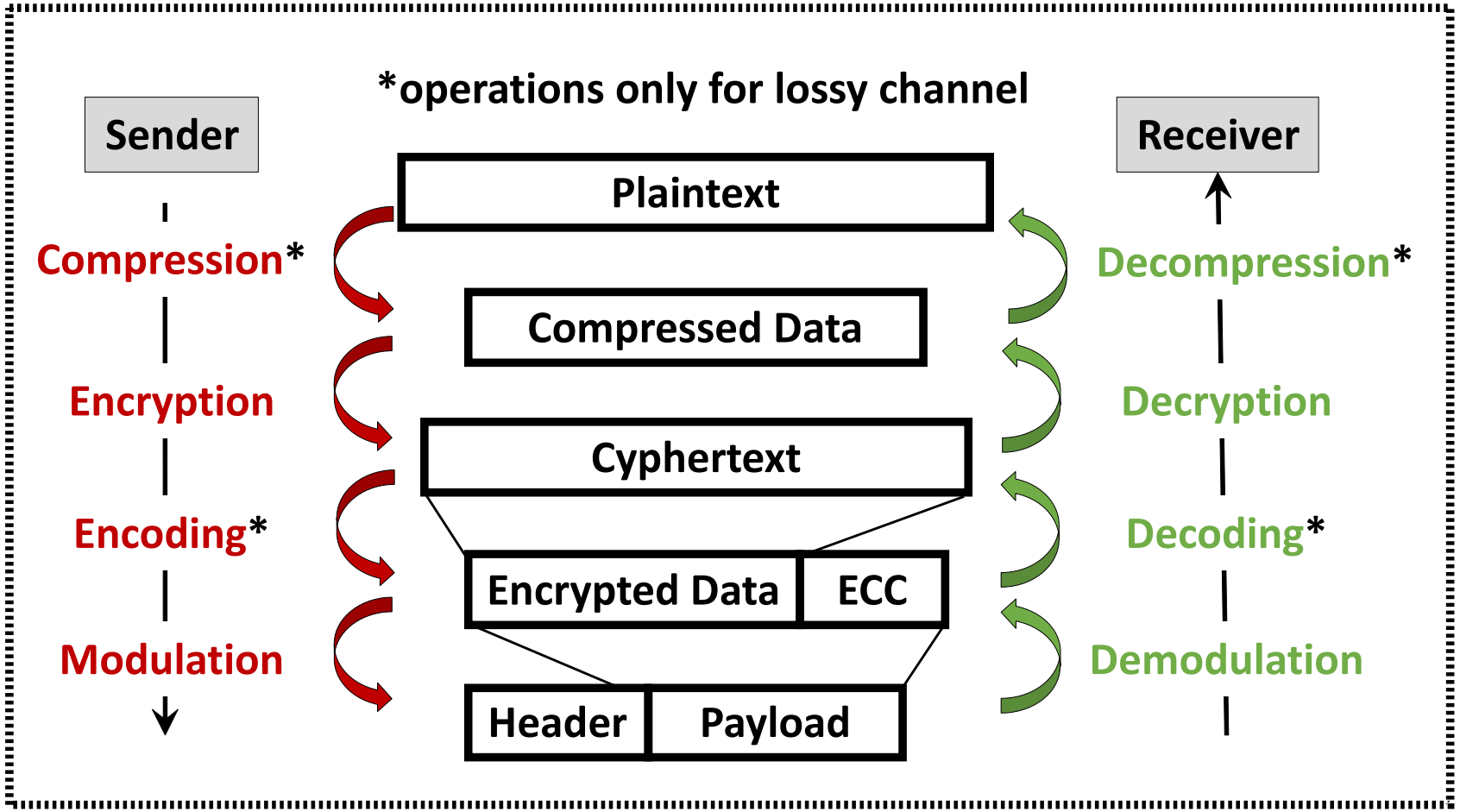
- *e.g.* Video, audio



Sender's client

Receiver's client

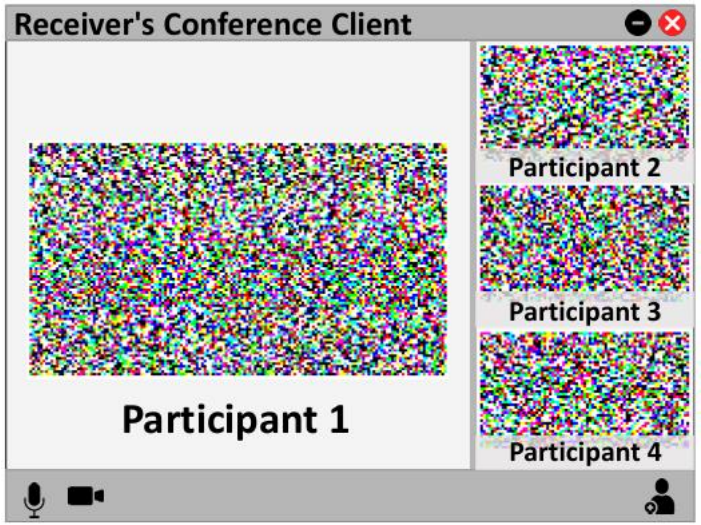
Solution – ECC Encoding and Modulation



Example - Video Channel Modulation

(a) Original Video Frame

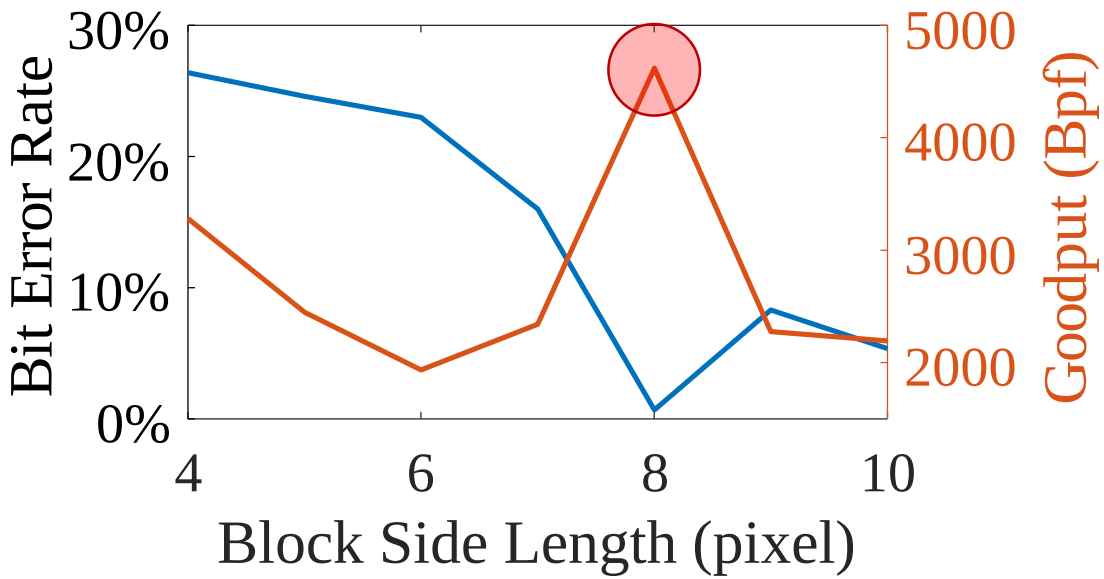
(b) 2D Barcode Structure



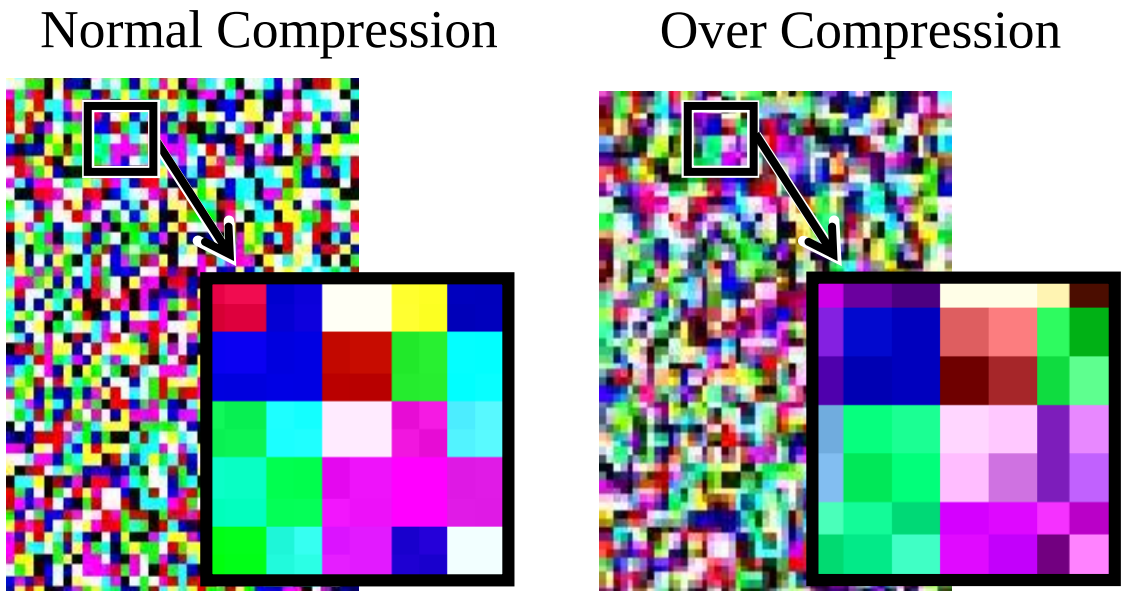
(c) Client UI

(d) Recovered and Recomposited Client UI

Results - Video Quality



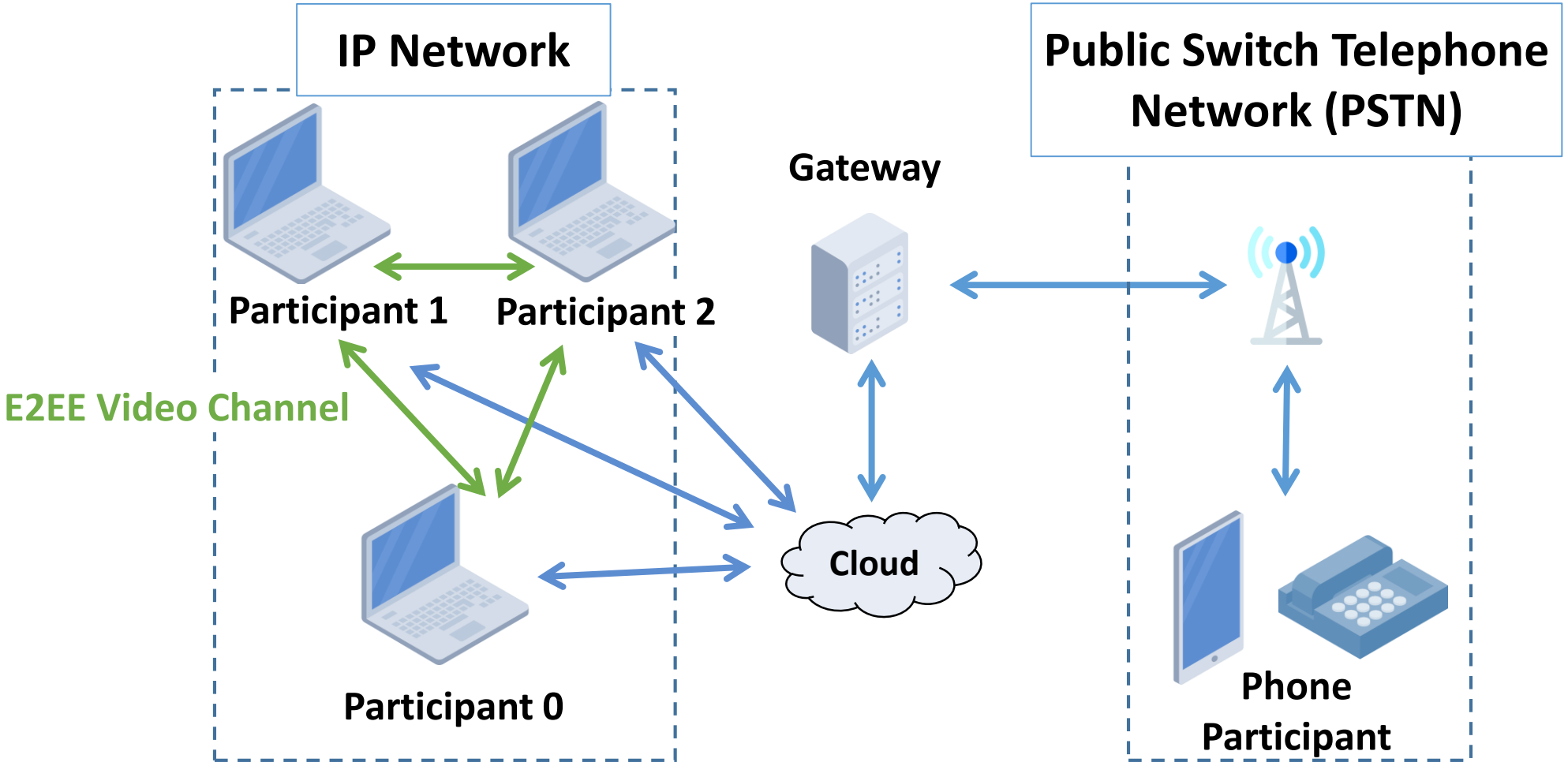
(a) BER, Goodput v.s. Block Size



(b) Over Compression Situation

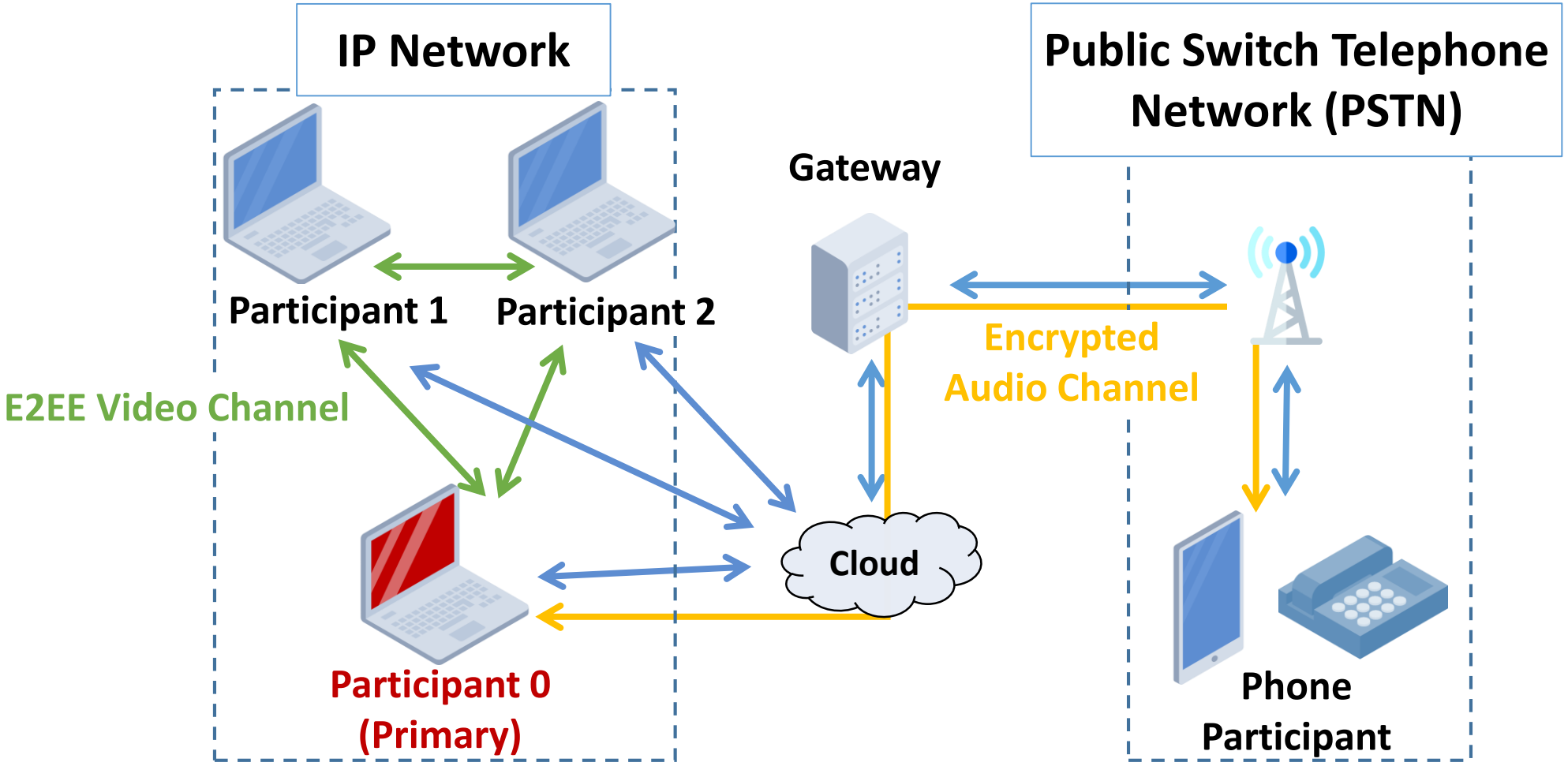
Challenge 3 - Support PSTN Dial-in Access

- Architecture of IP and PSTN hybrid conference



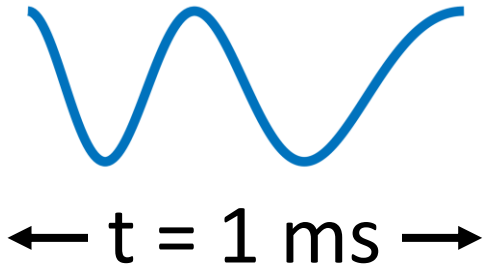
Solution - Relay Participant

- Introduce a primary participant to relay audio streams between IP network and PSTN



Example - Audio Channel Modulation

- Bit ‘1’: f0 = 2200 Hz to f1 = 1800 Hz
- Bit ‘0’: f0 = 800 Hz to f1 = 1200 Hz
- Resynchronization: Utilize chirps to resist sample offsets

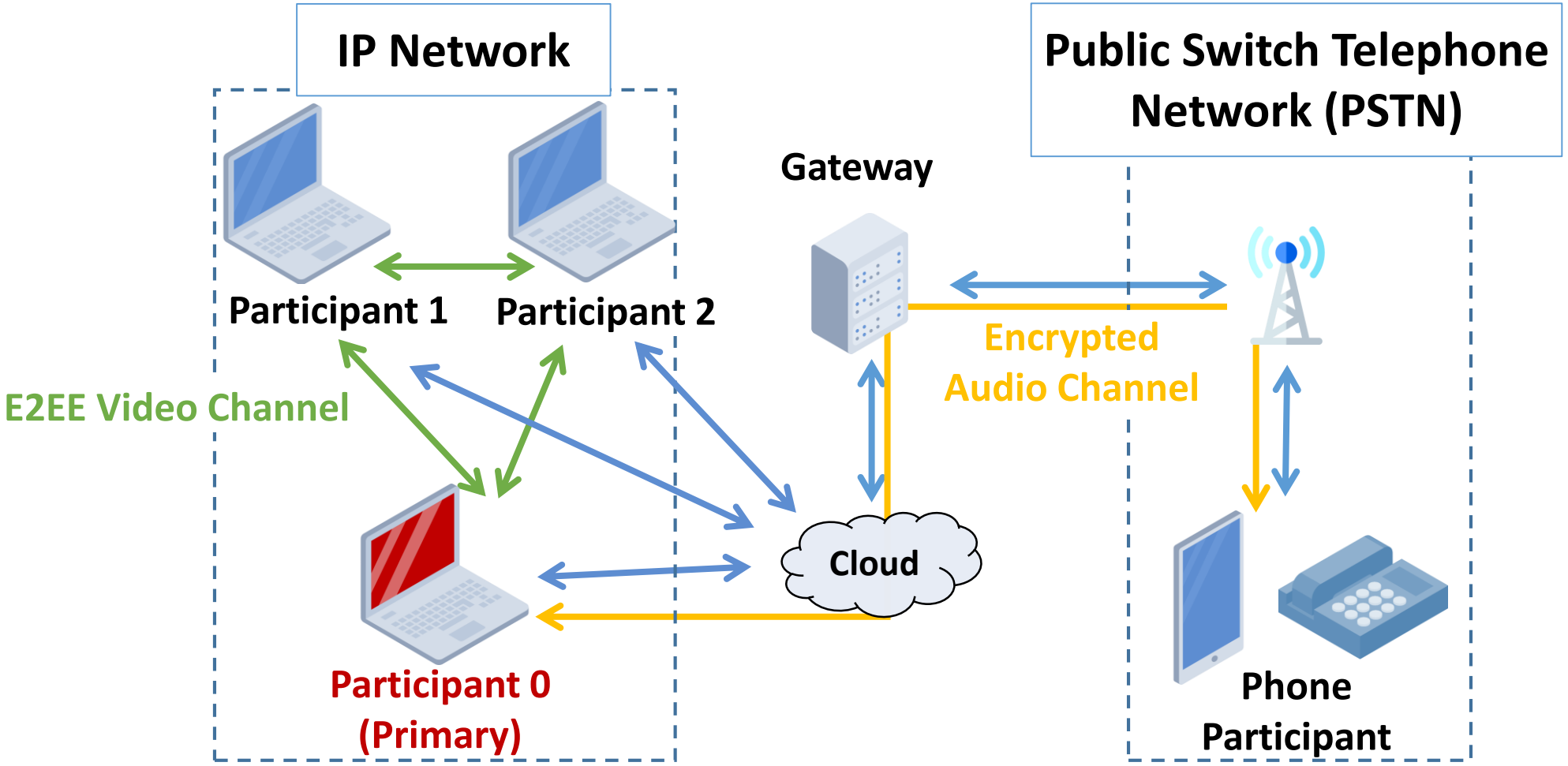


(a) ‘1’ waveform

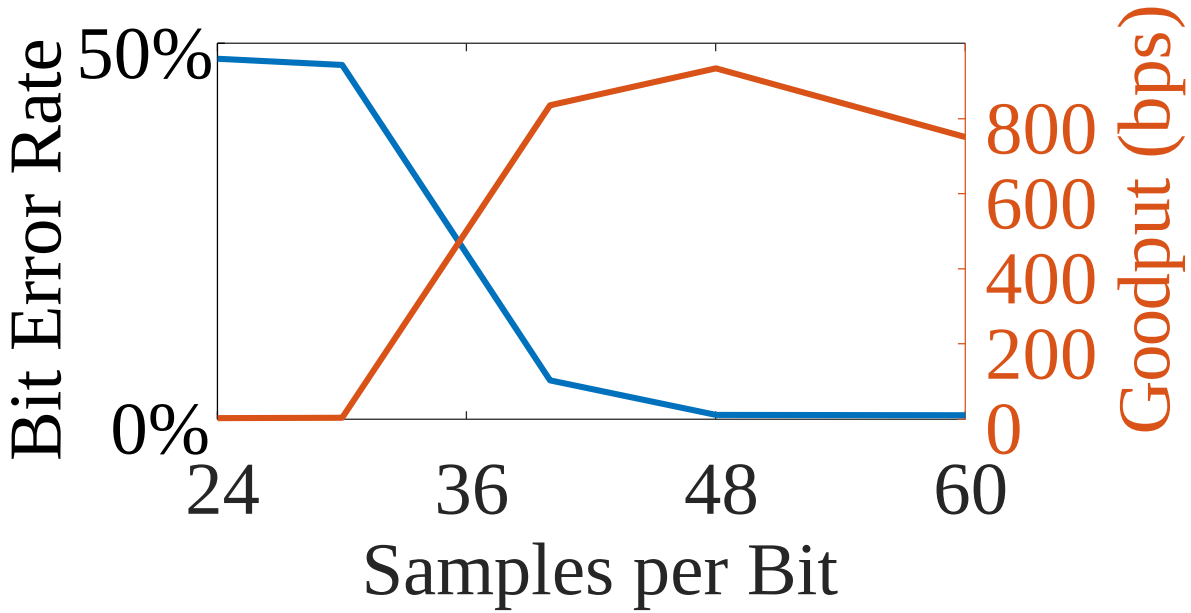
(b) ‘0’ waveform

Solution - Relay Participant

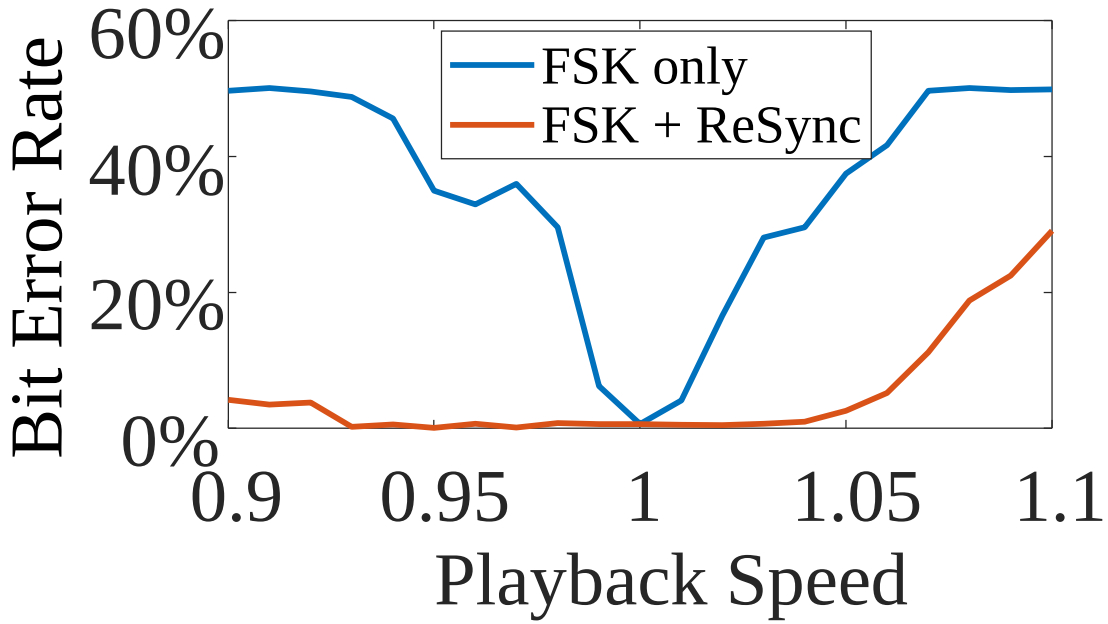
- Introduce a primary participant to relay audio streams between IP network and PSTN



Results – Audio Quality



(a) BER, Goodput of Audio Tunnel



(b) Performance of ReSync

Summary

- Propose a practical software layer in the host system to enforce end-to-end encryption on conference applications
- Build a lightweight I/O virtualization framework to enhance the compatibility and isolate private data from conference applications
- Propose methods to transmit data within conference applications against lossy compression

Thank You !