End-to-end Encrypted Audio Conferencing

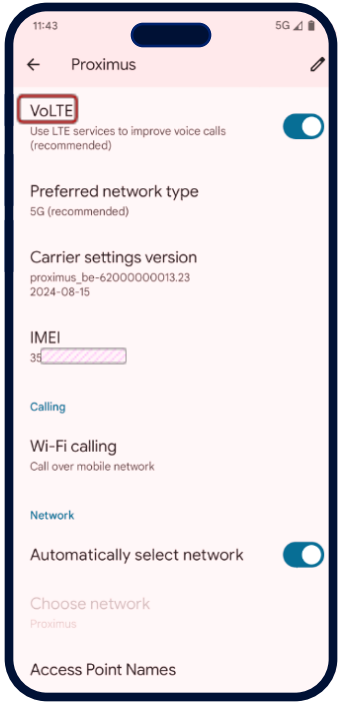
Dec 2025

Lode, **Emad**, Geert, Janwillem, Lieven, Paschalis, Paarijaat, Marc, Claudia, Barry, Robin, Bhavish, Aikata, Martin, Leo

NOKIA BELL LABS

VoLTE carrier-grade encryption

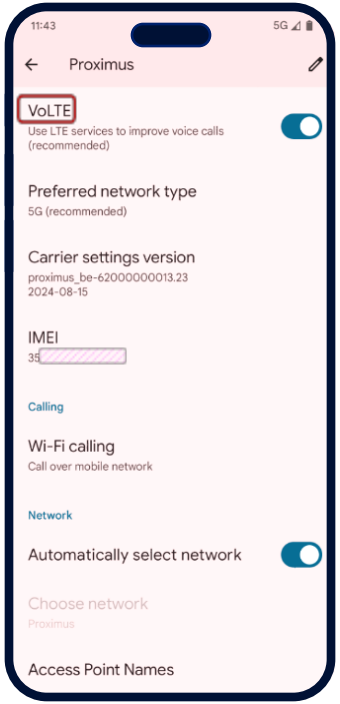
Problem: a prime wiretapping target

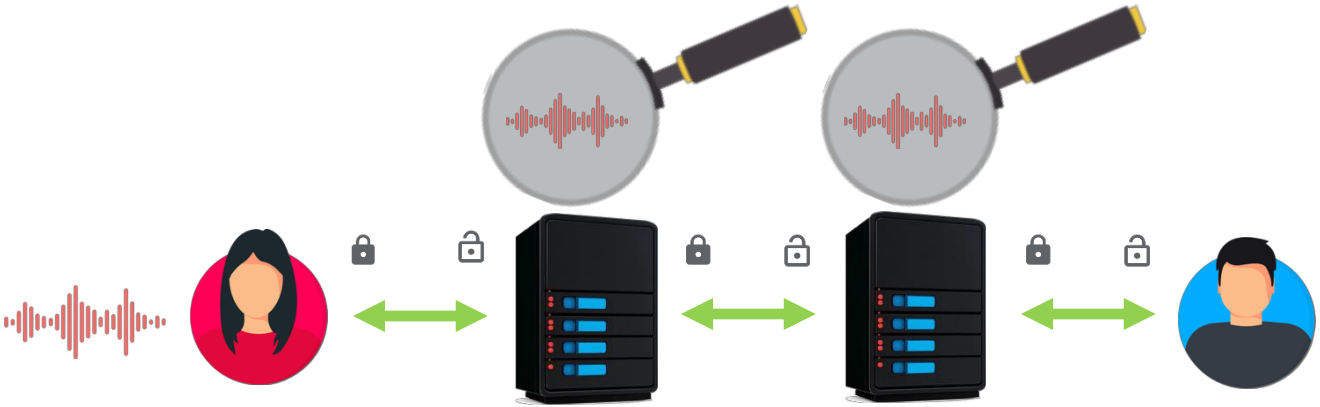


3GPP TS 23.228 (IMS architecture)
3GPP TS 24.147 (Conferencing Application)

VoLTE carrier-grade encryption

Problem: multiple “hop-by-hop” wiretap exposures

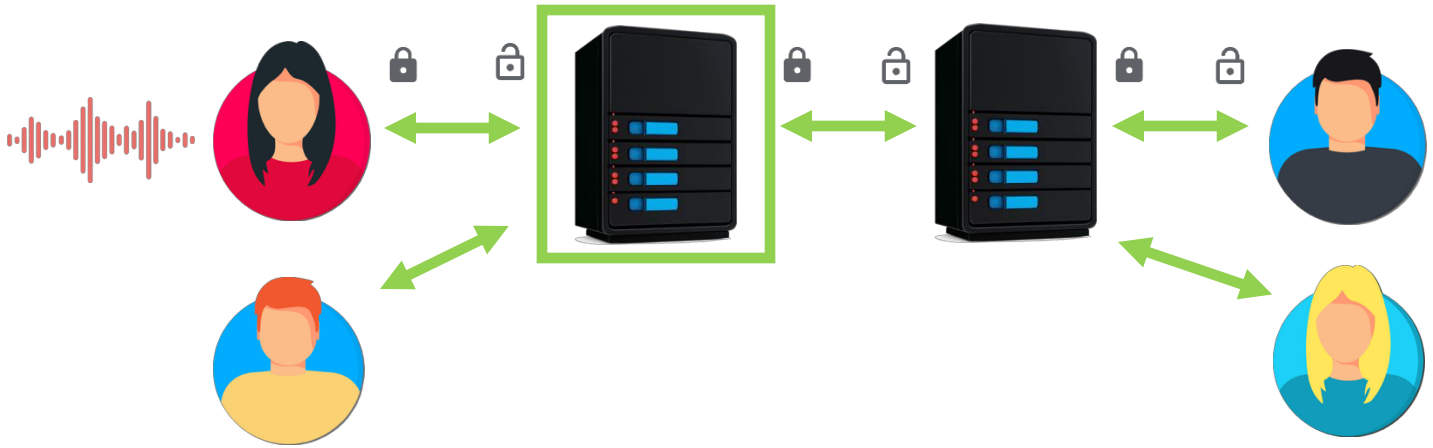




3GPP TS 23.228 (IMS architecture)
3GPP TS 24.147 (Conferencing Application)

VoLTE carrier-grade encryption

Today's approach: Group calls require a "secure focus" server



2013

The Intercept_

HOW U.K. SPIES HACKED A EUROPEAN ALLY AND GOT AWAY WITH IT

A British spy agency secretly hacked a company in Belgium then evaded an extraordinary police investigation.

Ryan Gallagher

February 17 2018, 2:10 a.m.

Share

https://theintercept.com/2018/02/17/gchq-belgacom-investigation-europe-hack/

2024

Salt Typhoon exploited technical vulnerabilities in some of the cybersecurity products like firewalls used to protect large organizations. Once inside the network, the attackers used more conventional tools and knowledge to expand their reach, gather information, stay hidden, and deploy malware for later use.

According to the FBI, Salt Typhoon allowed Chinese officials to obtain a large amount of records showing where, when, and who specific individuals were communicating with. In some cases, they noted that Salt Typhoon gave access to the contents of phone calls and text messages as well.

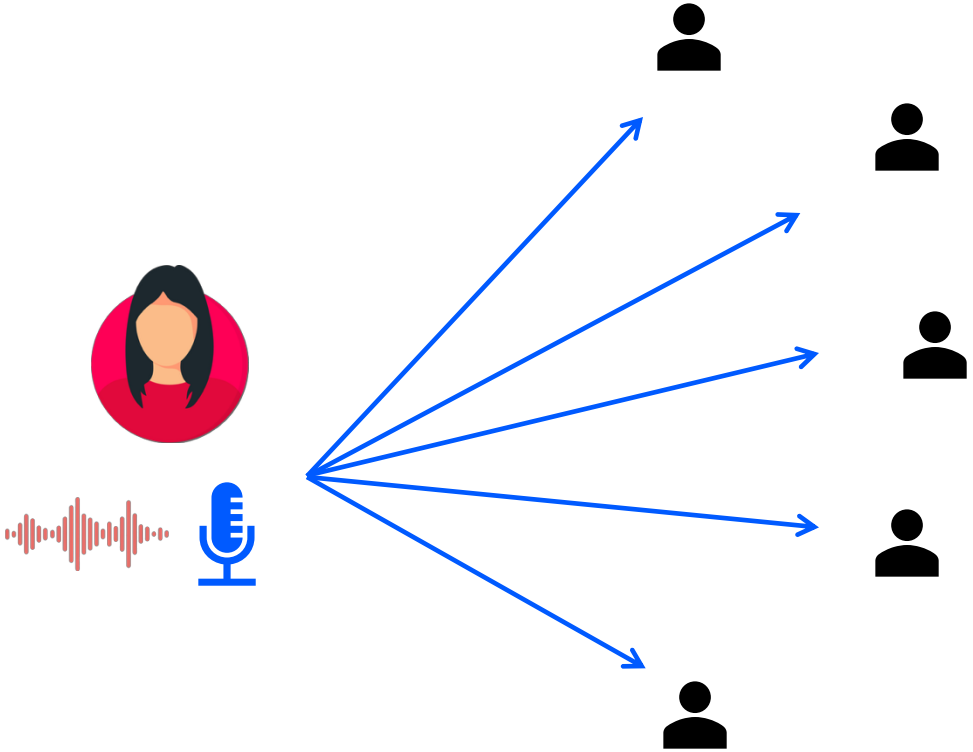
Salt Typhoon also compromised the private portals, or backdoors, that telephone companies provide to law enforcement to request court-ordered monitoring of phone numbers pursuant to investigations. This is also the same portal that is used by U.S. intelligence to surveil foreign targets inside the United States.

As a result, Salt Typhoon attackers may have obtained information about which Chinese spies and informants counterintelligence agencies were monitoring – knowledge that can help those targets try to evade such surveillance.

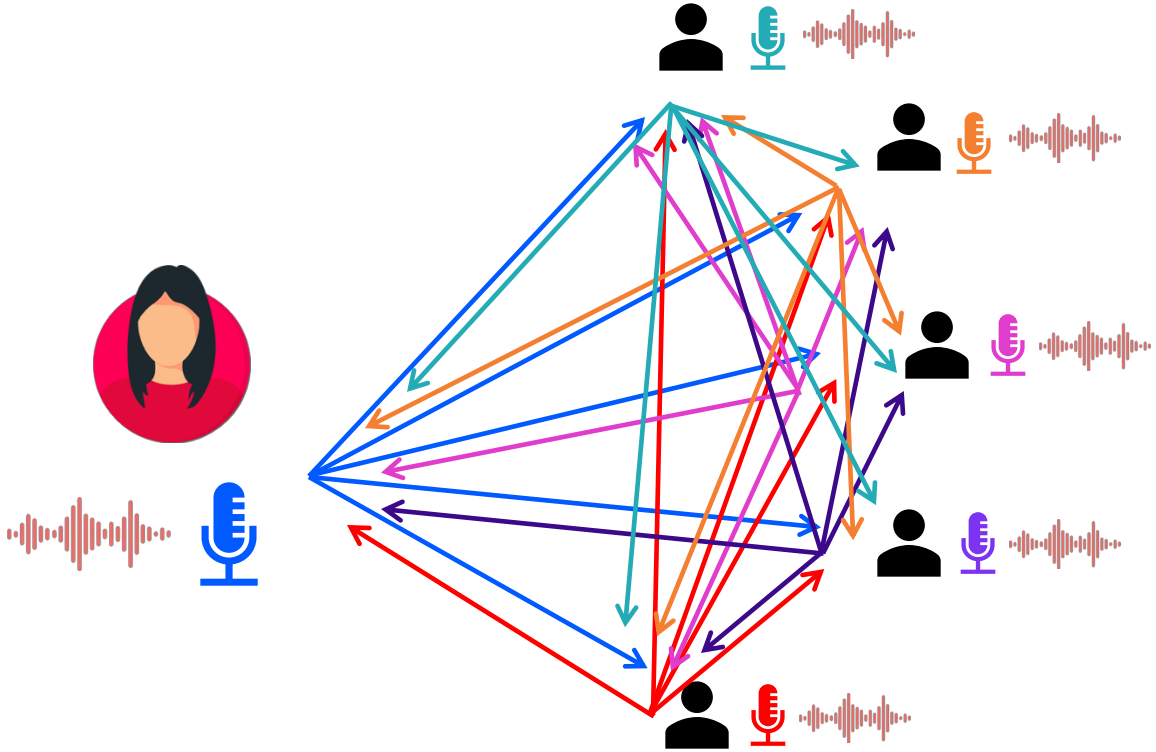
SIGSALY (1943)

"Speech Encipherment system"
by Homer Dudley (Bell Labs)
and Alan Turing

Audio Mixing

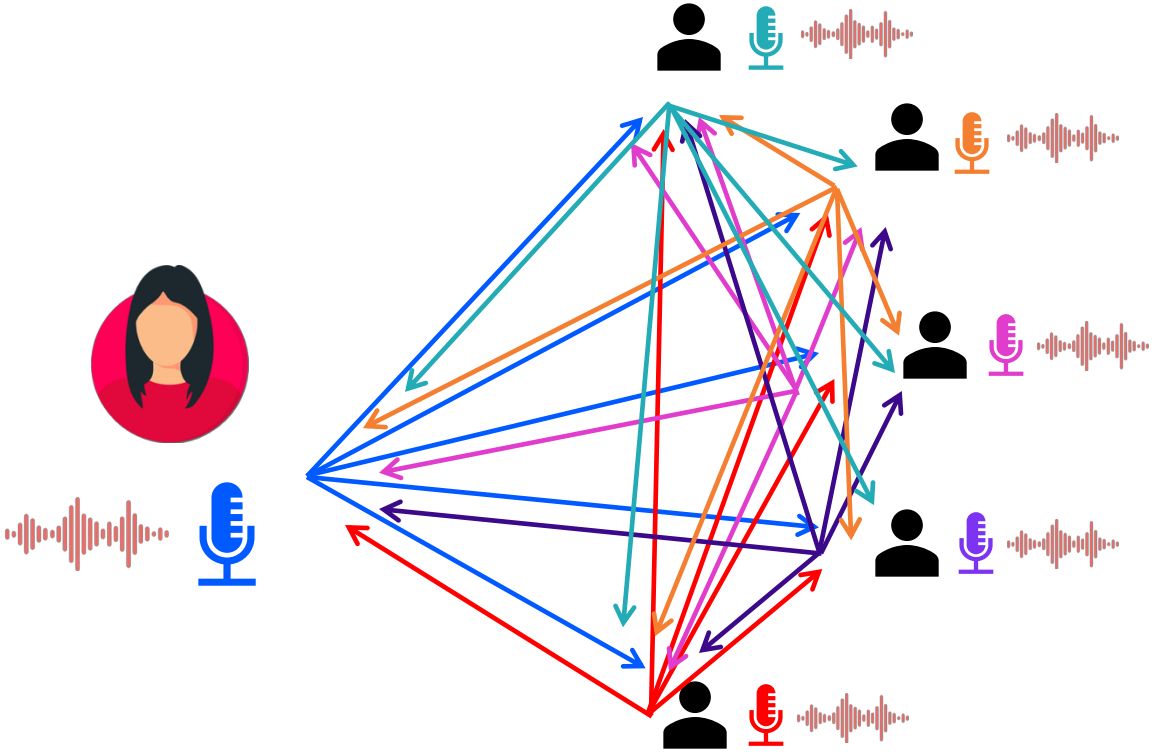


Audio Mixing

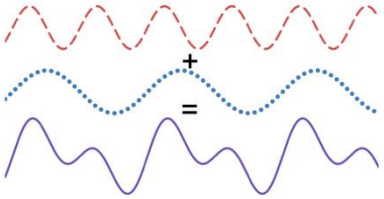


Traffic complexity grows $\boldsymbol{O(n^2)}$

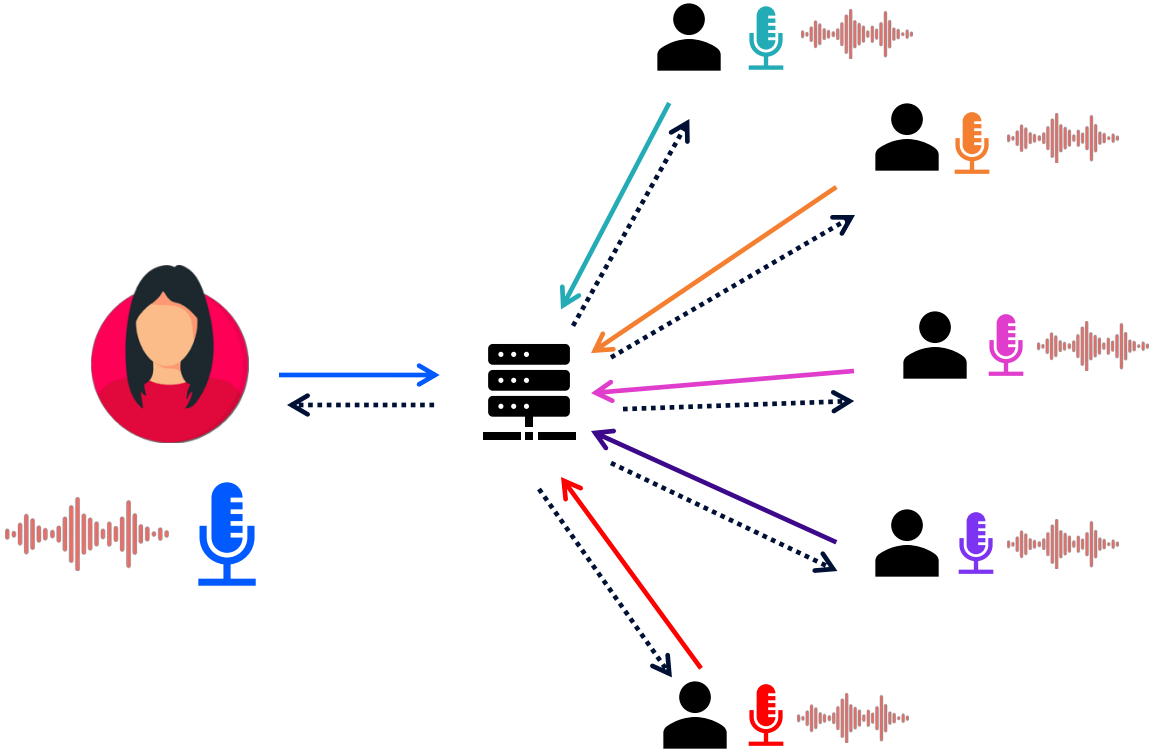
Audio Mixing



Traffic complexity grows $\boldsymbol{O(n^2)}$

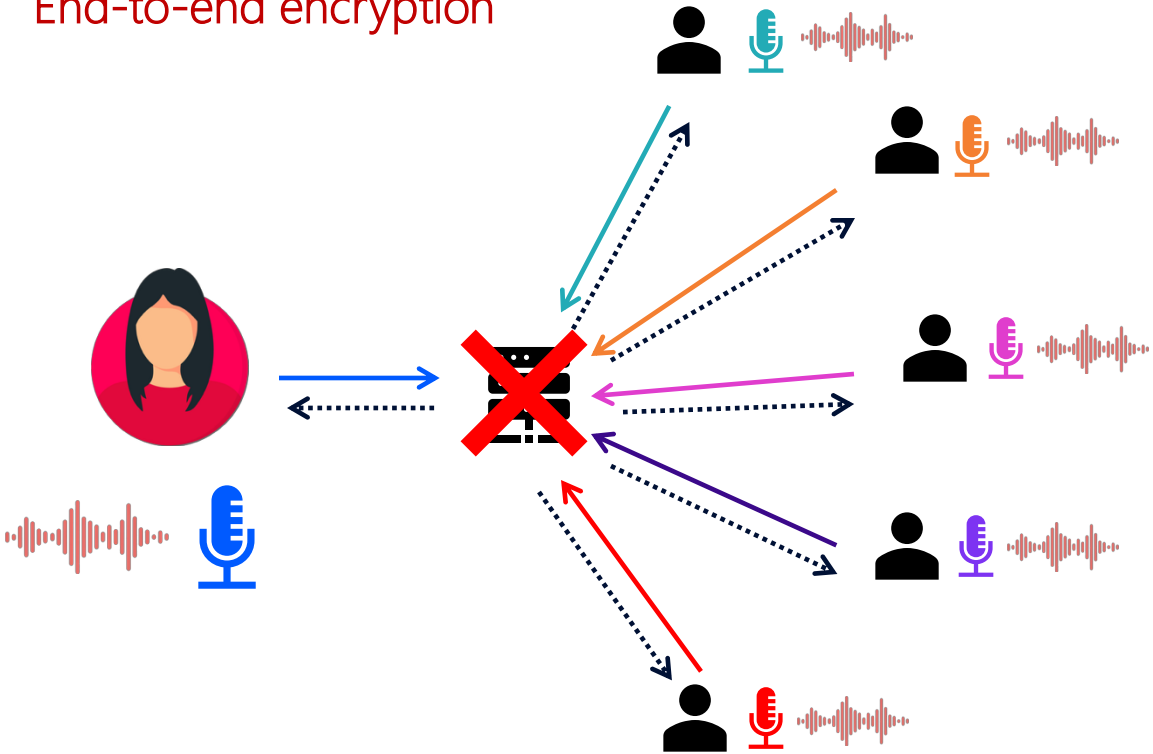


Audio Mixing

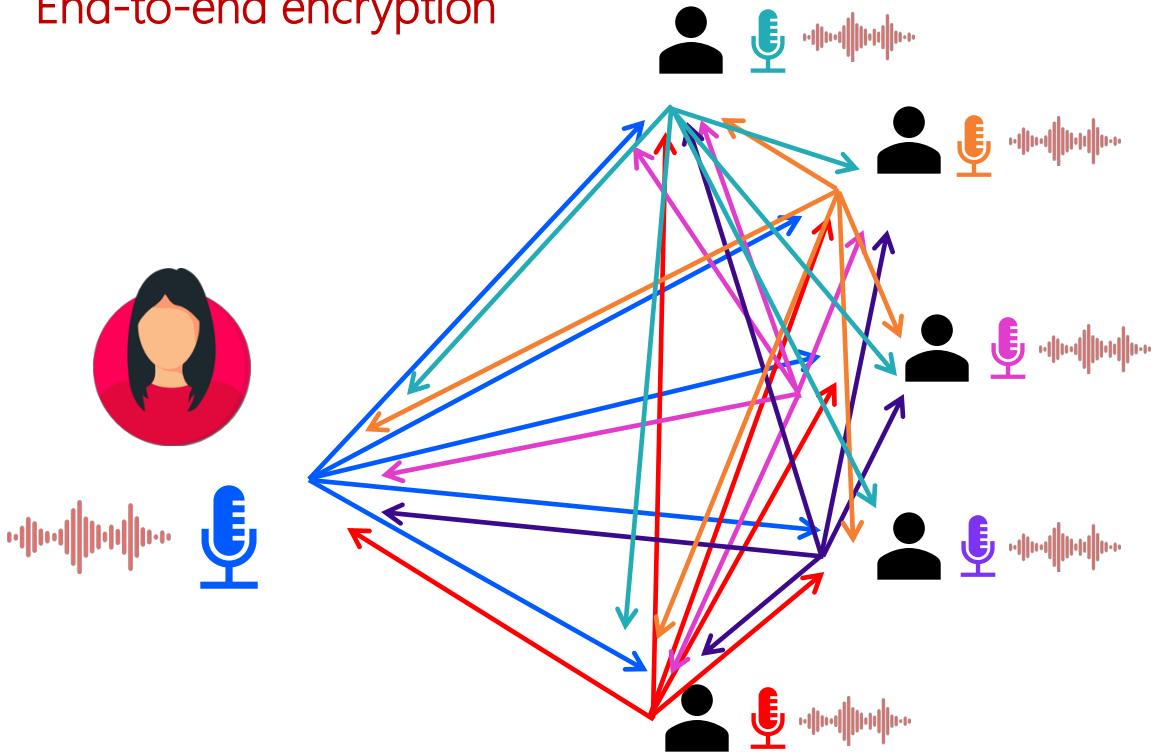


Audio Mixing

End-to-end encryption



Audio Mixing
End-to-end encryption

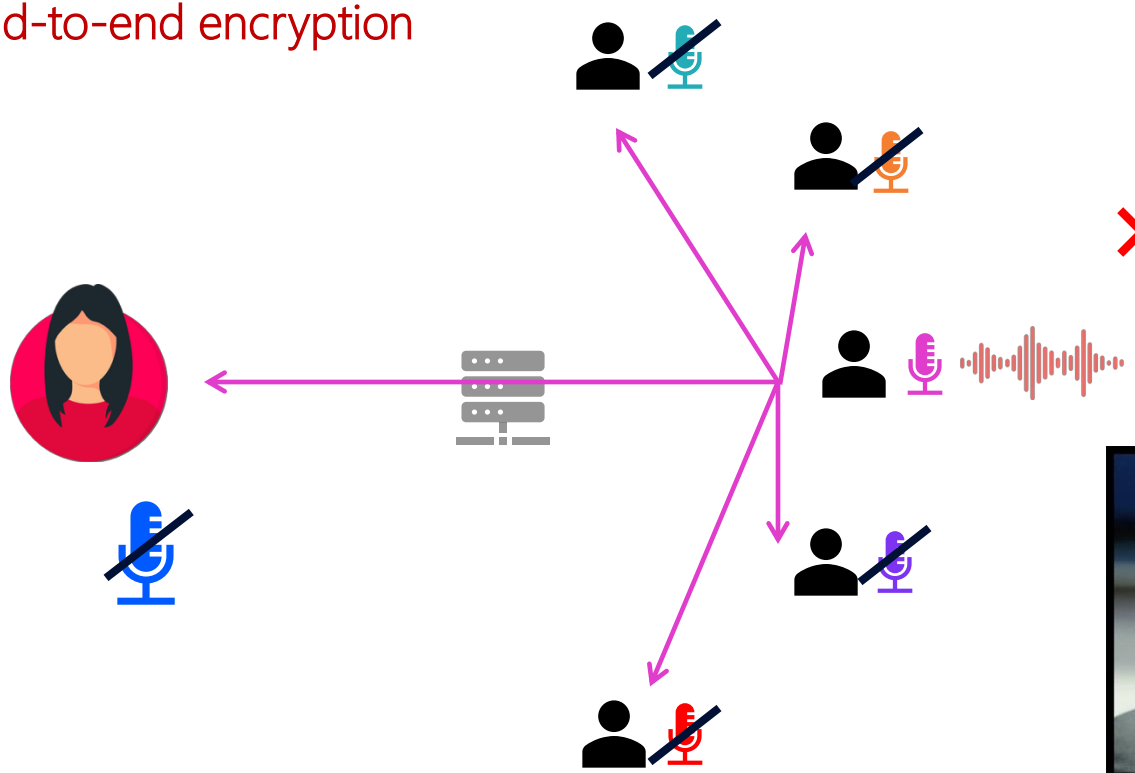


Traffic complexity grows $\boldsymbol{O(n^2)}$

Audio synchronization complexity

Limitations on audio Enhancement techniques

Audio Mixing
End-to-end encryption

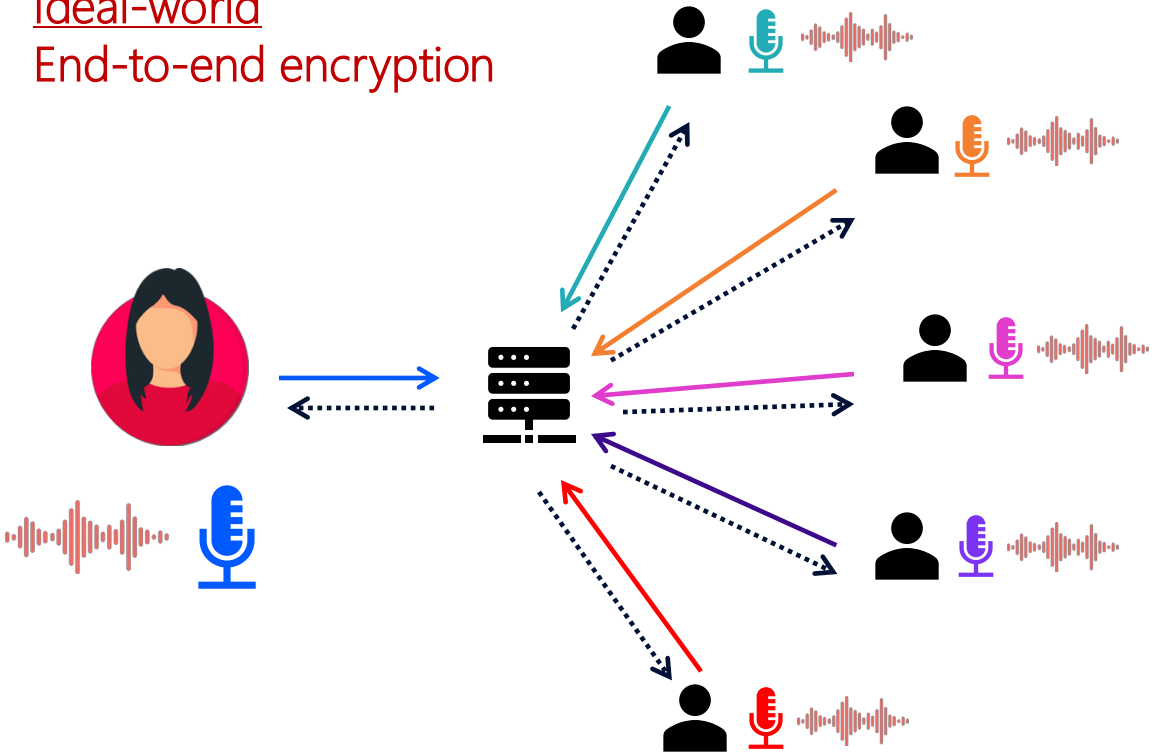


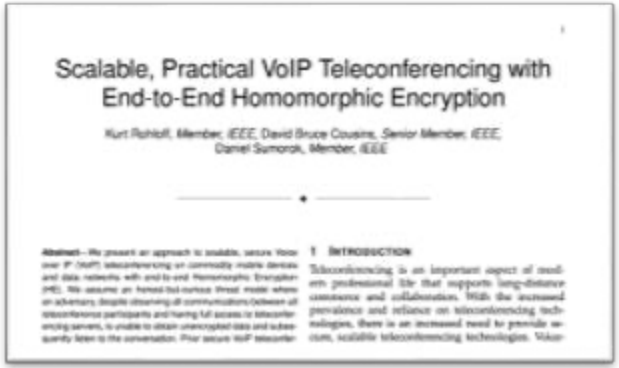
✕ Speaker anonymity

Audio Mixing

Ideal-world

End-to-end encryption





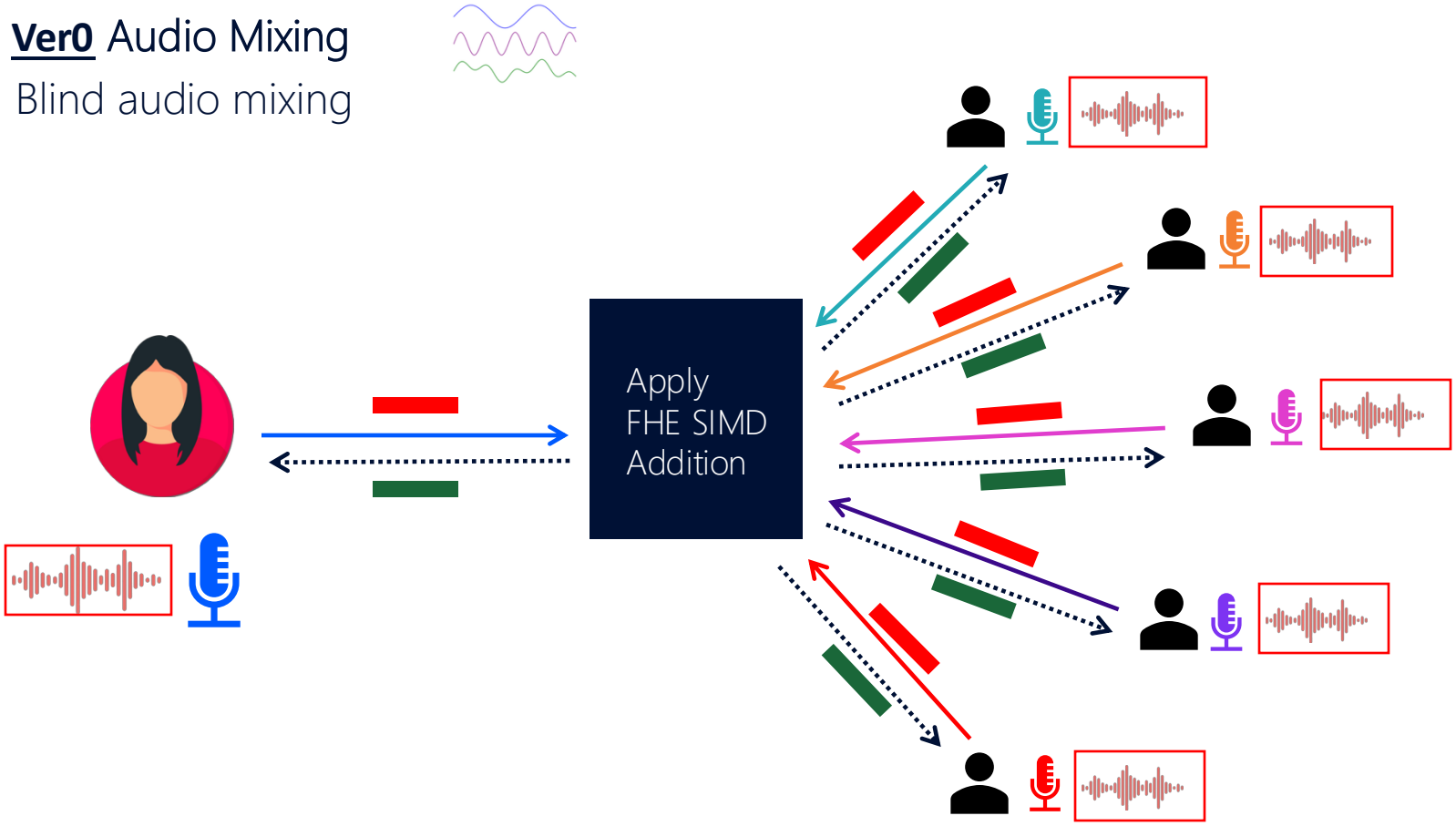
Scalable, Practical VoIP Teleconferencing with End-to-End Homomorphic Encryption

Kurt Rohloff, *Member, IEEE*, David Bruce Cousins, *Senior Member, IEEE*, Daniel Sumorok, *Member, IEEE*

Homomorphic Encryption for Audio Conferencing

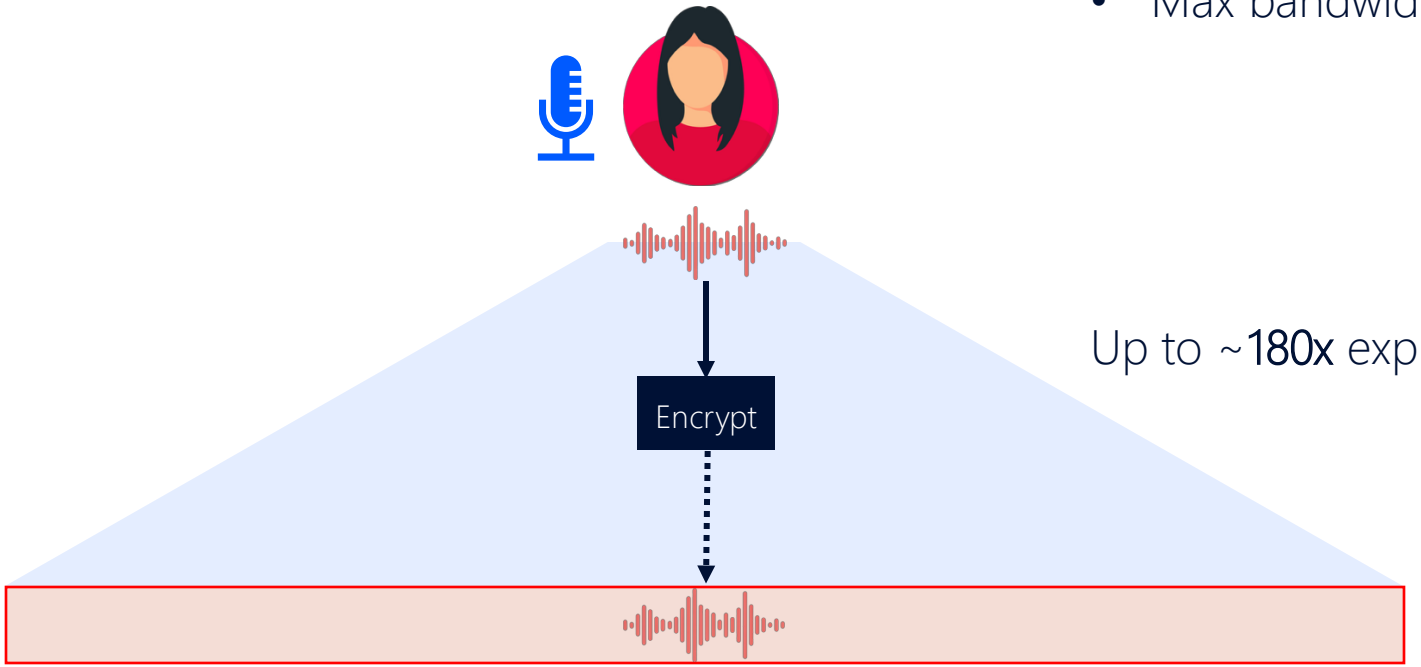
Ver0 Audio Mixing

Blind audio mixing



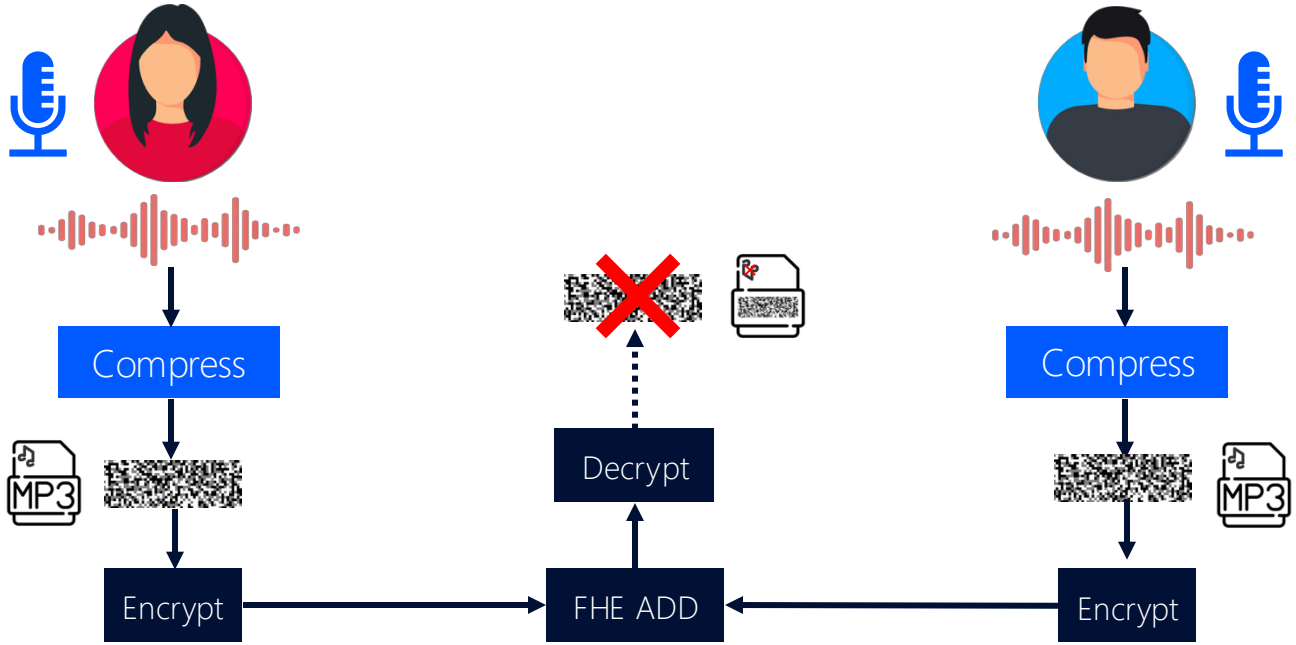
Blind audio mixing
Bandwidth limitations

Real-time audio requirement
- Max latency $\approx 0.25s$
- Max bandwidth ≈ 1 Mbps



Up to ~180x expansion

Compress then encrypt



Commonly used compression techniques (e.g. MP3)
do **not** preserve additive & mixing properties

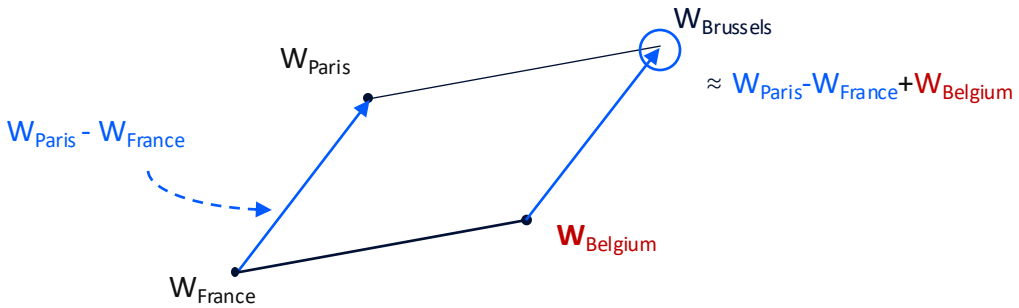
Additive Homomorphic Neural Compression

Embeddings are underrated!

https://technicalwriting.dev/ml/embeddings/overview.html

Word2Vec: Text embeddings

Paris – France + Belgium ≈ Brussels



Efficient Estimation of Word Representations in Vector Space

Tomas Mikolov
Google Inc., Mountain View, CA
tmikolov@google.com

Kai Chen
Google Inc., Mountain View, CA
kaichen@google.com

Greg Corrado
Google Inc., Mountain View, CA
gcorrado@google.com

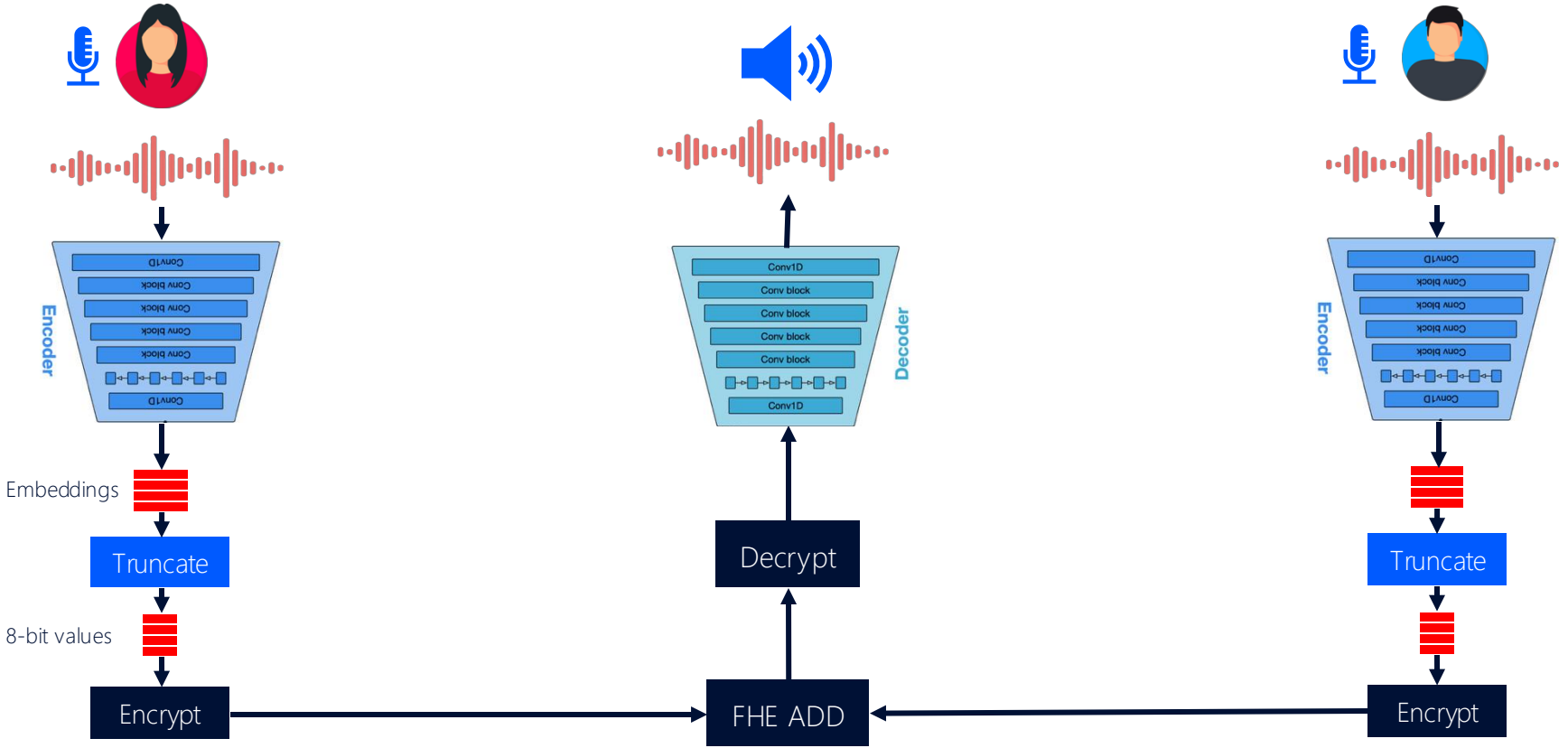
Jeffrey Dean
Google Inc., Mountain View, CA
jeff@google.com

Abstract

We propose two novel model architectures for computing continuous vector representations of words from very large data sets. The quality of these representations is measured in a word similarity task, and the results are compared to the previously best performing techniques based on different types of neural networks. We observe large improvements in accuracy at much lower computational cost, i.e. it takes less than a day to learn high quality word vectors from a 1.6 billion words data set. Furthermore, we show that these vectors provide state-of-the-art performance on our test set for measuring syntactic and semantic word similarities.

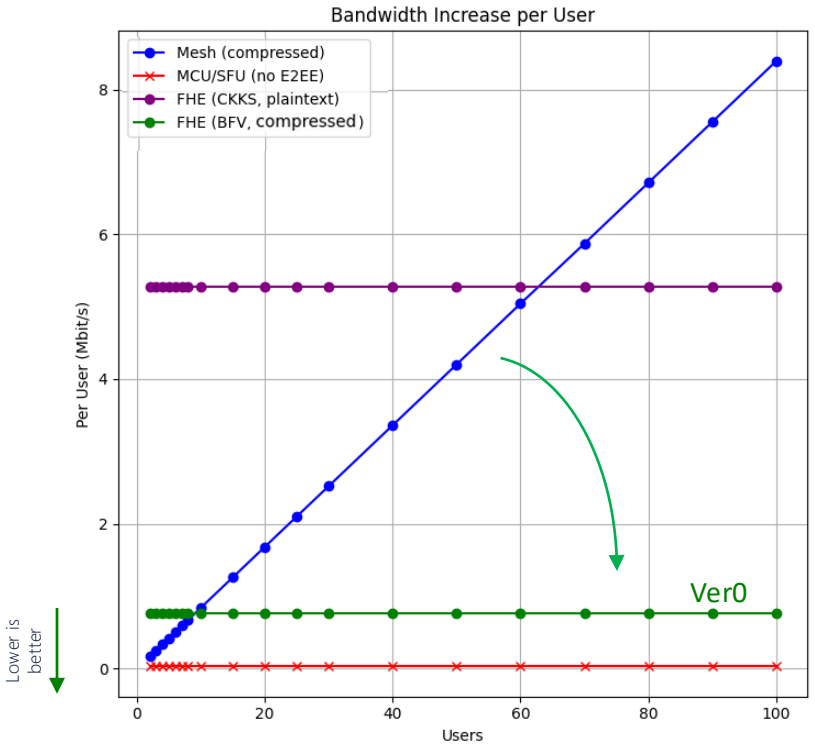
Q: Could additive properties be applicable for mixing compressed audio embeddings?

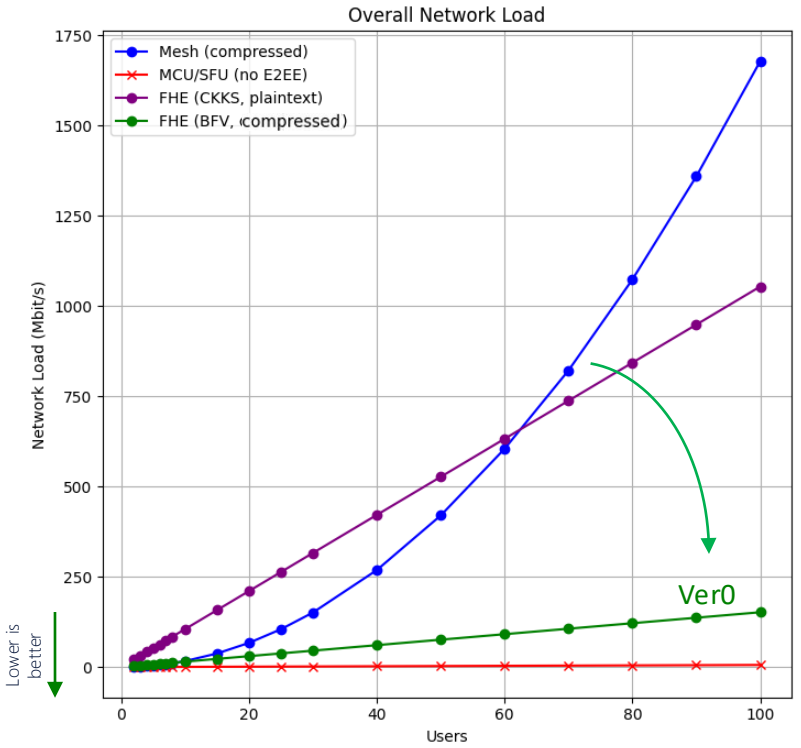
Can audio embeddings have homomorphism?



Discovery: neural compression preserves homomorphic **additive operations** in the **compressed** domain.

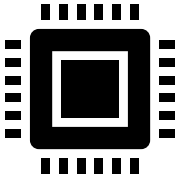
Evaluation: impact on network





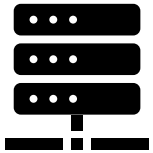
Ver0 scales efficiently in network, device, and compute usage as participants grow.

Open Challenges



Hardware acceleration
For FHE

Example:
Advanced (Spatial) Audio Processing



Bandwidth
Require more innovations

Example:
New Transciphering schemes

FHE Standardization
acceleration

Example:
It is hard to incorporate FHE into other specs.

Packet Loss Concealment

Challenge:
Mix late or missed encrypted audio

Group Key Management

Challenge:
Keys can easily get to 100+ MBs

Lawful interception

It's 2025. It's almost a law in every country.
Where are we with this?

NOKIA BELL LABS

Ver0

Lode **Hoste**, Emad **Heydari Beni**,
Geert **Heyman**, Lieven **Trappeniers**,
Paschalis **Tsiaflakis** & others

SDSR Lab, BLSR