



HAL
open science

Introducing a Verified Authenticated Key Exchange Protocol over Voice Channels for Secure Voice Communications

Piotr Krasnowski, Jerome Lebrun, Bruno Martin

► **To cite this version:**

Piotr Krasnowski, Jerome Lebrun, Bruno Martin. Introducing a Verified Authenticated Key Exchange Protocol over Voice Channels for Secure Voice Communications. INSTICC. 6th International Conference on Information Systems Security and Privacy, Feb 2020, Valetta, Malta. SciTePress, ICISSP (1), pp.683-690, Proceedings of the 6th International Conference on Information Systems Security and Privacy. 10.5220/0009156506830690 . hal-03059639v2

HAL Id: hal-03059639

<https://hal.science/hal-03059639v2>

Submitted on 7 Jan 2021

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.



Distributed under a Creative Commons Attribution - NonCommercial - NoDerivatives 4.0 International License

Introducing a Verified Authenticated Key Exchange Protocol over Voice Channels for Secure Voice Communications

P. Krasnowski, J. Lebrun, B. Martin

krasnowski@i3s.unice.fr
Université Côte d'Azur • I3S-CNRS



Voice Encryption (VE) device



Figure: The VE device visualization

The VE device provides real-time secure voice communications over 2G-4G networks and VoIP (Skype, WhatsApp, Signal...).

Recorded speech is encrypted into audio signal, adapted to transmission over voice channels with Voice Activity Detection.

Received signal can be decoded and decrypted only by a paired VE device sharing the cryptographic key.

The Session Key is freshly generated for each secure call, requiring a dedicated authenticated KE protocol.

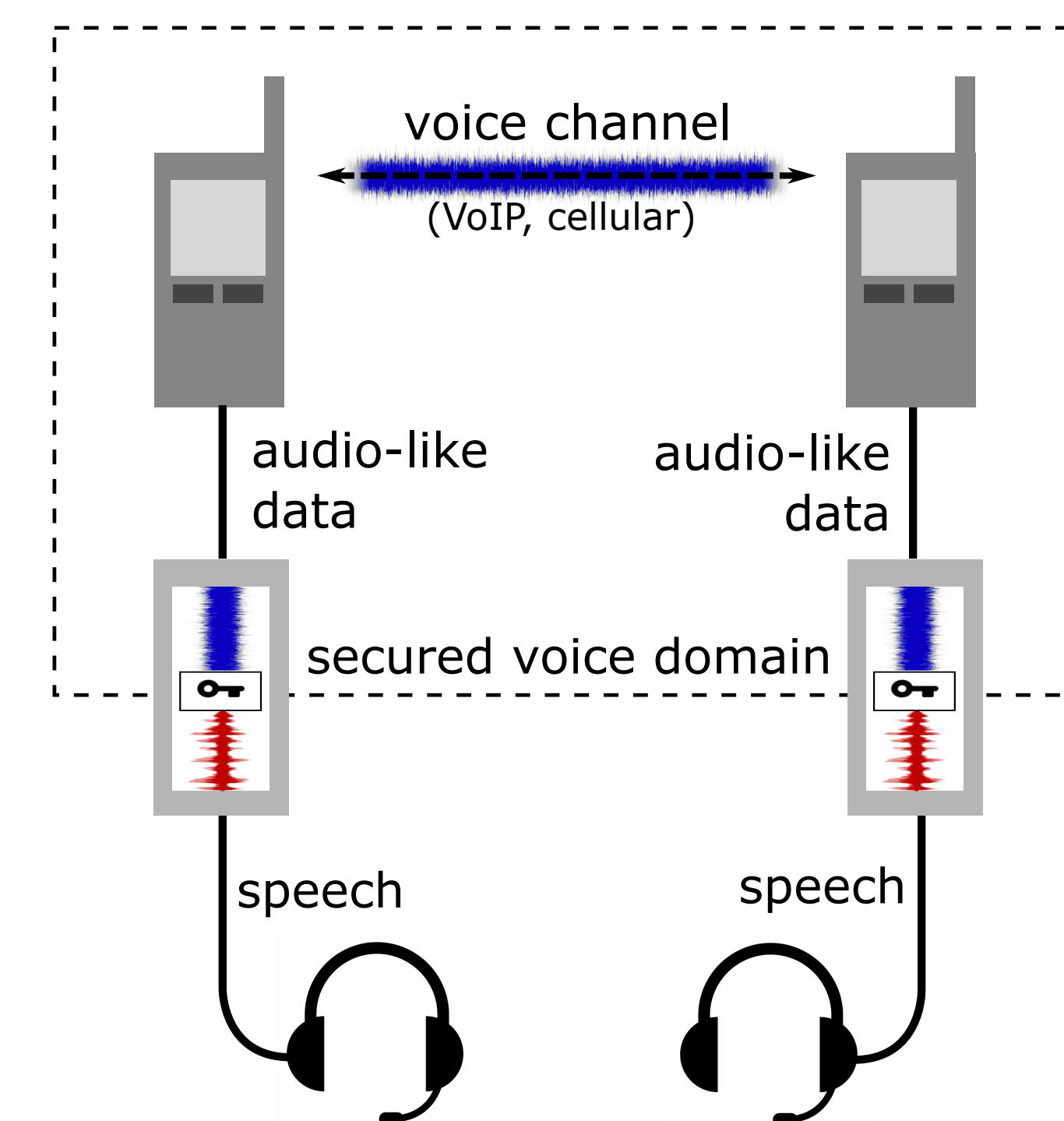
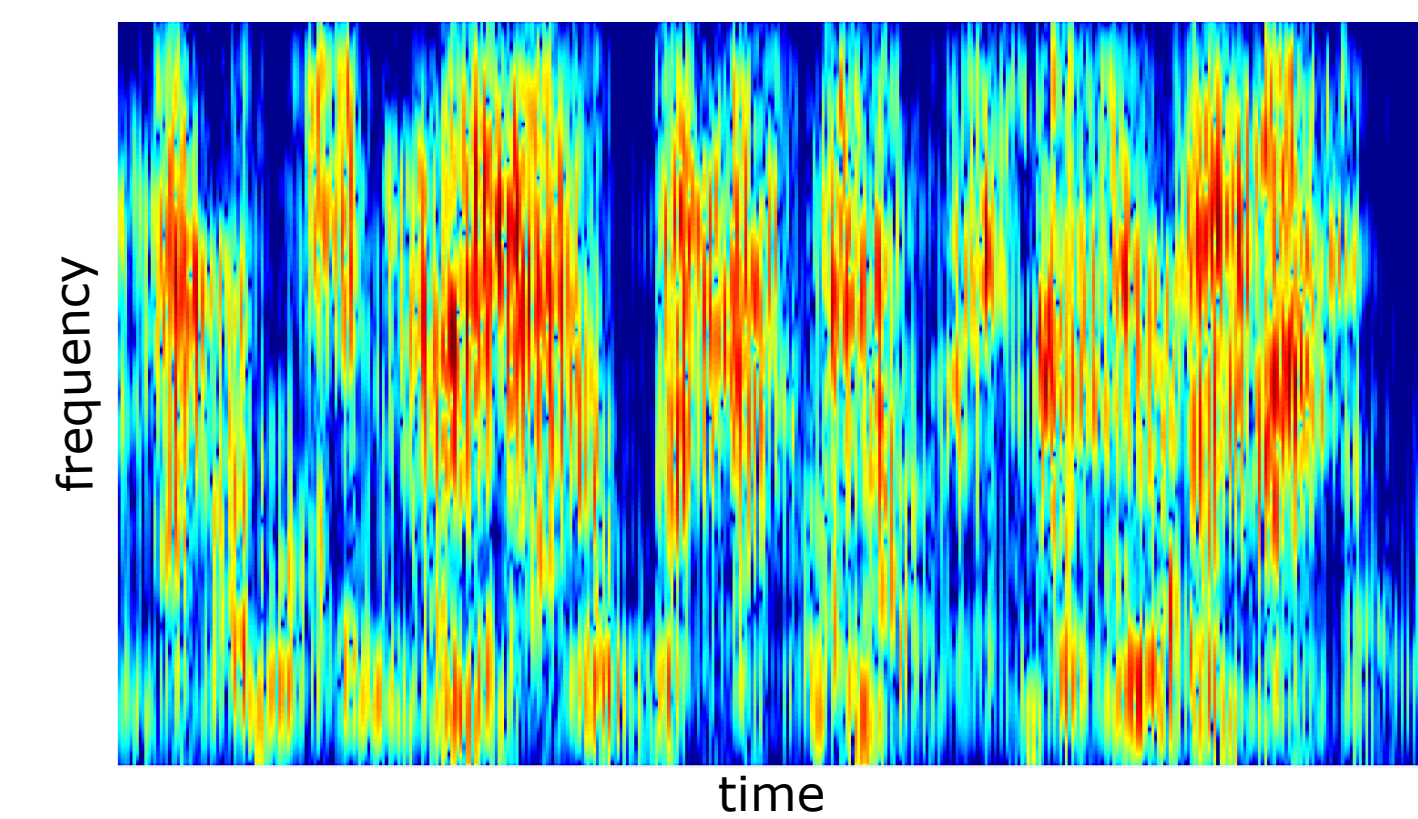
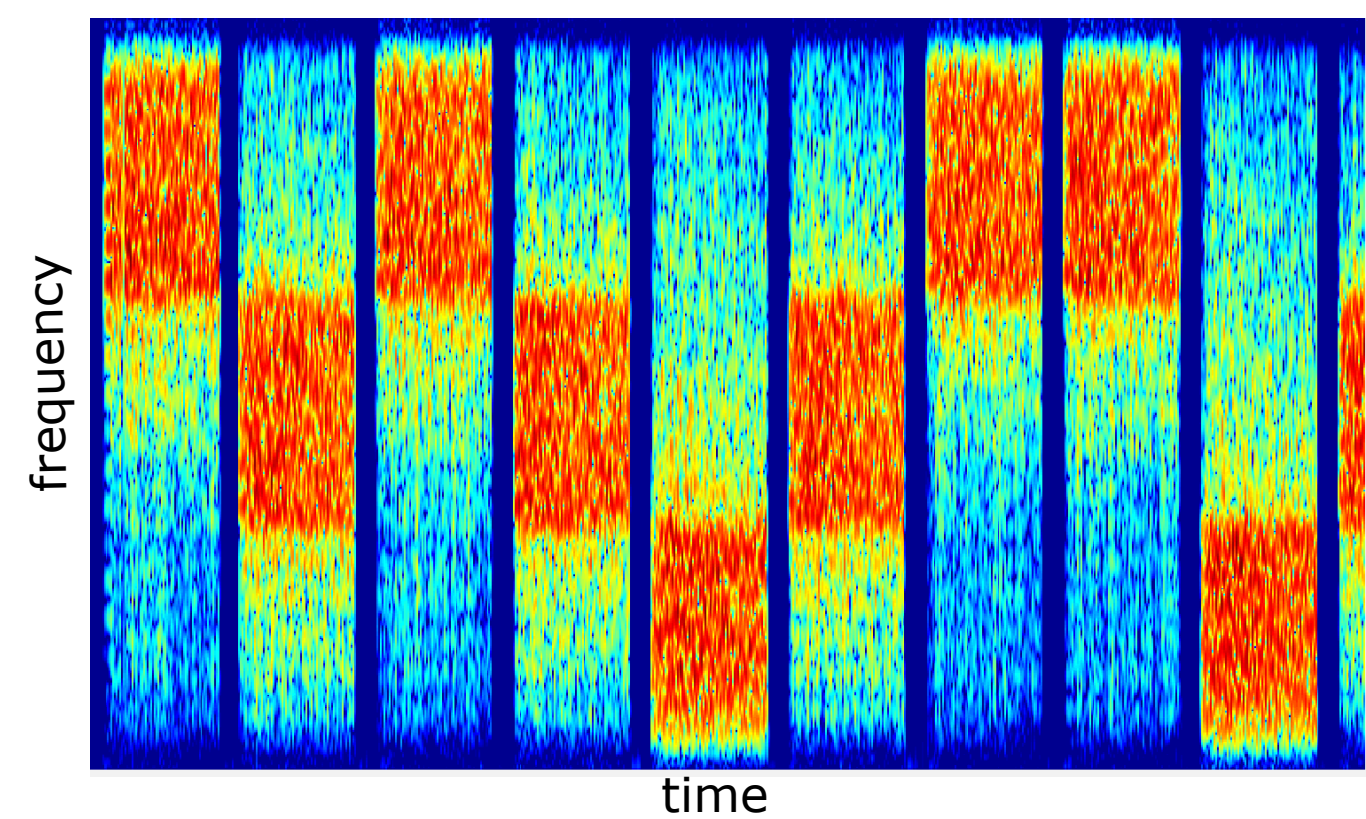


Figure: Secure voice communication scheme

Sending data over voice channel

Voice compression, filtering and quantization introduced by digital voice channels significantly distort the signal. Data over Voice (DoV) technique encodes binary data into a waveform with voice-like properties. The DoV signal is robust against blockage by voice detection algorithms and withstands voice compression by popular voice coders like AMR or Silk.



Figures: Spectrum of two different DoV techniques.

Protocol design challenges

- low bandwidth (~ 2kbps)
- signal distortion (~ 5-10% BER)
- flexible authentication (no shared secret by default)
- long round-trip time (~ 2s)
- no Public Key Infrastructure

Short Authentication String (SAS)

Short string of digits or words displayed on two VE devices after each key exchange. SAS is cooperatively compared vocally by speakers in order to verify the equality of strings.

- Speaker's voice recognition
- Session Key validation
- detecting a MITM adversary

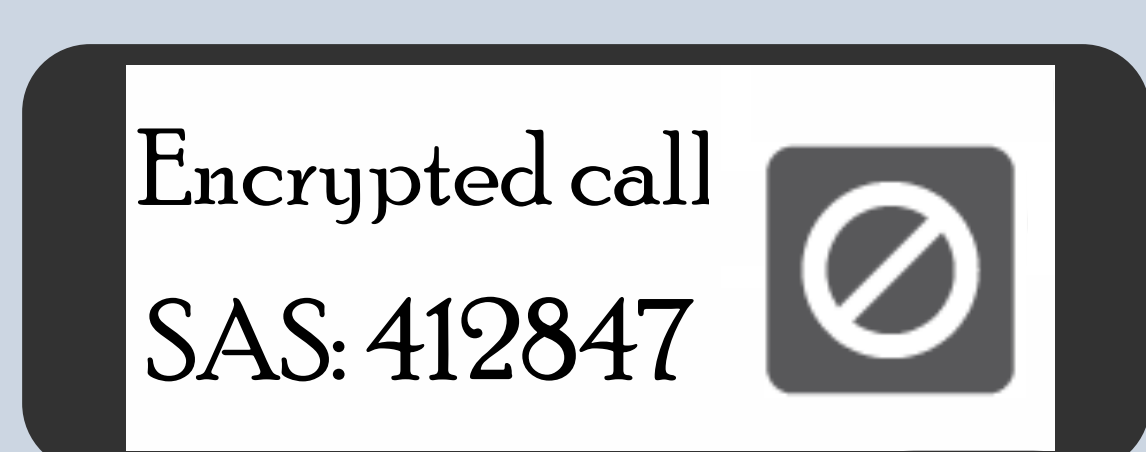
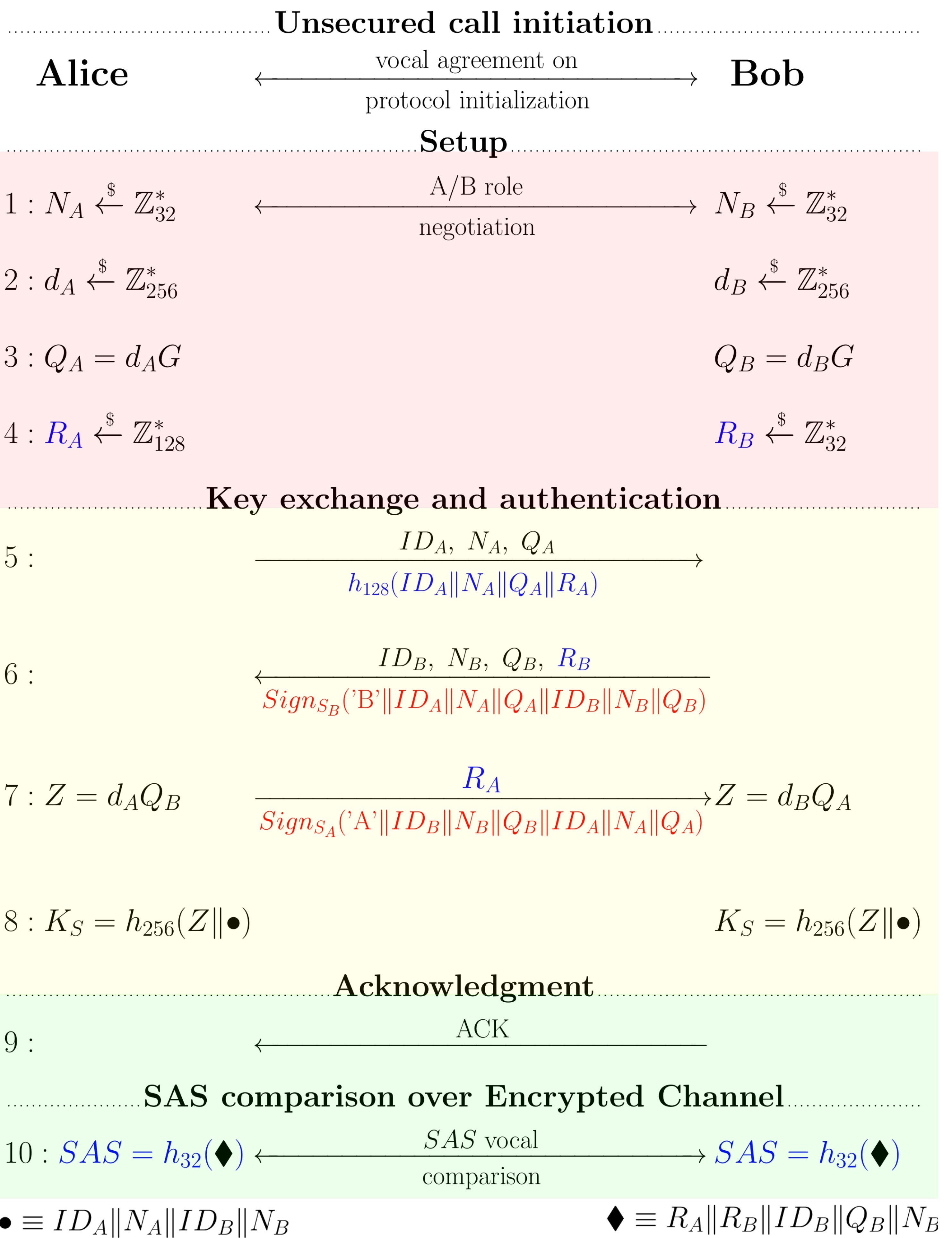


Figure: The VE device in encryption mode.

ECDHE Authenticated Key Exchange



Formal Verification with Tamarin Prover

Authentication scenario:	mutual signature	unilateral signature	vocal verification	nothing
Session Key secrecy	✓	✓	✓	✗
forward secrecy	✓	✓	✓	✗
injective agreement	✓	✓	✓	✗
reflection attack	✓	✓	✗	✗
key compromise impersonation	✓	✓	-	-

Conclusions

The proposed ECDHE key exchange protocol is highly adapted to the constraints of real-world voice-channels and is based on well-established and easily implementable primitives.

The security of the protocol relies on a scrupulous and cooperative authentication of speakers. Careless signature distribution or vocal verification are the biggest security threats.

New advances in artificial speech synthesis pose risk to security of vocal verification. Level of authentication can be improved by introducing contextual questions.

Acknowledgement:

This work is supported by grant DGA Cifre-Defense program No 01D17022178 DGA/DS/MRIS.