Secure voice communications over voice channels

Presented by: **Piotr Krasnowski**

PhD supervised by: Prof. Bruno Martin, Dr. Jerome Lebrun and Arnaud Graube

DGA supervision: Thierry Plesse

DGA Cifre-Defense program No 01D17022178 DGA/DS/MRIS

4 December 2019, Seoul

Security of voice communications

VoIP apps like **Signal** or **Telegram** are gaining popularity ...

... but are insecure against malware on the phone

" (...) governments around the world use digital spying tools designed for criminal investigations and counterintelligence to target journalists, human rights defenders, and others " Citizen Lab, 2017

Alternative: Crypto Phones

- closed and unverifiable systems
- expensive and not flexible

Project Outline

Figure: $CBOX^{TM}$ by BlackBoxSecu.

Characteristics:

- end-to-end voice encryption
- audio-to-audio processing
- real-time operation

Key technologies:

- 1. Data over voice channels
- 2. Key Exchange over voice channels
- 3. Speech encryption over voice channels (in progress)

Project Outline

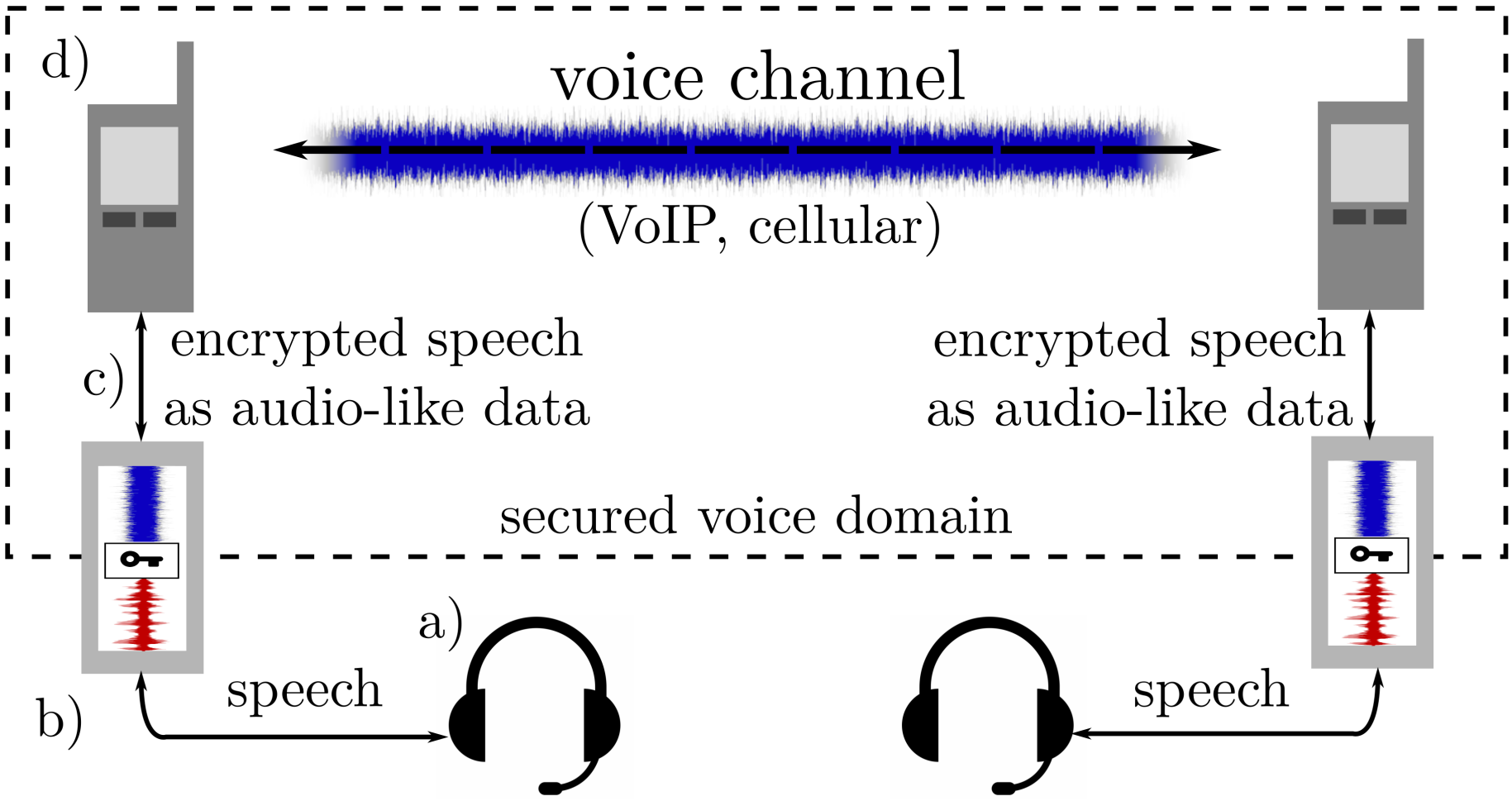
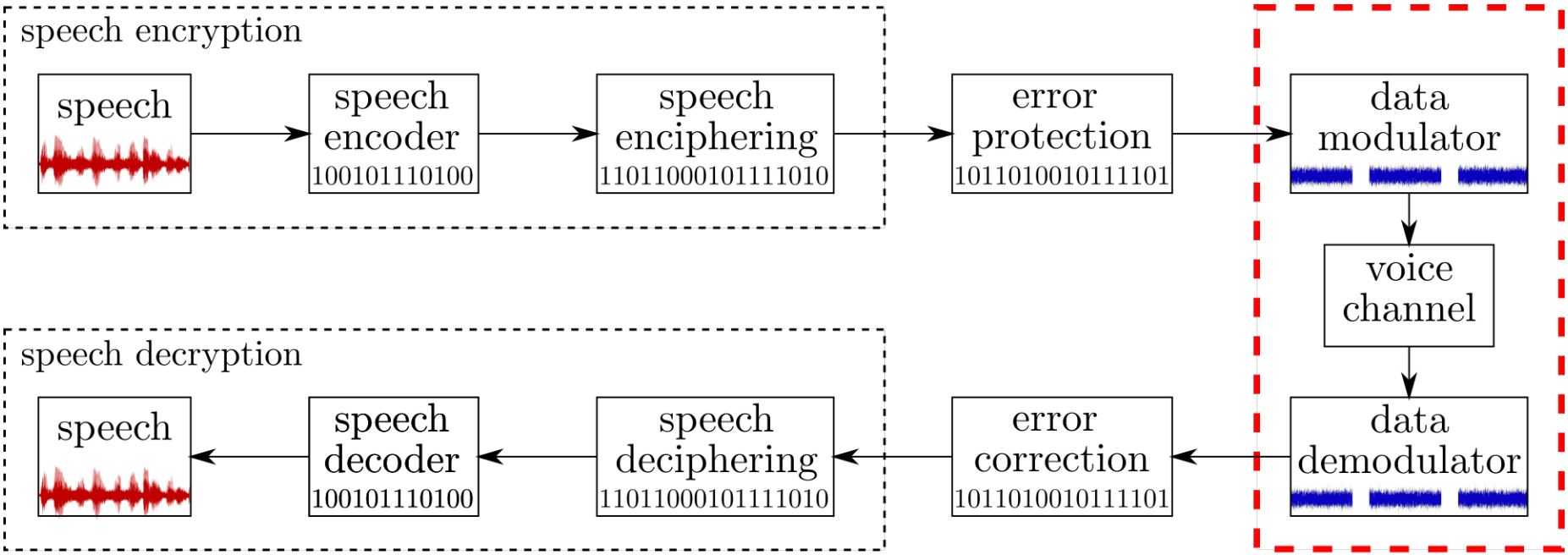


Figure: Encrypted voice over voice channel scheme.

1. Data over voice channels



How to send data over voice channels?

Digital voice channels

Elements of digital voice channels:

- **Speech compression**
  AMR, Speex, Silk ...
- **Quality of Service**
  Voice Activity Detection (VAD), Adaptive Gain Control (AGC), Noise Suppression (NS) ...

Objective of voice channels:

- to preserve speech **intelligibility**
- with an acceptable loss of **subjective** quality




Voice characteristics

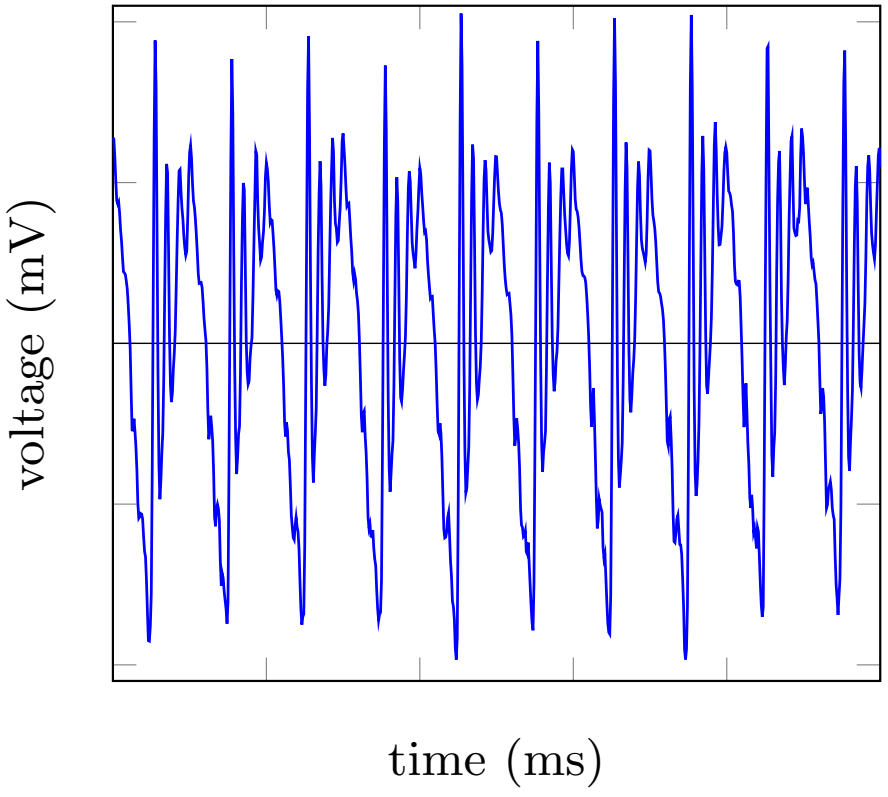


Figure: Vowel /a/ in time domain.

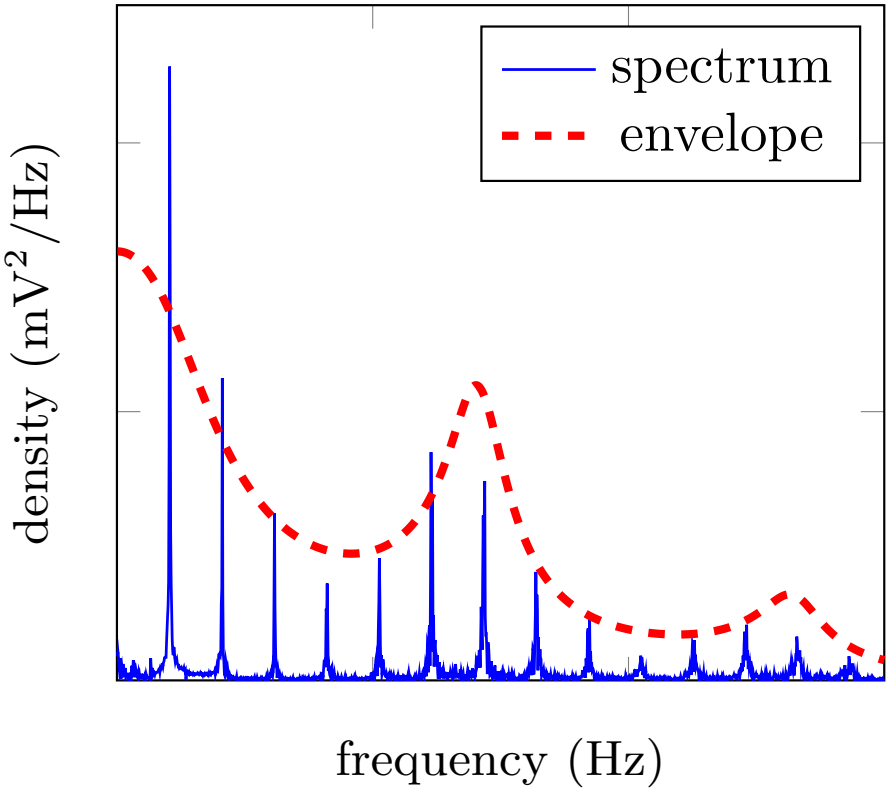
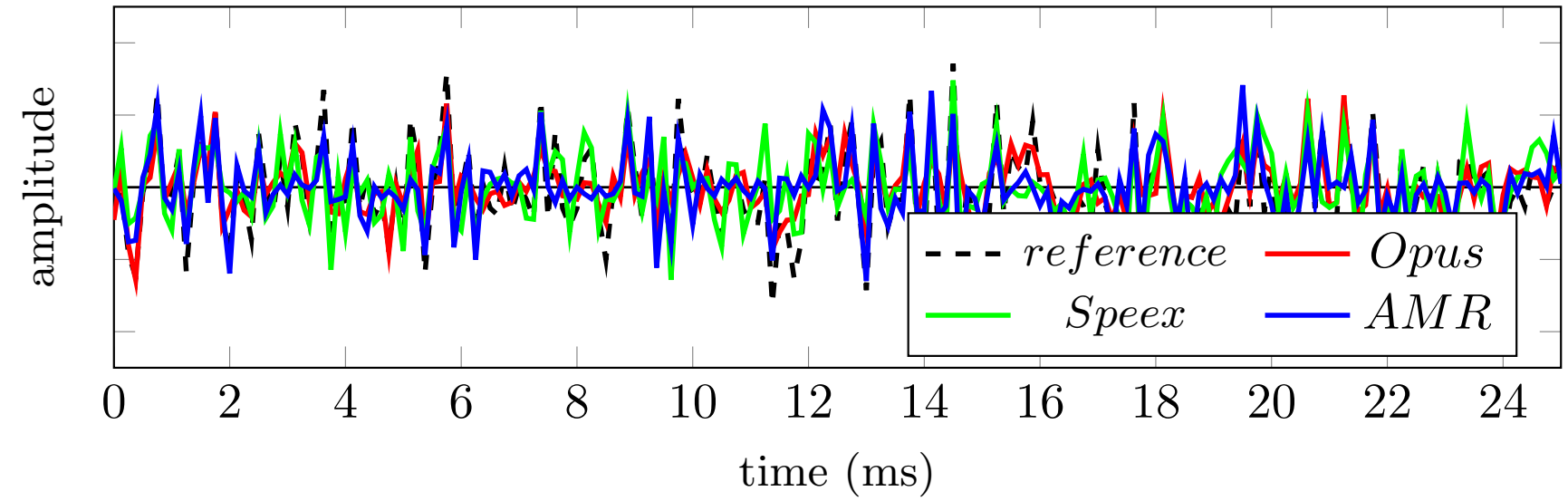
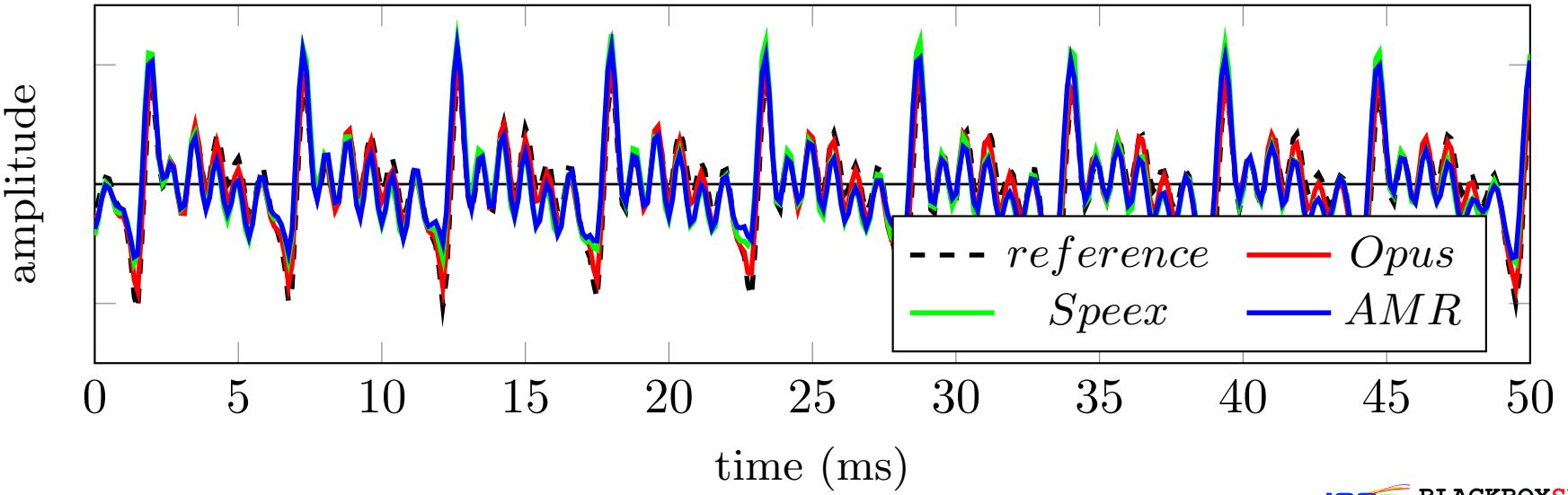


Figure: Vowel /a/ in frequency domain.

Voice compression





Linear Predictive Coding (LPC)

- most popular speech coding technique (AMR, Silk, Speex...)
- used in 2G-5G networks and VoIP (Skype, WhatsApp, Signal...)
- based on a model of **speech production mechanism**

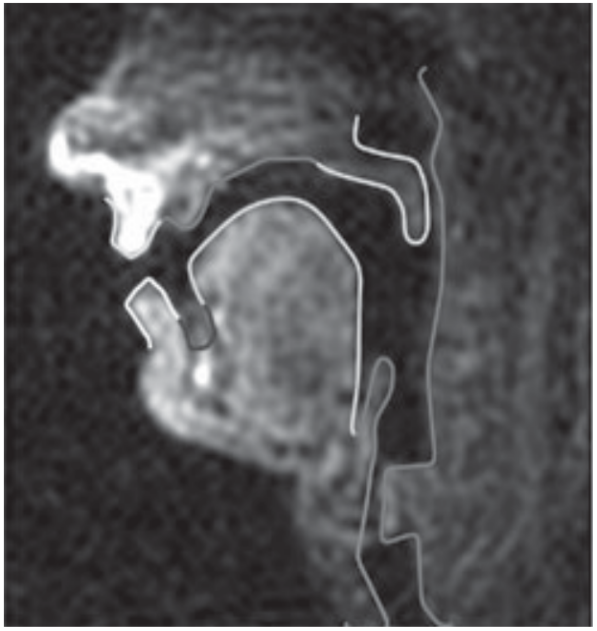


Figure: Vocal tract[a].

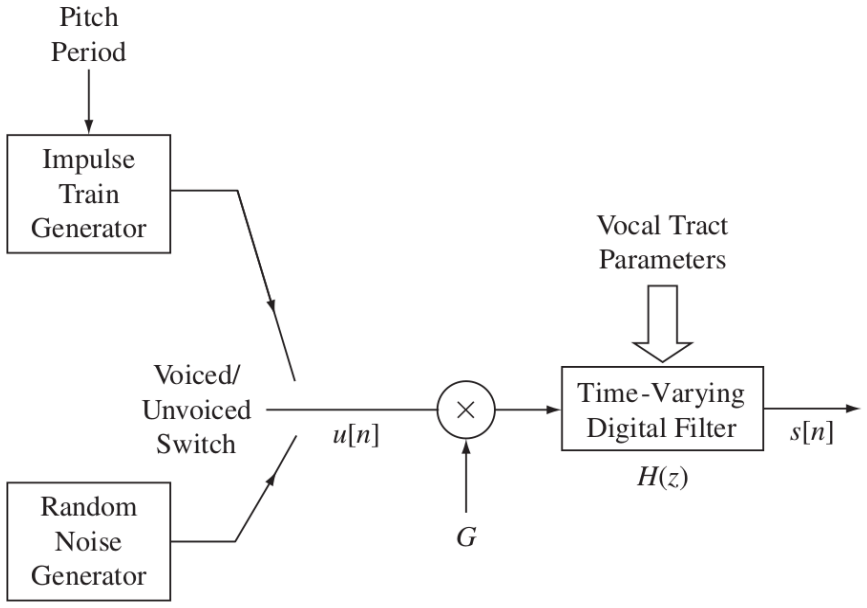


Figure: LPC synthetizer[a]

[a] Lawrence et al. *Theory and applications of digital speech processing*. 2011.

Multiharmonic signals over voice channels

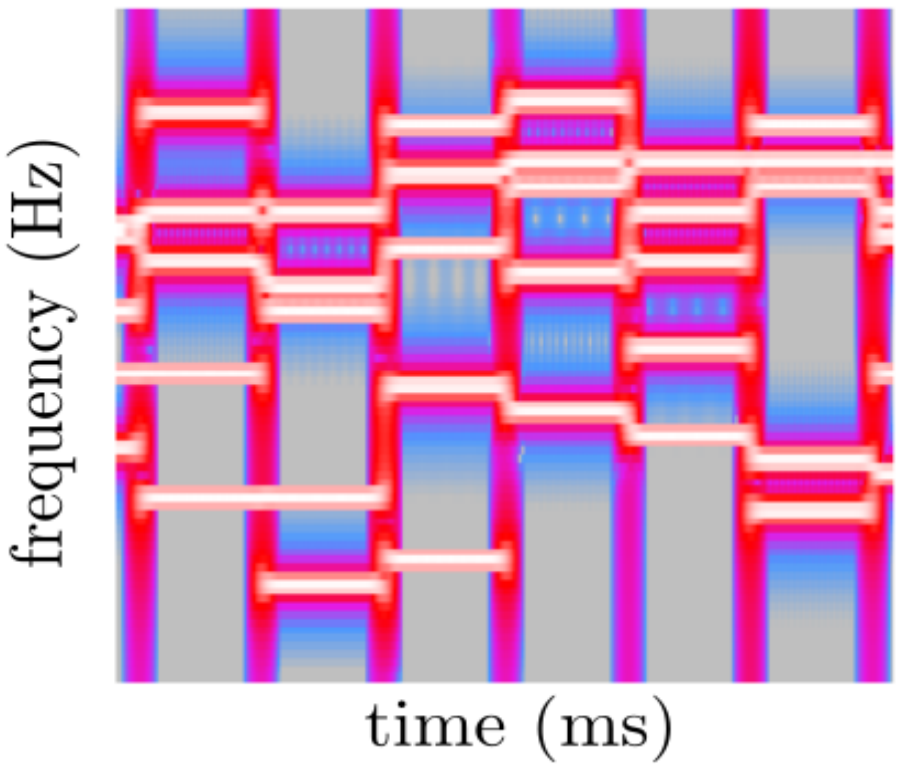


Figure: Multitone modulation.

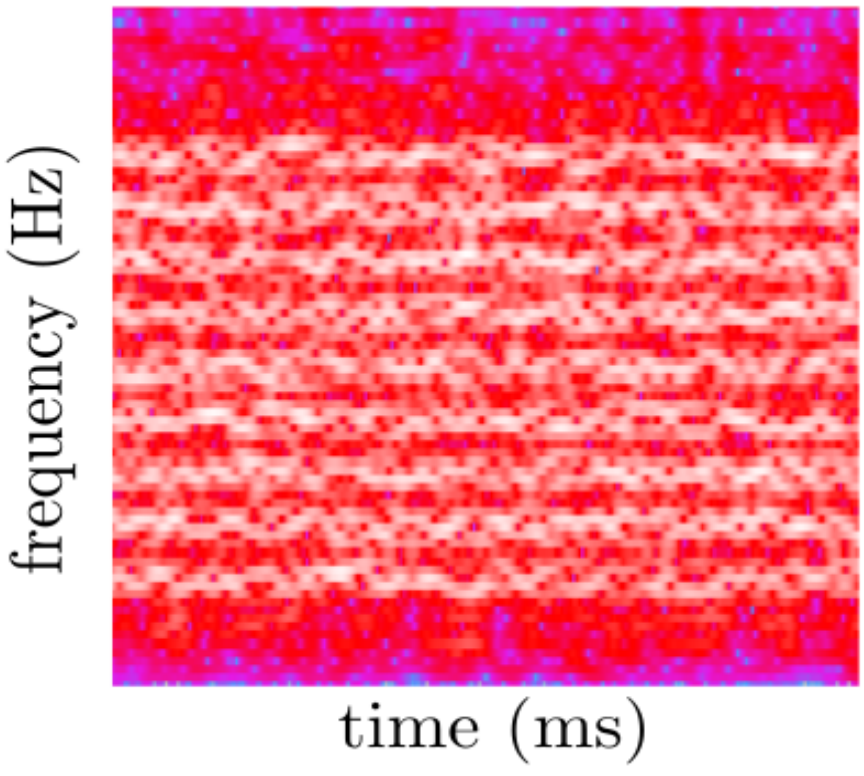
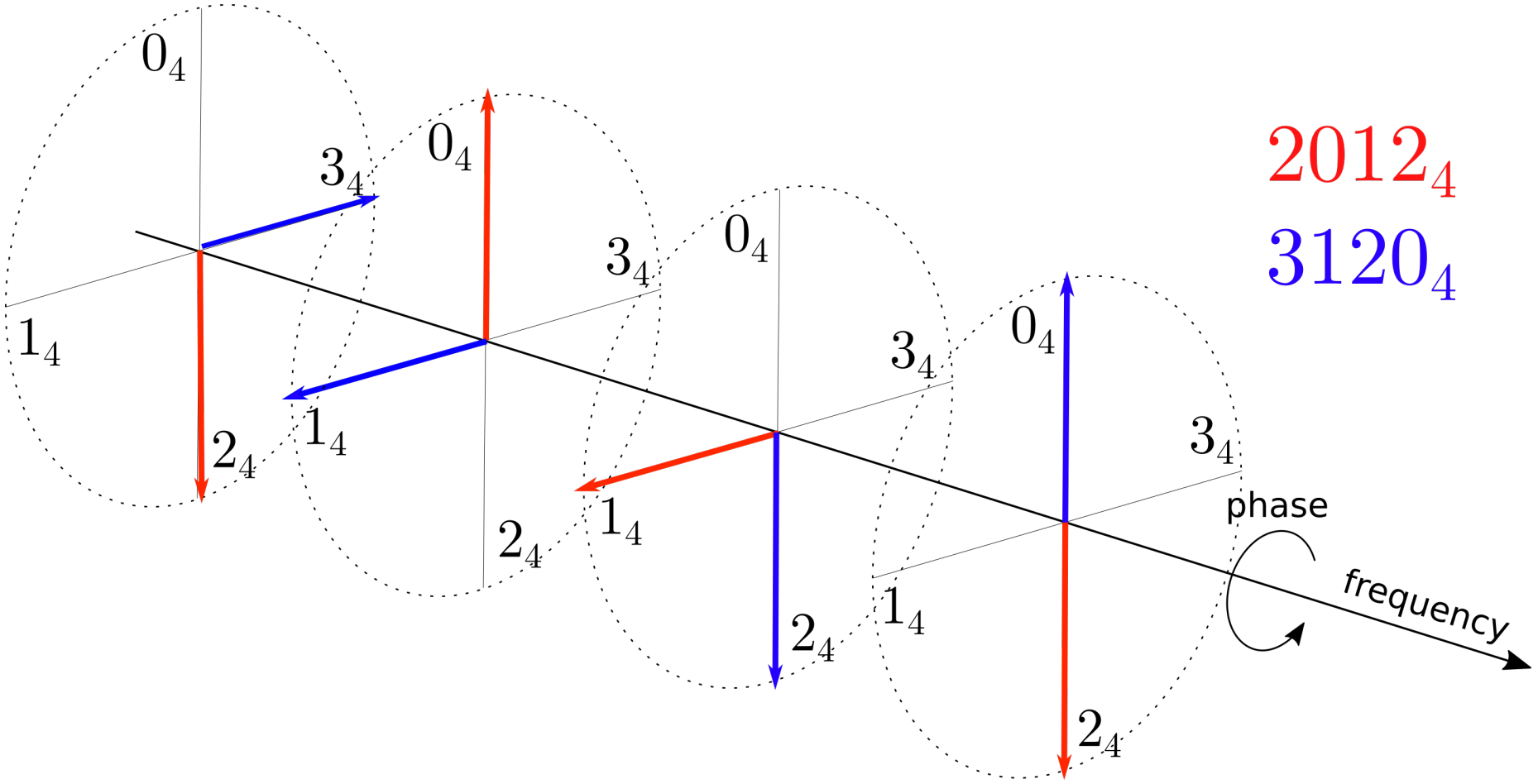


Figure: OFDM modulation.

OFDM and quaternary error correction codes



Performance of DoV

Application	Bitrate	Error rate
3G	1.6 - **3.2** kbps	$\approx 1\%$
Skype	3.2 - **6.4** kbps	$\approx 0.1\%$
WhatsApp	3.2 - **6.4** kbps	$\approx 0.1\%$
Signal	3.2 - **6.4** kbps	$\approx 0.1\%$

Enough to send voice in real time!

Codec2: 700 bps, 1200 bps, 1400 bps, 1600 bps
MELP: 300 bps, 600 bps, 1200 bps, 2400 bps

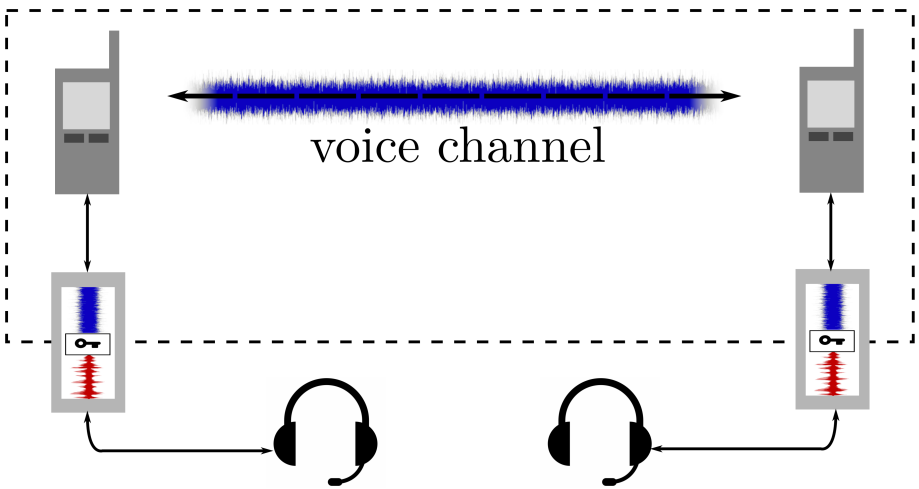
2. Key Exchange over voice channels

Challenges:

- **No Trusted Third Party**
- Small bandwidth and signal fading
- Half-duplex analog interfaces
- Large round-trip time $\sim 2s$

Requirements:

- **Strong authentication**
- Session Key secrecy
- Perfect Forward Secrecy
- Flexible and simple!



What the adversary can do?

Very likely:

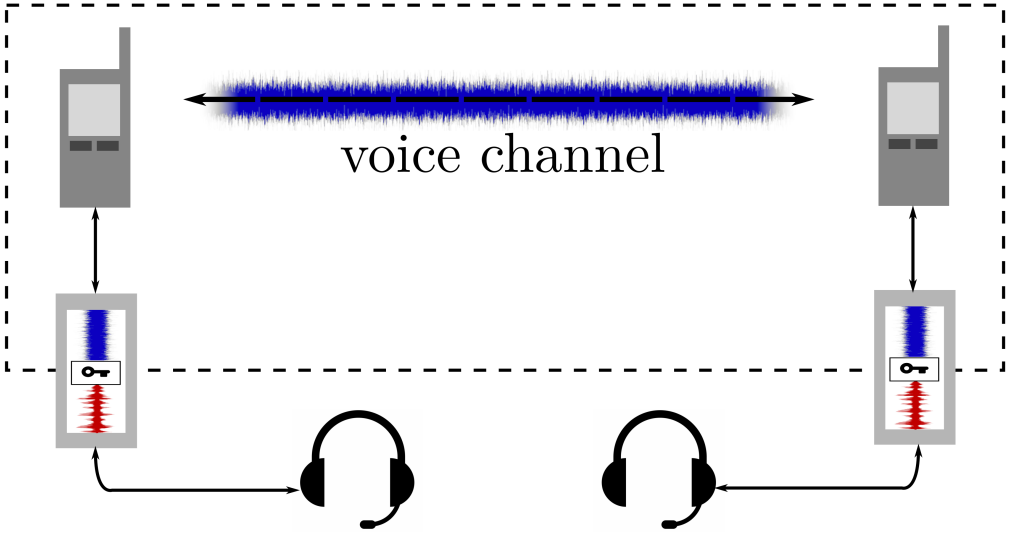
- Eavesdrop the traffic
- Distort the channel

Possibly:

- Replay messages
- Modify messages
- Perform **the MITM** attack
- Hijack the device

Assumption:

- Ephemeral values secure



ECDHE with Short Authentication Strings

Setup:	1 : **Alice**	$\xleftarrow[\text{negotiation}]{\text{A/B role}}$	**Bob**
	$N_A \leftarrow_\$ \mathbb{Z}^*_{32}$		$N_B \leftarrow_\$ \mathbb{Z}^*_{32}$
	$d_A \leftarrow_\$ \mathbb{Z}^*_{256}$		$d_B \leftarrow_\$ \mathbb{Z}^*_{256}$
	$Q_A = d_A G$		$Q_B = d_B G$
	$R_A \leftarrow_\$ \mathbb{Z}^*_{128}$		$R_B \leftarrow_\$ \mathbb{Z}^*_{32}$
Key Exchange:	2 :	$\xrightarrow[h_{128}(ID_A \Vert N_A \Vert Q_A \Vert R_A)]{ID_A,\ N_A,\ Q_A}$	
	3 : $Z = d_A Q_B$	$\xleftarrow{ID_B,\ N_B,\ Q_B,\ R_B}$	$Z = d_B Q_A$
	4 : $K_S = h_{256}(Z \Vert \bullet)$	$\xrightarrow{R_A}$	$K_S = h_{256}(Z \Vert \bullet)$
Acknowledgment:	5 :	$\xleftarrow{\text{ACK}}$	
Vocal Verification:	6 : $SAS = h_{32}(\blacklozenge)$	$\xleftrightarrow[\text{comparison}]{SAS \text{ vocal}}$	$SAS = h_{32}(\blacklozenge)$

$\blacklozenge \equiv R_A \Vert R_B \Vert ID_B \Vert Q_B \Vert N_B$

$\bullet \equiv ID_A \Vert N_A \Vert ID_B \Vert N_B$

ECDHE with Signature Authentication

Setup:	1 : **Alice**	$\xleftarrow[\text{negotiation}]{\text{A/B role}}$	**Bob**
	$N_A \leftarrow_{\$} \mathbb{Z}^*_{32}$		$N_B \leftarrow_{\$} \mathbb{Z}^*_{32}$
	$d_A \leftarrow_{\$} \mathbb{Z}^*_{256}$		$d_B \leftarrow_{\$} \mathbb{Z}^*_{256}$
	$Q_A = d_A G$		$Q_B = d_B G$
Key Exchange:	2 :	$\xrightarrow{ID_A,\ N_A,\ Q_A}$	
	3 : $Z = d_A Q_B$	$\xleftarrow[Sign_{S_B}(\text{'B'}\|\blacktriangle\|\blacktriangledown)]{ID_B,\ N_B,\ Q_B}$	$Z = d_B Q_A$
	4 : $K_S = h_{256}(Z\|\bullet)$	$\xrightarrow{Sign_{S_A}(\text{'A'}\|\blacktriangledown\|\blacktriangle)}$	$K_S = h_{256}(Z\|\bullet)$
Acknowledgment:	5 :	$\xleftarrow{\text{ACK}}$	

$\blacktriangle \equiv ID_A \| N_A \| Q_A$ $\quad \bullet \equiv ID_A \| N_A \| ID_B \| N_B$

$\blacktriangledown \equiv ID_B \| N_B \| Q_B$

ECDHE with Double Authentication

Setup:	1 : **Alice**	$\xleftarrow[\text{negotiation}]{\text{A/B role}}$	**Bob**
	$N_A \leftarrow_{\$} \mathbb{Z}^*_{32}$		$N_B \leftarrow_{\$} \mathbb{Z}^*_{32}$
	$d_A \leftarrow_{\$} \mathbb{Z}^*_{256}$		$d_B \leftarrow_{\$} \mathbb{Z}^*_{256}$
	$Q_A = d_A G$		$Q_B = d_B G$
	$R_A \leftarrow_{\$} \mathbb{Z}^*_{128}$		$R_B \leftarrow_{\$} \mathbb{Z}^*_{32}$
Key Exchange:	2 :	$\xrightarrow[h_{128}(ID_A \Vert N_A \Vert Q_A \Vert R_A)]{ID_A,\ N_A,\ Q_A}$	
	3 : $Z = d_A Q_B$	$\xleftarrow[Sign_{S_B}(\text{'B'} \Vert \blacktriangle \Vert \blacktriangledown)]{ID_B,\ N_B,\ Q_B,\ R_B}$	$Z = d_B Q_A$
	4 : $K_S = h_{256}(Z \Vert \bullet)$	$\xrightarrow[Sign_{S_A}(\text{'A'} \Vert \blacktriangledown \Vert \blacktriangle)]{R_A}$	$K_S = h_{256}(Z \Vert \bullet)$
Acknowledgment:	5 :	$\xleftarrow{\text{ACK}}$	
Vocal Verification:	6 : $SAS = h_{32}(\blacklozenge)$	$\xleftarrow[\text{comparison}]{SAS \text{ vocal}}$	$SAS = h_{32}(\blacklozenge)$

$\blacktriangle \equiv ID_A \Vert N_A \Vert Q_A$ $\quad$ $\bullet \equiv ID_A \Vert N_A \Vert ID_B \Vert N_B$

$\blacktriangledown \equiv ID_B \Vert N_B \Vert Q_B$ $\quad$ $\blacklozenge \equiv R_A \Vert R_B \Vert ID_B \Vert Q_B \Vert N_B$

Security verification

1. Are my ciphers secure?
2. **Is my protocol secure?**

   symbolic model verification
3. Is my implementation secure?

symbolic model analysis

Tamarin, ProVerif, AVISPA ...

Tamarin Prover

Running TAMARIN 1.4.1 | Index | Download | Actions » | Options »

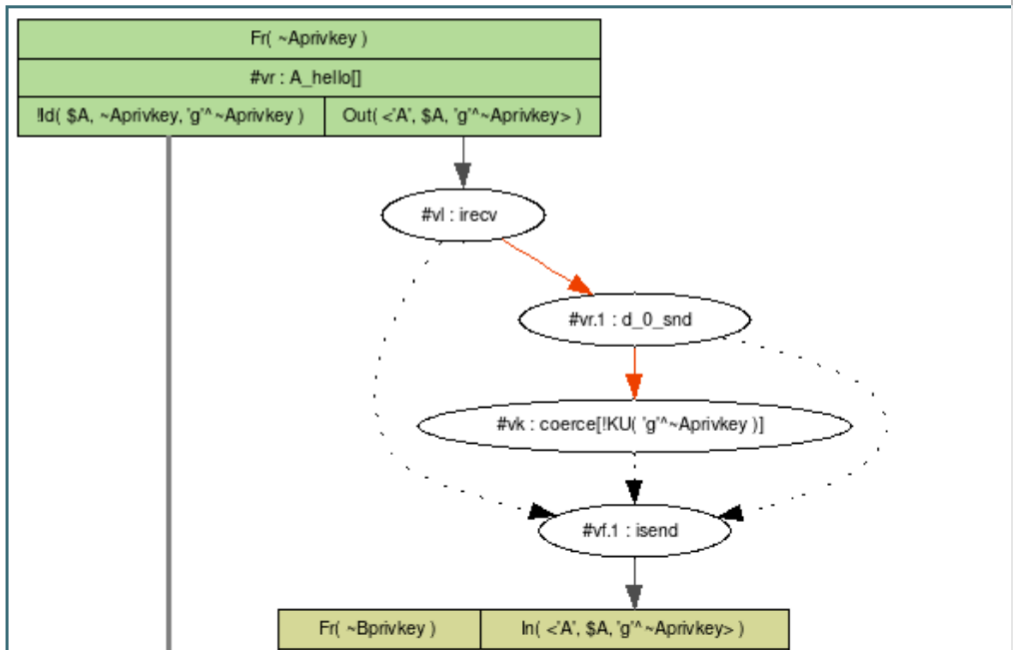
Proof scripts

```
theory Diffie_Hellman_Croatia begin

Message theory

Multiset rewriting rules (5)

Raw sources (5 cases, deconstructions complete)

Refined sources (5 cases, deconstructions complete)

lemma executable:
  exists-trace
  "∃ A B skey #i #j.
         ((SessionB( B, A, skey ) @ #i) ∧ (SessionA( A,
B, skey ) @ #j)) ∧
         (¬(A = B))"
simplify
solve( !Id( $A, ~Aprivkey, Apubkey.1 ) ▶₀ #j )
  case A_hello
  solve( splitEqs(0) )
    case split_case_1
    solve( splitEqs(1) )
      case split
      solve( !KU( Apubkey^(~Bprivkey*inv(~Aprivkey)) )
@ #vk.10 )
        case B_hello
        by solve( !KU( ~Aprivkey ) @ #vk.12 )
      next
        case c_exp
        by solve( !KU( ~Bprivkey ) @ #vk.12 )
      qed
```

Visualization display

Constraint System is Solved

Constraint system

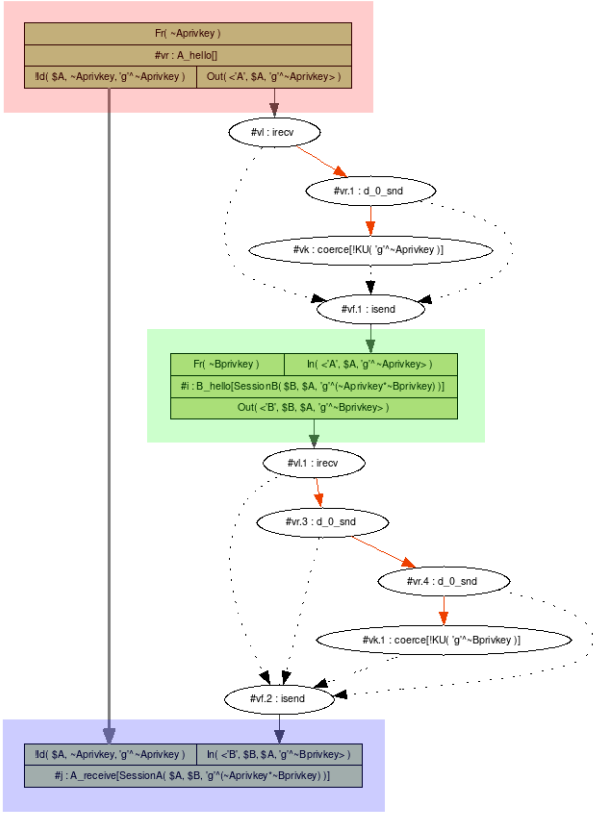


Tamarin Prover

Tamarin code:

```
theory Diffie_Hellman_Croatia
begin

builtins: diffie-hellman

rule A_hello:
    let
        Apubkey='g'^~Aprivkey
    in
    [Fr(~Aprivkey)]
    -->
    [!Id($A,~Aprivkey,Apubkey),
      Out(<'A',$A,Apubkey>)]

rule B_hello:
    let
        Bpubkey='g'^~Bprivkey
        skey=Apubkey^~Bprivkey
    in
    [ Fr(~Bprivkey),
      In(<'A',A,Apubkey>) ]
    --[SessionB($B,A,skey)]->
    [Out(<'B',$B,A,Bpubkey>)]

rule A_receive:
    let
        skey=Bpubkey^~Aprivkey
    in
    [ !Id($A,~Aprivkey,Apubkey),
       In(<'B',B,$A,Bpubkey>)]
    --[SessionA($A,B,skey)]->
    [ ]

lemma executable:
  exists-trace
  "Ex A B skey #i #j.
   SessionB(B,A,skey) @ i &
   SessionA(A,B,skey) @ j &
   not( A = B )"
end
```

Protocol diagram:



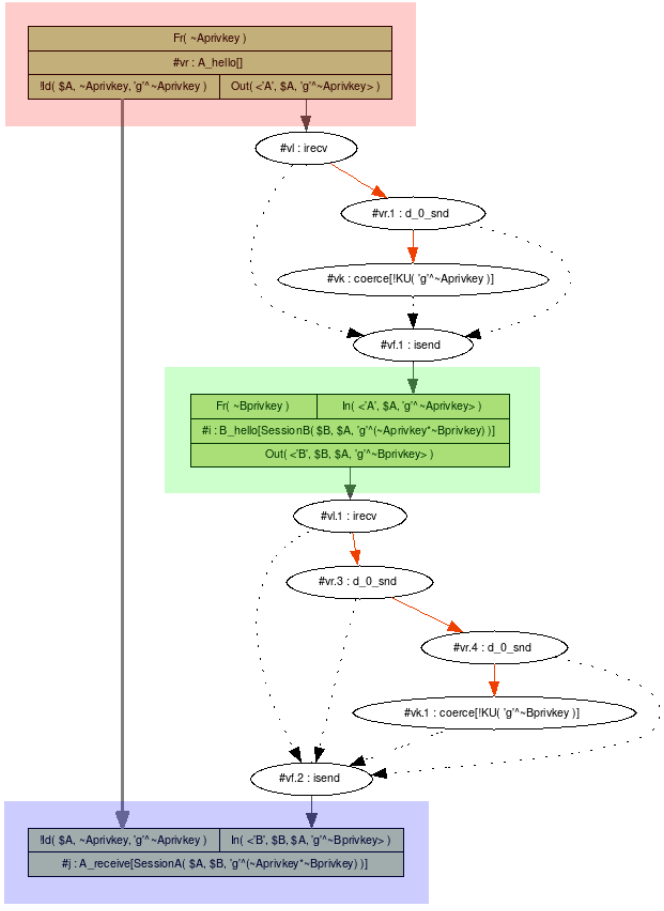
Lemma - example

lemma **secrecy:**

”**All** Alice Bob secret #i .
AliceSession(Alice, Bob, secret) @ i

==> /* implies */

Ex #j. BobSession(Bob, Alice, secret) @ j
& /* and */
/* adversary never knows the secret */
not(Ex #k. KU(secret) @ k)”

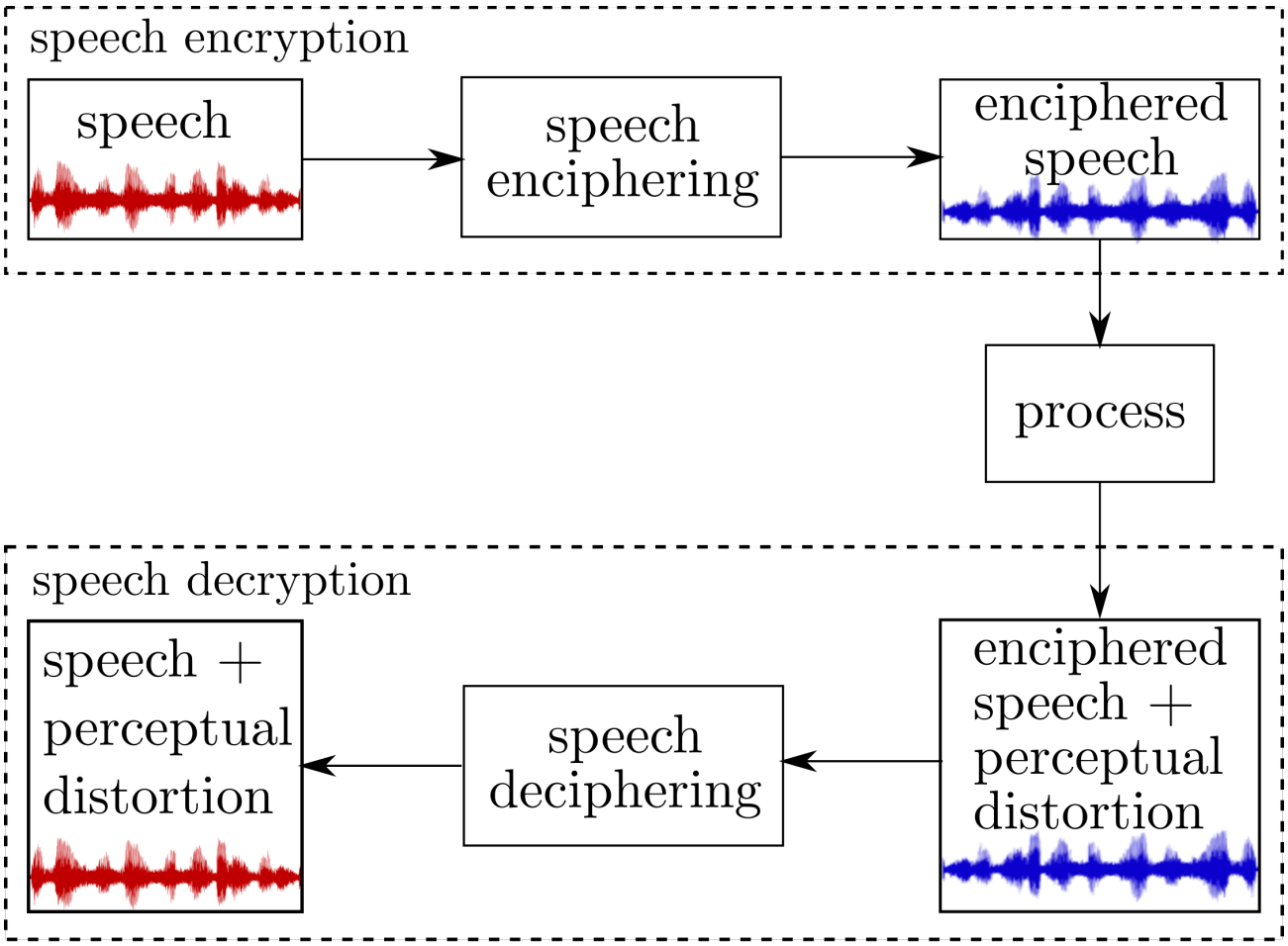


Security properties verified by Tamarin

Table: Security properties verified by Tamarin in four authentication scenarios.

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

3. Fully joint speech encryption over voice channels (in progress)



Distortion-tolerant speech encryption

Encryption properties:

- perceptually-oriented
- distortion-tolerant
- format-preserving
- **lossy**

Main challenges to solve:

1. what parameters to encrypt?
2. **how to encrypt?**
3. how to synthesize the signal?

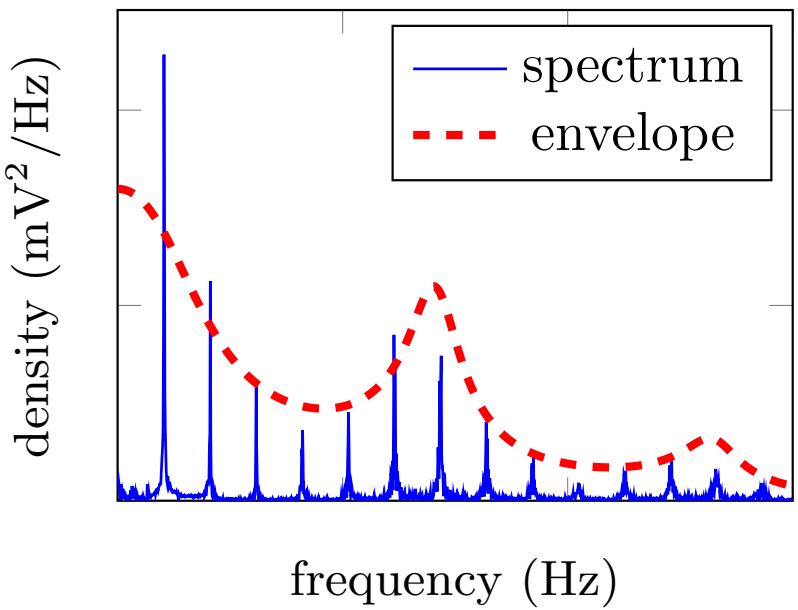
Towards a perceptually linear space of speech signals

Perceptual parameters of speech:

- loudness
- pitch
- timbre

Signal parameters:

- signal energy
- fundamental frequency
- $\approx$ spectral envelope



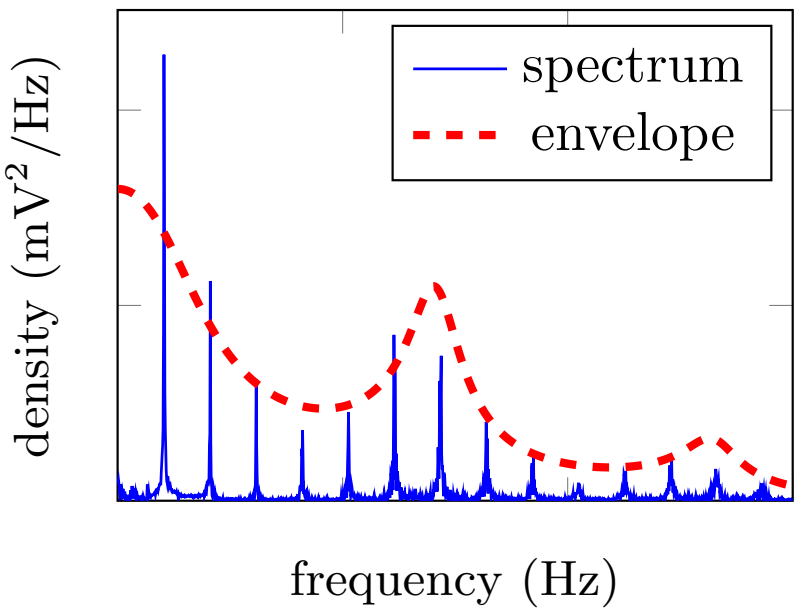
Towards a perceptually linear space of speech signals

Perceptual parameters of speech:

- loudness
- pitch
- timbre

Signal parameters:

- signal energy
- fundamental frequency
- $\approx$ spectral envelope

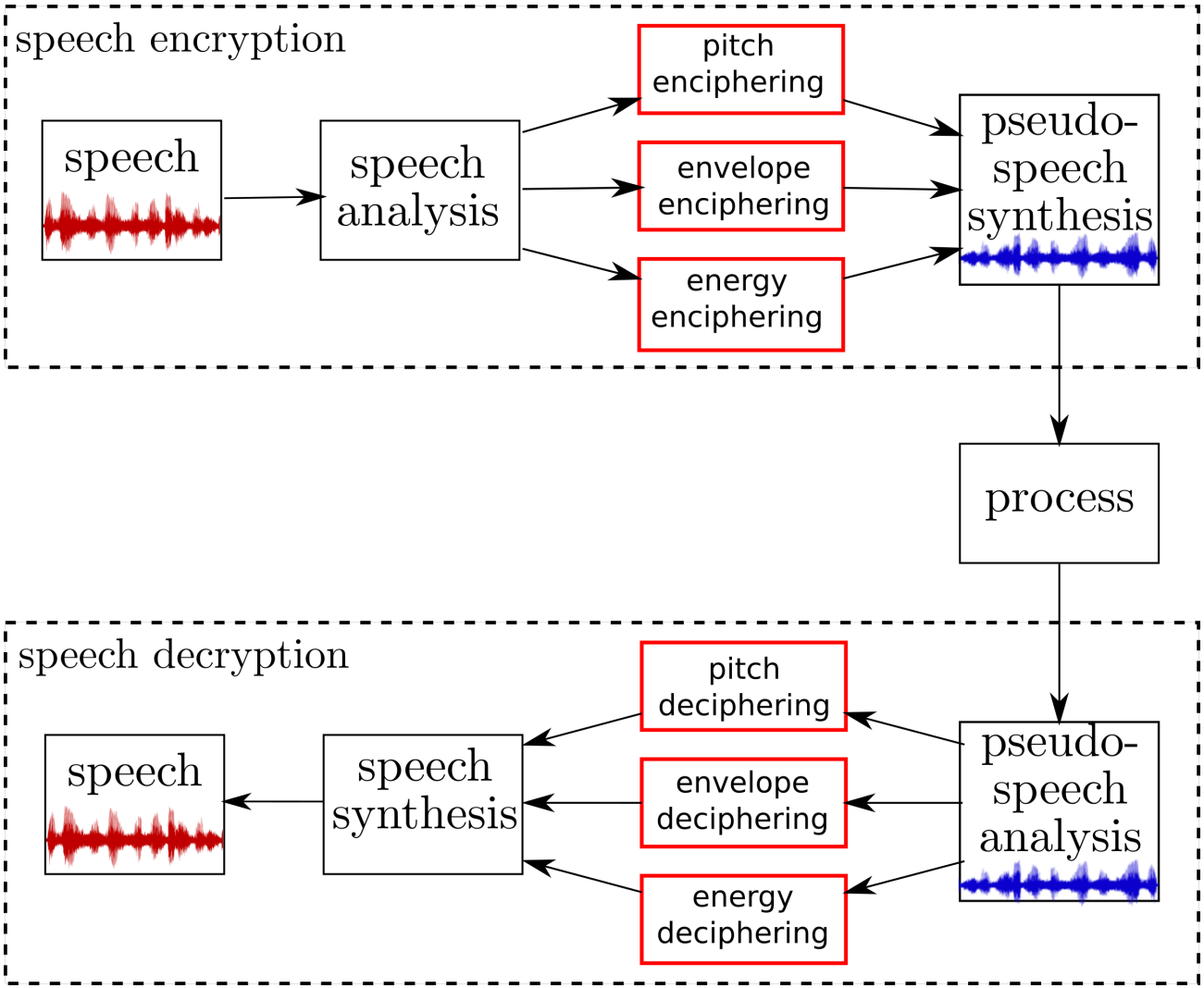


Perceptually (almost) linear representation:

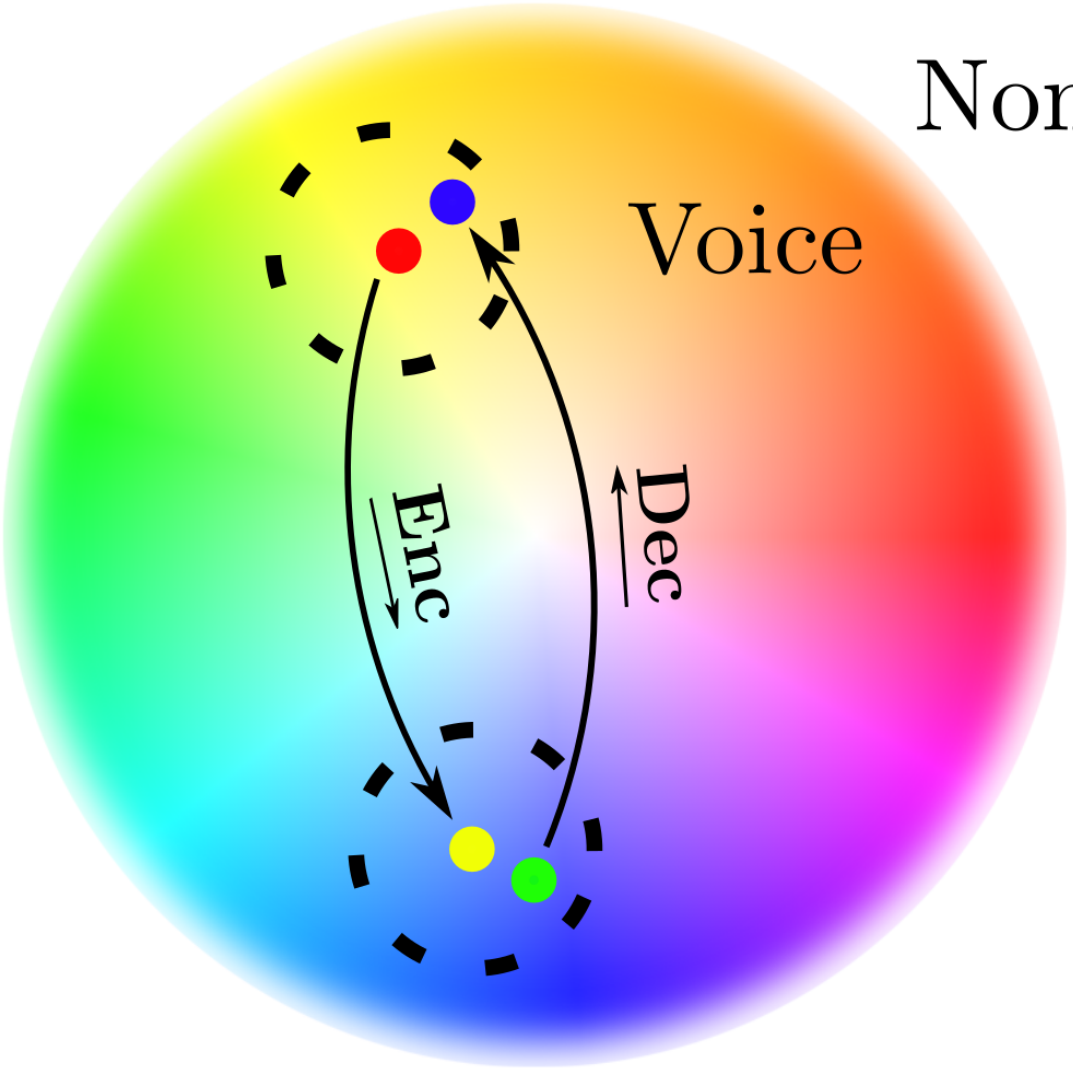
- logarithm of energy
- log. scaled fundamental freq.
- 10-13 MFCC coefficients

+ boundaries

Towards a distortion-tolerant encryption

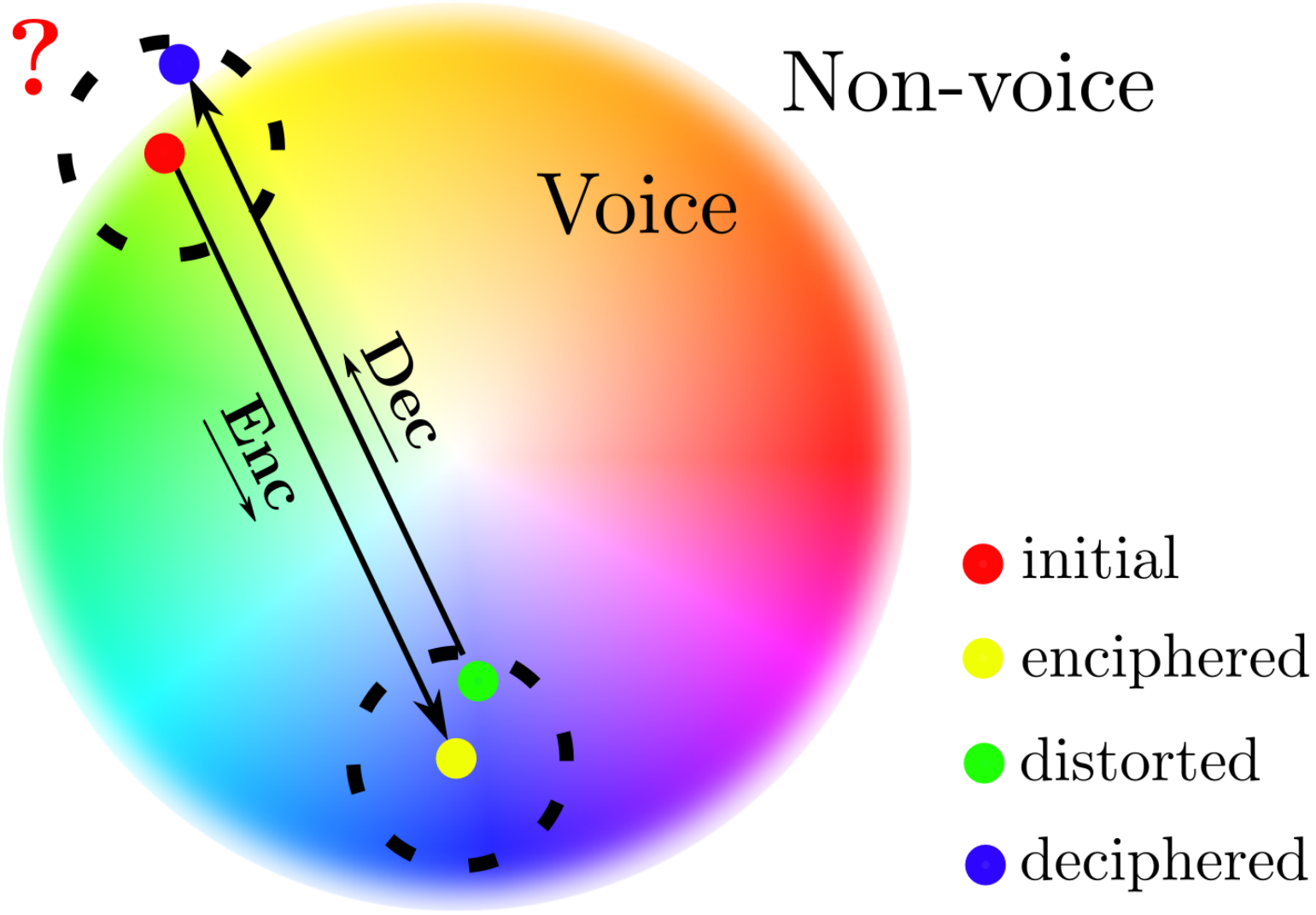


Towards a distortion-tolerant encryption



- initial
- enciphered
- distorted
- deciphered

Encryption by random translation



What next?

1. Improving the quality of synthesized speech.
   LPC-Net: A Real-Time Neural Vocoder (J.M. Valin, 2018)

2. Investigation into homomorphic encryption schemes.
   introducing more operations on encrypted speech
   homomorphic signal processing

3. Investigation into different speech representations.
   male-female-child, phonemic

Questions?