
CELLULAR
CRYPTO

End-to-End Voice Encryption over GSM:

A Different Approach

Wesley Tanner

Nick Lane-Smith

Keith Lareau

www.CellularCrypto.com

About Us:

Wesley Tanner

- Systems Engineer for a Software-Defined Radio (SDRF) company
- B.S. Electrical Engineering from RPI

Nick Lane-Smith

- Security Engineer for a computer company in Cupertino...
- B.S. Computer Science from UCSB

Keith Lareau (not present)

- B.S. Computer Science and Computer Systems Engineering from RPI

Presentation Overview

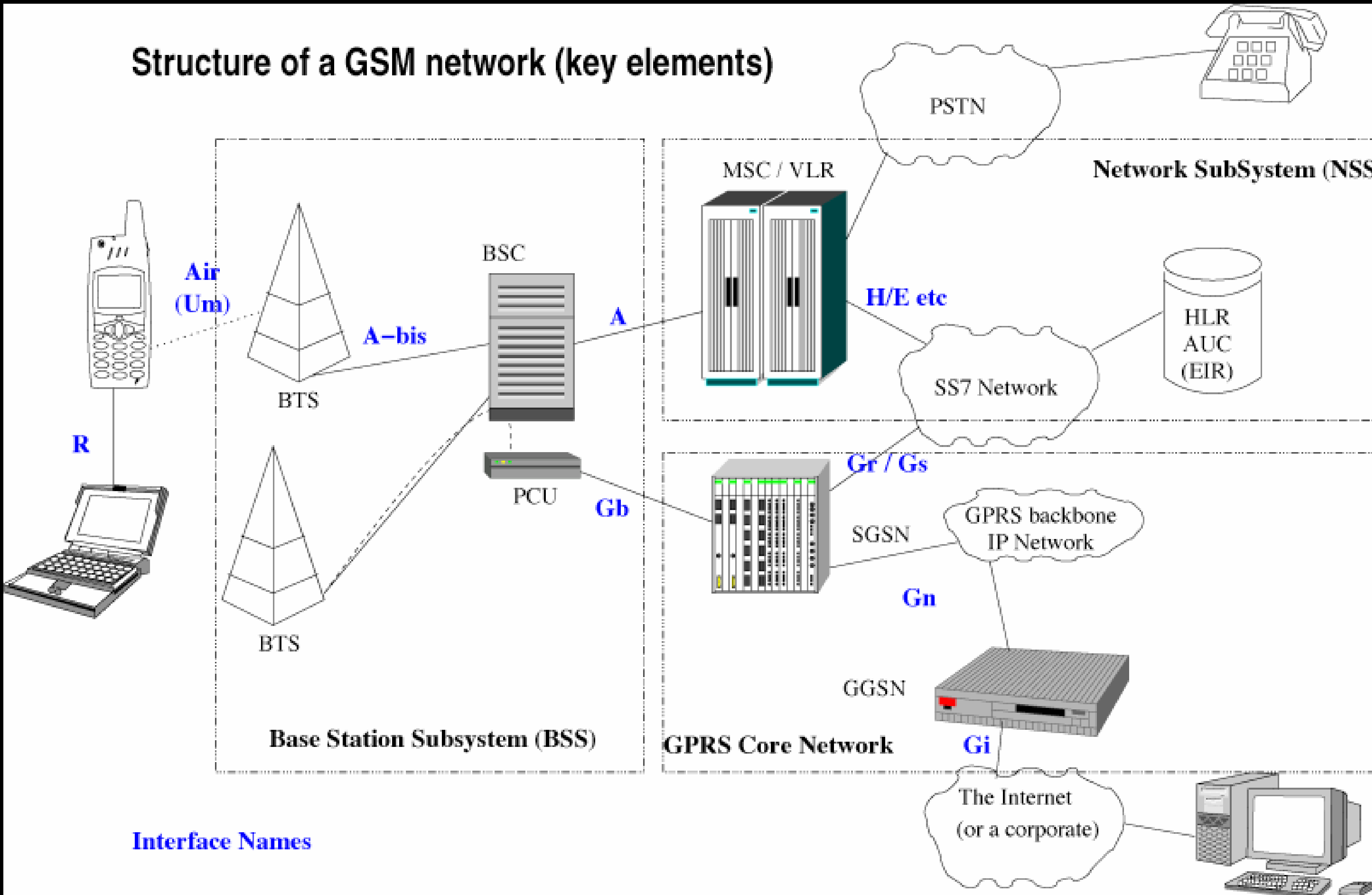
- Motivation, the need for Cellular Crypto
- Current market offerings
  - Operational details
- A new approach - GSM Voice Channel Modem
  - Details of the voice channel
  - Radio interface
  - Traditional PSTN modems over GSM
- Cryptographic Design
- Demonstrations

Motivation

Where is End-to-End voice protection over cellular?

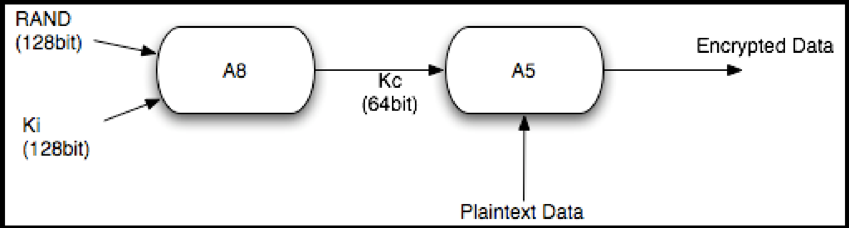
Why hasn't it become a reality for the average consumer?

GSM Overview



GSM Cryptography

- A3 - Authentication algorithm for the GSM security model
- A5 - The stream cipher used for voice-privacy
- A8 - Algorithm for voice-privacy key generation.



A5 weaknesses

Alex Biryukov, Adi Shamir and David Wagner demonstrated breaking a A5/1 key in less than a second on a PC with 128 MB RAM.

Elad Barkhan, Eli Biham and Nathan Keller have shown a ciphertext-only attack against A5/2.

Moral of the story…

GSM Cryptography provides limited, if any, true security to your voice channel. Something additional is needed.

The NEED for Cellular Crypto

- Cellular phones have almost completely supplanted PSTN.
- Cellular companies do not provide ANY meaningful protection for voice traffic.
- The ease of intercepting voice traffic is astounding…
- ***And people do it all the time!***

The NEED for Cellular Crypto

Two major classes of intercepts:

Government Perpetrated

- Authorized and Unauthorized
- Secret (FISA) and Reported
- Local, State and Federal
- Not just your own government

  - Large portions of Telecom infrastructure in the USA are owned by Foreign corporations, supported by Foreign and possibly adversarial governments. (Israel, China, etc.)

The NEED for Cellular Crypto

Two major classes of intercepts:

SecurTelecom.com

Non-government Perpetrated

- Private Investigators
- Business Partners
- Economic Espionage

CellularCrypto.com

The NEED for Cellular Crypto

Government Intercept

- Probably the most common
- Undetectable:
  - They don't waste time intercepting wireless transmission. CALEA Act allows to them execute intercept remotely via the telecom provider directly.
- "Untraceable" prepaid/disposable is no protection if you exhibit same calling pattern
- Presumably highest level (NRO, NSA ...) can perform voice match as well

The NEED for Cellular Crypto

Let's look at the data for reported intercepts

In 2004:

- 1,710 Authorized intercepts
- 1,507 Targeted "Portable device" (Cellular)

The NEED for Cellular Crypto

From U.S. Courts 2004 Wiretap Report:

Table 7
Authorized Intercepts Granted Pursuant to 18 U.S.C. 2519 as Reported in Wiretap Reports for Calendar Years 1994 - 2004

Wiretap Report Date	1994	1995	1996	1997	1998	1999	2000	2001	2002	2003	2004
Intercept applications requested	**1,154**	**1,058**	**1,150**	**1,186**	**1,331**	**1,350**	**1,190**	**1,491**	**1,359**	**1,442**	**1,710**
Intercept applications authorized	**1,154**	**1,058**	**1,149**	**1,186**	**1,329**	**1,350**	**1,190**	**1,491**	**1,358**	**1,442**	**1,710**
Federal	554	532	581	569	566	601	479	486	497	578	730
State	600	526	568	617	763	749	711	1,005	861	864	980
Avg. days of original authorization	29	29	28	28	28	27	28	27	29	29	28
Number of extensions	861	834	887	1,028	1,164	1,367	926	1,008	889	1,145	1,341
Average length of extensions (in days)	29	29	28	28	27	29	28	29	29	29	28
Location of authorized intercepts:											
Personal Residence	451	428	434	382	436	341	244	206	154	118	83
Business	118	101	101	78	87	59	56	60	37	35	30
Portable device	-	-	-	-	-	-	719	1,007	1,046	1,165	1,507
Multiple locations	97	115	149	197	222	287	109	117	85	95	65
Not indicated or other*	488	414	465	529	584	663	62	101	36	29	25

The NEED for Cellular Crypto

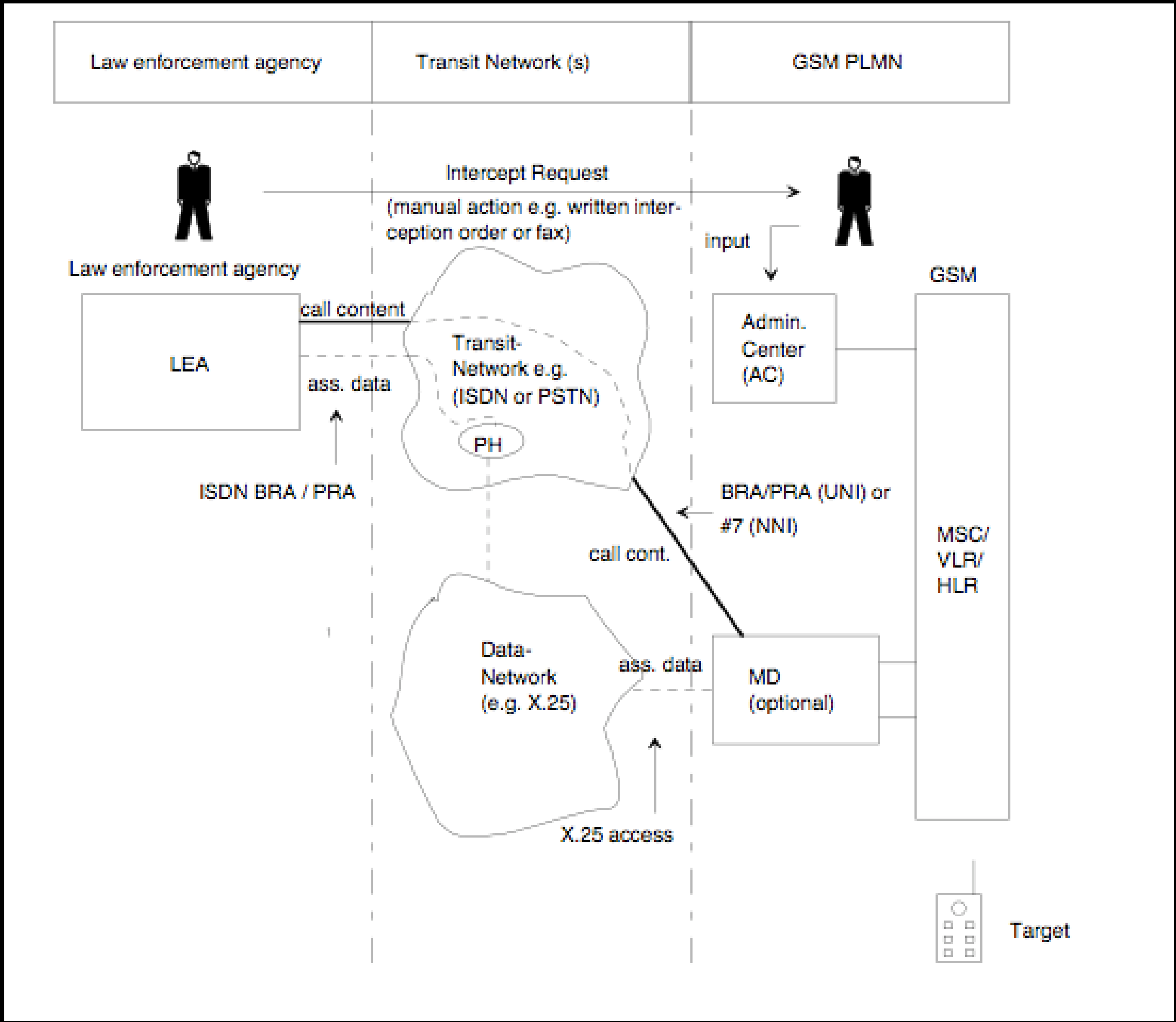
Cellular intercepts have doubled since 2000, the trend appears to suggest that the ease of intercepts is the reason behind growth.

Of note, there is no jump after Sept. 11th, which implies FISA intercepts are used for intercepts relating to terrorism. The overall number of intercepts is most likely orders of magnitude greater.

The **NEED** for Cellular Crypto

- GSM Spec TS 33.106
- Interception function should not alter the target's service or provide indication to any party involved.
- Output 'Product' and/or 'Network related data'
- Network related data - location, type of call, all party's numbers.
- Product - speech, user data, fax or SMS.

Diagram of a Lawful Intercept



Moral of the story…2

Even if the GSM crypto sufficiently protected the handset->tower, network transit layers are capable of being intercepted.

Only End-to-End crypto can provide sufficient security.

Current Market Offerings

Various GSM Crypto products:

- –Cryptophone G10
- –Sectera by General Dynamics (govt. contract)
- –Ancort Crypto Smart Phone
- –Several “vapor” products

Future Narrowband Digital Terminal

- FNBDT is a new US govt. standard for secure voice communication
- Needs minimum bandwidth of 2400 Hz.
- Replacement for STU-III
- Uses MELP for voice compression.

Problems with Current Products

They all use the GSM circuit switched data (CSD) channel

- This service is not part of the normal consumer-level package in all places.
- CSD is quickly being replaced by packet switched services, which do not have the necessary performance (currently) for a quality voice link.
- Long call setup times
- High latency, but not as bad as GPRS

Problems with Current Products

- CSD is meant to carry data, not voice. Voice can tolerate more transmission errors and does not require ARQ.

- High latency and retransmission rather than dropping a frame make data channel insufficient for voice.

Problems with Current Products

Some are only available for government or government contractor use, or are very expensive.

The solution needs to be available to everyone.

So, what then? Give up?

Wait for 3G? Will 3G even be sufficient?

Proposed Solution

Develop a modem that works over the GSM voice channel.

- Latency optimized
- Frame dropping

A fun and challenging technical problem to solve is a side benefit.

Technical Details of the GSM Voice Channel

The GSM Voice Channel

The voice channel has lots of useful properties

- Low latency
- High availability
- Friendly billing system from service providers. Use your standard voice minutes instead of possibly more expensive data packages.

However, the voice channel is forgiving only for speech-like waveforms.

GSM Voice Channel Data Rate Calculation

Description	Parameter	Parameter Number	Number of bits
	LAR 1	1	6
	LAR 2	2	6
	LAR 3	3	5
	LAR 4	4	5
	LAR 5	5	4
	LAR 6	6	4
Filter	LAR 7	7	3
Parameters	LAR 8	8	3
	LTP Lag	9	7
LTP Parameters	LTP gain	10	2
	RPE grid position	11	2
	Block amplitude	12	6
	RPE pulse 1	13	3
	RPE pulse 2	14	3
	RPE pulse 3	15	3
	RPE pulse 4	16	3
	RPE pulse 5	17	3
	RPE pulse 6	18	3
	RPE pulse 7	19	3
	RPE pulse 8	20	3
	RPE pulse 9	21	3
	RPE pulse 10	22	3
	RPE pulse 11	23	3
	RPE pulse 12	24	3
RPE Parameters	RPE pulse 13	25	3
	LTP Lag	26	7
LTP Parameters	LTP gain	27	2
	RPE grid position	28	2
	Block amplitude	29	6
	RPE pulse 1	30	3
	RPE pulse 2	31	3
	RPE pulse 3	32	3
	RPE pulse 4	33	3
	RPE pulse 5	34	3
	RPE pulse 6	35	3
	RPE pulse 7	36	3
	RPE pulse 8	37	3
	RPE pulse 9	38	3
	RPE pulse 10	39	3
	RPE pulse 11	40	3
	RPE pulse 12	41	3
RPE Parameters	RPE pulse 13	42	3

Description	Parameter	Parameter number	Number of bits
	LTP Lag	43	7
LTP Parameters	LTP gain	44	2
	RPE grid positio	45	2
	Block amplitud	46	6
	RPE pulse 1	47	3
	RPE pulse 2	48	3
	RPE pulse 3	49	3
	RPE pulse 4	50	3
	RPE pulse 5	51	3
	RPE pulse 6	52	3
	RPE pulse 7	53	3
	RPE pulse 8	54	3
	RPE pulse 9	55	3
	RPE pulse 10	56	3
	RPE pulse 11	57	3
	RPE pulse 12	58	3
RPE Parameters	RPE pulse 13	59	3
	LTP Lag	60	7
LTP Parameters	LTP gain	61	2
	RPE grid positio	62	2
	Block amplitud	63	6
	RPE pulse 1	64	3
	RPE pulse 2	65	3
	RPE pulse 3	66	3
	RPE pulse 4	67	3
	RPE pulse 5	68	3
	RPE pulse 6	69	3
	RPE pulse 7	70	3
	RPE pulse 8	71	3
	RPE pulse 9	72	3
	RPE pulse 10	73	3
	RPE pulse 11	74	3
	RPE pulse 12	75	3
RPE Parameters	RPE pulse 13	76	3

Total Bits	**260**
Frame rate (fps)	**50**
Data rate (kbps)	**13**

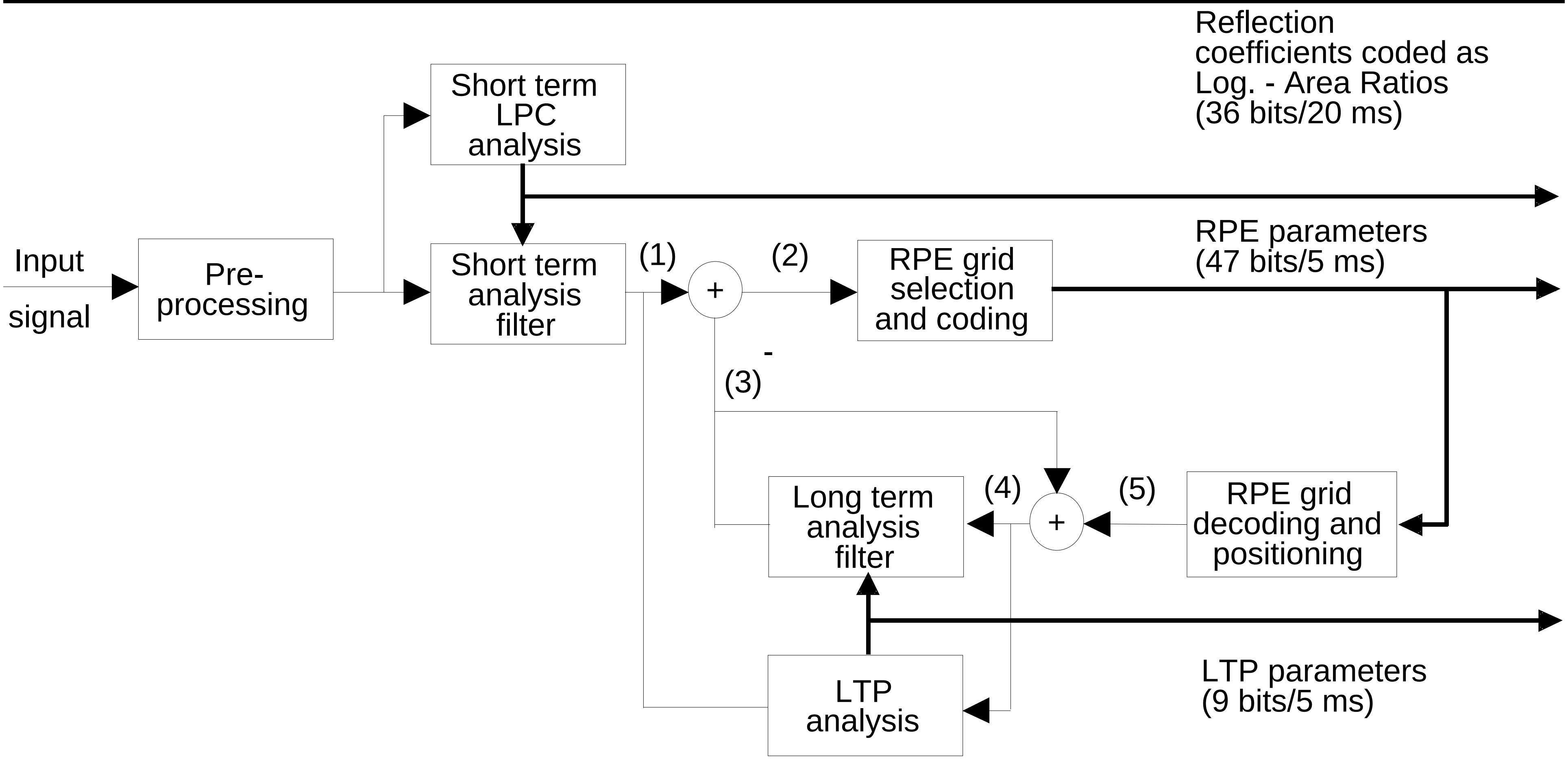
Full Rate Channel Properties

Parameter	Input	Output
bits per frame	2080	260
frames per second	50	50
data rate (kbps)	104000	13000
Compression ratio	**8**	

Full Rate Channel Properties

- Regular Pulse Excitation - Long Term prediction - Linear Predictive Coder
- 260 bits per frame
- Bandwidth of 13 kbps
- Input is 160, 13 bit uniform quantized PCM samples
  - 8 kHz sampling rate

Encoder Block Diagram



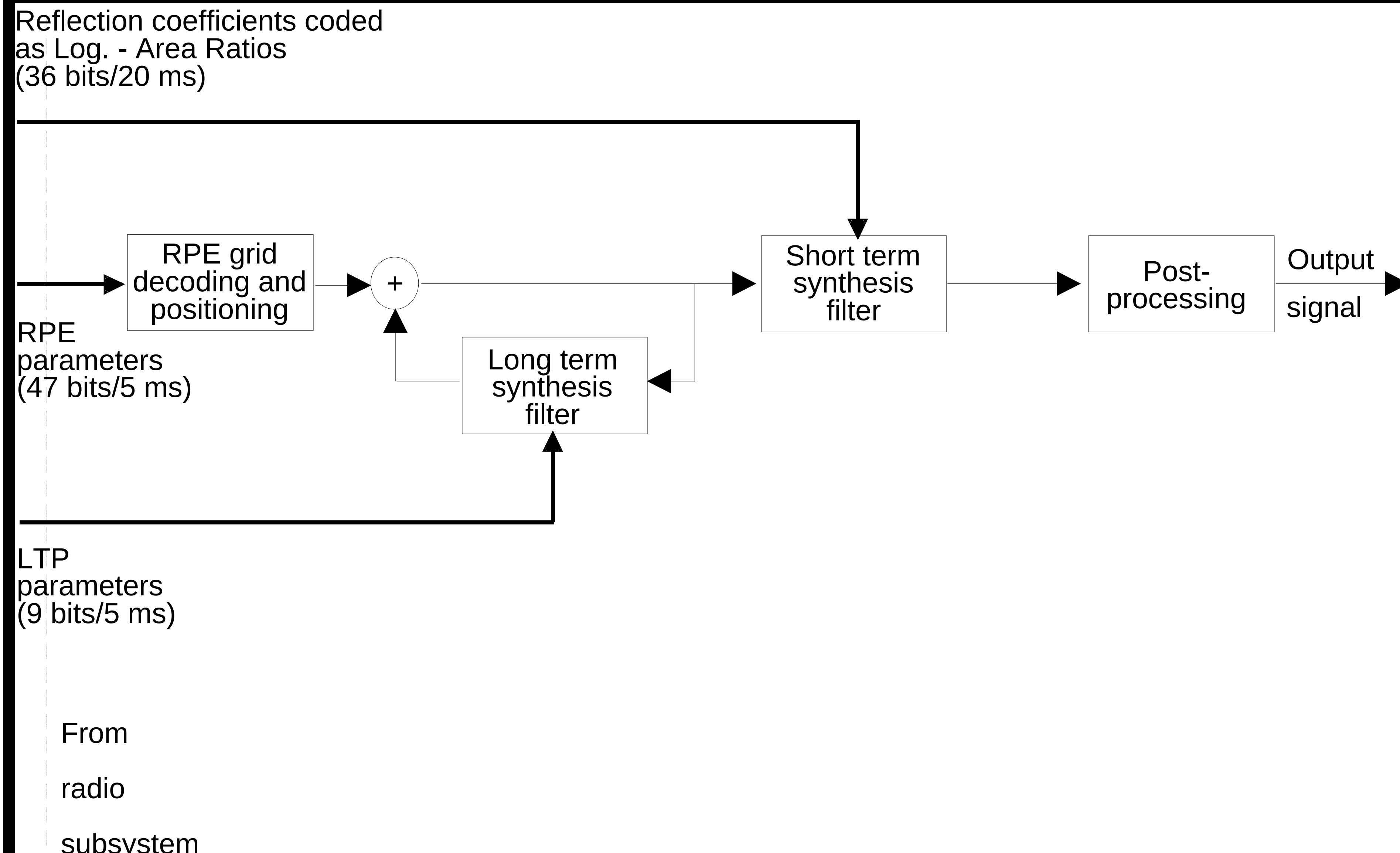
(1) Short term residual
(2) Long term residual (40 samples)
(3) Short term residual estimate (40 samples)
(4) Reconstructed short term residual (40 samples)
(5) Quantized long term residual (40 samples)

To

radio

subsystem

Decoder Block Diagram



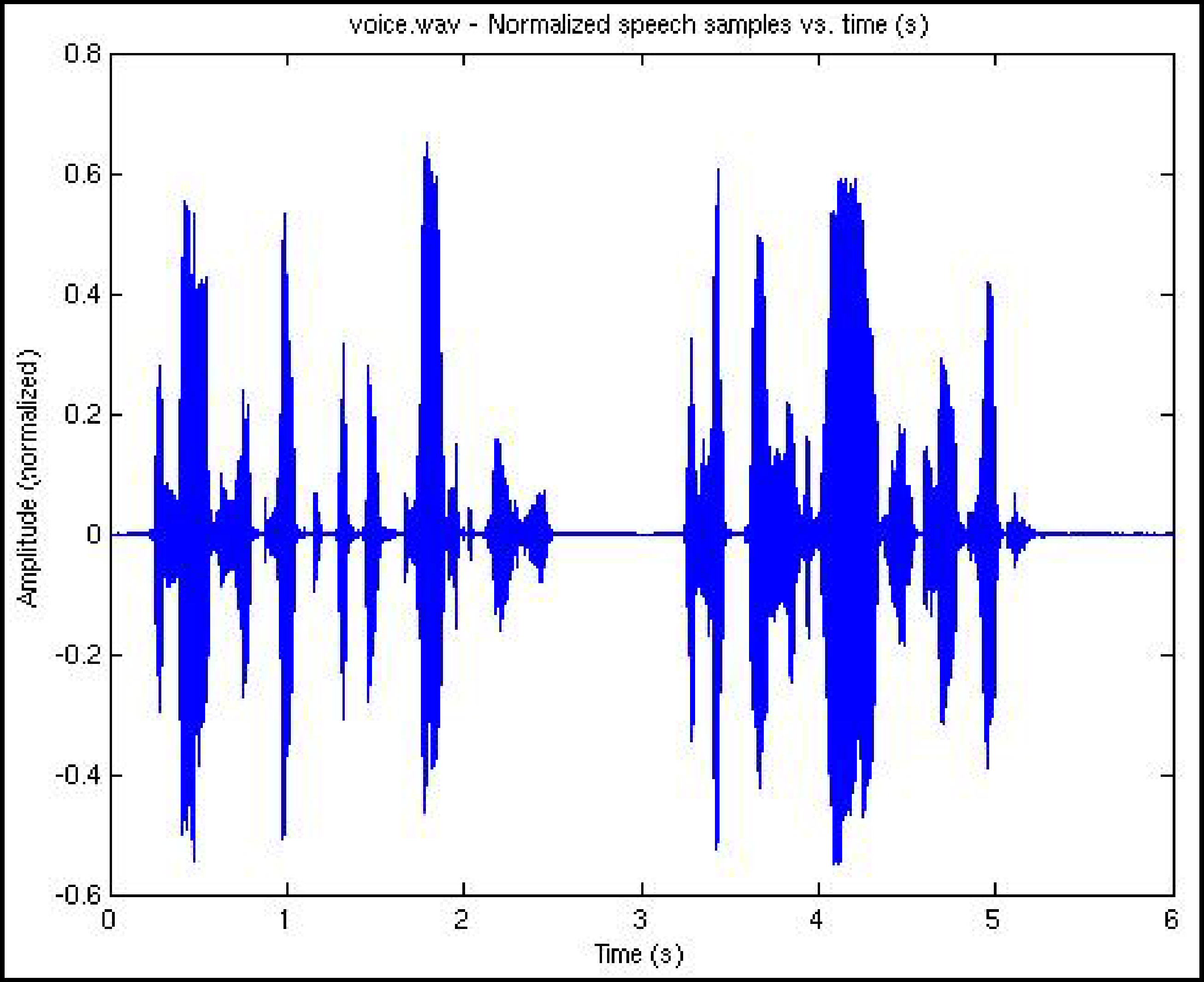
Voice packet structure

- Some bits are protected for transmission over radio
  - Class A bits CRC protected
  - Class B/C bits sent uncoded
- Class A bits are most important for intelligible voice.
- RFC 3267
  - Real-Time Transport Protocol (RTP) Payload Format and File Storage Format for the Adaptive Multi-Rate (AMR) and Adaptive Multi-Rate Wideband (AMR-WB) Audio Codecs

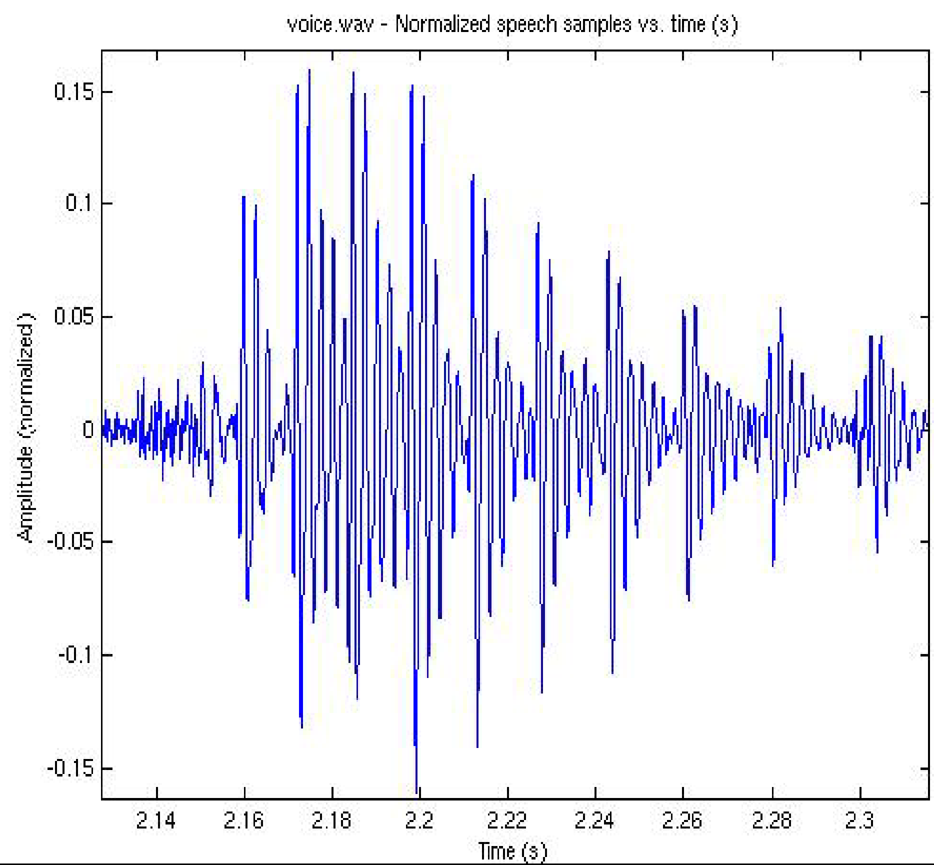
Properties of Speech (as related to GSM full rate codec)

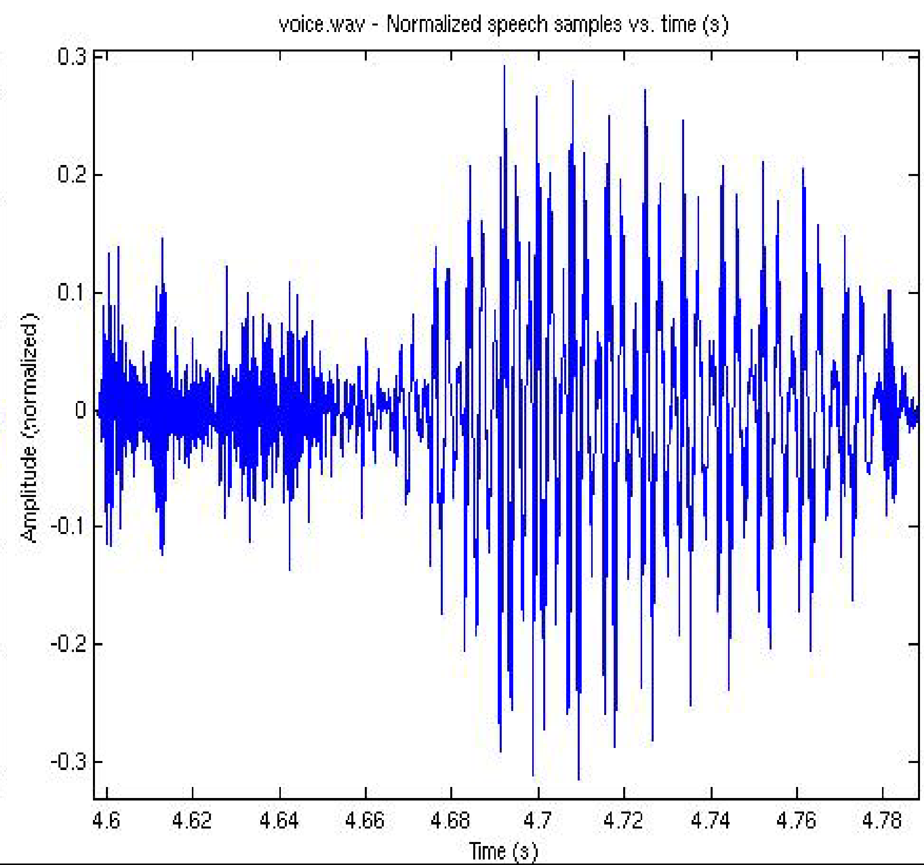
- **Short term parameters**
  - LPC
- **Long term prediction, computed based on the output of the short term filtering**
  - Lag
  - Gain
- **Residual information**
  - Calculated by the error in the estimated residual signal from the actual residual signal

Voice Samples - 8 kHz sample rate



Close-up Voice Samples





Telephone Modem Modulation

Name	Receive rate (bps)	Transmit rate (bps)	Symbol rate (baud)	Modulation Type	Transmit carrier frequencies (Hz)	Receive carrier frequencies (Hz)
Bell 103	300	300	300	FSK	1270/1070	2225/2025
CCITT V.22	1200	1200	600	DPSK	1200	2400
CCITT V.32	4800	4800	2400	QAM	1800	1800
ITU V.34	33600	33600	3429	TCM	1800	1800
ITU V.92	53000	48000	8000	PCM	N/A	N/A

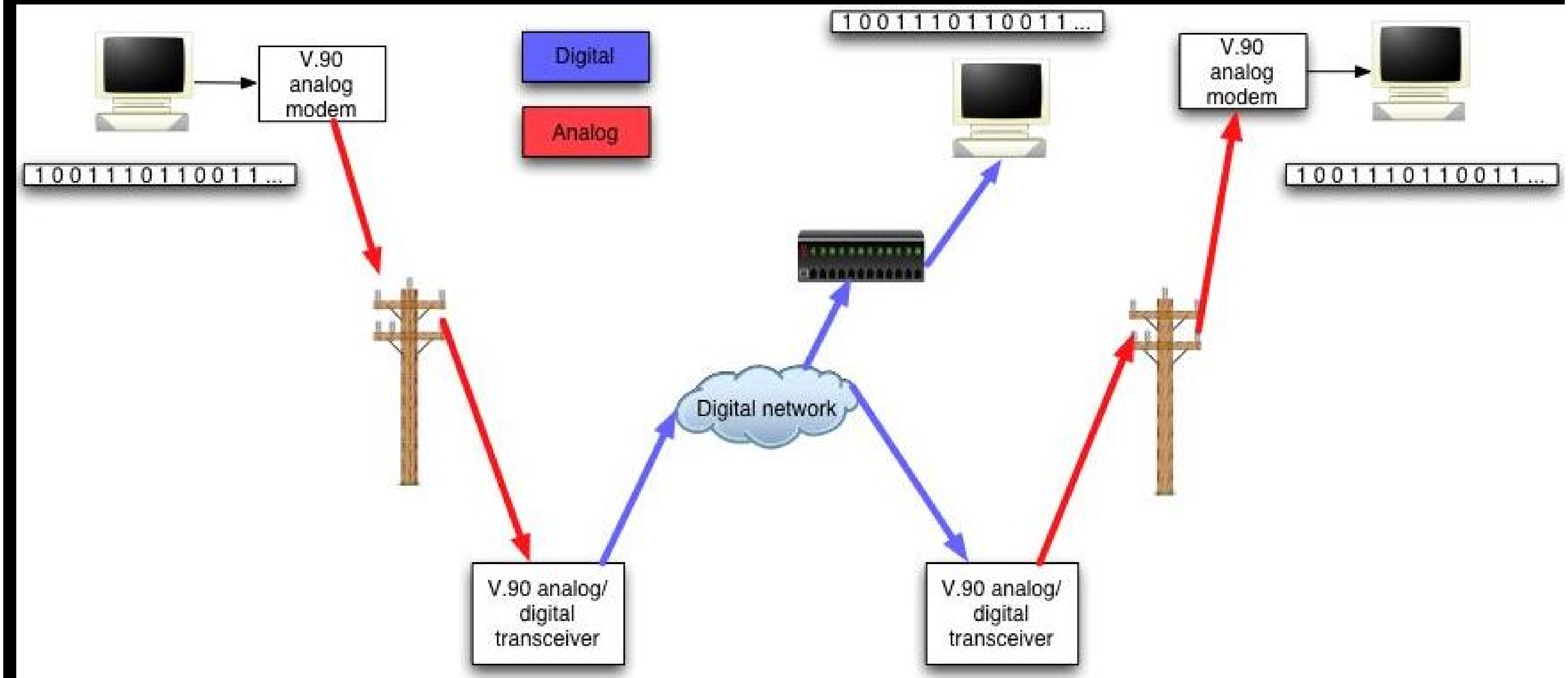
56 kbps Modem Description

- V.90 uses PCM (pulse coded modulation)
- Bits are sent from the transmitting modem over the digital telephone network to a receiving modem at the telco office.
- Converted to analog voltage levels that are sent over the analog wire to your modem.

56 kbps Modem Description

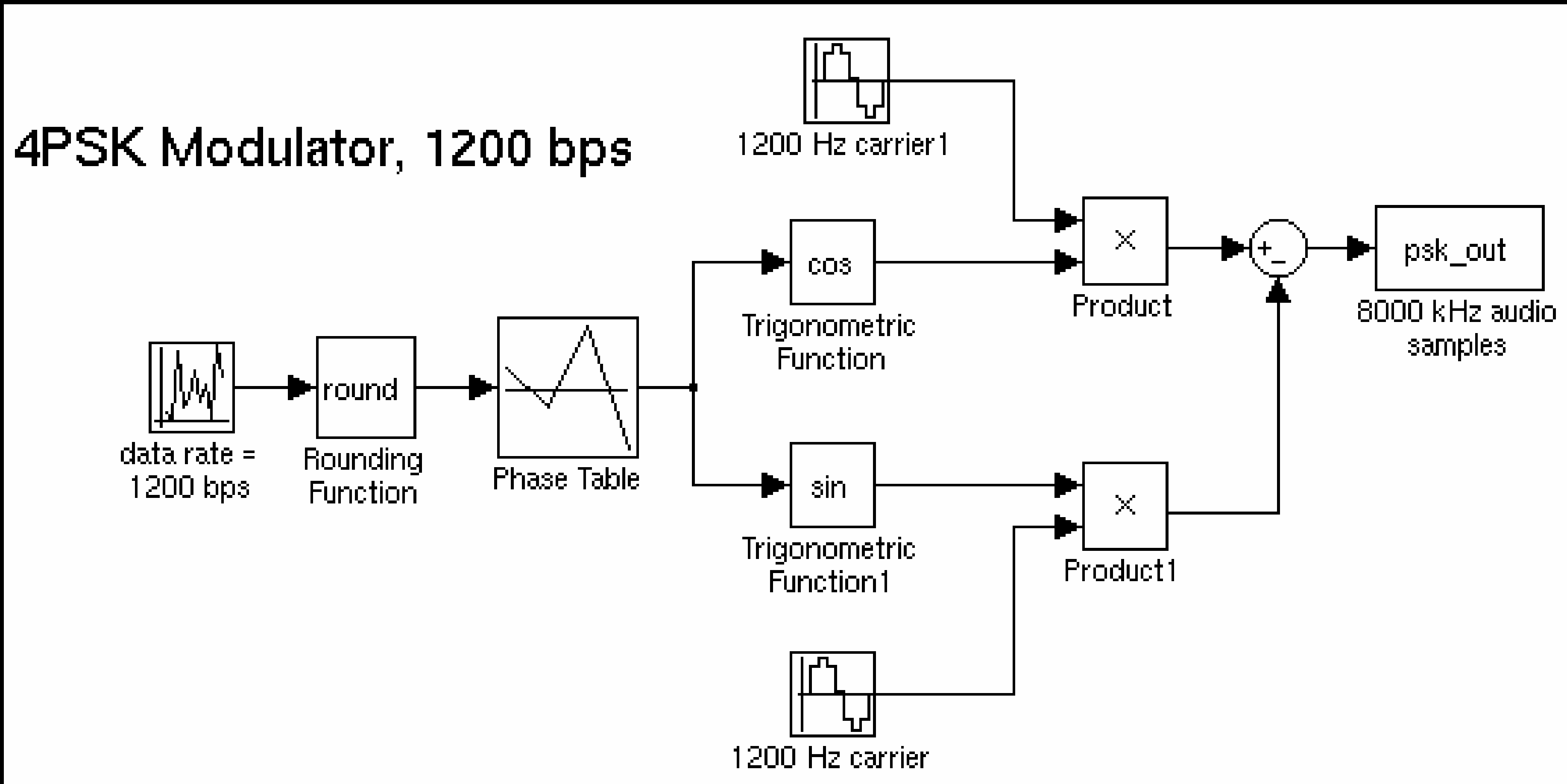
- Voltages held on the line for 125 microseconds (8000 per second).
- 8 bits per pulse equals 64 kbps
  - North American networks use 7 bits = 56 kbps
- This is the theoretical rate, but is limited by the connection.

V.90 Modem Connection



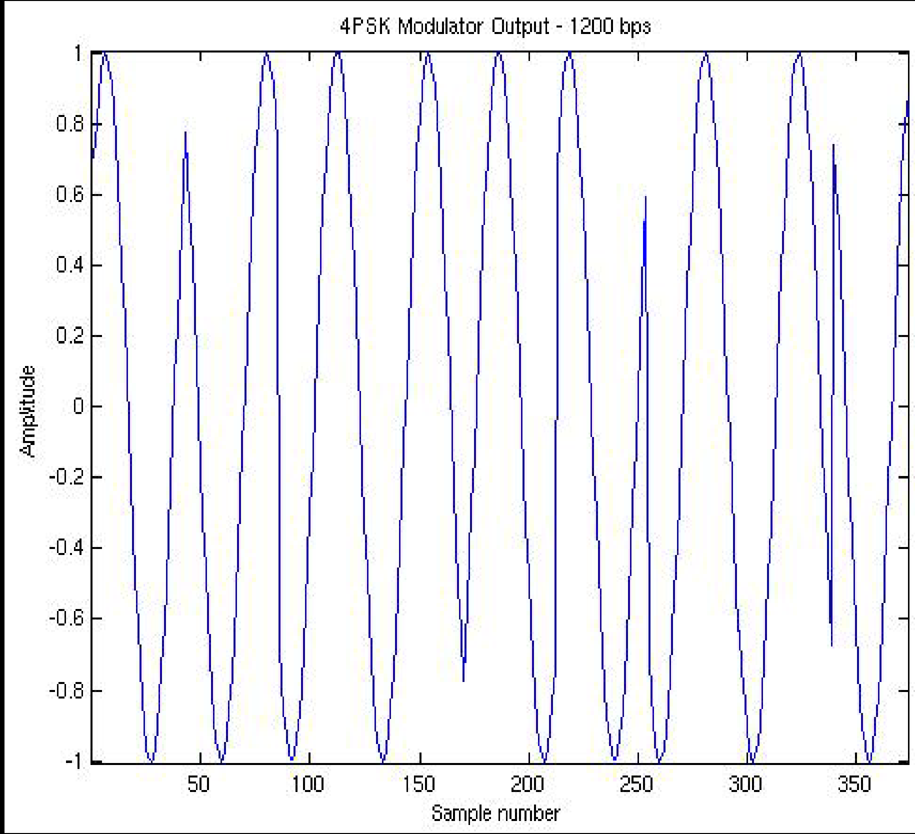
CellularCrypto.com

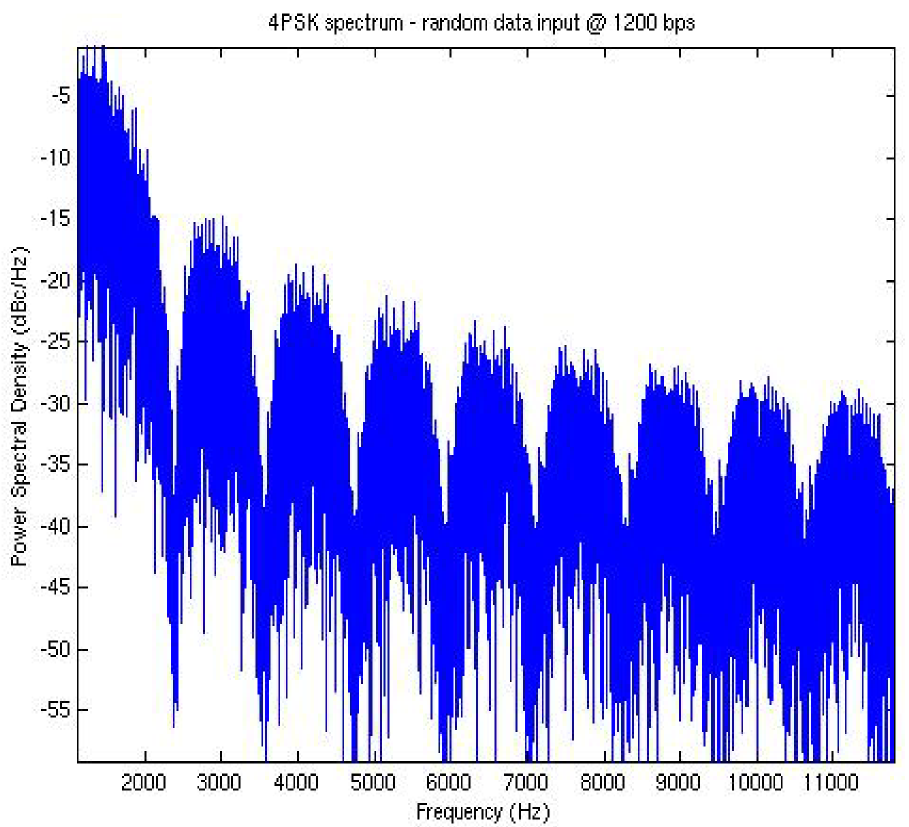
4PSK Modulator



CellularCrypto.com

4PSK Signal Properties





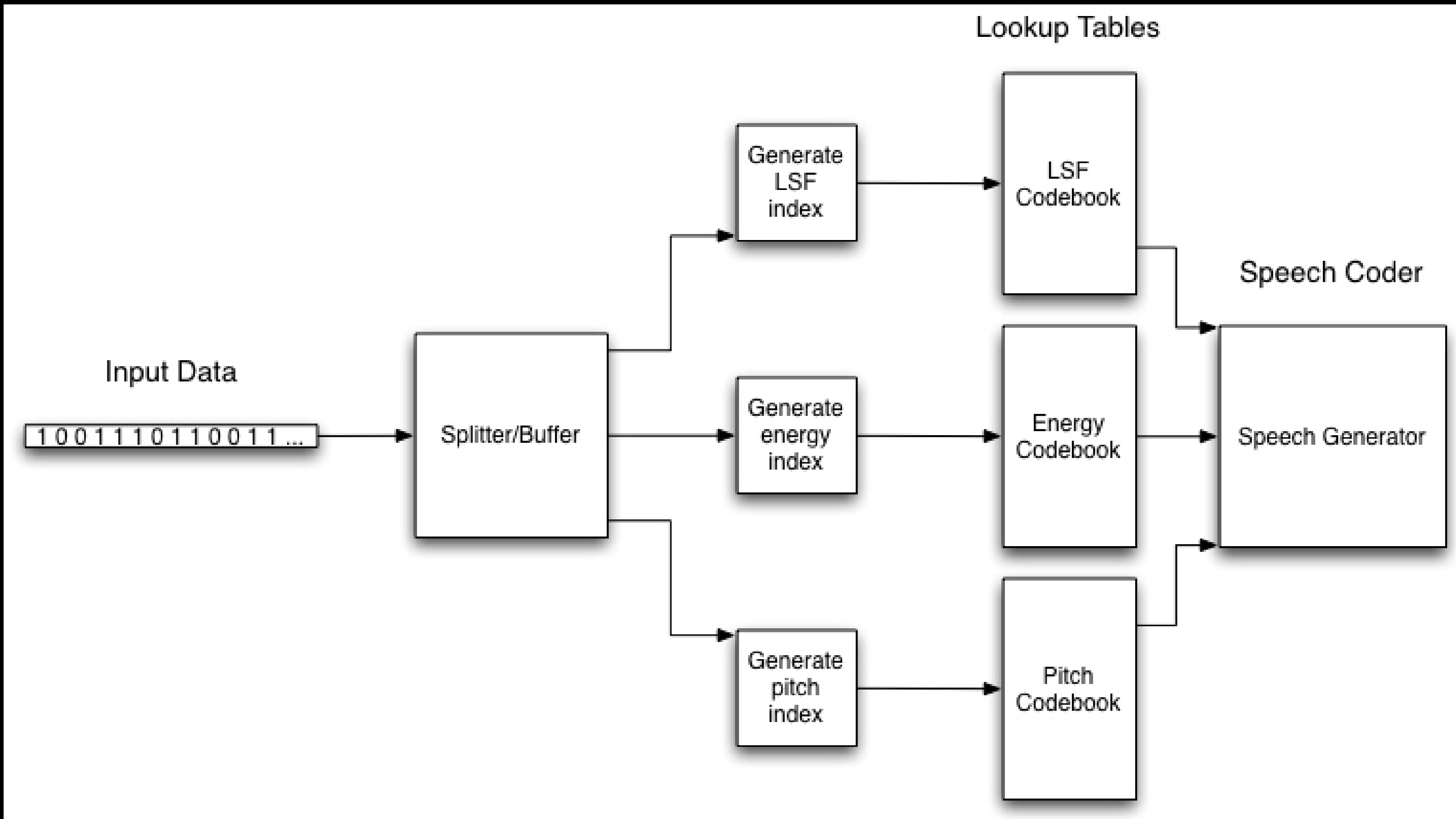
CellularCrypto.com

Phase Modulation Over GSM Voice Channel Demonstration

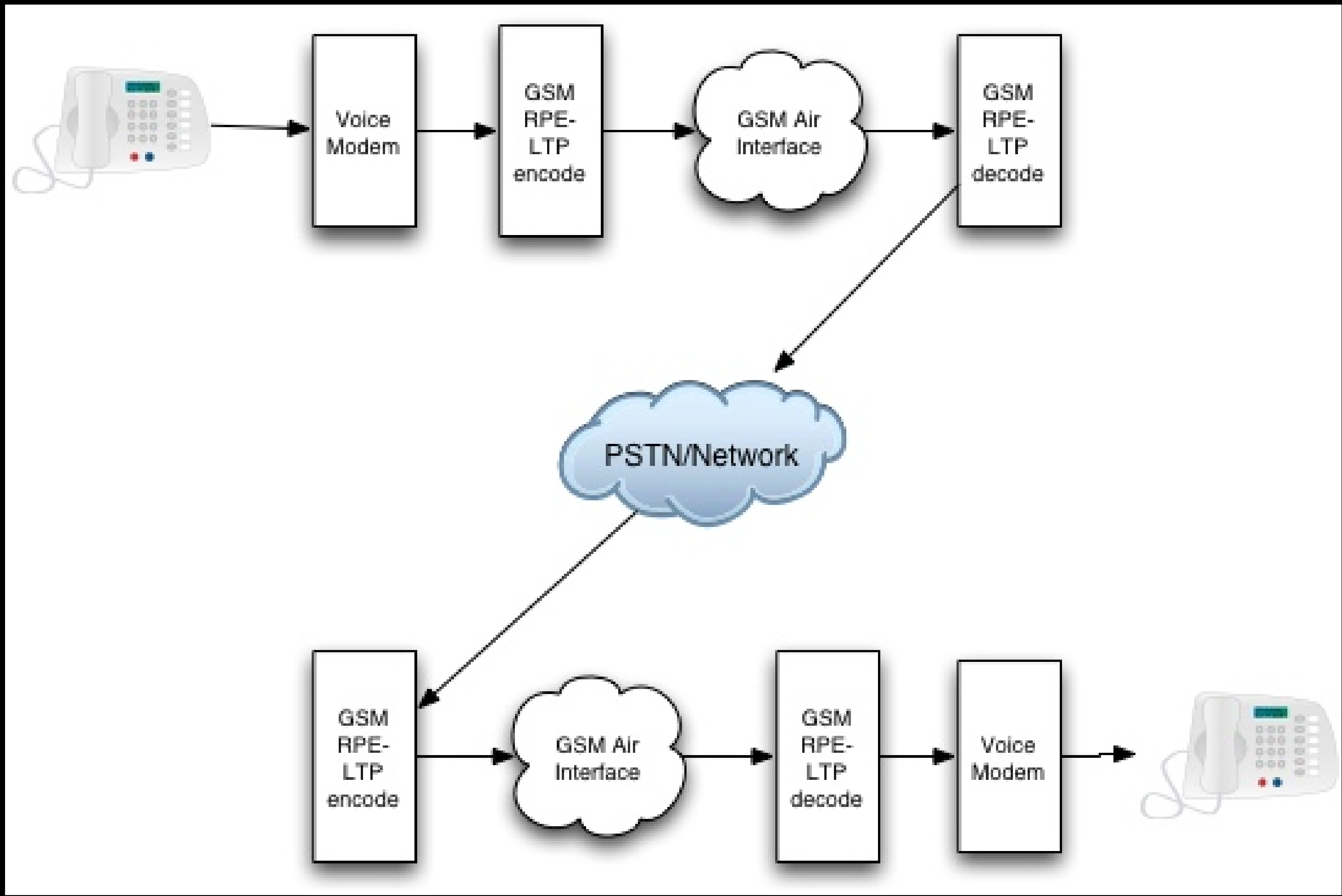
Frequency Modulation Over GSM Voice Channel Demonstration

Technical Details of Proposed GSM Voice Channel Modem and Cryptosystem

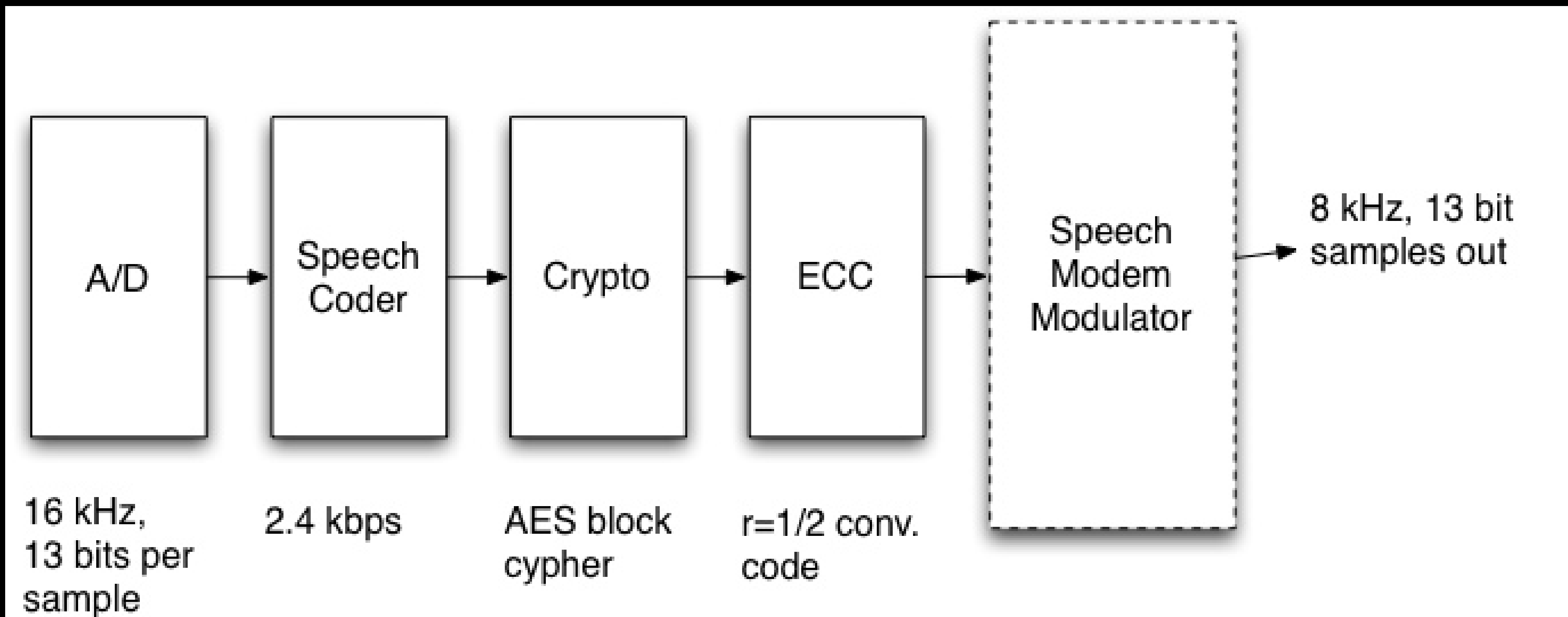
Katugampala, Villette, Kondoz (University of Surrey) Existing System



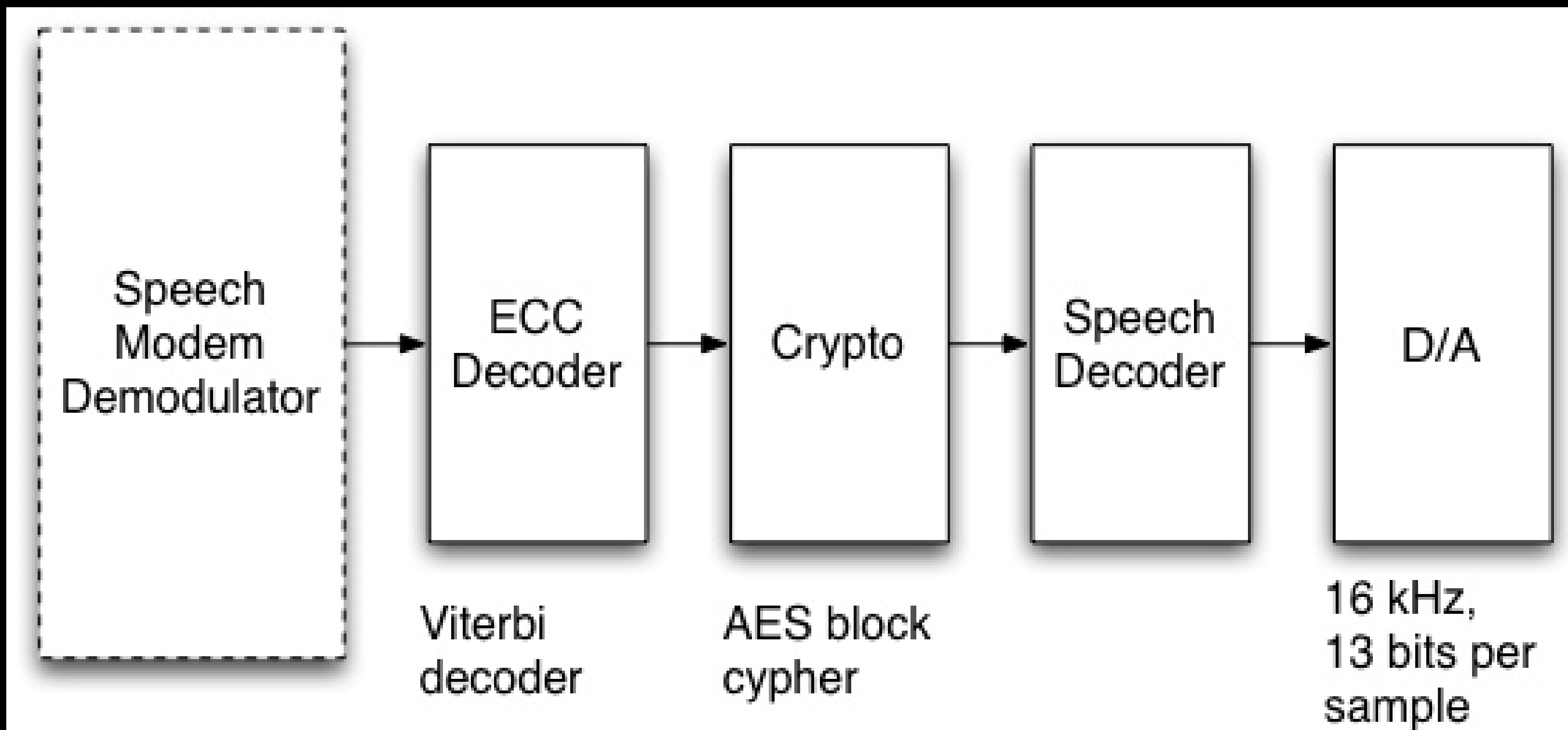
Proposed System Block Diagram



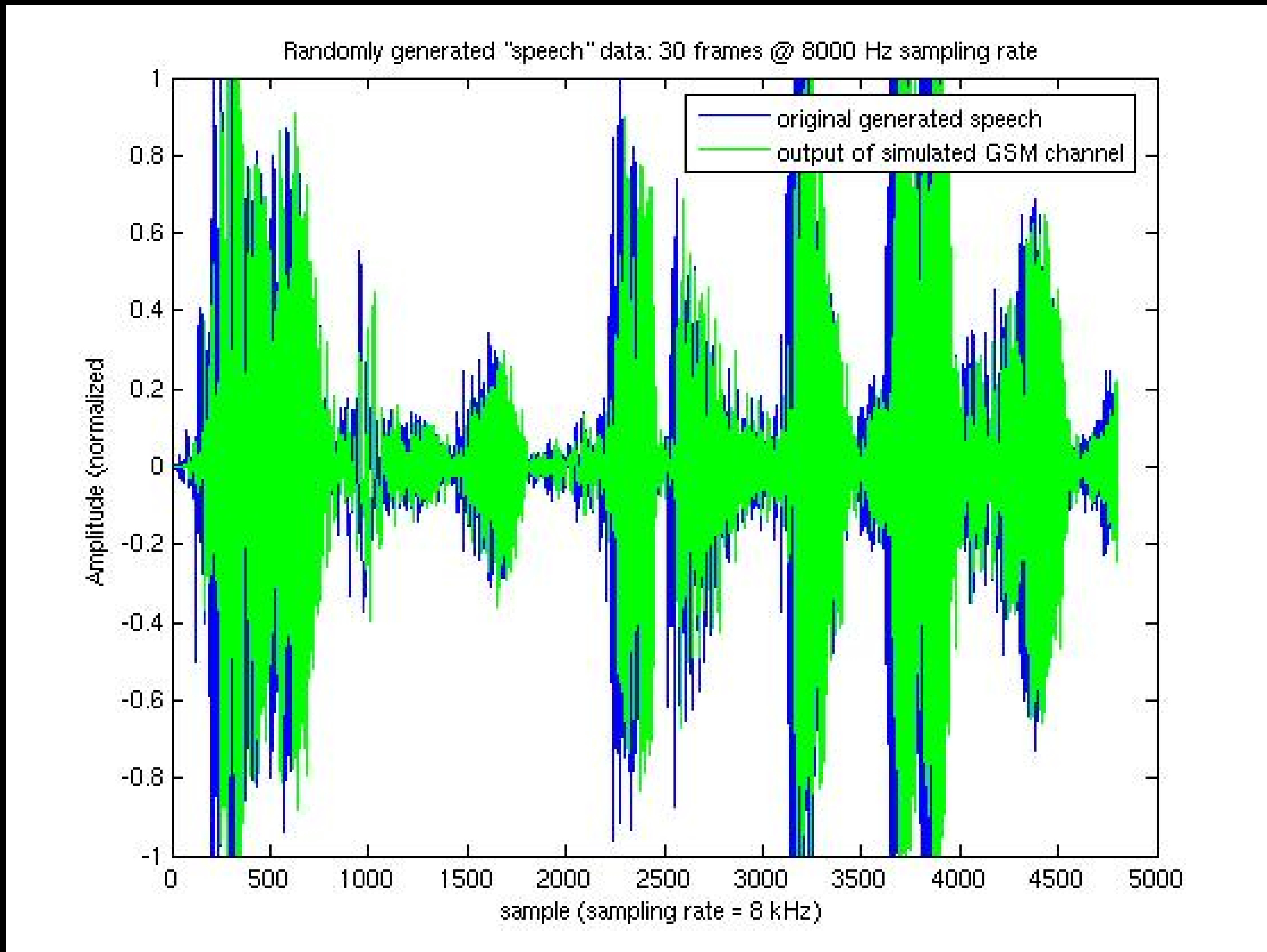
Encoder System Diagram



Decoder System Diagram

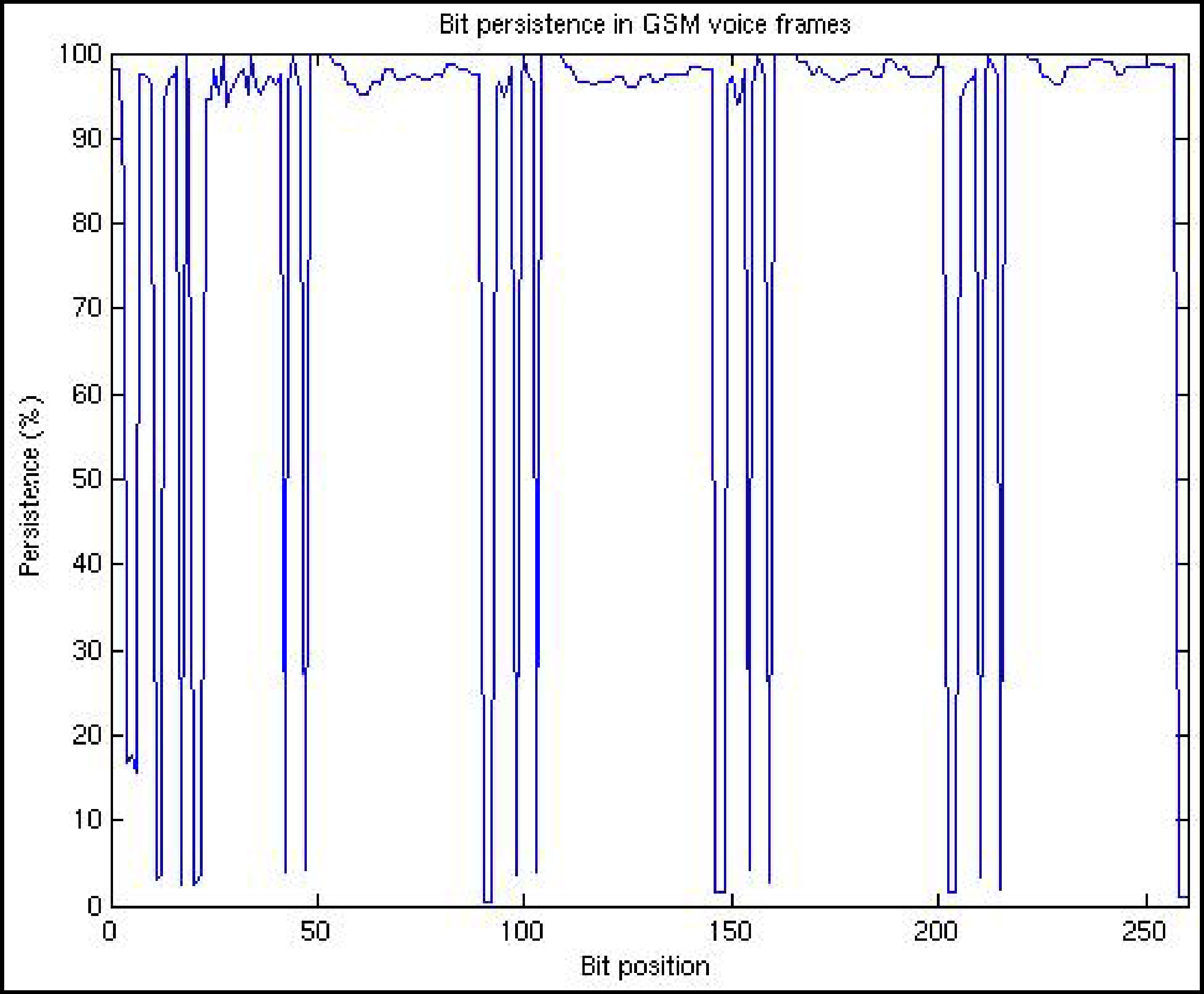


Generated speech channel output



CellularCrypto.com

Bit persistence in actual speech data 1000 frames



Speech Modem over GSM Voice Channel Demonstration

Underlying Cryptosystem

AES Block Cipher – Symmetric
- Fixed 128-bit block size
- 256-bit key

Exchanged over modified Diffie-Hellman

Adaptations to allow for frame drops
- Incrementing counter instead of typical block chaining

White Paper to be released during presentation.

Conclusion/Questions