Security in APCO P25 Networks

Steve Glass and Matt Robert

Who the Hell Are We?

Steve Glass

Researcher

Licensed Amateur radio operator

PhD candidate (If they can understand him and get past the accent)

Matt Robert

Independent Researcher

Licensed Amateur Radio Operator

Systems Engineer by day

Steve's translator when required.

Roadmap

- P25 Overview
- Introduction to Software Radio
- Free software for P25 - the OP25 project
- Security in APCO Project 25
- Questions/Comments

Roadmap

- P25 Overview
  - What is P25?
  - Who uses it and why?
  - Why should *we* care?
- Introduction to Software Radio
- Free software for P25 - the OP25 project
- Security in APCO Project 25
- Questions/Comments

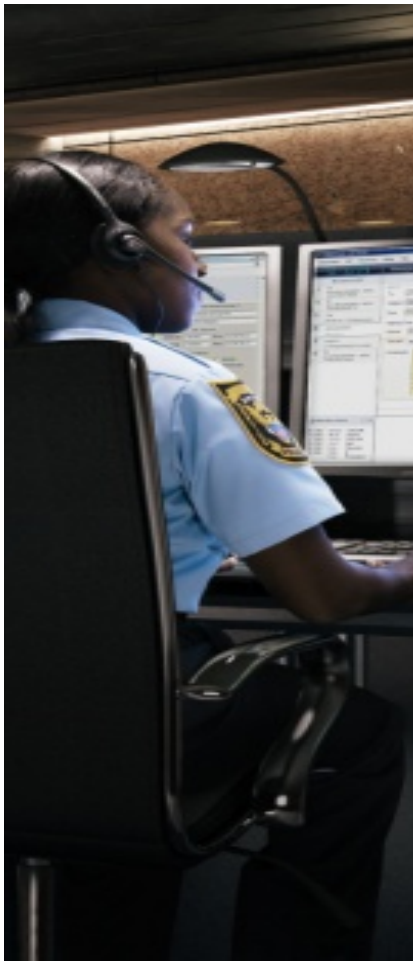
P25? Whuh?

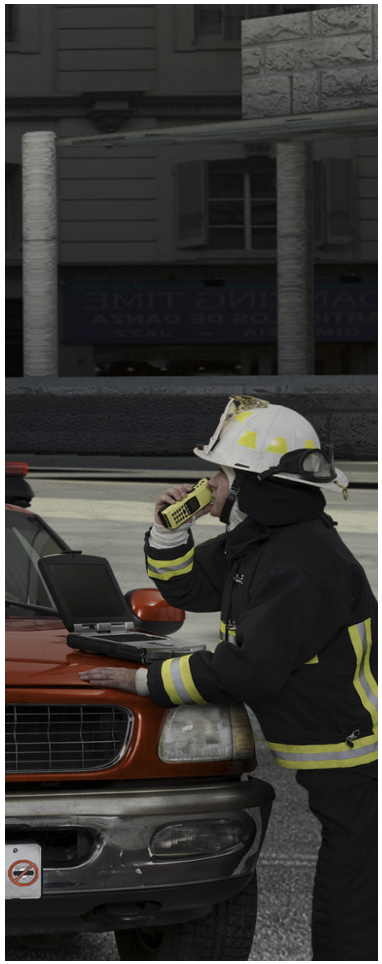
- Standardized public-safety communications
  - Hurricane Katrina
  - SAFECOM
  - Digital
    - Improved channel utilization
    - Provision for data services
    - Improved security

- Voice/data channels
  - 4800 two bit symbols/s
  - 6.125 kHz CQPSK
  - 12.5 kHz C4FM
  - Spectrally more efficient than analog voice

P25 Users

- Various Australia Federal law enforcement agencies
- NSW, QLD, SA State Police forces
- Victorian MMR – All emergency services in metro area are on a P25 trunked network
- NSW GRN – All metro NSW Emergency services in process of migrating to P25 trunking
- SA GRN - All metro SA Emergency services in process of migrating to P25 trunking





Photographs Source: Nivas Iver, Radio Authentication Customer Presentation, Motorola, 2006

P25 Technology

- Modes of operation:
  - Simplex
  - Repeater
  - Trunked
- Voice + Data
  - At 9600 b/s
- FS provides access to:
  - Other systems
  - PSTN
  - OTAR

Why should *we* care?

- Ensure that public safety agencies and officers can continue to do their jobs safely
- Make sure that law enforcement agencies have private, secure communications
- Protect public information from being disseminated (personal details – drivers license number, DOB, street address, etc)

Roadmap

- Overview

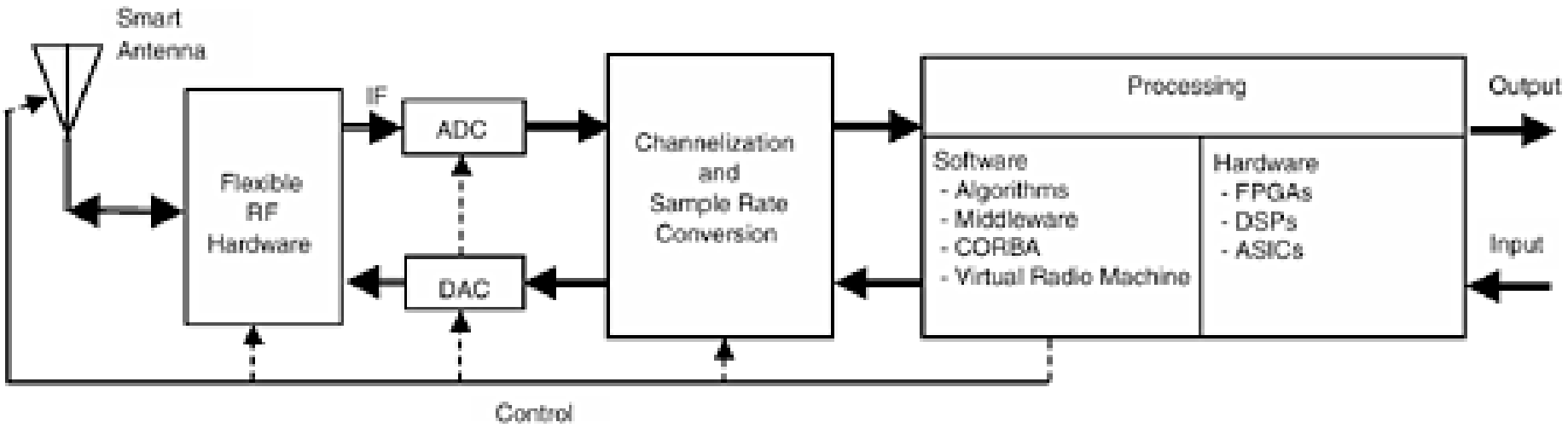
- Introduction to Software Radio
  - “ Software-defined Radio”
  - Sampling + Signal Processing
  - Sound card
  - Universal Software Radio Peripheral
  - GNU Radio
    - Signal processing blocks
    - Flow graphs

- Free software for P25 - the OP25 project

- Security in APCO Project 25

- Questions/Comments

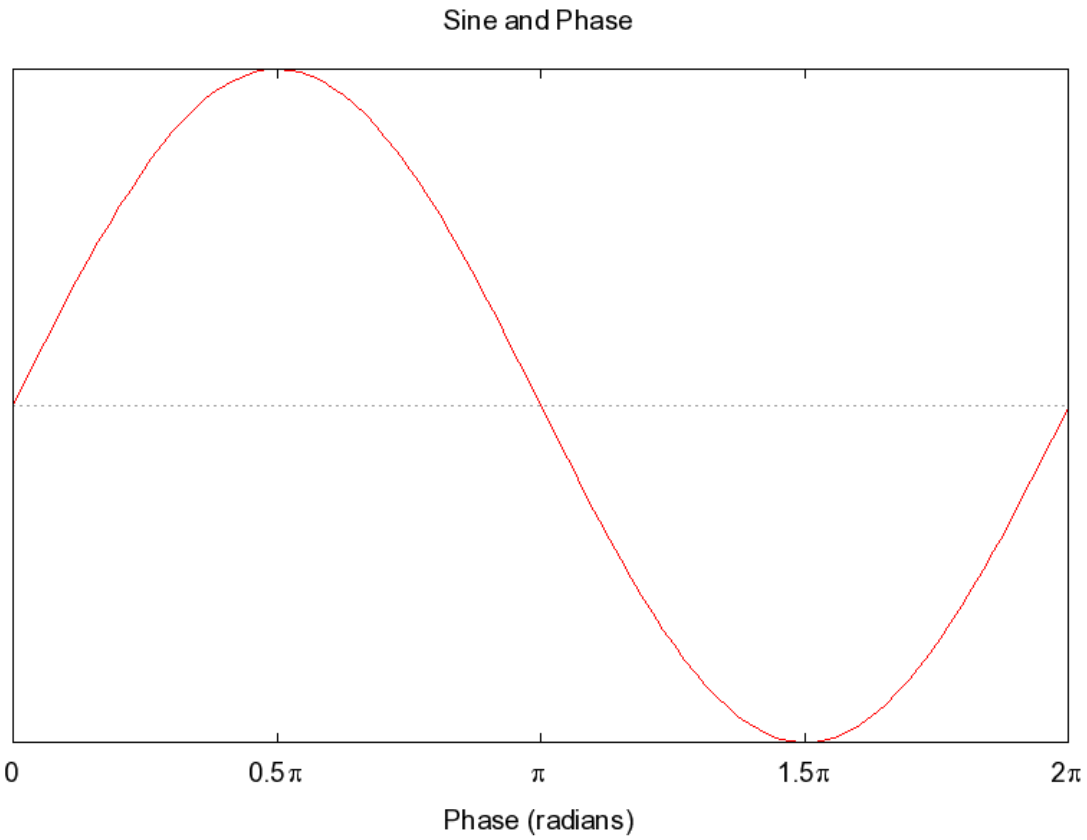
Software-Defined Radio



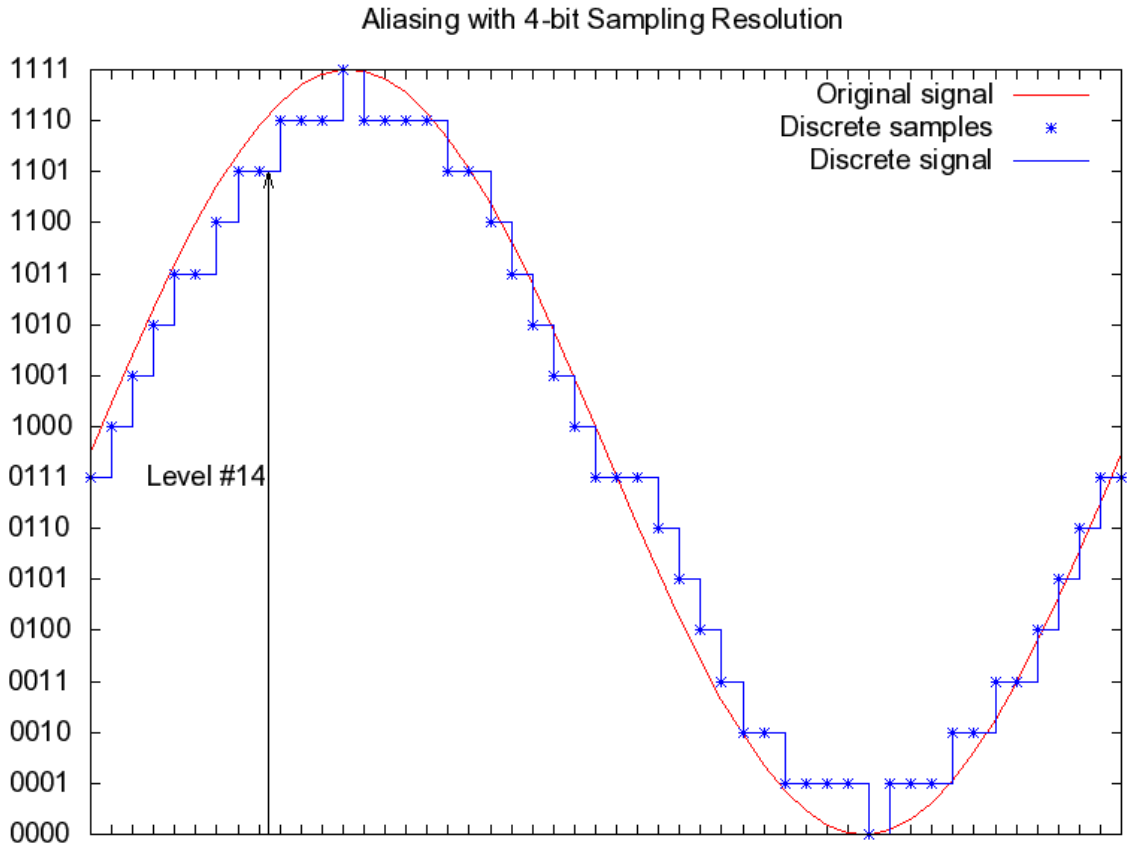
Source: The Scientist' and engineers guide to digital signal processing, 2nd ed, Steven W. Smith

- Receiver:
  - RF down-converter
  - ADC
  - Signal Processing
- Transmitter
  - Signal Generation
  - DAC
  - RF up-converter

Sampling – Here's our Source Signal



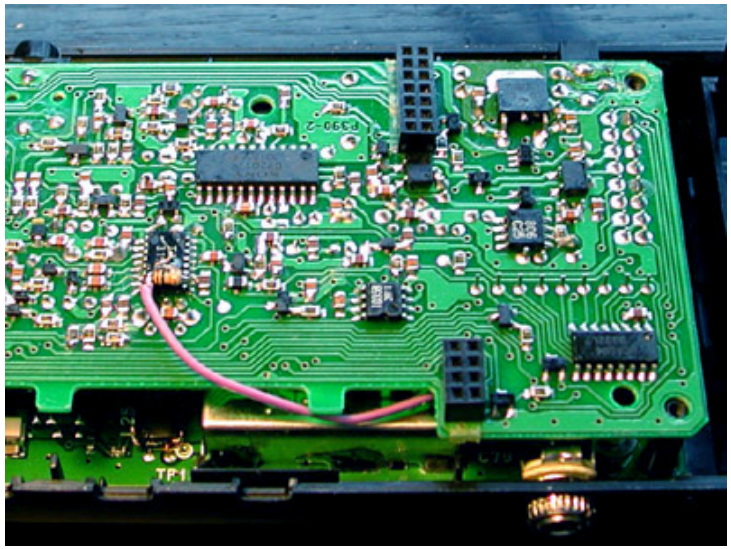
Discrete Time Series Sampling

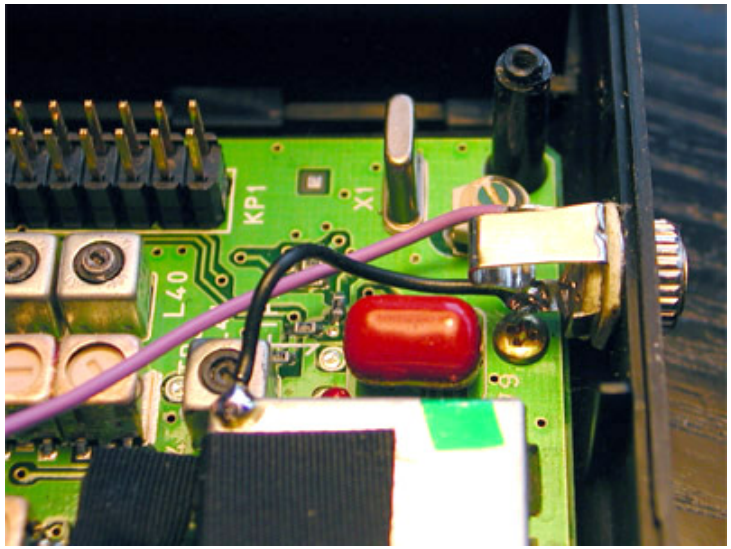


Sampling via Sound Card

- Capturing signals requires fast ADC
  - Cheap, can use existing VHF/UHF radio/scanner
  - Sound cards can sample up to ~200 kHz
  - Use output from radio/scanner
    - Scanner does tuning and conversion to baseband
    - Tap “FM discriminator” (unfiltered baseband)
    - Bridge circuitry
    - Some problems with soundcard filters
  - Single channel data capture

Scanner Modifications to Receive Digital Data





Source: http://www.discriminator.nl/

Sampling via USRP

- USRP1
  - 8 MHz bandwidth
  - 6,400 P25 channels at once!
  - Limited by USB 2.0 speed
  - About 1200 USD with WBX wideband RF transceiver daughterboard (50MHz-2.2GHz)
- USRP2
  - 25MHz bandwidth
  - 20,000 P25 channels at once!
  - Gigabit Ethernet instead of USB 2.0
  - Limiting factor is usually in host processing power/throughput
  - About 2000 USD with with WBX wideband RF transceiver daughterboard (50MHz-2.2GHz)

The Latest Toy From Ettus Research!

- USRP N210
- Bigger FPGA, high quality ADC chip
- Removed the SD card and replaced with onboard Flash RAM that is programmed over the ethernet interface at boot time.
- $1700 for base unit + $450 for WBX daughterboard

GNURadio

- Signal processing blocks:
  - *m* inputs × *n* outputs
  - Sources such as USRP, sine wave, saw wave, audio
  - Sinks such as USRP, audio, disk file, scopes
  - Filters, filter banks
  - Modulators
- Flow graphs
  - Connect blocks together
  - Direct-manipulation GRC
- Apps
  - Passive radar, Garage door-openers, FM radio, GSM BTS

http://www.gnuradio.org

GNURadio

Roadmap

- Overview
- Introduction to Software Radio
- Free software for P25 - the OP25 project
  - What is it?
  - Design of the receiver and transmitter
  - WireShark with P25 modifications
  - Brief demo
  - Project wiki and trac instance
- Security in APCO Project 25
- Questions/Comments

OP25 Receiver

OP25 Receiver

Acquisition + Filtering

- Capture from USRP1
  - 64 MS/s
  - User set decimation
  - All data logged to file
  - Migrate to UHD version
- Filtering
  - Setting Frequency using channel filter
  - Setting RF squelch level

Demodulation

- P25 uses 3 different modulation techniques:
  - 12.5 kHz C4FM
  - 6.125 kHz CQPSK
  - Linear Simulcast Modulation (LSM)
- We have C4FM working using “Frank’s” demodulator
- One contributor has written CQPSK modem

Decoding

- Decoder takes symbol stream and produces frames
  - Framing
  - Forward Error-Correction
  - Audio decoding
  - Writing to capture file or TUN/TAP device for analysis by WireShark

P25 Voice Traffic

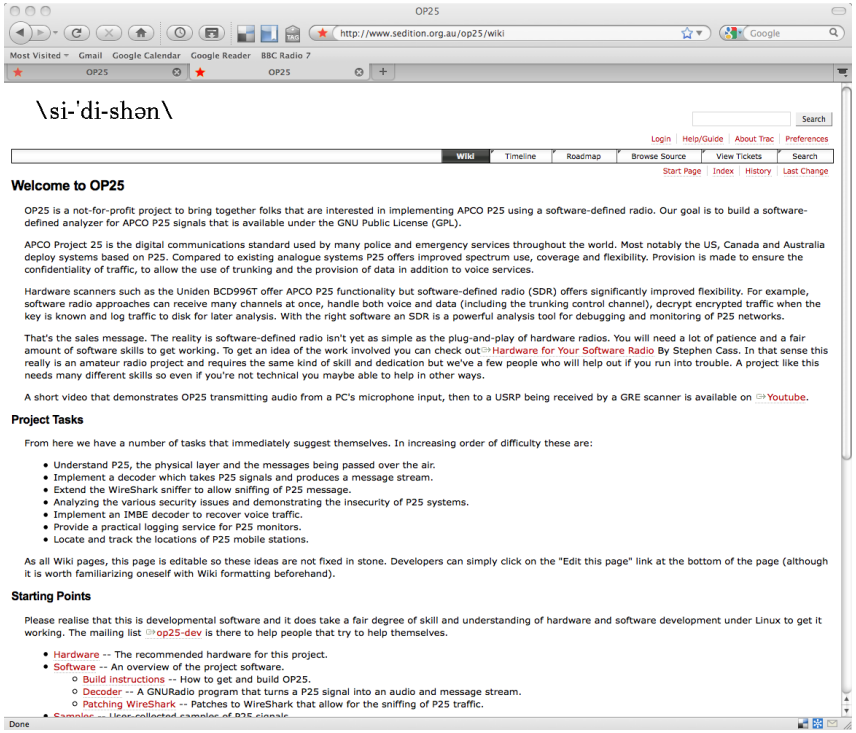
IMBE Vocoder

- A typical voice signal is sampled at 8 kS/s
  - Would require 64Kb/s channel
  - Most of the digital information is redundant
- IMBE Decoder
  - Receiver de-compresses voice signal
- IMBE Encoder
  - Transmitter compresses voice signal
- Patented technologies undermine open standards

WireShark + OP25

OP25 Transmitter

Project Website



- Project website
  - Wiki
    - Info on building etc.
    - Links to related projects
  - Subversion repository
- Yahoo e-group:
  - op25-dev
  - Around 130 subscribers

http://www.sedition.org.au

Roadmap

- Overview
- Introduction to Software Radio
- Free software for P25 - the OP25 project

- Security in APCO Project 25
  - Authentication
  - Remote Inhibit
  - P25 Cryptography
  - Brute-forcing Keys

- Questions/Comments

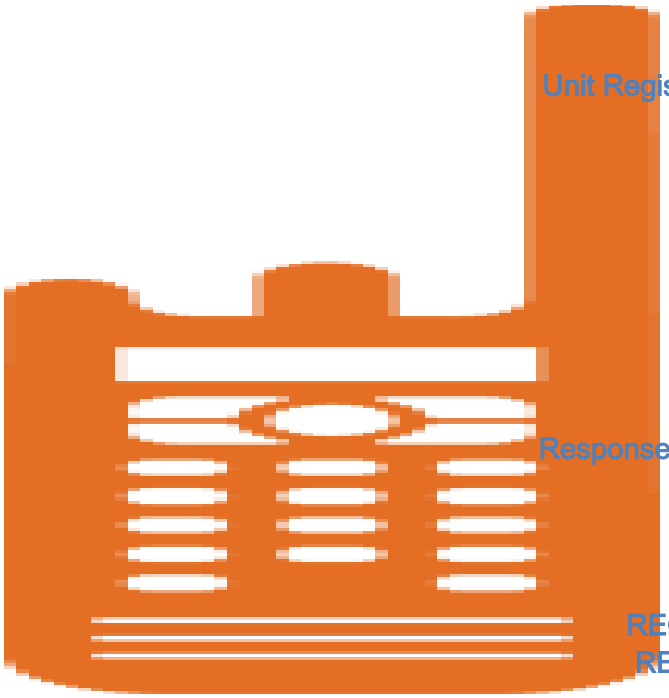
Remote Inhibit – aka “Stun”

- Part of the P25 standard includes a remote radio inhibit/uninhibit feature
  - It is mandatory to achieve conformance
  - Radio receiving stun becomes inoperative
- This feature does not use any authentication
  - Trunking packet sent to a target radio
  - Easily spoofed by an adversary/attacker
    - Control Channel needs to be overpowered in trunking mode

Authentication

- No effective authentication!
  - Anyone can access network
  - Nodes identified using a 24-bit address scheme
  - Implicit trust in sender's identity
- A Radio ID is simply looked up in a database, and if it's valid then that radio can transmit
- P25 introduces new authentication mechanism
  - Allows for radio (one-way) and mutual authentication
  - Not integrated with encryption
    - Encryption and Authentication are both *optional* services

Radio Authentication



Unit Registration

Challenge

Response

REG_ACCEPT /
REG_REFUSE

P25 Mobile Station

P25 Fixed Station

P25 Encryption

- Cipher produces keystream
  - Essentially a PRNG
- Keystream XORed with Plaintext to produce ciphertext:

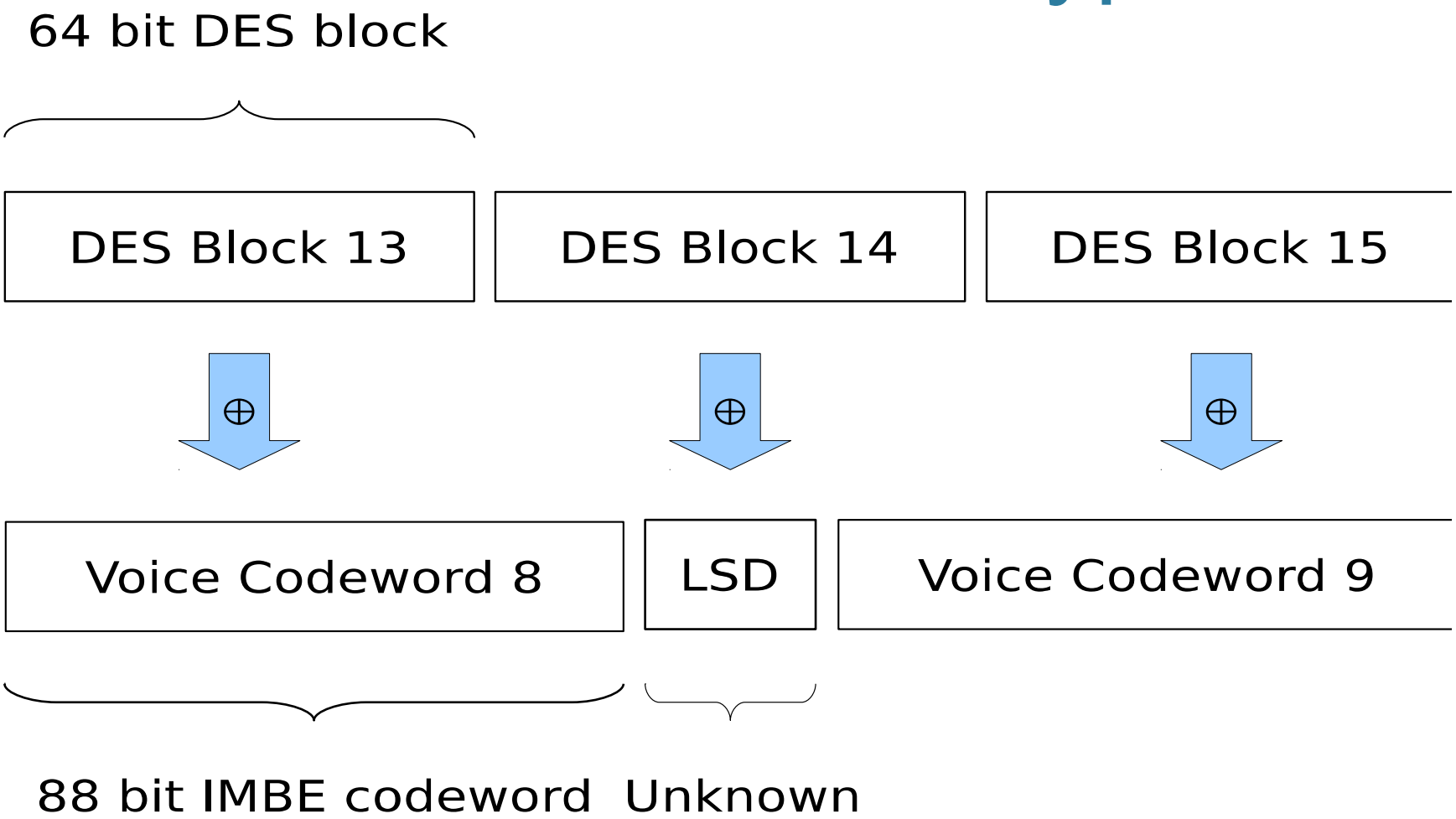
- There are some caveats:
  - (P1 XOR K) XOR (P2 XOR K) = P1 XOR P2
    - To avoid re-using K we use an Initialization Vector (IV)
      - IV is assigned per superframe
      - Computed by hardware RNG and LFSR

P25 Decryption

- Keystream XORed with Ciphertext to recover plaintext:

- Known-plaintext reveals Keystream
  - KP XOR C = KS
  - Enables brute-force key searching

P25 DES-OFB Encryption



DES Cracking

- DES/OFB not suited for TMTO
  - IV generation appears strong (hardware RNG)
  - Brute force remains best approach
- Various approaches:
  - Distributed computing
  - FPGA Approaches (Pico SC5, COPACOBANA)
  - GPU Implementation

Questions/Comments

Source: A Failure Of Initiative: Final Report of the Select Bipartisan Committee to Investigate the Preparation for and Response to Hurricane Katrina, US House of Representatives, 2006