A Ghost in your Transmitter :

analyzing polyglot signals for physical layer covert channels detection

José Lopes Esteves,

Emmanuel Cottais and Chaouki Kasmi

WHO WE ARE

E. Cottais, C. Kasmi, J. Lopes Esteves

- ANSSI-FNISA / Wireless Security Lab
  - 11 members, including 3 PhD
  - Electromagnetic security
  - RF communications security
  - Embedded systems
  - Signal processing

OUTLINE

- Covert channels
- Polyglot signals
- Target QPSK transmission
- Generating covert polyglot signals
- Exploiting covert polyglot signals
- Detection techniques and counter-measures
- Conclusion

Covert channels

Definitions

COVERT CHANNELS

- Covert channel:
  - Information transfer (uni- or bi-directional)
  - Entities not allowed to communicate
  - Channel not intended for communication
- Prerequisite: preliminary infection
  - Both ends know the covert channel
  - Both ends know the covert protocol
  - Out of scope of this talk

COVERT CHANNELS

- Host based: communication between processes on a host [1]
  - Shared file system: file contents, file lock…
  - Shared hardware: DRAMA [2]…
- Two classes :
  - Storage based
  - Timing based
- A lot of studies on design, characterization and detection

COVERT CHANNELS

- Network based: communication between remote processes on connected hosts
- Information hidden in [1,3]:
  - Protocol Data Units
  - Through the timing of PDUs or protocol commands
- A lot of studies on design, characterization and detection
- Mostly > layer 3 channels

COVERT CHANNELS

- Air gap based: communication between remote processes on disconnected hosts
- Exploitation of shared physical medium:
  - Light, pressure, vibration, sound, temperature, EM environment
- Also called physical covert channels
  - Modulate information directly on physical medium
- Recent security hype

Polyglot Signals

Physical layer network-based covert channels

POLYGLOT SIGNALS

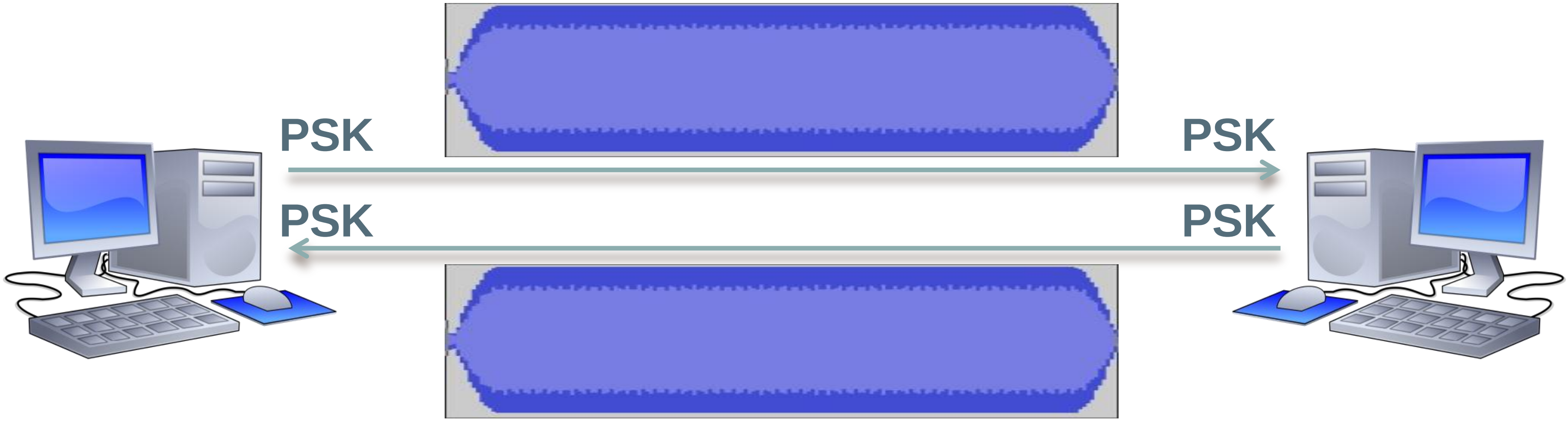
- Goodspeed, Bratus, ReCon 2015 [4]
- RF receivers are parsers
- Info received is different from info transmitted to upper layers:
  - Modulation
  - Error correction
- Try to recover familiar structures from unknown received signal

POLYGLOT SIGNALS

- Can be exploited for covert communications
- Exploit complementary modulations
- ASK modulation added to a PSK based protocol
  - The legitimate receiver will still get the PSK messages and will not consider amplitude variations, and likely correct them
  - The covert receiver is a ASK demodulator which will not consider the phase variations

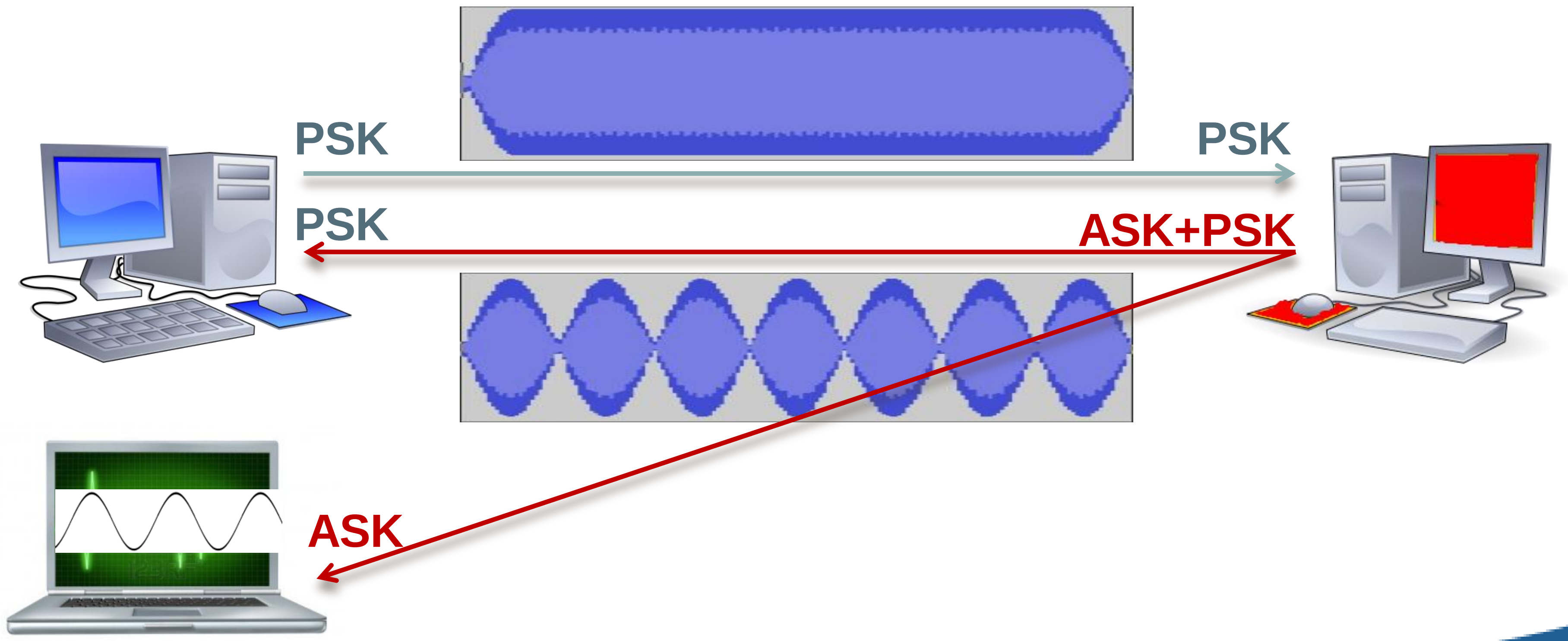
POLYGLOT SIGNALS

- Covert polyglot signal for data exfiltration
  - ASK modulation added to a PSK based protocol



POLYGLOT SIGNALS

- Covert polyglot signal for data exfiltration
  - ASK modulation added to a PSK based protocol



POLYGLOT SIGNALS

- Covert polyglot signal for data exfiltration
  - ASK modulation added to a PSK based protocol
- Attacker needs:
  - Minimize impact on legit channel
  - Maximize covert transmission quality
  - Minimize detectability
- Of course: trade-off !

POLYGLOT SIGNALS

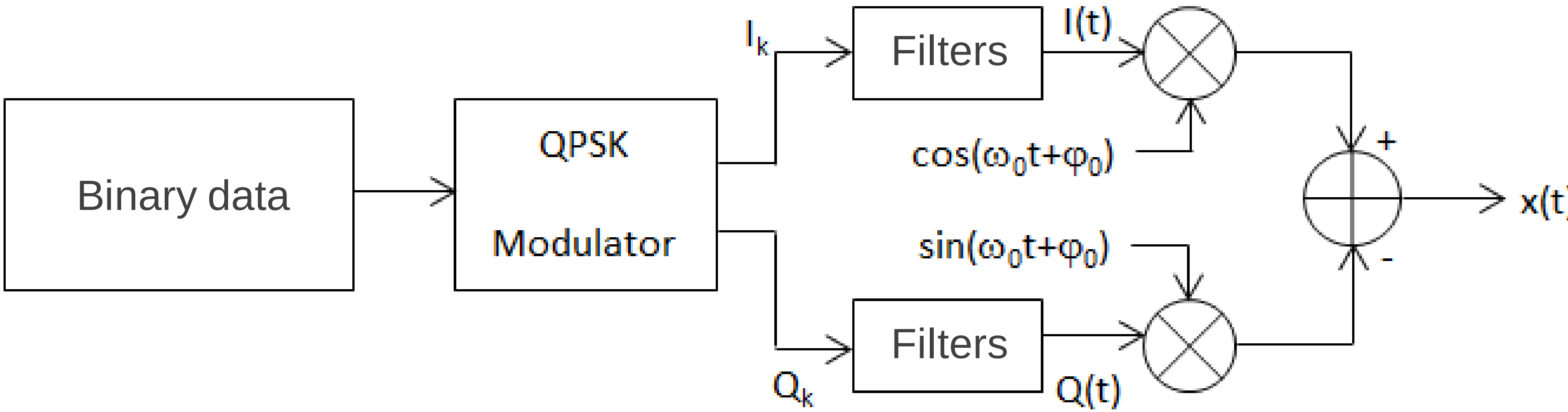
- Is this technique limited to complementary modulations ?
- How can an attacker generate a covert polyglot signal ?
- Is it possible to efficiently detect such covert channels?

Target QPSK transmission

Back to school

QPSK TRANSMISSION

- Architecture of an IQ transmitter



- Transmitted signal:

$$x(t) = \mathrm{I(t)}.\cos(\omega_0 t + \varphi_0) - \mathrm{Q(t)}.\sin(\omega_0 t + \varphi_0)$$

QPSK TRANSMISSION

- Transmitted signal:

$$x(t) = \mathrm{I(t)}.\cos(\omega_0 \mathrm{t} + \varphi_0) - \mathrm{Q(t)}.\sin(\omega_0 \mathrm{t} + \varphi_0)$$

- Received signal (ideal channel):

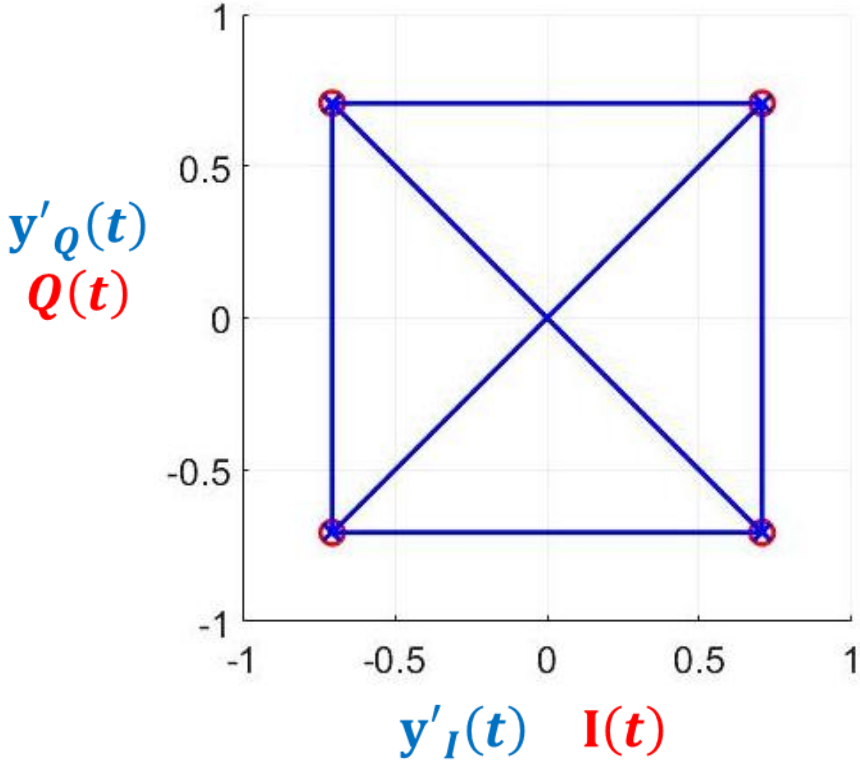
$$y_I(t) = x(t).\cos(\omega_0 \mathrm{t} + \varphi_0)$$
$$= \frac{I(t)}{2} + \frac{I(t)}{2}.\cos(2\omega_0 \mathrm{t} + 2\varphi_0) - \frac{Q(t)}{2}.sin(2\omega_0 \mathrm{t} + 2\varphi_0)$$
$$y_Q(t) = x(t).sin(\omega_0 \mathrm{t} + \varphi_0)$$
$$= \frac{I(t)}{2}.sin(2\omega_0 \mathrm{t} + 2\varphi_0) - \frac{Q(t)}{2} + \frac{Q(t)}{2}.cos(2\omega_0 \mathrm{t} + 2\varphi_0)$$

- After low-pass filtering:

$$y_I(t) = \frac{\mathrm{I(t)}}{2} \qquad (*2) \rightarrow y'_I(t) = \mathrm{I(t)}$$
$$y_Q(t) = -\frac{Q(t)}{2} \qquad (*\text{-}2) \rightarrow y'_{\mathrm{Q}}(t) = Q(\mathrm{t})$$

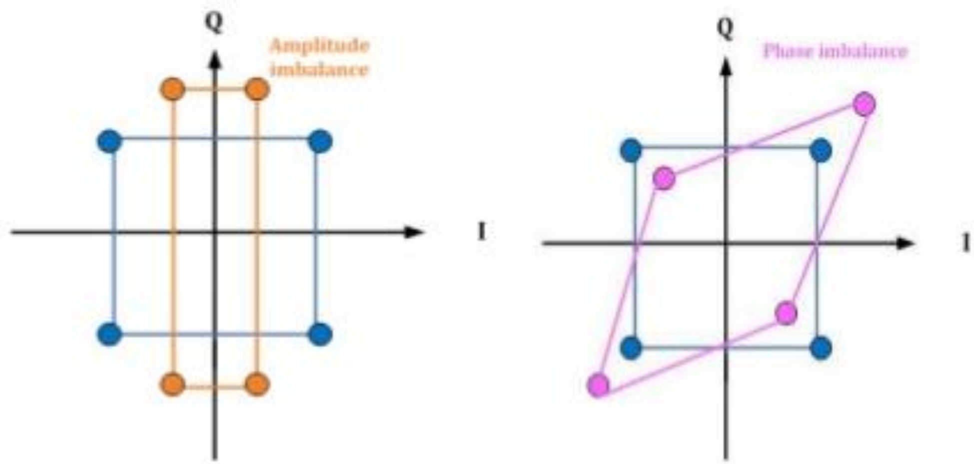
QPSK TRANSMISSION

- Received signal constellation (ideal channel):



QPSK TRANSMISSION

- Non-ideal channel:
  - Presence of noise
  - The receiver implements several correction blocks
- Especially:
  - IQ imbalance: amplitude and phase correction

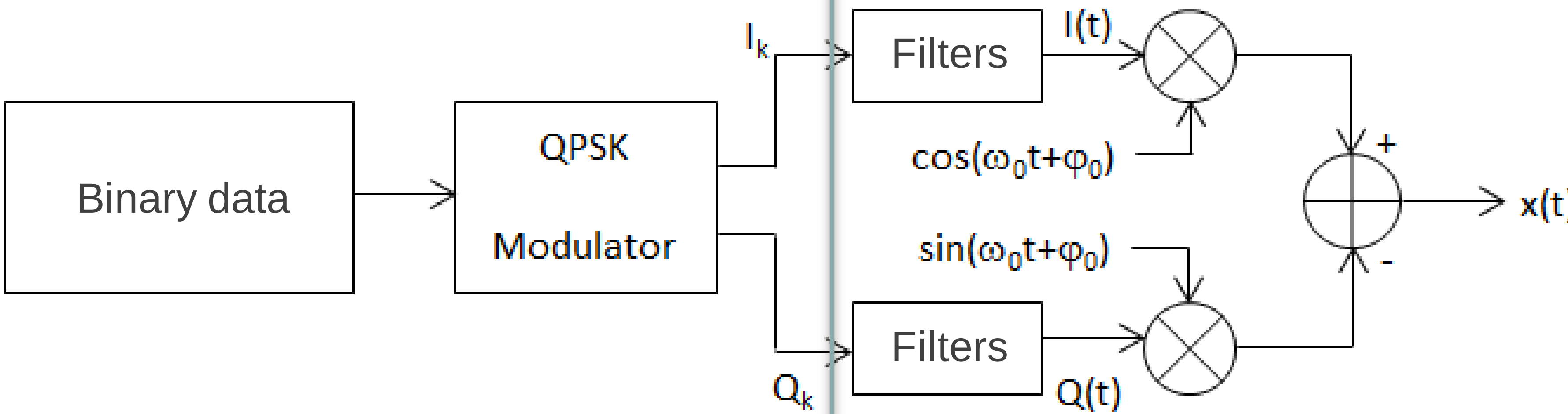


Generating Covert Polyglot Signals

Finding entry points for attacking

QPSK TRANSMISSION

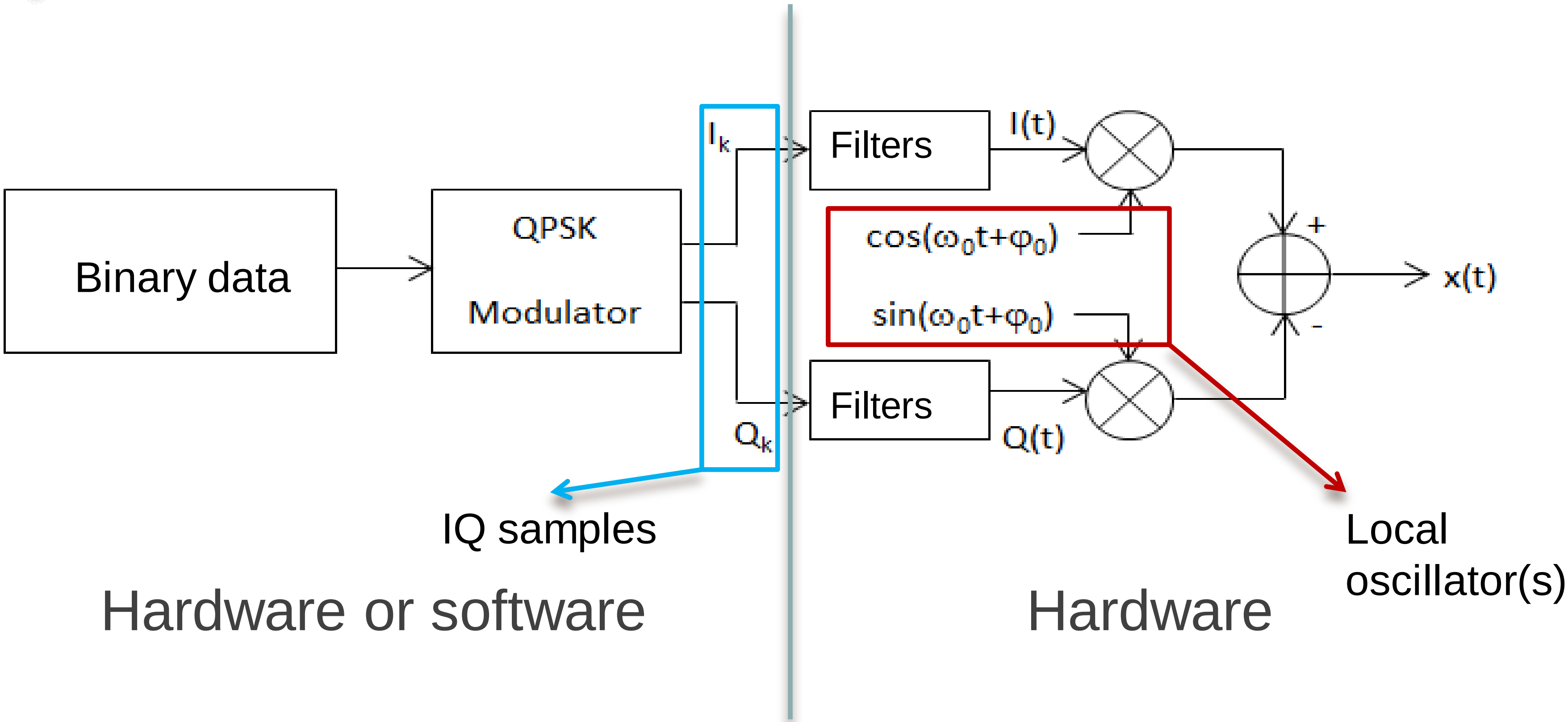
- Target QPSK transmitter



Hardware or software

Hardware

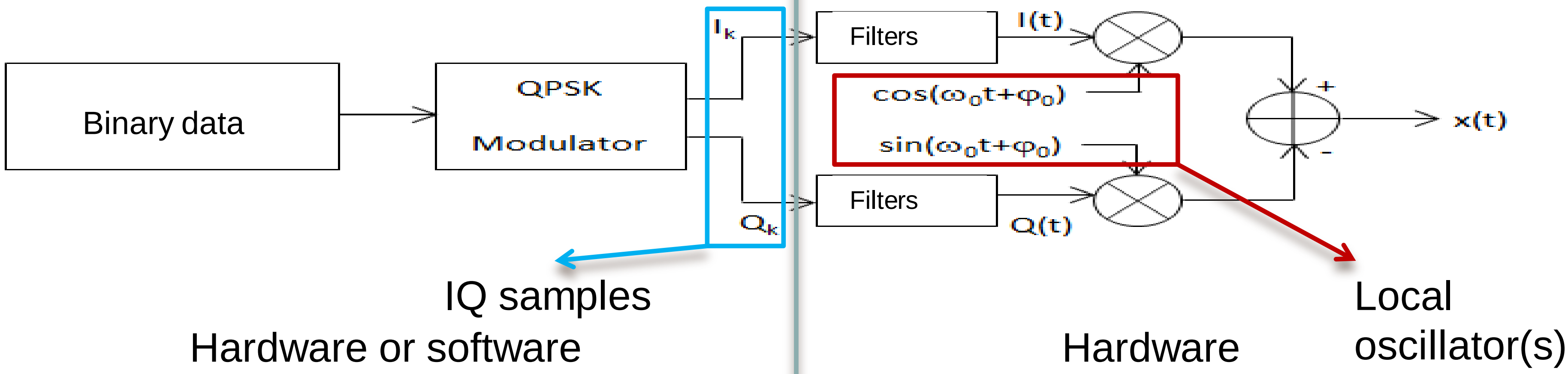
QPSK TRANSMISSION



- Transmitted signal:

$$x(t) = \mathrm{I(t)}.\cos(\omega_0 t + \varphi_0) - \mathrm{Q(t)}.\sin(\omega_0 t + \varphi_0)$$

GENERATING POLYGLOT SIGNALS



- Transmitted signal

$$x(t) = \mathrm{I(t)}.\cos(\omega_0 t + \varphi_0) - \mathrm{Q(t)}.\sin(\omega_0 t + \varphi_0)$$

Software attack:
- Amplitude of I
- Amplitude of Q

Hardware attack:
- Amplitude of cos
- Amplitude of sin
- Cos frequency
- Cos phase
- Sin frequency
- Sin phase

GENERATING POLYGLOT SIGNALS

- Software level
  - Configuration of radio front-end
  - Modification of IQ samples of SDR
  - Modification of FPGA code of SDR
- How
  - Malicious device drivers
  - Software flowgraph alteration
  - Specially crafted firmware/bitstream [12]
- Modification of I and Q independently possible

GENERATING POLYGLOT SIGNALS

- Hardware level
  - Alteration of local oscillator(s) behaviour
  - Hardware trojan
  - EMC phenomena
- How
  - Crosstalk, parasitic coupling, impedance mismatch
  - On power lines, on oscillator configuration lines (e.g. VCO, capacitors) [5]
- Separate operation on I and Q not straightforward

Exploiting Covert Polyglot Signals

Playing with the amplitude of I and Q

EXPLOITING POLYGLOT SIGNALS

- Modulating the amplitude of IQ channels
  - Can be done from hardware or software

$$x(t) = \boxed{I(t).(1+\alpha)}.\cos(\omega_0 t + \varphi_0) - \boxed{Q(t).(1+\beta)}.\sin(\omega_0 t + \varphi_0)$$

$$x(t) = I(t).\boxed{(1+\alpha).\cos(\omega_0 t + \varphi_0)} - Q(t).\boxed{(1+\beta).\sin(\omega_0 t + \varphi_0)}$$

- Two example polyglot signals:
  - ASK over QPSK
  - QPSK over QPSK

EXPLOITING POLYGLOT SIGNALS

- Transmitted signal:

$$x(t) = I(t).(1+\alpha).cos(\omega_0 t + \varphi_0) - Q(t).(1+\beta).sin(\omega_0 t + \varphi_0)$$

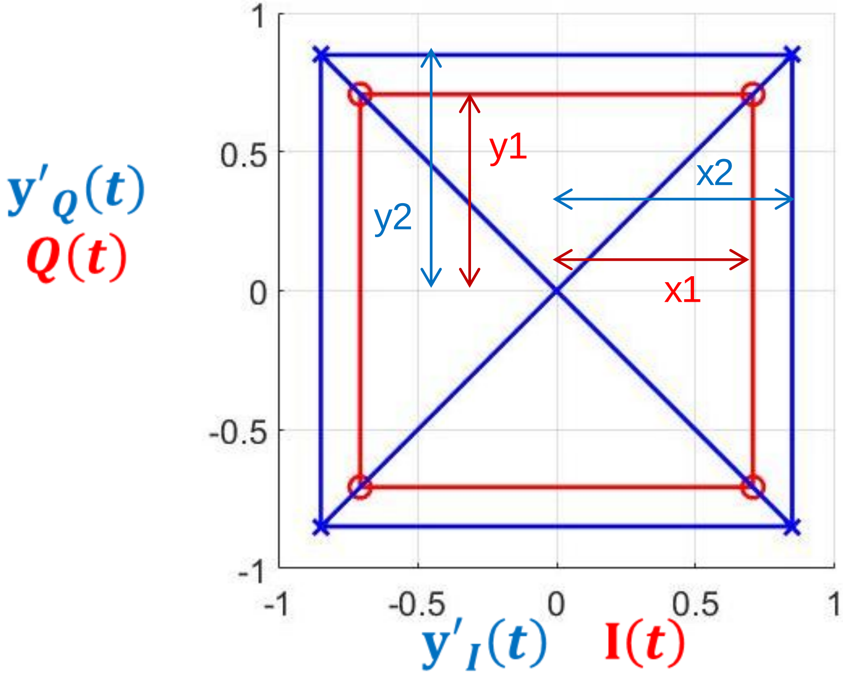
- Received signal (ideal channel):

$$y_I(t) = x(t).\cos(\omega_0 t + \varphi_0)$$
$$= \frac{I(t)}{2}.(1+\alpha) + \frac{I(t)}{2}.(1+\alpha).\cos(2\omega_0 t + 2\varphi_0) - \frac{Q(t)}{2}.(1+\beta).sin(2\omega_0 t + 2\varphi_0)$$
$$y_Q(t) = x(t).sin(\omega_0 t + \varphi_0)$$
$$= \frac{I(t)}{2}.(1+\alpha).sin(2\omega_0 t + 2\varphi_0) - \frac{Q(t)}{2}.(1+\beta) + \frac{Q(t)}{2}.(1+\beta).cos(2\omega_0 t + 2\varphi_0)$$

- After low-pass filtering:

$$y_I(t) = \frac{I(t)}{2}.(1+\alpha) \qquad (*2) \rightarrow y'_I(t) = I(t).(1+\alpha)$$
$$y_Q(t) = -\frac{Q(t)}{2}.(1+\beta) \qquad (*-2) \rightarrow y'_Q(t) = Q(t).(1+\beta)$$

EXPLOITING POLYGLOT SIGNALS



$$\alpha = \frac{x2 - x1}{x1}$$

$$\beta = \frac{y2 - y1}{y1}$$

- IQ imbalance correction block will:
  - Consider α and β effects as noise
  - Compensate α and β
- Transparent for legit receiver

EXPLOITING POLYGLOT SIGNALS

- On the covert receiver, how to recover α and β ?
  - We suppose α and β small
    - Do not change symbol quadrant (we target QPSK)
  - Compare received samples with expected ones

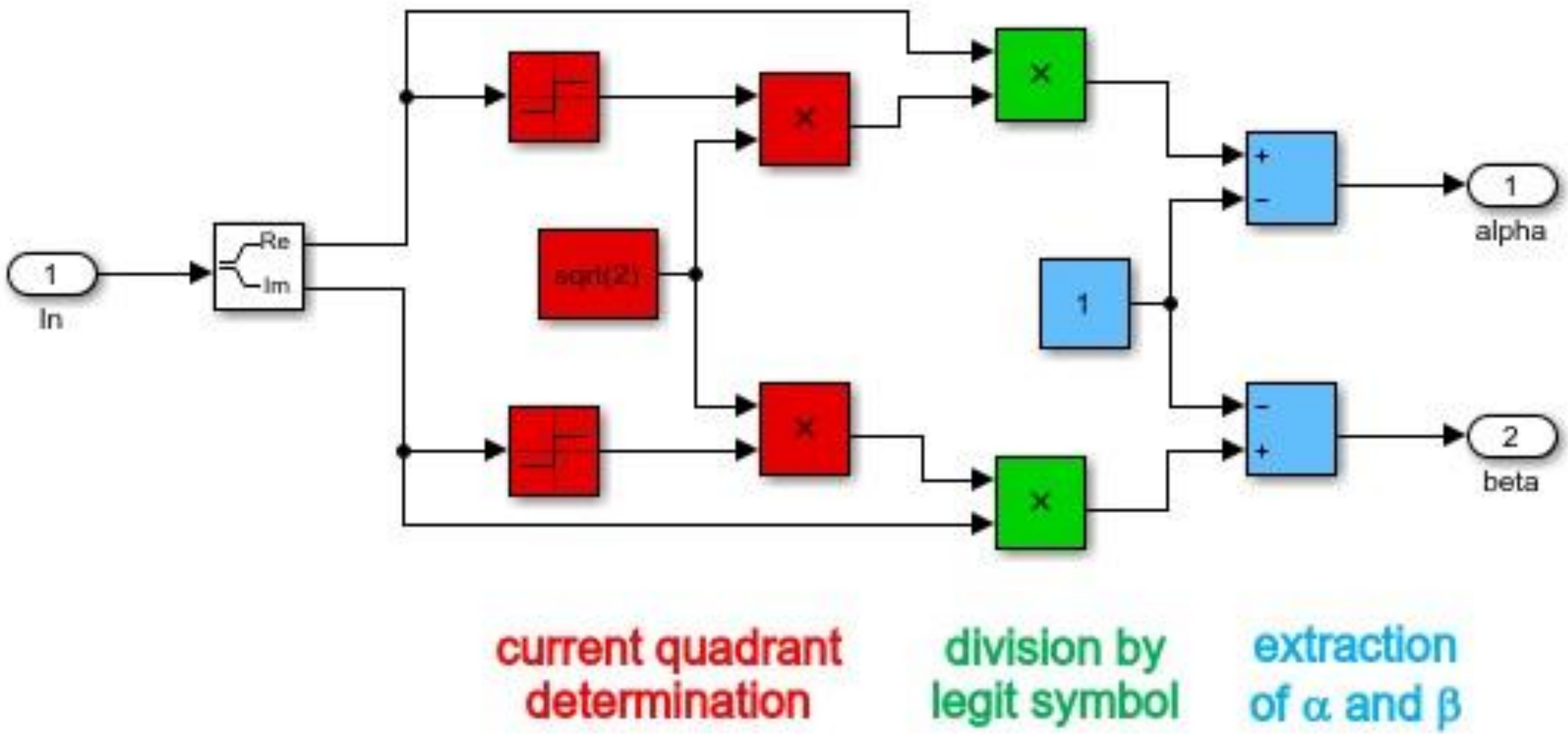
$$y'_I(t) = \mathrm{I}(\mathrm{t})\,.\,(1+\alpha) \qquad y'_{\mathrm{Q}}(t) = Q(\mathrm{t})\,.\,(1+\beta)$$

$$y''_I(\mathrm{kT}) = \frac{y'_I(\mathrm{kT})}{\mathrm{I}(\mathrm{kT})} = (1+\alpha) \qquad y''_{\mathrm{Q}}(\mathrm{kT}) = \frac{y'_{\mathrm{Q}}(\mathrm{kT})}{\mathrm{Q}(\mathrm{kT})} = (1+\beta)$$

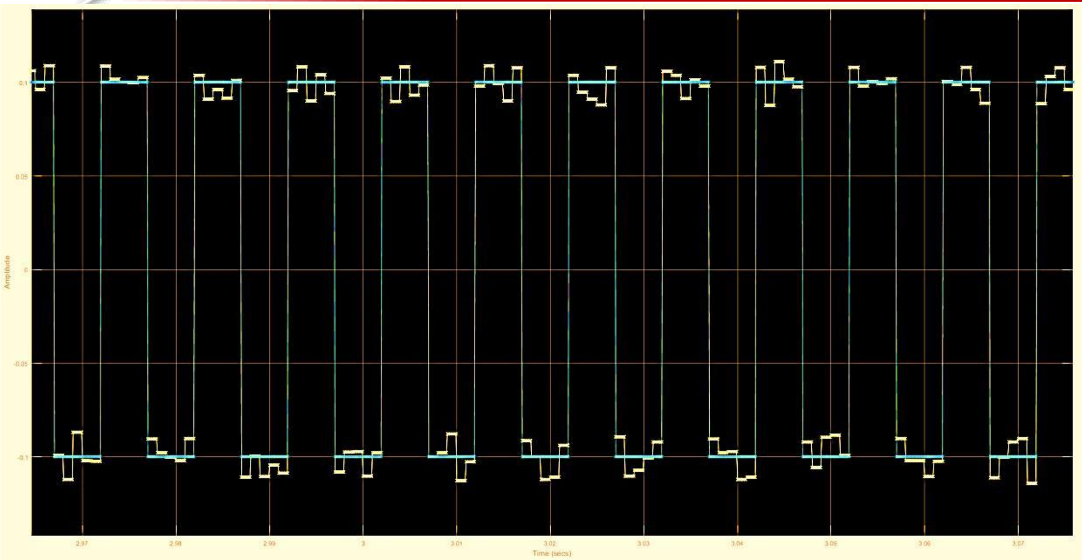
$$\alpha = -1 + \frac{y'_I(\mathrm{kT})}{\mathrm{I}(\mathrm{kT})} \qquad \beta = -1 + \frac{y'_{\mathrm{Q}}(\mathrm{kT})}{\mathrm{Q}(\mathrm{kT})}$$

EXPLOITING POLYGLOT SIGNALS

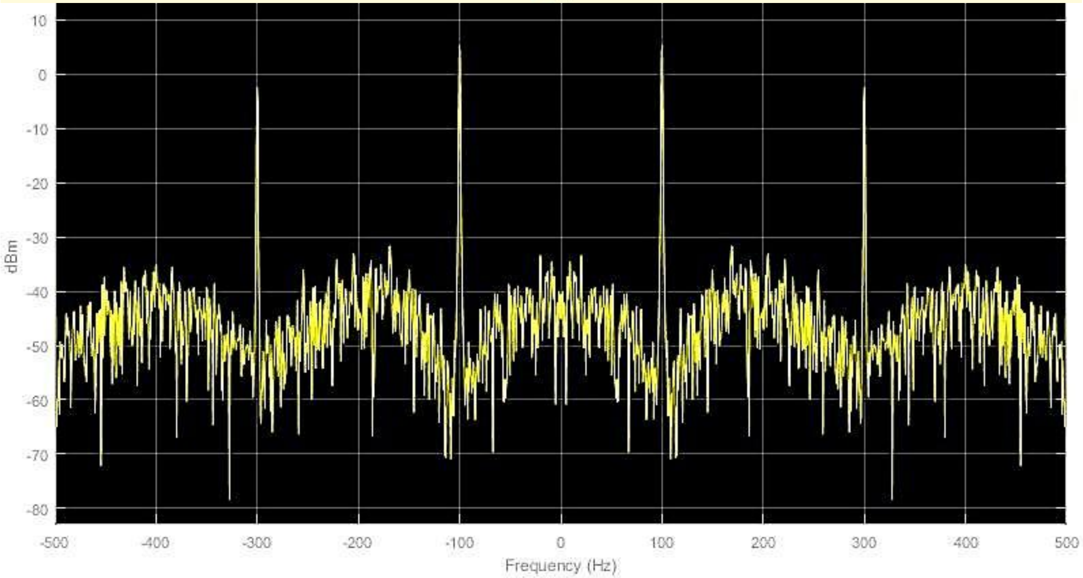
- Covert receiver data recovery:



EXPLOITING POLYGLOT SIGNALS



Original and recovered α

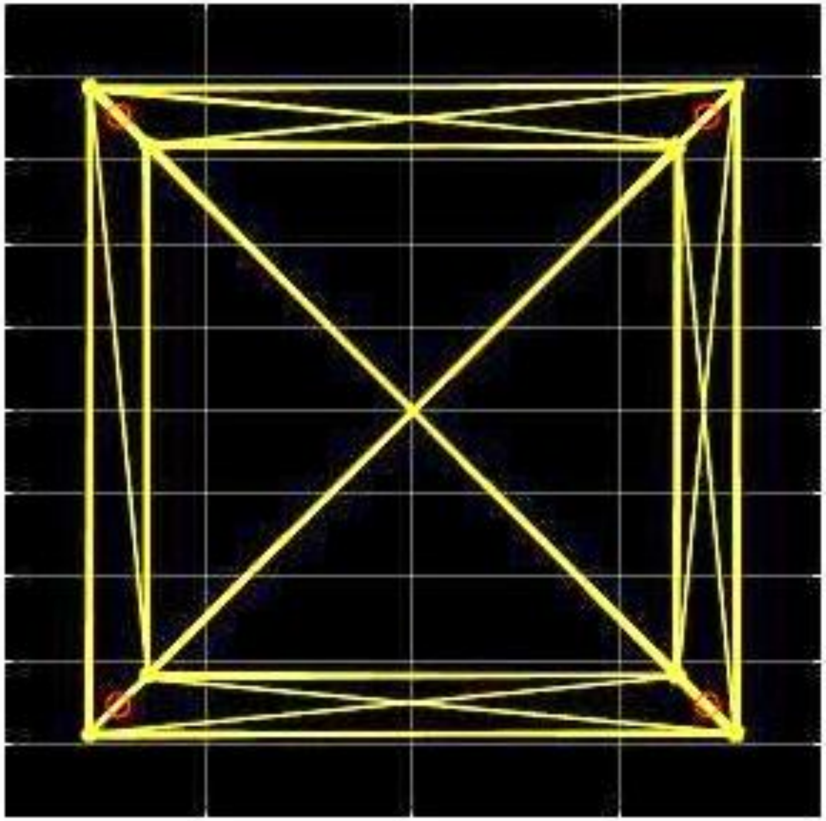


Spectrum of recovered α

EXPLOITING POLYGLOT SIGNALS

- ASK over QPSK
  - Just choose α = β

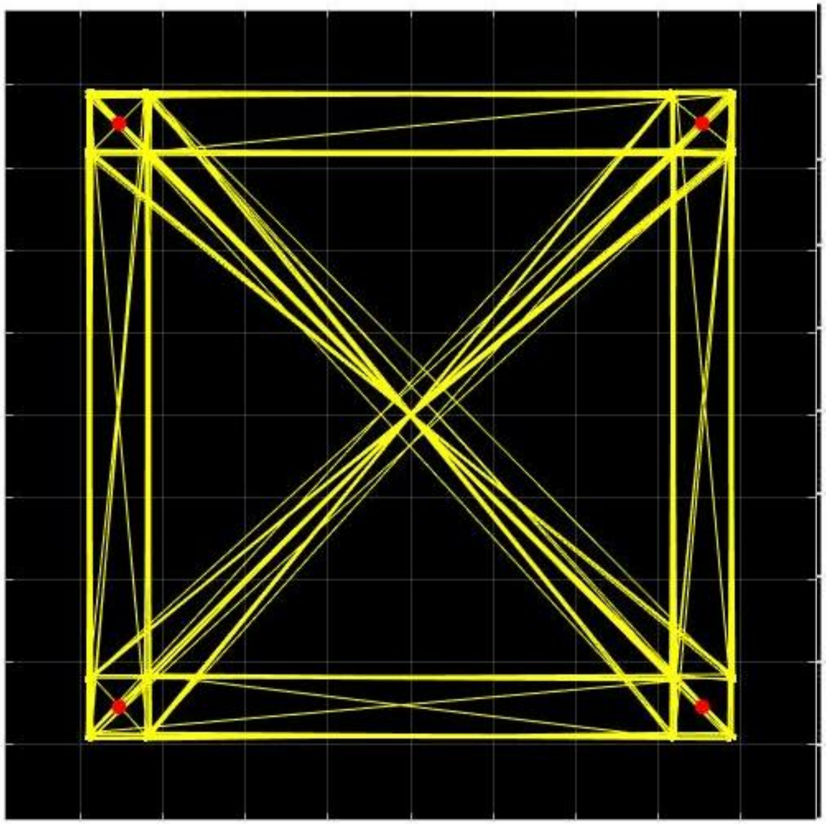
Data bit	Interference sign
0	α>0 and β>0
1	α<0 and β<0



EXPLOITING POLYGLOT SIGNALS

- QPSK over QPSK
  - Just give α and β two possible values

Data	Interference sign
00	α>0 and β>0
01	α>0 and β<0
10	α<0 and β>0
11	α<0 and β<0



Detection techniques

and

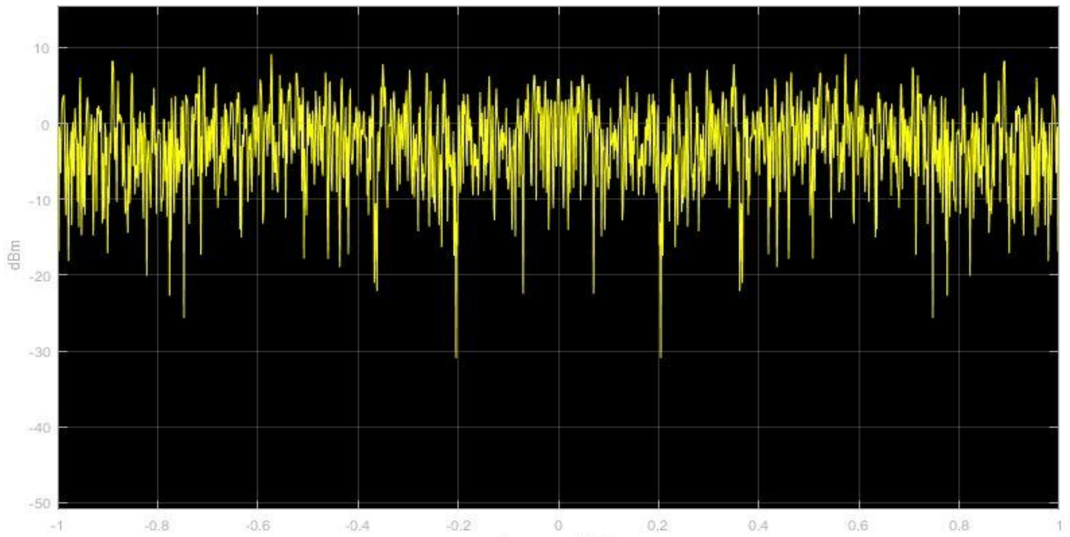
Counter-measures

Advanced signal processing

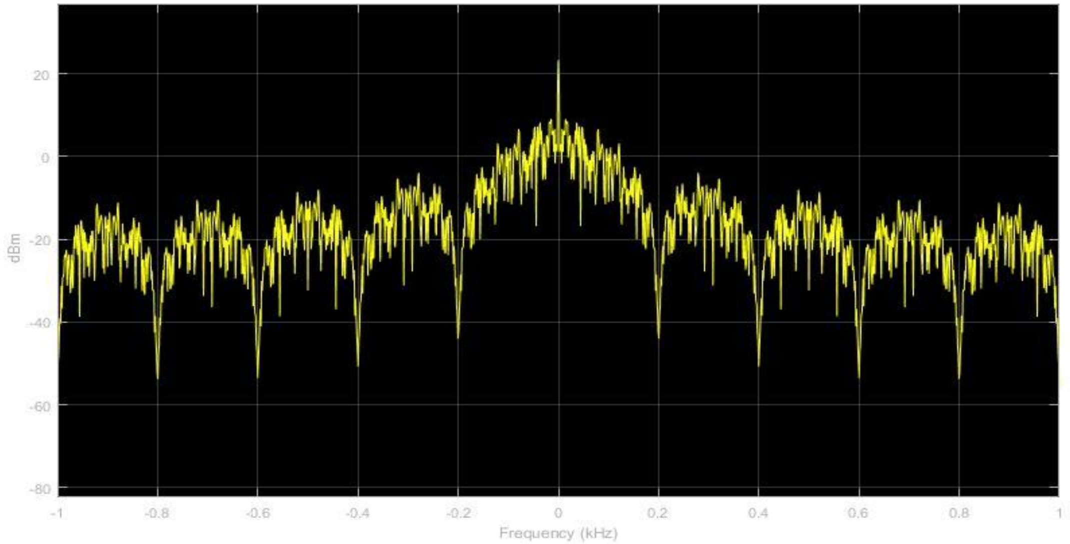
DETECTION TECHNIQUES

- Detection of such data exfiltration
  - Instrumentation of observables
  - Extract features of correction blocks at receiver
    - IQ imbalance correction [6]
      - Measuring the mismatch between parallel section of receivers
      - Fixing coefficient update interval -> limitation for detection !
    - Carrier recovery [7]
      - Phase/ Frequency differences
      - Estimate and compensate differences between RX and TX signals
    - Equalization algorithm [8]
      - Inter-symbol interference suppression -> detecting cyclic symbol modifications
      - Coefficients updated each packet
  - Monitoring of the variation of the correction coefficients

DETECTION TECHNIQUES



Almost random correction



Repetitive correction

Presence of periodic variations

DETECTION TECHNIQUES

- Detection of such data exfiltration
  - Implementation of a dedicated detection system
    - Prospective thoughts
  - Use of signal processing algorithms
    - Wavelet transform: recursive LF vs HF analysis [9]
    - Use blind demodulation techniques [10]
      - <u>Input</u>: IF signal, baseband
      - <u>Features</u> : amplitude, phase, phase difference, frequency, Cyclic Spectral analysis, complex envelop
      - <u>Statistics</u>: histogram, STD,
      - <u>Classifier</u>: maximum likelihood, max correlation, decision tree

COUNTER-MEASURES

- At FPGA level
  - Verify the integrity of the code at startup
  - Prevent code to be modified/rewritten
- At hardware level
  - Design hardened RF front-end
  - Active self test of hardware with control loops
  - Avoid coupling path (follow electronic rules and guidelines)
  - EMC Tests of PCB's with improved EMSEC capabilities
- At fab. level
  - Check PCB's fabrication process
  - Masks validation

Conclusion

CONCLUSION

- Polyglot signals:
  - Interesting phy layer network covert channels
- Attack vector:
  - Software based: can be a malware
  - Hardware based: can be a HW trojan (or interference)
- Not limited to complementary modulations
  - QPSK in QPSK
  - Any modulation should work on any modulation

CONCLUSION

- Channel capacity depends on:
  - Legitimate transmission
  - Covert transmission choices
- We propose detection methods:
  - Use correction blocks
  - Already present in receivers
  - Look for periodicity in correction factors
- Additional ideas:
  - Blind demodulation techniques

FURTHER THOUGHTS

- Explore the hardware based attack
  - We like RF interference
  - And HW trojans
- Covert channel is a hot topic
- Need of new detection systems
- Investigate physical layers against hidden communication
- Implementation of specific processes to avoid/detect HW trojans

References

REFERENCES

[1] Wojciech Mazurczyk et al., “Information Hiding in Communication Networks: Fundamentals, Mechanisms” March 2016, Wiley and Sons, 2016

[2] Peter Pessl, “DRAMA: Exploiting DRAM Addressing for Cross-CPU Attacks”, 25th Usenix Security Symposium 2016, August 2016

[3] E. Tumoian and M. Anikeev, "Network Based Detection of Passive Covert Channels in TCP/IP," The IEEE Conference on Local Computer Networks 30th Anniversary (LCN'05)l, Sydney, NSW, 2005

[4] Travis Goodspeed, Sergey Bratus , “Polyglots and Chimeras in Digital Radio Modes”, Recon 2015, 2015

[5]Ramon Cerda, “Sources of Phase Noise and Jitter in Oscillators”, March 2006, online: http://www.crystek.com/documents/appnotes/SourcesOfPhaseNoiseAndJitterInOscillators.pdf

[6] J. Tubbax et al., "Compensation of IQ imbalance and phase noise in OFDM systems," in IEEE Transactions on Wireless Communications, vol. 4, no. 3, pp. 872-877, May 2005.

[7] Timo Pfau et al., “Hardware-Efficient Coherent Digital Receiver Concept With Feedforward Carrier Recovery for -QAM Constellations”, Journal of lightwave technology, April 15, 2009

[8] L. He and S. A. Kassam, "Convergence analysis of blind equalization algorithms using constellation-matching," in IEEE Transactions on Communications, vol. 56, no. 11, pp. 1765-1768, November 2008.

[9] QI Li-mei et al., “Wavelet Transform Theory and Its Application in Signal Processing”, Journal of University of Electronic Science and Technology of China, March 2008

[10] Octavia A. Dobre et al., “Blind Modulation Classification: A Concept Whose Time Has Come”, Course online material:

http://ntrg.cs.tcd.ie/en/TCD_VT_Course_Cognitive_Radios_and_Networks/Week%204/Readings%20and%20discussion%20Questions/dobre2005.pdf

[11] S. Ghosh, A. Basak and S. Bhunia, "How Secure Are Printed Circuit Boards Against Trojan Attacks?," in IEEE Design & Test, vol. 32, no. 2, pp. 7-16, April 2015.

[12] Chrsitian Krieg, Clifford Wolf, and Axel Jantsch. Malicious LUT: A stealthy FPGA trojan injected and triggered by the design flow. In Proceedings of the International Conference on Computer Aided Design (ICCAD), Austin, Texas, November 2016.

Thank You

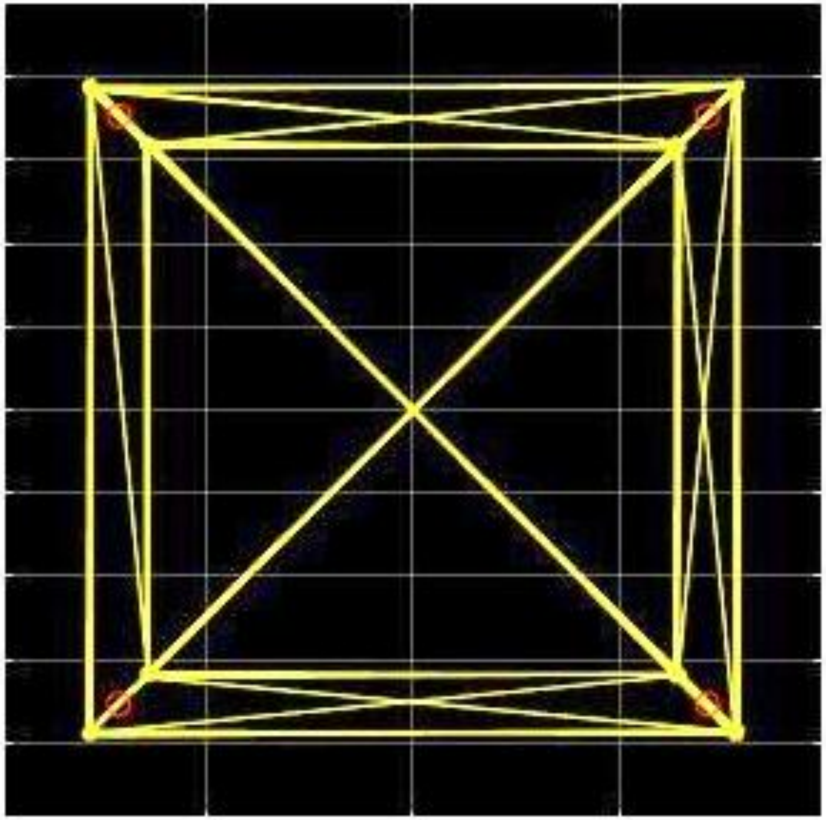
QUESTIONS ?

- Emmanuel COTTAIS, emmanuel.cottais@ssi.gouv.fr
- Chaouki KASMI, chaouki.kasmi@ssi.gouv.fr
- Jose LOPES ESTEVES, jose.lopes-esteves@ssi.gouv.fr

AMPLITUDE-BASED EXFILTRATION

- Simulation results

  - α=±0,1
  - β=±0,1
  - Freq. legit = 500Hz
  - Freq. α = 100Hz
  - Freq. β = 100Hz



Received constellation