

Authentication & Integrity for ADS-B

in a backwards compatible way!



November 10, 2020



Dr.-Ing. Matthias Schäfer | CEO & Founder

SeRo Systems GmbH
Augustastrasse 1
DE-67655 Kaiserslautern

Email: schaefer@sero-systems.de

<https://sero-systems.de>

Made in Germany

Quick Intro: ADS-B Security

2

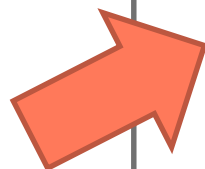
ADS-B is shift from

- Trusted ground-based surveillance to **untrusted** dependent positioning



Different talk, maybe next time!

- Harder-to-fake analog signals to **unprotected** digital broadcast communication

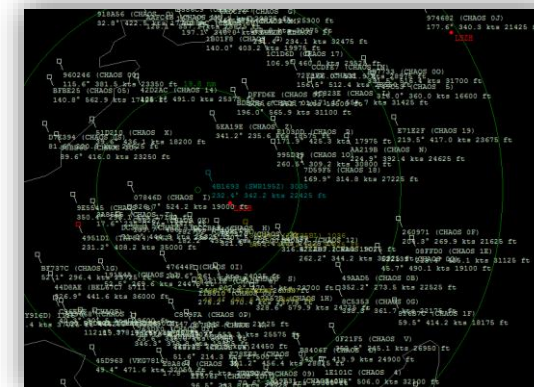


Air segment:

- GPS spoofing + jamming
- ADS-B spoofing + jamming
 - ADS-B In
 - ACAS X
- *Over-interrogations (Mode S)*

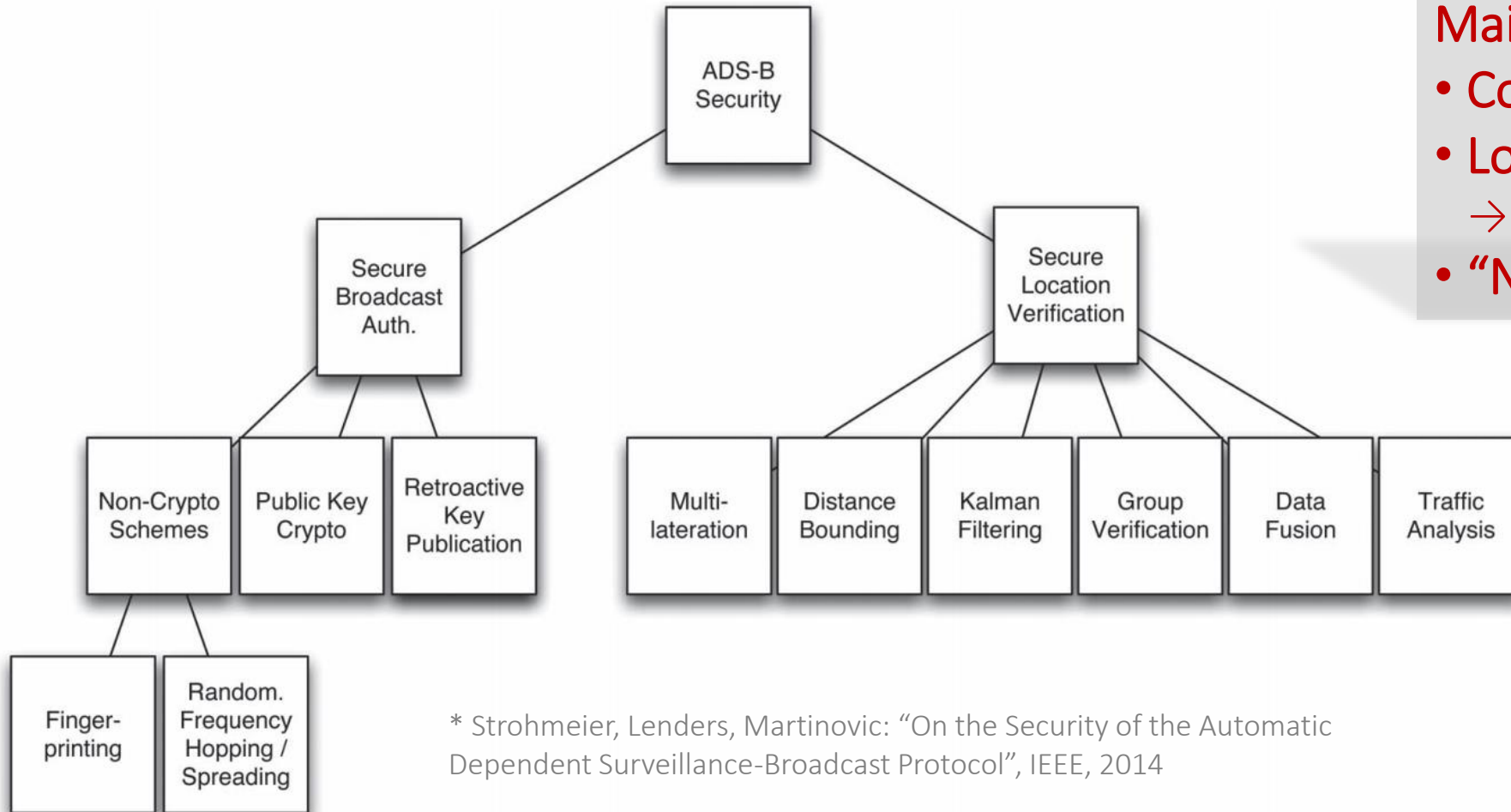
Ground segment:

- GPS spoofing + jamming
- ADS-B spoofing + jamming
 - Ghost targets
 - Denial of service
 - Data modification
- *Frequency congestion / interference*



There are many solutions, but...

3



Main enemies:

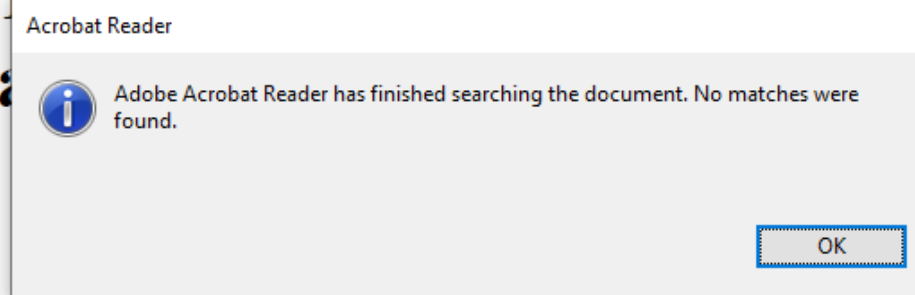
- Cost pressure
- Long life cycles of tech
→ *Backwards compatibility*
- “Need” for guarantees

* Strohmeier, Lenders, Martinovic: “On the Security of the Automatic Dependent Surveillance-Broadcast Protocol”, IEEE, 2014

Still possible to add security to ADS-B?

4

Minimum Operational Performance Standards (MOPS) for 1090 MHz Extended Squitter Automatic Dependent Surveillance – Broadcast (ADS-B) –

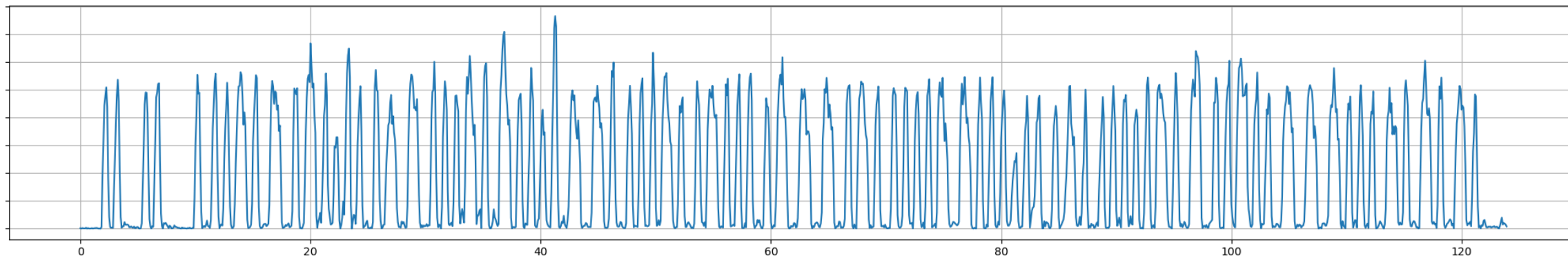


(Corrigendum 1, Appendix W, integrated and highlighted)

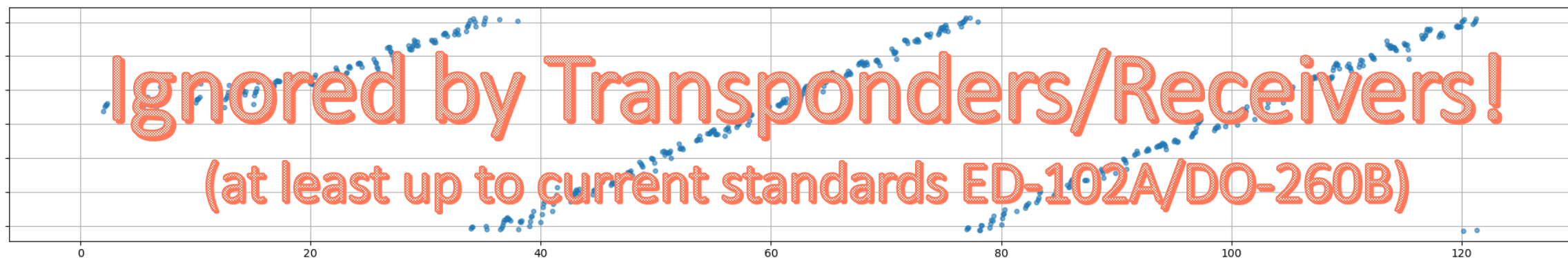
1090ES ADS-B Signals

5

Pulse Position Modulation:



The Signal Phase:



→ can be used to transmit *additional information* with each ADS-B signal!

- Part of the current draft of next ADS-B version:

2.2.3.5

(Optional) Phase Overlay Capability

The optional Phase Overlay capability consists of phase modulating the pulses of a standard 1090ES message. This phase modulation of the PPM signal is used to encode data in addition to the data conveyed in the 112 bit 1090ES message. The following sections define the encoding of the phase data and basic message structure.

- Transparent to legacy receivers (backwards compatible!)
 - Phase overlay has (almost) no effect on PPM modulation
- Unique opportunity:
Use PO to add security to ADS-B in a backwards compatible way!

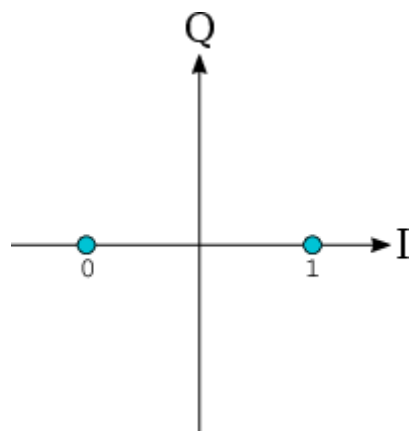
Q1: What's the net **capacity** that can be provided with the phase overlay under **realistic conditions**?

Q2: How can we use this additional capacity to provide **security services** to ADS-B users?

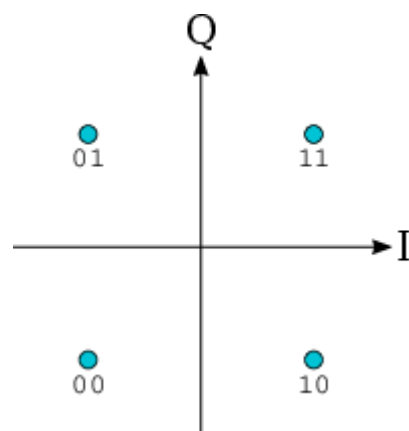
Net Capacity of Phase Overlay

8

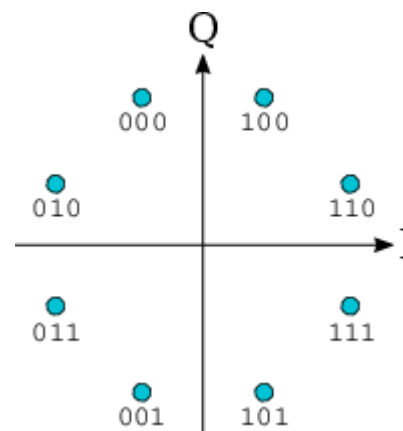
- What is the optimal PSK configuration?



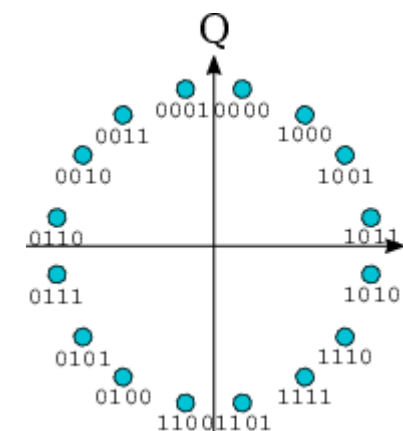
BPSK
($M = 2$)



QPSK
($M = 4$)



8PSK
($M = 8$)



16PSK
($M = 16$)

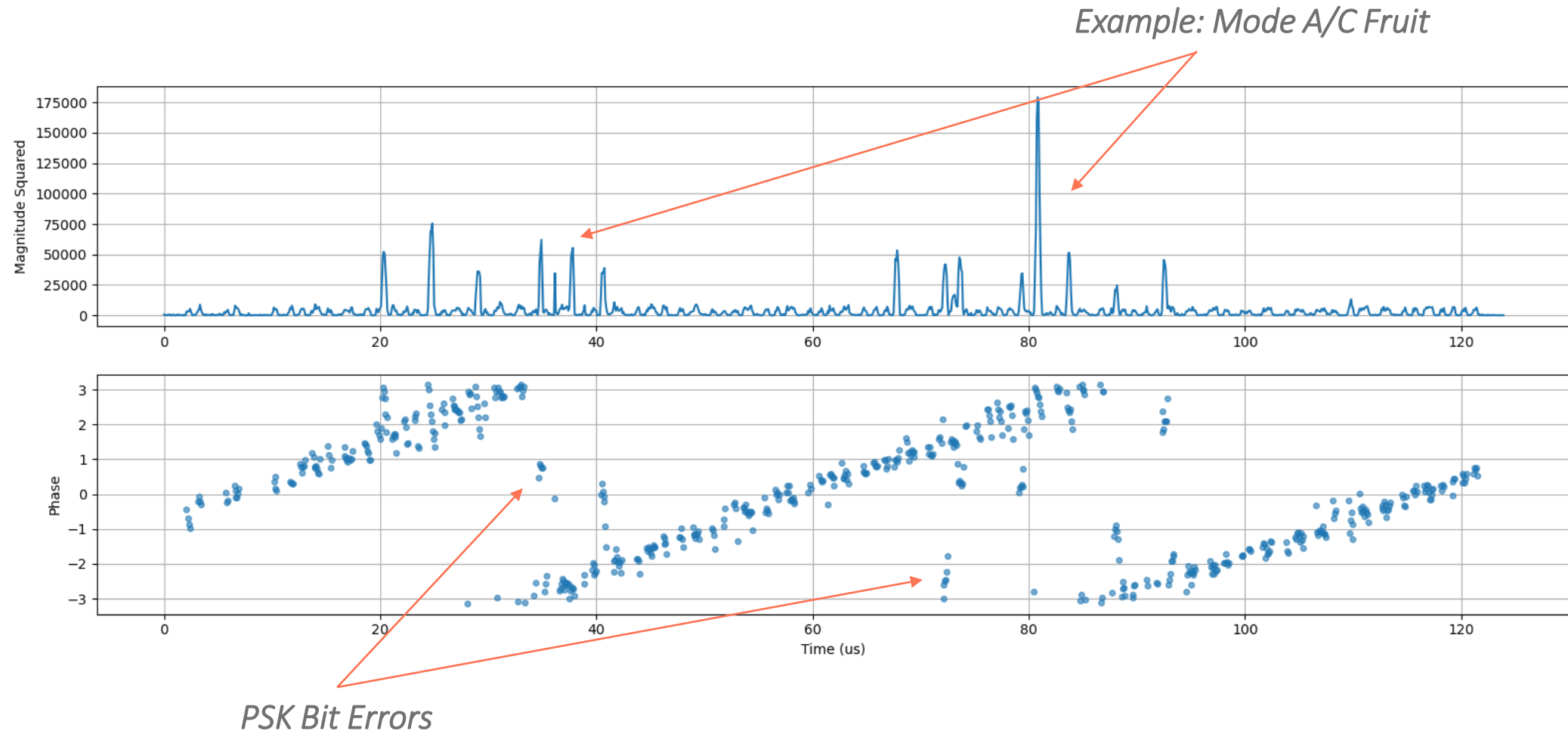
More bits per symbol but also more prone to errors

NET CAPACITY

Net Capacity of Phase Overlay

10

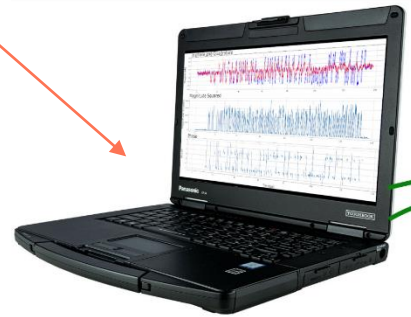
- Bit errors in a noisy (realistic) environment?



Evaluation Setup

11

- generates reference signal
- can mix in noise from recordings
- receives frames from GRX and counts symbol/bit errors



Controller



Ettus USRP X300



Combiner

1090 MHz
Antenna

- 1090 MHz receiver
- provides 12 bit I/Q data @ 12 MHz



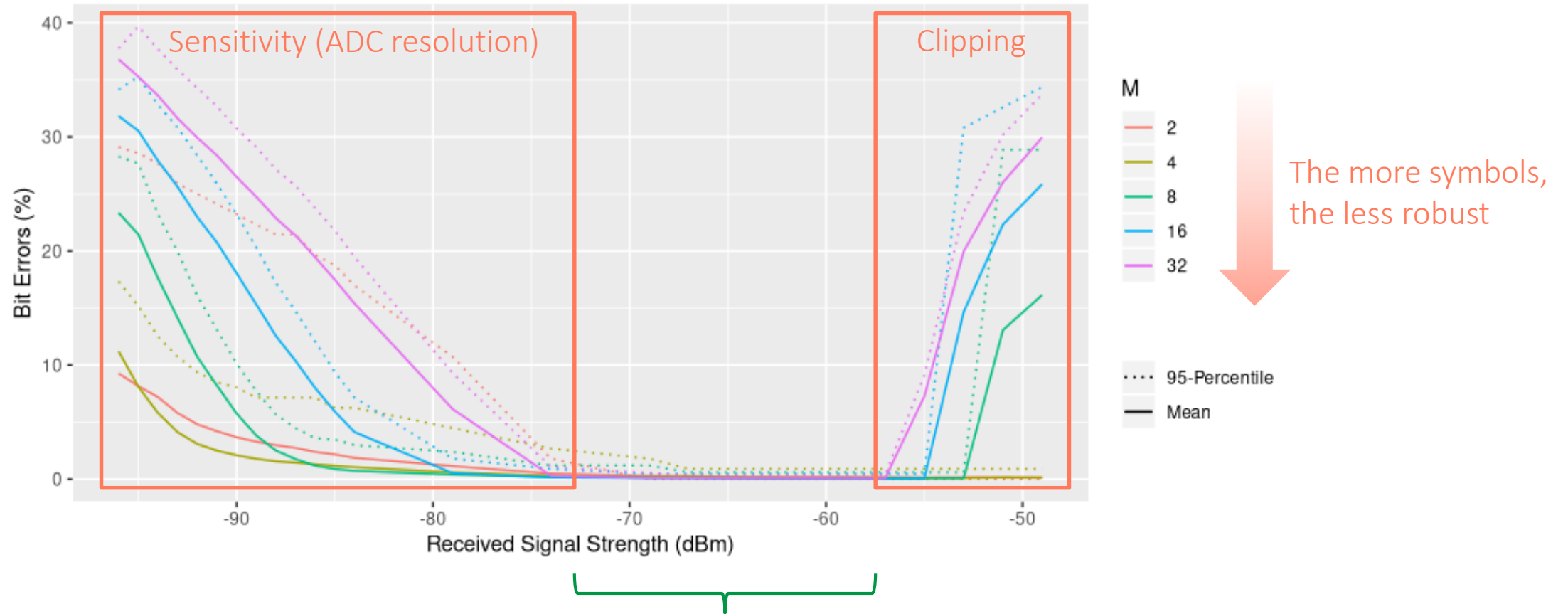
SeRo Systems GRX1090

- ADS-B transmitter (PPM + M-PSK)
- Noise/Interference transmitter

- optional real-time noise injection

Bit Error Rate vs. SNR

12



dynamic range of phase overlay narrower than that of PPM

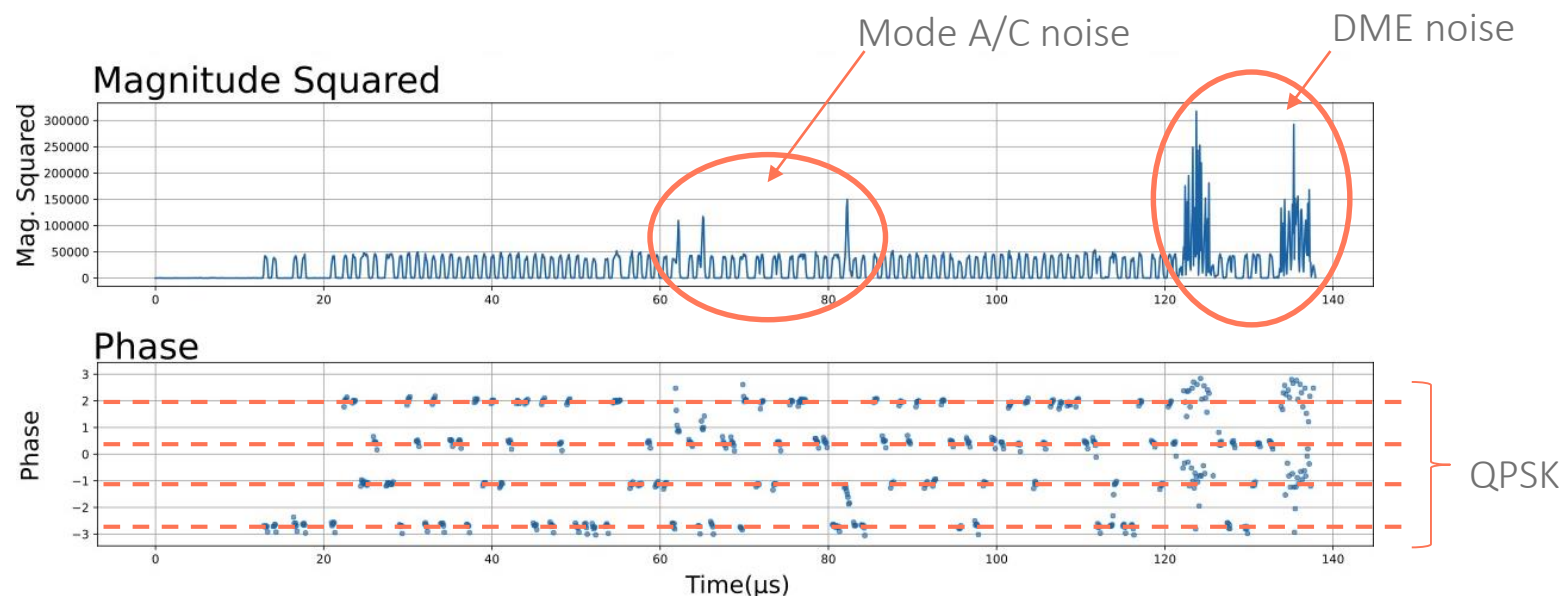
Expected Performance in the Real World

13

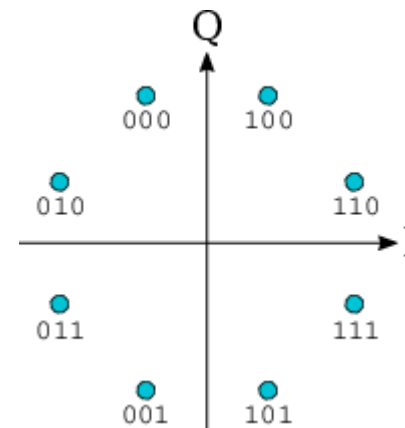
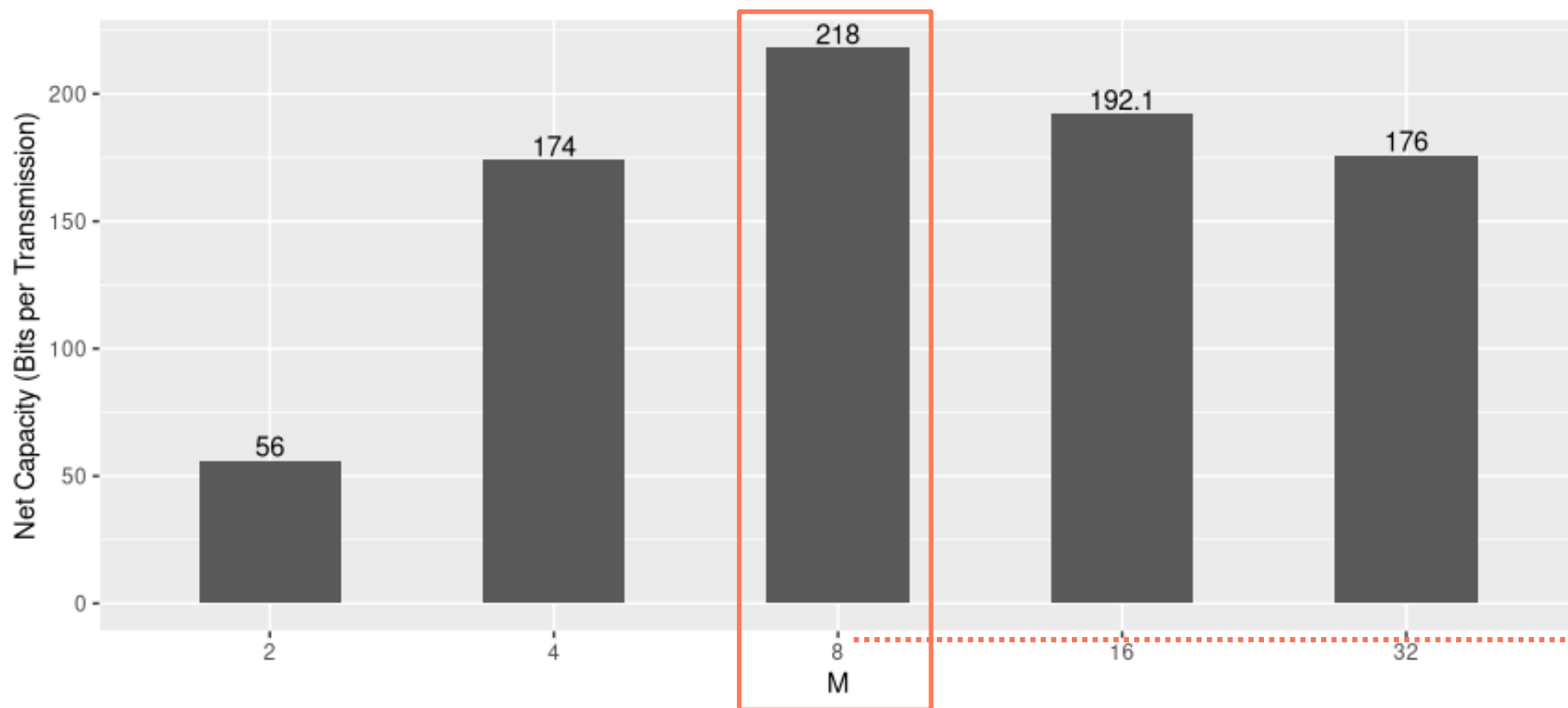
- Assumptions:
 - Transponder transmits at 56 dBm
 - Free-space path loss over 250 NM
 - Mixed in RF recording from FRA receiver (~200 aircraft)
 - No carrier frequency offset / Doppler shift

- ECC added for:

95% successful reception



- Net capacity = $\log_2(M)$ bits per PPM bit - ECC bits (RS coded)

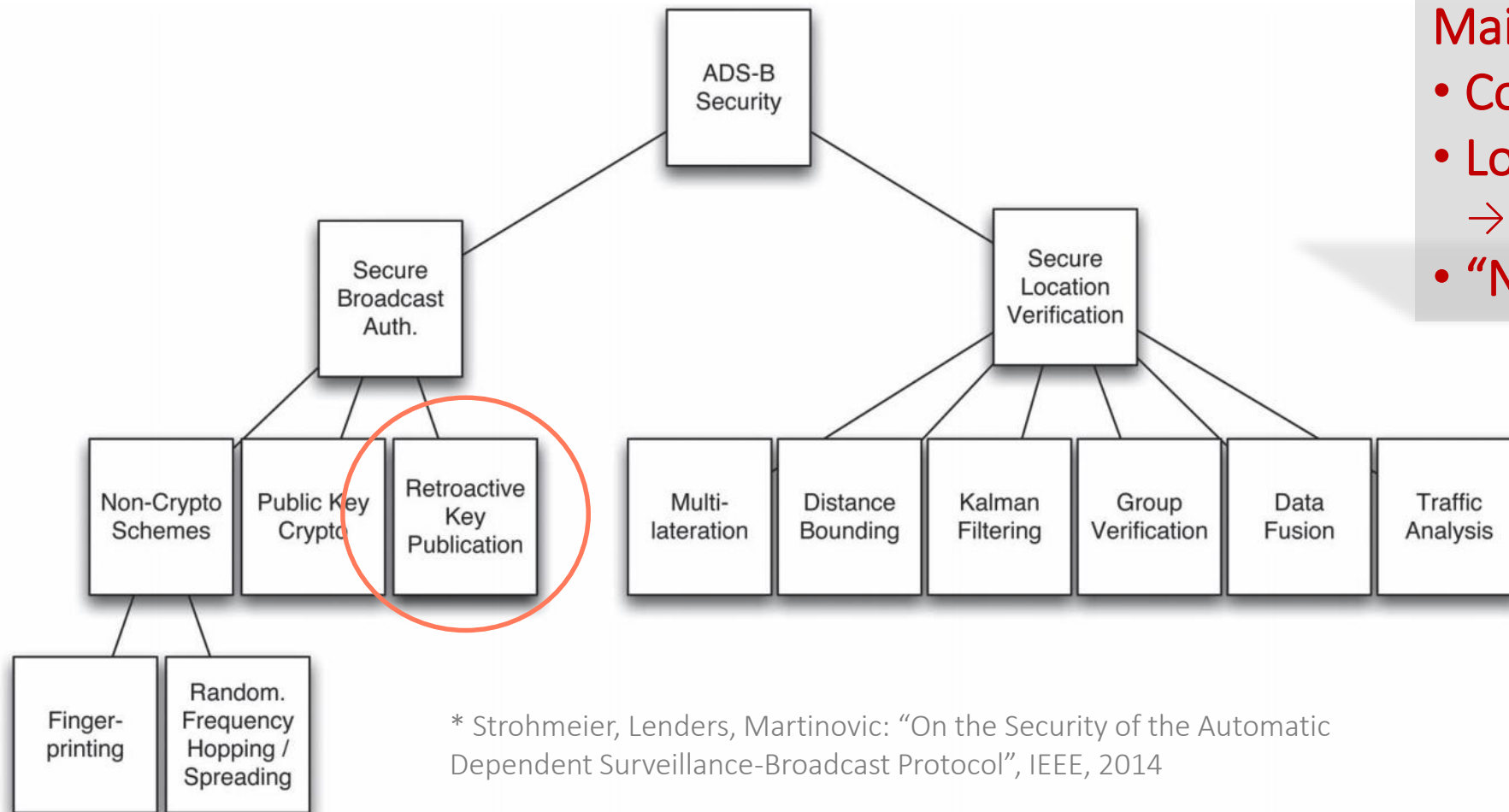


- Very close to current draft of ADS-B v3: 204 data bits

SECURITY

How to use these 218 bits?

16



Main enemies:

- Cost pressure
- Long life cycles of tech
→ *Backwards compatibility*
- “Need” for guarantees

* Strohmeier, Lenders, Martinovic: “On the Security of the Automatic Dependent Surveillance-Broadcast Protocol”, IEEE, 2014

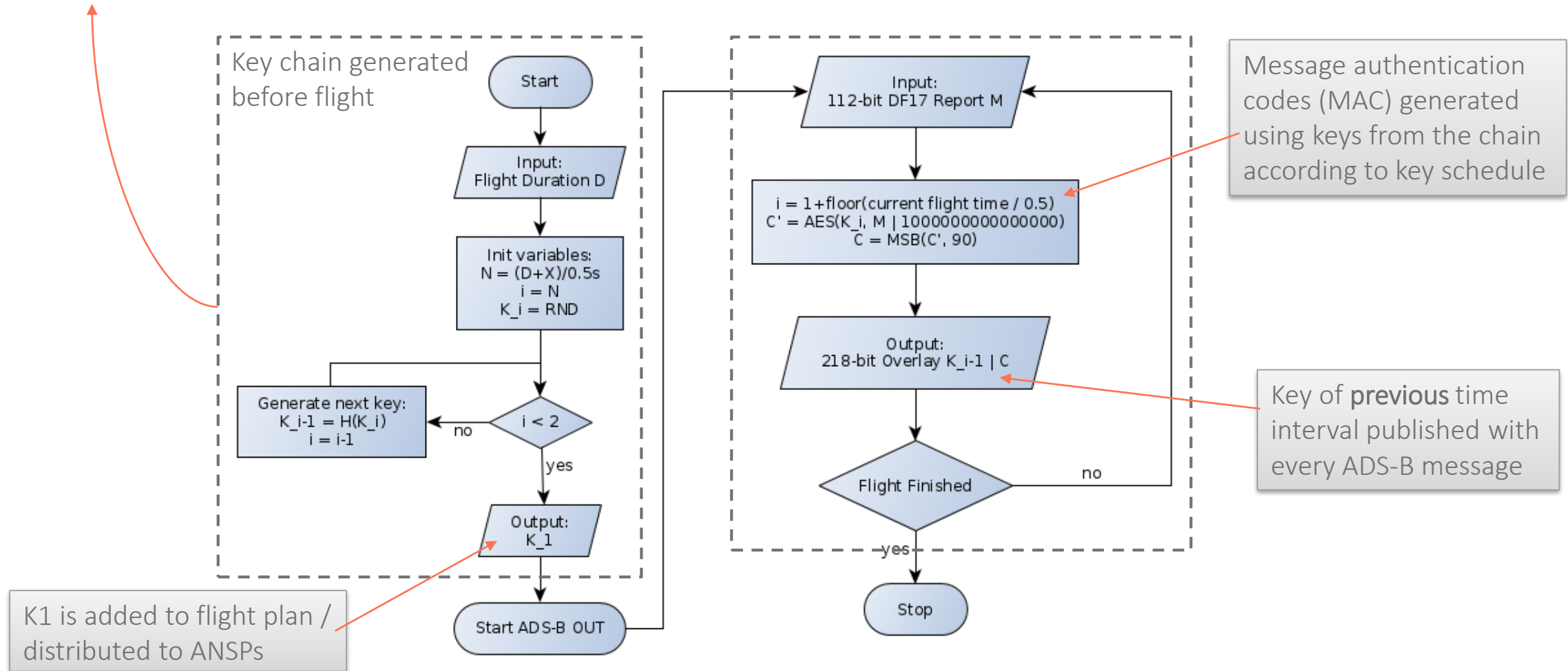
- Candidate protocol:



- Requires:
 - light time synchronization between transponder and receiver(s)
 - pre-calculated chain of keys linked with secure(!) one-way function
- Several variants of TESLA for ADS-B proposed in the literature

$$K_N \xrightarrow{F} K_{N-1} \xrightarrow{F} \dots \xrightarrow{F} K_i \xrightarrow{F} K_{i-1} \xrightarrow{F} \dots \xrightarrow{F} K_2 \xrightarrow{F} K_1$$

0.5s key disclosure, 6h flight \rightarrow 0.7 Mbyte keychain



- Expected net capacity gain through phase overlay is **218 bits**
 - actually 204 if implemented according to current ED-102B/DO-206C draft
- Additional capacity can/should be used to **improve security**
 - Backwards compatible 😊
 - But: update of transponder hardware required ☹️
- Would not solve all ADS-B security problems, but is giant leap forward
 - Only authentication of origin of information
 - Correctness of information itself not guaranteed