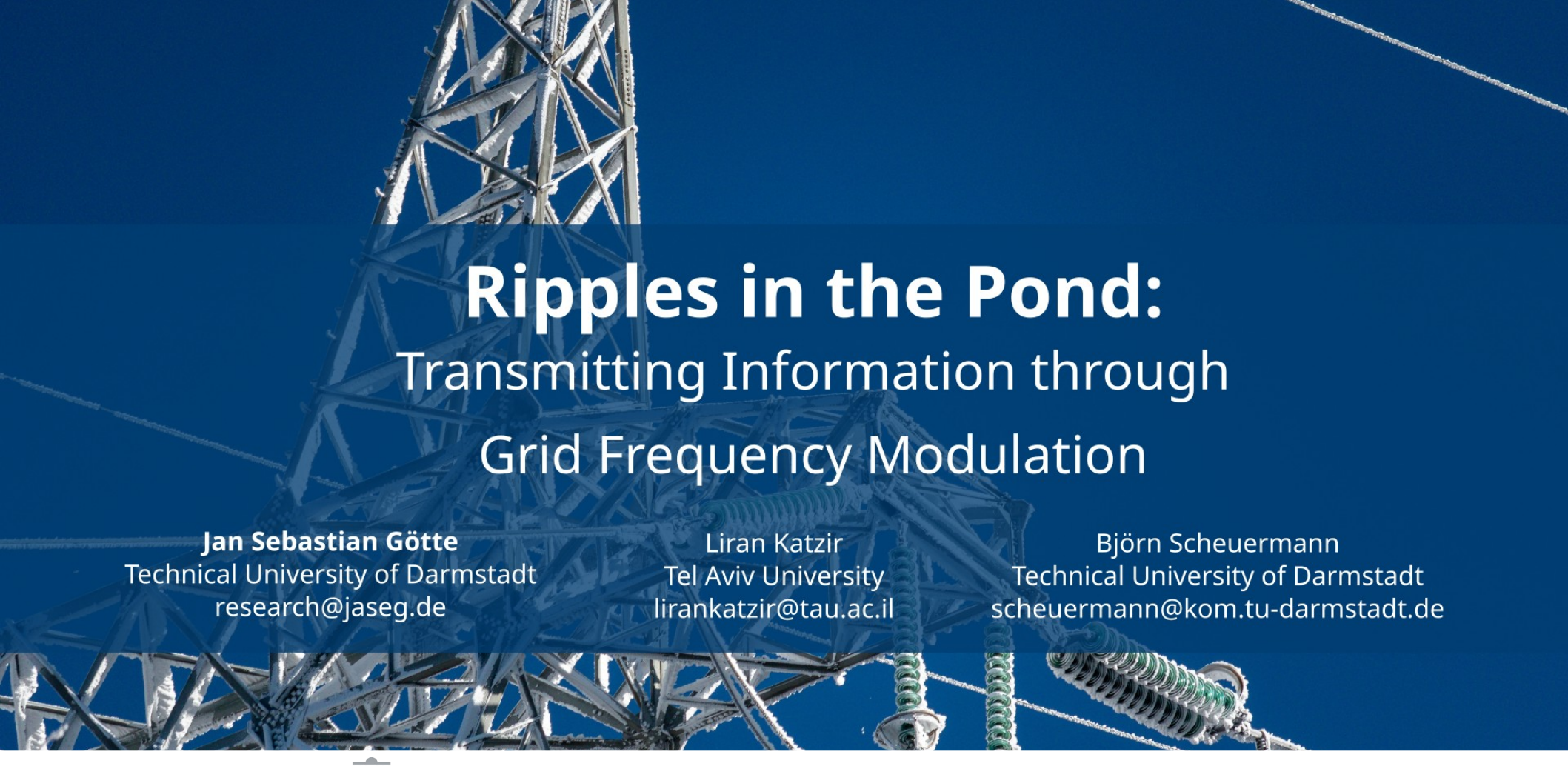


Ripples in the Pond:
Transmitting Information through Grid Frequency Modulation

Jan Sebastian Götte
Technical University of Darmstadt
research@jaseg.de

Liran Katzir
Tel Aviv University
lirankatzir@tau.ac.il

Björn Scheuermann
Technical University of Darmstadt
scheuermann@kom.tu-darmstadt.de

TECHNISCHE UNIVERSITÄT DARMSTADT

Alexander von Humboldt
INSTITUT FÜR INTERNET UND GESELLSCHAFT

LOEWE
Exzellente Forschung für Hessens Zukunft

emergenCITY

The Structure of the Electrical Grid

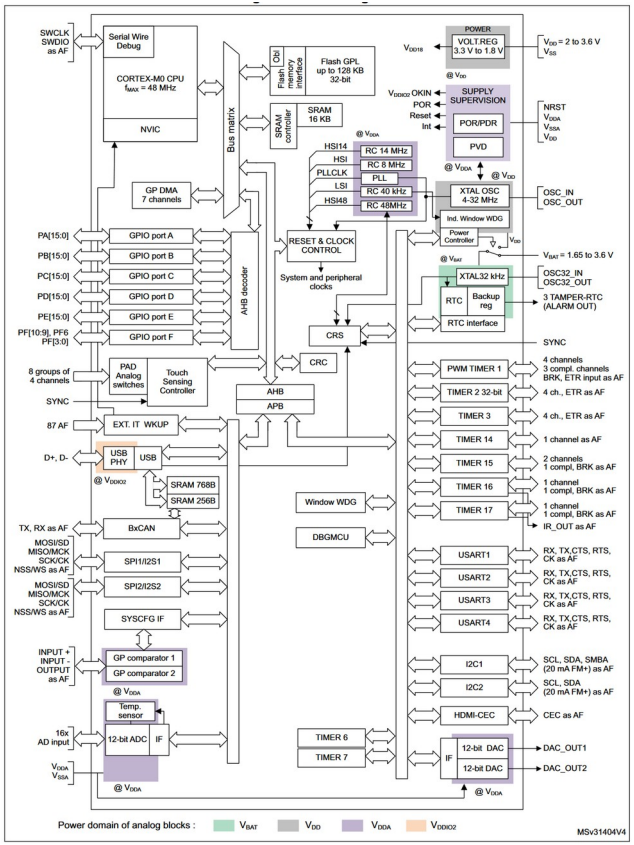
- Generators
- Transmission Lines
- Switchgear
- Transformers
- Loads

Attack Scenarios in the IoT era

- **An attacker can switch many loads at once to attack grid stability**
  - IoT devices
  - Smart Meters with remote switch to disconnect “delinquent” customers
- **Attacks scale, defense & recovery are expensive**

Hardware and Firmware are Complex

- **Complex HW/FW bundles are integrated**
  - Most common: radio modems
  - Also: AI accelerators
  - Also: Complex sensors (e.g. camera/barcode)
- **Firmware is *hard***
  - Smart Meter Vendor Landis+Gyr spend 36% of their R&D budget on code
- **Nobody is good at it**
  - Everybody fails: Apple, Samsung, Microsoft, Google
  - µCs lack many modern security features

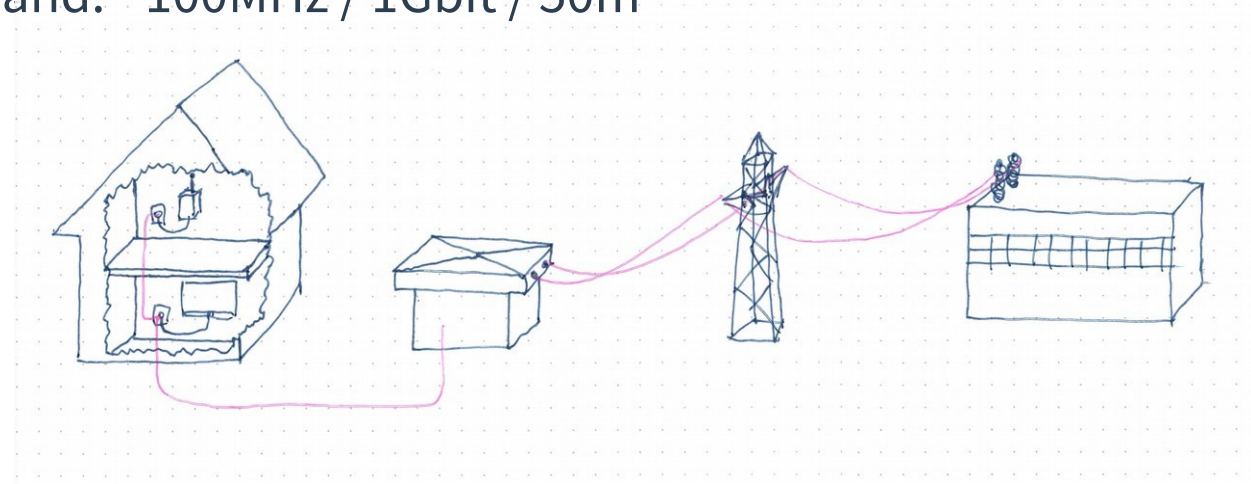


The Safety Reset

- **Triggerable over broadcast channel**
  - avoid 1-to-1 communication network overload in case of emergency
- **Hard firmware reset through JTAG / direct SPI flashing**
  - Do not trust either existing firmware or bootloader
- **Golden image: Known-good, all network interfaces disabled**
  - → True Fail-Safe

Powerline Communication (PLC)

- **Transmit at higher frequencies through grid wiring**
  - Classic demand-side response: ~300Hz / 10Bd / 50km
  - Narrowband: ~100kHz / 100kBd / 1000m
  - Broadband: ~100MHz / 1Gbit / 50m



The Hack: Grid Frequency Modulation (GFM)

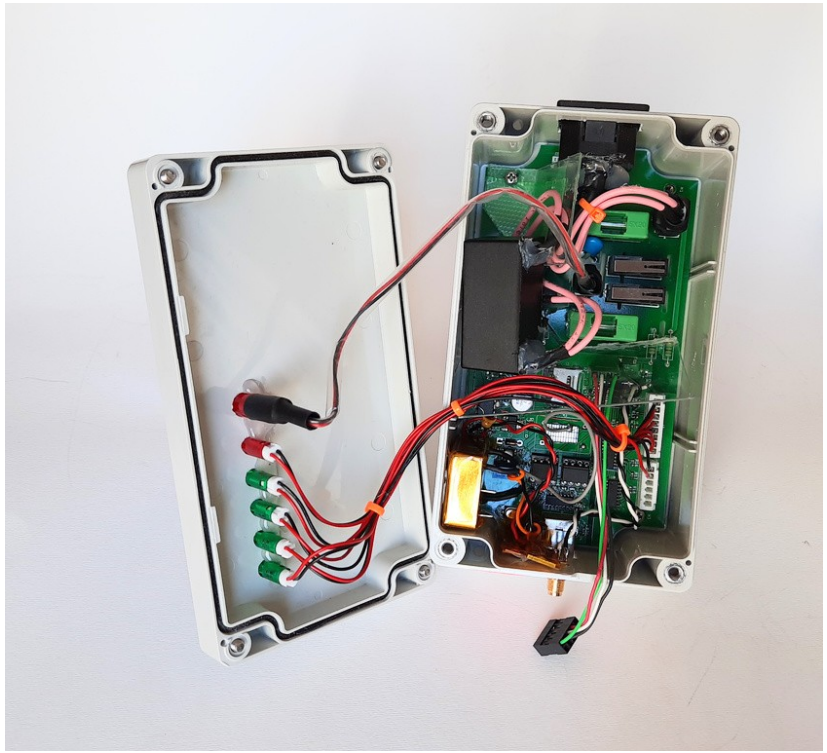
➧**Conventional communication channels do not work for us: Too expensive at scale or not reliable under attacks**

- **Grid frequency can be used for communication**
- **Grid frequency is load balance dependent**
  - Generators/Transmission lines act like spring-coupled oscillators
- **Apply a large load, f drops**
- **Modulate a large load to control Δf**

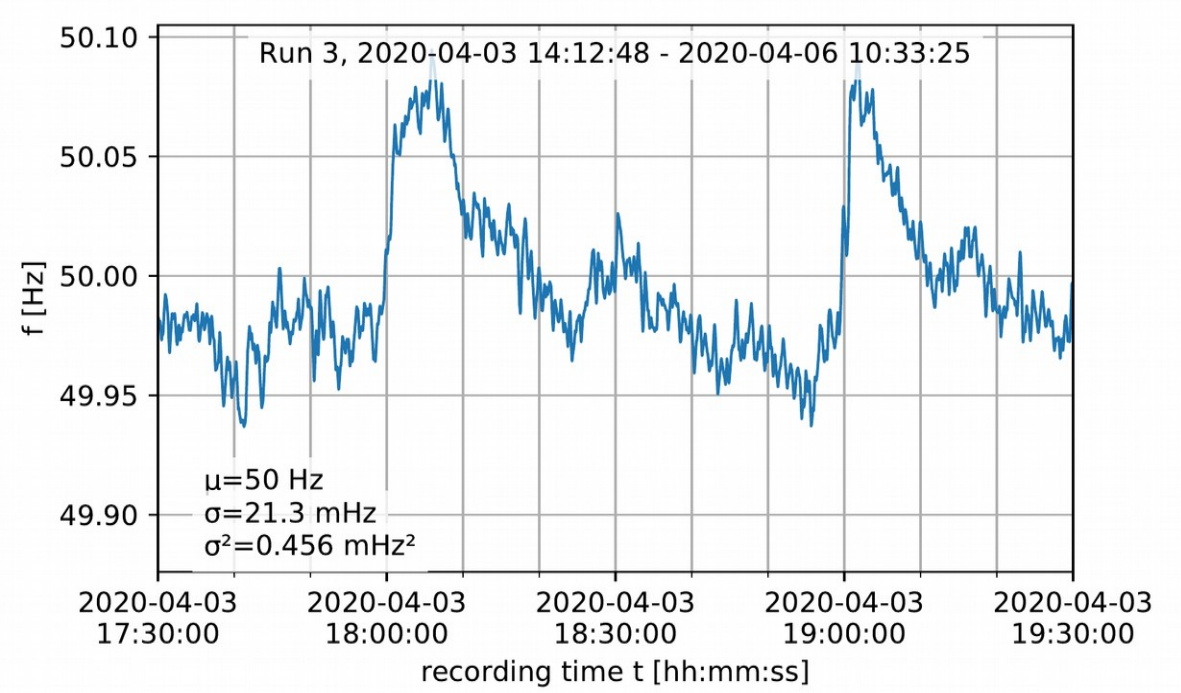
Channel properties

- We know grid frequency is a noisy variable
- Since f=50Hz, any modulation will be *extremely* narrowband
- Grid frequency is equal in all parts of the grid, but has a phase delay
- Now: Characterize noise characteristics
- Later: Characterize channel transmission characteristics through experiments

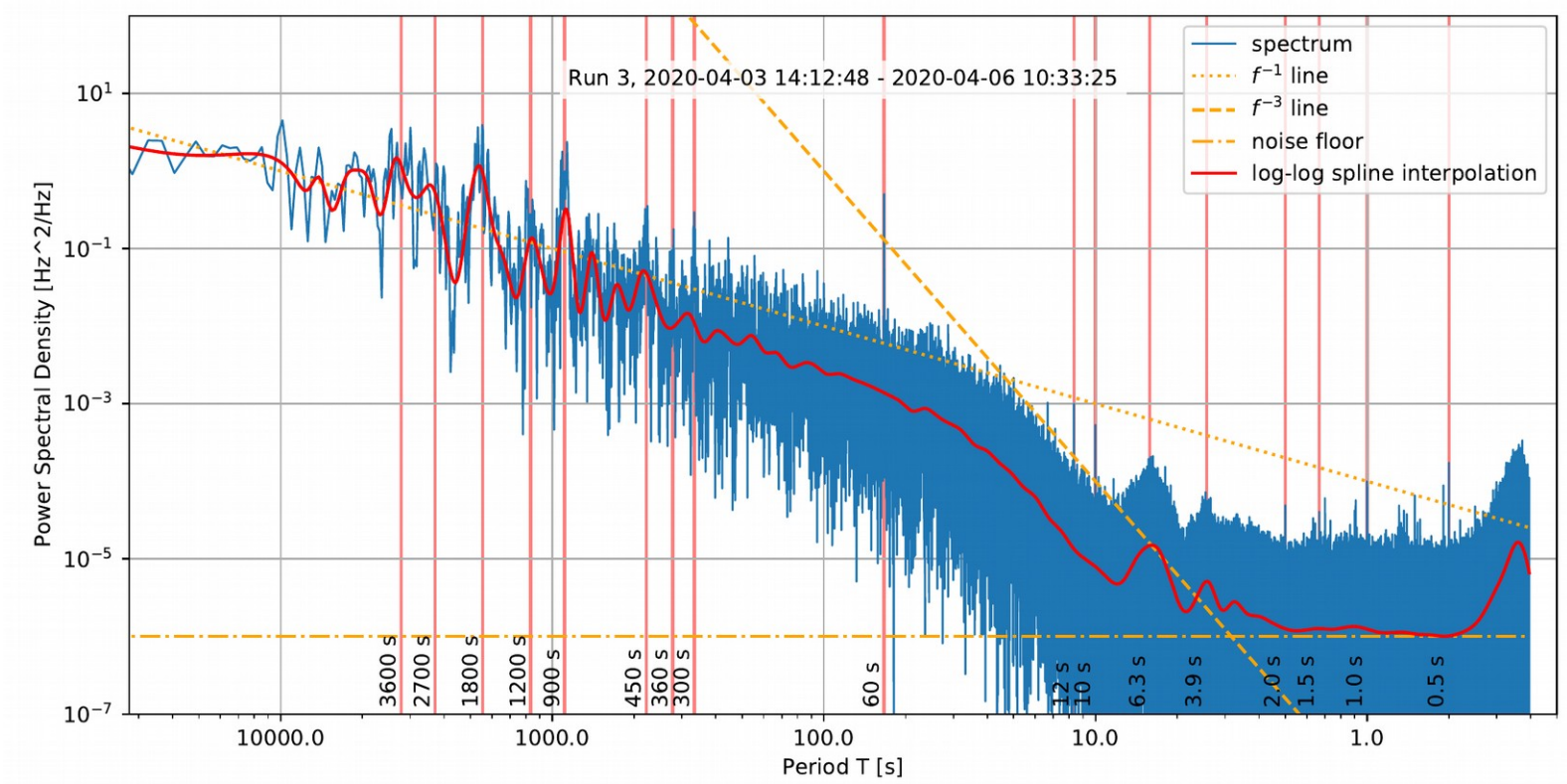
Characterizing Frequency Noise from Local Measurements



Frequency Noise Measurements



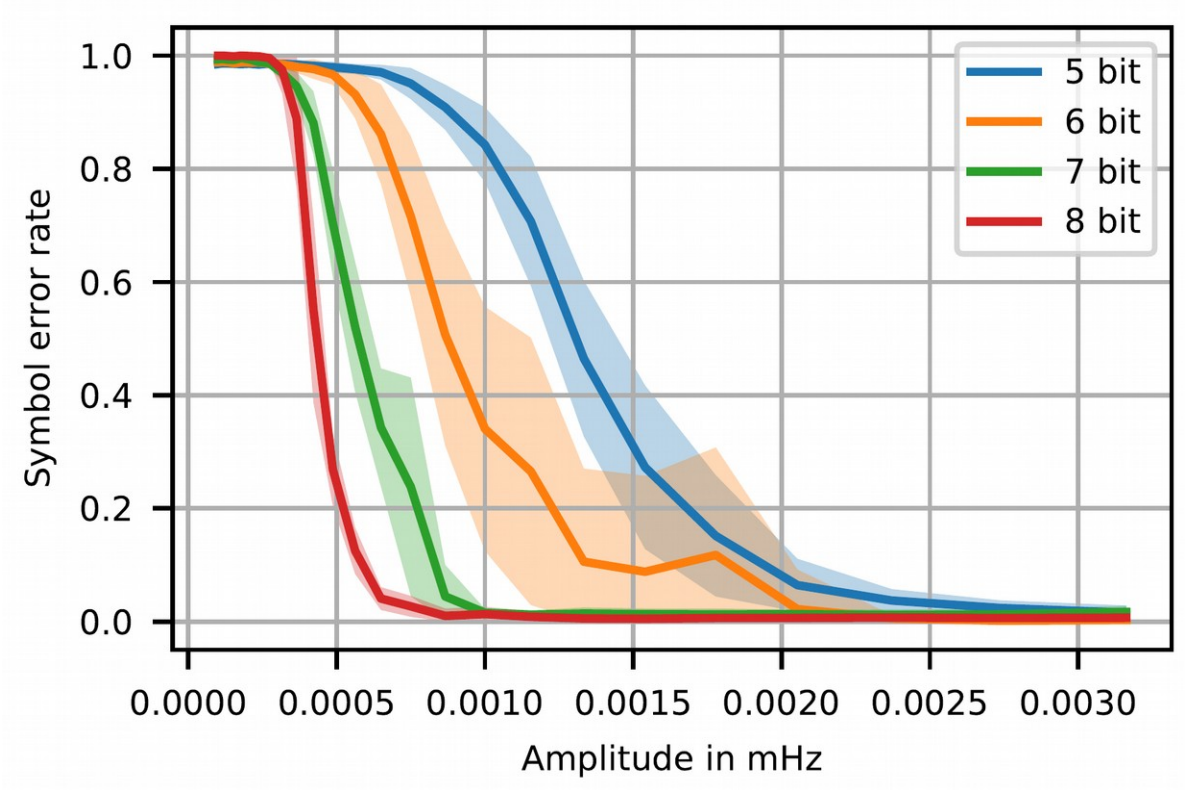
Frequency Noise PSD



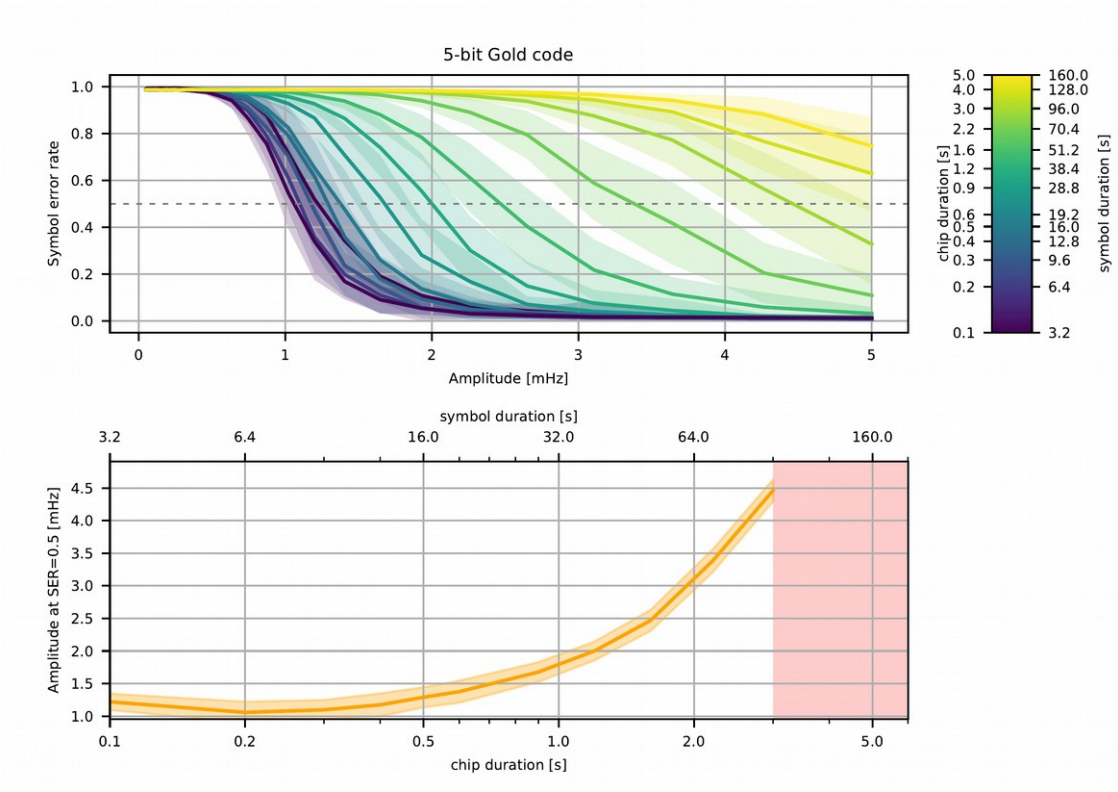
Modulation

- Poor SNR makes UWB necessary
- Limited CPU; Can’t be too complex → DSSS is a good compromise
- Long integration times (minutes) are necessary
- Accurate frequency measurement is a limiting factor

DSSS Modulation Parameters: Bit depth



DSSS Modulation Parameters: Chip duration



Chosen Modulation Parameters

- **5 bit** Gold Code
- **1s chip** duration
  → 31s symbol duration

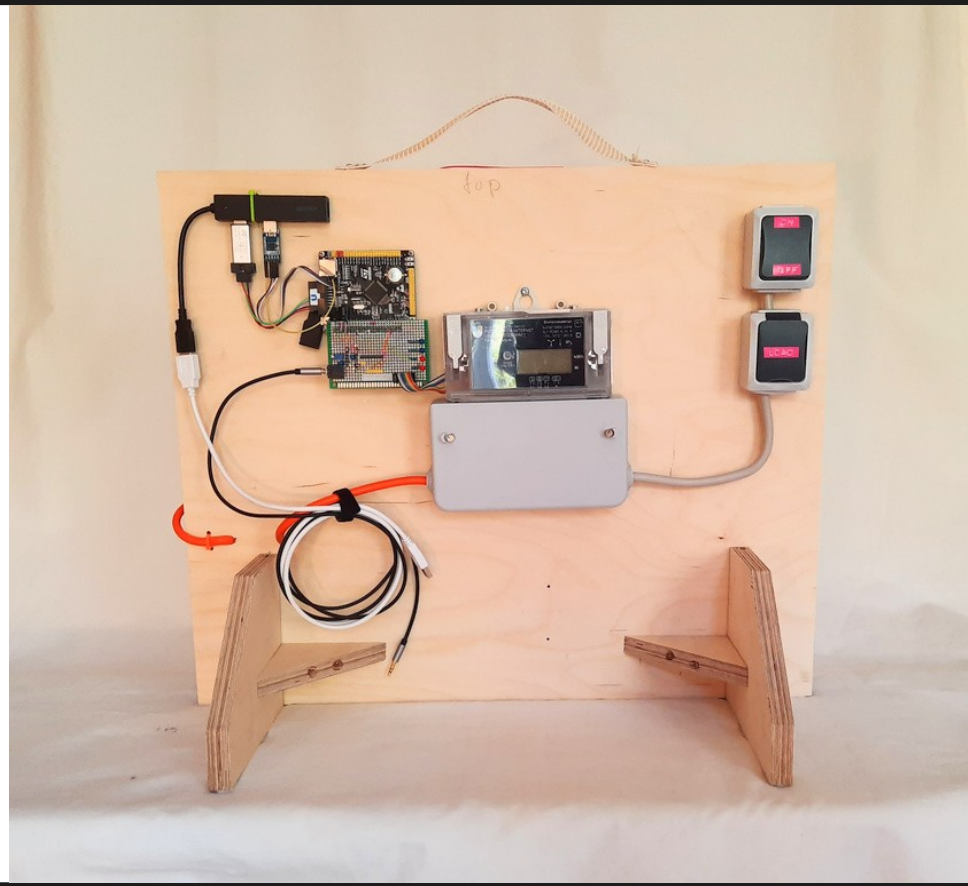
Cryptography & Error Correction

- Error correction required to make up for poor SNR
- Non-standard threat model allows very short cryptographic message size
- A custom solution is justifiable to save transmission bandwidth
- Simply use pre-computed hash chain (similar to Lamport signature)
  - Reset controller knows last hash
  - Reset authority knows first hash
  - RA reveals one previous hash to trigger reset

    → Small transmission size, trivial

Results

- **Safety reset is a viable last-resort mitigation for large-scale firmware attacks**
- **GFM is viable even during an attack**
- **7.5 s/bit shown in experiments with simulated voltage waveform on real hardware w/ < 64 kB code, 1 kSp/s ADC**
  - ~15min for complete trigger




Q&A

Signal Processing Chain

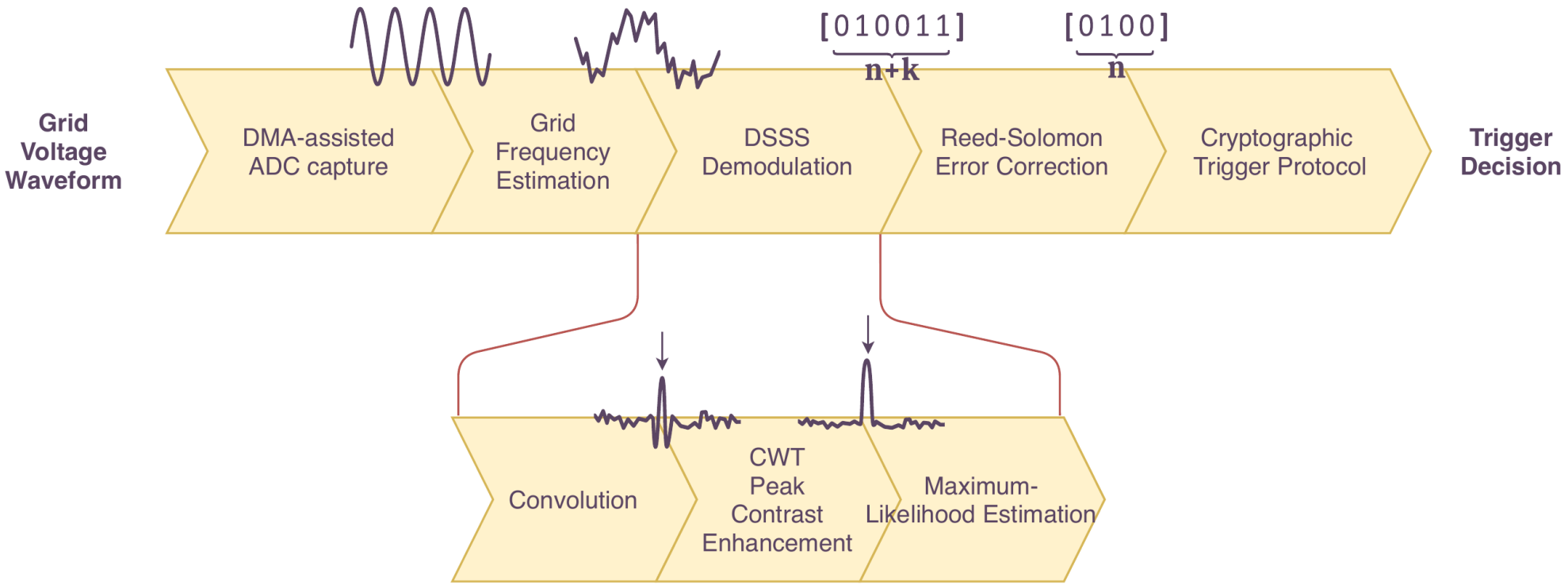


Image Sources (1/3)

1	Title Slide	Jerry Zhang: low-angle photography of electric tower under blue sky during daytime
2	Fundamentals	Atul Vinayak: black escalator in a tunnel
3	The Structure of the Electrical Grid	Iqram-O-dowla Shawon: white and gray industrial machine
3	The Structure of the Electrical Grid	ETA+: gray metal fence on green grass field during daytime
3	The Structure of the Electrical Grid	Jan Huber: green trees near snow covered mountain during daytime
3	The Structure of the Electrical Grid	Dirty Scan: Shoreham Power Station
3	The Structure of the Electrical Grid	Tyler Nix: person holding silver stainless steel electric kettle
4	Smart Meter Functionality	David Edelstein: Maynard Meters
5	Smart Meter Technology	Original work
6	Smart Metering Incentives	Ed Harvey: person holding black and silver smartphone
7	Endpoint Safety & Security	Atul Vinayak: text
8	Security in the Distribution Grid	DynamicWang: woman in gray and white checked overalls standing on metal bars
9	Hardware and Firmware are Complex	ST Microelectronics: STM32F072 datasheet
10	The State of Firmware Security	JESHOOTS.COM: woman biting pencil while sitting on chair in front of computer during daytime
11	The Safety Reset	Atul Vinayak: person holding clear umbrella across city building during nighttime
12	The Safety Reset	N/A
13	Communication along the Grid	Nicholas Bartos: gray transmission tower during daytime
14	Powerline Communication (PLC)	Original work

Image Sources (2/3)

15	Landline IP	Quino Al: black corded telephone
16	Wireless IP	MILKOVÍ: white and red satellite tower
17	Short-range wireless	Erik Mclean: Person holding black remote control
18	The Hack: Grid Frequency Modulation (GFM)	Fré Sonneveld: black transmission towers under green sky
19	From Grid Frequency to a Reliable Channel	Christian Kaindl: brown wooden ruler
20	Channel properties	N/A
21	Characterizing Frequency Noise from Local Measurements	Original work
22	Frequency Measurement Parameters	N/A
23	Frequency Measurement Accuracy	Original work
24	Frequency Noise Measurements	Original work
25	Frequency Noise PSD	Original work
26	Modulation	N/A
27	DSSS Modulation Parameters: Bit depth	Original work
28	DSSS Modulation Parameters: Detection threshold	Original work
29	DSSS Modulation Parameters: Chip duration	Original work
30	Chosen Modulation Parameters	Keila Hötzel: white notebook
31	Error Correction	N/A
32	Cryptography	Photos Hobby: Light

Image Sources (3/3)

33	Testing & Validation	StellrWeb: white Canon cash register
34	Extensive simulations in Jupyter	N/A
35	Host testing of instrumented firmware	N/A
36	Demonstrator experiments	Original work
37	Synthetic Signal Quality	Original work
38	Conclusion	Markus Spiske: yellow electric sign
39	Theoretical analysis results	ThisisEngineering RAEng: white printer paper with musical notes
40	Experimental results	N/A
41	Tangible products	Shahadat Rahman: shallow focus photography of computer codes
42	Q&A	Kevin Ku: closeup photo of eyeglasses
43	Smart Metering Regulation	Bernd Klutsch: pile of books
44	Signal Processing Chain	Original work
45	Attacker Prototypes	ABDURREHMAN: five electric meters on wall
46	System structure and security	Original work
47	The Structure of the Electrical Grid	Original work