CYBERSEC CEE 2019, 29. – 30. 10. 2019, Katowice

Acoustic Side-Channels in Cryptography

Viliam Hromada
Slovak University of Technology in Bratislava

Presented research was funded by
NATO Science for Peace and Security Programme

Contents

- Side-channel analysis.
- Hagelin cipher.
- Keyboards, dot-matrix printers.
- RSA acoustic attack.

Side-channel analysis

- The attacker tries to crack the cipher / extract secret information by targeting the physical implementation.
- Active attacks – inducing faults into the computation.
- Passive attacks – observing the behavior of the implementation
  - **Acoustic emanation**,
  - Electromagnetic emanation,
  - Power consumption, etc.

Hagelin cipher

- Acoustic attack against Egyptian Hagelin cipher machine in 1956 codenamed ENGULF.
- Tapping the telephone placed near the cipher machine allowed to determine the daily setting of the wheels.

(Source: Photograph by Rama, Wikimedia Commons, Cc-by-sa-2.0-fr)

Keyboards

- Noises emitted by keystrokes may also be used for an attack:
  - By using machine learning and language-models 10-minute recording is enough to subsequently determine 96% of typed text (Zhuang, et. al., 2005).
  - Even simpler technique using dictionary attacks is suitable for an attack against typed passwords – a 5-second recording is enough to determine 90% of typed passwords (Berger, et. Al., 2006).

Dot-matrix printers

- In 2010 Backes, et. al. published a paper on an acoustic side-channel attack on a dot-matrix printer.
- Placing a microphone 10cm from the printer allows to reconstruct printed words with success rate up to 72%.
- If an attacker assumes contextual knowledge about the text, the success rate may be up to 95%.

RSA acoustic cryptanalysis

- Attack presented in 2014 by Genkin, Shamir, Tromer – *RSA key extraction via low-bandwidth acoustic cryptanalysis.*
- NATO SPS 984520 Secure Implementation of Post-Quantum Cryptography
- Targets RSA implementation in GnuPG 1.4.14.
- Recent versions of GnuPG have been patched.

RSA

- The target is GnuPG running on a laptop.
- Some laptops emanate a specific sound during cryptographic operations.
- Source of the sound: coils and capacitors within the laptop's voltage regulator.

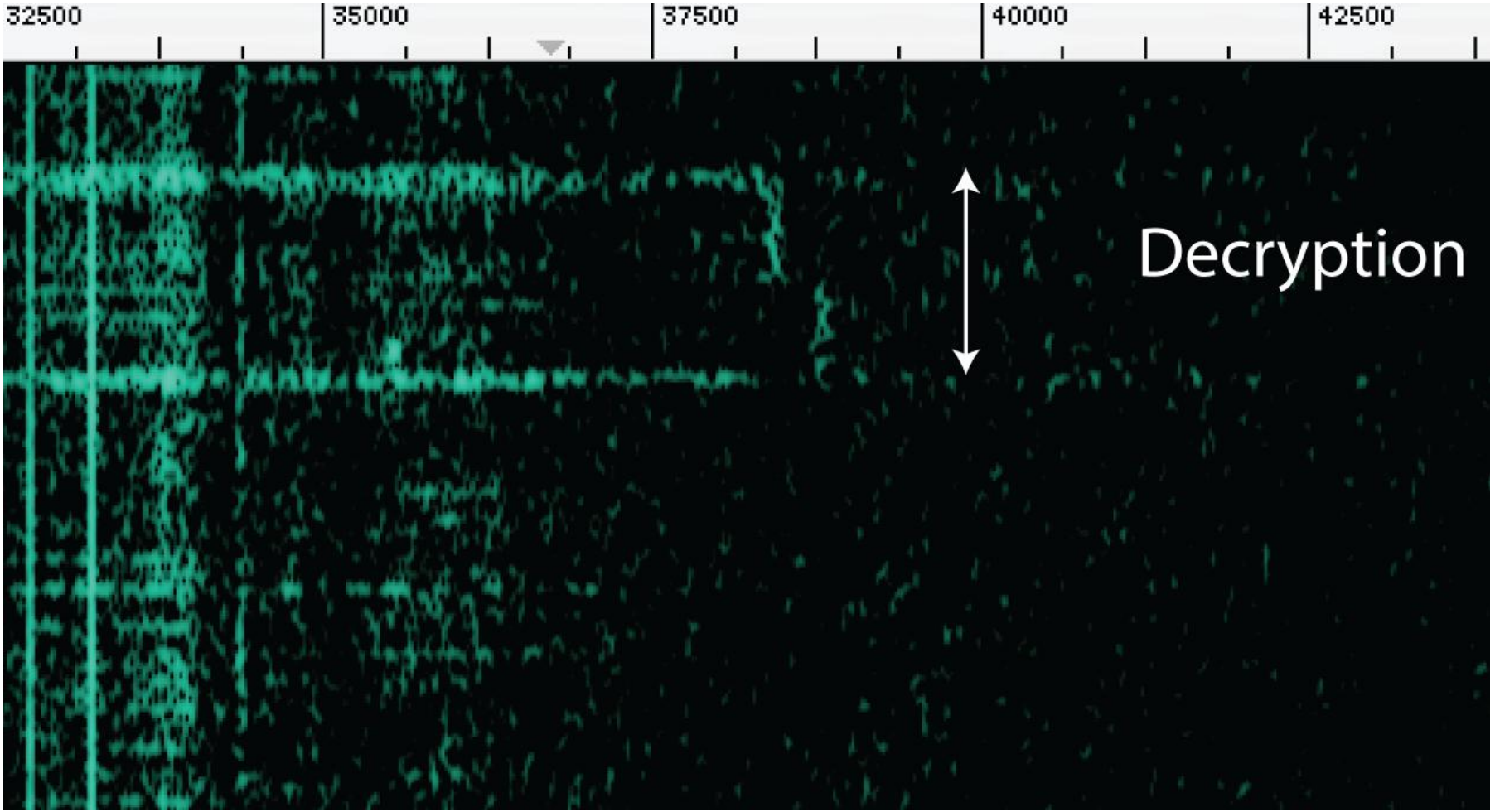
RSA

Attack setup

- Target laptop: Lenovo ThinkPad T61.
- Computer for the analysis of the recorded acoustic signal.
- Microphone from Bruel&Kjaer:
  - Microphone 4190
  - Preamplifier 2669
  - Amplifier and power supply 5935

Attack description

- RSA-algorithm:
  - Private key: p, q, d
  - Public key: n, e
  - Used for encryption and digital signatures.
  - If y is some ciphertext / message to be signed, then the decryption / signature often uses Chinese remainder theorem:
    - $y^d \bmod p$,
    - $y^d \bmod q$


32500
35000
37500
40000
42500
Decryption

Attack description

- The target is the prime q.
- Adaptive chosen ciphertext attack.
- The attack reveals bits of q bit-by-bit.
- The length of q is known.
- q starts with bit value 1.

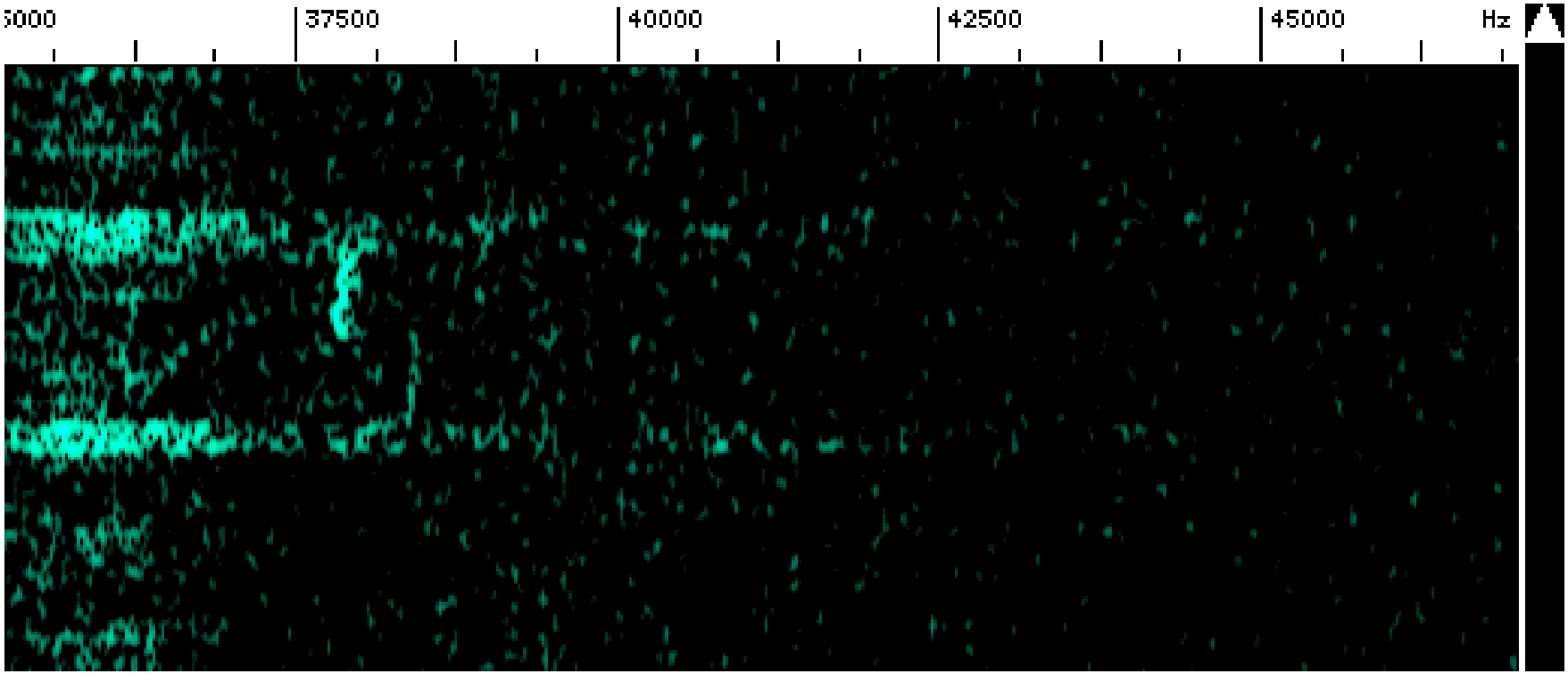
Attack description

- Make the laptop decrypt the binary ciphertext $y = 1011\ 1111\ 1111\ \ldots.\ 1111$ where y has the same length as q.
- If the second bit of q is zero, $y > q$ and $y \bmod q$ looks like a random binary sequence.
- If the second bit of q is one, y keeps the special structure.
- Observing the spectrogram we can detect which scenario occurred and determine the value of the second bit of q.

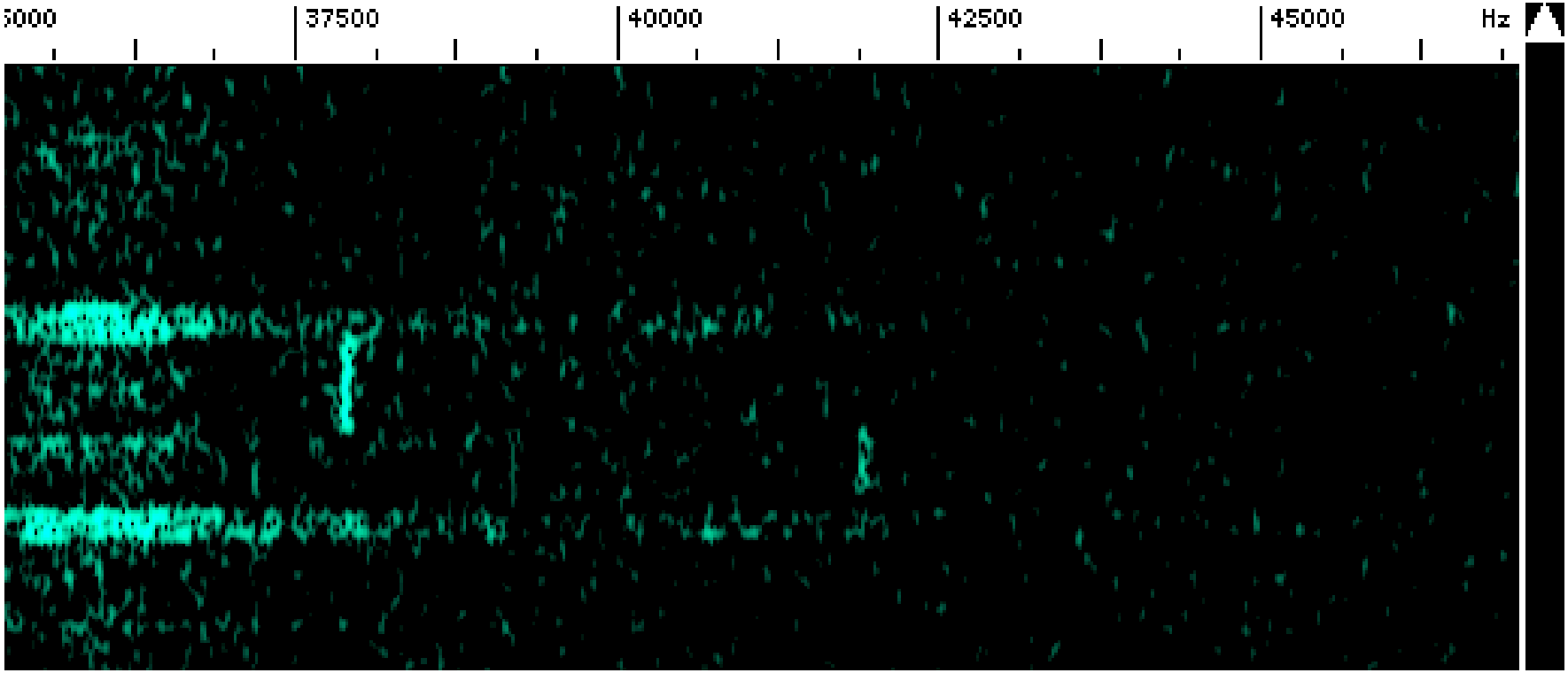
Attack continues…

- After learning the second bit q_2 the new ciphertext will be y = 1$q_2$01 1111 … 1111 to reveal the third bit of q in the same fashion…

$q_2 = 0$



$q_2 = 1$



Attack description

- The whole attack can be made automatic.
- Our student worked on an automated analysis and was able to extract several tens of bits.
- The original authors extracted the whole value of q in 1 hour.
- The attack is relevant is the victim uses the vulnerable version of GnuPG in some sensitive application, e.g. an e-mail client.

Countermeasures

- Hardware-based:
  - Acoustic shielding.
  - Carefully designed acoustic noise generator.

- Software-based:
  - Cipher text randomization.
  - Modulus randomization.
  - Cipher text normalization.

Thank you for your attention!