Implementation Attacks, Lightweight Crypto, and RNGs

Stjepan Picek; TU Delft, The Netherlands

Faculty of Electrical Engineering and Computing, Zagreb

Outline

Outline

Side-channels

Something that enables you to know something about something without directly observing that something.

Side-channels

Side-channels

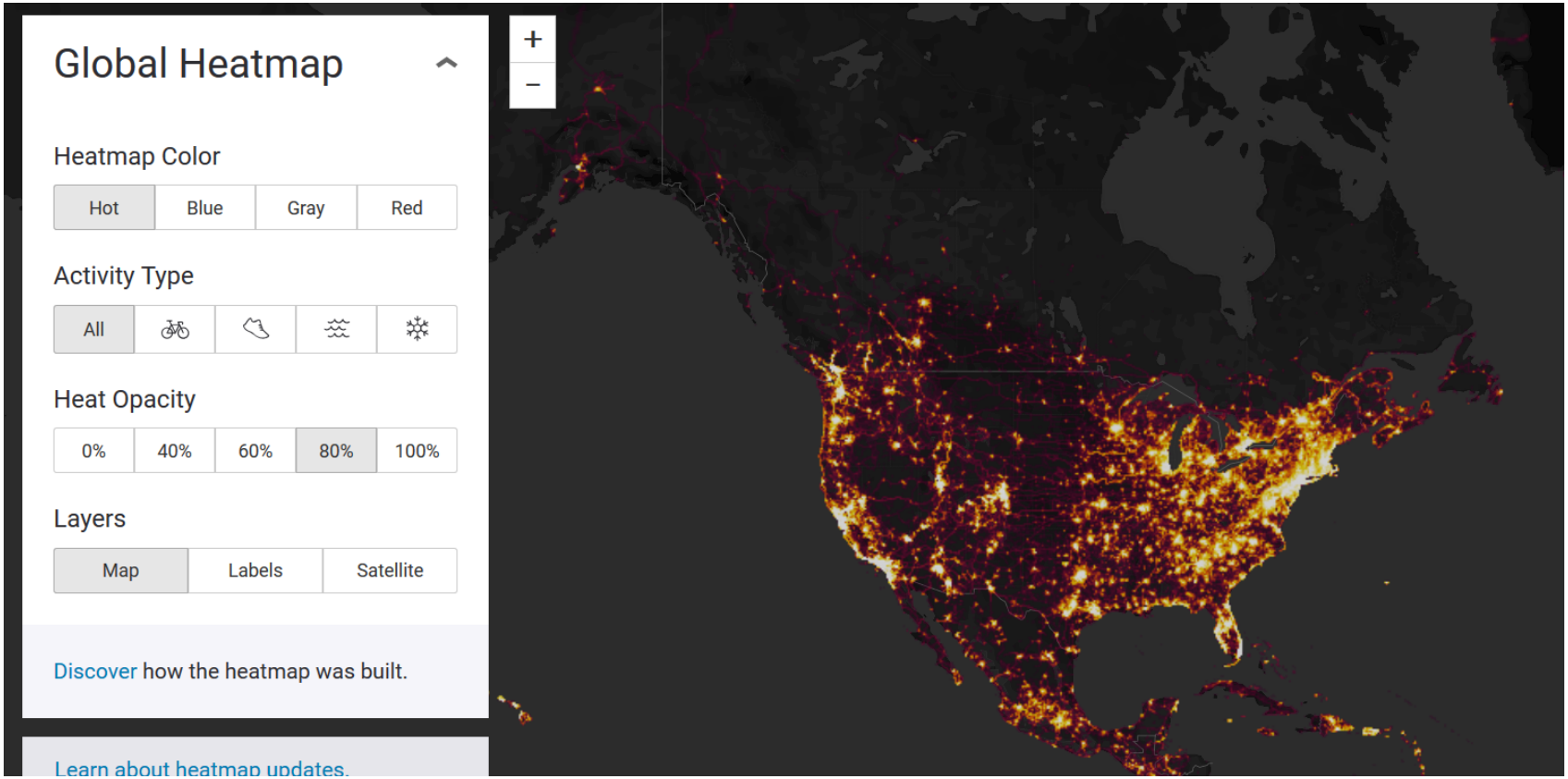
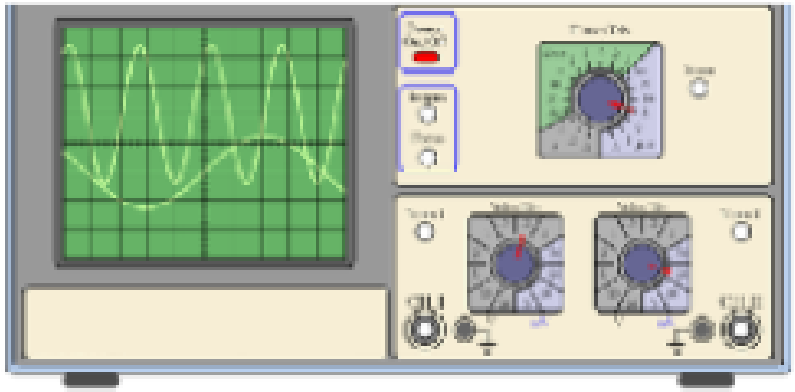


Figure: https://www.strava.com/heatmap#3.10/-108.57419/44.95226/hot/all

Side-channels

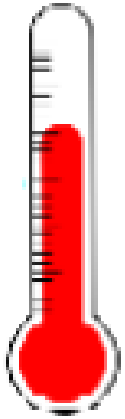
Side-channels

Power

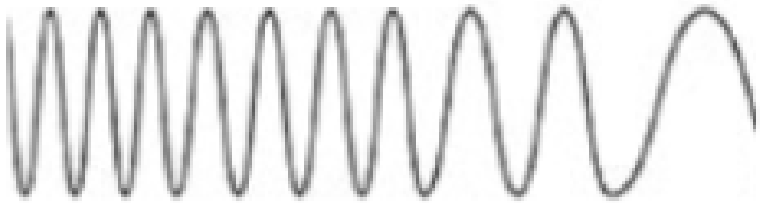


Timing

Temperature



Side channels



Outline

Implementation Attacks

"Researchers have extracted information from nothing more than the reflection of a computer monitor off an eyeball or the sounds emanating from a printer." - Scientific American, May 2009.

Cryptographic Theory vs Physical Reality

- Cryptographic algorithms are (supposed to be) theoretically secure.
- Implementations leak in physical world.

Implementation Attack Categories

- Side-channel attacks.
- Faults.
- Microprobing.

Taxonomy of Implementation Attacks

- Active vs passive.
- Active:
  1. Active: the key is recovered by exploiting some abnormal behavior.
  2. Insertion of signals.
- Passive:
  1. The device operates within its specifications.
  2. Reading hidden signals.

Implementation Attacks

Implementation attacks

Implementation attacks do not aim at the weaknesses of the algorithm, but on its implementation.

- **Side-channel attacks** (SCAs) are passive, non-invasive attacks.
- SCAs represent one of the most powerful categories of attacks on crypto devices.

Examples of Implementation Attacks

- KeeLoq: eavesdropping from up to 100 m.
- PS3 hack due to ECDSA implementation failed.
- Attacks on Mifare Classic, Atmel CryptoMemory.
- Spectre and Meltdown.

The Goals of Attackers

- Secret data.
- Location.
- Reverse engineering.
- Theoretical cryptanalysis.
- ...

Physical Security in the Beginning

- Tempest – already known in 1960s that computers generate EM radiation that leaks information about the processed data.
- 1965: MI5 used a microphone positioned near the rotor machine used by Egyptian embassy to deduce the positions of rotors.
- 1996: first academic publication on SCA – timing.
- 1997: Bellcore attack.
- 1999: first publication of SCA – power.

Outline

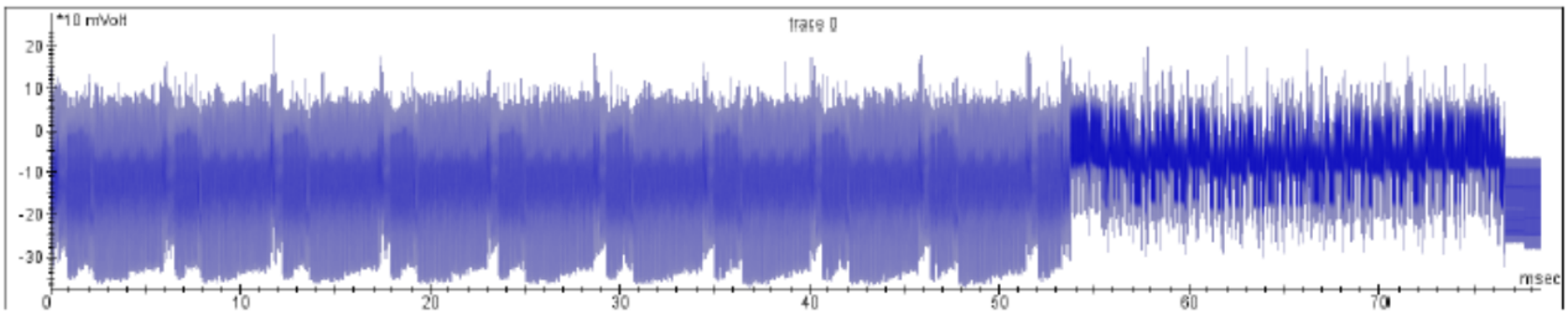
Power Analysis

- Direct attacks:
  1. Simple Power Analysis – SPA.
  2. Differential Power Analysis – DPA.
  3. Correlation Power Analysis – CPA.
  4. ...
- Two-stage attacks:
  1. Template attack – TA.
  2. Stochastic models.
  3. Machine learning-based attacks.
  4. ...

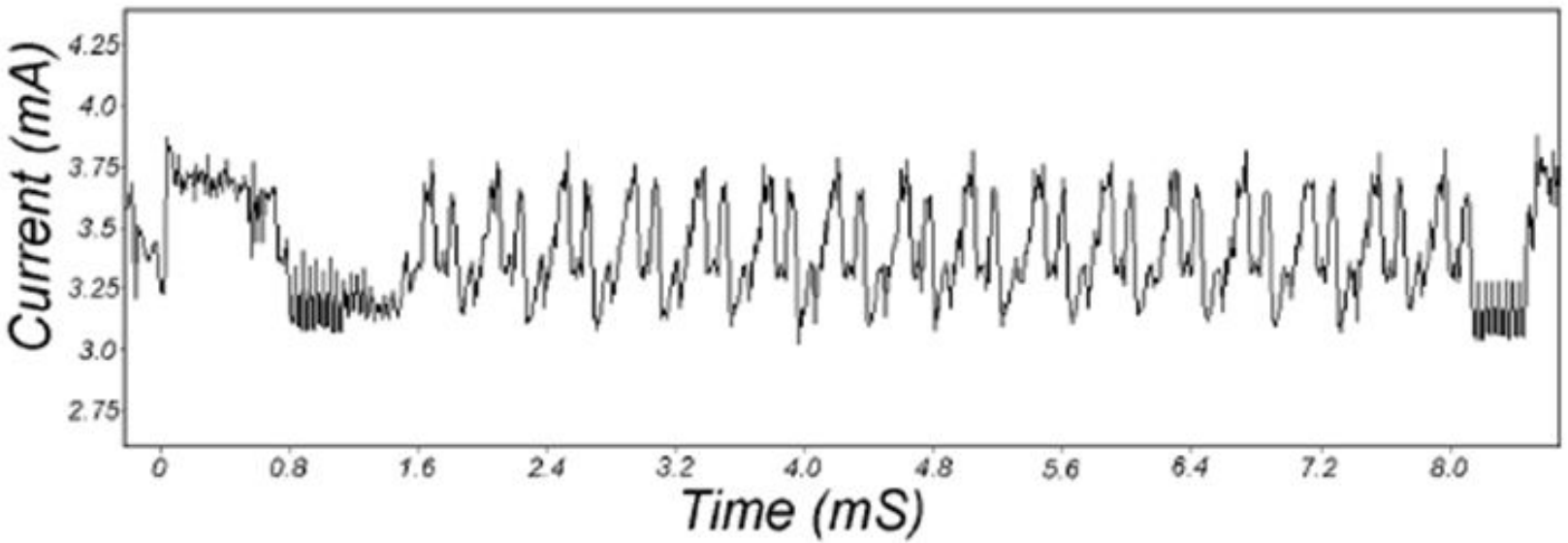
Simple Power Analysis

- Based on one or a few measurements.
- Visual inspection of measurements.
- Discovery of data independent but instruction dependent properties.
- In symmetric crypto:
  1. Number of rounds.
  2. Memory access.
- In asymmetric crypto:
  1. Key length.
  2. Implementation details.
  3. Key.

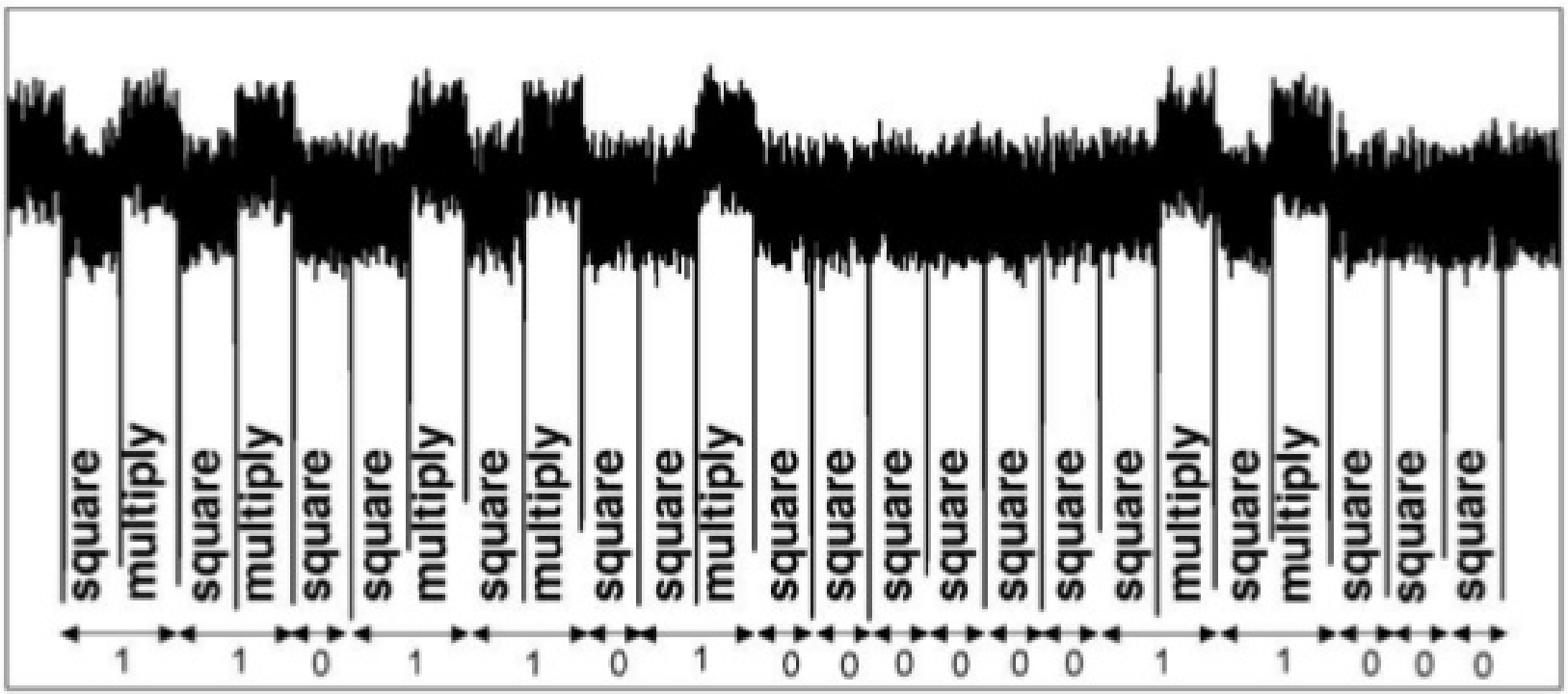
SPA



SPA

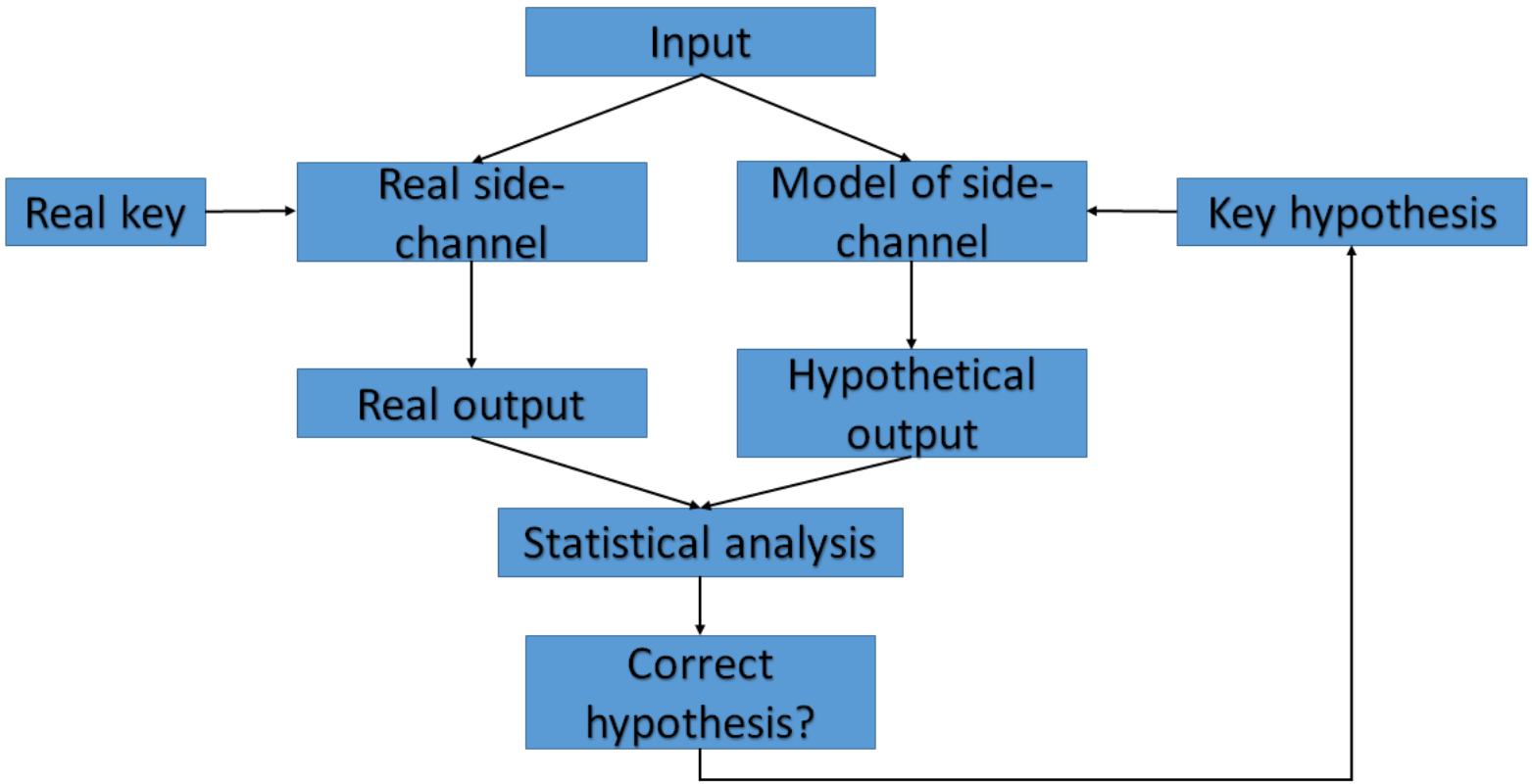

Current (mA)
4.25
4.0
3.75
3.5
3.25
3.0
2.75
0
0.8
1.6
2.4
3.2
4.0
4.8
5.6
6.4
7.2
8.0
Time (mS)

SPA


square
multiply
square
multiply
square
square
multiply
square
multiply
square
square
multiply
square
square
square
square
square
square
square
multiply
square
multiply
square
square
square
1 1 0 1 1 0 1 0 0 0 0 0 0 1 1 0 0 0

Differential Power Analysis

- Statistical analysis of measurements.



Correlation Power Analysis

- Write a leakage model for the power consumption.
- Obtain measurements of power consumption while device is running encryption over different plaintexts.
- Attack subparts of the key (divide and conquer approach):
  1. Consider all options for subkey. For each guess and trace, use plaintext and guessed subkey to calculate power consumption according to the model.
  2. Use the Pearson correlation to differentiate between the modeled and actual power consumption.
  3. Decide which subkey guess correlates best to the measured traces.
- Combine the best subkey guesses to obtain the secret key.

Pearson's Correlation

$$\rho_{X,Y} = \frac{cov(X,Y)}{\sigma_x \sigma_y} = \frac{E[(X-\mu_x)(Y-\mu_y)]}{\sqrt{E[(X-\mu_x)^2]E[(Y-\mu_y)^2]}} \quad (1)$$

Leakage Models

- Recall, power has two components: static and dynamic.
- Static power is required to keep the device running and it depends on the number of transistors inside the device.
- Dynamic power depends on data processing.

Leakage Models

- Transition = the Hamming distance model.
- Counts the number of transitions between $0 \rightarrow 1$ and $1 \rightarrow 0$.
- Typical model for ASIC.
- Requires j=knowledge of a previous (or succeeding) value.
- The Hamming weight model is typical on a precharged data bus in a microcontroller.

The Distinguishers

- Difference of Means.
- T-test.
- Variance test.
- Pearson correlation.
- Spearman's rank correlation.
- MIA.
- ...

Example

- Let us consider AES-128 where we use the Hamming weight model.
- After the first S-box operation,

$$state = sbox[input\ XOR\ key]$$

.

- Our modeled power consumption for one byte of plaintext p is then

$$h_p = Hamming(sbox[input_p\ XOR\ key])$$

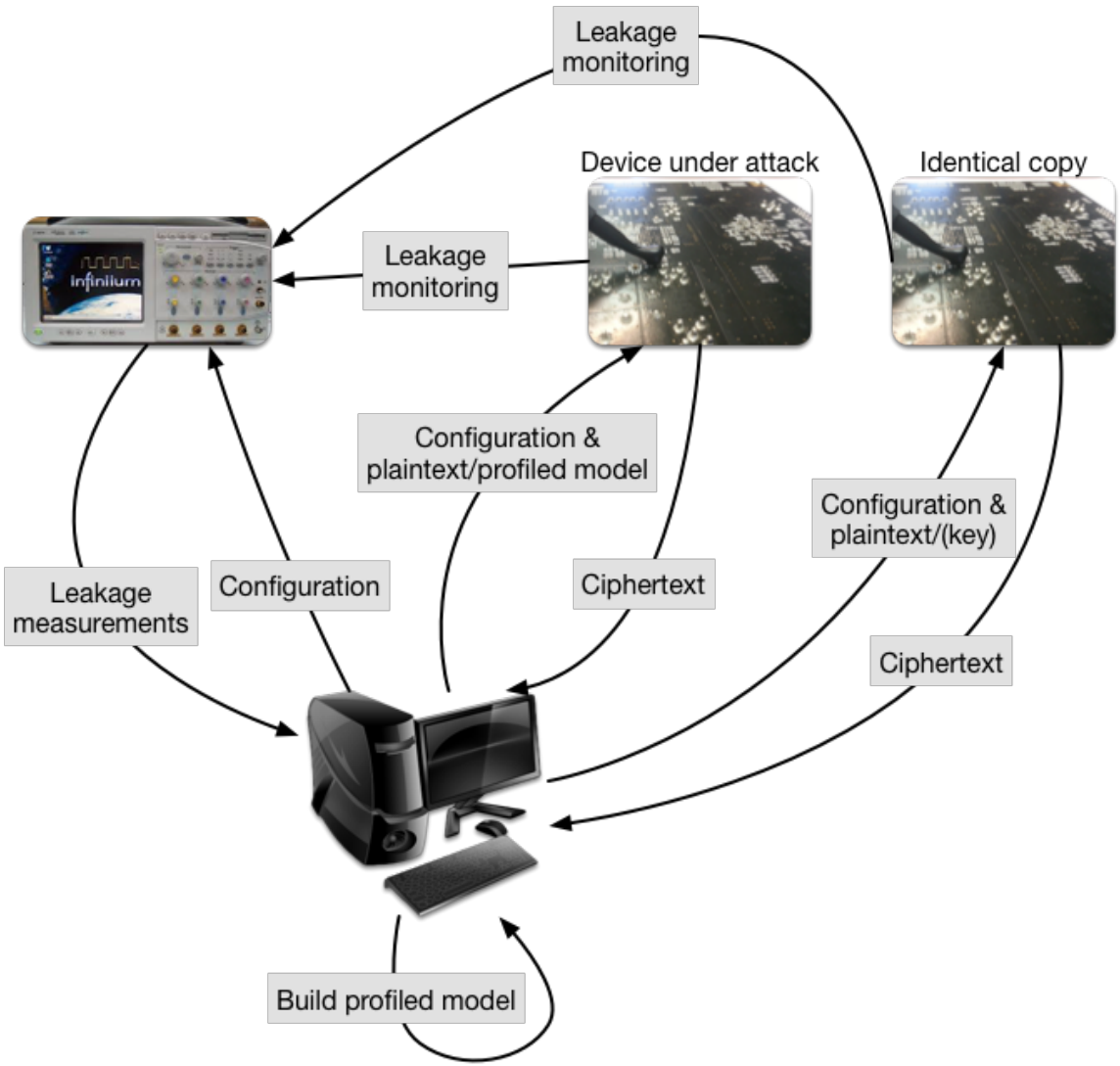
.

- How many key guesses do we need to do for each subkey?
- How many in total?

Profiled Attacks

- Profiled attacks have a prominent place as the most powerful among side channel attacks.
- Within profiling phase the adversary estimates leakage models for targeted intermediate computations, which are then exploited to extract secret information in the actual attack phase.
- Template Attack (TA) is the most powerful attack from the information theoretic point of view.
- Some machine learning (ML) techniques also belong to the profiled attacks.

Profiled Attacks



Profiled Attacks

- Two stage (profiled) attacks are more complicated than the direct attacks.
- The attacker must have access to a copy of the device to be attacked.

Template Attack

- Using the copy of device, record a large number of measurements using different plaintexts and keys. We require information about every possible subkey value.
- Create a template of device's operation. A template is a set of probability distributions that describe what the power traces look like for many different keys.
- On device that is to be attacked, record a (small) number of measurements (called attack traces) using different plaintexts.
- Apply the template to the attack traces. For each subkey, record what value is the most likely to be the correct subkey.

Template Attack

- When using high-quality templates made from many traces, it is possible to attack a system with a single trace.
- Template attack can become unstable if there are more points of interest than measurements per value.

Machine Learning-based Attacks

- In symmetric crypto, machine learning-based attacks are mostly supervised learning approaches.
- Up to now, various techniques have been used with great success: SVM, Random Forest, Multi layer Perceptron, CNNs.
- The attack goes in two phases:
  1. Train a model from the training set (measurements with labels).
  2. Apply the model to the testing set (measurements without labels).

Reality Is More Complicated

- Pre-processing.
- Feature engineering.
- Model Selection.
- Hyper parameter optimization.
- Fighting with countermeasures.
- ...

Reality Is More Complicated

- Constraints for implementing countermeasures (software and hardware).
- Optimization can make SCA easier.
- Trade-off between practical and academic attacks.

Outline

Fault Injection

- Alter the correct functioning of a system.
- Often called perturbation attacks.
- Fault injection is very hard (accuracy, reproducibility).
- The equipment is expensive.

Methods

- Variations in supply voltage.
- Variation in external clock.
- Change in temperature.
- White light.
- X-rays and ion beams.

Goals

- Insert computational fault (null key, wrong crypto result).
- Change software decision (force approval of wrong PIN, enforce access rights).
- ...

Force Approval of Wrong PIN

```
for (i = 0; i < 4; i++)
{
    if (pin[i] == input[i])
        ok_digits++;
}
if (ok_digits == 4)
    respond_code(0x00, SW_NO_ERROR_msb, SW_NO_ERROR_lsb);
else
    respond_code(0x00, 0x69, 0x85);
```

Types of Fault Injection

- Non invasive: glitching (clock, power supply).
- Semi invasive: UV lights, laser, optical fault injection.
- Invasive: microprobing, FIB probing.

Differential Fault Analysis – DFA

- The attacker obtains a pair of ciphertexts derived by encrypting the same plaintext.
- One is correct value and one is faulty.
- Two encryptions are identical up to the point where the fault occurred.
- Two ciphertexts can be regarded as outputs of round reduced ciphers where the inputs are unknown but show a small differential.

Outline

Constrained Devices

- Internet of Things – broad term describing how Internet will be used to connect devices rather than people.
- Some of these devices use powerful processors and can use the same cryptographic algorithms as standard PCs.
- Many of them use extremely low power microcontrollers which can only afford to devote a small fraction of their computing power to security.
- Sensors, RFID chips, smart grids, etc.
- If current algorithms can be made to fit into the limited resources of constrained environments, their performance may not be acceptable.
- Internet of Everything – the networked connection of people, process, data, and things (Cisco).

IoT

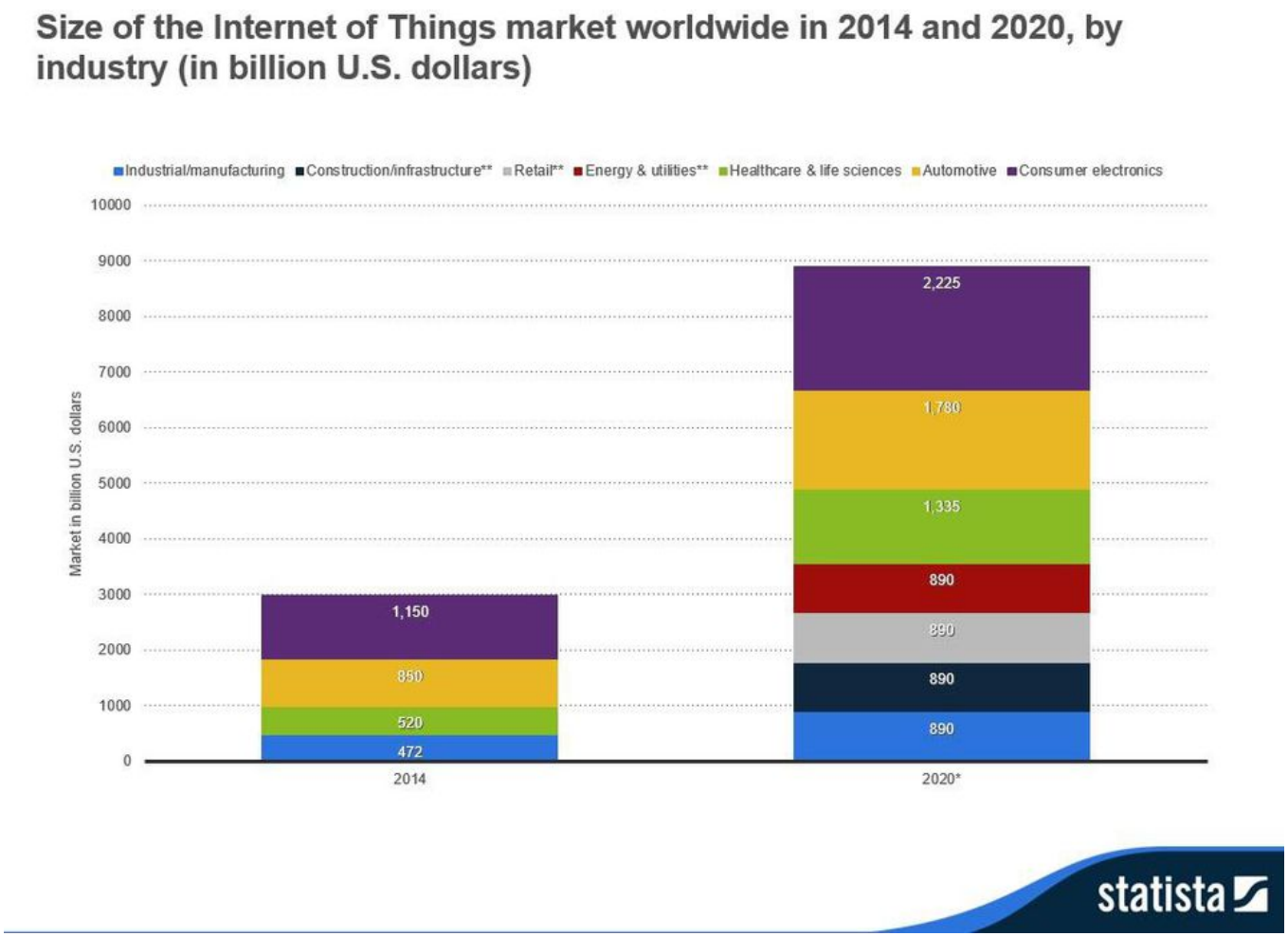


Figure: Source: https://www.forbes.com/sites/louiscolumbus/2017/12/10/2017-roundup-of-internet-of-things-forecasts/#c386d8e1480e.

IoT

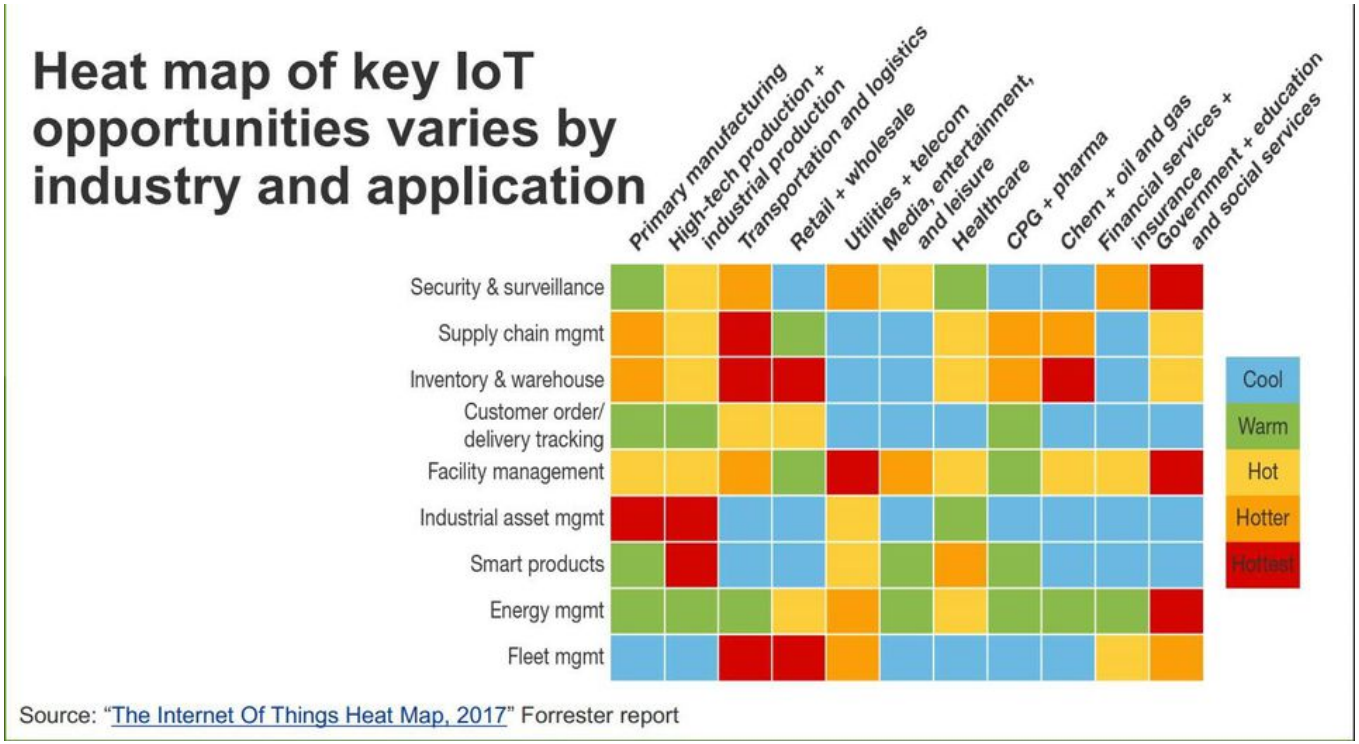


Figure: Source: https://www.forbes.com/sites/louiscolumbus/2017/12/10/2017-roundup-of-internet-of-things-forecasts/#c386d8e1480e.

Why We Need Security

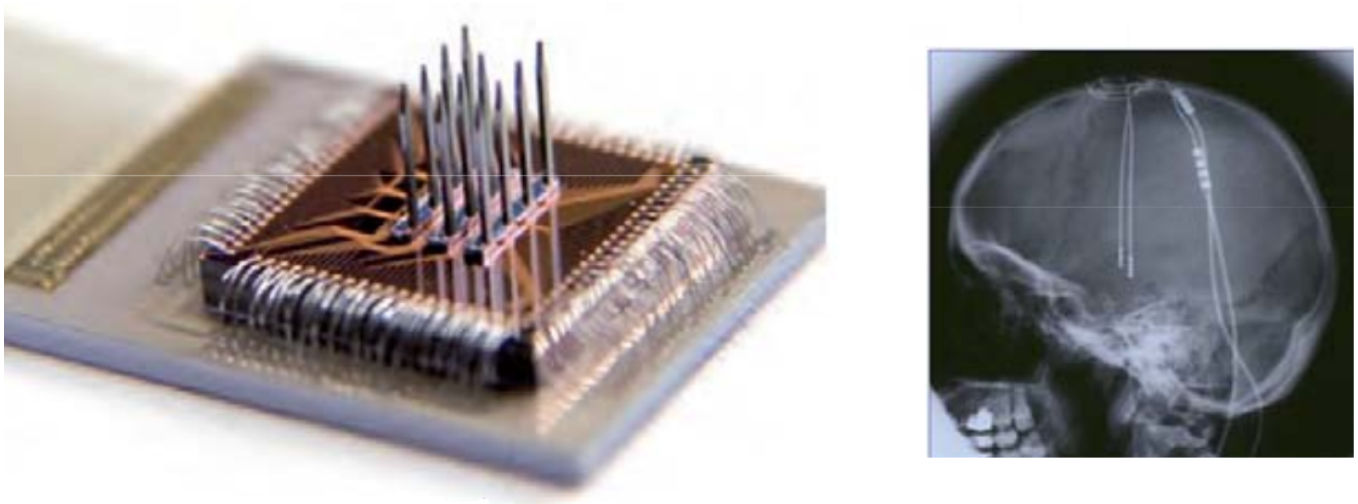


Figure: IMEC: NERF brain stimulant.

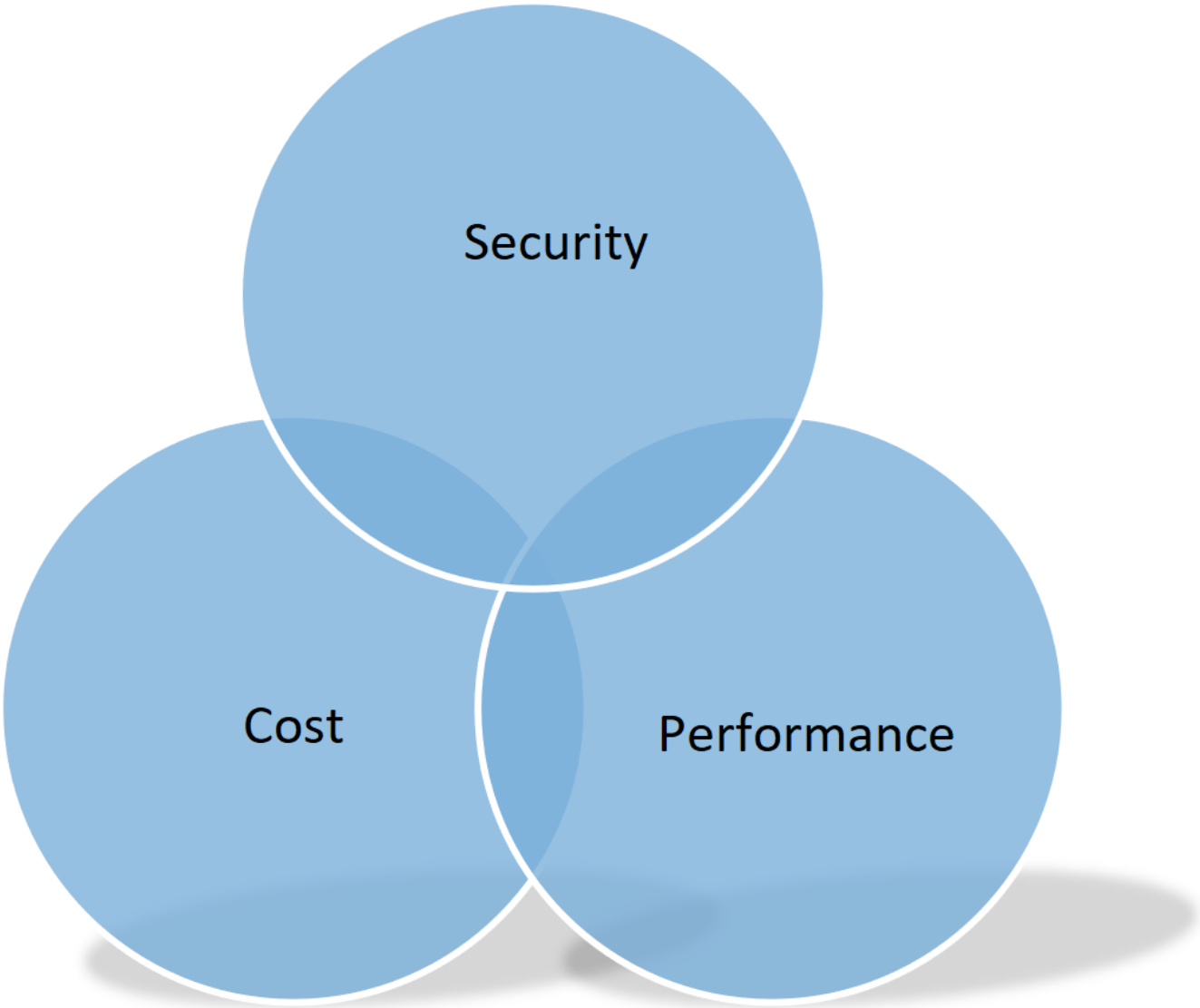
Why We Need Security

- Disabling wireless in pacemaker.
- https://nakedsecurity.sophos.com/2013/10/22/doctors-disabled-wireless-in-dick-cheneys-pacemaker-to-thwart-hacking/
- Hacking cars.
- https://www.wired.com/story/car-hack-shut-down-safety-features/

Lightweight Cryptography

- Cryptographic algorithms proposed for constrained devices/environments.
- We call lightweight algorithms a wide range of ciphers with different properties and designed for various scenarios.
- Sometimes lightweight cryptography is divided into ultra-lightweight cryptography and ubiquitous cryptography.
- The key concept is a trade-off between various aspects.

Lightweight Cryptography



Area

- ASIC – Application Specific Integrated Circuit, unit is NAND gate.
- GE (gate equivalence) – physical area of a single NAND (smallest logic gate with 2 inputs) gate.
- FPGA – Field Programmable Gate Area, unit is LUT, flip-flops.
- Embedded microcontrollers, unit is memory size (program size + data size).

Time

- Throughput – amount of data processed per time unit (the higher the better).
- Latency – delay from input to output (the lower the better).
- High throughput and low latency do not go together.

Power and Energy

Power $\neq$ Energy

- The total power consumption of a CMOS (Complementary Metal Oxide Semiconductor) device:

$$P_{total} = P_{static} + P_{dynamic},$$

$$P_{static} = V \cdot I,$$

$$P_{dynamic} = \alpha \cdot C \cdot V^2 \cdot f,$$

where α is the switching factor (the probability of a bit switching from 0 to 1), C is the switched capacitance, V is the voltage, f is the clock frequency, and I is the current.

Power and Energy

- Power (= Watt).
- Energy E (= Joule).

$$E = P \cdot t.$$

- For power consideration, cooling is important (implanted device only $\Delta 1\,\mathrm{deg}\,C$ temperature).
- Anything that is battery powered has low energy requirements.

Examples of Lightweight Ciphers

- PRESENT
- Prince
- Klein
- Rectangle
- MIDORI
- Gift
- Piccolo
- KATAN
- Simon
- Speck
- LED
- ...

Outline

Two-way communication

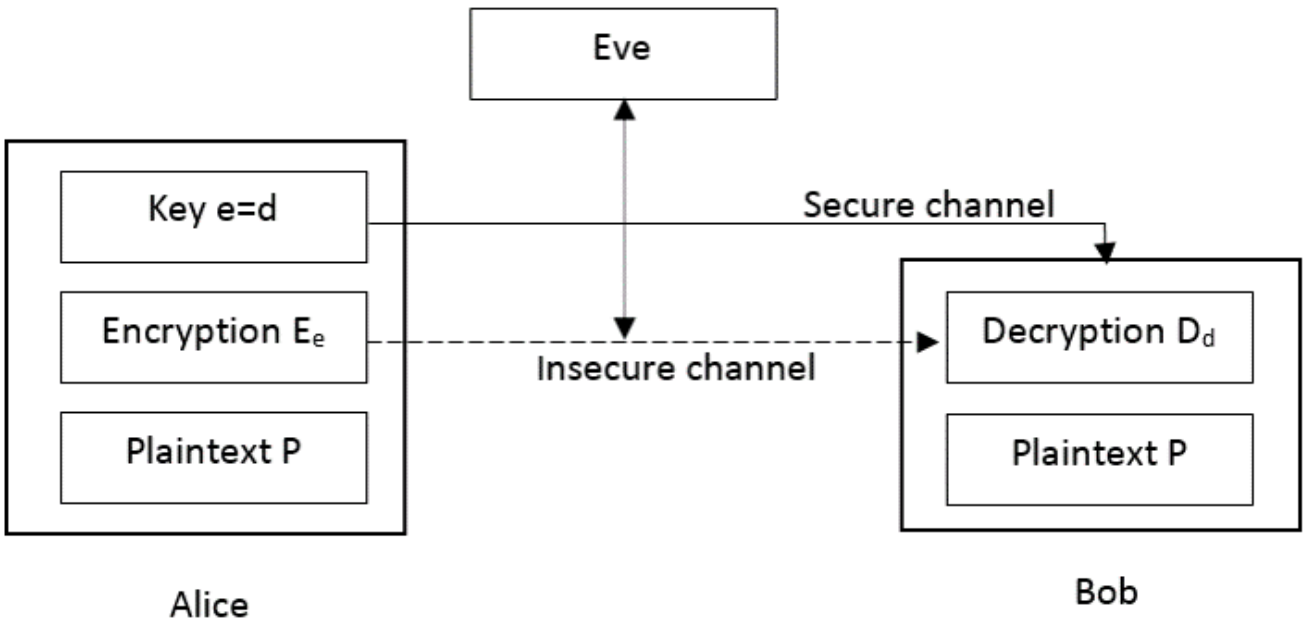


Figure: Two-way communication.

Random Number Generators – RNGs

- Kerckhoff principle: A cryptosystem should be secure even if everything about the system, except the key, is public knowledge.
- Extremely important in cryptography.
- Used for cryptographic keys, initialization vectors, nonces, padding, masks in side-channel attacks countermeasures, etc.

Random Number Generators – RNGs

- Kerckhoff principle: A cryptosystem should be secure even if everything about the system, except the key, is public knowledge.
- Extremely important in cryptography.
- Used for cryptographic keys, initialization vectors, nonces, padding, masks in side-channel attacks countermeasures, etc.

Security Requirements for RNGs

- Good statistical properties of output values.
- Output unpredictability.

Assessing Security

- Evaluate statistical parameters using statistical tests (FIPS140-2, NIST 800-22, DIEHARD, etc.).
- Evaluate entropy using entropy estimator (entropy cannot be measured, only estimated from a model).
- Test online the source of entropy using dedicated statistical tests.

Basic RNG Classes

- Deterministic (Pseudo) random number generators (PRNG).
- Physical (True) random number generators (TRNG).
- Hybrid random number generators (HRNG).

PRNG

- Algorithmic generators.
- Usually fast and with good statistical characteristics.
- Must have long period.
- Must be computationally secure (difficult to guess previous or next value).

TRNG

- Using physical source of randomness.
- Unpredictable and often with suboptimal statistical characteristics.
- Usually slower than PRNG.

Intels Hardware RNG

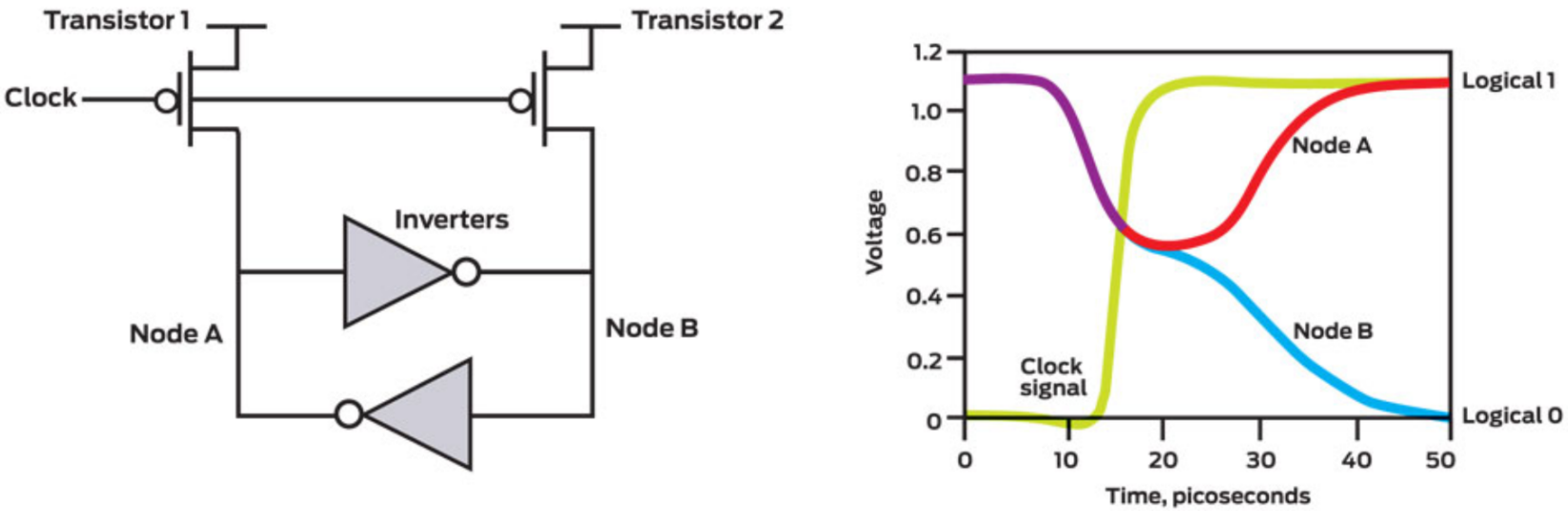


Figure: When transistor 1 and transistor 2 are switched on, a coupled pair of inverters force Node A and Node B into the same state [left]. When the clock pulse rises [yellow, right], these transistors are turned off. Initially the output of both inverters falls into an indeterminate state, but random thermal noise within the inverters soon jostles one node into the logical 1 state and the other goes to logical 0. Source: https://spectrum.ieee.org/computing/hardware/behind-intels-new-randomnumber-generator

HRNG

- Combining PRNG and TRNG.
- PRNG seeded by a TRNG.
- TRNG with post-processing.

HRNG as per AIS31 Recommendations

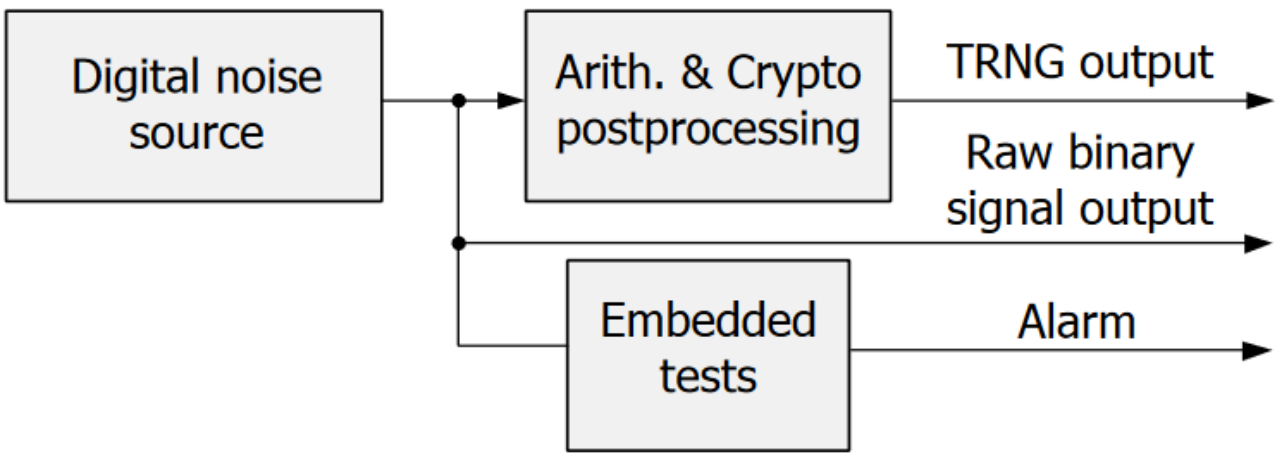


Figure: AIS setting for HRNG.

Post-processing for RNGs

- Cryptographic (e.g., cryptographic hash function).
- Arithmetic (linear, van Neumann).
- van Neumann processing: a simple method that produces perfectly unbiased outputs.
- Suppose an input stream has independent but biased bits.
- Process the stream of bits as a stream of non-overlapping pairs of successive bits and generates outputs as follows:
  1. If the input is "00" or "11", the input is discarded (no output).
  2. If the input is "01" or "10", output the first bit only.

Outline

Tamper Resistance

- Usually, secure cryptographic algorithms provide security against an adversary who has only black-box access to the secret information of honest parties.
- Often, such model is not adequate.
- Tamper resistant hardware helps keep the cryptographic key safe.
- Tamper Resistant Security Module (TRSM) – a set of hardware, software, firmware (and combination of those) that implements cryptographic logic or processes and is contained within the cryptographic boundary.

Tamper Resistance

- https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.140-2.pdf
- 5 security levels (https://csrc.nist.gov/CSRC/media/Publications/fips/140/3(2007)/3-final-draft-2007.pdf)

Basic Notions

- Tamper detection – the ability of a device to sense it is under physical attack and initiate defensive actions through tamper response.
- Tamper response – the action a device performs in order to prevent misuse of the cryptographic module.
- Tamper evidence – the action of a device that makes the unauthorized access to the device easily detected.
- Tamper resistance – the ability of a device to defend against a threat.

Types of Secure Hardware

- Tamper Resistant Security Module.
- Secure microcontroller.
- Smartcard.
- Other.

Hardware Security Module

- An HSM is a dedicated cryptographic processor specifically designed for the protection of the cryptographic key lifecycle.
- Secure managing, processing, and storing of cryptographic keys inside a hardened, tamper-resistant device.
- In order for a device to be HSM, it needs to be TRSM.

Defense Mechanisms

- Hardened casings, locks, encapsulation, security screws.
- Seals.
- Sensors, switches, special circuitry.