COMPUTER SCIENCE
& ENGINEERING
UNIVERSITY OF MICHIGAN

A Simple Power Analysis Attack on the TwoFish Key Schedule

Jose Javier Gonzalez Ortiz

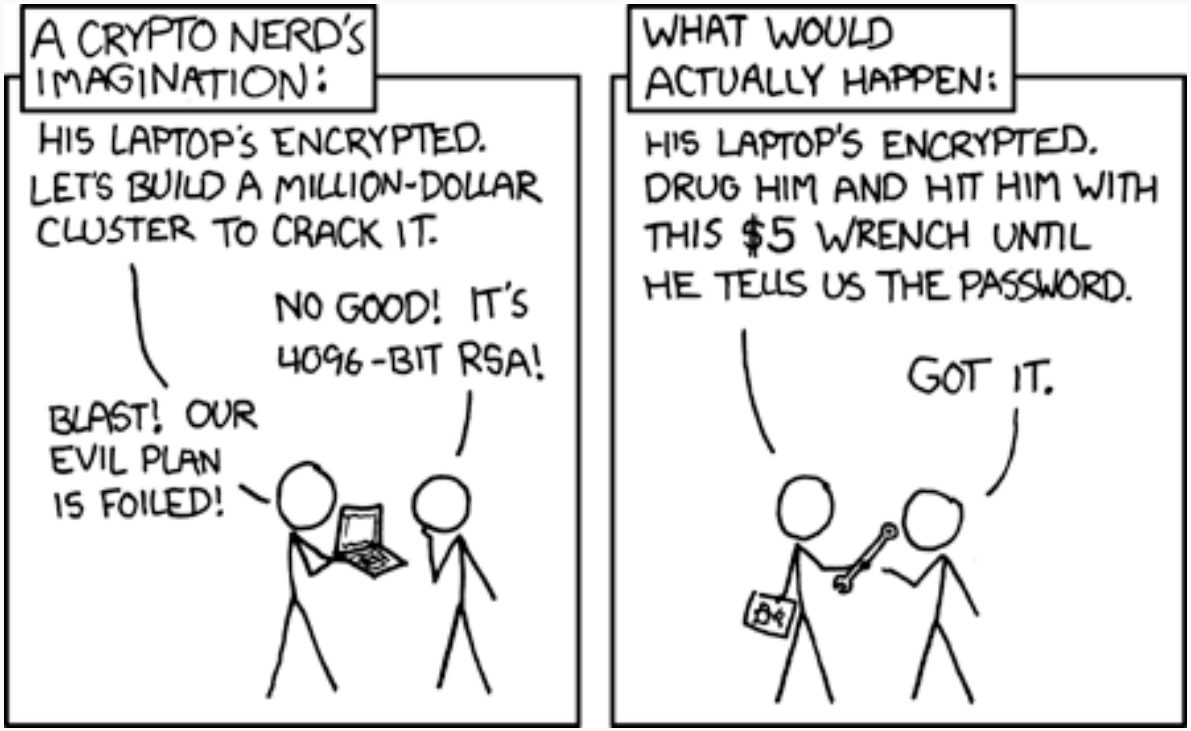
May 5, 2016

University of Michigan

Introduction

Cryptography Basics

Cryptography allows us to **securely communicate** information with other parties.



Credit: *Randall Munroe* `https://xkcd.com/538/`

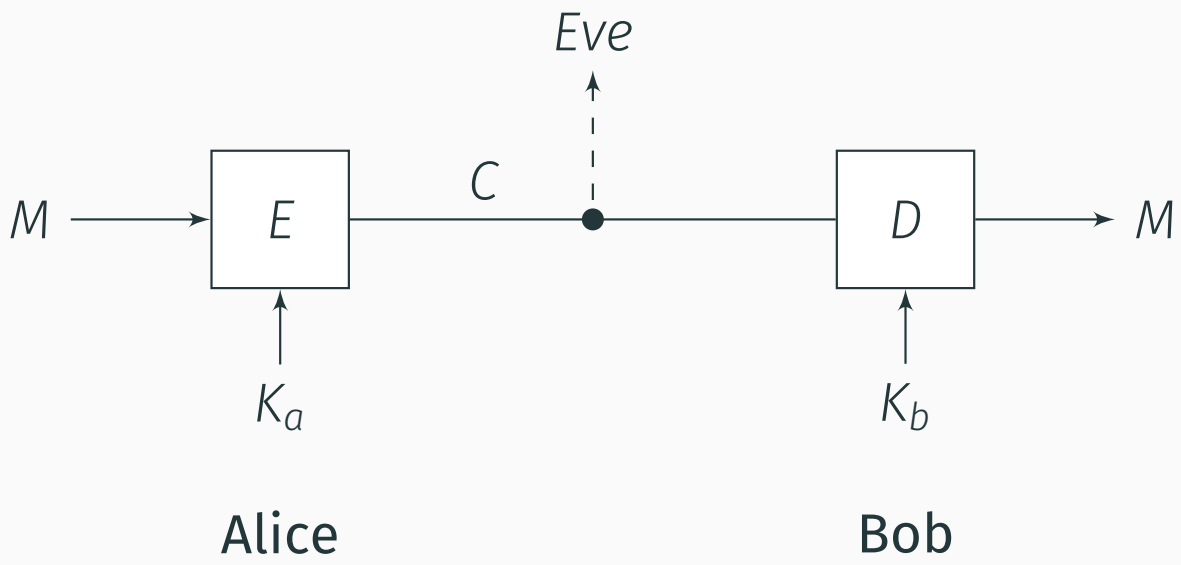
Cryptography involves using protocols that ensure data confidentiality, data integrity and authentication.

Encryption Systems

Cryptographic Algorithms are designed using **mathematical** constructs and are **publicly** available. Security relies on keys, secret pieces of information that dictate the output of the algorithm

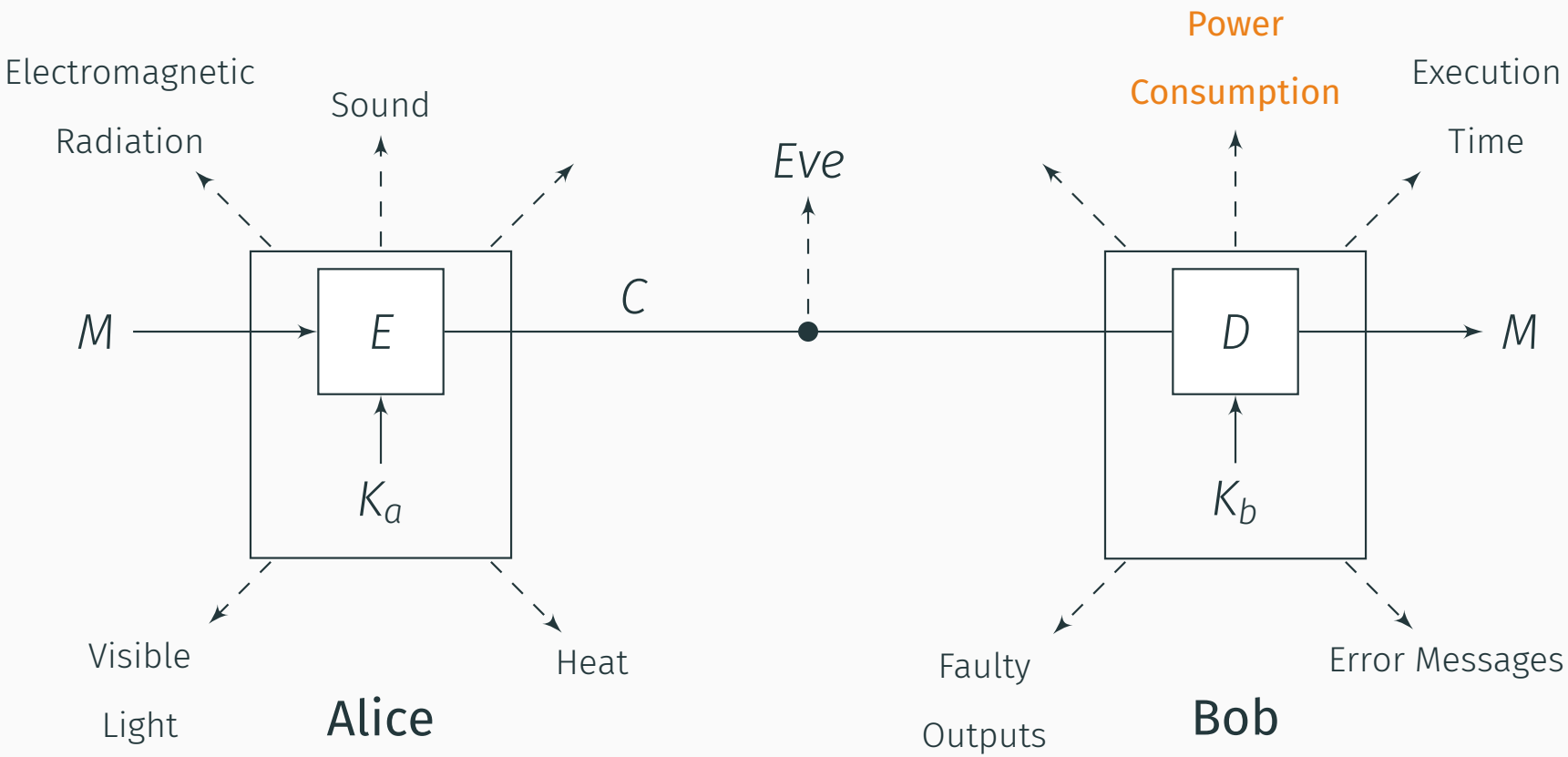
Types of encryption

- **Symmetric Key** - Shared secret key between agents
- **Asymmetric Key** - Public and Private Key.



Side Channel Attacks

A side-channel attack is any attack based on information gained from the **physical implementation** of a cryptosystem.



Embedded Devices I

What percent of computing devices are embedded?

A. 14%

B. 56%

C. 87%

D. 98%

Embedded Devices I

What percent of computing devices are embedded?

A. 14%

B. 56%

C. 87%

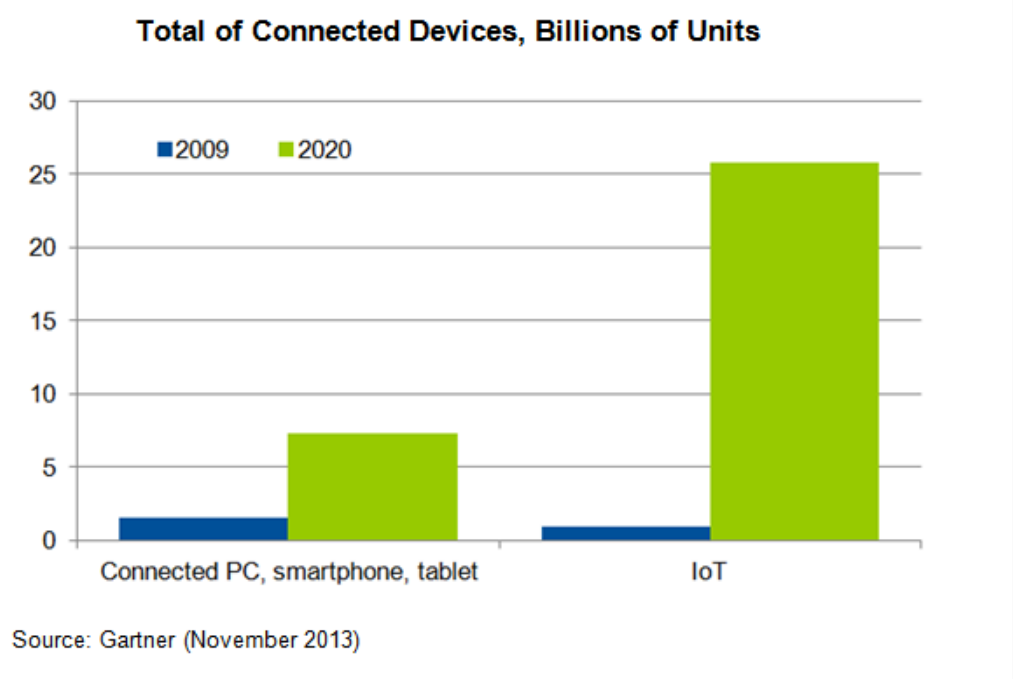
D. 98%

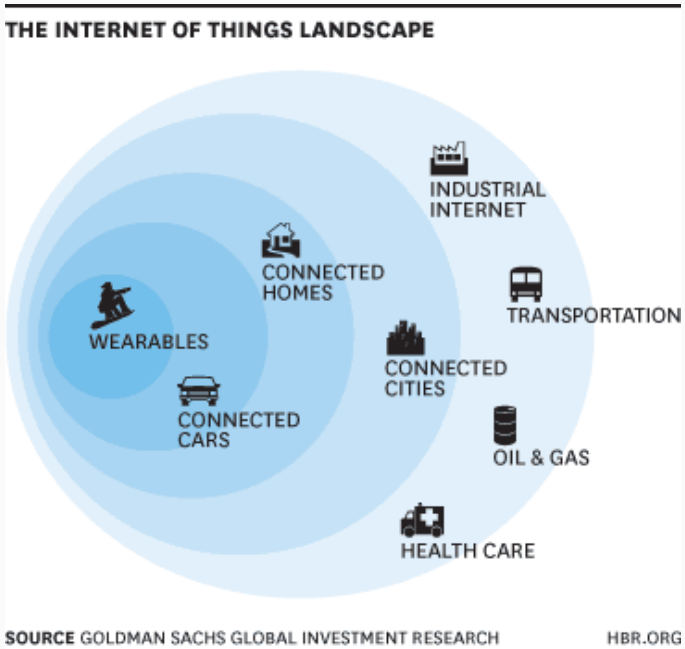
Embedded Devices II

As of 2015

- **98%** percent of computing devices are embedded[1]
- 15 billion connected devices in 2015[2]

In 2020 There will be over **30 billion** connected devices[3]





[1] G. Borriello and R. Want. Embedded Computation meets the *World Wide Web*. Commum. ACM

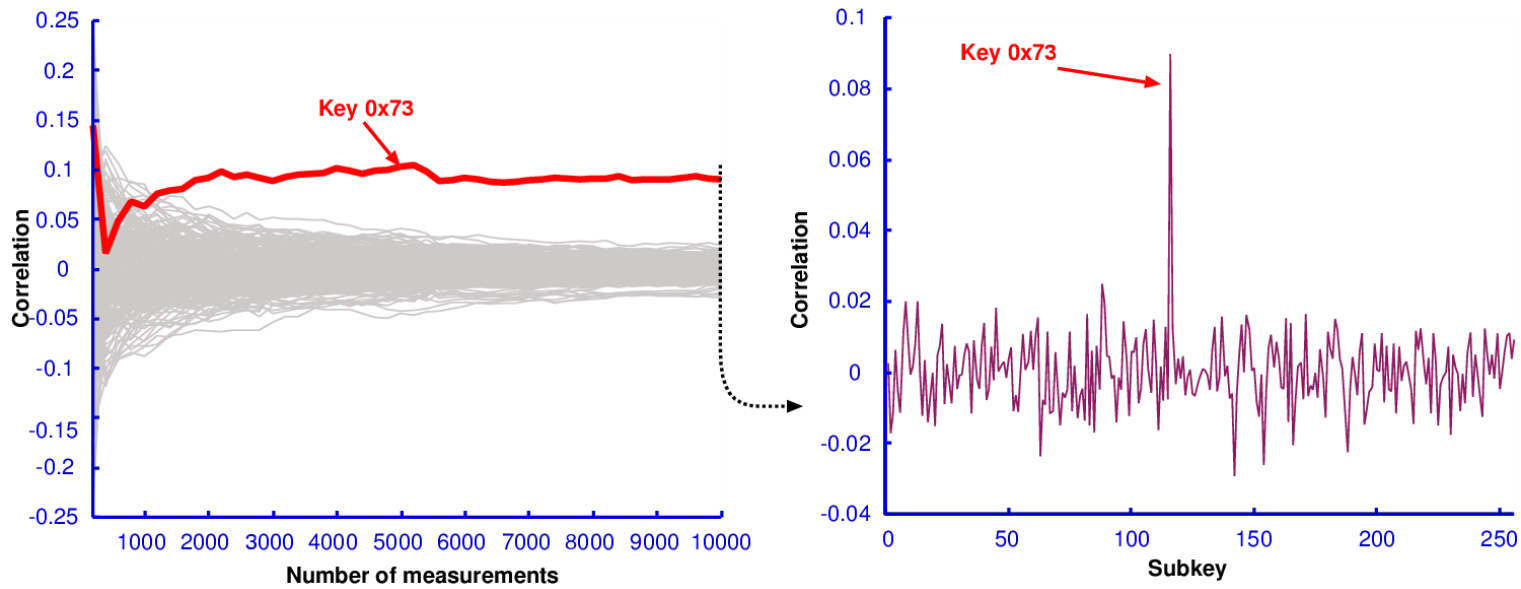
[2] John Gantz. The *Embedded Internet: Methodology and Findings*

[3] Gartner Says Personal Worlds and the Internet of Everything Are Colliding to Create New Markets

Types of Power attacks I

Differential Power Attacks

Black Box Statistical Analysis from large sample of power traces



Credit: *Frank Kagan*: Side Channel Attack Secure Cryptographic Accelerators

Types of Power attacks II

Simple Power Attacks

Focuses on particular vulnerabilities of the algorithm that could leak information from the message or the key.

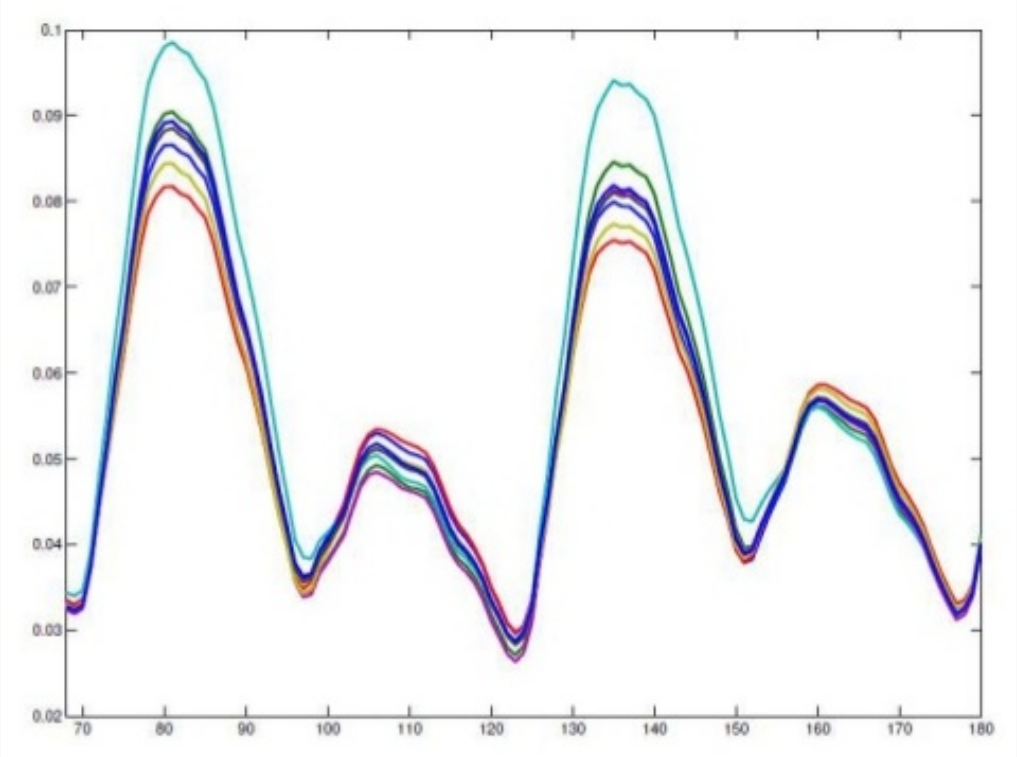
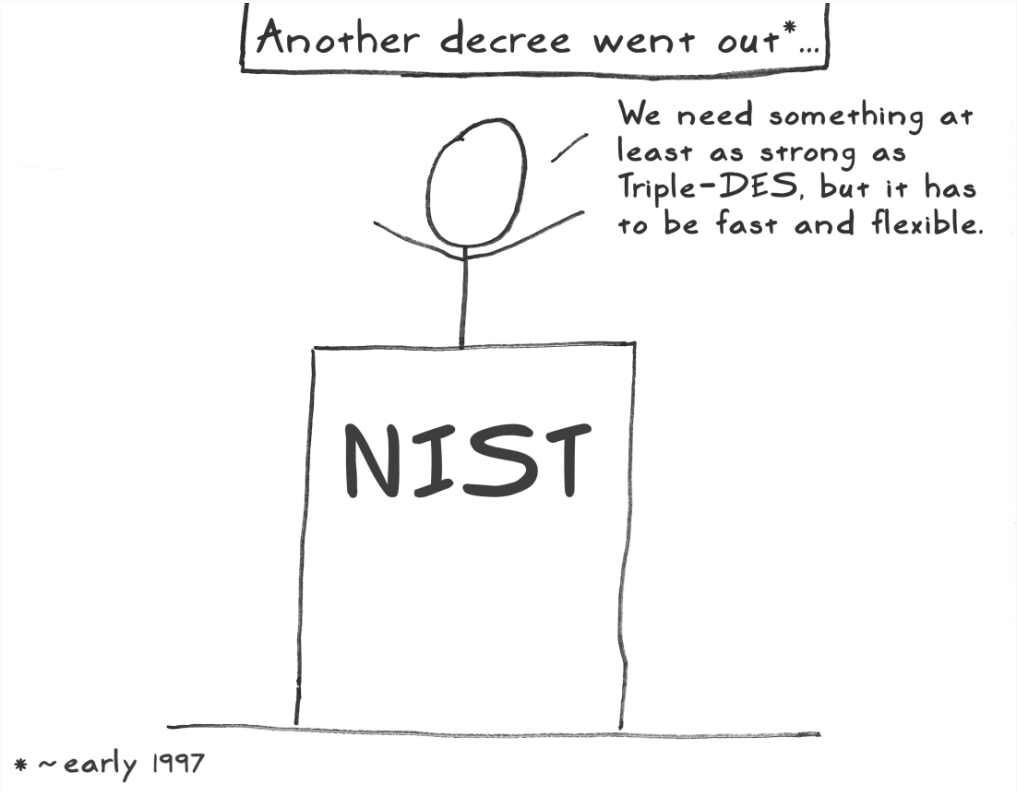


Figure 1: Hamming weight power trace leakage

AES Contest I

But where did all these cryptographic protocols come from?

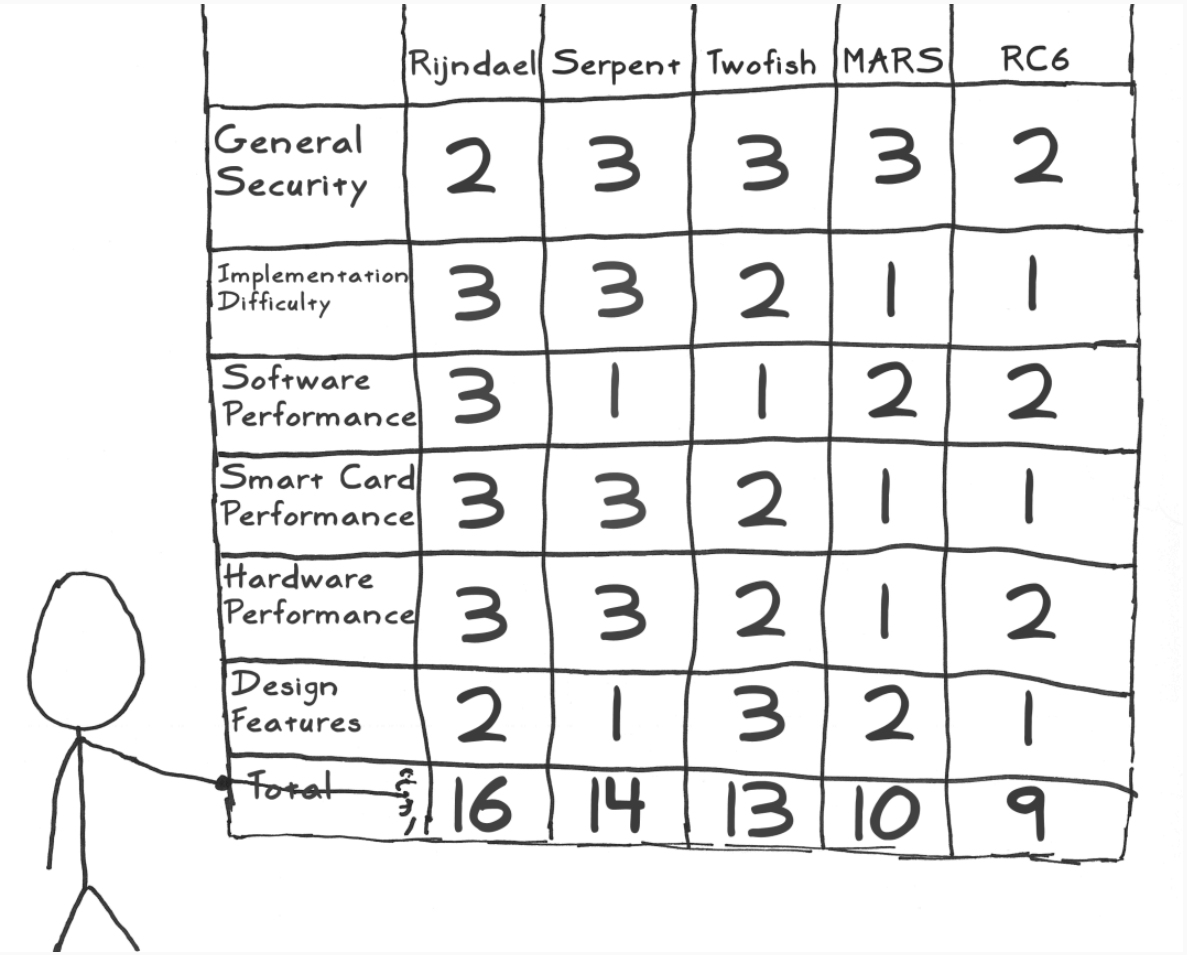
- DES - Designed by IBM and approved by NSA. Standard for 20 years (1977-1997)
- AES - Chosen by selection process over numerous contestants.



Credit: A Stick Figure Guide to the Advanced Encryption Standard (AES)

AES Contest II

Rijndael was chosen as AES. Contestants were evaluated in several metrics, including **hardware performance** and **smart card performance**



Credit: A Stick Figure Guide to the Advanced Encryption Standard (AES)

State-of-the-art

Known **Simple Power Attacks** for AES contest finalists

1. ~~Rijndael~~[4] (AES)
2. ~~Serpent~~[5]
3. Twofish
4. Mars
5. RC6

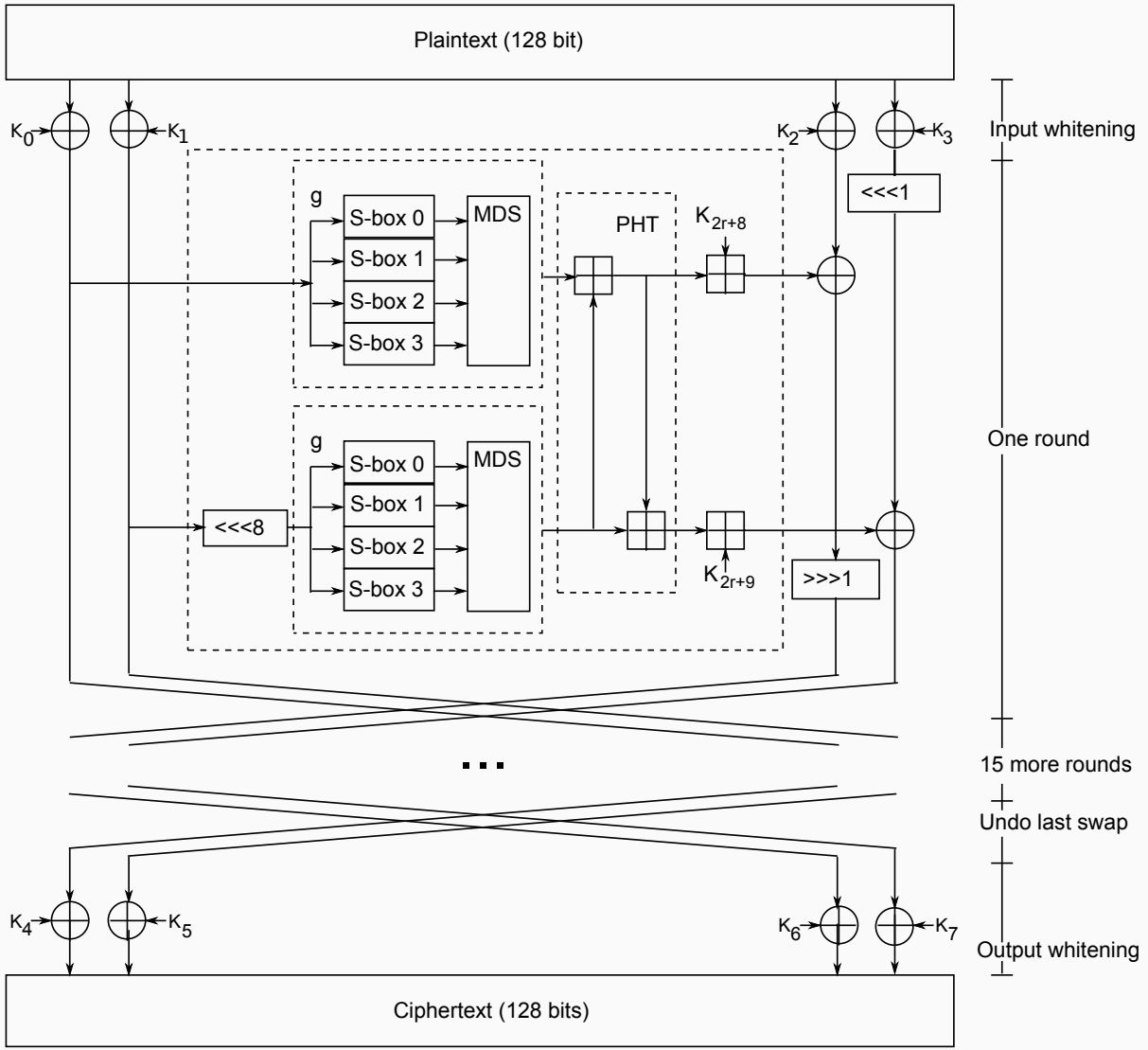
Known attacks describe how to recover the **secret key** from a single power reading.

[4] Joel VanLaven, Mark Brehob, and Kevin J. Compton. A computationally feasible SPA attack on AES via optimized search

[5] Kevin J. Compton, Brian Timm, and Joel VanLaven. A simple power analysis attack on the serpent key schedule

Attack Description

Encryption

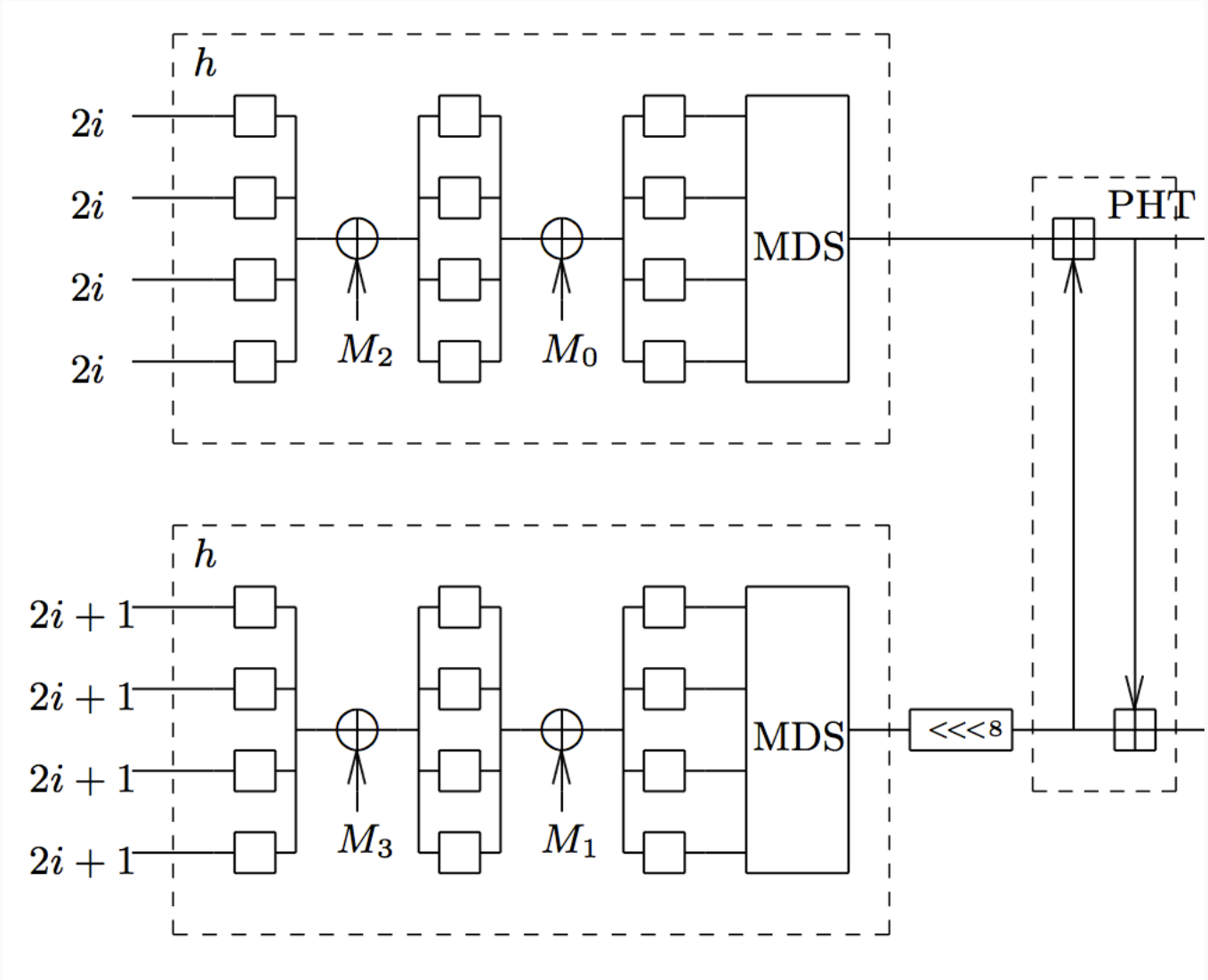


TwoFish can use 128,192 or 256-bit keys. Encryption is performed via 16 feistel rounds and requires the generation of 40 subkeys.

Key Schedule

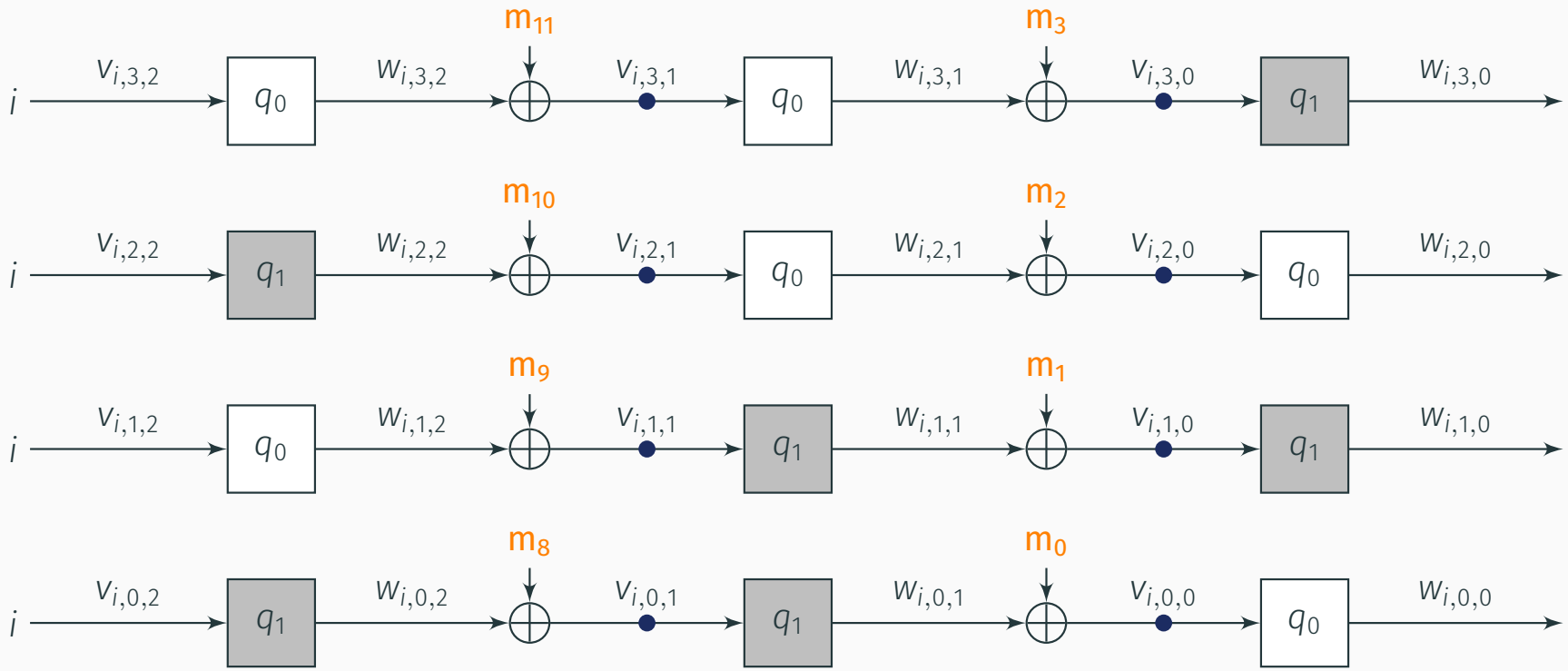
Keys are generated in even and odd pairs.

Each byte of the secret key is used 20 times.



Attack Description I

We want to infer the key from the power reading. Each row is independent, and we know the values of w and the hamming weights of v.



There are 20 values for i, so we can solve for the bytes of the key m. We solve one round at a time from left to right.

Attack Description II

For each byte m_l we have a 20 restrictions. We can do a *first meets all* search through the $2^8 = 256$ possible bytes.

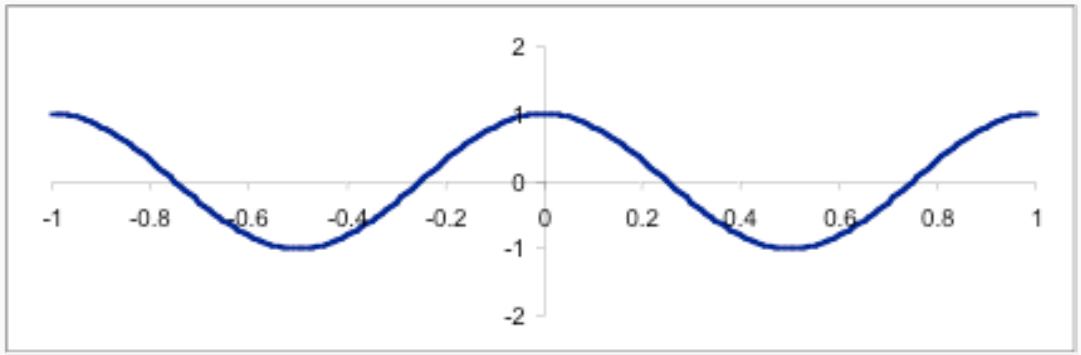
$$\begin{cases} \mathrm{H}\left[v_{0,j,(k-1)}\right] = d_{0,j,k,0} \oplus x_{l,0} + d_{0,j,k,1} \oplus x_{l,1} + \ldots + d_{0,j,k,7} \oplus x_{l,7} \\ \mathrm{H}\left[v_{2,j,(k-1)}\right] = d_{2,j,k,0} \oplus x_{l,0} + d_{2,j,k,1} \oplus x_{l,1} + \ldots + d_{2,j,k,7} \oplus x_{l,7} \\ \mathrm{H}\left[v_{4,j,(k-1)}\right] = d_{4,j,k,0} \oplus x_{l,0} + d_{4,j,k,1} \oplus x_{l,1} + \ldots + d_{4,j,k,7} \oplus x_{l,7} \\ \qquad\qquad \ldots \\ \mathrm{H}\left[v_{38,j,(k-1)}\right] = d_{38,j,k,0} \oplus x_{l,0} + d_{38,j,k,1} \oplus x_{l,1} + \ldots + d_{38,j,R,7} \oplus x_{l,7} \end{cases}$$

Key Size	Accuracy	Avg. Runtime
128	100%	3.75 ms
192	100%	5.7 ms
256	100%	7.39 ms

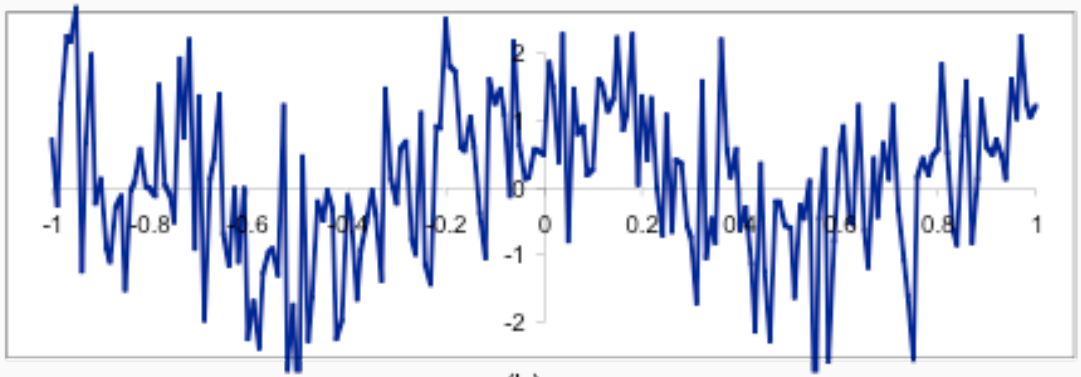
Presence of Noise

The attack so far is not perfect since it does not account for noise.

Power Traces have a non-negligible amount of noise superimposed. If the equipment is correctly tuned, noise will be gaussian and have zero mean.



(a)

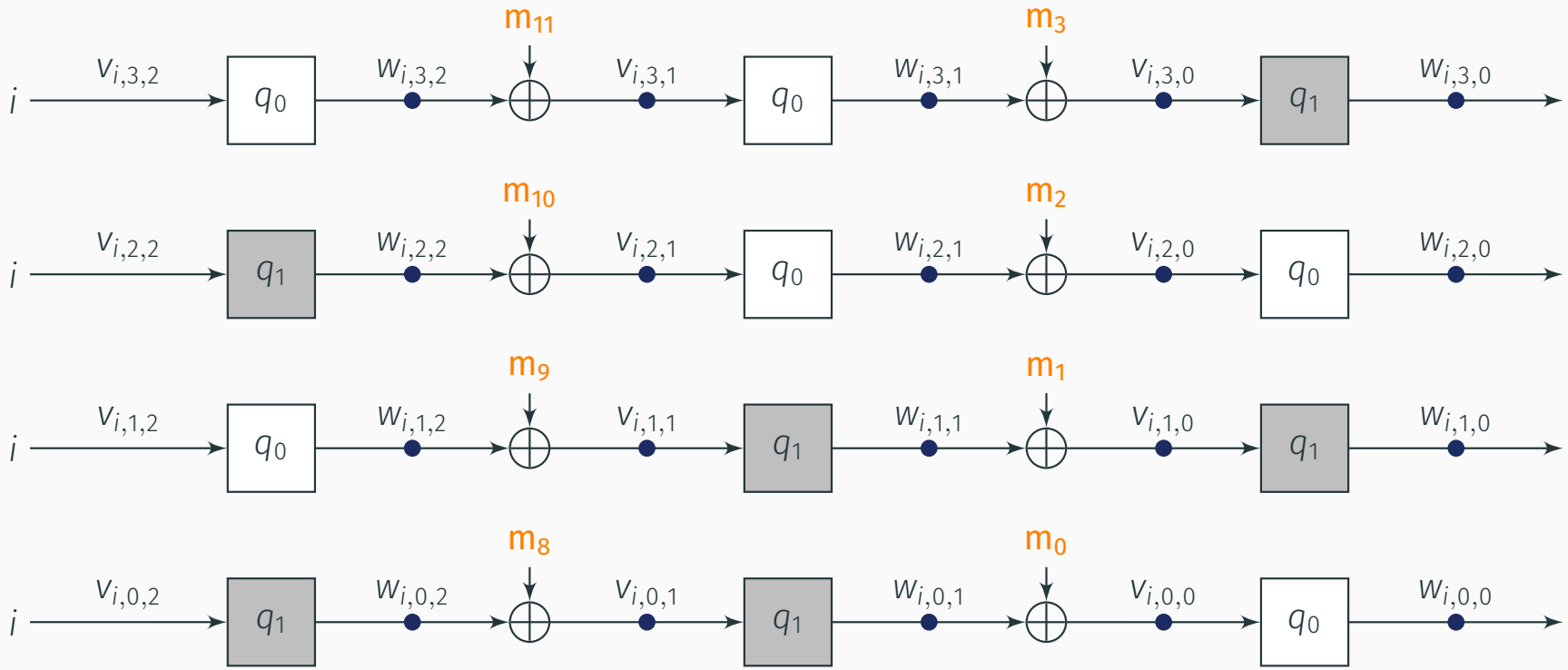


(b)

Least Mean Square Correction I

Let's try again

Due to the noise the system of equations may not have a solution.
Using the hamming weights of w we can transform the XORs to linear restrictions.



Least Mean Square Correction II

In order to solve the system we can use Least Minimum Squares.
Finally, map the values to $\{0, 1\}$ by comparing to 0.5.

$$
\begin{cases}
\mathrm{H}^*_\epsilon\left(v_{0,j,(k-1)}\right) - \mathrm{H}\left[w_{0,j,k}\right] = a_{0,j,k,0} \cdot x_{l,0} + a_{0,j,k,1} \cdot x_{l,1} + \ldots + a_{0,j,k,7} \cdot x_{l,7} \\
\mathrm{H}^*_\epsilon\left(v_{2,j,(k-1)}\right) - \mathrm{H}\left[w_{2,j,k}\right] = a_{2,j,k,0} \cdot x_{l,0} + a_{2,j,k,1} \cdot x_{l,1} + \ldots + a_{2,j,k,7} \cdot x_{l,7} \\
\mathrm{H}^*_\epsilon\left(v_{4,j,(k-1)}\right) - \mathrm{H}\left[w_{4,j,k}\right] = a_{4,j,k,0} \cdot x_{l,0} + a_{4,j,k,1} \cdot x_{l,1} + \ldots + a_{4,j,k,7} \cdot x_{l,7} \\
\ldots \\
\mathrm{H}^*_\epsilon\left(v_{38,j,(k-1)}\right) - \mathrm{H}\left[w_{38,j,k}\right] = a_{38,j,k,0} \cdot x_{l,0} + a_{38,j,k,1} \cdot x_{l,1} + \ldots + a_{38,j,R,7} \cdot x_{l,7}
\end{cases}
$$

Correction masks

Can we do better?

Mistakes are being made when estimating single bytes. Mistakes are propagated to the following rounds.

Not all mistakes are equally likely, we are most probably estimating incorrectly, one or two bits. We can flip individual bits and **minimize the error** to the hamming weights.

h_M000000000
000000001
000000010
000000100
000001000
...
000000011
000000101
000001001
...
111111111

Summary of Noise Correction

Round to nearest integer the whole power trace

For each byte m_l of the key

A. Solve equations with Least Mean Squares
B. Map real valued solutions $\mathbb{R} \to \{0, 1\}$ to get $\hat{m}_l$
C. Find the mask $h_M = 0 \ldots 255$ that minimizes the hamming distance to the measurements of inputs and outputs of the S-boxes. $\hat{m}_l^* = \hat{m}_l \oplus h_M$

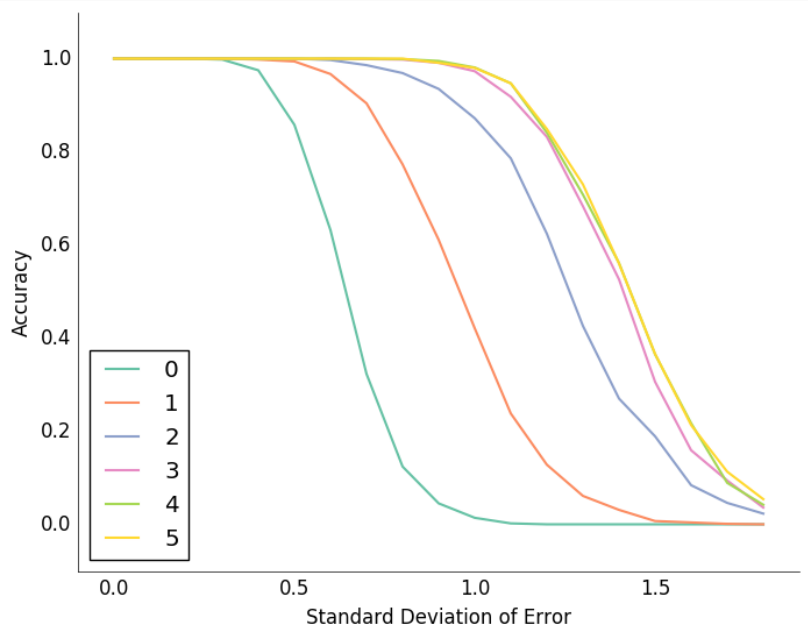
Simulation & Results

Results

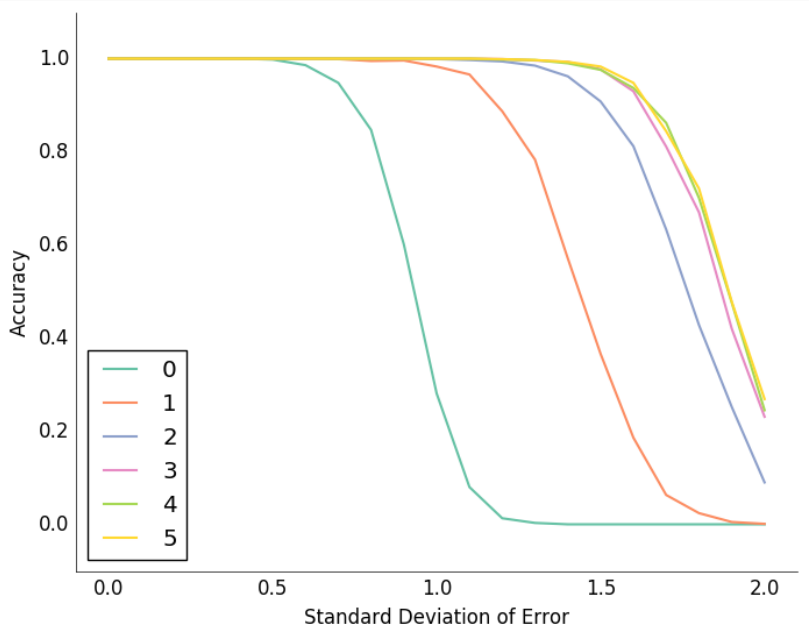
Applying noise correction techniques we can recover the key 99% of the time with $\sigma < 1.0$.

For each σ, mask size and key size combination 1000 simulations were run.

Accuracies 128-bit key



(a) One Reading



(b) Five Readings

Implications

Known **Simple Power Attacks** for AES contest finalists

1. ~~Rijndael~~
2. ~~Serpent~~
3. ~~Twofish~~
4. Mars
5. RC6

This attack can be performed in any implementation of **TwoFish** due to the byte nature of the S-boxes.

Summary

- Embedded Systems are increasing by number everyday and carry large amounts of personal private information.
- Current cryptographic protocols do not have secure implementations for most embedded devices.
- TwoFish has a **noise resistant** simple power attack for all of its implementations (8, 32, 64-bit **C** and **ASM**.)

Further Work

- Are Mars and RC6 secure against SPA?
- Need to devise new algorithms or implementations of current algorithms that are not susceptible to SPA

Thank you!

QUESTIONS

WHY DO WHALES JUMP
WHY ARE WITCHES GREEN
WHY ARE THERE MIRRORS ABOVE BEDS
WHY DO I SAY UH
WHY IS SEA SALT BETTER
WHY ARE THERE TREES IN THE MIDDLE OF FIELDS
WHY IS THERE NOT A POKEMON MMO
WHY IS THERE LAUGHING IN TV SHOWS
WHY ARE THERE DOORS ON THE FREEWAY
WHY ARE THERE SO MANY SVCHOST.EXE RUNNING
WHY AREN'T THERE ANY COUNTRIES IN ANTARCTICA
WHY ARE THERE SCARY SOUNDS IN MINECRAFT
WHY IS THERE KICKING IN MY STOMACH
WHY ARE THERE TWO SLASHES AFTER HTTP
WHY ARE THERE CELEBRITIES
WHY DO SNAKES EXIST
WHY DO OYSTERS HAVE PEARLS
WHY ARE DUCKS CALLED DUCKS
WHY DO THEY CALL IT THE CLAP
WHY ARE KYLE AND CARTMAN FRIENDS
WHY IS THERE AN ARROW ON AANG'S HEAD
WHY ARE TEXT MESSAGES BLUE
WHY ARE THERE MUSTACHES ON CLOTHES
WHY ARE THERE MUSTACHES ON CARS
WHY ARE THERE MUSTACHES EVERYWHERE
WHY ARE THERE SO MANY BIRDS IN OHIO
WHY IS THERE SO MUCH RAIN IN OHIO
WHY IS OHIO WEATHER SO WEIRD
WHY ARE THERE MALE AND FEMALE BIKES
WHY ARE THERE BRIDESMAIDS
WHY DO DYING PEOPLE REACH UP
WHY AREN'T THERE VARICOSE ARTERIES
WHY ARE OLD KLINGONS DIFFERENT
WHY IS THERE HELL IF GOD FORGIVES
WHY IS PROGRAMMING SO HARD
WHY IS THERE A 0 OHM RESISTOR
WHY DO AMERICANS HATE SOCCER
WHY DO RHYMES SOUND GOOD
WHY DO TREES DIE
WHY IS THERE NO SOUND ON CNN
WHY AREN'T POKEMON REAL
WHY AREN'T BULLETS SHARP
WHY DO DREAMS SEEM SO REAL
WHY ARE THERE SQUIRRELS

WHY AREN'T THERE DINOSAUR GHOSTS
WHY DO IGUANAS DIE
WHY DO TESTICLES MOVE
WHY ARE THERE PSYCHICS
WHY ARE HATS SO EXPENSIVE
WHY IS THERE CAFFEINE IN MY SHAMPOO
WHY DO YOUR BOOBS HURT
WHY ARE TREES TALL
WHY ARE THERE SLAVES IN THE BIBLE
WHY DO TWINS HAVE DIFFERENT FINGERPRINTS
WHY ARE AMERICANS AFRAID OF DRAGONS
WHY IS YKK ON ALL ZIPPERS
WHY IS HTTPS CROSSED OUT IN RED
WHY IS THERE A LINE THROUGH HTTPS
WHY IS THERE A RED LINE THROUGH HTTPS ON FACEBOOK
WHY IS HTTPS IMPORTANT
WHY ARE THERE WEEKS
WHY DO I FEEL DIZZY

WHY ARE THERE SWARMS OF GNATS
WHY IS THERE PHLEGM
WHY ARE THERE SO MANY CROWS IN ROCHESTER, MN
WHY AREN'T ECONOMISTS RICH
WHY DO AMERICANS CALL IT SOCCER
WHY ARE MY EARS RINGING
WHY ARE THERE SO MANY AVENGERS
WHY ARE THE AVENGERS FIGHTING THE X MEN
WHY IS WOLVERINE NOT IN THE AVENGERS
WHY IS THERE LAVA
WHY IS PSYCHIC WEAK TO BUG
WHY DO CHILDREN GET CANCER
WHY IS POSEIDON ANGRY WITH ODYSSEUS
WHY IS THERE ICE IN SPACE
WHY ARE THERE ANTS IN MY LAPTOP
WHY IS EARTH TILTED
WHY IS SPACE BLACK
WHY IS OUTER SPACE SO COLD
WHY ARE THERE PYRAMIDS ON THE MOON
WHY IS NASA SHUTTING DOWN
WHY ARE THERE FEMALE MR MIMES
WHY ARE THERE GHOSTS

WHY IS THERE AN OWL IN MY BACKYARD
WHY IS THERE AN OWL OUTSIDE MY WINDOW
WHY IS THERE AN OWL ON THE DOLLAR BILL
WHY DO OWLS ATTACK PEOPLE
WHY ARE AK 47S SO EXPENSIVE
WHY ARE THERE HELICOPTERS CIRCLING MY HOUSE
WHY ARE THERE GODS
WHY ARE THERE TWO SPOCKS
WHY IS LIFE SO BORING
WHY ARE MY BOOBS ITCHY
WHY ARE CIGARETTES LEGAL
WHY ARE THERE DUCKS IN MY POOL
WHY IS JESUS WHITE
WHY IS THERE LIQUID IN MY EAR
WHY DO Q TIPS FEEL GOOD
WHY DO GOOD PEOPLE DIE
WHY IS THERE NO KING IN ENGLAND
WHY ARE DOGS AFRAID OF FIREWORKS
WHY IS MT VESUVIUS THERE
WHY DO THEY SAY T MINUS
WHY ARE THERE OBELISKS
WHY ARE WRESTLERS ALWAYS WET
WHY ARE OCEANS BECOMING MORE ACIDIC
WHY IS ARWEN DYING
WHY AREN'T MY QUAIL LAYING EGGS
WHY AREN'T MY QUAIL EGGS HATCHING
WHY AREN'T THERE ANY FOREIGN MILITARY BASES IN AMERICA
WHY ARE ULTRASOUNDS IMPORTANT
WHY ARE ULTRASOUND MACHINES EXPENSIVE
WHY IS STEALING WRONG
WHY AREN'T THERE GUNS IN HARRY POTTER

WHY ARE THERE TINY SPIDERS IN MY HOUSE
WHY DO SPIDERS COME INSIDE
WHY ARE THERE HUGE SPIDERS IN MY HOUSE
WHY ARE THERE LOTS OF SPIDERS IN MY HOUSE
WHY ARE THERE SPIDERS IN MY ROOM
WHY ARE THERE SO MANY SPIDERS IN MY ROOM
WHY DO SPIDER BITES ITCH
WHY IS DYING SO SCARY
WHY IS THERE NO GPS IN LAPTOPS
WHY DO KNEES CLICK
WHY AREN'T THERE E GRADES
WHY IS ISOLATION BAD
WHY DO BOYS LIKE ME
WHY DON'T BOYS LIKE ME
WHY IS THERE ALWAYS A JAVA UPDATE
WHY ARE THERE RED DOTS ON MY THIGHS
WHY IS LYING GOOD
WHY IS GPS FREE
WHY IS RAIN SO IMPORTANT