Cryptanalysis, Attacks and Side Channel Attacks

B Tech III CSE

April 2024

Dhiren Patel

Cryptanalysis

- Two general approaches to attack a conventional encryption scheme
  - Brute-force attack
    - attacker tries every possible key on a piece of ciphertext
  - Cryptanalytic attack
    - rely on the nature of the algorithm plus perhaps some knowledge of the general characteristics of the plaintext or even some sample plaintext-ciphertext pairs

Brute-force Attack

- Trying every possible key until an intelligible translation of the ciphertext into plaintext is obtained. (Old slide – column 3 and 4 changed)

Key size (bits)	Number of alternative keys	Time required at 1 decryption/ms	Time required at 10^6 decryption/ms
32	$2^{32} = 4.3 \times 10^9$	2^{31} ms = 35.8 minutes	2.15 milliseconds
56	$2^{56} = 7.2 \times 10^{16}$	2^{55} ms = 1142 years	10.01 hours
128	$2^{128} = 3.4 \times 10^{38}$	2^{127} ms = 5.4×10^{24} years	5.4×10^{18} years
168	$2^{168} = 3.7 \times 10^{50}$	2^{167} ms = 5.9×10^{36} years	5.9×10^{30} years
26 characters (permutation)	$26! = 4 \times 10^{26}$	2×10^{26} ms = 6.4×10^{12} years	6.4×10^6 years

Cryptanalytic attacks

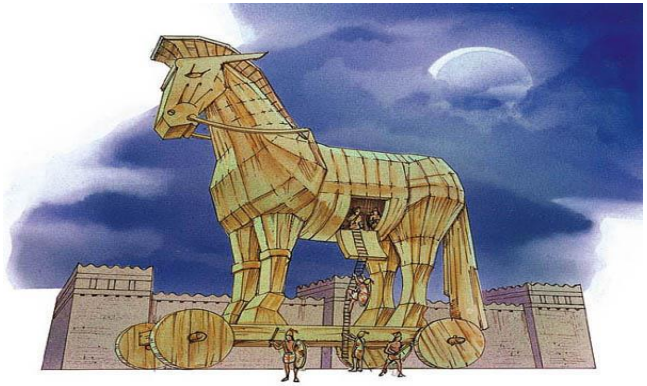
Type of Attack	Known to Cryptanalyst
Ciphertext only	• Encryption algorithm • Ciphertext
Known Plaintext	• Encryption algorithm • Ciphertext • One or more plaintext-ciphertext pairs formed with the secret key
Chosen Plaintext	• Encryption algorithm • Ciphertext • Plaintext message chosen by cryptanalyst, together with its corresponding ciphertext generated with the secret key

Cryptanalytic attacks

Type of Attack	Known to Cryptanalyst
Chosen Ciphertext	• Encryption algorithm • Ciphertext • Purported ciphertext chosen by cryptanalyst, together with its corresponding decrypted plaintext generated with the secret key
Chosen Text	• Encryption algorithm • Ciphertext • Purported ciphertext chosen by cryptanalyst, together with its corresponding decrypted plaintext generated with the secret key • Plaintext message chosen by cryptanalyst, together with its corresponding ciphertext generated with the secret key

Some Attacks

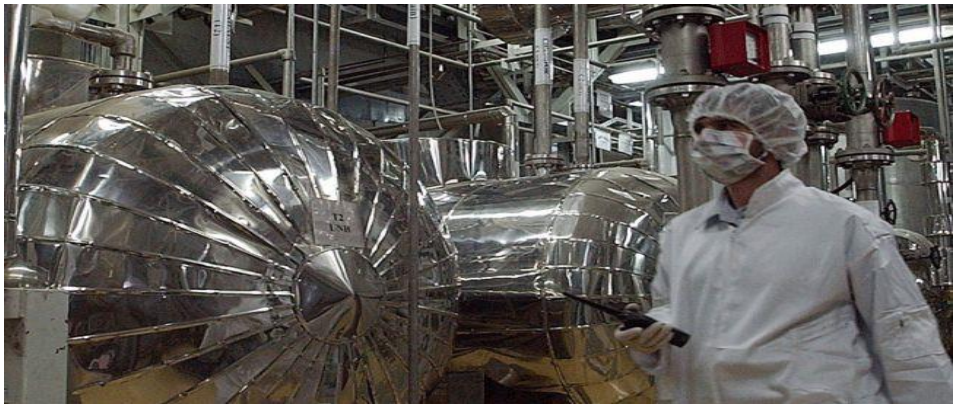
Ancient attackers…



Stuxnet (2009-10)

- Stuxnet was a highly sophisticated computer worm discovered in 2010 that targeted a very specific goal: disrupting Iran's nuclear program
- Target: Stuxnet infected computers that controlled industrial machinery in Iranian nuclear facilities.
- Function: It manipulated these systems to damage uranium enrichment centrifuges by speeding them up and causing them to self-destruct.
- Delivery: The worm spread through infected USB drives and used vulnerabilities in Microsoft Windows systems. (???)

Natanz fuel enrichment plant, Central Iran



9

Stuxnet attack

- The attack also highlighted the vulnerability of industrial control systems to cyberattacks
- It was tailored as a platform for attacking modern SCADA and PLC systems. (SCADA - supervisory control and data acquisition (SCADA), programmable logic controllers (PLC))
- Stuxnet is believed to be responsible for causing substantial damage to the nuclear program of Iran.

More Stuxnet

- Stuxnet specifically targets programmable logic controllers (PLCs), which allow the automation of electromechanical processes such as those used to control machinery and industrial processes including gas centrifuges for separating nuclear material.
- Stuxnet functions by targeting machines using the Microsoft Windows operating system and networks, then seeking out Siemens Step7 software.
- Stuxnet reportedly compromised Iranian PLCs, collecting information on industrial systems and causing the fast-spinning centrifuges, exhausting the uranium faster; to tear themselves apart

Regin (2014)

Regin was a complex cyberattack platform, not a singular attack

Regin functioned as a cyber espionage tool used for long-term intelligence gathering

Regin functioned in stages, with each stage hidden and encrypted. This modular design made it difficult to detect and analyze.

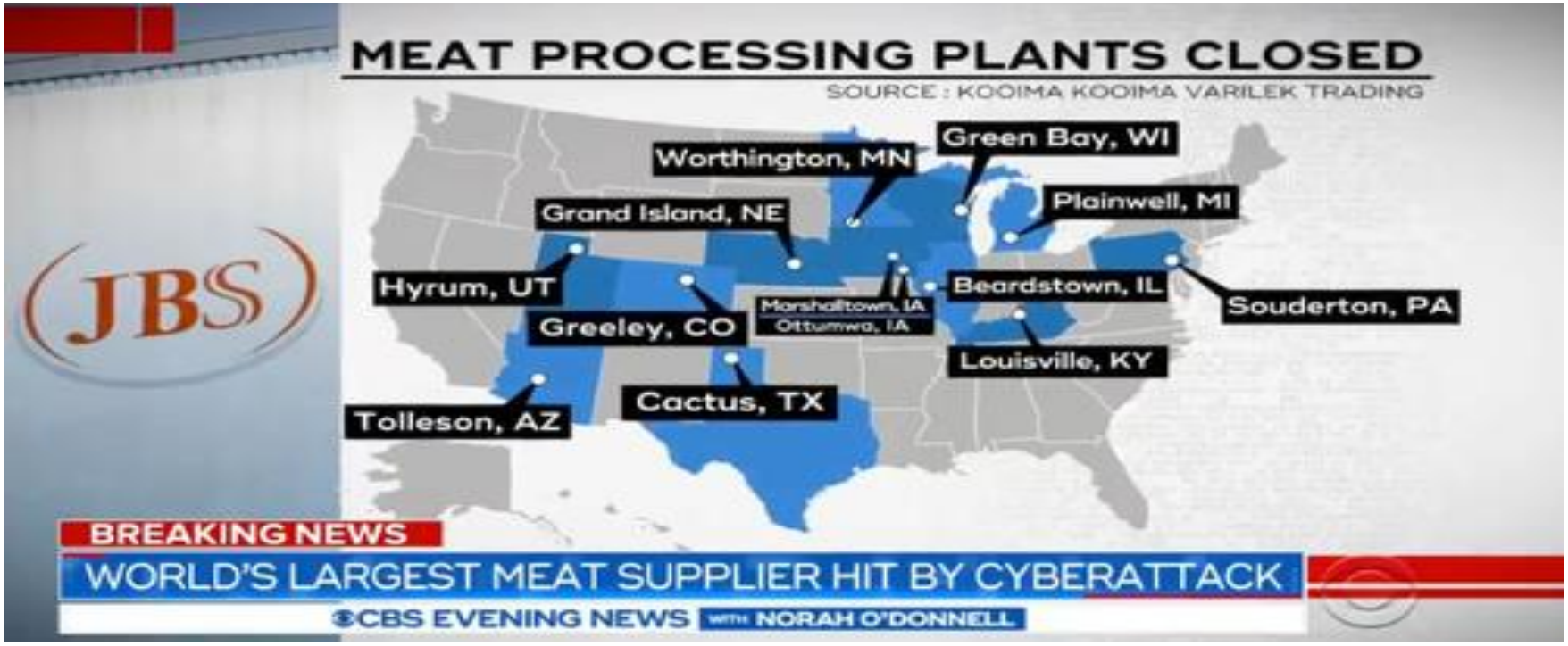
Persistent, long-term mass surveillance operations;
targets specific users of Microsoft Windows-based computers (key scientists/researchers, politicians/leaders, bureaucrats etc.) and has been linked to the intelligence gathering agency NSA and GCHQ.

12

Personalized Attack (Sept 2020)

- A**ttack targeting a German hospital** prevented emergency service personnel from communicating with the hospital, forcing the re-routing of an individual who required emergency services.
- It can happen anywhere – e.g. movement of political leader in the city

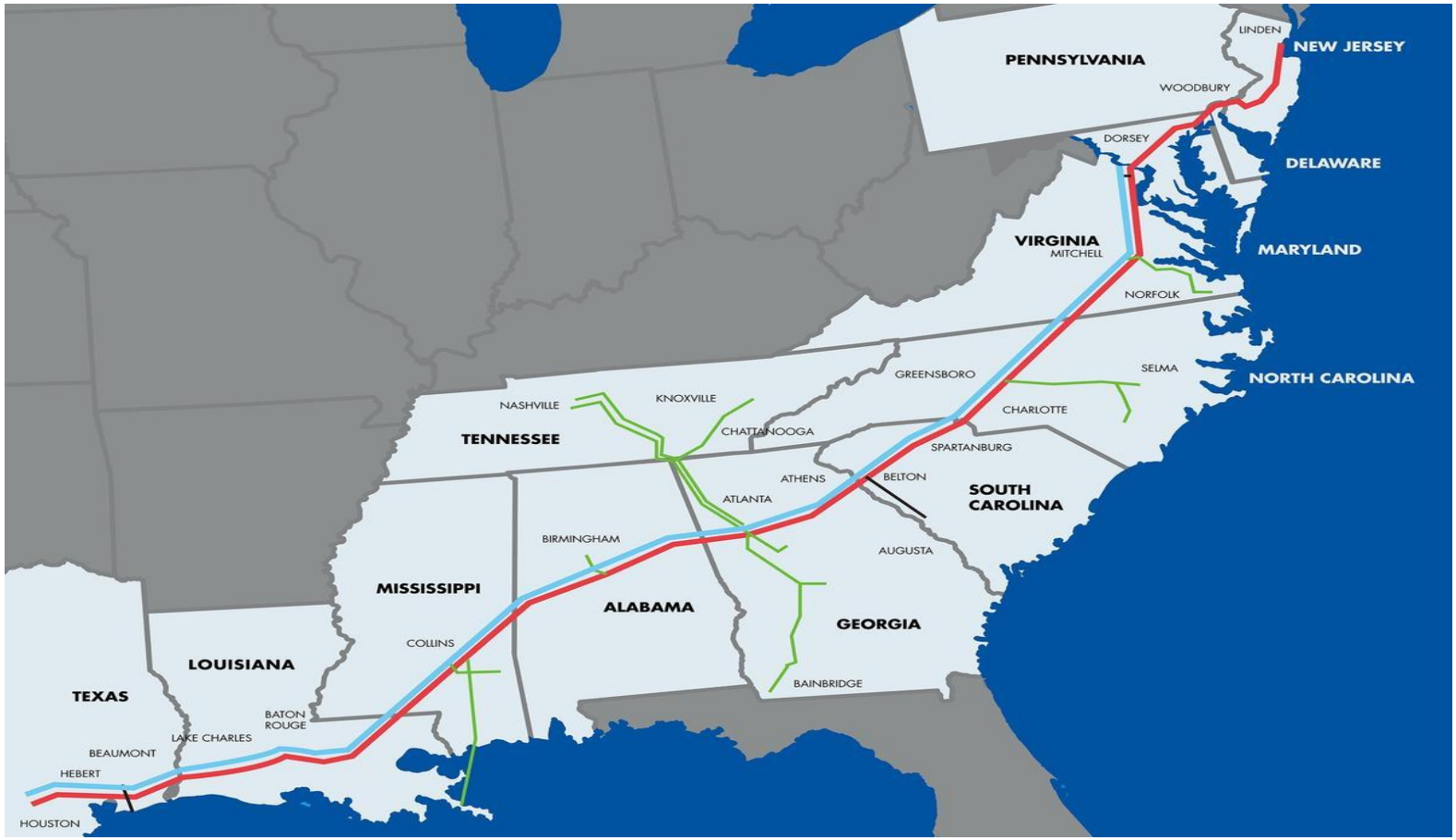
JBS attack (May-June, 2021)



JBS attack

- On May 30, 2021, JBS S.A., a Brazil-based meat processing company, suffered a cyberattack, disabling its beef and pork slaughterhouses. The attack impacted facilities in the United States, Canada, and Australia.
- JBS paid the hackers an $11 million ransom (in Bitcoin).

Colonial Pipeline Attack (May 2021)



Colonial Pipeline Attack

- On May 7, 2021, Colonial Pipeline, an American oil pipeline system that originates in Houston, Texas, and carries gasoline and jet fuel mainly to the Southeastern United States, suffered a ransomware cyberattack that impacted computerized equipment managing the pipeline.
- The Colonial Pipeline Company halted all pipeline operations to contain the attack. The primary target of the attack was the billing infrastructure of the company.
- the company paid the amount that was asked by the hacker group (75 bitcoin or $4.4 million) within several hours

Colonial Pipeline Attack

- The restart of pipeline operations began at 5 p.m. on May 12, ending a six-day shutdown
- On June 7, the US Department of Justice announced that it had recovered 63.7 of the bitcoins from the ransom payment
- Through possession of the private key of the ransom account, the FBI was able to retrieve the Bitcoin, though it did not disclose how it obtained the private key.
- Bitcoin nose dived with a fear that FBI has broken ECC – recovered next day.

AIIMS and NIC (Dec 1st week, 2022)

- **5 AIIMS Servers Hacked, 1.3 TB Data Encrypted in Recent Cyberattack, Govt Tells RS**
- Media reports citing investigators had earlier revealed that records of nearly 3-4 crore patients, including high-profile politicians, were compromised.
- AIIMS Delhi server attack was by the Chinese, FIR details that the attack had originated from China. Of 100 servers (40 physical and 60 virtual), five physical servers were successfully infiltrated by the hackers.

USA (Oct 10, 2022)

- The distributed denial of service (DDoS) attacks hit the airport websites of several major US cities including Atlanta, Chicago, Los Angeles, New York, Phoenix and St Louis.
- A DDoS attack involves knocking a website offline by flooding it with traffic. (made it inaccessible to the public).
- pro-Russian hacking group known as "KillNet" published a list of sites and encouraged its followers to attack them

Iran (Oct 9, 2022)

- the group Edalat-e Ali (Ali's Justice) – Iran
- "Woman, Life, Freedom"
- the biggest wave of social unrest
- new tactics to spread their message of resistance in public spaces
- (e.g. altering the wording of a government billboard, footage from the Ghezel Hesar prison was released to the public, Several water features in the Iranian capital were said to have been coloured blood-red)

Side Channel Attacks (Cryptanalysis)

- Black box model….

Side channel attack

- If Alice wants to secure her home, she could buy high-quality locks and install several of them on her door.
- However, a clever burglar might simply unscrew the hinges, remove the door and walk away with all of Alice's valuables with minimal effort.
- This example of an indirect attack on household security - there exists a parallel in the world of encryption that is quite real.
- It is called the side channel attack and it has been used to defeat some of the most popular encryption techniques!!!

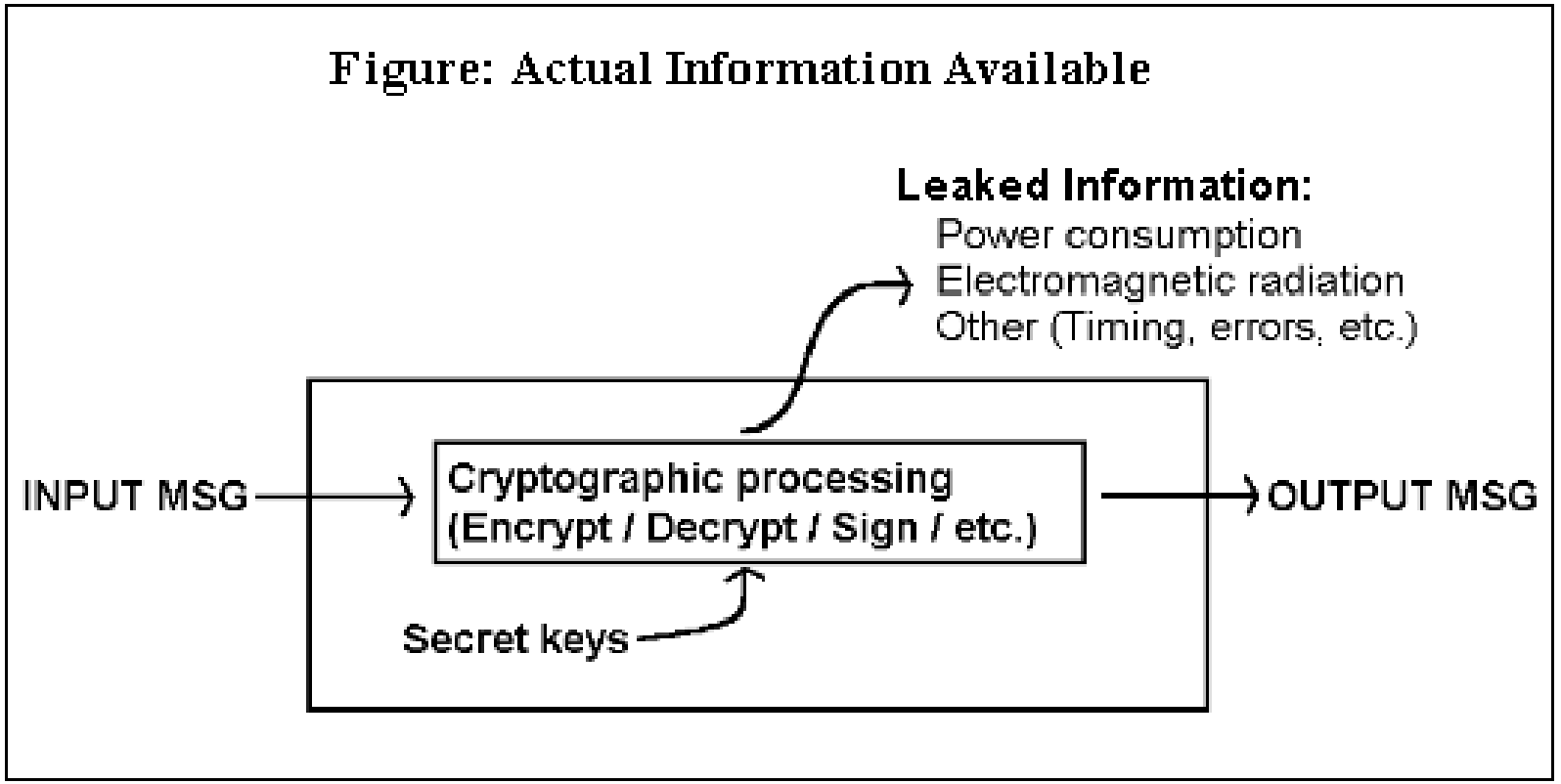
Side channel attacks

- EMI – e.g. CRT, copy of tty in next room
- Traffic analysis - war zones - Military movement, optical – IR US embassy
- Timing analysis (later slides)
- Power Consumption: Monitoring fluctuations in the embassy's power grid might give clues about overall activity levels, but wouldn't reveal specific data.
- Temperature Changes: Similarly, monitoring temperature changes in specific areas could hint at equipment usage patterns, but wouldn't provide concrete information.

Misc…

- In the 1980s, Soviet eavesdroppers were suspected to plant bugs inside IBM electric typewriters to monitor the **electrical noise** generated as the type ball rotated and pitched to strike the paper; the characteristics of those signals could determine which key was pressed.

Side channel attacks

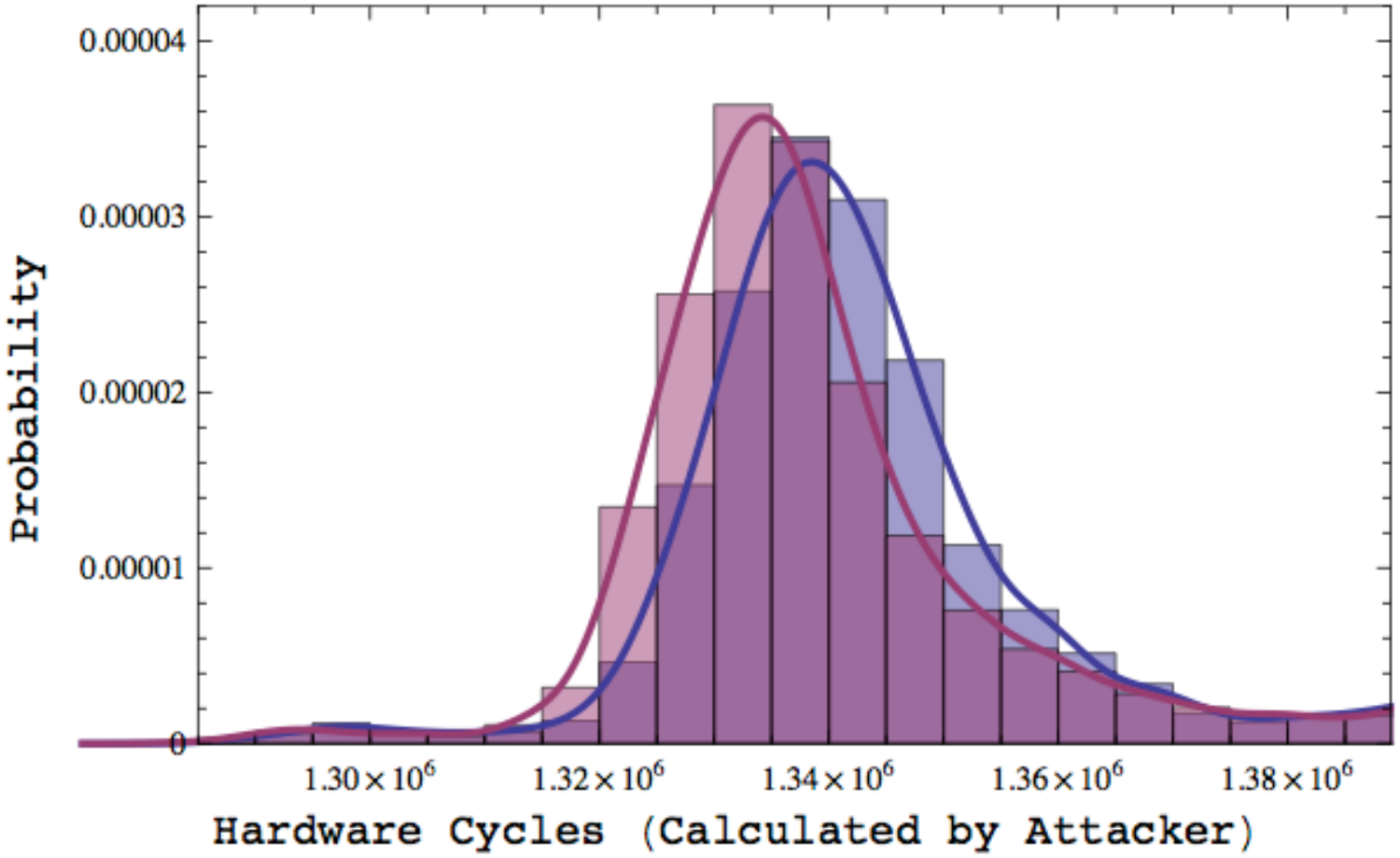


Timing attack

- Timing attacks are based on measuring how much time various computations take to perform.
- By observing variations in how long it takes to perform cryptographic operations, it can be possible to determine the entire secret key

Timing Attacks

- Timing attacks are a form of side channel attack where an attacker gains information from the implementation of a cryptosystem rather than from any inherent weakness in the mathematical properties of the system.
- Such attacks involve statistical analysis of timing measurements

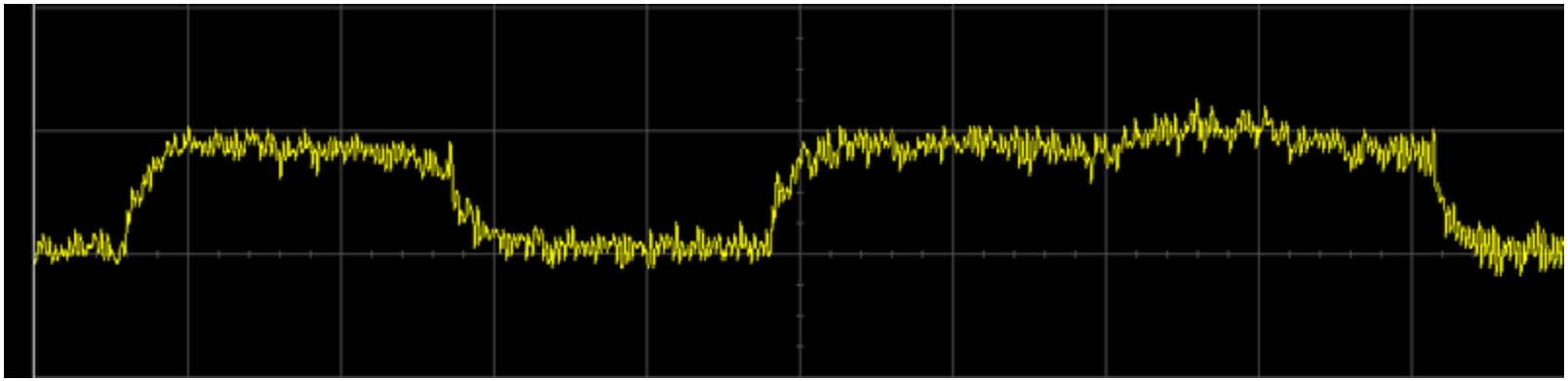

0.00004
0.00003
0.00002
0.00001
0
Probability
1.30×10^6
1.32×10^6
1.34×10^6
1.36×10^6
1.38×10^6
Hardware Cycles (Calculated by Attacker)

Countermeasures

- multiplications take a constant amount of time, independent of the size of the factors
- Montgomery algorithm
- Chinese Reminder Theorem
- Blinding

Power analysis

- by observing the power consumption of a hardware device such as CPU or cryptographic circuit



- Power variations, observed during work of the embedded processor, computing RSA signatures.
- The left (short) peak represents iteration without multiplication, and the right represents iteration with multiplication.
- The low power pause between iterations has been artificially implemented to make key decoding trivial.

Countermeasures (Side channel attacks)

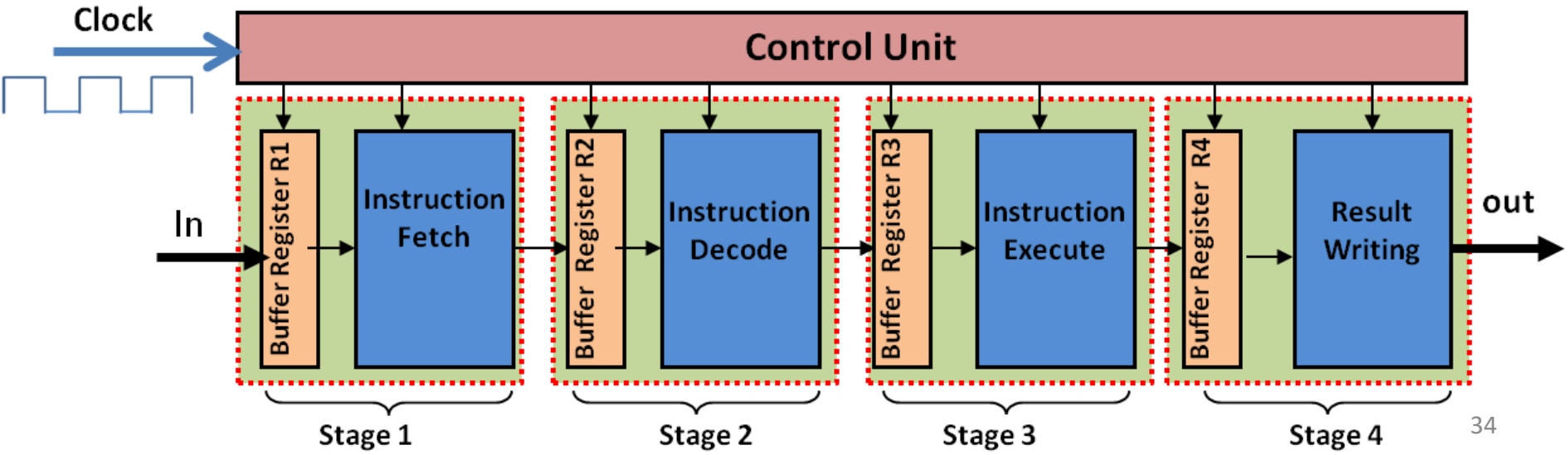
- Special shielding
- JAM
- Random delay
- Instruction set design
- constant execution path

Countermeasures

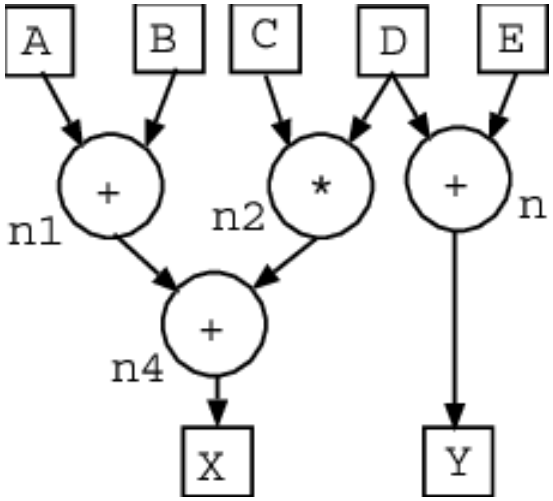
- E.g. RISC/CISC – pipelining, bubble, Instruction Set Design, weak computing device (smart card)
- RISC – Reduced Instruction Architecture, 80% of the CISC instructions are not been used most of the time!! (design a processor around 20% instructions and handle other less used instructions (when they appear in program) through micro-programming)
- Orthogonal instruction set – all instructions use similar time cycles (e.g. logic, arithmetic, read/write etc.) (loose efficiency, gain security – adversary cannot make out now, which instruction is under going execution by looking at timing analysis)

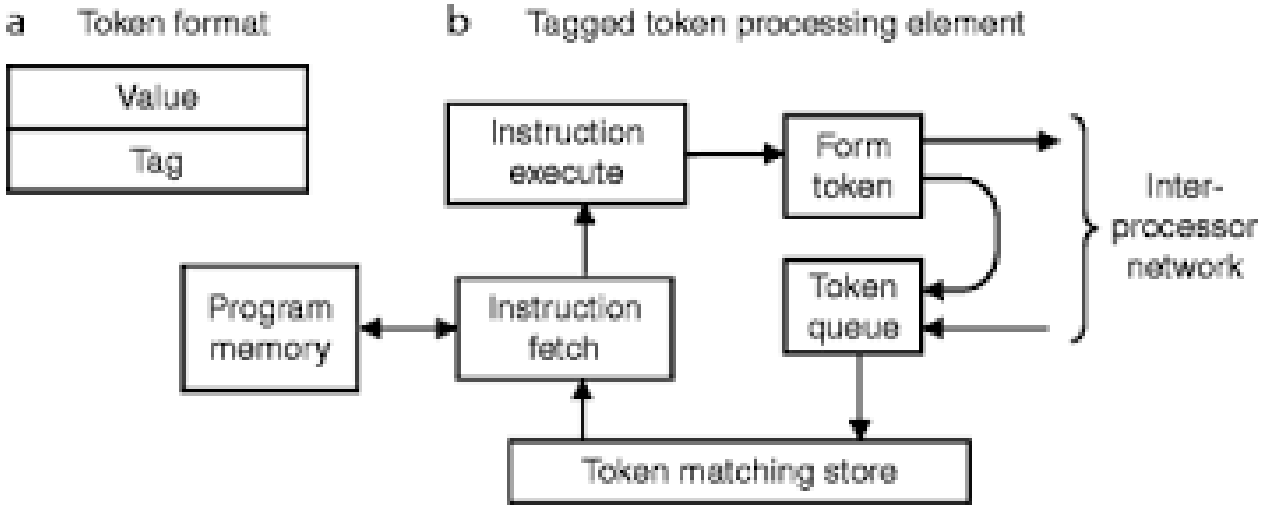
Instruction set architecture

- 3 address instructions – Von Neuman Architecture
- Serial execution of instructions, Address of instructions read from Program counter
- Due to Pipelining (see fig.), they may produce wrong outcome, as they are fetching old values from of operands, and compute – synchronization issue



Data flow graph – from simple program, Dataflow processor architecture (no Program counter)





Scalable v/s Targeted attacks

- When does targeting make sense for an attacker?
- Low yield automated attacks
- Expensive – high touch social engineering attack
- Drive-by-download, self replicating,
- Physical side channel, targeted

Security? What it is?

- Protecting from whom?
- Protecting what? Why?
- Who is good? White List
- Who is bad? Black List (Subjective)
- How to decide? Gray list
- Examples – Putin v/s Zelenski, Gaza
- Designing Security Systems