Cryptanalysis and Side Channel Attacks (CS302 Information Security and Cryptography)

Dhiren Patel, NIT Surat

(9 Feb 2023)

Background

- Classical ciphers, Weaknesses
- Hacking, Industry requirement
- Breaking or checking the strength!!
- (Hackers are computer experts that use advanced programming skills to neutralize security protocols and gain access to devices or networks.)

Type of Hackers

- **Black hat hackers -** Black hat hackers are cybercriminals that illegally crack systems with malicious intent.
- **White hat hackers -** White hat hackers are ethical security hackers who identify and fix vulnerabilities with the permission of organization.
- **Gray hat hackers -** Gray hat hackers may not have the criminal or malicious intent of a black hat hacker, but they also don’t have the prior knowledge or consent of those whose systems they hack into. Nevertheless, when gray hat hackers uncover weaknesses and vulnerabilities, they report them rather than fully exploiting them.

Ethical Hacking
(Security career opportunities)

- Ethical hacking involves an authorized attempt to gain unauthorized access to a computer system, application, or data.
- Carrying out an ethical hack involves duplicating strategies and actions of malicious attackers.
- **Blue hat hackers:** Blue hat hackers are white hat hackers who are actually employed by an organization to help improve their security systems by conducting penetration tests.

Open AI: Chat GPT
(news Feb first week, 2023)

- <ChatGPT has raised alarm among cybersecurity researchers for its unnerving ability in composing everything from sophisticated malware to phishing lures>
- ChatGPT makes life easier and simpler for threat actors in terms of creating an attack with little previous knowledge of technical capabilities
- <Positive - You can actually put a piece of code into ChatGPT and ask it to identify the malicious part in it – so indeed, it can aid a lot>

Chat GPT

- Malicious Code Analysis, Predicting Threats
- the **OpenAI AI Text Classifier**, the **Content at Scale AI Detector**, and the **GPT-2 Output Detector**

DES and AES

- NIST FIPS 46 (DES – Jan 1977)
- FIPS 46-3 Triple DES (3DES) - applies the DES cipher algorithm three times to each data block
- NIST FIPS 197 (AES - November 2001)
- (Dec 2022) request for update - **Classical security, Key size and Post quantum security and Implementation Security (Side Channel)**

Quantum computing

- Quantum computing uses quantum mechanics to perform operations on data at much greater speeds than modern computers.
- Many times more powerful than an average desktop PC, quantum computers are attractive in calculation-heavy cryptography, but are much more challenging to build, program, and use.
- Their speed and processing power, crypto enthusiast fear, may one day be able to break the encryption used to secure Bitcoin.

Estimate by University of Sussex

- a quantum computer with 1.9 billion qubits could essentially crack the encryption safeguarding Bitcoin within a mere 10 minutes.
- Just 13 million qubits could do the job in about a day.
- IBM unveiled its 127-qubit processor in 2021, while a unit sporting 1,000 qubits is set to be completed by the end of 2023.

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 (old slide)

- Trying every possible key until an intelligible translation of the ciphertext into plaintext is obtained.

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

Cryptanalytic attacks

- Weak structures
- Mathematical strength (RSA example)
- NP-Complete and NP-Hard
- Advancement in Technology (Computing)
- Fundamentals/Foundations change

One time pad and Two time pad

- Assignment discussion
- The system can be expressed as:

$c_i = m_i \oplus k_i$ – Encryption

$m_i = c_i \oplus k_i$ – Decryption //??

- where, $m_i = i^{th}$ binary digit of plain text
- $k_i = i^{th}$ binary digit of key material
- $c_i = i^{th}$ binary digit of cipher text
- $\oplus$ = exclusive-or (XOR) operation
- Random key generator
- Key discovery (16.5%) – due to ASCII plaintext nature
- Discovering msgs that are encrypted with two-time-pad!

Side Channel Attacks

- 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 timing attack and it has been used to defeat some of the most popular encryption techniques!!!

Side Channel Attacks (Cryptanalysis)

- Black box model….
- Side-channel attacks (SCAs) aim at extracting secrets from a chip or a system, through measurement and analysis of physical parameters.
- Timing information, power consumption, electromagnetic leaks, and sound are examples of extra information which could be exploited to facilitate side-channel attacks.

SCA

- These attacks pose a serious threat to modules that integrate cryptographic systems, as many side-channel analysis techniques have proven successful in breaking an algorithmically robust cryptographic operation and extracting the secret key.

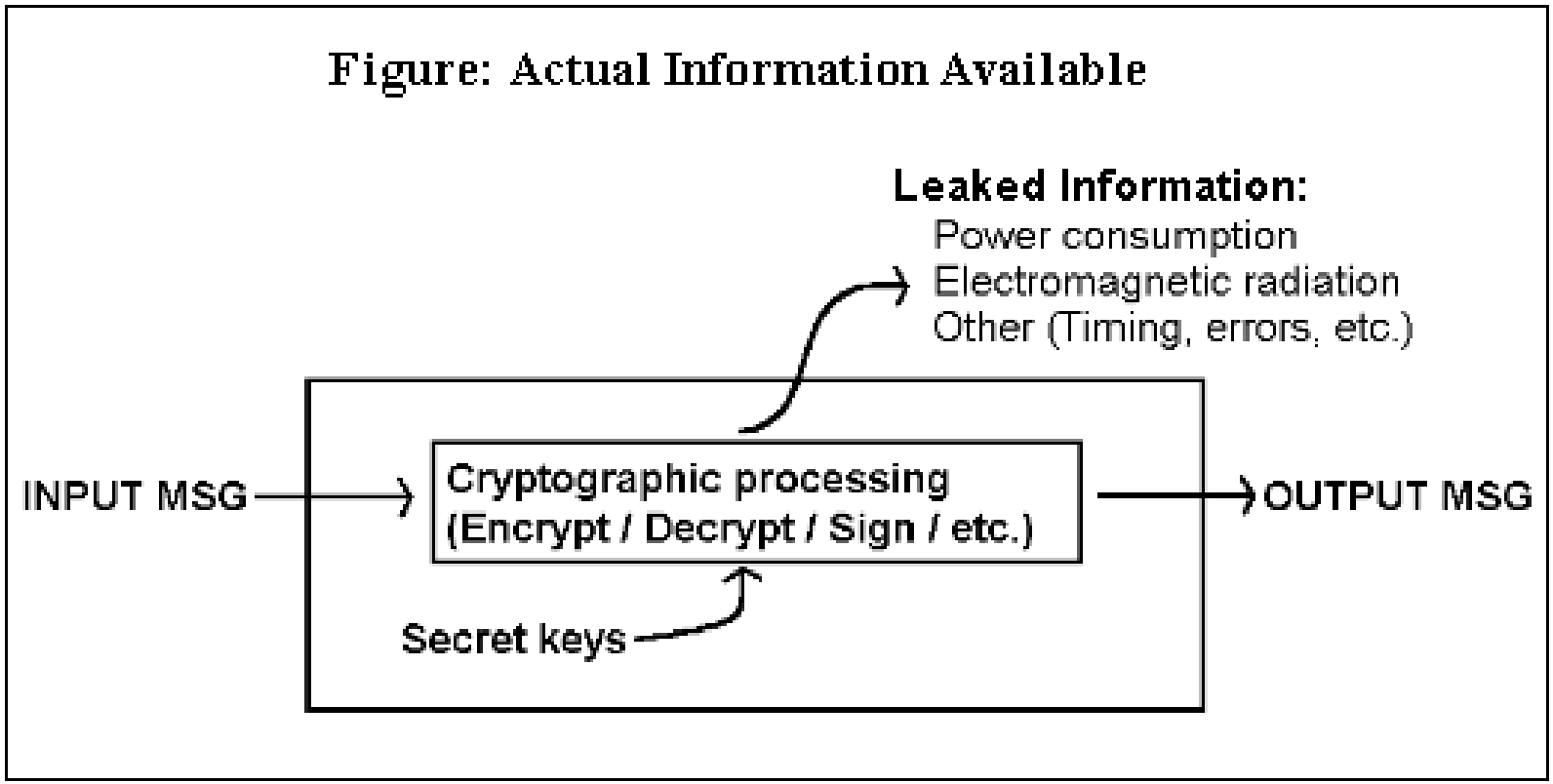
Side channel attacks

- EMI – e.g. CRT, copy of tty in next room
- Traffic analysis - war zones - Military movement,
- optical – IR US embassy
- Timing analysis (next slide)
- Power analysis

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

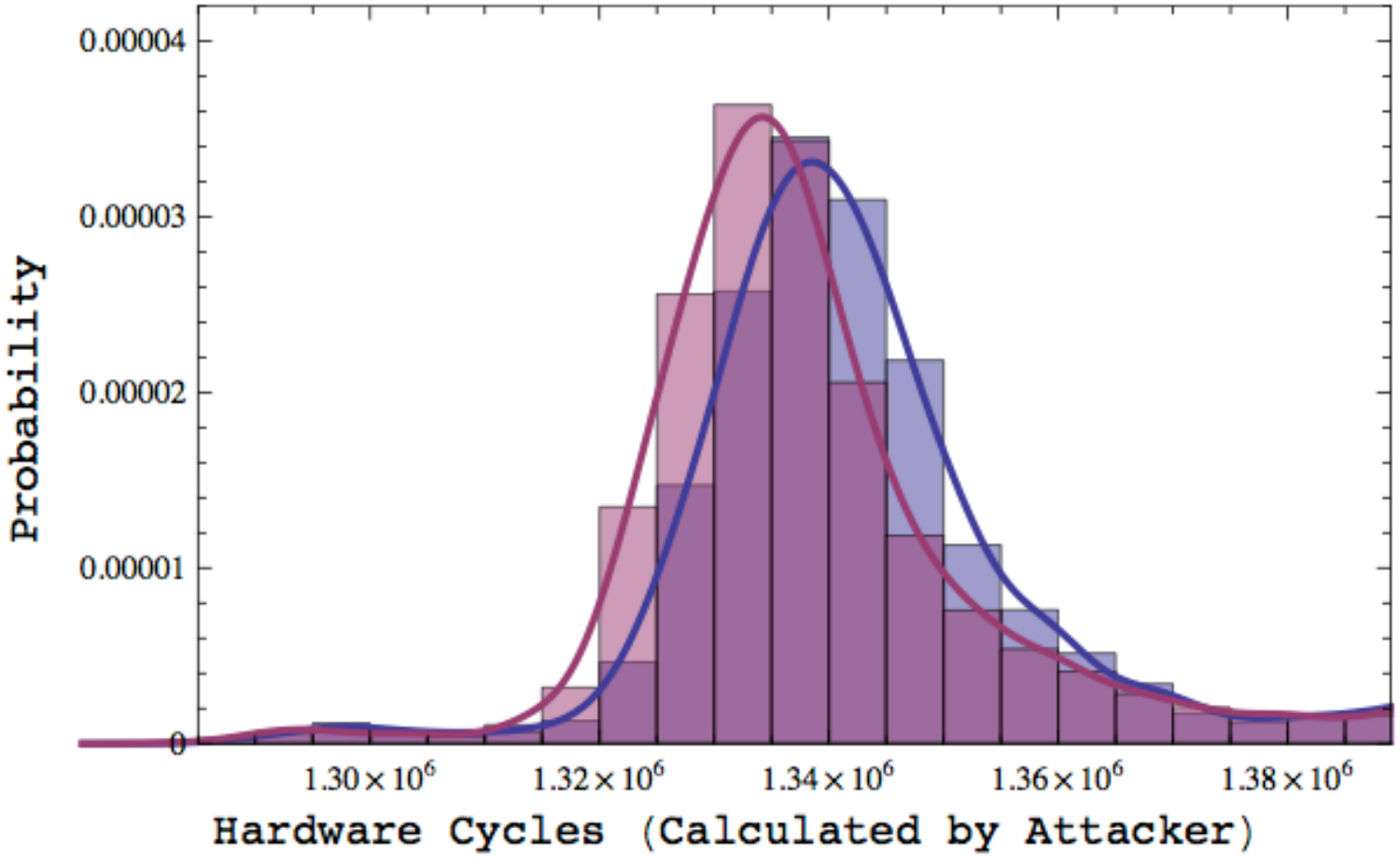


Timing attack

- 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 attack

- 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

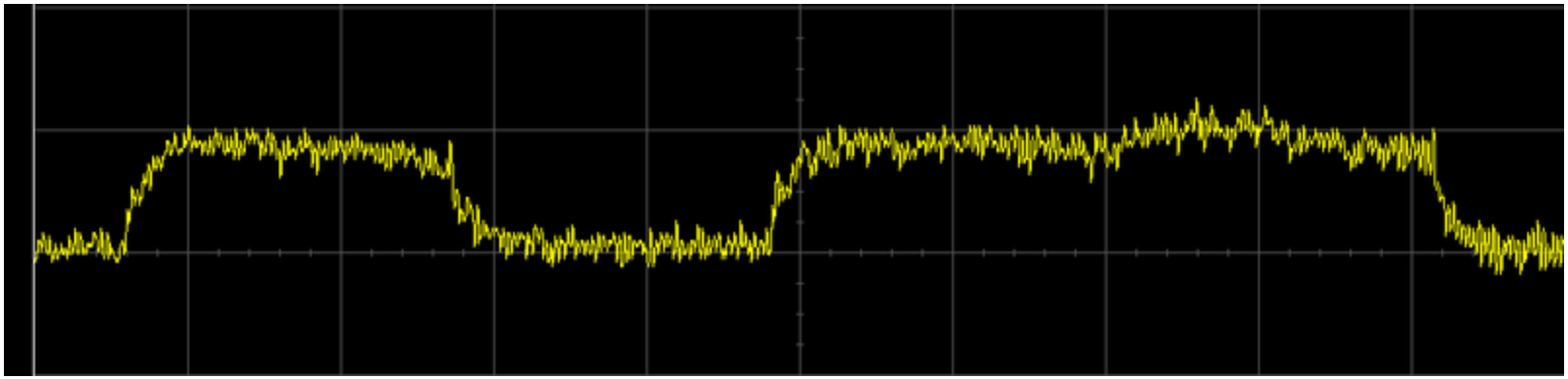
- multiplications take a constant amount of time, independent of the size of the factors
- Montgomery algorithm
- Chinese Reminder Theorem
- Blinding

Power attack

- Power attacks that make use of varying power consumption by the hardware during computation.

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 Background

- E.g. RISC/CISC – pipelining, bubble, Instruction Set Design, weak computing device (smart card)
- Countermeasures – orthogonal instruction set design
- Example – Von Neuman (Program counter) v/s Data Flow Architecture

Countermeasures
(Side channel attacks)

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

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

Cryptography Classification

- Cryptographic systems are characterized along three independent dimensions:

1. The type of operations used for transforming plaintext to cipher text
   - E.g. Substitution, transposition etc.
2. The type of keys used
   - Symmetric key
   - Asymmetric key (different keys for encryption/decryption)
3. The way in which the plaintext is processed
   - Block cipher
   - Stream cipher (one by one – bit/char)