New Trends in Cryptology and Cybersecurity

Erkay SAVAŞ

Sabancı Üniversitesi

Research Areas

- Applied Cryptography
- Postquantum Cryptography
- Homomorphic Encryption
- Privacy-Preserving Intrusion Detection
- Security in Big Data
- Side-Channel Attacks and Prevention
- Dynamic malware/APT Detection
- Cyber Intelligence + Machine Learning + Cyber Security

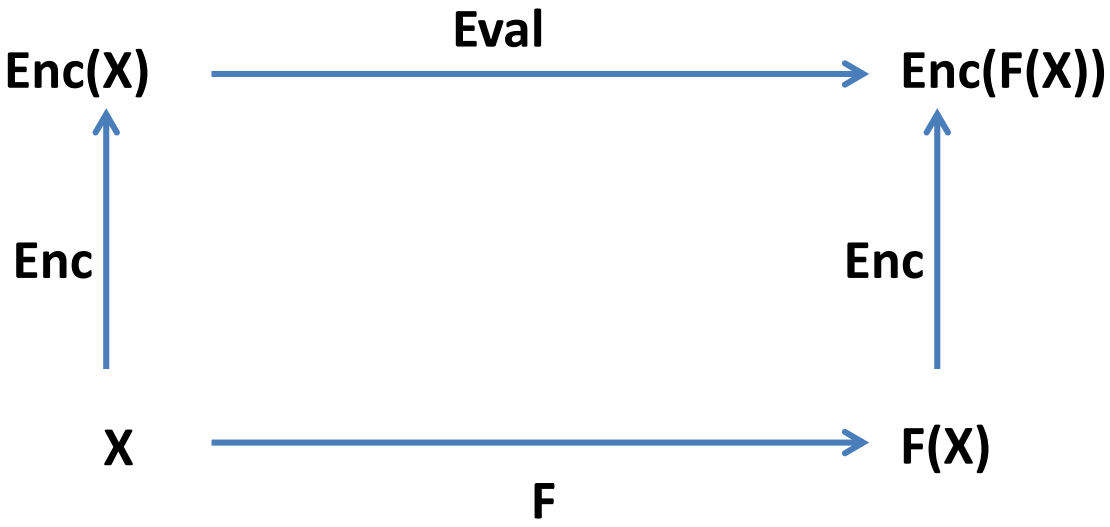
Quantum Computers

- Recent progress in building quantum computers
  - Their computing power increases exponentially in number of qubits
    - Google reported 72 qubit quantum computers
    - D-Wave reported 2000 qubit quantum computers
  - We have to change almost all cryptographic algorithms – especially public key cryptography algorithms
    - No RSA, DSA, ECDSA, SSL/TLS, digital signatures (72% of Internet traffic is encrypted by https)
  - New cryptographic primitives based on new and better hardness assumptions.

Related Projects

- ASIC implementation of post-quantum cryptographic algorithms for public key cryptography
- Funded by TÜBİTAK BİLGEM (since April 2018)
- Ending June 2020.

Homomorphic Encryption



Related Projects

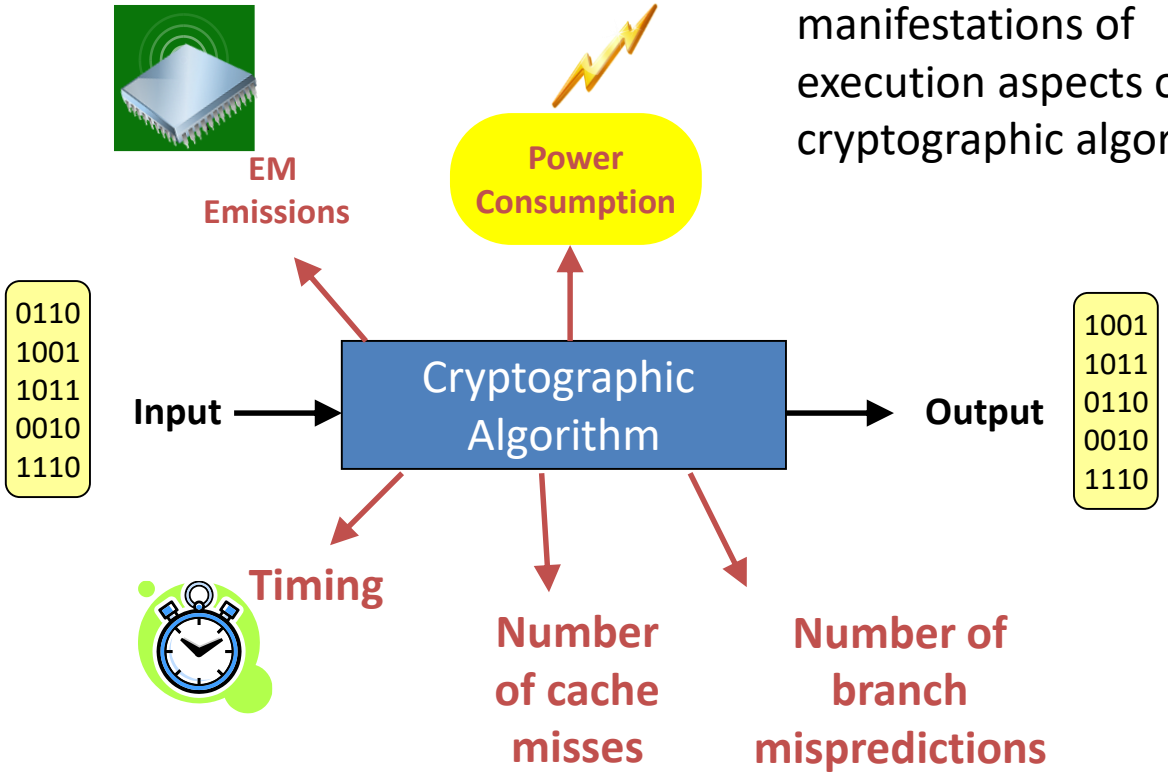
- Funded by TÜBİTAK (since August 2019)
- Acceleration of software libraries for homomorphic cryptographic by FPGA and GPU
- Application of homomorphic encryption such as searchable encryption, PIR, Privacy preserving intrusion detection, end-to-end security for publish-subscribe systems

Security and Privacy in Big Data

- Challenges:
  - Identifying security and privacy issues in big data and its applications
  - Providing efficient and scalable solutions
- Partially funded by Türkiye Finans Katılım Bankası

Side-Channel Attacks and Prevention

Side-channel: Unintended manifestations of execution aspects of cryptographic algorithms



Side-Channel Attacks

- There are notorious attacks such as Meltdown and Spectre
- We developed several techniques to detect and prevents these attacks
- Not currently funded

Dynamic malware/APT detection

- Our focus is detecting ransomware showing APT behavior
- Software based approach
- Collecting system call information
- Machine learning
- Special emphasis on anomaly detection
- Not currently funded

Cyber Intelligence + Machine Learning + Cyber Security

- Collect as much as data possible about attacks, malicious software, mailcious domains, system calls, pcap, etc
- Apply machine learning techiques to learn more about cyber security threats
- Not currently funded