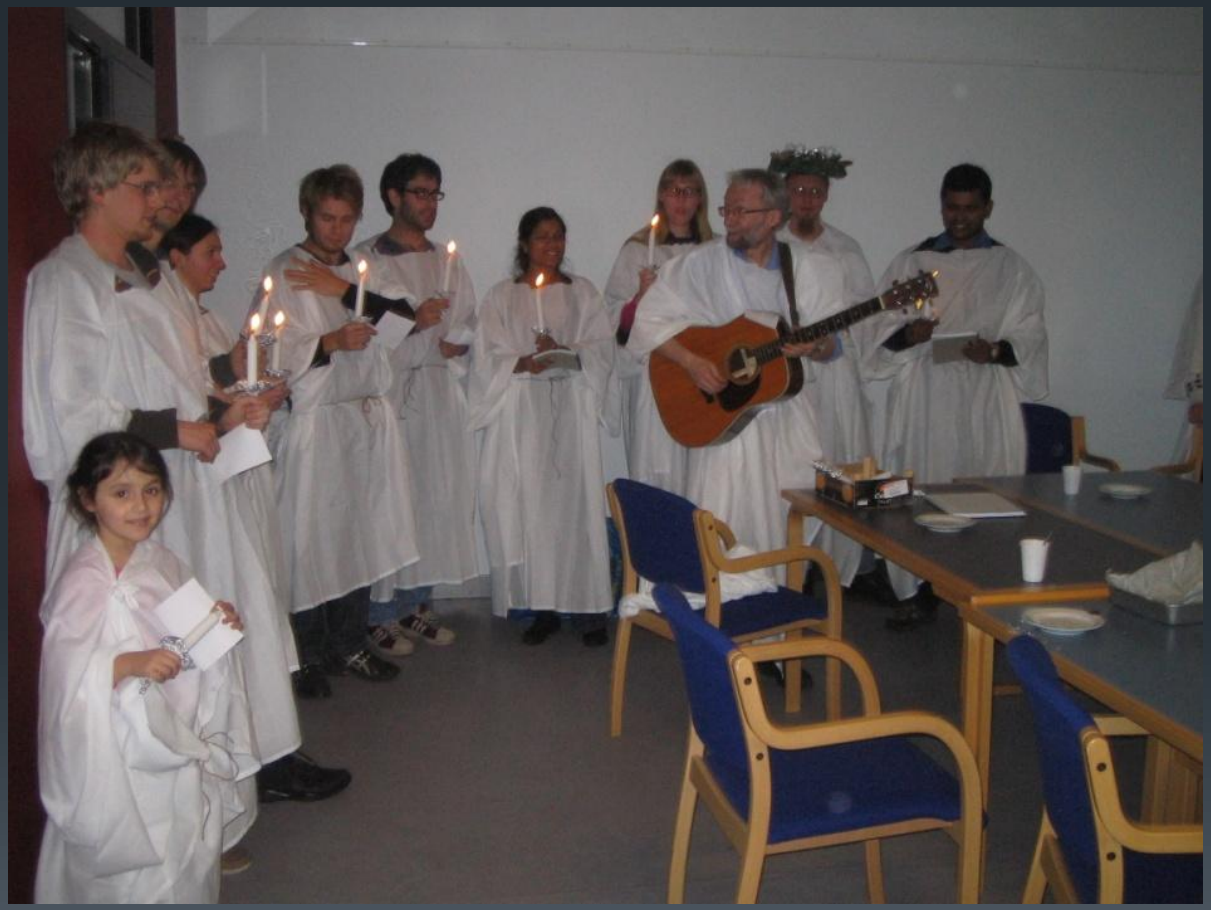
Leakage Resilient Cryptography

Carmit Hazay

Aarhus University

Cryptography and Security Research Group



http://cs.au.dk/research/areas/cryptography-and-security/

Cryptography and Security Research Group

CRYPTOGRAPHY AND SECURITY

MEMBERS OF THE CRYPTOGRAPHY AND SECURITY GROUP AT THE DEPARTMEN

Focus points for the Cryptography and Security group

Public-key cryptography, cryptographic protocols, and quantum cryptography. Public-key cryptography draws inspiration from both complexity theory and algebra, more specifically number theory and algebraic geometry, and is extremely useful in practice. The cryptographic protocol research area is experiencing an extremely fast development, where the group contributes both to the basic theory of the field and to efficient constructions and implementations. In quantum cryptography, the group contributes with efficient experimental implementations as well as theoretical work.

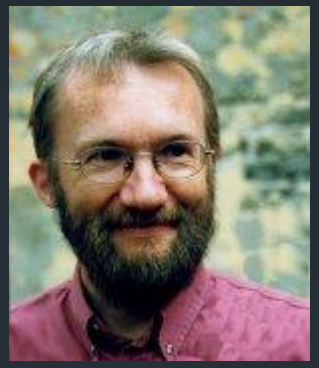
Permanent Staff

Ivan Bjerre Damgård

Email: ivan@cs.au.dk
Office: bldg.-5342 216
Phone: +45 8942 5780

Jesper Buus Nielsen

Email: buus@cs.au.dk
Office: bldg.-5342 218
Phone: +45 8942 5776



Cryptography and Security Research Group

Secure Multi-party Computation

Leakage Resilient Cryptography

and more...

Quantum Cryptography

What is Cryptography?

What is Cryptography?

Wikipedia: "The practice and study of hiding information"

- Most known task is encryption
- I.e., the process of transferring information privately against unauthorized user

Encryption Scheme

The classic problem:

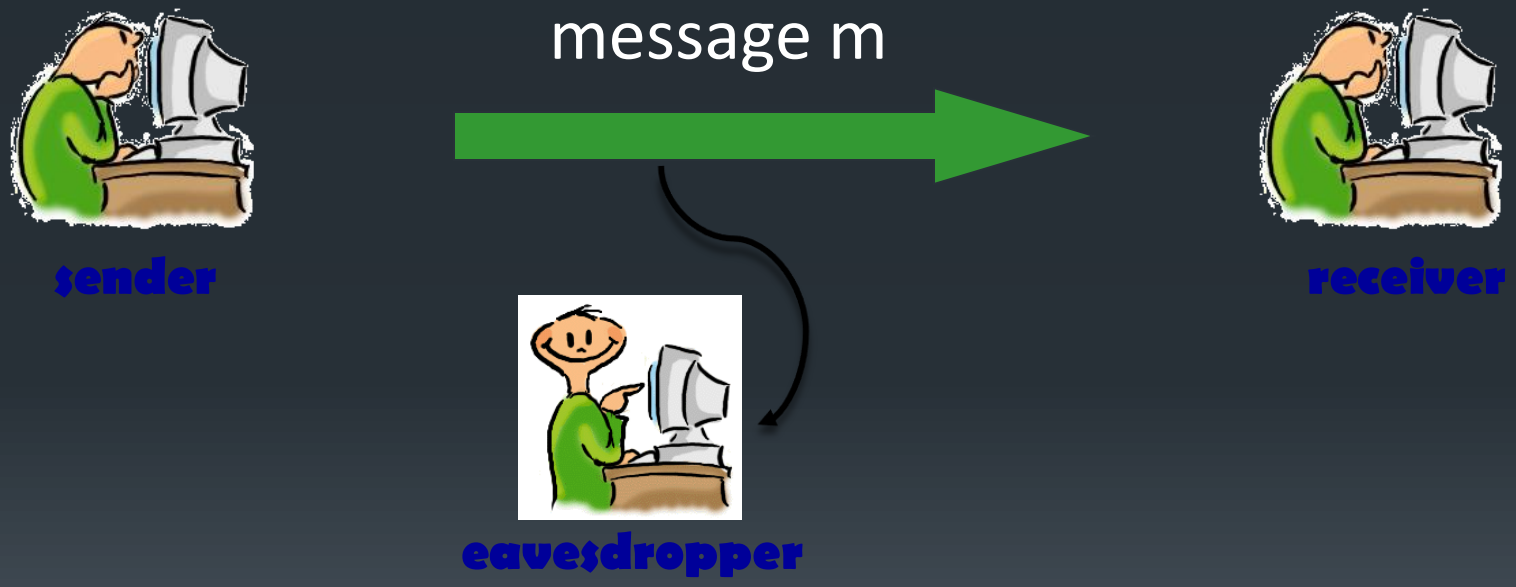
sender

message m

receiver

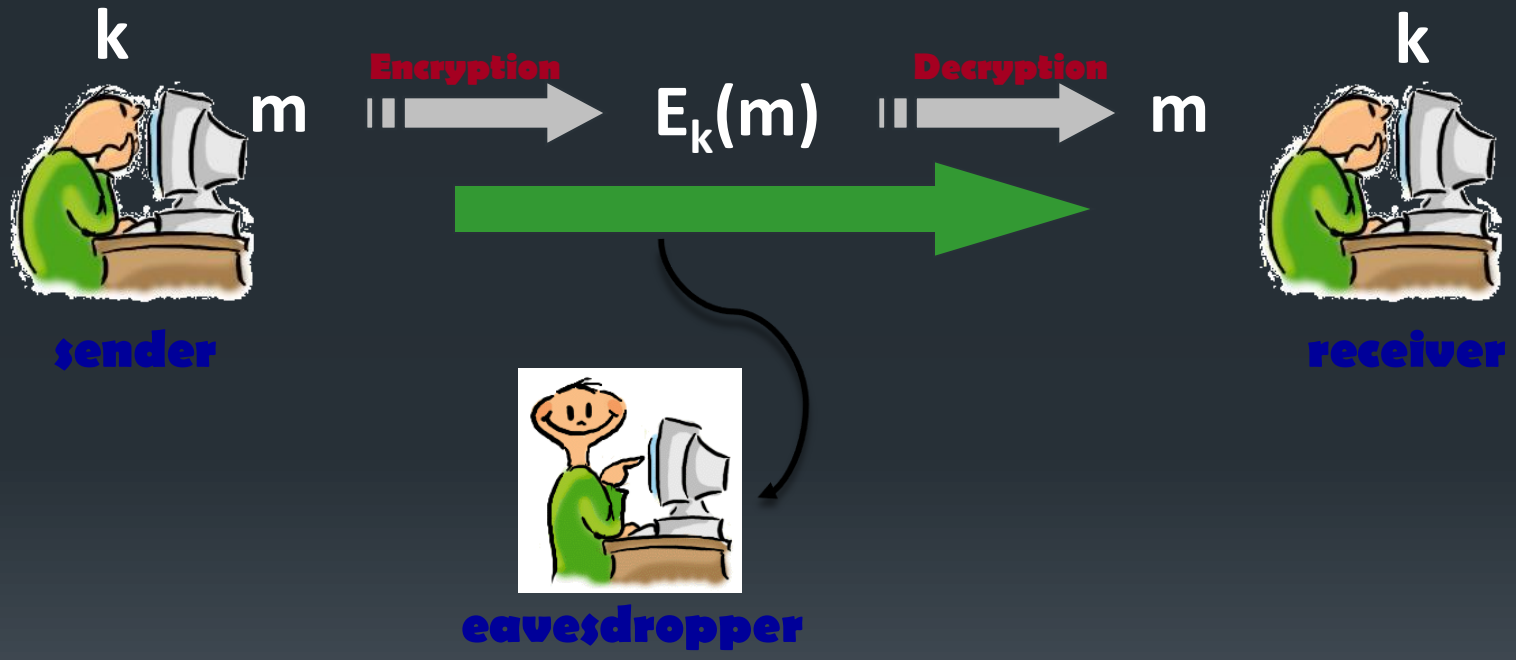
Encryption Scheme

The classic problem:

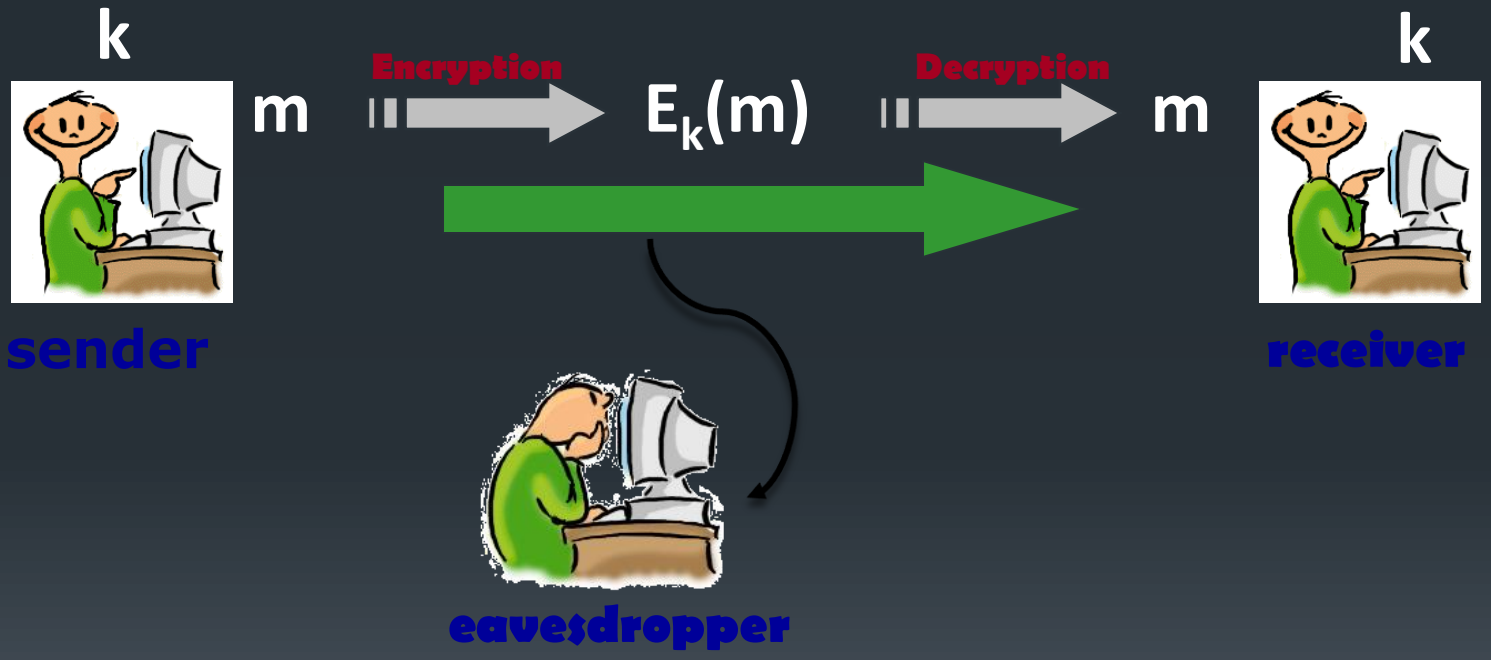


Encryption Scheme

The classic problem:



Encryption Scheme



Encryption Scheme

- Uses a secret key to encrypt and decrypt
- Until recently, all constructions assume security of the key is ultimate
  - Attacker cannot obtain any information about the key

In Real Life Secrets Do Leak…

In Real Life Secrets Do Leak…

Side Channels Attacks

- Exploiting physical properties of the circuits running cryptographic protocols
  - Analyzing power consumption, running time, electromagnetic radiations and more…
- Circumvent traditional security proofs and break security properties

How to Handle These Attacks?

- Let electrical engineers worry about it
  - Reduce the leakage directly at the implementation (hardware or software) level

How to Handle These Attacks?

- Let electrical engineers worry about it
  - Reduce the leakage directly at the implementation (hardware or software) level

- Problems:
  - Expensive
  - Ad-Hoc: only protects against known attacks

The Cryptographic Approach

- Design leakage resilient cryptographic primitives e.g., encryption scheme
  - Provably allow leakage from the secret key
  - Reduce the security needs at the implementation level

The Cryptographic Approach

- Design leakage resilient cryptographic primitives e.g., encryption scheme
  - Provably allow leakage from the secret key
  - Reduce the security needs at the implementation level

Need to define what leaks and how much

The Cryptographic Approach

- Leakage is arbitrary

The Cryptographic Approach

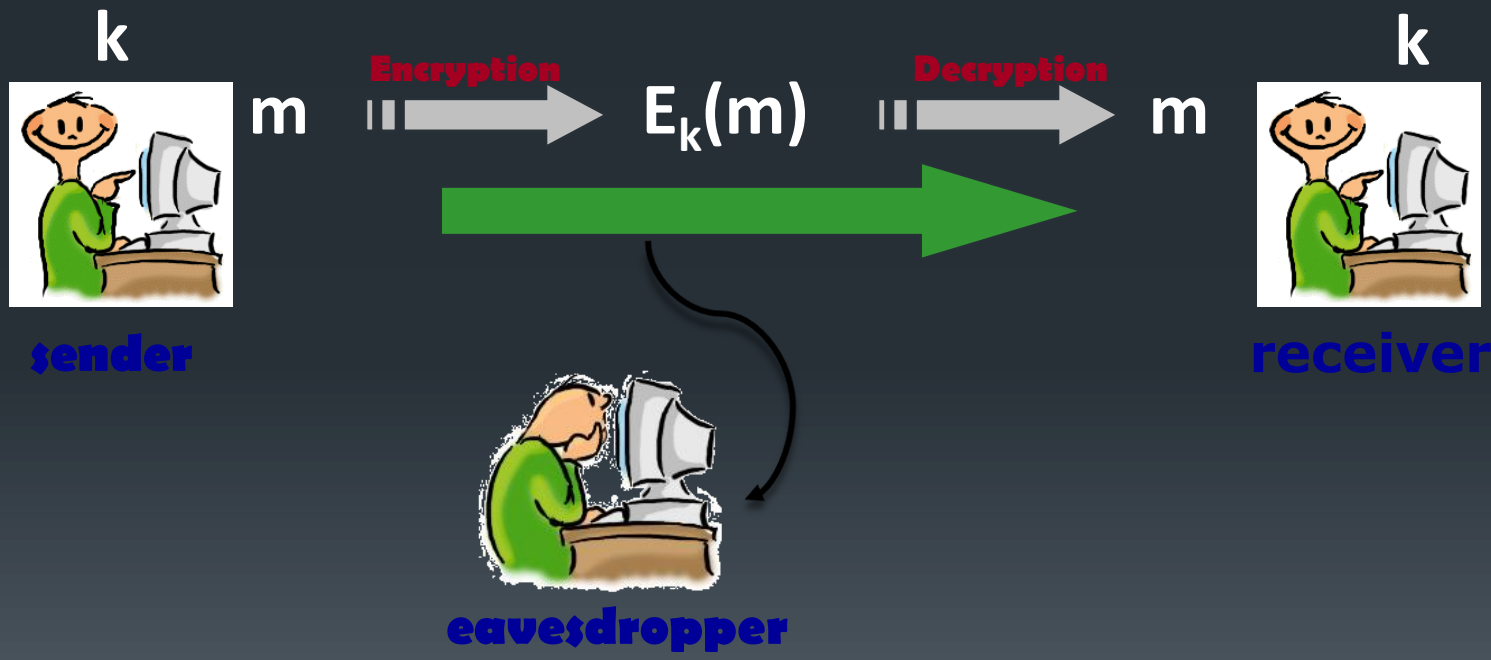
- Leakage is arbitrary

- Two axioms:

1. Leakage does not reveal the entire secret key
2. Leakage is formulized by a polynomial time commutable function f

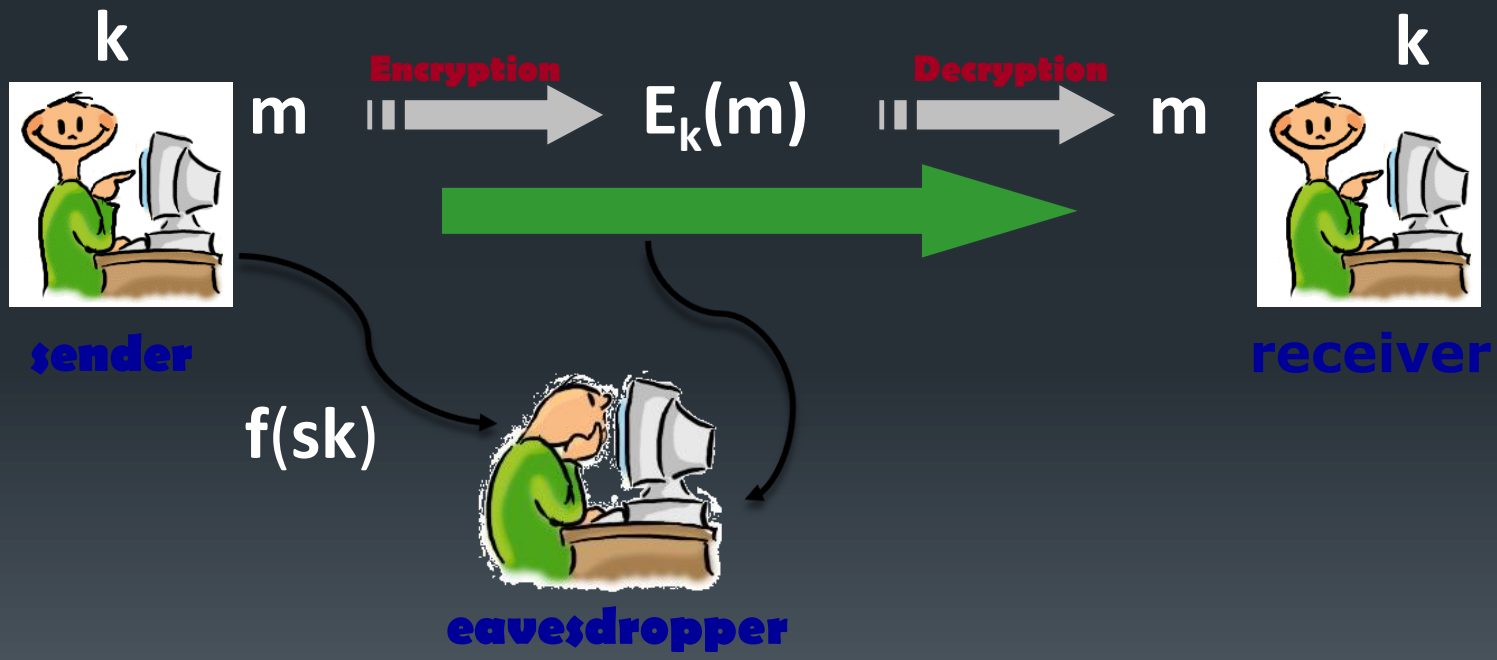
Modeling Leakage Resilient Encryption Scheme

Message is secure even if the attacker learns something about the secret key



Modeling Leakage Resilient Encryption Scheme

Message is secure even if the attacker learns something about the secret key



Designing Leakage Resilient Encryption Scheme

- Much work has been done so far optimizing leakage parameters
  - Privacy obtained even if all but small fraction of the secret key leaks

Designing Leakage Resilient Encryption Scheme

- Much work has been done so far optimizing leakage parameters
  - Privacy obtained even if all but small fraction of the secret key leaks
- Many open questions!

Designing Leakage Resilient Encryption Scheme

- One of current projects: design encryption scheme with security under factoring assumption

Designing Leakage Resilient Encryption Scheme

- One of current projects: design encryption scheme with security under factoring assumption

Factoring assumption:
Hard to factor multiplication of two large primes: $N=p \cdot q$

Designing Leakage Resilient Encryption Scheme

- Problem:
  - Factoring is easy in the presence of leakage from p and q [RivestShamir85]

Designing Leakage Resilient Encryption Scheme

- Problem:
  - Factoring is easy in the presence of leakage from p and q [RivestShamir85]
- Solution:
  - Consider a scheme that doesn't need to use p and q

Designing Leakage Resilient Encryption Scheme

- Problem:
  - Factoring is easy in the presence of leakage from p and q [RivestShamir85]
- Solution:
  - Consider a scheme that doesn't need to use p and q
- Preliminary results:
  - A secret key scheme based on factoring with security in the presence of leakage

Thank you!