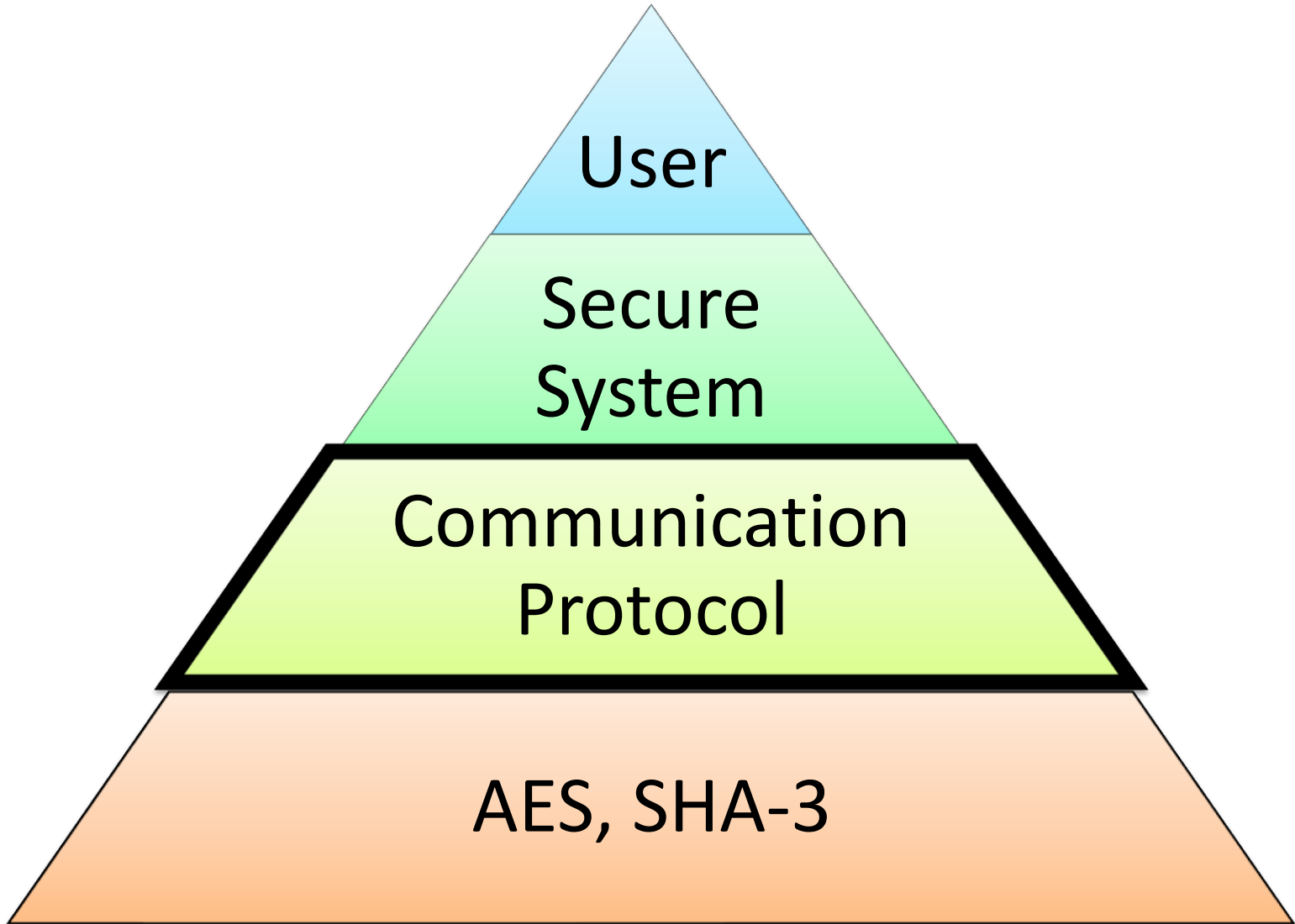


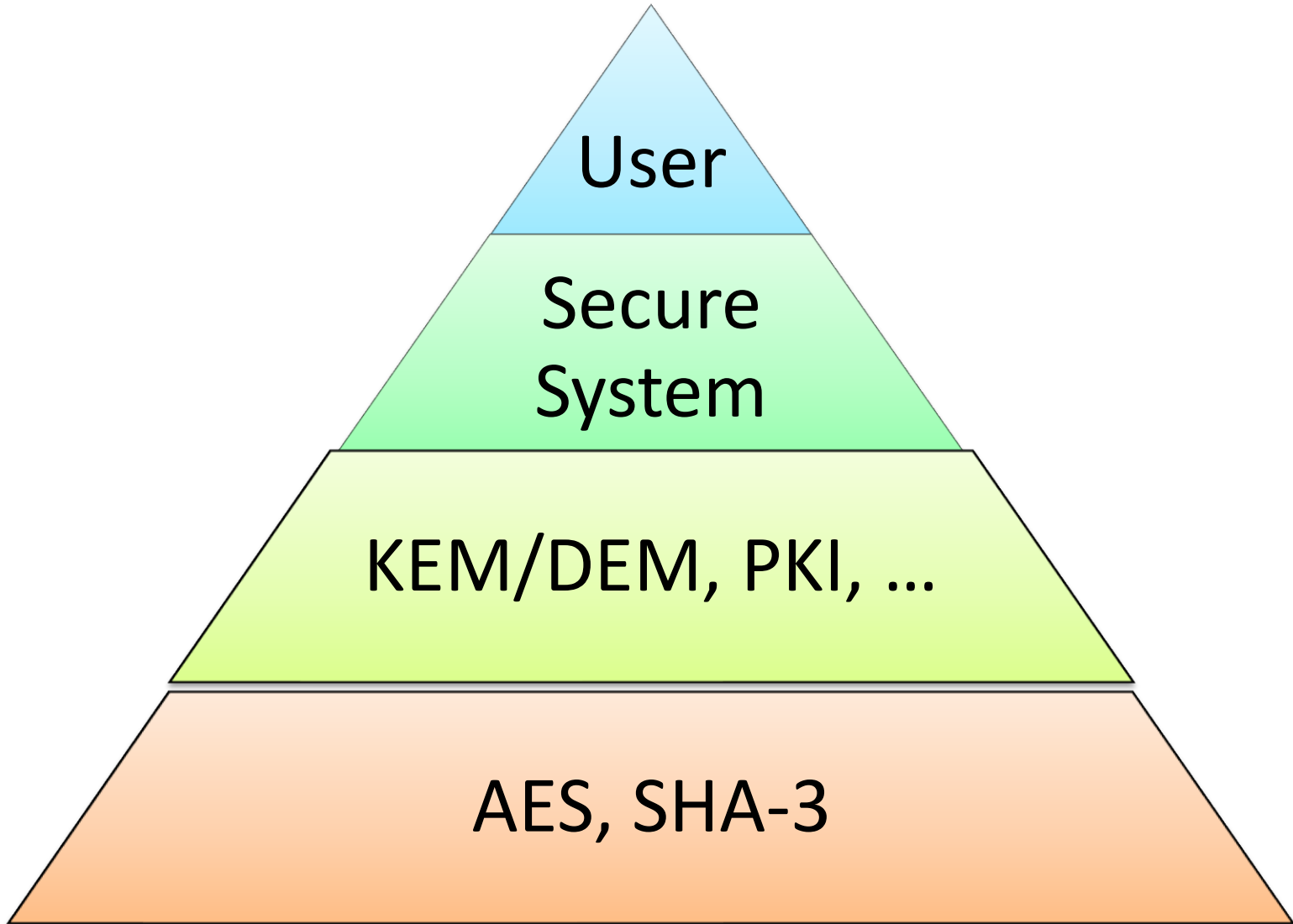
# The LowMC Cipher Breaking Challenge

Christian Rechberger,  
Hadi Soleimany, Tyge Tiessen

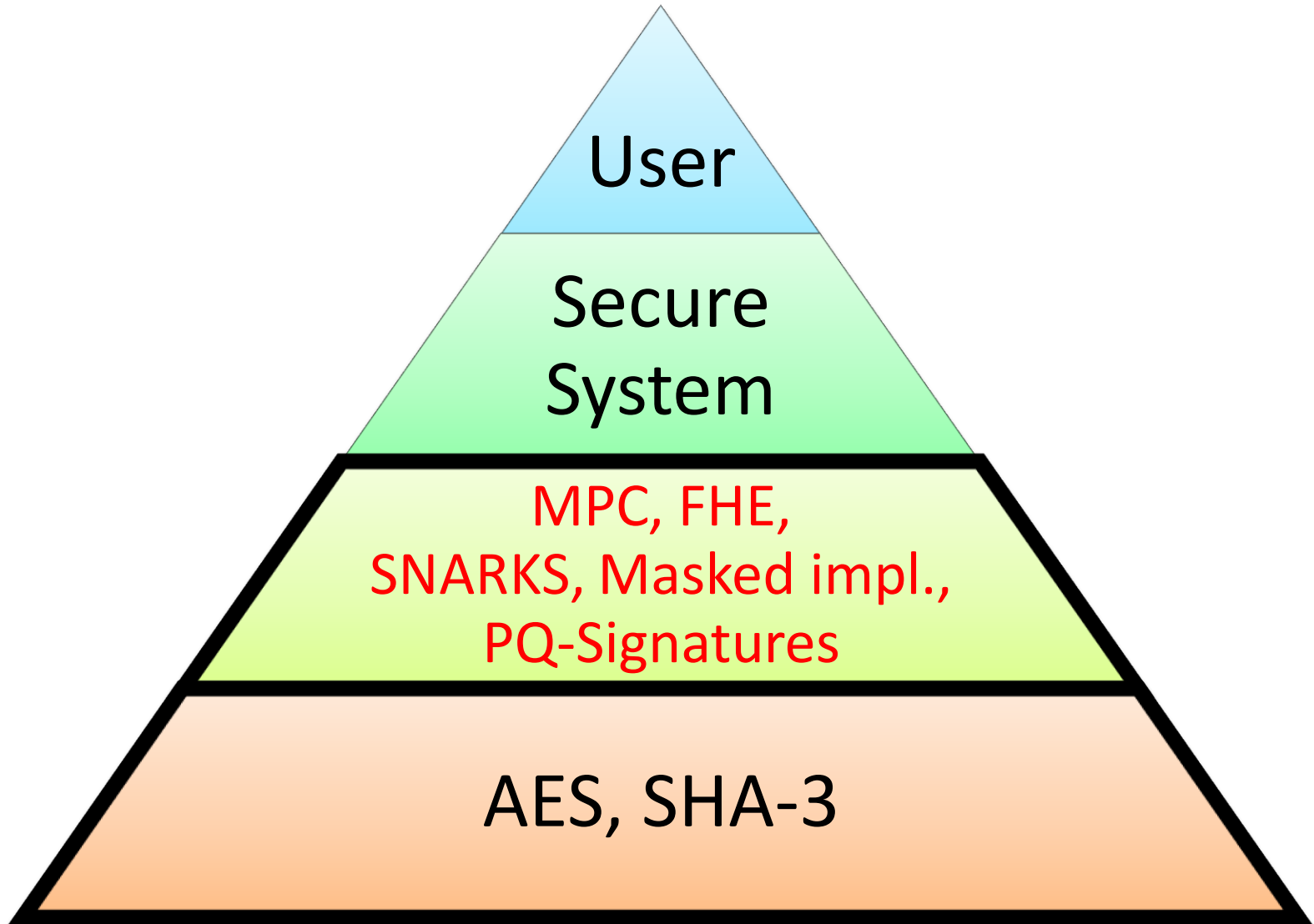
# Security of modern IT Systems



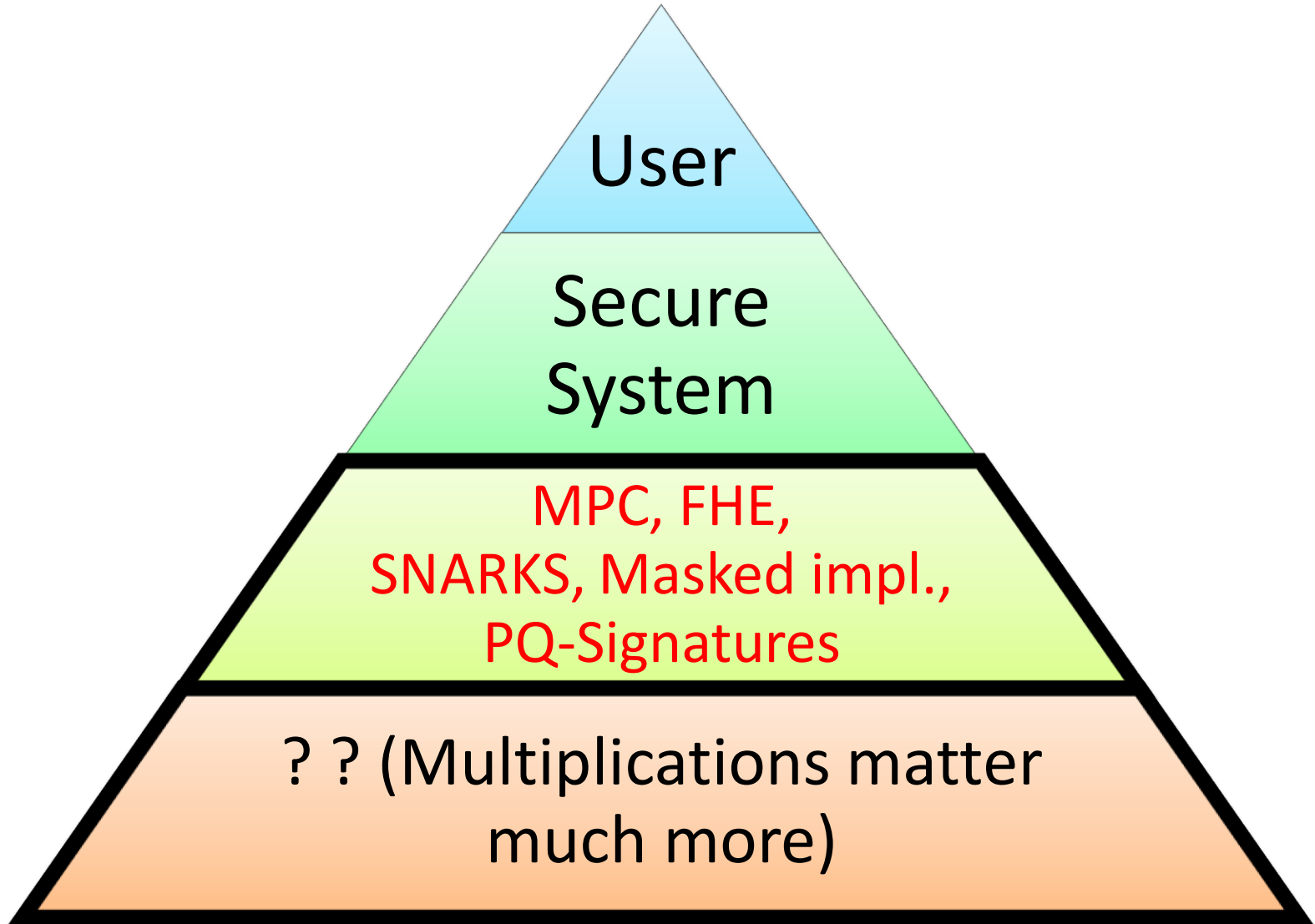
# Security of modern IT Systems



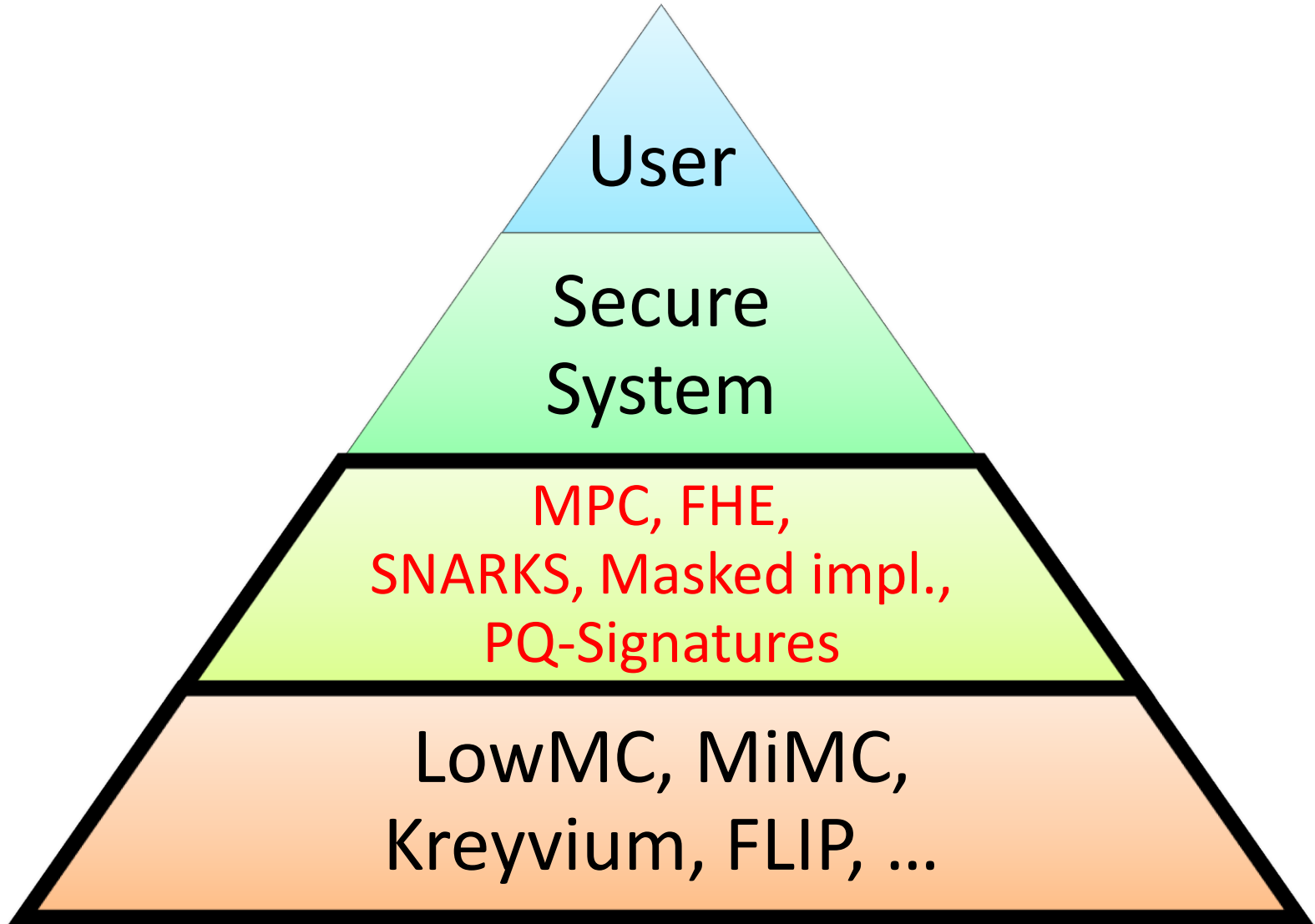
# Security of modern IT Systems



# Security of modern IT Systems



# Security of modern IT Systems



# LowMC

By

Martin Albrecht (RHUL)

Christian Rechberger (TUG, DTU)

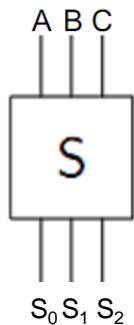
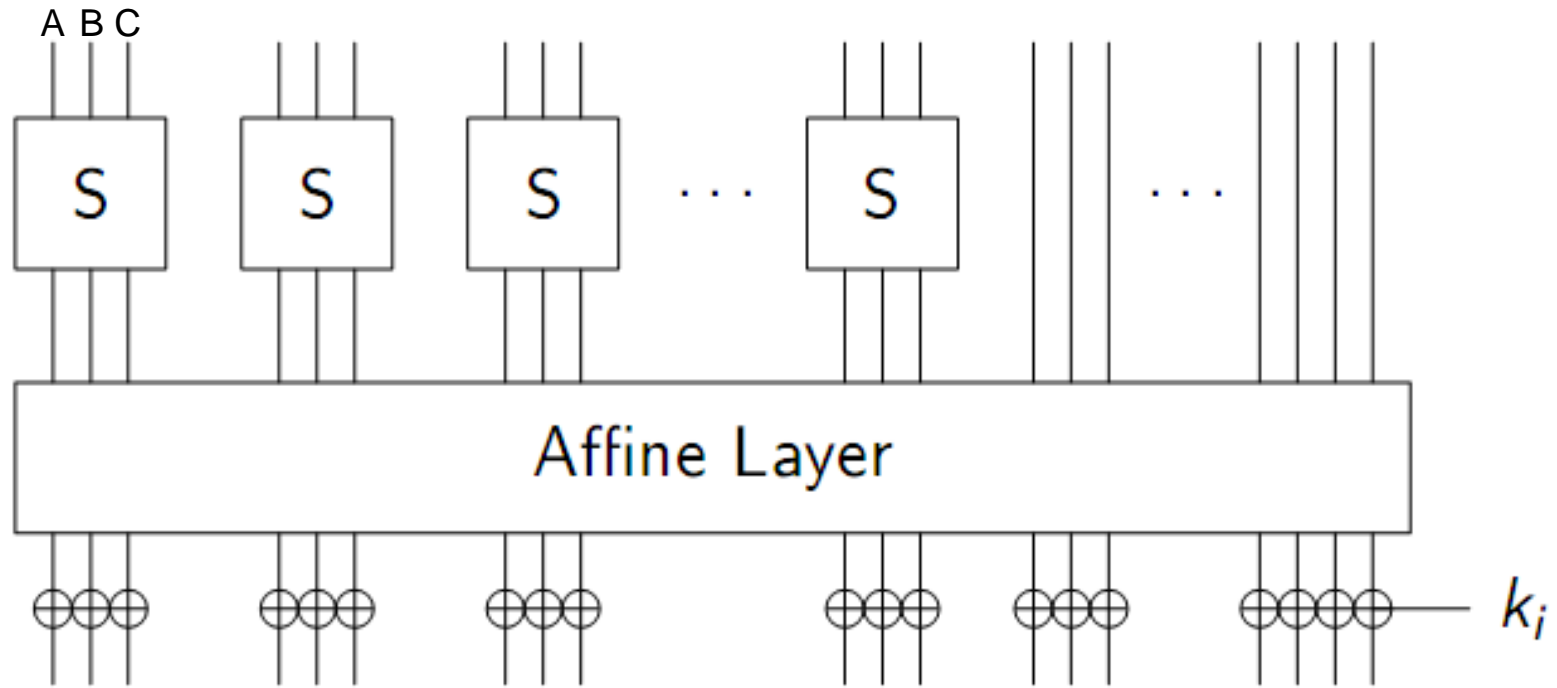
Thomas Schneider (TUD)

Michael Zohner (TUD)

Tyge Tiessen (DTU),

LowMC v1 published at Eurocrypt 2015

# Round transformation



$$S_0(A, B, C) = A \oplus BC$$

$$S_1(A, B, C) = A \oplus B \oplus AC$$

$$S_2(A, B, C) = A \oplus B \oplus C \oplus AB$$



# Design space

## Size

- n: Block size
- m: Number of Sboxes

## Security

- k: Key size (allowed time complexity)
- d: allowed data complexity

r: Number of rounds is function of  $(n,m,k,d)$

# Challenges for Three Use-Cases

# LowMC Challenge I

PQ-Signature use-case: minimizes  $m \cdot r$

Parameters:  $n=256$ ,  $k=256$ ,  $m=1$ ,  $d=1$

- How fast can you break  $r = 243$  rounds?
- Can you break  $r = 380$  rounds?

# LowMC Challenge II

FHE/MPC use-case: minimizes  $r$

Parameters:  $n=256, k=128, m=85, d=1$

- How fast can you break  $r=5$  rounds?
- Can you break  $r=8$  rounds?

Parameters:  $n=256, k=128, m=85, d=128$

- How fast can you break  $r=11$  rounds?
- Can you break  $r=14$  rounds?

# LowMC Challenge III

MPC use-case:

minimize  $m \cdot r / n$

Parameters:  $n=1024, k=128, m=1, d=128$

- How fast can you break  $r=600$  rounds?
- Can you break  $r=901$  rounds?

# Details

- Start: Now!
- Deadline: Nov 1<sup>st</sup>, 2017.
- Prices are gifts from Austria, Germany, Denmark, UK, Iran.
- More details on <https://github.com/lowmc>  
incl. affine-layer matrices and vectors for direct download