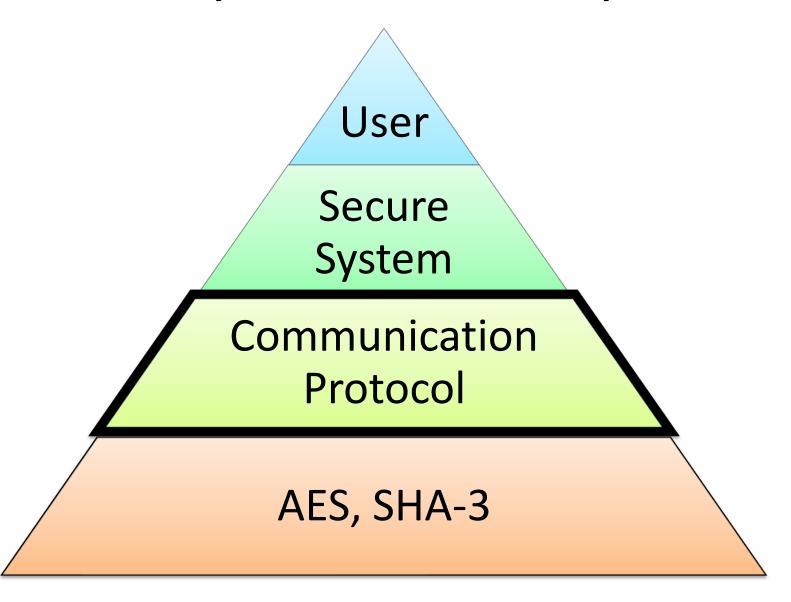
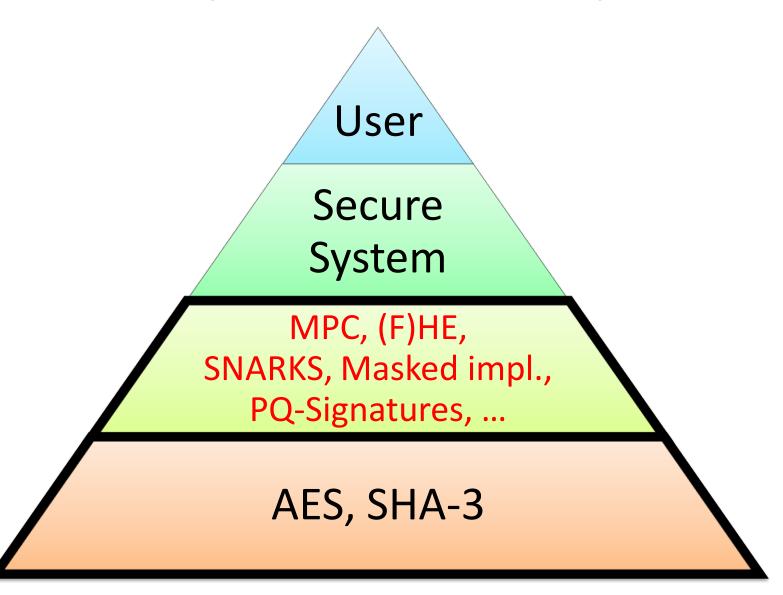
FewMul – Introduction

Start at 09.30 AM

Christian Rechberger



User Secure System KEM/DEM, PKI, ... AES, SHA-3



User

Secure System

MPC, (F)HE, SNARKS, Masked impl., PQ-Signatures, ...

? ? (Multiplications matter much more)

