Hash-Based Signatures

Johannes Buchmann, Andreas Hülsung
Supported by DFG and DAAD

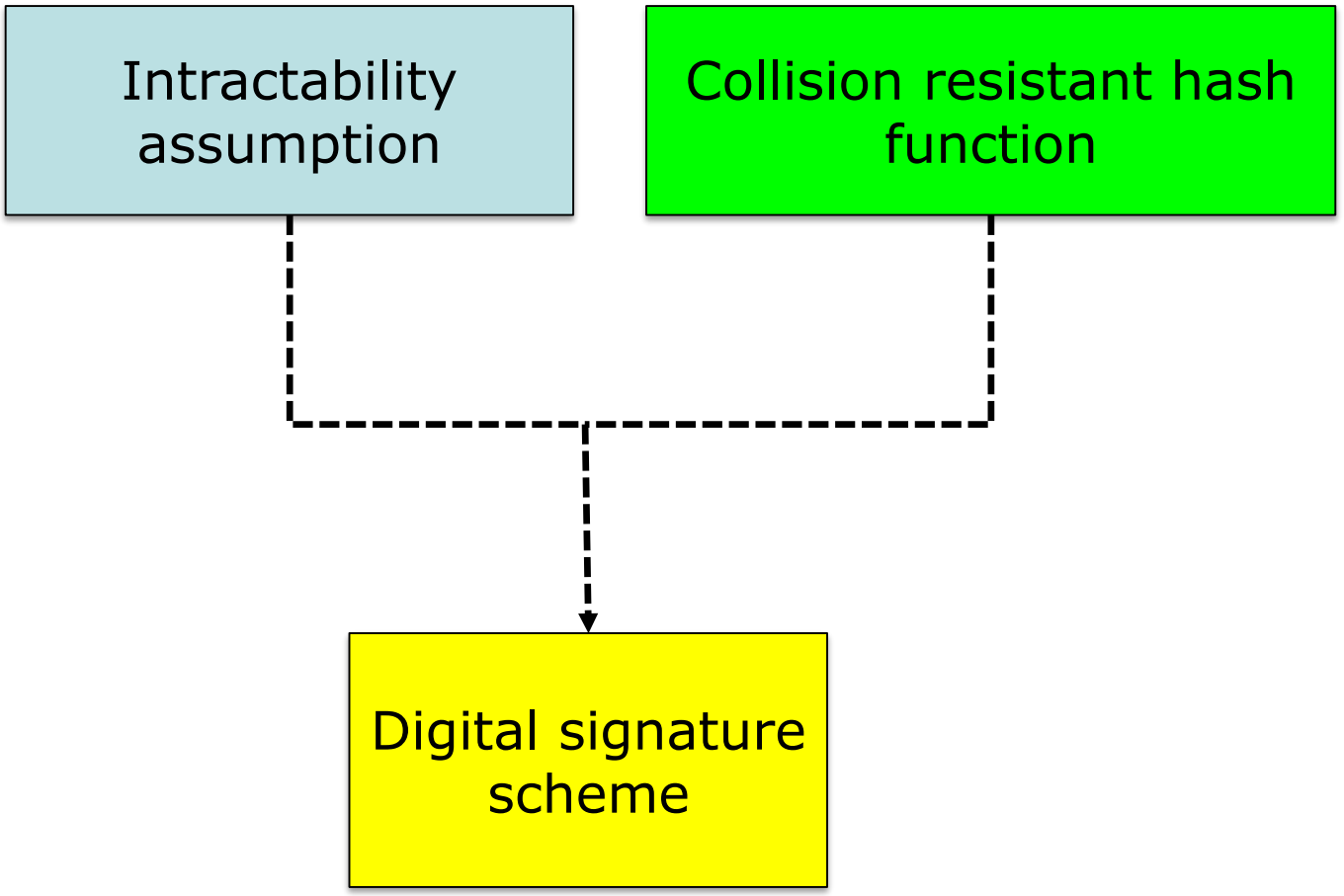
Part X:
XMSS Security

CASED

XMSS has Minimal Security Requirements

Security Requirements of Current Signature Schemes

CASED

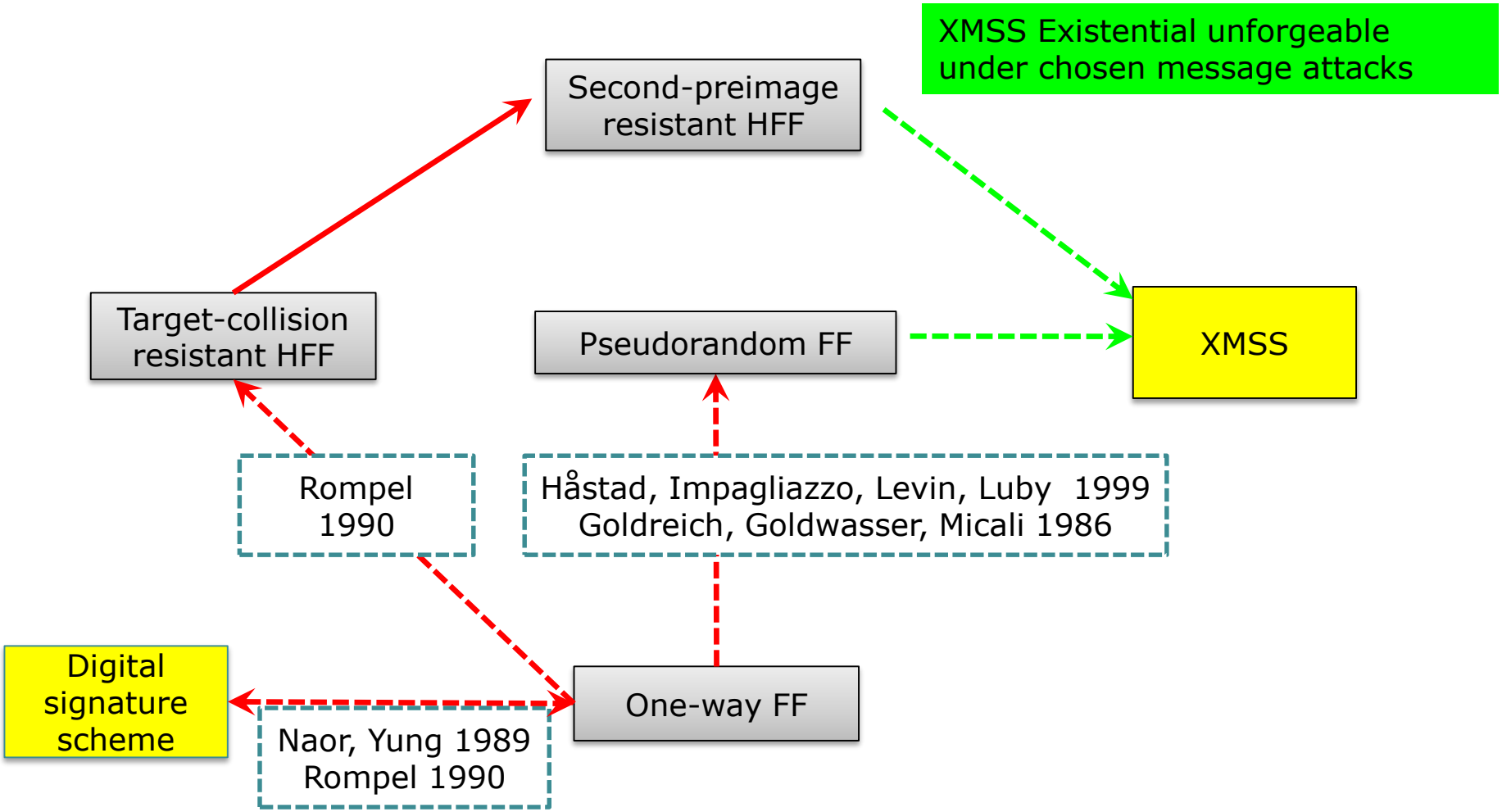


Minimal Security Requirement of Signatures

CASED

XMSS has minimal security requirements

CASED



Security proof

CASED