Supervisor

Nouri Alnahawi

MPSE Kolloquium

PQC integration in eID protocols

Gero Knoblauch - Matthias Merz - Chiara-Marie Zok - Peter Mueller - Dominik Heinz

Agenda


Introduction
Theory
Implementation
eID Protocols
Hardware
Outlook

Introduction

Problem

- eID and ePASS currently use standard protocols with classical cryptography
- Threatend by quantum computers (Shor‘s and Grover‘s Algorithm)
- Migration needs to be done

Our Goal

- Integration of PQC in protocols
- Focus on PACE protocol
- Fits our constraints


eID
Protocols

EAC Sub-protocols

PACE

Password Authenticated Connection Establishment

- PIN input
- Ephemeral Diffie-Hellman based
- Session keys generation

TA

Terminal Authentication

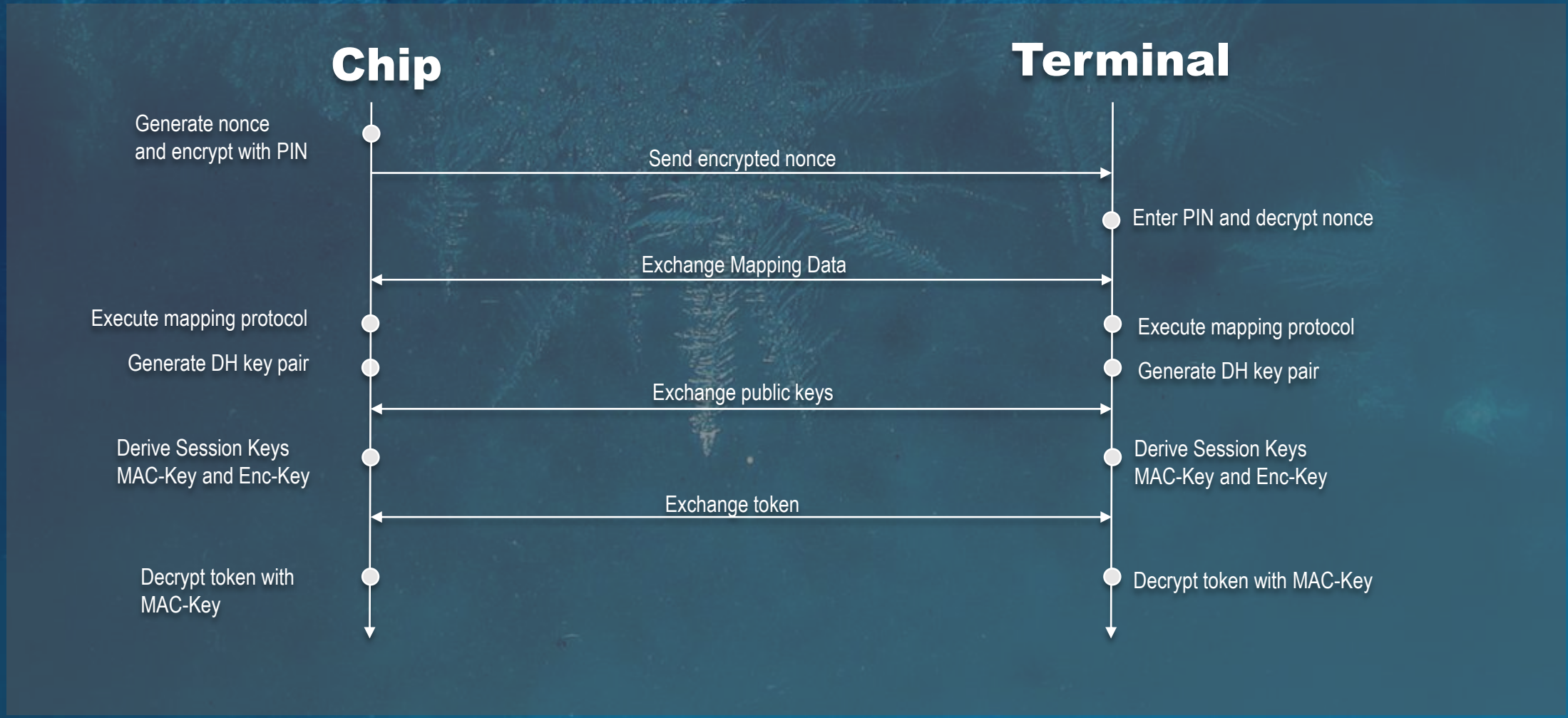
- Sends certificate chain
- Random number challenge and verify

CA

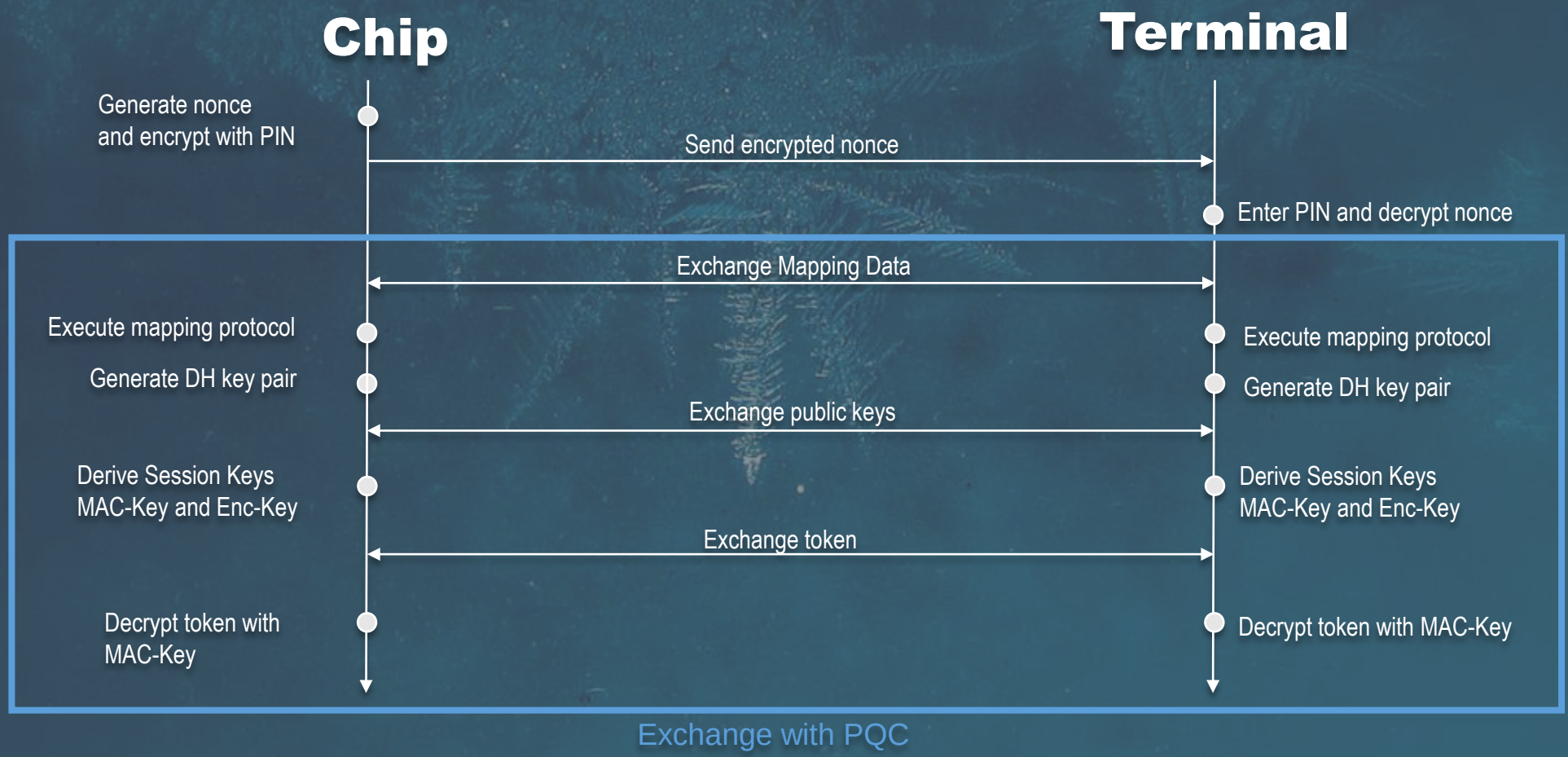
Chip Authentication

- Passive Authentication
- Static-ephemeral Diffie Hellman

PACE Protocol



PACE Protocol



Theory

Constraints

Before starting research

- Existing code / implementation / documentation
- Needs to fit on eID cards
- Preferably NIST Round 3
- Crypto-agility (security levels, signature schemes, backward compatibility)

KEX / AKE / KEM

Key Exchange
- Two parties establish together a symmetric key

Key Encapsulation Mechansim
- One party establishes key which is encapsulated and send to other party

Authenticated Key Exchange
- Combination with authentication mechanism
- Can be combined with passwords (PAKE)

PQC

Types

- Code based
- Hash based
- Isogeny based
- Multivariate based
- Lattice based

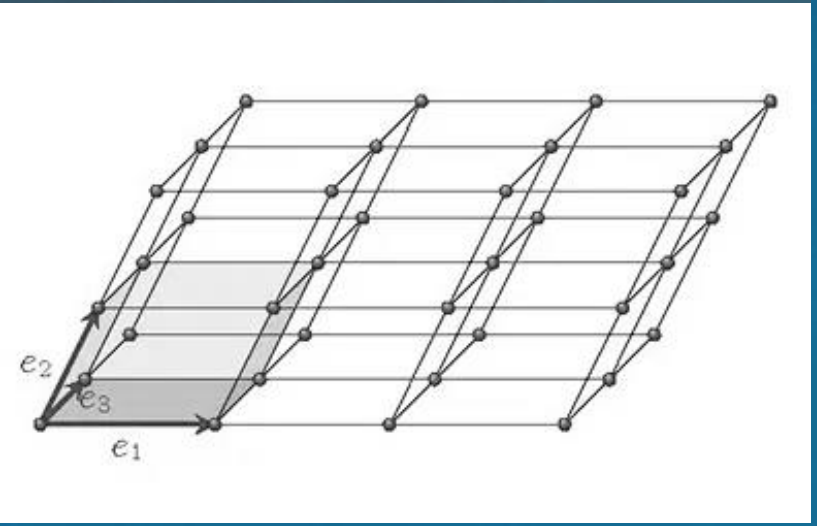
Lattice based Cryptography

Different Types:

- Most schemes based on SVP (shortest vector problem) or CVP (closest vector problem)
- Either use rounding or add error term
- Unstructured / Structured / Ideal lattices

Our finalists:

- NTRU, Kyber, Saber, 3Bears



Crystals Kyber

- IND-CCA2-secure KEM (Key Encapsulation Mechanism)
- Based on LWE (Learning with Errors) over Module lattices
- CBD (Centered Binomial Distribution) noise sampling
- 3 security levels similar to AES 128/192/256
  - Ring stays the same
  - Change dimensions k,n

Ring used:
$\mathbb{Z}_q\,[x]/(x^n+1)$


Hardware

RFID/NFC Cards

Current state of the Art:

- Tickets
- Key Cards
- eID (Personalausweis)

Manufacturers:

- NXP
- Infineon

OS:

- Java Card OS
- proprietary

Hardware Constraints

- Larger keys have to fit on card storage / RAM
- PQC: Different mathematical computations
  - PQC currently not in hardware
  - CoProcessor for RSA / ECC
- Overall Speed (2sec barrier)

Keysize at 128 bit post-quantum:		
	Public K	Private K
NTRU	766.25 B	842.875 B
McEliece	1.0 MB	11.5 KB
Kyber	800.0 B	1.6 KB
SIKE	378.0 B	434.0 B
ECC	32.0 B	32.0 B
eID	10KB (RAM) / 700KB (Flash)	

Decision

SUPERCOP [eBATS]

- Speed (keyGen, createCipher, generateSessionKey)
- Spacial requirements (publicKey, cipher)

pqm4

- Speed (cycles: keyGen, encaps, decaps)
- Memory footprint
- Program Size

Overall Performance
1. Kyber
2. NTRU
3. Saber
4. NewHope

Referenced Hardware in Papers

	l4r5zi	NXP eID
CPU	arm Cortex M4 120 Mhz	32 bit CPU / CoProcessor
Flash	2 MB	~ 700 KB
RAM	640 KB	10176 B

Purchased Hardware

life.augmented

Advantages

- already available implementations
  - PQClean
  - pqm4
- kind of restricted hardware
- NFC coverage

M24SR-DISCOVERY

NUCLEO-L476RG

NUCLEO-L4R5ZI

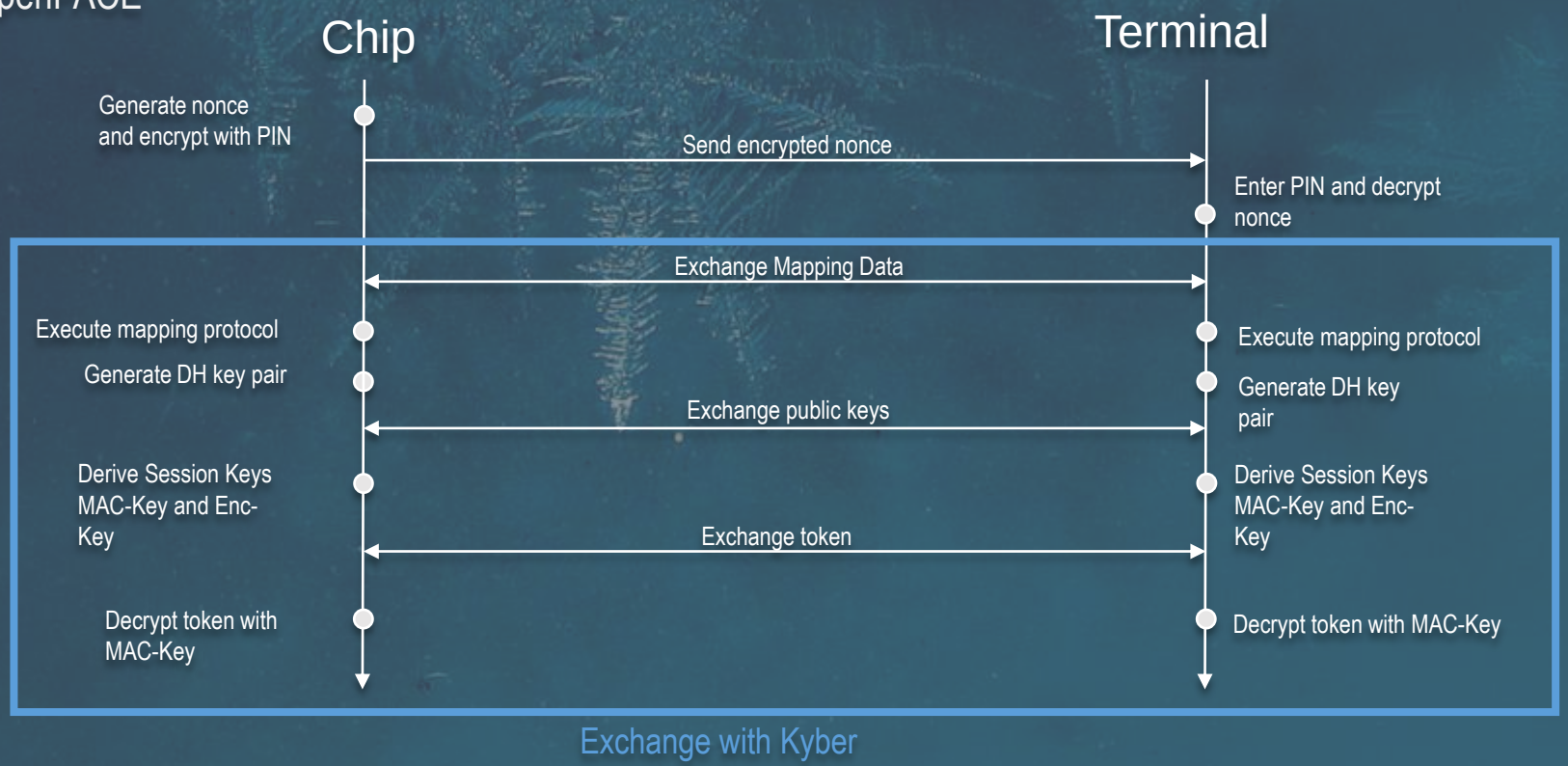
ST25R3911B-DISCO

ST25R3916-DISCO

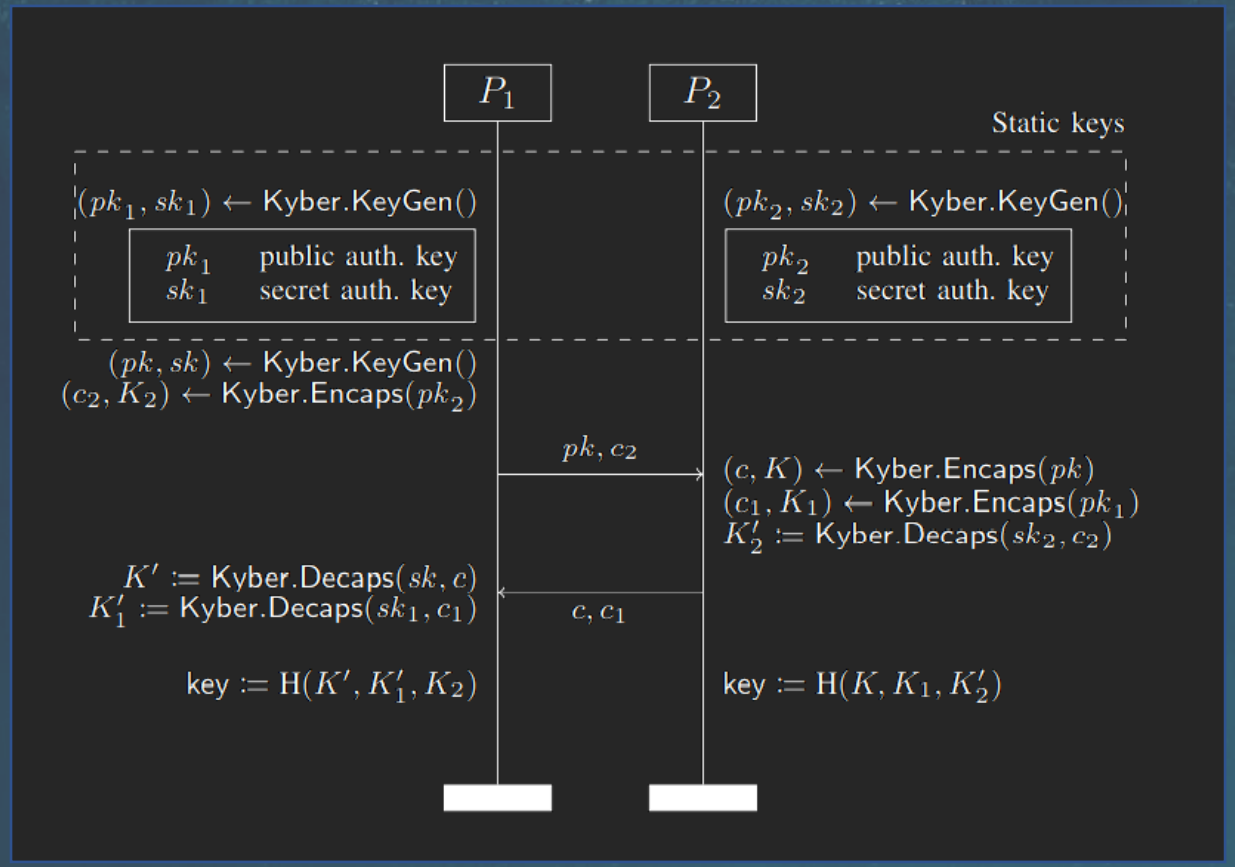

Implementation

Implementation

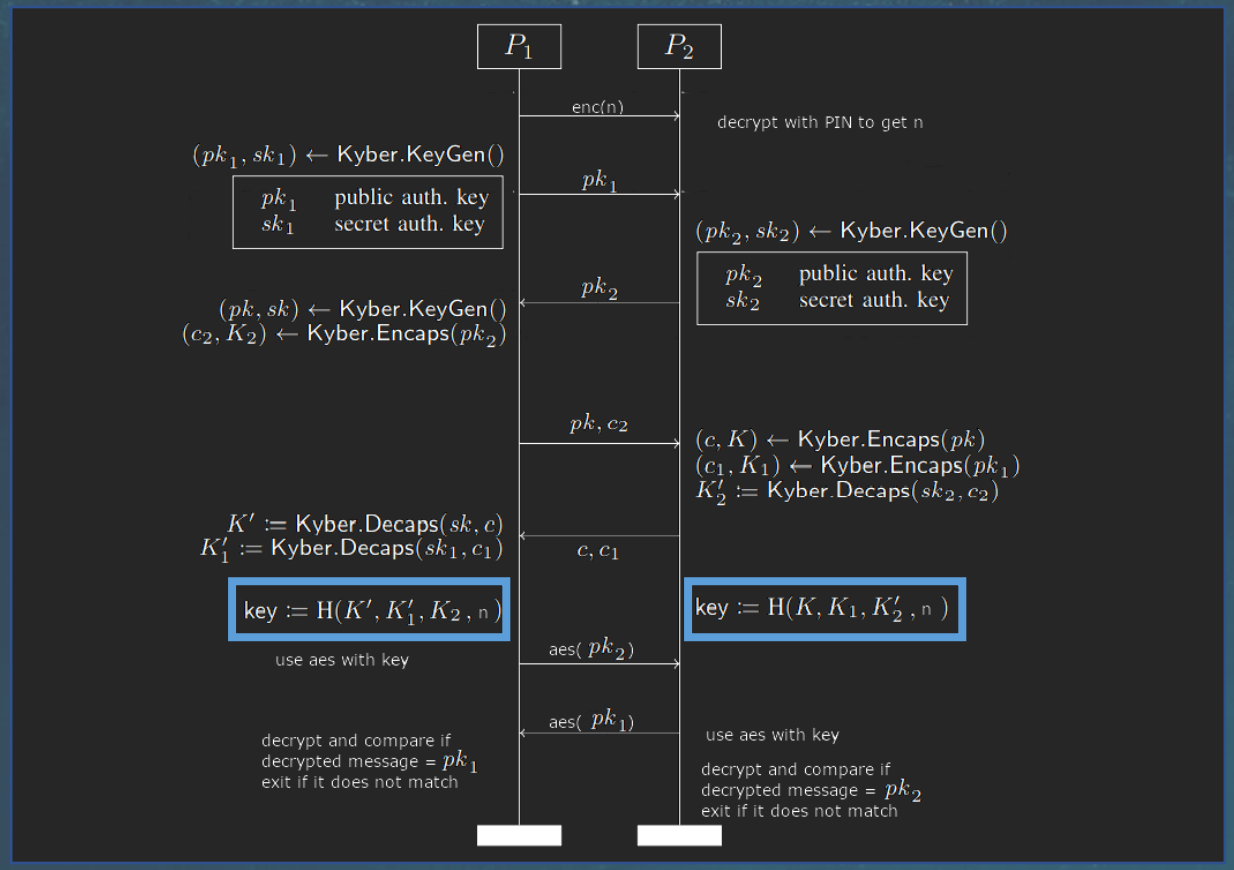
- Implemented standard PACE
- Based on OpenPACE



Implementation



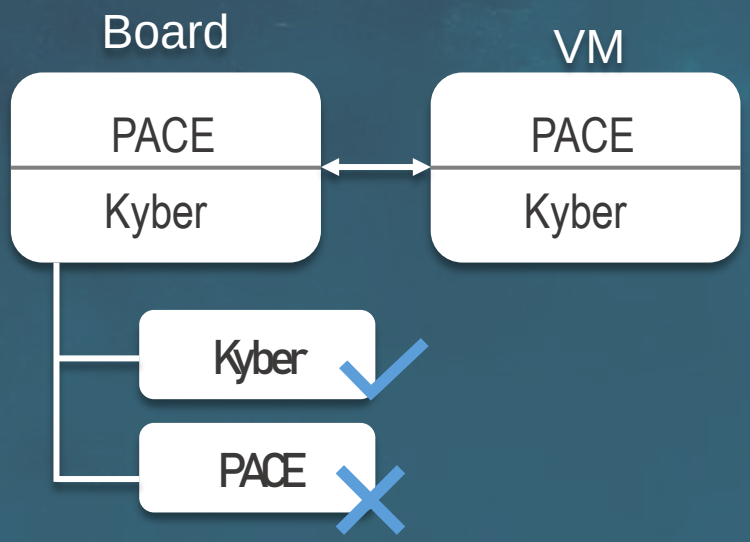
Implementation



Current State

Prototype implementation in C11 using Linux

- Dependencies: kyber, openpace
- Exchange of parameters via TCP (replace with NFC later on)
- GCC without optimization
- Can be dockerized

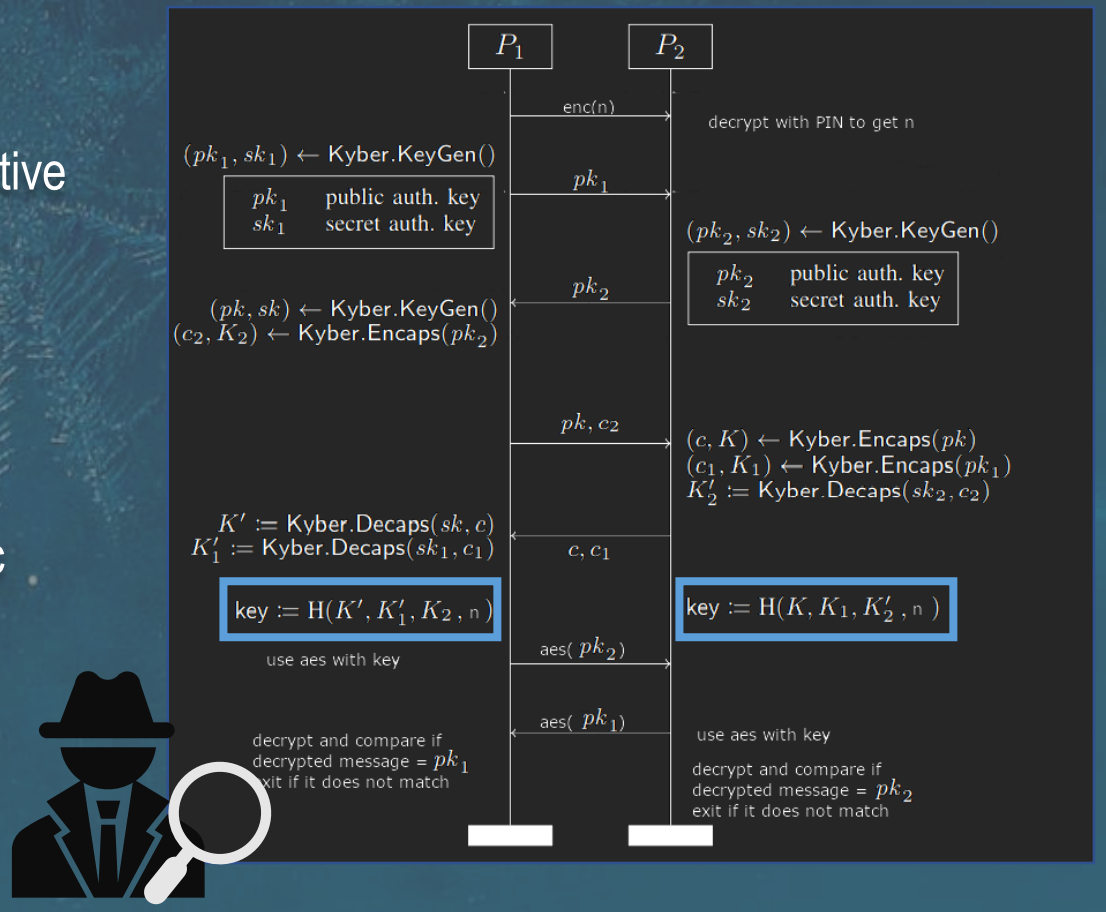


Showcase


Outlook

Challenges / Ideas

- Public Key authenticated
- Current protocol is only possibly secure for active attacks
- Passive attacks might be possible
- Create a malicious terminal and capture traffic
  - Bruteforce PIN
  - Try to decrypt AES message



Outlook

- Signatures for certificates (Terminal and Chip Authentification) using Dilithium
- Exchange second DH in TA and CA with Kyber
- Implement suitable PQC PAKE scheme (PACE mapping protocol)
- Proof of concept, proof of security (formal analysis)
- Test protocol on real hardware (benchmarking)

Any Questions?

Important Recources

EAC

https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TR03110/BSI_TR-03110_Part-1_V2-2.pdf?__blob=publicationFile&v=1
https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TR03110/BSI_TR-03110_Part-2-V2_2.pdf?__blob=publicationFile&v=1
https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TR03110/BSI_TR-03110_Part-3-V2_2.pdf?__blob=publicationFile&v=1
https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TR03110/BSI_TR-03110_Part-4-V2_2.pdf?__blob=publicationFile&v=1

Theory

https://github.com/mupq/pqm4
https://eprint.iacr.org/2020/1276.pdf
https://ninabindel.de/wp-content/uploads/2019/09/Bindel2018_Article_ComparingApplesWithApplesPerfo.pdf

Impl**ementation**

https://code.fbi.h-da.de/istmamerz/kyber-modifyed-for-pake
https://code.fbi.h-da.de/aw/prj/athenepqc/mpse-eid-implementation

Figure Sources

Background
- https://www.flickr.com/photos/james_mann/15997504965/in/album-72157640001081143/

Lattice
- https://icerm.brown.edu/programs/sp-s18/w4/

Constraints
- https://de.wikipedia.org/wiki/Datei:NIST_logo.svg

Crystals/Kyber/ Dilithium Logo
- https://pq-crystals.org/kyber/resources.shtml

Current State
- https://aws.amazon.com/de/docker/

Implementation
- https://www.pngfind.com/download/TTxhwb_question-mark-clipart-gif-png-download-transparent-question/

Purchased Hardware
- https://de.rs-online.com/web/p/entwicklungstools-microcontroller/9064624?cm_mmc=DE-PLA-DS3A
- https://hackspark.fr/en/dev-tools/584-m24sr-discovery-discovery-kit-for-the-m24sr-series-dynamic-nfcrfid-tag.html
- https://www.st.com/en/evaluation-tools/st25r3916-disco.html
- https://www.mouser.de/ProductDetail/STMicroelectronics/NUCLEO-L4R5ZI?qs=j%252B1pi9TdxUYHwRjgL7zLGg%3D%3D
- https://fr.farnell.com/productimages/large/fr_FR/2797958-40.jpg