NAMED DATA NETWORKING COMMUNITY MEETING 2026

A Security Library of a Decentralized Access Control in NDN

Ferhat Mecerhed, Youcef Imine, Antoine Gallais, Stefan Fischer, Mohamed Ahmed Hail

UNIVERSITÄT ZU LÜBECK

Université Polytechnique HAUTS-DE-FRANCE

Presentation Plan

1. Background & Motivation

- Data-centric Confidentiality
- Access control solutions in NDN
- Multi-Authority Attribute-based Encryption

2. Security Library for NDN

- An access control protocol for NDN
- Library’s Architecture
- Implementation under NDN-cxx & Use
- What’s next?

Data-centric Confidentiality

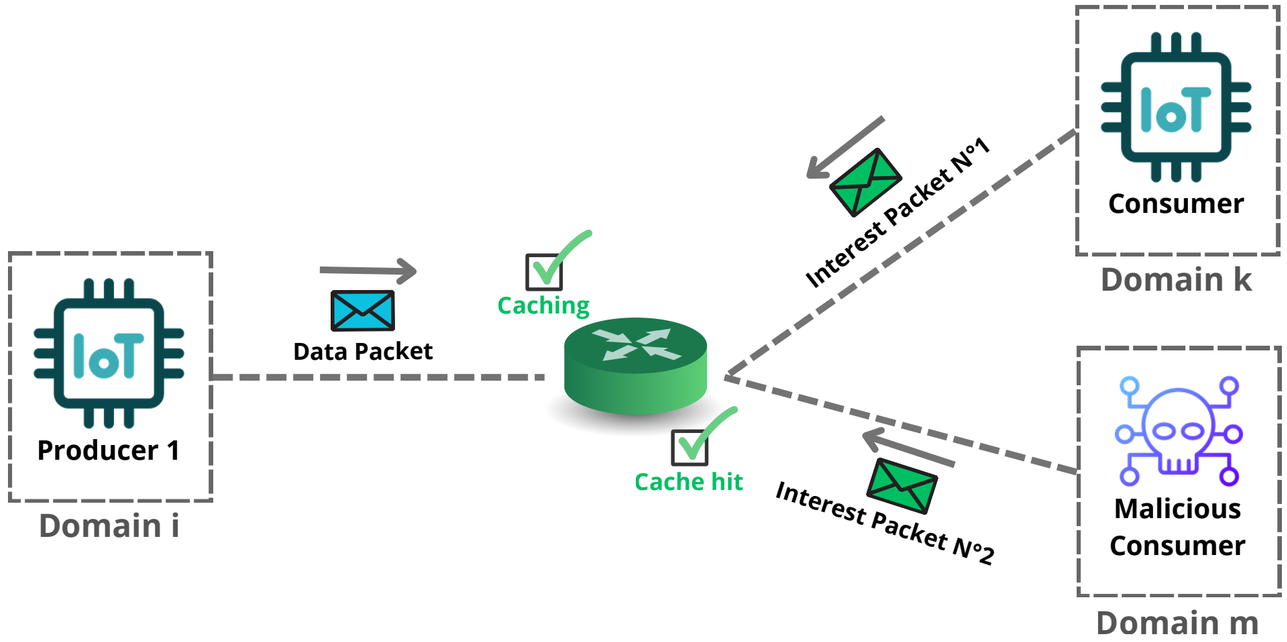
Communication in NDN follows a **group-based model** induced by:

- Pending interest at the PIT table
- In-network caching

Impact on Confidentiality solutions:

Switch from **peer-to-peer encrypted tunnels**

to **Encryption schemes**



Access Control in NDN

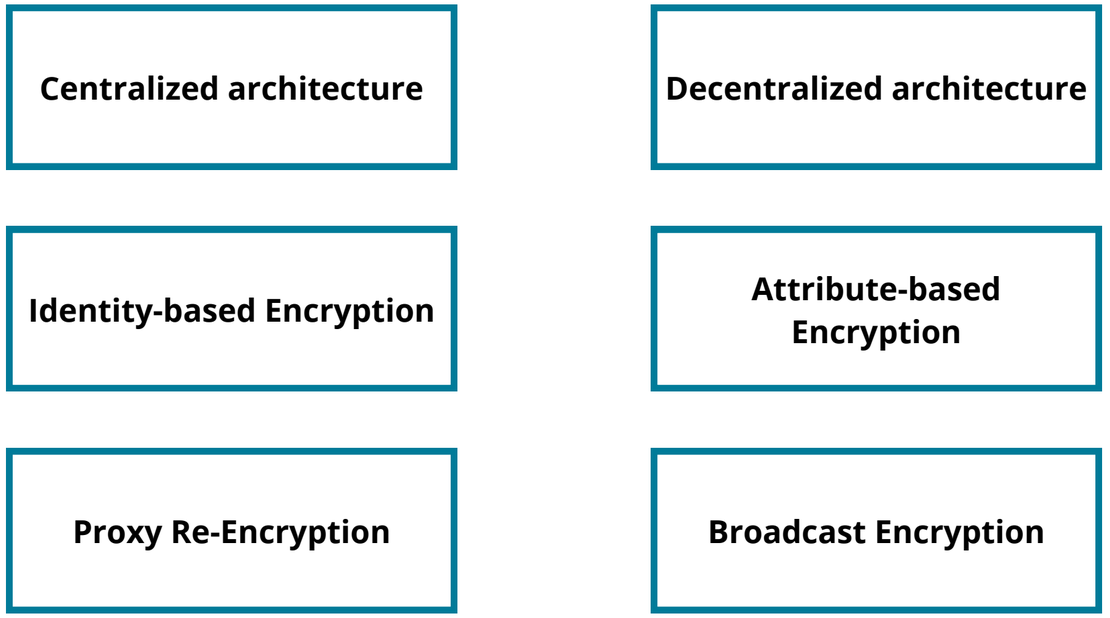
Advanced Cryptography

- **Architecture**: Unique central authority or Multi-authority
- **IBE**: Enables encryption directly from the receivers identity
- **ABE**: Fine-grained access control
- **Proxy Encryption**: Distribution of the encryption overhead
- **Broadcast Encryption**: Enables one-to-*N* communication and easy access revocation

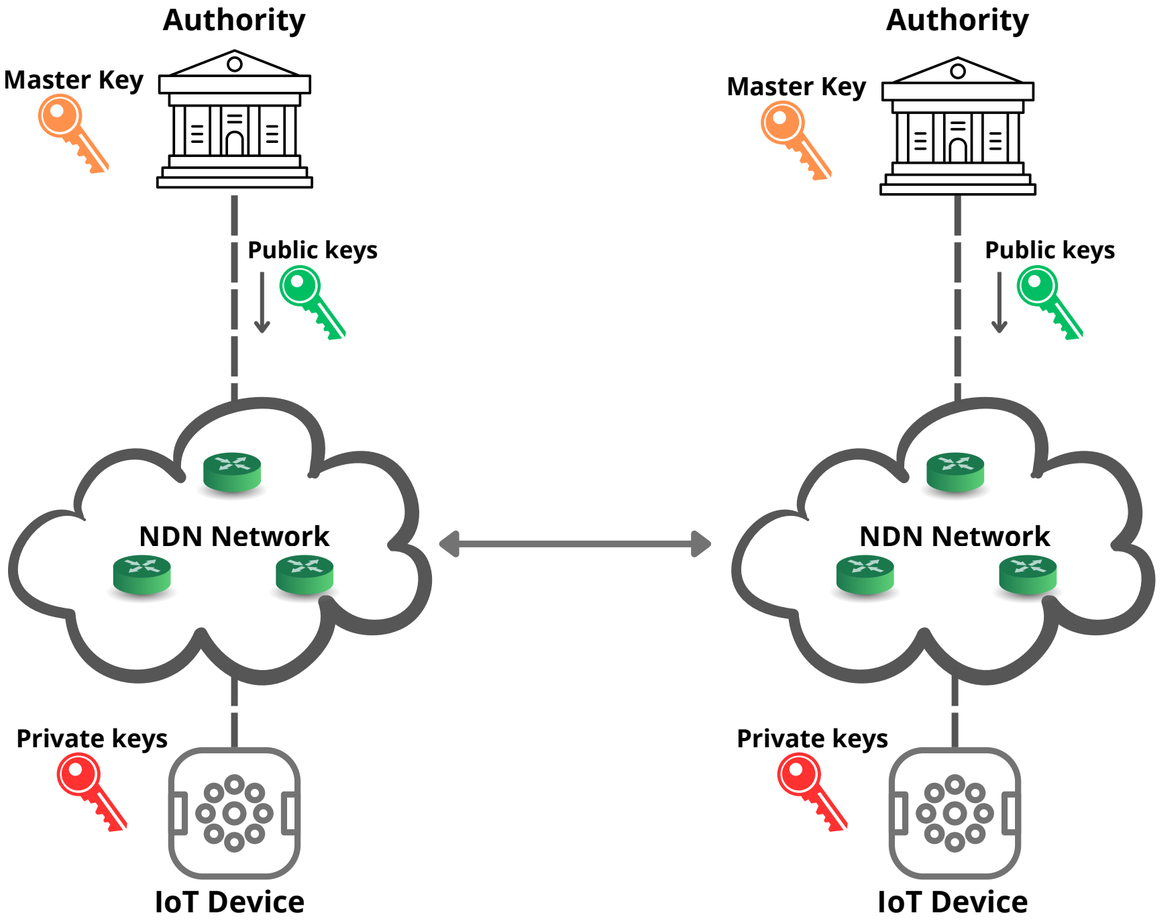
What mechanisms can better support confidentiality in NDN?

- An AC thats supports NDN decentralized systems
- An AC that expresses access policies not using identity
- An AC that is adapted with the group-based communication

Access Control Models



Multi-Authority Attribute-based Encryption

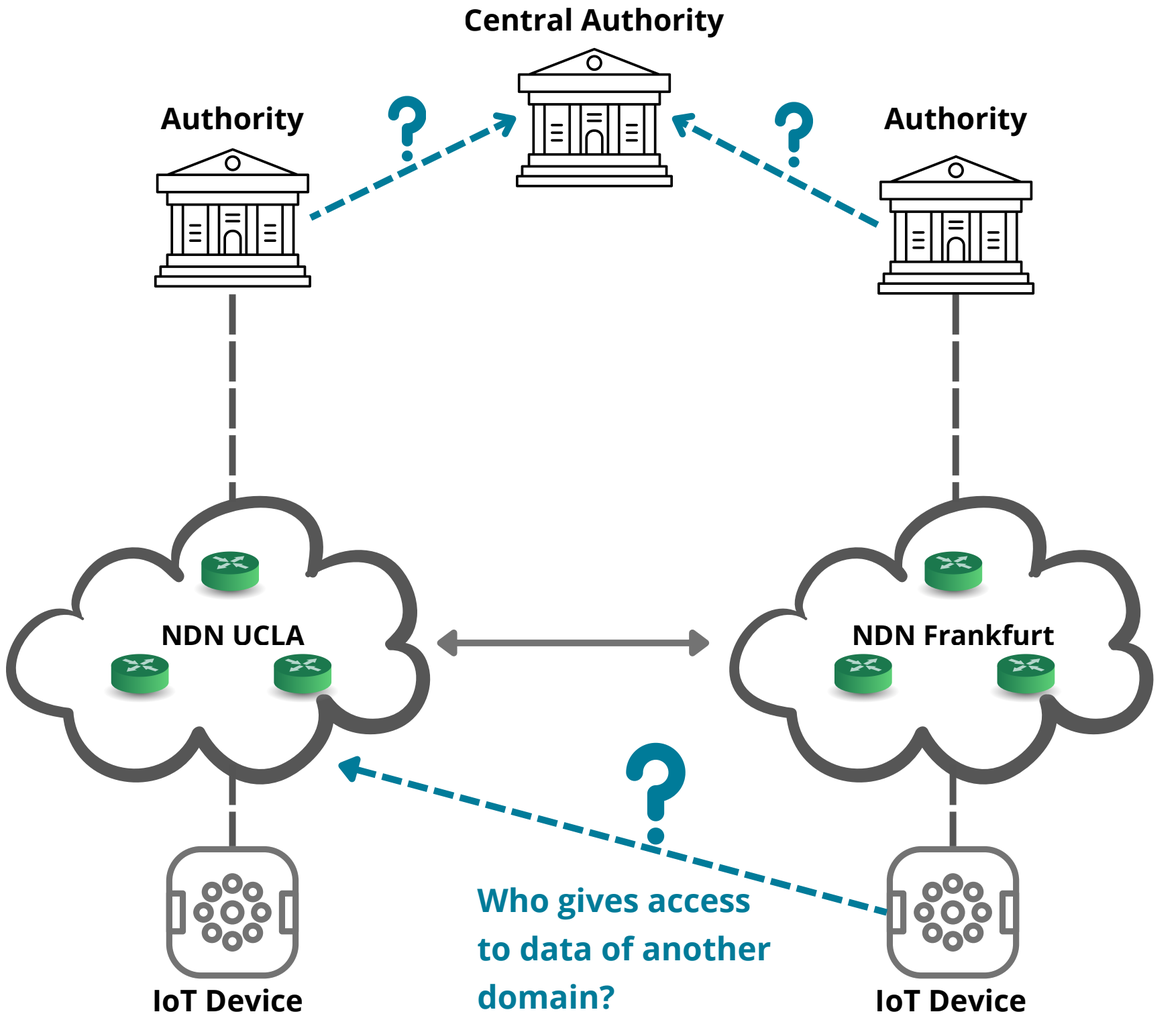


1 Attribute: (Master Key, Public key, Private key)

- **Access control based on attributes:** The access granularity is determined by attributes, with no reference to identities

Lewko, Allison, and Brent Waters. "Decentralizing attribute-based encryption." Annual international conference on the theory and applications of cryptographic techniques. Berlin, Heidelberg: Springer Berlin Heidelberg, 2011.

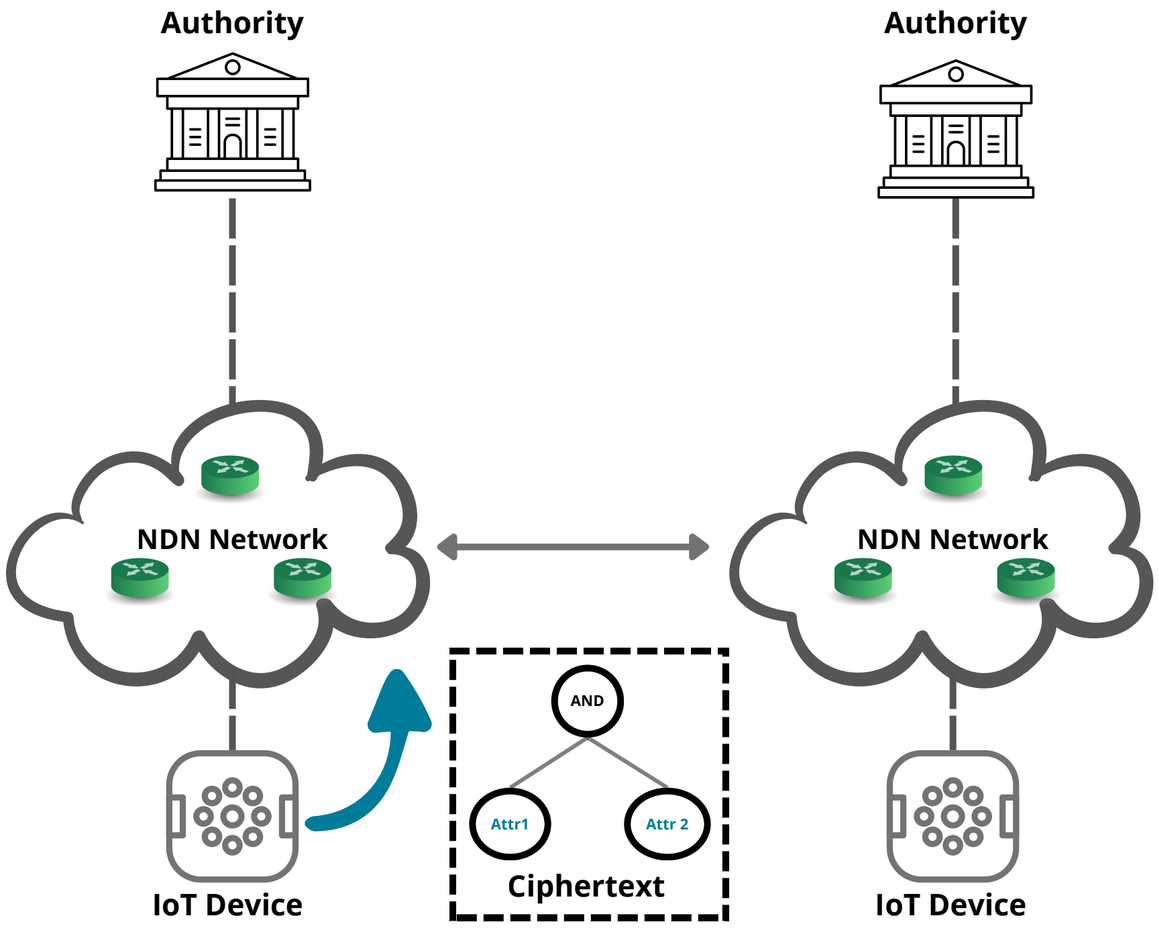
Multi-Authority Attribute-based Encryption



- **Access control based on attributes:** The access granularity is determined by attributes, with no reference to identities
- **No central authority**: Each authority manages its distinct set of attribut

Lewko, Allison, and Brent Waters. "Decentralizing attribute-based encryption." Annual international conference on the theory and applications of cryptographic techniques. Berlin, Heidelberg: Springer Berlin Heidelberg, 2011.

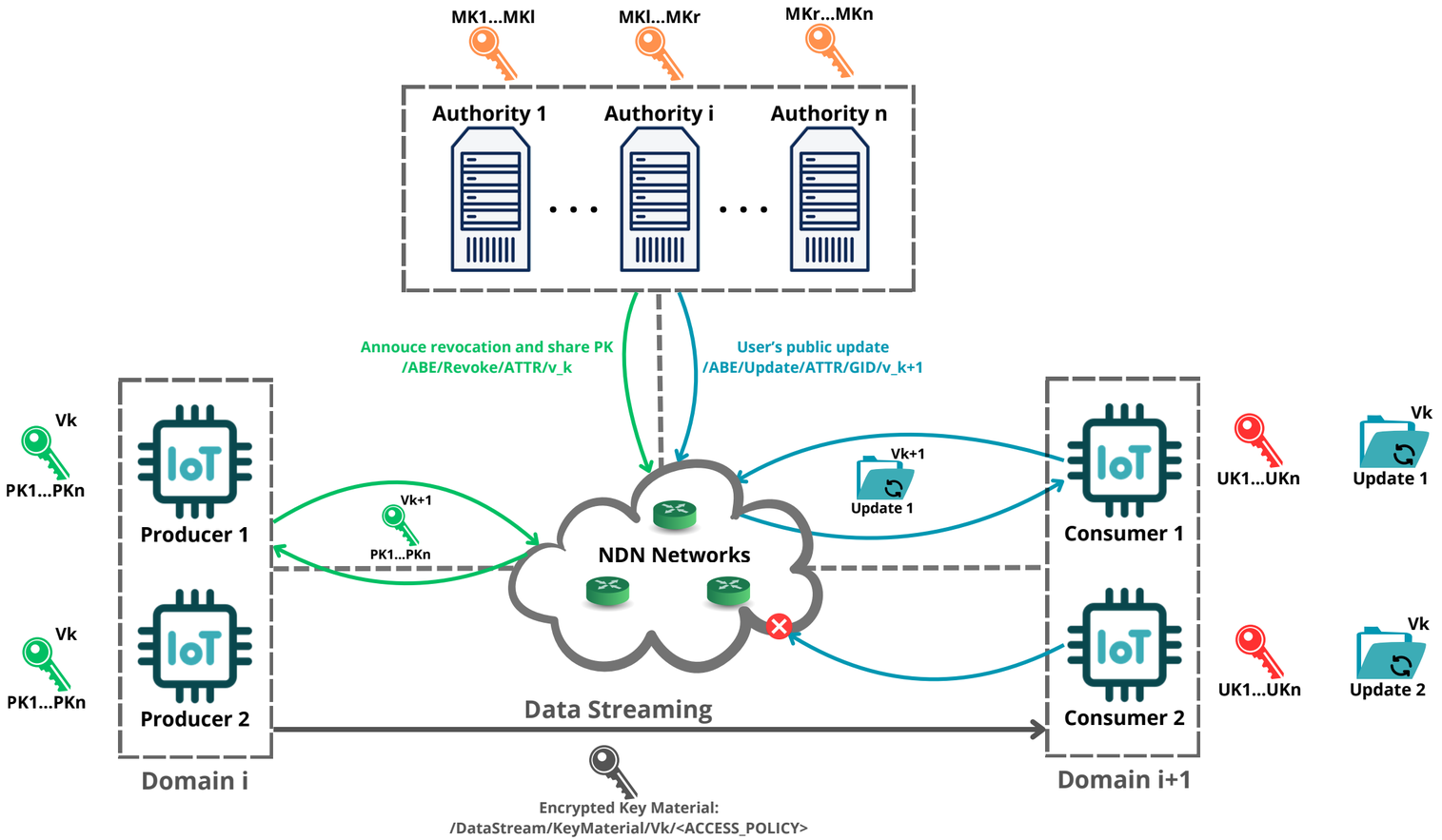
Multi-Authority Attribute-based Encryption



- **Access control based on attributes:** The access granularity is determined by attributes, with no reference to identities
- **No central authority**: Each authority manages its distinct set of attribut
- **Inheritant one-to-many communication**: Encrypted data can be accessed by multiple users meeting the access policy

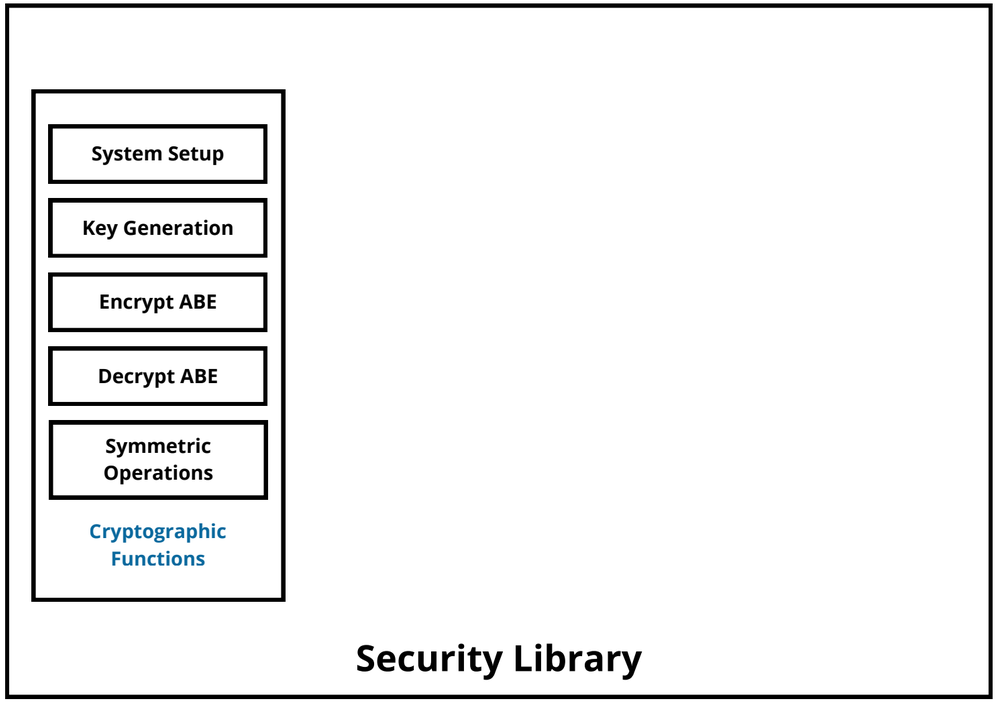
Lewko, Allison, and Brent Waters. "Decentralizing attribute-based encryption." Annual international conference on the theory and applications of cryptographic techniques. Berlin, Heidelberg: Springer Berlin Heidelberg, 2011.

Decentralized AC Library for NDN



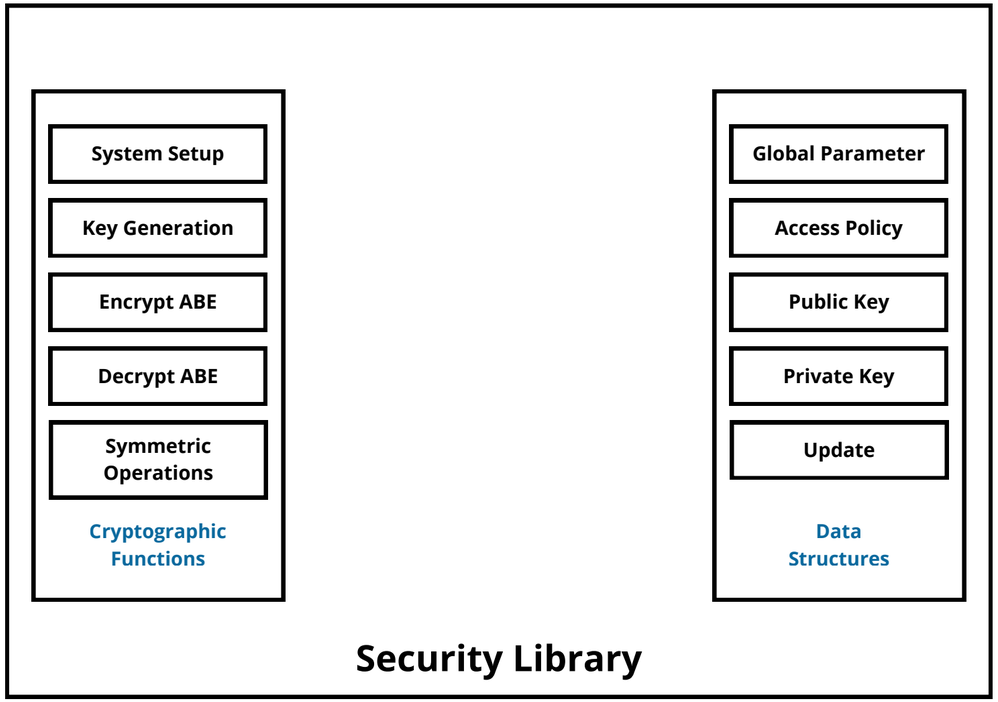
- **Open source security library** implementing a decentralized access control for NDN
- The C++ library allows **authorities to generate keys and manage access revocation**, and the clients to perform **encryption/decryption of data** in NDN under MA-ABE.
- The library aim to integrate into existing **NDN applications** and provide **confidentiality**

Library’s architecture



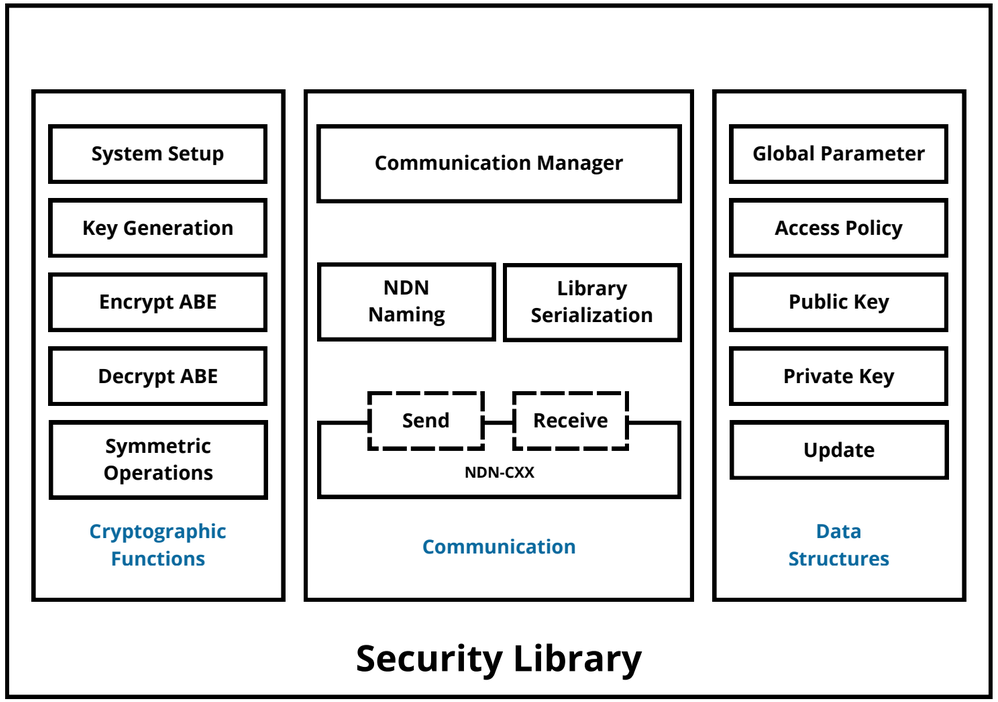
- **Cryptographic core**: Implementing the Decentralized Attribute-based Encryption Scheme

Library’s architecture

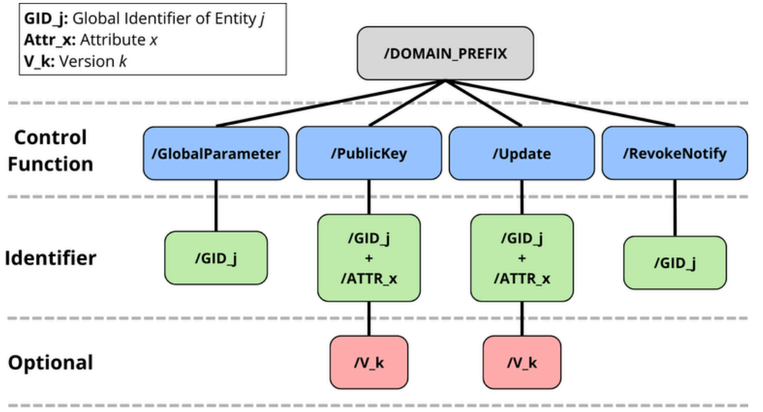


- **Cryptographic core**: Implementing the Decentralized Attribute-based Encryption Scheme
- **Data Structure**: Elements of the library that can serialized and exchanged on the network

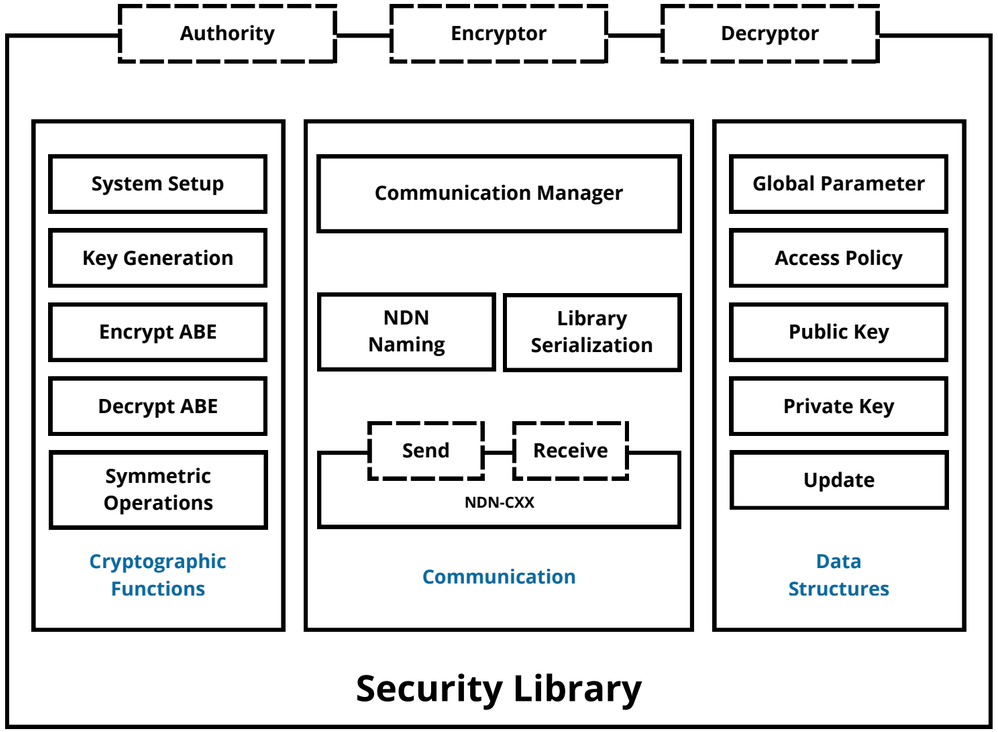
Library’s architecture



- **Cryptographic core**: Implementing the Decentralized Attribute-based Encryption Scheme
- **Data Structure**: Elements of the library that can serialized and exchanged on the network
- **Communication**: Handles the naming convention, object serialization, and callbacks of the library

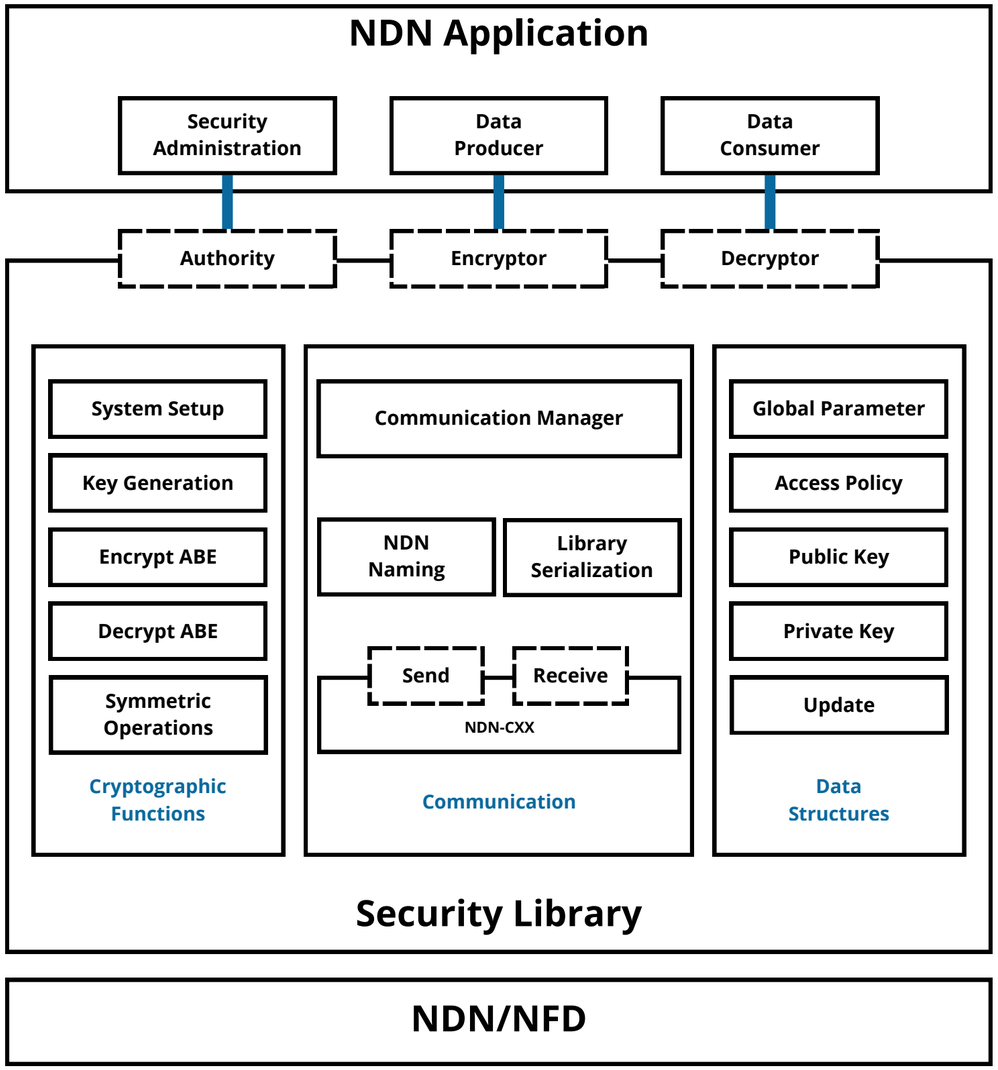


Library’s architecture



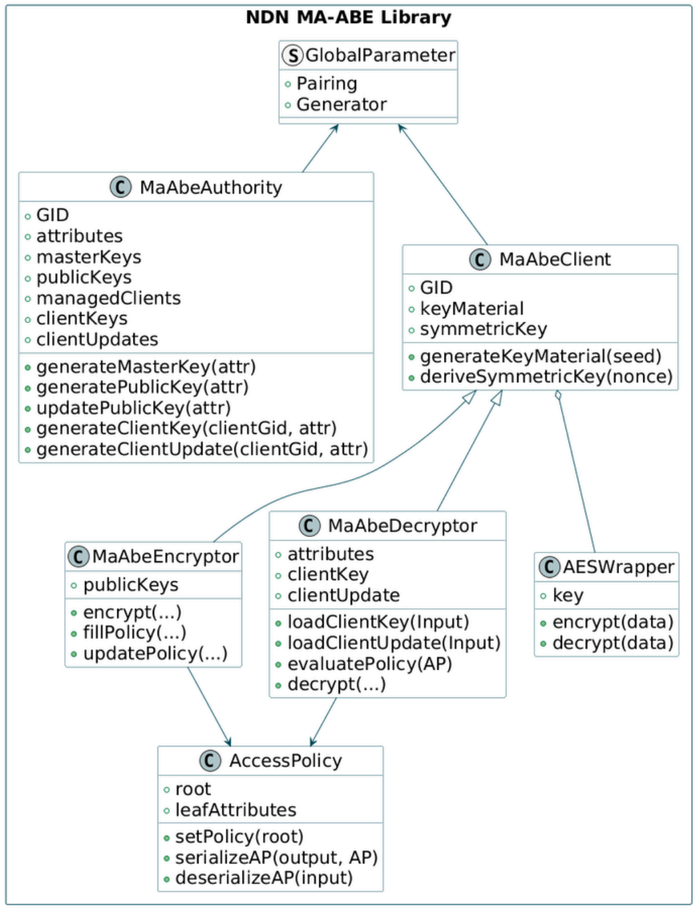
- **Cryptographic core**: Implementing the Decentralized Attribute-based Encryption Scheme
- **Data Structure**: Elements of the library that can serialized and exchanged on the network
- **Communication**: Handles the naming convention, object serialization, and callbacks of the library
- **AC roles**: The library allows nodes to perform one of three roles (Authority, Encryptor, Decryptor)

Library’s architecture



- **Cryptographic core**: Implementing the Decentralized Attribute-based Encryption Scheme
- **Data Structure**: Elements of the library that can serialized and exchanged on the network
- **Communication**: Handles the naming convention, object serialization, and callbacks of the library
- **AC roles**: The library allows nodes to perform one of three roles (Authority, Encryptor, Decryptor)
- **NDN Stack**: The library aim to sit between the Application and NDN layer, allowing encryption and decryption of data

Library's API



- **GMP/PBC**
- **Crypto++**
- **ndn-cxx**
- **NFD**

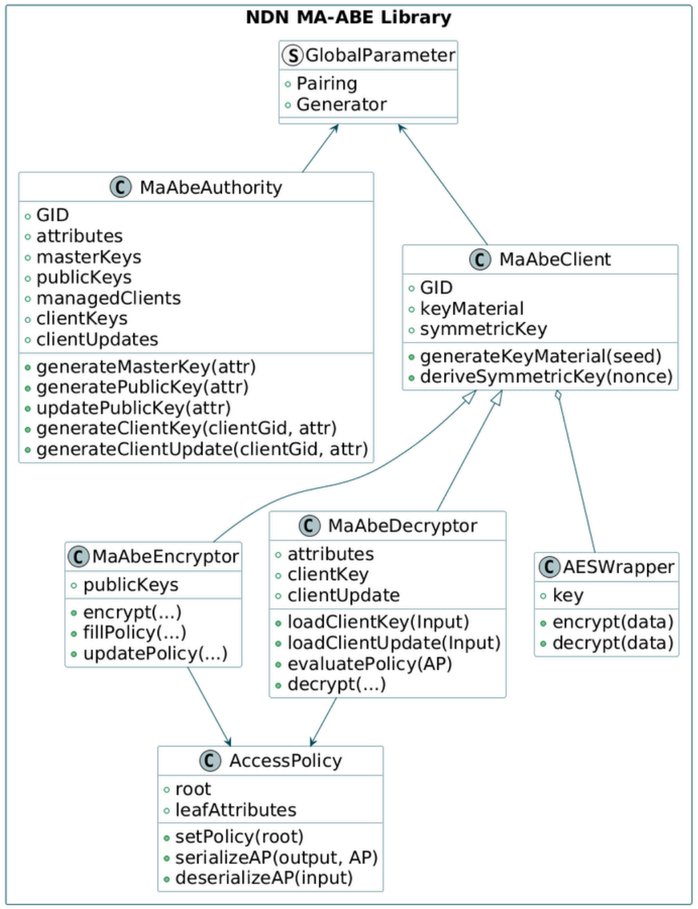
Only

Expose

Install

```
// Install the package
cd NDN-MA-ABE
cmake CMakeLists.txt
make
sudo make install
sudo ldconfig
```

Library's API



- **GMP/PBC**
- **Crypto++**
- **ndn-cxx**
- **NFD**

Only

Expose

Authority role

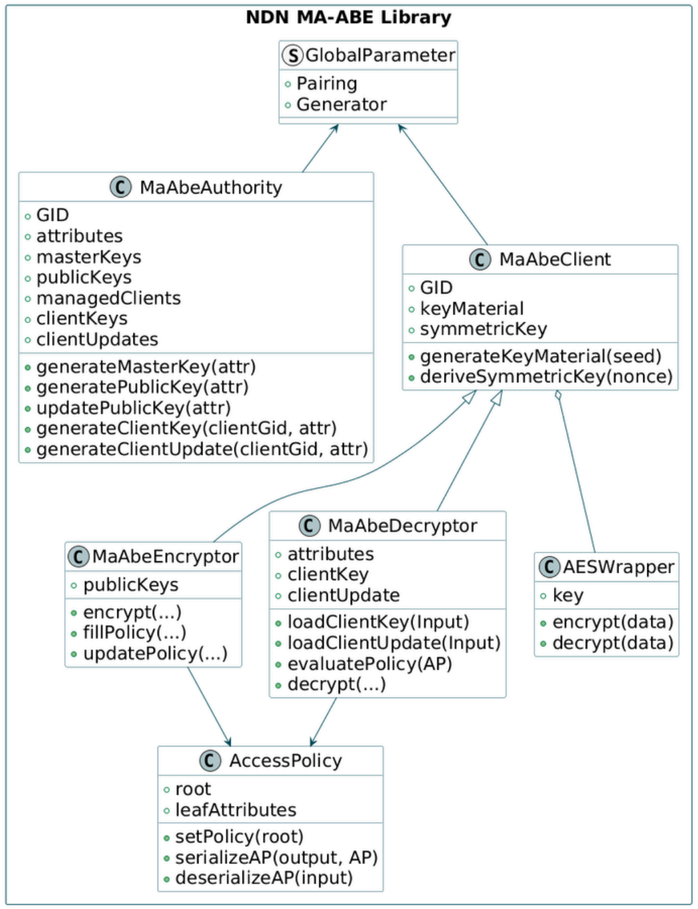
```
./MaAbeAuthorityNDN
    --gid AUTHORITY_GID
    --attrs ATTR_1,...,ATTR_N
    [--fetch-gp CONTENT_NAME]
```

```
authority> genkey CLIENT_GID ATTRIBUTE [OUTPUT_FILE]
authority> revoke CLIENT_GID ATTRIBUTE
```

Allows the authority to:

- Generate Master/Public/Private keys
- Publish Public keys into the network
- Revoke an access privilige

Library's API



- **GMP/PBC**
- **Crypto++**
- **ndn-cxx**
- **NFD**

Only

Expose

Encryptor role

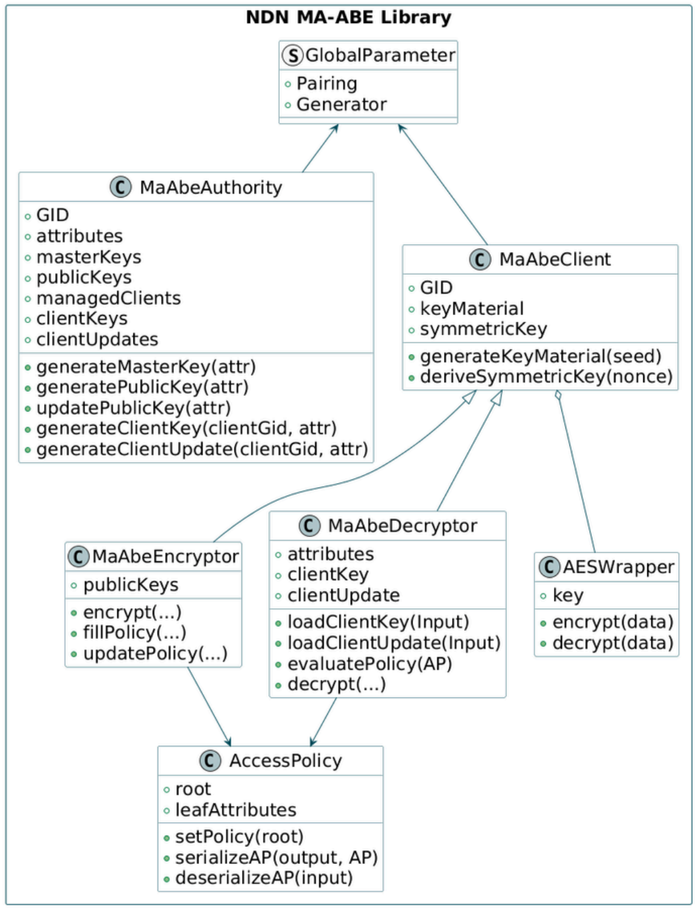
```
int publishEncryptedStream(
    ndn::Face& face,
    const ndn::Name& prefix,
    const std::string& accessPolicy,
    std::function<std::istream&(void)> provider);
```

***accessPolicy* recursive syntax:** $k/2(child1, child2)$

Allows the producer to:

- Retrieve public keys for the network
- Define an Attribute-based Access Policy
- Encrypt data

Library's API



- **GMP/PBC**
- **Crypto++**
- **ndn-cxx**
- **NFD**

Only

Expose

Decryptor role

```
int consumeEncryptedStream(
    ndn::Face& face,
    const ndn::Name& prefix,
    std::ostream& output,
    std::function<void(const uint8_t* data, size_t size)>
        onSegment = nullptr);
```

Allows the consumer to:

- Manage private keys
- Check satisfaction of Access Policies
- Decrypt ABE ciphertexts

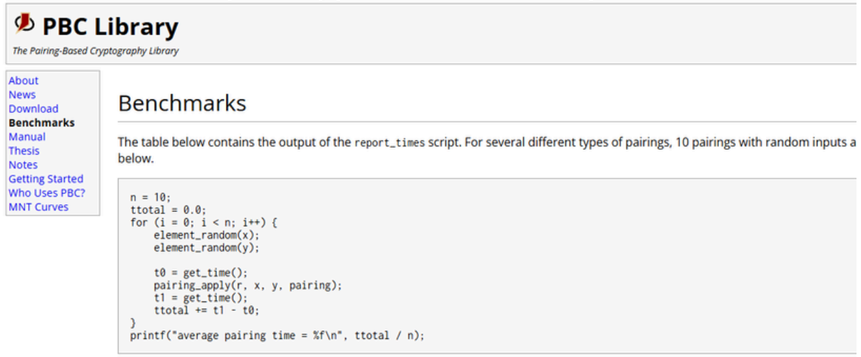
The goal

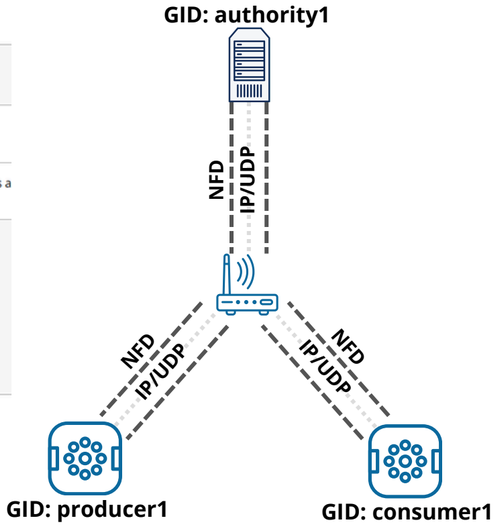
- Provide an **open source decentraliazed Attribute-based Encryption library** for the NDN Community.

- **Benchmark** of the library (To allow other work to compare to it), using:
  - Various **hardware configurations**
  - Various **security configurations/requirements**

- Evaluation of the library on a **small NDN testbed**

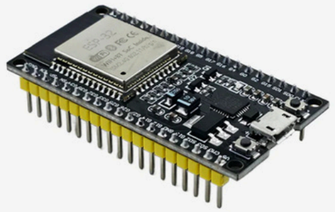
https://crypto.stanford.edu/pbc/





Jetson Nano

ESP32



x86 Machine

NAMED DATA NETWORKING COMMUNITY MEETING 2026

Thank you

Contact:

ferhat.mecerhed@uphf.fr

ferhat.mecerhed@student.uni-luebeck.de

UNIVERSITÄT ZU LÜBECK

Université Polytechnique HAUTS-DE-FRANCE