

IMPLEMENTATION AND ANALYSIS OF ATTRIBUTE-BASED ENCRYPTION PERFORMANCE IN ICN

Nurefşan Sertbaş & Samet Aytaç
CODE MANUAL

CCN-lite for Unix

<https://github.com/cn-uofbasel/ccn-lite.git>

- **Prerequisites**

Ubuntu: `sudo apt-get install libssl-dev`

OS X: `brew install openssl`

```
git clone https://github.com/cn-uofbasel/ccn-lite
export CCNL_HOME="$(pwd)/ccn-lite"
export PATH=$PATH:"$CCNL_HOME/bin"
cd $CCNL_HOME/src
make clean all
```

Ciphertext-Policy Attribute-Based Encryption

[<http://hms.isi.jhu.edu/acsc/cpabe/index.html>]

- Download `cpabe-0.11.tar.gz`, `libswabe-0.9.tar.gz` packages
- Untar, compile, and install as following

```
./configure
$ make
$ make install
```

Quick start Tutorial

1. Produce content, apply ABE and store in cache

```
sh producer.sh id filename.txt interest_name
```

*Note 'access policy' is embedded in the script you may want to change

Ex: sh producer.sh 1 demo.txt /ndn/test/cmp

2. Start node A and node B

```
sh node_a.sh
```

```
sh node_b.sh
```

3. Add forwarding rules

```
sh frules.sh
```

4. Create new user and set his/her attributes

```
sh createuser.sh name attributes
```

Ex: sh createuser.sh nurefsan sysadmin it_department

5. Send interest for an object

```
sh send_interest.sh interest_name name
```

Ex: sh send_interest.sh /ndn/test/mycontent samet