CYBERNETICA

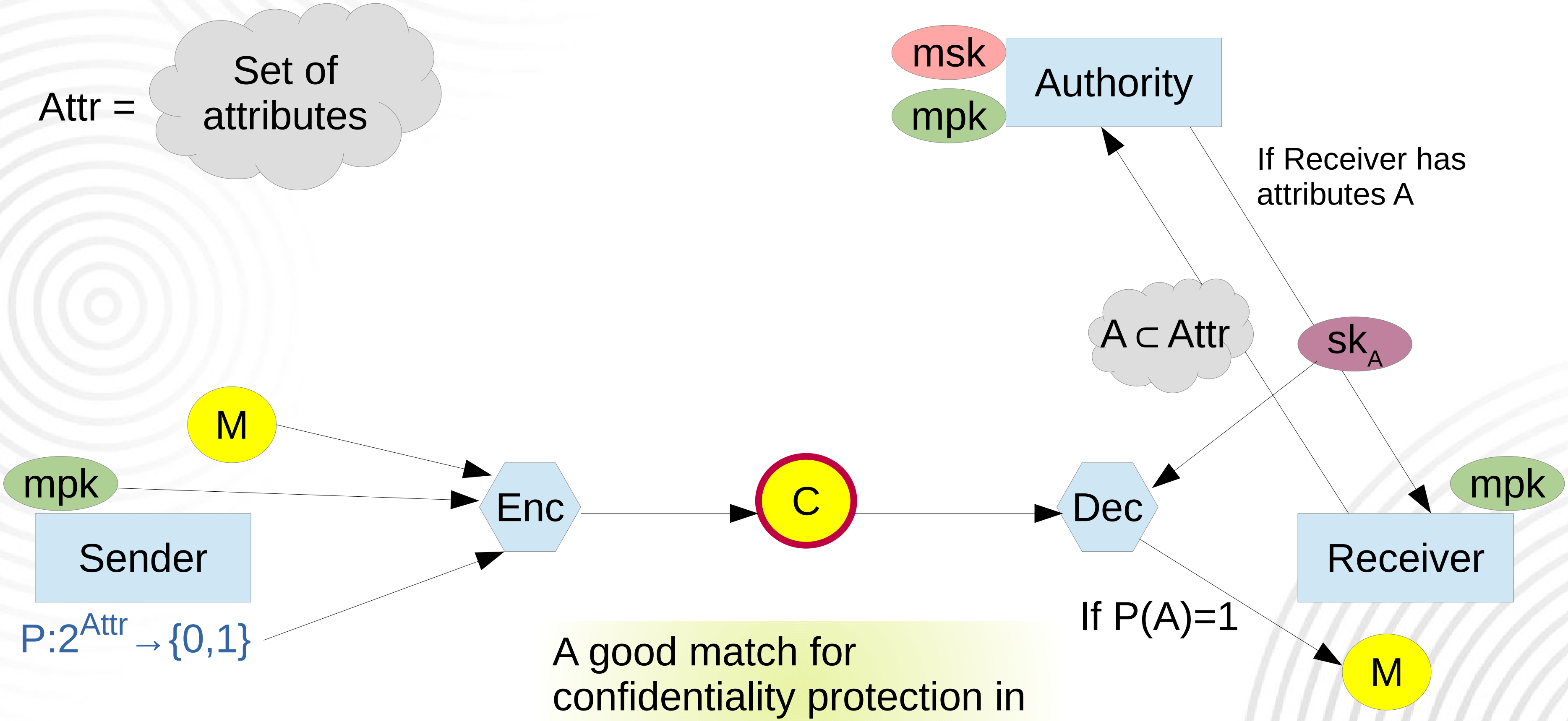
Attribute-Based Encryption for Named Data Networking

Aleksandr Lenin, Peeter Laud

peeter.laud@cyber.ee

This research has been funded by the Defense Advanced Research Projects Agency (DARPA) under contract HR0011-17-C-0111. The views, opinions, and/or findings expressed are those of the author(s) and should not be interpreted as representing the official views or policies of the Department of Defense or the U.S. Government.

Ciphertext-Policy Attribute-Based Encryption (CP-ABE)



Attr = Set of attributes

msk

mpk

Authority

If Receiver has attributes A

$A \subset Attr$

sk_A

M

mpk

Sender

$P:2^{Attr} \to \{0,1\}$

Enc

C

Dec

mpk

Receiver

If P(A)=1

M

A good match for confidentiality protection in content-centric networks

Parameters of CP-ABE constructions

- Expressiveness of policies
  - Conjunctions. Disjunctions?
  - Negations?
- Computational cost (depending on attributes, policies)
  - Encryption
  - Decryption
- Size (depending on attributes, policies)
  - mpk, sk, C

- Different constructions optimize different parameters (possibly at cost of others)
- One construction does not fit all applications

Our contribution

- Comparison of several different CP-ABE constructions
- Selection of one of them
  - With the goal to fit a particular application
- Measurement of the overheads in NDN from the use of CP-ABE
  - Compared to no encryption at all

CYBERNETICA

info@cyber.ee
www.cyber.ee

Cybernetica AS
Mäealuse 2/1
12618 Tallinn
Estonia

A B C D E F G H I J K L M N O P Q R S Š Z Ž T U V W Õ Ä Ö Ü X Y 0 1 2 3 4 5 6 7 8 9 –

CYBERNETICA