Formal Language Identity-based Cryptography

Ádám Vécsi
Attila Pethő

CECC 2020, Zagreb
June 24-26, 2020.

Identity-based Encryption

- An important branch of the public key cryptography.
  - The idea was given by Shamir in 1984.
  - The first, well working scheme was created by Boneh and Franklin (2001).
- The public keys are clear identifiers of individuals.
  - Local or global domain.
  - E-mail, phone number, etc.
- The encryptor key and the public key of the decryptor have to be identical. Both of them are handled as bitstrings.

Fuzzy Identity-based Encryption

- The core idea is to handle the public keys as sets of attributes.
- A certain amount of overlap required between the encryptor key and the public key of the decryptor.
- It is faster to encrypt to a group of people this way than encrypting to everyone individually.
- Slower *setup*, *extract* and *decrypt* algorithms.

Identity-based Encryption with wildcards

- The encryptor key is a pattern.
  - *@cs.*.edu
- In the system it is treated as a vector.
  - $P = (P_1, \dots, P_l) \in (\{0,1\}^* \cup \{*\})^l$
- The runtime of the algorithms are depending on the size of the vector.

Attribute-based Encryption

- Expands the idea of the Fuzzy IBE, that the public keys are sets of attributes.
- The novelty in these schemes is building an access-tree to the keys.
  - It allows using AND and OR gates.

KP-ABE

- Ciphertexts are associated with sets of descriptive attributes.
- User keys are associated with policies.

CP-ABE

- Ciphertexts are associated with policies.
- User keys are associated with sets of descriptive attributes.

ABE with more flexible encryption key

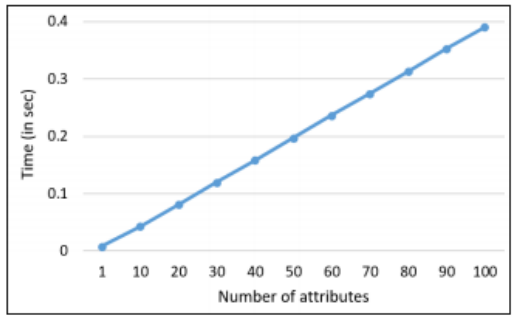
- There are ABE schemes with more feature:
  - access structures including negation

    NOT Year:1991-2000
    Year:NOT 1991-2000

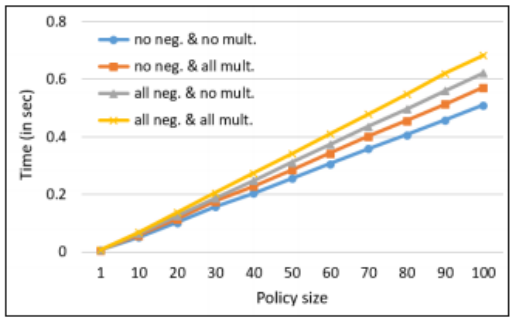
  - multi-use of attributes

    ((Year:1991-2000 AND Category:jazz)
    OR
    (Year:2001-2010 AND Category:jazz)
    OR
    (Year:2001-2010 AND Artist:The Beatles))

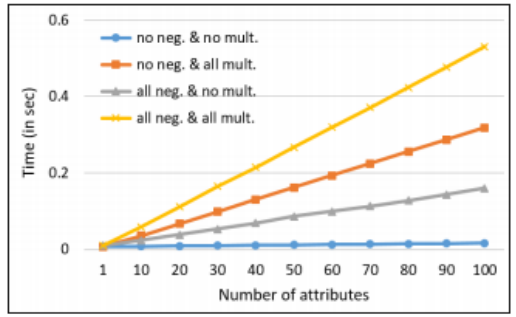
The disadvantage of the ABE schemes



(a) Enc

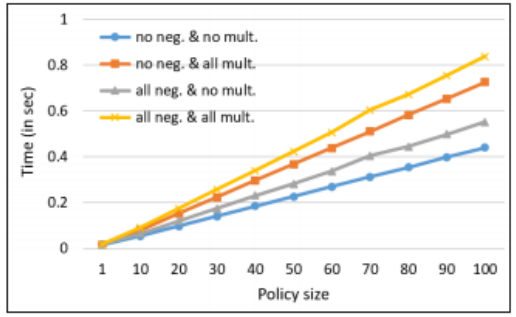


(b) KeyGen

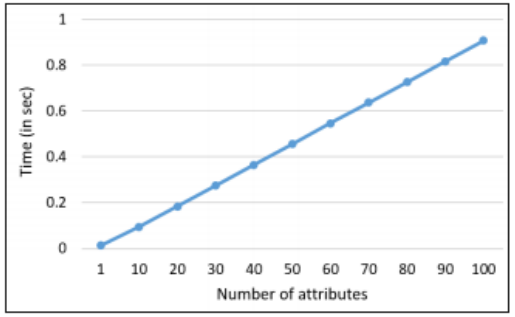


(c) Dec

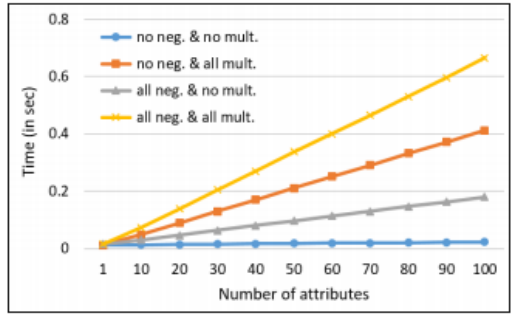
Figure 9: Benchmarks for KP-ABE on the personal computer.



(a) Enc



(b) KeyGen



(c) Dec

Figure 10: Benchmarks for CP-ABE on the personal computer.

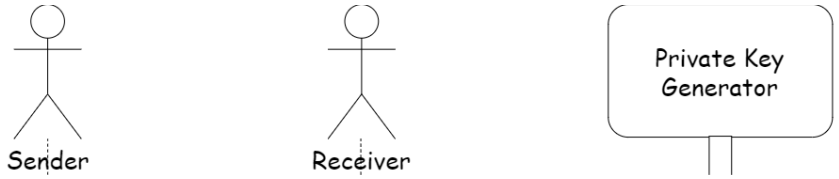
source: https://eprint.iacr.org/2019/966.pdf

Formal Language Identity-based Encryption

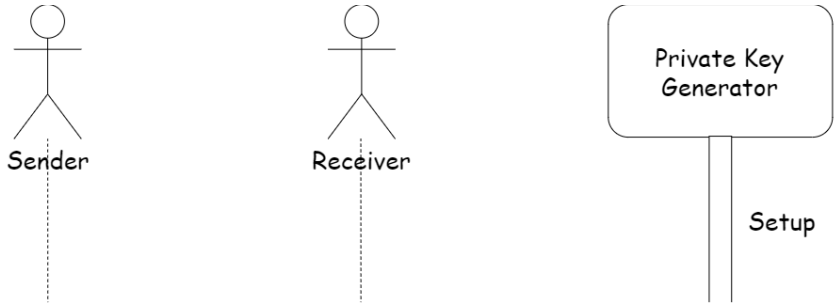
An **attribute** a is a pair (N_a, L_a), where N_a is the name of the attribute and L_a is the formal language including all possible values of the attribute.

A **property** $p = (N_p, V_p)$ defines the actual values of an entity regarding to the attribute a, if $N_p = N_a$ and $V_p \subseteq L_a$.

Let Ω be the set of entities and P the set of properties in a given domain. In our protocol PK_α is the public key of an $\alpha \in \Omega$ enitiy, if $PK_\alpha \subseteq P$ and $\exists\, ID_\alpha \subseteq PK_\alpha$, where for all $\beta \in \Omega$, $ID_\alpha \setminus ID_\beta \neq \emptyset$. ID_α is the identifier of α.



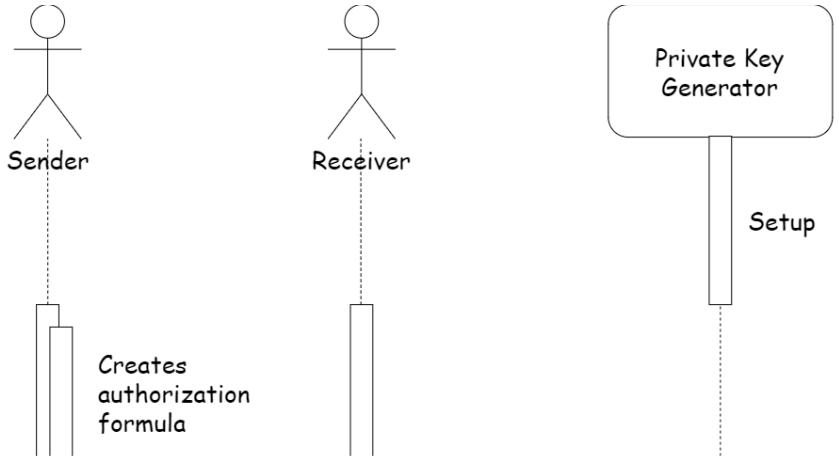
Formal Language Identity-based Encryption



Formal Language Identity-based Encryption

An **authorization formula** Υ is a logic formula that contains boolean operators and attribute constraints.

Let $a = (N_a, L_a)$ be an attribute. $\gamma = (N_\gamma, L_\gamma)$ is an **attribute constraint** for a, if $N_\gamma = N_a$ and $L_\gamma \subseteq L_a$, where L_a is the language, which containts the accepted property values.

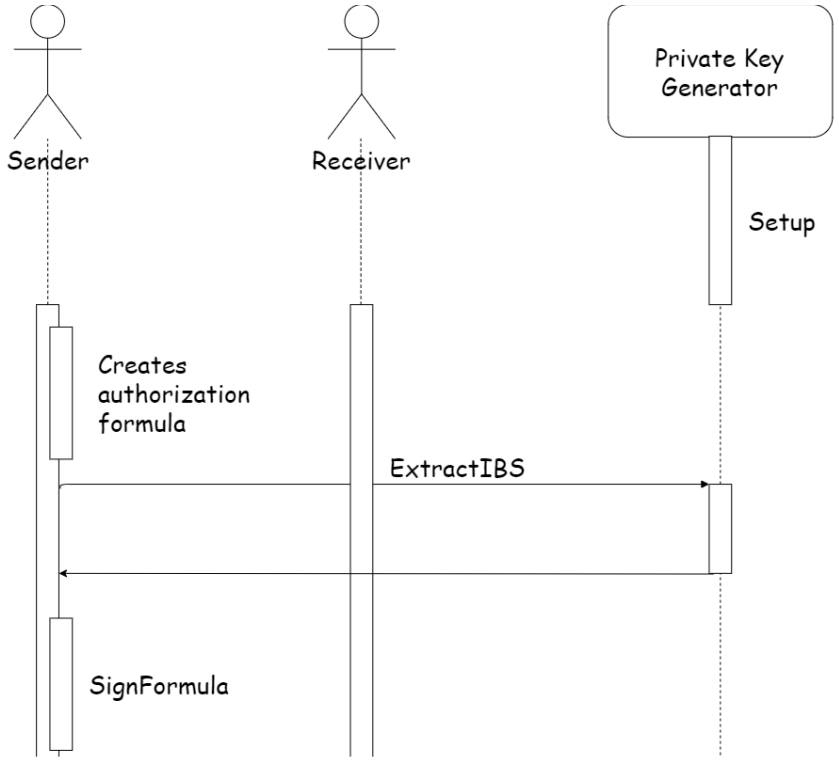


Example:

("e-mail", .*@company\.com)
AND
("job", {Lead developer, Chief Technology Officer})

Formal Language Identity-based Encryption

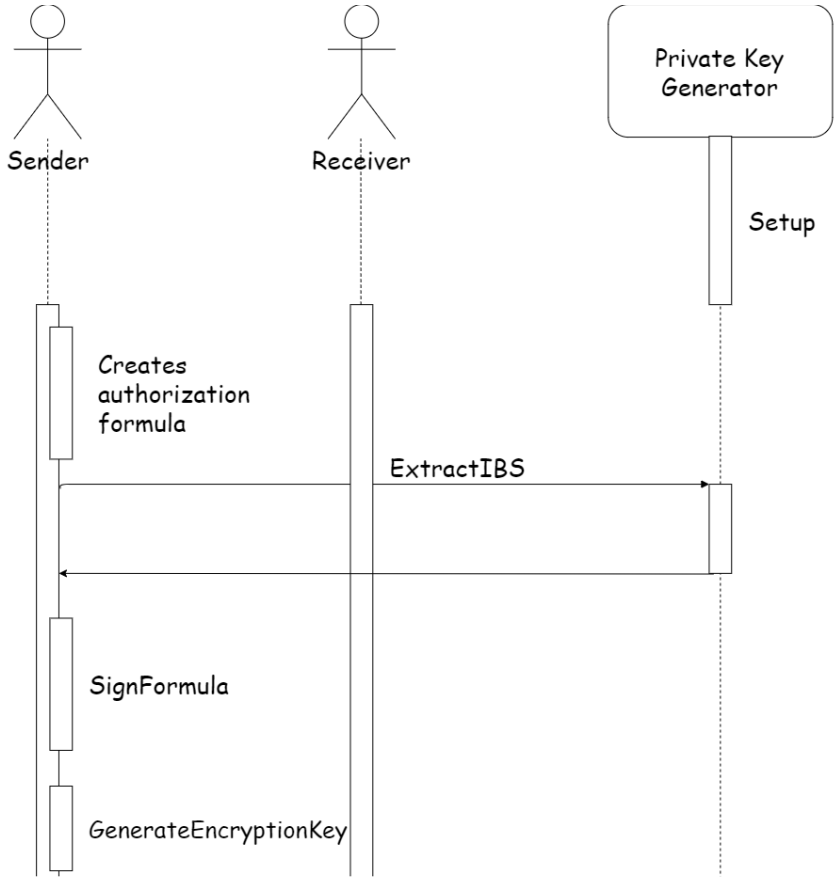
The purpose of the digital signature is to prevent the creation of fake authorization formula.



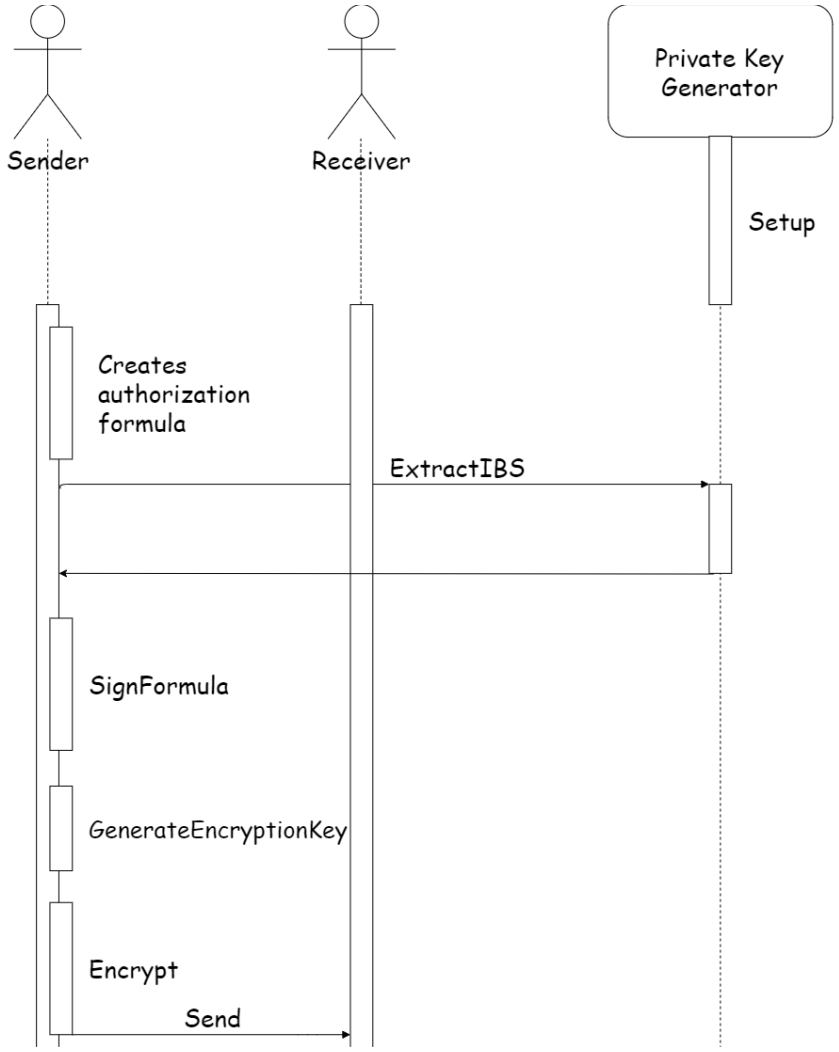
Formal Language Identity-based Encryption

A new encryption key should be generated for every authorization formula.

The key can be used multiple times with the same formula.

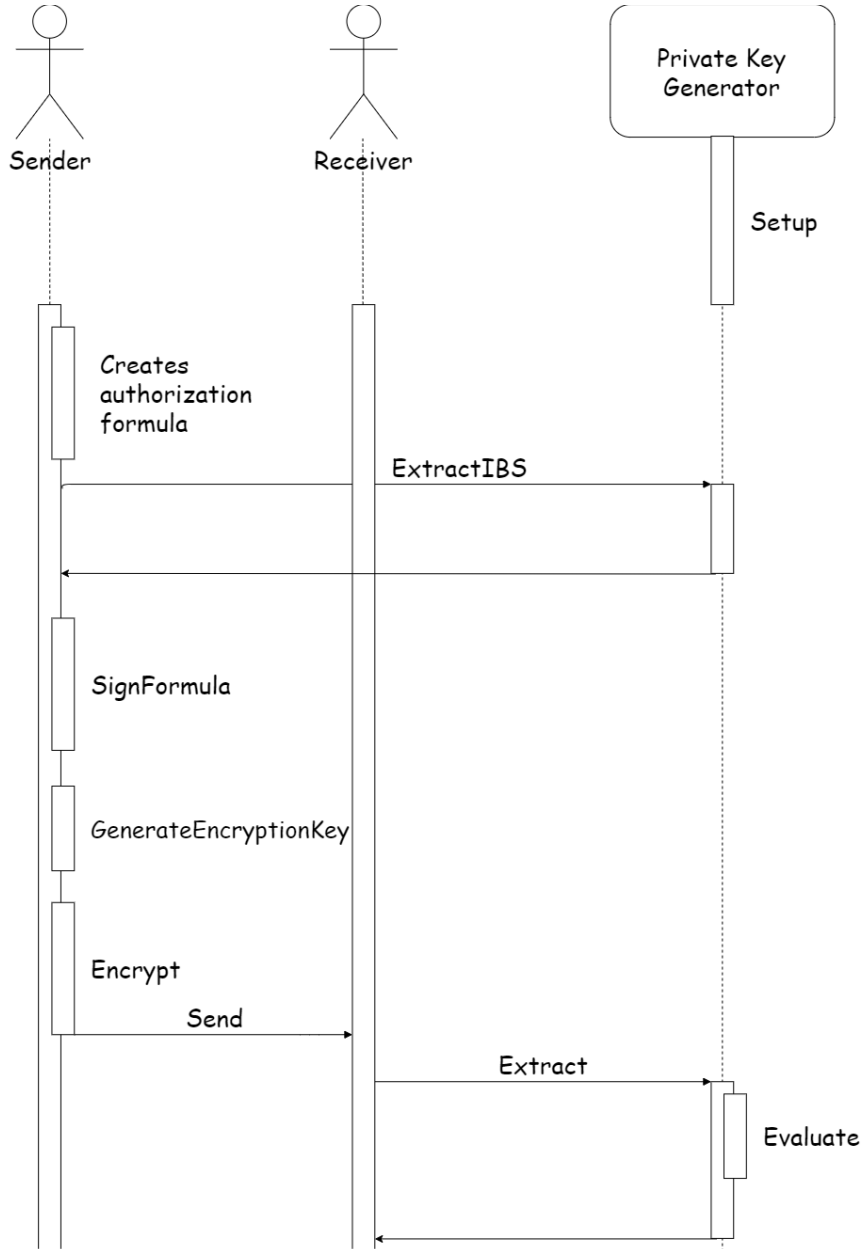


Formal Language Identity-based Encryption

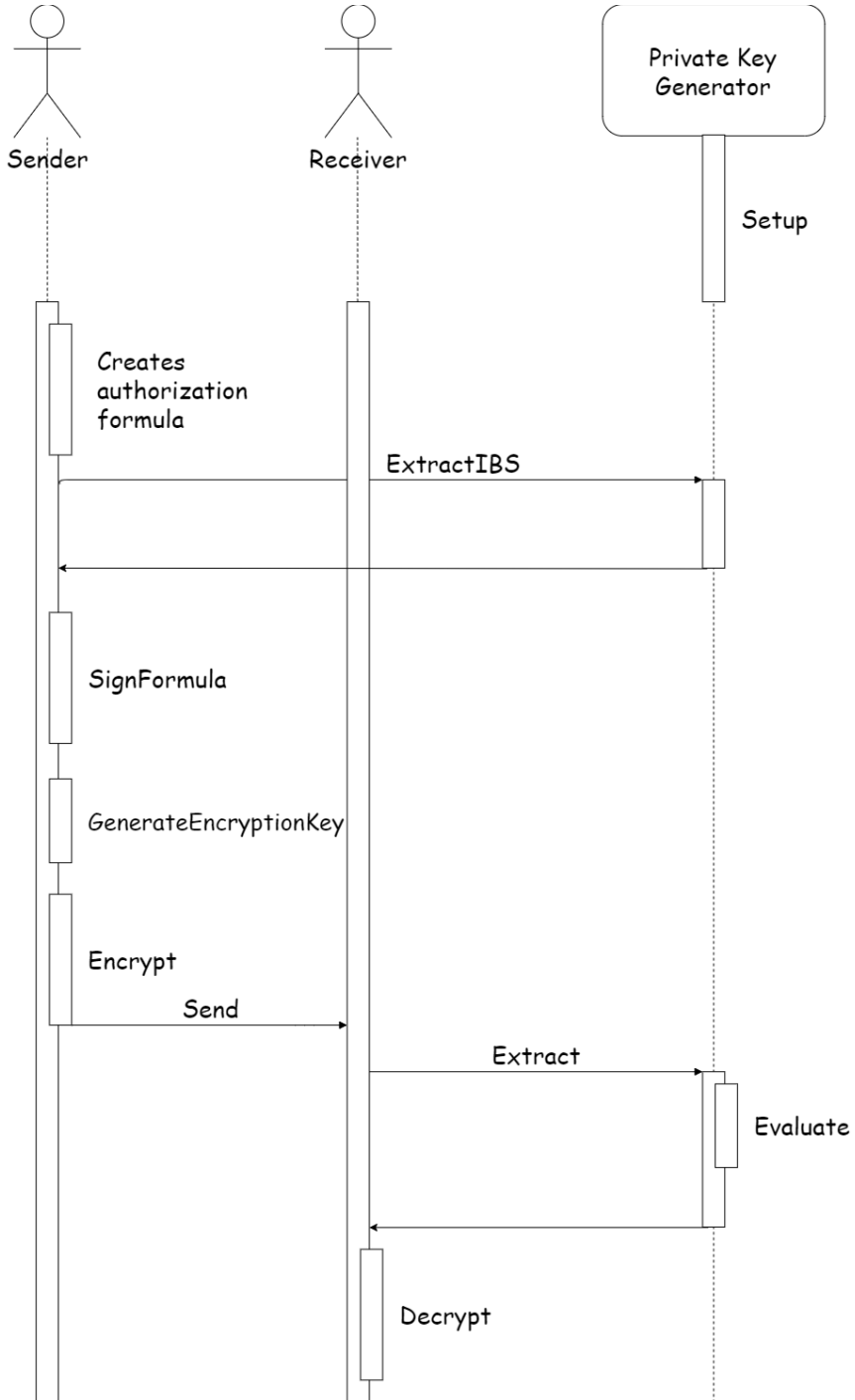


Formal Language Identity-based Encryption

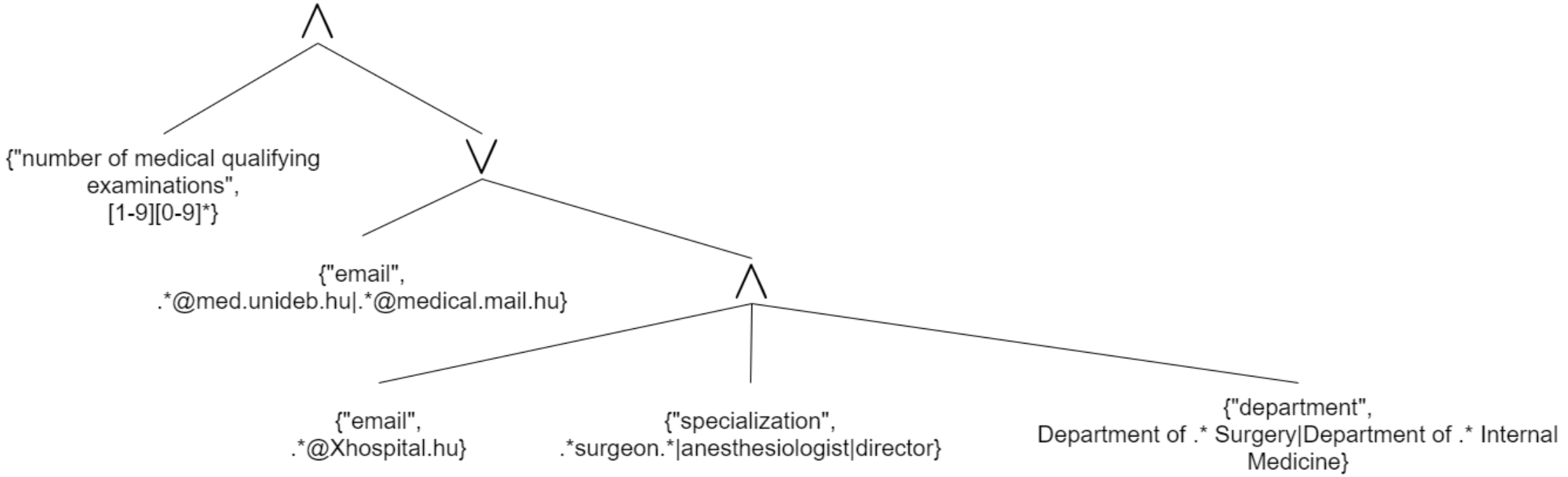
The *Extract* algorithm includes the signature verification and the evaluation process of the authorization formula.



Formal Language Identity-based Encryption



FLIBE usage example



FLIBE advantages

- Flexible target definition.
- Option to support future entities (currently not existing or not fitting).
- ”Constant” client-side runtime.
- The protocol can be used for digital signatures with minor changes.

FLIBE disadvantages

- The authorization formula is attached to the ciphertext, which means increased cipher size.
- The runtime of the *extract* method depends on the complexity of the authorization formula.

This work is supported partially by the construction EFOP-3.6.3-VEKOP-16-2017-00002. The project is supported by the European Union, co-financed by the European Social Fund.

This work is supported partially by the SETIT (2018-1.2.1-NKP-2018-00004) project.

Thank you
for your attention!