A prototype for efficient and secure file sharing and search on encrypted keywords

Emanuele Bellini
emanuele.bellini@telsy.it

Telsy S.p.A.

Trento, 28/10/2016

Telsy S.p.A.

Telsy is a reliable partner for ICT security solutions and services ever since 1971.

In 1990 TELSY enters the TELECOM ITALIA Group (TIM today)

TELSY is certified by the Italian National Authority for Security as a supplier of devices, systems and solutions for information protection at all security levels.

Dozens of Governments and Corporates have adopted Telsy’s solutions worldwide.

Index

- ✓ Commercial solutions for cloud encryption and file sharing
- ✓ Attribute-Based Encryption and file sharing
- ✓ Searchable Encryption
- ✓ Telsy prototype

Some notation and terminology...


Secret key


Public key


Encrypted file

Group = set of users sharing some data

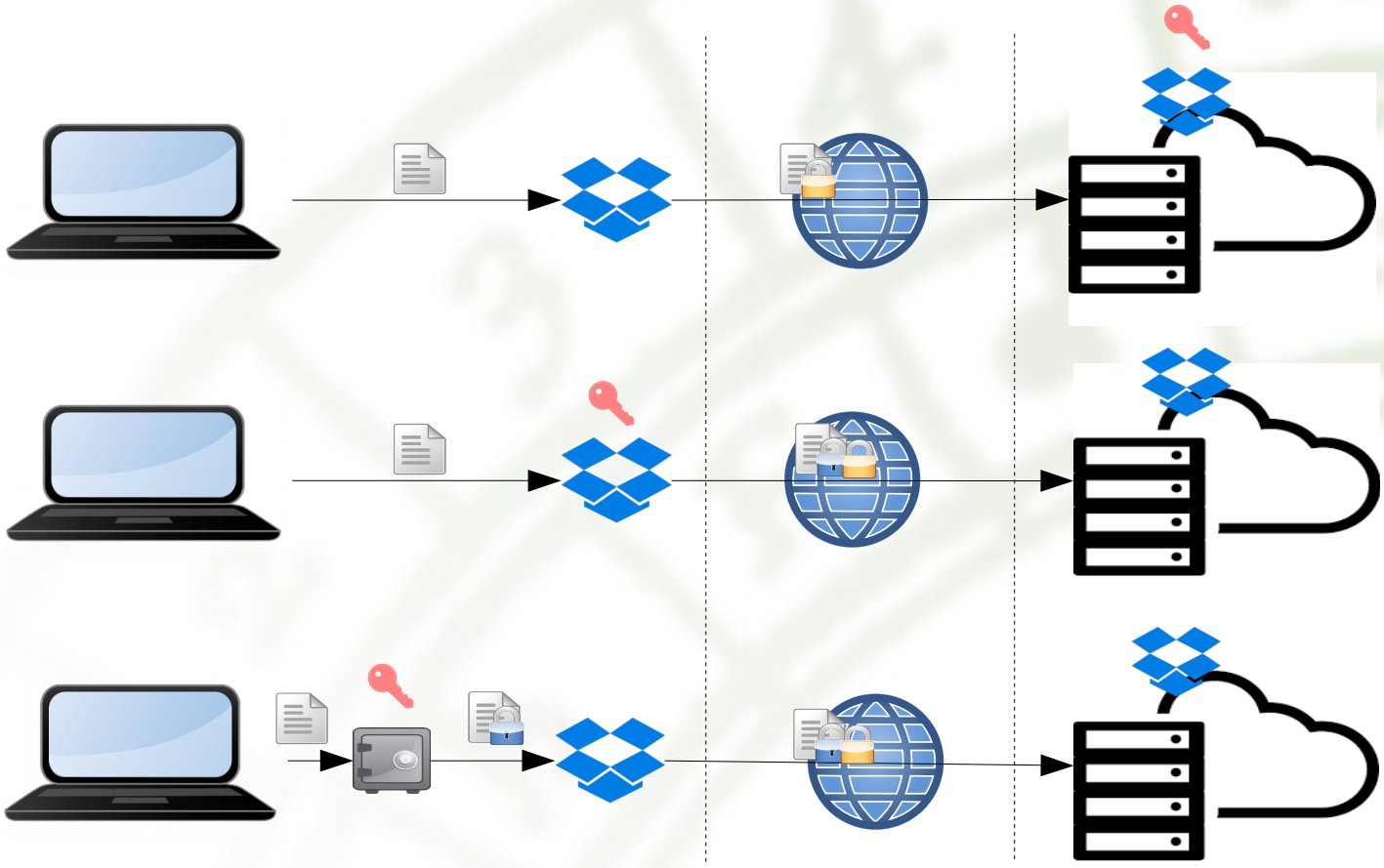
Commercial solutions for cloud encryption and file sharing

Encryption types

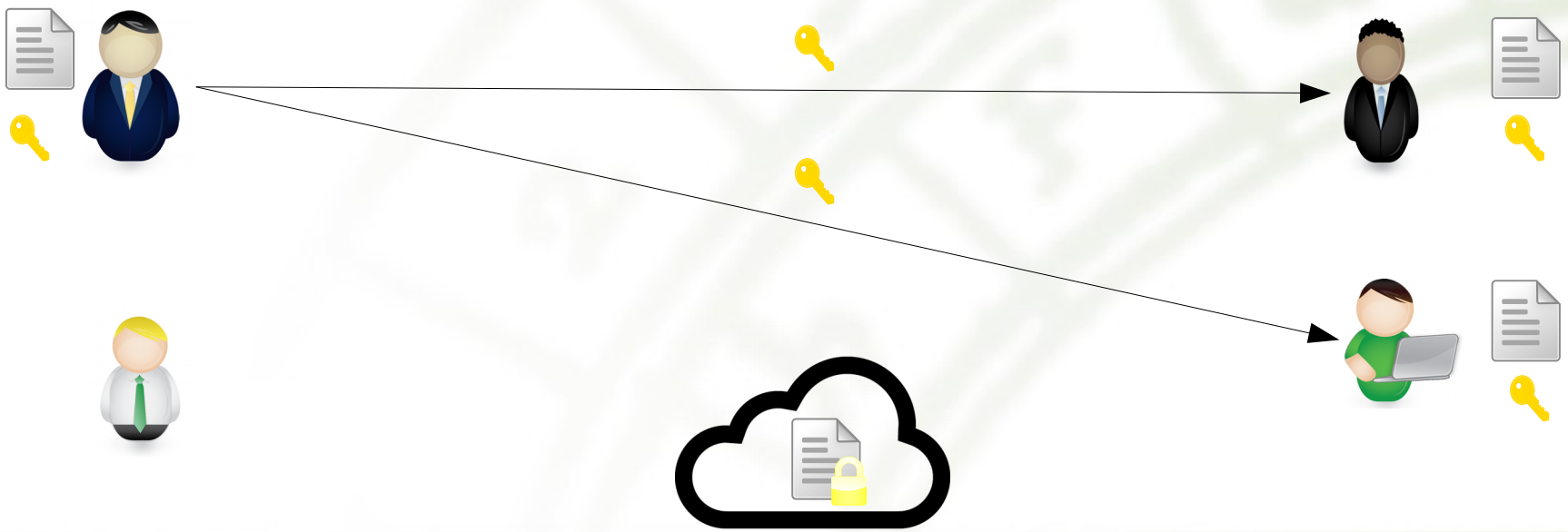
Server Side
Storage, Sharing,
Manipulate data
Ex: Dropbox, Google Drive, OneDrive, ...

Client Side (CS) Native
Storage, Sharing
Ex: Tresorit, Spideroak, ...

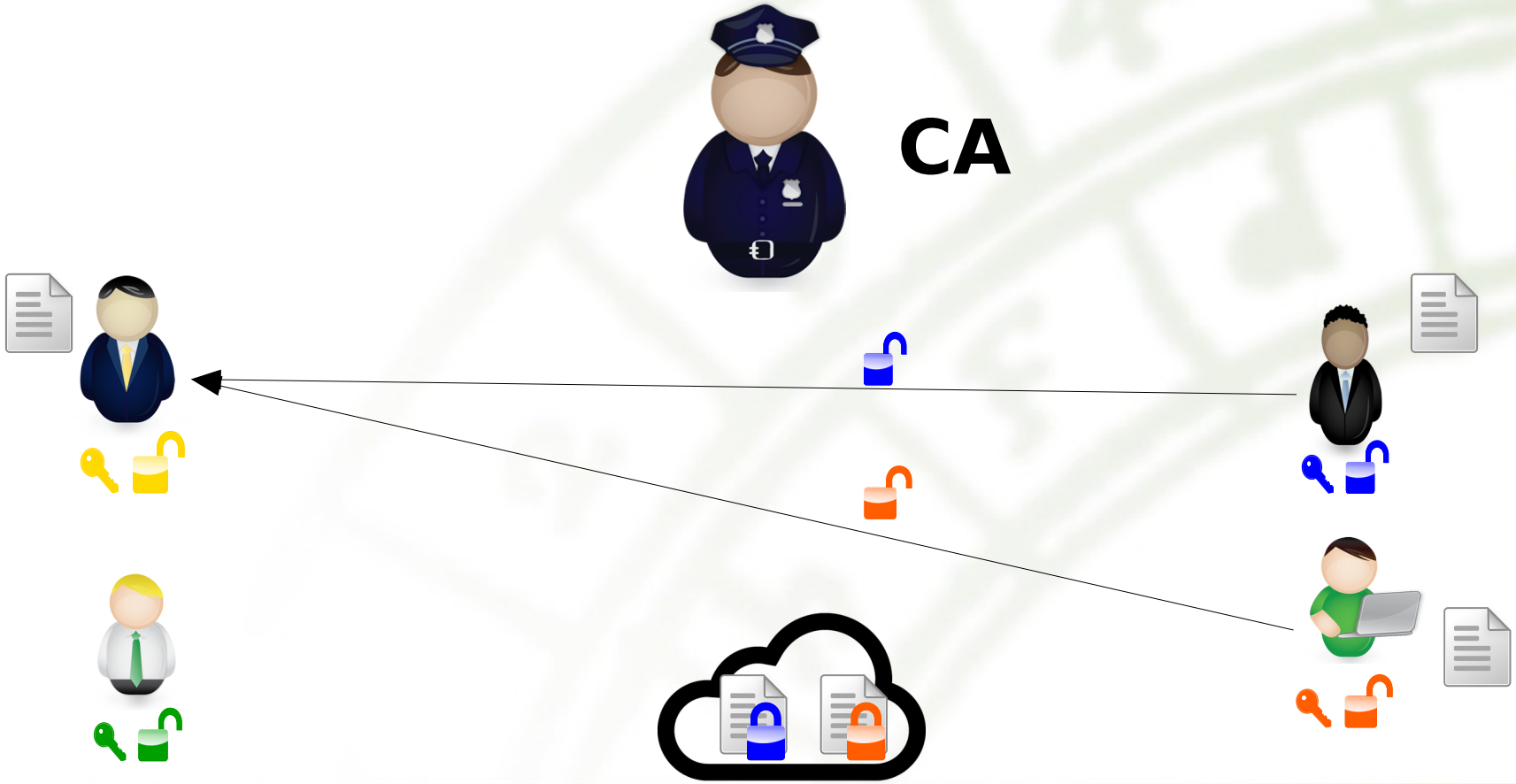
Client Side Third-party
Storage, Sharing,
Ex: Boxcryptor, Cloudfogger, Viivo, ...



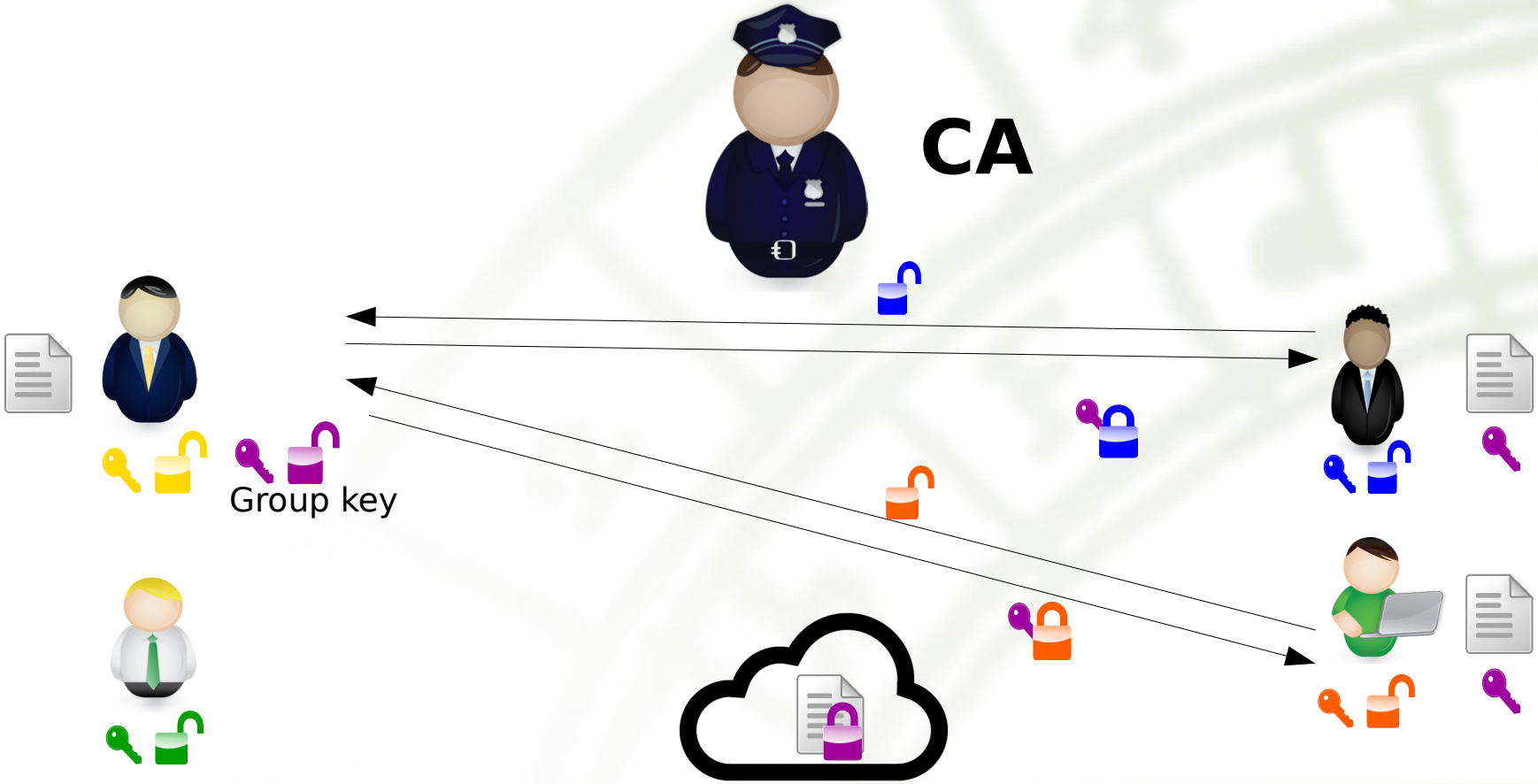
CS file sharing model: solution 0



CS file sharing model: solution 1



CS file sharing model: solution 2



CSE comparison

	Solution 1	Solution 2
Number of personal asymmetric key pairs	1	1
Number of group asymmetric key pairs per user	0	Linear with number of groups a user belongs to*
Ciphertext size	Linear with group size	Constant
Revocation	Delete part of the ciphertext	Re-encryption and key re-destribution
Public-key management	Certification Authority	Certification Authority

* The number of groups can possibly be exponential in the number of users of the system

Attribute-Based Encryption

Attribute-Based Encryption

Attribute-based encryption is a type of public-key encryption in which the secret key of a user and the ciphertext are dependent upon attributes.

In such a system, the decryption of a ciphertext is possible only if the set of attributes of the user key matches (a policy on) the attributes of the ciphertext.

Attribute-Based Encryption

- ✓ 2001 – IBE

  Boneh, Franklin - “Identity-Based Encryption from the Weil Pairing”

- ✓ …
- ✓ 2006 – CP-ABE

  Brent, Sahai, Waters - “Ciphertext-Policy Attribute-Based Encryption”

- ✓ 2006 – KP-ABE

  Goyal, Pandey, Sahai, Waters - “Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data”

- ✓ …
- ✓ 2009 – FULL SECURE IBE

  Waters - “Dual System Encryption: Realizing Fully Secure IBE and HIBE under Simple Assumptions”

- ✓ 2010 – FULL SECURE ABE

  Lewko, Sahai, Waters, Okamoto, Takashima - “Fully Secure Functional Encryption: ABE and (Hierarchical) Inner Product Encryption”

- ✓ 2011 – Constant ciphertext

  Attrapadung, Libert, de Panafieu - “Expressive Key-Policy ABE with Constant-Size Ciphertexts”

- ✓ …

Attribute-Based Encryption

- ✓ 2011 – Multi-Authority

  Lewko, Waters - “Decentralized Attribute-Based Encryption”

- ✓ 2012 – Dynamic Credential, Ciphertext Delegation

  Sahai, Seyalioglu, Waters - “Dynamic Credentials and Ciphertext Delegation for Attribute-Based Encryption”

- ✓ 2013 – Non-monotonic access structure

  Yang, Wu, Wang, Du - “Fully Secure Attribute-Based Encryption with Non-monotonic Access Structures”

- ✓ 2013 – Fast Decryption

  Hohenberger, Waters - “Attribute-Based Encryption with Fast Decryption”

- ✓ 2013 – Self-Updatable Encryption, Hidden Attributes

  Lee,Choi,Lee,Park,Yung - “Self-Updatable Encryption: Time Constrained Access Control with Hidden Attributes and Better Efficiency”

- ✓ 2014 – Traceble ABE

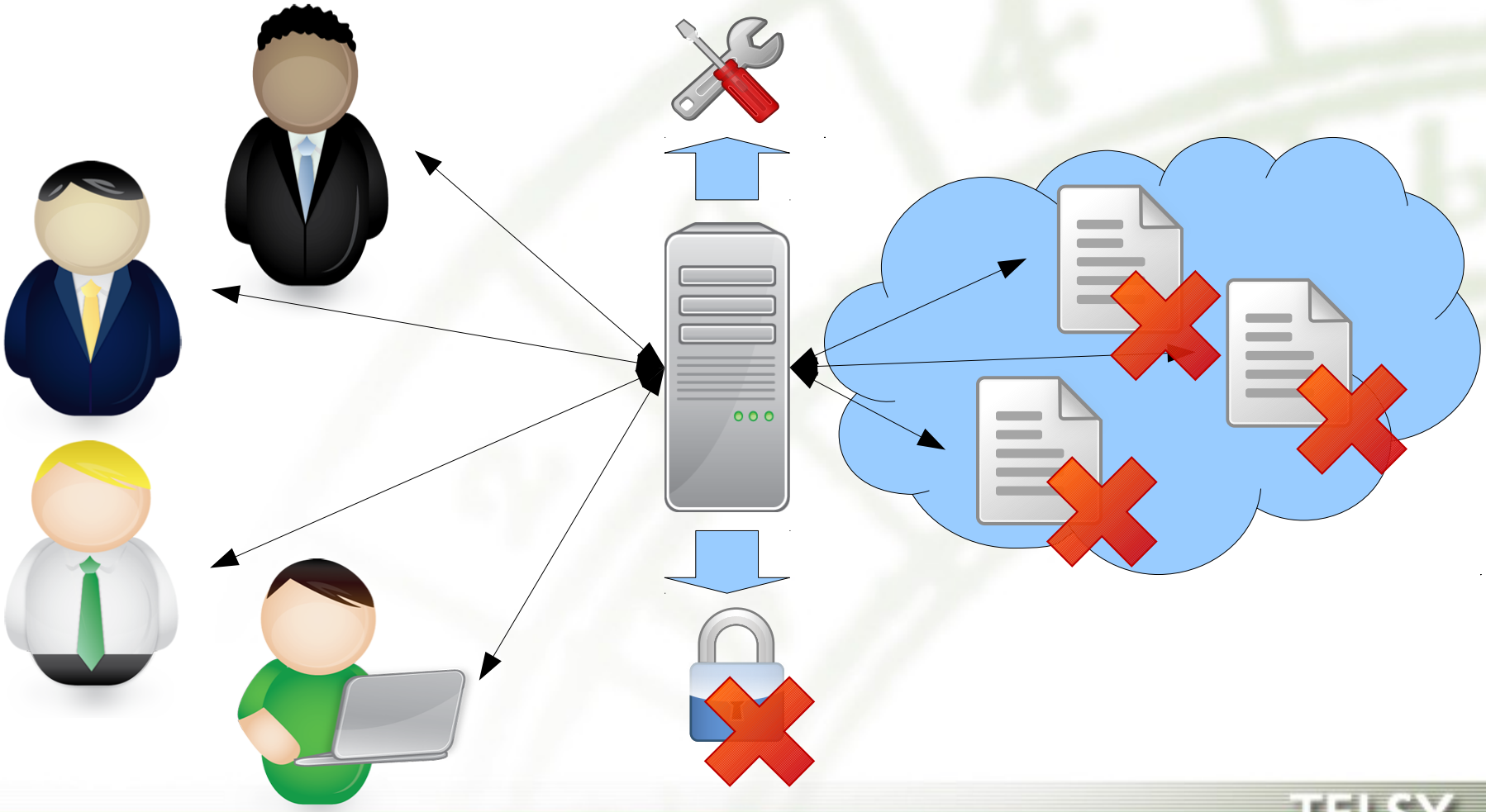
  Liu, Cao, Wong - “Fully Collusion-Resistant Traceable Key-Policy Attribute-Based Encryption with Sub-linear Size Ciphertexts

- ✓ 2015 – Anonymous ABE

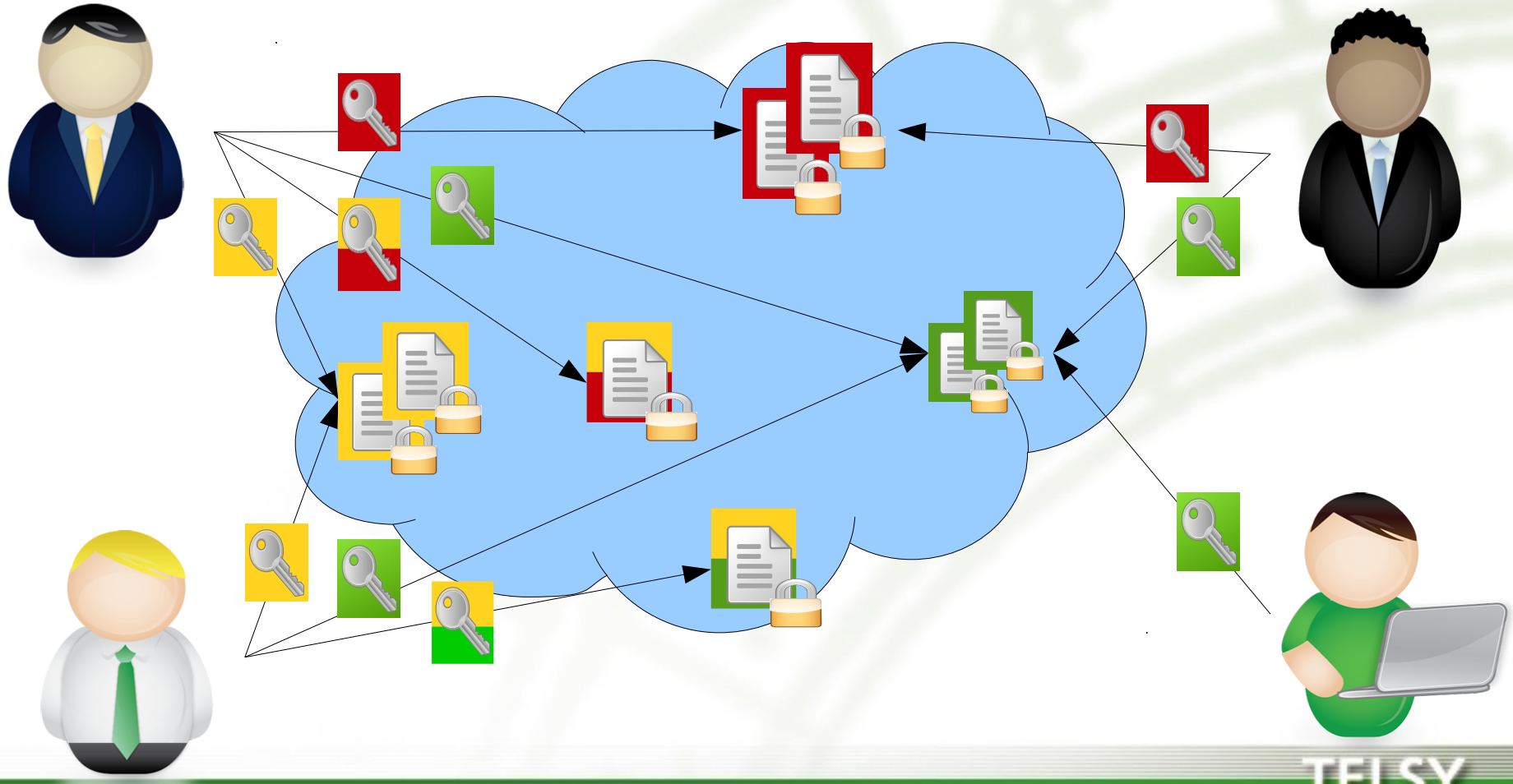
  Taeho, Xiang-Yang, Zhiguo, Meng - “Control Cloud Data Access Privilege and Anonymity With Fully Anonymous ABE”

- ✓ ...

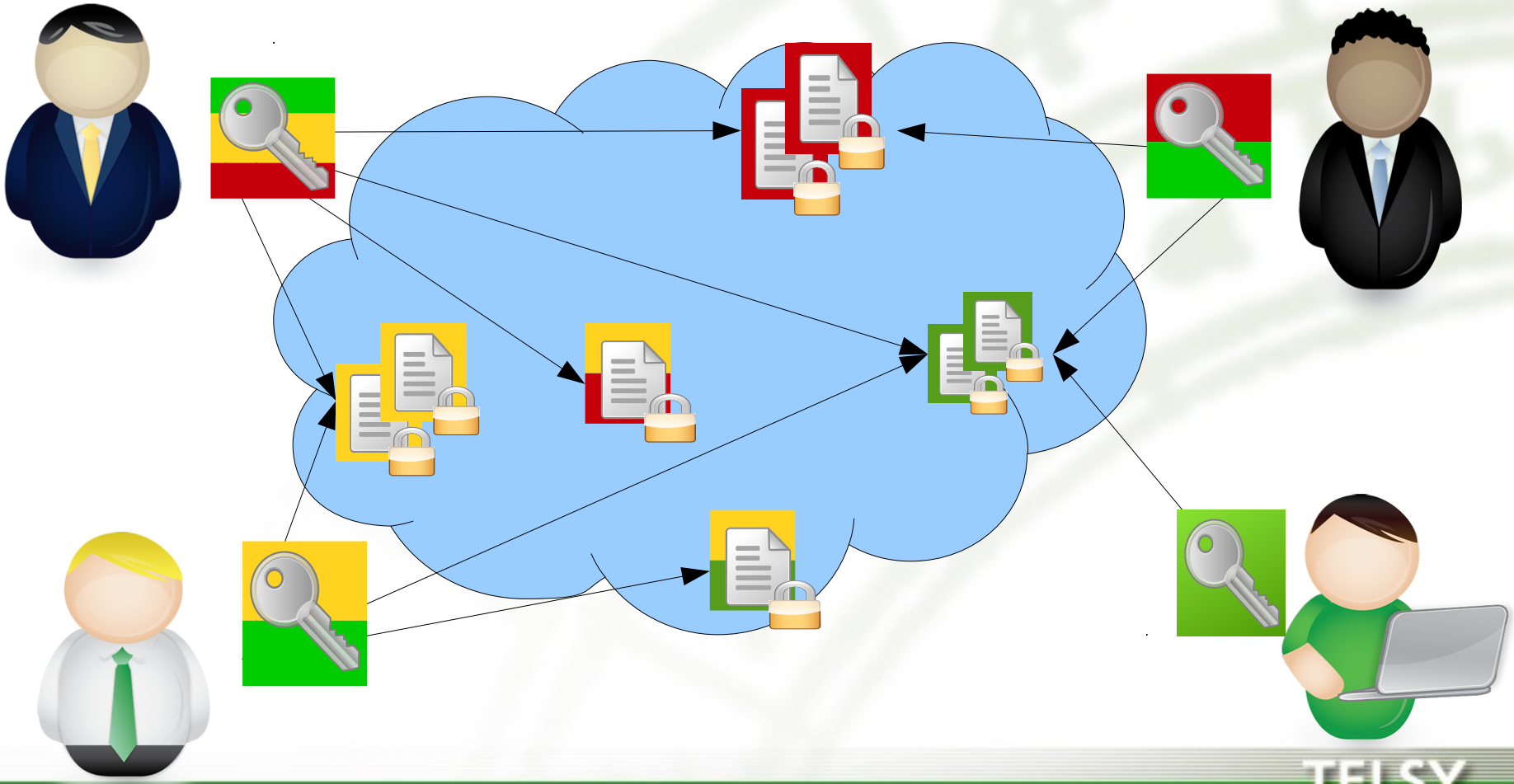
Access Control: Trusted Server



Access Control: Standard Encryption

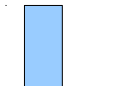


Access Control: Attribute-Based Encryption



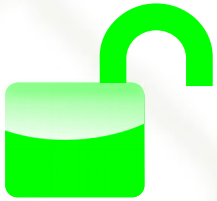
ABE: Characters

AUTHORITY



MASTER KEY

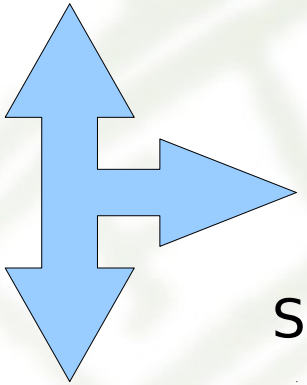
Sender



PUBLIC KEY

Receivers

Group 1
SECRET KEY



Group 2
SECRET KEY

Group 3
SECRET KEY

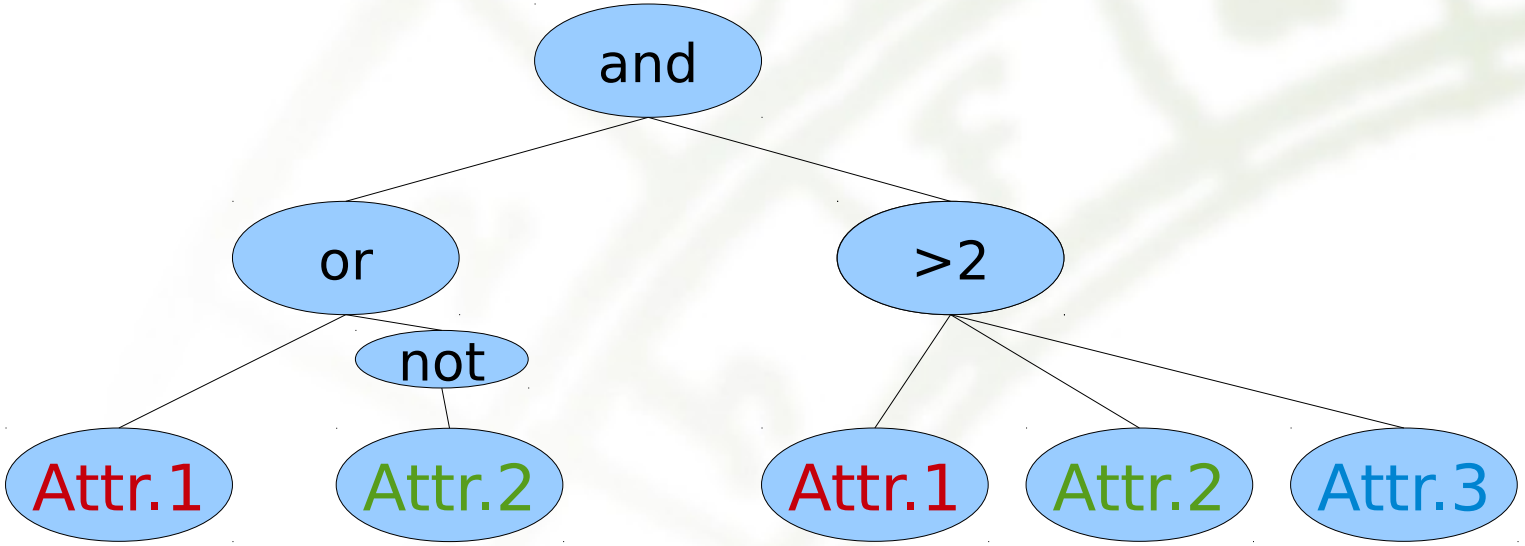
ABE: Attributes

2 Types:

- ✓ Data description (**KEY-POLICY**)
- ✓ User description (**CIPHERTEXT-POLICY**)

ABE: Policy

Can be seen as a tree graph with **and, or, not, threshold** gates



ABE: Performance example

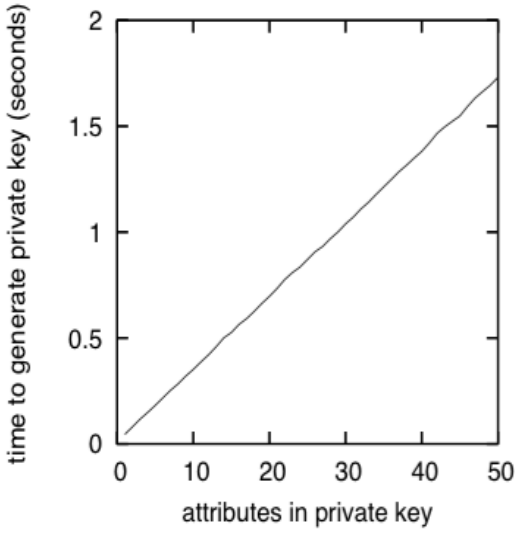
	6 Attributes	20 Attributes
KeyGen	~0.19 ms	~0.50 ms
Encryption	~0.70 ms	~2.10 ms
Decryption	~1.35 ms	~3.76 ms

126-bit Security Level Elliptic Curve, CP-ABE scheme

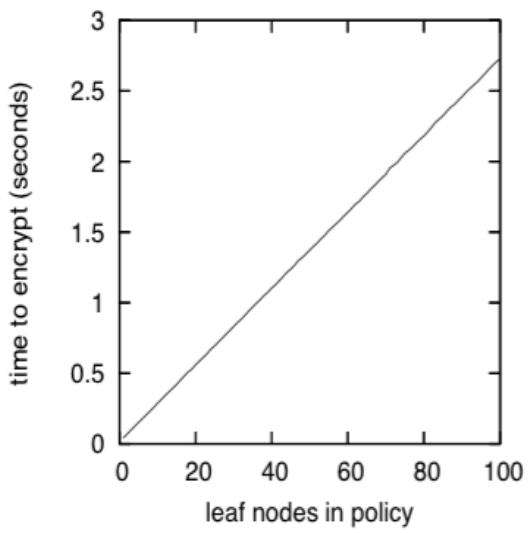
Intel Core i7 4770 @3.4GHz

From: http://sandia.cs.cinvestav.mx/Site/CPABE

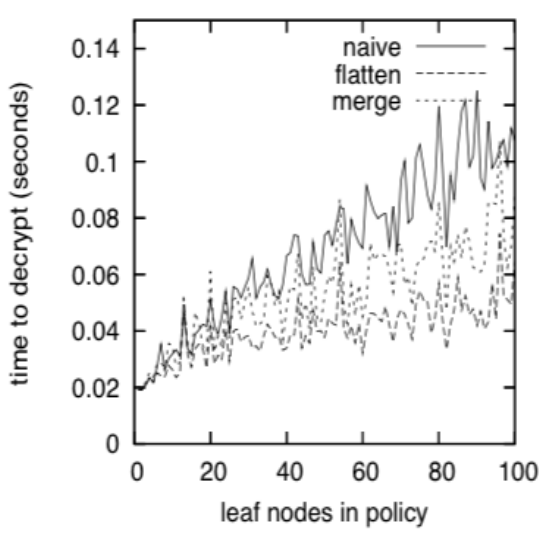
ABE: Performance example



(a) Key generation time.



(b) Encryption time.



(c) Decryption time with various levels of optimization.

Pentium 4 @3.2 GHz

ABE: mathematics

Pairings:

$$e(g^a,g^b) = e(g,g)^{ab}$$

Pairing-Based Cryptography:

- ✓ Elliptic curves (no Diffie-Hellman curves)
- ✓ Lattices
- ✓ Quadratic residues

Searchable Encryption

Searchable encryption

By searchable encryption we do not mean *search over data* (e.g. words inside an email or a file), but we mean an **indexed-based search**.

Searchable encryption

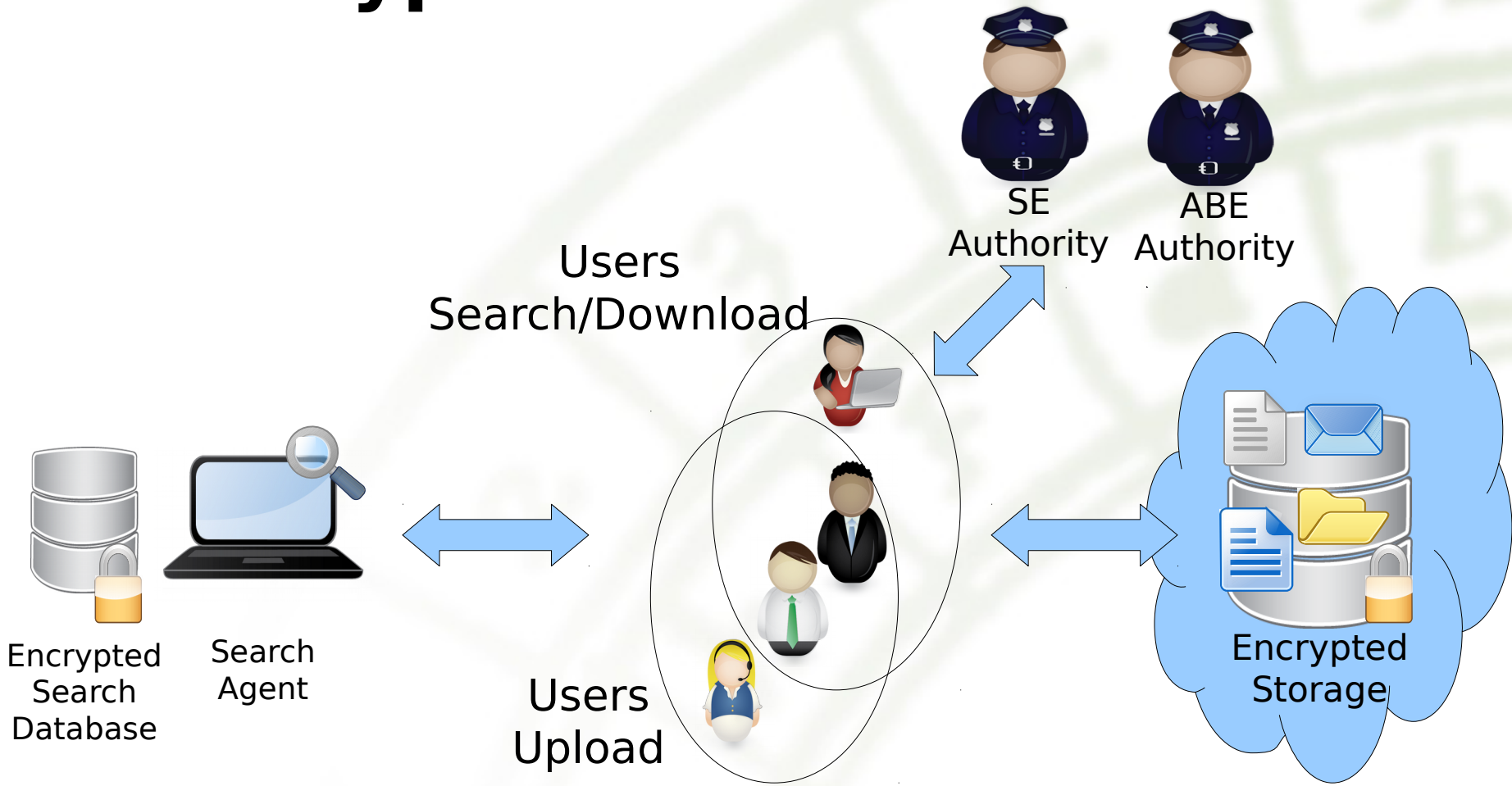
	EXAMPLE	LEAKS	EFFICIENCY	SECURITY	USE
Property-Preserving Encryption	Equality PE (Det.Encr./Token)	EDB and EDB+Token reveals: - access pattern - search pattern	Sublinear in number of docs	- Frequency analisys (FA) - Repeated search (RS) - Dictionary attack (DA), only if public key is used	- high minentropy data - not for mail, text, personal info
	Order PE				
	Orthogonality PE				
Functional Encryption	Anonymous IBE	- access pattern - search pattern	Linear in number of docs	- No FA - RS, DA	Hard to gues search terms
Oblivious RAM	FHE	No leaks	Very inefficient	No FA, RS, DA, ...	Not practical
	Symmetric Encryption Scheme		- Many communications - Reads blocks of memory instead of single encrypted keywords		“Small to medium” dataset
Searchable Symmetric Encryption	- Interactive/ Non-interactive - Response Hiding/Revealing	- search pattern - minimal controlled leakage	Sublinear + Linear Pre-Processing	- No FA	- real dataset

Telsy Prototype

Prototype

The prototype is part of a research project co-funded by the *Italian Ministry of Defence* in the context of the *National Plan for Military Research*

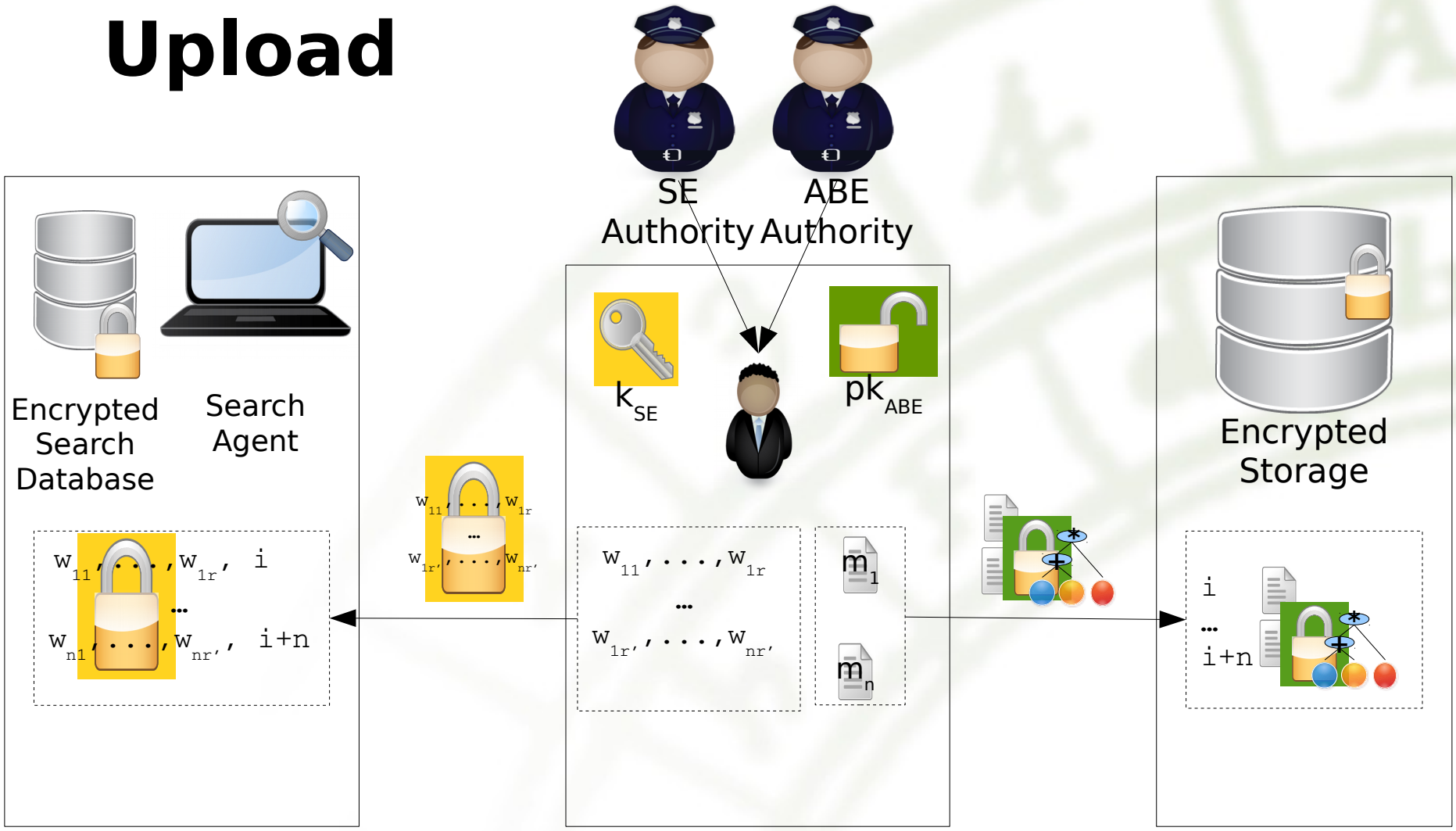
Prototype architecture



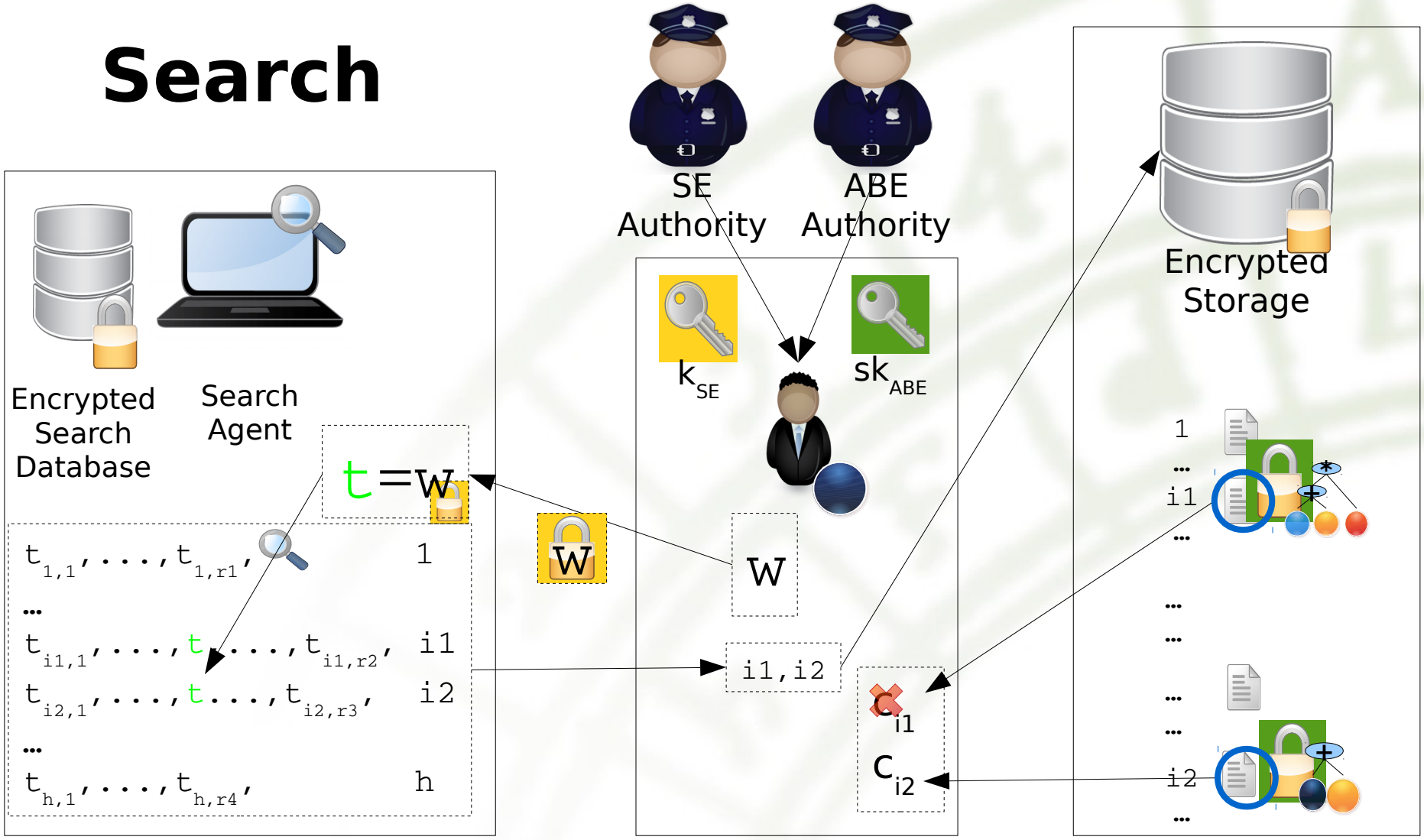
Pre-requisites

- ✓ We want to keep the search and storage servers independent
  - They do not communicate
  - Storage server can be a commercial one and easily replaced
- ✓ It should be possible to manage keys for search and keys for storage separately
- ✓ Access control must be implemented at a cryptographic level in order to have all ciphertext on the same place

Upload


SE Authority
ABE Authority
k_{SE}
pk_{ABE}
Encrypted Search Database
Search Agent
Encrypted Storage
$w_{11}, \ldots, w_{1r}$, i
$w_{n1}, \ldots, w_{nr'}$, i+n
$w_{11}, \ldots, w_{1r}$
$w_{1r'}, \ldots, w_{nr'}$
m_1
m_n
i
i+n

Search


SE Authority
ABE Authority
Encrypted Storage
Encrypted Search Database
Search Agent
t=w
k_SE
sk_ABE
w
w
i1,i2
c_i1
c_i2
1
i1
i2
t_1,1,...,t_1,r1, 1
t_i1,1,...,t...,t_i1,r2, i1
t_i2,1,...,t...,t_i2,r3, i2
t_h,1,...,t_h,r4, h

...thanks for the attention!