how Alice can protect her data a cryptographic approach

30 juin 2015
SEC2 2015

Sébastien Canard

let me introduce you Alice…

she has a smartphone

she works for a small company

she likes using new technologies… but not at any price

cloud computing

- in France(**)
  - 29% of companies use cloud computing
  - 5000 M€ in 2014 (+100% in 2 years)
- IaaS, PaaS, SaaS services
- storage and/or compute

can Alice make use these services in trust?

(**)source http://www.cloudindex.fr/

confidentiality of her companies' data

to protect and preserve the **confidentiality** of information means to ensure that it is **not made available** or disclosed to **unauthorized** entities

cloud services need to manipulate sensitive data

- **administrative documents**
- **sensitive data related to competitiveness**

what a cloud service provider can do to give confidence?

- **do they have access to the data…**
- **…while ensuring a good and appropriate service?**

protection of her privacy

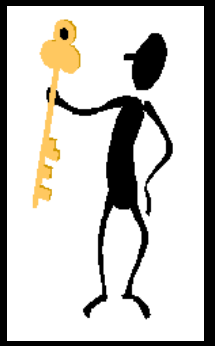
in France, cloud services should work in accordance to the “loi informatique et liberté”

- transparency of the data gathering
- use of the data should be clear
- relevant data gathering
- data precision
- right to oblivion

what a cloud service provider can do to give confidence?

- provide solutions to protect the privacy of customers
- how to protect the privacy of customers…
- … while offering them the best possible service?
- what about privacy w.r.t. these providers?

can cryptography be useful?



historical objectives

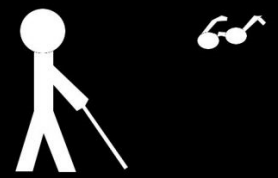
- confidentiality
- (data) authentication
- integrity
- non repudiation

new objectives

- provide tools to obtain conflicting properties
- including data protection

computations on encrypted data?

the concept of blind storage



data **storage**

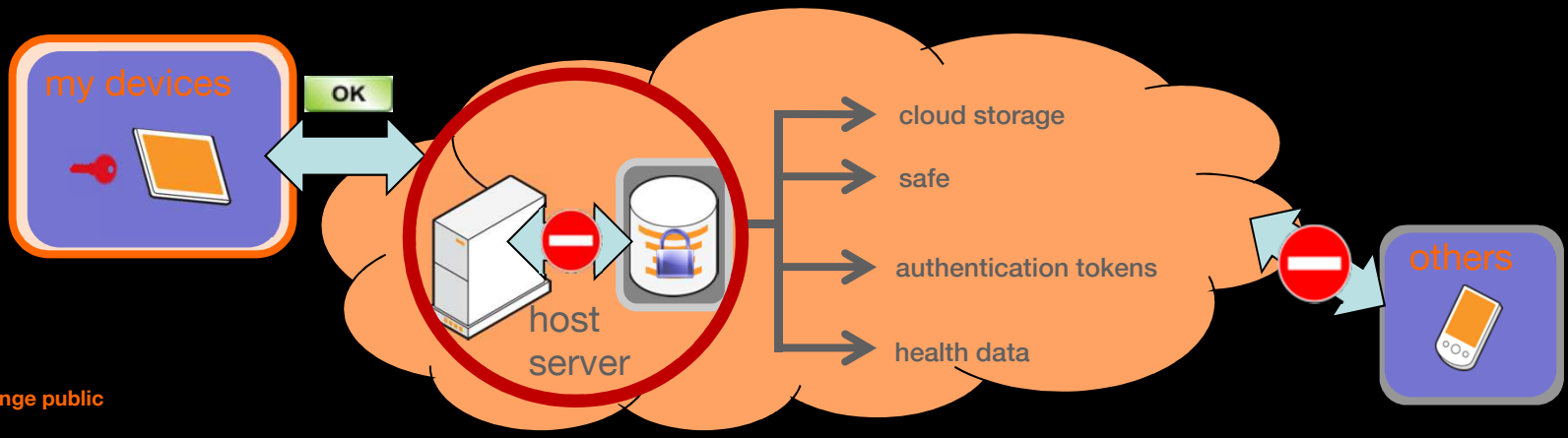
sensitive documents, administrative documents

personal data, …

confidentiality of data ⇒ encryption of the data

the host server CANNOT obtain the data in clear

it stores the data « in blind »



but what if Alice needs services on her data?

share of data,

between devices, people/collaborators

with the administration

in a hierarchical structure

inside a group

word indexation,

to make a search on documents related to a keyword

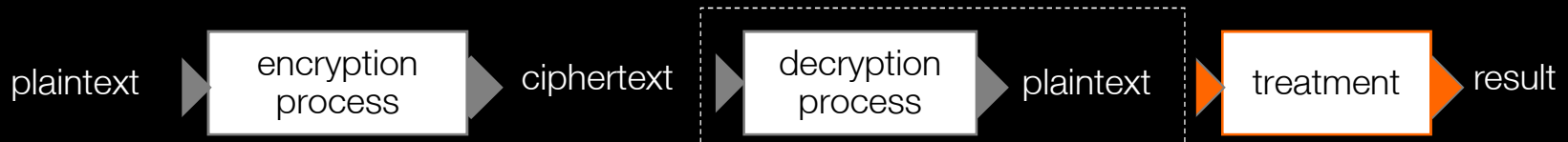
or more complicated computations

spam filtering, targeted advertising and pricing, medical applications, private “Google” search, code compiling, …

we need encryption schemes with new features

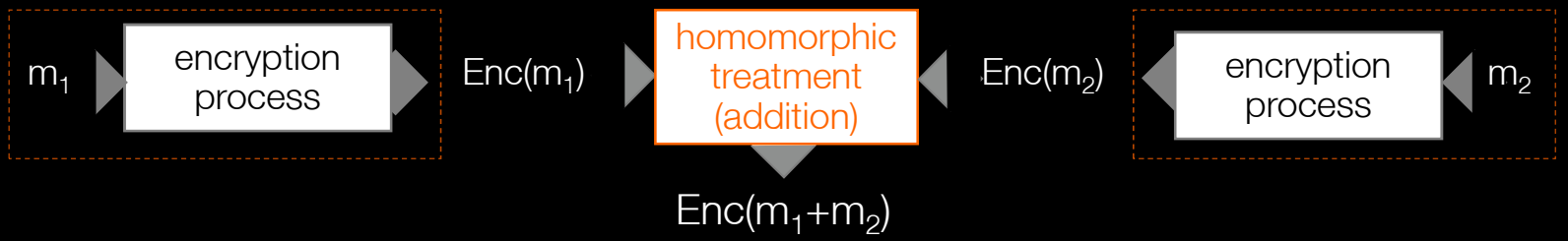
operations on encrypted data

conventional encryption



what if the treatment could not be performed by the same entity?
the latter obtains the information in clear

(fully) homomorphic encryption allows to perform computations on plaintexts while manipulating only the corresponding ciphertexts



example: addition of encrypted data without ever decrypting them!

any kind of treatment

addition ⇒ **secret ballot elections**

means / statistics ⇒ **medical applications**

word search ⇒ **spam filtering , private Google search**

greater than ⇒ **sealed-bid auctions**

comparison ⇒ **private database queries**

code compiling ⇒ **cloud computing**

current homomorphic encryption schemes support either addition or multiplication but not both!

fully homomorphic encryption schemes can handle both operations on encrypted data and thus perform **arbitrary computations.**

can (fully) homomorphic encryption be practical?

(*)source Coron et al., Eurocrypt 2012

security parameter	public key size	multiplication	bootstrapping
52 bits	1692 KB	0.59 sec	100 sec
62 bits	7.9 MB	9.1 sec	30 min
72 bits	18 MB	41 sec	2 h 30 min

partially homomorphic encryption (in comparison)

- **supports only addition (Paillier) or multiplication (ElGamal)**
- **size of the public key: less than 1 kb**
- **time for a treatment : some ms**

128 bits of security

in practice, do we really need fully homomorphism?

how to improve the efficiency

parameters of the scheme can depend on the evaluated circuit's depth

- notion of leveled FHE
- no more need to use a bootstrapping

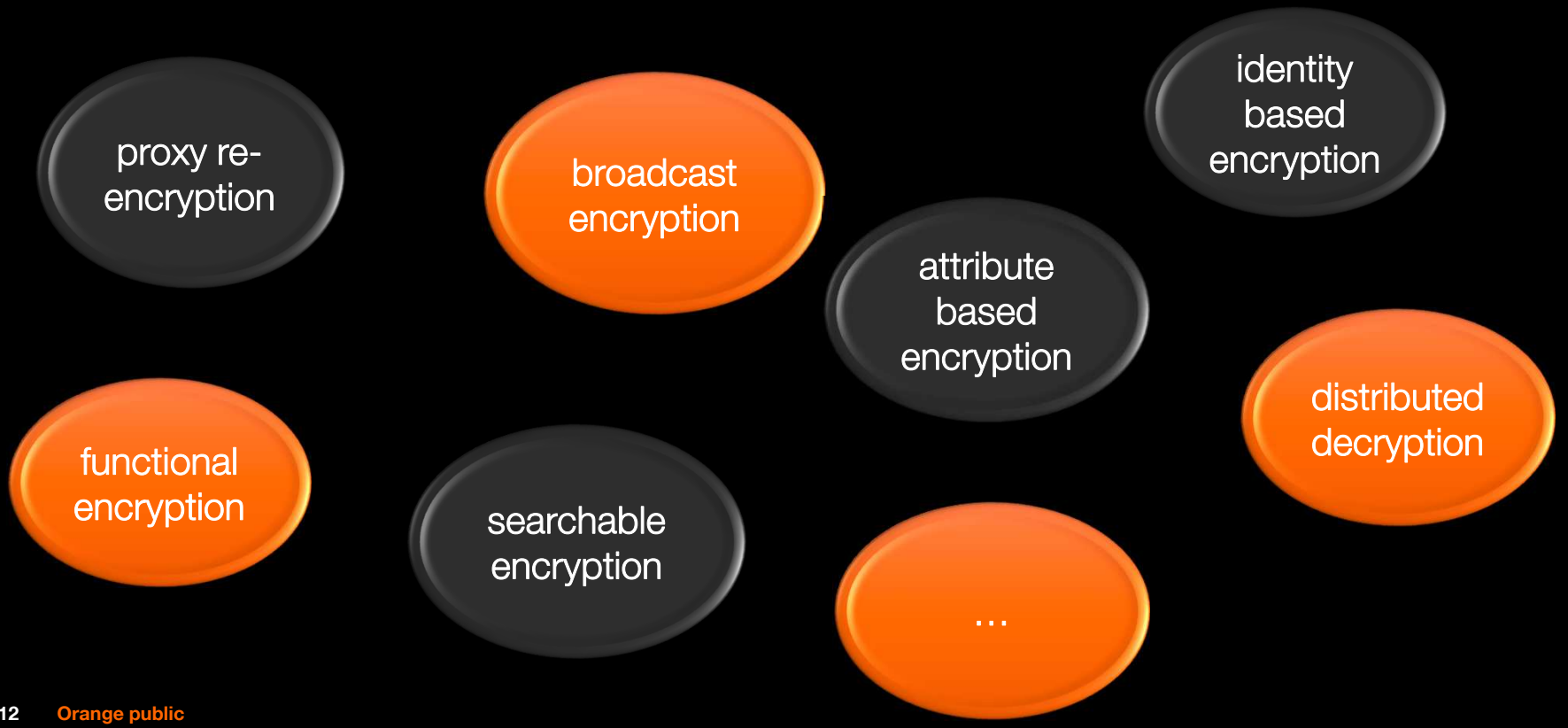
best implementations necessitates nearly 1 sec for a 128 bits security level(*)

but loss of generality

- need to know a priori an upper bound of the circuit depth

(*)source HELib

can we do even better?



possible solutions to share data

SHARE OF THE KEY

- security hole if key compromising
- such compromising necessitates a key update for all authorized devices

DUPLICATION OF FILES

- good security, less flexibility
- a lot of keys to manage
- additional work when withdrawing an access right

vs.

PROXY RE-ENCRYPTION

- + lost of a device
- + fine-grained rights

- best alliance of security and flexibility

concept of proxy re-encryption

based on a public key encryption system

- a public key to encrypt data
- a private key to decrypt data

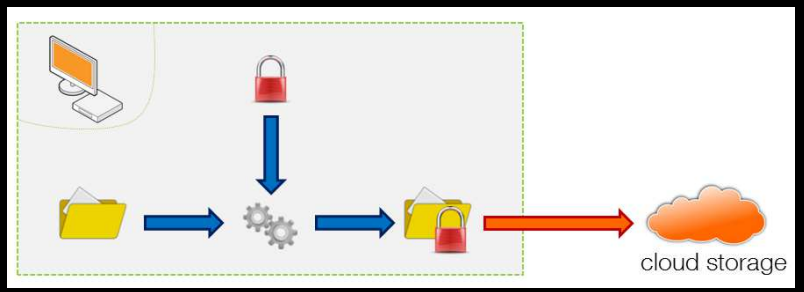
additional role (a blind storage back-end)

- transform a message encrypted for Alice into a message encrypted for Bob
  - if Alice agrees
  - without obtaining any knowledge on Alice and Bob's keys
  - without obtaining any knowledge of the encrypted message
- for this purpose, manage a particular cryptographic re-encryption key

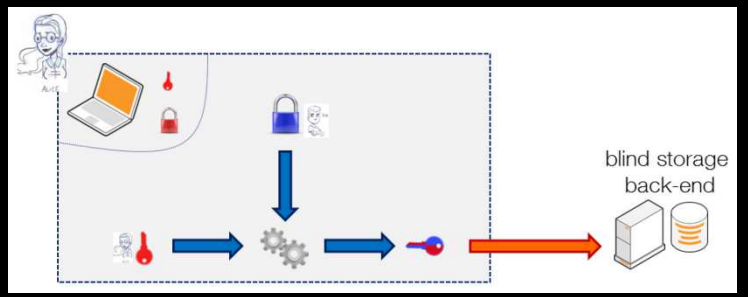
we encrypt an data specific secret key to manage big files

main steps

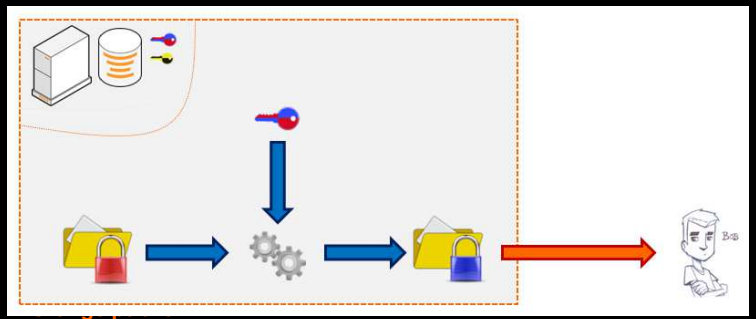
upload/encrypt



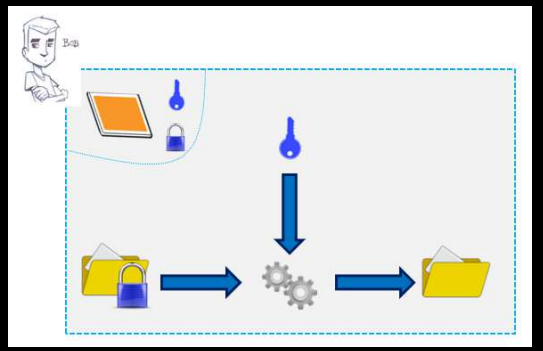
share



download/re-encrypt



download/decrypt



expected security

the decryption key is not shared between several devices

the data is not duplicated on servers

the owner is contacted only once for the creation of the re-encryption keys

the cloud storage provider is not trust

no need to know a priori the persons with which you will share data

each device owns a key pair

- the private key never goes outside the device

the data is never sent outside a device in a non-encrypted form

some possible additional features

multi-device setting

- share with a group of devices
- share with other users

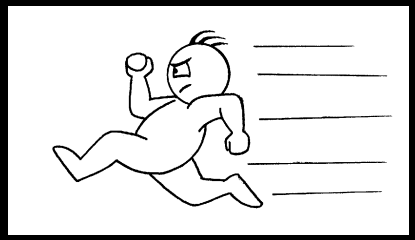
fine grain management of the rights

- to manage files and folders

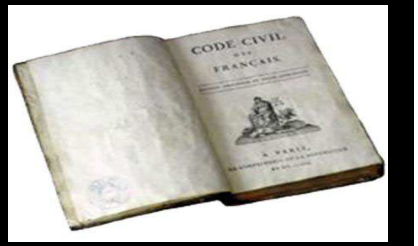
possibility to share a document with a group

what about a practical implementation?

- performances: 10% loss w.r.t. no encryption
- about 10 ms for encryption/decryption in a modern smartphone



legal aspects



the case of a digital safe from the CNIL point of view

- the service provide should not have access to the data

obligation to give the data if requested by legal authorities

it seems contradictory

- but cryptography can help
- possibility to share a “file opening” with authorities
- no unique actor can obtain the data in clear

conclusion

the way to **efficiently** protect the sensitive and personal data of Alice in cloud computing is now **a reality**

cryptography can help

- adaptive solutions
- efficient implementations
- big companies are working (IBM, Microsoft, Orange, …)

the professional world seems more ready

- but they do not want to lose their useful services

we need to show how powerful cryptography is…

thank you