PRIVACY IN CRYPTOGRAPHIC PROTOCOLS

HIEU PHAN (TELECOM PARIS)

Security of Data

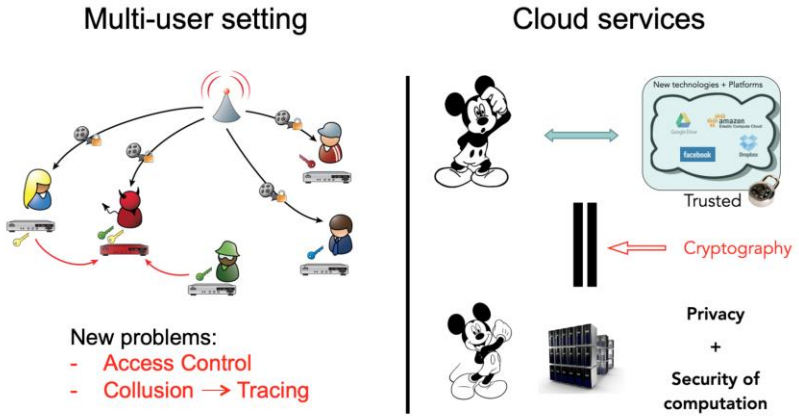
- Integrity with hash function
- Confidentiality with encryption
- Authenticity with MAC, signature
- Identification with zero-knowledge proof

New Technologies → Advanced cryptographic primitives

- Big Data, Cloud Computing → widespread real-life applications
- Privacy: protect personal information.
  - Security
  - Trust on Authorities

→ **Security of Computation on Untrusted Machine.**

CONTEXT: NEW TECHNOLOGIES AND PLATFORMS



Achieving Privacy:

1. Decentralized Cryptography / Efficient Multi-party Computation
2. Computing on untrusted servers
3. Critical scenarios: in a dictatorship

Some Previous Results

- Public Traceability in Broadcast Encryption
  - based on pairings **[EUROCRYPT '05]**
  - based on lattices **[CRYPTO '14, ACM CCS '17]**
- Delegated PSI and applications in Contact Tracing **[ASIACRYPT '20]**

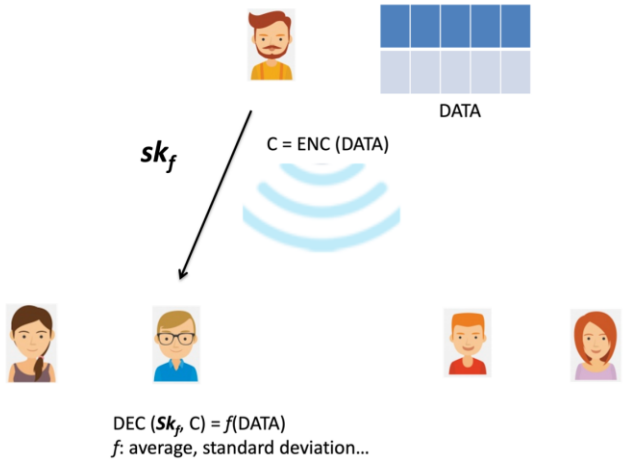
Vaudenay20: "centralized systems put the anonymity of all users in high danger while decentralized systems put the anonymity of diagnosed people in high danger against anyone."

$\rightarrow$ a third category that combines the best of both worlds.

Ongoing project

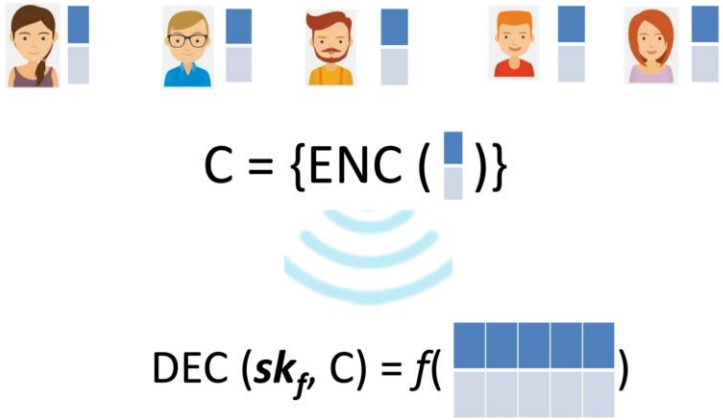
Decentralized Functional Encryption

FUNCTIONAL ENCRYPTION



In practice: number of functions is quite limited
→ centralized version has limited interest.

DECENTRALIZED FUNCTIONAL ENCRYPTION



- Decentralized Functional Encryption for linear functions **[ASIACRYPT '18, CRYPTO '20]**
- Challenge: more general functions and on fuzzy data (great interest to a large number of related areas such as biometric identification, privacy in machine learning.)

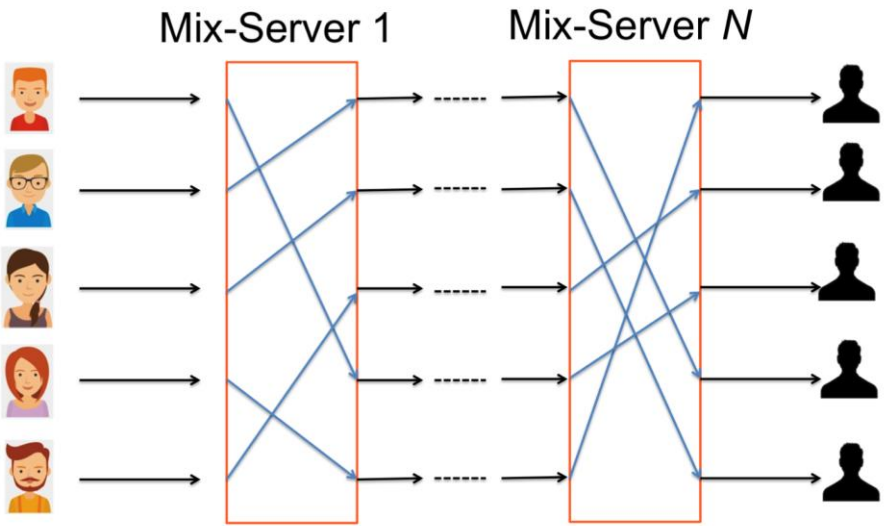
COMPUTING ON UNTRUSTED SERVERS

CONTEXT: ELECTRONIC VOTING

Decentralisation is not always possible

→ **security of computations on untrusted servers**

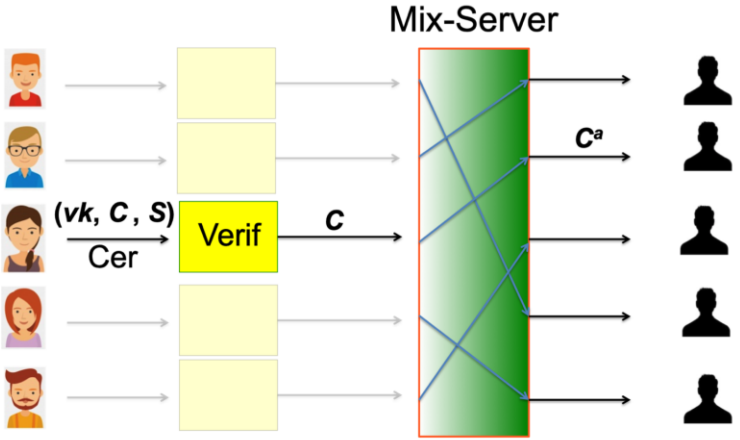
Typical Exemple: Electronic Voting.



Institut Mines-Télécom

COMPUTING ON UNTRUSTED SERVERS

CONTEXT: ELECTRONIC VOTING



User:
- given **Cer**: the right to vote
- encrypt the vote ➔ ***C***
- sign on ***C*** ➔ ***S***
- signature ***S*** is verifiable with ***vk***

Classical Shuffling: Re-encryption + Permutation

1. Re-encrypt $C \rightarrow C^a$: C^a and C are unlinkable
2. The input and output contain the same ballots
   $\rightarrow$ **Zero-knowledge Proof (ZKP) of a global permutation**

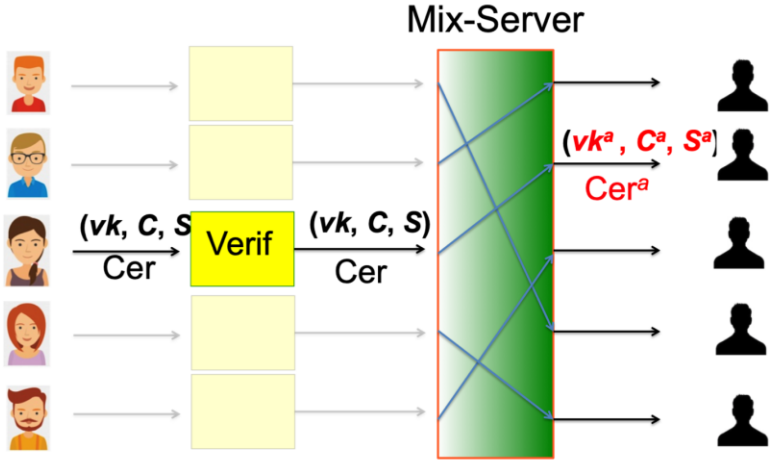
ELECTRONIC VOTING IN PRACTICE

Les scrutins des élections professionnelles sont clos depuis le 6 décembre 2018, à 17 heures, heure de Paris. Consultez les résultats.

1 023 211 électeurs relevant de l'éducation nationale étaient appelés à désigner leurs représentants au comité technique ministériel de l'éducation nationale. 436 321 suffrages ont été exprimés soit une participation de 42,64 %. Le taux de participation est en hausse de 0,91 point par rapport à 2014 (41,73 %).

COMPUTING ON UNTRUSTED SERVERS

ELECTRONIC VOTING: AVOIDING ZKP OF A GLOBAL PERMUTATION [PKC20]



Mix-Server can do randomization
- S^a is a valid signature of C^a, under vk^a
- Cer^a is a valid certification

Mix-Server cannot forge a signature on a new message

1. Each output ballot corresponds uniquely to one input ballot
2. One cannot link (vk^a, C^a, S^a, Cer^a) to (vk, C, S, Cer)

Tool: Linearly Homomorphic Signature

Anamorphic Encryption:
Private Communication against a Dictator

Giuseppe Persiano*, Duong Hieu Phan**, and Moti Yung***

(To appear in EUROCRYPT 2022)

Democrypt - Cryptography for Democracy:
Allowing Free Petitions In Dictatorships
(Preliminary version)

Duong Hieu Phan* and Moti Yung**

(To appear in ePrint)

Focus on Privacy:

- Decentralization
- Practical MPC
- Post-quantum Security