Searching Engine on Encrypted Data

Massimo Bertaccini I CEO

My concept of SECURITY


My concept of Privacy

The Problem

If the data are **Encrypted** how can I **search** for the informations **without decrypt** the files?

If the data remain unencrypted at least the Cloud Provider can spy inside my files!

How can be possible to search inside the files without decrypt them?

Encryption on the Cloud

The Solution

Cryptolab

Searching Engine for security and privacy

CSE provides to **search inside the encrypted data** independently by the algorithm used to store them. It allows storing sensitive files on the Cloud with a complete key management solution for each client with a **Total zero knowledge (only the client detect the encryption keyes)**.

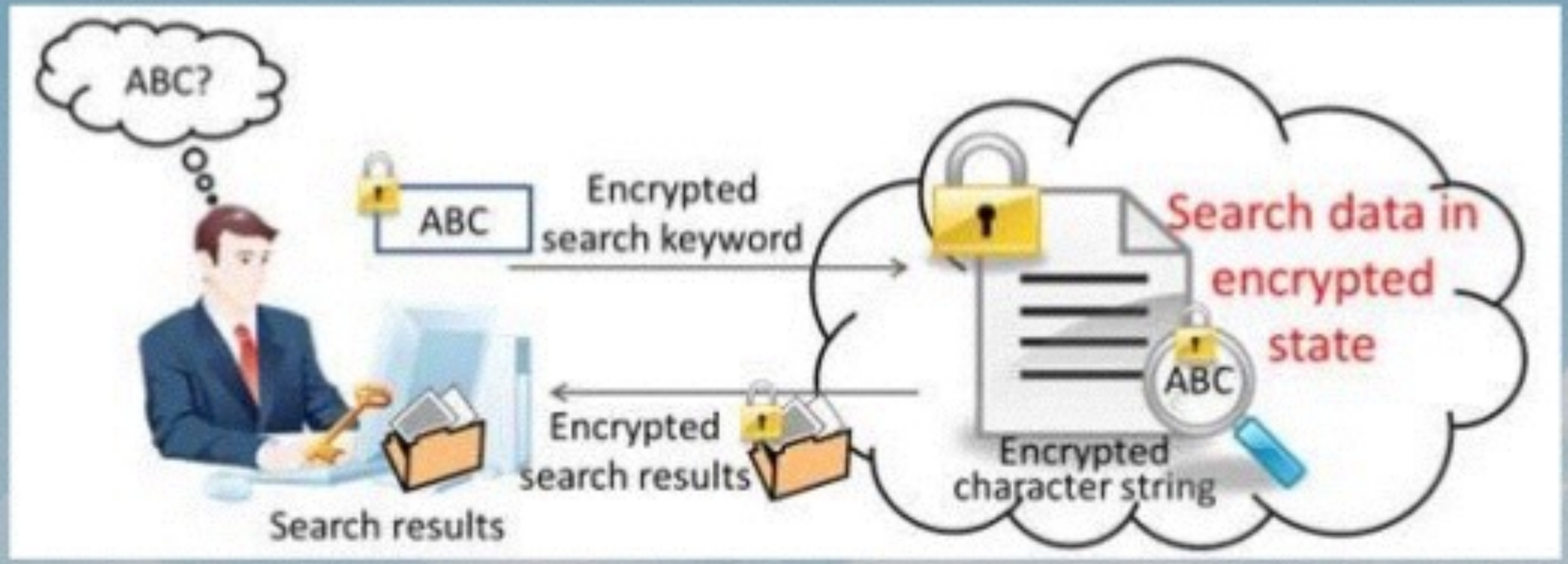
No decryption and better performances

No decryption is necessary to manage and search data in the cloud, thus eliminating unauthorized access and risk of exposure. The performances of CSE are **about 0.35 Sec/Searching** semi-independently by the amount of bit and the number of files stored.

Analytics on encrypted data

CSE enables analytics on encrypted data preserving the customer's privacy (HIPAA compatible) for Health Information Privacy.

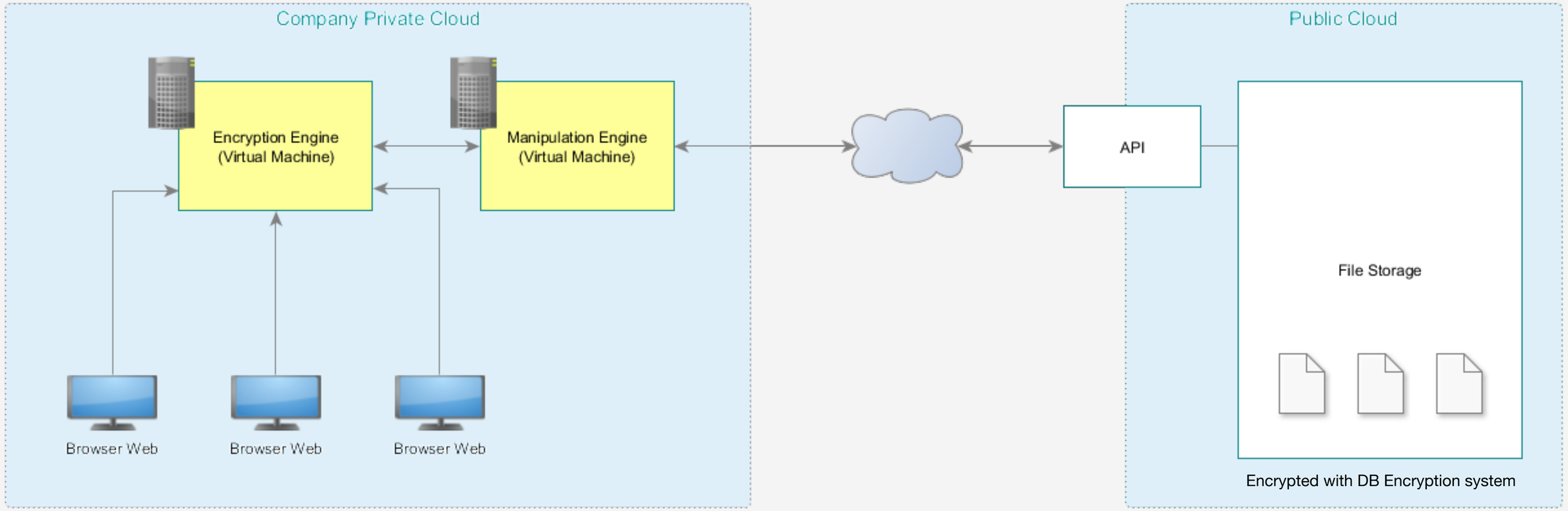
Homomorphic Encryption



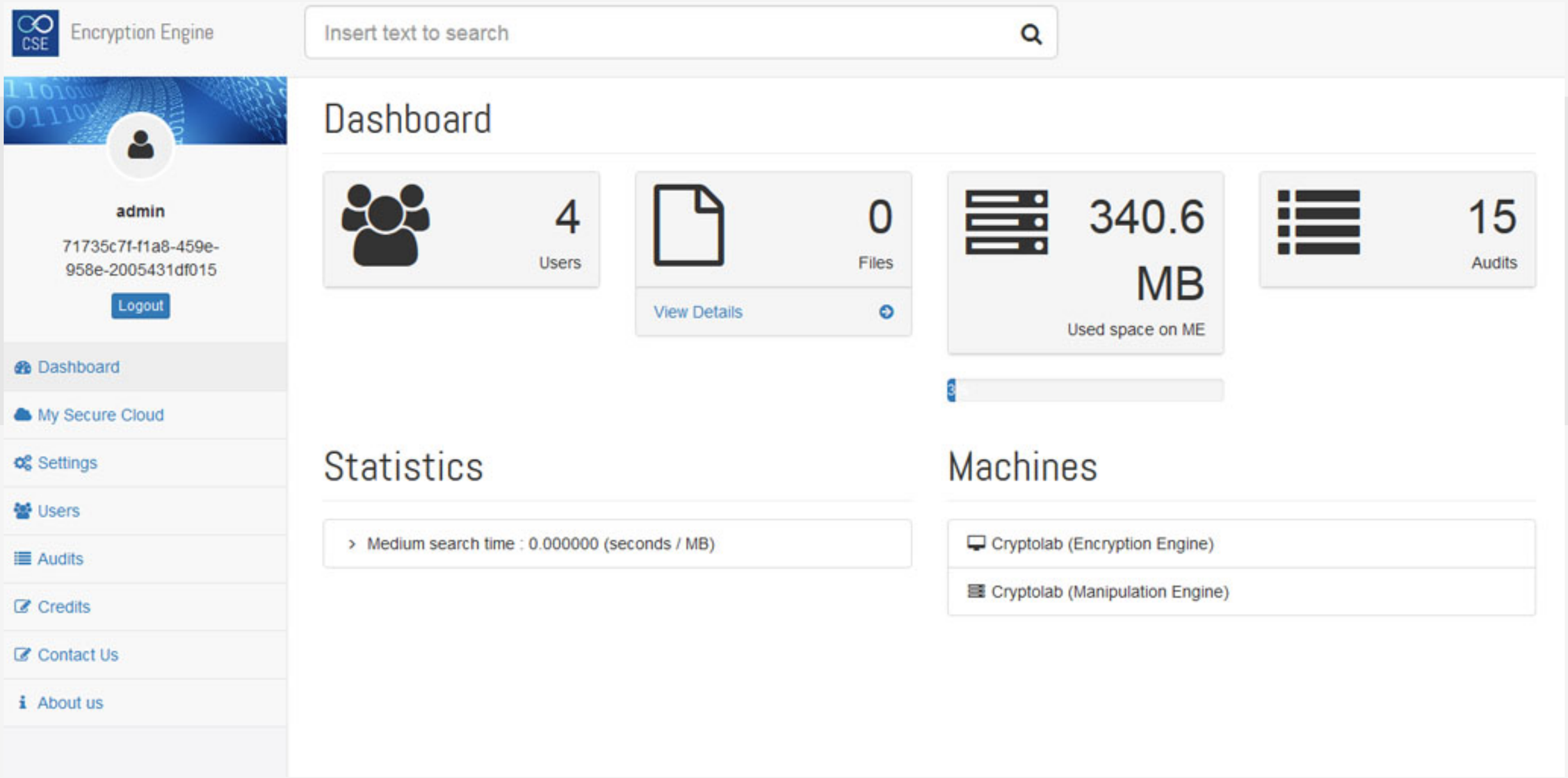
Party A **Party B**

Party B does NOT requires the secret key for answering this query from A

Technical architecture and integration



CSE Screenshot



C.S.E.

cloud searching encryption

HEALTH CARE

ENVIRONMENT SUIRVEILLANCE

BIOMETRICS

COUNTERTERRORISM SOLUTIONS

ANTI RANSOMWARE

BITCOIN CRYPTOCURRENCY

C.S.E.

crypto searching engine

CRYPTO
MAP

CRYPTO
CONNECTED VEHICLES

CRYPTO
CARE

Next Steps

-Implementing a scan for Anti-Ransomware

- Implementing file sharing

- Bettering the API and some functions

- Adding a Master Key for Anti-Wannacry

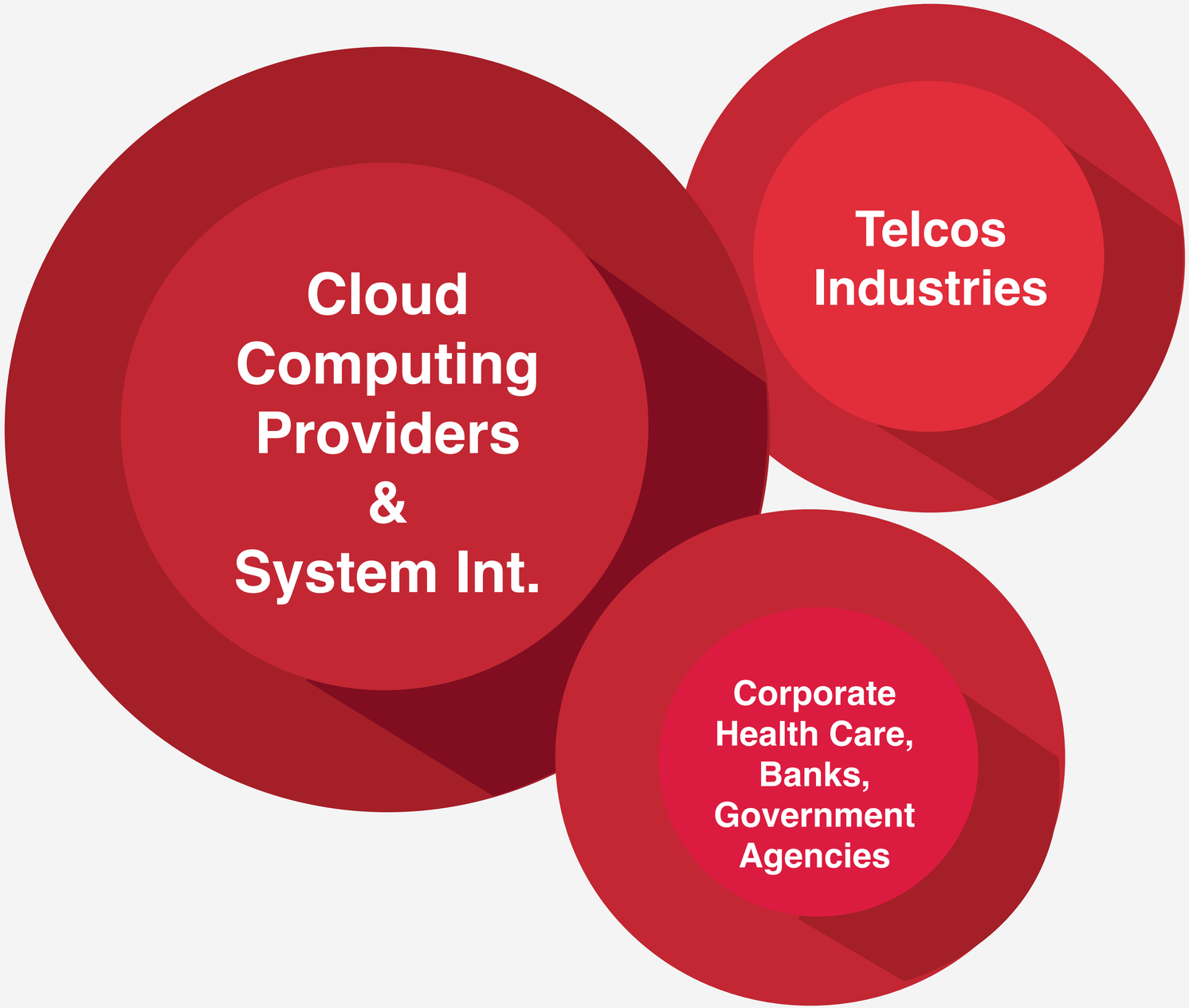
--?

Dissemination and Distributors :

- Cloud Providers
- System Integrators
- Government and Public Admin
- Health Care
- Insurance Co.

Business Model

B2B Model in the beginning
B2C after the dissemination



The team

Cryptolab

Massimo Bertaccini

Inventor and Co-Founder

Areas of expertise:
Mathematical cryptography

Tiziana Landi

SW Engineer

Areas of expertise:
Software design and development

Alessandro Passerini

Technical Architecture

Areas of expertise:
Software design and development

Marco Massari

Technical Support

Areas of expertise:
System Administrator (Windows , Linux)

Fabio Carati

ADVISOR

Areas of expertise:
Business, Strategy, advanced Technologies

Oana Calugar

ADVISOR

Areas of expertise:
Business, Finance

Patents and Know How

- MB 09 : Encryption System based on Public/Private Keys
- MB 11: Encryption System based on Public/Private Keys with Digital Signatures
- Z/K 13 : Zero knowledge Protocol used in CSE for VM Authentication
- Compression Algorithm : for transmission of very large keys
- MB23: Fully Homomorphic Encryption System (used in CSE as ME)
- CRYPTOON: Platform written in C++
- Anti-Ransomware (RSA)

Cryptolab US Office
2040 Martin Ave
Santa Clara CA 95050, USA
+1 415 7126269
m.bertaccini@cryptolab.us

Cryptolab ITA Office
Via Livia Venturini 15M
48026 Imola ITA
m.bertaccini@cryptolab.it

www.cryptolab.us