UNIVERSITÀ POLITECNICA DELLE MARCHE

DII
Dipartimento di Ingegneria dell'Informazione

unimc

HE-PA: Homomorphic Encryption per la PA.
A post-quantum, Privacy-by-Design and Privacy-by-Default prototype for digital services

Leonardo Guardati
univpm@guardati.it

Martedì 19 Luglio 2022

Corso di Perfezionamento in Cybersecurity, Cyber Risk and Data Protection

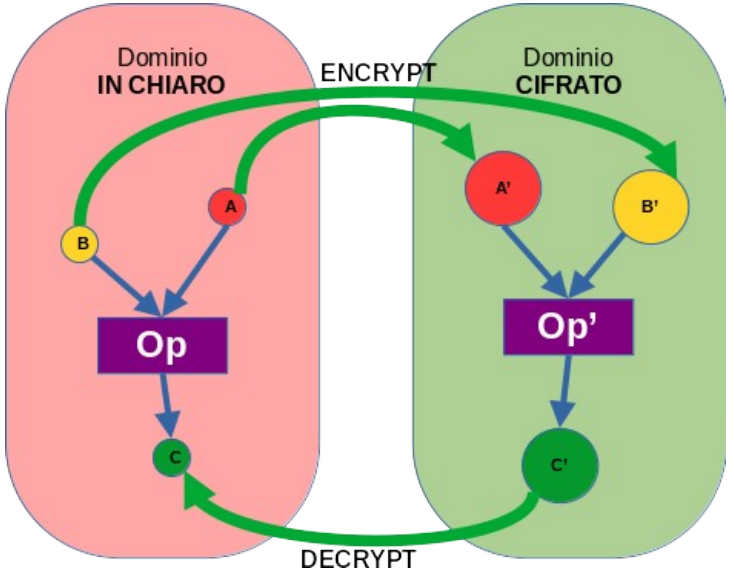
HE-PA: Homomorphic Encryption per la PA

1. Homomorphic Encryption (HE)
2. Applicazioni dell’HE
3. HE-PA: Prototipo di servizio digitale
4. HE-PA: Architettura e componenti
5. HE-PA: Demo
6. Risultati e sviluppi possibili

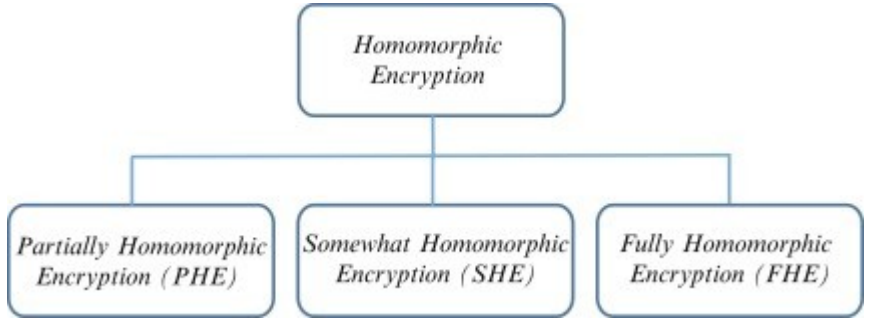
1. Homomorphic Encryption (HE)

1. Homomorphic Encryption (HE)

Tipologia di cifratura che consente di eseguire operazioni sui dati cifrati senza necessità di decifrarli

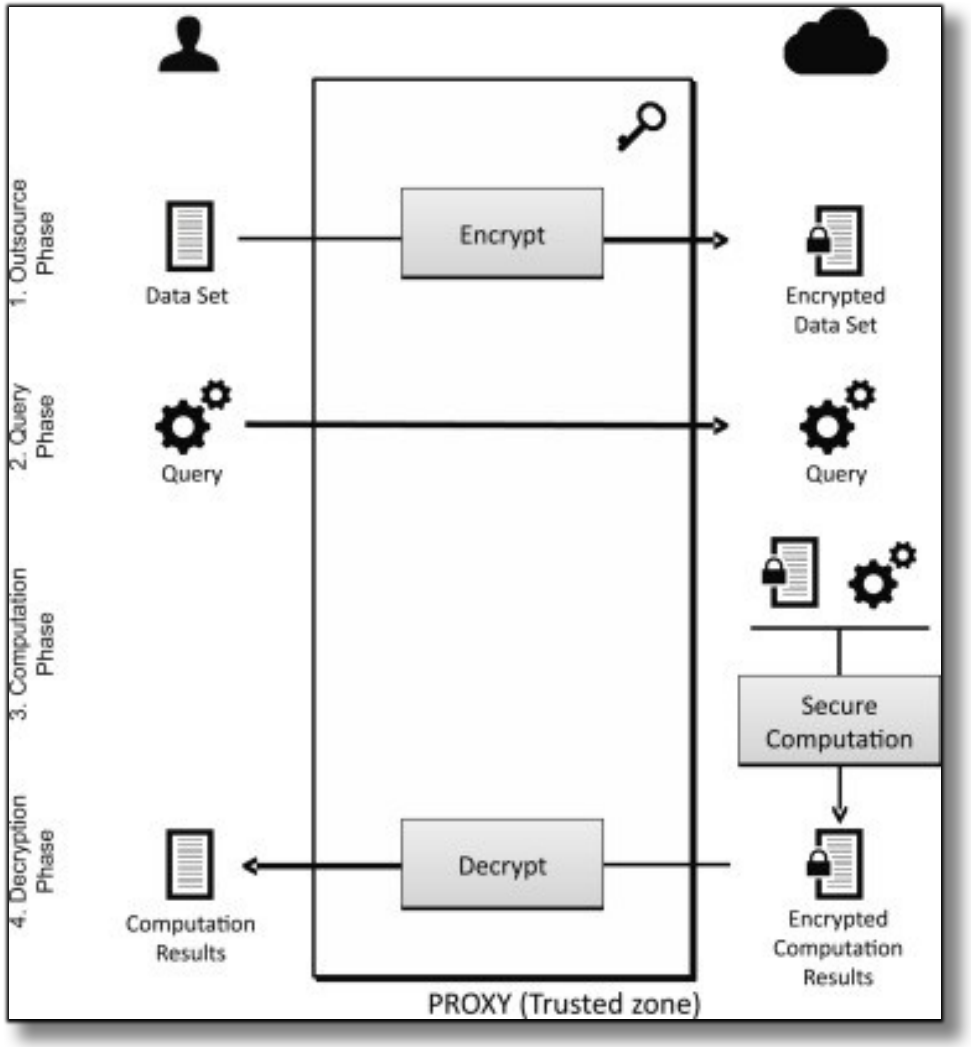


- **Storia**: Classe di metodi crittografici concepita nel 1978 da Rivest, Adleman e Dertouzos e prima implementazione nel 2009 da Craig Gentry.
- **Primitive**: La principale teoria matematica alla base dell'HE è basata sull'algebra dei reticoli (Lattice).
- **Sicurezza**: (average-case hard) Proven secure contro problemi equivalenti al SVP (RLWE): ritenuta quantum-resistant.
- **Riferimenti**:
  - https://en.wikipedia.org/wiki/Homomorphic_encryption
  - https://homomorphicencryption.org/



2. Applicazioni dell’HE

2. Applicazioni dell'HE



- Differenti schemi per operare sui seguenti tipi di dato:
  - **Booleani** (operazioni logiche → **circuiti cifrati!**):
    - FHEW: Ducas-Micciancio
    - TFHE: Chillotti-Gama-Georgieva-Izabachene
  - **Interi** (addizione, moltiplicazione, rotazione-bit):
    - BFV: Brakerski/Fan-Vercauteren
    - BGV: Brakerski-Gentry-Vaikuntanathan
  - **Reali:**
    - CKKS: Cheon-Kim-Kim-Song
- Scenario: Cloud services dove mettere dati e codice.
  - **Ricerca testuale sicura** (`char` like `int`)
  - **PRE:** Proxy re-encryption (ricifrare a terzi senza decifrare)
  - **IBE/ABE:** Identity-based/Attribute-based Encryption
  - **Multiparty crypto** (voting systems)

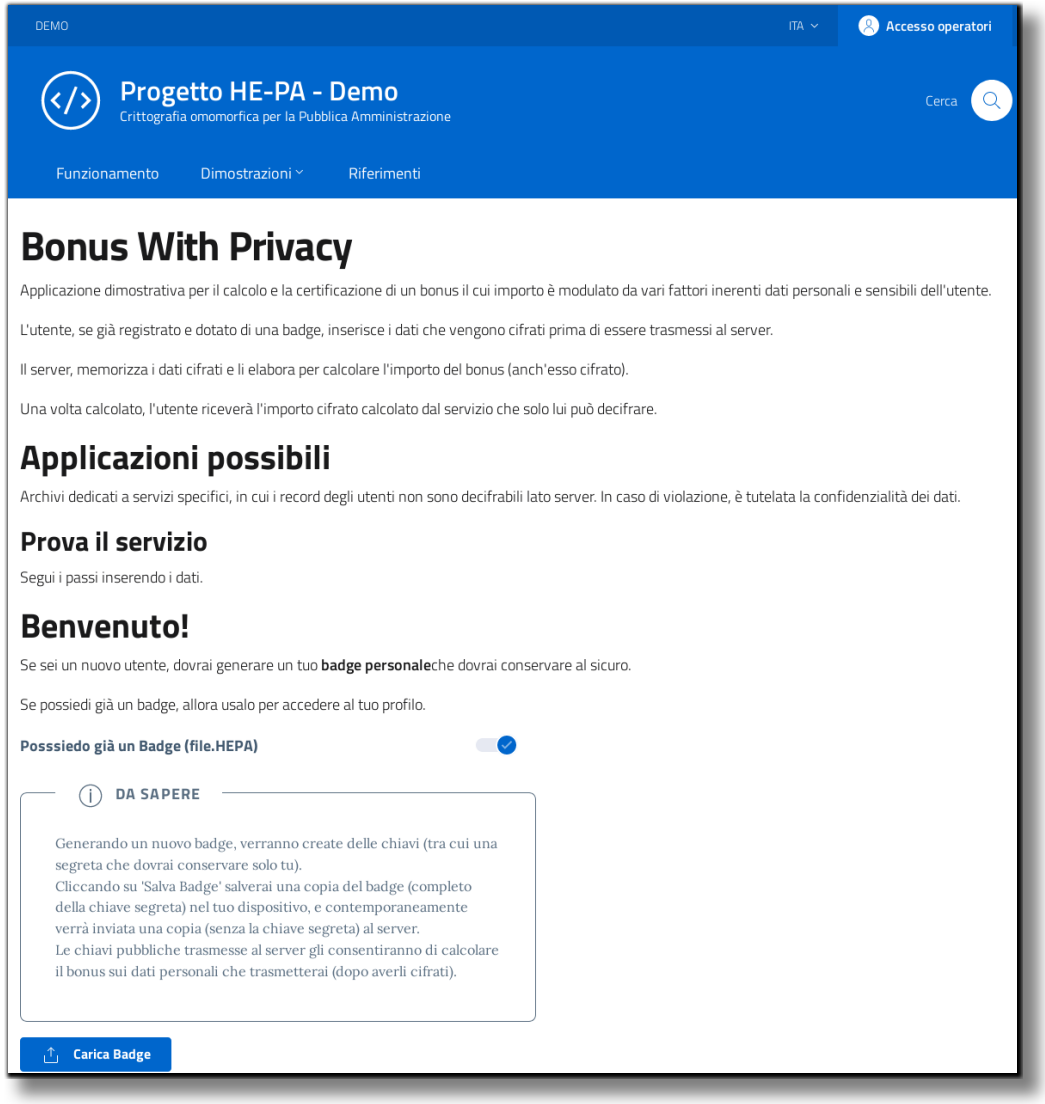
3. **HE-PA**: Prototipo di servizio digitale

3. **HE-PA**: Prototipo servizio digitale

- Testbed dove sperimentare l'applicazione "real-word" dell'HE.
- Scenario di riferimento:
  Servizi digitali offerti dalla P.A.
- Fruibile via web (mobile) all'URL:

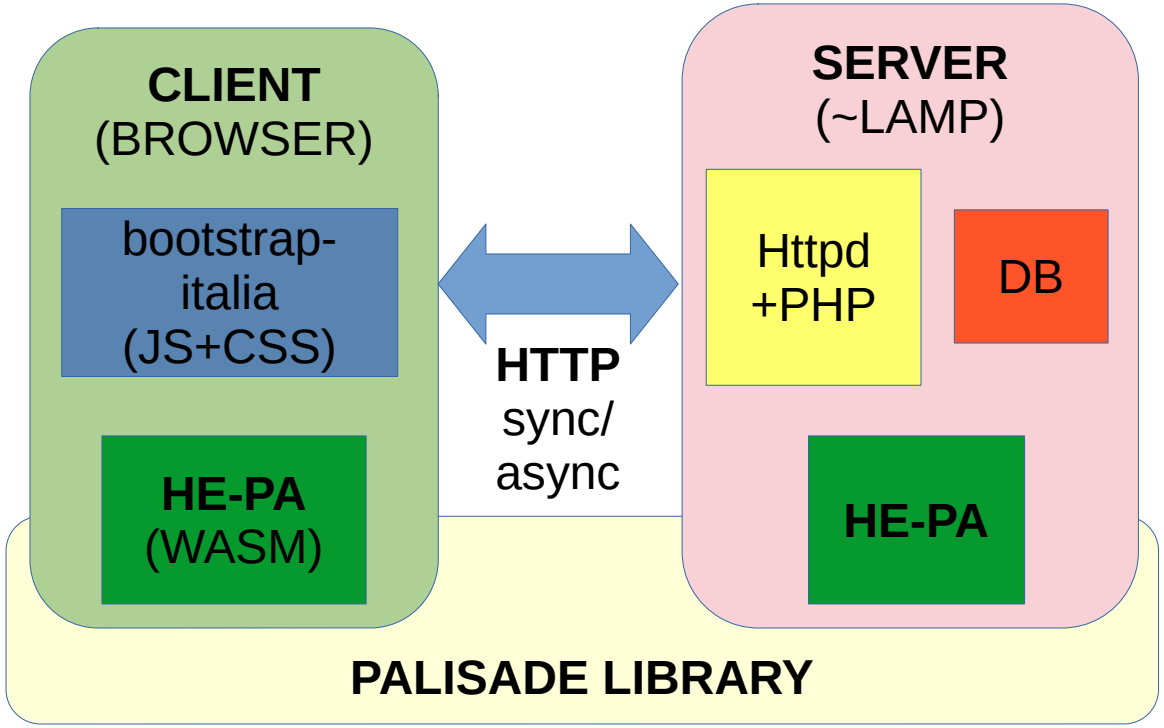
https://he.guardati.it

- Browser supportati:
  - ✔ **Firefox** (x86, ARM)
  - ✔ **Chrome** (x86, ARM***)
  - ✔ **Edge**



4. **HE-PA**: Architettura e componenti

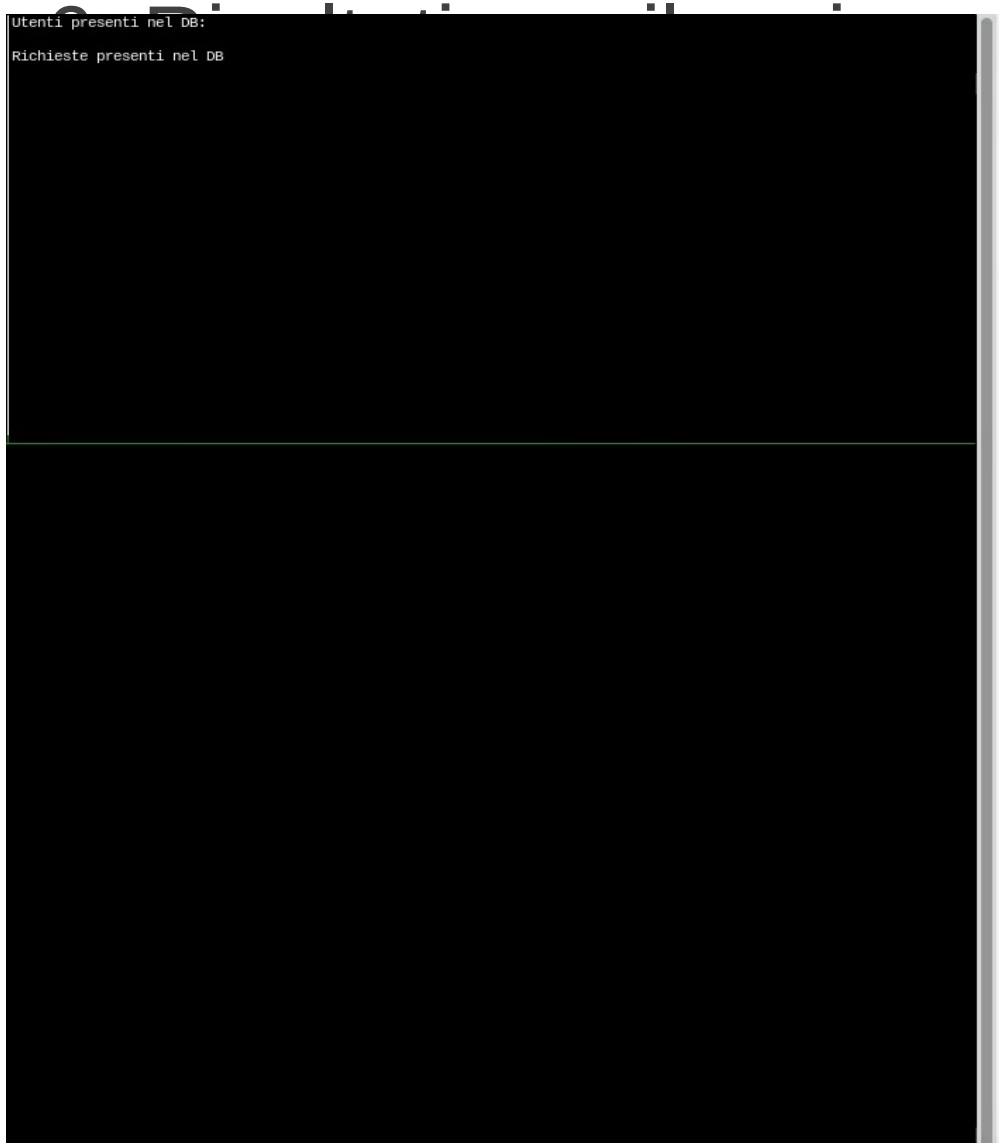
4. **HE-PA**: Architettura e componenti



- Architettura Client-Server.
- Il componente HE-PA è presente in entrambi i nodi ed effettua le operazioni di HE (utilizzando la libreria PALISADE)
- UI basata su **bootstrap-italia**

- Componenti:
  - **emscripten** (target WASM): per HE-PA lato client
  - **PALISADE** library: https://palisade-crypto.org/

5. **HE-PA**: Demo



DEMO ITA Accesso operatori

Progetto HE-PA - Demo
Crittografia omomorfica per la Pubblica Amministrazione

Cerca

Funzionamento Dimostrazioni Riferimenti

Bonus With Privacy

Applicazione dimostrativa per il calcolo e la certificazione di un bonus il cui importo è modulato da vari fattori inerenti dati personali e sensibili dell'utente.

L'utente, se già registrato e dotato di una badge, inserisce i dati che vengono cifrati prima di essere trasmessi al server.

Il server, memorizza i dati cifrati e li elabora per calcolare l'importo del bonus.

Una volta calcolato l'importo, l'utente può scaricare il certificato firmato digitalmente dal servizio

Applicazioni possibili

Archivi dedicati a servizi specifici, in cui i record degli utenti non sono decifrabili lato server. In caso di violazione, è tutelata la confidenzialità dei dati.

Prova il servizio

Segui i passi inserendo i dati.

Benvenuto!

Se sei un nuovo utente, dovrai generare un tuo **badge personale**che dovrai conservare al sicuro.

Se possiedi già un badge, allora usalo per accedere al tuo profilo.

Posssiedo già un Badge (file.HEPA)

DA SAPERE

6. Risultati e sviluppi possibili

6. Risultati e sviluppi possibili

- **Risultati**:
  - FHE consente di cifrare i DATI (ma anche il CODICE) e al contempo consente di eseguire le operazioni sugli stessi.
  - Logica di protezione delle chiavi stravolta! (...o no)
  - Requirements delle risorse pesanti rispetto alla classica crittografia asimmetrica (in particolare lo storage).
- **Sviluppi**:
  - Aggiungere la **firma** al bonus calcolato dal servizio.
  - Demo PRE: es. l'utente chiede supporto ad un operatore (il sistema **RI**-cifra i dati dell'utente per l'operatore scelto.

Grazie per l’attenzione