Financiado por la Unión Europea NextGenerationEU
Plan de Recuperación, Transformación y Resiliencia
GOBIERNO DE ESPAÑA | MINISTERIO DE CIENCIA E INNOVACIÓN
FEDER - FONDO EUROPEO DE DESENVOLVEMENTO REXIONAL
"Unha maneira de facer Europa"
UNIÓN EUROPEA
XUNTA DE GALICIA

Multi-Key Homomorphic Encryption for Collaborative Camera Attribution

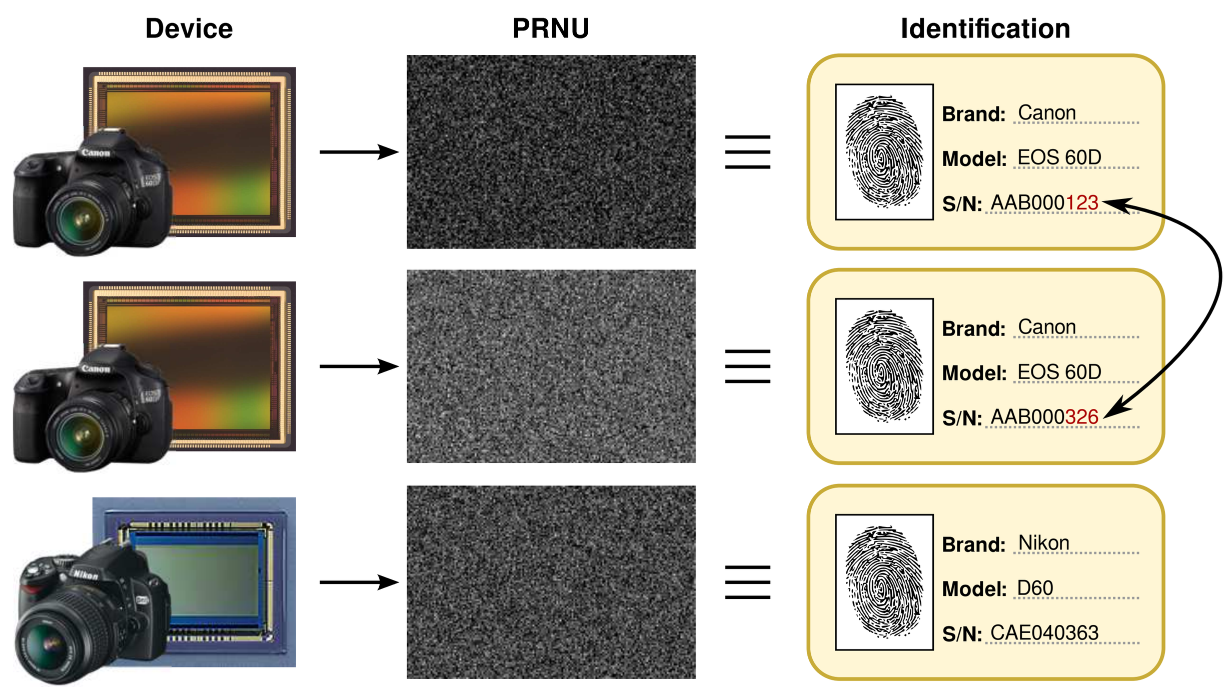
A. Pedrouzo-Ulloa, F. Pérez-González, D. Vázquez-Padín
{apedrouzo|fperez|dvazquez}@gts.uvigo.es

5th HomomorphicEncryption.org Workshop
1-2 September 2022, Geneva (Switzerland)

atlanTTic research center for Telecommunication Technologies
UniversidadeVigo
GPSC Signal Processing in Communications Group

Camera attribution problem

- The **amount of multimedia content** that law enforcement agencies (LEAs) must deal with in their investigations **is ballooning**.
- **Collaboration** between LEAs **is becoming essential** in a growing number of cases.
- **The exchange of multimedia is strongly limited by privacy and data-protection laws**.
- One **relevant scenario** within image forensics is the case of **camera attribution**.



Privacy-sensitive information

- **A number of images from the same device or camera model must be pooled together** in order to extract fingerprints reliably.
- **The images used to extract the fingerprints may be very sensitive** (e.g., in child abuse cases).
- Recent works have shown that **camera fingerprints estimates can leak a considerable amount of information** from the images used for extraction [1]

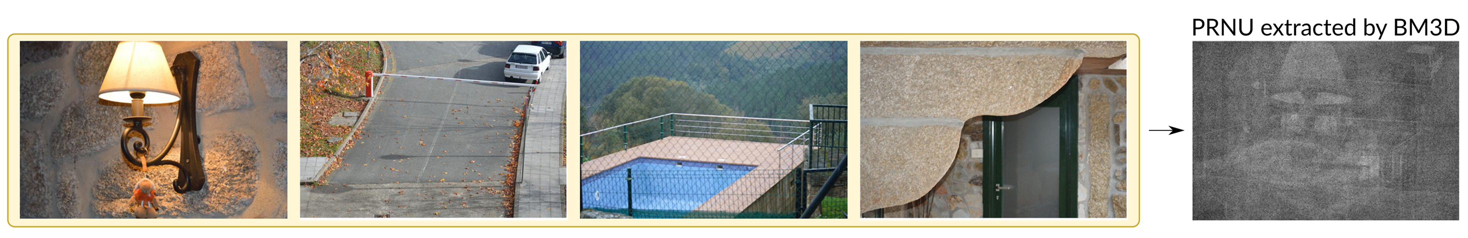
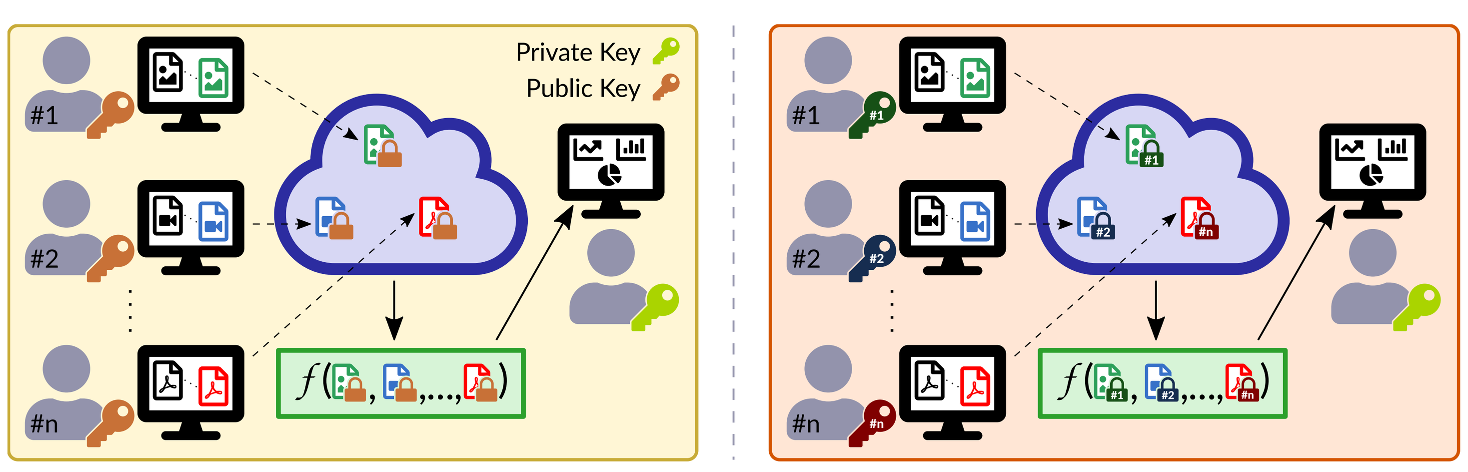


Illustration taken from Fig. 3 in [1] (CC BY 4.0) / Cropped and rearranged from original

Secure Camera Attribution

- Several works have addressed the mentioned privacy risks with different tools:
  - A fully unattended solution based on the use of lattice-based cryptosystems [2].
  - A combination of trusted hardware and HE (Homomorphic Encryption) [3].
  - The use of Shamir's secret sharing [4].
- These methods **assume an outsourcing scenario**, and **focus in fingerprint detection**.
- To the best of our knowledge, **our recent work** in secure camera attribution [5] is the first to propose **a federated framework for fingerprint extraction/detection**.

Collaborative Forensic Scenario

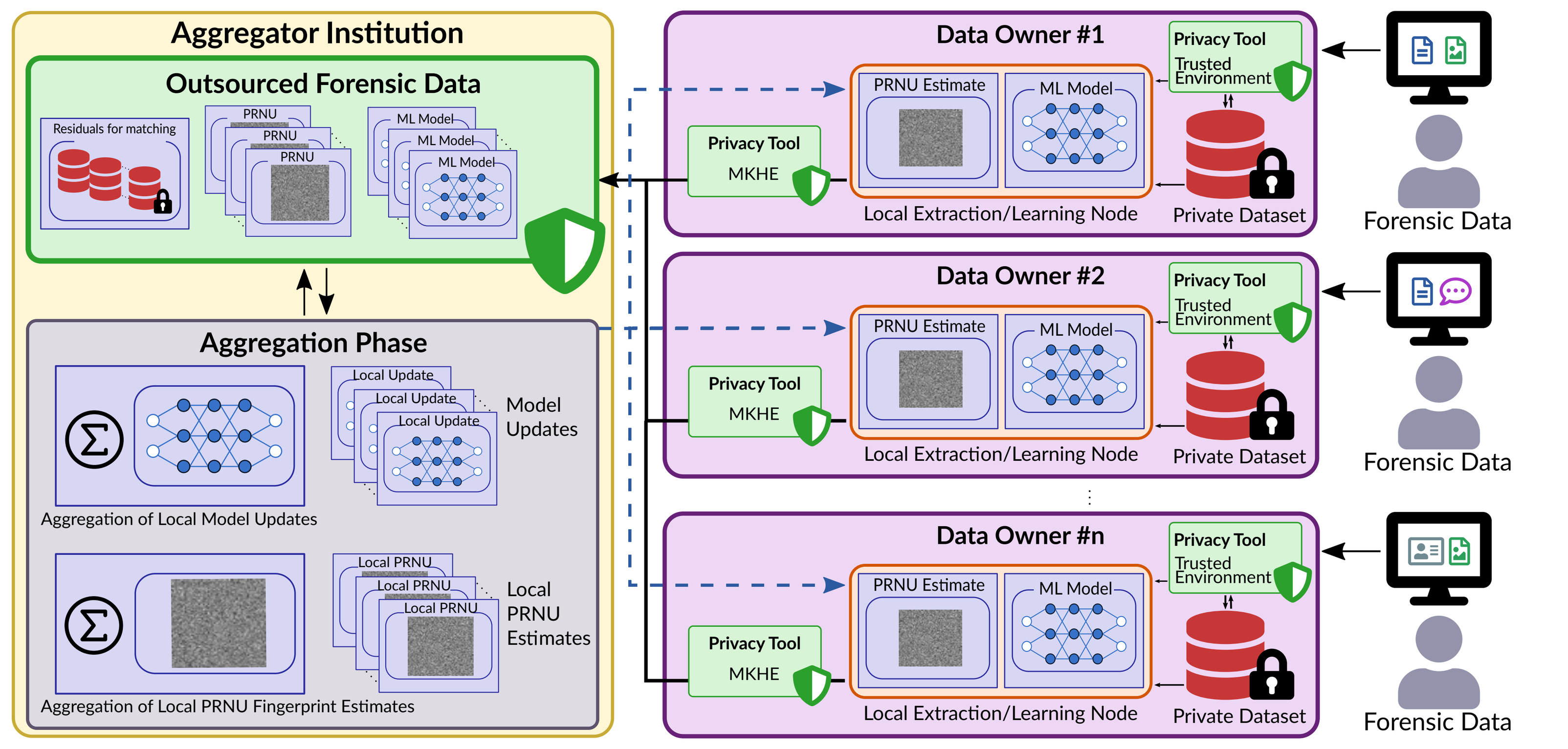


- **Data Owners** are LEAs or Forensic Institutions **aiming at camera fingerprint extraction** through **collectively trained models**.
- The **aggregator** can be a Data Owner, or a larger organization like Europol or Interpol.
- The **end users** would be the participating or other LEAs or Forensic institutions.
- **MKHE** (Multi-Key Homomorphic Encryption) **tools, instead of single-key HE, fit better the needs of our collaborative scenario** [6].

Proposed Collaborative Framework

Our federated framework builds upon two key concepts [5]:

- **Unprotected local data** is **isolated in different silos**.
- All **information leaving a silo** is **previously encrypted** with MKHE [6].



Workflow with MKHE

- All involved **Data Owners generate their own individual secret key and also a collective public key**.
- **Each Data Owner encrypts its data** to be outsourced under a collective public key.
- **One of the entities** will be **in charge of computing** a particular functionality f.
- All **involved parties collaboratively decrypt** the output.

Example functionalities inside the framework

- **Training of ML models for noiseprint extraction**.
  - The funcionality f is the aggregation of local models.
- **Aggregation of local fingerprint estimates** (e.g., PRNU or noiseprint).
  - The functionality f is implemented with a homomorphic addition, followed by a division after decryption.
- **Fingerprint matching**.
  - The functionality f corresponds with a set of homomorphic scalar products among encrypted fingerprint estimates.
- **Residuals matching and/or fingerprint/residual matching**.
  - The functionality f corresponds to a set of homomorphic scalar products with encrypted fingerprints/residuals.

Implementation runtimes

- Aggregation and matching functionalities implemented with Lattigo v3.0.4 [7]. Parameters: $\{\mathrm{T} = 2^{16}+1, \mathrm{bfv.PN12QP109}\}$ and $\{\mathrm{T} = 3 \cdot 2^{30}+1, \mathrm{bfv.PN13QP218}\}$.
- Evaluation runtimes were conducted multi-threaded on an Intel Core i7-4510U @ 2.00GHz x 4 with 7.7GB. The rest of primitives were conducted singled-threaded.

64 parties + Cloud fingerprint 1024 X 1024	CKG + RKG + RTG (Cloud + Parties)	Encryption	Evaluation	CKS (Cloud + Parties)	Decryption
Aggregation	2 *ms* + 716 *us*	826 *ms*	689 *ms*	594 *ms* + 735 *ms*	173 *ms*
Matching	227 *ms* + 98 *ms*	1.13 *s*	65 *s*	775 *ms* + 483 *ms*	166 *ms*

References

[1] S. Fernández-Menduiña and F. Pérez-González, "On the information leakage quantification of camera fingerprint estimates," *EURASIP J. Inf. Secur.*, vol. 2021, no. 1, pp. 6, 2021.

[2] A. Pedrouzo-Ulloa et al., "Camera attribution forensic analyzer in the encrypted domain," in *IEEE WIFS*. 2018, pp. 1–7, IEEE.

[3] M. Mohanty et al., "e-prnu: Encrypted domain prnu-based camera attribution for preserving privacy," *IEEE Tran. Dep. Sec. Comp.*, vol. 18, no. 1, pp. 426–437, 2021.

[4] R. Jena et al., "SSS-PRNU: privacy-preserving PRNU based camera attribution using shamir secret sharing," *CoRR*, vol. abs/2106.07029, 2021.

[5] A. Pedrouzo-Ulloa et al., "Secure collaborative camera attribution," in *ACM EICC*. 2022, pp. 97–98, ACM.

[6] C. Mouchet et al., "Multiparty Homomorphic Encryption from Ring-Learning-with-Errors," *Proc. Priv. Enhancing Technol.*, vol. 2021, no. 4, pp. 291–311, 2021.

[7] C. Mouchet et al., "Lattigo: a multiparty homomorphic encryption library in go," in *WAHC 2020*, 2020.