A Format Compliant Encryption Method For 3D Objects Allowing Hierarchical Decryption

Bianca Jansen van Rensburg[1,2], William Puech[1], Jean-Pierre Pedeboy[2]
[1] LIRMM, Univ. Montpellier, CNRS (France), [2] STRATEGIES S.A. (France)

ICASSP 2024 KOREA — IEEE International Conference on Acoustics, Speech and Signal Processing

Introduction

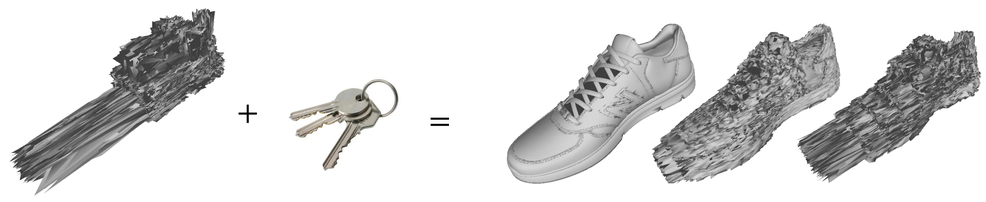
3D objects are frequently stored and shared **online** and therefore **security** is essential
3D objects are **encrypted** to secure their **content**. Users may have different **access rights**
State of the art solution: **Selective Encryption** [Beugnon 2018]

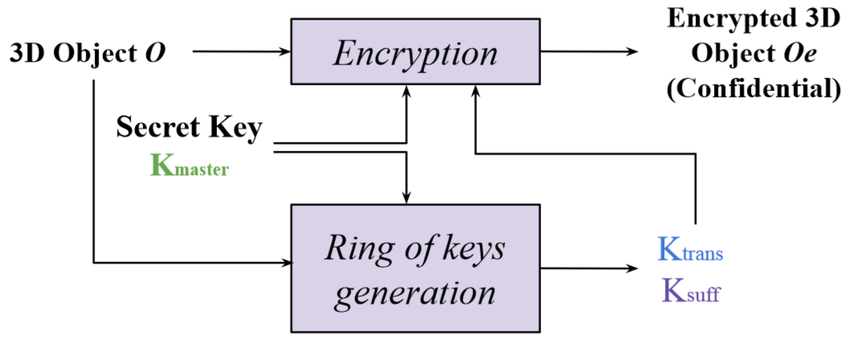
- ✅ **3 visual security levels:** Transparent, Sufficient, Confidential
- ⚠ **Not secured:** some information remains in the clear domain during transfer
- ⚠ **Not eco-friendly**: 3D objects are stored, encrypted and shared multiple times

Our method:

- ❖ Alternative to selective encryption
- ❖ Encryption method allowing for a hierarchical decryption of 3D objects
- ❖ Based on a ring of keys
- ❖ Secured during the transfer: a confidential level 3D object is transferred
- ❖ Eco-friendly: 3D is stored, encrypted and shared once

Encoding Phase Overview



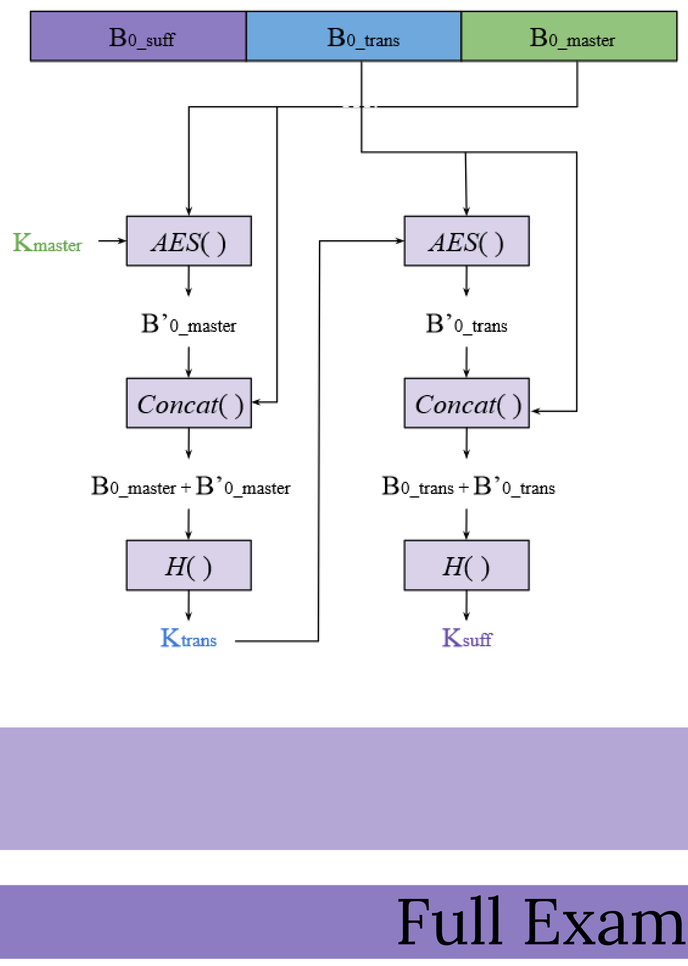


Encryption Method and Hierarchical Decryption

Encryption Phase

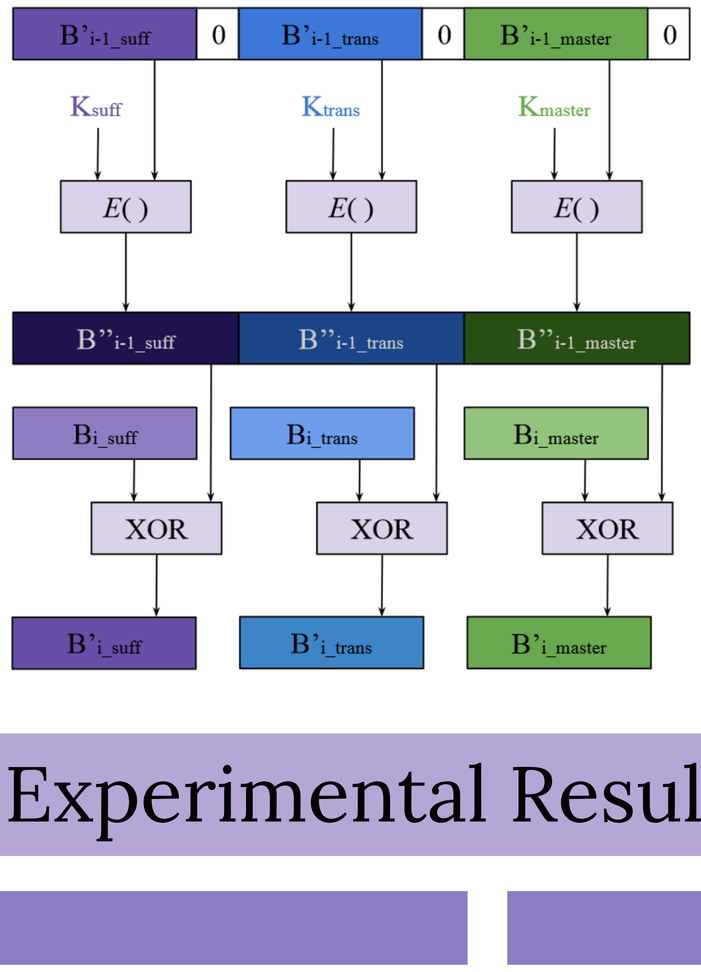
Hierarchical Key Generation

- ❖ Mantissas are grouped into blocks
- ❖ $K_{master} > K_{trans} > K_{suf}$
- ❖ Generated according to the **hierarchically superior** block:
  - Based on a hash function
  - Transparent and sufficient keys are generated according to the 3D object



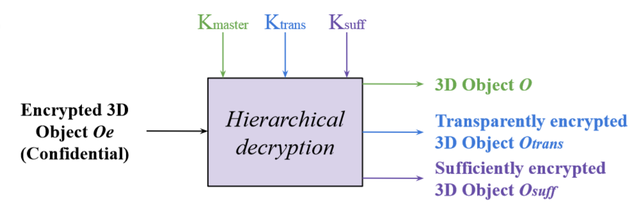
Encryption

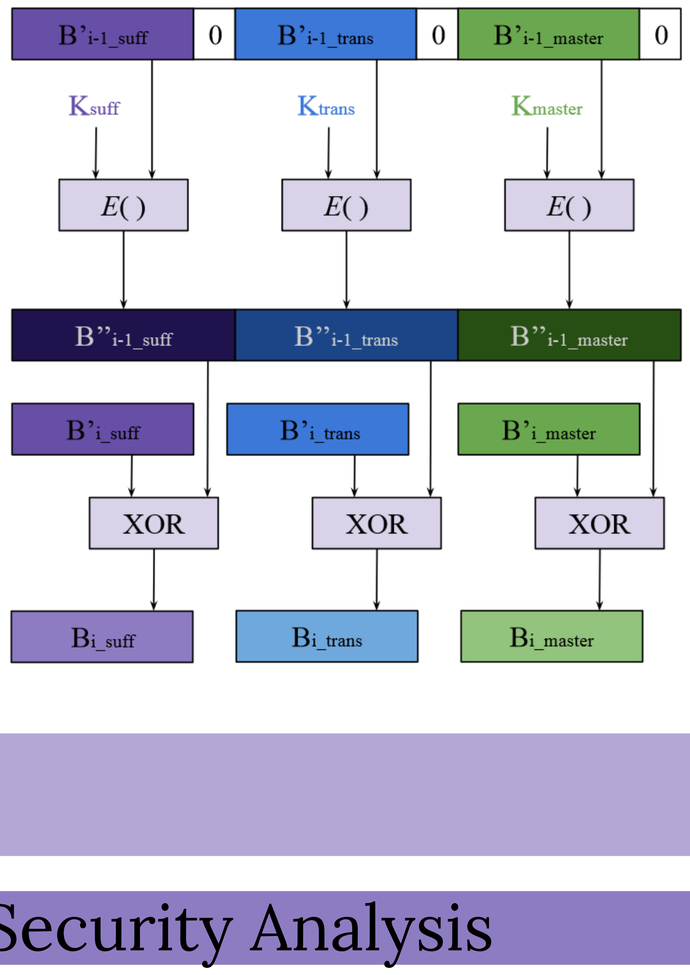
- ❖ Hierarchical keys generated during the encryption process
- ❖ Each block Bi encrypted according to the **generated hierarchical key**
- ❖ **AES** [Daemen 2002] encryption in CFB mode



Hierarchical Decryption

- ❖ Depends on the hierarchical key used
- ❖ Hierarchically inferior keys generated during the decryption
- ✅ ❖ Impossible to generate the hierarchically superior keys

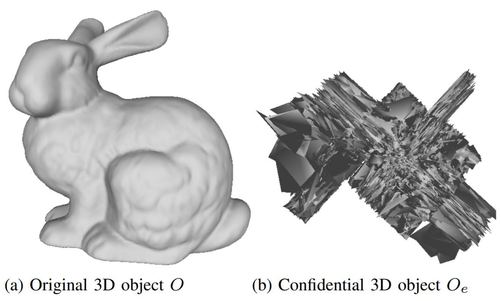




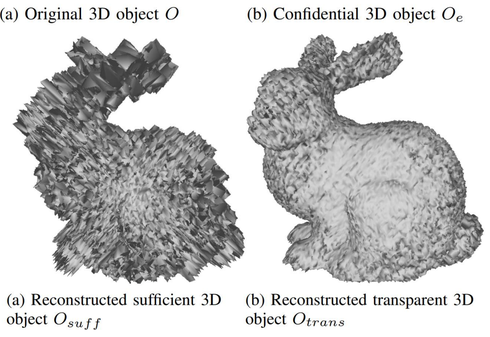
Experimental Results

Full Example

3D object ***Bunny*** (Stanford dataset)

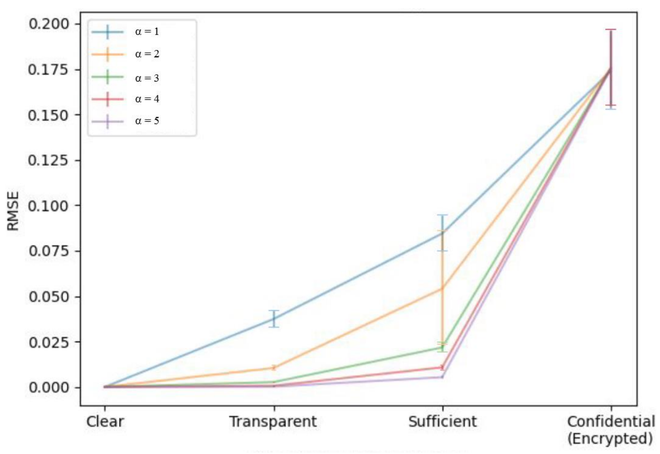


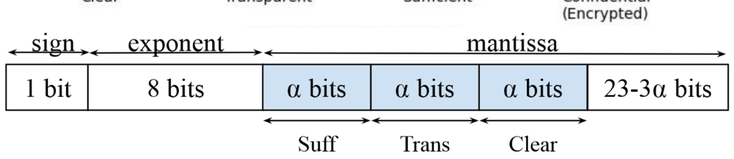
(a) Original 3D object O (b) Confidential 3D object O_e



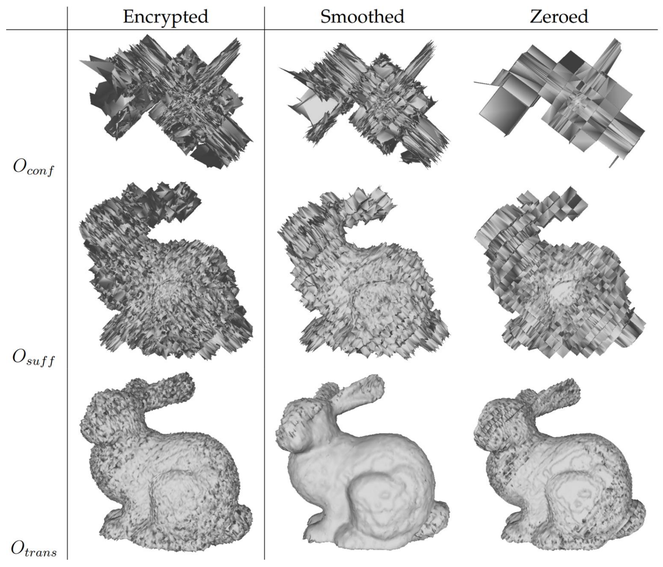
(a) Reconstructed sufficient 3D object O_{suff} (b) Reconstructed transparent 3D object O_{trans}

Average RMSE of the Stanford dataset





Security Analysis



- ❖ Key: AES security
- ❖ Form: laplacian smoothing and zeroing
  - At least 1 hierarchical key is required to perform an attack
  - Strong variations eliminated
  - Visual security level does not change

RMSE (10^{-3}) of the attacks

	Encrypted	Smoothed	Zeroed
Confidential	162.499	143.416	154.080
Sufficient	39.610	32.364	**49.200**
Transparent	9.512	6.425	**11.033**

Conclusion

- ❖ First encryption method which allows a hierarchical decryption for 3D objects
- ❖ Alternative to selective encryption:
  - Secured during the transfer and storage
  - Eco-friendly: stored, encrypted and shared once

References

[Daemen 2002] J. Daemen and V. Rijmen, The design of Rijndael, vol. 2. Springer, Berlin, Heidelberg, 2002.

[Beugnon 2018] S. Beugnon, W. Puech, and J. Pedeboy, "From Visual Confidentiality To Transparent Format-Compliant Selective Encryption Of 3D Objects," in 2018 IEEE International Conference on Multimedia and Expo Workshops (ICME Workshops). IEEE Computer Society, 2018.