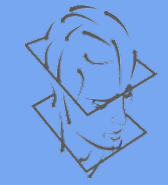
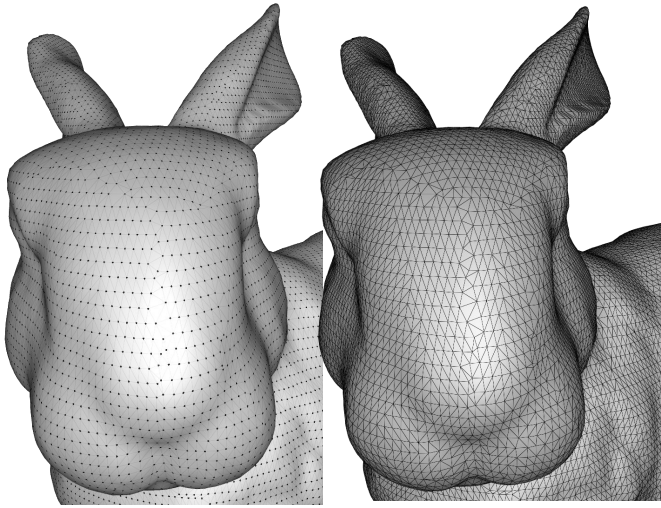
Draco 3D Object Crypto-Compression

26 juin 2023

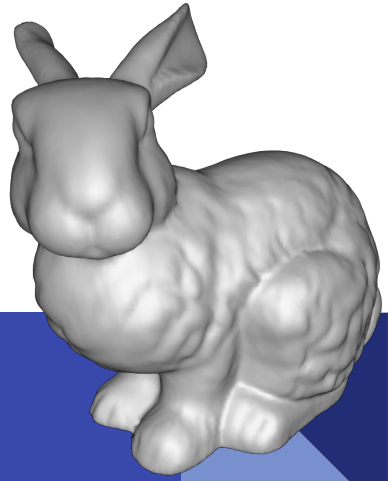
Bianca Jansen van Rensburg, William Puech, Jean-Pierre Pedeboy
Montpellier, France



Context



- Geometry: point cloud (cluster of vertices)
- Vertex **v**: 3 coordinates (v_x, v_y, v_z)
- Connectivity: polygons
- 3D objects are important assets
- Can be very large (millions of vertices)
  - Compression is needed
- Draco: an industry standard for 3D compression



Context

- Transferred over networks
- Stored on the cloud
- Security is needed
  - **Encryption**
  - Watermarking

Encryption and Compression

- Encryption first, then compression = compression very inefficient/ lossy compression cannot be decrypted
- Compression first, then encryption = not format compliant

Solution: Crypto-Compression

- Joint compression and encryption
- More difficult for attackers
- Format compliant

Plan

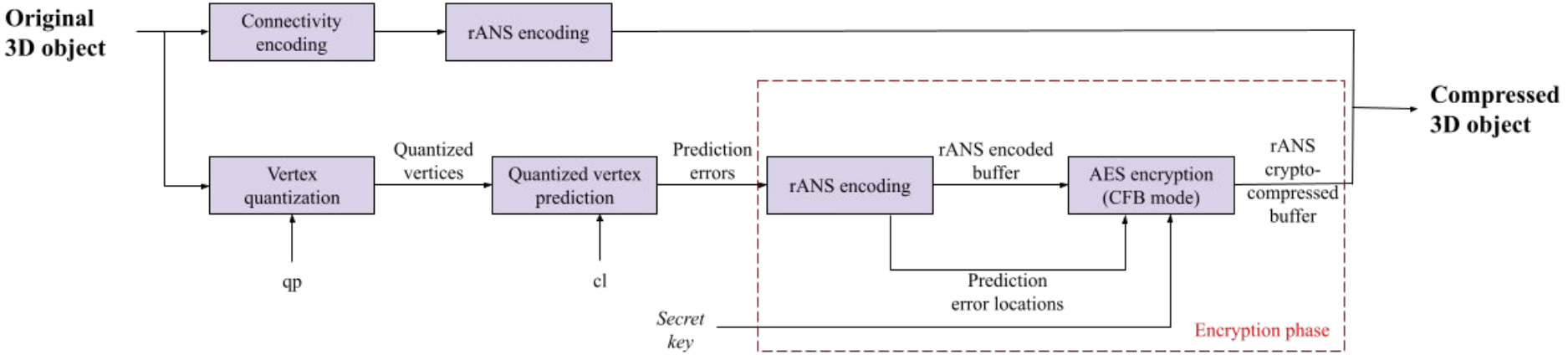
- Context
- Proposed method
- Experimental results
- Conclusion and perspectives

Overview

- First crypto-compression method for 3D objects
- Based on Draco

Overview

- AES encryption step added to Draco compression

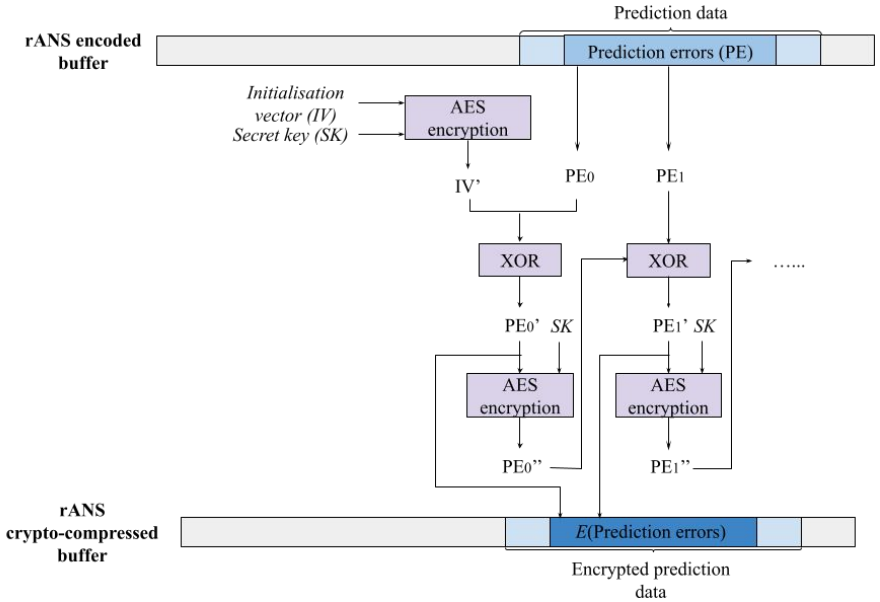


Geometry Crypto-Compression

- Coordinates v_i
  - 32-bit floating points
  - $i = \{x, y, z\}$
- Vertices quantized according to the Draco parameter *qp*
  - *qp*: number of bits conserved per coordinate
  - Range after quantization: $v_i \in [0, 2^{qp}]$
  - *qp* = [0, 30]
- Vertex prediction errors
  - Based on *cl* = [0, 10]
- Entropy encoding
  - rANS
  - Everything is encoded
  - Prediction error markers

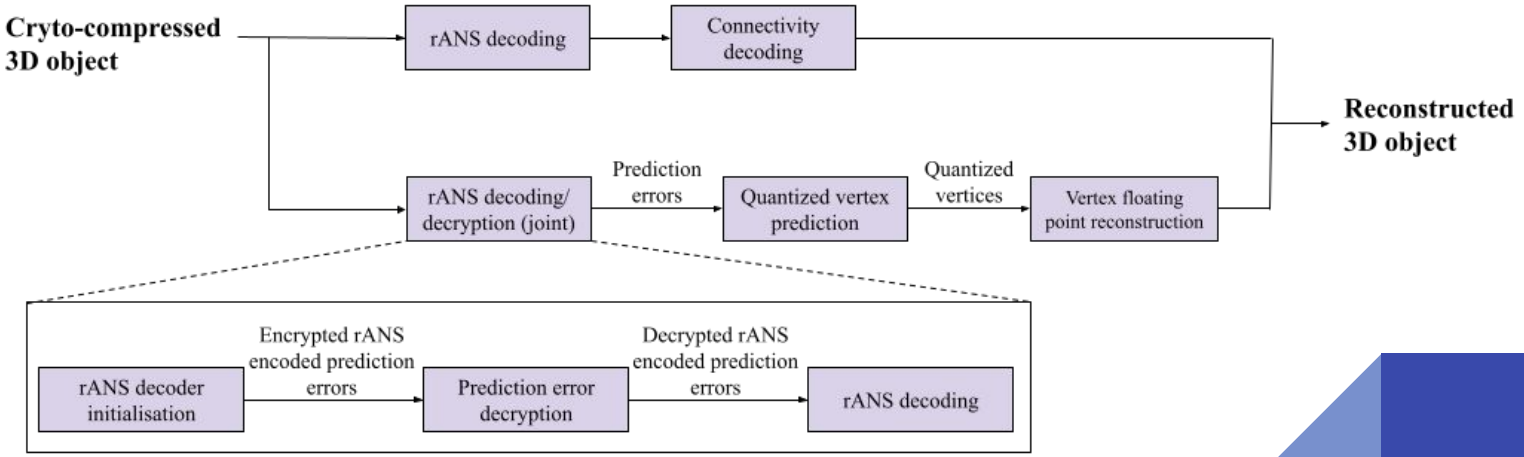
Encryption Step

- Prediction errors encrypted
- AES in CFB mode



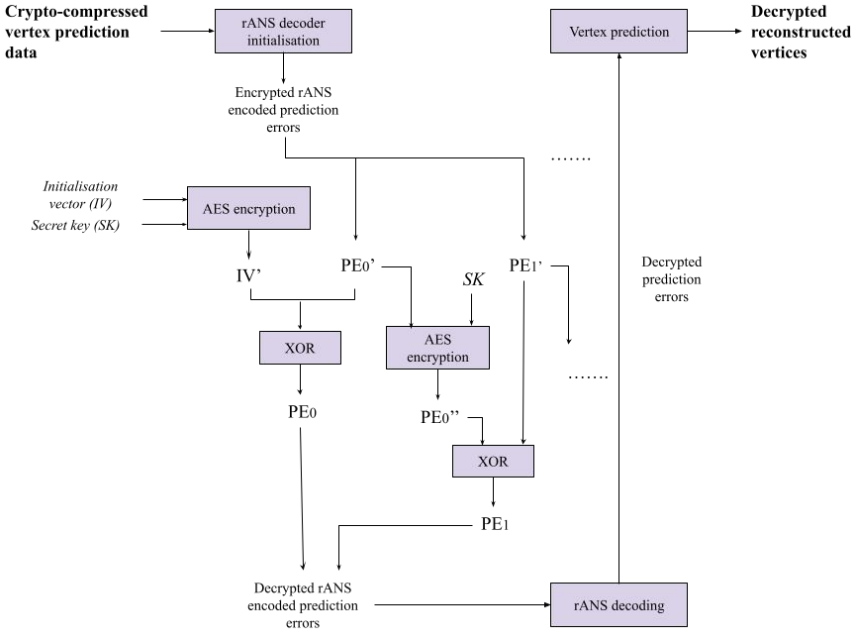
Decryption Overview

- Decoding phase
- Avoid auxiliary data: performed jointly with the rANS decoding step



Decryption

- AES in CFB mode

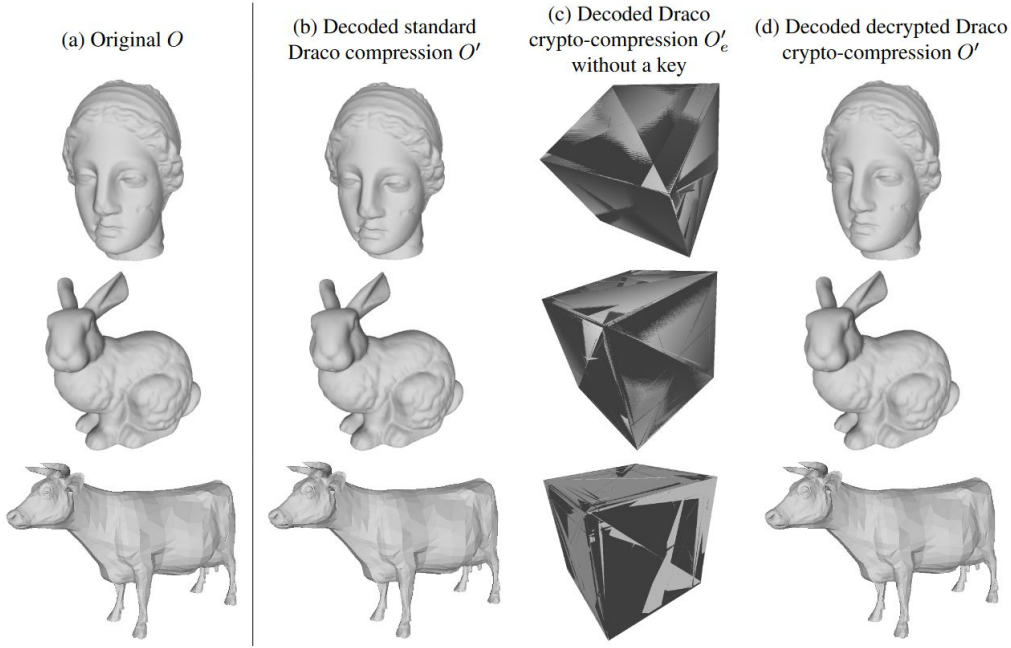


Plan

- Context
- Proposed method
- Experimental results
- Conclusion and perspectives

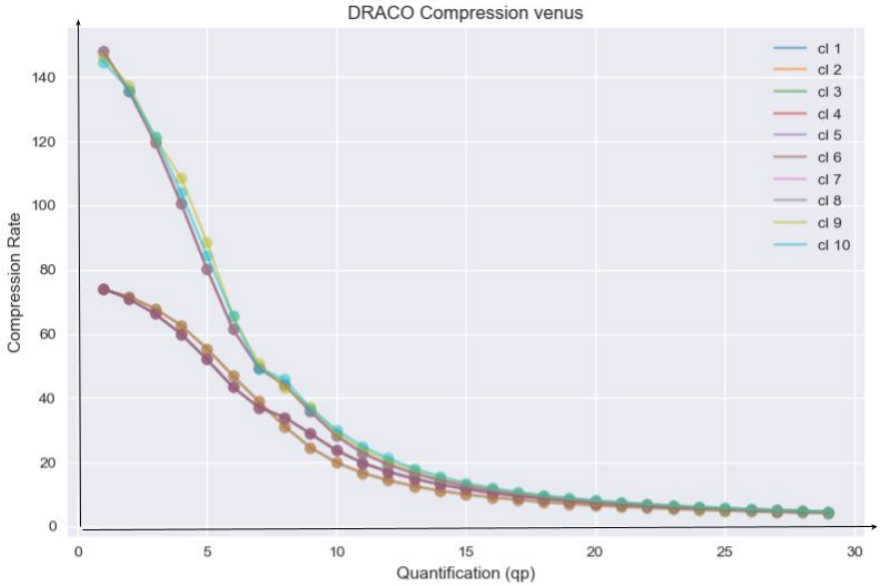
Visual Results

- Default Draco parameter: *qp*=11



Compression rate analysis

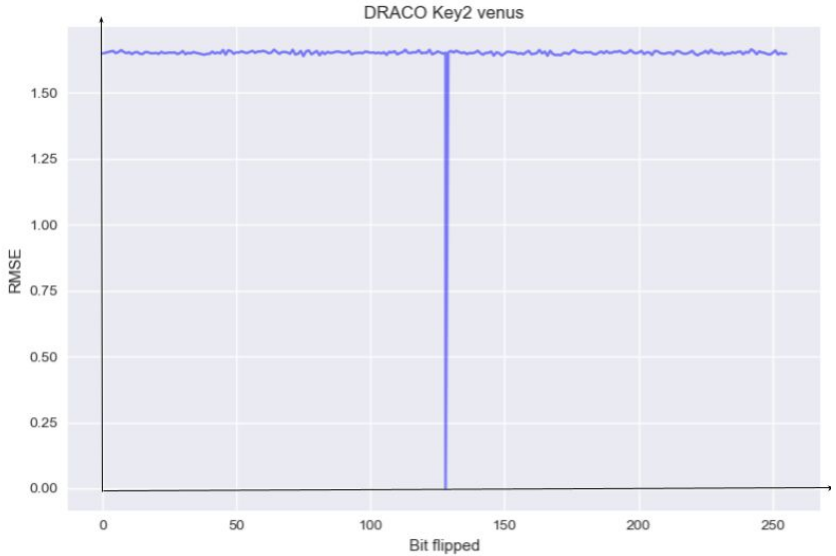
- Compression rate for *Venus*
- No compression rate loss



- Points: decrypted and decoded crypto-compressed 3D object
- Curve: original Draco decoded 3D object

Key analysis

- A single bit flipped in 256 key
- AES



Plan

- Context
- Proposed method
- Experimental results
- Conclusion and perspectives

Conclusion + Perspectives

- First crypto-compression method for 3D objects
- Based on Draco compression
- No size expansion and completely reversible

- Future work: other joint security methods for Draco