Vertical axis: Space (bytes) for a ciphertext
Horizontal axis: Time (cycles) to generate a session key given a ciphertext

• means that the SUPERCOP database does not list IND-CCA2 security as a goal for this primitive.
• means that the SUPERCOP database does not list constant time as a goal for this implementation.