Order-Revealing Encryption:
New Constructions, Applications and Lower Bounds

Kevin Lewi and David J. Wu

Stanford University

July, 2016

Order-Revealing Encryption [BLRSZ15]

secret-key encryption scheme

$$\begin{aligned} \mathrm{ct}_1 &= \mathrm{Enc}(\mathrm{sk}, 123) \\ \mathrm{ct}_2 &= \mathrm{Enc}(\mathrm{sk}, 512) \\ \mathrm{ct}_3 &= \mathrm{Enc}(\mathrm{sk}, 273) \end{aligned}$$

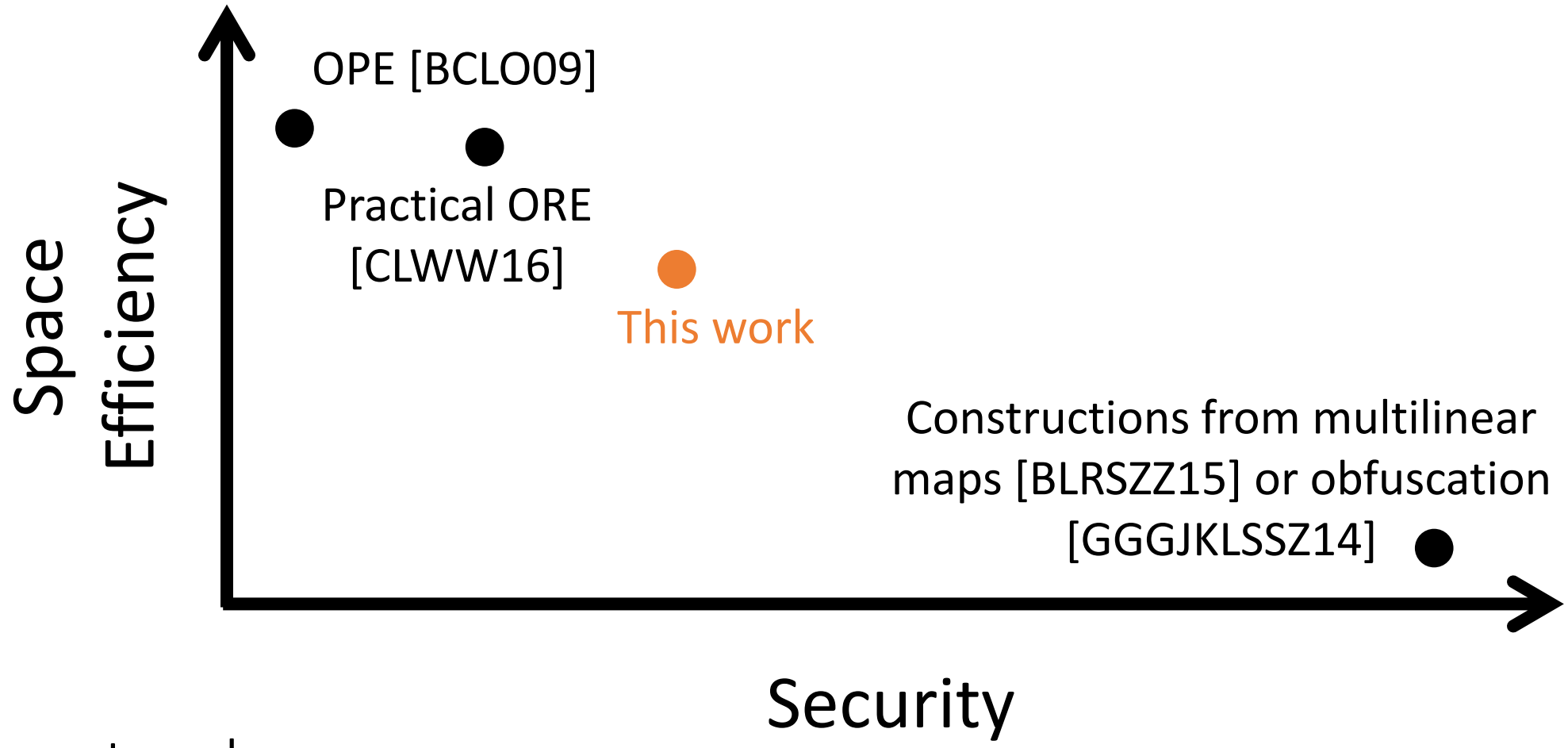
Which is greater: the value encrypted by ct_1 or the value encrypted by ct_2?

range queries on encrypted data

Client

Server

The Landscape of OPE/ORE



Not drawn to scale

The Elephant in the Room: Inference Attacks [NKW15]

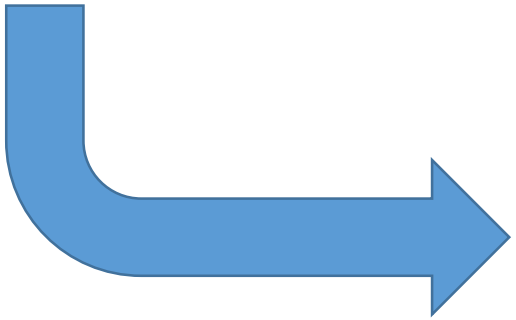
ID	Name	Age	Diagnosis
wpjOos	2wzXW8	SqX9l9	KqLUXE
XdXdg8	y9GFpS	gwilE3	MJ23b7
P6vKhW	EgN0Jn	S0pRJe	aTaeJk
orJRe6	KQWy9U	sERF3M	4FBEO0

encrypted database

+

public information

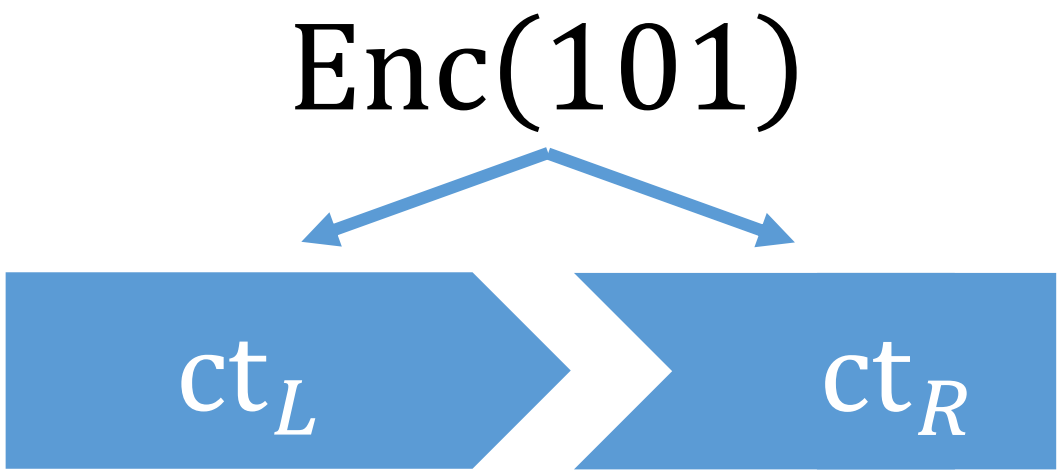
frequency and statistical analysis



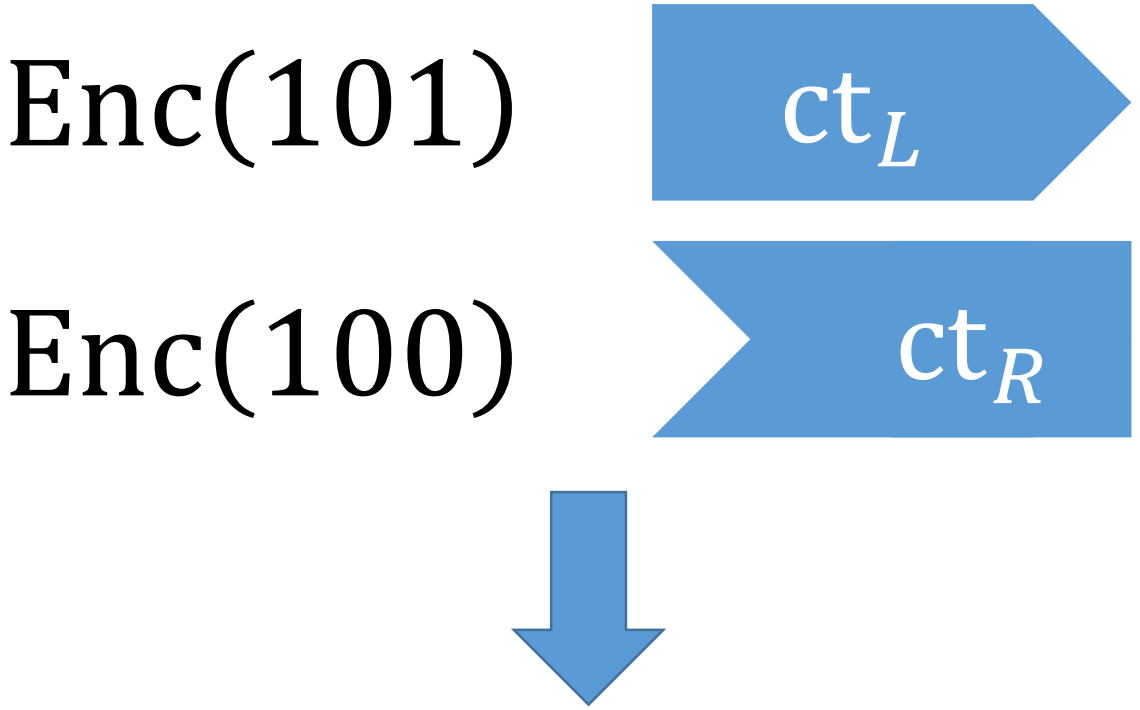
ID	Name	Age	Diagnosis
???	Alice	30-35	2
???	Bob	45-50	3
???	Charlie	40-45	2
???	???	40-45	4

plaintext recovery

Our ORE Scheme: Ciphertext Decomposition



ciphertexts naturally split into two components

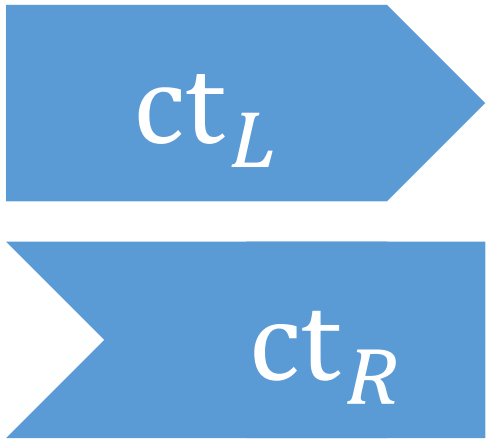


greater than

Our ORE Scheme: Ciphertext Decomposition

$\mathrm{Enc}(101)$

$\mathrm{Enc}(100)$



comparison can be performed between left ciphertext and right ciphertext

right ciphertexts provide **semantic security**!

robustness against offline inference attacks!

Thanks!

Project Page: `https://crypto.stanford.edu/ore/`

Paper Link: `https://eprint.iacr.org/2016/612.pdf`