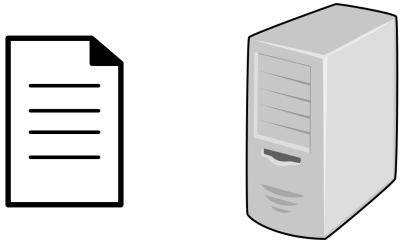
PIR: Private Information Retrieval

Andrea Guerra

Università di Pisa

Private Information Retrieval

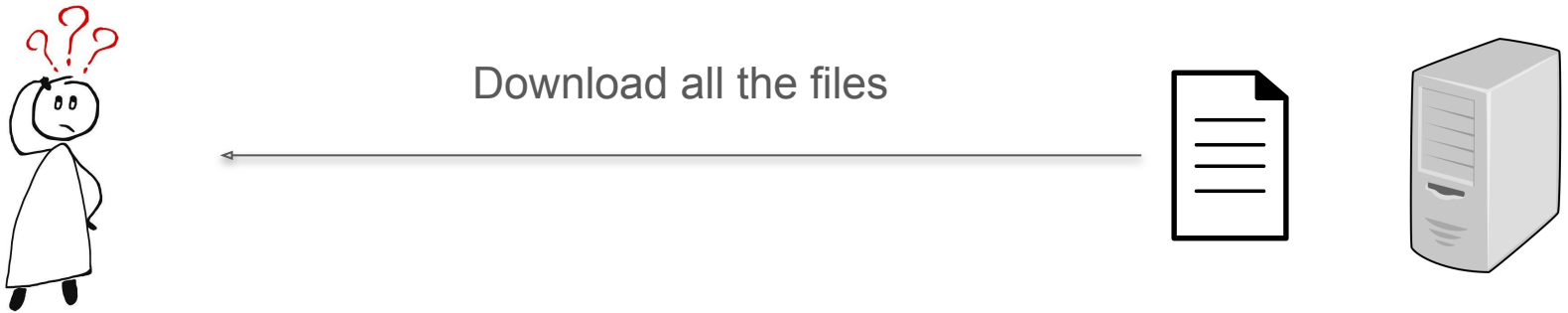
USER



SERVER

PIR allows a user to retrieve a file from a public database without revealing the file to the server

Trivial PIR



High network costs :(

Private Information Retrieval: Types

- Information-theoretic PIR (IT-PIR)
  - Requires multiple servers and non-collusion assumptions

- Computational PIR (cPIR)
  - Expensive and requires cryptographic assumptions

Applications

- Patent search
- Private ad network
- Private movie streaming

…

Outline

- Homomorphic Encryption
- Basic PIR construction
- XPIR
- SealPIR
- Evaluation

Homomorphic Encryption

KeyGen() = (pk, sk)

Enc(m, pk) = c

Dec(c, sk) = m

Homomorphic Properties:

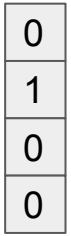
$Enc(m_1) \oplus Enc(m_2) = Enc(m_1 + m_2)$

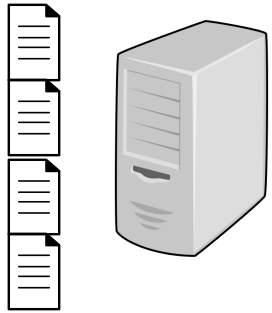
$e \otimes Enc(m) = Enc(e \times m)$

$Enc(m_1) \otimes Enc(m_2) = Enc(m_1 \times m_2)$

A PIR Protocol

The client wants the file **2**

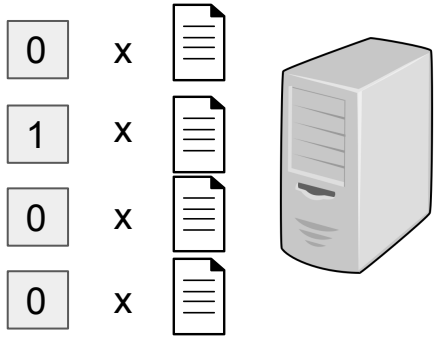




Client encryption is additively homomorphic

A PIR Protocol

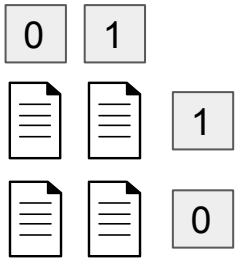
The client wants the file **2**

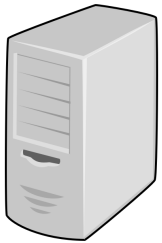


Client encryption is additively homomorphic

A PIR Protocol

The client wants the file **2**

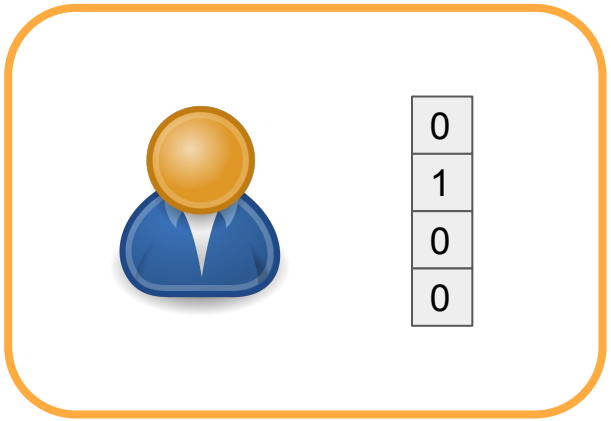




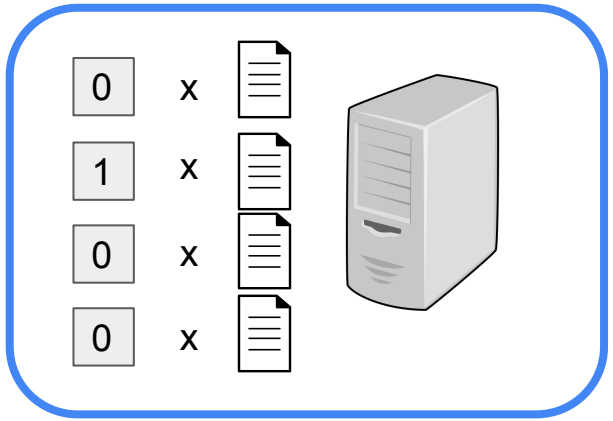
Communication complexity: $O(\sqrt{n})$

Problems

Problem: Query is very large

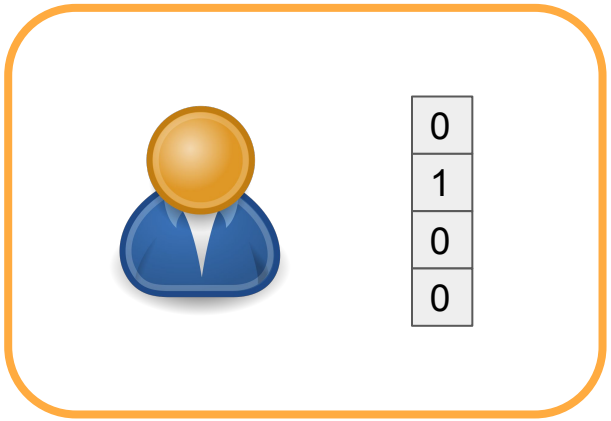


Problem: Computation is expensive

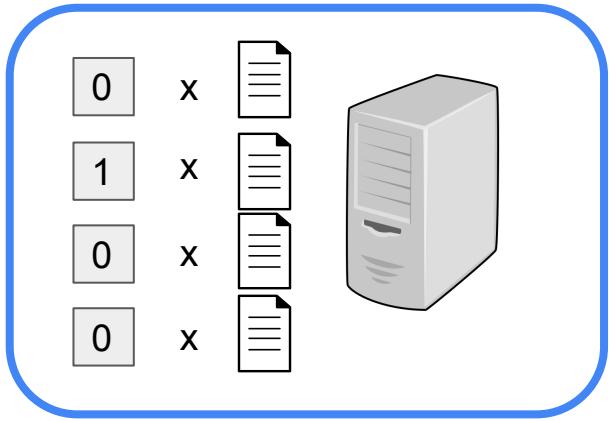


Problems

Problem: Query is very large

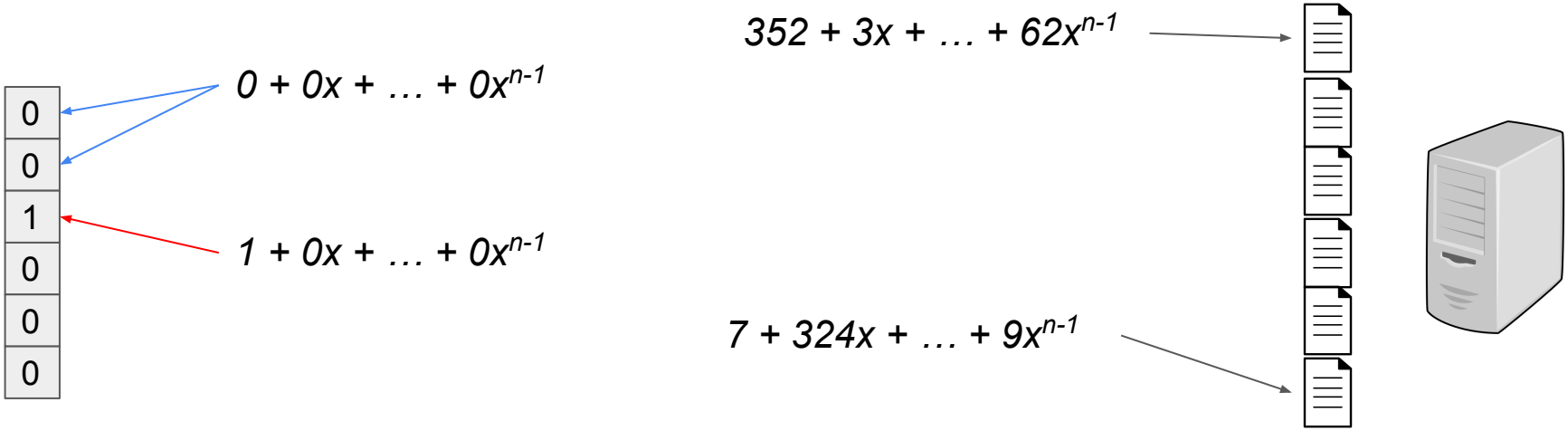


Problem: Computation is expensive



XPIR
Lattice crypto + preprocessing
DB

XPIR



Preprocessing speed: 5 Gbit/s

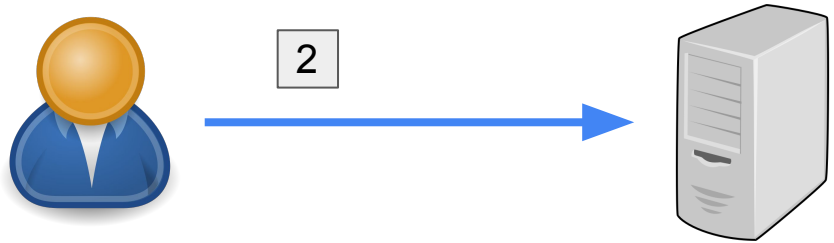
SealPIR

- Compressing Query
  - from a query vector to a single query ciphertext

- Probabilistic Batch Codes
  - processing a batch of queries from the same client to reduce the computational cost

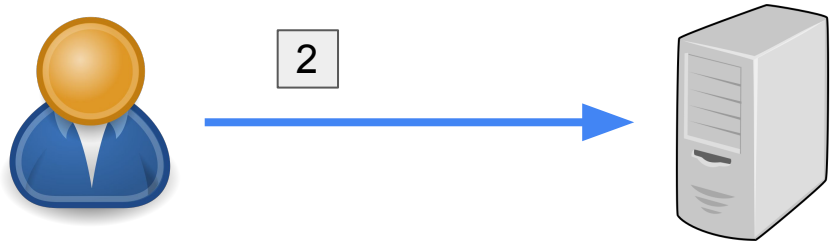
Compressing Query

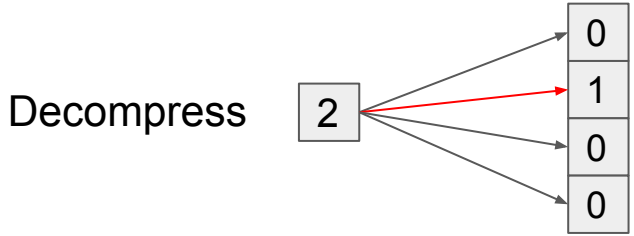
The client wants the file **2**



Compressing Query

The client wants the file **2**





The server does not learn the index

Fully Homomorphic Encryption

2 + 3 = 5	Addition of ciphertexts	0.002 ms
3 × 0 = 0	Multiplication of a ciphertext by a plaintext	0.14 ms
3 × 2 = 6	Multiplication of ciphertexts	**1.77 ms**

With × and + we can compute arbitrary functions (Decompression)

Substitution operation

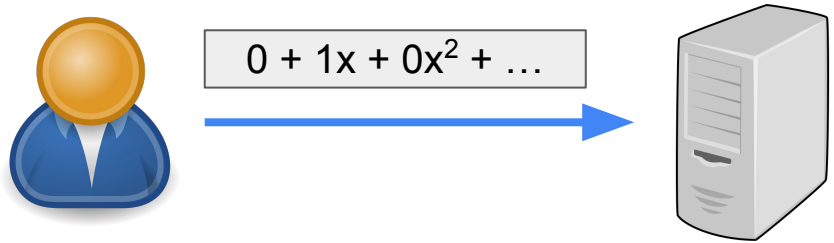
$\boxed{2} + \boxed{3} = \boxed{5}$	Addition of ciphertexts	0.002 ms
$3 \times \boxed{0} = \boxed{0}$	Multiplication of a ciphertext by a plaintext	0.14 ms

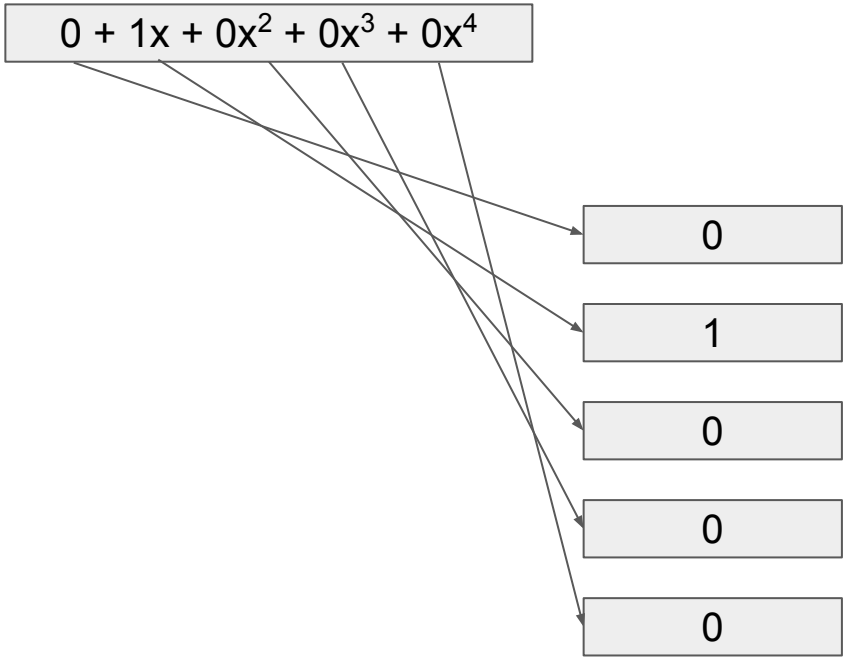
$$\boxed{x^3 + 5(x^3)^2} = \text{Sub}\left(\boxed{x + 5x^2},\ 3\right)$$

Order of magnitude cheaper than multiplying ciphertexts

Decompression

The client wants the file **2**





XPIR vs SealPIR

Costs of PIR on a database with 1 million entries (288-byte each)

	XPIR	SealPIR	Improvement
Query size	17 MB	64 KB	274x
Query generation	55 ms	3.3 ms	17x
Server processing	2.1 sec	2.24 sec	6% overhead

Conclusion

- PIR and its main application
  - Patent search
- Homomorphic Encryption
  - Additively
  - Fully
- PIR constructions
  - Trivial PIR and basic PIR protocol
  - XPIR
  - SealPIR
- Problems
  - communication complexity
  - computation complexity

Thank you for your attention!