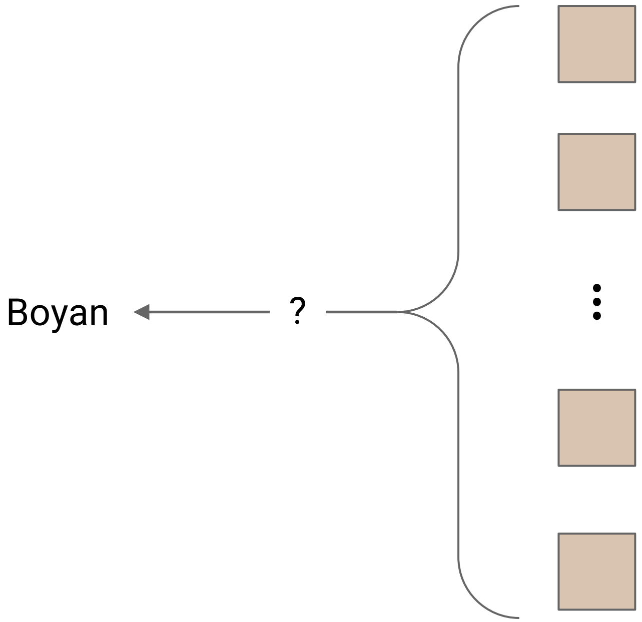
Improved Performance for Private Information Retrieval

By Boyan Litchev
Mentored by Simon Langowski

Private Information Retrieval (PIR)

The Problem

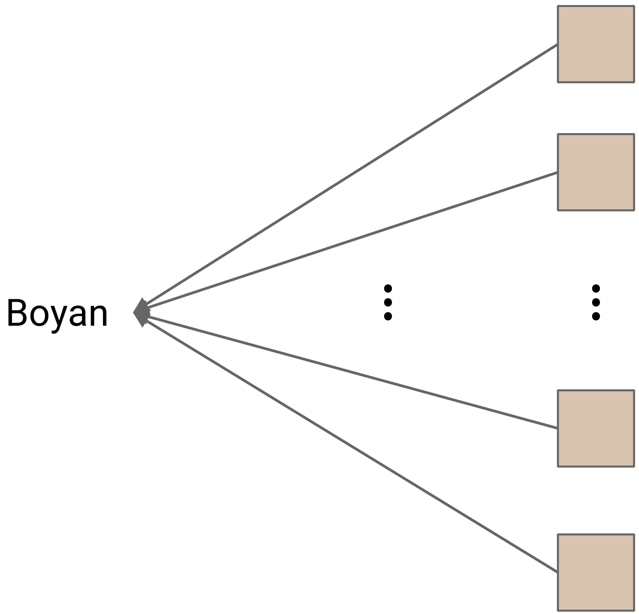
- Retrieve an item without revealing which one



Use Cases

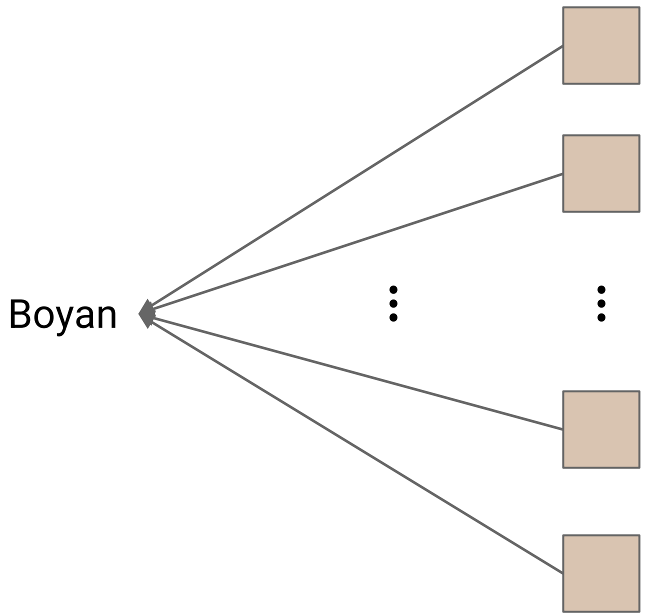
- Private Browsing
- Private Streaming
- Anonymous Messaging

A Simple Solution (1/2)



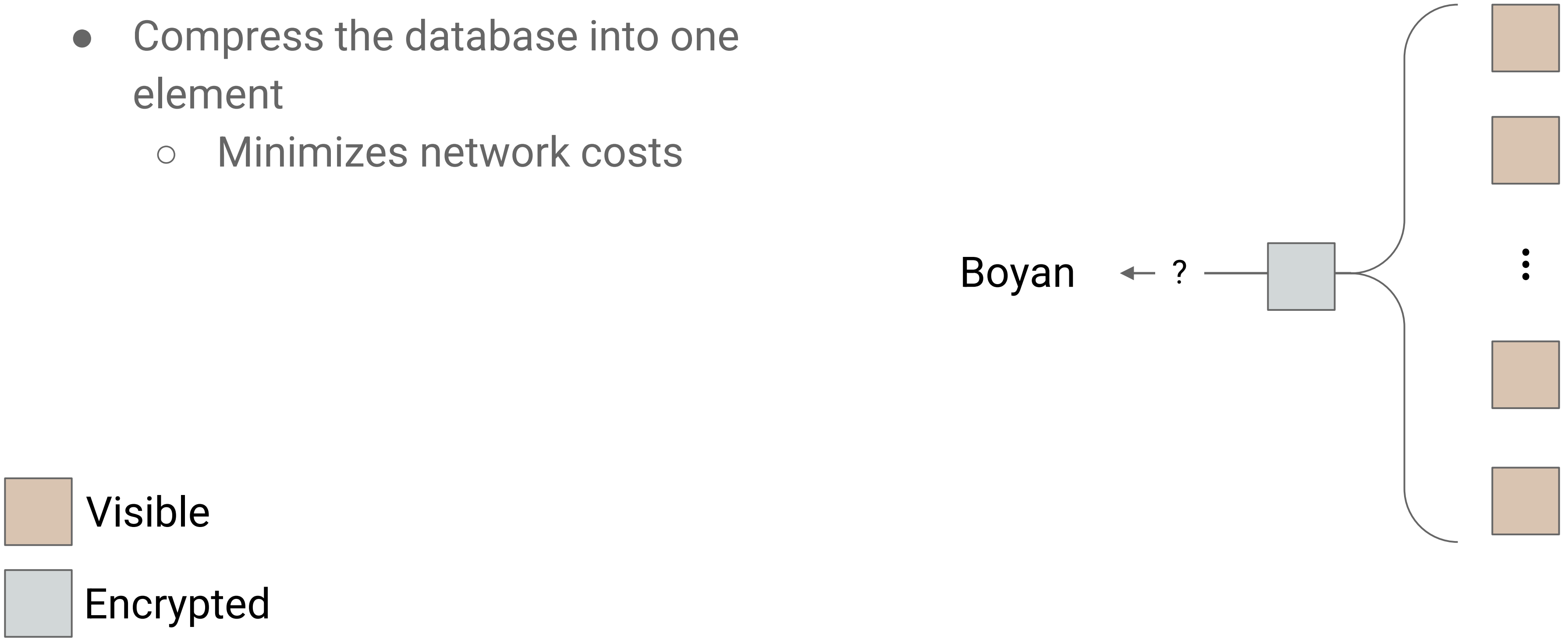
A Simple Solution (2/2)

- Network Costs are the entire database
    - Too high

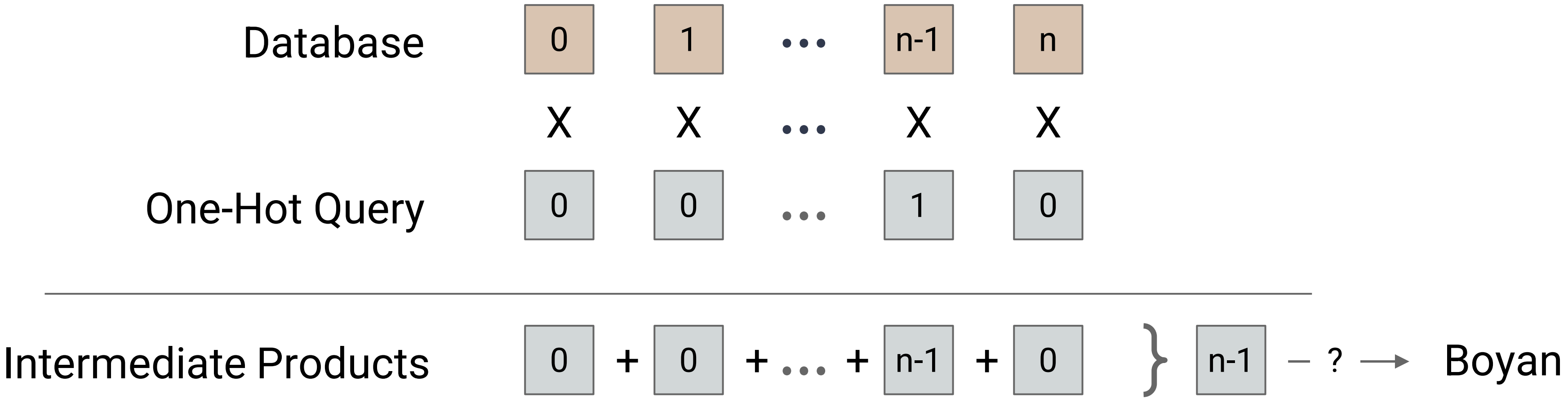


The Goal

- Compress the database into one element
  - Minimizes network costs

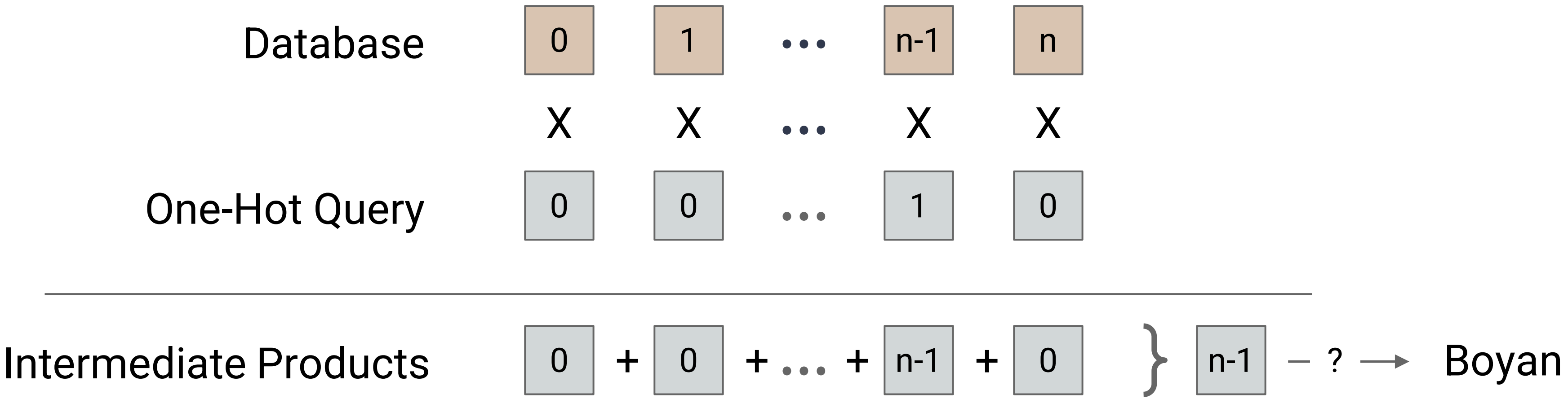


The Approach



A Note on Costs

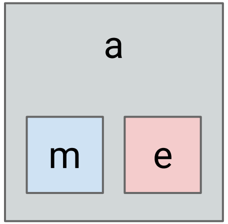
- Response is 1 element
- The query can be compressed



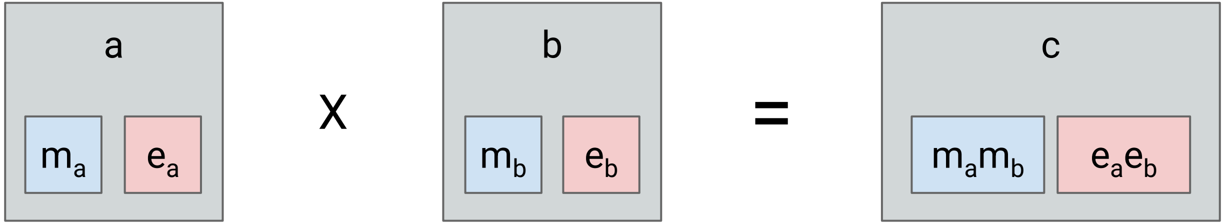
Homomorphic Encryption & Multiplications

Homomorphic Ciphertext

- A ciphertext a encodes
  - A hidden message m
  - With some error e

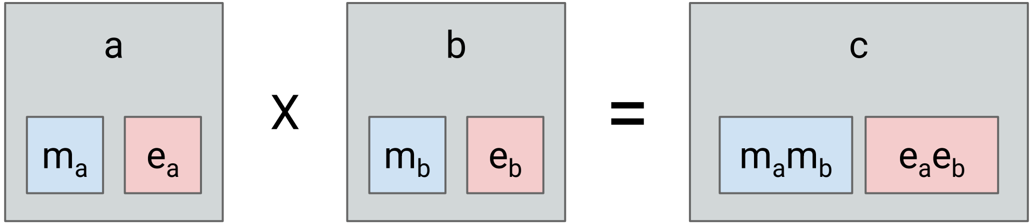


Multiplication



Multiplication

- Error scales multiplicatively
- Is very expensive



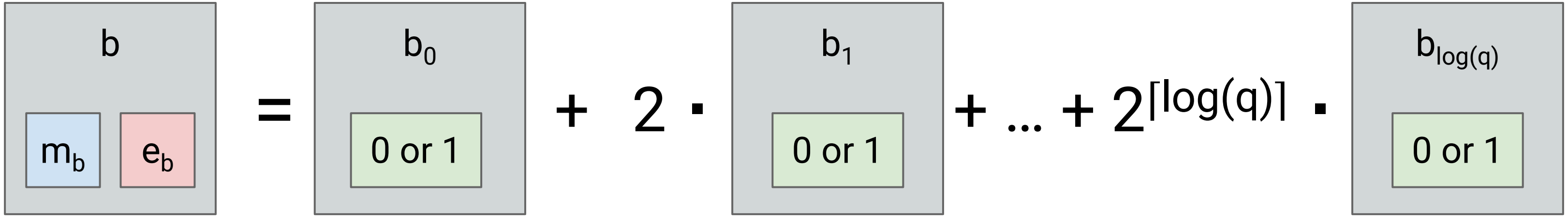
Gadget Inversions

Base-2 Gadget Inversion (1/2)

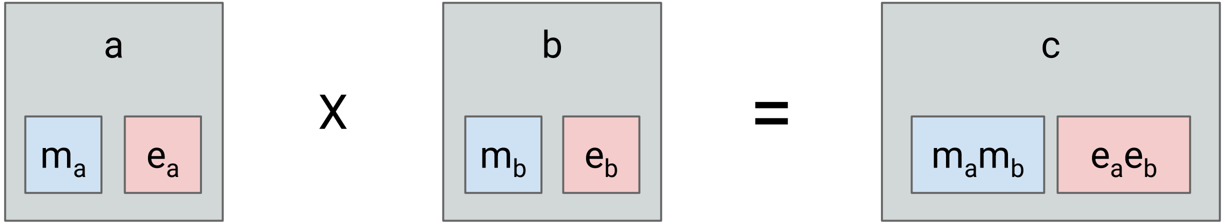
97 = 64 + 32 + 1

97 =	1	1	0	0	0	0	1

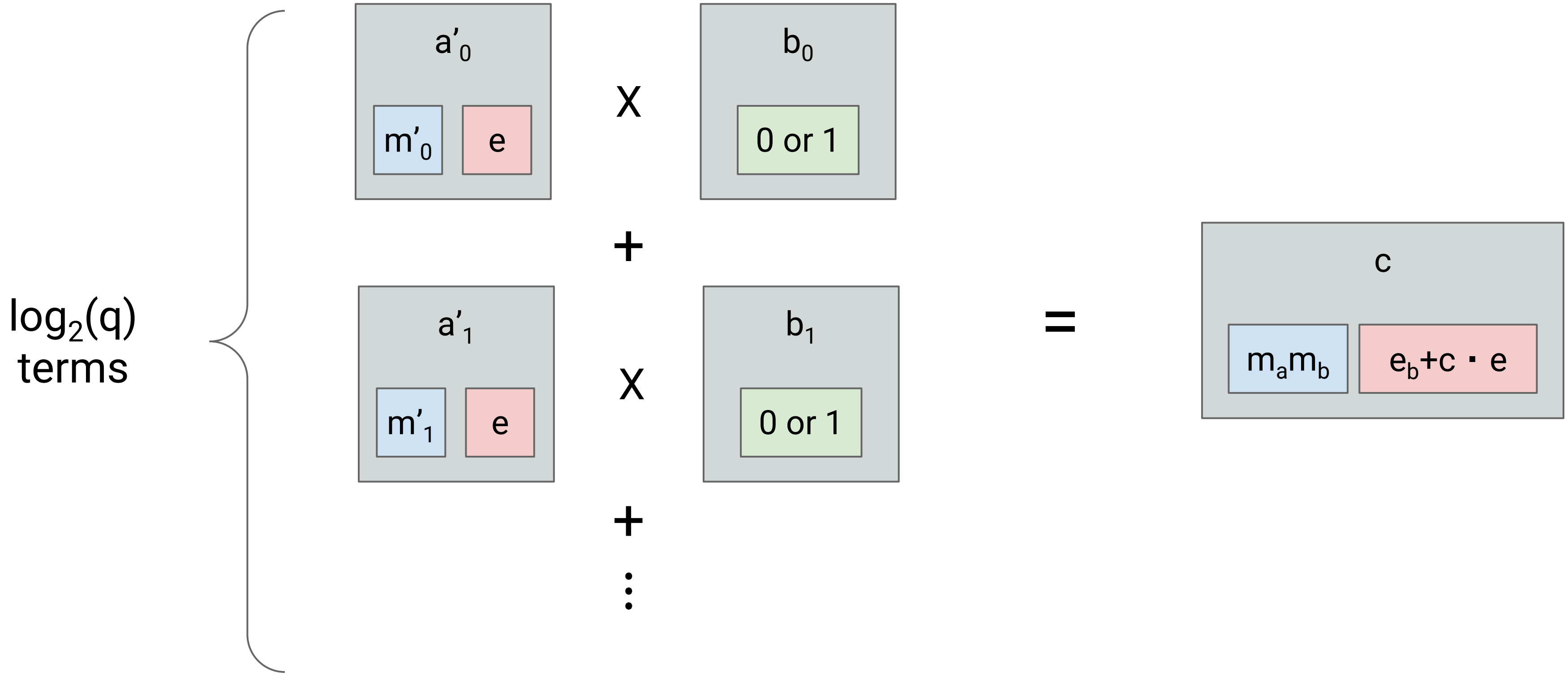
Base-2 Gadget Inversion (2/2)



Original Multiplication



Base-2 Gadget Multiplication



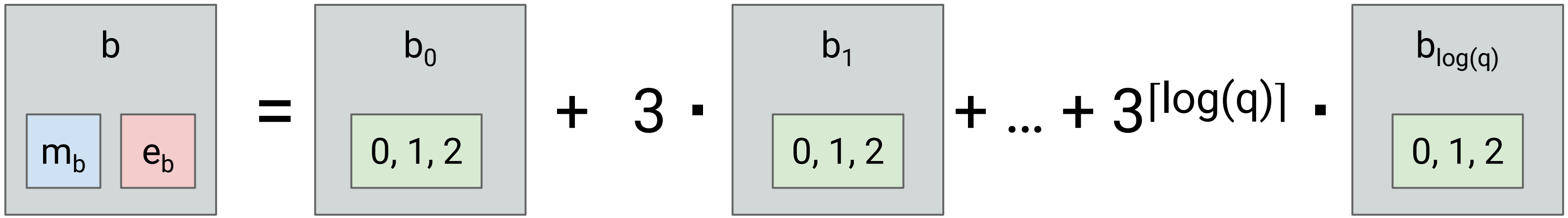
Our Work

Base-3 Gadget Inversion (1/2)

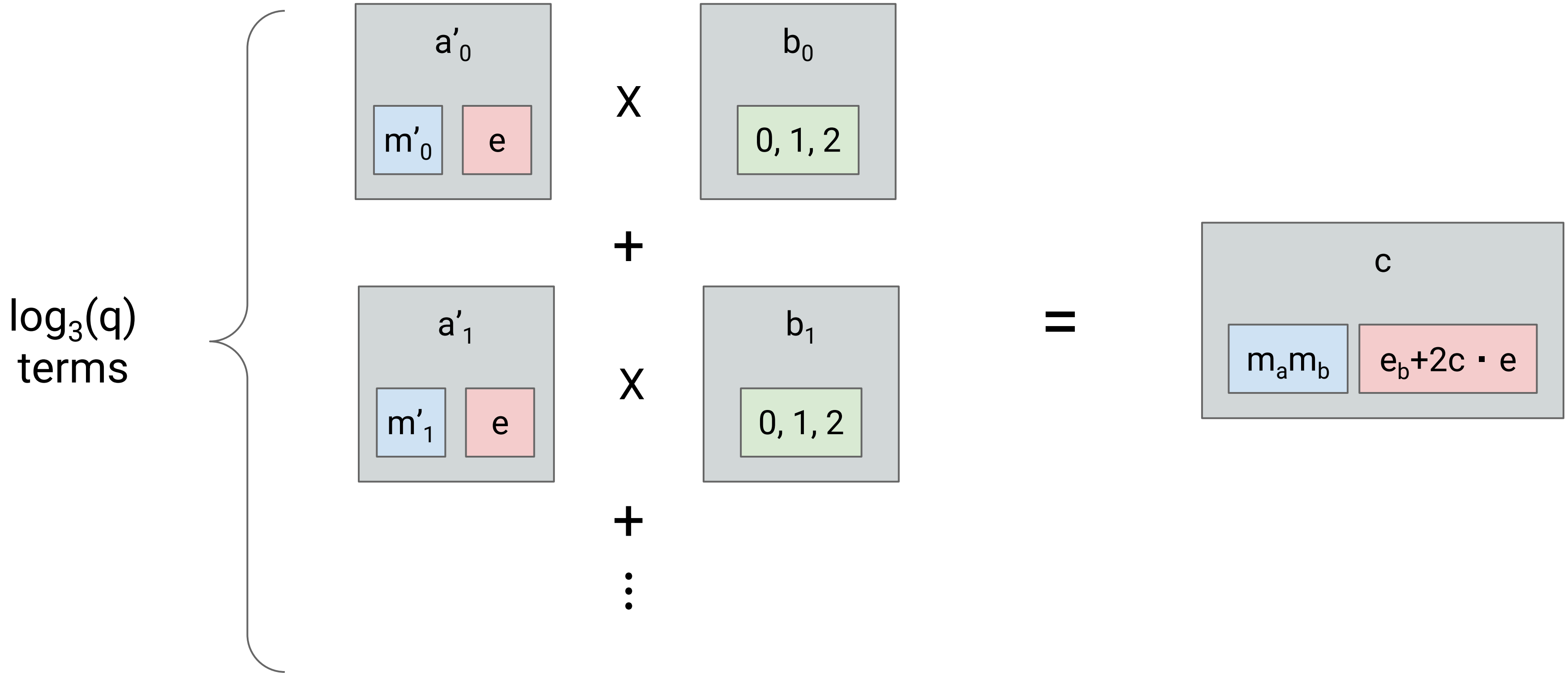
$$97 = 81 + 9 + 2 \cdot 3 + 1$$

97 =	1	0	1	2	1

Base-3 Gadget Inversion (2/2)



Base-3 Gadget Multiplication



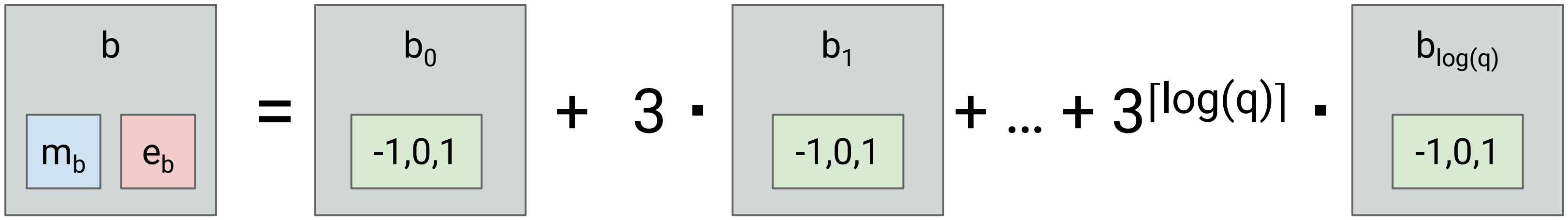
Balanced Base-3 Gadget Inversion (1/2)

97 = 81 + 27 - 9 - 3 + 1

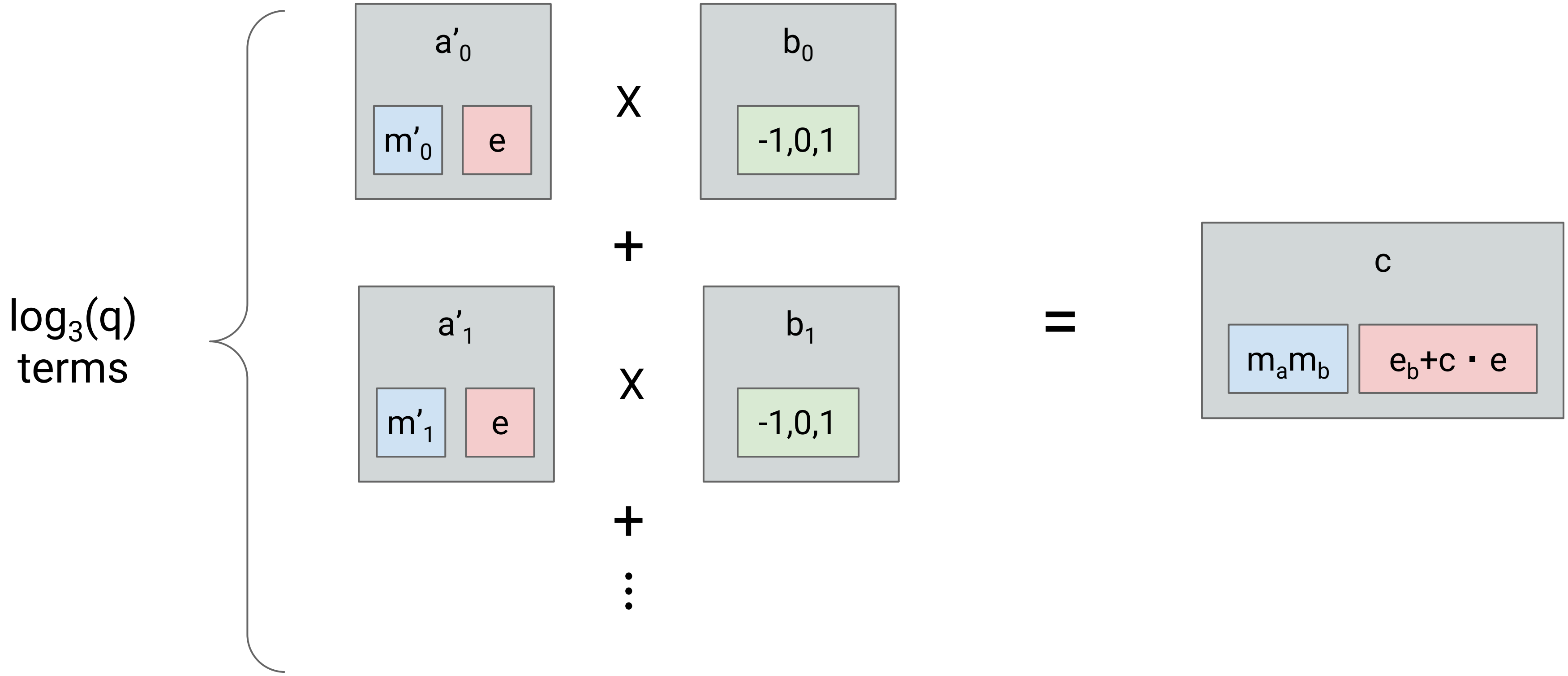
97 =

1	1	-1	-1	1

Balanced Base-3 Gadget Inversion (2/2)



Balanced Base-3 Gadget Multiplication



Preliminary Results

Per-Multiplication Costs

	Total Time (ms)	Gadget Inversion (ms)	Other Costs (ms)
Optimized Base 3	2.86		
Base 3	3.84	1.25	2.59
Base 2	5.29	0.6	4.62
Improvement	27%	-87%	44%

Future Work

- Testing Larger Databases
- Modified Parameter Sets
- Alternate Decompositions

Acknowledgments!

Thanks to my wonderful mentor Simon and MIT PRIMES for making this project possible!