

Improved Performance for Private Information Retrieval

By Boyan Litchev

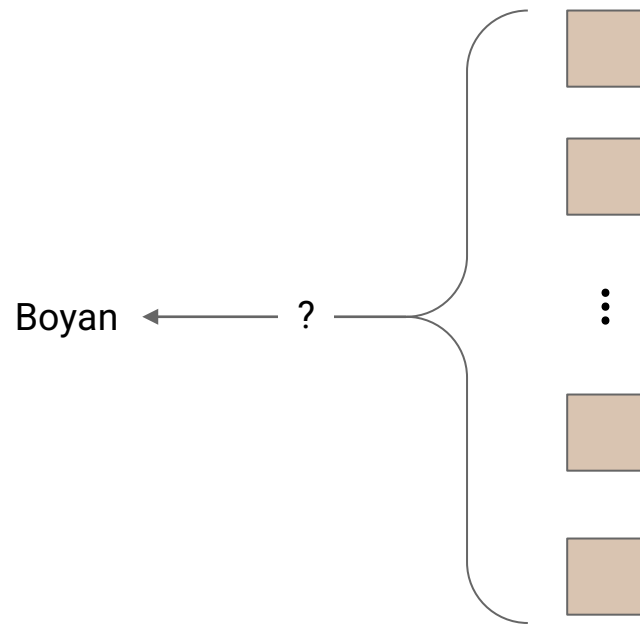
Mentored by Simon Langowski

Private Information Retrieval (PIR)



The Problem

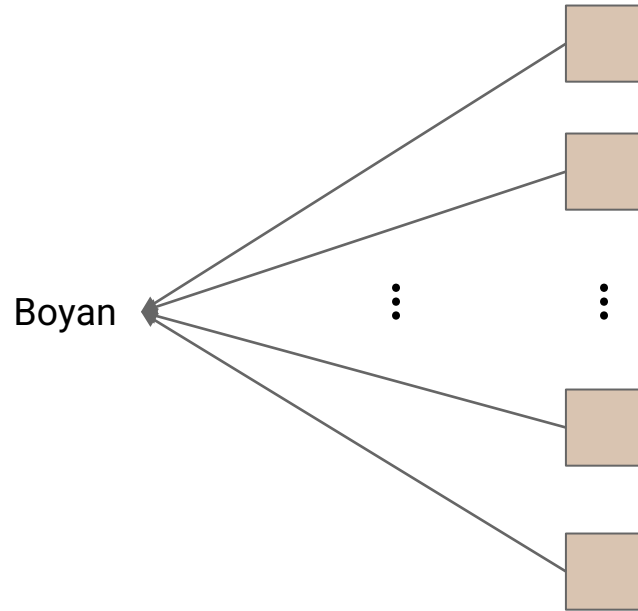
- Retrieve an item without revealing which one



Use Cases

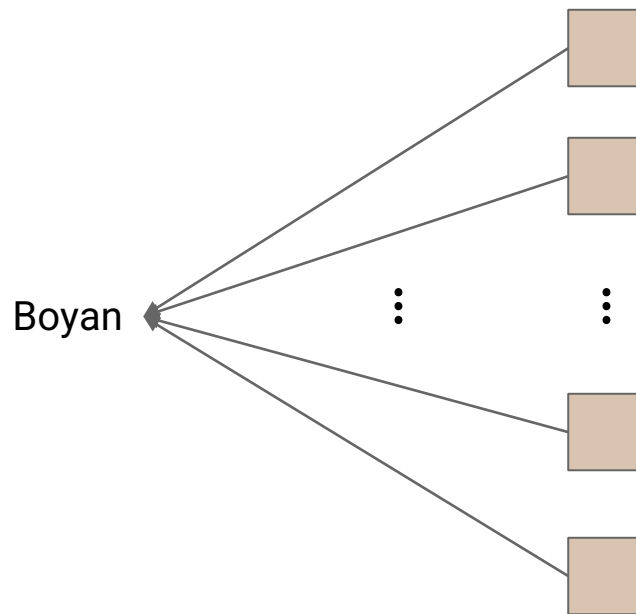
- Private Browsing
- Private Streaming
- Anonymous Messaging

A Simple Solution (1/2)



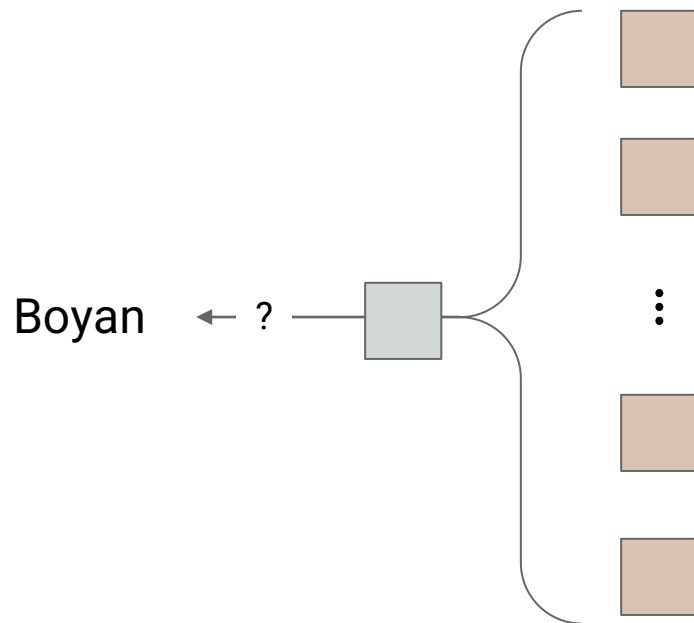
A Simple Solution (2/2)

- Network Costs are the entire database
 - Too high




The Goal

- Compress the database into one element
 - Minimizes network costs



 Visible

 Encrypted

The Approach

Database	0	1	...	n-1	n
	X	X	...	X	X
One-Hot Query	0	0	...	1	0

Intermediate Products 0 + 0 + ... + n-1 + 0 } n-1 - ? → Boyan

A Note on Costs

- Response is 1 element
- The query can be compressed

Database	0	1	...	n-1	n
	X	X	...	X	X
One-Hot Query	0	0	...	1	0

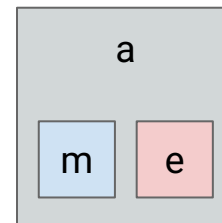
Intermediate Products 0 + 0 + ... + n-1 + 0 } n-1 - ? → Boyan

Homomorphic Encryption & Multiplications

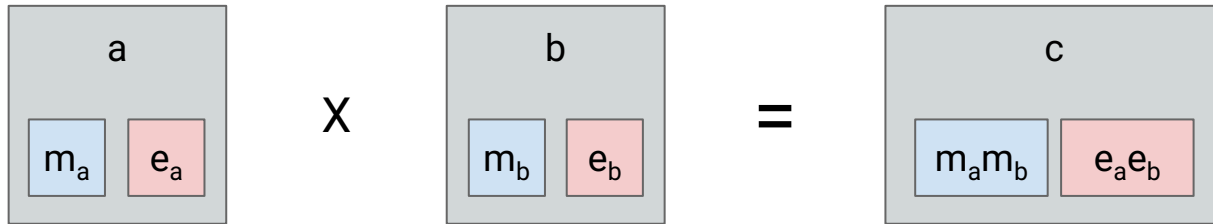


Homomorphic Ciphertext

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

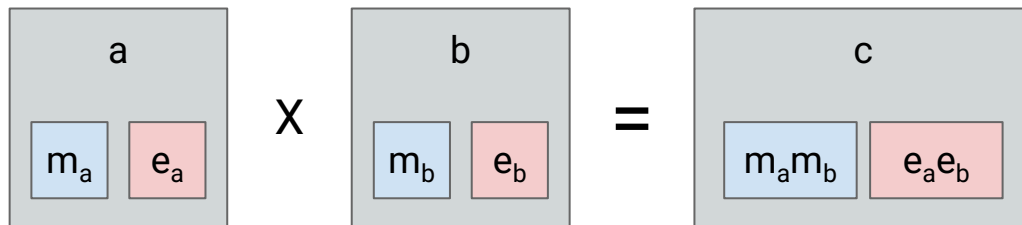


Multiplication



Multiplication

- Error scales multiplicatively
- Is very expensive



Gadget Inversions

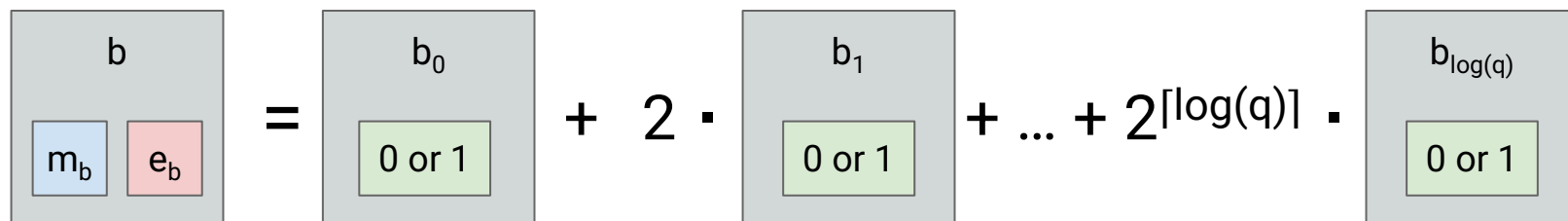


Base-2 Gadget Inversion (1/2)

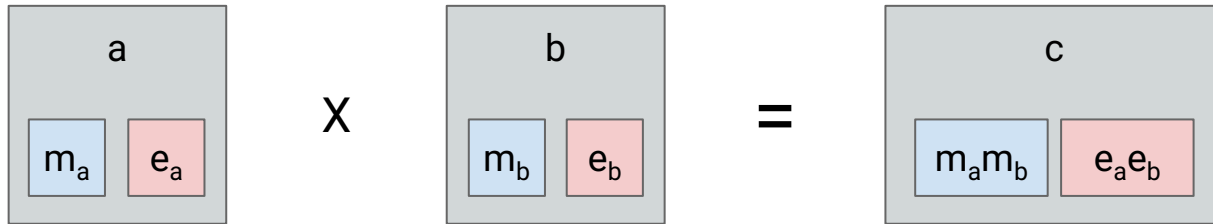
$$97 = 64 + 32 + 1$$

$$97 = \begin{array}{|c|c|c|c|c|c|c|} \hline 1 & 1 & 0 & 0 & 0 & 0 & 1 \\ \hline \end{array}$$

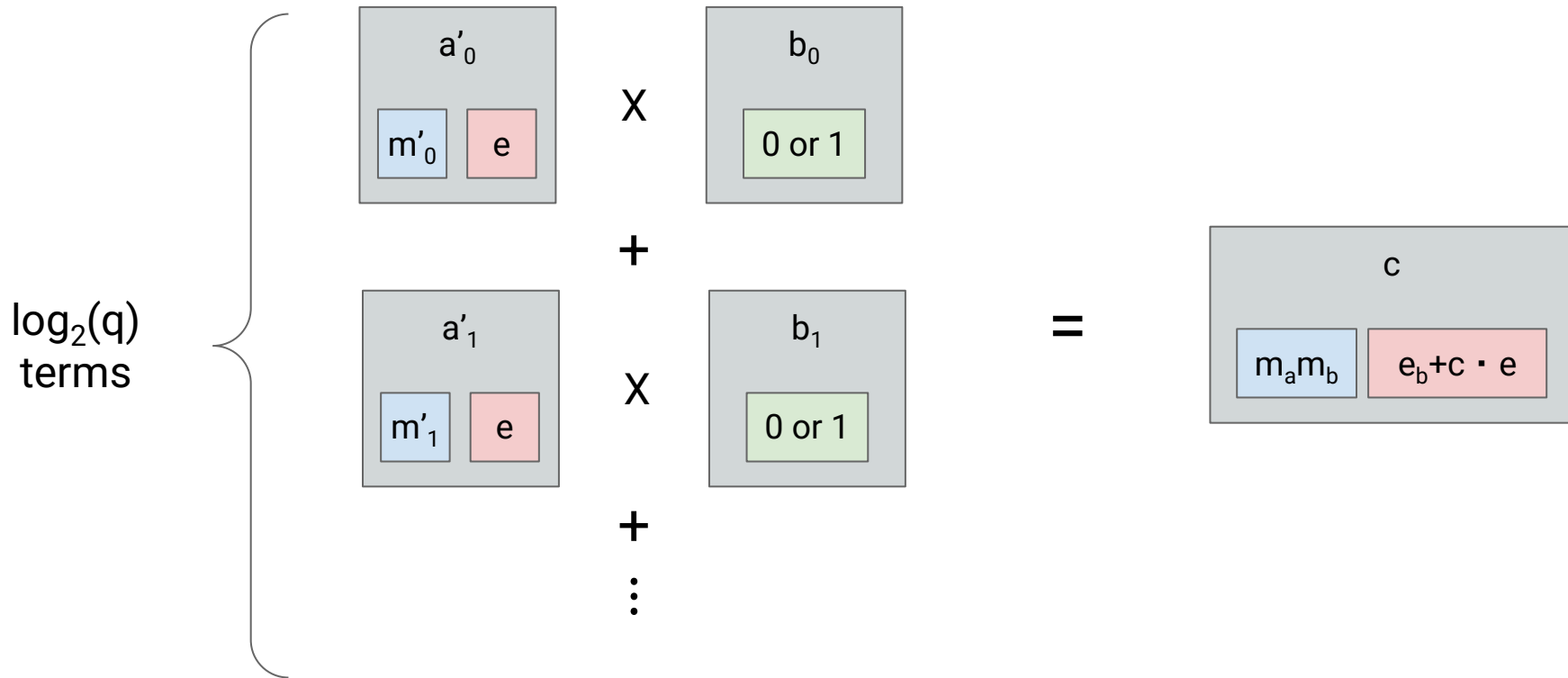
Base-2 Gadget Inversion (2/2)



Original Multiplication



Base-2 Gadget Multiplication



Our Work

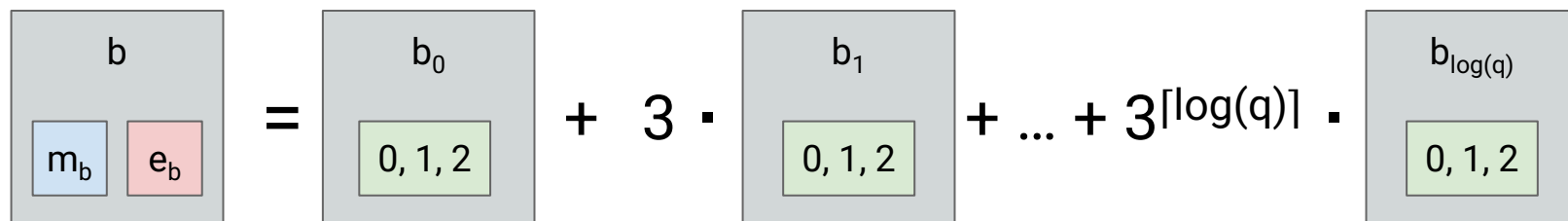


Base-3 Gadget Inversion (1/2)

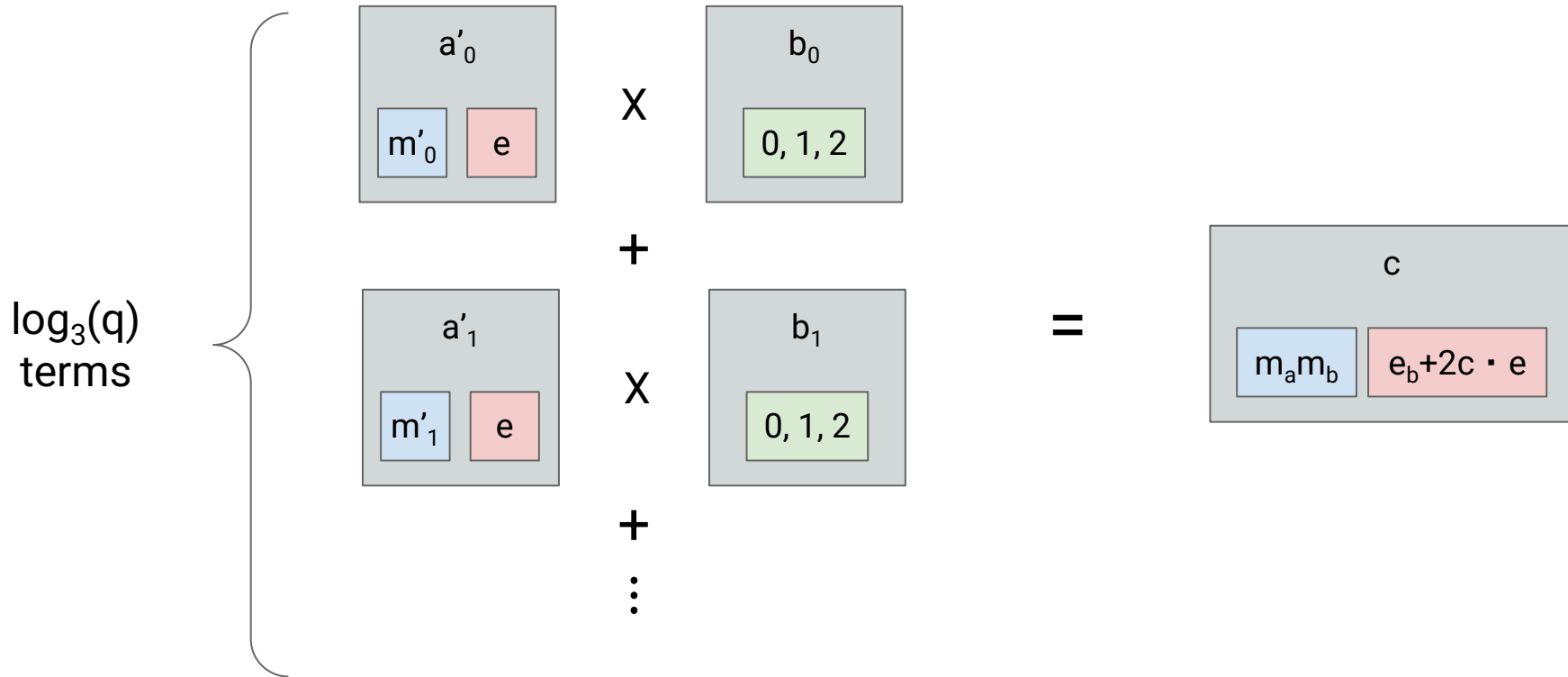
$$97 = 81 + 9 + 2 \cdot 3 + 1$$

$$97 = \begin{array}{|c|c|c|c|c|} \hline 1 & 0 & 1 & 2 & 1 \\ \hline \end{array}$$

Base-3 Gadget Inversion (2/2)



Base-3 Gadget Multiplication

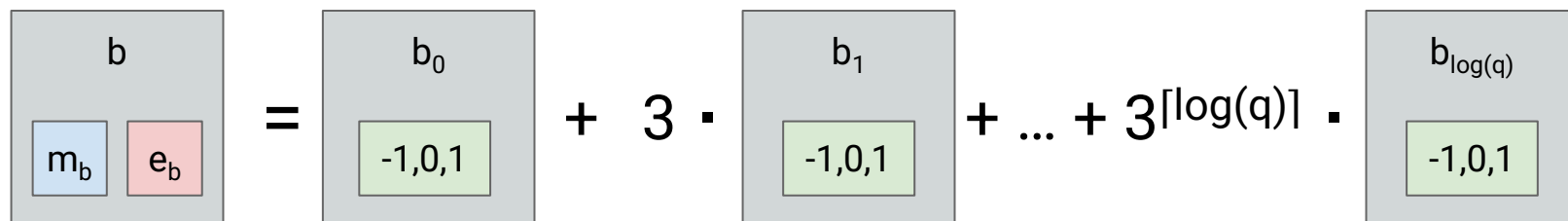


Balanced Base-3 Gadget Inversion (1/2)

$$97 = 81 + 27 - 9 - 3 + 1$$

$$97 = \begin{array}{|c|c|c|c|c|} \hline 1 & 1 & -1 & -1 & 1 \\ \hline \end{array}$$

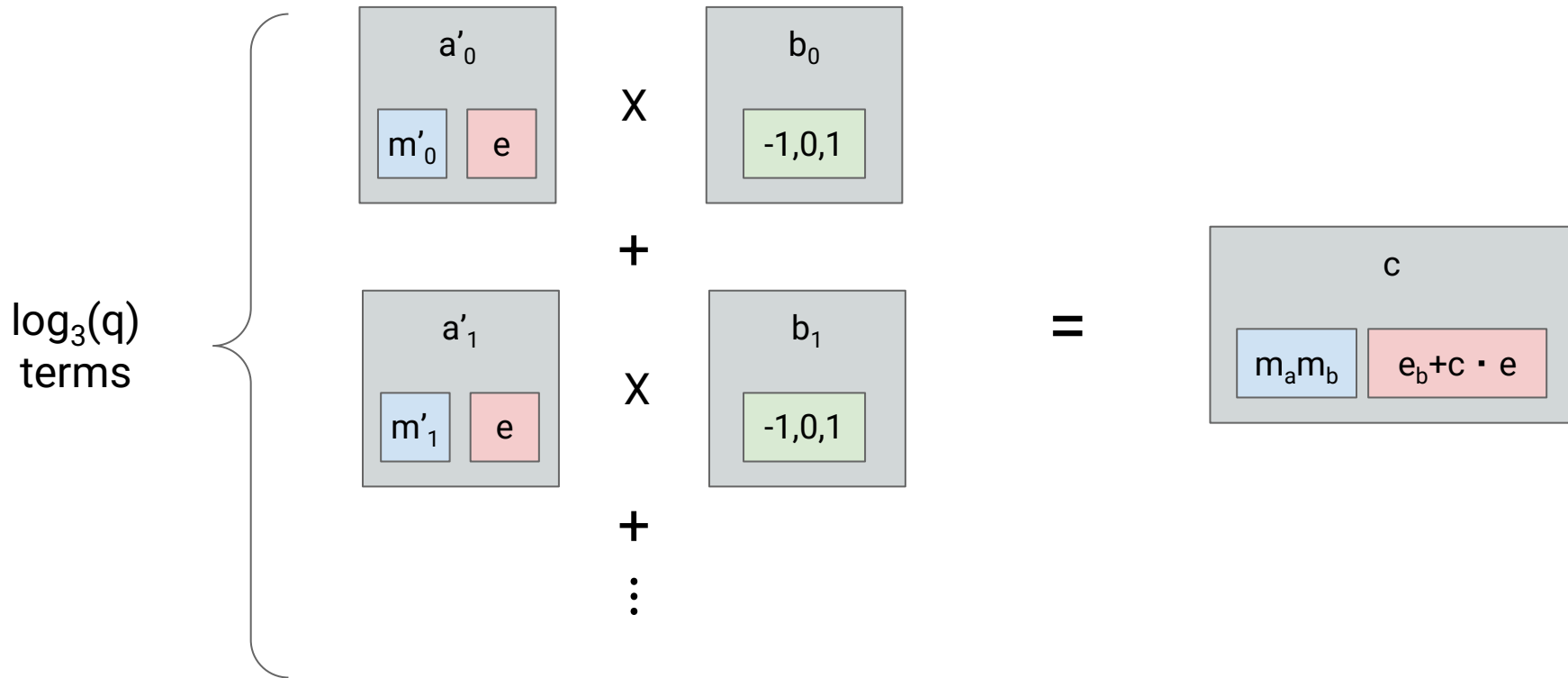
Balanced Base-3 Gadget Inversion (2/2)



The diagram illustrates the balanced base-3 gadget inversion. On the left, a gray box labeled b contains two smaller boxes: a blue one labeled m_b and a red one labeled e_b . This is followed by an equals sign. To the right of the equals sign is a sum of terms. The first term is a gray box labeled b_0 containing a green box with the values $-1, 0, 1$. This is followed by a plus sign, the number 3, a dot, another gray box labeled b_1 containing a green box with $-1, 0, 1$, another plus sign, an ellipsis, another plus sign, the number 3, a bracketed $\log(q)$, a dot, and finally a gray box labeled $b_{\log(q)}$ containing a green box with $-1, 0, 1$.

$$b = b_0 + 3 \cdot b_1 + \dots + 3^{\lceil \log(q) \rceil} \cdot b_{\log(q)}$$

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!