

Improving Latency for Secure Distributed Matrix Multiplication: Optimizing
the Secure Mat-Dot Code Algorithm
(Technical Report)

How Negative Gossip Enforces Social Conformity in Vietnamese
Communities
(Sociotechnical Research Paper)

An Undergraduate Thesis Portfolio
Presented to the Faculty of the
School of Engineering and Applied Science
In Partial Fulfillment of the Requirements for the Degree
Bachelor of Science in Computer Science

by

Tiffany Bui

May 7, 2024

Contents

Preface

Improving Latency for Secure Distributed Matrix
Multiplication: Optimizing the Secure Mat-Dot Code
Algorithm

How Negative Gossip Enforces Social Conformity in
Vietnamese Communities

Prospectus

Preface

How is system security best maintained? Where trust is low, security measures can compensate. System administrators must monitor and maintain system security.

What improvements can be made to secure distributed matrix multiplication methods to reduce latency for big data applications? Large-scale matrix multiplication is complex and costly, so it is commonly run on distributed systems for an efficient run time, but this risks data security within the matrices. Existing algorithms for Secure Distributed Matrix Multiplication include Secure Mat-Dot Code, Gap Additive Secure Polynomial Code, and Linear Code. The best algorithm was identified and selected, implemented with security measures, and optimized for efficiency. The Secure Mat-Dot Code algorithm was the best, given its flexibility and complexity. The project team implemented the solution with secret sharing, coding theory, and polynomial codes to reduce latency and keep the matrices private. On a 2048x2048 matrix, its average run time was 207 seconds. To further reduce latency and improve efficiency, the best optimization methods were multithreading, pre-calculating the computationally heavy operations, optimizing interpolation, and transposing the matrix. These modifications reduced the run time for a 2048x2048 matrix by 92.3% (207s to 16s). Implementations that would further speed up the program include removing modular arithmetic by implementing a Galois field, replacing the Vandermonde matrix with Lagrange's method, and using OpenMP instead of SHMEM.

In Vietnamese communities, how does negative gossip enforce social conformity? Gossiping can result in ostracization, loss of status, and changes in behavior for the

gossipers, the subjects of gossip, and the bystanders. In Vietnamese communities, negative gossip enforces social conformity, and despite its harm, people continue to engage in gossip culture due to its effectiveness in enforcing social norms. Gossip should never be taken as far as harming the well-being of others, but when used appropriately in a positive and truthful manner, it can be a powerful tool with social benefits that include fostering relationships and cooperation.