Sequential Half Aggregation of Lattice-Based Signatures

AMRITA VISHWA VIDYAPEETHAM – SCHOOL OF COMPUTING, CHENNAI

AMRITA VISHWA VIDYAPEETHAM
DEEMED TO BE UNIVERSITY UNDER SECTION 3 OF UGC ACT, 1956

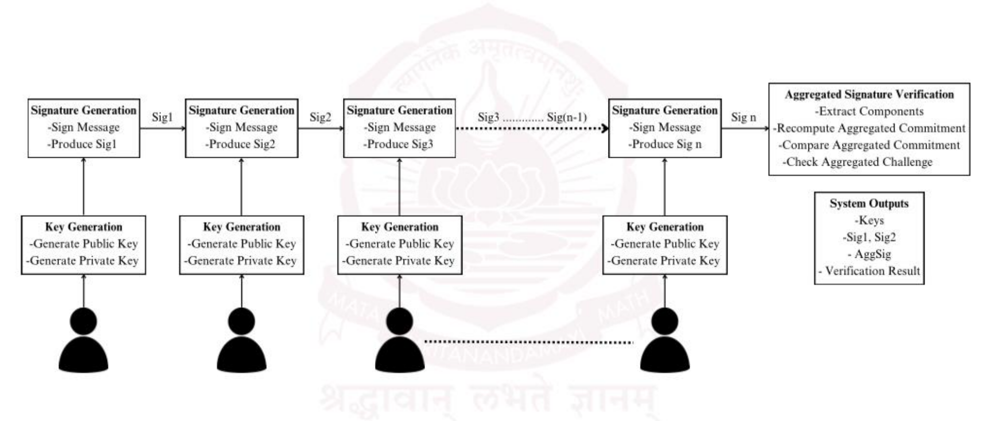
Introduction / Motivation

- Traditional communication systems are vulnerable to breaches.
- Authentication methods are often inadequate.
- Issues: scalability, latency, key management, privacy.

Problem Statement

- Need secure, efficient real-time communication.
- Develop robust authentication using lattice-based signatures.
- Address latency, key simplicity, and platform support.

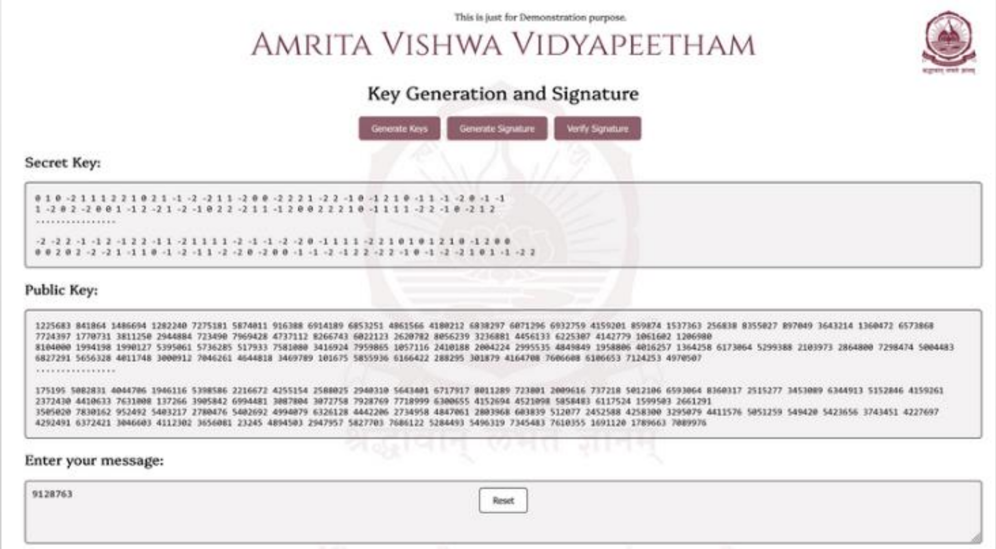
Architecture Diagram



Methodology

- User registration & login
- Key generation using lattice cryptography
- Signature generation with Half Aggregation
- Secure messaging via web sockets

Web App Snapshots



This is just for Demonstration purpose.

AMRITA VISHWA VIDYAPEETHAM

Key Generation and Signature

Secret Key:

```
0 1 0 -2 1 1 1 2 2 1 0 2 1 -1 -2 -2 1 1 -2 0 0 -2 2 2 1 -2 2 -1 0 -1 2 1 0 -1 1 -1 -2 0 -1 -1
1 -2 0 2 -2 0 0 1 -1 2 -2 1 -2 -1 0 2 2 -2 1 1 -1 2 0 0 2 2 2 1 0 -1 1 1 1 -2 2 -1 0 -2 1 2
.................

-2 -2 2 -1 -1 2 -1 2 2 -1 1 -2 1 1 1 1 -2 -1 -1 -2 -2 0 -1 1 1 1 -2 2 1 0 1 0 1 2 1 0 -1 2 0 0
0 0 2 0 2 -2 -2 1 -1 1 0 -1 -2 -1 1 -2 -2 0 -2 0 0 -1 -1 -2 -1 2 2 -2 2 -1 0 -1 -2 -2 1 0 1 -1 -2 2
```

Public Key:

```
1225683 841864 1486694 1282240 7275181 5874011 916388 6914189 6853251 4861566 4180212 6838297 6071296 6932759 4159201 859874 1537363 256838 8355027 897049 3643214 1360472 6573868
7724397 1770731 3811250 2944884 723490 7969428 4737112 8266743 6022123 2620782 8056239 3236881 4456133 6225307 4142779 1061602 1206980
8104000 1994198 1990127 5395061 5736285 517933 7581080 3416924 7959865 1057116 2410188 2004224 2995535 4849849 1958806 4016257 1364258 6173064 5299388 2103973 2864800 7298474 5004483
6827291 5656328 4011748 3000912 7046261 4644818 3469789 101675 5855936 6166422 288295 301879 4164708 7606608 6106653 7124253 4970507
.................

175195 5082831 4044706 1946116 5398586 2216672 4255154 2588025 2940310 5643401 6717917 8011289 723801 2009616 737218 5012106 6593064 8360317 2515277 3453089 6344913 5152846 4159261
2372430 4410633 7631008 137266 3905842 6994481 3087804 3072758 7928769 7718999 6300655 4152694 4521098 5858483 6117524 1599503 2661291
3505020 7830162 952492 5403217 2780476 5402692 4994079 6326128 4442206 2734958 4847061 2803968 603839 512077 2452588 4258300 3295079 4411576 5051259 549420 5423656 3743451 4227697
4292491 6372421 3046603 4112302 3656081 23245 4894503 2947957 5827703 7686122 5284493 5496319 7345483 7610355 1691120 1789663 7089976
```

Enter your message:

9128763

Objective & Scope

- Build a secure web app using lattice-based signature aggregation.
- Input: Credentials & messages
- Process: Auth using lattice-based aggregation
- Output: Secure communication
- Deliverables: Secure web app, real-time messaging

Tech Stack

- Frontend: HTML, CSS, JS
- Backend: Python
- Database: MongoDB Atlas
- Server: AWS EC2

Results / Outcome

- Quantum-resistant security
- Real-time secure messaging
- Simplified key management
- Scalable and privacy-preserving

Future Work & References

- Add blockchain-based logs
- Enable file sharing and group chats
- Cloud deployment
- GitHub: https://github.com/shanmukha-k/Real-Time-Secure-Communication using-Sequential-Half-Aggregation-of-Lattice-Based-Signatures