Dear Jasper,
Here is the copy of the Project Pitch with reference number : **00083744** submitted to the **Cybersecurity and Authentication (CA)** on **6/22/2024**.

1. Submitter Name

   Jasper Mayone

2. Submitter Email

   jasper@purplebubble.org

3. Submitter Phone

   8022793128

4. Company Name

   Purple Bubble C/O The Hack Foundation

5. State

   CA

6. Zip Code

   90069

7. Corporate Website

   https://purplebubble.org/

8. SBIR/STTR topic that best fits your projects technology area

   Cybersecurity and Authentication (CA)

9. Is this Project Pitch for a technology or project concept that was previously submitted as a full proposal by your company to the NSF SBIR/STTR Phase I Program – and was not awarded ?

   No

10. Has your company received a prior NSF SBIR or STTR award?

    No

11. Does your company currently have a full Phase I SBIR or STTR proposal under review at NSF?

    No

12. Briefly Describe the Technology Innovation?

The decentralized secure messaging protocol addresses the pressing need for enhanced privacy and security in digital communications, moving away from vulnerable centralized systems. Traditional messaging platforms risk data breaches, censorship, and surveillance due to their reliance on central servers. This protocol innovates by using a decentralized architecture, ensuring robust security and user anonymity.

Originating from the necessity to mitigate the increasing cyber threats and privacy concerns, the protocol's uniqueness lies in its design and functionality. It employs a mesh network of REST API servers, distributing control and eliminating single points of failure. This architecture ensures that even if some servers are compromised, the network remains operational and resilient.
A standout feature is the use of separate transmission (TX) and reception (RX) servers. This separation protects user anonymity by preventing the correlation of transmission and reception paths. Moreover, client messages are broadcasted to locate recipients efficiently, ensuring reliable message delivery even when the exact server location is initially unknown.
The protocol's approach to message retention and retrieval further distinguishes it. Undelivered messages are stored with a seven-day expiration, allowing clients to retrieve them later, ensuring message delivery despite temporary unavailability of recipients. RSA 2048 encryption secures messages, with signature verification preventing unauthorized access.
To maintain network integrity, the protocol includes mechanisms to detect and manage misbehaving servers, such as a reputation system and periodic audits. Decisions about server behavior are made through a quorum-based consensus, ensuring fairness and reliability.

In summary, this decentralized secure messaging protocol uniquely combines a resilient mesh network, robust encryption, and innovative anonymity measures, addressing critical privacy and security challenges in digital communications. This innovation aligns perfectly with the program's mandate to support high-impact, unproven research and development efforts, paving the way for a new era of secure messaging.

13. Briefly Describe the Technical Objectives and Challenges?

One significant technical challenge we aim to solve during the Purple Bubble project is designing a robust, user-friendly communication protocol. We will ensure encryption reliability by integrating advanced libraries and automated testing frameworks. To handle large groups (2,000-3,000 users), we will use distributed system techniques and optimize network protocols. Achieving interoperability with existing systems will involve developing compatibility layers and collaborating with other protocol developers. Creating an intuitive user interface will require user-centered design and thorough testing. To attract and retain motivated developers, we will foster a collaborative environment and offer competitive compensation. Ensuring compliance with global privacy and security regulations will involve consulting legal experts and continuous monitoring. Finally, we will promote adoption and build a vibrant community through targeted outreach and active community management. By tackling these challenges, we aim to deliver a technically superior and widely accepted communication protocol.

14. Briefly Describe the Market Opportunity?

The market opportunity for Purple Bubble lies in meeting the critical need for secure, reliable, and user-friendly communication, an area where existing protocols often fall short. Our primary customers include everyday individuals and small to medium-sized organizations increasingly concerned about privacy and security. These users might not have deep technical expertise but recognize the importance of secure communication and are frustrated with the fragmentation and encryption issues in current solutions like the Matrix protocol.

A significant pain point is the inconsistency and unreliability of encryption in existing communication platforms, often leading to security breaches and compromised data. Users want a communication tool that provides robust, default encryption without requiring extensive configuration or technical know-how. Additionally, the fragmented nature of current protocols results in a disjointed user experience, causing frustration and inefficiencies.
Organizations, in particular, need a scalable solution that seamlessly handles both large group communications and personal chats. They also require interoperability with existing systems to ensure a smooth transition and integration without disrupting their current operations.

Purple Bubble addresses these pain points by offering a unified communication standard that integrates advanced encryption libraries and automated testing frameworks to ensure reliability. Our protocol's focus on user-centered design makes it accessible to non-technical users, while its scalability and interoperability meet the needs of organizations. By solving these critical issues, Purple Bubble is poised to capture a significant market share, providing a superior alternative to existing communication protocols.

15. Briefly Describe the Company and Team?

Purple Bubble, a project under the fiscal sponsor of The Hack Foundation, was founded by a group of teenagers who want to change the way we think about messaging and communication. For too long, messaging apps have been restricted to work best with their own products and user bases, creating a fragmented ecosystem that alienates users. Our goal is to change that by building a new protocol from the ground up—one that communicates securely and unobtrusively. This open protocol is designed not only for one-on-one communication, but also to scale from small businesses to large companies.
Although we may lack the experience of established companies, we consider this our superpower. Approaching this challenge with fresh perspectives, starry eyes, and unwavering optimism, we passionately aim to transform a small slice of the world, one seamless communication at a time.

16. How did you first hear about our program?

`General web search or social media advertisement`

NSF SBIR/STTR Phase I Eligibility Information:
In addition to receiving an invitation to submit a full proposal from the NSF SBIR/STTR Phase I Program based upon the review of their submitted Project Pitch,potential proposers to the program must also qualify as a small business concern to participate in the program (see SBIR/STTR Eligibility Guidefor more information).
The firm must be in compliance with the SBIR/STTR Policy Directive(s) and the Code of Federal Regulations (13 CFR 121).

- Your company must be a small business (fewer than 500 employees) located in the United States. Please note that the size limit of 500 employees includes affiliates.
- At least 50% of your company's equity must be owned by U.S. citizens or permanent residents, and all funded work needs to take place in the United States (including work done by consultants and contractors).
- Primary employment is defined as at least 51 percent employed by the small business. NSF normally considers a full-time work week to be 40 hours and considers employment elsewhere of greater than 19.6 hours per week to be in conflict with this requirement.
- The Principal Investigator needs to commit to at least one month (173 hours) of effort to the funded project, per six months of project duration.

For more detailed information, please refer to the SBIR/STTR Eligibility Guide by using https://www.sbir.gov/sites/default/files/elig_size_compliance_guide.pdf. Please note that these requirements need to be satisfied at the time an SBIR/STTR award is made, and not necessarily when the proposal is submitted.