Private Anonymous Messaging

Ruchith Fernando, Bharat Bhargava
Department of Computer Science & The Center for Education and Research in Information Assurance and Security
Purdue University

Secret Agents of intelliOrg

Message sent to the only available agent

The organization is no longer accessible and other agents need the message

Requirements

• Dynamic set of agents
• Agents do not know each other
• Obtain messages from other agents
• Use public network
• Requester and provider anonymity

Hierarchical Identity Based Encryption

Proposed Scheme

• Select a random = \( I_r \)
• \( ID_r = h_1^{I_1} \cdot h_2^{I_2} \cdot h_3^{I_3} \)
• \( ID_r \) is the request for data

Group Membership Changes

Master key = \( K \)

\( K_{priv(Agent)} = (g_2^{K'} \cdot (A^r), B^r, C^r) \)

Generate a fresh master key = \( K' \)

Regenerate \( K_{priv(Agent_i)} \) of all agents

Publish \( r' \) & \( r' \)

Use \( r' \) to create key to look up and locate \( g_2^{K'} \cdot (A^r) \) component and update private key!