INTRODUCTION

- **PROBLEM UNDER STUDY:** Developing a dynamic public key infrastructure that allows a set of members to generate and maintain group keys without an external third party member. The private keys are generated as a composition of the private keys of the members without exposing the individual private keys. This work focuses on the Elgamal Keys.

- **APPLICATIONS:** Any secure group communication that may require group non-repudiation as well as individual member non-repudiation. A group of members that have the same binding ability such as a group of members permitted to sign digital certificates.

- **MODEL ASSUMPTIONS:** Members are not at the same trust level and are mutually suspicious. There is a trusted third party that can generate the initial pads and the group binding parameter. Each member is assumed to have an individual public key pair with the public key being available to anyone.

- **RELATED WORK:** This work is based on our previous work on “A Shared Key Generation Using Fractional Keys”

- **SPONSORS:** ARL FED LABS, and INFOSEC group of NSA
PROPOSED APPROACH

• INITIALIZATION
  • Third party based initialization
    • A trusted third party chooses a set of different initial pads, and computes the initial group binding parameter as a composition of the initial pads.
    • Each member is given a unique initial pad and the initial common group binding parameter.
  • Distributed initialization
    • Please see the accompanying slide

• GROUP KEY GENERATION FOR ITERATION STEP J (j>=1)
  • Individual members generate their public key pair
  • Members Publish their public component
  • Members add the current individual pad to their private key to generate the hidden private key - same as the hidden fractional key
  • Each member locally combines the hidden private keys received from all the members to obtain the hidden group private key.
  • Each member then uses the dynamic group binding parameter to remove the combined effect of the pads.
  • Each member computes its individual pads by modifying the new group binding parameter.
DISTRIBUTED INITIALIZATION

\[
\delta_n = \delta_{n-1} \oplus v_{n,1}
\]

\[
\theta_1 = \delta_n \oplus (-\gamma)
\]

\[
\delta_i = \delta_{i-1} \oplus v_{i,1}
\]

\[
\delta_1 = \gamma \oplus v_{1,1}
\]
SCHEMATIC DIAGRAM AT ITERATION J

\[
\begin{align*}
&\alpha_{i,j} \\
&\theta_j \\
&\text{iteration } j \\
&0 \quad 1 \quad 2 \quad 3 \quad 4
\end{align*}
\]
SHARED SECRET UPDATE FORMULAE AT ITERATION J

All the operations are with respect to modulo p

Member i Generates: \( FK_{i,j} \)

Computes & Exchanges: \( HFK_{i,j} = FK_{i,j} \oplus a_{i,j} \)

Combines \( \left( \sum_{i=1}^{n} \oplus HFK_{i,j} \right) = \left( \sum_{i=1}^{n} \oplus FK_{i,j} \right) \oplus (n-1)\theta_{j-1} \)

\( = (n-1)\theta_{j-1} \oplus \theta_{j} \)

New binding \( \theta_{j} = (p-n-1)\theta_{j-1} \oplus (n-1)\theta_{j-1} \oplus \theta_{j} \)

New dynamic pad = \( \theta_{j} \oplus FK_{i,j} \)