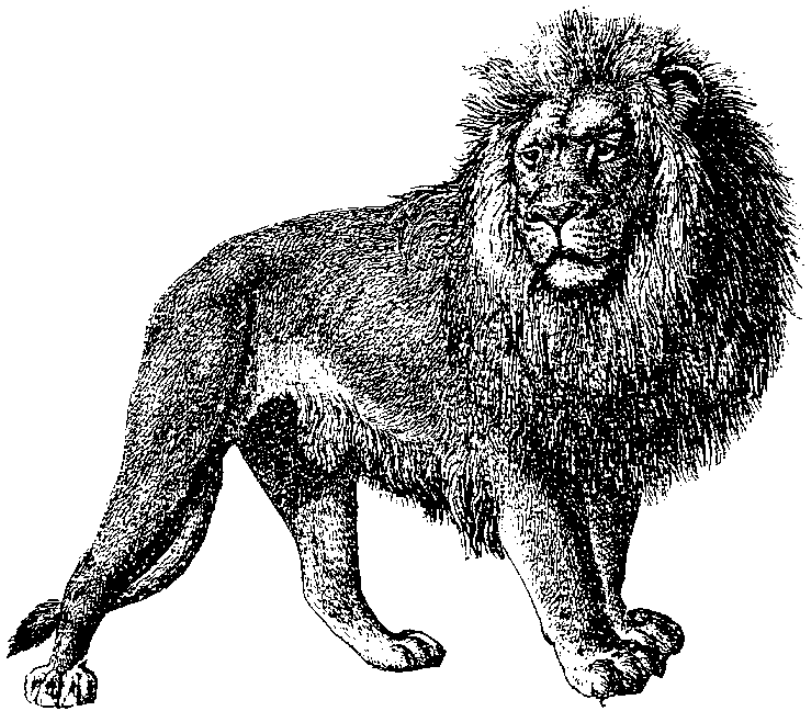
99-02

Proceedings of the 1999 IEEE Information Theory and Communications Workshop

Kruger National Park
South Africa



June 20 - 25, 1999

EDITORS:
Francis Swarts
Jacobus Swarts

IEEE CATALOG NUMBER: 99EX253

IEEE

A Private Scheme for Distributed, Shared Secret Generation

R. Poovendran, M. S. Corson, J. S. Baras[1]
Institute for Systems Research
University of Maryland
College Park, MD 20742, USA
{radha, corson, baras}@isr.umd.edu

Abstract — **We present a scheme for shared secret generation by n members that combines the contributions the members in a fashion such that the individual contribution of each member is not exposed to anyone—including the other members. We note that for an external attacker trying to break the n L-bit secrets of the members, the effective search space dimension is nL, meaning that all n keys must be broken *simultaneously* in order to crack system integrity. We also note that the scheme provides "Unconditional Secrecy" [1].**

I. INTRODUCTION

We present a scheme that allows a group of n mutually suspicious members to iteratively generate a shared secret sequence $\theta_j, j = 1 \ldots$ without exposing their individual contributions. At update step j, a member i (a) generates its "Fractional Share", denoted $FK_{i,j}$, (b) then adds a precomputed and member-specific dynamic, one-time pad, denoted $\alpha_{i,j}$, to its $FK_{i,j}$, and generates its "Hidden Fractional Share", denoted $HFK_{i,j}$, (c) then securely sends its HKF to all n group members, (d) then adds all n HFK's together and computes a new "group binding parameter" θ (which is still padded), (e) then removes the effect of combined pads using the group binding parameter from the previous step, and (f) then updates the new one-time pads. All computations are performed under group addition modulo p.

II. DESCRIPTION OF THE SCHEME

The scheme consists of a group initialization phase followed by an iterative group computation. The scheme assumes that *all* initial pads are generated i.i.d. and uniform. All $FK_{i,j}$ are also i.i.d. and uniform, and are mutually independent of all the initial pads. The computational steps involved in the scheme are first described below.

As a result of the initialization phase, which may be third party controlled or distributedly executed, n members are selected and each member $i; 1 \leq i \leq n$ is given $\alpha_{i,1}$ such that $\sum_{l=1}^{l=n} \alpha_{l,1} = \theta_1$, where $\theta_j; 1 \leq j$ is the group binding parameter at update step j.

During the iterative computation, the local computational steps of member i for iteration i are:

1. Generate $FK_{i,j}$
2. Compute $HFK_{i,j} = FK_{i,j} + \alpha_{i,j}$.
3. Securely send $HFK_{i,j}$ to *all* members of the group.
4. Using *all* HFK received at update step j, compute $\sum_{i=1}^{i=n} HFK_{i,j} = \sum_{i=1}^{i=n} (\alpha_{i,j} - FK_{i,j}) = \lambda_1\theta_j + \theta_{j+1}$ with $\theta_{j+1} = \sum_{i=1}^{i=n} FK_{i,j}$, $\lambda_1 = 1$, and $\lambda_{j>1} = (n-1)$.
5. Locally compute the *new* group binding parameter θ_{j+1} using, $\theta_{j+1} = \sum_{i=1}^{i=n} HFK_{i,j} + \mu_j\theta_j = \lambda_j\theta_j + \theta_{j+1} + \mu_j\theta_j$, where $\mu_1 = (p-1)$, and $\mu_{j>1} = (p-n+1)$.
6. Locally compute the *new* individual one time pad as $\alpha_{i,j+1} = \theta_{j+1} + \mu_j FK_{i,j}$, where $\mu_1 = (p-1)$, and $\mu_{j>1} = (p-n+1)$.

III. MAIN RESULTS

The proposed scheme can provide the following secrecy properties as long as the initial pads and *all* the fractional shares are i.i.d. and uniform: (a) for an external attacker, even the knowledge of all n hidden fractional keys does not directly permit computation of the group binding parameter and the individual members' shares, and (b) the search space is the same for an outside attacker or a group member who is trying to obtain the $FK_{i,j}$ of a member i from the knowledge of $HFK_{i,j}$. These claims arise from the following observations:

1. Since the initial pads $\alpha_{i,1}$ are i.i.d. and uniform, θ_1 is also uniformly distributed and mutually independent of each $\alpha_{i,1}$, i.e. for a given $\alpha_{i,1}$, $I(\alpha_{i,1} \wedge \theta_1) = 0$.
2. At the j-th iteration, since the $FK_{i,1}$'s are chosen as i.i.d., uniform and independent of *all* initial pads $\alpha_{i,1}$, the following *Perfect Secrecy*[2] conditions hold:
   (a) each $HFK_{i,j}$ is uniformly distributed and $I(HFK_{i,1} \wedge FK_{i,1}) = 0$ and $I(HFK_{i,1} \wedge \alpha_{i,1}) = 0$,
   (b) $I(FK_{l,j} \wedge \alpha_{i,1}) = 0, \forall l$,
   (c) $I(FK_{l,j} \wedge FK_{i,m}) = 0, \forall i \neq l, j \neq m$,
   (d) θ_j is uniformly distributed and $I(\theta_j \wedge FK_{i,j}) = 0, \forall i$, i.e. knowledge of the group binding parameter θ_j alone does give any knowledge about $FK_{i,j}$.
   (e) $\alpha_{i,j}$ is uniformly distributed and $I(FK_{i,j} \wedge \alpha_{i,j}) = 0$ and $I(\theta_j \wedge \alpha_{i,j}) = 0$,
   (f) $I(HKF_{l,j} \wedge \alpha_{i,j}) = 0$; for all i, l, i.e. knowledge of *all* hidden fractional keys at iteration j does not give any knowledge about the dynamic padding.

Additionally, the scheme can be shown to be collusion resistance as long as the number of colluding members is less than $(n-1)$. The method is also robust against self-secret revealing members as long as the number of such members is less than $(n-2)$.

[1]This work was supported in part by grants from ARL and LUCITE program of NSA

REFERENCES

[1] A. J. Menezes, P. C. van Oorschot and S. A. Vanstone, "Handbook of Applied Cryptography," 1st edition, CRC Press, New York, 1997.

[2]An encryption scheme E using key K is said to have *Unconditional or Perfect Secrecy* [1] if the cipher C corresponding to plain text m satisfies $I(C \wedge m) = 0$.

0-7803-5268-8/99/$10.00 ©1999 IEEE