International Journal of Pure and Applied Mathematics
Volume 85 No. 5 2013, 933-937
ISSN: 1311-8080 (printed version); ISSN: 1314-3395 (on-line version)
url: http://www.ijpam.eu
doi: http://dx.doi.org/10.12732/ijpam.v85i5.11

SECURE SCHEMES FOR SECRET SHARING AND KEY DISTRIBUTION USING PELL'S EQUATION

P. Muralikrishna[1] [§], S. Srinivasan[2], N. Chandramowliswaran[3]

[1,2]School of Advanced Sciences
VIT University
Vellore, 632014, Tamilnadu. INDIA

[3]Visiting Faculty
Indian Institute of Management Indore
Indore, 453 331, INDIA

Abstract: A key distribution scheme for dynamic conferences is a method by which initially an trusted server distributes private individual pieces of information to a set of users. Later each member of any group of users of given size can compute a common secure group key. In this setting any group of t users can compute a common key by each user computing using only his private initial piece of information and the identities of the other $t-1$ users in the group. Keys are secure against coalition of to k users, that is, even if k users pool together their pieces they cannot compute anything about a key of any t-size conference comprised of other users. In this paper, we introduce an algorithm for such perfectly secure scheme by using Pell's equation.

1. Introduction

Key distribution is a central problem in cryptographic systems, and major component of the security subsystem of distributed systems, communication systems, and data networks. Secret sharing was invented independently by Adi Shamir [3] and George Blakley [1] in 1979. Secret sharing schemes are ideal for storing information that is highly sensitive and highly important. If

Received: April 15, 2013

[§]Correspondence author

users of a group wish to communicate using symmetric encryption, they must share a common key. A secure secret sharing scheme distributes shares so that anyone with fewer than t shares has no extra information about the secret than someone with 0 shares. Recently, in [4], we discussed a secure secret key sharing algorithm using non-homogeneous equation. In this paper, we give an algorithm for such perfectly secure scheme by using *Pell's equation.*

2. Main Results

In this section we give key distribution problem and algorithm. The proposed system involves a design of a pre-distribution algorithm using a deterministic approach. Deterministic approach is the process of determining the keys before placing them within the network. A key pre-distribution algorithm using number theory with high connectivity, high resilience and memory requirements is being designed by implementing a deterministic approach. In [5], the Pell's equation of the number theory is used in the generation of the key chain.

Construction and Algorithm for Key Sharing

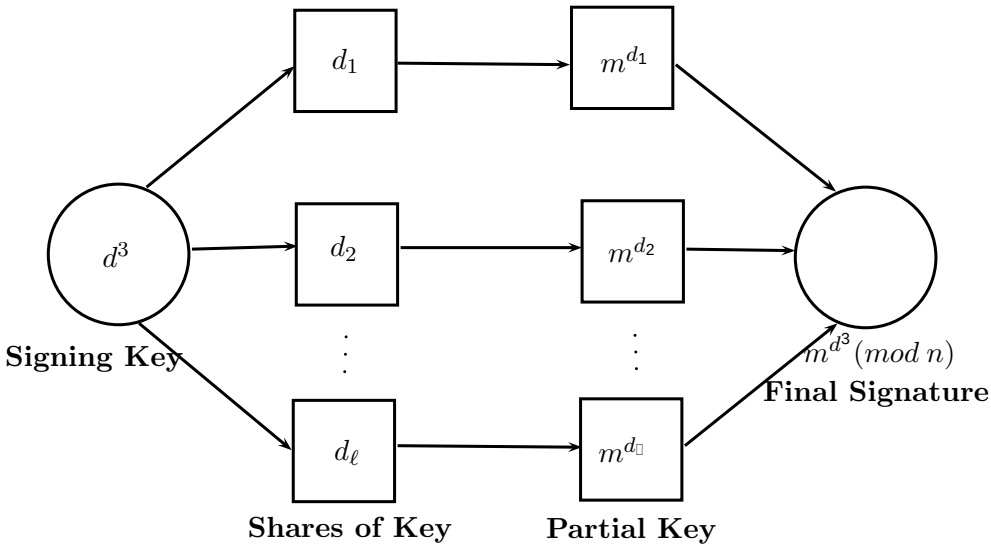
- Select a secret *odd prime* integer R.
- Consider the Pell's Equation:

$$y^2 - Rx^2 = 1. \tag{1}$$

- Let (x_0, y_0) be the *least positive integral* solution of (1).
  Here x_0, y_0 are kept as secret.
- Select two large *RSA odd primes* p and q.
- Define $N = pq$ then $\phi(N) = (p-1)(q-1)$
  where $\phi(N)$ is Euler phi function.
- Select a RSA secret exponent e such that $[1 < e < \phi(N)]$ such that $gcd(e, \phi(N)) = 1$.
- For this e, there is a unique d such that $ed \equiv 1(mod\ \phi(N))$.
- consider

$$a = (y_0 + \phi(N))^2 - R(x_0 + e)^2. \tag{2}$$

- e^3 is not congruent to $1(mod\ \phi(N))$ and d^3 is not congruent to $1(mod\ \phi(N))$.
- From (2) $ad^3 + Rd + 2x_0d^2R \equiv d^3\ (mod\ \phi(N))$.
- Let $S = ad^3 + 2x_0d^2R + Rd$ then $S \equiv d^3\ (mod\ \phi(N))$.
- Here we define S is the *exponent secret*.
- Represent the message m in the interval $[0, n-1]$ with $gcd(m, n) = 1$.



- Key distribution: Consider the ℓ exponent secret partition (share holders)

$$S = t_1 + t_2 + \cdots + t_\ell.$$

Define $Y_i \equiv m^{t_i}\ (mod\ N)$ for $1 \le i \le \ell$:

$$\begin{aligned}\textstyle\prod_1^\ell Y_i &\equiv m^S (mod\ N)\\ &\equiv m^{t_1+t_2+\cdots+t_\ell} (mod\ N)\\ &\equiv m^{t_1} m^{t_2} \ldots m^{t_\ell} (mod\ N).\end{aligned}$$

- For ℓ secret share holders we can distribute ℓ key's such as $Y_1, Y_2, \ldots, Y_\ell$.
- Secure Sharing Scheme:

$$\begin{aligned}E &\equiv m^s (mod\ n)\\ &\equiv m^{k\phi(n)+d^3} (mod\ n)\end{aligned}$$

$$\equiv m^{k\phi(n)} m^{d^3} (mod\ n)$$
$$\equiv [m^{\phi(n)}]^k m^{d^3} (mod\ n)$$
$$\equiv m^{d^3} (mod\ n).$$

- High Level Authentication Key manager is e^3:
$$(\prod_1^\ell Y_i)^{e^3} \equiv (m^{d^3})^{e^3} (mod\ N),$$
$$(\prod_1^\ell Y_i)^{e^3} \equiv m (mod\ N).$$

3. Conclusion

In resent years the security of operations taking place over a computer network become very important. It is necessary to protect such actions against bad users who may try to misuse the system. Many protocols and schemes were designed to solve problem of this type. To overcome the various security vulnerabilities in the networks the design of a pre distribution algorithm using a deterministic approach is initiated. The deterministic approach is the process of determining the keys or key chain based on some criteria. In this paper, we have proposed a novel deterministic key pre distribution algorithm using the pell's equation. In our future work, after analyzing the performance of key distribution algorithm, we plan to extend this novel algorithm for hierarchal wireless network by adapting probabilistic method.

References

[1] Adi Shamir, How to share a secret, *Communications of the ACM*, **22**, No. 11 (1979, 612-613.

[2] A. Beimel, Secret-sharing schemes: A survey, In: *Proceedings of the Third International Conference on Coding and Cryptology*, Berlin, Heidelberg, Springer-Verlag, IWCC'11 (2011), 11-46.

[3] G.R. Blakley, Safeguarding cryptographic keys, *Proceedings of the National Computer Conference*, **48** (1979), 313-317.

[4] N. Chandramowliswaran, S. Srinivasan, P. Muralikrishna, Secure schemes for secret sharing and key distribution using non-homogeneous equation, *Submitted*.

[5] Ivan Niven, Herbert S. Zuckerman and Hugh L. Montgomery, *An Introduction to the Theory of Numbers*, John Wiley.

[6] Tom M. Apostol, *Introduction to Analytic Number Theory*, Springer.