Generalisation of RSA Scheme using fundamental groups and ZKIP

M.Thiyagarajan
Professor, School of Computing
SASTRA University, Thanjavur, India

S.Samundeeswari
Assistant Professor , School of Computing
SASTRA University, Thanjavur, India

***Abstract* - We address the problem of computation involved in RSA algorithm namely exponentiation under modulo arithmetic and various mathematical and timing attacks in RSA. The computation is made easy and quick by assigning elements from the fundamental group in algebraic topology. This can also be regarded as a Zero Knowledge Interactive Protocol (ZKIP).**

Keywords- RSA algorithm, exponentiation in modular arithmetic, fundamental group in algebraic topology, Zero Knowledge Interactive Protocol

I. INTRODUCTION

Depending upon the applications of public key systems are characterized by either sender's private key or receiver's public key or both to perform some type of cryptographic functions. It can be encryption and decryption, digital signature or key exchange[9]. The counter measure to brute force attack is use of large key sizes. Diffie-Hellman change cryptologist that met the requirements of the public key cryptographic systems. The approaches attacking RSA mathematically[6] rest on factoring a number in product of primes, calculation of two relatively prime numbers to $\phi(n)$. It is in turn increased in computing power and refinement of factoring algorithm to avoid other timing attacks. We place here a cyclic group structure of the fundamental group in algebraic topology. We say this is a break through in the cryptographic protocols based on Zero Knowledge statistical zero knowledge interactive protocol in which a statistical Interactive Protocol.

Related Work

Kocher [7] was the first to discuss timing attacks.. Timing attacks exploit the timing variations in cryptographic operations. Because of performance optimizations, computations performed by a cryptographic algorithm often take different amounts of time depending on the input and the value of the secret parameter. If RSA private key operations can be timed reasonably accurately, in some cases statistical analysis can be applied to recover the secret key involved in the computations.

Cryptographic algorithms that rely on modular exponentiation such as RSA and Diffie-Hellman may be vulnerable to timing attacks. If the exponentiation operation that involves the secret key can be timed by an attacker with reasonable accuracy, the key can be recovered by using carefully selected input values, the number of which being proportional to the length of the key. It is feasible to recover the RSA private keys used in these systems. Defenses against such attacks are possible. Today, the most widely used method is RSA blinding which incurs a small performance penality of 2% to 10%. Timing attacks illustrate that attackers do not necessarily play by the presumed rules and they will always attack the weakest link in a system. Strong cryptography gives us security only if it is implemented and used in ways that complement its strength.

II. SECTION I

A. Basic Concepts

We start with the following definitions used in the subsequent work

B. Definition 1 Discrete log problem

An ordinary logarithm $\log_a(b)$ is a solution of the equation $a^x = b$ over the real or complex numbers. Similarly, if g and h are elements of a finite cyclic group G then a solution x of the equation $g^x = h$ is called a discrete logarithm to the base g of h in the group G

C. Definition 2 Discrete Exponentiation

In general, let G be a finite cyclic group with n elements. We assume that the group is written multiplicatively. Let b be a generator of G; then every element g of G can be written in the form $g = b^k$ for some integer k. Furthermore, any two such integers representing

g will be congruent modulo n. We can thus define a function $Log_b: G \rightarrow$ (where Z_n denotes the ring of integers modulo n) by assigning to g the congruence class of k modulo n. This function is a group isomorphism, called the discrete logarithm to base b [4].

Given an element g and the values of g^x and g^y. Formally, g is a generator of some group (typically the multiplicative of a finite field or an elliptic group) and x and y are randomly chosen integers. For example, in the Diffie-Hellman key exchange, an eavesdropper observes g^x and g^y exchanged as part of the protocol, and the two parties both compute the shared key g^{xy}.

D. Definition 3 Relative Entropy

Discrete logarithms are perhaps simplest to understand in the group $(Z_p)^{\times}$. This is the set of congruence classes $1,..., p-1)$ under multiplication modulo the prime p.

If we want to find the k^{th} power of one of the numbers in this group, we can do so by finding its k^{th} power as an integer and then finding the remainder after division by p. This process is called *discrete exponentiation*. For example, consider $(Z_{17})^{\times}$. To compute 3^4 in this group, we first compute $3^4 = 81,$ and then we divide 81 by 17, obtaining a remainder of 13. Thus $3^4 = 13$ in the group $(Z_{17})^{\times}$. *Discrete logarithm* is just the inverse operation. For example, take the equation $3^k \equiv 13(\text{mod}17)$ for k. As shown above $k = 4$ is a solution, but it is not the only solution. Since $3^{16} \equiv 1(\text{mod}17)$ it also follows that if n is an integer then $3^{4+16n} \equiv 13 \times 1^n \equiv 13(\text{mod}17).$ Hence the equation has infinitely many solutions of the form $4+16_n$. Moreover, since 16 is the smallest positive integer m satisfying $3^m \equiv 1(\text{mod}17),$ that is 16 is the order of 3 in $(Z_{17})^{\times},$ these are the only solutions. Equivalently, the solution can be expressed as $k \equiv 4(\text{mod}16).$

E. Definition 4 Discrete log Problem in finite Group

There are three main groups whose discrete logarithm is of interest to cryptographers [15].

The multiplicative group of prime fields: $GF(P)$

The multiplicative group of finite fields of characteristic 2: $GF(2_n)$

Elliptic curve groups over finite fields F: $EC(F)$

The security of many public key algorithms is based on the problem of finding discrete logarithms, so the problem has been extensively studied.

If P is the modular and is prime, then the complexity of finding discrete logarithm in $GF(P)$ is eventually the same as factoring an integer n of about the same size, when n is the product of two approximately equal–length primes. Computing discrete logarithms is closely related to factoring. If you can solve the discrete logarithm problem, then you can factor. Currently there are three methods for calculating discrete logarithms in prime field: the linear Sieve, the Gaussian integer Scheme and the number field sieve.

F. *Definition 5 Homotopy*

Let X and Y be topological spaces, and let f_0 and f_1 be continuous maps $X \rightarrow Y$. f_0 is homotopic to f_1(Written $f_0 \approx f_1$) if there exists a continuous maps $F: X \times I \rightarrow Y$ such that $F(x,0) = f_0(x)$ and $F(x,1) = f_1(x)$ for all $x \in X$. The map F is called a homotopy from f_0 to f_1.

G. *Properties of Zero Knowledge Proof*

Zero-knowledge proofs (ZKPs) are interactive proofs (protocols) in which the prover proves the knowledge (or the possession) of a secret without revealing any information about the secret itself[5]. ZKPs can be used whenever there is critical data to exchange while only proving the possession of such data is needed, without a real need for exchanging the critical data.

Completeness Property

For any $c > 0$ and sufficiently long $x \notin L,$ Probability (V accepts x) $> 1 - |x|^{-c}$. In other words, an interactive proof (protocol) is *complete* if, given an honest prover and an honest verifier, the protocol succeeds with overwhelming probability.

Soundness Property

For any $c > 0$ and sufficiently long $x \notin L$, Probability (V accepts x) $< |x|^{-c}$, i.e. negligible, even if the prover deviates from the prescribed protocol. In other words, if a dishonest prover P' can successfully execute the protocol with non negligible probability, then P' has knowledge essentially equivalent to the actual secret

Zero Knowledge Proof

An interactive proof $< P,V >$ is called *zero-knowledge* if for every probabilistic polynomial-time V^*, there exists a probabilistic expected polynomial-time simulator (algorithm) M_{v^*} that on inputs $x \in L$ produces probability distributions $M_{v^*}(x)$ polynomially indistinguishable from the distributions $< P,V^* > (x)$.

III. SECTION II

A. *Problem specification*

Early Version of RSA

1. Pick 2 primes p and q make $n = pq$ public
2. find $\phi(n)$ and an element e < n and relatively prime to $\phi(n)$
$$\gcd(\phi(n), e) = 1$$
3. For a plain text $m < n$ the cipher text is given by
$$c = M^e \bmod n$$
4. From c to get M
$$M = c^d \bmod n$$
where d is the multiplicative inverse of e, $\bmod \phi(n)$
$$ed \equiv 1 \bmod \phi(n)$$

Here we take the n, the number of elements in the F fundamental group which is cyclic. Since the order of a cyclic group is prime, n is prime[8]. Find two fundamental group of order p and q. As with RSA

$$n = pq$$

To calculate e, we identify M to be a generator of the cyclic group F and

$$M = g$$

Therefore $c = g^e \bmod n$, e < n and relatively prime to $\phi(n)$ and other steps of RSA

$$M = c^d \bmod n$$
$$= (M^e)^d \bmod n$$
$$= M^{ed} \bmod n$$

Using Euler's theorem

$$ed = k\phi(n) + 1$$

Thus generating the discrete log problem to F group.

We can find e, d and hence the scheme is derived.

The computation of n, e and M^e are done using a ZKIP between two paties and making this computation to be done in 50 % of trials.[2]

This is strong over any timing and transport confidentiality attack.

To find a crypto system using fundamental group in algebraic topology, we need to find a hard problem corresponding to factoring the product of two primes are taking the discrete logarithm in modulo multiplication and modulo exponentiation employed in RSA scheme which are prone to mathematical and timing attacks.

B. *Illustration*

Let $p = 61,\ q = 59$

$$n = pq$$
$$= 61 * 59 = 3599$$
$$\phi(n) = 60 * 58 = 3480$$
$$e = 31$$

We find by extended Equlips algorithm, the multiplicative inverse $\bmod 3480$ as $d = 449$.

For any text, which has the value of the generator of cyclic group can be taken as the plain text M. M^{31} will be the cipher text.

IV. SECTION III

A. *Our Method*

Each element in RSA setup is identified as an element in the fundamental group as a product of two mapping is the multiplication modulo n, as viewed in RSA algorithm.

Thus the modulo arithmetic and exponentiation are done as compositions and expressing elements as a power of a generator of a cyclic group. [1]

The computation of are done using a ZKIP between two parties and making this computation to be done in 50 % of trials.[3]

This is strong over any timing and transport confidentiality attack

V. SECTION V

A. *Conclusion and Future work*

This concludes that the mathematical and timing attacks from the RSA algorithm is made hard by identifying the fundamental group S_n and alternative generator along with the inverses in the fundamental group. This protocol is considered as a discrete log problem presented in Zero Knowledge Interactive Protocol in one round.

Thus completeness , soundness and zero knowledge are evident from the analysis of the algebraic structure for the cyclic group S_n

VI. REFERENCES

[1] Alfred Renyi, Foundations of Probability, London: Holden-Day, Inc., 1970

[2] Cramer, R. and Damgard, I. "Linear zero-knowledge – a note on efficient zero-knowledge proofs and arguments." *Proceedings of the Twenty-ninth Annual ACM Symposium on Theory of Computing*. Texas: United States (1997), pp.436-445.

[3] Deborah Joseph. Polynomial time computations in models of ET. *Journal of Computer and System Sciences*, Vol.26, No.3 (1993), pp.311-338

[4] Diffie, W. and Hellman, M.E,"New directions in cryptography",*IEEE Trans. Inform. Theory*, Vol.IT-22, No.6 (1976), pp.644-654.

[5] Goldwasser, S., Milcli, S. and Rackoff, C. The knowledge complexity of interactive proof-systems. *SIAM Journal on Computing*, Vol.18 (1989), pp.186-208.

[6] Kaliski, B., and Robshaw, M.," The Secure use of RSA", Crypto Bytes,Autumn 1995.

[7] Kocher, P, " Timing attacks on Implementations of Diffie-Hellman, RSA, DSS and other systems", *Proceedings, crypto* (1996), August 1996.

[8] S.Samundeeswari, "ZKIPS and their Variants for Crypto Systems", Thesis submitted to SASTRA University, India, 2009.

[9] Stallings, William. *Cryptography and Network Security*. India: Pearson Education, 2007.

VII. AUTHORS PROFILE

A. *Prof . M . Thiyagarajan*

He has graduated from university of madras at 1960 and Post Graduate from Annamalai University. He has obtained his M.Phil from the University of Madras with Specialization in Stochastic Processes and Application . He has guided more than 50 M.Phil research scholars and 20 Phd scholars. He has Published /Presented more than 100 papers in various known applications of stochastic processes invariant for and abstract algebra. At present he is guiding 4 people on Cryptography parallel algorithms and VLSI design. He is currently working as a Professor in the School of Computing of SASTRA University , Tanjore, Tamil Nadu.

B. *Mrs. S.Samundeeswari*

Hails from Thanjavur,Tamil Nadu. She received the B.Tech Degree in Computer Science and Engineering from Bharathidasan University ,Trichy in 1993 and M.Tech degree in Computer Science and Engineering from SASTRA University in 2005.She is currently with SASTRA University as a senior faculty in the School of Computing. Her research interests include Network security and Cryptography. She has published more than 10 National/International articles in various journals. She has attended more than 15 National/International Conferences and seminars conducted by leading Engineering Institutions. She has also guided projects for IT Graduate students.