ISSN 2250-3153

A Lightweight Privacy Preserved Buyer Seller Watermarking Protocol Based on Priced Oblivious Transfer

Ananthi. P[1], G.Selva Vinayagam[2]

[1]PG Student, Dept of IT, SNS College Technology, Coimbatore, India
[2]Assistant Professor, Dept of IT, SNS College of Technology, Coimbatore, India

Abstract- Advent of Internet has resulted in e-commerce replacing traditional selling of digital products (such as songs, videos,movies, software, books, documents, images, etc.) through shops. This mode of sale can bring the product price down as infrastructure cost in setting up shops and retail chain is reduced. On downside, however, this may increase problem of piracy as digital data can be easily copied, manipulated and transmitted. To protect copyright of owner, establish right of buyer on purchased copy and yet check data piracy, it is required that a rusted e-distribution system be built. Such a system should be able to ensure secure transaction between buyer and seller, check ownership and track the origin of unauthorized copies..The buyer seller watermarking protocols are heavyweight protocols.These protocols require large computation power and network bandwidth.The heavyweight protocols could not be used for the resource constrained devices since the devices does not support battery power.A lightweight protocol has been proposed which is best suited for the resource constrained devices. The protocol is based on a fast asymmetric encryption with novel simplification.In this approach the seller authenticates the buyer but does not learn which items are purchased. The protocol is designed in such a way that the buyers pay the right price without disclosing the purchased item, and the sellers are able to identify buyers that released pirated copies. The protocol is constructed based on the priced oblivious transfer and the existing techniques for asymmetric watermark embedding.

Index Terms- Buyer–seller watermarking protocol, fair exchange, priced oblivious transfer (POT).

I. INTRODUCTION

BUYER-SELLER watermarking protocols allow copyright protection of digital goods. Digital watermarks have recently been proposed for the purposes of copy protection and copy deterrence for multimedia content. In copy deterrence, a content owner (seller) inserts a unique watermark into a copy of the content before it is sold to a buyer. If the buyer sells unauthorized copies of the watermarked content, then these copies can be traced to the unlawful reseller (original buyer) using a watermark detection algorithm.

Fast growing information technology permits perfect duplication and cheap distribution for digital works. The problems associated with intellectual property protection have become important issues. In the realm of security, encryption and digital watermarking are recognized as promising techniques for copyright protection. Encryption is to prevent unauthorized access to a digital content. The limitation is that once the content is decrypted, it doesn't prevent illegal replications by an authorized user. Digital watermarking, complementing encryption techniques, provides provable copyright ownership by imperceptibly embedding the seller's information in the distributed content. Similarly, digital fingerprinting is to trace and identify copyright violators by embedding the buyer's information in the distributed content.

The existing buyer seller watermarking protocols are heavyweight protocols. These protocols require large computation power and network bandwidth. The heavyweight protocols could not be used for the resource constrained devices since the device does not support battery power. A lightweight protocol has been proposed which is best suited for the resource constrained devices. The protocol is based on a fast asymmetric encryption with novel simplification..The protocol is designed in such a way that the buyers pay the right price without disclosing the purchased item, and the sellers are able to identify buyers that released pirated copies. Consequently, privacy concerns discourage online e-commerce [1], and regulations to enforce privacy protection are being promulgated [2].

II. RELATED WORK

Fingerprinting schemes deter people from illegally redistributing digital copies by enabling the seller of the data to identify the buyer.A scheme is said to be collusion-resistant [3] when it prevents a collusion of buyers up to a maximum size from producing nontraceable copies. In asymmetric fingerprinting schemes [4], the fingerprinted copy is only known to the buyer at the end of the purchase protocol. Thanks to this property, when the seller finds a redistributed copy, he can present it as a proof of the buyer's misbehavior, and the buyer cannot claim that the copy was produced by the seller. In order to protect privacy, fingerprinting protocols that provide buyers with anonymity have been proposed [5].Buyer–seller watermarking protocols [6] are asymmetric fingerprinting schemes in which the fingerprint is embedded by means of watermarking techniques. The basic idea is that each buyer obtains a slightly different copy of the digital content.Such difference, the watermark, does not harm the quality of the copy and cannot be removed by the buyer. Some buyer–seller Watermarking protocols also provide buyers with anonymity [7]–[9].As noted in [10], anonymous e-

commerce protocols have several disadvantages. First, they hinder customer management. For example, the seller cannot give discounts to regular buyers or apply other loyalty marketing techniques. Second, they have to be used together with anonymous payment protocols (e.g., anonymous e-cash), which makes it impossible to use currently deployed payment protocols. Finally, they require the use of an underlying anonymous communication network, such as Tor. It is well-known that achieving strong anonymity in such networks is a difficult goal. Furthermore, some applications allow side-channel attacks against anonymity. For example, in location-based services, the service provider learns a customer's location, and this information can be used to identify the *a priori* anonymous customer .Additionally, e-commerce protocols are usually analyzed in order to prove their fairness. Roughly speaking, fair exchange ensures that, at the end of the transaction, either the seller receives the payment and the buyer receives the purchased item, or both parties receive nothing. However, to the best of our knowledge, no fair buyer–seller watermarking protocol has been proposed. We propose a different approach to provide privacy protection in buyer–seller watermarking protocols. In our approach, based on oblivious e-commerce protocols, buyers are authenticated by the seller, but the seller does not learn which items are purchased. This overcomes the disadvantages of anonymous purchase. Since buyers are authenticated, customer management is eased and currently deployed methods of payment can be utilized. As possible disadvantages, one can argue that the seller can find it difficult to learn which However, as noted in, this information can be obtained by other means, e.g., by conducting marketing research.

We define formally privacy-preserving buyer–seller watermarking (PBSW) protocols, i.e., buyer–seller watermarking protocols in which the seller does not learn which items are purchased. We also provide a construction of such a protocol based on existing techniques for asymmetric watermark embedding and on priced oblivious transfer (POT). (POT is the key building block of oblivious e-commerce protocols.) Finally, we explain how to extend our protocol to provide fair exchange.

III. SYSTEM MODEL

The privacy preserving buyer seller watermarking protocol based on niederreiter encryption [11], which makes use of a particular asymmetric encryption.

Niederreiter Asymmetric Encryption

First, we review the cryptographic primitive — Niederreiter Asymmetric encryption scheme .Setup. The public key and secret key are built by generating several matrices and an (n, k)-linear code.S: A random $(n-k)\times(n-k)$ binary non-singular matrix.H: An $(n-k)\times n$ parity-check matrix H for a binary (n, k)-linear code that can correct t errors, and for H an efficient decoding algorithm ψ is known.

P: A random $n \times n$ permutation matrix.

Make use of (S, H, P) to compute an $(n - k) \times n$ matrix

K = *SHP*, let

Public Key: PK=(K, t)

Secret Key: SK=(S, P, ψ)

Encryption. Given a clear text *msg* which is encoded as an n-bit binary vector, let KT denote the transpose of K, then the ciphertext is computed as follows:

$c = msg \cdot \mathrm{KT}$

Where *msg* contains no more than t 1's. This is because Niederreiter scheme employs a (n, k)-linear code with the capability of decoding less than t errors. If the Hamming weight of clear text $WH(msg) \le t$, then the mapping of clear text to ciphertext is injective.

Decryption. Given an input c, decryption algorithm computes cT from c, and $S-1$ from matrix S to get the following,

$H(P \cdot msg\mathrm{T}) = S-1 \cdot c\mathrm{T}$

where $S-1$ denotes the inverse of the matrix S.Since it is known by the decoder an efficient decoding algorithm Ψ for H, when $WH(msg) \le t$, the following holds:

$P \cdot msg\mathrm{T} = \psi (S-1 \cdot c\mathrm{T})$

Hence, it is easy to compute cleartext *msg* by:

$MsgT = P-1(P \cdot msg\mathrm{T})$

Remark. In particular, it is clear to see that quite simple matrix operations are needed in the encryption process. Thus, the encryption could be executed very fast.

A Basic Protocol

A direct application of asymmetric encryption would be to simply encrypt the real ID of the device with the server's public key, and send the resulting ciphertext c to the server. Then the server takes advantage of its secret key to recover all users' ID, which handles the ID directly after decoding and enjoys the convenience of the privacy (ID) management. Consequently, this protocol successfully avoids maintaining any synchronization or the exhaustive search in the database that typically costs a lot of resources when a huge number of IDs need to be managed. Obviously, the security of the above protocol relies on the Niederreiter asymmetric encryption [12]. Anyone who intends to know the encrypted ID will have to break the Niederreiter asymmetric encryption.

More importantly, it is noteworthy that not all secure asymmetric encryptions are eligible for our approach, because Most of the asymmetric encryptions are too heavy to run on severely resource-constrained devices. However, since the Niederreiter scheme has a very speedy encryption and especially by simplification technique, the operation of device can be efficiently accomplished. In the following, we describe the basic protocol. The protocol employs the Niederreiter encryption to generate ciphertext c according to the device's ID d and a randomly generated number r, such that clear text $msg = r||d$, where "||" denotes the bit concatenation. Meanwhile, ciphertext c could be also considered as a PID corresponding to d.

Let R, ID denote the sets of random number and valid ID respectively, such that,

$R = \{r \in \{0, 1\}^{n1} \mid WH(r) = t1\}$
$ID = \{d \in \{0, 1\}^{n2} \mid WH(d) = t2\}$

Where all the integers are positive and $t = t1+t2$, $n = n1+n2$. It is obvious to see that the number of ID, $\_ID = \_{n2\ t2}\_$, where $\cdot\_$ is the binomial coefficient. Suppose K be composed of two sub-matrices K1, K2, corresponding to r, d respectively (See Figure.1). For a certain SK of the server and an ID d of the device, $c2 = d \cdot KT2$ is fixed. Consequently, it is convenient to pre-distribute the value $c2$ to the device beforehand, and compute r and K1 to obtain $c1$, which drastically saves the computation for the device. Besides, $c2$ is stored instead of both d and K2, which further saves the memory cost. More precisely, the basic protocol consists of several phases, which are briefly described in the following. Key Generation. The system first generates public key and secret key of the server as (PK,SK), such that

PK= (K, t),
SK=(S, P, ψ). Since $c2$ part of the computation of PID

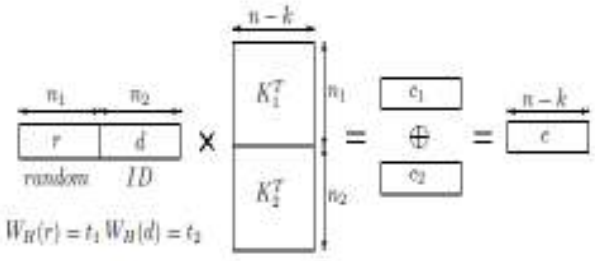

Fig. 1: Niederreiter Encryption

Public Key: PK= (K1, $t1$)
Secret Key: SK=(S, P, ψ)
The K1 is the left $(n - k) \times n1$ matrix of K, and K2 is
The remained $(n - k) \times n2$ part of K, namely K = [K1K2].

ID Allocation. The server chooses $d \in ID$ as device's identity and computes

$c2 = d \cdot KT2$
Then $c2$ together with K1 will be assigned to the device, where $c2$ needs to be kept secret.

Query and Reply. In this phase, the server queries the unknowndevice for its ID. The device chooses a random number $r \in R$, computes
$c1 = r \cdot KT1$
and then sends back the pseudo-ID PID to the server, as
$PID = c1 \oplus c2$

ID Retrieval. Since PID is actually an encryption of $msg = r||d$ with public key PK, such that,
$PID = c1 \oplus c2 = (r \cdot KT1) \oplus (d \cdot KT2) = (r||d) \cdot KT$on receiving the PID, the server makes use of secret key
SK=(S, P, ψ) to recover d.

IV. TECHNICAL PRELIMINARIES

A. Blind Watermarking

A blind and readable watermarking scheme consists of a setup algorithm, a watermark embedding algorithm, and a watermark detection algorithm .outputs a secret watermarking key, a message space, and a watermark space. , on input, message, and watermark, outputs a watermarked message. The algorithm can be computed in the encrypted domain, where both and the result are encrypted with a public key of a public key encryption scheme. The algorithm outputs the watermark embedded in .A secure watermarking scheme should be robust and collusion resistant. Let be a distortion metric that quantifies the distortion suffered by a watermarked content when it underwent signal processing operations such as compression, filtering, noise addition, desynchronization, cropping, insertions, mosaicing, and collage. Let be a distorted content. The robustness property requires that under a distortion metric and a distortion bound, given output by and output by, outputs with overwhelming probability if .The collusion resistance property requires that collusion up to parties cannot manipulate or remove the watermark from a watermarked content by comparing or composing their differently watermarked copies. This property can be formalized

Definition 1 *(Collusion Resistant Watermarking):* The collusion resistance property is defined through the following game between a challenger and an adversary. • Challenge. Runs to get, picks random original content, and, for to, picks random watermark and runs .sends to. • Response. outputs watermarked content .wins if there exists such that and outputs watermark such that, for to , .A blind watermarking scheme is collusion resistant if all p.p.t. adversaries win the game above with negligible probability. Current practical watermarking schemes do not provide collusion-resistance against any p.p.t. adversary. We assume that the watermarking scheme used to instantiate the protocol fulfills this definition, and thus we conclude that our protocol is secure against any p.p.t. adversary. When the protocol is instantiated with a concrete watermarking scheme, the security offered against malicious buyers is lowered to the security offered by the watermarking scheme.

B. Signature Schemes

A signature scheme consists of the algorithms, and. Outputs a secret key and a public key . Outputs a signature of message. Outputs if is a valid signature of and otherwise. A signature scheme must be correct and unforgeable. Informally speaking, correctness implies that the algorithm always accepts an honestly generated signature. Existential unforgeability means that no p.p.t.adversary should be able to output a message-signature pair unless he has previously obtained a signature on.

C. Homomorphic Encryption

A public key encryption scheme consists of the algorithms and. Outputs a public key and a secret key. Outputs a ciphertext on input a public key and a message. Outputs the message on input the ciphertext and the secret key. Roughly speaking, indistinguishability under chosen plaintext attack (IND-CPA)

guarantees that an adversary does not get any knowledge about from .

We employ a homomorphic public key encryption scheme that supports two operations. An operation that, on input two ciphertexts and that encrypts messages and, outputs a ciphertext that encrypts the addition of the messages, and an operation that, on input a message and a ciphertext, outputs a ciphertext that encrypts the multiplication of the messages. The homomorphic public key encryption scheme proposed by Paillier, and its generalization by Damgård and Jurik, support these operations, and therefore can be used to instantiate the encryption scheme In our construction we need a function that, on input a bit and an encryption of a bit , computes the encryption , where denotes the exclusive or operation.

.

D. Zero-Knowledge Proofs of Knowledge

A zero-knowledge proof of knowledge is a two-party protocol between a prover and a verifier. The prover proves to the verifier knowledge of some secret input that fulfils some statement without disclosing this input to the verifier. The protocol should fulfil two properties. First, it should be a proof of knowledge, i.e., a prover without the knowledge of the secret input convinces the verifier with negligible probability. More technically, there exists a knowledge extractor that extracts the secret input from a successful prover with all but negligible probability. Second, it should be zero-knowledge, i.e., the verifier does not learn any information about the secret input. More technically, for all possible verifiers there exists a simulator that, without knowledge of the secret input, yields a transcript that cannot be distinguished from the interaction with a real prover.To express a zero-knowledge proof of knowledge, we follow the notation introduced by Camenisch and Stadler.

For example, denotes a "zero-*knowledge proof of knowledge of secret input such that.*" Letters in the parenthesis, in this example , denote the secret input, while and the function are also known to the verifier.We employ a proof of knowledge , i.e., a proof that is a correct encryption under of the secret key related with public key , so that a party in possession of the secret key related with can recover from . The verifiable encryption schemes proposed by Camenisch *et al.* And by Poupard and Stern, which are provided with such a proof of knowledge, can be employed to instantiate the encryption scheme used in our construction we also use a proof of knowledge of the statement, i.e., a proof that the value encrypted in ciphertext under public key is a bit.

V. PBSW PROTOCOL

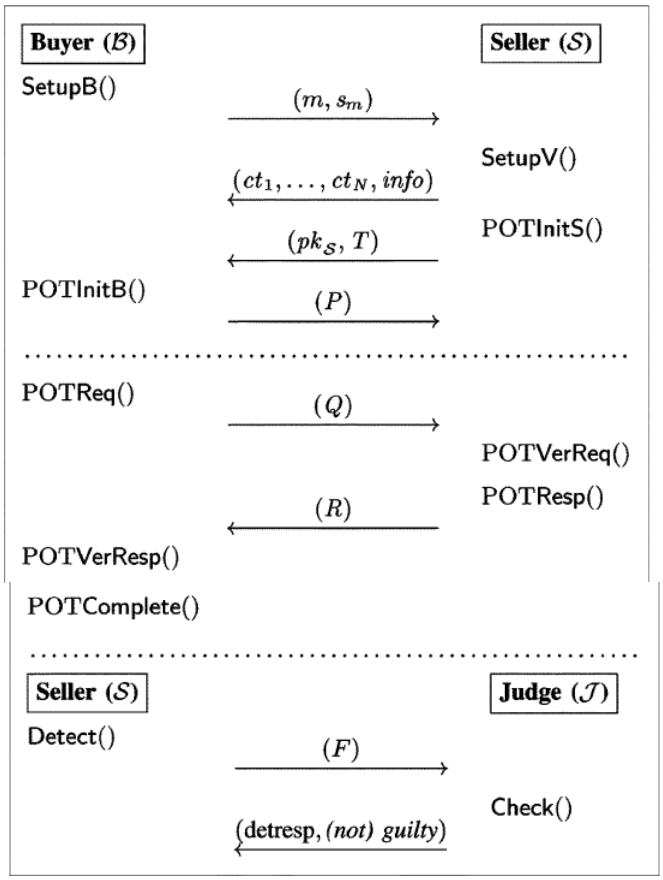

Fig. 2: Phases of PBSW protocol: initialization (top), purchase (middle), arbitration (bottom).

PBSW protocol is based on POT. POT allows buyers to purchase messages from the seller without the seller learning Which messages are bought. Existing secure POT schemes follow an assisted decryption approach in which the interaction between a seller and a buyer is divided into an initialization phase and several purchase phases. In the initialization phase, encrypts the messages to be sold and sends the ciphertexts to. In each purchase phase, helps to decrypt one of the ciphertexts via an interactive protocol.

VI. SECURITY AND PERFORMANCE ANALYSIS

The security of the proposals relies on the Niederreiter encryption and the hash function *h*, which is shown in the following theorem.

Theorem 1 *If the Niederriter encryption is one-way secure and the one-way hash function is collision-resistant, then the proposed protocols are secure against active attacks.*

Proof. Generally speaking, the intuition behind the security is that if the privacy information ID *d* is cracked or impersonated

By an active adversary *A*, then *A* can either break the Niederreiter encryption or find a collision of hash function *h*.

We show the security of explicit auxiliary protocol in details.

1. When an active adversary *A* intends to steal the ID from certain device D, *A* pretends to be S. *A* can select adaptive, non-random *cha* and send it to D. According to the response of D, the adversary gets the following.• What *A* can obtain from D is exactly the encryption of randomness *r* and ID, and a hash value *aux*. Note here that the *cha* chosen by *A* is not included
In the cleartext, but is a partial pre-image of the hash value *aux*. The *r* is chosen by the D, and ID embedded in *c*2 is pre-computed and stored in the D, out of control of *A*. From a cryptographic point of view, it means that the attack employed by *A* is weaker than the chosen-plaintext attack, in which *A* can get the encryption of what he chooses. If *A* can guess the ID, then he must be able to *invert* the Niederreiter encryption and thus *break* its one-wayness,only by a weaker attack than chosen-plaintext attack! The above is contradicting to the security of Niederreiter encryption which is known as one-way secure against chosen-plaintext attack.

Without breaking the Niederreiter encryption, *A* has to invert hash function *h* (*c*2||*r*||*cha*). The only advantage is that *A* is able to choose *cha* as he likes. It is obviously impossible if a secure hash function is applied.From the above, it is easy to see that *A* has to break the encryption or find full pre-image of hash function, to get the privacy information ID.

VII. FAIR PRIVACY-PRESERVING PBSW PROTOCOL

Recently, a transformation that takes as input a secure POT scheme and turns it into an optimistic fair POT scheme has been proposed. This transformation requires a neutral third party, an adjudicator, who is only involved in case of dispute between a seller and a buyer (hence the protocol is called optimistic).Other fair e-commerce protocols that do not protect privacy also require the involvement of a third party .The transformation is based on the use of verifiably encrypted signatures (VES) . Roughly speaking, a VES is a signature encrypted under the public key of the adjudicator that can be publicly verified; i.e., the verifier can check that the ciphertext contains a valid signature without the secret key of the adjudicator. The transformation works as follows. The buyer computes a VES on her purchase request, and sends to the seller.Upon receiving a correct response from seller, the buyer reveals a valid signature on her request. This signature can be used by the seller to prove that the buyer accepted the result and that a payment was done. If a malicious buyer does not reveal the signature, the adjudicator, upon being requested by the seller, can verify that the seller fulfilled his delivery obligations and, in that case, extract a valid signature from the VES. Similarly, if a malicious seller does not fulfil his delivery obligations, the adjudicator, upon being requested by the buyer, can tell the seller to fulfil them and, in the end, send the seller a valid signature.We refers to for a detailed description. One of the appealing properties of this transformation is that it adds very little overhead in terms of communication and computation.Our PBSW protocol can also be extended to achieve fairness by applying this transformation to the POT scheme used as a building block. In our protocol, the role of the adjudicator can be played by the judge. Both judge and buyers have to compute a key pair as defined in the VES scheme used and register the public key at the registration authority.

VIII. EFFICIENCY

The efficiency of our construction depends on the efficiency of the building blocks used to instantiate it. Efficiency measurements for the asymmetric watermark embedding technique we employ (algorithms , , ,) can be found in [9], which describes and implements an instantiation based on the homomorphic public key encryption scheme due to Paillier [16]. In [9], images of size 512 512 pixels are employed as digital content offered by , whose size after embedding thewatermark in the encrypted domain is 536, 870, 912 bits when each DCT coefficient is encrypted, or 6, 318, 080 bits when composite signal representation is used. In the following, we employ watermarked messages of those sizes as input to the POT scheme.To evaluate the performance of the whole PBSW protocol,we implement the POT scheme proposed in a workstation equipped with an IntelCore2Duo processor at 3 GHz and 4 Gbyte of RAM. All the functionalities are implemented in the C programming language. We use the PBC library for elliptic curve and pairing operations. We select type A pairings constructed on the curve over the field for a 512-bit prime mod 4. For other cryptographic primitives, we employ the OpenSSL library.3 specifically; we employ RIPEMD-160 as hash function and AES in counter mode as block cipher. The efficiency of the POT scheme in terms of computation and communication depends on the selection of three parameters: the number of messages offered by, the size of the watermarked messages, and the values and that define the maximum deposit allowed .The performance of the initialization phase (algorithms and) depends on the number of messages and on the message size. Table I shows performance measurements when is 100, 1000, and 10 000, and when the message size is 536, 870, 912 and 6, 318, 080 bits.

IX. CONCLUSION

Copyright protection for the digital contents is provided. Buyers purchase from sellers without the seller learning the items they buy. Best suited for the resource constrained devices. Improved power consumption and network bandwidth utilization. It provides both buyers and sellers with optimistic fair exchange.The efficiency of the protocol is improved .
The future work includes the signal processing using Discrete Wavelet Transform and Discrete Cosine Transform. The wavelet transform has emerged as a cutting edge technology, within the field of image compression. Wavelet based coding provides substantial improvements in picture quality at higher compression ratios. DWT yields higher compression ratio and better visual quality.

REFERENCES

[1] J. Tsai, S. Egelman, L. Cranor, and R. Acquisti, The effect of online privacy information on purchasing behavior: An experimental

study,working paper Jun. 2007.212 IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 6, NO. 1, MARCH 2011

[2] Enforcing Privacy Promises Section 5 of the Ftc Act Federal Trade CommissionAct[Online].Available: http://www.ftc.gov/privacy/privacyinitiatives/promises.html

[3] D. Boneh and J. Shaw, "Collusion-secure fingerprinting for digital data (extended abstract)," in *CRYPTO*, ser. Lecture Notes in Computer Science, D. Coppersmith, Ed. New York: Springer, 1995, vol. 963, pp.452–465.

[4] B. Pittzmann and M. Schunter, "Asymmetric fingerprinting," in *Adv.in Cryptology (EUROCRYPT'96)*, 1996, pp. 84–95, ser. LNCS 1070.

[5] B. Pfitzmann and M. Waidner, "Anonymous fingerprinting," *EUROCRYPT*,pp. 88–102, 1997.

[6] N. D. Memon and P. W. Wong, "A buyer-seller watermarking protocol,"*IEEE Trans. Image Process.*, vol. 10, no. 4, pp. 643–649, Apr.2001.

[7] H.-S. Ju, H.-J. Kim, D.-H. Lee, and J.-I. Lim, "An anonymous buyerseller watermarking protocol with anonymity control," *Inf. Security Cryptology*, pp. 421–432, Nov. 2002.

[8] C.-L. Lei, P.-L. Yu, P.-L. Tsai, and M.-H. Chan, "An efficient and anonymous buyer-seller watermarking protocol," *IEEE Trans. Image Process.*, vol. 13, no. 12, pp. 1618–1626, Dec. 2004.

[9] M. Deng, T. Bianchi, A. Piva, and B. Preneel, "An efficient buyer-seller watermarking protocol based on composite signal representation," in *Proc. 11th ACMWorkshop on Multimedia and Security.*, Princeton, NJ,2009, pp. 9–18.

[10] A. Rial, M. Kohlweiss, and B. Preneel, "Universally composable adaptive priced oblivious transfer," in *Pairing*, ser. Lecture Notes in Computer Science, H. Shacham and B.Waters, Eds. New York: Springer,2009, vol. 5671, pp. 231–247.

[11] H. Niederreiter, "Knapsack-type Cryptosystems and Algebraic Coding Theory". Problems of Control and Information Theory, vol.15, no.2, pp.159-166, 1986.

[12] R. Dingledine, N. Mathewson, and P. F. Syverson, "Tor: The secondgeneration onion router," in *Proc. USENIX Security Symp.*, 2004, pp.303–320, .

[13] M. Suzuki, K. Kobara and H. Imai, "Privacy Enhancd and Light Weight RFID System without Tag Synchronization and Exhaustive Search". In Proc. of 2006 IEEE International Conference on Systems, Man, and Cybernetics, 2006.

[14] S. Goldwasser, S.Micali, and R. L. Rivest, "A digital signature scheme secure against adaptive chosen-message attacks," *SIAM J. Comput.*,vol. 17, no. 2, pp. 281–308, 1988.

[15] S. Goldwasser and S. Micali, "Probabilistic encryption," *J. Comput.Syst. Sci.*, vol. 28, no. 2, pp. 270–299, 1984.

[16] P. Paillier, "Public-key cryptosystems based on composite degree residuosity classes," in *Proc. EUROCRYPT*, 1999, pp. 223–238.

[17] I. Damgård and M. Jurik, "A generalisation, a simplification and some applications of paillier's probabilistic public-key system," in *Public Key Cryptography*, ser. Lecture Notes in Computer Science, K. Kim,Ed. New York: Springer, 2001, vol. 1992, pp. 119–136.

[18] M. Bellare and O. Goldreich, "On defining proofs of knowledge," in *CRYPTO '92*, E. F. Brickell, Ed. New York: Springer-Verlag, 1992,vol. 740, pp. 390–420.

AUTHORS

First Author – Ananthi. P, PG Student, Dept of IT, SNS College Technology, Coimbatore, India

Second Author – G.Selva Vinayagam, Assistant Professor, Dept of IT, SNS College of Technology, Coimbatore, India