ZERO KNOWLEDGE UNDENIABLE SIGNATURE SCHEME OVER SEMIGROUP ACTION PROBLEM

Neha Goel*
Department of Mathematics
University of Delhi
Delhi 110 007
India
nehagoel_7@yahoo.com

Indivar Gupta
SAG
Metcalfe House
DRDO
Delhi 110 054
Indiaindivar_gupta@yahoo.com

B. K. Dass
Department of Mathematics
University of Delhi
Delhi 110 007
India
dassbk@rediffmail.com

Abstract. The concept of Semigroup Action Problem (SAP) was introduced by C. Monico in 2002. He defined Diffie-Hellman key exchange and ElGamal cryptosystem taking SAP as an underlying problem.

The aim of this paper is to define the application of SAP in designing a zero knowledge undeniable signature scheme. We also discuss the security analysis of the proposed scheme.

Keywords: Group action, semigroup action problem, undeniable signature scheme, zero knowledge proof systems.

1. Introduction

In 1976, Diffie-Hellman proposed the idea of public-key cryptography and digital signatures in [4]. Since then many ideas have been proposed to cover the different security aspects of open communication channel. One such idea in the direction of achieving authenticity, was proposed by David Chaum and V. Antwerpen in [2]. They introduced the concept of undeniable signature scheme which provides authenticity, data integrity and non-repudiation like digital signatures but not publicly verifiable. The aim of introducing these signature schemes is to achieve

∗. Corresponding author

the security in the scenarios where signer wants that only authorized parties can verify his/her signatures. For example, if a software company launches a software and want that only the payable customers can use it then instead of applying digital signatures on software, the company will use undeniable signatures which will be verified by the verifier only if the company found that the involving verifier is payable.

After proposing undeniable signature schemes in [2], a zero knowledge undeniable signature scheme is proposed in [3], which is considered more efficient than the undeniable signature scheme. The advantage of using zero knowledge proof in designing of cryptographic schemes is that it assures the validity of an assertion without revealing any secret information and it also force two communicating parties to follow a protocol properly. Some undeniable signature schemes and zero knowledge undeniable signature schemes have also been proposed in [3, 14, 5] whose security relies on different mathematical hard problems like discrete logarithm problem, factorisation problem, elliptic curve discrete logarithm problem [10] etc.

Many other such mathematical hard problems have been presented in literature on which public-key cryptographic protocols can be designed efficiently. One such mathematical problem was introduced by C. Monico in 2002, which is named as the Semigroup Action Problem (SAP) which is generalised form of the Discrete Logarithm Problem (DLP). Taking SAP as computational hard problem he defined Diffie-Hellman key exchange and ElGamal cryptosystem. After the proposal of SAP, different key-exchange protocols were designed taking different algebraic structures. But the designing was confined to key-exchange protocols and ElGamal cryptosystems only.

Our contribution: The aim of this paper is to design a zero-knowledge undeniable signature scheme whose security relies on the hardness of the SAP. The proposed zero knowledge undeniable signature scheme is proved to satisfy the completeness and soundness property.

The paper is organize in following manner. In section *2*, we give the basic preliminaries for the understanding of paper. In section *3*, we define zero knowledge undeniable signature scheme over SAP. In section *4*, security of the proposed scheme is analysed with respect to completeness and soundness . Finally in section *5*, we conclude the paper.

2. Preliminaries

In this section, we discuss some basic definitions which will be useful for understanding of the paper.

Definition 2.1 (Group action)**.** Let $(G, \cdot)$ be a group and S be a non empty set then G is said to act on S if there exist a function

$$\varphi : G \times S \mapsto S,\ \varphi(a, x) = a * x \quad \text{for} \quad a \in G, x \in S$$

where, $*$ is the operation between elements of G and S and satisfies following properties:

$$a * (b * x) = (a \cdot b) * x \qquad \text{and} \qquad e * x = x \ \forall \ a, b \in G \qquad \text{and} \qquad x \in S.$$

Here, e is the identity element of G.

Definition 2.2 (Semi-group action)**.** Let $(G, \cdot)$ be a semi-group and S be a non-empty set then the semi-group action is defined as the mapping $\varphi : G \times S \mapsto S$ such that $\varphi(g, s) = g * s$ satisfying $g * (h * s) = (g \cdot h) * s \ \forall \ g, h \in G$ and $s \in S$.

Definition 2.3 (Zero knowledge undeniable signature scheme)**.** Zero knowledge undeniable signature scheme consists of following steps:

Set-up. A security parameter κ is given as an input to the algorithm and it outputs the system parameters.

Key-gen. This algorithm takes system parameters as an input generated by set-up algorithm. Then it returns the key-pairs $(sk_{\mathcal{S}}, pk_{\mathcal{S}})$ and $(sk_{\mathcal{V}}, pk_{\mathcal{V}})$ of signer and verifier respectively.

Sign-gen. This algorithm takes $sk_{\mathcal{S}}$ and hash of the message $m \in \mathcal{M}$ as an input and generate the signature over it.

Verification protocol. After getting the signature, verifier interacts with the signer for the verification of signature. If the signature is correct verifier accepts the signature otherwise proceed the disavowal protocol. If the signature is invalid then the probability that a signer is able to convince the verifier that the corresponding signature belongs to his/her public key is negligible.

Disavowal protocol. If the signature is found as an invalid signature, then verifier interacts with the signer in disavowal protocol. With the help of disavowal protocol signer is able to prove that the corresponding signature do not belongs to his/her public key. But if the signer tried to show dishonesty i.e., if he/she tried to convince the verifier for accepting a valid signature as fraud signature then the probability that the signer succeeds in doing so is negligible.

3. Semigroup action problem and its security analysis

In this section we explain the semigroup action problem proposed by Chris Monico in [7].

Definition 3.1 (Semigroup Action Problem(SAP))**.** Let $(G, \cdot)$ be a commutative semigroup and S be a set. Then to find $a \in G$ in the equation $y = a * s$ for given $y \in S$ and $s \in S$ is known as SAP where $*$ is the operation between the elements of G and S.

The SAP can be considered as a generalised form of discrete logarithm problem in groups. For example, let $G = \mathbb{Z}$ be a the set of positive integers, S be a group and φ be the action of $(\mathbb{Z}, \cdot)$ over S i.e.,

$$\varphi : \mathbb{Z} \times S \mapsto S \quad \text{defined as}$$

$$\varphi(l, s) = s^l.$$

Then in this particular example the semigroup action problem of finding l for given (a, s^l) is equivalent to the DLP in group. Thus, the DLP can be considered as special case of the SAP.

3.1 Security analysis of SAP

The attacks like Pollard's rho attack and square root attack which are applicable to the DLP cannot be applied directly to the SAP. As the algebraic structure used to define SAP does not possess invertible elements. Now, we examine the Brute force complexity of SAP. Let η be the cardinality of G. To break the SAP, adversary needs to find an $a \in G$ such that $y = as$. For this adversary will calculate $y_i = a_i s$ where $a_i \in G, 1 \leq i \leq \eta$ and compare this with y. The complexity of applying Brute force attack over the SAP is explained in algorithm 1.

Algorithm 1: Exhaustive search algorithm to solve SAP

Input: $y, s \in S$ such that $y = as$
Output: Secret parameter $a \in G$

for $i \leftarrow 1$ ***to*** η **do**
  $a_i \leftarrow a$;
  $y_i \leftarrow a_i s$;
  Compare $y = y_i$;
  if $y = y_i$;
  return a_i *& exit;*
  else
    go to next step;
  $i \leftarrow i + 1$;
return a

The number of steps used in the above algorithm are at most η times. Therefore, the brute force complexity of solving SAP is proportional to $O(\eta)$.

4. The scheme

The zero knowledge undeniable signature scheme over SAP is defined as below:

Set-up. The security parameter κ is given to the algorithm as an input and it returns system parameters $(R, G, S, \hbar, \varphi)$, where $(R, \cdot)$ is a commutative semigroup, G and S are commutative sub-semigroups of R such that $G \cap S = \{\Phi\}$, $\hbar$ is the hash function defined as, $\hbar : \{0,1\}^* \mapsto S$ and φ is the semigroup action defined as $\varphi : G \times S \to S$ such that $\varphi(a, x) = ax \in S$ for $a \in G$ and $x \in S$.

Key-gen. The system parameters $(R, G, S, \hbar, \varphi)$ are given as an input to this algorithm then algorithm returns the secret key $sk_{\mathcal{S}} = b$ and public key $pk_{\mathcal{S}} = y = bs$ of signer, where $b \in G$ and $y, s \in S$.

Sign-gen. This algorithm takes the message $m \in \{0,1\}^*$ to be signed and secret key $sk_{\mathcal{S}} = b \in G$. After this, it generates the signature on the message and returns the signature $\sigma = bc\hbar(m) \in S$, where c is randomly chosen from G.

Verification protocol. After getting signature (m, σ), verifier interacts with the signer and follow the verification protocol to check validity of the signature. The complete protocol is depicted in table 1. At the end, if the verifier gets $A_1 = (ra)(\hbar(m)y)$ and $A_2 = (ra)(\sigma s)$ then the signature will be accepted otherwise the verifier will switch to follow the disavowal protocol with the signer.

Signer		Verifier
		$a \leftarrow G$
		$v = a(\hbar(m)s)$
	$\underleftarrow{v}$	
$r \leftarrow G$		
$A_1 = (rb)v \in S$		
$A_2 = cA_1 \in S$		
	$\xrightarrow{A_1, A_2}$	
	$\underleftarrow{a}$	
$v \stackrel{?}{=} a(\hbar(m)s)$		
	$\underrightarrow{r}$	
		$A_1 \stackrel{?}{=} ra(y\hbar(m)) \in S$
		$A_2 \stackrel{?}{=} (ra)(\sigma s) \in S$

Table 1: Verification protocol

Disavowal protocol. After finding the signature as an invalid in verification protocol, the verifier interacts with the signer in disavowal protocol. The complete protocol is depicted in table 2. At the end of protocol if the verifier gets $k = k'$ the verifier convinced that the signature were forged.

5. Security analysis of the scheme

In this section we will prove that the scheme is secure with respect to completeness, soundness and existential unforgeability.

Completeness. According to completeness property which the signer is able to convince the verifier for accepting a valid statement. The proposed zero

Signer		Verifier
		$k \leftarrow \mathbb{Z}_n$
		$\alpha \leftarrow G$
		$C_1 = \alpha\hbar(m)^k \in S$
		$C_2 = \alpha(y\sigma^k) \in S$
	$\xleftarrow{(C_1, C_2)}$	
find k's.t., $b^2(C_1\sigma^{k'}s) = b(C_2\hbar(m)^{k'})$		
	$\xrightarrow{\text{commit}(k')}$	
	$\xleftarrow{\alpha}$	
$C_1 \stackrel{?}{=} \alpha(\hbar(m))^{k'}$		
$C_2 \stackrel{?}{=} \alpha(y\sigma^{k'})$		
	$\xrightarrow{\text{reveal}(k')}$	
		$k \stackrel{?}{=} k'$

In the protocol, commit(k')(k' is a blob[1]) denotes the commitment of k' made by signer and reveal(k') denotes that signer reveals k'.

Table 2: Disavowal protocol

knowledge undeniable signature scheme is complete because both the verification and disavowal protocols are complete as shown by following theorems.

Theorem 5.1 (Completeness of verification protocol)**.** *The verification protocol is said to be complete if the signer always gets $v = a(\hbar(m)s)$ and the verifier gets $A_1 = (ra)(y\hbar(m))$ and $A_2 = (ra)(\sigma s)$ where both of them follow the verification protocol properly.*

Proof. When the verifier sends a to the signer, then the signer checks the equality $v = a(\hbar(m)s)$ and this will hold if the correct value of a is sent by the verifier.

Similarly the signer sends r to the verifier. Then the verifier checks whether $A_1 = (rb)v$ and $A_2 = cA_1$, using signature and public key of the signer. For this, the verifier calculates $A_1 = ra(y\hbar(m))$ and $A_2 = (ra)(\sigma s)$ because value of these terms will be equal to $(rb)v$ and cA_1 respectively as explained below:

$$\begin{aligned} A_1 &= (ra)(y\hbar(m)) = (ra)(bs\hbar(m)) \\ &= (rab)(\hbar(m)s) = (rba)(\hbar(m)s) \\ &= (rb)(a(\hbar(m)s)) = (rb)v. \end{aligned}$$

and

$$\begin{aligned} A_2 &= (ra)(\sigma s) = (ra)((bc\hbar(m))s) \\ &= (rabc)(\hbar(m)s) \\ &= (crb)(a(\hbar(m)s)) = c((rb)v) = cA_1. \end{aligned}$$

□

Theorem 5.2 (Completeness of disavowal protocol)**.** *The disavowal protocol is said to be complete if signer always gets* $C_1 = \alpha(\hbar(m))^{k'}$, $C_2 = \alpha(y\sigma^{k'})$ *and verifier gets* $k = k'$ *when signer and verifier follow the disavowal protocol properly.*

Proof. On receiving α, the signer calculates C_1, C_2 using his/her public-key, signature, hash of the message $\hbar(m)$, and k'. The value of C_1, C_2 calculated by the signer will be equal to the value of C_1, C_2 respectively send by the verifier if the signer finds correct value of k' and the verifier sends correct value of α.

Similarly on receiving k', the verifier checks the equality $k = k'$? The equality will hold if the signer is able to find correct value of k. □

Soundness. The proposed zero knowledge undeniable signature scheme is said to satisfy soundness property, if the probability that the dishonest signer will be able to convince the verifier for accepting an inaccurate result of the communication is negligible.

Theorem 5.3 (Soundness of verification protocol)**.** *The probability that the dishonest signer convince the verifier for accepting invalid signature is not greater than maximum of* $(\frac{1}{\eta}, \frac{1}{\rho}^2)$.

Proof. On receiving v from the verifier, the signer will try to guess a such that $A_1 = (ra)(y\hbar(m))$ and $A_2 = (ra)(\sigma s)$ or the signer will pick (A_1, A_2) such that the equalities $A_1 = (ra)(y\hbar(m))$ and $A_2 = (ra)(\sigma s)$ holds.

The probability of choosing such $a \in G$ is not greater than $\frac{1}{\eta}$, where η is order of G and the probability of choosing $(A_1, A_2) \in S$ is not greater than $\frac{1}{\rho^2}$, where ρ is the cardinality of S. Thus the probability that the dishonest signer can convince the verifier for accepting invalid signature is not greater than maximum of $(\frac{1}{\eta}, \frac{1}{\rho^2})$ and this will be negligible if the size of G and S is chosen appropriately.

□

Theorem 5.4 (Soundness of disavowal protocol)**.** *The probability that the dishonest signer convince the verifier for accepting a valid signature as fraud signature is not greater than* $\frac{1}{n}$.

Proof. Let $\sigma = bc\hbar(m)$ be a valid signature of signer on the message m. Suppose dishonest signer tries to convince the verifier for accepting a valid signature as a fraud signature. To achieve this, signer should guess the correct value of $k \in \mathbb{Z}_n$.

The probability of guessing the correct value of $k \in \mathbb{Z}_n$ is not greater than $\frac{1}{n}$. □

Example 5.5 (Example for defining SAP based protocols)**.** Let R be a semiring and $Mat_m(R)$ be the set of all $m \times m$ matrices with entries in semiring R i.e.,

$$Mat_m(R) = \left\{ \begin{pmatrix} a_{11} & \cdots & a_{1m} \\ \vdots & \ddots & \vdots \\ a_{m1} & \cdots & a_{mm} \end{pmatrix} \text{ such that } a_{ij} \in R \right\} \tag{1}$$

Let $C \subset R$ be the center of R i.e., the subset of R consisting of elements that commutes with any other element. Then C forms a commutative semiring and $C[t]$, the polynomial semiring in the indeterminant t also forms commutative semiring over C. If $A \in Mat_{m\times m}(R)$ then $C[A]$ forms a commutative semiring [15] of the matrix semiring $Mat_{m\times m}(R)$.

If $p(t) = u_0 + u_1t + u_2t^2 + \cdots + u_nt^n \in C[t]$ then,

$$p(A) = u_0 + u_1A + u_2A^2 + \cdots + u_nA^n.$$

Now, consider the semiring,

$$G = C[A] = \{p(A) \mid p(t) \in C[t]\}$$

and

$$M = C_1[A] = \{p(A) \mid p(t) \in C[t] \text{ where } u_0 = u_{2k+1} = 0 \text{ for } n, k = 0, 1, 2, \cdots\}$$

and $S = C_2[A] = \{q(A) \mid q(t) \in C[t]$ where $u_i \neq 0$ for any $i = 0, 1, 2, \cdots\}$ then $S \cap M = \{\Phi\}$.

Now, φ define a semigroup action of M over S i.e., $\varphi : M \times S \to S$ such that $p(A)q(A) = t(A) \in S$.

This example can be taken to design the above proposed zero knowledge undeniable signature scheme.

6. Conclusion

In this paper we proposed a zero knowledge undeniable signature scheme whose security relies on the hardness of SAP. We also proved that the proposed scheme satisfies the completeness and soundness property. In future, we will try to give the security proof of scheme in random oracle and the appropriate size of parameters to achieve better security. We will also try to design other cryptographic protocols like digital signature scheme, authentication scheme, signcryption scheme over SAP.

References

[1] G. Brassard, D. Chaum, C. Crépeau, *Minimum disclosure proofs of knowledge*, Journal of computer and system sciences, 37 (1988), 156-189.

[2] D. Chaum, H. V. Antwerpen, *Undeniable Signatures*, LNCS, 435 (1989), 212-216, (CRYPTO'89).

[3] D. Chaum, *Zero-Knowledge Undeniable Signatures*, LNCS, 435 (1990), 458-464, (Eurocrypt'90).

[4] W. Diffie, M. E. Hellman, *New Directions in Cryptography*, IEEE Transactions on Information Theory, 1976.

[5] R. Gennaro, H. Krawczyk, T. Rabin, *RSA-based Undeniable Signatures*, LNCS 1294 (1997), 132-149, (CRYPTO '97).

[6] Jonathan Katz, Yehuda Lindell, *Introduction to Modern Cryptography*, Chapmen & Hall/CRC Press, 2008.

[7] C. Monico, *Semirings and Semigroup Actions in Public-Key Cryptography*, Ph.D. thesis, University of Notre Dame, May 2002.

[8] Gerard Maze, C. Monico, Joachim Rosenthal, *Public Key Cryptography Based on Semigroup Action*, January 2005.

[9] Gerard Maze, C. Monico, Joachim Rosenthal, *Public Key Cryptography Based on Semigroup Action*, Advances in Mathematics communication, 2007.

[10] A. J. Menezes, P. C. Van Oorschot, S. A. Vanstone, *Handbook of Applied Cryptography*, CRC Press, 1997.

[11] W. Ogata, K. Kurosawa, *The Security of FDH Variant of Chaum's Undeniable Signature Scheme*, IEEE Transactions of Information Theory, May 2006.

[12] R. L. Rivest, A. Shamir, L. Adleman, *A Method for Obtaining Digital Signature and Public Key Cryptosystems*, Commun. ACM, Feb. 1978.

[13] Douglas R. Stinson, *Cryptography Theory and Practice*, Chapmen & Hall/CRC Press, Second Indian reprint, 2013.

[14] T. Thomas, A. K. Lal, *A Zero Knowledge Undeniable Signature Scheme in Non-abelian Group Setting*, International journal of Network Security, May 2008.

[15] Jens Zumbr̈agel, *Public-key cryptography based on simple semirings*, Ph.D. Thesis, University of Zürich, 2008.

Accepted: 12.08.2016