# A NON-REPUDIABLE BIASED BITSTRING COMMITMENT SCHEME ON A POST QUANTUM CRYPTOSYSTEM

**[1]D.B.OJHA , [2]J.P.PANDEY, [3]AJAY SHARMA, [4]ABHISHEK DWIVEDI**

[1] Asstt.Prof., Department of Mathematics, RKGIT, Ghaziabad, India -201003

[2] Prof., Department of Electrical Engineering, KNIT, U.P.T.U., Sultanpur India

[3] Asstt.Prof., Department of Information Technology, RKGIT, Ghaziabad, India -201003

[4] Lecturer, Department of M.C.A., RKGEC, Ghaziabad, India -201003

**ABSTRACT**

Commitment schemes are fundamental bricks for guaranteeing fairness in upper level cryptographic protocols. Most commitment schemes in the literature rely on hash functions, which should be strongly collision free for the scheme to be secure. We present a commitment scheme, which avoids hash functions by using a public-key cryptosystem based on braid conjugator search problem instead.

**Key words:** *Biased bit string commitment, braid group, conjugator search problem.*

## 1. INTRODUCTION

In cryptography, a commitment scheme or a bit commitment scheme is a method that allows a user to commit to a value while keeping it hidden and preserving the user's ability to reveal the committed value later. A useful way to visualize a commitment scheme is to think of the sender as putting the value in a locked box, and giving the box to the receiver. The value in the box is hidden from the receiver, who cannot open the lock (without the help of the sender), but since the receiver has the box, the value inside cannot be changed. Commitment schemes are important to a variety of cryptographic protocols, especially zero-knowledge proofs and secure computation [1, 2].

Over the past two decades, a bulk of excellent protocols based upon bit commitment has been followed by the first constructions on bit commitment [1,7,8], many improvements have been proposed [2,9,10,11,12]. In 1988, Goldreich *et al*. [9] presented another factoring-based bit commitment scheme which is more efficient than Blum's [1]. In 1989, Naor [2] reduced the properties of bit commitment schemes on information-theoretically binding and computationally hiding to pseduo-randomness.

Shortly afterwards, Naor *et al*. [2] also reduced the properties of bit commitment schemes on *computationally binding* and information-theoretically hiding to one-way permutation. In 1992, Pedersen [10] proposed a bit commitment scheme based on discrete logarithm problem.

In 1996, Halevi and Micali [11] also put forward a new bit commitment scheme by using a collision-free one-way hash function. In [2], a general framework was introduced for building bit commitments using one-way functions. The drawback of those early schemes is that they only allow commitment to a single bit, whereas committing to a bitstring is a fundamental need in many cryptographic applications. Most commitment schemes in the literature are based on hash functions, which cause them to share two shortcomings:

1. The hash functions used should be strongly collision free. However, this property can only be empirically checked. It actually turns out that some

schemes are inadvertently based on weakly collision-free hash functions [13].
2. Hash functions alone cannot offer non-repudiability.

## 2. PRELIMINARIES:

### 2.1. Crisp Commitment Schemes:

In a commitment scheme, one party Alice (sender) aim to entrust a concealed message m to the second party Bob(receiver) , intuitively a commitment scheme may be seen as the digital equivalent of a sealed envelope. If Alice wants to commit to some message m she just puts it into the sealed envelope, so that whenever Alice wants to reveal the message to Bob, she opens the envelope. First of all the digital envelope should hide the message from, Bob should be able to learn m from the commitment. Second, the digital envelope should be binding , meaning with this that Alice can not change her mind about m, and by checking the opening of the commitment one can verify that the obtained value is actually the one Alice had in mind originally[3,4].

### 2.2 Braid Groups:

Emil Artin [5] in 1925 defined $B_n$, the braid group of index n, using following generators and relations: Consider the generators $\sigma_1, \sigma_2, \ldots\ldots \sigma_n$, where $\sigma_i$ represents the braid in which the $(i+1)^{st}$ string crosses over the ith string while all other strings remain uncrossed. The defining relations are

1. $\sigma_i \sigma_j = \sigma_j \sigma_i$ for $|i-j| \geq 2$,

2. $\sigma_i \sigma_j \sigma_i = \sigma_j \sigma_i \sigma_j$ for $|i-j| = 1$

An n-braid has the following geometric interpretation: It is a set of disjoint n-strands all of which are attached to two horizontal bars at the top and at the bottom such that each strands always heads downward as one walks along the strand from the top to the bottom. In this geometric interpretation, each generator $\sigma_i$ represents the process of swapping the $i^{th}$ strand with the next one (with $i^{th}$ strand going under the $(i+1)^{th}$ one). Two braids are equivalent if one can be deformed to the other continuously in the set of braids. $B_n$ is the set of all equivalence classes of geometric n-braids with a natural group structure. The multiplication *ab* of two braids *a* and *b* is the braid obtained by positioning *a* on the top of *b*. The identity *e* is the braid consisting of *n* straight vertical strands and the inverse of *a* is the reflection of a with respect to a horizontal line. So $\sigma^{-1}$ can be obtained from $\sigma$ by switching the over-strand and under-strand.

$\Delta = (\sigma_1, \sigma_2 \ldots\ldots\ldots \sigma_{n-1})(\sigma_1, \sigma_2 \ldots\ldots\ldots \sigma_{n-2}) \ldots\ldots$
$\ldots\ldots\ldots (\sigma_1, \sigma_2)(\sigma_1)$

is called the fundamental braid.

We describe some mathematically hard problems in braid groups. We say that *x* and *y* are conjugate if there is an element *a* such that $y = axa^{-1}$. For $m < n; B_m$ can be considered as a subgroup of $B_n$ generated by $\sigma_1, \sigma_2 \ldots\ldots\ldots \sigma_{m-1}$.

In 2000, Ko et al. [6] proposed a new public key cryptosystem on braid groups based on the hardness of the conjugacy problem.
Since the scheme based on Braid groups is one of the interesting candidates for post quantum cryptography[14]. Hence our proposed scheme is useful for post quantum cryptographic commitment scenario.

## 3. OUR PROPOSED SCHEME:

A commitment should be *non-repudiable*: it should not be possible for party A to deny having committed to value. Non-repudiability can be achieved by having the commitment signed by the committing party. Here we also considers a different non-trivial generalization, Party A commits a number to Party B with a given, fixed bias 1/*k*, while the basic bit commitment can be viewed as a special case of setting bias value to 1/2. Now a non-repudiable 1/*k*-biased bit string commitment primitive is a two-parties, says *A* and *B*, interactive procedure which includes two protocols, a protocol 1 for commitment and a protocol 2 for opening/verifying the commitment.

### Protocol 1(commitment):

**1. Initial State:** The committing party A is assumed to have an asymmetric key pair $(P_A, S_A)$. Where $P_A$ is the public key and $S_A$ is the private key. Further it is assumed that public key is duly certified and publicly accessible.
Two braids $S_A(\mathrm{V})$ and $S_A(w)$ are conjugate, if there exist at least one braid $P_A(\mathrm{R})$ such that $S_A(w) = P_A(R) S_A(V) P_A^{-1}(R)$. In general, if $S_A(V) \approx S_A(w)$, their conjugators are not

unique. $B_n$ is infinite and non- commutative so conjugacy problems on braid are non-trivial. Let $b \in \{0,1,2.....k-1\}$ B choose $k$ random braids $V_0, V_1.....V_{k-1} \in B_n^k$ and sends them to $A$.

**2. Commit phase:**

(i). $A$ chooses the bitstring $v_b$ and generates a pseudo-random value $r$, such that $R = Id_A \square r$ and $P_A(R) \in_R B_n$.

(ii). $A$ concatenates his identifier $Id_A$ with and obtain $V = Id_A \square v_b$.

(iii) $A$ signs $V$ to obtain $S_A(V)$.

(iv) The commitment $C_A$ to be published is obtained as $C_A = P_A(R)S_A(V)P_A^{-1}(R)$ .

( v) A publishes $C_A$ and also sends to B.

Now $A$ sends the procedure for revealing the hidden commitment at required time interval and $B$ use this. So $A$ disclose the procedure and $r$ to $B$ to open the commitment

**Protocol 2 (commitment opening and verification):**

(i) A reveals the value $r$ to a verifier $B$ ( infact , $A$ can publish $r$ at large).

(ii) The verifier $B$ retrieves $S_A(V)$ as $P_A^{-1}(R)C_A P_A(R) = S_A(V)$.

(iii). $B$ encrypts $S_A(V)$ under $P_A$ to obtain $V$.

(iv) $B$ verifies that $V$ contains $Id_A$ as prefix (if everything is correct, one should have $V = Id_A \square v_b$).

(v) The commitment is deemed valid if and only if $Id_A$ is a prefix of $V$. In that case the suffix $v_b$ of $V$ is taken as the value committed to.

**4. ANALYSIS:**

**4.1** Let us now drive the probability that the commitment can be non-uniquely opened. For $A$ to open $C_A$ as $V' \neq V$ one must have $P_A(R')C_A P_A^{-1}(R') = S_A(V')$ for some $R'$.This is equivalent to requiring that $R' = S_A(S_A(V')C_A S_A^{-1}(V'))$ for some $R'$.If correct public-key cryptosystem is used, the probability that the prefix of $S_A(S_A(V')C_A S_A^{-1}(V'))$ matches $Id_A$ can be approximated by $2^{-|Id_A|}$, where $|Id_A|$ is the bit length of $Id_A$.

Finally, non-repudiability of $C_A$ follows from the fact that the $V$ committed to is concatenated to $A$'s identifier $Id_A$ and the whole is signed by $A$ as $S_A(V)$.

**4.2** The proposed scheme in section 3 is correct.

The correctness of $1/k$ -biased bit string commitment means

(i) $A$'s commitment will be accepted if $A$ opens the original committed value.

(ii) $A$'s commitment will be rejected if $A$ opens value which is different from the original committed value.

(iii) $A$'s commitment is concealed before open phase.

If $A$ commits a value $v_b \in \{v_0, v_1, .....v_{k-1}\}$ in the commit phase, $A$ sets $x = P_A(R)S_A(V)P_A^{-1}(R)$ and sends $x$ to B. In the open phase, let $A$ wants to open the original committed value, then sends $(b, R)$ to $B$. Then $B$ will output 'Yes', when $B$ checks whether $x = P_A(R)S_A(V)P_A^{-1}(R)$. Therefore, $B$ will accept $A$'s commitment . Later, in the open phase $A$ wants to open another value $b' \neq b$, $A$ sends $(b', R)$ to $B$. Now, $B$ will output 'No', when $B$ checks whether $x = P_A(R)S_A(V')P_A^{-1}(R)$, since $S_A(V') \neq S_A(V)$. Therefore, $B$ will reject $A$'s commitment.

Before the open phase, $B$ knows the $\{V_0, V_1.....V_{k-1}\}$ and $x$, which are not enough to reveal $b$, since for each $V_i$, there may exist $R_i$ such that $x = P_A(R_i)S_A(V_i)P_A^{-1}(R_i)$ . So $A$'s committed value $b$ is concealed before the open phase. By guessing, $B$ has exactly $1/k$ probability to reveal the committed value. Therefore, the proposed scheme is a correct $1/k$ -biased bit string commitment protocol also.

**4.3** The proposed scheme in Section 3 is computationally binding.

Can $A$ find a way to commit a value and later another value to $B$ without being detected? In order to cheat successfully, $A$ has to find a pair of collisions i.e., two elements $P_A(R_1), P_A(R_2) \in B_n$ such that

$$P_A(R_1)S_A(V_i)P_A^{-1}(R_1) = P_A(R_2)S_A(V_j)P_A^{-1}(R_2), (i \neq j) \quad (1)$$

Suppose that $A$ can indeed find such a pair of collisions. Then $A$ can get the following:

$$P^{-1}{}_A(R_2)P_A(R_1)S_A(V_i)P_A^{-1}(R_1)P_A(R_2) = S_A(V_j), (i \neq j) \quad (2)$$

This suggest that $A$ can find the conjugator $w = P^{-1}{}_A(R_2)P_A(R_1)$ for the pair $(V_i, V_j) \in B_n \times B_n$. However, under the assumption that the conjugator search problem is intractable, that is $A$ can find a conjugator for the pair $(V_i, V_j) \in B_n \times B_n$ is negligible.

Therefore, under the assumption that the conjugator search problem is intractable, $A$ has no way to cheat , i.e., the proposed scheme is computationally binding.

**4.4** The proposed scheme in section 3 is information theoretically hiding.

Can $B$ find a way to practice fraud i.e., intract $A$'s commitment before the open phase? Let, if $B$ find $R$ and $RT$ are at $A$'s choice with the same property. $B$ has no any clue to deduce that $A$ picks $R$ instead of $RT$; and vice-verse. Further, for each $V_i$, there may exist $R_i$ such that $x = P_A(R_i)S_A(V_i)P_A^{-1}(R_i)$. Thus, if $B$ has the capability to find all conjugators for $(x, V_0), .., (x, V_{k-1})$, $B$ still has no any clue to deduce which $i$ has the commitment value $v_b$, since $B$ still can not decide which conjugator is $A$'s choice of $R$.

Infact, $B$ has no chance to practice fraud no matter how powerful computation ability possesses, i.e., the proposed scheme is information theoretically binding.

## 5. CONCLUSION

Non-repudiable commitment schemes are an essential part of secure e-gaming and e-gambling protocols. In fact, such schemes are a guarantee that player misbehaviors or deviations from the protocols will be detected. Using the new primitive, one party is allowed to commit a value to another party with a given, fixed bias while the basic bitstring commitment can be viewed as special case when the bias value is set to $1/2$. Using a public-key cryptosystem to construct a commitment is away of achieving non-repudiability, a property which cannot be offered by hash functions alone. In this paper, we have presented a commitment scheme that allows a player to commit to a bitstring in a non-repudiable way based on the braid conjugator search problems with $1/k$-biased bitstring commitment scheme, which is information theoretically hiding and computationally binding.

## REFERENCES:


[1] M. Blum, "Coin flipping by telephone: a protocol for solving impossible problems", Proc. IEEE Computer Conference, pp. 133-137, 1982.

[2] M. Naor, "Bit commitment using pseudorandomness", in Advances in Cryptology-Crypto'89, LNCS 435, Berlin: Springer, pp.128-136, 1990.

[3] Alawi A. Al-saggaf, Acharya H. S. "A generalized Framework for Crisp Commitment Schemes" eprint.iacr.org/2009

[4] Alawi A. Al-saggaf, Acharya H. S: Mathematics Of Bit-Commitment Schemes, Bulletin of the Marathwada Mathematical Society,Vol. 8, No. 1, June 2007, pages 08 – 15.

[5] E. Artin, "Theory of braids," Annals of Mathematics, vol. 48, pp. 101-126, 1947.

[6] K. Ko, S. Lee, J. Cheon, J. Han, J. kang C. Park. New public key cryptosystem using braid groups, Crypto'2000, LNCS 1880, pp.166-183, Springer 2000.

[7]. M. Rabin, "How to exchange secrets by oblivious transfer," Technical Report No.TR-81, Harvard Aiken Computation Laboratory, Cambridge, 1981.

[8]. A. Shamir, R. L. Rivest, and L. M. Adleman, "Mental poker," in D. Klarner ed., TheMathematical Gardner, Wadsworth, Belmont, California, 1981, pp. 37-43.

[9]. S. Goldreich, S. Micali, and R. Rivest, "A digital signature scheme secure against

adaptive chosen message attacks," SIAM Journal of Computing, Vol. 17, 1988, pp.281-308.

[10]. T. P. Pedersen, "Non-interactive and information theoretic secure verifiable secret sharing," in Proceedings on Advances in Cryptology – CRYPTO, LNCS 576, Springer, 1992, pp. 129-140.

[11]. S. Halevi and S. Micali, "Practical and provably secure commitment schemes from collision free hashing," in Proceedings on Advances in Cryptology –CRYPTO,LNCS 1109, Springer, 1996, pp. 201-215.

[12]. D. Zheng, K. Chen, D. Gu, and J. You, "Efficient bit-commitment schemes," Journalof China Institute of communications, Vol. 21, 2000, pp. 78-80.

[13]. B. Preneel, "The state of cryptographic hash functions", in Lectures on Data Security: ModernCryptology in Theory and Practice, LNCS 1561, Berlin: Springer, pp. 158-192, 1999.

[14].Johannes Buchmann, Carlos Coronado, Martin D¨oring, Daniela Engelbert, Christoph udwig, Raphael Overbeck, Arthur Schmidt ,Ulrich Vollmer, Ralf-Philipp Weinmann,"Post-Quantum Signatures",eprint.iacr.org/2004/297.