IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 18 April 2024, accepted 24 June 2024, date of publication 2 July 2024, date of current version 20 August 2024.

Digital Object Identifier 10.1109/ACCESS.2024.3421995

RESEARCH ARTICLE

Lattice-Based Commitment Scheme for Low Communication Costs

HIDEAKI MIYAJI[1], (Member, IEEE), YUNTAO WANG[2], (Member, IEEE), AND ATSUKO MIYAJI[3], (Member, IEEE)

[1]College of Information Science and Technology, Ritsumeikan University, Ibaraki, Osaka 567-8570, Japan
[2]Graduate School of Informatics and Engineering, The University of Electro-Communications, Chofu, Tokyo 182-8585, Japan
[3]Graduate School of Engineering, Osaka University, Suita, Osaka 565-0871, Japan

Corresponding author: Hideaki Miyaji (h-miyaji@fc.ritsumei.ac.jp)

This work was supported in part by the Japan Society for the Promotion of Science (JSPS) KAKENHI under Grant JP21H03443, Grant JP21K11751, and Grant JP24K20774; and in part by the SECOM Company Ltd., Science and Technology Foundation.

ABSTRACT Commitment schemes are cryptographic schemes that can be applied to zero-knowledge proof construction and blockchain construction. Recently, lattice-based cryptography has been intensively investigated due to the promising potential in quantum cryptography. Accordingly, commitment schemes based on lattice assumptions have been studied for practical applications. Notably, applications often require committing an arbitrary message with low communication costs, so commitment schemes must be satisfied with fewer length restrictions and fewer extensions to the messages. Several studies have been conducted to achieve the problem, including the study published by Baum et al. in 2018. However, the output length of their scheme is large in relation to the input length. We design a *length-extension-free* commitment scheme $\mathsf{Com}_{\mathsf{MWM}}$ in which the length of the message string is large relative to the length of the commitment string, improving on the commitment scheme of Baum et al. Furthermore, we prove that the hiding and binding properties of $\mathsf{Com}_{\mathsf{MWM}}$ are based on the hardness of the decisional search knapsack problem and extended search knapsack problems, respectively. Finally, we evaluate the computation costs of generating commitment value between ours and Baum et al.'s commitment scheme.

INDEX TERMS Commitment scheme, lattice-based protocol, hiding property, binding property, AES-128.

I. INTRODUCTION

Commitment schemes are important cryptosystems since they are used in blockchain construction [2], [3] and the zero-knowledge proof construction [4], [5]. A commitment scheme is executed between the commitment phase and the decommitment phase. In a commitment scheme, commitment string and decommitment string are used. The commitment string is the encrypted value of the message string, and the decommitment string includes the message. During the commitment phase, the sender sends the commitment string to the receiver. During the decommitment phase, the sender sends the decommitment string to the receiver. The receiver verifies whether the decommitment string is constructed from the commitment string. In other words, the receiver can verify whether the commitment string and decommitment string are valid or not in the decommitment phase. The commitment scheme is secure when both the binding property and the hiding property satisfied [6], [7]. In the binding property, we have to prove that the sender cannot construct a commitment string from two different decommitment strings. In the hiding property, when the receiver gets two different commitment strings, we have to prove that the receiver cannot determine whether they are composed of one or the other before the decommitment string is sent in the decommitment phase. In other words, the receiver cannot get any partial message information in the commitment phase. Lattice-based commitment schemes have attracted much attention in recent years since they can prevent quantum computer attacks.

A. EXISTING RESEARCH

In 1982, Blum proposed the concept of a one-way commitment scheme but Blum did not propose the concrete construction [8]. The first commitment scheme was designed based on the hardness of factoring by Goldwasser et al.

The associate editor coordinating the review of this manuscript and approving it for publication was Gang Li.

in 1988 [9]. Another scheme based on the discrete logarithm problem was developed by Pedersen in 1991 [10]. Also, Halevi and Micali proposed the commitment scheme based on the collision resistance hash function (Message Digest) in 1996 [11].

A commitment scheme is a key tool for designing cryptographic protocols. Furthermore, commitment schemes have numerous applications, such as threshold encryption [12] and electronic voting [13]. In particular, the security of the protocol against malicious attacks can be enhanced by using commitment schemes to construct zero-knowledge proof [14]. If a commitment scheme is designed based on post-quantum cryptography, its security can be guaranteed in the long term.

Research on post-quantum commitment schemes is important since they can prevent attacks from quantum computers. One of the post-quantum commitment schemes is the lattice-based commitment scheme. Several security notions, including the module short integer solution problem (M-SIS), search knapsack problem (SKS), and decisional knapsack problem (DKS), exist in conjunction with the lattice problem. The objective of M-SIS is to determine a search short vector of ring polynomial x that satisfies $A \cdot x = 0$ from ring polynomial matrix A. M-SIS essentially exemplifies the vector knapsack problem over a particular ring. SKS, expressed as $SKS^2_{n,k,\beta}$, is the problem of searching for a short vector of ring polynomial x that satisfies $(I||A)\cdot x = 0$, where A is a polynomial ring matrix, and I is an identity matrix. DKS, expressed as $DKS^{\infty}_{m,k,\beta}$, is a problem of determining whether a distribution is uniform or originates from $A \cdot x$.

In 2008, Kawachi et al. constructed the first lattice-based commitment scheme [15], based on the SIS problem committed to vectors over binary numbers. However, the message length or dimensionality of committable messages is restricted to small-norm vectors to maintain the binding property. This limitation is not found in the standard cryptographic commitment scheme based on the discrete logarithm or factoring problems. In the lattice-based commitment scheme, several studies have tried to eliminate the limitation on message length. Benhamouda et al. used the ring-learning with errors (R-LWE) problem to construct a commitment scheme with the small limitation of the message length [16] in 2015 (BKLP15). BKLP15 eliminates certain restrictions on the message length using the residue ring of a polynomial ring. The message length of BKLP15 is *one*, and the output length of BKLP15 is k. In contrast, Baum et al. constructed a commitment scheme based on the knapsack problem [14] in 2018. This scheme is referred to as BDLOP18. The message length and the output length of BDLOP18 are $m - n$ and m respectively.

Although the aforementioned schemes offer less restricted input lengths, their output lengths are still extensions of their message lengths. A commitment scheme with less restriction of input length with respect to output length is needed for message transmission at a smaller communication cost.

B. OUR CONTRIBUTION

We define the novel concept of the extension ratio (ER) in a commitment scheme as

$$ER = \frac{|\text{length of commitment string}|}{|\text{length of message string}|}.$$

The extension ratio (ER) is the ratio of the output length to the input length of a commitment scheme. For example, when the input length is m and the output length is m, the input and output length have the same ratio, $ER = 1$. Consequently, ER measures the ratio of messages sent in a commitment scheme. We call the commitment scheme with $ER = 1$ as a ***length-extension-free*** commitment scheme. On the other hand, ER of BKLP15 and BDLOP18 is 2. In this paper, we propose a commitment scheme satisfying $ER = 1$ to realize a length-extension-free commitment scheme. We propose the $ER = 1$ commitment scheme by extending the lattice-based commitment scheme in BDLOP18 [14]. Our proposed commitment scheme is the smallest ER lattice-based commitment scheme. We remark that it is obvious that a commitment scheme based on the hash function satisfies $ER < 1$. However, it is not easy to apply them to zero-knowledge Boolean or arithmetic circuits [17]. In this paper, we focus on the commitment scheme that are based on some mathematical assumptions and could be combined with some zero-knowledge Boolean or arithmetic circuits. In BDLOP18 [14], the commitment string $c^{\mathsf{BDLOP}}_{m-n,m}(x, r)$ is constructed by using the message string x, public parameter A, random vector r, and positive integer n. BDLOP18 is defined as follows, focusing on the lengths of the message and commitment strings:

$$c^{\mathsf{BDLOP}}_{m-n,m}(x, r) = A \cdot r + \begin{bmatrix} 0^n \\ x \end{bmatrix}.$$

Here, the message length and the output length of $c^{\mathsf{BDLOP}}_{m-n,m}(x, r)$ are $m - n$ and m respectively. Note that this scheme exactly extends the length of the commitment string to that of the message string. BDLOP18 satisfies the binding property under $SKS^2_{n,k,\beta}$ and the hiding property under $DKS^{\infty}_{m,k,\beta}$.

We designed a commitment scheme in which the length of the commitment string has no expansion to the length of the message string. To achieve this, we implemented a message vector x to commitment string $c_{m,m}(x, r)$ by using a public parameter A and a random vector r. The construction of our proposed commitment scheme is expressed as follows.

$$c_{m,m}(x, r) = A \cdot r + x.$$

Here, the message length and the output length of $c_{m,m}(x, r)$ is m. Consequently, our proposed $c_{m,m}(x, r)$ optimizes the length of the commitment string to that of the message string, thus satisfying an ER of 1. The binding property of our $c_{m,m}(x, r)$ is secure based on Extended-$SKS^2_{n,k,\beta}$ problem. The hiding property of our $c_{m,m}(x, r)$ is secure based on $DKS^{\infty}_{m,k,\beta}$ problem.

This paper is the final version of the studies presented at ISPEC 2021 [1]. In this paper, the following sections have been added:

- A detailed proof of the binding and hiding properties of $\mathsf{Com}_{\mathsf{MWM}}$.
- An evaluation comparing $\mathsf{Com}_{\mathsf{MWM}}$, BDLOP18, and BKLP15.
- Suggested parameters for $\mathsf{Com}_{\mathsf{MWM}}$, BDLOP18, and BKLP15 based on AES-128.
- Implement $\mathsf{Com}_{\mathsf{MWM}}$ and the BDLOP18 commitment schemes and compares the computation cost.

Since our commitment scheme can input larger messages within the same output length compared with BDLOP18 [14], various applications that make use of commitments can improve their performance by using our commitment scheme. For example, the location-based service proposed by Peng et al. [18] and blockchains in combination with neural networks such as [19] are good applications that can use our commitment scheme.

C. PAPER ORGANIZATION

Section II summarizes the definitions and the notations. Section III describes previous research on our design. Our commitment scheme is presented in detail in Section IV. A comparison between our commitment scheme and existing schemes is described in Section V. Finally, the paper is concluded in Section VI.

II. PRELIMINARIES

This section summarizes all the notations and definitions used throughout the paper.

A. LATTICE PROBLEM

This subsection describes the basic notations and definitions required for the lattice problem. First, we summarize the basic notation of the lattice problem used in this paper, and then we define the lattice problem.

- $\mathbb{R}$: set of real numbers
- $\mathbb{Z}$: set of integers
- $\mathbb{N}$: set of positive integers
- q: prime number
- $N(=2^r)$: degree of polynomial rings
- $\mathbb{F}_2$: prime field with a characteristic of 2
- Lattice L: set of all linearly independent integer linear combinations of vectors
- $vol(L)$: volume of lattice L
- polynomial rings $R = \mathbb{Z}[X]/\langle X^N + 1\rangle$
- polynomial rings $R_q = \mathbb{Z}_q[X]/\langle X^N + 1\rangle$
- In each $f \in R$, let f denote as $f = \Sigma_i f_i X^i$ and each norm expressed as
  - $||f||_1 = \Sigma_i |f_i|$: l_1 norm
  - $||f||_2 = \left(\Sigma_i |f_i|^2\right)^{1/2}$: l_2 norm
  - $||f||_\infty = \max_i |f_i|$: l_∞ norm
- I_n: identity matrix with $n \times n$
- S_β: set of all elements $x \in R$ with l_∞-norm at most β
- C: subset of S_1 that encompasses challenges
- κ: maximum l_1 norm of any element in C
- $\sigma = 11 \cdot \kappa \cdot \beta \cdot \sqrt{k \cdot N}$: standard deviation used in zero-knowledge proof
- gamma function $\Gamma(s) = \int_0^\infty t^{s-1} \cdot e^{-t} dt$
- $(x^i)^{1 \le i \le n}$: $1 \le i \le n$ th column element of vector x.

Next, we define the lattice problem.

Definition 1 (Lattice Problem [20]): Let $\mathbb{R}$ be the set of real numbers and let $\mathbb{R}^n$ be the Euclidean space of n-dimensional real vectors. If $a_1, \ldots, a_n$ are linearly independent vectors in an $\mathbb{R}^n$, then we say that the set $\{\sum_{i=1}^n k_i a_i | k_1, \ldots, k_n$ are integers$\}$ is a lattice in $\mathbb{R}^n$. We denote lattice by $L(a_1, \ldots, a_n)$. The set $a_1, \ldots, a_n$ is called a basis of the lattice.

B. RELATED WITH COMMITMENT SCHEME

This subsection describes the basic notation and definitions of commitment schemes used in this paper and describes the definitions of the security problem necessary to securely construct a commitment scheme. We introduce an abbreviation of notations used in this paper in Table 1.

- 1^k: security parameter
- Sender: sender
- Receiver: receiver
- $\mathsf{Com}_{\mathsf{MWM}}$: our proposed commitment scheme
- com: commitment string
- dec: decommitment string
- message space: domain of messages that can be committed
- PP: public parameter used in a commitment scheme
- $\varepsilon(k)$: negligible function with k
- PPT: probabilistic polynomial-time algorithm
- $\perp$: rejection output for the invalid inputs
- $\mathrm{Hw}(x)$: Hamming weight of x
- $\Delta(x)$: ratio of "1"s in x, also called as the relative Hamming weight
- extension ratio (ER): the ratio of the output length to the input length of a commitment scheme
- *Length-extension-free* commitment scheme: the commitment scheme which satisfies ER=1

We define a commitment scheme that follows [21].

Definition 2 (Commitment Scheme [21]): A commitment scheme Com(Sender, Receiver) *is constructed by the commitment phase and the decommitment phase between* Sender *and* Receiver.

In the commitment phase, Sender *constructs a commitment string* com *from a message string a and public parameter PP.* Sender *also constructs decommitment string* dec *which includes a by executing* Sender$(1^k, a, PP) \rightarrow$ (com, dec). Sender *sends commitment string* com *to* Receiver.

In the decommitment phase, Sender *sends decommitment string* dec *to* Receiver. *Then,* Receiver *verifies whether* com *can be constructed from* dec *by executing*

TABLE 1. Abbreviations used in this paper.

Abbreviations	Meanings
BKLP15	Benhamouda-Krenn-Lyubashevsky-Pietrzak-2015 [16]
BDLOP18	Baum-Damgard-Lyubashevsky-Oechsner-Peikert-2018 [14]
SKS	Search KnapSack problem
DKS	Decisional KnapSack problem
SIS	Short Integer Solution problem
LWE	Learning With Errors problem
ER	extension ratio

Receiver(com, dec). *If* com *is not constructed from* dec *during commitment phase,* Receiver(com, dec) *outputs a special string* $\perp$. *Otherwise,* Receiver(com, dec) *outputs message string a.*

We define the computational binding property of a commitment scheme. The computational binding property defines the difficulty for a malicious PPT adversary $\mathcal{A}$ to construct the commitment string com. When it is difficult to construct the same commitment string com from the different message strings a, a' by the PPT adversary $\mathcal{A}$, the commitment scheme satisfies the computational binding property. A more detailed definition is given in Definition 3.

Definition 3 (Computational Binding Property [14]): Let $\mathcal{M}$ *be a message space, let* $a \in \mathcal{M}$ *be a message string, let* com *be a commitment string, and let* dec *be a decommitment string where* dec *is a string used by* Receiver *for verification in the decommitment phase.* **Sender** *construct a commitment string by executing* Com(Sender, Receiver)*, and* $\mathcal{A}$ *be a PPT adversary. The commitment scheme satisfies the binding property if the following is satisfied.*

$$\Pr\left[\begin{array}{c} \textbf{\textit{KeyGen}} \rightarrow PP \\ \mathcal{A}(PP) \rightarrow (\mathsf{dec}, \mathsf{dec}', \mathsf{com})\ s.t.\ a \neq a' \wedge \\ \textbf{Sender}(1^k, a, PP) = (\mathsf{com}, \mathsf{dec}) \wedge \\ \textbf{Sender}(1^k, a', PP) = (\mathsf{com}, \mathsf{dec}') \end{array}\right] < \varepsilon(k)$$

We next define the computational hiding property of a commitment scheme. The computational hiding property defines the difficulty for a malicious PPT adversary $\mathcal{A}$ to identify the commitment string com. If the PPT adversary $\mathcal{A}$ is given the commitment string com or a uniform distribution u, and it is difficult to correctly identify which distribution was given, the commitment scheme satisfies the computational hiding property. A more detailed definition is given in Definition 4.

Definition 4 (Computational Hiding Property [7], [14]): Let $\mathcal{M}$ *be a message space, let* com *be a commitment string constructed from a message string* $a \in \mathcal{M}$*, and let* $\mathcal{A}$ *be a PPT adversary.* $\mathcal{A}$ *given a commitment string* com *or a uniform distribution u, and the commitment scheme satisfies the computational hiding property when the probability that* $\mathcal{A}$ *can determine either is less than* $\varepsilon(k)$*.*

$$|\Pr[\mathcal{A}(\mathsf{com}) = 1] - \Pr[\mathcal{A}(U) = 1]| < \varepsilon(k)$$

We define the statistical distance before we define the statistical hiding property.

Definition 5 (Statistical Distance [11]): Let ϕ_1 *and* ϕ_2 *as probability distributions, let S as a finite set. The statistical distance between two probability distribution* $d(\phi_1, \phi_2)$ *can be defined as*

$$d(\phi_1, \phi_2) = \frac{1}{2}\sum_{x \in S} |\phi_1(x) - \phi_2(x)|.$$

Definition 6 (Statistical Hiding Property [11]): Let $a \in \{0,1\}^*$ *be a message string, let* Com(Sender, Receiver) *be a commitment scheme constructed from a, let* $C_k(a)$ *denote the distribution over the commitment string for a, and let* ϕ_1, ϕ_2 *be a probability distributions.* $C_k(a)$ *is then the distribution of the first coordinates of the pair obtained by the algorithm* Sender$(1^k, a)$. ϕ_1 *denotes the probability distribution of* $C_k(a_1)$ *and* ϕ_2 *denotes the probability distribution of* $C_k(a_2)$ *where* $a_1 \neq a_2$. $\forall a_1, a_2 \in \{0,1\}^*$*, the commitment scheme* Com(Sender, Receiver) *satisfies statistically hiding property if the following equation satisfies*

$$d(\phi_1, \phi_2) < \varepsilon(k)$$

where $\varepsilon(k)$ *is a negligible function in k.*

Definition 7 (Shortest Vector Problem(SVP) [22]): Given an input basis $B = (b_1, \ldots, b_n)$ *of a lattice L, the shortest vector problem (SVP) aims to identify a non-zero shortest vector in L.*

Definition 8($M-SIS_{q,m,m+k,\gamma}$*(Module Short Integer Solution Problem) [23]:) Let* R_q *denote as* $R_q = \mathbb{Z}_q[X]/\langle X^N + 1\rangle$*, and given* $A' \in R_q^{m\times(m+k)}$ *sampled uniformly at random. The* $M-SIS_{q,m,m+k,\gamma}$ *problem is to find* $z \in R^{m+k}$ *such that* $A'z = 0$ *and* $0 < ||z||_2 \leq \gamma$.

The following definition 9 pertains to the SKS.

Definition 9 $SKS^2_{n,k,\beta}$*(Search Knapsack) Problem) [14]:) Let Adv be a PPT adversary, and let* $A' \in R_q^{n\times(k-n)}$ *be a random matrix. The* $SKS^2_{n,k,\beta}$ *problem involves identifying a short vector* $y \in S^k_\beta$ *satisfying* $[I_n\ A'] \cdot y = 0^n$*, when given* $A' \in R_q^{n\times(k-n)}$.

$$\Pr[\mathrm{Adv}(A') \rightarrow y = \begin{bmatrix} y_1 \\ \vdots \\ y_k \end{bmatrix} \neq 0|$$
$$||y_i||_2 \leq \beta \wedge [I_n\ A'] \cdot y = 0^n \wedge A' \leftarrow R_q^{n\times(k-n)}] \leq \varepsilon(k).$$

Next, We introduce an extension of Definition 9, henceforth referred to as the Extended-$SKS^2_{n,k,\beta}$(extended-search knapsack) problem.

Definition 10 (Extended-$SKS^2_{n,k,\beta}$*(Search Knapsack) Problem: Let Adv be a PPT adversary, and let* $A' \in R_q^{n\times(k-n)}$ *be*

a random matrix. The Extended-SKS$^2_{n,k,\beta}$ problem involves identifying either a short vector $y \in S^{n+k}_\beta$ satisfying $[I_n\ A'\ I_n]\cdot y = 0^n$ or a short vector $y \in S^k_\beta$ satisfying $[I_n\ A'] \cdot y = 0^n$, when given $A' \in R_q^{n\times(k-n)}$.

$$\Pr[\mathrm{Adv}(A') \to y = \begin{bmatrix} y_1 \\ \vdots \\ y_{n+k} \end{bmatrix} \neq 0 |$$
$$||y_i||_2 \le \beta \wedge [I_n\ A'\ I_n]\cdot y = 0^n \wedge A' \leftarrow R_q^{n\times(k-n)}]$$
$$\le \varepsilon(k)$$

or either

$$\Pr[\mathrm{Adv}(A') \to y = \begin{bmatrix} y_1 \\ \vdots \\ y_k \end{bmatrix} \neq 0 |$$
$$||y_i||_2 \le \beta \wedge [I_n\ A'] \cdot y = 0^n \wedge A' \leftarrow R_q^{n\times(k-n)}] \le \varepsilon(k).$$

The following Definition 11 pertains to the DKS.

Definition 11 (DKS$^\infty_{m,k,\beta}$ (Decisional Knapsack Problem) [14]:) Let Adv be a PPT adversary, let $A' \in R_q^{m\times(k-m)}$ be a random matrix, and let I_m be an identity matrix. The DKS$^\infty_{m,k,\beta}$ problem involves determining whether the distribution arises from a uniform distribution u, or arises from a short $y = (y_1, \ldots, y_k) \in S^k_\beta$, $A' \in R_q^{m\times(k-m)}$, and I_m.

$$|\ \Pr[b = 1 | b \leftarrow \mathrm{Adv}\left(A', [I_m\ A'] \cdot y\right) \wedge$$
$$A' \leftarrow R_q^{m\times(k-m)} \wedge y \leftarrow S^k_\beta]$$
$$-\ \Pr[b = 1 | b \leftarrow \mathrm{Adv}\left(A', u\right)$$
$$\wedge A' \leftarrow R_q^{m\times(k-m)}]\ | < \varepsilon(k).$$

III. PREVIOUS RESEARCH

We describe the previous research in this section. We describe the commitment scheme $\mathsf{Com}_{\mathsf{BDLOP}}$ [14].

The commitment scheme $\mathsf{Com}_{\mathsf{BDLOP}}$ was constructed by *Keygen*, Commitment Phase by Sender, and Decommitment Phase in Receiver in Algorithm 1, Algorithm 2, and Algorithm 3, respectively.

$\mathsf{Com}_{\mathsf{BDLOP}}$(S, R):

Algorithm 1 *Keygen*

Input: security parameter 1^k

Output: $A = \begin{bmatrix} A_1 \\ A_2 \end{bmatrix} \in R_q^{m\times k}$.

1: Select matrix $I_n, 0^{(m-n)\times n}, A'_1 \in R_q^{n\times(k-n)}$ and define as $A_1 = [I_n\ A'_1]$
2: Select matrix $I_n, 0^{(m-n)\times n}, I_{m-n}, A'_2 \in R_q^{(m-n)\times(k-m)}$ and define as $A_2 = [0^{(m-n)\times n}\ I_{m-n}\ A'_2]$.
3: **return** $\begin{bmatrix} A_1 \\ A_2 \end{bmatrix}$

After the Algorithm 2, Sender sends decommitment string $(x', r') \in R_q^{m-n} \times S^k_\beta$ as dec to Receiver. Then, Receiver executes the following as Algorithm 3.

Algorithm 2 Commitment Phase by Sender

Input: $\begin{bmatrix} A_1 \\ A_2 \end{bmatrix} \in R_q^{m\times k}$

Output: $c^{\mathsf{BDLOP}}_{m-n,m}(x, r) \in R_q^m$

1: Select a message string $x \in R_q^{m-n}$ and $r \in S^k_\beta$ (random string), with $||r_i||_2 \le 4\cdot\sigma\cdot\sqrt{N}$
2: A commitment string is constructed from (x, r) as

$$c^{\mathsf{BDLOP}}_{m-n,m}(x, r) = \begin{bmatrix} A_1 \\ A_2 \end{bmatrix} \cdot r + \begin{bmatrix} 0^n \\ x \end{bmatrix}.$$

3: **return** $c^{\mathsf{BDLOP}}_{m-n,m}(x, r)$

Algorithm 3 Decommitment Phase in Receiver

Input: $\begin{bmatrix} A_1 \\ A_2 \end{bmatrix} \in R_q^{m\times k}$, $c^{\mathsf{BDLOP}}_{m-n,m}(x, r) \in R_q^m$, and dec $= (x', r') \in R_q^{m-n} \times S^k_\beta$

Output: $x' \in R_q^{m-n}$ or $\perp$

1: Receiver computes $c^{\mathsf{BDLOP}}_{m-n,m}(x', r') = \begin{bmatrix} A_1 \\ A_2 \end{bmatrix} \cdot r' + \begin{bmatrix} 0^n \\ x' \end{bmatrix}$ from dec $= (x', r')$ and verifies $c^{\mathsf{BDLOP}}_{m-n,m}(x, r) = c^{\mathsf{BDLOP}}_{m-n,m}(x', r')$.
2: Receiver outputs x if it satisfies $c^{\mathsf{BDLOP}}_{m-n,m}(x, r) = c^{\mathsf{BDLOP}}_{m-n,m}(x', r')$ and that for all i, $||r_i||_2 \le 4\cdot\sigma\cdot\sqrt{N}$. Otherwise, Receiver outputs $\perp$.
3: **return** $x' \in S^m_\beta$ or $\perp$

Figure 1 shows each relation between input and output in $\mathsf{Com}_{\mathsf{BDLOP}}$ and $\mathsf{Com}_{\mathsf{MWM}}$, where $\mathsf{Com}_{\mathsf{MWM}}$ will be presented in Section IV.

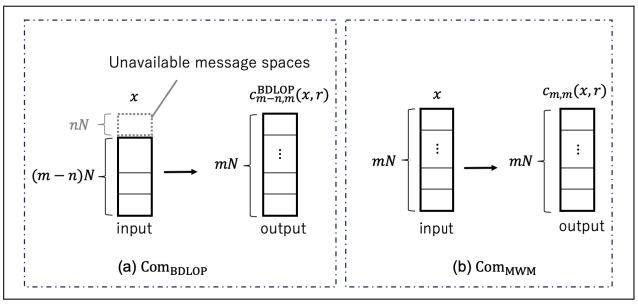


FIGURE 1. Relation between input and output ($\mathsf{Com}_{\mathsf{BDLOP}}$ vs $\mathsf{Com}_{\mathsf{MWM}}$).

IV. OUR PROPOSAL

The following section proposes the length-extension-free commitment scheme referred to as $\mathsf{Com}_{\mathsf{MWM}}$. We provide proof of the computational hiding and binding properties of $\mathsf{Com}_{\mathsf{MWM}}$ that ensure the scheme's efficiency. We also provide proof of the scheme's statistical hiding and binding properties, which ensure security.

A. (OPTIMAL) EXTENSION RATIO

We rigorously defined the *length-extension-free* commitment scheme and examined how $\mathsf{Com}_{\mathsf{BDLOP}}$ does not satisfy the *length-extension-free* commitment scheme.

Definition 12 (Length-Extension-Free Commitment Scheme): For a commitment scheme Com(Sender, Receiver)*, the extension ratio* ER *between the commitment and message string lengths is defined as*

$$\mathrm{ER} = \frac{|\text{length of commitment string}|}{|\text{length of message string}|}.$$

If the commitment scheme satisfies $\mathrm{ER} = 1$*, we call the commitment scheme a* length-extension-free *commitment scheme.*

B. PROPOSED COMMITMENT SCHEME

Our *length-extension-free* commitment scheme, called $\mathsf{Com}_{\mathsf{MWM}}$ throughout this paper, comprises three algorithms: *Keygen*, Commitment Phase by Sender, and Decommitment Phase in Receiver. We describe each algorithm in Algorithm 4, Algorithm 5, and Algorithm 6 respectively.

$\mathsf{Com}_{\mathsf{MWM}}$(Sender, Receiver):

Algorithm 4 *Keygen*

Input: security parameter 1^k

Output: $A = \begin{bmatrix} A_1 \\ A_2 \end{bmatrix} \in R_q^{m\times k}$.

1: Select matrix $I_n, 0^{(m-n)\times n}, A_1' \in R_q^{n\times(k-n)}$ and define as $A_1 = [I_n\ A_1']$

2: Select matrix $I_n, 0^{(m-n)\times n}, I_{m-n}, A_2' \in R_q^{(m-n)\times(k-m)}$ and define as $A_2 = [0^{(m-n)\times n}\ I_{m-n}\ A_2']$.

3: **return** $\begin{bmatrix} A_1 \\ A_2 \end{bmatrix}$

Algorithm 5 Commitment Phase by Sender

Input: $\begin{bmatrix} A_1 \\ A_2 \end{bmatrix} \in R_q^{m\times k}$

Output: $c_{m,m}(x, r) \in R_q^m$

1: Select a message string $x \in S_\beta^m$ and random string $r \in S_\beta^k$, with $||r_i||_2 \le 4\cdot\sigma\cdot\sqrt{N}$

2: Construct a commitment string as

$$c_{m,m}(x, r) = \begin{bmatrix} A_1 \\ A_2 \end{bmatrix} \cdot r + x.$$

3: **return** $c_{m,m}(x, r)$

After the Algorithm 5, Sender sends decommitment string $(x', r') \in S_\beta^m \times S_\beta^k$ as dec to Receiver. Then, Receiver executes the following as Algorithm 6. From Algorithm 5, the input length of x of $\mathsf{Com}_{\mathsf{MWM}}$ is mN, and the output length of $c_{m,m}(x, r)$ is mN. Thus, the ratio of the output length to the input length of $\mathsf{Com}_{\mathsf{MWM}}$ is

$$\mathrm{ER} = \frac{|\text{length of commitment string}|}{|\text{length of message string}|}$$

Algorithm 6 Decommitment Phase in Receiver

Input: $\begin{bmatrix} A_1 \\ A_2 \end{bmatrix} \in R_q^{m\times k}$, $c_{m,m}(x, r) \in R_q^m$, and $\mathsf{dec} = (x', r')$

Output: $x' \in S_\beta^m$ or $\perp$

1: Receiver Computes $c_{m,m}(x', r')$ by using $\mathsf{dec} = (x', r')$. Receiver verifies whether $c_{m,m}(x', r')$ satisfies $c_{m,m}(x', r') = A\cdot r' + x'$.

2: If it satisfies $c_{m,m}(x, r) = c_{m,m}(x', r')$ and $||r_i||_2 \le 4\cdot\sigma\cdot\sqrt{N}$, Receiver outputs the message string x'. Otherwise, Receiver outputs $\perp$.

3: **return** $x' \in S_\beta^m$ or $\perp$

$$= \frac{mN}{mN} = 1.$$

$\mathsf{Com}_{\mathsf{MWM}}$ satisfies ER=1 and $\mathsf{Com}_{\mathsf{MWM}}$ is length-extension-free commitment scheme. The following subsection provides proof of the computational binding and hiding properties in the proposed commitment scheme.

C. BINDING PROPERTY AND HIDING PROPERTY

In this subsection, we show the computational hiding and binding properties of $\mathsf{Com}_{\mathsf{MWM}}$. The computational hiding property of $\mathsf{Com}_{\mathsf{MWM}}$ is proved by using the technique of computational hiding property of Baum et al. [14]. The computational binding property of $\mathsf{Com}_{\mathsf{MWM}}$ is proved by Extended-$SKS^2_{n,k,\beta}$ problem which is a similar technique of the computational binding property of Baum et al. [14].

We have proven our scheme's computational hiding property based on the $DKS^\infty_{m,k,\beta}$ problem in Theorem 1 and its computational binding property based on Extended-$SKS^2_{n,k,\beta}$ problem in Theorem 2.

Theorem 1: For any $x \in S_\beta^m$, let k be the length of a random number $r \in S_\beta^k$ and $A\cdot r + x$ be a commitment string. If there exists a PPT algorithm $\mathcal{A}$ that has an advantage ε in breaking the hiding property of $\mathsf{Com}_{\mathsf{MWM}}$*, then there exists another algorithm $\mathcal{A}'$ that can solve the $DKS^\infty_{m,k,\beta}$ problem with ε.*

Proof: We first assume that $\mathcal{A}$ can break computational hiding property. Then, we subsequently demonstrate how another $\mathcal{A}'$ tries to solve the $DKS^\infty_{m,k,\beta}$ problem.

$\mathcal{A}'$ obtains the value $(B, t) = R_q^{m\times k} \times S_\beta^k$ from the $DKS^\infty_{m,k,\beta}$ problem. Here, B can be expressed as

$$B = [I_m\ B']$$

where B is constructed from $B' \in R_q^{m\times(k-m)}$. Next, $\mathcal{A}'$ computes $A \in R_q^{m\times k}$ (public parameter). By using $R \in R_q^{n\times(m-n)}$, I_n (identity matrices), I_{m-n} (identity matrices), and $B \in R_q^{m\times k}$, $A \in R_q^{m\times k}$ can be calculated as

$$A = \begin{bmatrix} I_n & R^{n\times(m-n)} \\ 0^{(m-n)\times n} & I_{m-n} \end{bmatrix} \cdot B.$$

Next, we illustrate how $\mathcal{A}'$ computes the commitment string $c_{m,m}$.

If we select x_b, $\mathcal{A}'$ selects $x \in S_\beta^m$ and computes $c_{m,m}$ as

$$c_{m,m} = \begin{bmatrix} I_n & R \\ 0^{(m-n)\times n} & I_{m-n} \end{bmatrix} \cdot t + x_b^m.$$

Then, $\mathcal{A}'$ sends $c_{m,m}$ to $\mathcal{A}$. After $\mathcal{A}$ obtains the value $c_{m,m}$, it guesses whether $c_{m,m}$ is constructed by $\mathsf{Com}_{\mathsf{MWM}}$ or a uniform distribution.

If t is constructed by $t = B \cdot r$, then $c_{m,m}$ can be expressed as follows.

$$\begin{aligned} c_{m,m} &= \begin{bmatrix} I_n & R \\ 0^{(m-n)\times n} & I_{m-n} \end{bmatrix} \cdot \begin{bmatrix} I_m & B' \end{bmatrix} \cdot r + x_b^m \\ &= A \cdot r + x_b^m \end{aligned}$$

In other words, if $t = B \cdot r$, $c_{m,m}$ is expressed using the same equation as that of the commitment scheme $\mathsf{Com}_{\mathsf{MWM}}$. Consequently, $\mathcal{A}$ can identify $c_{m,m}$ as $\mathsf{Com}_{\mathsf{MWM}}$ with a probability higher than ε.

If $t \neq B \cdot r$, however, $c_{m,m}$ cannot be expressed with the commitment scheme $\mathsf{Com}_{\mathsf{MWM}}$. Consequently, $\mathcal{A}$ can determine that $c_{m,m}$ is obtained from a uniform distribution when $t \neq B \cdot r$. Thus, $\mathcal{A}'$ can identify how t was constructed by observing the answer from $\mathcal{A}$. Therefore, $\mathcal{A}'$ can solve the $DKS^{\infty}_{m,k,\beta}$ problem.

From Theorem 1, our $\mathsf{Com}_{\mathsf{MWM}}$ satisfies the computational hiding property under the $DKS^{\infty}_{m,k,\beta}$ problem with an advantage of ε.

We now present a proof of the computational binding property of $\mathsf{Com}_{\mathsf{MWM}}$.

Theorem 2: For any $x \in S_\beta^m$, let k be the length of a random number $r \in S_\beta^k$, $A \in R_q^{m\times k}$ be a public parameter, and m be the output length of $A \cdot r + x$. Assume that there exists a PPT algorithm $\mathcal{A}$ that has an advantage ε in breaking the binding property of the commitment scheme $\mathsf{Com}_{\mathsf{MWM}}$, $\mathcal{A}$ can find $\left(\begin{bmatrix} r_1 \\ x_1 \end{bmatrix}, \begin{bmatrix} r_2 \\ x_2 \end{bmatrix}\right)$ which satisfies $A \cdot r_1 + x_1 = A \cdot r_2 + x_2 \wedge ||\begin{bmatrix} r_1 - r_2 \\ x_1 - x_2 \end{bmatrix}||_2 \leq \sqrt{(m+k)} \cdot \beta \wedge x_1 \neq x_2$. Then, there exists another algorithm $\mathcal{A}'$ that incurs an equivalent time complexity and has an advantage ε in solving the Extended-$SKS^2_{n,k,\beta}$ problem.

Proof: We first assume that $\mathcal{A}$ can break the computational binding property of $\mathsf{Com}_{\mathsf{MWM}}$. We try to determine whether another adversary $\mathcal{A}'$ is able to solve the Extended-$SKS^2_{n,k,\beta}$ problem. $\mathcal{A}'$ obtains the value $A'_1 \in R_q^{n\times(k-n)}$ from the oracle of the Extended-$SKS^2_{n,k,\beta}$ problem and attempts to obtain y, which satisfies

$$[I_n\, A'] \cdot y^k = 0^n$$

or

$$[I_n\, A'\, I_n] \cdot y^{n+k} = 0^n.$$

To gain y, adversary $\mathcal{A}'$ computes $A'_1 \in R_q^{n\times(k-n)}$ in Algorithm 7, and then sends $A \in R_q^{m\times k}$ to adversary $\mathcal{A}$. Then, $\mathcal{A}$ breaks the binding property of $\mathsf{Com}_{\mathsf{MWM}}$ and outputs

$$\left(\begin{bmatrix} r_1 \\ x_1 \end{bmatrix}, \begin{bmatrix} r_2 \\ x_2 \end{bmatrix}\right) \tag{1}$$

Algorithm 7 Step of Adversary $\mathcal{A}$

Input: $A'_1 \in R_q^{n\times(k-n)}$
Output: $A \in R_q^{m\times k}$

1: Select matrix $I_n, 0^{(m-n)\times n}, I_{m-n}, A'_2 \in R_q^{(m-n)\times(k-m)}$
2: Construct the matrix as

$$A = \begin{bmatrix} I_n & A'_1 \\ 0^{(m-n)\times n} & I_{m-n}\, A'_2 \end{bmatrix}$$

3: **return** A

to $\mathcal{A}'$, which satisfies $A \cdot r_1 + x_1 = A \cdot r_2 + x_2 \wedge ||\begin{bmatrix} r_1 - r_2 \\ x_1 - x_2 \end{bmatrix}||_2 \leq \sqrt{(m+k)} \cdot \beta \wedge x_1 \neq x_2$. Here,

$$A \cdot r_1 + x_1 = A \cdot r_2 + x_2.$$

Then sends the input values of Equation (1) to $\mathcal{A}'$. $\mathcal{A}'$ computes

$$\left[I_n\, A'_1\right] \cdot (r_1 - r_2) + (x_1^i - x_2^i)^{1\leq i\leq n} = 0^n \tag{2}$$

and

$$\begin{aligned} &\left[0^{(m-n)\times n}\, I_{m-n}\, A'_2\right] \cdot (r_1 - r_2) + (x_1^i - x_2^i)^{n+1\leq i\leq m} \\ &= 0^{m-n}. \end{aligned} \tag{3}$$

$\mathcal{A}'$ finds the solution of the Extended-$SKS^2_{n,k,\beta}$ problem by splitting it into the following cases: $(x_1^i - x_2^i)^{1\leq i\leq n} = 0$ and $(x_1^i - x_2^i)^{1\leq i\leq n} \neq 0$.

- Case 1: $(x_1^i - x_2^i)^{1\leq i\leq n} = 0$

Equation (3) can be expressed as Equation (4)

$$\left[0^{(m-n)\times n}\, I_{m-n}\, A'_2\right] \cdot (r_1 - r_2) = -(x_1^i - x_2^i)^{n+1\leq i\leq m}. \tag{4}$$

If $r_1 - r_2 = 0$, then, the LHS of Equation (4) is

$$\left[0^{(m-n)\times n}\, I_{m-n}\, A'_2\right] \cdot 0 = 0,$$

and the RHS of Equation (4) is

$$-(x_1^i - x_2^i)^{n+1\leq i\leq m} \neq 0.$$

The LHS and RHS are mutually contradictory. Consequently, if $(x_1^i - x_2^i)^{1\leq i\leq n} = 0$, then it always satisfies $r_1 - r_2 = 0$. Because the length $||r_1 - r_2||$ is $||r_1 - r_2|| \leq \sqrt{k} \cdot \beta \leq \sqrt{m+k} \cdot \beta$, $(r_1 - r_2)$ is the solution of the Extended-$SKS^2_{n,k,\beta}$ problem.

- Case 2: $(x_1^i - x_2^i)^{n+1\leq i\leq m} \neq 0$:

We set $r' = r_1 - r_2$ and $x' = (x_1^i - x_2^i)^{1\leq i\leq n}$. Then, Equation (2) can be expressed as Equation (5)

$$\left[I_n\, A'_1\right] \cdot r' + x' = 0. \tag{5}$$

Equation (5) can then be transformed into the following equation.

$$[I_n\, A'\, I_n] \cdot \begin{bmatrix} r_1 \\ x_1 \end{bmatrix} = 0.$$

Here, we can easily verify that $||\begin{bmatrix} r_1 \\ x_1 \end{bmatrix}||_2 = \sqrt{n+k} \cdot \beta < \sqrt{m+k} \cdot \beta$ from the condition $n < m$. Consequently, from the above equation and the condition that $||\begin{bmatrix} r_1 \\ x_1 \end{bmatrix}||_2 < \sqrt{m+k} \cdot \beta$, $\begin{bmatrix} r_1 \\ x_1 \end{bmatrix}$ is the solution of Extended-$SKS^2_{n,k,\beta}$ problem if $(x^i_1 - x^i_2)^{n+1 \le i \le m} \neq 0$.

Thus if an adversary $\mathcal{A}$ can break the computational binding property, then there exists an adversary $\mathcal{A}'$ that can solve the Extended-$SKS^2_{n,k,\beta}$ problem.

From Theorem 2, $\mathsf{Com}_{\mathsf{MWM}}$ satisfies the computationally binding property under the Extended-$SKS^2_{n,k,\beta}$ problem.

D. UNCONDITIONAL HARDNESS OF THE $DKS^{\infty}_{M,K,\beta}$ PROBLEM

This subsection demonstrates that $\mathsf{Com}_{\mathsf{MWM}}$ satisfies the statistical hiding property when certain parameter ranges in the $DKS^{\infty}_{m,k,\beta}$ problem become unconditionally hard. We prove the computational hiding property of $\mathsf{Com}_{\mathsf{MWM}}$ in Theorem 1 and the computational binding property of $\mathsf{Com}_{\mathsf{MWM}}$ in Theorem 2. In general, information-theoretic security can guarantee higher security than computational security because there is no need to make assumptions about the adversary's computational capabilities. In this paper, we apply information-theoretic security to the hiding property of commitment schemes, which we refer to as statistical hiding property. To prove the statistical hiding property of $\mathsf{Com}_{\mathsf{MWM}}$, we present a lemma on how to compute the statistical distance in Lemma 1, and then we prove in Theorem 3 that $\mathsf{Com}_{\mathsf{MWM}}$ satisfies the statistically hiding property by using Lemma 1.

To show the parameter conditions of the $DKS^{\infty}_{m,k,\beta}$ problem for which $\mathsf{Com}_{\mathsf{MWM}}$ satisfies statistical hiding, we first explain how to compute the statistical distance. In 2009, Regev proved the modified version of the leftover hash lemma [24]. This modification is specified in Lemma 1.

Lemma 1: Compute the Statistical Distance Between Two Different Distributions [24]: Let G and ℓ be a finite Abelian group and a positive integer. We select any ℓ elements $g_1, \ldots, g_\ell \in G$, and consider the statistical distance between the distribution given by the sum of a random subset of $g_1, \ldots, g_\ell$ and the uniform distribution on G. This statistical distance cannot exceed $\sqrt{|G|/2^\ell}$. In particular, the probability that it exceeds $\sqrt[4]{|G|/2^\ell}$ is at most $\sqrt[4]{|G|/2^\ell}$.

Lemma 1 analyzes the sum of a given set's random subset. The following Theorem 3 analyzes the set $c_{m,m} = A \cdot r + x$. From the method designed by Kawachi et al. [15], we can determine the weights of $c_{m,m}$ to be uniformly distributed by including a random number r. Therefore, it is possible to employ Lemma 1 in this Theorem 3.

Theorem 3: Let $x, x' \in S^m_\beta$, let k be the length of $r \in S^k_\beta$ (random number). The commitment string $c_{m,m} = A \cdot r + x$ is constructed from $A \in R^{m \times k}_q$, $1 < d < N$ be a power of 2, and $A = \begin{bmatrix} I_n & A'_1 \\ 0^{(m-n)\times n} & I_{m-n}\ A'_2 \end{bmatrix}$. It satisfies $A'_1 \in R^{n \times (k-n)}_q$, $A'_2 \in R^{(m-n)\times(k-m)}_q$, and $G = R^m_q$. Here, m is the output string of $\mathsf{Com}_{\mathsf{MWM}}$. We assume that q satisfies the condition of a prime congruent to $2d + 1 \pmod{4d}$, and also satisfies the following

$$q^{m/k} \cdot 2^{2m/(k \cdot N)} \le \beta < \frac{1}{\sqrt{d}} \cdot q^{1/d}.$$

The computationally unbounded algorithm computes the statistical distance over $\mathsf{Com}_{\mathsf{MWM}}$, and the uniform distribution is at most 2^{-m}.

Proof:

$$c_{m,m} = \{h_A : S^{m+k}_\beta \to R^m_q\} \text{ where}$$
$$h_A(y) = [A\ I_m] \cdot y.$$

Let $g = (g_1, \ldots, g_{m+k})$ and g be any element that belongs to the finite Abelian group. For $h \in G$, we define

$$P_g(h) = \frac{1}{\beta^{(m+k)N}} \left| \left\{ y \in S^{m+k}_\beta | \sum_{i=1}^{k} y_i g_i = h \right\} \right|.$$

The expectation of the statistical distance between the uniform distribution and the distribution $(A, h_A(y))$ over g is computed as

$$\mathop{\mathrm{Ex}}_{g} \left[\sum_{h \in R^m_q} |P_g(h) - |1/G|| \right].$$

The above equation can then be parsed as

$$\mathop{\mathrm{Ex}}_{g} \left[\sum_{h \in R^m_q} |P_g(h) - 1/q^{mN}| \right] \le \sqrt{\frac{q^{mN}}{\beta^{(m+k)N}}}$$

from Lemma 1 and $|G| = q^{mN}$. Likewise, $\sqrt{\frac{q^{mN}}{\beta^{(m+k)N}}}$ can be parsed as

$$\begin{aligned} \log \sqrt{\frac{q^{mN}}{\beta^{(m+k)N}}} &= \frac{1}{2} \log \left(\frac{q^{mN}}{\beta^{(m+k)N}} \right) \\ &= \frac{1}{2} \left\{ \log q^{mN} - \log \beta^{kN} \right\} \\ &= \frac{1}{2} \{ m \cdot N \cdot \log q - (m+k) \cdot N \cdot \log \beta \} \end{aligned}$$

In contrast, the condition $q^{m/k} \cdot 2^{2m/(k \cdot N)} \le \beta$ can be parsed as follows

$$m \cdot N \cdot \log q + 2m < k \cdot N \cdot \log \beta$$
$$k \cdot N \cdot \log \beta < -m \cdot N \cdot \log q - 2m.$$

From the conditions $m > 0, k > 0, N > 0$, and above equations, $\frac{1}{2}\{m \cdot N \cdot \log q - (m+k) \cdot N \cdot \log \beta\}$ can be parsed as follows.

$$\begin{aligned} &\frac{1}{2} \{ m \cdot N \cdot \log q - (m+k) \cdot N \cdot \log \beta \} \\ &< \frac{1}{2} \{ (m \cdot N \cdot \log q) - (k \cdot N \cdot \log \beta) \} \\ &< \frac{1}{2} \{ (m \cdot N \cdot \log q) - (m \cdot N \cdot \log q - 2m) \} \\ &= -m. \end{aligned}$$

Consequently, the expectation of the statistical distance between the uniform distribution and $(A, h_A(y))$ over g is computed as

$$\mathop{\mathrm{Ex}}_{g}\left[\sum_{h\in R_q^m}|P_g(h)-1/q^{mN}|\right]\leq\sqrt{\frac{q^{mN}}{\beta^{(m+k)N}}}<2^{-m}.$$

Our proposed $\mathsf{Com}_{\mathsf{MWM}}$ satisfies the statistical hiding property based on the $DKS^{\infty}_{m,k,\beta}$ problem by using Theorem 3. Consequently, we can state Theorem 4.

Theorem 4: Our $\mathsf{Com}_{\mathsf{MWM}}$ *satisfies the statistical hiding property based on the* $DKS^{\infty}_{m,k,\beta}$ *problem with the condition of* $q^{m/k}\cdot 2^{2m/(k\cdot N)}\leq\beta<\frac{1}{\sqrt{d}}\cdot q^{1/d}$. *At the same time,* $\mathsf{Com}_{\mathsf{MWM}}$ *satisfies the computational binding property based on the Extended-*$SKS^{2}_{n,k,\beta}$ *problem.*

V. COMPARISON OF COMMITMENT SCHEMES

In this section, we calculate *ER* for each commitment scheme and compare our commitment schemes.

In BKLP15, the input length is N and the output length is mN. The parameter ER becomes

$$\mathrm{ER}=\frac{|\text{length of commitment string}|}{|\text{length of message string}|}=\frac{mN}{N}=m>1.$$

The computationally hiding and statistical binding property of BKLP15 can be proven using D-R-LWE.

In BDLOP18, the input length is $(m-n)N$ and the output length is mN. The parameter ER becomes

$$\mathrm{ER}=\frac{mN}{(m-n)N}=\frac{m}{m-n}>1.$$

The hiding property and the binding property of BDLOP18 can be proven by the $DKS^{\infty}_{m,k,\beta}$ and $SKS^{2}_{n,k,\beta}$ problems, respectively. They also show how to develop a statistically binding scheme and a statistically hiding scheme. Furthermore, they develop only computationally hiding and binding properties.

In $\mathsf{Com}_{\mathsf{MWM}}$, the input/output length is mN. The parameter ER becomes

$$\mathrm{ER}=\frac{mN}{mN}=1.$$

The hiding property and the binding property of our proposed scheme $\mathsf{Com}_{\mathsf{MWM}}$ can be proven by the $DKS^{\infty}_{m,k,\beta}$ and Extended-$SKS^{2}_{n,k,\beta}$ problems, respectively. We also proved that the commitment scheme $\mathsf{Com}_{\mathsf{MWM}}$ satisfies the statistical hiding property and the computationally binding property in Theorem 4.

Comparison among existing commitment schemes and $\mathsf{Com}_{\mathsf{MWM}}$**:** In both BKLP15 and BDLOP18 satisfies $\mathrm{ER}>1$, and our proposed $\mathsf{Com}_{\mathsf{MWM}}$ satisfies $\mathrm{ER}=1$. Consequently, when sending the same message length, BKLP15 and BDLOP18 require a larger output length (commitment length) than $\mathsf{Com}_{\mathsf{MWM}}$. Thus, our $\mathsf{Com}_{\mathsf{MWM}}$ can achieve a smaller output length commitment scheme compared to BKLP15 and BDLOP18. Table 2 compares $\mathsf{Com}_{\mathsf{MWM}}$, BKLP15, and BDLOP18 from the perspectives of security and *ER*.

A. EVALUATION

This subsection evaluates the proposed $\mathsf{Com}_{\mathsf{MWM}}$ from the point of view of the length of commitment. Using the secure parameter evaluation in [25], $\mathsf{Com}_{\mathsf{MWM}}$, BDLOP18, and BKLP15 satisfy AES-128 security when $(q, N) = (2^{32}, 1024)$. $\mathsf{Com}_{\mathsf{MWM}}$, BDLOP18, and BKLP15 are implemented with $(q, N) = (2^{32}, 1024)$, and the length of the commitment value for a 2048-bit message is then evaluated in Table 3.

When $N = 1024$, each scheme's commitment length can be computed as

$$m*N=2*1024=2048\ (\text{bit})\ .$$

In BKLP15, the message length can be computed by $1*N=1024$(bit). In BDLOP18, the message length can be computed by $(m-n)*N=1024$(bit). In $\mathsf{Com}_{\mathsf{MWM}}$, the message length can be computed by $m*N=2048$(bit). From these analyses, $\mathsf{Com}_{\mathsf{MWM}}$ allows a message length twice as long as the other two schemes.

For example, if we want to send a 2048-bit message length, $\mathsf{Com}_{\mathsf{MWM}}$ requires an input length of 2048 bits and an output length (commitment length) of 2048 bits. On the other hand, BKLP15 and BDLOP18 require an output length of 4096 bits to send a 2048-bit message length. If a commitment scheme or application has a limitation on output length, BKLP15 or BDLOP18 may be unable to send the desired message length. Therefore, it is more feasible to use $\mathsf{Com}_{\mathsf{MWM}}$ than BKLP15 or BDLOP18 to realize a commitment scheme that can send more input lengths. Our scheme $\mathsf{Com}_{\mathsf{MWM}}$ is therefore the only commitment scheme that satisfies the condition $\mathrm{ER}=1$.

B. IMPLEMENTATION

This subsection evaluates the proposed $\mathsf{Com}_{\mathsf{MWM}}$ from the point of view of the computational cost of commitment. Note that the hiding property of $\mathsf{Com}_{\mathsf{MWM}}$ and BDLOP18 is based on the DKS problem, and the binding property is based on a similar security problem. Thus, we implement $\mathsf{Com}_{\mathsf{MWM}}$ and BDLOP18 in terms of computational complexity. We implement $\mathsf{Com}_{\mathsf{MWM}}$ and BDLOP18 with $(q, m, n) = (2^{32}, 2048, 1024)$, respectively, and show the computational complexity of generating a 2048-bit message length in Table 4.

We implement $\mathsf{Com}_{\mathsf{MWM}}$ using Python 3.10.6.[1] Matrix generation is done using the NumPy package. The experiment involves generating commitment values 10000 times and calculating the average time required to generate each commitment value. We calculate the generation time of the commitment values of the proposed $\mathsf{Com}_{\mathsf{MWM}}$ and BDLOP18. The experiment is executed by reducing polynomial rings to integers.

In Table 4, we calculate the time required to generate the commitment values for $\mathsf{Com}_{\mathsf{MWM}}$ and BDLOP18. Table 3 shows that $\mathsf{Com}_{\mathsf{MWM}}$ can generate a 2048-bit message in the same message space, while BDLOP18 can only generate

[1]The implementation is available at https://github.com/ENLINKER/commitment_experiment

TABLE 2. Comparison between commitment schemes.

Commitment Scheme	Binding Property	Hiding Property	**ER (Extension Ratio)**
BKLP15 [16]	statistical/computational	computational	2
BDLOP18 [14]	statistical/computational	computational/statistical	2
Our Propose $\mathsf{Com}_{\mathsf{MWM}}$	computational	statistical/computational	**1**

TABLE 3. Parameter settings in $\mathsf{Com}_{\mathsf{MWM}}$, BDLOP18, and BKLP15.

Parameter	$\mathsf{Com}_{\mathsf{MWM}}$	BDLOP18	BKLP15
q	2^{32}	2^{32}	2^{32}
N	1024	1024	1024
m	2	2	2
k	1	1	-
$m-n$	1	1	-
n	1	1	-
Commitment Length	**2048 bit**	2048 bit	2048 bit
Message Length (bit)	**2048 bit**	1024 bit	1024 bit

TABLE 4. Computation costs of generating commitment value between $\mathsf{Com}_{\mathsf{MWM}}$ and BDLOP18.

Parameter	$\mathsf{Com}_{\mathsf{MWM}}$	BDLOP18
q	2^{32}	2^{32}
m	2048	2048
n	1024	1024
β	5	5
Computation costs required to generate a 2048-bit message (ms)	**0.02905**	**0.05857**

a commitment for a half-length message size in the same message space at a time. Thus, two operations are required to generate a commitment value for a 2048-bit message in BDLOP18. As shown in Table 4, $\mathsf{Com}_{\mathsf{MWM}}$ costs 49.6% of the time required to generate the commitment values compared with BDLOP18. Consequently, from Tables 3 and 4, $\mathsf{Com}_{\mathsf{MWM}}$ can send more messages and spend less time generating commitment values compared to BDLOP18.

C. OUR PROPOSED SCHEME CONTRIBUTES TO EXISTING STUDIES

This subsection provides how our $\mathsf{Com}_{\mathsf{MWM}}$ contributes to the existing studies. Galal and Youssef realized a sealed-bid auction on the Ethereum Blockchain using a commitment scheme [26]. By using the commitment scheme, their system can be divided into two phases: a phase in which the bid values of each user are collected secretly, and a phase in which the winner can be determined. However, existing blockchains have limited scalability [27]. In our $\mathsf{Com}_{\mathsf{MWM}}$, the input length and output length (commitment length) are the same size, so even if the output length is limited, it is possible to send an input length that is the same size as the output length. Consequently, using $\mathsf{Com}_{\mathsf{MWM}}$ for sealed-bit auctions on blockchains is one solution to the problem of limited scalability of blockchains.

VI. CONCLUSION

This paper proposes a commitment scheme $\mathsf{Com}_{\mathsf{MWM}}$ that satisfies

$$\mathrm{ER} = \frac{|\text{length of commitment string}|}{|\text{length of message string}|} = 1.$$

To verify the practicality and efficiency of $\mathsf{Com}_{\mathsf{MWM}}$, we have proven that it satisfies the statistical hiding property based on the $DKS^{\infty}_{m,k,\beta}$ problem, as well as the computationally binding property based on the Extended-$SKS^{2}_{n,k,\beta}$ problem. We have suggested secure parameter settings between the $\mathsf{Com}_{\mathsf{MWM}}$, BDLOP18, and BKLP15 commitment schemes under AES-128. Finally, we implemented $\mathsf{Com}_{\mathsf{MWM}}$ and BDLOP18 and compared the computation cost of generating a commitment value.

The research regarding the practical application of lattice-based commitment schemes is crucial. This paper defines the novel concept of *ER*, and commitment schemes with $ER = 1$ will play an essential role in realizing applications using lattice-based commitment, as any other value of *ER* is insufficient for practical use. Furthermore, $\mathsf{Com}_{\mathsf{MWM}}$ can send twice as large a message dimension as BDLOP18 or BKLP15 which satisfies $ER > 1$. Our results are therefore expected to play a crucial role in realizing applications using lattice-based commitment schemes.

ACKNOWLEDGMENT

An earlier version of this paper was presented at ISPEC 2021 [DOI: 10.1007/978-3-030-93206-0_7].

REFERENCES

[1] H. Miyaji, Y. Wang, and A. Miyaji, "Message-restriction-free commitment scheme based on lattice assumption," in *Proc. 16th Int. Conf. Inf. Secur. Pract. Exper. (ISPEC)* (Lecture Notes in Computer Science), vol. 13107. Nanjing, China: Springer, Dec. 2021, pp. 90–105, doi: 10.1007/978-3-030-93206-0_7.

[2] A. Deshpande and M. Herlihy, "Privacy-preserving cross-chain atomic swaps," in *Proc. Int. Workshops Financial Cryptogr. Data Secur.* (Lecture Notes in Computer Science), vol. 12063. Kota Kinabalu, Malaysia: Springer, Feb. 2020, pp. 540–549, doi: 10.1007/978-3-030-54455-3_38.

[3] C. Zhang, W. Wang, W. Zhang, J. Nie, J. Liang, and L. Zhu, "Achieving distributed and privacy-preserving cross-chain transactions in account-model blockchain systems," in *Proc. IEEE Int. Conf. Metaverse Comput., Netw. Appl. (MetaCom)*, Jun. 2023, pp. 297–305.

[4] E. Fujisaki and T. Okamoto, "Statistical zero knowledge protocols to prove modular polynomial relations," in *Proc. 17th Annu. Int. Cryptol. Conf. (CRYPTO)* (Lecture Notes in Computer Science), vol. 1294. Santa Barbara, CA, USA: Springer, Aug. 1997, pp. 16–30, doi: 10.1007/BFb0052225.

[5] S. Bayer and J. S. Groth, "Zero-knowledge argument for polynomial evaluation with application to blacklists," in *Proc. 32nd Annu. Int. Conf. Theory Appl. Cryptograph. Techn. (EUROCRYPT)* (Lecture Notes in Computer Science), vol. 7881. Athens, Greece: Springer, May 2013, pp. 646–663, doi: 10.1007/978-3-642-38348-9_38.

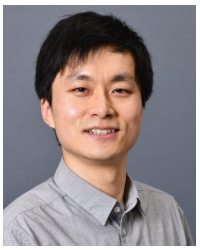
[6] I. Damgard, "Commitment schemes and zero-knowledge protocols," in *Lectures on Data Security, Modern Cryptology in Theory and Practice, Summer School*. Aarhus, Denmark: Springer, Jul. 1998, pp. 63–86.

[7] I. Haitner, M.-H. Nguyen, S. J. Ong, O. Reingold, and S. Vadhan, "Statistically hiding commitments and statistical zero-knowledge arguments from any one-way function," *SIAM J. Comput.*, vol. 39, no. 3, pp. 1153–1218, Jan. 2009.

[8] M. Blum, "Coin flipping by telephone—A protocol for solving impossible problems," in *Proc. 24th IEEE Comput. Soc. Int. Conf.*, San Francisco, CA, USA, Feb. 1982, pp. 133–137.

[9] 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, Apr. 1988.
[10] T. P. Pedersen, "Non-interactive and information-theoretic secure verifiable secret sharing," in *Proc. 11th Annu. Int. Cryptol. Conf.*, Santa Barbara, CA, USA, Aug. 1991, pp. 129–140.
[11] S. Halevi and S. Micali, "Practical and provably-secure commitment schemes from collision-free hashing," in *Proc. 16th Annu. Int. Cryptol. Conf.*, Santa Barbara, CA, USA, Aug. 1996, pp. 201–215.
[12] Y. Desmedt and Y. Frankel, "Threshold cryptosystems," in *Proc. 9th Annu. Int. Cryptol. Conf. (CRYPTO)* (Lecture Notes in Computer Science), vol. 435. Santa Barbara, CA, USA: Springer, Aug. 1989, pp. 307–315, doi: 10.1007/0-387-34805-0_28.
[13] R. Cramer, M. K. Franklin, B. Schoenmakers, and M. Yung, "Multi-autority secret-ballot elections with linear work," in *Proc. Int. Conf. Theory Appl. Cryptograph. Techn. (EUROCRYPT)* (Lecture Notes in Computer Science), vol. 1070. Saragossa, Spain: Springer, May 1996, pp. 72–83, doi: 10.1007/3-540-68339-9_7.
[14] C. Baum, I. Damgrard, V. Lyubashevsky, S. Oechsner, and C. Peikert, "More efficient commitments from structured lattice assumptions," in *Proc. 11th Int. Conf. Secur. Cryptogr. Netw. (SCN)* (Lecture Notes in Computer Science), vol. 11035. Amalfi, Italy: Springer, Sep. 2018, pp. 368–385, doi: 10.1007/978-3-319-98113-0_20.
[15] A. Kawachi, K. Tanaka, and K. Xagawa, "Concurrently secure identification schemes based on the worst-case hardness of lattice problems," in *Proc. 14th Int. Conf. Theory Appl. Cryptol. Inf. Secur.*, Melbourne, VIC, Australia, Dec. 2008, pp. 372–389.
[16] F. Benhamouda, S. Krenn, V. Lyubashevsky, and K. Pietrzak, "Efficient zero-knowledge proofs for commitments from learning with errors over rings," in *Proc. 20th Eur. Symp. Res. Comput. Secur. (ESORICS)* (Lecture Notes in Computer Science), vol. 9326. Vienna, Austria: Springer, Sep. 2015 pp. 305–325, doi: 10.1007/978-3-319-24174-6_16.
[17] E. Abraham, "Circuit friendly, post-quantum dynamic accumulators from RingSIS with logarithmic prover time," *IACR Cryptol. ePrint Arch.*, p. 1010, 2021. [Online]. Available: https://eprint.iacr.org/2021/1010
[18] Y. Peng, L. Wang, J. Cui, X. Liu, H. Li, and J. Ma, "LS-RQ: A lightweight and forward-secure range query on geographically encrypted data," *IEEE Trans. Dependable Secure Comput.*, vol. 19, no. 1, pp. 388–401, Jan. 2022.
[19] X. Meng, Y. Yang, X. Liu, and N. Jiang, "Active forgetting via influence estimation for neural networks," *Int. J. Intell. Syst.*, vol. 37, no. 11, pp. 9080–9107, Nov. 2022.
[20] M. Ajtai, "Generating hard instances of lattice problems (extended abstract)," in *Proc. 28th Annu. ACM Symp. Theory Comput.*, Philadelphia, PA, USA, G. L. Miller, Ed., May 1996, pp. 99–108.
[21] G. Di Crescenzo, J. Katz, R. Ostrovsky, and A. D. Smith, "Efficient and non-interactive non-malleable commitment," in *Proc. Int. Conf. Theory Appl. Cryptograph. Techn.*, Innsbruck, Austria, May 2001, pp. 40–59.
[22] J. Ding, X. Gao, T. Takagi, and Y. Wang, "One sample ring-lwe with rounding and its application to key exchange," in *Proc. 17th Int. Conf. Appl. Cryptogr. Netw. Secur. (ACNS)* (Lecture Notes in Computer Science), vol. 11464. Bogota, Colombia: Springer, 2019, pp. 323–343, doi: 10.1007/978-3-030-21568-2_16.
[23] R. del Pino, V. Lyubashevsky, and G. Seiler, "Lattice-based group signatures and zero-knowledge proofs of automorphism stability," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, D. Lie, M. Mannan, M. Backes, and X. Wang, Eds., Toronto, ON, Canada, Oct. 2018, pp. 574–591.
[24] O. Regev, "On lattices, learning with errors, random linear codes, and cryptography," *J. ACM*, vol. 56, no. 6, pp. 1–40, Sep. 2009.
[25] H. Miyaji, A. Miyaji, and Y. Wang, "Homomorphic commitment scheme with constant output locality," in *Proc. 8th Int. Symp. Comput. Netw. (CANDAR)*, Naha, Japan, Nov. 2020, pp. 167–173.
[26] H. S. Galal and A. M. Youssef, "Verifiable sealed-bid auction on the Ethereum blockchain," in *Proc. Int. Workshops Financial Cryptogr. Data Secur.* (Lecture Notes in Computer Science), vol. 10958. Nieuwpoort, Curavcao. Springer, Mar. 2018, pp. 265–278, doi: 10.1007/978-3-662-58820-8_18.
[27] L. Hughes, Y. K. Dwivedi, S. K. Misra, N. P. Rana, V. Raghavan, and V. Akella, "Blockchain research, practice and policy: Applications, benefits, limitations, emerging research themes and research agenda," *Int. J. Inf. Manage.*, vol. 49, pp. 114–129, Dec. 2019.

HIDEAKI MIYAJI (Member, IEEE) received the B.S. degree from Kanazawa University, in 2018, and the M.Eng. and D.Sc. degrees from Osaka University, in 2020 and 2023, respectively. He is currently an Assistant Professor with Ritsumeikan University. His current research interests include cryptography, including lattice, hash functions, commitment schemes, zero-knowledge protocol, and blockchain.



YUNTAO WANG (Member, IEEE) received the B.Sc. degree in information and computing science from Yunnan University, in 2011, and the M.Sc. degree in mathematics and the Ph.D. degree in mathematics for key technologies from Kyushu University, in 2016. From April 2020 to February 2024, he was with Japan Advanced Institute of Science and Technology (JAIST) and Osaka University as an Assistant Professor and a Lecturer, respectively. He is currently an Associate Professor with the University of Electro-Communications (UEC), Tokyo. After graduation, he worked on the CREST Project of Mathematical Modelling for Next-Generation Cryptography for one year and did JSPS PD for half a year. His research interests include information security and cryptography. He is especially interested in post-quantum cryptography. He received the Research Fellowship for Young Scientists of Japan Society for the Promotion of Science (JSPS) during the Ph.D. degree.

ATSUKO MIYAJI (Member, IEEE) received the B.Sc., M.Sc., and Dr.Sci. degrees in mathematics from Osaka University, in 1988, 1990, and 1997, respectively. She joined Panasonic Company Ltd., from 1990 to 1998, and engaged in research and development for secure communication. She was an Associate Professor with Japan Advanced Institute of Science and Technology (JAIST), in 1998. She joined the Computer Science Department, University of California at Davis, from 2002 to 2003. She has been a Professor with JAIST, since 2007. She has been a Professor with the Graduate School of Engineering, Osaka University, since 2015. Her research interests include the application of number theory to cryptography and information security. She is currently an IPSJ Fellow. She is a member of the International Association for Cryptologic Research, the Institute of Electrical and Electronics Engineers, the Institute of Electronics, Information and Communication Engineers, the Information Processing Society of Japan, and the Mathematical Society of Japan. She received the Young Paper Award of SCIS'93, in 1993; the Notable Invention Award of the Science and Technology Agency, in 1997; the IPSJ Sakai Special Researcher Award, in 2002; the Standardization Contribution Award, in 2003; the Award for the Contribution to Culture of Security, in 2007; the Director-General of Industrial Science and Technology Policy and Environment Bureau Award, in 2007; the DoCoMo Mobile Science Awards, in 2008; the Advanced Data Mining and Applications (ADMA 2010) Best Paper Award; the Prizes for Science and Technology; the Commendation for Science and Technology by the Minister of Education, Culture, Sports, Science and Technology; the International Conference on Applications and Technologies in Information Security (ATIS 2016) Best Paper Award; the 16th IEEE TrustCom 2017 Best Paper Award; the IEICE Milestone Certification, in 2017; the 14th Asia Joint Conference on Information Security (AsiaJCIS 2019) Best Paper Award; the Information Security Applications-20th International Conference (WISA 2020) Best Paper Gold Award; the IEICE Distinguished Educational Practitioners Award, in 2020; and the IEICE Achievement Award, in 2023.