Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 29 (2026), No. 7, pp. 2831–2844
DOI : 10.47974/JDMSC-2580

ALGAES : An authenticated lattice-based generic asymmetric encryption scheme

S. S. Aravind Vishnu *
M. Sethumadhavan †
K. V. Lakshmy §
TIFAC-CORE in Cyber Security
Amrita School of Engineering
Amrita Vishwa Vidyapeetham
Coimbatore Campus
Amritanagar P. O.
Ettimadai 641112
Tamil Nadu
India

Abstract

In this article, we propose a generic hybrid encryption scheme providing entity authentication. The scheme is based on lossy trapdoor functions relying on the hardness of the Learning With Errors problem. The construction can be used on a number of different security requirements with minimal reconfiguration. It ensures entity authentication and ciphertext integrity while providing security against adaptive chosen ciphertext attacks in the standard model. As a desired characteristic of schemes providing entity authentication, we prove the strong unforgeability under chosen message attack for the construction. In addition, the scheme is post-quantum secure based on the hardness of the underlying assumption.

Subject Classification: *94A60, 94A62, 68P25.*

Keywords: *Hybrid encryption, Learning with errors, IND-CCA2, Lossy trapdoor, Lattice-based, signcryption, Post-quantum.*

* *ORCID-ID:* **0000-0002-2374-5764**
† *ORCID-ID:* **0000-0001-5476-5461**
§ *ORCID-ID:* **0000-0001-5344-2855**

* *E-mail:* **ss_aravindvishnu@cb.amrita.edu (Corresponding Author)**
† *E-mail:* **m_sethu@cb.amrita.edu**
§ *E-mail:* **kv_lakshmy@cb.amrita.edu**

1. Introduction

The development of lattice-based cryptography until 2016 was studied and detailed by Chris Peikert in an article titled 'A decade of lattice cryptography' [1]. The hybrid encryption algorithm introduced by Victor Shoup [2], and the notion of key encapsulation scheme, now called key encapsulation mechanism (KEM), made a huge impact on asymmetric cryptographic constructions. The Fujisaki-Okamoto transformation [3] for securely integrating a symmetric and asymmetric cryptosystem has a seminal impact on the growth and popularity of the above mentioned hybrid KEMs. In 2008, Chris Peikert and Brent Waters introduced the lossy trapdoor functions [4]. The work aimed to construct a new primitive and construction technique for asymmetric cryptosystems. The article proposes a generic construction mechanism. It also specifies how to realise Diffie-Hellman assumption and Lattice-based problems to the proposed construction. The lossy trapdoor functions find their significance in many black box-mannered cryptographic constructions [5], and some of the best examples and optimizations can be found in [6, 7, 8].

Bertoni *et al.* introduced the sponge-based hash functions [9, 10]. The sponge-based constructions are preferred in integrating symmetric and asymmetric cryptosystems into a hybrid cryptosystem due to its properties. Zheng [11] introduced `signcryption' that combines entity authentication technique and message integrity in the same ciphertext. The sponge-based hash function named Hash-One [12] was used in one such recent construction of a certificateless hybrid signcryption scheme [13]. Also there are articles which combined mathematical objects with already existing architecture [14]. They used the sponge-based property of Hash-one and proposed a construction that allows users to switch among symmetric cryptosystems, according to the security requirement.

This article proposes a hybrid KEM that provides entity authentication. So our proposal is similar and comparable to signcryption schemes. We employ the concept of a Master Authority in every communication channel so that a user who wants to communicate with another user in a particular network needs to register under the master authority and obtain their user id. At the time of registration, the user chooses a signature scheme along with a signing key and exchanges the verification key securely with the master authority. We use a sponge-based hash function that enables us to change the symmetric cryptosystem according to the security requirement. The security of the proposed construction is analysed against adversaries performing different attacks. Peikert and Waters [4] proposed a construction to use one-time strong unforgeable signatures and used that in proving IND-CCA2 security in the standard model. Our scheme allows signature reuse while maintaining the IND-CCA2 security in the standard model.

Motivation and Related works: Recently, we can see many of the signcryption schemes finds applications in networks [15, 16]. We already have many elliptic curve-based public key encryption schemes [17, 18]. So we are approaching the asymmetric cryptography in a different approach other than elliptic curves. Post-quantum signcryption schemes existing in the literature are

very limited. The lattice-based constructions using SIS, LWE problems and their adaptations are secure. But our construction stands alone from those as we do not directly employ these problems. We use the LWE problem for the construction of a lossy trapdoor function involved in our construction.

In this article, the proposed construction and correctness proof is mentioned in Section 2. Section 3 describes the security analysis, compares the proposed construction with similar schemes and Section 4 concludes the article.

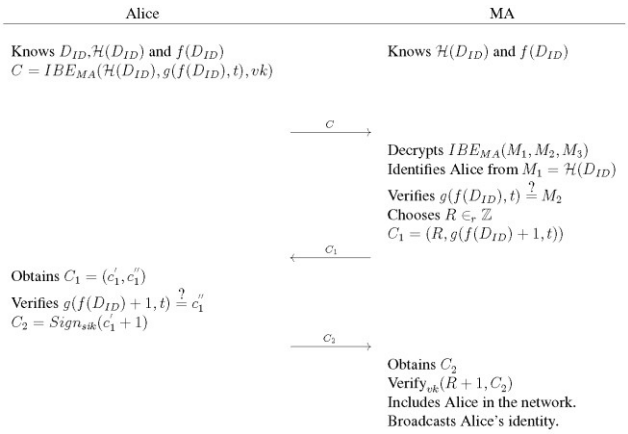
2. Proposed Construction

The proposed hybrid encryption scheme with entity authentication provides ciphertext integrity and is secure against IND-CCA2 attack in the standard model. In the registration phase, the entity Alice registers at the Master Authority (MA) and obtains a user identity. Using that, Alice will communicate with other users in the network in the subsequent communication phase.

2.1 *Registration*

This section explains how a new entity (Alice) can register with Master Authority(MA) and become part of the network to communicate with other entities. Suppose that a user, Alice, has a device identifier (D_{ID}). The following are known only to Alice and the Master Authority (MA):

1. $\mathcal{H}(D_{ID})$, a hash value of the (D_{ID})
2. $f(D_{ID})$, a function of D_{ID}
3. A time stamp, t
4. A one-way function g defined on an extended domain formed by the cartesian product $Range(f) \times Domain(t)$.
5. A strongly unforgeable signature scheme agreed by the users with signing key (denoted by sik) and verification key (denoted by vk).



Protocol 1
Registration

2.2 *Communication*

This section describes the communication between two entities, Alice and Bob, already registered with MA under the same network. Consider the case where Alice encrypts a message m to Bob using Bob's Public key. Bob's public key is the 3-tuple $(\mathcal{B}_1, \mathcal{B}_2, \mathcal{B}_3) = (F_{Bob}, G_{Bob}, h_{Bob})$, where F_{Bob} is the lossy trapdoor function, G_{Bob} is the ABO-trapdoor function and h_{Bob} is the hash function chosen by Bob [4]. Since we are using the LWE-based construction, the injective function is the same for all the users, but only the trapdoor varies from user to user.

Let $p_1, p_2, p_3, m, q \in \mathbb{Z}^+$, q prime. Let $A \xleftarrow{\$} \mathbb{Z}_q^{p_3 \times m}$, $S \xleftarrow{\$} \mathbb{Z}_q^{p_2 \times m}$ and $E \leftarrow \chi^{p_3 \times p_2}$. $C = (A, B = AS^T + E) \in \mathbb{Z}_q^{p_3 \times (m+p_2)}$ is called the concealer matrix output by the function $Conceal_\chi(p_3, p_2)$.

Bob invokes the $Conceal_\chi(n, m_3)$ and outputs a function index $F_{Bob} = (A_{Bob}, B_{Bob} + M_{Bob}) \in \mathbb{Z}_q^{n \times (m_2 + m_3)}$ with the trapdoor S_{Bob}. Consider $\emptyset \neq ID, K\ddot{O}\{0,1\}^{m_3}$ with $ID \cap K = \emptyset$. ID is the set from which the user identities are assigned. Before starting the encryption process, Bob chooses an element $v^* \in K$ to form the ABO function. G_{Bob} corresponds to the ABO function chosen by Bob in which $G_{Bob} = (A_{Bob}, B'_{Bob})$. That is, $G_{Bob} = (A_{Bob}, B_{Bob} - r(v^*))$ and hence $G_{Bob} = (A_{Bob}, A_{Bob}S_{Bob}^T + E - r(v^*))$. $\mathcal{B}_3 = \mathcal{H}_{Bob}$ is a sponge based hash function. The representation of the protocol is shown in Protocol 2.

Alice		Bob
Obtain $\mathcal{B} = \{\mathcal{B}_1, \mathcal{B}_2, \mathcal{B}_3\}$		
$x \xleftarrow[r]{} \{0,1\}^n$		
Computes $\mathcal{B}_3(x)$		
$C_1 := \mathcal{B}_1(x), C_2 := \mathcal{B}_2(ID_A, x)$		
For the message m, computes $C_3 = \mathcal{E}^{sy}_{\mathcal{B}_3(x)}(m)$		
$\sigma = Sign(C_1, C_2, C_3)$		
$C = (ID_A, C_1, C_2, C_3, \sigma)$		
	$\xrightarrow{C}$	
		Receives $(ID', C_1' C_2', C_3', \sigma')$
		Obtains $vk \leftrightarrow ID'$
		Verify σ'
		$\mathcal{B}_1^{-1}(C_1) = x'$
		$C_2' \stackrel{?}{=} \mathcal{B}_2(ID', x')$ or $\perp$
		$m := \mathcal{D}^{sym}_{\mathcal{B}_3(x)}(C_3)$ or $m := \perp$

Protocol 2
Encryption and Decryption

2.3 *Correctness of the Scheme*

Let us prove the correct inversion of the LTDF function. That is, we show that $x' = x$ in protocol 2. We use the following lemma from [4] in the process.

Lemma 2.1: *Let* $0 < n, p, m_3 \in \mathbb{Z}$. *Let* $q \geq 4pn$, *let* $\frac{1}{\alpha} \geq 8p(n+g)$ *for some* $g > 0$ *and let* $\chi = \bar{\Psi}_\alpha$, *then* $\forall x \in \{0,1\}^n$, *every element of* $\frac{xE}{q}$ *belongs to* $(\frac{-1}{4p}, \frac{1}{4p})$ *except with probability* $m_3 \cdot 2^{-g}$ *over the choice of* $E \leftarrow \chi^{n \times m_3}$.

Now we prove the correctness of $\mathcal{B}_1^{-1}(C_1)$.

Theorem 2.1: *Let* $q \geq 4pn$ *and* $\chi = \bar{\Psi}_\alpha; \frac{1}{\alpha} \geq 16np$, *then the correct inversion of the function* $\mathcal{B}_1$ *follows.*

Proof: Suppose that Bob obtained $C_1 = (k_1, k_2) = (xA_{Bob}, x(B_{Bob} + M))$. For obtaining x from C_1, Bob computes

$$\begin{aligned} k &= k_2 - k_1 S_{Bob}^T \\ &= xB_{Bob} + xM - xA_{Bob}S_{Bob}^T \\ &= xA_{Bob}S_{Bob}^T + x(E+M) - xA_{Bob}S_{Bob}^T \\ &= xE + xM \\ &= xE + x\rho(\bar{I} \bmod p) \\ &= xE + x\left\lfloor q \cdot \frac{\bar{I}}{p} \right\rceil \end{aligned}$$

Let $I_1 = \left[\frac{-1}{2}, \frac{1}{2}\right] \subset \mathbb{R}$, I_1^k denote the vector of length k taking entries from I_1, $I_1^{k \times l}$ denote the $k \times l$ matrix taking entries from I_1 and $T = \rho^{-1}(k)$.

$$\begin{aligned} T &= \left\lfloor p \cdot \frac{xE + x\left\lfloor q \cdot \frac{\bar{I}}{p} \right\rceil}{q} \right\rceil \\ &\in \left\lfloor p \cdot \frac{xE}{q} + \frac{p}{q} \cdot x\left(I_1^{n \times m_3} + q \cdot \frac{\bar{I}}{p}\right) \right\rceil && \text{(Remark after Lemma 2.1)} \\ &\in \left\lfloor p \cdot \left(\frac{-1}{4p}, \frac{1}{4p}\right)^{m_3} + \frac{p}{q} \cdot xI_1^{n \times m_3} + x\bar{I} \right\rceil && \text{(Lemma 2.1)} \\ &\in \left\lfloor \frac{1}{2} \cdot I_1^{m_3} + \frac{p}{q} \cdot xI_1^{n \times m_3} + x\bar{I} \right\rceil \end{aligned}$$

We have, by the triangle inequality, $xI_1^{n \times m_3} \in n \cdot I_1^{m_3}$. Also by the choice of parameters, we have $q \geq 4pn \Longrightarrow \frac{p}{q} \leq \frac{p}{4pn} = \frac{1}{4n}$. Therefore,

$$\begin{aligned} T &\in \left\lfloor \frac{1}{2} \cdot I_1^{m_3} + \frac{1}{4} \cdot I_1^{m_3} + x\bar{I} \right\rceil \\ T &\in \left\lfloor \frac{3}{4} \cdot I_1^{m_3} + x\bar{I} \right\rceil \\ T &= x\bar{I} \end{aligned}$$

Now let $k' = x\bar{I} (\mathrm{mod}\, p)$. The binary representation of k' will yield x.

The trapdoor for the function G_{Bob} is available and hence the correct inversion is possible. But we only need to recreate the same for verification of

ciphertext integrity. We already proved that $x' = \mathcal{B}_1^{-1}(C_1) = x$. Now, $ID = ID' \Longrightarrow C_{2'} = B_2(ID', x') = B_2(ID, x) = C_2$ and the verification will be successful.

Irrespective of the symmetric cryptosystem used, the key used by Alice to encrypt m as $\mathcal{E}^{sym}_{\mathcal{B}_3(x)}(m) = C_3$ will be $\mathcal{B}_3(x)$. Since $\mathcal{B}_1^{-1}(C_1) = x$, we have $\mathcal{D}^{sym}_{\mathcal{B}_3(x')}(C_3) = \mathcal{D}^{sym}_{\mathcal{B}_3(x)}\left(\mathcal{E}^{sym}_{\mathcal{B}_3(x)}(m)\right) = m$.

3. Security Analysis

3.1 *IND-CCA2 Security*

We prove that our construction is secure against an adversary capable of performing an IND-CCA2 attack.

We are employing a game-hopping technique model for the proof. Before defining the hybrids, we are quoting two very important lemmas proposed in [19]

Lemma 3.1: *If Y takes at most 2^r possible values and X is any random variable, then*

$$\widetilde{H}_\infty(X|Y) \geq H_\infty(X) - r$$

Definition 3.1: *A collection $\mathbb{H}$ of functions from $\{0,1\}^n \to \{0,1\}^l$ is an average case (n, k, l, ε) strong extractor if for all the pairs of random variables (X,Y) such that $X \in \{0,1\}^n$ and $\widetilde{H}_\infty(X|Y) \geq k$, it holds that for $\mathcal{H} \leftarrow \mathbb{H}$ and $r \leftarrow \{0,1\}^l$,*

$$\Delta((\mathcal{H}, \mathcal{H}(X), Y), (\mathcal{H}, r, Y)) \leq \varepsilon$$

Lemma 3.2: *Let X and Y be random variables such that $x \in \{0,1\}^n$ and $\widetilde{H}_\infty(X|Y) \geq k$. Let $\mathbb{H}$ be a family of universal hash functions from $\{0,1\}^n \to \{0,1\}^l$, where $l \leq k - 2log_2\left(\frac{1}{\varepsilon}\right)$. Then $\mathbb{H}$ is an average case (n, k, l, ε)-strong extractor.*

We define the function triplets $(\mathcal{G}, \mathcal{E}, \mathcal{D})$ for the following theorem.

- $\mathcal{G}$, the key generation algorithm, takes a security parameter as input and outputs an ordered pair (*pk,sk*) .
- $\mathcal{E}$, the encryption algorithm takes pk and $n \in \mathcal{M}$ as input and outputs a ciphertext c.
- $\mathcal{D}$ takes the ciphertext c and the secret key sk as input and outputs $m \in \mathcal{M}' = \mathcal{M} \cup \{\perp\}$

Theorem 3.1: *The triplet of algorithms key generation, encryption and decryption $(\mathcal{G}, \mathcal{E}, \mathcal{D})$gives an IND-CCA2-secure cryptosystem.*

Proof: We engage the game-hopping technique to prove the claim. As we already have proven the correctness of the scheme, we will now set up the paraphernalia

required to design the experiments. Each experiment contains primarily three algorithms, which we will alter according to the experiment. They are

- Set: The algorithm runs and outputs a public key pk.
- Dec: This is an algorithm which works as a decryption oracle. This one takes a ciphertext c as input and outputs a value m from the message space or outputs $\perp$.
- Chal: This algorithm corresponds to the challenge phase where the adversary provides two values m_0 and m_1 which Chal takes as input and outputs c^*.

Now we define the hybrids one by one and will prove that each hybrid is either computationally or statistically indistinguishable from the preceding one. For the notation convenience, we define that

- Hybrid_1: Set_1 gets $(\text{pk}, \text{sk}) \leftarrow \mathcal{G}$ and outputs pk. $\text{Dec}_1(c) \rightarrow \mathcal{D}(sk, c)$ and $\text{Chal}_1(m_0, m_1) \rightarrow \mathcal{E}(pk, m_b)$. In addition, the lossy branch will be 0^v.
- Hybrid_2: In the ciphertext $c = (ID, C_1, C_2, C_3, \sigma)$ if $ID = v^*$ output $\perp$. else return $\text{Dec}_1(c)$
- Hybrid_3: The lossy branch of the ABO function is v^* instead of 0^v. In $\mathcal{G}$, $(\zeta', \eta') \leftarrow \Phi_{abo}(v^*)$.
- Hybrid_4: The witness recovery was using the injective function trapdoor. But in this hybrid, ABO inversion function and trapdoor is used. Mathematically, $x = G_{abo}^{-1}(\eta', ID, C_2)$. Here the verification check will be $C_1 \stackrel{?}{=} F_l(\zeta, x)$.
- Hybrid_5: $(\zeta, \eta) \leftarrow \Phi_i$ is replaced with $(\zeta, \perp) \leftarrow \Phi_l$. The setup in Hybrid_5 is as follows: $(\zeta', \eta') \leftarrow \Phi_{abo}(v^*)$,

  $(\zeta, \eta) \leftarrow \Phi_l, \mathcal{H} \leftarrow \mathcal{H}$ and outputs $pk = (\zeta, \zeta', h)$.
- Hybrid_6: The C_3 component is replaced with a uniform random value of the same length. The final description will be

  $x \leftarrow \{0,1\}^{\mu}$, $C_1 = F_l(\zeta, x), C_2 = G_{abo}(\zeta', v^*, x)$,
  $C_3 \underset{r}{\leftarrow} \{0,1\}^{l}$, $\sigma = \text{Sign}(sik_{\sigma}, (C_1, C_2, C_3))$ and output
  $c = (v^*, C_1, C_2, C_3, \sigma)$.

Claim 3.1: The adversary has only a negligible advantage in computationally distinguishing between $Hybrid_1$ and $Hybrid_2$.

Proof of claim: W e are choosing values from a set of cardinality 2^{m_3}. Consider a finite set S having cardinality K. Let $\alpha \in_r S$ be taken, noted down and replaced. Now take $\beta \in_r S$. Since the events are iids, $Pr[|\alpha - \beta| = 0] = \frac{1}{K}$. Here in our case, if we denote H_i to be the event in Hybrid_i, $|Pr[H_1] - Pr[H_2]| = \frac{1}{2^{m_3}}$.

Claim 3.2: The adversary has only a negligible advantage in computationally distinguishing between $Hybrid_2$ and $Hybrid_3$.

Proof of claim: T o prove this claim, we are using a PPT simulator $\mathcal{T}$ to interact in the hidden lossy branch experiment of the ABO collection. Suppose that $\mathcal{T}$ gives the experiment two branches 0^v and v^* and obtains ζ' as the output of either $\Phi_{abo}(0^v)$ or $\Phi_{abo}(v^*)$. Now the process works as follows: $\mathcal{T}$ implements Set and $(\zeta, \eta) \leftarrow \Phi_i, \mathcal{H} \leftarrow \mathbb{H}$ and outputs $pk = (\zeta, \zeta', h)$. The algorithms Dec and Chal are unchanged between both the hybrids. Now observe that the view generated by $\mathcal{T}$ is exactly Hybrid_3 provided $\zeta \leftarrow \Phi_{abo}(v^*)$ and is of Hybrid_2 when $\zeta \leftarrow \Phi_{abo}(0^v)$.

Claim 3.3: The adversary has only a negligible advantage in distinguishing between $Hybrid_3$ and $Hybrid_4$.

Proof of claim: T he implementation of the algorithm Dec is the only difference between Hybrid_3 and Hybrid_4. It is evident that $f_\zeta(\cdot)$ and $g_{\zeta',ID}(\cdot)$ are both injective, and hence x is unique since it satisfies both the decryptions and both the verification simultaneously, though obtained in both the hybrids in different ways. Hence the claim.

Claim 3.4: The adversary has only a negligible advantage in distinguishing between $Hybrid_4$ and $Hybrid_5$.

Proof of claim: T o prove this claim, we engage a PPT simulator $\mathcal{T}$ once again. Let $\zeta \leftarrow \Phi_i$ be a function index, then $\mathcal{T}$ simulates Hybrid_4 and if $\zeta \leftarrow \Phi_l$, then $\mathcal{T}$ simulates Hybrid_5.

$\mathcal{T}$ takes ζ as input and implements Set, Dec and Chal as in Hybrid_4. $(\zeta', \eta') \leftarrow \Phi_{abo}(v^*), \mathcal{H} \leftarrow \mathbb{H}$ and $pk = (\zeta, \zeta', h)$. So $\mathcal{T}$ knows the ABO trapdoor η', which is used for witness recovery in both Hybrid_4 and Hybrid_5. Without knowing the trapdoor, η corresponding to the function index ζ, $\mathcal{T}$ is able to implement successfully both Hybrid_4 and Hybrid_5. Hence by the indistinguishability of injective and lossy functions, the claim follows.

Claim 3.5: The adversary has only a negligible advantage in statistically distinguishing between $Hybrid_5$ and $Hybrid_6$.

Proof of claim: A ssume that except for the hash function h and x used by Chal, all the randomness is fixed. Note that we are now on the lossy function instead of the injective function and on the lossy branch of the ABO function, also. Hence $F_l(\zeta, \cdot) = f_\zeta(\cdot)$ has an image size not exceeding $2^{\mu-\nu}$ and $G_{abo}(\zeta', v^*, \cdot) = g_{\zeta', v^*}(\cdot)$ has an image size not more than $2^{\mu-\nu'}$. Hence the random variables (c_1^*, c_2^*) can take at most $2^{\gamma+\gamma'} \leq 2^{\mu-\kappa}$

By lemma 3.1, we have

$$\widetilde{H}_\infty(x|(c_1^*, c_2^*)) \geq H_\infty(x) - (\mu - \kappa) = \mu - (\mu - \kappa) = \kappa$$

Now by the assumption that $l \leq \kappa - 2\log_2\left(\frac{1}{\varepsilon}\right)$ and lemma 3.2, we have

$$\Delta((c_1^*, c_2^*, h, \mathcal{E}^{\mathrm{sy}}_{h(x)}(m)), (c_1^*, c_2^*, h, r')) \leq \varepsilon = \mathrm{negl}(\lambda)$$

where r' is independent of all other variables. Hence the claim.

3.2 *Unforgeability*

We recommend the user a strong unforgeable signature scheme. The security of the scheme depends on the security of the signature used [20]. So it is evident that our scheme, if used as directed, provides sUF-CMA security.

3.3 *Secure against Man-in-the-Middle Attack*

The adversary can replace $C = IBE_{MA}(h(D_{ID}), g(f(D_{ID}), t), vk)$ with $C' = (h(D'_{ID}), g(f(D_{ID}), t), vk)$, formed using the hash of his device id. Since the MA verifies C' by checking whether $M_2 \stackrel{?}{=} g(f(D'_{ID}), t)$, it will turn out to be a mismatch if the adversary doesn't change the second component (originally $g(f(D_{ID}), t)$). Once the adversary changes the component M_2 also to $g(f(D'_{ID}), t)$, it will turn out to be a legitimate registration of the adversary and not an impersonation as user Alice. Hence the proposed construction is secure against a man-in-the-middle attack.

3.4 *Secure against Replay Attack*

Suppose that the adversary is trying to replay a previous message to impersonate as Alice to MA. The components C_1 and $C_2 = Sign_{sik}(R + 1)$ contain a fresh and randomly chosen value R and hence the replay can be identified. Thus we can conclude that the scheme is secure against Replay attacks.

3.5 *Post Quantum Security*

Oded Regev [21] showed that the LWE problem is as hard as some standard worst-case lattice problems for quantum algorithms. A modified version of the main theorem by Regev is given by Peikert and Waters in [4], which can be interpreted as follows.

Theorem 3.2: *Let* $\alpha(d) \in (0,1)$ *and* $q(d)$ *be a prime number such that* $\alpha \cdot q > 2\sqrt{d}$. *There is a quantum polynomial time reduction from solving either SIVP or GapSVP problems in the worst case to solving* $LWE_{q,\bar{\Psi}_\alpha}$

In literature, there are no successful algorithms available that solves the above problems. So if the user chooses a post-quantum secure signature scheme for their use, the proposed construction will be post-quantum secure.

3.6 *Comparison with similar schemes*

In this section, we compare our scheme with some of the similar schemes in literature regarding the security they provide and the properties they possess. Most of the schemes similar to our scheme are based on elliptic curve pairings. So, in Comparison Table 1, we compare our construction with some of the recent

or standard schemes on the basis of the security properties, whether it involves pairing computation, whether it provides post-quantum security etc. To resolve ambiguity, by privacy, we mean that the original identity of the user is never shared in the protocol. Instead, an alias identity or a function output of the device identifier will be used in the protocol. The computation assumptions which the schemes are based on are also listed in the same table. The abbreviations used in Comparison Table 1 are listed below in Table 1.

Comparison Table 1

Properties

Scheme	IND-CCA2	EUF-CMA	Privacy/ Anonimity	Pairing free	Post-Quantum Security	Computation Assumption
Xiaoguang Liu *et al*. [22]	✓	✓	✓	✓	×	IFP
YW Zhou *et al.* [23]	✓	✓	✓	✓	×	CDH, DLP
Fuxiao Zhou *et al*. [24]	✓	✓	×	×	×	DDH-CDH
Insaf Ullah *et al*. [25]	✓	✓	✓	✓	×	DLP
Ahmed Elkhalil *et al*. [16]	✓	✓	✓	✓	×	CDH
Mutaz Elradi S Saeed *et al*. [26]	✓	✓	✓	×	×	q-BDHIP
Bo Zhang*et al.* [27]	✓	✓	✓	✓	×	ECDLP
Ikram Ali *et al.* [15]	✓	✓	✓	×	×	q-BDHIP,q-SDH
Aravind Vishnu *et al*. [13]	✓	✓	×	×	×	VDP
ALGAES	✓	✓	✓	✓	✓	LWE

Table 1

Legend to the notations in Comparison Table 1

Notation	Description	Notation	Description
DDH	Decisional Diffie-Hellman	CDH	Computational Diffie-Hellman
DLP	Discrete Logarithm Problem	IFP	Integer Factorisation Problem
LWE	Learning With Errors	ECDLP	Elliptic Curve DLP
q-BDHIP	q-Bilinear Diffie-Hellman Inversion Problem		
q-SDH	q-Strong Diffie Hellman		
VDP	Vector Decomposition Problem		

We also compared our scheme with some of the existing similar schemes for security features like confidentiality, authentication, integrity, privacy, non-repudiation, traceability, unlinkability, resistance to replay attacks and resistance to impersonation.

Comparison Table 2

Security feature comparison

Scheme	S-1	S-2	S-3	S-4	S-5	S-6	S-7	S-8	S-9
Fuxiao Zhou *et al*. [24]	✓	✓	✓	×	✓	×	✓	×	✓
Ahmed Elkhalil *et al*. [16]	✓	✓	✓	✓	✓	✓	✓	×	✓
Ikram Ali *et al.* [15]	✓	✓	✓	✓	✓	✓	✓	✓	✓
Fagen Li and Pan Xiong [28]	✓	✓	✓	×	✓	×	✓	×	✓
ALGAES	✓	✓	✓	✓	✓	✓	✓	✓	✓

Table 2

Legend to the notations in Comparison Table 2

Notation	Description	Notation	Description
S-1	Confidentiality	S-6	Traceability
S-2	Authentication	S-7	Unlinkability
S-3	Integrity	S-8	Resistance to replay attacks
S-4	Privacy	S-9	Resistance to impersonation
S-5	Non-Repudiation		

4. Conclusion

The article proposes a hybrid encryption algorithm based on lossy trapdoor functions. The conventional lossy trapdoor based constructions uses XOR function as the symmetric encryption. We introduced a method to incorporate any symmetric encryption scheme into the hybrid construction instead of simple XOR operation. This makes the proposed construction stand out from similar constructions. The choice for the symmetric encryption scheme makes the system compatible to various user requirements. In our construction, we allowed signature reuse, resulting in improved efficiency. The scheme is proved to be IND-CCA2 secure in the standard model using game-hopping technique and it performs witness recovery. The strongly existential unforgeable (sUF-CMA) signature scheme under chosen message attack ensures ciphertext integrity and unforgeability. Typically in hybrid encryption schemes, there is no entity authentication, but, we incorporated an entity authentication technique in our hybrid construction. The hard problem that holds the scheme is the Learning With Errors problem on lattices which is post-quantum secure. Therefore, the construction is an efficient post-quantum IND-CCA2 secure hybrid encryption with entity authentication.

Acknowledgement

The authors would like to thank Prof. Veni Madhavan for his valuable suggestions. We also would like to thank the anonymous reviewer for a very high quality detailed feedback.

References

[1] C. Peikert et al., "A decade of lattice cryptography," *Foundations and trends in theoretical computer science,* vol. 10, no. 4, pp. 283–424 (2016).

[2] V. Shoup, "Using hash functions as a hedge against chosen ciphertext attack," in International Conference on the Theory and Applications of Cryptographic Techniques, pp. 275–288, Springer (2000).

[3] E. Fujisaki and T. Okamoto, "Secure integration of asymmetric and symmetric encryption schemes," *Journal of cryptology*, vol. 26, no. 1, pp. 80–101 (2013).

[4] C. Peikert and B. Waters, "Lossy trapdoor functions and their applications," *SIAM Journal on Computing*, vol. 40, no. 6, pp. 1803–1844 (2011).

[5] N. Alamati, H. Montgomery, S. Patranabis, and A. Roy, "Minicrypt primitives with algebraic structure and applications," *Journal of Cryptology,* vol. 36, no. 1, pp. 1–106 (2023).

[6] V. Goyal, O. Pandey, and S. Richelson, "Textbook nonmalleable commitments," in Proceedings of the forty-eighth annual ACM symposium on Theory of Computing, pp. 1128–1141 (2016).

[7] M. Bellare, D. Hofheinz, and S. Yilek, "Possibility and impossibility results for encryption and commitment secure under selective opening," in Annual International Conference on the Theory and Applications of Cryptographic Techniques, pp. 1–35, Springer (2009).

[8] S. Katsumata, T. Tomita, and S. Yamada, "Direct computation of branching programs and its applications to more efficient lattice-based cryptography," *Designs, Codes and Cryptography*, vol. 91, no. 2, pp. 391–431 (2023).

[9] G. Bertoni, J. Daemen, M. Peeters, and G. Van Assche, "Sponge functions," in ECRYPT hash workshop, vol. 2007, Citeseer (2007).

[10] G. Bertoni, J. Daemen, M. Peeters, and G. V. Assche, "Keccak," in Annual international conference on the theory and applications of cryptographic techniques, pp. 313–314, Springer (2013).

[11] Y. Zheng, "Digital signcryption or how to achieve cost (signature & encryption) $\ll$ cost (signature)+ cost (encryption)," in Annual international cryptology conference, pp. 165–179, Springer (1997).

[12] P. Megha Mukundan, S. Manayankath, C. Srinivasan, and M. Sethumadhavan, "Hash-one: a lightweight cryptographic hash function," *IET Information Security,* vol. 10, no. 5, pp. 225–231 (2016).

[13] S. Aravind Vishnu, I. Praveen, and M. Sethumadhavan, "An IND-CCA2 Secure Certificateless Hybrid Signcryption," *Wireless Personal Communications*, vol. 119, no. 4, pp. 3589–3608 (2021).

[14] K. Prasad and H. Mahato, "Cryptography using generalized fibonacci matrices with affine-hill cipher," *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 25, no. 8, pp. 2341–2352 (2022).

[15] I. Ali, T. Lawrence, A. A. Omala, and F. Li, "An efficient hybrid signcryption scheme with conditional privacypreservation for heterogeneous vehicular communication in vanets," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 10, pp. 11266–11280 (2020).

[16] A. Elkhalil, J. zhang, R. Elhabob, and N. Eltayieb, "Poosc: Provably online/offline signcryption scheme for vehicular communication in vanets," *Computing*, vol. 105, no. 11, pp. 2539–2561 (2023).

[17] I. Praveen, K. Rajeev, and M. Sethumadhavan, "An authenticated key agreement scheme using vector decomposition," *Defence Science Journal,* vol. 66, no. 6, p. 594 (2016).

[18] I. Praveen, S. A. Vishnu, and M. Sethumadhavan, "An efficient composable 1-out-of-2 oblivious transfer scheme using vector decomposition," *International Journal of Advanced Intelligence Paradigms,* vol. 27, no. 2, pp. 178–194 (2024).

[19] Y. Dodis, R. Ostrovsky, L. Reyzin, and A. Smith, "Fuzzy extractors: How to generate strong keys from biometrics and other noisy data," *SIAM journal on computing*, vol. 38, no. 1, pp. 97–139 (2008).

[20] T. E. Bjørstad and A. W. Dent, "Building better signcryption schemes with tag-kems," in Public Key Cryptography-PKC 2006: 9th International Conference on Theory and Practice in Public-Key Cryptography, New York, NY, USA, April 24-26, 2006. Proceedings 9, pp. 491–507, Springer (2006).

[21] O. Regev, "On lattices, learning with errors, random linear codes, and cryptography," *Journal of the ACM* (JACM), vol. 56, no. 6, pp. 1–40 (2009).

[22] X. Liu, Z. Wang, Y. Ye, and F. Li, "An efficient and practical certificateless signcryption scheme for wireless body area networks," *Computer Communications*, vol. 162, pp. 169–178 (2020).

[23] Y. Zhou, B. Yang, and W. Zhang, "Provably secure and efficient certificateless generalized signcryption," *Chinese Journal of Computers*, vol. 39, no. 3, pp. 543–551 (2016).

[24] F. Zhou, Y. Li, and Y. Ding, "Practical v2i secure communication schemes for heterogeneous vanets," *Applied Sciences*, vol. 9, no. 15, p. 3131 (2019).

[25] I. Ullah, A. Alomari, N. Ul Amin, M. A. Khan, and H. Khattak, "An energy efficient and formally secured certificate-based signcryption for wireless body area networks with the internet of things," *Electronics*, vol. 8, no. 10, p. 1171 (2019).

[26] M. E. S. Saeed, Q. Liu, G. Tian, B. Gao, and F. Li, "Hoosc: heterogeneous online/offline signcryption for the internet of things," *Wireless Networks*, vol. 24, pp. 3141–3160 (2018).

[27] B. Zhang, Z. Jia, and C. Zhao, "An efficient certificateless generalized signcryption scheme," *Security and Communication Networks*, vol. 2018 (2018).

[28] F. Li and P. Xiong, "Practical secure communication for integrating wireless sensor networks into the internet of things," *IEEE Sensors Journal*, vol. 13, no. 10, pp. 3677–3684 (2013).

Received February, 2025