IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received December 10, 2021, accepted January 6, 2022, date of publication January 19, 2022, date of current version January 31, 2022.

Digital Object Identifier 10.1109/ACCESS.2022.3144725

An Efficient Public-Key Dual-Receiver Encryption Scheme

CHENGLONG GAO[1], KAI CHEN[1], QIANG WANG[2], AND ZHIXIAN CHEN[3]
[1]Information Technology Department, Shanghai Pudong Development Bank, Shanghai 200002, China
[2]College of Computer Science and Technology, Zhejiang University, Hangzhou 310027, China
[3]Department of Information Security, Zhejiang Gongshang University, Hangzhou 310018, China

Corresponding author: Zhixian Chen (chenzx@zjgsu.edu.cn)

ABSTRACT Public-key dual-receiver encryption (PK-DRE) is a kind of particular public-key encryption for enabling two independent recipients to obtain the same plaintext from the same ciphertext. Due to its dual-receiver property, PK-DRE is quite helpful in many scenarios, such as deniable authentication, global key escrow, security puzzle, and even blockchain. In this paper, we revisit the PK-DRE scheme CFZ14 proposed at CT-RSA 2014 and propose a variant. This variant is original from a new security proof which allows us to remove some steps in CFZ14. To the best of our knowledge, the obtained variant is more efficient than the existing PK-DRE schemes in terms of public verifiability and key size.

INDEX TERMS Public-key dual-receiver encryption, CCA security, standard model.

I. INTRODUCTION

Public key dual-receiver encryption (PK-DRE) allows two independent recipients to recover the same plaintext from the same ciphertext. As shown in [1] and [2], PK-DRE is very suitable for the setting where it requires simultaneous escrow of decryption rights while keeping the signing rights for the single private key per user. Besides the dual-receiver property, PK-DRE usually requires public verifiability that enables everyone to check whether the two recipients can get the same plaintext. Due to the dual-receiver property and public verifiability, PK-DRE can also be applied in the following scenarios, including deniable authentication [3], security puzzle [4], PKE with the non-interactive opening [5], and even blockchain [6]. The concept of PK-DRE and the first concrete PK-DRE scheme are proposed by Diament *et al.* [1] at ACM CCS 2004, and Chow *et al.* [7] refined the syntax of PK-DRE later on. Since then, many PK-DRE schemes with different properties have been proposed. Generally speaking, the existing PK-DRE schemes can be classified into two categories according to the underlying complexity assumptions, namely pairing-based [1], [7]–[9] and lattice-based [10]–[12]. Although the lattice-based schemes are quantum-safe, the pairing-based schemes are usually preferable for practical use for the following reasons.

- All the existing lattice-based schemes do not support the public verifiability. As mentioned in [7], public verifiability is useful in many applications, such as threshold decryption.
- The key size of lattice-based schemes is usually quite large, and it is even as large as several megabytes in some cases [12]. This situation hinders the use of lattice-based PK-DRE in some storage-limited settings, such as the Internet of Things.
- The design of quantum computer is still in process. There is no public-known experimental quantum computer breaking any real cryptographic algorithm.

On the other hand, the scheme (we call it CFZ14 in this paper) proposed in [7] is the best one among the current pairing-based PK-DRE schemes in terms of the security level and computational cost. The detailed comparison can be found in Section II. In this paper, we restudy CFZ14, especially its security proof. We find another security proving method for CFZ14, which leads us to a variant of CFZ14. In particular, according to our new security proof, we can remove "g^r" from the ciphertext and obtain a more efficient PK-DRE scheme in terms of ciphertext size and encryption/decryption cost. As a result, our variant of CFZ14 would be the best one among the current pairing-based PK-DRE schemes instead of CFZ14.

The rest of this paper is organized as follows. In section II, we summarize the existing PK-DRE schemes. Section III reviews the definition and security model for public-key

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

TABLE 1. Summary of the existing DRE schemes in terms of security, public verifiability, and key size.

	DLK+04 [1]	CFZ14 [7]	ZCL+17 [8]	ZZL+18 [10]	LZD+19 [11]	LWS+20 [12]	PP21 [9]	Ours
Quantum-safe	×	×	✓	✓	✓	×	×	×
CCA secure in standard model	×	✓	✓	✓	✓	✓	×	✓
Public verifiability	×	✓	✓	×	×	×	×	✓
No large key size problem	✓	✓	×	×	×	×	✓	✓

dual-receiver encryption and some basic knowledge. In what follows, we give the description of the proposed variant of CFZ14 along with the description of CFZ14 for clarification. After that, we present the security proof of our variant and the performance comparison with CFZ14. At last, we end this paper with the conclusion in Section VI.

II. RELATED WORK

As we mentioned before, the concept of public-key dual-receiver encryption was proposed by Diament *et al.* [1] at ACM CCS 2004. In the same work, they also proposed a concrete PK-DRE scheme with CCA security in the random oracle model by using the three-party key exchange protocol due to Joux [13]. Ten years later, Chow *et al.* [7] refined the syntax of PK-DRE and proposed the first PK-DRE scheme with CCA security in the standard model and public verifiability. Since then, many PK-DRE schemes with different properties have been proposed. For instance, Zhang *et al.* [8] and Patil and Purushothama [9] extended the PK-DRE to the identity-based setting and proxy re-encryption setting, respectively. However, due to the use of Waters' hash function [14], the key size and computational cost in Zhang *et al.*'s scheme [8] are linearly correlated with the bit-length of the identity. Furthermore, Patil and Purushothama's scheme [9] is only CPA-secure and does not support public verifiability.

The above PK-DRE schemes are all based on pairings, and several researchers tried to construct PK-DRE based on lattice for security against attacks from quantum computers. The first lattice-based (identity-based) PK-DRE scheme is proposed by Zhang *et al.* [10], and the corresponding CCA security can be obtained based on the standard Learning with Errors assumption. Based on this result, Liu *et al.* [11] proposed two generic constructions for PK-DRE and identity-based DRE by using (weak) lattice-based programmable hash functions with high min-entropy. Recently, Liu *et al.* [12] improved the result in [10] and proposed the concept of hierarchical identity-based DRE along with a concrete scheme. However, none of the above lattice-based schemes support public verifiability, and all of them suffer from the large key size problem.

We give a summary of the existing DRE schemes in Table 1, where we can see that CFZ14 is the best one among the existing DRE schemes, in terms of security level, public verifiability, and key size.

There are many one-to-many public key encryptions, such as broadcast encryption and attribute-based encryption. The main difference between PK-DRE and these encryptions is the independence of recipients. In these one-to-many public key encryptions, there usually exists a trusted party who is responsible for generating the user's decryption key. In contrast, users generate the decryption key by themselves in PK-DRE. Clearly, these one-to-many encryptions cannot realize the delegation of decryption rights while keeping the signing rights, since the trusted party already knows the signing key.

III. PRELIMINARIES

In this section, we review the definition of public-key dual-receiver encryption and the corresponding security model for chosen-ciphertext (CCA) security. We also review some basic knowledge related to the construction of CFZ14, including the bilinear groups and strong-unforgeable one-time signature.

A. PUBLIC-KEY DUAL-RECEIVER ENCRYPTION

Generally speaking, a public-key dual-receiver encryption (PK-DRE) scheme consists of the following four algorithms: Setup, KeyGen, Enc, and Dec.

- $\mathtt{Setup}(1^\lambda) \rightarrow pp$: On input the security parameter λ, the setup algorithm Setup outputs the public parameter pp.
- $\mathtt{KeyGen}(pp) \rightarrow ((pk_1, sk_1), (pk_2, sk_2))$: On input the public parameter pp, the key generation algorithm KeyGen outputs two public/private key pairs (pk_1, sk_1) and (pk_2, sk_2) for two independent users, respectively.
- $\mathtt{Enc}(pp, pk_1, pk_2, m) \rightarrow \mathtt{ct}$: On input the public parameter pp, two independent users' public-keys pk_1 and pk_2, and a message m from the plaintext space $\mathcal{M}$, the encryption algorithm Enc outputs a ciphertext ct.
- $\mathtt{Dec}(pp, pk_1, pk_2, sk_i, \mathtt{ct}) \rightarrow m/\perp$: On input the public parameter pp, two independent users' public-keys pk_1 and pk_2, one private key sk_i ($i \in \{1, 2\}$) of the corresponding two independent users, and a ciphertext ct, the decryption algorithm Dec outputs a message m or a failure symbol $\perp$.

1) CORRECTNESS

We say a PK-DRE scheme is correct if the following requirement always holds for $pp \leftarrow \mathtt{Setup}(1^\lambda)$,

$((pk_1, sk_1), (pk_2, sk_2)) \leftarrow \mathtt{KeyGen}(pp)$, and $\mathtt{ct} \leftarrow \mathtt{Enc}(pp, pk_1, pk_2, m)$.

$\mathtt{Dec}(pp, pk_1, pk_2, sk_1, \mathtt{ct}) = \mathtt{Dec}(pp, pk_1, pk_2, sk_2, \mathtt{ct}) = m$.

2) SOUNDNESS

At CT-RSA 2014, Chow *et al.* [7] gave the definition of soundness for PK-DRE. In particular, the soundness states that any probabilistic polynomial time (ppt) adversary, even knowing the private keys of the two independent users, can generate a ciphertext $\mathtt{ct}$ satisfying the following requirement only with a negligible probability.

$$\mathtt{Dec}(pp, pk_1, pk_2, sk_1, \mathtt{ct}) \neq \mathtt{Dec}(pp, pk_1, pk_2, sk_2, \mathtt{ct}).$$

3) SECURITY AGAINST CHOSEN-CIPHERTEXT ATTACKS

The security model for the confidentiality of messages in PK-DRE is given by the following chosen-ciphertext attack game played between an adversary $\mathcal{A}$ and a challenger $\mathcal{C}$.

- **Setup:** In this phase, the challenger $\mathcal{C}$ runs $\mathtt{Setup}$ and $\mathtt{KeyGen}$ to get the public parameter pp and the two independent users' key pairs $((pk_1, sk_1), (pk_2, sk_2))$, respectively. After that, the challenger $\mathcal{C}$ sends pp and (pk_1, pk_2) to the adversary $\mathcal{A}$ while keeping (sk_1, sk_2) secret.
- **Phase 1:** In this phase, the adversary $\mathcal{A}$ can adaptively issue queries to the two decryption oracles.
  - $\mathcal{O}_{d1}$: On input a ciphertext $\mathtt{ct}$ by the adversary $\mathcal{A}$, the challenger $\mathcal{C}$ returns the result of $\mathtt{Dec}(pp, pk_1, pk_2, sk_1)$.
  - $\mathcal{O}_{d2}$: On input a ciphertext $\mathtt{ct}$ by the adversary $\mathcal{A}$, the challenger $\mathcal{C}$ returns the result of $\mathtt{Dec}(pp, pk_1, pk_2, sk_2)$.
- **Challenge:** Once the adversary $\mathcal{A}$ decides to close Phase 1, it can send the challenger $\mathcal{C}$ two messages m_0 and m_1 with the same length from the plaintext space $\mathcal{M}$. The challenger $\mathcal{C}$ returns $\mathtt{Enc}(pp, pk_1, pk_2, m_b)$ to the adversary $\mathcal{A}$ as the challenge ciphertext $\mathtt{ct}^*$, where b is a random bit chosen by the challenger $\mathcal{C}$.
- **Phase 2:** The adversary can continue to issue queries to the oracles as that in Phase 1, except that the challenge ciphertext $\mathtt{ct}^*$ cannot be issued to the decryption oracles.
- **Guess:** The adversary $\mathcal{A}$ outputs a guess b' on b. If $b = b'$, then the adversary wins the game.

Note that there is only one decryption oracle in [7] due to the soundness property. However, we list both two decryption oracles of the two independent users for easy understanding.

Definition 1 (CCA Security): We say a PK-DRE scheme is chosen-ciphertext secure (CCA-secure) if for all ppt adversaries $\mathcal{A}$'s, the advantage of winning the CCA game $|\Pr[b = b'] - 1/2|$ is always negligible.

B. BILINEAR GROUPS

Assume that $\mathbb{G}$ and $\mathbb{G}_t$ are two cyclic groups with prime order q. We say $\mathbb{G}$ and $\mathbb{G}_t$ are bilinear groups if they are equipped with an admissible bilinear map $\hat{e} : \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_t$, satisfying $\hat{e}(g_1^a, g_2^b) = \hat{e}(g_1, g_2)^{ab}$ for all $a, b \in Z_q^*$ and any $g_1, g_2 \in \mathbb{G}$. For convenience, we denote $\mathtt{BSetup}$ as an algorithm that takes the security parameter λ as the input and outputs the parameter of bilinear groups $(\mathbb{G}, \mathbb{G}_t, q, g, \hat{e})$, where $q \in \Theta(2^\lambda)$, and g is a generator of $\mathbb{G}$.

The security proof of our variant is based on the DBSDH (decisional bilinear square Diffie-Hellman) assumption in the bilinear groups, which is stated as follows. Given $g, h, g^a \in \mathbb{G}$ and $T \in \mathbb{G}_t$, it is hard to decide whether $T = \hat{e}(g, h)^{a^2}$. It is easy to see that the DBSDH assumption is a special case of the decisional 2-wBDHI* assumption proposed in [15].

The security proof of the original $\mathtt{CFZ14}$ is based on the DBDH (decisional bilinear Diffie-Hellman) assumption in the bilinear groups. In particular, given $g, g^a, g^b, g^c \in \mathbb{G}$ and $T \in \mathbb{G}_t$, it is hard to decide whether $T = \hat{e}(g, g)^{abc}$.

Although the DBSDH assumption is stronger than the DBDH assumption, it has been shown that the CBSDH (computational bilinear square Diffie-Hellman) assumption and CBDH (computational bilinear Diffie-Hellman) assumption are equivalent [16].

C. ONE-TIME SIGNATURE

Expect that the key pair should be used only once, one-time signature $\mathtt{OTS}$ is almost the same as the regular digital signature. It also contains the following three algorithms $\mathtt{OTS.G}$, $\mathtt{OTS.S}$, and $\mathtt{OTS.V}$.

- $\mathtt{OTS.G}(1^\lambda) \rightarrow (vk, sk)$. On input the security parameter λ, $\mathtt{OTS.G}$ outputs a key pair (vk, sk).
- $\mathtt{OTS.S}(sk, m) \rightarrow \sigma$. On input a signing key sk and a message m, $\mathtt{OTS}.\mathcal{S}$ outputs a signature σ on m.
- $\mathtt{OTS.V}(vk, m, \sigma) \rightarrow 1$ or 0. On input a verifying key vk, a message m and a signature σ, $\mathtt{OTS.V}$ outputs 1 if σ is a signature of m under vk; otherwise, it outputs 0.

For simplicity, we assume $vk \in Z_q^*$ in this paper, where q is the order of the underlying bilinear groups.

1) CORRECTNESS

We say the one-time signature scheme holds the correctness, if for any message $m \neq m'$ in the message space and any key pair $(vk, sk) \leftarrow \mathtt{OTS.G}(1^\lambda)$, both the following conditions are satisfied:

$$\mathtt{OTS.V}(vk, m, \mathtt{OTS.S}(sk, m)) = 1,$$

and

$$\mathtt{OTS.V}(vk, m, \mathtt{OTS.S}(sk, m')) = 0.$$

2) STRONG UNFORGEABILITY

The strong unforgeability of digital signature states that the adversary cannot output any new valid signature on any message without knowing the corresponding signing key, even if the underlying message has been signed before. Strong-unforgeable one-time signature is usually applied for obtaining CCA security of public-key encryption [17].

TABLE 2. The description of the original CFZ14 and our variant.

	CFZ14	Ours
Setup	**Input:** 1^λ **Output:** $pp = (\mathbb{G}, \mathbb{G}_t, q, g, \hat{e}, \mathtt{OTS})$, where $(\mathbb{G}, \mathbb{G}_t, \hat{e}, q, g)$ are obtained from $\mathtt{BSetup}(1^\lambda)$, and OTS is a strong-unforgeable one-time signature scheme.	Identical to that in CFZ14.
KeyGen	**Input:** pp **Output:** $pk_i = (u_i, v_i)$, $sk_i = x_i$ for $\forall i \in \{1,2\}$, where (x_i, y_i) are random numbers from Z_q^*, and $u_i = g^{x_i}$ and $v_i = g^{y_i}$.	**Input:** pp **Output:** $pk_i = (u_i, v_i)$, $sk_i = (x_i, y_i)$ for $\forall i \in \{1,2\}$, where (x_i, y_i) are random numbers from Z_q^*, and $u_i = g^{x_i}$ and $v_i = g^{y_i}$.
Enc	**Input:** pp, pk_1, pk_2, and $m \in \mathbb{G}_t$ **Output:** $\mathtt{ct} = (vk, c, \pi_1, \pi_2, \pi, \sigma)$, where $(vk, sk) \leftarrow \mathtt{OTS.G}(1^\lambda)$, $c = g^r$, $\pi_1 = (u_1^{vk} v_1)^r$, $\pi_2 = (u_2^{vk} v_2)^r$, $\pi = e(u_1, u_2)^r \cdot m$, $\sigma = \mathtt{OTS.S}(sk, (c, \pi_1, \pi_2, \pi))$.	**Input:** pp, pk_1, pk_2, and $m \in \mathbb{G}_t$ **Output:** $\mathtt{ct} = (vk, \pi_1, \pi_2, \pi, \sigma)$, where $(vk, sk) \leftarrow \mathtt{OTS.G}(1^\lambda)$, $\pi_1 = (u_1^{vk} v_1)^r$, $\pi_2 = (u_2^{vk} v_2)^r$, $\pi = e(u_1, u_2)^r \cdot m$, $\sigma = \mathtt{OTS.S}(sk, (\pi_1, \pi_2, \pi))$.
Dec	**Input:** pp, pk_1, pk_2, ct, and x_i $(i \in \{1,2\})$ **Output:** $\perp$ if one of $\mathtt{OTS.V}(vk, (c, \pi_1, \pi_2, \pi), \sigma) = 1$, $\hat{e}(g, \pi_1) = \hat{e}(c, u_1^{vk} v_1)$, and $\hat{e}(g, \pi_2) = \hat{e}(c, u_2^{vk} v_2)$ does not hold; otherwise, output m, where $m = \pi / \hat{e}(c, u_2)^{x_1}$ or $m = \pi / \hat{e}(c, u_1)^{x_2}$.	**Input:** pp, pk_1, pk_2, ct, and (x_i, y_i) $(i \in \{1,2\})$ **Output:** $\perp$ if one of $\mathtt{OTS.V}(vk, (\pi_1, \pi_2, \pi), \sigma) = 1$, and $\hat{e}(\pi_1, u_2^{vk} v_2) = \hat{e}(u_1^{vk} v_1, \pi_2)$ does not hold; otherwise, output m, where $m = \pi / \hat{e}(\pi_1, u_2)^{x_1/(x_1 \cdot vk + y_1)}$ or $m = \pi / \hat{e}(\pi_2, u_1)^{x_2/(x_2 \cdot vk + y_2)}$.

IV. PROPOSED VARIANT OF CFZ14

In this section, we give the description of our variant of CFZ14 along with the description of the original CFZ14. In particular, we give them in Table 2, where we highlight the differences between the two schemes for easy clarification.

A. CORRECTNESS

The correctness of our variant can be obtained due to the following equations.

$$\begin{aligned}\frac{\pi}{\hat{e}(\pi_1, u_2)^{x_1/(x_1 \cdot vk + y_1)}} &= \frac{\hat{e}(u_1, u_2)^r \cdot m}{\hat{e}((u_1^{vk} v_1)^r, g^{x_2})^{\frac{x_1}{x_1 \cdot vk + y_1}}} \\ &= \frac{\hat{e}((g^{x_1}, g^{x_2})^r \cdot m}{\hat{e}(g^{x_1 \cdot vk + y_1})^r, g^{x_2})^{\frac{x_1}{x_1 \cdot vk + y_1}}} \\ &= \frac{\hat{e}(g, g)^{x_1 \cdot x_2 \cdot r} \cdot m}{\hat{e}(g, g)^{x_1 \cdot x_2 \cdot r}} \\ &= m\end{aligned}$$

and

$$\begin{aligned}\frac{\pi}{\hat{e}(\pi_2, u_1)^{x_2/(x_2 \cdot vk + y_2)}} &= \frac{\hat{e}(u_2, u_1)^r \cdot m}{\hat{e}((u_2^{vk} v_2)^r, g^{x_1})^{\frac{x_2}{x_2 \cdot vk + y_2}}} \\ &= \frac{\hat{e}((g^{x_2}, g^{x_1})^r \cdot m}{\hat{e}(g^{x_2 \cdot vk + y_2})^r, g^{x_1})^{\frac{x_2}{x_2 \cdot vk + y_2}}} \\ &= \frac{\hat{e}(g, g)^{x_2 \cdot x_1 \cdot r} \cdot m}{\hat{e}(g, g)^{x_2 \cdot x_1 \cdot r}} \\ &= m\end{aligned}$$

B. SOUNDNESS

As mentioned in [7], the key point of soundness is the public verifiability on the consistency of the ciphertext. As we can see from Table 2, the ciphertext in our variant is public-verifiable. In particular, anyone can verify whether π_1 and π_2 are respectively $(u_1^{vk} v_1)^r$ and $(u_2^{vk} v_2)^r$ through $\hat{e}(\pi_1, u_2^{vk} v_2) = \hat{e}(u_1^{vk} v_1, \pi_2)$. Furthermore, anyone can also verify whether π is corresponding to π_1 and π_2 through $\mathtt{OTS.V}(vk, (\pi_1, \pi_2, \pi)\sigma) = 1$. Once the ciphertext is well-formed, either of the users with (x_1, y_1) and (x_2, y_2) can get the same plaintext due to

$$\hat{e}(\pi_1, u_2)^{x_1/(x_1 \cdot vk + y_1)} = \hat{e}(\pi_2, u_1)^{x_2/(x_2 \cdot vk + y_2)} = \hat{e}(u_1, u_2)^r.$$

As a result, we always have that $\mathtt{Dec}(pp, pk_1, pk_2, \mathtt{ct}, (x_1, y_1)) = \mathtt{Dec}(pp, pk_1, pk_2, \mathtt{ct}, (x_2, y_2))$.

C. CCA SECURITY OF OUR VARIANT

Theorem 1: If the underlying one-time signature is strong-unforgeable and the DBSDH assumption holds, then our variant of CFZ14 described in Table 2 is a CCA-secure PK-DRE scheme.

Proof: Assume that there is an adversary $\mathcal{A}$ breaking the CCA security of our variant, we can build an algorithm $\mathcal{S}$ solving the DBSDH problem, i.e., on input the DBSDH tuple (g, h, g^a, T), the goal is to decide whether $T = \hat{e}(g, h)^{a^2}$.

- **Setup:** $\mathcal{S}$ sets $pp = (\mathbb{G}, \mathbb{G}_t, q, g, \hat{e}, \mathtt{OTS})$, $u_i = (g^a)^{\alpha_i}$, and $v_i = u_i^{-vk^*} \cdot g^{\beta_i}$, $\forall i \in \{1,2\}$, where α_i and β_i are random numbers from Z_q^*, and $(vk^*, sk^*) \leftarrow \mathtt{OTS.G}(1^\lambda)$. Note that $\mathcal{S}$ implicitly sets $x_i = a \cdot \alpha_i \bmod q$ and $y_i = a \cdot \alpha_i \cdot (-vk^*) + \beta_i \bmod q$ but without knowing their concrete values.
- **Phase 1:** The adversary $\mathcal{A}$ can issue queries to the following two oracles adaptively.
  - $\mathcal{O}_{d1}$: On input a ciphertext $\mathtt{ct} = (vk, \pi_1, \pi_2, \pi, \sigma)$ by the adversary $\mathcal{A}$, $\mathcal{S}$ first checks the validity of the ciphertext as the real execution. If it is invalid, it simply aborts; otherwise, $\mathcal{S}$ responds as follows.
    - If $vk = vk^*$, it aborts and reports fail.
    - If $vk \neq vk^*$, it responds with $\pi / \hat{e}(\delta, g^a)^{\alpha_1 \cdot \alpha_2}$, where
    $$\delta = \left(\frac{\pi_1^{\frac{1}{\beta_1}}}{\pi_2^{\frac{1}{\beta_2}}} \right)^{\frac{1}{(vk - vk^*)\left(\frac{\alpha_1}{\beta_1} - \frac{\alpha_2}{\beta_2}\right)}}.$$
  - $\mathcal{O}_{d2}$: On input a ciphertext $\mathtt{ct} = (vk, \pi_1, \pi_2, \pi, \sigma)$ by the adversary $\mathcal{A}$, $\mathcal{S}$ responds as that in $\mathcal{O}_{d1}$.

- **Challenge:** Once the adversary $\mathcal{A}$ decides to close Phase 1, it can send $\mathcal{S}$ two messages m_0 and m_1 with the same length from $\mathbb{G}_t$. $\mathcal{S}$ returns $\mathtt{ct}^* = (vk^*, \pi_1^*, \pi_2^*, \pi^*, \sigma^*)$ to the adversary $\mathcal{A}$ as the challenge ciphertext, where

$$\pi_1^* = h^{\beta_1},\ \pi_2^* = h^{\beta_2},\ \pi^* = T^{\alpha_1 \cdot \alpha_2} \cdot m_{\mathbf{b}},$$
$$\sigma^* = \mathtt{OTS.S}(sk, (\pi_1^*, \pi_2^*, \pi^*)),$$

  and $\mathbf{b}$ is a random bit chosen by $\mathcal{S}$.
- **Phase 2:** The adversary can continue to issue queries to the oracles as that in Phase 1, except for the following constraints.
  - $\mathcal{O}_{d1}$: The input ciphertext $\mathtt{ct}$ cannot be $\mathtt{ct}^*$.
  - $\mathcal{O}_{d2}$: The input ciphertext $\mathtt{ct}$ cannot be $\mathtt{ct}^*$.
- **Guess:** The adversary $\mathcal{A}$ outputs a guess $\mathbf{b}'$ on $\mathbf{b}$. If $b = b'$, then $\mathcal{S}$ decides that $T = \hat{e}(g,h)^{a^2}$; otherwise, $T \neq \hat{e}(g,h)^{a^2}$.

The above simulation works well if the decryption oracles and challenge oracle work well, which is analyzed as follows.

- **Decryption oracles.** Regarding the case of $vk = vk^*$, it means that the adversary can produce a valid signature without knowing the corresponding signing key, which is clearly against the strong unforgeability of the underlying one-time signature scheme. Hence, the case of $vk = vk^*$ happens with probability $\epsilon_{\mathtt{OTS}}$ at most, where $\epsilon_{\mathtt{OTS}}$ is the advantage that the adversary breaks the strong unforgeability of the underlying one-time signature scheme.
  Regarding the case of $vk \neq vk^*$, we just need to show that $\delta = (g^a)^r$ holds.

$$\begin{aligned}
&\left(\frac{\pi_1^{\frac{1}{\beta_1}}}{\pi_2^{\frac{1}{\beta_2}}}\right)^{\frac{1}{(vk-vk^*)\left(\frac{\alpha_1}{\beta_1}-\frac{\alpha_2}{\beta_2}\right)}} \\
&= \left(\frac{((u_1^{vk}v_1)^r)^{\frac{1}{\beta_1}}}{((u_2^{vk}v_2)^r)^{\frac{1}{\beta_2}}}\right)^{\frac{1}{(vk-vk^*)\left(\frac{\alpha_1}{\beta_1}-\frac{\alpha_2}{\beta_2}\right)}} \\
&= \left(\frac{((g^a)^{\alpha_1 \cdot vk - \alpha_1 \cdot vk^*} g^{\beta_1})^{\frac{r}{\beta_1}}}{((g^a)^{\alpha_2 \cdot vk - \alpha_2 \cdot vk^*} g^{\beta_2})^{\frac{r}{\beta_2}}}\right)^{\frac{1}{(vk-vk^*)\left(\frac{\alpha_1}{\beta_1}-\frac{\alpha_2}{\beta_2}\right)}} \\
&= \left(\frac{((g^a)^r)^{\alpha_1 \cdot (vk-vk^*)/\beta_1} \cdot g^r}{((g^a)^r)^{\alpha_2 \cdot (vk-vk^*)/\beta_2} \cdot g^r}\right)^{\frac{1}{(vk-vk^*)\left(\frac{\alpha_1}{\beta_1}-\frac{\alpha_2}{\beta_2}\right)}} \\
&= \left(((g^a)^r)^{(vk-vk^*)\left(\frac{\alpha_1}{\beta_1}-\frac{\alpha_2}{\beta_2}\right)}\right)^{\frac{1}{(vk-vk^*)\left(\frac{\alpha_1}{\beta_1}-\frac{\alpha_2}{\beta_2}\right)}} \\
&= (g^a)^r
\end{aligned}$$

- **Challenge Oracle.** If $T = \hat{e}(g,h)^{a^2}$, then the challenge ciphertext is a valid (well-formed) ciphertext due to the following equations, and the adversary can get the right guess with probability ϵ at most, where ϵ is the advantage that the adversary breaks the CCA security of our variant.

$$\begin{aligned}
\pi_1^* &= h^{\beta_1} \\
&= (u_1^{vk^*} u_1^{-vk^*})^{\log_g h} \cdot g^{\beta_1 \cdot \log_g h} \\
&= (u_1^{vk^*} u_1^{-vk^*} g^{\beta_1})^{\log_g h} \\
&= (u_1^{vk^*} v_1)^{\log_g h} \\
\pi_2^* &= h^{\beta_2} \\
&= (u_2^{vk^*} u_2^{-vk^*})^{\log_g h} \cdot g^{\beta_2 \cdot \log_g h} \\
&= (u_2^{vk^*} u_2^{-vk^*} g^{\beta_2})^{\log_g h} \\
&= (u_2^{vk^*} v_2)^{\log_g h} \\
\pi^* &= T^{\alpha_1 \cdot \alpha_2} \cdot m_{\mathbf{b}} \\
&= (\hat{e}(g,h)^{a^2})^{\alpha_1 \cdot \alpha_2} \cdot m_{\mathbf{b}} \\
&= \hat{e}(g^{a \cdot \alpha_1}, g^{a \cdot \alpha_2})^{\log_g h} \cdot m_{\mathbf{b}} \\
&= \hat{e}(u_1, u_2)^{\log_g h} \cdot m_{\mathbf{b}}
\end{aligned}$$

  If $T \neq \hat{e}(g,h)^{a^2}$, π_1^* and π_2^* have nothing to do with $m_{\mathbf{b}}$. Hence, in this case, the adversary can get the right $\mathbf{b}$ with probability 1/2.

As a result, the adversary $\mathcal{A}$ can break the CCA security of our variant with a negligible advantage. ■

Note that, in the CCA security proof of CFZ14 [7], $c = g^r$ and $\pi_1 = (u_1^{vk} v_1)$ are used to simulate the decryption oracle without using π_2. However, in our proof, we make use of π_1 and π_2 to do the decryption.

V. PERFORMANCE EVALUATION

As we mentioned before, the pairing-based schemes are usually preferable for practical use, and CFZ14 is the best one among the pairing-based schemes. Hence, we only compare the original CFZ14 and our variant in this section. The high-level comparison is given in Table 3, where T_p, $T_{e,\mathbb{G}}$, $T_{e,\mathbb{G}_t}$, $T_{me,\mathbb{G}}$, $T_{m,\mathbb{G}}$, $T_{m,\mathbb{G}_t}$, and $T_{d,\mathbb{G}_t}$ are respectively denoted as the computational cost of pairing, exponentiation in $\mathbb{G}$, exponentiation in $\mathbb{G}_t$, multi-exponentiation in $\mathbb{G}$, multiplication in $\mathbb{G}$, multiplication in $\mathbb{G}_t$, and division in $\mathbb{G}_t$, and $L_{\mathbb{G}}$, $L_{\mathbb{G}_t}$, and $L_{Z_q^*}$ are the bit length of the element in $\mathbb{G}$, $\mathbb{G}_t$, and Z_q^*, respectively.

From Table 3, we can see that our variant achieves almost the same security level as the original CFZ14, except that the CCA security in the standard model is obtained by a slightly stronger complexity assumption (DBSDH vs. DBDH).

From Table 3, we can also note that the main advantages of our variant over the original CFZ14 are the ciphertext size and encryption/decryption cost. In particular, the ciphertext size is reduced by an element in $\mathbb{G}$, the encryption cost is reduced by an exponentiation in $\mathbb{G}$, and the decryption cost is reduced by two pairings. Note that we ignore the storage and computational cost due to the underlying one-time signature scheme in Table 3, since the original CFZ14 and our variant are the same for this part. The reduction of ciphertext size and encryption cost is mainly from removing $c = g^r$, and the reduction of decryption cost is mainly from changing $\hat{e}(g,\pi_1) = \hat{e}(c, u_1^{vk} v_1)$ and $\hat{e}(g,\pi_2) = \hat{e}(c, u_2^{vk} v_2)$ to $\hat{e}(\pi_1, u_2^{vk} v_2) = \hat{e}(u_1^{vk} v_1, \pi_2)$.

TABLE 3. Comparison between the original CFZ14 and our variant.

		CFZ14	Ours
Security	Public verifiability	✓	✓
	CCA security	✓	✓
	Standard model	✓	✓
	Complexity assumption	DBDH	DBSDH
Computational Cost	KeyGen	$4T_{e,\mathbb{G}}$	$4T_{e,\mathbb{G}}$
	Enc	$T_p + T_{e,\mathbb{G}} + 2T_{me,\mathbb{G}} + T_{e,\mathbb{G}_t} + T_{m,\mathbb{G}_t}$	$T_p + 2T_{me,\mathbb{G}} + T_{e,\mathbb{G}_t} + T_{m,\mathbb{G}_t}$
	Dec	$5T_p + 2T_{e,\mathbb{G}} + 2T_{m,\mathbb{G}} + T_{e,\mathbb{G}_t} + T_{d,\mathbb{G}_t}$	$3T_p + 2T_{e,\mathbb{G}} + 2T_{m,\mathbb{G}} + T_{e,\mathbb{G}_t} + T_{d,\mathbb{G}_t}$
Storage Cost	Key pair	$2L_{\mathbb{G}} + L_{Z_q^*}$	$2L_{\mathbb{G}} + 2L_{Z_q^*}$
	Ciphertext	$3L_{\mathbb{G}} + L_{\mathbb{G}_t}$	$2L_{\mathbb{G}} + L_{\mathbb{G}_t}$

TABLE 4. Experimental results of the original CFZ14 and our variant.

	Computational cost (ms)						**Storage cost** (byte)	
	Without preprocessing			With preprocessing				
	KeyGen	Enc	Dec	KeyGen	Enc	Dec	Key pair	Ciphertext
CFZ14	42.10	59.76	52.25	23.53	8.07	24.28	276	512
Ours	42.21	50.33	40.77	23.39	6.49	18.91	296	384

To show the advantages of our variant on storage and computational cost more clearly, we also implemented the original CFZ14 and our variant by using the Java Pairing-Based Cryptography Library [18]. Both schemes are implemented with two versions. One strictly follows the description of the scheme, and the other utilizes some optimization methods, such as pre-computation and pre-processing. The underlying curve used in our experiments is Type A, and all the experiments were conducted in Windows 10 Pro running a machine with an Intel(R) Core(TM) i5-7300HQ CPU @ 2.50GHz 2.50GHz, 16.0GB RAM. All the values in Table 4 are the average values of 100 runs. Note that we still omit the cost due to the underlying one-time signature scheme. From Table 4, the encryption and decryption cost of our variant is about 75% of that of CFZ14 *at most*, no matter whether the optimization methods are applied or not. Furthermore, the ciphertext size of our variant is only 75% of CFZ14. As a result, it is fair to say that our variant is more efficient than the original CFZ14.

VI. CONCLUSION

In this paper, we have revisited a PK-DRE scheme—CFZ14, particularly its proof security. We have found that the original security proof in [7] only utilizes g^r and π_1 but without using π_2. We have also observed that the security proof can be also processed by using π_1 and π_2 with the DBSDH assumption. According to this observation, we have proposed a variant of CFZ14. The experimental results show our variant is more efficient than the original CFZ14 in terms of storage and computational cost. Our variant can also be extended to dual-receiver KEM and threshold PKE-DRE like the original CFZ14, which we omit in this paper as the underlying methods are the same.

REFERENCES

[1] T. Diament, H. K. Lee, A. D. Keromytis, and M. Yung, "The dual receiver cryptosystem and its applications," in *Proc. 11th ACM Conf. Comput. Commun. Secur.*, 2004, pp. 330–343.
[2] Y. Chen, Q. Tang, and Y. Wang, "Hierarchical integrated signature and encryption," in *ASIACRYPT*, 2021, pp. 514–543.
[3] Y. Dodis, J. Katz, A. D. Smith, and S. Walfish, "Composability and on-line deniability of authentication," in *Proc. TCC* (Lecture Notes in Computer Science), vol. 5444. Berlin, Germany: Springer, 2009, pp. 146–162.
[4] R. Zhang, G. Hanaoka, and H. Imai, "A generic construction of useful client puzzles," in *Proc. 4th Int. Symp. Inf., Comput., Commun. Secur.*, 2009, pp. 70–79.
[5] I. Damgård, D. Hofheinz, E. Kiltz, and R. Thorbek, "Public-key encryption with non-interactive opening," in *Topics in Cryptology* (Lecture Notes in Computer Science), vol. 4964. Berlin, Germany: Springer, 2008, pp. 239–255.
[6] Y. Hei, J. Liu, H. Feng, D. Li, Y. Liu, and Q. Wu, "Making MA-ABE fully accountable: A blockchain-based approach for secure digital right management," *Comput. Netw.*, vol. 191, May 2021, Art. no. 108029.
[7] S. S. M. Chow, M. K. Franklin, and H. Zhang, "Practical dual-receiver encryption - soundness, complete non-malleability, and applications," in *CT-RSA* (Lecture Notes in Computer Science), vol. 8366. Cham, Switzerland: Springer, 2014, pp. 85–105.
[8] K. Zhang, W. Chen, X. Li, J. Chen, and H. Qian, "New application of partitioning methodology: Identity-based dual receiver encryption," *Secur. Commun. Netw.*, vol. 9, no. 18, pp. 5789–5802, Dec. 2016.
[9] S. M. Patil, "DR-PRE: Dual receiver proxy re-encryption scheme," *Inf. Secur. J., Global Perspective*, vol. 29, no. 2, pp. 62–72, Mar. 2020.
[10] D. Zhang, K. Zhang, B. Li, X. Lu, H. Xue, and J. Li, "Lattice-based dual receiver encryption and more," in *ACIS* (Lecture Notes in Computer Science), vol. 10946. Cham, Switzerland: Springer, 2018, pp. 520–538.
[11] Y. Liu, D. Zhang, Y. Deng, and B. Li, "(Identity-based) dual receiver encryption from lattice-based programmable hash functions with high min-entropy," *Cybersecurity*, vol. 2, no. 1, p. 18, Dec. 2019.

[12] Y. Liu, L. Wang, X. Shen, and L. Li, "New constructions of identity-based dual receiver encryption from lattices," *Entropy*, vol. 22, no. 6, p. 599, May 2020.
[13] A. Joux, "A one round protocol for tripartite Diffie–Hellman," in *ANTS-IV* (Lecture Notes in Computer Science), vol. 1838. Berlin, Germany: Springer, 2000, pp. 385–394.
[14] B. Waters, "Efficient identity-based encryption without random oracles," in *EUROCRYPT* (Lecture Notes in Computer Science), vol. 3494. Berlin, Germany: Springer, 2005, pp. 114–127.
[15] D. Boneh, X. Boyen, and E. Goh, "Hierarchical identity based encryption with constant size ciphertext," in *EUROCRYPT* (Lecture Notes in Computer Science), vol. 3494. Berlin, Germany: Springer, 2005, pp. 440–456.
[16] F. Zhang, R. Safavi-Naini, and W. Susilo, "An efficient signature scheme from bilinear pairings and its applications," in *Proc. 7th Int. Workshop Theory Pract. Public Key Cryptogr.* (Lecture Notes in Computer Science), vol. 2947, Singapore: Springer, Mar. 2004, pp. 277–290.
[17] R. Canetti, S. Halevi, and J. Katz, "Chosen-ciphertext security from identity-based encryption," in *EUROCRYPT* (Lecture Notes in Computer Science), vol. 3027. Berlin, Germany: Springer, 2004, pp. 207–222.
[18] A. De Caro and V. Iovino, "JPBC: Java pairing based cryptography," in *Proc. IEEE Symp. Comput. Commun. (ISCC)*, Jun. 2011, pp. 850–855.

CHENGLONG GAO received the B.S. degree in biomedical science from the University of Electronic Science and Technology of China, Chengdu, Sichuan, China, in 2013, and the M.S. degree in software engineering from Lanzhou University, Lanzhou, Gansu, China, in 2017. He is currently a Senior Engineer with Shanghai Pudong Development Bank, Shanghai, China.

KAI CHEN received the B.S. degree in statistics from the Anhui University of Finance and Economics, Bengbu, Anhui, China, in 2018, and the M.Sc. degree in data science from the University of Glasgow, Glasgow, U.K., in 2019. He is a Research Assistant with the Joint Innovation Center, Zhejiang University, and Shanghai Pudong Development Bank, Hangzhou, China.

QIANG WANG received the B.S. and M.S. degrees in mathematics from Zhejiang University, China, in 1990 and 1993, respectively, where he is currently pursuing the Ph.D. degree in computer science. He is an Associate Professor with the College of Computer Science, Zhejiang University. His current research interests include artificial intelligence, blockchain, and digital image processing.

ZHIXIAN CHEN received the Ph.D. degree in communication and information systems from the Nanjing University of Posts and Telecommunications, Nanjing, China, in 2007. He was a Postdoctoral Fellow with the Department of Computer Science and Technology, Nanjing University, Nanjing, from 2008 to 2011. He is currently an Associate Professor with the Department of Information Security, Zhejiang Gongshang University, Hangzhou, China. His research interests include security and privacy in cloud computing.