I. INTRODUCTION

Public key dual-receiver encryption (PK-DRE) allows two independent recipients to recover the same plaintext from the same ciphertext. Due to the dual-receiver property, PK-DRE is quite helpful in many scenarios, such as deniable authentication, global key escrow, security puzzle, and even blockchain. To the best of our knowledge, the PK-DRE scheme proposed by Chow, Franklin, and Zhang at CT-RSA 2014 is the best one among the existing schemes in terms of security, public verifiability, and key size. In this paper, we restudy their scheme and find a new security proof that leads to a variant. The resulting PK-DRE scheme is more efficient than the original scheme in terms of ciphertext size and encryption/decryption cost, without losing the CCA security in the standard model and public verifiability.

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. To the best of our knowledge, the PK-DRE scheme proposed by Chow, Franklin, and Zhang at CT-RSA 2014 is the best one among the existing schemes in terms of security, public verifiability, and key size. In this paper, we restudy their scheme and find a new security proof that leads to a variant. The resulting PK-DRE scheme is more efficient than the original scheme in terms of ciphertext size and encryption/decryption cost, without losing the CCA security in the standard model and public verifiability.

INDEX TERMS

Public-Key Dual-Receiver Encryption, CCA Security, Standard Model

II. SUMMARY OF THE EXISTING PK-DRE SCHEMES

In this section, we summarize the existing PK-DRE schemes. There are two categories of PK-DRE schemes according to the underlying complexity assumptions, namely pairing-based [6]–[9] and lattice-based [10]–[12]. The former one is usually preferable for practical use for the following reasons.

- All the existing lattice-based schemes do not support the public verifiability, which enables anyone to check whether the two independent recipients can recover the same plaintext from the same ciphertext. 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 internet of things.

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" 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 III, we summarize the existing PK-DRE schemes. Section III reviews the definition and security model for public-key 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. [6] 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]. After ten years later, Chow, Franklin, and Zhang [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. 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.

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-unforfeignable 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.

- **Setup**: On input security parameter $\lambda$, the setup algorithm Setup outputs the public parameter $pp$. 
- **KeyGen**(pp) → $(pk_1, sk_1), (pk_2, sk_2)$: 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.
- **Enc**(pp, pk_1, pk_2, m) → c: On input the public parameter $pp$, two independent users’ public-keys $pk_1$ and $pk_2$, and a message $m$ from the plaintext space $M$, the encryption algorithm Enc outputs a ciphertext $ct$.
- **Dec**(pp, pk_1, pk_2, sk_1, ct) → m/⊥: On input the public parameter $pp$, two independent users’ public-keys $pk_1$ and $pk_2$, one private key $sk_1$ ($i \in \{1, 2\}$) of the corresponding two independent users, and a ciphertext $ct$, the decryption algorithm Dec outputs a message $m$ or a failure symbol ⊥.

1) **Correctness**
We say a PK-DRE scheme is correct if the following requirement always holds for $pp \leftarrow$ Setup($\lambda$), $(pk_1, sk_1), (pk_2, sk_2) \leftarrow$ KeyGen($pp$), and $ct \leftarrow$ Enc($pp, pk_1, pk_2, m$).

\[
\text{Dec}(pp, pk_1, pk_2, sk_1, ct) = \text{Dec}(pp, pk_1, pk_2, sk_2, ct) = m.
\]

2) **Soundness**
At CT-RSA 2014, Chow, Franklin, and Zhang [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 $c$ satisfying the following requirement only with a negligible probability.

\[
\text{Dec}(pp, pk_1, pk_2, sk_1, ct) \neq \text{Dec}(pp, pk_1, pk_2, sk_2, ct).
\]

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 $A$ and a challenger $C$.

- **Setup**: In this phase, the challenger $C$ runs Setup and 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 $C$ sends $pp$ and $(pk_1, pk_2)$ to the adversary $A$ while keeping $(sk_1, sk_2)$ secret.
- **Phase 1**: In this phase, the adversary $A$ can adaptively issue queries to the two decryption oracles.
  - $O_{d_1}$: On input a ciphertext $ct$ by the adversary $A$, the challenger $C$ returns the result of $\text{Dec}(pp, pk_1, pk_2, sk_1)$.
  - $O_{d_2}$: On input a ciphertext $ct$ by the adversary $A$, the challenger $C$ returns the result of $\text{Dec}(pp, pk_1, pk_2, sk_2)$.

- **Challenge**: Once the adversary $A$ decides to close Phase 1, it can send the challenger $C$ two messages $m_0$ and $m_1$ with the same length from the plaintext space $M$. The challenger $C$ returns $\text{Enc}(pp, pk_1, pk_2, m_b)$ to the adversary $A$ as the challenge ciphertext $ct^*$, where $b$ is a random bit chosen by the challenger $C$.
- **Phase 2**: The adversary can continue to issue queries to the oracles as that in Phase 1, except that the challenge
TABLE 1. Summary of the existing DRE schemes in terms of security, public verifiability, and key size.

|                | DLK +04 [6] | CFZ14 [7] | ZCL +17 [8] | ZZL +18 [10] | LZD +19 [11] | LWS +20 [12] | PP21 [9] |
|----------------|-------------|------------|-------------|-------------|-------------|-------------|---------|
| CCA secure in standard model | ×          | ✓          | ✓           | ✓           | ✓           | ✓           | ×       |
| Public verifiability | ×          | ✓          | ✓           | ✓           | ✓           | ✓           | ×       |
| No large key size problem | ✓          | ✓          | ×           | ×           | ×           | ×           | ✓       |

 ciphertext $ct^*$ cannot be issued to the decryption oracles.

• **Guess:** The adversary $A$ 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 $A$, the advantage of winning the CCA game $| Pr[b = b'] - 1/2 |$ is always negligible.

**B. BILINEAR GROUPS**

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

The security proof of our variant is based on the DBSDH (decisional bilinear square Diffie-Hellman) assumption in the bilinear groups [15], which is stated as follows. Given $g, h, g^a \in G$ and $T \in G_t$, 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-WBDH* assumption proposed in [16].

The security proof of the original CFZ14 is based on the DBDH (decisional bilinear Diffie-Hellman) assumption in the bilinear groups. In particular, given $g, g^a, g^b, g^c \in G$ and $T \in G_t$, 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 (computationally bilinear square Diffie-Hellman) assumption and CBDH (computational bilinear Diffie-Hellman) assumption are equivalent [15].

**C. ONE-TIME SIGNATURE**

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

• $OTS.G(\lambda^*) \rightarrow (vk, sk)$. On input the security parameter $\lambda$, $OTS.G$ outputs a key pair $(vk, sk)$.

• $OTS.S(sk, m) \rightarrow \sigma$. On input a signing key $sk$ and a message $m$, $OTS.S$ outputs a signature $\sigma$ on $m$.

• $OTS.S.(vk, m, \sigma) \rightarrow 1$ or 0. On input a verifying key $vk$, a message $m$ and a signature $\sigma$, $OTS.V$ outputs 1 if $\sigma$ is a signature of $m$ under $vk$; otherwise, it outputs 0.

**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 $(vk, sk) \leftarrow OTS.G(\lambda^*)$, both the following conditions are satisfied:

$$OTS.V(vk, m, OTS.S(sk, m)) = 1,$$

and

$$OTS.V(vk, m, OTS.S(sk, m')) = 0.$$

**Strong Unforgeability.** The strong unforgeability of digital signature states that the adversary cannot output a 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].

**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.

$$\frac{\pi}{\hat{e}(\pi_1, u_2)^{x_1/(x_1 \cdot v k + y_1)}} = \frac{\hat{e}(u_1, u_2)^x \cdot m}{\hat{e}((u_1^2 v k)^{x_1}, g^{x_2})^{\frac{x_1}{x_1 \cdot v k + y_1}}},$$

$$\frac{\pi}{\hat{e}(\pi_2, u_1)^{x_2/(x_2 \cdot v k + y_2)}} = \frac{\hat{e}(u_2, u_1)^x \cdot m}{\hat{e}((u_2^2 v k)^{x_2}, g^{x_1})^{\frac{x_2}{x_2 \cdot v k + y_2}}},$$

and

$$\frac{\pi}{\hat{e}(\pi_1, u_2)^{x_1/(x_1 \cdot v k + y_1)}} = \frac{\hat{e}(g^{x_1}, g^{x_2})^{\frac{x_1}{x_1 \cdot v k + y_1}} \cdot m}{\hat{e}(g, g)^{x_1 \cdot x_2 \cdot \tau}},$$

$$\frac{\pi}{\hat{e}(\pi_2, u_1)^{x_2/(x_2 \cdot v k + y_2)}} = \frac{\hat{e}(g^{x_2}, g^{x_1})^{\frac{x_2}{x_2 \cdot v k + y_2}} \cdot m}{\hat{e}(g, g)^{x_2 \cdot x_1 \cdot \tau}}.$$
TABLE 2. The description of the original CF214 and our variant

|          | CF214                                      | Ours                                      |
|----------|--------------------------------------------|--------------------------------------------|
| Setup    | Input: $I^\Lambda$                         | Identical to that in CF214.                |
|          | Output: $pp = (G, G_t, q, g, \hat{e}, \text{OTS})$, where $(G, G_t, \hat{e}, q, g)$ are obtained from $B_{\text{Setup}}(\lambda)$, and OTS is a strong-unforgeable one-time signature scheme. |                                            |
| KeyGen   | Input: $pp$                                 |                                            |
|          | Output: $pk_i = (u_i, v_i), sk_i = x_i$ for all $i \in \{1, 2\}$, where $x_i$ are random numbers from $Z_q^*$, and $v_i = g^{x_i}$, and $u_i = g^{x_i}$ and $v_i = g^{x_i}$. |                                            |
| Enc      | Input: $pp, pk_1, pk_2, m \in \mathcal{G}_t$ |                                            |
|          | Output: $ct = \text{OTS} \cdot (vk, sk, \pi_1, \pi_2, \pi, \sigma)$, where $(vk, sk) \leftarrow \text{OTS} \cdot S(\lambda), \pi_1 = (u_1^{\pi_1} v_1)^{\pi}, \pi_2 = (u_2^{\pi_2} v_2)^{\pi}$ | $\pi = e(v_1, u_2)^\gamma \cdot m, \sigma = \text{OTS} \cdot \text{S}(sk, \pi, \pi_1, \pi_2)$. |
| Dec      | Input: $pp, pk_1, pk_2, ct$, and $x_i$ (i \in \{1,2\}) |                                            |
|          | Output: $\bot$ if one of $\text{OTS} \cdot V(vk, \pi_1, \pi_2, \pi, \sigma) \neq 1$, $\hat{e}(g, \pi_1) = \hat{e}(c, u_1^{\pi_1} v_1)$, and $\hat{e}(g, \pi_2) = \hat{e}(c, u_2^{\pi_2} v_2)$ does not hold; otherwise, output $m$, where $m = \pi/\hat{e}(c, u_1^{\pi_1} v_1)$ or $m = \pi/\hat{e}(c, u_2^{\pi_2} v_2)$ | $\hat{e}(\pi_1, u_2)^{x_1/(x_1 \cdot v_1 + y_1)} = \hat{e}(\pi_2, u_1^{x_2/\cdot v_2 + y_2}) = \hat{u}(u_1, u_2)^\gamma$. |

B. SOUNDKNESS

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 is the ciphertext in our variant is public-verifiable. In particular, anyone can verify whether $\pi_1$ and $\pi_2$ are respectively $(r, u_1^{\pi_1} v_1)$ and $(r, u_2^{\pi_2} v_2)$ through $\hat{e}(\pi_1, u_2^{\pi_2} v_2) = \hat{e}(u_1^{\pi_1} v_1, \pi_2)$. Furthermore, anyone can also verify whether $\pi$ is corresponding to $\pi_1$ and $\pi_2$ through $\text{OTS} \cdot V(vk, \pi_1, \pi_2, \pi, \sigma) = 1$. 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 $\hat{e}(\pi_1, u_2)^{x_1,(x_1 \cdot v_1 + y_1)} = \hat{e}(\pi_2, u_1^{x_2/\cdot v_2 + y_2}) = \hat{u}(u_1, u_2)^\gamma$.

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

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 CF214 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 $pp = (G, G_t, q, g, \hat{e}, \text{OTS})$, $u_i = (g^a)^{\alpha_i}$, and $u_i = u_1^{\alpha_i} \cdot g^{\beta_i}$, $\forall i \in \{1, 2\}$, where $\alpha_i$ and $\beta_i$ are random numbers from $Z_q^*$, and $(vk^*, sk^*) \leftarrow \text{OTS} \cdot S(\lambda)$. Note that $\mathcal{S}$ implicitly sets $x_i = a \cdot \alpha_i \mod q$ and $y_i = a \cdot \alpha_i \cdot (\cdot v_1 + \beta_i \mod q$ but without knowing their concrete values.
- **Phase 1:** The adversary $\mathcal{A}$ can issue queries to the following two oracles adaptively.
  - $\mathcal{O}_1$: On input a ciphertext $ct = (vk, \pi_1, \pi_2, \pi, \sigma)$ 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 $\pi/\hat{e}(\delta, g^{a^2})^{\alpha_1 \cdot \alpha_2}$, where
      $\delta = \frac{(v_1^{\pi_1} v_2^{\pi_2})}{(v_1^{\pi_1} v_2^{\pi_2})}$.
      
  - $\mathcal{O}_2$: On input a ciphertext $ct = (vk, \pi_1, \pi_2, \pi, \sigma)$ by the adversary $\mathcal{A}$, $\mathcal{S}$ responds as that in $\mathcal{O}_1$.
    - **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 $\mathcal{G}_t$, $\mathcal{S}$ returns $ct = (vk^*, \pi_1^*, \pi_2^*, \pi^*, \sigma^*)$ to the adversary $\mathcal{A}$ as the challenge ciphertext, where
      $\pi_1^* = h^{\beta_1}, \pi_2^* = h^{\beta_2}, \sigma^* = T^{\alpha_1 \cdot \alpha_2} \cdot m_1, \sigma^* = \text{OTS} \cdot \text{S}(sk, (\pi_1^*, \pi_2^*, \pi^*))$, and $b$ 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.
    - $\mathcal{O}_1$: The input ciphertext $ct$ cannot be $ct^*$. 
    - $\mathcal{O}_2$: The input ciphertext $ct$ cannot be $ct^*$.
  - **Guess:** The adversary $\mathcal{A}$ outputs a guess $b'$ on $b$. 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 $\epsilon_{\text{OTS}}$ at most, where $\epsilon_{\text{OTS}}$ is the advantage that the adversary breaks the strong unforgeability of the underlying one-time signature scheme.
Regarding the case of \( v^k \neq v^k \), we just need to show that \( \delta = (g^a)^r \) holds.

\[
\begin{align*}
\left( \frac{1}{\pi_1} \right)^{\frac{\delta}{\beta}} &= \left( \frac{1}{\pi_2} \right)^{\frac{\delta}{\beta}} \\
\left( \left( u_1^{v_1} v_1 \right)^{\frac{\delta}{\beta}} \right) &= \left( \left( u_2^{v_2} v_2 \right)^{\frac{\delta}{\beta}} \right) \\
\left( \frac{\delta}{\beta} \right) &= \left( \frac{\delta}{\beta} \right) \\
\end{align*}
\]

\[
\begin{align*}
\left( \frac{1}{\pi_1} \right)^{\frac{\delta}{\beta}} &= \left( \frac{1}{\pi_2} \right)^{\frac{\delta}{\beta}} \\
\left( \left( u_1^{v_1} v_1 \right)^{\frac{\delta}{\beta}} \right) &= \left( \left( u_2^{v_2} v_2 \right)^{\frac{\delta}{\beta}} \right) \\
\left( \frac{\delta}{\beta} \right) &= \left( \frac{\delta}{\beta} \right) \\
\end{align*}
\]

\[
\begin{align*}
\left( \frac{1}{\pi_1} \right)^{\frac{\delta}{\beta}} &= \left( \frac{1}{\pi_2} \right)^{\frac{\delta}{\beta}} \\
\left( \left( u_1^{v_1} v_1 \right)^{\frac{\delta}{\beta}} \right) &= \left( \left( u_2^{v_2} v_2 \right)^{\frac{\delta}{\beta}} \right) \\
\left( \frac{\delta}{\beta} \right) &= \left( \frac{\delta}{\beta} \right) \\
\end{align*}
\]

V. PERFORMANCE EVALUATION

We give the comparison between the original CFZ14 and our variant in Table 3, where \( T_p, T_e, T_{c,g}, T_{c,e}, T_{m,c}, T_{m,g}, T_{m,c,g} \), and \( T_{d,g} \) 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 \( \mathbb{G}_t \), respectively. \( L_G, L_{G_t}, \) and \( L_{Z_2} \) 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 slight 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.

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 found that the original security proof in [7] only utilizes \( g^a \) and \( \pi_1 \) but without using \( \pi_2 \). We also observed that the security proof can be also processed by using \( \pi_1 \) and \( \pi_2 \) with the DBSDH assumption. According to this observation, we 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.
### TABLE 3. Comparison between the original CFZ14 and our variant

| Security      | CFZ14 | Ours |
|---------------|-------|------|
| Public verifiability | ✓     | ✓    |
| CCA security  | ✓     | ✓    |
| Standard model| ✓     | ✓    |
| Complexity assumption | DBSDH | DBSDH |

| Computational Cost | CFZ14 | Ours |
|--------------------|-------|------|
| KeyGen             | $4T_{e,G}$ | $4T_{e,G}$ |
| Enc                | $T_p + T_{e,G} + 2T_{me,G} + T_{e,G_1} + T_{m,G_1}$ | $T_p + 2T_{me,G} + T_{e,G_4} + T_{m,G_4}$ |
| Dec                | $5T_p + 2T_{e,G_4} + 2T_{m,G} + T_{e,G_1} + T_{d,G_1}$ | $3T_p + 2T_{e,G_4} + 2T_{m,G} + T_{e,G_4} + T_{d,G_4}$ |

| Storage Cost | CFZ14 | Ours |
|--------------|-------|------|
| Key pair     | $2L_G + L_{Z_q}$ | $2L_G + 2L_{Z_q}$ |
| Ciphertext   | $3L_G + L_{G_1}$ | $2L_G + L_{G_1}$ |

### 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        |

### REFERENCES

[1] Y. Dodis, J. Katz, A. D. Smith, and S. Walfish, “Composability and online deniability of authentication,” in TCC 2009, ser. Lecture Notes in Computer Science, vol. 5444. Springer.

[2] R. Zhang, G. Hanaoka, and H. Imai, “A generic construction of useful client puzzles,” in ASIACCS 2009. ACM, 2009, pp. 70–79.

[3] I. Damgård, D. Hofheinz, E. Kiltz, and R. Thorbek, “Public-key encryption with non-interactive opening,” in CT-RSA 2008, ser. Lecture Notes in Computer Science, vol. 4964. Springer, 2008, pp. 239–255.

[4] Y. Chen, Q. Tang, and Y. Wang, “Hierarchical integrated signature and encryption,” in ASIACRYPT 2021.

[5] 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,” Computer Networks, vol. 191, p. 108029, 2021.

[6] T. Diamant, H. K. Lee, A. D. Keromytis, and M. Yung, “The dual receiver cryptosystem and its applications,” in ACM CCS 2004. ACM, 2004, pp. 330–343.

[7] S. S. M. Chow, M. K. Franklin, and H. Zhang, “Practical dual-receiver encryption - soundness, complete non-malleability, and applications,” in CT-RSA 2014, ser. Lecture Notes in Computer Science, vol. 8366. 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,” Security and Communication Networks, vol. 9, no. 18, pp. 5789–5802, 2016.

[9] S. M. Patil and B. R. Purushothama, “DR-PRE: dual receiver proxy re-encryption scheme,” Information Security Journal: A Global Perspective, vol. 29, no. 2, pp. 62–72, 2020.

[10] D. Zhang, K. Zhang, B. Li, X. Lu, H. Xue, and J. Li, “Lattice-based dual receiver encryption and more,” in ACISP 2018, ser. Lecture Notes in Computer Science, vol. 10946. 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, 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, 2020.

[13] A. Jouks, “A one round protocol for tripartite diffie-hellman,” in ANTS-IV, ser. Lecture Notes in Computer Science, vol. 1838. Springer, 2000, pp. 385–394.

[14] B. Waters, “Efficient identity-based encryption without random oracles,” in EUROCRYPT 2005, ser. Lecture Notes in Computer Science, vol. 3494. Springer, 2005, pp. 114–127.

[15] F. Zhang, R. Safavi-Naini, and W. Susilo, “An efficient signature scheme from bilinear pairings and its applications,” in Public Key Cryptography - PKC 2004, 7th International Workshop on Theory and Practice in Public Key Cryptography, Singapore, March 1-4, 2004, ser. Lecture Notes in Computer Science, vol. 2947. Springer, 2004, pp. 277–290.

[16] D. Boneh, X. Boyen, and E. Goh, “Hierarchical identity based encryption with constant size ciphertext,” in EUROCRYPT 2005, ser. Lecture Notes in Computer Science, vol. 3494. Springer, 2005, pp. 440–456.

[17] R. Canetti, S. Halevi, and J. Katz, “Chosen-ciphertext security from identity-based encryption,” in EUROCRYPT 2004, ser. Lecture Notes in Computer Science, vol. 3027. Springer, 2004, pp. 207–222.

[18] A. De Caro and V. Iovino, “jpbc: Java pairing based cryptography,” in ISCC 2011, Kerkvliet, Corfu, Greece, June 28 - July 1, 2011, pp. 850–855.

CHENGLONG GAO received the B.S. degree in biomedical from University of Electronic Science and Technology of China, Chengdu, Sichuan Province, China, in 2013 and the M.S. degree in software engineering from Lanzhou University, Lanzhou, Gansu Province, China, in 2017. He is currently a senior engineer in Shanghai Pudong Development Bank, Shanghai, China.
KAI CHEN received the B.S. degree in statistics from Anhui University of Finance and Economics, Bengbu, Anhui Province, China, in 2018 and the M.Sc. degree in data science from University of Glasgow, Glasgow, UK, in 2019. He is a Researcher Assistant with the Joint Innovation Center of Zhejiang University and Shanghai Pudong Development Bank, Hangzhou, China.

QIANG WANG received his BS and MS degrees in mathematics from Zhejiang University, China in 1990 and 1993, respectively. He has a PhD in computer science from Zhejiang University. He is an associate professor in the College of Computer Science at Zhejiang University, China. His current research interests include artificial intelligence, blockchain, and digital image processing.

ZHIXIAN CHEN received the Ph.D. degree in communication and information system from 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, China, 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.