# Adaptively Secure Functional Encryption for Finitite Languages from DLIN Assumption

Tapas Pandit
Stat-Math Unit
Indian Statistical Institute, Kolkata
tapasgmmath@gmail.com

Rana Barua
Stat-Math Unit
Indian Statistical Institute, Kolkata
rana@isical.ac.in

**Abstract**

In this paper, we present Functional Encryption (FE) schemes for finite languages from standard static assumption, viz., *Decisional Linear* (DLIN) assumption. These finite languages are described by Deterministic Finite Automatas (DFAs). Our first scheme is ciphertext-policy functional encryption (CP-FE), where a key $\mathcal{SK}_w$ is labeled with a string $w$ over a fixed alphabet $\Sigma$ and a ciphertext $\mathcal{C}_{\mathcal{M}}$ is associated with a DFA $\mathcal{M}$ over the same alphabet $\Sigma$. The key $\mathcal{SK}_w$ can extract the message from the ciphertext $\mathcal{C}_{\mathcal{M}}$ if the DFA $\mathcal{M}$ accepts the string $w$. This CP-FE scheme is constructed based on attribute-based encryption (ABE) structure of Okamoto-Takashima in Asiacrypt, 2012. To achieve the adaptive security, we put bounds on number of occurrences of any symbol in a string and in the set of transition tuples of a DFA. Due to this restriction, the size of key space (where the keys are indexed with strings) is reduced to finite. Hence, the functional scope of any DFA in our system can capture only finite language. Similarly, we obtain our second adaptively secure FE scheme in key-policy flavor from DLIN assumption. Both the schemes are shown to be secure in the standard model.

## 1 Introduction

Functional Encryption provides a smart way of setting a fine-grained share of a secret among many users in a distributed system. In this encryption, message (resp. user's key) is encoded with an expressive parameter $\Phi$ (called policy) and user's key (resp. message) is encoded with a less expressive parameter $\Psi$ (called attributes). The decryption will be legitimate if relation $R(\Phi, \Psi)$ holds. There are two types of FE, viz, Ciphertext-Policy Functional Encryption (CP-FE) [BSW07, LOS$^+$10, OT10, Wat11, LW12], where message is associated with a policy and key is encoded with a set of attributes and Key-Policy Functional Encryption (KP-FE) [GPSW06, OSW07, LOS$^+$10, OT10, ALdP11], where the role of policy and set of attributes are interchanged.

FEs are partitioned again into two ways: FE with "public index" [LW12, GPSW06, Wat11, OSW07, LOS$^+$10, OT10, ALdP11], where message is hidden but not the function and the other is FE "without public index" [KSW08, SW08, OT09, OT11, OT12a], where the ciphertext conceals both the plaintext and policy. Attribute-Based Encryptions (ABE) form one of the larger class of the former category. In ABE, the policies (access structures) are represented by access trees, span programs or the sets of minimal sets. Other FEs that exist in the literature are spatial-encryption [Ham11, BH08], inner-product encryption [OT12a, KSW08, OT12b], hidden-vector encryption [BW07, IP08], identity-based broadcast encryption [BH08, SF07].

Sahai and Waters [SW05] introduced the concept of ABE, through the construction of Fuzzy IBE, in which an identity was viewed as a set of attributes. Although, the IBE is a special case of ABE, where policy is equality of IDs, yet the Fuzzy IBE was the first step (in the sense of non-trivial functionalities) towards exploration of many FE schemes.

Later, Boneh et al. [BSW11] formalized the functional encryption to capture all the FEs under the same template: The functionality $f$ over $(K \times X)$ is defined in [BSW11] as function $f : K \times X \to \{0,1\}^*$, where $K$ is the key space

and $X$ is the message space. The message space may be of the form $X = (M \times I)$, where $M$ is the payload space and $I$ is the policy space. Let $c = enc(PP, x = (m, \Phi))$ be the encryption of the $(m, \Phi)$, then secret key $\mathcal{SK}_\Psi$, for $\Psi \in K$ can evaluate $f(\Psi, x = (m, \Phi))$ as $dec(PP, c, \mathcal{SK}_\Psi)$. For all aforementioned FEs (or predicate encryptions), functionality $f : K \times X \to \{0,1\}^*$ is defined as $f(\Psi, x = (m, \Phi)) = m$ if $R(\Phi, \Psi)$ holds and else it is defined as $f(\Psi, x = (m, \Phi)) = (len(m), \Phi)$ for "public index" and $f(\Psi, x = (m, \Phi)) = len(m)$ for "without public index". Therefore, all the aforesaid FEs are sub-class of formalized FE.

Till date, there are very few adaptively secure FE schemes [LW12, OT10, LOS$^+$10, OT12b] without random oracles, where the policy is more expressive and fine-grained and surprisingly, most of them belong to the ABE family. However, the existing ABE (FE) systems support only bounded policies, where the policies can give access to a bounded number of users, i.e., if the formula is defined over fixed $n$ variables, then it supports at most exponential number of users.

Recently, Waters [Wat12] proposed a Key-policy functional encryption for regular languages over an alphabet. Since, the size of a regular language may be unbounded, their system can support unbounded access control over the encrypted messages. The KP-FE scheme of [Wat12] was shown to be selectively secure under a non-static assumption, the decisional $\ell$-Expanded BDHE assumption.

Very recently, S.C.Ramanna [Ram13] proposed an adaptively secure DFA-based FE over an alphabet in the standard model. To capture the adaptive security, they first obtained the basic FE construction by imposing two restrictions, viz., the DFA (policy) must contain at most a single transition corresponding to each symbol and the string must contain at most a single occurrence of each symbol. In their full construction, these restriction are relaxed to support a large class of regular language but they put bounds on number of occurrences of any symbol in a string and in the set of transition tuples of a DFA. This emphasizes that their system supports nothing but the finite languages over a fixed alphabet. However, their system is proven secure under non-standard assumptions, Decisional SubGroup (DSG) assumptions over composite order bilinear groups.

## 1.1 Our Contribution

We propose an adaptively secure CP-FE scheme for finite language over an alphabet $\Sigma$. The security of the proposed scheme relies on standard, static assumption, DLIN in the standard model. Our construction follows the ABE construction of [OT12b] based on Dual Pairing Vector Spaces (DPVS) technique. In this construction, the ciphertext components are generated by the bases of a DPVS and the keys are obtained by it's dual. Let $\mathcal{M} = (Q, \Sigma, q_0, F, \delta)$ be a deterministic finite automaton for which the ciphertext components will be generated. For each state $q_x \in Q$, random $d_x$ is chosen from $\mathbb{F}_q$. There will be two initial components, viz, $C_m$, the masking of the message $m$ using a random exponent $\xi$ and $\vec{C}_0$, the encoding of initial state $q_0$ and it is connected with $C_m$ via the random $\xi$. For each transition $t = (q_x, q_y, \sigma_h)$, there will be three ciphertext components, i.e., $\vec{C}_{t,1}, \vec{C}_{t,2}$ and $\vec{C}_{t,3}$ which encode respectively the target state $q_y$ and transition $t$, the source state $q_x$ and the transition $t$, and the transition $t$. The common symbol $\sigma_h$ is embedded in all the above three components. For each final state $q_z \in F$, the ciphertext component $\vec{C}_{z,4}$ represents the encoding of $q_z$.

Let $\mathcal{SK}_w$ denote the secret key of a user for a string $w = w_1 \cdots w_\ell$ of length $\ell$ over the alphabet $\Sigma$. Let $r_0, r_1, \ldots, r_\ell$ be chosen at random from $\mathbb{F}_q$. The key $\mathcal{SK}_w$ consists of the following components: One initial key component $\vec{K}^*_0$, the encoding of $r_0$. For each $i \in \{1, \ldots, \ell\}$, there are three key components, $\vec{K}^*_{i,1}$, $\vec{K}^*_{i,2}$ and $\vec{K}^*_{i,3}$, wherein the values $r_i$, $r_{i-1}$ and $r_i + r_{i-1}$ are embedded respectively. All these three components are related via a common $i^{th}$ symbol $w_i$. There is a final component $\vec{K}^*_{\ell+1,4}$ to embed the random $r_\ell$. For all $i \in \{1, \ldots, \ell\}$, $j \in \{1, 2, 3\}$, the components $\vec{K}^*_{i,j}$ are connected chain-wise via the random values $r_0 \ldots, r_\ell$.

If the pairing between $\vec{C}_0$ and $\vec{K}^*_0$ is computed, we have $A_0 = g_T^{r_0 d_0 + \xi}$, where $g_T$ is an element from target group of the pairing groups and since, $C_m = m.g_T^\xi$, we have to compute $g_T^\xi$ from $A_0$ using the others key and ciphertext components to unmask the message m. If the $i^{th}$ symbol $w_i$ of $w$ matches[1] with a transition $t = (q_x, q_y, \sigma_h)$, then we have $e(\vec{C}_{t,j}, \vec{K}^*_{i,j}) = g_T^{r_i(s_t + d_y)}$ for $j = 1$. Similarly, for $j = 2$ and $j = 3$, we have respectively $g_T^{-r_{i-1}(-s_t + d_x)}$ and $g_T^{(-r_i - r_{i-1})s_t}$. If we multiply last three terms, we have a coupling value of the form $g_T^{r_i d_y - r_{i-1} d_x}$. Now, if the DFA

[1]It means the $i^{th}$ symbol $w_i$ is equal to the symbol $\sigma_h$ that appears in the transition $t$

$\mathcal{M}$ accepts the string $w$, then there exist a sequence of $\ell+1$ states $q_{x_0}, q_{x_1}, q_{x_2}, \ldots, q_{x_\ell}$ and transitions $t_1, \ldots, t_\ell$, where $x_0 = 0$ and $q_{x_\ell} \in F$ and for $i = 1, 2, \ldots, \ell$, we have $t_i = (q_{x_{i-1}}, q_{x_i}, \sigma)$ with $w_i = \sigma$. The first coupling value through this sequence, is computed as $A_1 = g_T^{r_1 d_{x_1} - r_0 d_0}$. Iteratively, the $i^{th}$ coupling value is obtained as $A_i = A_{i-1}.g_T^{r_i d_{x_i} - r_{i-1} d_{x_{i-1}}} = g_T^{r_{i-1} d_{x_{i-1}} - r_0 d_0}.g_T^{r_i d_{x_i} - r_{i-1} d_{x_{i-1}}} = g_T^{r_i d_{x_i} - r_0 d_0}$. Similarly, the $\ell^{th}$ coupling value through this path, is calculated as $A_\ell = g_T^{r_\ell d_{x_\ell} - r_0 d_0}$. Then, we compute the final value as $A_{\ell+1} = A_\ell.e(\vec{C}_{x_\ell,4}, \vec{K}^*_{\ell+1,4}) = g_T^{r_\ell d_{x_\ell} - r_0 d_0}.g_T^{-r_\ell d_{x_\ell}} = g_T^{-r_0 d_0}$. Thus, the message can be extracted from $C_m$ using $A_0$ and $A_{\ell+1}$. Our KP-FE scheme is found in Appendix C.

**Limitation:** Most of the adaptively secure FE schemes [LW12, OT10, LOS$^+$10, OT12b] supporting wide functionalities are proven by putting a burden on the functionalities. These restrictions are required to pass through some crucial arguments to the sequence of hybrid games in dual system proof methodology [Wat09]. For example, in [OT10, LOS$^+$10, OT12b], an adaptively secure basic scheme is first constructed by imposing a restriction that the attributes must not repeat in the span programs. Then this basis scheme is lifted to a full adaptively secure scheme without the above restriction, but it imposes another restriction on degree of the span programs, i.e, maximum number of times an attribute can repeat in the span programs, are bounded by a pre-fixed threshold value. Similarly, we first impose some restrictions on the DFAs and the strings to achieve a basic adaptively secure scheme under a standard static assumption. The imputed restrictions are: for each symbol, there is at most a single transition and the strings for key can have at most a single occurrence of symbol. Likewise, the above restrictions are relaxed but an additional burden is put on the DFAs and the strings for keys to obtain full adaptively secure scheme for DFAs under the same assumption. If $t_{max}$ and $w_{max}$ are the bounds on maximum number of times a symbol may repeat in the transitions of a DFA and string respectively, then the size of the new alphabet $\Sigma_b$ will be $t_{max}w_{max}$ times the size of old alphabet $\Sigma$. Indeed, for each symbol $\sigma \in \Sigma$, we have a matrix $W_\sigma$ with order $t_{max} \times w_{max}$ of new symbols for $\Sigma_b$. Suppose $\mathcal{M}$ and $w$ are respectively the DFA (to be embedded in ciphertext) and $\ell$-length string (for key) over the alphabet $\Sigma$ without any restrictions on both the symbols and the transitions. Then, this DFA $\mathcal{M}$ and string $w$ are converted to DFA $\mathcal{N}$ and a matrix $W$ of order $t_{max} \times \ell$ over the new alphabet $\Sigma_b$. If the DFA $\mathcal{M}$ accepts $w$, there is exactly one string $w_b$, comprising exactly one symbol from each column of the matrix $W$ such that the DFA $\mathcal{N}$ accepts $w_b$. And if DFA $\mathcal{M}$ rejects the string $w$, then, for all possible strings $w_b$, by choosing exactly one symbol from each column of $W$, the DFA $\mathcal{N}$ rejects the strings $w_b$.

### 1.2 Related Work

From opening [SW05], many FE schemes [KSW08, SW08, OT09, Wat11, LW12, OT10, LOS$^+$10, OT12b, ALdP11] have been proposed on focusing several issues. But there are very few schemes [LW12, OT10, LOS$^+$10, OT12b] supporting wide functionalities and capture adaptive security in the standard model at the same time. The CP-ABE and KP-ABE schemes in [OT10, LOS$^+$10, OT12b], are proven adaptively secure under static assumption in the standard model but the policies are restricted by imposing a bound on the degree. In [Ram13], similar kinds of restrictions are imposed on DFAs and strings to get the adaptive security from static, non-standard assumptions over composite order bilinear groups. The above bounds diminish the performance of the scheme by increasing either key size or ciphertext size by a factor or both. In contrast, there is no such imposition in the scheme of [LW12] but the adaptive security has to rely on non-static assumption and some other assumptions.

## 2 Preliminaries

Basic notation, definitions and hardness assumptions are provided in this section. For definition and security model of CP-FE for DFAs, refer to Appendix A.

**Deterministic Finite Automaton** A deterministic finite automaton (DFA) $\mathcal{M}$ is a quintuple $(Q, \Sigma, q_0, F, \delta)$, where $Q$ is a finite set of states, $\Sigma$ is a set of symbols, called alphabet, $q_0 \in Q$ is called the start state, $F \subseteq Q$ is called the set of final states and the function $\sigma : Q \times \Sigma \to Q$ is called transition function.

**Notation** Let $\mathcal{T}$ denote the set of all transitions $t = (q_x, q_y, \sigma)$ of a DFA $\mathcal{M} = (Q, \Sigma, q_0, F, \delta)$, where $t = (q_x, q_y, \sigma)$ carries meaning of $\delta(q_x, \sigma) = q_y$. $\mathcal{L}(\mathcal{M})$ stands for the language recognized by the DFA $\mathcal{M}$. The notation $[\ell]$ stands for the set $\{i \in \mathbb{N} : 1 \leq i \leq \ell\}$. For a set $X$, $x \xleftarrow{\mathrm{R}} X$ denotes that $x$ is randomly picked from $X$ according to the distribution, $R$. Likewise, $x \xleftarrow{\mathrm{U}} X$ indicates $x$ is uniformly selected from $X$. For a basis $\mathbb{B} := (\vec{b}_1, \ldots, \vec{b}_N)$, $(x_1, \ldots, x_N)\mathbb{B}$ represents $\sum_{i=1}^{N} x_i \vec{b}_i$. The vector $\vec{e}_1$ and $\vec{e}_2$ stand for $(1, 0)$ and $(0, 1)$ respectively. Let $\mathbb{F}_q^{\times}$ stand for $\mathbb{F}_q \setminus \{0\}$

## 2.1 Dual Pairing Vector Spaces

A prime order bilinear pairing groups are a tuple $(q, \mathbb{G}, \mathbb{G}_T, e)$, where $q$ is prime, $\mathbb{G}$ and $\mathbb{G}_T$ are cyclic groups of prime order $q$ and $e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$ is a efficiently computable map such that

1. (Bilinear) $\forall P_1, P_2 \in \mathbb{G}, a, b \in \mathbb{F}_q, e(aP_1, bP_2) = e(P_1, P_2)^{ab}$,
2. (Non-degenerate) $\exists P \in \mathbb{G}$ such that $e(P, P)$ has order $q$ in $\mathbb{G}_T$.

Let $\mathcal{G}_{bpg}$ denote an algorithm that takes $\kappa$ as input parameter and generates a description of a prime order bilinear pairing $param_{\mathbb{G}} := (q, \mathbb{G}, \mathbb{G}_T, P, e)$.

**Definition 2.1** ([OT12b])**.** Dual Pairing Vector Spaces (DPVS)$(q, \mathbb{V}, \mathbb{G}_T, \mathbb{A}, e)$ is defined as a direct product over symmetric prime-order pairing groups $(q, \mathbb{G}, \mathbb{G}_T, P, e)$, where

- $\mathbb{V} := \overbrace{\mathbb{G} \times \ldots \times \mathbb{G}}^{N}$ is a $N$-dimensional vector space over $\mathbb{F}_q$
- $\mathbb{G}_T$ is a cyclic group of order $q$ (as in the pairing)
- $\mathbb{A} := (\vec{a}_1, \ldots, \vec{a}_N)$ is the canonical basis of $\mathbb{V}$ with $\vec{a}_i = (\overbrace{0, \ldots, 0}^{i-1}, P, \overbrace{0, \ldots, 0}^{N-i})$
- $e : \mathbb{V} \times \mathbb{V} \to \mathbb{G}_T$ is a bilinear map defined by $e(\vec{x}, \vec{y}) = \prod_{i=1}^{N} e(x_i, y_i)$, where $\vec{x} := (x_1, \ldots, x_N) \in \mathbb{V}$ and $\vec{y} := (y_1, \ldots, y_N) \in \mathbb{V}$

Let $\mathcal{G}_{dpvs}$ denote an algorithm that takes $\kappa$, a dimension $N$ and $param_{\mathbb{G}}$ as input and outputs a description of a dual pairing vector spaces $param_{\mathbb{V}} := (q, \mathbb{V}, \mathbb{G}_T, \mathbb{A}, e)$.

To construct our encryption system based on DPVS, we need dual orthogonal bases for a DPVS. Let $\mathcal{G}_{ob}$ denote the dual orthogonal basis generator.

$\mathcal{G}_{ob}(\kappa, N_0, N_1, N_2, N_3, N_4)$:
$param_{\mathbb{G}} := (q, \mathbb{G}, \mathbb{G}_T, P, e) \longleftarrow \mathcal{G}_{bpg}(\kappa)$, $\psi \xleftarrow{\mathrm{U}} \mathbb{F}_q^{\times}$,
For $t = 0, \ldots, 4$, $param_{\mathbb{V}_t} := (q, \mathbb{V}_t, \mathbb{G}_T, \mathbb{A}_t, e) \leftarrow \mathcal{G}_{dpvs}(\kappa, N_t, param_{\mathbb{G}})$,
$X_t := (X_{t,i,j})_{i,j=1,\ldots,N_t} \xleftarrow{\mathrm{U}} GL(N_t, \mathbb{F}_q)$, $X_t^* := (Y_{t,i,j})_{i,j=1,\ldots,N_t} := \psi(X_t^T)^{-1} \xleftarrow{\mathrm{U}} GL(N_t, \mathbb{F}_q)$,
where $\vec{X}_{t,i}$ and $\vec{Y}_{t,i}$ respectively denote the $i^{th}$ vector of $X_t$ and $X_t^*$ for $i = 1, \ldots, N_t$
$\vec{b}_{t,i} := (\vec{X}_{t,i})\mathbb{A}_t = \sum_{j=1}^{N_t} X_{t,i,j} a_{t,j}$ for $i = 1, \ldots, N_t$, $\mathbb{B}_t = (\vec{b}_{t,1}, \ldots, \vec{b}_{t,N_t})$
$\vec{b}^*_{t,i} := (\vec{X}^*_{t,i})\mathbb{A}_t = \sum_{j=1}^{N_t} Y_{t,i,j} a_{t,j}$ for $i = 1, \ldots, N_t$, $\mathbb{B}^*_t = (\vec{b}^*_{t,1}, \ldots, \vec{b}^*_{t,N_t})$
$g_T = e(P, P)^{\psi}$, param:=$(\{param_{\mathbb{V}_t}\}_{t=0,1,\ldots,4}, \ \psi P, \ g_T)$, return (param, $\{\mathbb{B}_t, \ \mathbb{B}^*_t\}_{t=0,1,\ldots,4}$)

## 2.2 Hardness Assumptions

We describe here two Decisional SubSpace (DSS) assumptions, DSS1 and DSS2 in dual pairing vector spaces over prime order groups. We show that both the assumptions hold if DLIN assumption holds in the source groups. The assumption DSS1 (resp. DSS2) is obtained by taking two parallel copies of 5 dimensional vector and three parallel copies of a 14 dimensional vector from assumption 1-ABE (resp. 2-ABE) of [OT12b]. (Here, 1-ABE (resp. 2-ABE) is an assumption weaker than assumption DSS1 (resp. DSS2)). But some of the scalars of interest are same for each

copy and some are independent for different copies. Due to this independence, we are unable to reduce DSS1 (resp. DSS2) from 1-ABE (resp. 2-ABE). Although the approach for obtaining reductions of 1-ABE and 2-ABE from DLIN is adapted from [OT12b], we modify some of the intermediate "basic problems" to "modified" basic problems. A brief reduction of DSS1 and DSS2 from DLIN is given in Appendix B.

### Assumption Decisional Linear (DLIN)

Define the following distribution :

$$param_{\mathbb{G}} := (q, \mathbb{G}, \mathbb{G}_T, P, e) \longleftarrow \mathcal{G}_{bpg}(\kappa),\ \xi, \lambda, \delta, \sigma \xleftarrow{\text{U}} \mathbb{F}_q$$

$$D := (param_{\mathbb{G}}, \xi P, \lambda P, \delta\xi P, \sigma\lambda P),\ T_0 = (\delta + \sigma)P,\ T_1 \xleftarrow{\text{U}} \mathbb{G}$$

Now, the advantage of an algorithm $\mathscr{A}$ in breaking Assumption DLIN is defined by

$$\mathsf{Adv}^{\text{DLIN}}_{\mathscr{A}}(\kappa) = |Pr[\mathscr{A}(D, T_0) = 1] - Pr[\mathscr{A}(D, T_1) = 1]|$$

We say that the DLIN assumption holds if for every PPT algorithm $\mathscr{A}$, the advantage $\mathsf{Adv}^{\text{DLIN}}_{\mathscr{A}}(\kappa)$ is a negligible function in the security parameter $\kappa$.

### Assumption DSS1

Choose $\phi_0, \phi_4, \omega \xleftarrow{\text{U}} \mathbb{F}_q$ and $\tau \xleftarrow{\text{U}} \mathbb{F}_q^{\times}$. Also choose $Z_h^1, Z_h^2, Z_h^3 \xleftarrow{\text{U}} GL(2, \mathbb{F}_q)$ for $h = 1, \ldots, d$.

$$(param, (\mathbb{B}_0, \mathbb{B}_0^*), (\mathbb{B}_1, \mathbb{B}_1^*), (\mathbb{B}_2, \mathbb{B}_2^*), (\mathbb{B}_3, \mathbb{B}_3^*), (\mathbb{B}_4, \mathbb{B}_4^*)) \longleftarrow \mathcal{G}_{ob}(\kappa, 5, 14, 14, 14, 5)$$

$$\widehat{\mathbb{B}}_j := (\vec{b}_{j,1},\ \vec{b}_{j,3},\ \vec{b}_{j,5}),\ \widehat{\mathbb{B}}_j^* := (\vec{b}^*_{j,1},\ \vec{b}^*_{j,3},\ \vec{b}^*_{j,4})\quad for\ j = 0, 4$$

$$\widehat{\mathbb{B}}_j := (\vec{b}_{j,1}, \ldots, \vec{b}_{j,4},\ \vec{b}_{j,13},\ \vec{b}_{j,14}),\ \widehat{\mathbb{B}}_j^* := (\vec{b}^*_{j,1}, \ldots, \vec{b}^*_{j,4},\ \vec{b}^*_{j,11},\ \vec{b}^*_{j,12})\quad for\ j = 1, 2, 3$$

$$\vec{e}^{\,j}_0 := (\omega,\ 0,\ 0,\ 0,\ \phi_j)\mathbb{B}_j,\ \vec{e}^{\,j}_1 := (\omega,\ \tau,\ 0,\ 0,\ \phi_j)\mathbb{B}_j \text{ for } j = 0, 4$$

For $h = 1, ..., d$, $i = 1, 2$, $j = 1, 2, 3$, choose $\delta^j_{h,i}, \phi^j_{h,i,1}, \phi^j_{h,i,2} \xleftarrow{\text{U}} \mathbb{F}_q$

$$\vec{e}^{\,j}_{0,h,i} := \quad ( \overbrace{\delta^j_{h,i}(1,h), \omega\vec{e}_i}^{4},\ \overbrace{0^6}^{6},\ \overbrace{0^2}^{2},\ \overbrace{\phi^j_{h,i,1}, \phi^j_{h,i,2}}^{2} )\mathbb{B}_j$$

$$\vec{e}^{\,j}_{1,h,i} := \quad ( \overbrace{\delta^j_{h,i}(1,h), \omega\vec{e}_i}^{4},\ \overbrace{\tau\vec{e}_i, 0^2, \tau\vec{e}_i Z^j_h}^{6},\ \overbrace{0^2}^{2},\ \overbrace{\phi^j_{h,i,1}, \phi^j_{h,i,2}}^{2} )\mathbb{B}_j$$

$$D := (param, \{\widehat{\mathbb{B}}_j, \widehat{\mathbb{B}}_j^*\}_{j=0,1,\ldots,4})\ \text{For } \beta = 0, 1, \text{define } T_\beta := (\{\vec{e}^{\,j}_\beta\}_{j=0,4}, \{\vec{e}^{\,j}_{\beta,h,i}\}_{h=1,\ldots,d;\ i=1,2;\ j=1,2,3})$$

Now, the advantage of an algorithm $\mathscr{A}$ in breaking Assumption DSS1 is defined by

$$\mathsf{Adv}^{\text{DSS1}}_{\mathscr{A}}(\kappa) = |Pr[\mathscr{A}(D, T_0) = 1] - Pr[\mathscr{A}(D, T_1) = 1]|$$

We say that the DSS1 assumption holds if for every PPT algorithm $\mathscr{A}$, the advantage $\mathsf{Adv}^{\text{DSS1}}_{\mathscr{A}}(\kappa)$ is a negligible function in the security parameter $\kappa$.

**Lemma 2.1.** *If the decisional linear (DLIN) assumption holds for a bilinear pairing group generator $\mathcal{G}$, then the decisional subspace assumption, DSS1 also holds for $\mathcal{G}$*

*Proof.* Proof of the lemma 2.1 is found in Appendix B.1 (lemma B.3). □

**Assumption DSS2**

Choose $\phi_0, \phi_4, \eta_0, \eta_4, \zeta, \omega \xleftarrow{U} \mathbb{F}_q$ and $\tau, \rho \xleftarrow{U} \mathbb{F}_q^{\times}$. Also choose $Z_h^1, Z_h^2, Z_h^3 \xleftarrow{U} GL(2, \mathbb{F}_q)$ and set $U_h^j = ((Z_h^j)^{-1})^T$ for $h = 1, ..., d,\ j = 1, 2, 3$.

$$(param, (\mathbb{B}_0, \mathbb{B}_0^*), (\mathbb{B}_1, \mathbb{B}_1^*), (\mathbb{B}_2, \mathbb{B}_2^*), (\mathbb{B}_3, \mathbb{B}_3^*), (\mathbb{B}_4, \mathbb{B}_4^*)) \longleftarrow \mathcal{G}_{ob}(\kappa, 5, 14, 14, 14, 5)$$

$$\widehat{\mathbb{B}}_j := (\vec{b}_{j,1},\ \vec{b}_{j,3},\ \vec{b}_{j,5}),\ \widehat{\mathbb{B}}_j^* := (\vec{b}_{j,1}^*, \ldots, \vec{b}_{j,4}^*)\ \ for\ j = 0, 4$$

$$\widehat{\mathbb{B}}_j := (\vec{b}_{j,1}, \ldots, \vec{b}_{j,4},\ \vec{b}_{j,13},\ \vec{b}_{j,14}),\ \widehat{\mathbb{B}}_j^* := (\vec{b}_{j,1}^*, \ldots, \vec{b}_{j,4}^*,\ \vec{b}_{j,11}^*,\ \vec{b}_{j,12}^*)\ \ for\ j = 1, 2, 3$$

$$\vec{\Upsilon}^j := (\omega,\ \tau,\ 0,\ 0,\ \phi_j)\mathbb{B}_j,\ \vec{\Upsilon}_0^{j*} := (\zeta,\ 0,\ 0,\ \eta_j,\ 0)\mathbb{B}_j^*,\ \vec{\Upsilon}_1^{j*} := (\zeta,\ \rho,\ 0,\ \eta_j,\ 0)\mathbb{B}_j^* \text{ for } j = 0, 4$$

For $h = 1, \ldots, d,\ i = 1, 2,\ j = 1, 2, 3$, choose $\mu_{h,i}^j, \delta_{h,i}^j, \eta_{h,i,1}^j, \eta_{h,i,2}^j, \phi_{h,i,1}^j, \phi_{h,i,2}^j \xleftarrow{U} \mathbb{F}_q$

$$\vec{\Upsilon}_{0,h,i}^{j*} := \quad ( \overbrace{\mu_{h,i}^j(h,-1), \zeta\vec{e}_i}^{4}, \quad \overbrace{0^6}^{6}, \quad \overbrace{0^2}^{2}, \quad \overbrace{\eta_{h,i,1}^j, \eta_{h,i,2}^j}^{2} \quad )\mathbb{B}_j^*$$

$$\vec{\Upsilon}_{1,h,i}^{j*} := \quad ( \overbrace{\mu_{h,i}^j(h,-1), \zeta\vec{e}_i}^{4}, \quad \overbrace{0^4, \rho\vec{e}_i U_h^j}^{6}, \quad \overbrace{0^2}^{2}, \quad \overbrace{\eta_{h,i,1}^j, \eta_{h,i,2}^j}^{2} \quad )\mathbb{B}_j^*$$

$$\vec{e}_{h,i}^{\,j} := \quad ( \overbrace{\delta_{h,i}^j(1,h), \omega\vec{e}_i}^{4}, \quad \overbrace{\tau\vec{e}_i, 0^2, \tau\vec{e}_i Z_h^j}^{6}, \quad \overbrace{0^2}^{2}, \quad \overbrace{\phi_{h,i,1}^j, \phi_{h,i,2}^j}^{2} \quad )\mathbb{B}_j$$

$$D := (param, \{\widehat{\mathbb{B}}_j, \widehat{\mathbb{B}}_j^*\}_{j=0,1,\ldots,4}, \{\vec{\Upsilon}^j\}_{j=0,4}, \{\vec{e}_{h,i}^{\,j}\}_{h=1,\ldots,d;\ i=1,2;\ j=1,2,3})$$

$$\text{For } \beta = 0, 1, \text{define } T_\beta := (\{\vec{\Upsilon}_\beta^{j*}\}_{j=0,4}, \{\vec{\Upsilon}_{\beta,h,i}^{j*}\}_{h=1,\ldots,d;\ i=1,2;\ j=1,2,3})$$

Now, the advantage of an algorithm $\mathscr{A}$ in breaking Assumption DSS2 is defined by

$$\mathsf{Adv}_{\mathscr{A}}^{\mathrm{DSS2}}(\kappa) = |Pr[\mathscr{A}(D, T_0) = 1] - Pr[\mathscr{A}(D, T_1) = 1]|$$

We say that the DSS2 assumption holds if for every PPT algorithm $\mathscr{A}$, the advantage $\mathsf{Adv}_{\mathscr{A}}^{\mathrm{DSS2}}(\kappa)$ is a negligible function in the security parameter $\kappa$.

**Lemma 2.2.** *If the decisional linear (DLIN) assumption holds for a bilinear pairing group generator $\mathcal{G}$, then the decisional subspace assumption, DSS2 also holds for $\mathcal{G}$*

*Proof.* Proof of the lemma 2.2 is found in Appendix B.2 (lemma B.18). □

# 3 Basic CP-FE Construction

In this section, we describe a basic Ciphertext-Policy Functional Encryption scheme for DFAs in the prime order bilinear pairing groups. This scheme is based on the structure of ABE construction of [OT12b], where encryption is done using the bases of a dual pairing vector spaces and the keys are generated by it's dual. In their basic construction([OT12b]), they restricted the access structures by putting a limitation that the attributes must not repeat in the access structures. This type of restrictions is required to guarantee the adaptive security of the basic construction. Similarly, our basic construction involved here has the following restrictions (similar to [Ram13]).

– There is at most a single transition corresponding to each symbol in the DFAs (policies)

– The strings for keys can have at most a single occurrence of each symbol (keys)

We illustrate how to relax the above restrictions in section 5.

$\mathsf{Setup}(\kappa)$: $(param, (\mathbb{B}_0, \mathbb{B}_0^*), (\mathbb{B}_1, \mathbb{B}_1^*), (\mathbb{B}_2, \mathbb{B}_2^*), (\mathbb{B}_3, \mathbb{B}_3^*), (\mathbb{B}_4, \mathbb{B}_4^*)) \longleftarrow \mathcal{G}_{ob}(1^\lambda, 5, 14, 14, 14, 5)$

$\widehat{\mathbb{B}}_j := (\ \vec{b}_{j,1},\ \vec{b}_{j,3},\ \vec{b}_{j,5}),\quad \widehat{\mathbb{B}}_j^* := (\ \vec{b}_{j,1}^*,\ \vec{b}_{j,3}^*,\ \vec{b}_{j,4}^*\ )\quad$ for j=0,4

$\widehat{\mathbb{B}}_j := (\ \vec{b}_{j,1} \ldots, \vec{b}_{j,4},\ \vec{b}_{j,11},\ \vec{b}_{j,12}\ ),\quad \widehat{\mathbb{B}}_j^* := (\ \vec{b}_{j,1}^*, \ldots, \vec{b}_{j,4}^*,\ \vec{b}_{j,13}^*,\ \vec{b}_{j,14}^*\ )\quad$ for j=1,2,3

Choose a set, alphabet of symbols $\Sigma = \{\sigma_1, \ldots, \sigma_d\} \subseteq \mathbb{F}_q$, where $d = poly(\kappa)$. The public parameters and master secret are given by

$\mathcal{PP} := (\Sigma, param,\ \{\widehat{\mathbb{B}}_j\}_{j=0,1,2,3,4})$,
$\mathcal{MSK} := (\{\widehat{\mathbb{B}}^*_j\}_{j=0,1,2,3,4})$.

$\mathsf{Encrypt}(\mathcal{PP}, \mathcal{M} = (Q, \Sigma, q_0, F, \delta), m)$: For each $q_x \in Q$, pick $d_x \xleftarrow{\text{U}} \mathbb{F}_q$. For each $q_z \in F$, choose $\phi_z \xleftarrow{\text{U}} \mathbb{F}_q$. Pick random $\xi \in \mathbb{F}_q$. For each transition $t = (q_x, q_y, \sigma_h) \in \mathcal{T}$, choose $s_t, \delta_{t,1}, \delta_{t,2}, \delta_{t,3} \xleftarrow{\text{U}} \mathbb{F}_q;\ \vec{\phi}_{t,1},\ \vec{\phi}_{t,2},\ \vec{\phi}_{t,3} \xleftarrow{\text{U}} \mathbb{F}_q^2$. Now, compute

$\vec{C}_0 := (\ d_0,\ 0,\ \xi,\ 0,\ \phi_0)\mathbb{B}_0 \quad C_m := m.g_T^{\xi}$

For each transition $t = (q_x, q_y, \sigma_h) \in \mathcal{T}$, compute the ciphertext components

$\vec{C}_{t,1} := (\ \overbrace{\delta_{t,1}(1,h)}^{2},\ \overbrace{(s_t + d_y)(1,\sigma_h)}^{2},\ \overbrace{0^6}^{6},\ \overbrace{0^2}^{2},\ \overbrace{\vec{\phi}_{t,1}}^{2}\ )\ \mathbb{B}_1$

$\vec{C}_{t,2} := (\ \overbrace{\delta_{t,2}(1,h)}^{2},\ \overbrace{(-s_t + d_x)(1,\sigma_h)}^{2},\ \overbrace{0^6}^{6},\ \overbrace{0^2}^{2},\ \overbrace{\vec{\phi}_{t,2}}^{2}\ )\ \mathbb{B}_2$

$\vec{C}_{t,3} := (\ \overbrace{\delta_{t,3}(1,h)}^{2},\ \overbrace{s_t(1,\sigma_h)}^{2},\ \overbrace{0^6}^{6},\ \overbrace{0^2}^{2},\ \overbrace{\vec{\phi}_{t,3}}^{2}\ )\ \mathbb{B}_3$

For each $q_z \in F$, compute the ciphertext component
$\vec{C}_{z,4} := (\ d_z,\ 0,\ 0,\ 0,\ \phi_z)\mathbb{B}_4$

$\mathcal{C}_{\mathcal{M}} := (\ \mathcal{M},\ C_m,\ \vec{C}_0,\ \{\vec{C}_{t,1},\ \vec{C}_{t,2},\ \vec{C}_{t,3}\}_{t=(q_x,q_y,\sigma_h)\in\mathcal{T}},\ \{\vec{C}_{z,4}\}_{q_z\in F})$

$\mathsf{KeyGen}(\mathcal{MSK}, w = w_1 \cdots w_\ell)$: For each $i \in [\ell]$, choose $\mu_{i,1},\ \mu_{i,2},\ \mu_{i,3}, \theta_i, r_i \xleftarrow{\text{U}} \mathbb{F}_q;\ \vec{\eta}_{i,1}, \vec{\eta}_{i,2}, \vec{\eta}_{i,3} \xleftarrow{\text{U}} \mathbb{F}_q^2$. Pick $r_0, \eta_0, \eta_{\ell+1} \xleftarrow{\text{U}} \mathbb{F}_q$. Now compute

$\vec{K}^*_0 := (\ r_0,\ 0,\ 1,\ \eta_0,\ 0)\mathbb{B}^*_0$

For each $i \in [\ell]$, (let $w_i = \sigma_h$, for some index $h$) continue to compute

$\vec{K}^*_{i,1} := (\ \overbrace{\mu_{i,1}(h,-1)}^{2},\ \overbrace{r_i + \theta_i\sigma_h,\ -\theta_i}^{2},\ \overbrace{0^6}^{6},\ \overbrace{\vec{\eta}_{i,1}}^{2},\ \overbrace{0^2}^{2}\ )\ \mathbb{B}^*_1$

$\vec{K}^*_{i,2} := (\ \overbrace{\mu_{i,2}(h,-1)}^{2},\ \overbrace{-r_{i-1} + \theta_i\sigma_h,\ -\theta_i}^{2},\ \overbrace{0^6}^{6},\ \overbrace{\vec{\eta}_{i,2}}^{2},\ \overbrace{0^2}^{2}\ )\ \mathbb{B}^*_2$

$\vec{K}^*_{i,3} := (\ \overbrace{\mu_{i,3}(h,-1)}^{2},\ \overbrace{-r_i - r_{i-1} + \theta_i\sigma_h, -\theta_i}^{2},\ \overbrace{0^6}^{6},\ \overbrace{\vec{\eta}_{i,3}}^{2},\ \overbrace{0^2}^{2}\ )\ \mathbb{B}^*_3$

$\vec{K}^*_{\ell+1,4} := (\ r_\ell,\ 0,\ 0,\ \eta_{\ell+1},\ 0)\mathbb{B}^*_4$

The secret key for the string $w$ is given by

$$SK_w := \big(w, \vec{K}^*_0,\ \{\vec{K}^*_{i,1},\ \vec{K}^*_{i,2},\ \vec{K}^*_{i,3}\}_{i\in[\ell]}, \vec{K}^*_{\ell+1,4}\big)$$

$\mathsf{Decrypt}(C_{\mathcal{M}}, SK_w)$: Suppose the DFA $\mathcal{M}$ accepts the string $w = w_1 \cdots w_\ell$, then there exist a sequence of $\ell + 1$ states $q_{x_0}, q_{x_1}, q_{x_2}, \ldots, q_{x_\ell}$ and transitions $t_1, \ldots, t_\ell$, where $x_0 = 0$ and $q_{x_\ell} \in F$ and for $i = 1, 2, \ldots, \ell$, we have $t_i = (q_{x_{i-1}}, q_{x_i}, \sigma) \in \mathcal{T}$ with $w_i = \sigma$. First, compute the initial value

$$A_0 = e(\vec{C}_0,\ \vec{K}^*_0) = g_T^{r_0 d_0 + \xi}$$

Then, compute the first value $A_1$ of intermediate values as

$$A_1 = e(\vec{C}_{t_1,1},\ \vec{K}^*_{1,1}).e(\vec{C}_{t_1,2},\ \vec{K}^*_{1,2}).e(\vec{C}_{t_1,3},\ \vec{K}^*_{1,3}) = g_T^{r_1 d_{x_1} - r_0 d_0}$$

Next, compute the intermediate values $A_i$ (for $i = 2, \ldots, \ell$) as follows:

$$A_i = A_{i-1}.e(\vec{C}_{t_i,1},\ \vec{K}^*_{i,1}).e(\vec{C}_{t_i,2},\ \vec{K}^*_{i,2}).e(\vec{C}_{t_i,3},\ \vec{K}^*_{i,3}) = g_T^{r_{i-1} d_{x_{i-1}} - r_0 d_0}\, g_T^{r_i d_{x_i} - r_{i-1} d_{x_{i-1}}} = g_T^{r_i d_{x_i} - r_0 d_0}$$

Similarly, the $\ell^{th}$ intermediate value is obtained in the form $A_\ell = g_T^{r_\ell d_{x_\ell} - r_0 d_0}$
The final value $A_{\ell+1}$ is computed as

$$A_{\ell+1} = A_\ell . e(\vec{C}_{x_\ell,4},\ \vec{K}^*_{\ell+1,4}) = g_T^{r_\ell d_{x_\ell} - r_0 d_0} g_T^{-r_\ell d_{x_\ell}} = g_T^{-r_0 d_0}$$

Using $A_0, A_{\ell+1}$ and $C_m$, the message is extracted as $m = C_m/(A_0\ A_{\ell+1})$.

# 4 Security Proof

We prove the adaptive security of our basic CP-FE construction by adopting the proof technique of Okamoto–Takashima [OT12b] and the dual system methodology of Brent Waters [Wat09]. This methodology requires to define semi-functional ciphertexts and keys. Here, we define two types of semi-functional ciphertexts, viz., type 1 and type 2. Three forms of semi-functional keys are considered here – type 1, type 2 and type 3. In the sequence of games, challenge ciphertext is first changed from normal to semi-functional type 1. Then each queried key is changed from normal to semi-functional type 1, then semi-functional type 1 to type 2 and lastly from semi-functional type 2 to type 3. In the final game, the semi-functional type 1 ciphertext is changed to semi-functional type 2 ciphertext, where the message is masked by an independently and uniformly chosen value.

In the following material, the part framed by a box indicates that either it will be changed in next description or it has been changed from previous description. Also, we use the abbreviation 'sf' for 'semi-functional'.

**Semi-functional Type 1 Ciphertext.** For each $q_x \in Q$, pick $\widehat{d}_x \xleftarrow{U} \mathbb{F}_q$. For each transition $t = (q_x, q_y, \sigma_h) \in \mathcal{T}$, choose $\widehat{s}_t \xleftarrow{U} \mathbb{F}_q$; $Z_h^1, Z_h^2, Z_h^3 \xleftarrow{U} GL(2, \mathbb{F}_q)$. The sf-type 1 ciphertext is obtained by modifying normal ciphertext $\mathcal{C}_\mathcal{M} = (\mathcal{M},\ C_m,\ \vec{C}_0,\ \{\vec{C}_{t,1},\ \vec{C}_{t,2},\ \vec{C}_{t,3}\}_{t=(q_x,q_y,\sigma_h)\in\mathcal{T}},\ \{\vec{C}_{z,4}\}_{q_z\in F})$ as given below:

$$\vec{C}_0 := (\ d_0,\ \boxed{\widehat{d}_0},\ \xi,\ 0,\ \phi_0)\mathbb{B}_0 \qquad C_m := m.g_T^\xi$$

$$\vec{C}_{t,1} := (\ \overbrace{\delta_{t,1}(1,h)}^{2},\ \overbrace{(s_t + d_y)(1,\sigma_h)}^{2},\ \overbrace{\boxed{(\widehat{s}_t + \widehat{d}_y)(1,\sigma_h)},\ 0^2,\ \boxed{(\widehat{s}_t + \widehat{d}_y)(1,\sigma_h)Z_h^1}}^{6},\ \overbrace{0^2}^{2},\ \overbrace{\vec{\phi}_{t,1}}^{2})\ \mathbb{B}_1$$

$$\vec{C}_{t,2} := (\ \overbrace{\delta_{t,2}(1,h)}^{2},\ \overbrace{(-s_t + d_x)(1,\sigma_h)}^{2},\ \overbrace{\boxed{(\widehat{-s}_t + \widehat{d}_x)(1,\sigma_h)}, 0^2, \boxed{(\widehat{-s}_t + \widehat{d}_x)(1,\sigma_h)Z_h^2}}^{6},\ \overbrace{0^2}^{2},\ \overbrace{\vec{\phi}_{t,2}}^{2})\ \mathbb{B}_2$$

$$\vec{C}_{t,3} := (\ \overbrace{\delta_{t,3}(1,h)}^{2},\ \overbrace{s_t(1,\sigma_h)}^{2},\ \overbrace{\boxed{\widehat{s}_t(1,\sigma_h)},\ 0^2,\ \boxed{\widehat{s}_t(1,\sigma_h)Z_h^3}}^{6},\ \overbrace{0^2}^{2},\ \overbrace{\vec{\phi}_{t,3}}^{2})\ \mathbb{B}_3$$

$$\vec{C}_{z,4} := (\ d_z,\ \boxed{\widehat{d}_z},\ 0,\ 0,\ \phi_z)\mathbb{B}_4$$

**Semi-functional Type 2 Ciphertext.** This is same as sf-type 1 ciphertext except the following

$\vec{C}_0 := (\ d_0,\ \widehat{d}_0,\ \boxed{\xi'},\ 0,\ \phi_0)\mathbb{B}_0 \qquad C_m := m.g_T^\xi$ where $\xi' \xleftarrow{U} \mathbb{F}_q$ (independent of $\xi \xleftarrow{U} \mathbb{F}_q$)

**Semi-functional Type 1 Key.** For each $i \in [\ell]$, choose $\widehat{r}_i, \widehat{\theta}_i \xleftarrow{U} \mathbb{F}_q$. Also choose $\widehat{r}_0 \xleftarrow{U} \mathbb{F}_q$. For $i \in [\ell]$, let $w_i = \sigma_h$ for some index $h$, choose $Z_h^j \xleftarrow{U} GL(2, \mathbb{F}_q)$ for $j = 1, 2, 3$ and set $U_h^j = ((Z_h^j)^{-1})^T$. The sf-type 1 key generation algorithm first creates a normal key $SK_w = \big(w, \vec{K}_0^*,\ \{\vec{K}_{i,1}^*,\ \vec{K}_{i,2}^*,\ \vec{K}_{i,3}^*\}_{i\in[\ell]}, \vec{K}_{\ell+1,4}^*\big)$ and then modifies its components as shown below.

$$\vec{K}_0^* := (\ r_0,\ \boxed{\widehat{r}_0},\ 1,\ \eta_0,\ 0)\mathbb{B}_0^*$$

$$\vec{K}_{i,1}^* := (\ \overbrace{\mu_{i,1}(h,-1)}^{2},\ \overbrace{r_i + \theta_i\sigma_h,\ \ -\theta_i}^{2},\ \overbrace{0^4, \boxed{(\widehat{r}_i + \widehat{\theta}_i\sigma_h,\ \ -\widehat{\theta}_i)U_h^1}}^{6},\ \overbrace{\vec{\eta}_{i,1}}^{2},\ \overbrace{0^2}^{2})\ \mathbb{B}_1^*$$

$$\vec{K}_{i,2}^* := (\ \overbrace{\mu_{i,2}(h,-1)}^{2},\ \overbrace{-r_{i-1} + \theta_i\sigma_h,\ \ -\theta_i}^{2},\ \overbrace{0^4, \boxed{(-\widehat{r}_{i-1} + \widehat{\theta}_i\sigma_h,\ \ -\widehat{\theta}_i)U_h^2}}^{6},\ \overbrace{\vec{\eta}_{i,2}}^{2},\ \overbrace{0^2}^{2})\ \mathbb{B}_2^*$$

$$\vec{K}^*_{i,3} := (\overbrace{\mu_{i,3}(h,-1)}^{2}, \overbrace{-r_i - r_{i-1} + \theta_i\sigma_h, -\theta_i}^{2}, \quad \overbrace{0^4, \boxed{(-\widehat{r}_i - \widehat{r}_{i-1} + \widehat{\theta}_i\sigma_h, -\widehat{\theta}_i)U^3_h}}^{6}, \quad \overbrace{\vec{\eta}_{i,3}}^{2}, \overbrace{0^2}^{2}) \mathbb{B}^*_3$$

$$\vec{K}^*_{\ell+1,4} := (r_\ell, \boxed{\widehat{r}_\ell}, 0, \eta_{\ell+1}, 0)\mathbb{B}^*_4$$

**Semi-functional Type 2 Key.** This is same as sf-type 1 key except $\vec{K}^*_0$

$\vec{K}^*_0 := (r_0, \boxed{r}, 1, \eta_0, 0)\mathbb{B}^*_0$, where $r \xleftarrow{U} \mathbb{F}_q$ (independent of $\widehat{r}_0 \xleftarrow{U} \mathbb{F}_q$)

Note that $\widehat{r}_0$ appears in $\vec{K}^*_{1,2}$ and $\vec{K}^*_{1,3}$

**Semi-functional Type 3 Key.** This is same as normal key except $\vec{K}^*_0$

$\vec{K}^*_0 := (r_0, \boxed{r}, 1, \eta_0, 0)\mathbb{B}^*_0$, where $r \xleftarrow{U} \mathbb{F}_q$

A legitimate normal key (resp. sf-type 1 key, sf-type 2 key, sf-type 3 key) $\mathcal{SK}_w$ can extract the message from an sf-type 1 ciphertext (resp. normal ciphertext) $\mathcal{C}_\mathcal{M}$. Similarly, a legitimate sf-type 1 key $\mathcal{SK}_w$ can succeed in decrypting an sf-type 1 ciphertext $\mathcal{C}_\mathcal{M}$, because the mimicked parts get canceled just like the normal components. But, if a legitimate sf-type 2 key or sf-type 2 key $\mathcal{SK}_w$ runs decryption on an sf-type 1 ciphertext $\mathcal{C}_\mathcal{M}$, it will get an extra term $g_T^{r\widehat{d}_0}$ hampering the message extraction.

**Theorem 4.1.** *The proposed Basic CP-FE scheme is adaptively secure under the DLIN assumption.*

### Proof Sketch of Theorem 4.1

The proof technique of the above theorem is adopted from that of ABE of Okamoto–Takashima [OT12b]. By applying hybrid arguments over the sequence of games $\mathrm{Game}_{Real}, \mathrm{Game}_0, \{\mathrm{Game}_{k,1}, \mathrm{Game}_{k,2}, \mathrm{Game}_{k,3}\}_{k\in[\nu]}$ and $\mathrm{Game}_{Final}$, the game $\mathrm{Game}_{Real}$ is changed to $\mathrm{Game}_{Final}$.

In $\mathrm{Game}_0$, the challenge ciphertext is changed from normal to sf-type 1. If there are at most $\nu$ secret key queries made by an adversary $\mathscr{A}$, there are $3\nu$ game changes from $\mathrm{Game}_0$ ($\mathrm{Game}_{0,3}$), $\mathrm{Game}_{1,1}$, $\mathrm{Game}_{1,2}$, $\mathrm{Game}_{1,3}$ through $\mathrm{Game}_{\nu,2}$ and $\mathrm{Game}_{\nu,3}$. In $\mathrm{Game}_{k,1}$ (for $1 \le k \le \nu$), the challenge ciphertext is sf-type 1, the first $(k-1)$ keys are sf-type 3, $k^{th}$ key is sf-type 1 and the rest are normal. $\mathrm{Game}_{k,2}$ (for $1 \le k \le \nu$) is same as $\mathrm{Game}_{k,1}$ except that $k^{th}$ key is sf-type 2. $\mathrm{Game}_{k,3}$ (for $1 \le k \le \nu$) is same as $\mathrm{Game}_{k,2}$ except that $k^{th}$ key is sf-type 3. $\mathrm{Game}_{Final}$ is similar to $\mathrm{Game}_{\nu,3}$ except that the challenge ciphertext is a sf-type 2 ciphertext, i.e., in $\mathrm{Game}_{Final}$, the challenge message is masked with an uniformly and independently chosen value implying that $\mathscr{A}$ has no advantage in breaking the final game. We prove that the gap advantage between any two consecutive games are at most negligible.

In lemma 4.2, we show that the advantage gap between $\mathrm{Game}_{Real}$ and $\mathrm{Game}_0$ is equivalent to that of DSS1: we establish a PPT simulator $\mathscr{B}$ for $\mathrm{Game}_{Real}$ and $\mathrm{Game}_0$ against a PPT adversary $\mathscr{A}$. The simulator $\mathscr{B}$ takes an instance of DSS1 (with $\beta \xleftarrow{U} \{0,1\}$) and simulates either $\mathrm{Game}_{Real}$ or $\mathrm{Game}_0$ for adversary $\mathscr{A}$. We show that the distribution of secret keys and challenge ciphertext replied by $\mathscr{B}$ is equivalent to $\mathrm{Game}_{Real}$ (resp. $\mathrm{Game}_0$) if $\beta = 0$ (resp. $\beta = 1$).

In lemma 2.1, we prove that assumption DSS1 holds for a bilinear pairing groups if DLIN assumption holds for the same pairing groups. Therefore, $\mathrm{Game}_{Real}$ and $\mathrm{Game}_0$ are indistinguishable under DLIN assumption. Seemingly, this shows that the normal ciphertext and sf-type 1 ciphertext are indistinguishable under DLIN assumption.

Similarly, in lemma 4.3, we show that the advantage gap between $\mathrm{Game}_{(k-1),3}$ and $\mathrm{Game}_{k,1}$ is bounded by the advantage of DSS2. Likewise, in lemma 2.2, we prove that assumption DSS2 holds for a bilinear pairing groups if DLIN assumption holds for the same pairing groups. Thus, $\mathrm{Game}_{(k-1),3}$ and $\mathrm{Game}_{k,1}$ are indistinguishable if DLIN assumption holds. In other words, it shows that the $k^{th}$ normal key and $k^{th}$ sf-type 1 key are indistinguishable if DLIN assumption holds.

Then, we show that gap advantage between $\mathrm{Game}_{k,1}$ and $\mathrm{Game}_{k,2}$ is zero (without any assumption) (lemma 4.4) as: the distribution of $(\mathcal{PP}, \{\mathcal{SK}_{w^\iota}\}_{\iota=1,\ldots,\nu}, \mathcal{C}_{\mathcal{M}^*})$ in $\mathrm{Game}_{k,1}$ and that in $\mathrm{Game}_{k,2}$ are exactly same except at $k^{th}$ key, where $w^\iota$ is $\iota^{th}$ query string. So, we have to show that the joint distribution of $k^{th}$ key $\mathcal{SK}_{w^k}$ and the challenge

ciphertext in both the games are equivalent. In lemma 4.4, we basically show that the scalar $\widehat{r}_0$ in $\vec{K}_0^*$ of $k^{th}$ key $\mathcal{SK}_{w^k}$ (described in definition of sf-type 1 key) is uniformly and independently distributed from the other variables in the joint distribution of $\mathscr{A}$'s view. This shows that distribution of $k^{th}$ sf-type 1 key and $k^{th}$ sf-type 2 key are indistinguishable by any polynomial time adversary.

In a similar manner, we show that the advantage gap between $\text{Game}_{k,2}$ and $\text{Game}_{k,3}$ is bounded by the advantage of DSS2 adversary (lemma 4.5). This implies that $k^{th}$ sf-type 2 key and $k^{th}$ sf-type 3 key are indistinguishable under DSS2.

Finally, we show that $\text{Game}_{\nu,3}$ and $\text{Game}_{Final}$ are indistinguishable (without any assumption) (lemma 4.6). In lemma 4.6, we first apply a suitable transformation to form new bases $(\mathbb{D}_0, \mathbb{D}_0^*)$ from original bases $(\mathbb{B}_0, \mathbb{B}_0^*)$. Then, we show that the distribution of keys and ciphertext over $(\mathbb{B}_0, \mathbb{B}_0^*)$ (resp. $(\mathbb{D}_0, \mathbb{D}_0^*)$) is identical with $\text{Game}_{\nu,3}$ (resp. $\text{Game}_{Final}$),

*Proof.* The security proof consists of hybrid argument over a sequence of $3\nu+3$ games. The games are defined below:

- $\text{Game}_0$ ($\text{Game}_{0,3}$) is just like $\text{Game}_{Real}$ except that the challenge ciphertext is sf-type 1 ciphertext.
- In $\text{Game}_{k,1}$ (for $1 \le k \le \nu$)[2], challenge ciphertext is sf-type 1, the first $k-1$ keys returned to the adversary are sf-type 3, $k^{th}$ key is sf-type 1 and the rest are normal.
- In $\text{Game}_{k,2}$ (for $1 \le k \le \nu$), challenge ciphertext is sf-type 1, the first $k-1$ keys returned to the adversary are sf-type 3, $k^{th}$ key is sf-type 2 and the rest are normal.
- In $\text{Game}_{k,3}$ (for $1 \le k \le \nu$), challenge ciphertext is sf-type 1, the first $k$ keys returned to the adversary are sf-type 3 and the rest are normal.
- $\text{Game}_{Final}$ is similar to $\text{Game}_{\nu,3}$ except that now the challenge ciphertext is a sf-type 2 ciphertext.

Let $\mathsf{Adv}^{\text{Real}}_{\mathscr{A}}(\kappa)$, $\mathsf{Adv}^{0}_{\mathscr{A}}(\kappa)$, $\mathsf{Adv}^{k,1}_{\mathscr{A}}(\kappa)$, $\mathsf{Adv}^{k,2}_{\mathscr{A}}(\kappa)$, $\mathsf{Adv}^{k,3}_{\mathscr{A}}(\kappa)$ and $\mathsf{Adv}^{\text{Final}}_{\mathscr{A}}(\kappa)$ denote the advantages of an adversary $\mathscr{A}$ in $\text{Game}_{Real}$, $\text{Game}_0$, $\text{Game}_{k,1}$, $\text{Game}_{k,2}$, $\text{Game}_{k,3}$ and $\text{Game}_{Final}$ for $1 \le k \le \nu$ respectively. In $\text{Game}_{Final}$, the value of $b$ is independent from the adversary's view implying that $\mathsf{Adv}^{\text{Final}}_{\mathscr{A}}(\kappa) = 0$.

Using lemmas 4.2, 4.3, 4.4, 4.5 and 4.6, we have the following inequalities

$$\begin{aligned}
\mathsf{Adv}^{\text{CP-FE}}_{\mathscr{A}}(\kappa) &= \mathsf{Adv}^{\text{Real}}_{\mathscr{A}}(\kappa) \\
&\le |\mathsf{Adv}^{\text{Real}}_{\mathscr{A}}(\kappa) - \mathsf{Adv}^{0}_{\mathscr{A}}(\kappa)| + \sum_{k=1}^{\nu}(|\mathsf{Adv}^{k-1,3}_{\mathscr{A}}(\kappa) - \mathsf{Adv}^{k,1}_{\mathscr{A}}(\kappa)| + |\mathsf{Adv}^{k,1}_{\mathscr{A}}(\kappa) - \mathsf{Adv}^{k,2}_{\mathscr{A}}(\kappa)| \\
&\quad + |\mathsf{Adv}^{k,2}_{\mathscr{A}}(\kappa) - \mathsf{Adv}^{k,3}_{\mathscr{A}}(\kappa)|) + |\mathsf{Adv}^{\nu,3}_{\mathscr{A}}(\kappa) - \mathsf{Adv}^{\text{Final}}_{\mathscr{A}}(\kappa)| \\
&\le \mathsf{Adv}^{\text{DSS1}}_{\mathscr{A}}(\kappa) + \nu(\mathsf{Adv}^{\text{DSS2}}_{\mathscr{A}}(\kappa) + 2/q + \mathsf{Adv}^{\text{DSS2}}_{\mathscr{A}}(\kappa) + 2/q) + 1/q \\
&\le \mathsf{Adv}^{\text{DSS1}}_{\mathscr{A}}(\kappa) + 2\nu\mathsf{Adv}^{\text{DSS2}}_{\mathscr{A}}(\kappa) + (4\nu+1)/q
\end{aligned}$$

Final conclusion follows from lemmas 2.1 and 2.2. □

**Lemma 4.2.** $\text{Game}_{Real}$ *and* $\text{Game}_0$ *are indistinguishable under the DSS1 assumption. That is,* $|\mathsf{Adv}^{\text{Real}}_{\mathscr{A}}(\kappa) - \mathsf{Adv}^{0}_{\mathscr{A}}(\kappa)| \le \mathsf{Adv}^{\text{DSS1}}_{\mathscr{A}}(\kappa)$.

Proof is in Appendix A.3.

**Lemma 4.3.** $\text{Game}_{(k-1),3}$ *and* $\text{Game}_{k,1}$ *are indistinguishable under the DSS2 assumption. That is,* $|\mathsf{Adv}^{k-1,3}_{\mathscr{A}}(\kappa) - \mathsf{Adv}^{k,1}_{\mathscr{A}}(\kappa)| \le \mathsf{Adv}^{\text{DSS2}}_{\mathscr{A}}(\kappa) + 2/q$ *for* $1 \le k \le \nu$.

Proof can be found in Appendix A.4.

**Lemma 4.4.** $\text{Game}_{k,1}$ *and* $\text{Game}_{k,2}$ *are indistinguishable. That is,* $\mathsf{Adv}^{k,1}_{\mathscr{A}}(\kappa) = \mathsf{Adv}^{k,2}_{\mathscr{A}}(\kappa)$ *for* $1 \le k \le \nu$.

[2]In both the games, $\text{Game}_{k,1}$ and $\text{Game}_{k,2}$ (for $1 \le k \le \nu$), the matrices $Z_h^j$ in sf-type 1 ciphertext and the matrices $U_h^j$ in sf-type 1 key(resp. sf-type 2) of $\text{Game}_{k,1}$(resp. $\text{Game}_{k,2}$) are related by $U_h^j = ((Z_h^j)^{-1})^T$ for $j = 1, 2, 3$

Refer to Appendix A.5 for proof.

**Lemma 4.5.** $\text{Game}_{k,2}$ *and* $\text{Game}_{k,3}$ *are indistinguishable under the DSS2 assumption. That is,* $|\mathsf{Adv}^{k,3}_{\mathscr{A}}(\kappa) - \mathsf{Adv}^{k,2}_{\mathscr{A}}(\kappa)| \leq \mathsf{Adv}^{\text{DSS2}}_{\mathscr{A}}(\kappa) + 2/q$ *for* $1 \leq k \leq \nu$.

For proof, see Appendix A.6.

**Lemma 4.6.** $\text{Game}_{\nu,3}$ *and* $\text{Game}_{Final}$ *are indistinguishable. That is,* $|\mathsf{Adv}^{\text{Final}}_{\mathscr{A}}(\kappa) - \mathsf{Adv}^{\nu,3}_{\mathscr{A}}(\kappa)| \leq 1/q$

Proof is described in Appendix A.7.

# 5 Full CP-FE Construction

In this section, we illustrate our full CP-FE construction for finite languages over an alphabet $\Sigma$ accepted by a DFA. The size of the language accepted by a DFA may be infinite (unbounded). But our system supports only bounded number of users by restricting the size of strings. Let $w_{max}$ be a bound on maximum number of times a symbol may repeat in a string. So this bound automatically restricts the size of strings. Let $Trans_\sigma = \{(q_x, q_y, \sigma_h) \in \mathcal{T} \ : \sigma_h = \sigma\}$ for $\sigma \in \Sigma$. We also assume that for each symbol $\sigma \in \Sigma$, $|Trans_\sigma|$ is bounded by $t_{max}$, i.e., each symbol may repeat in the transitions of a DFA $\mathcal{M}$ at most $t_{max}$ times. These bounds are fixed during setup. Suppose, we are interested in full CP-FE construction for DFAs over a fixed alphabet $\Sigma$. Then, this full construction is obtained from the basic construction over a new alphabet $\Sigma_b$, where $\Sigma_b = \{\sigma^\iota_\varsigma = \Lambda(\sigma, \varsigma, \iota) \ : \sigma \in \Sigma, \varsigma \in [t_{max}], \ \iota \in [w_{max}]\}$, $\Lambda : \Sigma \times [t_{max}] \times [w_{max}] \to \mathbb{F}_q$ is an injective function i.e., $\Sigma_b$ can be thought of as a collection of $t_{max}w_{max}$ copies of each symbol $\sigma$ in $\Sigma$. Therefore, for each symbol $\sigma$ in $\Sigma$, we have a matrix $W_\sigma$ of order $t_{max} \times w_{max}$, with $(\varsigma, \iota)$-entry $W_\sigma[\varsigma][\iota] = \sigma^\iota_\varsigma = \Lambda(\sigma, \varsigma, \iota)$.

A string $w = w_1 \cdots w_\ell$ over $\Sigma$ is converted to a matrix[3] $W$ with order $t_{max} \times \ell$ of symbols from $\Sigma_b$ by the following rule

- for the $i^{th}$ occurrence $w_i = \sigma$, the $i^{th}$ column $\vec{W}_i$ of the matrix $W$ is obtained as $(\sigma^i_1 = \Lambda(\sigma, 1, i), \ldots, \sigma^i_{t_{max}} = \Lambda(\sigma, t_{max}, i))^T$. Note that all the entries in W are distinct.

A set of transitions, $\mathcal{T}$ of a DFA $\mathcal{M}$ over $\Sigma$ is converted to a set of transitions, $\mathcal{T}_b$ for DFA $\mathcal{N}$ (satisfying the restrictions of basic construction as stated in Section 3) over $\Sigma_b$ by the following rules:

- for each $\sigma \in \Sigma$, first transfer the set $Trans_\sigma$ to an another set $Trans^E_\sigma$ by enumerating the symbol $\sigma$ in each transition of $Trans_\sigma$. (Seemingly, in $Trans^E_\sigma$, all the transitions of $Trans_\sigma$ are enumerated)
- Then for each transition[4] $t = (q_x, q_y, \sigma_\varsigma) \in Trans^E_\sigma$, add the transitions $t_{\Lambda(\sigma,\varsigma,\iota)} = (q_x, q_y, \sigma^\iota_\varsigma)$ to $\mathcal{T}_b$ for each $\iota \in [w_{max}]$. ($\mathcal{T}_b$ is initially empty)

In other words, the above rules convert a DFA $\mathcal{M} = (Q, \Sigma, q_0, F, \delta)$ to a restricted DFA $\mathcal{N} = (Q, \Sigma_b, q_0, F, \delta_b)$. Note that if a string $w$ is in $\mathcal{L}(\mathcal{M})$ over $\Sigma$, then there is exactly one string $w_b$, comprising exactly one symbol from each column of the matrix $W$, is legitimate in $\mathcal{L}(\mathcal{N})$ over $\Sigma_b$ and else, for all strings $w_b$ (by picking exactly one symbol from each column of $W$), $w_b \notin \mathcal{L}(\mathcal{N})$.

$\mathsf{Setup}(\kappa)$: $(param, (\mathbb{B}_0, \mathbb{B}^*_0), (\mathbb{B}_1, \mathbb{B}^*_1), (\mathbb{B}_2, \mathbb{B}^*_2), (\mathbb{B}_3, \mathbb{B}^*_3), (\mathbb{B}_4, \mathbb{B}^*_4)) \longleftarrow \mathcal{G}_{ob}(1^\lambda, 5, 14, 14, 14, 5)$

$\widehat{\mathbb{B}}_j := (\ \vec{b}_{j,1}, \vec{b}_{j,3}, \vec{b}_{j,5})$, $\quad \widehat{\mathbb{B}}^*_j := (\ \vec{b}^*_{j,1}, \vec{b}^*_{j,3}, \vec{b}^*_{j,4}\ )$ for j=0,4

$\widehat{\mathbb{B}}_j := (\ \vec{b}_{j,1} \ldots, \vec{b}_{j,4}, \vec{b}_{j,11}, \vec{b}_{j,12}\ )$, $\quad \widehat{\mathbb{B}}^*_j := (\ \vec{b}^*_{j,1}, \ldots, \vec{b}^*_{j,4}, \vec{b}^*_{j,13}, \vec{b}^*_{j,14}\ )$ for j=1,2,3

Choose a set, alphabet of symbols $\Sigma = \{\sigma_1, \ldots, \sigma_d\} \subseteq \mathbb{F}_q$, where $d = poly(\kappa)$. The public parameters and master secret are given by

$\mathcal{PP} := (\Sigma, param, \ \{\widehat{\mathbb{B}}_j\}_{j=0,1,2,3,4})$,

$\mathcal{MSK} := (\{\widehat{\mathbb{B}}^*_j\}_{j=0,1,2,3,4})$.

[3]For each occurrence of symbol $w_i = \sigma$ in $w$, we have $t_{max}$ copies of that symbol $\sigma$ in $i^{th}$ column of the matrix $W$.

[4]Note that all the transitions have a common symbol $\sigma$ in $Trans_\sigma$, but in $Trans^E_\sigma$, $\sigma$ is enumerated as $\sigma_\varsigma$ to make all copies of $\sigma$ distinct.

Remark : $\Sigma_b$ is not given in $\mathcal{PP}$, since it can be computed using the public function $\Lambda : \Sigma \times [t_{max}] \times [w_{max}] \to \mathbb{F}_q$. The variable $h$ appearing in key and ciphertext, indicates the index of the symbol $\Lambda(\sigma, \varsigma, \iota)$ in $\Sigma_b$.

$\mathsf{Encrypt}(\mathcal{PP}, \mathcal{M} = (Q, \Sigma, q_0, F, \delta), m)$: First, obtain the restricted DFA $\mathcal{N} = (Q, \Sigma_b, q_0, F, \delta_b)$ from given DFA $\mathcal{M}$ by applying the above rules. Let $\mathcal{T}_b$ be the set of transition for $\delta_b$. For each $q_x \in Q$, pick $d_x \xleftarrow{U} \mathbb{F}_q$. For each $q_z \in F$, choose $\phi_z \xleftarrow{U} \mathbb{F}_q$. For each transition $t_{\Lambda(\sigma,\varsigma,\iota)} = (q_x, q_y, \sigma_\varsigma^\iota = \Lambda(\sigma, \varsigma, \iota)) \in \mathcal{T}_b$, choose $s_{t_{\Lambda(\sigma,\varsigma,\iota)}}, \delta_{t_{\Lambda(\sigma,\varsigma,\iota)},1}, \delta_{t_{\Lambda(\sigma,\varsigma,\iota)},2}, \delta_{t_{\Lambda(\sigma,\varsigma,\iota)},3} \xleftarrow{U} \mathbb{F}_q$, $\vec{\phi}_{t_{\Lambda(\sigma,\varsigma,\iota)},1}$, $\vec{\phi}_{t_{\Lambda(\sigma,\varsigma,\iota)},2}$, $\vec{\phi}_{t_{\Lambda(\sigma,\varsigma,\iota)},3} \xleftarrow{U} \mathbb{F}_q^2$. Pick random $\xi \in \mathbb{F}_q$. Now, compute

$$\vec{C}_0 := (\ d_0,\ 0,\ \xi,\ 0,\ \phi_0)\mathbb{B}_0 \quad C_m := m.g_T^\xi$$

For each transition $t_{\Lambda(\sigma,\varsigma,\iota)} = (q_x, q_y, \sigma_\varsigma^\iota = \Lambda(\sigma, \varsigma, \iota)) \in \mathcal{T}_b$, compute

$$\vec{C}_{t_{\Lambda(\sigma,\varsigma,\iota)},1} := (\ \overbrace{\delta_{t_{\Lambda(\sigma,\varsigma,\iota)},1}(1,h)}^{2},\ \overbrace{(s_{t_{\Lambda(\sigma,\varsigma,\iota)}} + d_y)(1, \sigma_\varsigma^\iota = \Lambda(\sigma,\varsigma,\iota))}^{2},\ \overbrace{0^6}^{6},\ \overbrace{0^2}^{2},\ \overbrace{\vec{\phi}_{t_{\Lambda(\sigma,\varsigma,\iota)},1}}^{2}\ )\ \mathbb{B}_1$$

$$\vec{C}_{t_{\Lambda(\sigma,\varsigma,\iota)},2} := (\ \overbrace{\delta_{t_{\Lambda(\sigma,\varsigma,\iota)},2}(1,h)}^{2},\ \overbrace{(-s_{t_{\Lambda(\sigma,\varsigma,\iota)}} + d_x)(1, \sigma_\varsigma^\iota = \Lambda(\sigma,\varsigma,\iota))}^{2},\ \overbrace{0^6}^{6},\ \overbrace{0^2}^{2},\ \overbrace{\vec{\phi}_{t_{\Lambda(\sigma,\varsigma,\iota)},2}}^{2}\ )\ \mathbb{B}_2$$

$$\vec{C}_{t_{\Lambda(\sigma,\varsigma,\iota)},3} := (\ \overbrace{\delta_{t_{\Lambda(\sigma,\varsigma,\iota)},3}(1,h)}^{2},\ \overbrace{s_{t_{\Lambda(\sigma,\varsigma,\iota)}}(1, \sigma_\varsigma^\iota = \Lambda(\sigma,\varsigma,\iota))}^{2},\ \overbrace{0^6}^{6},\ \overbrace{0^2}^{2},\ \overbrace{\vec{\phi}_{t_{\Lambda(\sigma,\varsigma,\iota)},3}}^{2}\ )\ \mathbb{B}_3$$

For each $q_z \in F$, compute the ciphertext component

$$\vec{C}_{z,4} := (\ d_z,\ 0,\ 0,\ 0,\ \phi_z)\mathbb{B}_4$$

$$\mathcal{C}_{\mathcal{M}} := (\ \mathcal{M},\ C_m,\ \vec{C}_0,\ \{\vec{C}_{t_{\Lambda(\sigma,\varsigma,\iota)},1},\ \vec{C}_{t_{\Lambda(\sigma,\varsigma,\iota)},2},\ \vec{C}_{t_{\Lambda(\sigma,\varsigma,\iota)},3}\}_{t_{\Lambda(\sigma,\varsigma,\iota)} = (q_x, q_y, \sigma_\varsigma^\iota = \Lambda(\sigma,\varsigma,\iota)) \in \mathcal{T}_b},\ \{\vec{C}_{z,4}\}_{q_z \in F})$$

$\mathsf{KeyGen}(\mathcal{MSK}, w = w_1 \cdots w_\ell)$: Convert this string $w$ to the matrix $W$ of order $t_{max} \times \ell$ by aforesaid law, i.e., if $w_i = \sigma$ is the $i^{th}$ occurrence in the string $w$, the $i^{th}$ column of the matrix W is $(\sigma_1^i = \Lambda(\sigma, 1, i), \ldots, \sigma_{t_{max}}^i = \Lambda(\sigma, t_{max}, i))^T$. For each symbol $\Lambda(\sigma, \varsigma, i)$ of $W$, choose $\mu_{\Lambda(\sigma,\varsigma,i),1}$, $\mu_{\Lambda(\sigma,\varsigma,i),2}$, $\mu_{\Lambda(\sigma,\varsigma,i),3}, \theta_{\Lambda(\sigma,\varsigma,i)} \xleftarrow{U} \mathbb{F}_q$, $\vec{\eta}_{\Lambda(\sigma,\varsigma,i),1}, \vec{\eta}_{\Lambda(\sigma,\varsigma,i),2}, \vec{\eta}_{\Lambda(\sigma,\varsigma,i),3} \xleftarrow{U} \mathbb{F}_q^2$. For each $i \in [\ell] \cup \{0\}$, pick $r_i \xleftarrow{U} \mathbb{F}_q$. Also choose $\eta_0, \eta_{\ell+1} \xleftarrow{U} \mathbb{F}_q$. Now compute

$$\vec{K}_0^* := (\ r_0,\ 0,\ 1,\ \eta_0,\ 0)\mathbb{B}_0^*$$

For each symbol $\sigma_\varsigma^i = \Lambda(\sigma, \varsigma, i)$ of the matrix $W$, compute

$$\vec{K}^*_{\Lambda(\sigma,\varsigma,i),1} := (\ \overbrace{\mu_{\Lambda(\sigma,\varsigma,i),1}(h,-1)}^{2},\ \overbrace{r_i + \theta_{\Lambda(\sigma,\varsigma,i)}\sigma_\varsigma^i,\quad -\theta_{\Lambda(\sigma,\varsigma,i)}}^{2},\ \overbrace{0^6}^{6},\ \overbrace{\vec{\eta}_{\Lambda(\sigma,\varsigma,i),1}}^{2},\ \overbrace{0^2}^{2}\ )\ \mathbb{B}_1^*$$

$$\vec{K}^*_{\Lambda(\sigma,\varsigma,i),2} := (\ \overbrace{\mu_{\Lambda(\sigma,\varsigma,i),2}(h,-1)}^{2},\ \overbrace{-r_{i-1} + \theta_{\Lambda(\sigma,\varsigma,i)}\sigma_\varsigma^i,\quad -\theta_{\Lambda(\sigma,\varsigma,i)}}^{2},\ \overbrace{0^6}^{6},\ \overbrace{\vec{\eta}_{\Lambda(\sigma,\varsigma,i),2}}^{2},\ \overbrace{0^2}^{2}\ )\ \mathbb{B}_2^*$$

$$\vec{K}^*_{\Lambda(\sigma,\varsigma,i),3} := (\ \overbrace{\mu_{\Lambda(\sigma,\varsigma,i),3}(h,-1)}^{2},\ \overbrace{-r_i - r_{i-1} + \theta_{\Lambda(\sigma,\varsigma,i)}\sigma_\varsigma^i,\ -\theta_{\Lambda(\sigma,\varsigma,i)}}^{2},\ \overbrace{0^6}^{6},\ \overbrace{\vec{\eta}_{\Lambda(\sigma,\varsigma,i),3}}^{2},\ \overbrace{0^2}^{2}\ )\ \mathbb{B}_3^*$$

$$\vec{K}^*_{\ell+1,4} := (\ r_\ell,\ 0,\ 0,\ \eta_{\ell+1},\ 0)\mathbb{B}_4^*$$

The secret key for the string $w$ is given by

$$SK_w := \big(w, \vec{K}_0^*,\ \{\vec{K}^*_{\Lambda(\sigma,\varsigma,i),1},\ \vec{K}^*_{\Lambda(\sigma,\varsigma,i),2},\ \vec{K}^*_{\Lambda(\sigma,\varsigma,i),3}\}_{i \in [\ell],\ \varsigma \in [t_{max}]}, \vec{K}^*_{\ell+1,4}\big)$$

$\mathsf{Decrypt}(C_{\mathcal{M}}, SK_w)$: Suppose the DFA $\mathcal{M}$ accepts the string $w = w_1 \cdots w_\ell$, then there exist a sequence of $\ell + 1$ states $q_{x_0}, q_{x_1}, q_{x_2}, \ldots, q_{x_\ell}$ and transitions $t_1, \ldots, t_\ell$, where $x_0 = 0$ and $q_{x_\ell} \in F$ and for $i = 1, 2, \ldots, \ell$, we have $t_i = (q_{x_{i-1}}, q_{x_i}, \sigma) \in \mathcal{T}$ with $w_i = \sigma$. First, compute the initial value

$$A_0 = e(\vec{C}_0,\ \vec{K}_0^*) = g_T^{r_0 d_0 + \xi}$$

For each transition[5] $t_i = (q_{x_{i-1}}, q_{x_i}, \sigma = \sigma_\varsigma) \in \mathcal{T}$, there are $w_{max}$ many transitions $t_{\Lambda(\sigma,\varsigma,\iota)} = (q_{x_{i-1}}, q_{x_i}, \sigma_\varsigma^\iota =$

[5]Here, $\varsigma$ indicates that $t_i$ is the $\varsigma^{th}$ transition in $Trans_\sigma^E$. If $i$ is changed then $\varsigma$ will change accordingly. In computation of

$\Lambda(\sigma, \varsigma, \iota))$ in $\mathcal{T}_b$ for $\iota \in [w_{max}]$. Also, for each occurrence $w_i = \sigma$ in $w$, there are $t_{max}$ many symbols represented as the column vector $\vec{W}_i = (\sigma_1^i = \Lambda(\sigma, 1, i), \ldots, \sigma_{t_{max}}^i = \Lambda(\sigma, t_{max}, i))^T$.

To get the success in decryption, we have to choose an unique $\ell$ length sequence of transitions from $\mathcal{T}_b$ and an unique $\ell$ length string $w_b$ from the matrix $W$. The $i^{th}$ candidate of above is the pair $< i^{th}\ transition, i^{th}\ bit\ of\ w_b >$, obtained by choosing a transition $t_{\Lambda(\sigma,\varsigma,\iota)}$ from $\{t_{\Lambda(\sigma,\varsigma,\iota)} = (q_{x_{i-1}}, q_{x_i}, \sigma_\varsigma^\iota = \Lambda(\sigma, \varsigma, \iota)) : \iota \in [w_{max}]\}$ and a symbol $\Lambda(\sigma, \jmath, i)$ from $\vec{W}_i = (\sigma_1^i = \Lambda(\sigma, 1, i), \ldots, \sigma_{t_{max}}^i = \Lambda(\sigma, t_{max}, i))^T$ such that $i^{th}$ symbol of $w_b$ is equal to the symbol of $i^{th}$ candidate transition, i.e., we have $< t_{\Lambda(\sigma,\varsigma,i)}, w_{b,i} = \Lambda(\sigma, \varsigma, i) >$. Therefore, to compute $A_i$ for $i \in [\ell]$, we use the ciphertext and key components corresponding to the transition $t_{\Lambda(\sigma,\varsigma,i)}$ and symbol $\Lambda(\sigma, \varsigma, i)$ respectively. Compute the first value $A_1$ of intermediate values as

$$A_1 = e(\vec{C}_{t_{\Lambda(\sigma,\varsigma,1)},1},\ \vec{K}^*_{\Lambda(\sigma,\varsigma,1),1}).e(\vec{C}_{t_{\Lambda(\sigma,\varsigma,1)},2},\ \vec{K}^*_{\Lambda(\sigma,\varsigma,1),2}).e(\vec{C}_{t_{\Lambda(\sigma,\varsigma,1)},3},\ \vec{K}^*_{\Lambda(\sigma,\varsigma,1),3}) = g_T^{r_1 d_{x_1} - r_0 d_0}$$

Next, compute the intermediate values $A_i$ (for $i = 2, \ldots, \ell$) as follows:

$$\begin{aligned} A_i &= A_{i-1}.e(\vec{C}_{t_{\Lambda(\sigma,\varsigma,i)},1},\ \vec{K}^*_{\Lambda(\sigma,\varsigma,i),1}).e(\vec{C}_{t_{\Lambda(\sigma,\varsigma,i)},2},\ \vec{K}^*_{\Lambda(\sigma,\varsigma,i),2}).e(\vec{C}_{t_{\Lambda(\sigma,\varsigma,i)},3},\ \vec{K}^*_{\Lambda(\sigma,\varsigma,i),3}) \\ &= g_T^{r_{i-1} d_{x_{i-1}} - r_0 d_0}\, g_T^{r_i d_{x_i} - r_{i-1} d_{x_{i-1}}} = g_T^{r_i d_{x_i} - r_0 d_0} \end{aligned}$$

Similarly, the $\ell^{th}$ intermediate value has of the form: $A_\ell = g_T^{r_\ell d_{x_\ell} - r_0 d_0}$
The final value $A_{\ell+1}$ is computed as

$$A_{\ell+1} = A_\ell.e(\vec{C}_{x_\ell,4},\ \vec{K}^*_{\ell+1,4}) = g_T^{r_\ell d_{x_\ell} - r_0 d_0}\, g_T^{-r_\ell d_{x_\ell}} = g_T^{-r_0 d_0}$$

Using $A_0, A_{\ell+1}$ and $C_m$, the message is unmasked as $m = C_m/(A_0\ A_{\ell+1})$.

**Theorem 5.1.** *The proposed Full CP-FE scheme is adaptively secure under the DLIN assumption.*

*Proof.* Since each entry of $W$ is distinct and there is at most a single transition of $\mathcal{T}_b$ corresponding to each symbol in $\Sigma_b$, proof of this theorem is follows from theorem 4.1. □

# References


[ALdP11] Nuttapong Attrapadung, Benot Libert, and Elie de Panafieu. Expressive key-policy attribute-based encryption with constant-size ciphertexts. In *Public Key Cryptography*, pages 90–108, 2011.

[BH08] Dan Boneh and Mike Hamburg. Generalized identity-based and broadcast encryption schemes. In *ASIACRYPT*, pages 455–470, 2008.

[BSW07] John Bethencourt, Amit Sahai, and Brent Waters. Ciphertext-policy attribute-based encryption. In *IEEE Symposium on Security and Privacy*, pages 321–334. IEEE Computer Society, 2007.

[BSW11] Dan Boneh, Amit Sahai, and Brent Waters. Functional encryption: Definitions and challenges. In Yuval Ishai, editor, *TCC*, volume 6597 of *Lecture Notes in Computer Science*, pages 253–273. Springer, 2011.

[BW07] Dan Boneh and Brent Waters. Conjunctive, subset, and range queries on encrypted data. In *TCC*, pages 535–554, 2007.

[GPSW06] Vipul Goyal, Omkant Pandey, Amit Sahai, and Brent Waters. Attribute-based encryption for fine-grained access control of encrypted data. In Ari Juels, Rebecca N. Wright, and Sabrina De Capitani di Vimercati, editors, *ACM Conference on Computer and Communications Security*, pages 89–98. ACM, 2006.

[Ham11] Mike Hamburg. Spatial encryption. Cryptology ePrint Archive, Report 2011/389, 2011. `http://eprint.iacr.org/`.

[IP08] Vincenzo Iovino and Giuseppe Persiano. Hidden-vector encryption with groups of prime order. In *Pairing*, pages 75–88, 2008.


$A_1$ and $A_i$, we use the same $\sigma$ and $\varsigma$ to reduce the complication of indexing. Note that if $i$ changes, $\sigma$ and $\varsigma$ change accordingly

[KSW08] Jonathan Katz, Amit Sahai, and Brent Waters. Predicate encryption supporting disjunctions, polynomial equations, and inner products. In Nigel P. Smart, editor, *EUROCRYPT*, volume 4965 of *Lecture Notes in Computer Science*, pages 146–162. Springer, 2008.

[LOS+10] Allison B. Lewko, Tatsuaki Okamoto, Amit Sahai, Katsuyuki Takashima, and Brent Waters. Fully secure functional encryption: Attribute-based encryption and (hierarchical) inner product encryption. In Henri Gilbert, editor, *EUROCRYPT*, volume 6110 of *Lecture Notes in Computer Science*, pages 62–91. Springer, 2010.

[LW12] Allison Lewko and Brent Waters. New proof methods for attribute-based encryption: Achieving full security through selective techniques. In Safavi-Naini and Canetti [SNC12], pages 180–198.

[OSW07] Rafail Ostrovsky, Amit Sahai, and Brent Waters. Attribute-based encryption with non-monotonic access structures. In Peng Ning, Sabrina De Capitani di Vimercati, and Paul F. Syverson, editors, *ACM Conference on Computer and Communications Security*, pages 195–203. ACM, 2007.

[OT09] Tatsuaki Okamoto and Katsuyuki Takashima. Hierarchical predicate encryption for inner-products. In Mitsuru Matsui, editor, *ASIACRYPT*, volume 5912 of *Lecture Notes in Computer Science*, pages 214–231. Springer, 2009.

[OT10] Tatsuaki Okamoto and Katsuyuki Takashima. Fully secure functional encryption with general relations from the decisional linear assumption. In Tal Rabin, editor, *CRYPTO*, volume 6223 of *Lecture Notes in Computer Science*, pages 191–208. Springer, 2010.

[OT11] Tatsuaki Okamoto and Katsuyuki Takashima. Adaptively attribute-hiding (hierarchical) inner-product encryption. Cryptology ePrint Archive, Report 2011/543, 2011. `http://eprint.iacr.org/`.

[OT12a] Tatsuaki Okamoto and Katsuyuki Takashima. Adaptively attribute-hiding (hierarchical) inner product encryption. In *EUROCRYPT*, pages 591–608, 2012.

[OT12b] Tatsuaki Okamoto and Katsuyuki Takashima. Fully secure unbounded inner-product and attribute-based encryption. In *ASIACRYPT*, pages 349–366, 2012.

[Ram13] Somindu C. Ramanna. Dfa-based functional encryption: Adaptive security from dual system encryption. Cryptology ePrint Archive, Report 2013/638, 2013. `http://eprint.iacr.org/`.

[SF07] Ryuichi Sakai and Jun Furukawa. Identity-based broadcast encryption. Cryptology ePrint Archive, Report 2007/217, 2007. `http://eprint.iacr.org/`.

[SNC12] Reihaneh Safavi-Naini and Ran Canetti, editors. *Advances in Cryptology - CRYPTO 2012 - 32nd Annual Cryptology Conference, Santa Barbara, CA, USA, August 19-23, 2012. Proceedings*, volume 7417 of *Lecture Notes in Computer Science*. Springer, 2012.

[SW05] Amit Sahai and Brent Waters. Fuzzy identity-based encryption. In Ronald Cramer, editor, *EUROCRYPT*, volume 3494 of *Lecture Notes in Computer Science*, pages 457–473. Springer, 2005.

[SW08] Elaine Shi and Brent Waters. Delegating capabilities in predicate encryption systems. In *Automata, Languages and Programming*, pages 560–578, 2008.

[Wat09] Brent Waters. Dual system encryption: Realizing fully secure IBE and HIBE under simple assumptions. In Shai Halevi, editor, *CRYPTO*, volume 5677 of *Lecture Notes in Computer Science*, pages 619–636. Springer, 2009.

[Wat11] Brent Waters. Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization. In *Public Key Cryptography*, pages 53–70, 2011.

[Wat12] Brent Waters. Functional encryption for regular languages. In Safavi-Naini and Canetti [SNC12], pages 218–235.

# A Ciphertext-Policy Functional Encryption for DFAs

## A.1 Definition

A ciphertext-policy functional encryption (CP-FE) scheme for DFAs consists of four PPT algorithms - Setup, KeyGen, Encrypt and Decrypt.

- Setup: It takes a security parameter $\kappa$, an alphabet $\Sigma$ as input, outputs the public parameters $\mathcal{PP}$ which explicitly contains $\Sigma$ and the master secret $\mathcal{MSK}$.
- KeyGen: It takes as input a string $w = w_1 w_2 \cdots w_\ell$ over $\Sigma$ and master secret $\mathcal{MSK}$ and outputs a secret key $\mathcal{SK}_w$ corresponding to $w$.
- Encrypt: takes a message $m$, the description of a DFA $\mathcal{M}$ and public parameters $\mathcal{PP}$ and returns a ciphertext $\mathcal{C}_{\mathcal{M}}$ which implicitly contains $\mathcal{M}$.
- Decrypt: It receives a ciphertext $\mathcal{C}_{\mathcal{M}}$ and secret key $\mathcal{SK}_w$ as input. If the DFA $\mathcal{M}$ accepts $w$, the algorithm returns $m$.

## A.2 Security definition of CP-FE for DFAs

The adaptive security model is defined as an indistinguishability game, $\text{Game}_{Real}$ between a challenger $\mathcal{C}$ and an adversary $\mathscr{A}$, where the adversary has to distinguish the ciphertexts under a chosen plaintext attack (CPA). The game, $\text{Game}_{Real}$ consists of the following phases:

**Setup:** The challenger $\mathcal{C}$ runs the Setup algorithm to produce the master secret key $\mathcal{MSK}$ and the public parameter $\mathcal{PP}$. Then, $\mathcal{C}$ gives $\mathcal{PP}$ to the adversary $\mathscr{A}$ and keeps $\mathcal{MSK}$ to itself.

**Phase 1:** The adversary $\mathscr{A}$ queries for the secret keys corresponding to the strings $w_1, \ldots, w_l$. The challenger $\mathcal{C}$ returns the secret keys $sk_{w_i}$ by running the KeyGen algorithm on $w_i$, for $i = 1, \ldots, l$.

**Challenge:** The adversary provides two equal length messages $m_0, m_1$ and a challenge DFA $\mathcal{M}^* = (Q^*, \Sigma, q_0^*, F^*, \delta^*)$ with the condition that the DFA $\mathcal{M}^*$ does not accept any queried string $w_i$ for $i = 1, \ldots, l$. The challenger chooses $\beta \xleftarrow{\text{U}} \{0,1\}$ and encrypts the message $m_\beta$ using the challenge DFA $\mathcal{M}^*$ and gives the challenge ciphertext $\mathcal{C}_{\mathcal{M}^*}$ to the adversary A

**Phase 2:** $\mathscr{A}$ again queries for the secret keys corresponding to the strings $w_{l+1}, \ldots, w_\nu$ with the restriction that no $w_i$ is accepted by the challenge DFA $\mathcal{M}^*$. $\mathcal{C}$ answers to the adversary $\mathscr{A}$ in similar manner as in **Phase 1**.

**Guess:** The challenger $\mathscr{A}$ outputs a bit $\beta'$.

The advantage of $\mathscr{A}$ in above game is defined by

$$\mathsf{Adv}_{\mathscr{A}}^{\text{CP}-\text{FE}}(\kappa) = \left| \Pr[\beta = \beta'] - \frac{1}{2} \right|.$$

The CP-FE scheme is said to be adaptively secure if all PPT adversary $\mathscr{A}$, the advantage $\mathsf{Adv}_{\mathscr{A}}^{\text{CP}-\text{FE}}(\kappa)$ is at most a negligible function in security parameter $\kappa$.

**Lemma A.1** ([OT10]). *For $p \in \mathbb{F}_q$, let $C_p = \{(\vec{x}, \vec{v}) | \vec{x}.\vec{v} = p\} \subset \mathbb{V} \times \mathbb{V}^*$, where $\mathbb{V}$ is n-dimensional vector spaces $\mathbb{F}_q^n$ and $\mathbb{V}^*$ its dual. For all $(\vec{x}, \vec{v}) \in C_p$, for all $(\vec{\Psi}, \vec{\Phi}) \in C_p$, $Pr[\vec{x}U = \vec{\Psi} \wedge \vec{v}Z = \vec{\Phi}] = Pr[\vec{x}Z = \vec{\Psi} \wedge \vec{v}U = \vec{\Phi}] = 1/|C_p|$, where $Z \xleftarrow{\text{U}} GL(2, \mathbb{F}_q)$, $U = (Z^{-1})^T$.*

## A.3 Proof of Lemma 4.2

We establish a PPT algorithm $\mathscr{B}$ (Simulator) who receives an instance of DSS1, $(param, \{\widehat{\mathbb{B}}_j, \widehat{\mathbb{B}}_j^*\}_{j=0,1,\ldots,4}, \{\vec{e}_\beta^{\,j}\}_{j=0,4}, \{\vec{e}_{\beta,h,\varsigma}^{\,j}\}_{h=1,\ldots,d;\ \varsigma=1,2;\ j=1,2,3})$ and depending on the distribution of $\beta$, $\mathscr{B}$ either simulates $\text{Game}_{Real}$ or $\text{Game}_0$.

**Setup:** $\mathscr{B}$ fixes an alphabet of symbols $\Sigma = \{\sigma_1, \ldots, \sigma_d\} \subseteq \mathbb{F}_q$, where $d = poly(\kappa)$. It provides $\mathcal{PP} = (\Sigma, param, \{\widehat{\mathbb{B}}_j\}_{j=0,1,2,3,4})$ to $\mathscr{A}$ and keeps $\mathcal{MSK}$ to itself.

**Key Query Answering:** $\mathscr{B}$ can handle the key queries of $\mathscr{A}$, since the $\mathcal{MSK}$ is known to him.

**Challenge:** $\mathscr{A}$ provides two equal length messages $m_0, m_1$ and challenge restricted DFA $\mathcal{M}^* = (Q^*, \Sigma, q_0^*, F^*, \delta^*)$. $\mathscr{B}$ chooses $b \xleftarrow{U} \{0,1\}$; $\tilde{d}_0, \vartheta_0, \xi \xleftarrow{U} \mathbb{F}_q$. For each state $q_x \in Q^*$, $\mathscr{B}$ picks $\tilde{d}_x, \vartheta_x \xleftarrow{U} \mathbb{F}_q$. For each transition $t = (q_x, q_y, \sigma_h) \in \mathcal{T}^*$, it chooses $\tilde{s}_t, f_t \xleftarrow{U} \mathbb{F}_q$ and encrypts $m_b$ to $\mathcal{M}^*$ as follows.

$\vec{C}_0 := \tilde{d}_0 \vec{e}^{\,0}_{\beta} + \vartheta_0 \vec{b}_{0,1} + \xi \vec{b}_{0,3}, \quad C_m := m_b . g_T^{\xi}$

For each transition $t = (q_x, q_y, \sigma_h) \in \mathcal{T}^*$, it computes
$\vec{C}_{t,1} := (\vec{e}^{\,1}_{\beta,h,1} + \sigma_h \vec{e}^{\,1}_{\beta,h,2})(\tilde{d}_y + \tilde{s}_t) + (\vartheta_y + f_t)(1,\ \sigma_h)(\vec{b}_{1,3}, \vec{b}_{1,4})$
$\vec{C}_{t,2} := (\vec{e}^{\,2}_{\beta,h,1} + \sigma_h \vec{e}^{\,2}_{\beta,h,2})(\tilde{d}_x - \tilde{s}_t) + (\vartheta_x - f_t)(1,\ \sigma_h)(\vec{b}_{2,3}, \vec{b}_{2,4})$
$\vec{C}_{t,3} := (\vec{e}^{\,3}_{\beta,h,1} + \sigma_h \vec{e}^{\,3}_{\beta,h,2})\tilde{s}_t + f_t(1,\ \sigma_h)(\vec{b}_{3,3}, \vec{b}_{3,4})$

For each $q_z \in F$, it computes
$\vec{C}_{z,4} := \tilde{d}_z \vec{e}^{\,4}_{\beta} + \vartheta_z \vec{b}_{4,1}$

$\mathscr{B}$ returns $\mathcal{C}_{\mathcal{M}^*} = (\mathcal{M}^*,\ C_m,\ \vec{C}_0,\ \{\vec{C}_{t,1},\ \vec{C}_{t,2},\ \vec{C}_{t,3}\}_{t=(q_x,q_y,\sigma_h)\in\mathcal{T}^*},\ \{\vec{C}_{z,4}\}_{q_z \in F^*})$ to $\mathscr{A}$.

**Guess:** $\mathscr{A}$ sends a guess $b'$ to $\mathscr{B}$. If $b = b'$ then $\mathscr{B}$ returns 1; otherwise it returns 0.

The simulator $\mathscr{B}$ implicitly sets $s_t = \omega \tilde{s}_t + f_t$, $d_y = \omega \tilde{d}_y + \vartheta_y$, $\widehat{s}_t = \tau \tilde{s}_t$ and $\widehat{d}_y = \tau \tilde{d}_y$. Since $\tilde{s}_t, \tilde{d}_y, f_t$ and $\vartheta_y$ are uniformly and independently[6] distributed over $\mathbb{F}_q$, so are $s_t, d_y, \widehat{s}_t$ and $\widehat{d}_y$.

It is obvious to show that if $\beta = 1$, then $\mathcal{C}_{\mathcal{M}^*}$ is properly distributed sf-type 1 ciphertext ($\text{Game}_0$), else it is properly distributed normal ciphertext ($\text{Game}_{Real}$).

## A.4 Proof of Lemma 4.3

We establish a PPT algorithm $\mathscr{B}$ to whom an instance

$(param, \{\widehat{\mathbb{B}}_j, \widehat{\mathbb{B}}^*_j\}_{j=0,1,\ldots,4}, \{\vec{\Upsilon}^j\}_{j=0,4}, \{\vec{e}^{\,j}_{h,\varsigma}\}_{h=1,\ldots,d;\ \varsigma=1,2;\ j=1,2,3},$
for $\beta = 0, 1$, $T_\beta = (\{\vec{\Upsilon}^{j*}_{\beta}\}_{j=0,4}, \{\vec{\Upsilon}^{j*}_{\beta,h,\varsigma}\}_{h=1,\ldots,d;\ \varsigma=1,2;\ j=1,2,3}))$

of DSS2 is given and it simulates either $\text{Game}_{k-1,3}$ or $\text{Game}_{k,1}$ depending on the distribution of $\beta$.

**Setup:** $\mathscr{B}$ fixes an alphabet of symbols $\Sigma = \{\sigma_1, \ldots, \sigma_d\} \subseteq \mathbb{F}_q$, where $d = poly(\kappa)$. It provides $\mathcal{PP} = (\Sigma, param, \{\widehat{\mathbb{B}}_j\}_{j=0,1,2,3,4})$ to $\mathscr{A}$ and keeps $\mathcal{MSK}$ to itself.

**Key Query Answering:** For both the games, the first $(k-1)$ keys are sf-type 3 and last $(\nu - k)$ are normal keys. For $\text{Game}_{k-1,3}$, the $k^{th}$ key is normal and it is sf-type 1 for $\text{Game}_{k,1}$. Let $w^1, \ldots, w^\nu$ be the query strings issued by $\mathscr{A}$. The simulator $\mathscr{B}$ answers the key $\mathcal{SK}_{w^\iota}$ for the string $w^\iota$ depending on $\iota$ as follows.

- If $\iota > k$, then $\mathscr{B}$ runs the $\mathsf{KeyGen}$ algorithm and gives the normal key to $\mathscr{A}$.
- If $\iota < k$, then it is sf-type 3 key. First note that the distribution of sf-type 3 key and normal key are almost the same except $\vec{K}^*_0$. $\mathscr{B}$ first generates $\mathcal{SK}_{w^\iota} \longleftarrow \mathsf{KeyGen}(\mathcal{MSK}, w^\iota)$ and then modifies the component $\vec{K}^*_0$ as shown below to obtain type 3 component $\vec{K}^*_0$

  $\vec{K}^*_0 \longleftarrow \vec{K}^*_0 + r\vec{b}^*_{0,2}$, where $r \xleftarrow{U} \mathbb{F}_q$
- If $\iota = k$ then it is either normal or sf-type 1 key. $\mathscr{B}$ generates $\mathcal{SK}_{w^k}$ using the challenge $T_\beta$ as bait from the instance of DSS2. Let $w^k = w^k_1 \cdots w^k_\ell$. For each $i \in [\ell] \cup \{0\}$, $\mathscr{B}$ picks $\varrho_i, \tilde{\theta}_i, \tilde{r}_i, \pi_i \xleftarrow{U} \mathbb{F}_q$

[6] First, note that $\vec{C}_{t,j}$ (resp. $\vec{K}^*_{i,j}$) is represented as the linear combination of 14 dimensional basis vectors $\mathbb{B}_j = (\vec{b}_{j,1}, \ldots, \vec{b}_{j,14})$ (resp. $\mathbb{B}^*_j = (\vec{b}^*_{j,1}, \ldots, \vec{b}^*_{j,14})$. In lemmas 4.2, 4.3 and 4.5, we only show that the scalars of 3rd, 4th, 5th, 6th, 9th and 10th basis vectors either in the ciphertext part or in the key part or in both are properly distributed, since the rest of the scalars are either defined to be zero or can be properly randomized by the supplied vectors from the problem.

For $i = 1, \ldots, \ell;\ \varsigma = 1, 2;\ j = 1, 2, 3$, let $w_i^k = \sigma_h$ for some index h. Then $\mathscr{B}$ defines the following

$\vec{\Delta}^{*j}_{\beta,i,\varsigma} := \pi_i \vec{\Upsilon}^{*j}_{\beta,h,\varsigma} + \tilde{\theta}_i \vec{b}^*_{j,2+\varsigma} \quad \vec{\Pi}^{*j}_{\beta,i,\varsigma} := \varrho_i \vec{\Upsilon}^{*j}_{\beta,h,1} + \tilde{r}_i \vec{b}^*_{j,3}$

The simulator $\mathscr{B}$ computes the $k^{th}$ key $\mathcal{SK}_{w^k}$ as described below

$\vec{K}^*_0 := \varrho_0 \vec{\Upsilon}^{*0}_{\beta} + \tilde{r}_0 \vec{b}^*_{0,1} + \vec{b}^*_{0,3}$

For each $i \in [\ell]$, it computes key components

$\vec{K}^*_{i,1} := \sigma_h \vec{\Delta}^{*1}_{\beta,i,1} - \vec{\Delta}^{*1}_{\beta,i,2} + \vec{\Pi}^{*1}_{\beta,i,1}$
$\vec{K}^*_{i,2} := \sigma_h \vec{\Delta}^{*2}_{\beta,i,1} - \vec{\Delta}^{*2}_{\beta,i,2} - \vec{\Pi}^{*2}_{\beta,(i-1),1}$
$\vec{K}^*_{i,3} := \sigma_h \vec{\Delta}^{*3}_{\beta,i,1} - \vec{\Delta}^{*3}_{\beta,i,2} - \vec{\Pi}^{*3}_{\beta,i,1} - \vec{\Pi}^{*3}_{\beta,(i-1),1}$

$\vec{K}^*_{\ell+1} := \tilde{\varrho}_\ell \vec{\Upsilon}^{*4}_{\beta} + \tilde{r}_\ell \vec{b}^*_{4,1}$

For each $i \in [\ell] \cup \{0\}$, $\mathscr{B}$ implicitly sets $\theta_i = \pi_i \zeta + \tilde{\theta}_i$, $r_i = \varrho_i \zeta + \tilde{r}_i$, $\widehat{\theta}_i = \pi_i \rho$ and $\widehat{r}_i = \varrho_i \rho$. Since $\tilde{\theta}_i, \tilde{r}_i, \pi_i$ and $\varrho_i$ are uniformly and independently distributed over $\mathbb{F}_q$, so are $\theta_i, r_i, \widehat{\theta}_i$ and $\widehat{r}_i$. Now, it can be easily verified that if $\beta = 0$, then $\mathcal{SK}_{w^k}$ is properly distributed normal key (in $\text{Game}_{(k-1),3}$) except that $\zeta$ defined in DSS2 is zero, i.e., except with probability 1/q. Similarly if $\beta = 1$, it is properly distributed sf-type 1 key ($\text{Game}_{k,1}$) except with probability 1/q.

**Challenge:** $\mathscr{B}$ receives two equal length messages $m_0, m_1$ and challenge restricted DFA $\mathcal{M}^* = (Q^*, \Sigma, q_0^*, F^*, \delta^*)$ from $\mathscr{A}$. $\mathscr{B}$ chooses $b \xleftarrow{U} \{0, 1\}$; $\tilde{d}_0, \vartheta_0, \xi \xleftarrow{U} \mathbb{F}_q$. For each state $q_x \in Q^*$, $\mathscr{B}$ picks $\tilde{d}_x, \vartheta_x \xleftarrow{U} \mathbb{F}_q$. For each transition $t = (q_x, q_y, \sigma_h) \in \mathcal{T}$, it chooses $\tilde{s}_t, f_t \xleftarrow{U} \mathbb{F}_q$ and encrypts $m_b$ to $\mathcal{M}^*$ as follows.

$\vec{C}_0 := \tilde{d}_0 \vec{\Upsilon}^0 + \vartheta_0 \vec{b}_{0,1} + \xi \vec{b}_{0,3}, \quad C_m := m_b . g_T^{\xi}$

For each transition $t = (q_x, q_y, \sigma_h) \in \mathcal{T}^*$, it computes

$\vec{C}_{t,1} := (\vec{e}^1_{h,1} + \sigma_h \vec{e}^1_{h,2})(\tilde{d}_y + \tilde{s}_t) + (\vartheta_y + f_t)(1,\ \sigma_h)(\vec{b}_{1,3}, \vec{b}_{1,4})$
$\vec{C}_{t,2} := (\vec{e}^2_{h,1} + \sigma_h \vec{e}^2_{h,2})(\tilde{d}_x - \tilde{s}_t) + (\vartheta_x - f_t)(1,\ \sigma_h)(\vec{b}_{2,3}, \vec{b}_{2,4})$
$\vec{C}_{t,3} := (\vec{e}^3_{h,1} + \sigma_h \vec{e}^3_{h,2})\tilde{s}_t + f_t(1,\ \sigma_h)(\vec{b}_{3,3}, \vec{b}_{3,4})$

For each $q_z \in F$, it computes

$\vec{C}_{z,4} := \tilde{d}_z \vec{\Upsilon}^4 + \vartheta_z \vec{b}_{4,1}$

$\mathscr{B}$ returns $\mathcal{C}_{\mathcal{M}^*} = (\mathcal{M}^*,\ C_m,\ \vec{C}_0,\ \{\vec{C}_{t,1},\ \vec{C}_{t,2},\ \vec{C}_{t,3}\}_{t=(q_x,q_y,\sigma_h)\in\mathcal{T}^*},\ \{\vec{C}_{z,4}\}_{q_z \in F^*})$ to $\mathscr{A}$.

In ciphertext simulation, $\mathscr{B}$ implicitly sets $s_t = \omega \tilde{s}_t + f_t$, $d_y = \omega \tilde{d}_y + \vartheta_y$, $\widehat{s}_t = \tau \tilde{s}_t$ and $\widehat{d}_y = \tau \tilde{d}_y$. Since $\tilde{s}_t, \tilde{d}_y, f_t$ and $\vartheta_y$ are uniformly and independently distributed over $\mathbb{F}_q$, so are $s_t, d_y, \widehat{s}_t$ and $\widehat{d}_y$. Therefore, $\mathcal{C}_{\mathcal{M}^*}$ is a properly distributed semi-functional ciphertext.

**Guess:** $\mathscr{A}$ returns its guess $b'$. If $b = b'$ then $\mathscr{B}$ returns 1; otherwise it returns 0.

Thus, the distribution of the keys and the challenge ciphertext is the same as that of $\text{Game}_{k-1,3}$ (resp. $\text{Game}_{k,1}$) except with probability 1/q if $\beta = 0$ (resp. $\beta = 1$).

## A.5 Proof of Lemma 4.4

The distribution of $(\mathcal{PP},\ \{\mathcal{SK}_{w^\iota}\}_{\iota=1,\ldots,\nu},\ \mathcal{C}_{\mathcal{M}^*})$ in $\text{Game}_{k,1}$ and that in $\text{Game}_{k,2}$ are exactly same except at $k^{th}$ key. We show that the joint distribution of $k^{th}$ key $\mathcal{SK}_{w^k}$ and the challenge ciphertext in both the games are equivalent. It is sufficient to show that the scalar $\widehat{r}_0$ in $\vec{K}^*_0$ of $k^{th}$ key $\mathcal{SK}_{w^k}$(described in definition of sf-type 1 key) is uniformly and independently distributed from the other variables in the joint distribution of $\mathscr{A}$'s view. Since $\widehat{r}_0$ is related to $\{\vec{\Phi}_{i,1}, \vec{\Phi}_{i,2}, \Phi_{i,3}\}_{i\in[\ell]}$ and $U_h^j = ((Z_h^j)^{-1})^T$ (for $j = 1, 2, 3$) holds, so, $\widehat{r}_0$ is only related to joint distribution of $\{\vec{\Phi}_{i,1}, \vec{\Phi}_{i,2}, \vec{\Phi}_{i,3}\}_{i\in[\ell]}$ and $\{\vec{\Psi}_{h,1}, \vec{\Psi}_{h,2}, \vec{\Psi}_{h,3}\}_{h\in\{a\ :\sigma_a = w_i^k \text{ for } i\in[\ell]\}}$, where

$\vec{\Phi}_{i,1} := (\widehat{r}_i + \widehat{\theta}_i \sigma_h, -\widehat{\theta}_i) U_h^1 \qquad \vec{\Psi}_{h,1} := (\widehat{s}_t + \widehat{d}_y)(1, \sigma_h) Z_h^1$
$\vec{\Phi}_{i,2} := (-\widehat{r}_{i-1} + \widehat{\theta}_i \sigma_h, -\widehat{\theta}_i) U_h^2 \qquad \vec{\Psi}_{h,2} := (-\widehat{s}_t + \widehat{d}_x)(1, \sigma_h) Z_h^2$
$\vec{\Phi}_{i,3} := (-\widehat{r}_i - \widehat{r}_{i-1} + \widehat{\theta}_i \sigma_h, -\widehat{\theta}_i) U_h^3 \qquad \vec{\Psi}_{h,3} := \widehat{s}_t (1, \sigma_h) Z_h^3$

For $i \in [\ell]$, $j = 1, 2, 3$, $(Z_h^j, U_h^j)$ with $w_i^k = \sigma_h$ is independent from the other variables, since each symbol $w_i^k$ in the string $w^k$ is distinct and no two transitions have a common symbol. For each $i \in [\ell]$, there are two cases

**Case Matching** : For $i^{th}$ symbol $w_i^k$ in the string $w^k$, there exist a transition $t = (q_x, q_y, \sigma_h)$ such that $w_i^k = \sigma_h$

1. By Lemma A.1, the joint distribution of $(\vec{\Psi}_{h,1}, \vec{\Phi}_{i,1})$ is uniformly and independently distributed on $C_{\widehat{r}_i(\widehat{s}_t+\widehat{d}_y)} := \{(\vec{\Psi}, \vec{\Phi}) | \vec{\Psi}.\vec{\Phi} = \widehat{r}_i(\widehat{s}_t + \widehat{d}_y)\}$ (over the choice of $Z_h^1 \xleftarrow{\text{U}} GL(2, \mathbb{F}_q)$)
2. By Lemma A.1, the joint distribution of $(\vec{\Psi}_{h,2}, \vec{\Phi}_{i,2})$ is uniformly and independently distributed on $C_{-\widehat{r}_{i-1}(-\widehat{s}_t+\widehat{d}_x)} := \{(\vec{\Psi}, \vec{\Phi}) | \vec{\Psi}.\vec{\Phi} = -\widehat{r}_{i-1}(-\widehat{s}_t + \widehat{d}_x)\}$ (over the choice of $Z_h^2 \xleftarrow{\text{U}} GL(2, \mathbb{F}_q)$)
3. By Lemma A.1, the joint distribution of $(\vec{\Psi}_{h,3}, \vec{\Phi}_{i,3})$ is uniformly and independently distributed on $C_{(-\widehat{r}_i-\widehat{r}_{i-1})\widehat{s}_t} := \{(\vec{\Psi}, \vec{\Phi}) | \vec{\Psi}.\vec{\Phi} = (-\widehat{r}_i - \widehat{r}_{i-1})\widehat{s}_t\}$ (over the choice of $Z_h^3 \xleftarrow{\text{U}} GL(2, \mathbb{F}_q)$)

Therefore, in the matching case, the adversary $\mathscr{A}$ could get the legitimate value $\widehat{r}_i\widehat{d}_y - \widehat{r}_{i-1}\widehat{d}_x$ by taking the sum of values in above three cases.

**Case Non-Matching** : For $i^{th}$ symbol $w_i^k$, for every transition $t = (q_x, q_y, \sigma_h)$ we have $w_i^k \neq \sigma_h$. Then, for $j = 1, 2, 3$, the distribution of $\vec{\Phi}_{i,j}$ is uniformly and independently distributed on $F_q^2$.

The vectors appearing in non-matching case are obviously independent of $\widehat{r}_0$. Since $\mathscr{A}$ is allowed the key query for the string $w$ with the restriction $w \notin \mathcal{L}(\mathcal{M}^*)$, we can infer that $\widehat{r}_0$ is independent from the joint distribution of $\widehat{d}_0$ and $\{\widehat{r}_i\widehat{d}_y - \widehat{r}_{i-1}\widehat{d}_x |$ $i^{th}$ symbol $w_i^k$ matches with the unique transition $t = (q_x, q_y, \sigma_h = w_i^k)\}$ (this is found in Case Matching). Therefore, $\widehat{r}_0$ is uniformly and independently distributed from the other variables in the joint distribution of $\mathscr{A}$'s view.

## A.6 Proof of Lemma 4.5

We establish a PPT algorithm $\mathscr{B}$ to whom an instance

$(param, \{\widehat{\mathbb{B}}_j, \widehat{\mathbb{B}}_j^*\}_{j=0,1,\ldots,4}, \{\vec{\Upsilon}^j\}_{j=0,4}, \{\vec{e}_{h,\varsigma}^{\,j}\}_{h=1,\ldots,d;\ \varsigma=1,2;\ j=1,2,3},$
for $\beta = 0, 1$, $T_\beta = (\{\vec{\Upsilon}_\beta^{j*}\}_{j=0,4}, \{\vec{\Upsilon}_{\beta,h,\varsigma}^{j*}\}_{h=1,\ldots,d;\ \varsigma=1,2;\ j=1,2,3}))$

of DSS2 is given and it simulates either $\text{Game}_{k,2}$ or $\text{Game}_{k,3}$ depending on the distribution of $\beta$.

Now $\mathscr{B}$ proceeds the same way as in Lemma 4.4 except the $\vec{K}_0^*$ component in $k^{th}$ key $\mathcal{SK}_{w^k}$

$$\vec{K}_0^* := \tilde{\varrho}_0\vec{\Upsilon}_\beta^{*0} + \tilde{r_0}\vec{b}_{0,1}^* + \vec{b}_{0,3}^* + \boxed{r_0'\vec{b}_{0,2}^*}, \text{ where } r_0' \xleftarrow{\text{U}} \mathbb{F}_q$$

So, the coefficient of $\vec{b}_{0,2}^*$ in $\vec{K}_0^*$ is uniformly and independently distributed over $\mathbb{F}_q$. Thus if $\beta = 1$, then $\mathcal{SK}_{w^k}$ is properly distributed sf-type 2 key ($\text{Game}_{k,2}$) except with probability 1/q, else it is properly distributed sf-type 3 key ($\text{Game}_{k,3}$) except with probability 1/q.

## A.7 Proof of Lemma 4.6

The proof is similar to that of lemma 29 in [OT12b]. Indeed, we show that the distribution of $(param, \{\widehat{\mathbb{B}}_j\}_{j=0,1,\ldots,4},\ \{\mathcal{SK}_{w^\iota}\}_{\iota=1,\ldots,\nu},\ \mathcal{C}_{\mathcal{M}^*})$ in $\text{Game}_{\nu,3}$ and that in $\text{Game}_{Final}$ are equivalent except with probability $1/q$. We define new bases $\mathbb{D}_0$ of $\mathbb{V}_0$ and $\mathbb{D}_0^*$ of $\mathbb{V}_0^*$ as follows: Choose $\theta \xleftarrow{\text{U}} \mathbb{F}_q$ and set

$$\vec{d}_{0,2} := \vec{b}_{0,2} - \theta\vec{b}_{0,3} \qquad \vec{d}_{0,3}^* := \vec{b}_{0,3}^* - \theta\vec{b}_{0,2}^*$$
$$\mathbb{D}_0 := (\vec{b}_{0,1}, \boxed{\vec{d}_{0,2}}, \vec{b}_{0,3}, \vec{b}_{0,4}, \vec{b}_{0,5}) \quad \mathbb{D}_0^* := (\vec{b}_{0,1}^*, \vec{b}_{0,2}^*, \boxed{\vec{d}_{0,3}^*}, \vec{b}_{0,4}^*, \vec{b}_{0,5}^*)$$

It is easily verified that $(\mathbb{D}_0, \mathbb{D}_0^*)$ are dual orthonormal bases and are distributed the same as the original bases, $(\mathbb{B}_0, \mathbb{B}_0^*)$. For $\iota = 1, \ldots, \nu$, $\vec{K}_0^{\iota*}$ component of the key $\mathcal{SK}_{w^\iota}$ and $\vec{C}_0$ component of the challenge ciphertext $\mathcal{C}_{\mathcal{M}^*}$ are expressed over $\mathbb{B}_0$ and $\mathbb{B}_0^*$ as

$\vec{K}_0^{\iota *} := (r_0,\ r,\ 1,\ \eta_0,\ 0)\mathbb{B}_0^* \qquad \vec{C}_0 := (d_0,\ \widehat{d}_0,\ \xi,\ 0,\ \phi_0)\mathbb{B}_0$

Then we can express these over the bases $(\mathbb{D}_0, \mathbb{D}_0^*)$ as shown below

$\vec{K}_0^{\iota *} := (r_0, \boxed{r-\theta},\ 1,\ \eta_0,\ 0)\mathbb{D}_0^* \quad \vec{C}_0 := (d_0, \widehat{d}_0,\ \boxed{\xi + \theta\widehat{d}_0},\ 0,\ \phi_0)\mathbb{D}_0$

$\vec{K}_0^{\iota *} := (r_0, r',\ 1,\ \eta_0,\ 0)\mathbb{D}_0^* \qquad \vec{C}_0 := (d_0, \widehat{d}_0, \xi',\ 0,\ \phi_0)\mathbb{D}_0$

Since $\theta$ is uniformly distributed over $\mathbb{F}_q$, so $r' = r - \theta$ and $\xi' = \xi + \theta\widehat{d}_0$ are uniformly and independently distributed over $\mathbb{F}_q$.

Therefore, the distribution of the keys and ciphertext, $(\{\mathcal{SK}_{w^\iota}\}_{\iota=1,\ldots,\nu},\ \mathcal{C}_{\mathcal{M}^*})$ is the same as that of $\mathrm{Game}_{\nu,3}$ (resp. $\mathrm{Game}_{Final}$) over the bases $(\mathbb{B}_0, \mathbb{B}_0^*)$ (resp. $(\mathbb{D}_0, \mathbb{D}_0^*)$). Thus two games $\mathrm{Game}_{\nu,3}$ and $\mathrm{Game}_{Final}$ are equivalent from $\mathscr{A}$'s view if $\widehat{d}_0 \neq 0$, i.e., except with probability $1/q$.

# B Reduction of DSS1 and DSS2 from DLIN

The assumption, 1-ABE in [OT12b], consists of the vectors computed over a dual bases $(\mathbb{B}_0, \mathbb{B}_0^*)$ of dimension 5 and another dual bases $(\mathbb{B}_1, \mathbb{B}_1^*)$ of dimension 14. There are (1+2d) many vectors in 1-ABE, of which, one is 5-dimensional vector, $\vec{e}_{\beta,0}$, computed by the basis $\mathbb{B}_0$ and others are 14-dimensional vectors $\{\vec{e}_{\beta,t,i}\}_{t=1,\ldots,d;\ i=1,2}$, constructed using the basis $\mathbb{B}_1$. These (1+2d) many vectors either belong to a class $\beta = 0$ or belong to another class $\beta = 1$. So, the task of an adversary $\mathscr{A}$ is to classify these (1+2d) many vectors, i.e., to guess $\beta \in \{0,1\}$. All these vectors are connected via a common variable $\omega$ (and $\tau$ if $\beta = 1$). If $\beta = 1$, then, for $t = 1, \ldots, d;\ i = 1, 2$, the $9^{th}$ and $10^{th}$ scalars in the vector $\vec{e}_{t,i}$ (while expressing over the basis $\mathbb{B}_1$) are randomized by $Z_t$, where $Z_t \xleftarrow{\mathrm{U}} GL(2, \mathbb{F}_q)$.

But, in DSS1, we consider two 5-dimensional dual bases $(\mathbb{B}_j, \mathbb{B}_j^*)$ for $j = 0, 4$ and three 14-dimensional dual bases $(\mathbb{B}_j, \mathbb{B}_j^*)$ for $j = 1, 2, 3$. The assumption, DSS1 consists of two 5-dimensional vectors $\vec{e}_\beta^{\,j}$ for $j = 0, 4$ and 6d many 14-dimensional vectors $\vec{e}_{\beta,t,i}^{\,j}$, i.e., for each $t = 1, \ldots, d;\ i = 1, 2$, there are three vectors $\vec{e}_{\beta,t,i}^{\,j}$ for $j = 1, 2, 3$. As usual, all these vectors $\{\vec{e}_\beta^{\,j}\}_{j=0,4}$ and $\{\vec{e}_{\beta,t,i}^{\,j}\}_{t=1,\ldots,d;\ j=1,2,3;\ i=1,2}$ are connected via a common variable $\omega$ (and $\tau$ if $\beta = 1$). If $\beta = 1$, then, for $t = 1, \ldots, d;\ j = 1, 2, 3$, the $9^{th}$ and $10^{th}$ scalars in the vector $\vec{e}_{\beta,t,i}^{\,j}$ (when expressed as a combination of basis vectors in $\mathbb{B}_j$) are randomized by $Z_t^j$, where $Z_t^j \xleftarrow{\mathrm{U}} GL(2, \mathbb{F}_q)$. So, it is obvious that 1-ABE is weaker assumption than DSS1 assumption. Note that $Z_t^j$'s are independent for $j = 1, 2, 3$. Due to this independence, we could not deduce DSS1 from 1-ABE by employing the usual transformations $W_j$ and $((W_j)^{-1})^T$ respectively over the bases $\mathbb{B}_j$ and $\mathbb{B}_j^*$ for $j = 0, \ldots, 4$, where $W_j \xleftarrow{\mathrm{U}} GL(5, \mathbb{F}_q)$ for $j = 0, 4$ and $W_j \xleftarrow{\mathrm{U}} GL(14, \mathbb{F}_q)$ for $j = 1, 2, 3$.

The assumption, 2-ABE in [OT12b], consists of (1+2d) many vectors $\vec{e}_{1,0}, \{\vec{e}_{1,t,i}\}_{t=1,\ldots,d;\ i=1,2}$ (i.e., $\beta = 1$ instance of 1-ABE) expressed over the bases $\mathbb{B}_0, \mathbb{B}_1$ and (1+2d) many vectors $\vec{h}^*_{\beta,0}, \{\vec{h}^*_{\beta,t,i}\}_{t=1,\ldots,d;\ i=1,2}$ over the bases $\mathbb{B}_0^*, \mathbb{B}_1^*$. The task of the adversary is to guess $\beta \in \{0,1\}$. The later (1+2d) many vectors, $\vec{h}^*_{\beta,0}$ and $\vec{h}^*_{\beta,t,i}$'s are connected via a common variable $\zeta$ (and $\rho$ if $\beta = 1$). Likewise, if $\beta = 1$, then, for $t = 1, \ldots, d;\ i = 1, 2$, the $9^{th}$ and $10^{th}$ scalars in the vector $\vec{e}_{t,i}$ (while expressing over the basis $\mathbb{B}_1^*$) are randomized by $U_t$, where $Z_t \xleftarrow{\mathrm{U}} GL(2, \mathbb{F}_q)$ and $U_t = (Z_t^{-1})^T$.

Similarly, DSS2 consists of the vectors expressed over the 5-dimensional dual bases $(\mathbb{B}_j, \mathbb{B}_j^*)$ for $j = 0, 4$ and 14-dimensional dual bases $(\mathbb{B}_j, \mathbb{B}_j^*)$ for $j = 1, 2, 3$. There are (4+12d) many vectors $\{\vec{e}^{\,j}, \vec{h}_\beta^{\,j*}\}_{j=0,4}$ and $\{\vec{e}_{t,i}^{\,j}, \vec{h}_{\beta,t,i}^{\,j*}\}_{t=1,\ldots,d;\ i=1,2;\ j=1,2,3}$ and the task of $\mathscr{A}$ is to guess $\beta \in \{0,1\}$. For $t = 1, \ldots, d;\ j = 1, 2, 3$, let $Z_t^j \xleftarrow{\mathrm{U}} GL(2, \mathbb{F}_q)$ and set $U_t^j := ((Z_t^j)^{-1})^T$. Then, the $9^{th}$ and $10^{th}$ scalars in the vector $\vec{e}_{t,i}^{\,j}$ (when it is expressed over the basis $\mathbb{B}_j$) are randomized by the matrix $Z_t^j$ and those in $\vec{h}_{\beta,t,i}^{\,j*}$ (over the basis $\mathbb{B}_j^*$) are randomized by $U_t^j$, where for $t = 1, \ldots, d;\ j = 1, 2, 3$, $Z_t^j \xleftarrow{\mathrm{U}} GL(2, \mathbb{F}_q)$ and $U_t^j := ((Z_t^j)^{-1})^T$. Similarly, as discussed above, 2-ABE assumption is weaker than DSS2 assumption and we are unable to deduce DSS2 from 2-ABE.

In [OT12b], 1-ABE (2-ABE) was shown to be intractable under DLIN assumption by defining 1-ABE (2-ABE) as a hybrid of some experiments, where first (resp. final) experiment was defined to be the $\beta = 0$ (resp. $\beta = 1$) case of 1-ABE (2-ABE). The first experiment ($\mathsf{Exp}$ 0) and final experiment ($\mathsf{Exp}$ 2-d-2-2 if 1-ABE and $\mathsf{Exp}$ 2-d-8 if 2-ABE) were shown to be indistinguishable under some intermediate basic problems. Our approach for proving

intractability of DSS1 and DSS2 under DLIN assumption follows the same proof technique of above but we change the intermediate basic problems to "modified" basic problems and then apply these modified basic problems (MBP) to show that the neighboring experiments are equivalent from $\mathscr{A}$'s point of view.

Some intermediate basic problems of [OT12b] described here, may not be using in the reduction of DSS1 and DSS2 but, are still given to differentiate these intermediate basic problems from the modified basic problems.

## B.1 Reduction of DSS1 from DLIN

**Definition B.1.** For $(t_1, i_1), (t_2, i_2) \in \mathbb{N}^2$, we define

$$(t_1, i_1) < (t_2, i_2) \Longleftrightarrow (t_1 < t_2) \textit{ or } (t_1 = t_2 \textit{ and } i_1 < i_2)$$

$$(t_1, i_1) > (t_2, i_2) \Longleftrightarrow (t_2, i_2) < (t_1, i_1)$$

**Definition B.2** (Basic Problem 1 in [OT12b])**.** Choose $\phi_0, \omega \xleftarrow{\text{U}} \mathbb{F}_q$ and $\tau \xleftarrow{\text{U}} \mathbb{F}_q^{\times}$.

$$(param, (\mathbb{B}_0, \mathbb{B}_0^*), (\mathbb{B}, \mathbb{B}^*)) \longleftarrow \mathcal{G}_{ob}(\kappa, 5, 14)$$

$$\widehat{\mathbb{B}}_0^* := (\vec{b}_{0,1}^*,\ \vec{b}_{0,3}^*, \ldots, \vec{b}_{0,5}^*) \qquad \widehat{\mathbb{B}}^* := (\vec{b}_1^*, \ldots, \vec{b}_4^*,\ \vec{b}_7^*, \ldots, \vec{b}_{14}^*)$$

$$\vec{e}_0^{\,0} := (\omega,\ 0,\ 0,\ 0,\ \phi_0)\mathbb{B}_0,\ \vec{e}_1^{\,0} := (\omega,\ \tau,\ 0,\ 0,\ \phi_0)\mathbb{B}_0$$

For $i = 1, 2$, choose $\phi_{i,1}, \phi_{i,2} \xleftarrow{\text{U}} \mathbb{F}_q$

$$\vec{e}_{0,i} := \quad ( \quad \overbrace{0^2, \omega\vec{e}_i}^{4}, \quad \overbrace{0^6}^{6}, \quad \overbrace{0^2}^{2}, \quad \overbrace{\phi_{i,1}, \phi_{i,2}}^{2} \quad )\mathbb{B}$$

$$\vec{e}_{1,i} := \quad ( \quad \overbrace{0^2, \omega\vec{e}_i}^{4}, \quad \overbrace{\tau\vec{e}_i, 0^4}^{6}, \quad \overbrace{0^2}^{2}, \quad \overbrace{\phi_{i,1}, \phi_{i,2}}^{2} \quad )\mathbb{B}$$

$D := (param, \mathbb{B}_0, \widehat{\mathbb{B}}_0^*, \mathbb{B}, \widehat{\mathbb{B}}^*)$ For $\beta = 0, 1,$ define $T_\beta := (\vec{e}_\beta^{\,0}, \{\vec{e}_{\beta,i}\}_{i=1,2})$

Now, the advantage of an algorithm $\mathscr{A}$ in breaking this Basic Problem 1 (BP1) is defined by

$$\mathsf{Adv}_{\mathscr{A}}^{\text{BP1}}(\kappa) = |Pr[\mathscr{A}(D, T_0) = 1] - Pr[\mathscr{A}(D, T_1) = 1]|$$

The BP1 assumption holds if for all PPT adversary $\mathscr{A}$, the advantage $\mathsf{Adv}_{\mathscr{A}}^{\text{BP1}}(\kappa)$ is a negligible function in security parameter $\kappa$.

**Lemma B.1** (lemma 34 in [OT12b])**.** *For any adversary $\mathscr{A}$, there exist a PPT algorithm $\mathscr{B}$, such that* $\mathsf{Adv}_{\mathscr{A}}^{\text{BP1}}(\kappa) \leq \mathsf{Adv}_{\mathscr{B}}^{\text{DLIN}}(\kappa) + 5/q$*, for all $\kappa$.*

**Definition B.3** (**Modified Basic Problem 1**)**.** Choose $\phi_0^0, \phi_0^4, \omega \xleftarrow{\text{U}} \mathbb{F}_q$ and $\tau \xleftarrow{\text{U}} \mathbb{F}_q^{\times}$.

$$(param, (\mathbb{B}_0, \mathbb{B}_0^*), (\mathbb{B}_1, \mathbb{B}_1^*), (\mathbb{B}_2, \mathbb{B}_2^*), (\mathbb{B}_3, \mathbb{B}_3^*), (\mathbb{B}_4, \mathbb{B}_4^*)) \longleftarrow \mathcal{G}_{ob}(\kappa, 5, 14, 14, 14, 5)$$

$$\widehat{\mathbb{B}}_\iota^* := (\vec{b}_{\iota,1}^*,\ \vec{b}_{\iota,3}^*, \ldots, \vec{b}_{\iota,5}^*) \ \textit{ for } \iota = 0, 4; \qquad \widehat{\mathbb{B}}_j^* := (\vec{b}_{j,1}^*, \ldots, \vec{b}_{j,4}^*,\ \vec{b}_{j,7}^*, \ldots, \vec{b}_{j,14}^*) \ \textit{ for } j = 1, 2, 3$$

$$\vec{e}_0^{\,\iota} := (\omega,\ 0,\ 0,\ 0,\ \phi_0^\iota)\mathbb{B}_\iota,\ \vec{e}_1^{\,\iota} := (\omega,\ \tau,\ 0,\ 0,\ \phi_0^\iota)\mathbb{B}_\iota \text{ for } \iota = 0, 4$$

For $i = 1, 2,\ j = 1, 2, 3$, choose $\phi_{i,1}^j, \phi_{i,2}^j \xleftarrow{\text{U}} \mathbb{F}_q$

$$\vec{e}_{0,i}^{\,j} := \quad ( \quad \overbrace{0^2, \omega\vec{e}_i}^{4}, \quad \overbrace{0^6}^{6}, \quad \overbrace{0^2}^{2}, \quad \overbrace{\phi_{i,1}^j, \phi_{i,2}^j}^{2} \quad )\mathbb{B}_j$$

$$\vec{e}_{1,i}^{\,j} := \quad ( \quad \overbrace{0^2, \omega\vec{e}_i}^{4}, \quad \overbrace{\tau\vec{e}_i, 0^4}^{6}, \quad \overbrace{0^2}^{2}, \quad \overbrace{\phi_{i,1}^j, \phi_{i,2}^j}^{2} \quad )\mathbb{B}_j$$

$$D := (param, \{\mathbb{B}_j, \widehat{\mathbb{B}}^*_j\}_{j=0,1,\ldots,4}) \text{ For } \beta = 0, 1, \text{define } T_\beta := (\{\vec{e}^{\,j}_\beta\}_{j=0,4}, \{\vec{e}^{\,j}_{\beta,i}\}_{i=1,2;\ j=1,2,3})$$

Now, the advantage of an algorithm $\mathscr{A}$ in breaking this **Modified Basic Problem 1** (MBP1) is defined by

$$\mathsf{Adv}^{\mathrm{MBP1}}_{\mathscr{A}}(\kappa) = |Pr[\mathscr{A}(D, T_0) = 1] - Pr[\mathscr{A}(D, T_1) = 1]|$$

The MBP1 assumption is said to hold if for all PPT adversary $\mathscr{A}$, the advantage $\mathsf{Adv}^{\mathrm{MBP1}}_{\mathscr{A}}(\kappa)$ is a negligible function in security parameter $\kappa$.

**Lemma B.2.** *For any adversary $\mathscr{A}$, there exist a PPT algorithm $\mathscr{B}_1$, such that $\mathsf{Adv}^{\mathrm{MBP1}}_{\mathscr{A}}(\kappa) \leq \mathsf{Adv}^{\mathrm{BP1}}_{\mathscr{B}_1}(\kappa)$, for all $\kappa$.*

*Proof.* $\mathscr{B}_1$ is given the instance $(param, \mathbb{B}_0, \widehat{\mathbb{B}}^*_0, \mathbb{B}, \widehat{\mathbb{B}}^*, \vec{e}_\beta, \{\vec{e}_{\beta,i}\}_{i=1,2})$ of Basic Problem 1, where $\widehat{\mathbb{B}}^*_0 := (\vec{b}^*_{0,1}, \vec{b}^*_{0,3}, \ldots, \vec{b}^*_{0,5})$, $\widehat{\mathbb{B}}^* := (\vec{b}^*_1, \ldots, \vec{b}^*_4, \vec{b}^*_7 \ldots, \vec{b}^*_{14})$. $\mathscr{B}$ chooses $W_0, W_4 \xleftarrow{\mathrm{U}} GL(5, \mathbb{F}_q)$, $W_1, W_2, W_3 \xleftarrow{\mathrm{U}} GL(14, \mathbb{F}_q)$. Now, $\mathscr{B}_1$ defines new bases $(\mathbb{D}_j, \mathbb{D}^*_j)$ for $j = 0, \ldots, 4$ by setting the following

$$\begin{array}{lll}
\vec{d}_{j,\iota} & := \vec{b}_{j,\iota} W_j, \quad \vec{d}^*_{j,\iota} := \vec{b}^*_{j,\iota} (W_j^{-1})^T, \text{ for } j = 0, 4,\ \iota = 1, \ldots, 5 \\
\vec{d}_{j,\iota} & := \vec{b}_{j,\iota} W_j, \quad \vec{d}^*_{j,\iota} := \vec{b}^*_{j,\iota} (W_j^{-1})^T, \text{ for } j = 1, 2, 3,\ \iota = 1, \ldots, 14 \\
\vec{e}^{\,j}_\beta & := \vec{e}_\beta W_j \text{ for } j = 0, 4 \\
\vec{e}^{\,j}_{\beta,i} & := \vec{e}_{\beta,i} W_j \text{ for } j = 1, 2, 3,\ i = 1, 2 \\
\mathbb{D}_t & := (\vec{d}_{t,1}, \ldots, \vec{d}_{t,5}) \quad \mathbb{D}^*_t := (\vec{d}^*_{t,1}, \ldots, \vec{d}^*_{t,5}),\ \widehat{\mathbb{D}}^*_t := (\vec{d}^*_{t,1}, \vec{d}^*_{t,3}, \ldots, \vec{d}^*_{t,5}) \text{ for } t = 0, 4 \\
\mathbb{D}_t & := (\vec{d}_{t,1}, \ldots, \vec{d}_{t,14}) \quad \mathbb{D}^*_t := (\vec{d}^*_{t,1}, \ldots, \vec{d}^*_{t,14}),\ \widehat{\mathbb{D}}^*_t := (\vec{d}^*_{t,1}, \ldots, \vec{d}^*_{t,4}, \vec{d}^*_{t,7} \ldots, \vec{d}^*_{t,14}) \text{ for } t = 1, 2, 3
\end{array}$$

It is verified that $(\mathbb{D}_t, \mathbb{D}^*_t)$ for $t = 0, \ldots, 4$ are dual orthonormal bases. Then, $\mathscr{B}_1$ returns $\mathcal{G} := (param, \{\mathbb{D}_j, \widehat{\mathbb{D}}^*_j\}_{j=0,1,\ldots,4}, \{\vec{e}^{\,j}_\beta\}_{j=0,4}, \{\vec{e}^{\,j}_{\beta,i}\}_{i=1,2;\ j=1,2,3})$ to the adversary $\mathscr{A}$. It is straightforward that $\mathcal{G}$ is an instance of MBP1 for $\beta$. This concludes the lemma. □

**Lemma B.3.** *If DLIN assumption holds for a bilinear pairing group generator $\mathcal{G}$, then the DSS1 assumption also holds for $\mathcal{G}$. That is for any adversary $\mathscr{A}$, there exist PPT algorithms $\mathscr{F}_1, \mathscr{F}_2$, such that for any $\kappa$, $\mathsf{Adv}^{\mathrm{DSS1}}_{\mathscr{A}}(\kappa) \leq \mathsf{Adv}^{\mathrm{DLIN}}_{\mathscr{F}_1}(\kappa) + \sum_{p=1}^{d} \sum_{i=1}^{2} \mathsf{Adv}^{\mathrm{DLIN}}_{\mathscr{F}_{2-p-i}}(\kappa) + \mathcal{O}(d)/q$, where $\mathscr{F}_{2-p-i}(.) = \mathscr{F}_2(p, i, .)$*

*Proof.* The proof technique of lemma B.3 is adapted from that of lemma 23 in [OT12b], i.e., DSS1 is organized as hybrid of the experiments $\mathsf{Exp}$ 0, $\mathsf{Exp}$ 1,..., $\mathsf{Exp}$ 2-d-2-2. Thus, the advantage of $\mathscr{A}$ in DSS1 is the advantage gap between $\mathsf{Exp}$ 0 and $\mathsf{Exp}$ 2-d-2-2, i.e., we have $\mathsf{Adv}^{\mathrm{DSS1}}_{\mathscr{A}}(\kappa) = |Pr[\mathsf{Exp}^0_{\mathscr{A}}(\kappa) = 1] - Pr[\mathsf{Exp}^{\text{2-d-2-2}}_{\mathscr{A}}(\kappa) = 1]|$. Therefore, from the lemmas B.1, B.2, B.4, B.5 and B.6, we have

$\mathsf{Adv}^{\mathrm{DSS1}}_{\mathscr{A}}(\kappa) = |Pr[\mathsf{Exp}^0_{\mathscr{A}}(\kappa) = 1] - Pr[\mathsf{Exp}^{\text{2-d-2-2}}_{\mathscr{A}}(\kappa) = 1]|$

$\leq |Pr[\mathsf{Exp}^0_{\mathscr{A}}(\kappa) = 1] - Pr[\mathsf{Exp}^1_{\mathscr{A}}(\kappa) = 1]| + \sum_{p=1}^{d} \big(|Pr[\mathsf{Exp}^{\text{2-(p-1)-2-2}}_{\mathscr{A}}(\kappa) = 1] - Pr[\mathsf{Exp}^{\text{2-p-1-1}}_{\mathscr{A}}(\kappa) = 1]| + |Pr[\mathsf{Exp}^{\text{2-p-1-1}}_{\mathscr{A}}(\kappa) = 1] - Pr[\mathsf{Exp}^{\text{2-p-1-2}}_{\mathscr{A}}(\kappa) = 1]| + |Pr[\mathsf{Exp}^{\text{2-p-1-2}}_{\mathscr{A}}(\kappa) = 1] - Pr[\mathsf{Exp}^{\text{2-p-2-1}}_{\mathscr{A}}(\kappa) = 1]| + |Pr[\mathsf{Exp}^{\text{2-p-1-2}}_{\mathscr{A}}(\kappa) = 1] - Pr[\mathsf{Exp}^{\text{2-p-2-1}}_{\mathscr{A}}(\kappa) = 1]|\big)$

$= |Pr[\mathsf{Exp}^0_{\mathscr{A}}(\kappa) = 1] - Pr[\mathsf{Exp}^1_{\mathscr{A}}(\kappa) = 1]| + \sum_{p=1}^{d} \big(|Pr[\mathsf{Exp}^{\text{2-(p-1)-2-2}}_{\mathscr{A}}(\kappa) = 1] - Pr[\mathsf{Exp}^{\text{2-p-1-1}}_{\mathscr{A}}(\kappa) = 1]| + |Pr[\mathsf{Exp}^{\text{2-p-1-2}}_{\mathscr{A}}(\kappa) = 1] - Pr[\mathsf{Exp}^{\text{2-p-2-1}}_{\mathscr{A}}(\kappa) = 1]|\big)$

$\leq \mathsf{Adv}^{\mathrm{MBP1}}_{\mathscr{B}_1}(\kappa) + \sum_{p=1}^{d} \sum_{i=1}^{2} \mathsf{Adv}^{\mathrm{MBP1}}_{\mathscr{B}_{2-p-i}}(\kappa)$

$\leq \mathsf{Adv}^{\mathrm{DLIN}}_{\mathscr{F}_1}(\kappa) + \sum_{p=1}^{d} \sum_{i=1}^{2} \mathsf{Adv}^{\mathrm{DLIN}}_{\mathscr{F}_{2-p-i}}(\kappa) + \mathcal{O}(d)/q$

This concludes the lemma B.3. □

### Experiments

One can define the sequence of experiments almost the same as in lemma 23 of [OT12b], except that one considers here, two 5-dimensional dual bases and three 14-dimensional dual bases. In the following sketch, we show how to change $\mathsf{Exp}$ 0 to $\mathsf{Exp}$ 2-d-2-2 under MBP1.

$$\boxed{Exp\ 0} \overset{\mathrm{MBP1}}{\approx} \boxed{Exp\ 1} = \boxed{Exp\ \text{2-0-2-2}} \overset{\mathrm{MBP1}}{\approx} \boxed{Exp\ \text{2-1-1-1}} \approx \boxed{Exp\ \text{2-1-1-2}}$$

$$\boxed{Exp\ \text{2-1-1-2}} \overset{\mathrm{MBP1}}{\approx} \boxed{Exp\ \text{2-1-2-1}} \cdots \boxed{Exp\ \text{2-d-1-2}} \overset{\mathrm{MBP1}}{\approx} \boxed{Exp\ \text{2-d-2-1}} \approx \boxed{Exp\ \text{2-d-2-2}}$$

$\mathsf{Exp}\ 0$ : This is defined to be the $\beta = 0$ case of DSS1, i.e.,

$$\vec{e}_0^j := (\omega,\ \boxed{0},\ 0,\ 0,\ \phi_0^j)\mathbb{B}_j \text{ for } j = 0, 4$$

for $h = 1, \ldots, d;\ j = 1, 2, 3;\ i = 1, 2$

$$\vec{e}_{h,i}^j := \quad ( \quad \overbrace{\delta_{h,i}^j(1,h), \omega\vec{e}_i}^{4},\quad \overbrace{\boxed{0^2},\ 0^2,\ \boxed{0^2}}^{6},\quad \overbrace{0^2}^{2},\quad \overbrace{\phi_{i,1}^j, \phi_{i,2}^j}^{2} \quad )\mathbb{B}_j$$

Rest of the variables are defined as in DSS1.

$\mathsf{Exp}\ 1$ : This is Same as $\mathsf{Exp}\ 0$ except the following

$$\vec{e}_0^j := (\omega,\ \boxed{\tau},\ 0,\ 0,\ \phi_0^j)\mathbb{B}_j \text{ for } j = 0, 4$$

for $h = 1, \ldots, d;\ j = 1, 2, 3;\ i = 1, 2$

$$\vec{e}_{h,i}^j := \quad ( \quad \overbrace{\delta_{h,i}^j(1,h), \omega\vec{e}_i}^{4},\quad \overbrace{\boxed{\tau\vec{e}_i},\ 0^2,\ 0^2}^{6},\quad \overbrace{0^2}^{2},\quad \overbrace{\phi_{i,1}^j, \phi_{i,2}^j}^{2} \quad )\mathbb{B}_j, \quad \text{where } \tau \xleftarrow{\text{U}} \mathbb{F}_q$$

$\mathsf{Exp}$ 2-p-i-1 (for $p = 1, \ldots, d;\ i = 1, 2$) : This is same as $\mathsf{Exp}$ 2-(p-1)-2-2 if $i = 1$ and $\mathsf{Exp}$ 2-p-1-2 if $i = 2$ except the following: for $j = 1, 2, 3;\ i = 1, 2$

$$\vec{e}_{p,i}^j := \quad ( \quad \overbrace{\delta_{p,i}^j(1,p), \omega\vec{e}_i}^{4},\quad \overbrace{\tau\vec{e}_i,\ 0^2,\ \boxed{\tilde{\sigma}_{p,i}(1,p)}}^{6},\quad \overbrace{0^2}^{2},\quad \overbrace{\phi_{i,1}^j, \phi_{i,2}^j}^{2} \quad )\mathbb{B}_j, \quad \text{where } \tilde{\sigma}_{p,i} \xleftarrow{\text{U}} \mathbb{F}_q$$

This shows that $\mathsf{Exp}$ 2-0-2-2 is $\mathsf{Exp}$ 1.

$\mathsf{Exp}$ 2-p-i-2 (for $p = 1, \ldots, d;\ i = 1, 2$) : This is same as $\mathsf{Exp}$ 2-p-i-1 except: for $j = 1, 2, 3;\ i = 1, 2$

$$\vec{e}_{p,i}^j := \quad ( \quad \overbrace{\delta_{p,i}^j(1,p), \omega\vec{e}_i}^{4},\quad \overbrace{\tau\vec{e}_i,\ 0^2,\ \boxed{\tau(z_{p,i,1}^j, z_{p,i,2}^j)}}^{6},\quad \overbrace{0^2}^{2},\quad \overbrace{\phi_{i,1}^j, \phi_{i,2}^j}^{2} \quad )\mathbb{B}_j$$

where $z_{p,i,1}^j, z_{p,i,2}^j \xleftarrow{\text{U}} \mathbb{F}_q$

So, the distribution of $\vec{e}_{h,i}^j$ in $\mathsf{Exp}$ 2-d-2-2 can be written as: for $h = 1, \ldots, d;\ i = 1, 2;\ j = 1, 2, 3,$

$$\vec{e}_{h,i}^j := \quad ( \quad \overbrace{\delta_{h,i}^j(1,h), \omega\vec{e}_i}^{4},\quad \overbrace{\tau\vec{e}_i,\ 0^2,\ \tau\vec{e}_i Z_h^j}^{6},\quad \overbrace{0^2}^{2},\quad \overbrace{\phi_{i,1}^j, \phi_{i,2}^j}^{2} \quad )\mathbb{B}_j$$

where $Z_h^j \xleftarrow{\text{U}} \mathbb{F}_q^{2\times 2}$ (Implicitly, the $(\iota, \varsigma)$-entry of the matrix $Z_h^j$ is set as $Z_{h,\iota,\varsigma}^j$). Therefore, $\mathsf{Exp}$ 2-d-2-2 is identical to the $\beta = 1$ case of DSS1, except for the case, $det(Z_h^j) = 0$ for some $h$, i.e., except probability $3d/q$

**Lemma B.4.** *For any adversary $\mathscr{A}$, there exist a PPT algorithm $\mathscr{B}_1$, such that $|Pr[\mathsf{Exp}_{\mathscr{A}}^0(\kappa) = 1] - Pr[\mathsf{Exp}_{\mathscr{A}}^1(\kappa) = 1]| \leq \mathsf{Adv}_{\mathscr{B}_1}^{\text{MBP1}}(\kappa)$, for all $\kappa$.*

*Proof.* The proof of the lemma B.4 is almost the same as that of lemma 45 in [OT12b]. In lemma 45 in [OT12b], $\mathsf{Exp}$ 0 and $\mathsf{Exp}$ 1 were shown to be indistinguishable under BP1. But, in this lemma, rather we use MBP1.

$\mathscr{B}_1$ receives an instance of MBP1, $(param, \{\mathbb{B}_j, \widehat{\mathbb{B}}_j^*\}_{j=0,1,\ldots,4}, \{\vec{e}_\beta^j\}_{j=0,4}, \{\vec{e}_{\beta,i}^j\}_{i=1,2;\ j=1,2,3})$ and its task is to decide whether $\beta = 0$ or $\beta = 1$. For $h = 1, \ldots, d;\ i = 1, 2;\ j = 1, 2, 3$, $\mathscr{B}$ computes

$$\vec{e}_{\beta,h,i}^j := \delta_{h,i}^j(\vec{b}_{j,1} + h\vec{b}_{j,2}) + \vec{e}_{\beta,i}^j + \phi_{h,i,1}^j\vec{b}_{j,13} + \phi_{h,i,2}^j\vec{b}_{j,14}$$

where $\delta_{h,i}^j, \phi_{h,i,1}^j, \phi_{h,i,2}^j \xleftarrow{\text{U}} \mathbb{F}_q$.
Now, $\mathscr{B}_1$ sets

$\widehat{\mathbb{B}}_\iota := (\vec{b}_{\iota,1}, \vec{b}_{\iota,3}, \vec{b}_{\iota,5}), \quad \widehat{\mathbb{B}'}_\iota^* := (\vec{b}^*_{\iota,1}, \vec{b}^*_{\iota,3}, \vec{b}^*_{\iota,4})$, for $\iota = 0, 4$
$\widehat{\mathbb{B}}_j := (\vec{b}_{j,1}, \ldots, \vec{b}_{j,4}, \vec{b}_{j,13}, \vec{b}_{j,14}), \quad \widehat{\mathbb{B}'}_j^* := (\vec{b}^*_{j,1}, \ldots, \vec{b}^*_{j,4}, \vec{b}^*_{j,11}, \vec{b}^*_{j,12})$, for $j = 1, 2, 3$

$\mathscr{B}_1$ gives the parameters $\mathcal{G} = (param, \{\widehat{\mathbb{B}}_j, \widehat{\mathbb{B}'}_j^*\}_{j=0,1,\ldots,4}, \{\vec{e}^j_\beta\}_{j=0,4}, \{\vec{e}^j_{\beta,h,i}\}_{h=1,\ldots,d;\ i=1,2;\ j=1,2,3})$ to $\mathscr{A}$ and outputs a bit $b \in \{0,1\}$ if the adversary $\mathscr{A}$ outputs $b$. It is straightforward that if $\beta = 0$ (resp. $\beta = 1$), the distribution of $\mathcal{G}$ is exactly same as that of $\mathsf{Exp}\ 0$ (resp. $\mathsf{Exp}\ 1$). □

**Lemma B.5.** *For any adversary $\mathscr{A}$, there exist a PPT algorithm $\mathscr{B}_2$, such that for any $\kappa$, $|Pr[\mathsf{Exp}^{\text{2-(p-1)-2-2}}_{\mathscr{A}}(\kappa) = 1] - Pr[\mathsf{Exp}^{\text{2-p-1-1}}_{\mathscr{A}}(\kappa) = 1]| \leq \mathsf{Adv}^{\text{MBP1}}_{\mathscr{B}_{2-p-i}}(\kappa)$, if $i = 1$, and $|Pr[\mathsf{Exp}^{\text{2-p-1-2}}_{\mathscr{A}}(\kappa) = 1] - Pr[\mathsf{Exp}^{\text{2-p-2-1}}_{\mathscr{A}}(\kappa) = 1]| \leq \mathsf{Adv}^{\text{MBP1}}_{\mathscr{B}_{2-p-i}}(\kappa)$, if $i = 2$, where $\mathscr{B}_{2-p-i}(.) = \mathscr{B}_2(p, j, .)$.*

*Proof.* The proof of the lemma B.5 is almost the same as that of lemma 46 in [OT12b]. In lemma 46 in [OT12b], $\mathsf{Exp}$ 2-(p-1)-2-2 and $\mathsf{Exp}$ 2-p-1-1 (also $\mathsf{Exp}$ 2-p-1-2 and $\mathsf{Exp}$ 2-p-2-1) were shown to be indistinguishable under BP1. But, in this lemma, we rather use MBP1. $\mathscr{B}_2$ receives an instance of MBP1, $(param, \{\mathbb{B}_j, \widehat{\mathbb{B}}^*_j\}_{j=0,1,\ldots,4}, \{\vec{e}^j_\beta\}_{j=0,4}, \{\vec{e}^j_{\beta,i}\}_{i=1,2;\ j=1,2,3})$ and its task is to decide whether $\beta = 0$ or $\beta = 1$. For $j = 1, 2, 3$, $\mathscr{B}_2$ defines new dual bases $(\mathbb{D}_j, \mathbb{D}^*_j)$ as follows

$$\mathbb{D}_j = (\vec{d}_{j,1}, \ldots, \vec{d}_{j,14}) = (\vec{b}_{j,3}, \vec{b}_{j,4}, \vec{b}_{j,1}, \vec{b}_{j,2}, \vec{b}_{j,9}, \vec{b}_{j,10}, \vec{b}_{j,7}, \vec{b}_{j,8}, \vec{b}_{j,5}, \vec{b}_{j,6}, \vec{b}_{j,11}, \ldots, \vec{b}_{j,14})$$

$$\mathbb{D}^*_j = (\vec{d}^*_{j,1}, \ldots, \vec{d}^*_{j,14}) = (\vec{b}^*_{j,3}, \vec{b}^*_{j,4}, \vec{b}^*_{j,1}, \vec{b}^*_{j,2}, \vec{b}^*_{j,9}, \vec{b}^*_{j,10}, \vec{b}^*_{j,7}, \vec{b}^*_{j,8}, \vec{b}^*_{j,5}, \vec{b}^*_{j,6}, \vec{b}^*_{j,11}, \ldots, \vec{b}^*_{j,14})$$

Now $\mathscr{B}_2$ sets

$\widehat{\mathbb{B}}_\iota := (\vec{b}_{\iota,1}, \vec{b}_{\iota,3}, \vec{b}_{\iota,5}), \quad \widehat{\mathbb{B}'}_\iota^* := (\vec{b}^*_{\iota,1}, \vec{b}^*_{\iota,3}, \vec{b}^*_{\iota,4})$, for $\iota = 0, 4$
$\widehat{\mathbb{D}}_j := (\vec{d}_{j,1}, \ldots, \vec{d}_{j,4}, \vec{d}_{j,13}, \vec{d}_{j,14}), \quad \widehat{\mathbb{D}'}_j^* := (\vec{d}^*_{j,1}, \ldots, \vec{d}^*_{j,4}, \vec{d}^*_{j,11}, \vec{d}^*_{j,12})$, for $j = 1, 2, 3$

$\mathscr{B}_2$ can handle $\vec{e}^j_{h,\iota}$ for $(h, \iota) < (p, i)$ as in $\mathsf{Exp}$ 2-p-i-2 and the same for $(h, \iota) > (p, i)$ as in $\mathsf{Exp}$ 1 using $\mathbb{D}_j$ and $\tilde{\omega}, \tilde{\tau}, z^j_{h,\iota,1}, z^j_{h,\iota,1}, \phi^j_{h,\iota,1}, \phi^j_{h,\iota,2} \xleftarrow{\text{U}} \mathbb{F}_q$. Now, for $i = 1, 2;\ j = 1, 2, 3$, $\mathscr{B}_2$ computes $\vec{e}^j_{p,i}$ as shown below

$$\vec{e}^0_1 = (\tilde{\omega},\ \tilde{\tau},\ 0,\ 0,\ \phi_0) \quad \vec{e}^4_1 = (\tilde{\omega},\ \tilde{\tau},\ 0,\ 0,\ \phi_4)$$

$$\vec{e}^j_{p,i} = \vec{e}^j_{\beta,1} + p\vec{e}^j_{\beta,2} + \tilde{\omega}\vec{d}_{j,2+i} + \tilde{\omega}\vec{d}_{j,4+i}$$

where $\phi_0, \phi_4 \xleftarrow{\text{U}} \mathbb{F}_q$.
$\mathscr{B}_2$ gives the parameters $\mathcal{G} = (param, \{\mathbb{B}_j, \widehat{\mathbb{B}}^*_j\}_{j=0,4}, \{\mathbb{D}_j, \widehat{\mathbb{D}}^*_j\}_{j=1,2,3}, \{\vec{e}^j_1\}_{j=0,4}, \{\vec{e}^j_{h,i}\}_{h=1,\ldots,d;\ i=1,2;\ j=1,2,3})$ to $\mathscr{A}$ and outputs a bit $b \in \{0,1\}$ if the adversary $\mathscr{A}$ outputs $b$. It is straightforward that if $i = 1$ and $\beta = 0$ (resp. $\beta = 1$), the distribution of $\mathcal{G}$ is exactly same as that of $\mathsf{Exp}$ 2-(p-1)-2-2 (resp. $\mathsf{Exp}$ 2-p-1-1). Similarly, if $i = 2$ and $\beta = 0$ (resp. $\beta = 1$), the distribution of $\mathcal{G}$ is exactly same as that of $\mathsf{Exp}$ 2-p-1-2 (resp. $\mathsf{Exp}$ 2-p-2-1). □

**Lemma B.6.** *For any adversary $\mathscr{A}$, and for any $\kappa$, we have $Pr[\mathsf{Exp}^{\text{2-p-i-1}}_{\mathscr{A}}(\kappa) = 1] = Pr[\mathsf{Exp}^{\text{2-p-i-2}}_{\mathscr{A}}(\kappa) = 1]$.*

*Proof.* The proof technique of this lemma is adapted form that of lemma 47 in [OT12b]. For $j = 1, 2, 3$, pick $Z^j \xleftarrow{\text{U}} GL(2, \mathbb{F}_q)$ and set $U^j = ((Z^j)^{-1})^T$. Now, we define new bases $(\mathbb{D}_j, \mathbb{D}^*_j)$ for $j = 1, 2, 3$, by setting the following

$$\begin{pmatrix} \vec{d}_{j,9} \\ \vec{d}_{j,10} \end{pmatrix} := (U^j)^T \begin{pmatrix} \vec{b}_{j,9} \\ \vec{b}_{j,10} \end{pmatrix} \qquad \begin{pmatrix} \vec{d}^*_{j,9} \\ \vec{d}^*_{j,10} \end{pmatrix} := (Z^j)^T \begin{pmatrix} \vec{b}^*_{j,9} \\ \vec{b}^*_{j,10} \end{pmatrix}$$

$$\mathbb{D}_j = (\vec{b}_{j,1}, \ldots, \vec{b}_{j,8}, \boxed{\vec{d}_{j,9}, \vec{d}_{j,10}}, \vec{b}_{j,11}, \ldots, \vec{b}_{j,14}) \quad \mathbb{D}^*_j = (\vec{b}^*_{j,1}, \ldots, \vec{b}^*_{j,8}, \boxed{\vec{d}^*_{j,9}, \vec{d}^*_{j,10}}, \vec{b}^*_{j,11}, \ldots, \vec{b}^*_{j,14})$$

It is easily verified that $(\mathbb{D}_j, \mathbb{D}^*_j)$ are dual pairing orthonormal basis and are distributed the same as the original bases, $(\mathbb{B}_j, \mathbb{B}^*_j)$.

For $(h,\iota) < (p,i)$, we express $\vec{e}^{\,j}_{h,\iota}$ using the bases $(\mathbb{B}_j, \mathbb{B}^*_j)$ and $(\mathbb{D}_j, \mathbb{D}^*_j)$ as:

$$\begin{aligned}\vec{e}^{\,j}_{h,\iota} &:= (\overbrace{\delta^j_{h,\iota}(1,h),\ \omega\vec{e}_\iota}^{4},\ \overbrace{\tau\vec{e}_\iota,\ 0^2,\ \tau\vec{z}^{\,j}_{h,\iota}}^{6},\ \overbrace{0^2}^{2},\ \overbrace{\phi^j_{h,\iota,1}, \phi^j_{h,\iota,2}}^{2})\ \mathbb{B}_j \\ &:= (\overbrace{\delta^j_{h,\iota}(1,h),\ \omega\vec{e}_\iota}^{4},\ \overbrace{\tau\vec{e}_\iota,\ 0^2,\ \tau\vec{z'}^{\,j}_{h,\iota}}^{6},\ \overbrace{0^2}^{2},\ \overbrace{\phi^j_{h,\iota,1}, \phi^j_{h,\iota,2}}^{2})\ \mathbb{D}_j\end{aligned}$$

For $(h,\iota) = (p,i)$, we express $\vec{e}^{\,j}_{p,i}$ using the bases $(\mathbb{B}_j, \mathbb{B}^*_j)$ and $(\mathbb{D}_j, \mathbb{D}^*_j)$ as:

$$\begin{aligned}\vec{e}^{\,j}_{p,i} &:= (\overbrace{\delta^j_{p,i}(1,p),\ \omega\vec{e}_i}^{4},\ \overbrace{\tau\vec{e}_i,\ 0^2,\ \tilde{\sigma}_{p,i}(1,p)}^{6},\ \overbrace{0^2}^{2},\ \overbrace{\phi^j_{p,i,1}, \phi^j_{p,i,2}}^{2})\ \mathbb{B}_j \\ &:= (\overbrace{\delta^j_{p,i}(1,p),\ \omega\vec{e}_i}^{4},\ \overbrace{\tau\vec{e}_i,\ 0^2,\ \tau\vec{z}^{\,j}_{p,i}}^{6},\ \overbrace{0^2}^{2},\ \overbrace{\phi^j_{p,i,1}, \phi^j_{p,i,2}}^{2})\ \mathbb{D}_j\end{aligned}$$

For $(h,\iota) > (p,i)$, we express $\vec{e}^{\,j}_{h,\iota}$ using the bases $(\mathbb{B}_j, \mathbb{B}^*_j)$ and $(\mathbb{D}_j, \mathbb{D}^*_j)$ as:

$$\begin{aligned}\vec{e}^{\,j}_{h,\iota} &:= (\overbrace{\delta^j_{h,\iota}(1,h),\ \omega\vec{e}_\iota}^{4},\ \overbrace{\tau\vec{e}_\iota,\ 0^2,\ 0^2}^{6},\ \overbrace{0^2}^{2},\ \overbrace{\phi^j_{h,\iota,1}, \phi^j_{h,\iota,2}}^{2})\ \mathbb{B}_j \\ &:= (\overbrace{\delta^j_{h,\iota}(1,h),\ \omega\vec{e}_\iota}^{4},\ \overbrace{\tau\vec{e}_\iota,\ 0^2,\ 0^2}^{6},\ \overbrace{0^2}^{2},\ \overbrace{\phi^j_{h,\iota,1}, \phi^j_{h,\iota,2}}^{2})\ \mathbb{D}_j\end{aligned}$$

where $\vec{z}^{\,j}_{p,i} = \tau^{-1}.\tilde{\sigma}_{p,i}(1,p).Z^j$ and $\vec{z}^{\,j}_{h,\iota} = (z^j_{h,\iota,1}, z^j_{h,\iota,2})$, $\vec{z'}^{\,j}_{h,\iota} = \vec{z}^{\,j}_{h,\iota}.Z^j$ for $(h,\iota) < (p,i)$. Thus, for $j = 1,2,3$ and for $(h,\iota) < (p,i)$, $\vec{z}^{\,j}_{p,i}$ and $\vec{z'}^{\,j}_{h,\iota}$ are uniformly and independently distributed. Therefore, for $h = 1,\ldots,d;\ j = 1,2,3; \iota = 1,2$, the distribution of $\vec{e}^{\,j}_{h,\iota}$ is identical to that of $\mathsf{Exp}$ 2-p-i-1 (resp. $\mathsf{Exp}$ 2-p-i-2) expressed over the bases $(\mathbb{B}_j, \mathbb{B}^*_j)$ (resp. $(\mathbb{D}_j, \mathbb{D}^*_j)$). This concludes the lemma. □

## B.2 Reduction of DSS2 from DLIN

**The Sketch of reduction of intermediate modified basic problems :**

$$\boxed{DLIN} \overset{\text{Lemma B.8}}{\Longrightarrow} \boxed{BP2} \overset{\text{Lemma B.9}}{\Longrightarrow} \boxed{MBP2}$$

$$\boxed{DLIN} \overset{\text{Lemma B.11}}{\Longrightarrow} \boxed{BP4-p} \overset{\text{Lemma B.12}}{\Longrightarrow} \boxed{BP3-p} \overset{\text{Lemma B.10}}{\Longrightarrow} \boxed{MBP3-p}$$

$$\boxed{DLIN} \overset{\text{Lemma B.11}}{\Longrightarrow} \boxed{BP4-p} \overset{\text{Lemma B.13}}{\Longrightarrow} \boxed{MBP4-p}$$

$$\boxed{DLIN} \overset{\text{Lemma B.7}}{\Longrightarrow} \boxed{BP0} \overset{\text{Lemma B.14}}{\Longrightarrow} \boxed{MBP6} \overset{\text{Lemma B.16}}{\Longrightarrow} \boxed{MBP5-p}$$

**Definition B.4** (Basic Problem 0 in [OT12b])**.** Choose $\mu_1, \mu_2, \phi_1, \phi_2, \chi_1, \chi_2, \rho, \sigma \xleftarrow{\text{U}} \mathbb{F}_q$.

$$(param_{BP0}, (\mathbb{B}, \mathbb{B}^*), \lambda P, \xi P) \longleftarrow \mathcal{G}_{ob}(\kappa, 5) \quad \widehat{\mathbb{B}}^* := (\vec{b}^*_1,\ \vec{b}^*_4,\ \vec{b}^*_5)$$

$$h^*_1 = (\mu_1,\ \rho,\ 0,\ 0,\ 0)\mathbb{B}^*, \quad h^*_2 = (\mu_2,\ 0,\ \rho,\ 0,\ 0)\mathbb{B}^*$$

$$\vec{e}_0 := (\sigma,\ 0,\ 0,\ \phi_1,\ \phi_2)\mathbb{B}, \quad \vec{e}_1 := (\sigma,\ \chi_1,\ \chi_2,\ \phi_1,\ \phi_2)\mathbb{B}$$

$$D := (param_{BP0}, \mathbb{B}, \widehat{\mathbb{B}}^*, \{\vec{h}^*_i\}_{i=1,2}, \lambda P, \xi P, \rho\xi P) \ \text{ for } \beta = 0,1, \text{ define } T_\beta := \vec{e}_\beta$$

Now, the advantage of an algorithm $\mathscr{A}$ in breaking this Basic Problem 0 (BP0) is defined by

$$\mathsf{Adv}^{\text{BP0}}_{\mathscr{A}}(\kappa) = |Pr[\mathscr{A}(D, T_0) = 1] - Pr[\mathscr{A}(D, T_1) = 1]|$$

We say that the BP0 assumption holds if for all PPT adversary $\mathscr{A}$, the advantage $\mathsf{Adv}^{\text{BP0}}_{\mathscr{A}}(\kappa)$ is a negligible function in security parameter $\kappa$.

**Lemma B.7** (lemma 32 in [OT12b]). *For any adversary $\mathscr{A}$, there exist a PPT algorithm $\mathscr{B}$, such that* $\mathsf{Adv}^{\mathrm{BP0}}_{\mathscr{A}}(\kappa) \leq \mathsf{Adv}^{\mathrm{DLIN}}_{\mathscr{B}}(\kappa) + 5/q$, *for all* $\kappa$.

**Definition B.5** (Basic Problem 2 in [OT12b]). Choose $\zeta, \omega, \eta_0 \xleftarrow{\mathrm{U}} \mathbb{F}_q$. For $i = 1, 2$, pick $\eta_{i,1}, \eta_{i,2} \xleftarrow{\mathrm{U}} \mathbb{F}_q$ and $\rho, \tau \xleftarrow{\mathrm{U}} \mathbb{F}_q^{\times}$.

$$(param, (\mathbb{B}_0, \mathbb{B}_0^*), (\mathbb{B}, \mathbb{B}^*)) \longleftarrow \mathcal{G}_{ob}(\kappa, 5, 14)$$

$$\widehat{\mathbb{B}}_0 := (\vec{b}_{0,1},\ \vec{b}_{0,3}, \ldots, \vec{b}_{0,5}), \qquad \widehat{\mathbb{B}} := (\vec{b}_1, \ldots, \vec{b}_4,\ \vec{b}_9, \ldots, \vec{b}_{14})$$

$$\vec{h}^*_{0,0} := (\zeta,\ 0,\ 0,\ \eta_0,\ 0)\mathbb{B}^*_0, \quad \vec{h}^*_{1,0} := (\zeta,\ \rho,\ 0,\ \eta_0,\ 0)\mathbb{B}^*_0 \quad \vec{\varepsilon}_0 := (\omega,\ \tau,\ 0,\ 0,\ 0)\mathbb{B}_0$$

For $i = 1, 2$, define

$$\begin{aligned}
\vec{h}^*_{0,i} &:= \quad ( \overbrace{0^2, \zeta\vec{e}_i}^{4}, \quad \overbrace{0^6}^{6}, \quad \overbrace{\eta_{i,1}, \eta_{i,2}}^{2}, \quad \overbrace{0^2}^{2} \quad )\mathbb{B}^* \\
\vec{h}^*_{1,i} &:= \quad ( \overbrace{0^2, \zeta\vec{e}_i}^{4}, \quad \overbrace{\rho\vec{e}_i, 0^4}^{6}, \quad \overbrace{\eta_{i,1}, \eta_{i,2}}^{2}, \quad \overbrace{0^2}^{2} \quad )\mathbb{B}^* \\
\vec{\Upsilon}_i &:= \quad ( \overbrace{0^2, \omega\vec{e}_i}^{4}, \quad \overbrace{\tau\vec{e}_i, 0^4}^{6}, \quad \overbrace{0^2}^{2}, \quad \overbrace{0^2}^{2} \quad )\mathbb{B}
\end{aligned}$$

$D := (param, \widehat{\mathbb{B}}_0, \mathbb{B}^*_0, \widehat{\mathbb{B}}, \mathbb{B}^*, \vec{\varepsilon}_0, \{\vec{\Upsilon}_i\}_{i=1,2})$ For $\beta = 0, 1$, define $T_\beta := (\vec{h}^*_{\beta,0}, \{\vec{h}^*_{\beta,i}\}_{i=1,2})$

Now, the advantage of an algorithm $\mathscr{A}$ in breaking this Basic Problem 2 (BP2) is defined by

$$\mathsf{Adv}^{\mathrm{BP2}}_{\mathscr{A}}(\kappa) = |Pr[\mathscr{A}(D, T_0) = 1] - Pr[\mathscr{A}(D, T_1) = 1]|$$

The BP2 assumption is said to hold if for all PPT adversary $\mathscr{A}$, the advantage $\mathsf{Adv}^{\mathrm{BP2}}_{\mathscr{A}}(\kappa)$ is a negligible function in security parameter $\kappa$.

**Lemma B.8** (lemma 35 in [OT12b]). *For any adversary $\mathscr{A}$, there exist a PPT algorithm $\mathscr{B}$, such that* $\mathsf{Adv}^{\mathrm{BP2}}_{\mathscr{A}}(\kappa) \leq \mathsf{Adv}^{\mathrm{DLIN}}_{\mathscr{B}}(\kappa) + 5/q$, *for all* $\kappa$.

**Definition B.6** (**Modified Basic Problem 2**). Choose $\zeta, \omega, \eta_0, \eta_4 \xleftarrow{\mathrm{U}} \mathbb{F}_q$. For $j = 1, 2, 3$, $i = 1, 2$, pick $\eta^j_{i,1}, \eta^j_{i,2} \xleftarrow{\mathrm{U}} \mathbb{F}_q$ and $\rho, \tau \xleftarrow{\mathrm{U}} \mathbb{F}_q^{\times}$.

$$(param, (\mathbb{B}_0, \mathbb{B}_0^*), (\mathbb{B}_1, \mathbb{B}_1^*), (\mathbb{B}_2, \mathbb{B}_2^*), (\mathbb{B}_3, \mathbb{B}_3^*), (\mathbb{B}_4, \mathbb{B}_4^*)) \longleftarrow \mathcal{G}_{ob}(\kappa, 5, 14, 14, 14, 5)$$

For $j = 0, 4$, define $\widehat{\mathbb{B}}_j := (\vec{b}_{j,1},\ \vec{b}_{j,3}, \ldots, \vec{b}_{j,5})$ For $j = 1, 2, 3$, define $\widehat{\mathbb{B}}_j := (\vec{b}_{j,1}, \ldots, \vec{b}_{j,4},\ \vec{b}_{j,9}, \ldots, \vec{b}_{j,14})$

For $j = 0, 4$, define

$$\vec{h}^{j*}_0 := (\zeta,\ 0,\ 0,\ \eta_j,\ 0)\mathbb{B}^*_j, \quad \vec{h}^{j*}_1 := (\zeta,\ \rho,\ 0,\ \eta_j,\ 0)\mathbb{B}^*_j \quad \vec{\varepsilon}_j := (\omega,\ \tau,\ 0,\ 0,\ 0)\mathbb{B}_j$$

For $j = 1, 2, 3$, $i = 1, 2$, define

$$\begin{aligned}
\vec{h}^{j*}_{0,i} &:= \quad ( \overbrace{0^2, \zeta\vec{e}_i}^{4}, \quad \overbrace{0^6}^{6}, \quad \overbrace{\eta^j_{i,1}, \eta^j_{i,2}}^{2}, \quad \overbrace{0^2}^{2} \quad )\mathbb{B}^*_j \\
\vec{h}^{j*}_{1,i} &:= \quad ( \overbrace{0^2, \zeta\vec{e}_i}^{4}, \quad \overbrace{\rho\vec{e}_i, 0^4}^{6}, \quad \overbrace{\eta^j_{i,1}, \eta^j_{i,2}}^{2}, \quad \overbrace{0^2}^{2} \quad )\mathbb{B}^*_j \\
\vec{\Upsilon}^j_i &:= \quad ( \overbrace{0^2, \omega\vec{e}_i}^{4}, \quad \overbrace{\tau\vec{e}_i, 0^4}^{6}, \quad \overbrace{0^2}^{2}, \quad \overbrace{0^2}^{2} \quad )\mathbb{B}_j
\end{aligned}$$

$D := (param, \{\widehat{\mathbb{B}}_\iota, \mathbb{B}^*_\iota\}_{\iota=0,4}, \{\widehat{\mathbb{B}}_j, \mathbb{B}^*_j\}_{j=1,2,3}, \{\vec{\varepsilon}_j\}_{j=0,4}, \{\vec{\Upsilon}^j_i\}_{j=1,2,3;\ i=1,2})$. For $\beta = 0, 1$, define the challenge $T_\beta := (\{\vec{h}^{j*}_\beta\}_{j=0,4}, \{\vec{h}^{j*}_{\beta,i}\}_{j=1,2,3;\ i=1,2})$.
Now, the advantage of an algorithm $\mathscr{A}$ in breaking this **Modified Basic Problem 2** (MBP2) is defined by

$$\mathsf{Adv}^{\mathrm{MBP2}}_{\mathscr{A}}(\kappa) = |Pr[\mathscr{A}(D, T_0) = 1] - Pr[\mathscr{A}(D, T_1) = 1]|$$

The MBP2 assumption is said to hold if for all PPT adversary $\mathscr{A}$, the advantage $\mathsf{Adv}^{\mathrm{MBP2}}_{\mathscr{A}}(\kappa)$ is a negligible function in security parameter $\kappa$.

**Lemma B.9.** *For any adversary $\mathscr{A}$, there exist a PPT algorithm $\mathscr{B}$, such that* $\mathsf{Adv}^{\mathrm{MBP2}}_{\mathscr{A}}(\kappa) \leq \mathsf{Adv}^{\mathrm{BP2}}_{\mathscr{B}}(\kappa)$*, for all* $\kappa$*.*

*Proof.* This is proven in the same manner as lemma B.2. □

**Definition B.7** (Basic Problem 3-p in [OT12b] for $p = 1, \ldots, d$)**.** For $i = 1, 2$, choose $\mu_{p,i}, \theta_{p,i}, \eta_{p,i,1}, \eta_{p,i,2} \xleftarrow{\mathrm{U}} \mathbb{F}_q$ and $\tau \xleftarrow{\mathrm{U}} \mathbb{F}_q^{\times}$.

$$(param, (\mathbb{B}_0, \mathbb{B}_0^*), (\mathbb{B}, \mathbb{B}^*)) \longleftarrow \mathcal{G}_{ob}(\kappa, 5, 14)$$

$$\widehat{\mathbb{B}} := (\vec{b}_1, \ldots, \vec{b}_4,\ \vec{b}_9, \ldots, \vec{b}_{14}), \quad \vec{\varepsilon}_0 := (0,\ \tau,\ 0,\ 0,\ 0)\mathbb{B}_0$$

For $i = 1, 2$, define

$$\begin{aligned}
\vec{h}^*_{0,p,i} &:= (\ \overbrace{\mu_{p,i}(p,-1),0^2}^{4},\ \overbrace{0^6}^{6},\ \overbrace{\eta_{p,i,1},\eta_{p,i,2}}^{2},\ \overbrace{0^2}^{2}\ )\mathbb{B}^*\\
\vec{h}^*_{1,p,i} &:= (\ \overbrace{\mu_{p,i}(p,-1),0^2}^{4},\ \overbrace{-\theta_{p,i}\vec{e}_i,\theta_{p,i}\vec{e}_i,0^2}^{6},\ \overbrace{\eta_{p,i,1},\eta_{p,i,2}}^{2},\ \overbrace{0^2}^{2}\ )\mathbb{B}^*\\
\vec{\Upsilon}_i &:= (\ \overbrace{0^4}^{4},\ \overbrace{\tau\vec{e}_i,\tau\vec{e}_i,0^2}^{6},\ \overbrace{0^2}^{2},\ \overbrace{0^2}^{2}\ )\mathbb{B}\\
\vec{g}_i &:= (\ \overbrace{0^4}^{4},\ \overbrace{0^4,\tau\vec{e}_i}^{6},\ \overbrace{0^2}^{2},\ \overbrace{0^2}^{2}\ )\mathbb{B}
\end{aligned}$$

$D := (param, \mathbb{B}_0, \mathbb{B}_0^*, \widehat{\mathbb{B}}, \mathbb{B}^*, \vec{\varepsilon}_0, \{\vec{\Upsilon}_i, \vec{g}_i\}_{i=1,2})$ For $\beta = 0, 1$, define $T_\beta := (\{\vec{h}_{\beta,p,i}\}_{i=1,2})$

Now, the advantage of an algorithm $\mathscr{A}$ in breaking this Basic Problem 3-p (BP3-p) is defined by

$$\mathsf{Adv}^{\mathrm{BP3-p}}_{\mathscr{A}}(\kappa) = |Pr[\mathscr{A}(D, T_0) = 1] - Pr[\mathscr{A}(D, T_1) = 1]|$$

The BP3-p assumption is said to hold if for all PPT adversary $\mathscr{A}$, the advantage $\mathsf{Adv}^{\mathrm{BP3-p}}_{\mathscr{A}}(\kappa)$ is a negligible function in security parameter $\kappa$.

**Definition B.8** (**Modified Basic Problem 3-p** for $p = 1, \ldots, d$)**.** For $i = 1, 2$, pick $\theta_{p,i} \xleftarrow{\mathrm{U}} \mathbb{F}_q$. For $j = 1, 2, 3$, $i = 1, 2$, choose $\mu^j_{p,i}, \eta^j_{p,i,1}, \eta^j_{p,i,2} \xleftarrow{\mathrm{U}} \mathbb{F}_q$ and $\tau \xleftarrow{\mathrm{U}} \mathbb{F}_q^{\times}$.

$$(param, (\mathbb{B}_0, \mathbb{B}_0^*), (\mathbb{B}_1, \mathbb{B}_1^*), (\mathbb{B}_2, \mathbb{B}_2^*), (\mathbb{B}_3, \mathbb{B}_3^*), (\mathbb{B}_4, \mathbb{B}_4^*)) \longleftarrow \mathcal{G}_{ob}(\kappa, 5, 14, 14, 14, 5)$$

$$\text{For } j = 1, 2, 3,\ \text{define } \widehat{\mathbb{B}}_j := (\vec{b}_{j,1}, \ldots, \vec{b}_{j,4},\ \vec{b}_{j,9}, \ldots, \vec{b}_{j,14})$$

$$\text{For } \iota = 0, 4,\ \vec{\varepsilon}_\iota := (0,\ \tau,\ 0,\ 0,\ 0)\mathbb{B}_\iota$$

For $j = 1, 2, 3$, $i = 1, 2$, define

$$\begin{aligned}
\vec{h}^{j*}_{0,p,i} &:= (\ \overbrace{\mu^j_{p,i}(p,-1),0^2}^{4},\ \overbrace{0^6}^{6},\ \overbrace{\eta^j_{p,i,1},\eta^j_{p,i,2}}^{2},\ \overbrace{0^2}^{2}\ )\mathbb{B}^*_j\\
\vec{h}^{j*}_{1,p,i} &:= (\ \overbrace{\mu^j_{p,i}(p,-1),0^2}^{4},\ \overbrace{-\theta_{p,i}\vec{e}_i,\theta_{p,i}\vec{e}_i,0^2}^{6},\ \overbrace{\eta^j_{p,i,1},\eta^j_{p,i,2}}^{2},\ \overbrace{0^2}^{2}\ )\mathbb{B}^*_j\\
\vec{e}^{j}_i &:= (\ \overbrace{0^4}^{4},\ \overbrace{\tau\vec{e}_i,\tau\vec{e}_i,0^2}^{6},\ \overbrace{0^2}^{2},\ \overbrace{0^2}^{2}\ )\mathbb{B}_j\\
\vec{g}^{j}_i &:= (\ \overbrace{0^4}^{4},\ \overbrace{0^4,\tau\vec{e}_i}^{6},\ \overbrace{0^2}^{2},\ \overbrace{0^2}^{2}\ )\mathbb{B}_j
\end{aligned}$$

$D := (param, \{\mathbb{B}_\iota, \mathbb{B}^*_\iota\}_{\iota=0,4}, \{\widehat{\mathbb{B}}_j, \mathbb{B}^*_j\}_{j=1,2,3}, \{\vec{\varepsilon}_\iota\}_{\iota=0,4}, \{\vec{e}^j_i, \vec{g}^j_i\}_{j=1,2,3;\ i=1,2})$. For $\beta = 0, 1$, define $T_\beta := (\{\vec{h}^j_{\beta,p,i}\}_{j=1,2,3;\ i=1,2})$.

Now, the advantage of an algorithm $\mathscr{A}$ in breaking this **Modified Basic Problem 3-p** (MBP3-p) is defined by

$$\mathsf{Adv}^{\mathrm{MBP3-p}}_{\mathscr{A}}(\kappa) = |Pr[\mathscr{A}(D, T_0) = 1] - Pr[\mathscr{A}(D, T_1) = 1]|$$

The MBP3-p assumption is said to hold if for all PPT algorithm $\mathscr{A}$, the advantage $\mathsf{Adv}^{\mathrm{MBP3-p}}_{\mathscr{A}}(\kappa)$ is a negligible function in security parameter $\kappa$.

**Lemma B.10.** *For any adversary $\mathscr{A}$, there exist a PPT algorithm $\mathscr{B}$, such that* $\mathsf{Adv}^{\mathrm{MBP3-p}}_{\mathscr{A}}(\kappa) \leq \mathsf{Adv}^{\mathrm{BP3-p}}_{\mathscr{B}}(\kappa)$*, for all $\kappa$.*

*Proof.* Similar to the proof of lemma B.2. □

**Definition B.9** (Basic Problem 4-p in [OT12b] for $p = 1, \ldots, d$)**.** For $i = 1, 2$, choose $\mu_{p,i}, \theta_{p,i}, \eta_{p,i,1}, \eta_{p,i,2} \xleftarrow{\mathrm{U}} \mathbb{F}_q$.

$$(param, (\mathbb{B}_0, \mathbb{B}_0^*), (\mathbb{B}, \mathbb{B}^*)) \longleftarrow \mathcal{G}_{ob}(\kappa, 5, 14)$$

$$\widehat{\mathbb{B}} := (\vec{b}_1, \ldots, \vec{b}_6,\ \vec{b}_9, \ldots, \vec{b}_{14})$$

For $i = 1, 2$ define

$$\vec{h}^*_{0,p,i} := \quad ( \overbrace{\mu_{p,i}(p,-1), 0^2}^{4}, \quad \overbrace{0^6}^{6}, \quad \overbrace{\eta_{p,i,1}, \eta_{p,i,2}}^{2}, \quad \overbrace{0^2}^{2} \quad )\mathbb{B}^*$$

$$\vec{h}^*_{1,p,i} := \quad ( \overbrace{\mu_{p,i}(p,-1), 0^2}^{4}, \quad \overbrace{0^2, \theta_{p,i}\vec{e}_i, 0^2}^{6}, \quad \overbrace{\eta_{p,i,1}, \eta_{p,i,2}}^{2}, \quad \overbrace{0^2}^{2} \quad )\mathbb{B}^*$$

$$D := (param, \mathbb{B}_0, \mathbb{B}_0^*, \widehat{\mathbb{B}}, \mathbb{B}^*) \text{ For } \beta = 0, 1, \text{define } T_\beta := (\{\vec{h}_{\beta,p,i}\}_{i=1,2})$$

Now, the advantage of an algorithm $\mathscr{A}$ in breaking this Basic Problem 4-p (BP4-p) is defined by

$$\mathsf{Adv}^{\mathrm{BP4-p}}_{\mathscr{A}}(\kappa) = |Pr[\mathscr{A}(D, T_0) = 1] - Pr[\mathscr{A}(D, T_1) = 1]|$$

The BP4-p assumption is said to hold if for all PPT algorithm $\mathscr{A}$, the advantage $\mathsf{Adv}^{\mathrm{BP4-p}}_{\mathscr{A}}(\kappa)$ is a negligible function in security parameter $\kappa$.

**Lemma B.11** (lemma 38 in [OT12b])**.** *For any adversary $\mathscr{A}$, there exist a PPT algorithm $\mathscr{B}$, such that for all $\kappa$,* $\mathsf{Adv}^{\mathrm{BP4-p}}_{\mathscr{A}_p}(\kappa) \leq \sum_{i=1}^{2} \mathsf{Adv}^{\mathrm{DLIN}}_{\mathscr{B}_{p,i}}(\kappa) + 10/q$*, where $\mathscr{A}_p(.) = \mathscr{A}(p, .)$ and $\mathscr{B}_{p,i}(.) = \mathscr{B}(p, i, .)$*

**Lemma B.12** (lemma 37 in [OT12b])**.** *For any adversary $\mathscr{A}$, there exist a PPT algorithm $\mathscr{B}$, such that for all $\kappa$,* $\mathsf{Adv}^{\mathrm{BP3-p}}_{\mathscr{A}_p}(\kappa) \leq \sum_{i=1}^{2} \mathsf{Adv}^{\mathrm{BP4-p}}_{\mathscr{B}_{p,i}}(\kappa)$*, where $\mathscr{A}_p(.) = \mathscr{A}(p, .)$ and $\mathscr{B}_p(.) = \mathscr{B}(p, .)$*

**Definition B.10** (**Modified Basic Problem 4-p** for $p = 1, \ldots, d$)**.** For $i = 1, 2$, pick $\theta_{p,i} \xleftarrow{\mathrm{U}} \mathbb{F}_q$. For $j = 1, 2, 3$, $i = 1, 2$, choose $\mu^j_{p,i}, \eta^j_{p,i,1}, \eta^j_{p,i,2} \xleftarrow{\mathrm{U}} \mathbb{F}_q$.

$$(param, (\mathbb{B}_0, \mathbb{B}_0^*), (\mathbb{B}_1, \mathbb{B}_1^*), (\mathbb{B}_2, \mathbb{B}_2^*), (\mathbb{B}_3, \mathbb{B}_3^*), (\mathbb{B}_4, \mathbb{B}_4^*)) \longleftarrow \mathcal{G}_{ob}(\kappa, 5, 14, 14, 14, 5)$$

$$\text{For } j = 1, 2, 3, \text{ define } \widehat{\mathbb{B}}_j := (\vec{b}_{j,1}, \ldots, \vec{b}_{j,6},\ \vec{b}_{j,9}, \ldots, \vec{b}_{j,14})$$

For $j = 1, 2, 3$, $i = 1, 2$ define

$$\vec{h}^{j*}_{0,p,i} := \quad ( \overbrace{\mu^j_{p,i}(p,-1), 0^2}^{4}, \quad \overbrace{0^6}^{6}, \quad \overbrace{\eta^j_{p,i,1}, \eta^j_{p,i,2}}^{2}, \quad \overbrace{0^2}^{2} \quad )\mathbb{B}^*_j$$

$$\vec{h}^{j*}_{1,p,i} := \quad ( \overbrace{\mu^j_{p,i}(p,-1), 0^2}^{4}, \quad \overbrace{0^2, \theta_{p,i}\vec{e}_i, 0^2}^{6}, \quad \overbrace{\eta^j_{p,i,1}, \eta^j_{p,i,2}}^{2}, \quad \overbrace{0^2}^{2} \quad )\mathbb{B}^*_j$$

$$D := (param, \{\mathbb{B}_\iota, \mathbb{B}^*_\iota\}_{\iota=0,4}, \{\widehat{\mathbb{B}}_j, \mathbb{B}^*_j\}_{j=1,2,3}) \text{ For } \beta = 0, 1, \text{define } T_\beta := (\{\vec{h}^j_{\beta,p,i}\}_{j=1,2,3;\ i=1,2})$$

Now, the advantage of an algorithm $\mathscr{A}$ in breaking this **Modified Basic Problem 4-p** (MBP4-p) is defined by

$$\mathsf{Adv}^{\mathrm{MBP4-p}}_{\mathscr{A}}(\kappa) = |Pr[\mathscr{A}(D, T_0) = 1] - Pr[\mathscr{A}(D, T_1) = 1]|$$

The MBP4-p assumption is said to hold if for all PPT algorithm $\mathscr{A}$, the advantage $\mathsf{Adv}^{\mathrm{MBP4-p}}_{\mathscr{A}}(\kappa)$ is a negligible function in security parameter $\kappa$.

**Lemma B.13.** *For any adversary $\mathscr{A}$, there exist a PPT algorithm $\mathscr{B}$, such that* $\mathsf{Adv}^{\mathrm{MBP4-p}}_{\mathscr{A}}(\kappa) \leq \mathsf{Adv}^{\mathrm{BP4-p}}_{\mathscr{B}}(\kappa)$*, for all $\kappa$.*

*Proof.* This proof is similar to that of lemma B.2. □

**Definition B.11** (Basic Problem 6 in [OT12b])**.** For $i = 1, 2$, choose $\mu_i, \sigma_i, \rho \xleftarrow{U} \mathbb{F}_q$; $\vec{\chi}_i, \vec{\phi}_i \xleftarrow{U} \mathbb{F}_q^2$.

$$(param, (\mathbb{B}_0, \mathbb{B}_0^*), (\mathbb{B}, \mathbb{B}^*)) \longleftarrow \mathcal{G}_{ob}(\kappa, 5, 14)$$

$$\widehat{\mathbb{B}}^* := (\vec{b}_1^*, \ldots, \vec{b}_6^*, \ \vec{b}_9^*, \ldots, \vec{b}_{14}^*), \quad \vec{h}_0^* := \rho \vec{b}_{0,2}^*, \ \vec{\tilde{h}}_\iota^* := \rho \vec{b}_\iota^* \text{ for } \iota = 5, 6, 9, 10$$

For $i = 1, 2$, define

$$\begin{aligned}
\vec{h}_i^* &:= \quad ( \ \overbrace{\mu_i, 0^3}^{4}, \ \overbrace{0^2, \rho\vec{e}_i, 0^2}^{6}, \ \overbrace{0^2}^{2}, \ \overbrace{0^2}^{2} \ )\mathbb{B}^* \\
\vec{e}_{0,i} &:= \quad ( \ \overbrace{\sigma_i, 0^3}^{4}, \ \overbrace{0^6}^{6}, \ \overbrace{0^2}^{2}, \ \overbrace{\vec{\phi}_i}^{2} \ )\mathbb{B} \\
\vec{e}_{1,i} &:= \quad ( \ \overbrace{\sigma_i, 0^3}^{4}, \ \overbrace{0^2, \vec{\chi}_i, 0^2}^{6}, \ \overbrace{0^2}^{2}, \ \overbrace{\vec{\phi}_i}^{2} \ )\mathbb{B}
\end{aligned}$$

$D := (param, \mathbb{B}_0, \mathbb{B}_0^*, \mathbb{B}, \widehat{\mathbb{B}}^*, \vec{h}_0^*, \{\vec{\tilde{h}}_\iota^*\}_{\iota=5,6,9,10}, \{\vec{h}_i^*\}_{i=1,2})$ For $\beta = 0, 1$, define $T_\beta := (\{\vec{e}_{\beta,i}\}_{i=1,2})$

Now, the advantage of an algorithm $\mathscr{A}$ in breaking this Basic Problem 6 (BP6) is defined by

$$\mathsf{Adv}_{\mathscr{A}}^{\mathrm{BP6}}(\kappa) = |Pr[\mathscr{A}(D, T_0) = 1] - Pr[\mathscr{A}(D, T_1) = 1]|$$

The BP6 assumption is said to hold if for all PPT algorithm $\mathscr{A}$, $\mathsf{Adv}_{\mathscr{A}}^{\mathrm{BP6}}(\kappa)$ is a negligible function in security parameter $\kappa$.

**Definition B.12** (**Modified Basic Problem 6**)**.** For $j = 1, 2, 3$, $i = 1, 2$, choose $\mu_i^j, \sigma_i^j, \rho \xleftarrow{U} \mathbb{F}_q$; $\vec{\chi}_i^j, \vec{\phi}_i^j \xleftarrow{U} \mathbb{F}_q^2$.

$$(param, (\mathbb{B}_0, \mathbb{B}_0^*), (\mathbb{B}_1, \mathbb{B}_1^*), (\mathbb{B}_2, \mathbb{B}_2^*), (\mathbb{B}_3, \mathbb{B}_3^*), (\mathbb{B}_4, \mathbb{B}_4^*)) \longleftarrow \mathcal{G}_{ob}(\kappa, 5, 14, 14, 14, 5)$$

For $j = 1, 2, 3$, $\widehat{\mathbb{B}}_j^* := (\vec{b}_{j,1}^*, \ldots, \vec{b}_{j,6}^*, \ \vec{b}_{j,9}^*, \ldots, \vec{b}_{j,14}^*)$, $\vec{\tilde{h}}_{j,\iota}^* := \rho \vec{b}_{j,\iota}^*$ for $\iota = 5, 6, 9, 10$; $\vec{h}_0^* := \rho \vec{b}_{0,2}^*, \vec{h}_4^* := \rho \vec{b}_{4,2}^*$

For $j = 1, 2, 3$, $i = 1, 2$, define

$$\begin{aligned}
\vec{h}_i^{j*} &:= \quad ( \ \overbrace{\mu_i^j, 0^3}^{4}, \ \overbrace{0^2, \rho\vec{e}_i, 0^2}^{6}, \ \overbrace{0^2}^{2}, \ \overbrace{0^2}^{2} \ )\mathbb{B}_j^* \\
\vec{e}_{0,i}^{j} &:= \quad ( \ \overbrace{\sigma_i^j, 0^3}^{4}, \ \overbrace{0^6}^{6}, \ \overbrace{0^2}^{2}, \ \overbrace{\vec{\phi}_i^j}^{2} \ )\mathbb{B}_j \\
\vec{e}_{1,i}^{j} &:= \quad ( \ \overbrace{\sigma_i^j, 0^3}^{4}, \ \overbrace{0^2, \vec{\chi}_i^j, 0^2}^{6}, \ \overbrace{0^2}^{2}, \ \overbrace{\vec{\phi}_i^j}^{2} \ )\mathbb{B}_j
\end{aligned}$$

$D := (param, \{\mathbb{B}_\iota, \mathbb{B}_\iota^*\}_{\iota=0,4}, \{\mathbb{B}_j, \widehat{\mathbb{B}}_j^*\}_{j=1,2,3}, \vec{h}_0^*, \vec{h}_4^*, \{\vec{\tilde{h}}_{j,\iota}^*\}_{j=1,2,3;\ \iota=5,6,9,10}, \{\vec{h}_i^{j*}\}_{j=1,2,3;\ i=1,2})$. For $\beta = 0, 1$, define $T_\beta := (\{\vec{e}_{\beta,i}^{j}\}_{j=1,2,3;\ i=1,2})$.
Now, the advantage of an algorithm $\mathscr{A}$ in breaking this **Modified Basic Problem 6** (MBP6) is defined by

$$\mathsf{Adv}_{\mathscr{A}}^{\mathrm{MBP6}}(\kappa) = |Pr[\mathscr{A}(D, T_0) = 1] - Pr[\mathscr{A}(D, T_1) = 1]|$$

The MBP6 assumption is said to hold if for all PPT algorithm $\mathscr{A}$, the advantage $\mathsf{Adv}_{\mathscr{A}}^{\mathrm{MBP6}}(\kappa)$ is a negligible function in security parameter $\kappa$.

**Lemma B.14.** *For any adversary $\mathscr{A}$, there exist a PPT algorithm $\mathscr{B}_1$, such that for all $\kappa$, $\mathsf{Adv}_{\mathscr{A}}^{\mathrm{MBP6}}(\kappa) \leq \sum_{j=1}^{3}\sum_{i=1}^{2} \mathsf{Adv}_{\mathscr{B}_{1-j-i}}^{\mathrm{BP0}}(\kappa)$, where $\mathscr{B}_{1-j-i}(.) = \mathscr{B}_1(j, i, .)$*

*Proof.* The proof technique of lemma B.14 is adapted from that of lemma 43 in [OT12b], i.e., MBP6 is organized as hybrid of the experiments Exp 0, Exp 1-1-1, Exp 1-1-2, Exp 1-2-1, …,Exp 1-3-2. Thus, the advantage of $\mathscr{A}$ in MBP6 is the advantage gap between Exp 0 and Exp 1-3-2, i.e., we have $\mathsf{Adv}_{\mathscr{A}}^{\mathrm{MBP6}}(\kappa) = |Pr[\mathsf{Exp}_{\mathscr{A}}^{0}(\kappa) = 1] - Pr[\mathsf{Exp}_{\mathscr{A}}^{1\text{-}3\text{-}2}(\kappa) = 1]|$. Therefore, from lemma B.15, we conclude the lemma B.14. □

**Experiments**

Below, we define the sequence of experiments almost the same as in lemma 43 in [OT12b], except we consider here, two 5-dimensional dual bases and three 14-dimensional dual bases. In the following sketch, we show how to change Exp 0 to Exp 1-3-2 under BP0.

$$\boxed{\mathsf{Exp\ 0}} = \boxed{\mathsf{Exp\ 1\text{-}0\text{-}2}} \overset{\text{BP0}}{\approx} \boxed{\mathsf{Exp\ 1\text{-}1\text{-}1}} \overset{\text{BP0}}{\approx} \boxed{\mathsf{Exp\ 1\text{-}1\text{-}2}} \overset{\text{BP0}}{\approx} \boxed{\mathsf{Exp\ 1\text{-}2\text{-}1}} \cdots \boxed{\mathsf{Exp\ 1\text{-}3\text{-}1}} \overset{\text{BP0}}{\approx} \boxed{\mathsf{Exp\ 1\text{-}3\text{-}2}}$$

Exp 0 : It is defined to be the $\beta = 0$ case of MBP6 as shown below

for $j = 1, 2, 3$, $\vec{\vec{h}}^*_{j,\iota} := \rho \vec{b}^*_{j,\iota}$ for $\iota = 5, 6, 9, 10$; $\vec{h}^*_0 := \rho \vec{b}^*_{0,2}, \vec{h}^*_4 := \rho \vec{b}^*_{4,2}$

for $j = 1, 2, 3$; $i = 1, 2$

$$\vec{h}^{j*}_i := \quad ( \overbrace{\mu^j_i, 0^3}^{4}, \quad \overbrace{0^2, \rho\vec{e}_i, 0^2}^{6}, \quad \overbrace{0^2}^{2}, \quad \overbrace{0^2}^{2} \quad )\mathbb{B}^*_j$$

$$\vec{e}^j_i := \quad ( \overbrace{\sigma^j_i, 0^3}^{4}, \quad \overbrace{0^2, \boxed{0^2}, 0^2}^{6}, \quad \overbrace{0^2}^{2}, \quad \overbrace{\vec{\phi}^j_i}^{2} \quad )\mathbb{B}_j$$

Rest of the variables are defined as in MBP6.

Exp 1-j-i (for $j = 1, 2, 3$, $i = 1, 2$): This is Same as Exp 1-j-(i-1) if $i = 2$, or this is Same as Exp 1-(j-1)-(i+1) if $i = 1$ except the following

$$\vec{e}^j_i := \quad ( \overbrace{\sigma^j_i, 0^3}^{4}, \quad \overbrace{0^2, \boxed{\vec{\chi}^j_i}, 0^2}^{6}, \quad \overbrace{0^2}^{2}, \quad \overbrace{\vec{\phi}^j_i}^{2} \quad )\mathbb{B}_j, \quad \text{where } \vec{\chi}^j_i \xleftarrow{\text{U}} \mathbb{F}_q^2$$

Thus, Exp 1-0-2 is Exp 0.

**Lemma B.15.** *For any adversary $\mathscr{A}$, there exist a PPT algorithm $\mathscr{B}_1$, such that for all $\kappa$, $j = 1, 2, 3$, we have $|Pr[\mathsf{Exp}^{1\text{-}j\text{-}i}_{\mathscr{A}}(\kappa) = 1] - Pr[\mathsf{Exp}^{1\text{-}j\text{-}(i\text{-}1)}_{\mathscr{A}}(\kappa) = 1]| \leq \mathsf{Adv}^{\text{BP0}}_{\mathscr{B}_{1-j-i}}(\kappa)$, if $i = 2$, $|Pr[\mathsf{Exp}^{1\text{-}j\text{-}i}_{\mathscr{A}}(\kappa) = 1] - Pr[\mathsf{Exp}^{1\text{-}(j\text{-}1)\text{-}(i+1)}_{\mathscr{A}}(\kappa) = 1]| \leq \mathsf{Adv}^{\text{BP0}}_{\mathscr{B}_{1-j-i}}(\kappa)$, if $i = 1$, where $\mathscr{B}_{1-j-i}(.) = \mathscr{B}_1(j, i, .)$.*

*Proof.* We only prove the case $i = 2$. Similarly, lemma B.15 for the case $i = 1$ can be proven. The proof of the lemma B.15 is almost the same as that of lemma 44 in [OT12b]. $\mathscr{B}_1$ is given the instance $(param_{BP0}, \mathbb{B}, \widehat{\mathbb{B}}^*, \{\vec{h}^*_i\}_{i=1,2}, \vec{e}_\beta, \lambda P, \xi P, \rho\xi P)$ of Basic Problem 0. Now, using $param_{\mathbb{G}} := (q, \mathbb{G}, \mathbb{G}_T, P, e)$ of $param_{BP0}$, $\mathscr{B}_1$ computes $param_{\mathbb{V}_t} := (q, \mathbb{V}_t, \mathbb{G}_T, \mathbb{A}_t, e) \leftarrow \mathcal{G}_{dpvs}(\kappa, N_t, param_{\mathbb{G}})$ for $t = 0, \ldots, 4$, where $N_t = 5$ for $t = 0, 4$ and $N_t = 14$ for $t = 1, 2, 3$. Then, $\mathscr{B}_1$ sets $param := (\{param_{\mathbb{V}_t}\}_{t=0,\ldots,4}, g_T)$, where $g_T = e(\lambda P, \xi P)$ belongs to $param_{BP0}$. $\mathscr{B}_1$ chooses $W_0, W_4 \xleftarrow{\text{U}} GL(5, \mathbb{F}_q)$, $W_1, W_2, W_3 \xleftarrow{\text{U}} GL(14, \mathbb{F}_q)$. Now, $\mathscr{B}_1$ defines new bases $(\mathbb{D}_j, \mathbb{D}^*_j)$ for $j = 0, \ldots, 4$ by setting the following

$$\begin{aligned}
\vec{d}_{t,\iota} &:= (0^{\iota-1}, \lambda P, 0^{5-\iota})W_t \quad \vec{d}^*_{t,\iota} := (0^{\iota-1}, \xi P, 0^{5-\iota})(W_t^{-1})^T \text{ for } t = 0, 4,\ \iota = 1, \ldots, 5\\
\vec{d}_{t,1} &:= (\vec{b}_1, 0^9)W_t \quad \vec{d}^*_{t,1} := (\vec{b}^*_1, 0^9)(W_t^{-1})^T \text{ for } t = 1, 2, 3\\
\vec{d}_{t,7} &:= (\vec{b}_2, 0^9)W_t \quad \vec{d}^*_{t,7} := (\vec{b}^*_2, 0^9)(W_t^{-1})^T,\ \vec{d}_{t,8} := (\vec{b}_3, 0^9)W_t \quad \vec{d}^*_{t,8} := (\vec{b}^*_3, 0^9)(W_t^{-1})^T \text{ for } t = 1, 2, 3\\
\vec{d}_{t,13} &:= (\vec{b}_4, 0^9)W_t \quad \vec{d}^*_{t,13} := (\vec{b}^*_4, 0^9)(W_t^{-1})^T,\ \vec{d}_{t,14} := (\vec{b}_5, 0^9)W_t \quad \vec{d}^*_{t,14} := (\vec{b}^*_5, 0^9)(W_t^{-1})^T \text{ for } t = 1, 2, 3\\
\vec{d}_{t,\iota} &:= (0^5, 0^{\iota-2}, \lambda P, 0^{10-\iota})W_t \quad \vec{d}^*_{t,\iota} := (0^5, 0^{\iota-2}, \xi P, 0^{10-\iota})(W_t^{-1})^T \text{ for } t = 1, 2, 3,\ \iota = 2, \ldots, 6\\
\vec{d}_{t,\iota} &:= (0^{\iota+1}, \lambda P, 0^{12-\iota})W_t \quad \vec{d}^*_{t,\iota} := (0^{\iota+1}, \xi P, 0^{12-\iota})(W_t^{-1})^T \text{ for } t = 1, 2, 3,\ \iota = 6, \ldots, 12\\
\vec{e}^j_{\beta,2} &:= (\vec{e}_\beta, 0^9)W_j \quad \vec{e}^j_{\beta,1} := (\sigma^j_1, 0^{11}, \vec{\phi}^j_1)W_j,\ \sigma^j_1 \xleftarrow{\text{U}} \mathbb{F}_q,\ \vec{\phi}^j_1\\
\vec{e}^t_{\beta,\iota} &:= (\sigma^t_\iota, 0^{11}, \vec{\phi}^t_\iota)W_t \text{ for } t = 1, 2, 3,\ t \neq j,\ \iota = 1, 2\ \sigma^t_\iota \xleftarrow{\text{U}} \mathbb{F}_q,\ \vec{\phi}^t_\iota \xleftarrow{\text{U}} \mathbb{F}_q^2\\
\vec{p}^*_t &:= (0, \rho\xi P, 0^3)(W_t^{-1})^T \text{ for } t = 0, 4 \quad \vec{p}^{t*}_\iota := (0^{\iota-1}, \rho\xi P, 0^{14-\iota})(W_t^{-1})^T \text{ for } t = 1, 2, 3,\ \iota = 5, 6, 9, 10\\
\vec{p}^{t*}_\iota &:= (\vec{h}^*_\iota, 0^9)(W_t^{-1})^T + \delta^t_\iota \vec{d}^*_{t,1} \text{ for } t = 1, 2, 3,\ \iota = 1, 2,\ \delta^t_\iota \xleftarrow{\text{U}} \mathbb{F}_q
\end{aligned}$$

$$\begin{aligned}
\mathbb{D}_t &:= (\vec{d}_{t,1}, \ldots, \vec{d}_{t,5}) \quad \mathbb{D}^*_t := (\vec{d}^*_{t,1}, \ldots, \vec{d}^*_{t,5}) \text{ for } t = 0, 4\\
\mathbb{D}_t &:= (\vec{d}_{t,1}, \ldots, \vec{d}_{t,14}) \quad \mathbb{D}^*_t := (\vec{d}^*_{t,1}, \ldots, \vec{d}^*_{t,14}) \text{ for } t = 1, 2, 3
\end{aligned}$$

It is verified that $(\mathbb{D}_t, \mathbb{D}^*_t)$ for $t = 0, \ldots, 4$ are dual orthonormal bases. Note, that $\mathscr{B}_1$ can compute almost all the vectors in $(\mathbb{D}_t, \mathbb{D}^*_t)$ for $t = 0, \ldots, 4$ from $\mathbb{B}, \widehat{\mathbb{B}}^* := (\vec{b}^*_1, \vec{b}^*_4, \vec{b}^*_5), \lambda P$ and $\xi P$ except

$\vec{d}_{t,7}, \vec{d}_{t,8}$ for $t = 1,2,3$. $\mathscr{B}_1$ sets $\widehat{\mathbb{B}}_t^* := (\vec{d}_{t,1}^*, \ldots, \vec{d}_{t,6}^*, \vec{d}_{t,9}^*, \ldots, \vec{d}_{t,14}^*)$ for $t = 1,2,3$. Then $\mathscr{B}_1$ returns $\mathcal{G} := (param, \{\mathbb{D}_t, \mathbb{D}_t^*\}_{t=0,4}, \{\mathbb{D}_t, \widehat{\mathbb{D}}_t^*\}_{t=1,2,3}, \{\vec{p}_t^*\}_{t=0,4}, \{\vec{p}_\iota^{t*}\}_{t=1,2,3;\ \iota=5,6,9,10}, \{\vec{p}_\iota^{t*}\}_{t=1,2,3;\ \iota=1,2}, \{\vec{e}_{\beta,\iota}^{t}\}_{t=1,2,3;\ \iota=1,2})$ to $\mathscr{A}$. Finally, $\mathscr{B}_1$ outputs a bit $b \in \{0,1\}$ if the adversary $\mathscr{A}$ returns $b$. Therefore, it shows that if $\beta = 0$ (resp. $\beta = 1$), the distribution of $\mathcal{G}$ is exactly the same as that of $\mathsf{Exp}$ 1-j-(i-1) (resp. $\mathsf{Exp}$ 1-j- i) for $i = 2;\ j = 1,2,3$. □

**Definition B.13** (Basic Problem 5-p in [OT12b] for $p = 1, \ldots, d$)**.**

$$(param, (\mathbb{B}_0, \mathbb{B}_0^*), (\mathbb{B}, \mathbb{B}^*)) \longleftarrow \mathcal{G}_{ob}(\kappa, 5, 14), \quad \text{choose } \rho \xleftarrow{\mathrm{U}} \mathbb{F}_q$$

$$\widehat{\mathbb{B}}^* := (\vec{b}_1^*, \ldots, \vec{b}_6^*,\ \vec{b}_9^*, \ldots, \vec{b}_{14}^*), \quad \vec{h}_0^* := \rho \vec{b}_{0,2}^*,\ \vec{\tilde{h}}_\iota^* := \rho \vec{b}_\iota^* \text{ for } \iota = 5,6,9,10$$

For $\ell = 1, \ldots, p-1, p+1, \ldots, d$, $i = 1,2$, choose $\vec{\eta}_{p,i}, \vec{\chi}_{\ell,i}, \vec{\phi}_{\ell,i} \xleftarrow{\mathrm{U}} \mathbb{F}_q^2$; $\mu_{p,i}, \sigma_{\ell,i} \xleftarrow{\mathrm{U}} \mathbb{F}_q$

$$\begin{aligned}
\vec{h}_{p,i}^* &:= \quad ( \overbrace{\mu_{p,i}(p,-1), 0^2}^{4}, \overbrace{0^2, \rho\vec{e}_i, 0^2}^{6}, \overbrace{\vec{\eta}_{p,i}}^{2}, \overbrace{0^2}^{2} )\mathbb{B}^* \\
\vec{e}_{0,\ell,i} &:= \quad ( \overbrace{\sigma_{\ell,i}(1,\ell), 0^2}^{4}, \overbrace{0^6}^{6}, \overbrace{0^2}^{2}, \overbrace{\vec{\phi}_{\ell,i}}^{2} )\mathbb{B} \\
\vec{e}_{1,\ell,i} &:= \quad ( \overbrace{\sigma_{\ell,i}(1,\ell), 0^2}^{4}, \overbrace{0^2, \vec{\chi}_{\ell,i}, 0^2}^{6}, \overbrace{0^2}^{2}, \overbrace{\vec{\phi}_{\ell,i}}^{2} )\mathbb{B}
\end{aligned}$$

$D := (param, \mathbb{B}_0, \mathbb{B}_0^*, \mathbb{B}, \widehat{\mathbb{B}}^*, \vec{h}_0^*, \{\vec{\tilde{h}}_\iota^*\}_{\iota=5,6,9,10}, \{\vec{h}_{p,i}^*\}_{i=1,2})$ For $\beta = 0,1$, define $T_\beta := (\{\vec{e}_{\beta,\ell,i}\}_{\ell=1,\ldots,p-1,p+1,\ldots,d;\ i=1,2})$

Now, the advantage of an algorithm $\mathscr{A}$ in breaking this Basic Problem 5-p (BP5-p) is defined by

$$\mathsf{Adv}_{\mathscr{A}}^{\mathrm{BP5-p}}(\kappa) = |Pr[\mathscr{A}(D, T_0) = 1] - Pr[\mathscr{A}(D, T_1) = 1]|$$

The BP5-p assumption is said to hold if for all PPT adversary $\mathscr{A}$, the advantage $\mathsf{Adv}_{\mathscr{A}}^{\mathrm{BP5-p}}(\kappa)$ is a negligible function in security parameter $\kappa$.

**Definition B.14** (**Modified Basic Problem 5-p** for $p = 1, \ldots, d$)**.** Choose $\rho \xleftarrow{\mathrm{U}} \mathbb{F}_q$.

$$(param, (\mathbb{B}_0, \mathbb{B}_0^*), (\mathbb{B}_1, \mathbb{B}_1^*), (\mathbb{B}_2, \mathbb{B}_2^*), (\mathbb{B}_3, \mathbb{B}_3^*), (\mathbb{B}_4, \mathbb{B}_4^*)) \longleftarrow \mathcal{G}_{ob}(\kappa, 5, 14, 14, 14, 5)$$

$$\text{For } j = 1,2,3,\ \widehat{\mathbb{B}}_j^* := (\vec{b}_{j,1}^*, \ldots, \vec{b}_{j,6}^*,\ \vec{b}_{j,9}^*, \ldots, \vec{b}_{j,14}^*)$$

$$\vec{h}_j^* := \rho \vec{b}_{j,2}^*, \quad \text{for } j = 0,4, \qquad \vec{\tilde{h}}_\iota^{j*} := \rho \vec{b}_{j,\iota}^* \text{ for } \ j = 1,2,3; \iota = 5,6,9,10$$

For $\ell = 1, \ldots, p-1, p+1, \ldots, d$; $j = 1,2,3$; $i = 1,2$, choose $\vec{\eta}_{p,i}^j, \vec{\chi}_{\ell,i}^j, \vec{\phi}_{\ell,i}^j \xleftarrow{\mathrm{U}} \mathbb{F}_q^2$; $\mu_{p,i}^j, \sigma_{\ell,i}^j \xleftarrow{\mathrm{U}} \mathbb{F}_q$

$$\begin{aligned}
\vec{h}_{p,i}^{j*} &:= \quad ( \overbrace{\mu_{p,i}^j(p,-1), 0^2}^{4}, \overbrace{0^2, \rho\vec{e}_i, 0^2}^{6}, \overbrace{\vec{\eta}_{p,i}^j}^{2}, \overbrace{0^2}^{2} )\mathbb{B}_j^* \\
\vec{e}_{0,\ell,i}^j &:= \quad ( \overbrace{\sigma_{\ell,i}^j(1,\ell), 0^2}^{4}, \overbrace{0^6}^{6}, \overbrace{0^2}^{2}, \overbrace{\vec{\phi}_{\ell,i}^j}^{2} )\mathbb{B}_j \\
\vec{e}_{1,\ell,i}^j &:= \quad ( \overbrace{\sigma_{\ell,i}^j(1,\ell), 0^2}^{4}, \overbrace{0^2, \vec{\chi}_{\ell,i}^j, 0^2}^{6}, \overbrace{0^2}^{2}, \overbrace{\vec{\phi}_{\ell,i}^j}^{2} )\mathbb{B}_j
\end{aligned}$$

$D := (param, \{\mathbb{B}_\iota, \mathbb{B}_\iota^*\}_{\iota=0,4}, \{\mathbb{B}_j, \widehat{\mathbb{B}}_j^*\}_{j=1,2,3}, \{\vec{h}_j^*\}_{j=0,4}, \{\vec{\tilde{h}}_\iota^{j*}\}_{j=1,2,3;\ \iota=5,6,9,10}, \{\vec{h}_{p,i}^{j*}\}_{j=1,2,3;\ i=1,2})$. For $\beta = 0,1$, define $T_\beta := (\{\vec{e}_{\beta,\ell,i}^j\}_{\ell=1,\ldots,p-1,p+1,\ldots,d;\ j=1,2,3;\ i=1,2})$.

Now, the advantage of an algorithm $\mathscr{A}$ in breaking this **Modified Basic Problem 5-p** (MBP5-p) is defined by

$$\mathsf{Adv}_{\mathscr{A}}^{\mathrm{MBP5-p}}(\kappa) = |Pr[\mathscr{A}(D, T_0) = 1] - Pr[\mathscr{A}(D, T_1) = 1]|$$

The MBP5-p assumption is said to hold if for all PPT adversary $\mathscr{A}$, $\mathsf{Adv}_{\mathscr{A}}^{\mathrm{MBP5-p}}(\kappa)$ is a negligible function in security parameter $\kappa$.

**Lemma B.16.** *For any adversary $\mathscr{A}$, there exist a PPT algorithm $\mathscr{B}$, such that* $\mathsf{Adv}^{\mathrm{MBP5-p}}_{\mathscr{A}_p}(\kappa) \leq \sum_{\ell=1,\ldots,p-1,p+1,\ldots,d} \mathsf{Adv}^{\mathrm{MBP6}}_{\mathscr{B}_{p,\ell}}(\kappa)$*, for all $\kappa$, where $\mathscr{A}_p(.) = \mathscr{A}(p,.)$ and $\mathscr{B}_{p,\ell}(.) = \mathscr{B}(p,\ell,.)$.*

*Proof.* The proof technique of lemma B.16 adapts the same of lemma 40 in [OT12b], i.e, MBP5-p is organized as hybrid of the experiments Exp 0, Exp 1,...,Exp p-1, Exp p+1,...,Exp d. Thus, the advantage of $\mathscr{A}$ in MBP5-p is the advantage gap between Exp 0 and Exp d i.e., $\mathsf{Adv}^{\mathrm{MBP5-p}}_{\mathscr{A}_p}(\kappa) = |Pr[\mathsf{Exp}^0_{\mathscr{A}_p}(\kappa) = 1] - Pr[\mathsf{Exp}^d_{\mathscr{A}_p}(\kappa) = 1]|$. Therefore, from lemma B.17, we conclude lemma B.16. □

**Experiments**

Below, we define the sequence of experiments almost the same as in lemma 40 in [OT12b], except we consider here, two 5-dimensional dual bases and three 14-dimensional dual bases. In the following sketch, we show how to change Exp 0 to Exp d under MBP6.

$$\boxed{\mathsf{Exp}\ 0} \overset{\mathrm{MBP6}}{\approx} \boxed{\mathsf{Exp}\ 1} \cdots \boxed{\mathsf{Exp}\ (\text{p-1})} \overset{\mathrm{MBP6}}{\approx} \boxed{\mathsf{Exp}\ (\text{p+1})} \cdots \boxed{\mathsf{Exp}\ \text{d-1}} \overset{\mathrm{MBP6}}{\approx} \boxed{\mathsf{Exp}\ \text{d}}$$

Exp 0 : It is defined to be the $\beta = 0$ case of MBP5-p as shown below
for $\ell = 1,\ldots,p-1,p+1,\ldots,d$, $j = 1,2,3$, $i = 1,2$

$$\vec{e}^{\,j}_{\ell,i} := \quad ( \overbrace{\sigma^j_{\ell,i}(1,\ell), 0^2}^{4}, \quad \overbrace{0^2, \boxed{0^2}, 0^2}^{6}, \quad \overbrace{0^2}^{2}, \quad \overbrace{\vec{\phi}^j_{\ell,i}}^{2} \quad )\mathbb{B}_j$$

Rest of the variables are defined as in MBP5-p.

Exp $\ell$ (for $\ell = 1,\ldots,p-1,p+1,\ldots,d$) : This is same as Exp $\ell-1$ if $\ell \neq p+1$ and Exp $p-1$ if $\ell = p+1$ except for $j = 1,2,3$, $i = 1,2$

$$\vec{e}^{\,j}_{\ell,i} := \quad ( \overbrace{\sigma^j_{\ell,i}(1,\ell), 0^2}^{4}, \quad \overbrace{0^2, \boxed{\vec{\chi}^j_{\ell,i}}, 0^2}^{6}, \quad \overbrace{0^2}^{2}, \quad \overbrace{\vec{\phi}^j_{\ell,i}}^{2} \quad )\mathbb{B}_j, \quad \text{where } \vec{\chi}^j_{\ell,i} \xleftarrow{\mathrm{U}} \mathbb{F}_q^2$$

**Lemma B.17.** *For any adversary $\mathscr{A}$, there exist a PPT algorithm $\mathscr{B}$, such that for all $\kappa$, $|Pr[\mathsf{Exp}^{\ell}_{\mathscr{A}_{p,\ell}}(\kappa) = 1] - Pr[\mathsf{Exp}^{\ell-1}_{\mathscr{A}_{p,\ell}}(\kappa) = 1]| \leq \mathsf{Adv}^{\mathrm{MBP6}}_{\mathscr{B}_{p,\ell}}(\kappa)$, if $\ell \neq p+1$, $|Pr[\mathsf{Exp}^{p+1}_{\mathscr{A}_{p,p+1}}(\kappa) = 1] - Pr[\mathsf{Exp}^{p-1}_{\mathscr{A}_{p,p+1}}(\kappa) = 1]| \leq \mathsf{Adv}^{\mathrm{MBP6}}_{\mathscr{B}_{p,p+1}}(\kappa)$, if $\ell = p+1$, where $\mathscr{B}_{p,\ell}(.) = \mathscr{B}(p,\ell,.)$, $\mathscr{A}_{p,\ell}(.) = \mathscr{A}(p,\ell,.)$.*

*Proof.* We only prove the case $\ell \neq p+1$. Similarly, the lemma B.17 for the case $\ell = p+1$ can be proven. The proof of the lemma B.17 is almost the same as that of lemma 41 in [OT12b]. $\mathscr{B}$ is given the instance $(param, \{\mathbb{B}_\iota, \mathbb{B}^*_\iota\}_{\iota=0,4}, \{\mathbb{B}_j, \widehat{\mathbb{B}}^*_j\}_{j=1,2,3}, \vec{h}^*_0, \vec{h}^*_4, \{\vec{\tilde{h}}^*_{j,\iota}\}_{j=1,2,3;\ \iota=5,6,9,10}, \{\vec{h}^{j*}_i, \vec{e}^{\,j}_{\beta,i}\}_{j=1,2,3;\ i=1,2})$ of **Modified Basic Problem 6** and integers $p,\ell$. For $j = 1,2,3$, $\mathscr{B}$ computes the following

$$\begin{pmatrix} \vec{d}_{j,1} \\ \vec{d}_{j,2} \end{pmatrix} := Z \begin{pmatrix} \vec{b}_{j,1} \\ \vec{b}_{j,2} \end{pmatrix} := \begin{pmatrix} p & \ell \\ -1 & -1 \end{pmatrix} \begin{pmatrix} \vec{b}_{j,1} \\ \vec{b}_{j,2} \end{pmatrix}, \text{ where } Z := \begin{pmatrix} p & \ell \\ -1 & -1 \end{pmatrix}$$

$$\begin{pmatrix} \vec{d}^*_{j,1} \\ \vec{d}^*_{j,2} \end{pmatrix} := U \begin{pmatrix} \vec{b}^*_{j,1} \\ \vec{b}^*_{j,2} \end{pmatrix} := (\ell - p)^{-1} \begin{pmatrix} -1 & 1 \\ -\ell & p \end{pmatrix} \begin{pmatrix} \vec{b}^*_{j,1} \\ \vec{b}^*_{j,2} \end{pmatrix}, \text{ where } U := (Z^{-1})^T$$

$\mathbb{D}_j := (\vec{d}_{j,1}, \vec{d}_{j,2}, \vec{b}_{j,3}, \ldots, \vec{b}_{j,14})$, $\mathbb{D}^*_j := (\vec{d}^*_{j,1}, \vec{d}^*_{j,2}, \vec{b}^*_{j,3}, \ldots, \vec{b}^*_{j,14})$
$\widehat{\mathbb{D}}^*_j := (\vec{d}^*_{j,1}, \vec{d}^*_{j,2}, \vec{b}^*_{j,3}, \ldots, \vec{b}^*_{j,6}, \vec{b}^*_{j,9}, \ldots, \vec{b}^*_{j,14})$
$\vec{h}^{j*}_{p,i} := \vec{h}^{j*}_i$, $\vec{e}^{\,j}_{\beta,\ell,i} := \vec{e}^{\,j}_{\beta,i}$

$\mathscr{B}$ can compute $\{\vec{e}^{\,j}_{\beta,t,i}\}_{t=1,\ldots,d,t\neq p,\ell;\ j=1,2,3}$ using the dual bases $\mathbb{B}_j, \mathbb{B}^*_j$ and $\vec{\delta}^j_{t,i}, \vec{\phi}^j_{t,i} \xleftarrow{\mathrm{U}} \mathbb{F}_q^2$ as defined in Exp $\ell$. Now, $\mathscr{B}$ returns $(param, \{\mathbb{B}_\iota, \mathbb{B}^*_\iota\}_{\iota=0,4}, \{\mathbb{D}_j, \widehat{\mathbb{D}}^*_j\}_{j=1,2,3}, \vec{h}^*_0, \vec{h}^*_4, \{\vec{\tilde{h}}^*_{j,\iota}\}_{j=1,2,3;\ \iota=5,6,9,10}, \{\vec{h}^{j*}_{p,i}, \vec{e}^{\,j}_{\beta,t,i}\}_{t=1,\ldots,p-1,p+1,\ldots,d;\ j=1,2,3;\ i=1,2})$ to $\mathscr{A}$. Finally, $\mathscr{B}$ outputs a bit $b \in \{0,1\}$ if the adversary $\mathscr{A}$ returns $b$. If $\beta = 0$ (resp. $\beta = 1$), the distribution of $\mathcal{G}$ can be shown to be exactly same as that of Exp $\ell-1$ (resp. Exp $\ell$) by using the similar kinds of arguments of claim 6 of lemma 41 in [OT12b]. □

**Lemma B.18.** *If DLIN assumption holds for a bilinear pairing group generator $\mathcal{G}$, then the DSS2 assumption also holds for $\mathcal{G}$. That is, for any adversary $\mathscr{A}$, there exist PPT algorithms $\mathscr{F}_1, \mathscr{F}_2$ such that for any $\kappa$,* $\mathsf{Adv}^{\mathrm{DSS2}}_{\mathscr{A}}(\kappa) \leq \mathsf{Adv}^{\mathrm{DLIN}}_{\mathscr{F}_1}(\kappa) + \sum_{p=1}^{d}\sum_{i=1}^{2}\big(\mathsf{Adv}^{\mathrm{DLIN}}_{\mathscr{F}_{2-1-p-i}}(\kappa) + \mathsf{Adv}^{\mathrm{DLIN}}_{\mathscr{F}_{2-2-p-i}}(\kappa) + \sum_{\ell=1,\ldots,p-1,p+1,\ldots,d}\big(\mathsf{Adv}^{\mathrm{DLIN}}_{\mathscr{F}_{2-3-p-i-\ell}}(\kappa) + \mathsf{Adv}^{\mathrm{DLIN}}_{\mathscr{F}_{2-4-p-i-\ell}}(\kappa)\big) + \mathsf{Adv}^{\mathrm{DLIN}}_{\mathscr{F}_{2-5-p-i}}(\kappa)\big) + \mathcal{O}(d)/q$, *where* $\mathscr{F}_{2-1-p-i}(.) = \mathscr{F}_2(1,p,i,.)$, $\mathscr{F}_{2-2-p-i}(.) = \mathscr{F}_2(2,p,i,.)$, $\mathscr{F}_{2-3-p-i-\ell}(.) = \mathscr{F}_2(3,p,i,\ell,.)$, $\mathscr{F}_{2-4-p-i-\ell}(.) = \mathscr{F}_2(4,p,i,\ell,.)$, $\mathscr{F}_{2-5-p-i}(.) = \mathscr{F}_2(5,p,i,.)$

*Proof.* The proof technique of lemma B.18 is adapted from that of lemma 24 in [OT12b], i.e., DSS2 is organized as hybrid of the experiments Exp 0, Exp 1,...,Exp 2-d-8. Thus, the advantage of $\mathscr{A}$ in DSS2 is the advantage gap between Exp 0 and Exp 2-d-8, i.e., $\mathsf{Adv}^{\mathrm{DSS2}}_{\mathscr{A}}(\kappa) = |Pr[\mathsf{Exp}^{0}_{\mathscr{A}}(\kappa) = 1] - Pr[\mathsf{Exp}^{\text{2-d-8}}_{\mathscr{A}}(\kappa) = 1]|$. Therefore, from lemmas B.7,...,B.17 and B.19,...,B.27, we have

$\mathsf{Adv}^{\mathrm{DSS2}}_{\mathscr{A}}(\kappa) = |Pr[\mathsf{Exp}^{0}_{\mathscr{A}}(\kappa) = 1] - Pr[\mathsf{Exp}^{2-d-8}_{\mathscr{A}}(\kappa) = 1]|$

$\leq |Pr[\mathsf{Exp}^{0}_{\mathscr{A}}(\kappa) = 1] - Pr[\mathsf{Exp}^{1}_{\mathscr{A}}(\kappa) = 1]| + \sum_{p=1}^{d}\big(|Pr[\mathsf{Exp}^{\text{2-p-1}}_{\mathscr{A}}(\kappa) = 1] - Pr[\mathsf{Exp}^{\text{2-p-2}}_{\mathscr{A}}(\kappa) = 1]| + |Pr[\mathsf{Exp}^{\text{2-p-3}}_{\mathscr{A}}(\kappa) = 1] - Pr[\mathsf{Exp}^{\text{2-p-4}}_{\mathscr{A}}(\kappa) = 1]| + |Pr[\mathsf{Exp}^{\text{2-p-4}}_{\mathscr{A}}(\kappa) = 1] - Pr[\mathsf{Exp}^{\text{2-p-5}}_{\mathscr{A}}(\kappa) = 1]| + |Pr[\mathsf{Exp}^{\text{2-p-6}}_{\mathscr{A}}(\kappa) = 1] - Pr[\mathsf{Exp}^{\text{2-p-7}}_{\mathscr{A}}(\kappa) = 1]| + |Pr[\mathsf{Exp}^{\text{2-p-7}}_{\mathscr{A}}(\kappa) = 1] - Pr[\mathsf{Exp}^{\text{2-p-8}}_{\mathscr{A}}(\kappa) = 1]|\big)$

$\leq \mathsf{Adv}^{\mathrm{MBP2}}_{\mathscr{B}_1}(\kappa) + \sum_{p=1}^{d}\big(\mathsf{Adv}^{\mathrm{MBP3-p}}_{\mathscr{B}_{2-1-p}}(\kappa) + \mathsf{Adv}^{\mathrm{MBP3-p}}_{\mathscr{B}_{2-2-p}}(\kappa) + \mathsf{Adv}^{\mathrm{MBP5-p}}_{\mathscr{B}_{2-3-p}}(\kappa) + \mathsf{Adv}^{\mathrm{MBP5-p}}_{\mathscr{B}_{2-4-p}}(\kappa) + \mathsf{Adv}^{\mathrm{MBP4-p}}_{\mathscr{B}_{2-5-p}}(\kappa)\big)$

$\leq \mathsf{Adv}^{\mathrm{DLIN}}_{\mathscr{F}_1}(\kappa) + \sum_{p=1}^{d}\sum_{i=1}^{2}\big(\mathsf{Adv}^{\mathrm{DLIN}}_{\mathscr{F}_{2-1-p-i}}(\kappa) + \mathsf{Adv}^{\mathrm{DLIN}}_{\mathscr{F}_{2-2-p-i}}(\kappa) + \sum_{\ell=1,\ldots,p-1,p+1,\ldots,d}\big(\mathsf{Adv}^{\mathrm{DLIN}}_{\mathscr{F}_{2-3-p-i-\ell}}(\kappa) + \mathsf{Adv}^{\mathrm{DLIN}}_{\mathscr{F}_{2-4-p-i-\ell}}(\kappa)\big) + \mathsf{Adv}^{\mathrm{DLIN}}_{\mathscr{F}_{2-5-p-i}}(\kappa)\big) + \mathcal{O}(d)/q.$

This concludes the lemma B.18. □

### Experiments

Below, we define the sequence of experiments almost the same as in lemma 24 in [OT12b], except we consider here, two 5-dimensional dual bases and three 14-dimensional dual bases. In the following sketch, we show how to change Exp 0 to Exp 2-d-8 under $MBP2, \{MBP3-p, MBP4-p, MBP5-p\}_{p=1,\ldots,d}$.

$$\boxed{\text{Exp 0}} \overset{\text{MBP2}}{\approx} \boxed{\text{Exp 1}} = \boxed{\text{Exp 2-0-8}} \approx \boxed{\text{Exp 2-1-1}} \cdots \boxed{\text{Exp 2-(p-1)-8}}$$

$$\boxed{\text{Exp 2-(p-1)-8}} \approx \boxed{\text{Exp 2-p-1}} \overset{\text{MBP3-p}}{\approx} \boxed{\text{Exp 2-p-2}} \approx \boxed{\text{Exp 2-p-3}} \overset{\text{MBP3-p}}{\approx} \boxed{\text{Exp 2-p-4}}$$

$$\boxed{\text{Exp 2-p-4}} \overset{\text{MBP5-p}}{\approx} \boxed{\text{Exp 2-p-5}} \approx \boxed{\text{Exp 2-p-6}} \overset{\text{MBP5-p}}{\approx} \boxed{\text{Exp 2-p-7}} \overset{\text{MBP4-p}}{\approx} \boxed{\text{Exp 2-p-8}}$$

$$\boxed{\text{Exp 2-p-8}} \approx \boxed{\text{Exp 2-(p+1)-1}} \cdots \boxed{\text{Exp 2-d-8}}$$

Exp 0 : It is defined to be the case of DSS2 as shown below

$$\vec{h}_0^{j*} := (\zeta,\ \boxed{0},\ 0,\ \eta_0^j,\ 0)\mathbb{B}_j^*,\ \text{for } j = 0, 4$$

$$\vec{e}^{j} := (\omega,\ \tau,\ 0,\ 0,\ \phi_0^j)\mathbb{B}_j,\ \text{for } j = 0, 4$$

For $t = 1, \ldots, d$; $j = 1, 2, 3$; $i = 1, 2$

$$\vec{h}^{j*}_{t,i} := \Big(\overbrace{\mu^j_{t,i}(t,-1), \zeta\vec{e}_i}^{4},\ \overbrace{\boxed{0^6}}^{6},\ \overbrace{\vec{\eta}^j_{t,i}}^{2},\ \overbrace{0^2}^{2}\Big)\mathbb{B}_j^*$$

$$\vec{e}^{j}_{t,i} := \Big(\overbrace{\sigma^j_{t,i}(1,t), \omega\vec{e}_i}^{4},\ \overbrace{\tau\vec{e}_i, \boxed{0^2}, \tau\vec{e}_i Z_t}^{6},\ \overbrace{0^2}^{2},\ \overbrace{\vec{\phi}^j_{t,i}}^{2}\Big)\mathbb{B}_j$$

Rest of the variables are defined as in DSS2.

Exp 1 : This is same as Exp 0 except the following

$$\vec{h}_0^{j*} := (\zeta,\ \boxed{\rho},\ 0,\ \eta_0^j,\ 0)\mathbb{B}_j^*,\ \text{for } j = 0, 4$$

For $t = 1, \ldots, d$; $j = 1, 2, 3$; $i = 1, 2$

$$\vec{h}^{j*}_{t,i} := \quad ( \quad \overbrace{\mu^j_{t,i}(t,-1), \zeta\vec{e}_i}^{4}, \quad \overbrace{\boxed{\rho\vec{e}_i}, 0^4}^{6}, \quad \overbrace{\vec{\eta}^j_{t,i}}^{2}, \quad \overbrace{0^2}^{2} \quad )\mathbb{B}^*_j, \quad \text{where } \rho \xleftarrow{\text{U}} \mathbb{F}_q$$

Exp 2-p-1 (for $p = 1, \ldots, d$) : This is same as Exp 2-(p-1)-8 except the following
For $t = 1, \ldots, d$; $j = 1, 2, 3$; $i = 1, 2$

$$\vec{e}^{j}_{t,i} := \quad ( \quad \overbrace{\sigma^j_{t,i}(1,t), \omega\vec{e}_i}^{4}, \quad \overbrace{\tau\vec{e}_i, \boxed{\tau\vec{e}_i}, \tau\vec{e}_i Z_t}^{6}, \quad \overbrace{0^2}^{2}, \quad \overbrace{\vec{\phi}^j_{t,i}}^{2} \quad )\mathbb{B}_j$$

Thus, Exp 1 is Exp 2-0-8.

Exp 2-p-2 (for $p = 1, \ldots, d$): This is same as Exp 2-p-1 except the following
For $j = 1, 2, 3$; $i = 1, 2$

$$\vec{h}^{j*}_{p,i} := \quad ( \quad \overbrace{\mu^j_{p,i}(p,-1), \zeta\vec{e}_i}^{4}, \quad \overbrace{\boxed{(\rho - \theta_{p,i})\vec{e}_i, \theta_{p,i}\vec{e}_i}, 0^2}^{6}, \quad \overbrace{\vec{\eta}^j_{p,i}}^{2}, \quad \overbrace{0^2}^{2} \quad )\mathbb{B}^*_j, \quad \text{where } \theta_{p,i} \xleftarrow{\text{U}} \mathbb{F}_q$$

Remark : for $j = 1, 2, 3$, we use the same $\theta_{p,i}$.

Exp 2-p-3 (for $p = 1, \ldots, d$) : This is same as Exp 2-p-2 except the following
For $j = 1, 2, 3$; $i = 1, 2$

$$\vec{h}^{j*}_{p,i} := \quad ( \quad \overbrace{\mu^j_{p,i}(p,-1), \zeta\vec{e}_i}^{4}, \quad \overbrace{\boxed{\theta_{p,i}\vec{e}_i, (\rho - \theta_{p,i})\vec{e}_i}, 0^2}^{6}, \quad \overbrace{\vec{\eta}^j_{p,i}}^{2}, \quad \overbrace{0^2}^{2} \quad )\mathbb{B}^*_j$$

Remark : for $j = 1, 2, 3$, we use the same $\theta_{p,i}$.

Exp 2-p-4 (for $p = 1, \ldots, d$): This is same as Exp 2-p-3 except the following
For $j = 1, 2, 3$; $i = 1, 2$

$$\vec{h}^{j*}_{p,i} := \quad ( \quad \overbrace{\mu^j_{p,i}(p,-1), \zeta\vec{e}_i}^{4}, \quad \overbrace{\boxed{0^2, \rho\vec{e}_i}, 0^2}^{6}, \quad \overbrace{\vec{\eta}^j_{p,i}}^{2}, \quad \overbrace{0^2}^{2} \quad )\mathbb{B}^*_j$$

Exp 2-p-5 (for $p = 1, \ldots, d$): This is same as Exp 2-p-4 except the following
For $\ell = 1, \ldots, p-1, p+1, \ldots, d$; $j = 1, 2, 3$; $i = 1, 2$

$$\vec{e}^{j}_{\ell,i} := \quad ( \quad \overbrace{\sigma^j_{\ell,i}(1,\ell), \omega\vec{e}_i}^{4}, \quad \overbrace{\tau\vec{e}_i, \boxed{\vec{\chi}^j_{\ell,i}}, \tau\vec{e}_i Z_\ell}^{6}, \quad \overbrace{0^2}^{2}, \quad \overbrace{\vec{\phi}^j_{\ell,i}}^{2} \quad )\mathbb{B}_j, \quad \text{where } \vec{\chi}^j_{\ell,i} \xleftarrow{\text{U}} \mathbb{F}_q^2$$

Remark : for a fixed $\ell$ and $i$, $\vec{\chi}^j_{\ell,i}$ are independent for $j = 1, 2, 3$.

Exp 2-p-6 (for $p = 1, \ldots, d$): This is same as Exp 2-p-5 except the following
For $j = 1, 2, 3$; $i = 1, 2$

$$\vec{h}^{j*}_{p,i} := \quad ( \quad \overbrace{\mu^j_{p,i}(p,-1), \zeta\vec{e}_i}^{4}, \quad \overbrace{0^2, \boxed{\xi\vec{e}_i, \rho\vec{e}_i U_p}}^{6}, \quad \overbrace{\vec{\eta}^j_{p,i}}^{2}, \quad \overbrace{0^2}^{2} \quad )\mathbb{B}^*_j$$

$$\vec{e}^{j}_{p,i} := \quad ( \quad \overbrace{\sigma^j_{p,i}(1,p), \omega\vec{e}_i}^{4}, \quad \overbrace{\tau\vec{e}_i, \boxed{0^2}, \tau\vec{e}_i Z_p}^{6}, \quad \overbrace{0^2}^{2}, \quad \overbrace{\vec{\phi}^j_{p,i}}^{2} \quad )\mathbb{B}_j$$

where $\xi \xleftarrow{\text{U}} \mathbb{F}_q^2$, $Z_p \xleftarrow{\text{U}} GL(2F_q)$, $U_p := (Z_p^{-1})^T$

$\mathsf{Exp}$ 2-p-7 (for $p = 1, \ldots, d$): This is same as $\mathsf{Exp}$ 2-p-6 except the following
For $\ell = 1, \ldots, p-1, p+1, \ldots, d$; $j = 1, 2, 3$; $i = 1, 2$

$$\vec{e}^{\,j}_{\ell,i} := \quad ( \overbrace{\sigma^j_{\ell,i}(1,\ell), \omega\vec{e}_i}^{4}, \quad \overbrace{\tau\vec{e}_i, \boxed{0^2}, \tau\vec{e}_i Z_\ell}^{6}, \quad \overbrace{0^2}^{2}, \quad \overbrace{\vec{\phi}^j_{\ell,i}}^{2} \quad )\mathbb{B}_j$$

$\mathsf{Exp}$ 2-p-8 (for $p = 1, \ldots, d$): This is same as $\mathsf{Exp}$ 2-p-7 except the following
For $j = 1, 2, 3$; $i = 1, 2$

$$\vec{h}^{j*}_{p,i} := \quad ( \overbrace{\mu^j_{p,i}(p,-1), \zeta\vec{e}_i}^{4}, \quad \overbrace{0^2, \boxed{0^2}, \rho\vec{e}_i U_p}^{6}, \quad \overbrace{\vec{\eta}^j_{p,i}}^{2}, \quad \overbrace{0^2}^{2} \quad )\mathbb{B}^*_j$$

**Lemma B.19.** *For any adversary $\mathscr{A}$, there exist a PPT algorithm $\mathscr{B}_1$, such that for all $\kappa$, $|Pr[\mathsf{Exp}^0_{\mathscr{A}}(\kappa) = 1] - Pr[\mathsf{Exp}^1_{\mathscr{A}}(\kappa) = 1]| \leq \mathsf{Adv}^{\mathrm{MBP2}}_{\mathscr{B}_1}(\kappa)$.*

*Proof.* The lemma B.19 is proven almost the same way as lemma 48 in [OT12b]. $\mathscr{B}_1$ is given the instance $(param, \{\widehat{\mathbb{B}}_\iota, \mathbb{B}^*_\iota\}_{\iota=0,4}, \{\widehat{\mathbb{B}}_j, \mathbb{B}^*_j\}_{j=1,2,3}, \{\vec{\varepsilon}_j\}_{j=0,4}, \{\vec{g}^{\,j}_i\}_{j=1,2,3;\ i=1,2}, \{\vec{h}^{j*}_\beta\}_{j=0,4}, \{\vec{h}^{j*}_{\beta,i}\}_{j=1,2,3;\ i=1,2})$ of **Modified Basic Problem 2**. $\mathscr{B}_1$ computes

For $t = 1, \ldots, d$, $j = 1, 2, 3$, $i = 1, 2$
$\vec{h}^{j*}_{t,i} := \mu^j_{t,i}(t\vec{b}^*_{j,1} - \vec{b}^*_{j,2}) + \vec{h}^{j*}_{\beta,i} + \vec{\eta}^j_{t,i}(\vec{b}^*_{j,11}, \vec{b}^*_{j,12})$, where $\mu^j_{t,i} \xleftarrow{\mathrm{U}} \mathbb{F}_q$, $\vec{\eta}^j_{t,i} \xleftarrow{\mathrm{U}} \mathbb{F}_q^2$
$\vec{e}^{\,j}_{t,i} := \vec{g}^{\,j}_i + \tau \sum_{\iota=1}^2 z^j_{t,i,\iota}\vec{b}^j_{j,8+\iota} + \sum_{\iota=1}^2 \phi^j_{t,i,\iota}\vec{b}^j_{j,12+\iota}$, where $\phi^j_{t,i,\iota} \xleftarrow{\mathrm{U}} \mathbb{F}_q$, $(z^j_{t,i,\iota})_{i,\iota=1,2} := Z^j_t \xleftarrow{\mathrm{U}} GL(2, \mathbb{F}_q)$

$\vec{e}_\iota := \vec{\varepsilon}_\iota + \phi_\iota\vec{b}_{\iota,5}$, where $\phi_\iota \xleftarrow{\mathrm{U}} \mathbb{F}_q$, for $\iota = 0, 4$
$\widehat{\mathbb{B}}'_\iota := (\vec{b}_{\iota,1}, \vec{b}_{\iota,3}, \vec{b}_{\iota,5})$, $\widehat{\mathbb{B}}^*_\iota := (\vec{b}^*_{\iota,1}, \ldots, \vec{b}^*_{\iota,4})$, for $\iota = 0, 4$
$\widehat{\mathbb{B}}'_\iota := (\vec{b}_{\iota,1}, \ldots, \vec{b}_{\iota,4}, \vec{b}_{\iota,13}, \vec{b}_{\iota,14})$, $\widehat{\mathbb{B}}^*_\iota := (\vec{b}^*_{\iota,1}, \ldots, \vec{b}^*_{\iota,4}, \vec{b}^*_{\iota,11}, \vec{b}^*_{\iota,12})$, for $\iota = 1, 2, 3$

Then, $\mathscr{B}_1$ returns $\mathcal{G} := (param, \{\widehat{\mathbb{B}}'_\iota, \widehat{\mathbb{B}}^*_\iota\}_{\iota=0,4}, \{\widehat{\mathbb{B}}'_j, \widehat{\mathbb{B}}^*_j\}_{j=1,2,3}, \{\vec{h}^{\iota*}_\beta, \vec{e}_\iota\}_{\iota=0,4}, \{\vec{e}^{\,j}_{t,i}, \vec{h}^{j*}_{t,i}\}_{t=1,\ldots,d;\ j=1,2,3;\ i=1,2})$ to $\mathscr{A}$. Finally, $simu_1$ outputs a bit $b \in \{0, 1\}$ if the adversary $\mathscr{A}$ returns $b$. It is to check that $\beta = 0$ (resp. $\beta = 1$), the distribution of $\mathcal{G}$ is exactly the same as that of $\mathsf{Exp}$ 0 (resp. $\mathsf{Exp}$ 1). □

**Lemma B.20.** *For any adversary $\mathscr{A}$, for any $\kappa$, $Pr[\mathsf{Exp}^{2\text{-}(p\text{-}1)\text{-}8}_{\mathscr{A}}(\kappa) = 1] = Pr[\mathsf{Exp}^{2\text{-}p\text{-}1}_{\mathscr{A}}(\kappa) = 1]$.*

*Proof.* Lemma B.20 is proven almost the same way as the lemma 49 in [OT12b]. Set $\vec{d}_{j,7+\iota} := \vec{b}_{j,7+\iota} - \vec{b}_{j,9+\iota}$, $\vec{d}^*_{j,9+\iota} := \vec{b}^*_{j,9+\iota} + \vec{b}^*_{j,7+\iota}$, for $\iota = 0, 1$. Then set

$\mathbb{D}_j := (\vec{b}_{j,1}, \ldots, \vec{b}_{j,6}, \boxed{\vec{d}_{j,7}, \vec{d}_{j,8}}, \vec{b}_{j,9}, \ldots, \vec{b}_{j,14})$, $\mathbb{D}^*_j := (\vec{b}^*_{j,1}, \ldots, \vec{b}^*_{j,8}, \boxed{\vec{d}^*_{j,9}, \vec{d}^*_{j,10}}, \vec{b}^*_{j,11}, \ldots, \vec{b}^*_{\iota,14})$, for $\iota = 1, 2, 3$

Then $(\mathbb{D}_j, D^*_j)$ for $j = 1, 2, 3$ are dual orthonormal bases and consistent with $(\mathbb{B}_j, B^*_j)$. The rest of the proof of the lemma B.20 follow from lemma 49 in [OT12b]. □

**Lemma B.21.** *For any adversary $\mathscr{A}$, there exist a PPT algorithm $\mathscr{B}_{2-1}$, such that for all $\kappa$, $|Pr[\mathsf{Exp}^{2\text{-}p\text{-}1}_{\mathscr{A}}(\kappa) = 1] - Pr[\mathsf{Exp}^{2\text{-}p\text{-}2}_{\mathscr{A}}(\kappa) = 1]| \leq \mathsf{Adv}^{\mathrm{MBP3-p}}_{\mathscr{B}_{2\text{-}1\text{-}p}}(\kappa)$, where $\mathscr{B}_{2-1-p}(.) = \mathscr{B}_{2-1}(p, .)$.*

*Proof.* The proof is similar to lemma 50 in [OT12b]. $\mathscr{B}_{2-1}$ is given an integer $p$ and the instance $(param, \{\mathbb{B}_\iota, \mathbb{B}^*_\iota\}_{\iota=0,4}, \{\widehat{\mathbb{B}}_j, \mathbb{B}^*_j\}_{j=1,2,3}, \{\vec{\varepsilon}_\iota\}_{\iota=0,4}, \{\vec{e}^{\,j}_i, \vec{g}^{\,j}_i\}_{j=1,2,3;\ i=1,2}, \{\vec{h}^{j*}_{\beta,p,i}\}_{j=1,2,3;\ i=1,2})$ of **Modified Basic Problem 3-p**. For $t = 1, \ldots, d$, $j = 1, 2, 3$, $\mathscr{B}_{2-1}$ chooses $(z^j_{t,i\iota})_{i,\iota=1,2} := Z^j_t \xleftarrow{\mathrm{U}} GL(2, \mathbb{F}_q)$, $U^j_t := ((Z^j_t)^{-1})^T$ and can compute $\vec{h}^*_0, \vec{h}^*_4$, $\vec{h}^{j*}_{t,i}$ for $(t < p)$ as defined in $\mathsf{Exp}$ 2-p-8 and $\vec{h}^{j*}_{t,i}$ for $(t > p)$ as defined in $\mathsf{Exp}$ 1 by using $\rho, \zeta, \mu^j_{t,i}, \eta^j_{t,i,1}, \eta^j_{t,i,1} \xleftarrow{\mathrm{U}} \mathbb{F}_q$ and $(Z^j_t, U^j_t)$ for $t \neq p$. $\mathscr{B}_{2-1}$ computes

$\vec{g}_\iota := \vec{\varepsilon}_\iota + \omega\vec{b}_{\iota,1} + \phi_\iota\vec{b}_{\iota,5}$, $\omega, \phi_\iota \xleftarrow{\mathrm{U}} \mathbb{F}_q$ for $\iota = 0, 4$
$\vec{g}^{\,j}_{t,i} := \sigma^j_{t,i}(\vec{b}_{j,1} + t\vec{b}_{j,2}) + \omega\vec{b}_{j,2+i} + \vec{e}^{\,j}_i + \sum_{\iota=1}^2 z^j_{t,i,\iota}\vec{g}^{\,j}_\iota + \sum_{\iota=1}^2 \phi^j_{t,i,\iota}\vec{b}_{j,12+\iota}$, where $\sigma^j_{t,i}, \phi^j_{t,i,1}, \phi^j_{t,i,2} \xleftarrow{\mathrm{U}} \mathbb{F}_q$
for $t = 1, \ldots, d$, $j = 1, 2, 3$, $i = 1, 2$,

$\vec{p}^{j*}_{p,i} := \vec{h}^{j*}_{\beta,p,i} + \zeta\vec{b}^{*}_{j,2+i} + \rho\vec{b}^{*}_{j,6+i}$
$\widehat{\mathbb{B}}_\iota := (\vec{b}_{\iota,1}, \vec{b}_{\iota,3}, \vec{b}_{\iota,5}), \quad \widehat{\mathbb{B}}^*_\iota := (\vec{b}^*_{\iota,1}, \ldots, \vec{b}^*_{\iota,4})$, for $\iota = 0, 4$
$\widehat{\mathbb{B}}'_\iota := (\vec{b}_{\iota,1}, \ldots, \vec{b}_{\iota,4}, \vec{b}_{\iota,13}, \vec{b}_{\iota,14}), \quad \widehat{\mathbb{B}}^*_\iota := (\vec{b}^*_{\iota,1}, \ldots, \vec{b}^*_{\iota,4}, \vec{b}^*_{\iota,11}, \vec{b}^*_{\iota,12})$, for $\iota = 1, 2, 3$

Then, $\mathscr{B}_{2-1}$ returns $\mathcal{G} := (param, \{\widehat{\mathbb{B}}_\iota, \widehat{\mathbb{B}}^*_\iota\}_{\iota=0,4}, \{\widehat{\mathbb{B}'}_j, \widehat{\mathbb{B}}^*_j\}_{j=1,2,3}, \{\vec{h}^*_\iota, \vec{g}_\iota\}_{j=0,4}, \{\vec{g}^j_{t,i}\}_{t=1,\ldots,d;\ j=1,2,3;\ i=1,2}$, $\{\vec{h}^{j*}_{t,i}, \vec{p}^{j*}_{p,i}\}_{t=1,\ldots,p-1,p+1,\ldots,d;\ j=1,2,3;\ i=1,2})$ to $\mathscr{A}$. Finally, $\mathscr{B}_{2-1}$ outputs a bit $b \in \{0,1\}$ if the adversary $\mathscr{A}$ returns $b$. It is easily verified that $\beta = 0$ (resp. $\beta = 1$), the distribution of $\mathcal{G}$ is exactly the same as that of Exp 2-p-1 (resp. Exp 2-p-2). □

**Lemma B.22.** *For any adversary $\mathscr{A}$, for any $\kappa$, $Pr[\mathsf{Exp}^{2\text{-}p\text{-}2}_{\mathscr{A}}(\kappa) = 1] = Pr[\mathsf{Exp}^{2\text{-}p\text{-}3}_{\mathscr{A}}(\kappa) = 1]$.*

*Proof.* This follows from lemma 51 in [OT12b]. □

**Lemma B.23.** *For any adversary $\mathscr{A}$, there exist a PPT algorithm $\mathscr{B}_{2-2}$, such that for any $\kappa$, $|Pr[\mathsf{Exp}^{2\text{-}p\text{-}3}_{\mathscr{A}}(\kappa) = 1] - Pr[\mathsf{Exp}^{2\text{-}p\text{-}4}_{\mathscr{A}}(\kappa) = 1]| \leq \mathsf{Adv}^{\mathrm{MBP3-p}}_{\mathscr{B}_{2\text{-}p\text{-}2}}(\kappa)$, where $\mathscr{B}_{2-p-2}(.) = \mathscr{B}_{2-2}(p, .)$.*

*Proof.* Similar to that of lemma B.21. □

**Lemma B.24.** *For any adversary $\mathscr{A}$, there exist a PPT algorithm $\mathscr{B}_{2-3}$, such that for any $\kappa$, $|Pr[\mathsf{Exp}^{2\text{-}p\text{-}4}_{\mathscr{A}}(\kappa) = 1] - Pr[\mathsf{Exp}^{2\text{-}p\text{-}5}_{\mathscr{A}}(\kappa) = 1]| \leq \mathsf{Adv}^{\mathrm{MBP5-p}}_{\mathscr{B}_{2\text{-}3\text{-}p}}(\kappa)$, where $\mathscr{B}_{2-3-p}(.) = \mathscr{B}_{2-3}(p, .)$.*

*Proof.* The lemma B.19 is proven almost the same way as lemma 53 in [OT12b]. $\mathscr{B}_{2-3}$ is given an integer $p$ and the instance $(param, \{\mathbb{B}_\iota, \mathbb{B}^*_\iota\}_{\iota=0,4}, \{\mathbb{B}_j, \widehat{\mathbb{B}}^*_j\}_{j=1,2,3}, \{\vec{h}^*_j\}_{j=0,4}, \{\vec{\tilde{h}}^{j*}_\iota\}_{j=1,2,3;\ \iota=5,6,9,10}, \{\vec{h}^{j*}_{p,i}\}_{j=1,2,3;\ i=1,2}$, $\{\vec{e}^j_{\beta,\ell,i}\}_{\ell=1,\ldots,p-1,p+1,\ldots,d;\ j=1,2,3;\ i=1,2})$ of **Modified Basic Problem 5-p**. $\mathscr{B}_{2-3}$ can compute $\vec{g}_\iota := (\omega,\ \tau,\ 0,\ 0,\ \phi_\iota)\mathbb{B}_\iota$ using $\mathbb{B}_\iota$ and $\omega, \tau, \phi_\iota \xleftarrow{\mathrm{U}} \mathbb{F}_q$, for $\iota = 0, 4$. Now, it computes

For $t = 1, \ldots, d$; $j = 1, 2, 3$; $i = 1, 2$; $\zeta, \mu^j_{t,i}, \sigma^j_{p,i} \xleftarrow{\mathrm{U}} \mathbb{F}_q$, $\vec{\eta}^j_{t,i}, \vec{\phi}^j_{p,i} \xleftarrow{\mathrm{U}} \mathbb{F}^2_q$
$U^j_t := (u^j_{t,i,\iota})_{i,\iota=1,2} \xleftarrow{\mathrm{U}} GL(2, \mathbb{F}_q), \quad (z^j_{t,i,\iota})_{i,\iota=1,2} := ((U^j_t)^{-1})^T$
$\vec{p}^*_\iota := \vec{h}^*_\iota + (\zeta,\ 0,\ 0,\ \eta_\iota,\ 0)\mathbb{B}^*_\iota$, where $\eta_\iota \xleftarrow{\mathrm{U}} \mathbb{F}_q$ for $\iota = 0, 4$
$\vec{p}^{j*}_{t,i} := \sum_{\iota=1}^{2} u^j_{t,i,\iota}\vec{\tilde{h}}^{j*}_{8+\iota} + (\mu^j_{t,i}(t,-1),\ \zeta\vec{e}_i,\ 0^6,\ \vec{\eta}^j_{t,i},\ 0^2\ )\mathbb{B}^*_j$ if $t < p$
$\vec{p}^{j*}_{p,i} := \sum_{\iota=1}^{2} u^j_{p,i,\iota}\vec{\tilde{h}}^{j*}_{p,\iota} + (0^2,\ \zeta\vec{e}_i,\ 0^{10}\ )\mathbb{B}^*_j$ if $t = p$
$\vec{p}^{j*}_{t,i} := \sum_{\iota=1}^{2} u^j_{t,i,\iota}\vec{\tilde{h}}^{j*}_{4+\iota} + (\mu^j_{t,i}(t,-1),\ \zeta\vec{e}_i,\ 0^6,\ \vec{\eta}^j_{t,i},\ 0^2\ )\mathbb{B}^*_j$ if $t > p$
$\vec{g}^j_{t,i} := \vec{e}^j_{\beta,t,i} + (0^2,\ \omega\vec{e}_i,\ \tau\vec{e}_i,\ \tau\vec{e}_i,\ \tau\vec{e}_i Z^j_t,\ 0^4\ )\mathbb{B}_j$, if $t \neq p$
$\vec{g}^j_{p,i} := (\sigma^j_{p,i}(1,p),\ \omega\vec{e}_i,\ \tau\vec{e}_i,\ \tau\vec{e}_i,\ \tau\vec{e}_i Z^j_p,\ 0^2\ \vec{\phi}^j_{p,i})\mathbb{B}_j$, if $t = p$
$\widehat{\mathbb{B}}_\iota := (\vec{b}_{\iota,1}, \vec{b}_{\iota,3}, \vec{b}_{\iota,5}), \quad \widehat{\mathbb{B}}^*_\iota := (\vec{b}^*_{\iota,1}, \ldots, \vec{b}^*_{\iota,4})$, for $\iota = 0, 4$
$\widehat{\mathbb{B}}_\iota := (\vec{b}_{\iota,1}, \ldots, \vec{b}_{\iota,4}, \vec{b}_{\iota,13}, \vec{b}_{\iota,14}), \quad \widehat{\mathbb{B}'}^*_\iota := (\vec{b}^*_{\iota,1}, \ldots, \vec{b}^*_{\iota,4}, \vec{b}^*_{\iota,11}, \vec{b}^*_{\iota,12})$, for $\iota = 1, 2, 3$

Then, $\mathscr{B}_{2-1}$ returns $\mathcal{G} := (param, \{\widehat{\mathbb{B}}_\iota, \widehat{\mathbb{B}}^*_\iota\}_{\iota=0,4}, \{\widehat{\mathbb{B}}_j, \widehat{\mathbb{B}'}^*_j\}_{j=1,2,3}, \{\vec{p}^*_\iota, \vec{g}_\iota\}_{j=0,4}, \{\vec{g}^j_{t,i}, \vec{p}^{j*}_{t,i}\}_{t=1,\ldots,d;\ j=1,2,3;\ i=1,2})$ to $\mathscr{A}$. Finally, $\mathscr{B}_{2-1}$ outputs a bit $b \in \{0,1\}$ if the adversary $\mathscr{A}$ returns $b$. It is easy to see that $\beta = 0$ (resp. $\beta = 1$), the distribution of $\mathcal{G}$ is exactly same as that of Exp 2-p-4 (resp. Exp 2-p-5). □

**Lemma B.25.** *For any adversary $\mathscr{A}$, for any $\kappa$, $Pr[\mathsf{Exp}^{2\text{-}p\text{-}5}_{\mathscr{A}}(\kappa) = 1] = Pr[\mathsf{Exp}^{2\text{-}p\text{-}6}_{\mathscr{A}}(\kappa) = 1]$.*

*Proof.* One suitably adapts the proof of lemma 54 in [OT12b]. Choose $\tilde{\xi} \xleftarrow{\mathrm{U}} \mathbb{F}_q$. For $j = 1, 2, 3$, pick $Z^j_p \xleftarrow{\mathrm{U}} GL(2, \mathbb{F}_q)$ and set $U^j_p = ((Z^j_p)^{-1})^T$. Let $I_2$ and $O_2$ respectively denote the $2 \times 2$ identity matrix and null matrix. Now, we define new bases $(\mathbb{D}_j, \mathbb{D}^*_j)$ for $j = 1, 2, 3$, by setting the following

$$\begin{pmatrix} \vec{d}_{j,7} \\ \vec{d}_{j,8} \\ \vec{d}_{j,9} \\ \vec{d}_{j,10} \end{pmatrix} := \begin{pmatrix} \tilde{\xi} I_2 & O_2 \\ (Z^j_p)^{-1} & I_2 \end{pmatrix} \begin{pmatrix} \vec{b}_{j,7} \\ \vec{b}_{j,8} \\ \vec{b}_{j,9} \\ \vec{b}_{j,10} \end{pmatrix} \qquad \begin{pmatrix} \vec{d}^*_{j,7} \\ \vec{d}^*_{j,8} \\ \vec{d}^*_{j,9} \\ \vec{d}^*_{j,10} \end{pmatrix} := \begin{pmatrix} \tilde{\xi}^{-1} I_2 & -\tilde{\xi}^{-1} U^j_p \\ O_2 & I_2 \end{pmatrix} \begin{pmatrix} \vec{b}^*_{j,7} \\ \vec{b}^*_{j,8} \\ \vec{b}^*_{j,9} \\ \vec{b}^*_{j,10} \end{pmatrix}$$

$$\mathbb{D}_j := (\vec{b}_{j,1}, \ldots, \vec{b}_{j,6}, \boxed{\vec{d}_{j,7}, \ldots, \vec{d}_{j,10}}, \vec{b}_{j,11}, \ldots, \vec{b}_{j,14}) \quad \mathbb{D}^*_j := (\vec{b}^*_{j,1}, \ldots, \vec{b}^*_{j,6}, \boxed{\vec{d}^*_{j,7}, \ldots, \vec{d}^*_{j,10}}, \vec{b}^*_{j,11}, \ldots, \vec{b}^*_{j,14})$$

It is easily verified that $(\mathbb{D}_j, \mathbb{D}^*_j)$ are dual pairing orthonormal basis and are distributed the same as the original bases, $(\mathbb{B}_j, \mathbb{B}^*_j)$.

For $t = 1, \ldots, p-1, p+1, \ldots, d;\ j = 1,2,3;\ i = 1,2$, we express $\vec{e}^{\,j}_{t,i}$ using the bases $\mathbb{B}_j$ and $\mathbb{D}_j$ as:

$$\begin{aligned}
\vec{e}^{\,j}_{t,i} &:= (\overbrace{\delta^j_{t,i}(1,t),\ \omega\vec{e}_i}^{4},\quad \overbrace{\tau\vec{e}_i,\ \vec{\chi}^j_{t,i},\ \tau\vec{e}_i Z^j_t}^{6},\quad \overbrace{0^2}^{2},\quad \overbrace{\phi^j_{t,i,1}, \phi^j_{t,i,2}}^{2})\ \mathbb{B}_j \\
&:= (\overbrace{\delta^j_{t,i}(1,t),\ \omega\vec{e}_i}^{4},\quad \overbrace{\tau\vec{e}_i,\ \vec{\tilde{\chi}}^j_{t,i},\ \tau\vec{e}_i Z^j_t}^{6},\quad \overbrace{0^2}^{2},\quad \overbrace{\phi^j_{t,i,1}, \phi^j_{t,i,2}}^{2})\ \mathbb{D}_j \\
&\text{where } \vec{\tilde{\chi}}^j_{t,i} := \tilde{\xi}^{-1}(\vec{\chi}^j_{t,i} - \tau\vec{e}_i.Z^j_t.(Z^j_p)^{-1})
\end{aligned}$$

For $t = p;\ j = 1,2,3;\ i = 1,2$, we express $\vec{e}^{\,j}_{p,i}$ using the bases $\mathbb{B}_j$ and $\mathbb{D}_j$ as:

$$\begin{aligned}
\vec{e}^{\,j}_{p,i} &:= (\overbrace{\delta^j_{p,i}(1,p),\ \omega\vec{e}_i}^{4},\quad \overbrace{\tau\vec{e}_i,\ \tau\vec{e}_i,\ \tau\vec{e}_i Z^j_p}^{6},\quad \overbrace{0^2}^{2},\quad \overbrace{\phi^j_{p,i,1}, \phi^j_{p,i,2}}^{2})\ \mathbb{B}_j \\
&:= (\overbrace{\delta^j_{p,i}(1,p),\ \omega\vec{e}_i}^{4},\quad \overbrace{\tau\vec{e}_i,\ 0^2,\ \tau\vec{e}_i Z^j_p}^{6},\quad \overbrace{0^2}^{2},\quad \overbrace{\phi^j_{p,i,1}, \phi^j_{p,i,2}}^{2})\ \mathbb{D}_j
\end{aligned}$$

For $t = 1, \ldots, p-1;\ j = 1,2,3;\ i = 1,2$, we express $\vec{h}^{j*}_{t,i}$ using the bases $\mathbb{B}^*_j$ and $\mathbb{D}^*_j$ as:

$$\begin{aligned}
\vec{h}^{j*}_{t,i} &:= (\overbrace{\mu^j_{t,i}(t,-1),\ \delta\vec{e}_i}^{4},\quad \overbrace{0^4,\ \rho\vec{e}_i U^j_t}^{6},\quad \overbrace{\eta^j_{t,i,1}, \eta^j_{t,i,2}}^{2},\quad \overbrace{0^2}^{2})\ \mathbb{B}^*_j \\
&:= (\overbrace{\mu^j_{t,i}(t,-1),\ \delta\vec{e}_i}^{4},\quad \overbrace{0^4,\ \rho\vec{e}_i U^j_t}^{6},\quad \overbrace{\eta^j_{t,i,1}, \eta^j_{t,i,2}}^{2},\quad \overbrace{0^2}^{2})\ \mathbb{D}^*_j
\end{aligned}$$

For $t = p;\ j = 1,2,3;\ i = 1,2$, we express $\vec{h}^{j*}_{t,i}$ using the bases $\mathbb{B}^*_j$ and $\mathbb{D}^*_j$ as:

$$\begin{aligned}
\vec{h}^{j*}_{p,i} &:= (\overbrace{\mu^j_{t,i}(t,-1),\ \delta\vec{e}_i}^{4},\quad \overbrace{0^2,\ \rho\vec{e}_i,\ 0^2}^{6},\quad \overbrace{\eta^j_{t,i,1}, \eta^j_{t,i,2}}^{2},\quad \overbrace{0^2}^{2})\ \mathbb{B}^*_j \\
&:= (\overbrace{\mu^j_{t,i}(t,-1),\ \delta\vec{e}_i}^{4},\quad \overbrace{0^2,\ \xi\vec{e}_i,\ \rho\vec{e}_i U^j_p}^{6},\quad \overbrace{\eta^j_{t,i,1}, \eta^j_{t,i,2}}^{2},\quad \overbrace{0^2}^{2})\ \mathbb{D}^*_j, \text{ where } \xi := \tilde{\xi}\rho
\end{aligned}$$

For $t = p+1, \ldots, d;\ j = 1,2,3;\ i = 1,2$, we express $\vec{h}^{j*}_{t,i}$ using the bases $\mathbb{B}^*_j$ and $\mathbb{D}^*_j$ as:

$$\begin{aligned}
\vec{h}^{j*}_{t,i} &:= (\overbrace{\mu^j_{t,i}(t,-1),\ \delta\vec{e}_i}^{4},\quad \overbrace{\rho\vec{e}_i,\ 0^4}^{6},\quad \overbrace{\eta^j_{t,i,1}, \eta^j_{t,i,2}}^{2},\quad \overbrace{0^2}^{2})\ \mathbb{B}^*_j \\
&:= (\overbrace{\mu^j_{t,i}(t,-1),\ \delta\vec{e}_i}^{4},\quad \overbrace{\rho\vec{e}_i,\ 0^4}^{6},\quad \overbrace{\eta^j_{t,i,1}, \eta^j_{t,i,2}}^{2},\quad \overbrace{0^2}^{2})\ \mathbb{D}^*_j
\end{aligned}$$

For $t = 1, \ldots, d;\ j = 1,2,3;\ i = 1,2$, since $\vec{\chi}^j_{t,i}$'s are uniformly and independently distributed over $\mathbb{F}_q^2$, so are $\vec{\tilde{\chi}}^j_{t,i}$'s. Therefore, from $\mathscr{A}$'s view, the distribution of $\mathcal{PP}, \{\vec{e}^{\,j}_{t,i}, \vec{h}^{j*}_{t,i}\}_{t=1,\ldots,d;\ j=1,2,3;\ i=1,2}$ is identical to that of $\mathsf{Exp}$ 2-p-5 (resp. $\mathsf{Exp}$ 2-p-6) over the bases $(\mathbb{B}_j, \mathbb{B}^*_j)$ (resp. $(\mathbb{D}_j, \mathbb{D}^*_j)$). □

**Lemma B.26.** *For any adversary $\mathscr{A}$, there exist a PPT algorithm $\mathscr{B}_{2-4}$, such that for any $\kappa$, $|Pr[\mathsf{Exp}^{2\text{-}p\text{-}6}_{\mathscr{A}}(\kappa) = 1] - Pr[\mathsf{Exp}^{2\text{-}p\text{-}7}_{\mathscr{A}}(\kappa) = 1]| \leq \mathsf{Adv}^{\mathrm{MBP5-p}}_{\mathscr{B}_{2\text{-}4\text{-}p}}(\kappa)$, where $\mathscr{B}_{2-4-p}(.) = \mathscr{B}_{2-4}(p, .)$.*

*Proof.* Similar to lemma B.24. □

**Lemma B.27.** *For any adversary $\mathscr{A}$, there exist a PPT algorithm $\mathscr{B}_{2-5}$, such that for any $\kappa$, $|Pr[\mathsf{Exp}^{2\text{-}p\text{-}7}_{\mathscr{A}}(\kappa) = 1] - Pr[\mathsf{Exp}^{2\text{-}p\text{-}8}_{\mathscr{A}}(\kappa) = 1]| \leq \mathsf{Adv}^{\mathrm{MBP4-p}}_{\mathscr{B}_{2\text{-}5\text{-}p}}(\kappa)$, where $\mathscr{B}_{2-5-p}(.) = \mathscr{B}_{2-5}(p, .)$.*

*Proof.* The proof can be obtained as in lemma B.24. □

# C Key-Policy Functional Encryption for DFAs

## C.1 Definition

A key-policy functional encryption (KP-FE) scheme for DFAs consists of four PPT algorithms - Setup, KeyGen, Encrypt and Decrypt.

- Setup: It takes a security parameter $\kappa$, an alphabet $\Sigma$ as input, outputs the public parameters $\mathcal{PP}$ which explicitly contains $\Sigma$ and the master secret $\mathcal{MSK}$.
- KeyGen: It takes as input the description of a DFA $\mathcal{M}$ and master secret $\mathcal{MSK}$ and outputs a secret key $\mathcal{SK}_{\mathcal{M}}$ corresponding to $\mathcal{M}$.
- Encrypt: takes a message $m$, a string $w = w_1 w_2 \cdots w_\ell$ over $\Sigma$ and public parameters $\mathcal{PP}$ and returns a ciphertext $\mathcal{C}_w$ which implicitly contains $w$.
- Decrypt: It receives a ciphertext $\mathcal{C}_w$ and secret key $\mathcal{SK}_{\mathcal{M}}$ as input. If the DFA $\mathcal{M}$ accepts $w$, the algorithm returns $m$.

## C.2 Security definition of KP-FE for DFAs

The adaptive security model is defined as an indistinguishability game, $\text{Game}_{Real}$ between a challenger $\mathcal{C}$ and an adversary $\mathscr{A}$, where the adversary has to distinguish the ciphertexts under a chosen plaintext attack (CPA). The game, $\text{Game}_{Real}$ consists of the following phases:

**Setup:** The challenger $\mathcal{C}$ runs the Setup algorithm to produce the master secret key $\mathcal{MSK}$ and the public parameter $\mathcal{PP}$. Then, $\mathcal{C}$ gives $\mathcal{PP}$ to the adversary $\mathscr{A}$ and keeps $\mathcal{MSK}$ to itself.

**Phase 1:** The adversary $\mathscr{A}$ queries for the secret keys corresponding to the DFAs $\mathcal{M}_1, \ldots, \mathcal{M}_l$. The challenger $\mathcal{C}$ returns the secret keys $sk_{\mathcal{M}_i}$ by running the KeyGen algorithm on $\mathcal{M}_i$, for $i = 1, \ldots, l$.

**Challenge:** The adversary provides two equal length messages $m_0, m_1$ and a challenge string $w^*$ with the condition that no queried DFA $\mathcal{M}_i$ can accept the challenge string $w^*$. The challenger chooses $\beta \xleftarrow{\text{U}} \{0,1\}$ and encrypts the message $m_\beta$ using the challenge string $w^*$ and gives the challenge ciphertext $\mathcal{C}_{w^*}$ to the adversary A

**Phase 2:** $\mathscr{A}$ again queries for the secret keys corresponding to the DFAs $\mathcal{M}_{l+1}, \ldots, \mathcal{M}_\nu$ with the restriction that no queried DFA $\mathcal{M}_i$ can accept the challenge string $w^*$. $\mathcal{C}$ answers to the adversary $\mathscr{A}$ in similar manner as in **Phase 1**.

**Guess:** The challenger $\mathscr{A}$ outputs a bit $\beta'$.

The advantage of $\mathscr{A}$ in above game is defined by

$$\mathsf{Adv}_{\mathscr{A}}^{\text{KP}-\text{FE}}(\kappa) = \left| \Pr[\beta = \beta'] - \frac{1}{2} \right|.$$

The KP-FE scheme is said to be adaptively secure if all PPT adversary $\mathscr{A}$, the advantage $\mathsf{Adv}_{\mathscr{A}}^{\text{KP}-\text{FE}}(\kappa)$ is at most a negligible function in security parameter $\kappa$.

## C.3 Basic KP-FE Construction

In this section, we illustrate a basic Key-Policy Functional Encryption scheme for DFAs in the prime order bilinear pairing groups. This scheme is based on the structure of ABE construction of [OT12b], where encryption is done using some basis vectors of dual pairing vector spaces. The keys are generated using some basis vectors of it's dual. Similar to section 3, this basic construction has the following restrictions.

– The strings for ciphertexts can have at most a single occurrence of each symbol (policies)

– There is at most a single transition corresponding to each symbol in the DFAs (keys)

Similar to section 5, one can extend the basic KP-FE scheme to a full KP-FE scheme without the attributed restrictions and the scheme entertains the similar type of security.

$\mathsf{Setup}(\kappa)$: $(param, (\mathbb{B}_0, \mathbb{B}_0^*), (\mathbb{B}_1, \mathbb{B}_1^*), (\mathbb{B}_2, \mathbb{B}_2^*), (\mathbb{B}_3, \mathbb{B}_3^*), (\mathbb{B}_4, \mathbb{B}_4^*)) \longleftarrow \mathcal{G}_{ob}(1^\lambda, 5, 14, 14, 14, 5)$

$\widehat{\mathbb{B}}_j := (\ \vec{b}_{j,1},\ \vec{b}_{j,3},\ \vec{b}_{j,5}),$ $\quad \widehat{\mathbb{B}}_j^* := (\ \vec{b}_{j,1}^*,\ \vec{b}_{j,3}^*,\ \vec{b}_{j,4}^*\ )$ for j=0,4

$\widehat{\mathbb{B}}_j := (\ \vec{b}_{j,1} \ldots, \vec{b}_{j,4},\ \vec{b}_{j,11},\ \vec{b}_{j,12}\ ),$ $\quad \widehat{\mathbb{B}}_j^* := (\ \vec{b}_{j,1}^*, \ldots, \vec{b}_{j,4}^*,\ \vec{b}_{j,13}^*,\ \vec{b}_{j,14}^*\ )$ for j=1,2,3

Choose a set, alphabet of symbols $\Sigma = \{\sigma_1, \ldots, \sigma_d\} \subseteq \mathbb{F}_q$, where $d = poly(\kappa)$. The public parameters and master secret are given by

$\mathcal{PP} := (\Sigma, param,\ \{\widehat{\mathbb{B}}_j\}_{j=0,1,2,3,4})$,

$\mathcal{MSK} := (\{\widehat{\mathbb{B}}_j^*\}_{j=0,1,2,3,4})$.

$\mathsf{Encrypt}(\mathcal{PP}, w = w_1 \cdots w_\ell, m)$: For each $i \in [\ell]$, choose $\mu_{i,1},\ \mu_{i,2},\ \mu_{i,3}, \theta_i, r_i \xleftarrow{\text{U}} \mathbb{F}_q$; $\vec{\eta}_{i,1}, \vec{\eta}_{i,2}, \vec{\eta}_{i,3} \xleftarrow{\text{U}} \mathbb{F}_q^2$. Pick $\xi, r_0, \eta_0, \eta_{\ell+1} \xleftarrow{\text{U}} \mathbb{F}_q$. Compute the ciphertext components

$\vec{C}_0 := (\ r_0,\ 0,\ \xi,\ 0,\ \eta_0)\mathbb{B}_0 \quad C_m := m.g_T^\xi$

For each $i \in [\ell]$, (let $w_i = \sigma_h$, for some index $h$) continue to compute

$\vec{C}_{i,1} := (\ \overbrace{\mu_{i,1}(h,-1)}^{2},\ \overbrace{r_i + \theta_i\sigma_h,\ -\theta_i}^{2},\ \overbrace{0^6}^{6},\ \overbrace{0^2}^{2},\ \overbrace{\vec{\eta}_{i,1}}^{2})\ \mathbb{B}_1$

$\vec{C}_{i,2} := (\ \overbrace{\mu_{i,2}(h,-1)}^{2},\ \overbrace{-r_{i-1} + \theta_i\sigma_h,\ -\theta_i}^{2},\ \overbrace{0^6}^{6},\ \overbrace{0^2}^{2},\ \overbrace{\vec{\eta}_{i,2}}^{2})\ \mathbb{B}_2$

$\vec{C}_{i,3} := (\ \overbrace{\mu_{i,3}(h,-1)}^{2},\ \overbrace{-r_i - r_{i-1} + \theta_i\sigma_h, -\theta_i}^{2},\ \overbrace{0^6}^{6},\ \overbrace{0^2}^{2},\ \overbrace{\vec{\eta}_{i,3}}^{2})\ \mathbb{B}_3$

$\vec{C}_{\ell+1,4} := (\ r_\ell,\ 0,\ 0,\ 0,\ \eta_{\ell+1})\mathbb{B}_4$

The ciphertext is given by $\mathcal{C}_w := (\ w,\ C_m,\ \vec{C}_0,\ \{\vec{C}_{i,1},\ \vec{C}_{i,2},\ \vec{C}_{i,3}\}_{i\in[\ell]},\ \vec{C}_{\ell+1,4})$

$\mathsf{KeyGen}(\mathcal{MSK}, \mathcal{M} = (Q, \Sigma, q_0, F, \delta))$: For each $q_x \in Q$, pick $d_x \xleftarrow{\text{U}} \mathbb{F}_q$. For each $q_z \in F$, choose $\phi_z \xleftarrow{\text{U}} \mathbb{F}_q$. Pick random $\xi \in \mathbb{F}_q$. For each transition $t = (q_x, q_y, \sigma_h) \in \mathcal{T}$, choose $s_t, \delta_{t,1}, \delta_{t,2}, \delta_{t,3} \xleftarrow{\text{U}} \mathbb{F}_q$; $\vec{\phi}_{t,1},\ \vec{\phi}_{t,2},\ \vec{\phi}_{t,3} \xleftarrow{\text{U}} \mathbb{F}_q^2$. Now compute

$\vec{K}_0^* := (\ d_0,\ 0,\ 1,\ \phi_0,\ 0)\mathbb{B}_0^*$

For each transition $t = (q_x, q_y, \sigma_h) \in \mathcal{T}$, compute the ciphertext components

$\vec{K}_{t,1}^* := (\ \overbrace{\delta_{t,1}(1,h)}^{2},\ \overbrace{(s_t + d_y)(1,\sigma_h)}^{2},\ \overbrace{0^6}^{6},\ \overbrace{\vec{\phi}_{t,1}}^{2},\ \overbrace{0^2}^{2}\ )\ \mathbb{B}_1^*$

$\vec{K}_{t,2}^* := (\ \overbrace{\delta_{t,2}(1,h)}^{2},\ \overbrace{(-s_t + d_x)(1,\sigma_h)}^{2},\ \overbrace{0^6}^{6},\ \overbrace{\vec{\phi}_{t,2}}^{2},\ \overbrace{0^2}^{2}\ )\ \mathbb{B}_2^*$

$\vec{K}_{t,3}^* := (\ \overbrace{\delta_{t,3}(1,h)}^{2},\ \overbrace{s_t(1,\sigma_h)}^{2},\ \overbrace{0^6}^{6},\ \overbrace{\vec{\phi}_{t,3}}^{2},\ \overbrace{0^2}^{2}\ )\ \mathbb{B}_3^*$

For each $q_z \in F$, compute the ciphertext component

$\vec{K}_{z,4}^* := (\ d_z,\ 0,\ 0,\ \phi_z,\ 0)\mathbb{B}_4^*$

The secret key for the string $w$ is given by

$$\mathcal{SK}_\mathcal{M} := \big(\mathcal{M}, \vec{K}_0^*,\ \{\vec{K}_{t,1}^*,\ \vec{K}_{t,2}^*,\ \vec{K}_{t,3}^*\}_{t=(q_x,q_y,\sigma_h)\in\mathcal{T}}, \{\vec{K}_{z,4}^*\}_{q_z\in F}\big)$$

$\mathsf{Decrypt}(C_w, \mathcal{SK}_\mathcal{M})$: Suppose the DFA $\mathcal{M}$ accepts the string $w = w_1 \cdots w_\ell$, then there exist a sequence of $\ell + 1$ states $q_{x_0}, q_{x_1}, q_{x_2}, \ldots, q_{x_\ell}$ and transitions $t_1, \ldots, t_\ell$, where $x_0 = 0$ and $q_{x_\ell} \in F$ and for $i = 1, 2, \ldots, \ell$, we have $t_i = (q_{x_{i-1}}, q_{x_i}, \sigma) \in \mathcal{T}$ with $w_i = \sigma$. First compute the initial value

$$A_0 = e(\vec{C}_0,\ \vec{K}_0^*) = g_T^{r_0 d_0 + \xi}$$

Then, compute the first value $A_1$ of intermediate values as

$$A_1 = e(\vec{C}_{1,1},\ \vec{K}^*_{t_1,1}).e(\vec{C}_{1,2},\ \vec{K}^*_{t_1,2}).e(\vec{C}_{1,3},\ \vec{K}^*_{t_1,3}) = g_T^{r_1 d_{x_1} - r_0 d_0}$$

Then compute intermediate values $A_i$ (for $i = 2, \ldots, \ell$) as follows:

$$A_i = A_{i-1}.e(\vec{C}_{i,1},\ \vec{K}^*_{t_i,1}).e(\vec{C}_{i,2},\ \vec{K}^*_{t_i,2}).e(\vec{C}_{i,3},\ \vec{K}^*_{t_i,3}) = g_T^{r_{i-1} d_{x_{i-1}} - r_0 d_0} g_T^{r_i d_{x_i} - r_{i-1} d_{x_{i-1}}} = g_T^{r_i d_{x_i} - r_0 d_0}$$

So, the last intermediate value has of the form

$$A_\ell = g_T^{r_\ell d_{x_\ell} - r_0 d_0}$$

The final value $A_{\ell+1}$ is computed as

$$A_{\ell+1} = A_\ell.e(\vec{C}_{\ell+1,4},\ \vec{K}^*_{x_\ell,4}) = g_T^{r_\ell d_{x_\ell} - r_0 d_0} g_T^{-r_\ell d_{x_\ell}} = g_T^{-r_0 d_0}$$

Using $A_0, A_{\ell+1}$ and $C_m$, the message is unmasked as $m = C_m/(A_0\ A_{\ell+1})$.

## C.4 Security Proof

The proof technique is similar to section 4. For this, we define two types of semi-functional ciphertexts, viz., type 1 and type 2 and three types of semi-functional keys, viz., type 1, type 2 and type 3.

**Semi-functional Type 1 Ciphertext.** For each $i \in [\ell]$, choose $\widehat{r}_i, \widehat{\theta}_i \xleftarrow{U} \mathbb{F}_q$. Also choose $\widehat{r}_0 \xleftarrow{U} \mathbb{F}_q$. For $i \in [\ell]$, let $w_i = \sigma_h$ for some index $h$, choose $Z_h^1, Z_h^2, Z_h^3 \xleftarrow{U} GL(2, \mathbb{F}_q)$. The sf-type 1 ciphertext is obtained by modifying normally generated ciphertext $\mathcal{C}_w := (w,\ C_m,\ \vec{C}_0,\ \{\vec{C}_{i,1},\ \vec{C}_{i,2},\ \vec{C}_{i,3}\}_{i\in[\ell]},\ \vec{C}_{\ell+1,4}\ )$ as:

$\vec{C}_0 := (\ r_0,\ \boxed{\widehat{r}_0},\ \xi,\ 0,\ \eta_0)\mathbb{B}_0 \quad C_m := m.g_T^{\xi}$

$\vec{C}_{i,1} := (\overbrace{\mu_{i,1}(h,-1)}^{2}, \overbrace{r_i + \theta_i\sigma_h,\quad -\theta_i}^{2}, \overbrace{\boxed{\widehat{r}_i + \widehat{\theta}_i\sigma_h,\quad -\widehat{\theta}_i}, 0^2, \boxed{(\widehat{r}_i + \widehat{\theta}_i\sigma_h,\quad -\widehat{\theta}_i)Z_h^1}}^{6},$
$\overbrace{0^2}^{2}, \overbrace{\vec{\eta}_{i,1}}^{2})\ \mathbb{B}_1$

$\vec{C}_{i,2} := (\overbrace{\mu_{i,2}(h,-1)}^{2}, \overbrace{-r_{i-1} + \theta_i\sigma_h,\quad -\theta_i}^{2}, \overbrace{\boxed{-\widehat{r}_{i-1} + \widehat{\theta}_i\sigma_h,\quad -\widehat{\theta}_i}, 0^2, \boxed{(-\widehat{r}_{i-1} + \widehat{\theta}_i\sigma_h,\quad -\widehat{\theta}_i)Z_h^2}}^{6},$
$\overbrace{0^2}^{2}, \overbrace{\vec{\eta}_{i,2}}^{2})\ \mathbb{B}_2$

$\vec{C}_{i,3} := (\overbrace{\mu_{i,3}(h,-1)}^{2}, \overbrace{-r_i - r_{i-1} + \theta_i\sigma_h, -\theta_i}^{2}, \overbrace{\boxed{-\widehat{r}_i - \widehat{r}_{i-1} + \widehat{\theta}_i\sigma_h, -\widehat{\theta}_i}, 0^2, \boxed{(-\widehat{r}_i - \widehat{r}_{i-1} + \widehat{\theta}_i\sigma_h, -\widehat{\theta}_i)Z_h^3}}^{6},$
$\overbrace{0^2}^{2}, \overbrace{\vec{\eta}_{i,3}}^{2})\ \mathbb{B}_3$

$\vec{C}_{\ell+1,4} := (\ r_\ell,\ \boxed{\widehat{r}_\ell},\ 0,\ 0,\ \eta_{\ell+1}\ )\ \mathbb{B}_4$

**Semi-functional Type 2 Ciphertext.** This is same as sf-type 1 ciphertext except the following

$\vec{C}_0 := (\ r_0,\ \widehat{r}_0,\ \boxed{\xi'},\ 0,\ \eta_0)\mathbb{B}_0 \quad C_m := m.g_T^{\xi}$ where $\xi' \xleftarrow{U} \mathbb{F}_q$ (independent of $\xi \xleftarrow{U} \mathbb{F}_q$)

**Semi-functional Type 1 Key.** For each $q_x \in Q$, pick $\widehat{d}_x \xleftarrow{U} \mathbb{F}_q$. For each transition $t = (q_x, q_y, \sigma_h) \in \mathcal{T}$, choose $\widehat{s}_t \xleftarrow{U} \mathbb{F}_q$; $Z_h^j \xleftarrow{U} GL(2, \mathbb{F}_q)$ and set $U_h^j = ((Z_h^j)^{-1})^T$ for $j = 1, 2, 3$. The sf-type 1 key generation algorithm first creates a normal key

$$\mathcal{SK}_{\mathcal{M}} := \big(\mathcal{M}, \vec{K}^*_0,\ \{\vec{K}^*_{t,1},\ \vec{K}^*_{t,2},\ \vec{K}^*_{t,3}\}_{t=(q_x,q_y,\sigma_h)\in\mathcal{T}}, \{\vec{K}^*_{z,4}\}_{q_z\in F}\big)$$

and then modifies its components as shown below.

$$\vec{K}_0^* := (\ d_0,\ \widehat{d_0},\ 1,\ \phi_0,\ 0)\mathbb{B}_0^*$$

$$\vec{K}_{t,1}^* := (\ \overbrace{\delta_{t,1}(1,h)}^{2},\ \overbrace{(s_t+d_y)(1,\sigma_h)}^{2},\quad \overbrace{0^4,\ \boxed{(\widehat{s}_t+\widehat{d}_y)(1,\sigma_h)U_h^1}}^{6},\ \overbrace{\vec{\phi}_{t,1}}^{2},\ \overbrace{0^2}^{2}\ )\ \mathbb{B}_1^*$$

$$\vec{K}_{t,2}^* := (\ \overbrace{\delta_{t,2}(1,h)}^{2},\ \overbrace{(-s_t+d_x)(1,\sigma_h)}^{2},\ \overbrace{0^4,\boxed{(-\widehat{s}_t+\widehat{d}_x)(1,\sigma_h)U_h^2}}^{6},\ \overbrace{\vec{\phi}_{t,2}}^{2},\ \overbrace{0^2}^{2}\ )\ \mathbb{B}_2^*$$

$$\vec{K}_{t,3}^* := (\ \overbrace{\delta_{t,3}(1,h)}^{2},\ \overbrace{s_t(1,\sigma_h)}^{2},\quad \overbrace{0^4,\quad \boxed{\widehat{s}_t(1,\sigma_h)U_h^3}}^{6},\ \overbrace{\vec{\phi}_{t,3}}^{2},\ \overbrace{0^2}^{2}\ )\ \mathbb{B}_3^*$$

$$\vec{K}_{z,4}^* := (\ d_z,\ \widehat{d_z},\ 0,\ \phi_z,\ 0)\mathbb{B}_4^*$$

**Semi-functional Type 2 Key.** This is same as sf-type 1 key except $\vec{K}_0^*$

$\vec{K}_0^* := (\ d_0,\ \boxed{d_{rand}},\ 1,\ \phi_0,\ 0)\mathbb{B}_0^*$, where $d_{rand} \xleftarrow{\mathrm{U}} \mathbb{F}_q$ (independent of $\widehat{d_0} \xleftarrow{\mathrm{U}} \mathbb{F}_q$)

**Semi-functional Type 3 Key.** This is same as normal key except $\vec{K}_0^*$

$\vec{K}_0^* := (\ d_0,\ \boxed{d_{rand}},\ 1,\ \phi_0,\ 0)\mathbb{B}_0^*$, where $d_{rand} \xleftarrow{\mathrm{U}} \mathbb{F}_q$

A legitimate normal key (resp. sf-type 1 key, sf-type 2 key, sf-type 3 key) $\mathcal{SK}_{\mathcal{M}}$ can extract the message from an sf-type 1 ciphertext (resp. normal ciphertext) $\mathcal{C}_w$. Similarly, a legitimate sf-type 1 key $\mathcal{SK}_{\mathcal{M}}$ can succeed in decrypting an sf-type 1 ciphertext $\mathcal{C}_w$, because the mimicked parts get canceled just like the normal components. But, if a legitimate sf-type 2 key or sf-type 2 key $\mathcal{SK}_{\mathcal{M}}$ runs decryption on an sf-type 1 ciphertext $\mathcal{C}_w$, it will get an extra factor $g_T^{\widehat{r}_0 d_{rand}}$ masking the message.

**Theorem C.1.** *The proposed basic KP-FE scheme is adaptively secure under the DLIN assumption.*

*Proof.* The theorem C.1 is proven in a similar manner to theorem 4.1 in section 5. □