ABE for DFA from k-Lin

Junqing Gong[1,⋆], Brent Waters[2,⋆⋆], and Hoeteck Wee[1,3,⋆⋆⋆]

[1] CNRS, ENS and PSL
{jgong,wee}@di.ens.fr
[2] University of Texas at Austin and NTT Research
bwaters@cs.utexas.edu
[3] Algorand

Abstract. We present the first attribute-based encryption (ABE) scheme for deterministic finite automaton (DFA) based on static assumptions in bilinear groups; this resolves an open problem posed by Waters (CRYPTO 2012). Our main construction achieves selective security against unbounded collusions under the standard k-linear assumption in prime-order bilinear groups, whereas previous constructions all rely on q-type assumptions.

1 Introduction

Attribute-based encryption (ABE) [19,11] is a generalization of public-key encryption to support fine-grained access control for encrypted data. Here, ciphertexts are associated with a description value x and keys with a policy f, and decryption is possible when $f(x) = 1$. In many prior ABE schemes, the policy f is specified using a boolean formula, but there are many applications where we want the policy f to operate over arbitrary sized input data. For example, we could imagine a network logging application where x represents an arbitrary number of events logged. Another example is where x is a database of patient data that includes disease history paired with gene sequences where the number of participants is not apriori bounded or known.

Following the work of Waters in 2012 [21], we consider ABE for regular languages, where the policies f are specified using deterministic finite automata (DFA). This allows us to capture applications such as tax returns and virus scanners. In spite of the substantial progress made in the design and analysis of ABE schemes over the past decade, all known constructions of ABE for DFA rely on q-type assumptions in bilinear groups [21,2,3,1], where the complexity of the assumption grows with the length of the string x. In this work, we address the following open problem posed in the original work of Waters [21]:

> *Can we build an ABE for DFA based on static assumptions in bilinear groups, notably the k-linear assumption in prime-order bilinear groups?*

⋆ Supported by ERC Project aSCEND (H2020 639554) and the French ANR ALAMBIC Project (ANR-16-CE39-0006). Part of this work was done while at ENS de Lyon.

⋆⋆ Supported by NSF CNS-1908611, CNS-1414082, DARPA SafeWare and Packard Foundation Fellowship.

⋆⋆⋆ Supported by ERC Project aSCEND (H2020 639554).

From both a practical and theoretical stand-point, we would like to base cryptography on weaker and better understood assumptions, as is the case with the k-linear assumption. This is also an intriguing problem from a conceptual stand-point because prior approaches exploit q-type assumptions in a fairly inherent manner. Waters' ABE for DFA was based on an "embedding paradigm" where the arbitrary-length challenge string was programmed into the public parameters, and embedding an arbitrary length string into fixed-size parameters seems to require a q-type assumption. The dual system encryption methodology developed in the context of ABE for boolean formula [20,15,16,18,6] allows us to overcome the latter limitation, provided the ciphertext or key size is allowed to grow with the size of the formula; this does not work in the DFA setting, since formula size roughly corresponds to $\ell \cdot Q$, where ℓ is the length of the string x and Q is the number of states in the DFA. Indeed, a key challenge that distinguishes ABE for DFA from ABE for boolean formula is that both the size of public parameters and the secret keys are independent of ℓ, which means that we cannot afford to unroll and embed the entire DFA computation path into the secret key.

This work. We present the first ABE for DFA based on static assumptions in bilinear groups, thereby providing an affirmative answer to the above open problem. Our main construction achieves selective security against unbounded collusions under the standard k-linear assumption in prime-order bilinear groups. Our proof strategy departs significantly from prior ABEs for DFA in that we design a series of hybrids that traces through the computation. Our proof of security carefully combines a "nested, two-slot" dual system argument [20,15,16,18,12,6] along with a novel combinatorial mechanism for propagating entropy along the computation path of a DFA.

We note that our high-level approach of tracing the computation path across hybrids is similar to that used in the recent ABE for boolean formula from static assumptions in [14], but we have to deal with the afore-mentioned challenge specific to DFAs. In a bit more detail, in our ABE for DFA, the secret keys contain random shares "in the exponent" corresponding to each state of the DFA; this is analogous to ABE for boolean formula where the random shares correspond to wires in a formula. Roughly speaking, in the i'th hybrid, we modify the distribution of the share corresponding to the state u_i reached upon reading the first i bits of the input string. In a DFA, a state could be reached many times throughout the DFA computation on a fixed input, which means that we need to modify the share corresponding to u_i (along with the challenge ciphertext) in such a way that it does not affect the functionality of the DFA. This difficulty does not arise in ABE for boolean formula, because each wire is only used once during the computation.

1.1 Technical overview – warm-up

We present an overview of our ABE scheme for DFAs. Recall that a DFA is specified by a tuple (Q, Σ, δ, F) where the state space is $[Q] := \{1, 2, \ldots, Q\}$; 1 is the unique start state; $F \subseteq [Q]$ is the set of accept states, and $\delta : [Q] \times \Sigma \to [Q]$ is the state transition function.

Warm-up construction. The starting point of our construction is Waters' ABE scheme for DFA [21] over asymmetric composite-order bilinear groups (G_N, H_N, G_T, e) whose order N is the product of three primes p_1, p_2, p_3. (The original scheme is instantiated over prime-order bilinear groups, but relies on q-type assumptions.) Let g_i, h_i denote generators of order p_i in G_N and H_N, for $i = 1, 2, 3$, and let h be a generator for H_N. The scheme is as follows:

$$\begin{aligned}
\mathsf{msk} &= \big(\, h, \alpha, w_{\text{start}}, w_{\text{end}}, z, \{w_\sigma\}_{\sigma\in\Sigma} \,\big) \qquad (1)\\
\mathsf{mpk} &= \big(\, g_1, g_1^{w_{\text{start}}}, g_1^{w_{\text{end}}}, g_1^{z}, \{g_1^{w_\sigma}\}_{\sigma\in\Sigma}, e(g_1,h)^\alpha \,\big)\\
\mathsf{ct}_x &= \begin{pmatrix} g_1^{s_0},\, g_1^{s_0 w_{\text{start}}}, \\ \{g_1^{s_i}, g_1^{s_{i-1}z + s_i w_{x_i}}\}_{i\in[\ell]}, \\ g_1^{s_\ell}, g_1^{s_\ell w_{\text{end}}},\, e(g_1,h)^{s_\ell\alpha}\cdot m \end{pmatrix}\\
\mathsf{sk}_f &= \begin{pmatrix} h^{d_1 + w_{\text{start}} r_1}, h^{r_1}, \\ \{h^{-d_u + z r_u}, h^{d_v + w_\sigma r_u}, h^{r_u}\}_{u\in[Q],\sigma\in\Sigma, v=\delta(u,\sigma)}, \\ \{h^{\alpha - d_u + w_{\text{end}} r_u}, h^{r_u}\}_{u\in F} \end{pmatrix}
\end{aligned}$$

Decryption proceeds as follows:

(i) compute $e(g_1^{s_0}, h^{d_1})$;
(ii) for $i = 1, \dots, \ell$, compute $e(g_1^{s_i}, h^{d_{u_i}})$, where u_i denotes the state reached upon reading $x_1, \dots, x_i$.
(iii) compute $e(g_1, h)^{s_\ell \alpha}$ and thus m.

To go from $e(g_1^{s_{i-1}}, h^{d_{u_{i-1}}})$ to $e(g_1^{s_i}, h^{d_{u_i}})$ in step (ii), we rely on the identity: for all $u \in [Q], \sigma \in \Sigma$,

$$s_i d_{\delta(u,\sigma)} - s_{i-1} d_u = s_i \cdot (d_{\delta(u,\sigma)} + w_\sigma r_u) + s_{i-1} \cdot (-d_u + z r_u) - (s_{i-1} z + s_i w_\sigma) \cdot r_u$$

We note that our scheme differs from Waters' scheme in that we reuse r_u for all the transitions starting from u instead of a fresh $r_{u,\sigma}$ for each (u, σ). This modification yields a smaller secret key (roughly $Q \cdot |\Sigma| + 2Q$ vs $3Q \cdot |\Sigma|$ group elements), and also simplifies the notation.

Proof strategy. At a very high level, the proof follows Waters' dual system encryption methodology [20,15]. This means that throughout the proof, we modify the ciphertext and key distributions but not mpk, and only in the p_2-subgroup generated by g_2, h_2 (which we also refer to as the p_2-components). In fact, we will rely on the "nested two-slot" variant of dual system encryption introduced in [16,18,12,6] for settings where the ciphertext uses independent randomness $s_0, s_1, \dots$, as is the case for our DFA scheme. Here, "nested" refers to the fact that the security proof interweaves a computational argument over ciphertexts with another over secret keys, whereas "two-slot" refers to the use of the p_3-subgroup to carry out this delicate interweaving. In contrast, the basic dual system encryption framework [2,22] applies a *single* computational argument over ciphertexts at the beginning and can be instantiated in asymmetric composite-order groups whose order is the product of *two* primes.

Proof – first idea. For this proof overview, we will focus on the selective setting where the adversary first picks a challenge x^* before seeing mpk and making secret key queries. In addition, we consider a further simplification where the adversary only makes a single key query for some DFA f where $f(x^*) = 0$ (i.e. rejecting). Let $u_0 = 1$ denote the start state, and let $u_1, \ldots, u_\ell$ denote the state in f reached upon reading $x_1^*, \ldots, x_\ell^*$. In particular, $u_\ell \notin F$.

Recall that decryption computes $e(g_1^{s_i}, h^{d_{u_i}})$ for each $i = 0, \ldots, \ell$. A natural proof strategy would be design a series of games $\mathsf{G}_0, \ldots, \mathsf{G}_\ell$ such that in G_i, the quantity $e(g_1^{s_i}, h^{d_u})$ is pseudorandom for each $u \neq u_i$. In particular, since $u_\ell \notin F$, this means that $e(g_1^{s_\ell}, h^{d_u})$ is pseudorandom for all $u \in F$, which should imply that $e(g_1^{s_\ell}, h^{\alpha})$ is pseudorandom.

Towards carrying out this strategy, we pick $\Delta \leftarrow \mathbb{Z}_N$ and define:

$$\Delta_{i,u} := \begin{cases} \Delta & \text{if } u \neq u_i \\ 0 & \text{otherwise} \end{cases}$$

In G_i, we switch the ciphertext-key distributions from $(\mathsf{ct}_{x^*}, \mathsf{sk}_f)$ to $(\mathsf{ct}_{x^*}^i, \mathsf{sk}_f^i)$ where

- $\mathsf{ct}_{x^*}^i$ is the same as ct_{x^*} except we replace $g_1^{s_i}$ with $(g_1 g_2)^{s_i}$;
- sk_f^i is the same as sk_f except we add a $h_2^{\Delta_{i,v}}$ term to $h^{d_v + w_\sigma r_u}$ for every u, σ.

Roughly speaking, this means that in G_i, the quantity $e(g_1^{s_i}, h^{d_u})$ would be masked by $e(g_2^{s_i}, h_2^{\Delta_{i,u}}) = e(g_2^{s_i}, h_2^{\Delta})$ whenever $u \neq u_i$. In particular, the quantity $e(g_1^{s_\ell}, h^{\alpha})$ would be masked by $e(g_2^{s_\ell}, h_2^{\Delta})$.

Proof – second idea. As it turns out, we cannot hope to show that the quantity $e(g_1^{s_i}, h^{d_u})$ is pseudorandom for each $u \neq u_i$. Consider a DFA with $Q = 3, \Sigma = \{0\}$ and $\delta(1, 0) = 2, \delta(3, 0) = 2$. Then, given an encryption of $x = 0$, an adversary can compute

$$e(g_1^{s_0}, h^{d_3})$$

by first computing $e(g_1^{s_1}, h^{d_2})$ using the transition $1 \xrightarrow{0} 2$, and then "back-tracking" along the transition $3 \xrightarrow{0} 2$; these are so-called "back-tracking attacks" in [21].

Instead, we will only argue that $e(g_1^{s_i}, h^{d_u})$ is pseudorandom, for $u \in F_{i,x^*}$ for some family of sets $F_{i,x^*} \subseteq [Q]$. (Our first attempt corresponds to setting $F_{i,x^*} = [Q] \setminus \{u_i\}$.) In order to argue that $e(g_1^{s_\ell}, h^{\alpha})$ is pseudorandom, we want $F_{\ell,x^*} = F$. For $i = 0, \ldots, \ell - 1$, we will define

$$F_{i,x^*} := \{\, u \in [Q] : \delta(u, x_{i+1}^*, \ldots, x_\ell^*) \in F \,\}.$$

Here, we use δ to also denote the "extended transition" function, namely

$$\delta(u, \sigma_1, \sigma_2, \ldots, \sigma_{\ell'}) = \delta(\delta(\delta(u, \sigma_1), \sigma_2), \ldots, \sigma_{\ell'}).$$

That is, F_{i,x^*} is the set of states that are reachable from the accept states in F by back-tracking along $x_\ell^*, \ldots, x_{i+1}^*$. In particular, if $f(x^*) = 0$, then $1 \notin F_{0,x^*}$ (recall that 1 denotes the start state) and more generally, $u_i \notin F_{i,x^*}$ (recall that $u_i = \delta(1, x_1^*, \ldots, x_i^*)$).

Finally, we modify $\Delta_{i,u}$ to be

$$\Delta_{i,u} := \begin{cases} \Delta & \text{if } u \in F_{i,x^*} \\ 0 & \text{otherwise} \end{cases}$$

Intuitively, the proof starts by introducing a unit of entropy captured by Δ to each state in F_{0,x^*} in G_0, and then propagates that entropy to the states in F_{1,x^*} in G_1, then F_{2,x^*} in G_2, and finally to $F_{\ell,x^*} = F$ in G_ℓ. We can then use Δ to mask α, upon which we can argue that the plaintext is perfectly hidden via an information-theoretic argument. Looking ahead, (5) captures precisely how we computationally propagate entropy from F_{i-1,x^*} in G_{i-1} to F_{i,x^*} in G_i. The key insight here is that these sets F_{i,x^*} are the states that are reachable by back-tracking from the accept states, and not the ones that are reachable from the start state.

Proof – interlude. Now, we are ready to describe how to carry out the hybrid argument from G_0 to G_ℓ. As mentioned earlier, we focus on the setting with a single key query f. This means that we need to show that for each $i = 1, \ldots, \ell$, we have:

$$\mathsf{G}_{i-1} = (\mathsf{mpk}, \mathsf{ct}_{x^*}^{i-1}, \mathsf{sk}_f^{i-1}) \approx_c (\mathsf{mpk}, \mathsf{ct}_{x^*}^{i}, \mathsf{sk}_f^{i}) = \mathsf{G}_i$$

To prove this, we will introduce an additional ciphertext distribution $\mathsf{ct}_{x^*}^{i-1,i}$, where:

- $\mathsf{ct}_{x^*}^{i-1,i}$ is the same as ct_{x^*} except we replace $g_1^{s_{i-1}}, g_1^{s_i}$ with $(g_1 g_2)^{s_{i-1}}, (g_1 g_2)^{s_i}$

and move from G_{i-1} to G_i via the following hybrid arguments:

$$\begin{aligned} \mathsf{G}_{i-1} = &\ (\mathsf{mpk},\ \mathsf{ct}_{x^*}^{i-1},\ \mathsf{sk}_f^{i-1}) \\ \approx_c &\ (\mathsf{mpk},\ \boxed{\mathsf{ct}_{x^*}^{i-1,i}},\ \mathsf{sk}_f^{i-1}) \\ \approx_c &\ (\mathsf{mpk},\ \mathsf{ct}_{x^*}^{i-1,i},\ \boxed{\mathsf{sk}_f^{i}}) \\ \approx_c &\ (\mathsf{mpk},\ \boxed{\mathsf{ct}_{x^*}^{i}},\ \mathsf{sk}_f^{i}) = \mathsf{G}_i \end{aligned} \tag{2}$$

Note that the proof interweaves a computational argument over ciphertexts with another over secret keys. In the proof, we will rely on the following computational assumptions in composite-order bilinear groups:

- $\mathrm{SD}^{G_N}_{p_1 \mapsto p_1 p_2}$ subgroup assumption in G_N, which says that $g_1^s \approx_c (g_1 g_2)^s$;
- $\mathrm{DDH}^{H_N}_{p_2}$ in H_N (w.r.t. w), which implies that $(h_2^r, h_2^{wr}) \approx_c (h_2^r, h_2^{\Delta + wr})$ given (h_2, h_2^w) for all Δ.

Later on, we will describe how to instantiate the scheme and these assumptions using the k-linear assumption in prime-order bilinear groups.

Proof – third idea. We begin with the first computational transition in (2), namely:

$$(\mathsf{mpk}, \mathsf{ct}_{x^*}^{i-1}, \mathsf{sk}_f^{i-1}) \approx_c (\mathsf{mpk}, \boxed{\mathsf{ct}_{x^*}^{i-1,i}}, \mathsf{sk}_f^{i-1})$$

The only difference between $\mathsf{ct}_{x^*}^{i-1}$ and $\mathsf{ct}_{x^*}^{i-1,i}$ is that we have $g_1^{s_i}$ in the former, and $(g_1 g_2)^{s_i}$ in the latter. Unfortunately, we cannot directly invoke the $\mathrm{SD}_{p_1 \mapsto p_1 p_2}^{G_N}$ assumption to carry out this transition, because we need h_2 to simulate the extra $h_2^{\Delta_{i-1,v}}$ terms in sk_f^{i-1}, and the $\mathrm{SD}_{p_1 \mapsto p_1 p_2}^{G_N}$ assumption is trivially broken in the presence of h_2. Instead, we crucially rely on the fact that the $h_2^{\Delta_{i-1,v}}$ terms appear in sk_f^{i-1} as:

$$h_2^{\Delta_{i-1,v}} \cdot h^{w_\sigma r_u},\ h^{r_u}$$

where $\Delta_{i-1,v} \in \{0, \Delta\}$. In particular, we will prove a statement of the form:

$$g_1^s \approx_c (g_1 g_2)^s \quad \text{given} \quad g_1, g_1^w, g_2, g_2^w, h, h^w, h_2^\Delta \cdot h^{wr}, h^r \tag{3}$$

where $s, w, r, \Delta \leftarrow \mathbb{Z}_N$. We refer to this as the (s,w)-switching lemma. Note the presence of the term g_2^w, which we need in the reduction to simulate the $g_2^{s_{i-1} w_{x^*_{i-1}}}$ term in $\mathsf{ct}_{x^*}^{i-1,i}$, and which means that $(h_2^\Delta \cdot h^{w_{x^*_{i-1}} r_u}, h^{r_u})$ is not pseudorandom. We will prove the (s,w)-switching lemma by exploiting the third p_3-subgroup, using a "two slot" dual system argument:

$$\begin{array}{rcllll}
\text{LHS} & = & g_1^s, & h^{wr} \cdot h_2^\Delta, & h^r & \\
& \overset{p_1 \mapsto p_1 p_3}{\approx_c} & g_1^s \cdot \boxed{g_3^s}, & h^{wr} \cdot h_2^\Delta, & h^r & \\
& \overset{\text{DDH}}{\approx_c} & g_1^s \cdot g_3^s, & h^{wr} \cdot h_2^\Delta \cdot \boxed{h_3^\Delta}, & h^r & \\
& \overset{p_3 \mapsto p_2}{\approx_c} & g_1^s \cdot \boxed{g_2^s}, & h^{wr} \cdot h_2^\Delta \cdot h_3^\Delta, & h^r & \\
& \overset{\text{DDH}}{\approx_c} & g_1^s \cdot g_2^s, & h^{wr} \cdot h_2^\Delta, & h^r & = \text{RHS}
\end{array} \tag{4}$$

We now clarify that there is in fact a catch here, namely that the (s,w)-switching lemma breaks down if the adversary is also given g_1^{sw}, which could indeed be the case due to the $g_2^{s_i w_{x^*_i}}$ term in $\mathsf{ct}_{x^*}^{i-1,i}$. We will circumvent this issue by modifying scheme (1) in the next section.

Looking ahead, we note that the same argument (once we fix the catch) would allow us to handle the third computational transition in (2), namely

$$(\mathsf{mpk}, \mathsf{ct}_{x^*}^{i-1,i}, \mathsf{sk}_f^i) \approx_c (\mathsf{mpk}, \boxed{\mathsf{ct}_{x^*}^i}, \mathsf{sk}_f^i).$$

Proof – fourth idea. Next, we handle the remaining computational transition in (2), namely

$$(\mathsf{mpk}, \mathsf{ct}_{x^*}^{i-1,i}, \mathsf{sk}_f^{i-1}) \approx_c (\mathsf{mpk}, \mathsf{ct}_{x^*}^{i-1,i}, \boxed{\mathsf{sk}_f^i})$$

By a standard argument based on the Chinese Remainder Theorem, it suffices to prove the statement for the p_2-components of the above expression, and since mpk has no p_2-components, this leaves us with:

$$(\mathsf{ct}_{x^*}^{i-1,i}[2], \mathsf{sk}_f^{i-1}[2]) \approx_c (\mathsf{ct}_{x^*}^{i-1,i}[2], \boxed{\mathsf{sk}_f^i[2]})$$

where $\mathsf{xx}[2]$ denotes the p_2-components of xx. That is, we will need to prove a statement of the form:

$$\begin{aligned}&\left\{h_2^{-d_u+zr_u},\, h_2^{d_v+\boxed{\Delta_{i-1,v}}+w_\sigma r_u},\, h_2^{r_u}\right\}_{u,\sigma,v=\delta(u,\sigma)}\\ \approx_c &\left\{h_2^{-d_u+zr_u},\, h_2^{d_v+\boxed{\Delta_{i,v}}+w_\sigma r_u},\quad h_2^{r_u}\right\}_{u,\sigma,v=\delta(u,\sigma)}\end{aligned}$$

given $\mathsf{ct}_{x^*}^{i-1,i}[2]$. Instead, we will sketch a proof that

$$\begin{aligned}&\left\{h_2^{-d_u+\boxed{\Delta_{i-1,u}}+zr_u},\, h_2^{d_v+w_\sigma r_u},\qquad h_2^{r_u}\right\}_{u,\sigma,v=\delta(u,\sigma)}\\ \approx_c &\left\{h_2^{-d_u+zr_u},\qquad h_2^{d_v+\boxed{\Delta_{i,v}}+w_\sigma r_u},\, h_2^{r_u}\right\}_{u,\sigma,v=\delta(u,\sigma)}\end{aligned} \tag{5}$$

given $(s_{i-1}, s_i, s_{i-1}z + s_i w_{x_i^*})$. The latter will be useful for simulating the terms in $\mathsf{ct}_{x^*}^{i-1,i}[2]$, which is given by:

$$\mathsf{ct}_{x^*}^{i-1,i}[2] = (g_2^{s_{i-1}w_{x^*_{i-1}}}, g_2^{s_{i-1}}, g_2^{s_{i-1}z+s_i w_{x_i^*}}, g_2^{s_i}, g_2^{s_i z})$$

We can interpret (5) as the key computational step that "propagates" the entropy from the states in F_{i-1,x^*} to those in F_{i,x^*}. We will explain the connection between (5) and the statement $\mathsf{sk}_f^{i-1} \approx_c \mathsf{sk}_f^i$ we need later on in the overview.

The proof of (5) relies on the following three observations:

1. by the $\mathrm{DDH}_{p_2}^{H_N}$ assumption w.r.t. $w_{x_i^*} \bmod p_2$, we have
$$(h_2^{zr}, h_2^{w_{x_i^*}r}, h_2^r) \approx_c (h_2^{zr-s_i\gamma}, h_2^{w_{x_i^*}r+s_{i-1}\gamma}, h_2^r) \tag{6}$$
given $(s_{i-1}, s_i, s_{i-1}z+s_i w_{x_i^*})$; this extends readily to the setting with many triplets corresponding to the r_u's. Note that the above triplets (X,Y,Z) satisfies a consistency check $X^{s_{i-1}} \cdot Y^{s_i} = Z^{s_{i-1}z+s_i w_{x_i^*}}$.
2. whenever $\sigma \neq x_i^*$, we can again invoke the $\mathrm{DDH}_{p_2}^{H_N}$ assumption, now w.r.t. $w_\sigma \bmod p_2$, to replace $h_2^{w_\sigma r_u}$ with $h_2^{\Delta_{i,v}+w_\sigma r_u}$ for all $u \in [Q], \sigma \neq x_i^*, v = \delta(u,\sigma)$.
3. for all x^* and $i \in [\ell], u \in [Q]$, we have
$$u \in F_{i-1,x^*} \iff \delta(u, x_i^*) \in F_{i,x^*}$$
This is one of two steps where we crucially relies on the definition of F_{i,x^*}.

We note that the analogue of (6) given also $g_2^{s_i z}$ in $\mathsf{ct}_x^{i-1,i}[2]$ is false due to the consistency check $e(g_2^{s_i}, h_2^{zr}) = e(g_2^{s_i z}, h_2^r)$. Again, we will circumvent this issue by modifying scheme (1) in the next section.

Proof – fifth idea. To make use of (5) in the proof, we introduce an additional key distribution $\mathsf{sk}_f^{i-1,i}$:

- $\mathsf{sk}_f^{i-1,i}$ is the same as sk_f except we add a $h_2^{\Delta_{i-1,u}}$ term to $h^{-d_u+zr_u}$ for every u.

Instead of

$$(\mathsf{mpk}, \mathsf{ct}_{x^*}^{i-1,i}, \mathsf{sk}_f^{i-1}) \approx_c (\mathsf{mpk}, \mathsf{ct}_{x^*}^{i-1,i}, \boxed{\mathsf{sk}_f^{i-1,i}}) \approx_c (\mathsf{mpk}, \mathsf{ct}_{x^*}^{i-1,i}, \boxed{\mathsf{sk}_f^{i}})$$

we will show:

$$(\mathsf{mpk}, \mathsf{ct}_{x^*}^{i-1}, \mathsf{sk}_f^{i-1}) \approx_c (\mathsf{mpk}, \mathsf{ct}_{x^*}^{i-1}, \boxed{\mathsf{sk}_f^{i-1,i}})$$
$$(\mathsf{mpk}, \mathsf{ct}_{x^*}^{i-1,i}, \boxed{\mathsf{sk}_f^{i-1,i}}) \approx_c (\mathsf{mpk}, \mathsf{ct}_{x^*}^{i-1,i}, \boxed{\mathsf{sk}_f^{i}})$$

That is, we will switch from sk_f^{i-1} to $\mathsf{sk}_f^{i-1,i}$ in the presence of $\mathsf{ct}_{x^*}^{i-1}$ instead of $\mathsf{ct}_{x^*}^{i-1,i}$ and employ the following strategy:

$$\begin{array}{rllll}
\mathsf{G}_{i-1} = & (\mathsf{mpk}, & \mathsf{ct}_{x^*}^{i-1}, & \mathsf{sk}_f^{i-1} &) \\
\approx_c & (\mathsf{mpk}, & \mathsf{ct}_{x^*}^{i-1}, & \boxed{\mathsf{sk}_f^{i-1,i}} &) \\
\approx_c & (\mathsf{mpk}, & \boxed{\mathsf{ct}_{x^*}^{i-1,i}}, & \mathsf{sk}_f^{i-1,i} &) \quad \text{similar to 1st transition in (2)} \\
\approx_c & (\mathsf{mpk}, & \mathsf{ct}_{x^*}^{i-1,i}, & \boxed{\mathsf{sk}_f^{i}} &) \quad \text{using (5)} \\
\approx_c & (\mathsf{mpk}, & \boxed{\mathsf{ct}_{x^*}^{i}}, & \mathsf{sk}_f^{i} &) = \mathsf{G}_i \quad \text{identical to 3rd transition in (2)}
\end{array} \tag{7}$$

Here, the last three computational transitions can be handled as before. This leaves us with the first transition, namely to show that

$$(\mathsf{mpk}, \mathsf{ct}_{x^*}^{i-1}, \mathsf{sk}_f^{i-1}) \approx_c (\mathsf{mpk}, \mathsf{ct}_{x^*}^{i-1}, \boxed{\mathsf{sk}_f^{i-1,i}}).$$

Roughly, we focus on the p_2-components and prove it via the following hybrid arguments:

$$\begin{aligned}
\mathsf{sk}_f^{i-1}[2] \;=\; & \left(\begin{array}{c} h_2^{d_1 + w_{\text{start}} r_1}, h_2^{r_1}, \\ \{h_2^{-d_u + z r_u}, h_2^{d_v + \boxed{\Delta_{i-1,v}} + w_\sigma r_u}, h_2^{r_u}\}_{u,\sigma,v=\delta(u,\sigma)}, \\ \{h_2^{\alpha - d_u + w_{\text{end}} r_u}, h_2^{r_u}\}_{u \in F} \end{array} \right) \\
\approx_s & \left(\begin{array}{c} h_2^{d_1 - \boxed{\Delta_{i-1,1}} + w_{\text{start}} r_1}, h_2^{r_1}, \\ \{h_2^{-d_u + \boxed{\Delta_{i-1,u}} + z r_u}, h_2^{d_v + w_\sigma r_u}, h_2^{r_u}\}_{u,\sigma,v=\delta(u,\sigma)}, \\ \{h_2^{\alpha - d_u + \boxed{\Delta_{i-1,u}} + w_{\text{end}} r_u}, h_2^{r_u}\}_{u \in F} \end{array} \right) \\
\approx_c & \left(\begin{array}{c} h_2^{d_1 - \cancel{\Delta_{i-1,1}} + w_{\text{start}} r_1}, h_2^{r_1}, \\ \{h_2^{-d_u + \Delta_{i-1,u} + z r_u}, h_2^{d_v + w_\sigma r_u}, h_2^{r_u}\}_{u,\sigma,v=\delta(u,\sigma)}, \\ \{h_2^{\alpha - d_u + \cancel{\Delta_{i-1,u}} + w_{\text{end}} r_u}, h_2^{r_u}\}_{u \in F} \end{array} \right) = \mathsf{sk}_f^{i-1,i}[2]
\end{aligned}$$

in the presence of $\mathsf{ct}_{x^*}^{i-1}[2]$, which is given by:

$$\mathsf{ct}_{x^*}^{i-1}[2] = \begin{cases} g_2^{s_0 w_{\text{start}}}, g_2^{s_0}, g_2^{s_0 z} & \text{if } i = 1 \\ g_2^{s_{i-1} w_{x^*_{i-1}}}, g_2^{s_{i-1}}, g_2^{s_{i-1} z} & \text{if } 2 \le i \le \ell \end{cases}$$

The first statistical step simply relies on the change of variable

$$d_u \mapsto d_u - \Delta_{i-1,u} \quad \forall u \in [Q].$$

Then we handle the second computational step by arguing

$$h_2^{-\Delta_{i-1,1}+w_{\mathsf{start}} r_1} \approx_c h_2^{w_{\mathsf{start}} r_1} \quad \text{and} \quad h_2^{\Delta_{i-1,u}+w_{\mathsf{end}} r_u} \approx_c h_2^{w_{\mathsf{end}} r_u} \quad \forall\, u \in F$$

This is implied by $\mathrm{DDH}_{p_2}^{H_N}$ assumption w.r.t. $w_{\mathsf{start}}, w_{\mathsf{end}} \bmod p_2$ with an exception:

- when $i = 1$, the ciphertext $\mathsf{ct}_{x^*}^0$ leaks $w_{\mathsf{start}} \bmod p_2$ via $g_2^{s_0 w_{\mathsf{start}}}$ and $\mathrm{DDH}_{p_2}^{H_N}$ assumption w.r.t. $w_{\mathsf{start}} \bmod p_2$ does not hold. In this case, we use the fact that $\Delta_{0,1} = 0$ which is implied by $1 \notin F_{0,x^*}$.

This is the second step where we crucially rely on the definition of F_{i,x^*}.

1.2 Our construction

Here is our final "alternating" construction, where we introduce two copies of $(z, \{w_\sigma\})$, and we alternate between the two copies in the ciphertext depending on the parity of i:

$$\begin{aligned}
\mathsf{msk} &= \big(\, h, \alpha, w_{\mathsf{start}}, w_{\mathsf{end}}, z_0, z_1, \{w_{\sigma,0}, w_{\sigma,1}\}_{\sigma\in\Sigma} \,\big) \\
\mathsf{mpk} &= \big(\, g_1, g_1^{w_{\mathsf{start}}}, g_1^{w_{\mathsf{end}}}, g_1^{z_0}, g_1^{z_1}, \{g_1^{w_{\sigma,0}}, g_1^{w_{\sigma,1}}\}_{\sigma\in\Sigma}, e(g_1,h)^{\alpha} \,\big) \\
\mathsf{ct}_x &= \begin{pmatrix} g_1^{s_0},\ g_1^{s_0 w_{\mathsf{start}}}, \\ \{g_1^{s_i}, g_1^{s_{i-1} z_{i \bmod 2} + s_i w_{x_i, i \bmod 2}}\}_{i\in[\ell]}, \\ g_1^{s_\ell}, g_1^{s_\ell w_{\mathsf{end}}},\ e(g_1,h)^{s_\ell \alpha}\cdot m \end{pmatrix} \\
\mathsf{sk}_f &= \begin{pmatrix} h^{d_1 + w_{\mathsf{start}} r_1}, h^{r_1}, \\ \{h^{-d_u + z_b r_u}, h^{d_v + w_{\sigma,b} r_u}, h^{r_u}\}_{b\in\{0,1\}, u\in[Q], \sigma\in\Sigma, v=\delta(u,\sigma)}, \\ \{h^{\alpha - d_u + w_{\mathsf{end}} r_u}, h^{r_u}\}_{u\in F} \end{pmatrix}
\end{aligned} \tag{8}$$

Note the additional $i \bmod 2$ subscript in ct_x and the additional quantifier $b \in \{0,1\}$ in sk_f. Decryption proceeds essentially as before by computing $e(g_1^{s_i}, h^{d_{u_i}})$ for $i = 0, \ldots, \ell$ and finally $e(g_1,h)^{s_\ell \alpha}$ and thus m.

Updating auxiliary distributions. The proof for the "alternating" construction still follows the strategy in (7). The distributions $\mathsf{ct}_{x^*}^i$ and $\mathsf{ct}_{x^*}^{i-1,i}$ are defined analogously; we update $\mathsf{sk}_f^i[2]$ and $\mathsf{sk}_f^{i-1,i}[2]$ for the "alternating" construction as follows:

$$\mathsf{sk}_f^i[2] = \begin{pmatrix} h_2^{d_1 + w_{\mathsf{start}} r_1}, h_2^{r_1}, \\ \{h_2^{-d_u + z_{i \bmod 2} r_u}, h_2^{d_v + \boxed{\Delta_{i,v}} + w_{\sigma, i \bmod 2} r_u}, h_2^{r_u}\}_{u,\sigma,v=\delta(u,\sigma)}, \\ \{h_2^{-d_u + z_{i-1 \bmod 2} r_u}, h_2^{d_v + w_{\sigma, i-1 \bmod 2} r_u}, h_2^{r_u}\}_{u,\sigma,v=\delta(u,\sigma)}, \\ \{h_2^{\alpha - d_u + w_{\mathsf{end}} r_u}, h_2^{r_u}\}_{u\in F} \end{pmatrix}$$

Game	$\mathsf{sk}_f[2]$			$\mathsf{ct}_x[2]$
0	$\llbracket d_u \mapsto d_v \rrbracket_{z_0,w_{\sigma,0}}$	$\llbracket d_u \mapsto d_v \rrbracket_{z_1,w_{\sigma,1}}$	$\llbracket d_u - \alpha \mapsto 0 \rrbracket_{w_{\text{end}},0}$	—
1	$\llbracket d_u \mapsto d_v \rrbracket_{z_0,w_{\sigma,0}}$	$\llbracket d_u \mapsto d_v \rrbracket_{z_1,w_{\sigma,1}}$	$\llbracket d_u - \alpha \mapsto 0 \rrbracket_{w_{\text{end}},0}$	$\boxed{s_0 w_{\text{start}}}, \boxed{s_0}, \boxed{s_0 z_1}$
2.1.0	$\llbracket d_u \mapsto d_v + \boxed{\Delta_{0,v}} \rrbracket_{z_0,w_{\sigma,0}}$	$\llbracket d_u \mapsto d_v \rrbracket_{z_1,w_{\sigma,1}}$	$\llbracket d_u - \alpha \mapsto 0 \rrbracket_{w_{\text{end}},0}$	$\downarrow$
2.1.1	$\llbracket d_u \mapsto d_v \rrbracket_{z_0,w_{\sigma,0}}$	$\llbracket d_u - \boxed{\Delta_{0,u}} \mapsto d_v \rrbracket_{z_1,w_{\sigma,1}}$	$\llbracket d_u - \alpha \mapsto 0 \rrbracket_{w_{\text{end}},0}$	$\downarrow$
2.1.2	$\llbracket d_u \mapsto d_v \rrbracket_{z_0,w_{\sigma,0}}$	$\llbracket d_u - \Delta_{0,u} \mapsto d_v \rrbracket_{z_1,w_{\sigma,1}}$	$\llbracket d_u - \alpha \mapsto 0 \rrbracket_{w_{\text{end}},0}$	$s_0 w_{\text{start}}, s_0, s_0 z_1 + \boxed{s_1 w_{x_1^*,1}}, \boxed{s_1}, \boxed{s_1 z_0}$
2.1.3	$\llbracket d_u \mapsto d_v \rrbracket_{z_0,w_{\sigma,0}}$	$\llbracket d_u \mapsto d_v + \boxed{\Delta_{1,v}} \rrbracket_{z_1,w_{\sigma,1}}$	$\llbracket d_u - \alpha \mapsto 0 \rrbracket_{w_{\text{end}},0}$	$\downarrow$
2.1.4 (=2.2.0)	$\llbracket d_u \mapsto d_v \rrbracket_{z_0,w_{\sigma,0}}$	$\llbracket d_u \mapsto d_v + \Delta_{1,v} \rrbracket_{z_1,w_{\sigma,1}}$	$\llbracket d_u - \alpha \mapsto 0 \rrbracket_{w_{\text{end}},0}$	$\cancel{s_0 w_{\text{start}}}, \cancel{s_0}, \cancel{s_0 z_1} + s_1 w_{x_1^*,1}, s_1, s_1 z_0$
2.2.1	$\llbracket d_u - \boxed{\Delta_{1,u}} \mapsto d_v \rrbracket_{z_0,w_{\sigma,0}}$	$\llbracket d_u \mapsto d_v \rrbracket_{z_1,w_{\sigma,1}}$	$\llbracket d_u - \alpha \mapsto 0 \rrbracket_{w_{\text{end}},0}$	$\downarrow$
2.2.2	$\llbracket d_u - \Delta_{1,u} \mapsto d_v \rrbracket_{z_0,w_{\sigma,0}}$	$\llbracket d_u \mapsto d_v \rrbracket_{z_1,w_{\sigma,1}}$	$\llbracket d_u - \alpha \mapsto 0 \rrbracket_{w_{\text{end}},0}$	$s_1 w_{x_1^*,1}, s_1, s_1 z_0 + \boxed{s_2 w_{x_2^*,0}}, \boxed{s_2}, \boxed{s_2 z_1}$
2.2.3	$\llbracket d_u \mapsto d_v + \boxed{\Delta_{2,v}} \rrbracket_{z_0,w_{\sigma,0}}$	$\llbracket d_u \mapsto d_v \rrbracket_{z_1,w_{\sigma,1}}$	$\llbracket d_u - \alpha \mapsto 0 \rrbracket_{w_{\text{end}},0}$	$\downarrow$
2.2.4 (=2.3.0)	$\llbracket d_u \mapsto d_v + \Delta_{2,v} \rrbracket_{z_0,w_{\sigma,0}}$	$\llbracket d_u \mapsto d_v \rrbracket_{z_1,w_{\sigma,1}}$	$\llbracket d_u - \alpha \mapsto 0 \rrbracket_{w_{\text{end}},0}$	$\cancel{s_1 w_{x_1^*,1}}, \cancel{s_1}, \cancel{s_1 z_0} + s_2 w_{x_2^*,0}, s_2, s_2 z_1$
2.3.1	$\llbracket d_u \mapsto d_v \rrbracket_{z_0,w_{\sigma,0}}$	$\llbracket d_u - \boxed{\Delta_{2,u}} \mapsto d_v \rrbracket_{z_1,w_{\sigma,1}}$	$\llbracket d_u - \alpha \mapsto 0 \rrbracket_{w_{\text{end}},0}$	$\downarrow$
2.3.2	$\llbracket d_u \mapsto d_v \rrbracket_{z_0,w_{\sigma,0}}$	$\llbracket d_u - \Delta_{2,u} \mapsto d_v \rrbracket_{z_1,w_{\sigma,1}}$	$\llbracket d_u - \alpha \mapsto 0 \rrbracket_{w_{\text{end}},0}$	$s_2 w_{x_2^*,0}, s_2, s_2 z_1 + \boxed{s_3 w_{x_3^*,1}}, \boxed{s_3}, \boxed{s_3 w_{\text{end}}}$
2.3.3	$\llbracket d_u \mapsto d_v \rrbracket_{z_0,w_{\sigma,0}}$	$\llbracket d_u \mapsto d_v + \boxed{\Delta_{3,v}} \rrbracket_{z_1,w_{\sigma,1}}$	$\llbracket d_u - \alpha \mapsto 0 \rrbracket_{w_{\text{end}},0}$	$\downarrow$
2.3.4	$\llbracket d_u \mapsto d_v \rrbracket_{z_0,w_{\sigma,0}}$	$\llbracket d_u \mapsto d_v + \Delta_{3,v} \rrbracket_{z_1,w_{\sigma,1}}$	$\llbracket d_u - \alpha \mapsto 0 \rrbracket_{w_{\text{end}},0}$	$\cancel{s_2 w_{x_2^*,0}}, \cancel{s_2}, \cancel{s_2 z_1} + s_3 w_{x_3^*,1}, s_3, s_3 w_{\text{end}}$
3	$\llbracket d_u \mapsto d_v \rrbracket_{z_0,w_{\sigma,0}}$	$\llbracket d_u \mapsto d_v \rrbracket_{z_1,w_{\sigma,1}}$	$\llbracket d_u - \boxed{\Delta_{3,u}} - \alpha \mapsto 0 \rrbracket_{w_{\text{end}},0}$	$\downarrow$

Fig. 1. Summary of game sequence for $\ell = 3$. We only describe the p_2-components here. Recall the notational short-hand $\llbracket d_u \mapsto d_v \rrbracket_{z,w} := (h_2^{-d_u + z r_u}, h_2^{d_v + w r_u}, h_2^{r_u})$. Here, secret key elements in the second and third columns are quantified over $u \in [Q], \sigma \in \Sigma, v = \sigma(u, \sigma)$ while those in the fourth column are over $u \in F$; we omit $\llbracket 0 \mapsto d_1 \rrbracket_{0,w_{\text{start}}}$. For the ciphertext elements, we omitted the terms $e(g_2^{s_3}, h^{\alpha})$ in games 2.3.$\star$ and 3. Throughout, a $\downarrow$ means "same as preceding row".

$$\mathsf{sk}_f^{i-1,i}[2] = \begin{pmatrix} h_2^{d_1+w_{\mathsf{start}}r_1}, h_2^{r_1}, \\ \{h_2^{-d_u+\boxed{\Delta_{i-1,u}}+z_{i \bmod 2}r_u}, h_2^{d_v+w_{\sigma,i \bmod 2}r_u}, h_2^{r_u}\}_{u,\sigma,v=\delta(u,\sigma)}, \\ \{h_2^{-d_u+z_{i-1 \bmod 2}r_u}, h_2^{d_v+w_{\sigma,i-1 \bmod 2}r_u}, h_2^{r_u}\}_{u,\sigma,v=\delta(u,\sigma)}, \\ \{h_2^{\alpha-d_u+w_{\mathsf{end}}r_u}, h_2^{r_u}\}_{u\in F} \end{pmatrix}$$

As an example, we illustrate a complete game sequence for 3-bit input in Fig. 1.

How alternation helps. We briefly describe how the alternating structure circumvents two of the issues in the earlier proof overview:

- To switch from $\mathsf{ct}_{x^*}^{i-1}$ to $\mathsf{ct}_{x^*}^{i-1,i}$ given $\mathsf{sk}_f^{i-1,i}$, we will rely on $(s_i, z_{i \bmod 2})$-switching lemma. The earlier issue with the terms $(g_1^{s_i}, g_1^{s_i z_{i+1 \bmod 2}})$ in $\mathsf{ct}_{x^*}^{i-1,i}$ simply goes away because $z_{i \bmod 2} \neq z_{i+1 \bmod 2}$, thanks to the alternation. A similar trick works for switching from $\mathsf{ct}_{x^*}^{i-1,i}$ to $\mathsf{ct}_{x^*}^{i}$.
- To switch from $\mathsf{sk}_f^{i-1,i}$ to sk_f^{i} given $\mathsf{ct}_{x^*}^{i-1,i}$, we will rely on the analogue of (6) with $(z_{i \bmod 2}, w_{x_i^*,i \bmod 2})$ in place of $(z, w_{x_i^*})$. The extra term in $\mathsf{ct}_{x^*}^{i-1,i}$ that enables the earlier attack now corresponds to $g_2^{s_i z_{i+1 \bmod 2}}$, and the attack is no longer applicable simply because $z_{i \bmod 2} \neq z_{i+1 \bmod 2}$, thanks again to the alternation.

Handling many secret keys. The proof extends to selective security for many keys, with fresh $\{d_u, r_u\}_{u\in[Q]}$ per key and the same Δ used across all the keys. Roughly speaking, the fresh r_u allows us to carry out the computational steps involving the $\mathrm{DDH}_{p_2}^{H_N}$ assumption, and in the final step, we rely on the fact that all the secret keys only leak $\alpha + \Delta$ and not α itself.

1.3 Prime-order groups

To complete the overview, we sketch our final ABE scheme which is secure under the k-Linear assumption in prime-order bilinear groups.[4] Here, we rely on the previous framework of Chen et al. [5,10,4,6] for simulating composite-order groups in prime-order ones. Let (G_1, G_2, G_T, e) be a bilinear group of prime order p. We start with our ABE scheme in composite-order groups (8) and carry out the following substitutions:

$$\begin{array}{llll} d_u, \alpha & \mapsto \mathbf{d}_u, \mathbf{k} & z_b, w_{\sigma,b} & \mapsto \mathbf{Z}_b, \mathbf{W}_{\sigma,b} \\ g_1^{s_i} & \mapsto [\mathbf{s}_i^\top \mathbf{A}_1^\top]_1 & h^{r_u} & \mapsto [\mathbf{r}_u]_2 \\ g_1^{s_i z_b}, g_1^{s_i w_{\sigma,b}} & \mapsto [\mathbf{s}_i^\top \mathbf{A}_1^\top \mathbf{Z}_b]_1, [\mathbf{s}_i^\top \mathbf{A}_1^\top \mathbf{W}_{\sigma,b}]_1 & h^{z_b r_u}, h^{w_{\sigma,b} r_u} & \mapsto [\mathbf{Z}_b \mathbf{r}_u]_2, [\mathbf{W}_{\sigma,b} \mathbf{r}_u]_2 \end{array}$$

where

$$\mathbf{A}_1 \leftarrow \mathbb{Z}_p^{(2k+1)\times k} \quad \text{and} \quad \mathbf{Z}_b, \mathbf{W}_{\sigma,b} \leftarrow \mathbb{Z}_p^{(2k+1)\times k},\ \mathbf{d}_u, \mathbf{k} \leftarrow \mathbb{Z}_p^{2k+1},\ \mathbf{s}_i, \mathbf{r}_u \leftarrow \mathbb{Z}_p^k$$

[4] e.g: $k = 1$ corresponds to the Symmetric External Diffie-Hellman Assumption (SXDH), and $k = 2$ corresponds to the Decisional Linear Assumption (DLIN).

and $[\cdot]_1, [\cdot]_2$ correspond respectively to exponentiations in the prime-order groups G_1, G_2. Note that $\mathbf{A}_1$ has height $2k+1$: we will use k-dimensional random subspaces to simulate each of the p_1 and p_3 subgroups, and a 1-dimensional subspace to simulate the p_2 subgroup; these are sufficient to simulate the $\mathrm{SD}^{G_N}_{p_1 \mapsto p_1 p_2}$, $\mathrm{SD}^{G_N}_{p_1 \mapsto p_1 p_3}$ and $\mathrm{SD}^{G_N}_{p_3 \mapsto p_3 p_2}$ assumptions (we would need to modify the proof of the (s,w)-switching lemma in (4) to avoid $\mathrm{SD}^{G_N}_{p_3 \mapsto p_2}$ assumption). It is sufficient to use $\mathbf{Z}_b, \mathbf{W}_{\sigma,b}$ of width k since we only rely on the $\mathrm{DDH}^{H_N}_{p_2}$, $\mathrm{DDH}^{H_N}_{p_3}$ assumptions.

This yields the following prime-order ABE scheme for DFA:

$$\begin{aligned}
\mathsf{msk} &= \big(\, \mathbf{k}, \mathbf{W}_{\text{start}}, \mathbf{W}_{\text{end}}, \mathbf{Z}_0, \mathbf{Z}_1, \{\mathbf{W}_{\sigma,0}, \mathbf{W}_{\sigma,1}\}_{\sigma \in \Sigma} \,\big) \\
\mathsf{mpk} &= \big(\, [\mathbf{A}_1^\top, \mathbf{A}_1^\top \mathbf{W}_{\text{start}}, \mathbf{A}_1^\top \mathbf{W}_{\text{end}}, \mathbf{A}_1^\top \mathbf{Z}_0, \mathbf{A}_1^\top \mathbf{Z}_1, \{\mathbf{A}_1^\top \mathbf{W}_{\sigma,0}, \mathbf{A}_1^\top \mathbf{W}_{\sigma,1}\}_{\sigma \in \Sigma}]_1, [\mathbf{A}_1^\top \mathbf{k}]_T \,\big) \\
\mathsf{ct}_x &= \begin{pmatrix} [\mathbf{s}_0^\top \mathbf{A}_1^\top]_1,\ [\mathbf{s}_0^\top \mathbf{A}_1^\top \mathbf{W}_{\text{start}}]_1 \\ \{[\mathbf{s}_i^\top \mathbf{A}_1^\top]_1, [\mathbf{s}_{i-1}^\top \mathbf{A}_1^\top \mathbf{Z}_{i \bmod 2} + \mathbf{s}_i^\top \mathbf{A}_1^\top \mathbf{W}_{x_i, i \bmod 2}]_1\}_{i \in [\ell]} \\ [\mathbf{s}_\ell^\top \mathbf{A}_1^\top]_1, [\mathbf{s}_\ell^\top \mathbf{A}_1^\top \mathbf{W}_{\text{end}}]_1,\ [\mathbf{s}_\ell^\top \mathbf{A}_1^\top \mathbf{k}]_T \cdot m \end{pmatrix} \\
\mathsf{sk}_f &= \begin{pmatrix} [\mathbf{d}_1 + \mathbf{W}_{\text{start}} \mathbf{r}_1]_2, [\mathbf{r}_1]_2, \\ \{[-\mathbf{d}_u + \mathbf{Z}_b \mathbf{r}_u]_2, [\mathbf{d}_v + \mathbf{W}_{\sigma,b} \mathbf{r}_u]_2, [\mathbf{r}_u]_2\}_{b \in \{0,1\}, u \in [Q], \sigma \in \Sigma, v = \delta(u,\sigma)} \\ \{[\mathbf{k} - \mathbf{d}_u + \mathbf{W}_{\text{end}} \mathbf{r}_u]_2, [\mathbf{r}_u]_2\}_{u \in F} \end{pmatrix}.
\end{aligned}$$

Decryption proceeds as before by first computing

$$[\mathbf{s}_i^\top \mathbf{A}_1^\top \mathbf{d}_{u_i}]_T \quad \forall i = 0, \ldots, \ell$$

via the associativity relations $\mathbf{A}_1^\top \mathbf{Z} \cdot \mathbf{r}_u = \mathbf{A}_1^\top \cdot \mathbf{Z} \mathbf{r}_u$ (ditto $\mathbf{W}_{\text{start}}, \mathbf{W}_{\sigma,b}, \mathbf{W}_{\text{end}}$) [7]; and finally recovers $[\mathbf{s}_\ell^\top \mathbf{A}_1^\top \mathbf{k}]_T$ and thus m.

1.4 Discussion

The main open problem arising in this work is to obtain an adaptively secure ABE scheme for DFA under the k-Lin assumption. One natural approach is to combine our techniques with the piecewise guessing framework in [14,13] to obtain an adaptively secure ABE scheme for DFA under the k-Lin assumption. The main obstacle here is that in the intermediate hybrids, we need to know the sets F_{i,x^*}, for which there can be up to 2^Q possibilities, where Q is the maximal number of states in a DFA provided by the adversary in the secret key queries. As such, naively applying the piecewise guessing framework would incur a 2^Q security loss. Another potential approach is to appeal to the doubly selective framework in [2,17], which reduces the problem to building a selectively secure ciphertext-policy ABE for DFA (alternatively, a co-selectively secure key-policy ABE for DFA) under the k-Lin assumption, in the single-key setting; again, naively applying the techniques in this work would incur a 2^Q security loss. To conclude, achieving adaptive security under the k-Lin assumption with only a polynomial loss appears to require new ideas that go beyond the state of the art.

Organization. The next section gives some background knowledge. We prove selective security of the composite-order scheme in the one-key setting in Section 3. We defer the prime-order scheme with proof in the many-key setting to the full paper.

2 Preliminaries

Notation. We denote by $s \leftarrow S$ the fact that s is picked uniformly at random from a finite set S. By PPT, we denote a probabilistic polynomial-time algorithm. Throughout this paper, we use 1^λ as the security parameter. We use lower case boldface to denote (column) vectors and upper case boldcase to denote matrices. We use $\approx_s$ to denote two distributions being statistically indistinguishable, and $\approx_c$ to denote two distributions being computationally indistinguishable.

Deterministic Finite Automaton (DFA). A deterministic finite automaton (DFA) f is defined by (Q, Σ, δ, F) where

- Q is the number of states and we take $[Q]$ as the state space;
- Σ is the alphabet;
- $\delta : [Q] \times \Sigma \to [Q]$ is a transition function;
- $F \subseteq [Q]$ is the set of accept states.

Here the (unique) start state is always state 1. We use $f(x) = 1$ to denote that an input $x = (x_1, \ldots, x_\ell) \in \Sigma^\ell$ is accepted by DFA f, which means that there exists a sequence of states $u_0, u_1, \ldots, u_\ell \in [Q]$ satisfying: (1) $u_0 = 1$; (2) for all $i = 1, \ldots, \ell$, we have $\delta(u_{i-1}, x_i) = u_i$; (3) $u_\ell \in F$. If input x is not accepted by DFA f, we write $f(x) = 0$.

2.1 Attribute-based encryption for Deterministic Finite Automaton

Syntax. An attribute-based encryption (ABE) scheme for DFA consists of four algorithms $(\mathsf{Setup}, \mathsf{Enc}, \mathsf{KeyGen}, \mathsf{Dec})$:

$\mathsf{Setup}(1^\lambda, \Sigma) \to (\mathsf{mpk}, \mathsf{msk})$. The setup algorithm gets as input the security parameter 1^λ and the alphabet Σ. It outputs the public parameter mpk and the master key msk. We assume mpk defines the message space $\mathcal{M}$.

$\mathsf{Enc}(\mathsf{mpk}, x, m) \to \mathsf{ct}_x$. The encryption algorithm gets as input mpk, an input $x \in \Sigma^*$ and a message $m \in \mathcal{M}$. It outputs a ciphertext ct_x. Note that x is public given ct_x.

$\mathsf{KeyGen}(\mathsf{mpk}, \mathsf{msk}, f) \to \mathsf{sk}_f$. The key generation algorithm gets as input mpk, msk and a description of DFA f. It outputs a secret key sk_f. Note that f is public given sk_f.

$\mathsf{Dec}(\mathsf{mpk}, \mathsf{sk}_f, \mathsf{ct}_x) \to m$. The decryption algorithm gets as input sk_f and ct_x such that $f(x) = 1$ along with mpk. It outputs a message m.

Correctness. For all input x and DFA f with $f(x) = 1$ and all $m \in \mathcal{M}$, we require

$$\Pr\left[\mathsf{Dec}(\mathsf{mpk}, \mathsf{sk}_f, \mathsf{ct}_x) = m : \begin{array}{c} (\mathsf{mpk}, \mathsf{msk}) \leftarrow \mathsf{Setup}(1^\lambda, \Sigma); \\ \mathsf{sk}_f \leftarrow \mathsf{KeyGen}(\mathsf{mpk}, \mathsf{msk}, f); \\ \mathsf{ct}_x \leftarrow \mathsf{Enc}(\mathsf{mpk}, x, m) \end{array}\right] = 1.$$

Security definition. For a stateful adversary $\mathcal{A}$, we define the advantage function

$$\mathsf{Adv}_{\mathcal{A}}^{\mathrm{ABE}}(\lambda) := \Pr\left[\beta = \beta' : \begin{array}{l} (\mathsf{mpk}, \mathsf{msk}) \leftarrow \mathsf{Setup}(1^\lambda, \Sigma); \\ (x^*, m_0, m_1) \leftarrow \mathcal{A}^{\mathsf{KeyGen}(\mathsf{mpk},\mathsf{msk},\cdot)}(\mathsf{mpk}); \\ \beta \leftarrow \{0,1\};\ \mathsf{ct}_{x^*} \leftarrow \mathsf{Enc}(\mathsf{mpk}, x^*, m_\beta); \\ \beta' \leftarrow \mathcal{A}^{\mathsf{KeyGen}(\mathsf{mpk},\mathsf{msk},\cdot)}(\mathsf{ct}_{x^*}) \end{array}\right] - \frac{1}{2}$$

with the restriction that all queries f that $\mathcal{A}$ makes to $\mathsf{KeyGen}(\mathsf{mpk}, \mathsf{msk}, \cdot)$ satisfy $f(x^*) = 0$. An ABE scheme is *adaptively secure* if for all PPT adversaries $\mathcal{A}$, the advantage $\mathsf{Adv}_{\mathcal{A}}^{\mathrm{ABE}}(\lambda)$ is a negligible function in λ. The *selective security* is defined analogously except that the adversary $\mathcal{A}$ selects x^* before seeing mpk.

2.2 Composite-order Groups

A generator $\mathcal{G}$ takes as input a security parameter 1^λ and outputs group description $\mathbb{G} := (N, G_N, H_N, G_T, e)$, where N is product of three primes p_1, p_2, p_3 of $\Theta(\lambda)$ bits, G_N, H_N and G_T are cyclic groups of order N and $e : G_N \times H_N \to G_T$ is a non-degenerate bilinear map. We require that the group operations in G_N, H_N and G_T as well the bilinear map e are computable in deterministic polynomial time with respect to λ. We assume that a random generator g (resp. h) of G_N (resp. H_N) is always contained in the description of bilinear groups. For every divisor n of N, we denote by G_n the subgroup of G_N of order n. We use g_1, g_2, g_3 to denote random generators of subgroups $G_{p_1}, G_{p_2}, G_{p_3}$ respectively and define h_1, h_2, h_3 random generators of subgroups $H_{p_1}, H_{p_2}, H_{p_3}$ analogously.

Computational assumptions. We review two static computational assumptions in the composite-order group, used e.g. in [15,8]. By symmetry, one may permute the indices for subgroups.

Assumption 1 ($\mathbf{SD}^{G_N}_{p_1 \mapsto p_1 p_2}$) *We say that $(p_1 \mapsto p_1 p_2)$-subgroup decision assumption, denoted by $SD^{G_N}_{p_1 \mapsto p_1 p_2}$, holds if for all PPT adversaries $\mathcal{A}$, the following advantage function is negligible in λ.*

$$\mathsf{Adv}_{\mathcal{A}}^{\mathsf{SD}^{G_N}_{p_1 \mapsto p_1 p_2}}(\lambda) := \big|\Pr[\mathcal{A}(\mathbb{G}, D, T_0) = 1] - \Pr[\mathcal{A}(\mathbb{G}, D, T_1) = 1]\big|$$

where $D := (g_1, g_2, g_3, h_1, h_3, h_{12})$ with $h_{12} \leftarrow H_{p_1 p_2}$ and

$$T_0 \leftarrow_{\mathrm{R}} \boxed{G_{p_1}},\ T_1 \leftarrow \boxed{G_{p_1 p_2}}.$$

Assumption 2 ($\mathbf{DDH}^{H_N}_{p_1}$) *We say that p_1-subgroup Diffie-Hellman assumption, denoted by $DDH^{H_N}_{p_1}$, holds if for all PPT adversaries $\mathcal{A}$, the following advantage function is negligible in λ.*

$$\mathsf{Adv}_{\mathcal{A}}^{\mathsf{DDH}^{H_N}_{p_1}}(\lambda) := \big|\Pr[\mathcal{A}(\mathbb{G}, D, T_0) = 1] - \Pr[\mathcal{A}(\mathbb{G}, D, T_1) = 1]\big|$$

where $D := (g_1, g_2, g_3, h_1, h_2, h_3)$ and

$$T_0 := (h_1^x, h_1^y, \boxed{h_1^{xy}}),\ T_1 := (h_1^x, h_1^y, \boxed{h_1^{xy+z}}), \quad x, y, z \leftarrow \mathbb{Z}_N.$$

3 ABE for DFA in Composite-Order Groups

In this section, we present our ABE for DFA in composite-order groups. Here, we focus on selective security in the *one-key* setting under static assumptions.

3.1 Scheme

Our ABE for DFA in composite-order groups is described as follows:

- $\mathsf{Setup}(1^\lambda, \Sigma)$: Run $\mathbb{G} = (N = p_1p_2p_3, G_N, H_N, G_T, e) \leftarrow \mathcal{G}(1^\lambda)$ and pick generators $g_1 \leftarrow G_{p_1}, h \leftarrow H_N$. Sample $\alpha, w_{\text{start}}, w_{\text{end}}, z_0, z_1, w_{\sigma,0}, w_{\sigma,1} \leftarrow \mathbb{Z}_N$ for all $\sigma \in \Sigma$. Choose a pairwise-independent hash function H. Output

$$\begin{aligned}\mathsf{mpk} &= \big(g_1, g_1^{w_{\text{start}}}, g_1^{w_{\text{end}}}, g_1^{z_0}, g_1^{z_1}, \{ g_1^{w_{\sigma,0}}, g_1^{w_{\sigma,1}} \}_{\sigma\in\Sigma}, e(g_1,h)^\alpha, \mathsf{H} \big) \quad \text{and} \\ \mathsf{msk} &= \big(h, \alpha, w_{\text{start}}, w_{\text{end}}, z_0, z_1, \{w_{\sigma,0}, w_{\sigma,1}\}_{\sigma\in\Sigma} \big)\end{aligned}$$

  The message space $\mathcal{M}$ is the image space of H.
- $\mathsf{Enc}(\mathsf{mpk}, x, m)$: Let $x = (x_1, \ldots, x_\ell) \in \Sigma^\ell$. Pick $s_0, s_1, \ldots, s_\ell \leftarrow \mathbb{Z}_N$ and output

$$\mathsf{ct}_x = \left(\begin{array}{c} g_1^{s_0},\ g_1^{s_0 w_{\text{start}}}, \\ \{ g_1^{s_i}, g_1^{s_{i-1} z_{i \bmod 2} + s_i w_{x_i, i \bmod 2}} \}_{i\in[\ell]}, \\ g_1^{s_\ell}, g_1^{s_\ell w_{\text{end}}},\ \mathsf{H}(e(g_1,h)^{s_\ell \alpha}) \cdot m \end{array} \right).$$

- $\mathsf{KeyGen}(\mathsf{mpk}, \mathsf{msk}, f)$: Pick $d_u, r_u \leftarrow \mathbb{Z}_N$ for all $u \in [Q]$ and output

$$\mathsf{sk}_f = \left(\begin{array}{c} h^{d_1 + w_{\text{start}} r_1}, h^{r_1}, \\ \{h^{-d_u + z_b r_u}, h^{d_v + w_{\sigma,b} r_u}, h^{r_u}\}_{b\in\{0,1\}, u\in[Q], \sigma\in\Sigma, v=\delta(u,\sigma)}, \\ \{h^{\alpha - d_u + w_{\text{end}} r_u}, h^{r_u}\}_{u\in F} \end{array} \right).$$

- $\mathsf{Dec}(\mathsf{mpk}, \mathsf{sk}_f, \mathsf{ct}_x)$: Parse ciphertext for input $x = (x_1, \ldots, x_\ell)$ as

$$\mathsf{ct}_x = (\, C_{0,1}, C_{0,2}, \{C_{i,1}, C_{i,2}\}_{i\in[\ell]}, C_{\text{end},1}, C_{\text{end},2}, C \,)$$

  and key for $f = (Q, \Sigma, \delta, F)$ as

$$\mathsf{sk}_f = (\, K_{0,1}, K_{0,2}, \{K_{b,u}, K_{b,u,\sigma}, K_u\}_{b,u,\sigma}, \{K_{\text{end},u}, K_u\}_{u\in F} \,).$$

  If $f(x) = 1$, compute $(u_0 = 1, u_1, \ldots, u_\ell) \in [Q]^{\ell+1}$ such that $\delta(u_{i-1}, x_i) = u_i$ for $i \in [\ell]$ and $u_\ell \in F$, and proceed as follows:
  1. Compute $B_0 = e(C_{0,1}, K_{0,1}) \cdot e(C_{0,2}, K_{0,2})^{-1}$;
  2. For all $i = 1, \ldots, \ell$, compute

$$B_i = e(C_{i-1,1}, K_{i \bmod 2, u_{i-1}}) \cdot e(C_{i,1}, K_{i \bmod 2, u_{i-1}, x_i}) \cdot e(C_{i,2}, K_{u_{i-1}})^{-1}$$

  3. Compute $B_{\text{end}} = e(C_{\text{end},1}, K_{\text{end},u_\ell}) \cdot e(C_{\text{end},2}, K_{u_\ell})^{-1}$ and

$$B = B_0 \cdot \prod_{i=1}^{\ell} B_i \cdot B_{\text{end}}$$

  4. Output the message $m' \leftarrow C \cdot \mathsf{H}(B)^{-1}$.

Due to the lack of space, we defer the proof of correctness to the full paper.

Security. We will prove the following theorem for the *one-key* setting where the adversary asks for at most one secret key. We explain how to handle *many* keys in Section 3.9.

Theorem 1 (composite-order ABE for DFA). *The ABE scheme for DFA in composite-order bilinear groups described above is selectively secure (cf. Section 2.1) in the one-key setting under the following static assumptions:* $\mathrm{SD}^{G_N}_{p_1 \mapsto p_1 p_2}$, $\mathrm{SD}^{G_N}_{p_1 \mapsto p_1 p_3}$, $\mathrm{SD}^{G_N}_{p_3 \mapsto p_3 p_2}$, $\mathrm{DDH}^{H_N}_{p_2}$ *and* $\mathrm{DDH}^{H_N}_{p_3}$.

3.2 Game sequence

Let $x^* \in \Sigma^\ell$ denote the selective challenge and let $\bar{\ell} = \ell \bmod 2$. WLOG, we assume $\ell > 1$. Recall that g_2, h_2 denote random generators for G_{p_2}, H_{p_2} respectively.

Auxiliary distributions. We describe the auxiliary ciphertext and secret key distributions that we use in the proof of security. Throughout, the distributions are the same as the original distributions except for the p_2-components. For notational simplicity, we will only write down the p_2-components and use $\mathsf{xx}[2]$ to denote p_2-components of xx.

Ciphertext distributions.

- for $i = 0, 1, \ldots, \ell$: $\mathsf{ct}^i_{x^*}$ is the same as ct_{x^*} except we replace $g_1^{s_i}$ with $(g_1 g_2)^{s_i}$;
- for $i = 1, 2, \ldots, \ell$: $\mathsf{ct}^{i-1,i}_{x^*}$ is the same as ct_{x^*} except we replace $g_1^{s_{i-1}}, g_1^{s_i}$ with $(g_1 g_2)^{s_{i-1}}, (g_1 g_2)^{s_i}$.

That is, we have: writing $\tau = i \bmod 2$,

$$\mathsf{ct}^i_{x^*}[2] = \begin{cases} g_2^{s_0 w_{\mathsf{start}}}, g_2^{s_0}, g_2^{s_0 z_1} & \text{if } i = 0 \\ g_2^{s_i w_{x^*_i,\tau}}, g_2^{s_i}, g_2^{s_i z_{1-\tau}} & \text{if } 0 < i < \ell \\ g_2^{s_\ell w_{x^*_\ell,\bar{\ell}}}, g_2^{s_\ell}, g_2^{s_\ell w_{\mathsf{end}}}, e(g_2^{s_\ell}, h_2^{\alpha}) & \text{if } i = \ell \end{cases}$$

$$\mathsf{ct}^{i-1,i}_{x^*}[2] = \begin{cases} g_2^{s_0 w_{\mathsf{start}}}, g_2^{s_0}, g_2^{s_0 z_1 + s_1 w_{x^*_1,1}}, g_2^{s_1}, g_2^{s_1 z_0} & \text{if } i = 1 \\ g_2^{s_{i-1} w_{x^*_{i-1},1-\tau}}, g_2^{s_{i-1}}, g_2^{s_{i-1} z_\tau + s_i w_{x^*_i,\tau}}, g_2^{s_i}, g_2^{s_i z_{1-\tau}} & \text{if } 1 < i < \ell \\ g_2^{s_{\ell-1} w_{x^*_{\ell-1},1-\bar{\ell}}}, g_2^{s_{\ell-1}}, g_2^{s_{\ell-1} z_{\bar{\ell}} + s_\ell w_{x^*_\ell,\bar{\ell}}}, g_2^{s_\ell}, g_2^{s_\ell w_{\mathsf{end}}}, e(g_2^{s_\ell}, h_2^{\alpha}) & \text{if } i = \ell \end{cases}$$

The Δ-distributions. Fix a DFA f. Let $F_{\ell,x^*} = F$; for $i = 0, \ldots, \ell - 1$, we will define

$$F_{i,x^*} := \{\, u \in [Q] : \delta(u, x^*_{i+1}, \ldots, x^*_\ell) \in F \,\}.$$

Here, we use δ to also denote the "extended transition" function, namely

$$\delta(u, \sigma_1, \sigma_2, \ldots, \sigma_{\ell'}) = \delta(\delta(\delta(u, \sigma_1), \sigma_2), \ldots, \sigma_{\ell'}).$$

That is, F_{i,x^*} is the set of states that are reachable from the accept states by backtracking along $x^*_\ell, \ldots, x^*_{i+1}$. In particular, if $f(x^*) = 0$, then $1 \notin F_{0,x^*}$ (recall that 1 denotes the start state) and more generally, $u_i \notin F_{i,x^*}$ (recall that $u_i = \delta(1, x^*_1, \ldots, x^*_i)$). Finally, we pick $\Delta \leftarrow \mathbb{Z}_N$ and define $\Delta_{i,u}$ to be

$$\Delta_{i,u} := \begin{cases} \Delta & \text{if } u \in F_{i,x^*} \\ 0 & \text{otherwise} \end{cases}$$

Secret key distributions.

- for $i = 0, 1, \ldots, \ell$: sk_f^i is the same as sk_f except we add $h_2^{\Delta_{i,v}}$ to $h^{d_v + w_{\sigma, i \bmod 2} r_u}$ for every $u \in [Q], \sigma \in \Sigma$ and $v = \delta(u, \sigma)$.
- for $i = 1, 2, \ldots, \ell$: $\mathsf{sk}_f^{i-1,i}$ is the same as sk_f except we add $h_2^{\Delta_{i-1,u}}$ to $h^{-d_u + z_{i \bmod 2} r_u}$ for every $u \in [Q]$.
- sk_f^* is the same as sk_f except we add $h_2^{\Delta_{\ell,u}}$ to $h^{\alpha - d_u + w_{\text{end}} r_u}$ for every $u \in F$.

That is, we have: writing $\tau = i \bmod 2$,

$$\mathsf{sk}_f^i[2] = \begin{pmatrix} h_2^{d_1 + w_{\text{start}} r_1}, h_2^{r_1}, \\ \{h_2^{-d_u + z_\tau r_u}, h_2^{d_v + \boxed{\Delta_{i,v}} + w_{\sigma,\tau} r_u}, h_2^{r_u}\}_{u \in [Q], \sigma \in \Sigma, v = \delta(u,\sigma)}, \\ \{h_2^{-d_u + z_{1-\tau} r_u}, h_2^{d_v + w_{\sigma,1-\tau} r_u}, h_2^{r_u}\}_{u \in [Q], \sigma \in \Sigma, v = \delta(u,\sigma)}, \\ \{h_2^{\alpha - d_u + w_{\text{end}} r_u}, h_2^{r_u}\}_{u \in F} \end{pmatrix}$$

$$\mathsf{sk}_f^{i-1,i}[2] = \begin{pmatrix} h_2^{d_1 + w_{\text{start}} r_1}, h_2^{r_1}, \\ \{h_2^{-d_u + \boxed{\Delta_{i-1,u}} + z_\tau r_u}, h_2^{d_v + w_{\sigma,\tau} r_u}, h_2^{r_u}\}_{u \in [Q], \sigma \in \Sigma, v = \delta(u,\sigma)}, \\ \{h_2^{-d_u + z_{1-\tau} r_u}, h_2^{d_v + w_{\sigma,1-\tau} r_u}, h_2^{r_u}\}_{u \in [Q], \sigma \in \Sigma, v = \delta(u,\sigma)}, \\ \{h_2^{\alpha - d_u + w_{\text{end}} r_u}, h_2^{r_u}\}_{u \in F} \end{pmatrix}$$

$$\mathsf{sk}_f^*[2] = \begin{pmatrix} h_2^{d_1 + w_{\text{start}} r_1}, h_2^{r_1}, \\ \{h_2^{-d_u + z_b r_u}, h_2^{d_v + w_{\sigma,b} r_u}, h_2^{r_u}\}_{b \in \{0,1\}, u \in [Q], \sigma \in \Sigma, v = \delta(u,\sigma)}, \\ \{h_2^{\alpha - d_u + \boxed{\Delta_{\ell,u}} + w_{\text{end}} r_u}, h_2^{r_u}\}_{u \in F} \end{pmatrix}$$

Game sequence. We prove Theorem 1 via a series of games described below and summarized in Fig 2.

- G_0: Identical to the real game.
- G_1: Identical to G_0 except that the challenge ciphertext is $\mathsf{ct}_{x^*}^0$.
- $\mathsf{G}_{2.i.0}$, $i = 1, \ldots, \ell$: In this game, the challenge ciphertext is $\mathsf{ct}_{x^*}^{i-1}$ and the secret key is sk_f^{i-1}. Note that $\mathsf{G}_{2.1.0}$ is identical to G_1 except that the secret key is sk_f^0 and we have $\mathsf{G}_{2.i.0} = \mathsf{G}_{2.i-1.4}$ for all $2 \le i \le \ell$.
- $\mathsf{G}_{2.i.1}$, $i = 1, \ldots, \ell$: Identical to $\mathsf{G}_{2.i.0}$ except that the secret key is $\mathsf{sk}_f^{i-1,i}$.
- $\mathsf{G}_{2.i.2}$, $i = 1, \ldots, \ell$: Identical to $\mathsf{G}_{2.i.1}$ except that the challenge ciphertext is $\mathsf{ct}_{x^*}^{i-1,i}$.
- $\mathsf{G}_{2.i.3}$, $i = 1, \ldots, \ell$: Identical to $\mathsf{G}_{2.i.2}$ except that the secret key is sk_f^i.
- $\mathsf{G}_{2.i.4}$, $i = 1, \ldots, \ell$: Identical to $\mathsf{G}_{2.i.3}$ except that the challenge ciphertext is $\mathsf{ct}_{x^*}^i$.
- G_3: Identical to $\mathsf{G}_{2.\ell.4}$ except that secret key is sk_f^*.

We use $\mathsf{Adv}_{\mathcal{A}}^{\mathsf{xxx}}(\lambda)$ to denote the advantage of adversary $\mathcal{A}$ in $\mathsf{G}_{\mathsf{xxx}}$ with parameter 1^λ.

3.3 Useful lemmas

We begin with a few useful lemmas which will be used throughout the proof of security.

Game	ct_{x^*}		p_2-components of sk_f			Remark
0	ct_{x^*}	sk_f	$[\![d_u \mapsto d_v]\!]_{z_0,w_{\sigma,0}}$	$[\![d_u \mapsto d_v]\!]_{z_1,w_{\sigma,1}}$	$[\![d_u - \alpha \mapsto 0]\!]_{w_{\text{end}},0}$	Real game
1	$\boxed{\mathsf{ct}^0_{x^*}}$	sk_f	$[\![d_u \mapsto d_v]\!]_{z_0,w_{\sigma,0}}$	$[\![d_u \mapsto d_v]\!]_{z_1,w_{\sigma,1}}$	$[\![d_u - \alpha \mapsto 0]\!]_{w_{\text{end}},0}$	SD
2.1.0	$\mathsf{ct}^0_{x^*}$	$\boxed{\mathsf{sk}^0_f}$	$[\![d_u \mapsto d_v + \boxed{\Delta_{0,v}}]\!]_{z_0,w_{\sigma,0}}$	$[\![d_u \mapsto d_v]\!]_{z_1,w_{\sigma,1}}$	$[\![d_u - \alpha \mapsto 0]\!]_{w_{\text{end}},0}$	DDH
2.i.0	$\mathsf{ct}^{i-1}_{x^*}$	sk^{i-1}_f	$[\![d_u \mapsto d_v]\!]_{z_\tau,w_{\sigma,\tau}}$	$[\![d_u \mapsto d_v + \boxed{\Delta_{i-1,v}}]\!]_{z_{1-\tau},w_{\sigma,1-\tau}}$	$[\![d_u - \alpha \mapsto 0]\!]_{w_{\text{end}},0}$	$\mathsf{G}_{2.i.0} = \mathsf{G}_{2.i-1.4}\ \forall\, 2 \le i \le \ell$
2.i.1	$\mathsf{ct}^{i-1}_{x^*}$	$\boxed{\mathsf{sk}^{i-1,i}_f}$	$[\![d_u - \boxed{\Delta_{i-1,u}} \mapsto d_v]\!]_{z_\tau,w_{\sigma,\tau}}$	$[\![d_u \mapsto d_v]\!]_{z_{1-\tau},w_{\sigma,1-\tau}}$	$[\![d_u - \alpha \mapsto 0]\!]_{w_{\text{end}},0}$	"$d_u \mapsto d_u - \Delta_{i-1,u}$" + DDH (+ Lem 1-1)
2.i.2	$\boxed{\mathsf{ct}^{i-1,i}_{x^*}}$	$\mathsf{sk}^{i-1,i}_f$	$[\![d_u - \Delta_{i-1,u} \mapsto d_v]\!]_{z_\tau,w_{\sigma,\tau}}$	$[\![d_u \mapsto d_v]\!]_{z_{1-\tau},w_{\sigma,1-\tau}}$	$[\![d_u - \alpha \mapsto 0]\!]_{w_{\text{end}},0}$	Lem 2
2.i.3	$\mathsf{ct}^{i-1,i}_{x^*}$	$\boxed{\mathsf{sk}^i_f}$	$[\![d_u \mapsto d_v + \boxed{\Delta_{i,v}}]\!]_{z_\tau,w_{\sigma,\tau}}$	$[\![d_u \mapsto d_v]\!]_{z_{1-\tau},w_{\sigma,1-\tau}}$	$[\![d_u - \alpha \mapsto 0]\!]_{w_{\text{end}},0}$	Lem 3 + DDH + Lem 1-2
2.i.4	$\boxed{\mathsf{ct}^i_{x^*}}$	sk^i_f	$[\![d_u \mapsto d_v + \Delta_{i,v}]\!]_{z_\tau,w_{\sigma,\tau}}$	$[\![d_u \mapsto d_v]\!]_{z_{1-\tau},w_{\sigma,1-\tau}}$	$[\![d_u - \alpha \mapsto 0]\!]_{w_{\text{end}},0}$	Lem 2 + DDH
3	$\mathsf{ct}^\ell_{x^*}$	$\boxed{\mathsf{sk}^*_f}$	$[\![d_u \mapsto d_v]\!]_{z_0,w_{\sigma,0}}$	$[\![d_u \mapsto d_v]\!]_{z_1,w_{\sigma,1}}$	$[\![d_u - \boxed{\Delta_{\ell,u}} - \alpha \mapsto 0]\!]_{w_{\text{end}},0}$	"$d_u \mapsto d_u - \Delta_{\ell,u}$" + DDH

Fig. 2. Game sequence for composite-order ABE for DFA with $i = 1, \ldots, \ell$. Recall that $\tau = i \bmod 2$. We only describe the p_2-components for keys with the notational short-hand $[\![d_u \mapsto d_v]\!]_{z,w} := (h_2^{-d_u+zr_u}, h_2^{d_v+wr_u}, h_2^{r_u})$. All secret key elements in the fourth and fifth columns are quantified over $u \in [Q], \sigma \in \Sigma, v = \sigma(u,\sigma)$ while those in the sixth column are over $u \in F$; we omit $[\![0 \mapsto d_1]\!]_{0,w_{\text{start}}}$. In the "Remark" column, "SD" and "DDH" mean $\mathrm{SD}^{G_N}_{p_1 \mapsto p_1 p_2}$ assumption and $\mathrm{DDH}^{H_N}_{p_2}$ assumption, respectively, cf. Section 2.2; all lemmas will be described in Section 3.3; "Lem 1-1" and "Lem 1-2" indicate the two statements in Lemma 1, respectively. Note that we use Lemma 1 for "$\mathsf{G}_{2.i.0} \mapsto \mathsf{G}_{2.i.1}$" only when $i = 1$ which is indicating by brackets.

Basic facts. We first state several facts which we will use in the proof.

Lemma 1. *For any $x^* \in \Sigma^\ell$ and f such that $f(x^*) = 0$, we have:*

1. $\Delta_{0,1} = 0$;
2. *for all $i \in [\ell], u \in [Q]$, we have*

$$u \in F_{i-1,x^*} \iff \delta(u, x_i^*) \in F_{i,x^*}.$$

Proof. The first statement follows from the fact $1 \notin F_{0,x^*}$. The second one can be proved as follows: For direction $\Longrightarrow$, we know $\delta(u, x_i^*, x_{i+1}^*, \ldots, x_\ell^*) \in F$ for all $u \in F_{i-1,x^*}$. This means $\delta(\delta(u, x_i^*), x_{i+1}^*, \ldots, x_\ell^*) \in F$ and thus $\delta(u, x_i^*) \in F_{i,x^*}$ by the definition. The direction $\Longleftarrow$ can be proved analogously. $\square$

Ciphertext switching. We use (s, w)-switching lemma (Lemma 2) when switching ciphertext distributions in Section 3.6. This extends the statement described in (3) by considering many tuples of form $(h^{wr} \cdot h_2^{\Delta}, h^r)$ each with fresh r. To prove Lemma 2, we follow hybrid arguments described in (4) except that (i) we use $\mathrm{SD}^{G_N}_{p_3 \mapsto p_3 p_2}$ instead of $\mathrm{SD}^{G_N}_{p_3 \mapsto p_2}$ assumption and (ii) we apply $\mathrm{SD}^{G_N}_{p_1 \mapsto p_1 p_3}$ assumption once more. Looking ahead, this allows us to derive a prime-order scheme with better parameters.

Lemma 2 **((s, w)-switching lemma).** *For all $Q \in \mathbb{N}$, we have*

$$\begin{aligned} &\mathsf{aux},\ g_1^s, \qquad\quad \{\ h^{w\bar{r}_u} \cdot h_2^{\bar{\Delta}},\ h^{\bar{r}_u}\ \}_{u \in [Q]} \\ \approx_c\ &\mathsf{aux},\ g_1^s \cdot \boxed{g_2^s},\ \{\ h^{w\bar{r}_u} \cdot h_2^{\bar{\Delta}},\ h^{\bar{r}_u}\ \}_{u \in [Q]} \end{aligned}$$

where $\mathsf{aux} = (g_1, g_2, h, h^w, g_1^w, g_2^w)$ and $w, s, \bar{\Delta}, \bar{r}_u \leftarrow \mathbb{Z}_N$ for all $u \in [Q]$. Concretely, the advantage function $\mathsf{Adv}^{\mathrm{SWITCH}}_{\mathcal{B}}(\lambda)$ is bounded by

$$2 \cdot \mathsf{Adv}^{\mathrm{SD}^{G_N}_{p_1 \mapsto p_1 p_3}}_{\mathcal{B}_1}(\lambda) + 4 \cdot \mathsf{Adv}^{\mathrm{DDH}^{H_N}_{p_3}}_{\mathcal{B}_2}(\lambda) + \mathsf{Adv}^{\mathrm{SD}^{G_N}_{p_3 \mapsto p_3 p_2}}_{\mathcal{B}_3}(\lambda)$$

with $\mathsf{Time}(\mathcal{B}_1), \mathsf{Time}(\mathcal{B}_2), \mathsf{Time}(\mathcal{B}_3) \approx \mathsf{Time}(\mathcal{B})$.

Proof. We prove the lemma via the following hybrid arguments:

$$\begin{array}{rlll} \mathrm{LHS} = & \mathsf{aux},\ g_1^s, & \{\ h^{w\bar{r}_u} \cdot h_2^{\bar{\Delta}},\quad h^{\bar{r}_u}\ \}_u & \\ \approx_c & \mathsf{aux},\ g_1^s \cdot \boxed{g_3^s}, & \{\ h^{w\bar{r}_u} \cdot h_2^{\bar{\Delta}},\quad h^{\bar{r}_u}\ \}_u & \text{using } \mathrm{SD}^{G_N}_{p_1 \mapsto p_1 p_3} \\ \approx_c & \mathsf{aux},\ g_1^s \cdot g_3^s, & \{\ h^{w\bar{r}_u} \cdot h_2^{\bar{\Delta}} \cdot \boxed{h_3^{\bar{\Delta}}},\ h^{\bar{r}_u}\ \}_u & \text{using } \mathrm{DDH}^{H_N}_{p_3} \\ \approx_c & \mathsf{aux},\ g_1^s \cdot \boxed{g_2^s} \cdot g_3^s, & \{\ h^{w\bar{r}_u} \cdot h_2^{\bar{\Delta}} \cdot h_3^{\bar{\Delta}},\quad h^{\bar{r}_u}\ \}_u & \text{using } \mathrm{SD}^{G_N}_{p_3 \mapsto p_3 p_2} \\ \approx_c & \mathsf{aux},\ g_1^s \cdot g_2^s \cdot g_3^s, & \{\ h^{w\bar{r}_u} \cdot h_2^{\bar{\Delta}} \cdot \cancel{h_3^{\bar{\Delta}}},\quad h^{\bar{r}_u}\ \}_u & \text{using } \mathrm{DDH}^{H_N}_{p_3} \\ \approx_c & \mathsf{aux},\ g_1^s \cdot g_2^s \cdot \cancel{g_3^s}, & \{\ h^{w\bar{r}_u} \cdot h_2^{\bar{\Delta}},\quad h^{\bar{r}_u}\ \}_u = \mathrm{RHS} & \text{using } \mathrm{SD}^{G_N}_{p_1 \mapsto p_1 p_3} \end{array}$$

We proceed as follows:

– The first and the last $\approx_c$ rely on the $\mathrm{SD}^{G_N}_{p_1 \mapsto p_1 p_3}$ assumption stating that:

$$g_1^s \approx_c g_1^s \cdot g_3^s \quad \text{given } g_1, g_2, h, h_2$$

where $s \leftarrow \mathbb{Z}_N$. All reductions are straight-forward.

– The second and the fourth $\approx_c$ rely on the following statement implied by $\mathrm{DDH}_{p_3}^{H_N}$ assumption w.r.t. $w \bmod p_3$: for all $\bar{\Delta} \in \mathbb{Z}_N$, we have

$$\{\, h_3^{w\bar{r}_u}, h_3^{\bar{r}_u} \,\}_{u\in[Q]} \approx_c \{\, h_3^{w\bar{r}_u+\bar{\Delta}}, h_3^{\bar{r}_u} \,\}_{u\in[Q]}$$

given $g_1, g_2, g_3, h_1, h_2, h_3, h_3^w$ where $w, \bar{r}_u \leftarrow \mathbb{Z}_N$ for all $u \in [Q]$. All reductions are straight-forward.

– The third $\approx_c$ relies on the $\mathrm{SD}_{p_3 \mapsto p_3 p_2}^{G_N}$ assumption stating that:

$$g_3^s \approx_c g_2^s \cdot g_3^s \quad \text{ given } g_1, g_2, h, h_{23} \tag{9}$$

where $s \leftarrow \mathbb{Z}_N$ and h_{23} is a random generator for $H_{p_2p_3}$. The reduction works as follows: On input (S, g_1, g_2, h, h_{23}) where either $S = g_3^s$ or $S = g_2^s \cdot g_3^s$, we sample $w, \bar{\Delta}, \bar{r}_u, \tilde{s} \leftarrow \mathbb{Z}_N$ for all $u \in [Q]$. First, we can trivially compute aux and challenge term $g_1^{\tilde{s}} \cdot S$. Second, we simulate $h_2^{\bar{\Delta}} \cdot h_3^{\bar{\Delta}}$ with $h_{23}^{\bar{\Delta}}$ by the fact: $h_2^{\bar{\Delta}} \cdot h_3^{\bar{\Delta}} \approx_s h_{23}^{\bar{\Delta}}$ for all h_2, h_3, h_{23} when $\bar{\Delta} \leftarrow \mathbb{Z}_N$; this is sufficient for simulating all remaining terms.

Combining all five steps proves the lemma. □

Remark 1. Observe that the distributions in the lemma are easily distinguishable if the view also contains g_1^{sw} or $(g_1g_2)^{sw}$ (on the LHS and RHS respectively).

Key switching. We use (z, w)-transition lemma (Lemma 3) for switching key distributions (see Section 3.7), which captures the core argument in the statement (5) in the Introduction. Due to the lack of space, we defer the detailed proof to the full paper.

Lemma 3 ((z, w)-transition lemma). *For all $Q \in \mathbb{N}$, $s_{i-1}, s_i \neq 0$ and $\bar{\Delta} \in \mathbb{Z}_N$, we have*

$$\begin{aligned} &\mathsf{aux},\ s_{i-1}z + s_i w,\ \{\, h_2^{\boxed{s_i\bar{\Delta}}+z\bar{r}_u},\ \ h_2^{w\bar{r}_u},\ h_2^{\bar{r}_u} \,\}_{u\in[Q]} \\ \approx_c\ &\mathsf{aux},\ s_{i-1}z + s_i w,\ \{\, h_2^{z\bar{r}_u},\ h_2^{\boxed{s_{i-1}\bar{\Delta}}+w\bar{r}_u},\ h_2^{\bar{r}_u} \,\}_{u\in[Q]} \end{aligned}$$

where $\mathsf{aux} = (g_1, g_2, h_1, h_2, h_3, h_2^z, h_2^w)$ *and* $z, w, \bar{r}_u \leftarrow \mathbb{Z}_N$ *for all* $u \in [Q]$. *Concretely, the advantage function* $\mathsf{Adv}_{\mathcal{B}}^{\mathrm{TRANS}}(\lambda)$ *is bounded by* $2 \cdot \mathsf{Adv}_{\mathcal{B}_1}^{\mathrm{DDH}_{p_2}^{H_N}}(\lambda)$ *with* $\mathsf{Time}(\mathcal{B}_1) \approx \mathsf{Time}(\mathcal{B})$.

3.4 Initialization: $\mathsf{G_0} \mapsto \mathsf{G_1}, \mathsf{G_1} \mapsto \mathsf{G_{2.1.0}}$

The first two transitions are straight-forward; we describe the following two lemmas with the first proof omitted.

Lemma 4 ($\mathsf{G}_0 \approx_c \mathsf{G}_1$). *There exists $\mathcal{B}$ with $\mathsf{Time}(\mathcal{B}) \approx \mathsf{Time}(\mathcal{A})$ such that*

$$|\mathsf{Adv}_{\mathcal{A}}^{0}(\lambda) - \mathsf{Adv}_{\mathcal{A}}^{1}(\lambda)| \le \mathsf{Adv}_{\mathcal{B}}^{\mathrm{SD}_{p_1\mapsto p_1p_2}^{G_N}}(\lambda).$$

Lemma 5 ($\mathsf{G}_1 \approx_c \mathsf{G}_{2.1.0}$). *There exists $\mathcal{B}$ with $\mathsf{Time}(\mathcal{B}) \approx \mathsf{Time}(\mathcal{A})$ such that*

$$|\mathsf{Adv}_{\mathcal{A}}^{1}(\lambda) - \mathsf{Adv}_{\mathcal{A}}^{2.1.0}(\lambda)| \le 2|\Sigma| \cdot \mathsf{Adv}_{\mathcal{B}}^{\mathrm{DDH}_{p_2}^{H_N}}(\lambda).$$

Proof. This roughly means that

$$(\,\mathsf{mpk},\, \mathsf{ct}^0_{x^*},\, \mathsf{sk}_f\,) \approx_c (\,\mathsf{mpk},\, \mathsf{ct}^0_{x^*},\, \boxed{\mathsf{sk}^0_f}\,).$$

By the Chinese Reminder Theorem, it suffices to focus on the p_2-components; concretely, we prove that

$$\mathsf{sk}_f[2] \;=\; \begin{pmatrix} h_2^{d_1+w_{\text{start}}r_1}, h_2^{r_1}, \\ \{h_2^{-d_u+z_0 r_u}, h_2^{d_v+w_{\sigma,0}r_u}, h_2^{r_u}\}_{u\in[Q],\sigma\in\Sigma,v=\delta(u,\sigma)}, \\ \{h_2^{-d_u+z_1 r_u}, h_2^{d_v+w_{\sigma,1}r_u}, h_2^{r_u}\}_{u\in[Q],\sigma\in\Sigma,v=\delta(u,\sigma)}, \\ \{h_2^{\alpha-d_u+w_{\text{end}}r_u}, h_2^{r_u}\}_{u\in F} \end{pmatrix}$$

$$\approx_c \begin{pmatrix} h_2^{d_1+w_{\text{start}}r_1}, h_2^{r_1}, \\ \{h_2^{-d_u+z_0 r_u}, h_2^{d_v+\boxed{\Delta_{0,v}}+w_{\sigma,0}r_u}, h_2^{r_u}\}_{u\in[Q],\sigma\in\Sigma,v=\delta(u,\sigma)}, \\ \{h_2^{-d_u+z_1 r_u}, h_2^{d_v+w_{\sigma,1}r_u}, h_2^{r_u}\}_{u\in[Q],\sigma\in\Sigma,v=\delta(u,\sigma)}, \\ \{h_2^{\alpha-d_u+w_{\text{end}}r_u}, h_2^{r_u}\}_{u\in F} \end{pmatrix} = \mathsf{sk}^0_f[2]$$

given g_1, h_1, h_3 and

$$\mathsf{ct}^0_{x^*}[2] := \big(\, g_2^{s_0 w_{\text{start}}},\, g_2^{s_0},\, g_2^{s_0 z_1}\,\big).$$

Here terms g_1, h_1, h_3 allow us to simulate the p_1- and p_3-components of $\mathsf{ct}^0_{x^*}$ and sk_f (or sk^0_f) as well as mpk, which is sufficient for proving the lemma. Furthermore, this statement immediately follows from the statement below which are implied by $\mathrm{DDH}^{H_N}_{p_2}$ assumption w.r.t. $w_{\sigma,0} \bmod p_2$ with $\sigma \in \Sigma$: for all $\sigma \in \Sigma$ and $\Delta \in \mathbb{Z}_N$, we have

$$\{\, h_2^{r_u},\, h_2^{w_{\sigma,0}r_u}\,\}_{u\in[Q]} \approx_c \{\, h_2^{r_u},\, h_2^{\Delta+w_{\sigma,0}r_u}\,\}_{u\in[Q]}$$

given g_1, g_2, h_1, h_2, h_3 and $h_2^{w_{\sigma,0}}$ where $w_{\sigma,0}, r_u \leftarrow \mathbb{Z}_N$ for $u \in [Q]$. Here we crucially rely on the fact the ciphertext $\mathsf{ct}^0_{x^*}[2]$ does not leak $w_{\sigma,0} \bmod p_2$ with $\sigma \in \Sigma$. $\square$

3.5 Switching secret keys I: $\mathsf{G}_{2.i.0} \mapsto \mathsf{G}_{2.i.1}$

In this section, we prove the following lemma.

Lemma 6 **($\mathsf{G}_{2.i.0} \approx_c \mathsf{G}_{2.i.1}$).** *For all $i = 1, \ldots, \ell$, there exists $\mathcal{B}$ with $\mathsf{Time}(\mathcal{B}) \approx \mathsf{Time}(\mathcal{A})$ such that*

$$|\mathsf{Adv}^{2.i.0}_{\mathcal{A}}(\lambda) - \mathsf{Adv}^{2.i.1}_{\mathcal{A}}(\lambda)| \le 2(|\Sigma|+3)\cdot \mathsf{Adv}^{\mathrm{DDH}^{H_N}_{p_2}}_{\mathcal{B}}(\lambda).$$

Proof organization. We need two auxiliary games $\mathsf{G}_{2.i.1.a}$ and $\mathsf{G}_{2.i.1.b}$ and prove that:

$$\mathsf{G}_{2.i.0} \overset{\text{Lemma 7}}{\approx_s} \mathsf{G}_{2.i.1.a} \overset{\text{Lemma 8}}{\approx_c} \mathsf{G}_{2.i.1.b} \overset{\text{Lemma 9}}{\approx_c} \mathsf{G}_{2.i.1}$$

where the p_2-components of the secret key in these games are recalled/defined as below

$$\mathsf{G}_{2.i.0}: \begin{pmatrix} h_2^{d_1+w_{\text{start}}r_1}, h_2^{r_1}, \\ \{h_2^{-d_u+z_\tau r_u}, h_2^{d_v+w_{\sigma,\tau}r_u}, h_2^{r_u}\}_{u\in[Q],\sigma\in\Sigma,v=\delta(u,\sigma)}, \\ \{h_2^{-d_u+z_{1-\tau} r_u}, h_2^{d_v+\boxed{\Delta_{i-1,v}}+w_{\sigma,1-\tau}r_u}, h_2^{r_u}\}_{u\in[Q],\sigma\in\Sigma,v=\delta(u,\sigma)}, \\ \{h_2^{\alpha-d_u+w_{\text{end}}r_u}, h_2^{r_u}\}_{u\in F} \end{pmatrix} = \mathsf{sk}^{i-1}_f[2]$$

$$
\mathsf{G}_{2.i.1.a}: \begin{pmatrix} h_2^{d_1 - \boxed{\Delta_{i-1,1}} + w_{\text{start}} r_1}, h_2^{r_1}, \\ \{ h_2^{-d_u + \boxed{\Delta_{i-1,u}} + z_\tau r_u}, h_2^{d_v - \boxed{\Delta_{i-1,v}} + w_{\sigma,\tau} r_u}, h_2^{r_u} \}_{u \in [Q], \sigma \in \Sigma, v = \delta(u,\sigma)}, \\ \{ h_2^{-d_u + \boxed{\Delta_{i-1,u}} + z_{1-\tau} r_u}, h_2^{d_v + w_{\sigma,1-\tau} r_u}, h_2^{r_u} \}_{u \in [Q], \sigma \in \Sigma, v = \delta(u,\sigma)}, \\ \{ h_2^{\alpha - d_u + \boxed{\Delta_{i-1,u}} + w_{\text{end}} r_u}, h_2^{r_u} \}_{u \in F} \end{pmatrix}
$$

$$
\mathsf{G}_{2.i.1.b}: \begin{pmatrix} h_2^{d_1 - \cancel{\Delta_{i-1,1}} + w_{\text{start}} r_1}, h_2^{r_1}, \\ \{ h_2^{-d_u + \Delta_{i-1,u} + z_\tau r_u}, h_2^{d_v - \Delta_{i-1,v} + w_{\sigma,\tau} r_u}, h_2^{r_u} \}_{u \in [Q], \sigma \in \Sigma, v = \delta(u,\sigma)}, \\ \{ h_2^{-d_u + \Delta_{i-1,u} + z_{1-\tau} r_u}, h_2^{d_v + w_{\sigma,1-\tau} r_u}, h_2^{r_u} \}_{u \in [Q], \sigma \in \Sigma, v = \delta(u,\sigma)}, \\ \{ h_2^{\alpha - d_u + \Delta_{i-1,u} + w_{\text{end}} r_u}, h_2^{r_u} \}_{u \in F} \end{pmatrix}
$$

$$
\mathsf{G}_{2.i.1}: \begin{pmatrix} h_2^{d_1 + w_{\text{start}} r_1}, h_2^{r_1}, \\ \{ h_2^{-d_u + \Delta_{i-1,u} + z_\tau r_u}, h_2^{d_v - \cancel{\Delta_{i-1,v}} + w_{\sigma,\tau} r_u}, h_2^{r_u} \}_{u \in [Q], \sigma \in \Sigma, v = \delta(u,\sigma)}, \\ \{ h_2^{-d_u + \cancel{\Delta_{i-1,u}} + z_{1-\tau} r_u}, h_2^{d_v + w_{\sigma,1-\tau} r_u}, h_2^{r_u} \}_{u \in [Q], \sigma \in \Sigma, v = \delta(u,\sigma)}, \\ \{ h_2^{\alpha - d_u + \cancel{\Delta_{i-1,u}} + w_{\text{end}} r_u}, h_2^{r_u} \}_{u \in F} \end{pmatrix} = \mathsf{sk}_f^{i-1,i}[2]
$$

and the p_2-components of ciphertext are recalled as follows

$$
\mathsf{ct}_{x^*}^{i-1}[2] = \begin{cases} g_2^{s_0 w_{\text{start}}}, g_2^{s_0}, g_2^{s_0 z_1} & \text{if } i = 1 \\ g_2^{s_{i-1} w_{x^*_{i-1}, 1-\tau}}, g_2^{s_{i-1}}, g_2^{s_{i-1} z_\tau} & \text{if } 2 \leq i \leq \ell \end{cases}
$$

The p_1- and p_3-components of secret key and ciphertext as well as mpk remain unchanged among all the four games.

Lemmas and Proofs. We describe and prove the following lemmas. Combining them together proves Lemma 6.

Lemma 7 **($\mathsf{G}_{2.i.0} \approx_s \mathsf{G}_{2.i.1.a}$).** *For all $i = 1, \ldots, \ell$, we have*

$$
\mathsf{Adv}_{\mathcal{A}}^{2.i.0}(\lambda) = \mathsf{Adv}_{\mathcal{A}}^{2.i.1.a}(\lambda).
$$

Proof. This immediately follows from the change of variables: $d_u \mapsto d_u - \Delta_{i-1,u} \bmod p_2$ for all $u \in [Q]$. □

Lemma 8 **($\mathsf{G}_{2.i.1.a} \approx_c \mathsf{G}_{2.i.1.b}$).** *For all $i = 1, \ldots, \ell$, there exists $\mathcal{B}$ with $\mathsf{Time}(\mathcal{B}) \approx \mathsf{Time}(\mathcal{A})$ such that*

$$
|\mathsf{Adv}_{\mathcal{A}}^{2.i.1.a}(\lambda) - \mathsf{Adv}_{\mathcal{A}}^{2.i.1.b}(\lambda)| \leq 2 \cdot \mathsf{Adv}_{\mathcal{B}}^{\mathrm{DDH}_{p_2}^{H_N}}(\lambda).
$$

Proof. We prove the lemma via a case analysis for i:

- Case $i = 1$: The two games are exactly identical due to the fact that $\Delta_{0,1} = 0$, see Lemma 1.
- Case $i > 1$: The lemma follows from the statement below implied by $\mathrm{DDH}_{p_2}^{H_N}$ assumption w.r.t. $w_{\text{start}} \bmod p_2$: for all $\Delta \in \mathbb{Z}_N$, we have

$$
\{ h_2^{r_1}, h_2^{w_{\text{start}} r_1} \} \approx_c \{ h_2^{r_1}, h_2^{-\Delta + w_{\text{start}} r_1} \}
$$

given g_1, g_2, h_1, h_2, h_3 and $h_2^{w_{\text{start}}}$ where $w_{\text{start}}, r_1 \leftarrow \mathbb{Z}_N$. Here we crucially rely on the fact the ciphertext $\mathsf{ct}_{x^*}^{i-1}[2]$ with $i > 1$ does not leak $w_{\text{start}} \bmod p_2$. □

Lemma 9 ($\mathsf{G}_{2.i.1.b} \approx_c \mathsf{G}_{2.i.1}$)**.** *For all* $i = 1, \ldots, \ell$, *there exists* $\mathcal{B}$ *with* $\mathsf{Time}(\mathcal{B}) \approx \mathsf{Time}(\mathcal{A})$ *such that*

$$|\mathsf{Adv}_{\mathcal{A}}^{2.i.1.b}(\lambda) - \mathsf{Adv}_{\mathcal{A}}^{2.i.1}(\lambda)| \leq 2(|\Sigma| + 2) \cdot \mathsf{Adv}_{\mathcal{B}}^{\mathrm{DDH}_{p_2}^{H_N}}(\lambda).$$

Proof. This follows from statements below implied by $\mathrm{DDH}_{p_2}^{H_N}$ assumption w.r.t $w_{\sigma,\tau}$, $z_{1-\tau}$, $w_{\text{end}} \bmod p_2$ with $\sigma \in \Sigma$:

- For all $\Delta \in \mathbb{Z}_N$, we have

$$\{\, h_2^{r_u},\, h_2^{z_{1-\tau} r_u},\, h_2^{w_{\text{end}} r_u} \,\}_{u \in [Q]} \approx_c \{\, h_2^{r_u},\, h_2^{\Delta + z_{1-\tau} r_u},\, h_2^{\Delta + w_{\text{end}} r_u} \,\}_{u \in [Q]}$$

  given g_1, g_2, h_1, h_2, h_3 and $h_2^{z_{1-\tau}}, h_2^{w_{\text{end}}}$ where $z_{1-\tau}, w_{\text{end}}, r_u \leftarrow \mathbb{Z}_N$ for all $u \in [Q]$.
- For all $\sigma \in \Sigma$ and $\Delta \in \mathbb{Z}_N$, we have

$$\{\, h_2^{r_u},\, h_2^{w_{\sigma,\tau} r_u} \,\}_{u \in [Q]} \approx_c \{\, h_2^{r_u},\, h_2^{-\Delta + w_{\sigma,\tau} r_u} \,\}_{u \in [Q]}$$

  given g_1, g_2, h_1, h_2, h_3 and $h_2^{w_{\sigma,\tau}}$ where $w_{\sigma,\tau}, r_u \leftarrow \mathbb{Z}_N$ for $u \in [Q]$.

Here we use the fact that $\mathsf{ct}_{x^*}^{i-1}[2]$ with $1 \leq i \leq \ell$ does not leak $w_{\sigma,\tau}, z_{1-\tau}, w_{\text{end}} \bmod p_2$ with $\sigma \in \Sigma$. □

3.6 Switching ciphertexts: $\mathsf{G}_{2.i.1} \mapsto \mathsf{G}_{2.i.2}$, $\mathsf{G}_{2.i.3} \mapsto \mathsf{G}_{2.i.4}$

In this section, we prove the following two lemmas for $\mathsf{G}_{2.i.1} \mapsto \mathsf{G}_{2.i.2}$ and $\mathsf{G}_{2.i.3} \mapsto \mathsf{G}_{2.i.4}$, respectively. The proofs are similar, we give the details for the first proof and only sketch the differences in the second proof.

Lemma 10 ($\mathsf{G}_{2.i.1} \approx_c \mathsf{G}_{2.i.2}$)**.** *For* $i = 1, \ldots, \ell$, *there exists* $\mathcal{B}$ *with* $\mathsf{Time}(\mathcal{B}) \approx \mathsf{Time}(\mathcal{A})$ *such that*

$$|\mathsf{Adv}_{\mathcal{A}}^{2.i.1}(\lambda) - \mathsf{Adv}_{\mathcal{A}}^{2.i.2}(\lambda)| \leq \mathsf{Adv}_{\mathcal{B}}^{\mathrm{SWITCH}}(\lambda).$$

Proof. This roughly means that

$$(\, \mathsf{mpk},\, \boxed{\mathsf{ct}_{x^*}^{i-1}},\, \mathsf{sk}_f^{i-1,i} \,) \approx_c (\, \mathsf{mpk},\, \boxed{\mathsf{ct}_{x^*}^{i-1,i}},\, \mathsf{sk}_f^{i-1,i} \,).$$

Recall that $\tau = i \bmod 2$. We prove the lemma using (s_i, z_τ)-switching lemma (see Lemma 2). On input

$$\mathsf{aux},\ S_i,\ \{h^{z_\tau \bar{r}_u} \cdot h_2^{\bar{\Delta}},\ h^{\bar{r}_u}\}_{u \in [Q]}$$

with $\mathsf{aux} = (g_1, g_2, h, h^{z_\tau}, g_1^{z_\tau}, g_2^{z_\tau})$ and

$$S_i = g_1^{s_i} \ \text{ or } \ S_i = g_1^{s_i} \cdot g_2^{s_i}$$

where $z_\tau, s_i, \bar{\Delta}, \bar{r}_u \leftarrow \mathbb{Z}_N$ for all $u \in [Q]$, the reduction proceeds as follows:

(Simulating mpk**)** We sample $\alpha, w_{\text{start}}, w_{\text{end}}, z_{1-\tau}, w_{\sigma,\tau}, w_{\sigma,1-\tau} \leftarrow \mathbb{Z}_N$ for all $\sigma \in \Sigma$; then we can trivially simulate mpk with terms $g_1, h, g_1^{z_\tau}$ given out in aux.

(Simulating key for f) We want to simulate $\mathsf{sk}_f^{i-1,i}$ in the form

$$\mathsf{sk}_f^{i-1,i} = \begin{pmatrix} h^{d_1+w_{\text{start}}r_1}, h^{r_1}, \\ \{\boxed{h^{-d_u+z_\tau r_u} \cdot h_2^{\Delta_{i-1,u}}}, h^{d_v+w_{\sigma,\tau}r_u}, \boxed{h^{r_u}}\}_{u\in[Q],\sigma\in\Sigma,v=\delta(u,\sigma)}, \\ \{h^{-d_u+z_{1-\tau}r_u}, h^{d_v+w_{\sigma,1-\tau}r_u}, h^{r_u}\}_{u\in[Q],\sigma\in\Sigma,v=\delta(u,\sigma)}, \\ \{h^{\alpha-d_u+w_{\text{end}}r_u}, h^{r_u}\}_{u\in F} \end{pmatrix}$$

On input f, we build $F_{i-1,x^*} \subseteq [Q]$ from f, then sample $d_u \leftarrow \mathbb{Z}_N$ for all $u \in [Q]$ and $r_u \leftarrow \mathbb{Z}_N$ for all $u \notin F_{i-1,x^*}$. We implicitly set

$$\Delta = \bar{\Delta} \quad \text{and} \quad r_u = \bar{r}_u \ \text{ for all } \ u \in F_{i-1,x^*}$$

and simulate $\mathsf{sk}_f^{i-1,i}$ as follows:

- By the definition of $\{\Delta_{i-1,u}\}_u$ and our implicit setting, we can rewrite all terms in the dashed boxes as:

$$\begin{cases} h^{r_u}, h^{-d_u+z_\tau r_u} & \text{if } u \notin F_{i-1,x^*} \\ h^{\bar{r}_u}, h^{-d_u+z_\tau \bar{r}_u} \cdot h_2^{\bar{\Delta}} & \text{if } u \in F_{i-1,x^*} \end{cases}$$

  Terms for $u \notin F_{i-1,x^*}$ can be computed honestly from $\{r_u, d_u\}_{u\notin F_{i-1,x^*}}$ we sampled and h, h^{z_τ} given in aux; terms for $u \in F_{i-1,x^*}$ can be computed from $\{d_u\}_{u\in F_{i-1,x^*}}$ we sampled and $\{h^{z_\tau \bar{r}_u} \cdot h_2^{\bar{\Delta}},\ h^{\bar{r}_u}\}_{u\in F_{i-1,x^*}}$ given out in the input.
- All remaining terms can be trivially simulated using $\{r_u\}_{u\notin F_{i-1,x^*}}$ and $\{h^{r_u} = h^{\bar{r}_u}\}_{u\in F_{i-1,x^*}}$ as well as α, $\{d_u\}_{u\in[Q]}$, w_{start}, $z_{1-\tau}$, $\{w_{\sigma,\tau}, w_{\sigma,1-\tau}\}_{\sigma\in\Sigma}$, w_{end} we sampled.

(Simulating ciphertext for x^*) We want to generate a ciphertext for x^* which is distributed as either $\mathsf{ct}_{x^*}^{i-1}$ or $\mathsf{ct}_{x^*}^{i-1,\boxed{i}}$:

$$\begin{cases} g_2^{s_0 w_{\text{start}}}, g_2^{s_0}, g_2^{s_0 z_1 + \boxed{s_1 w_{x_1^*,1}}}, \boxed{g_2^{s_1}}, \boxed{g_2^{s_1 z_0}} & \text{if } i = 1 \\ g_2^{s_{i-1} w_{x_{i-1}^*,1-\tau}}, g_2^{s_{i-1}}, g_2^{s_{i-1} z_\tau + \boxed{s_i w_{x_i^*,\tau}}}, \boxed{g_2^{s_i}}, \boxed{g_2^{s_i z_{1-\tau}}} & \text{if } 1 < i < \ell \\ g_2^{s_{\ell-1} w_{x_{\ell-1}^*,1-\bar{\ell}}}, g_2^{s_{\ell-1}}, g_2^{s_{\ell-1} z_{\bar{\ell}} + \boxed{s_\ell w_{x_\ell^*,\bar{\ell}}}}, \boxed{g_2^{s_\ell}}, \boxed{g_2^{s_\ell w_{\text{end}}}}, \boxed{e(g_2^{s_\ell}, h^\alpha)} & \text{if } i = \ell \end{cases}$$

On input $(m_0, m_1) \in \mathcal{M} \times \mathcal{M}$, we sample $\beta \leftarrow \{0,1\}$ and $s_j \leftarrow \mathbb{Z}_N$ for all $j \neq i$, and output the challenge ciphertext

$$\begin{cases} (\ \ldots, (g_1 g_2)^{s_0 z_1} \cdot S_1^{w_{x_1^*,1}}, S_1, S_1^{z_0} \cdot g_1^{s_2 w_{x_2^*,0}}, \ldots\ ) & \text{if } i = 1 \\ (\ \ldots, (g_1 g_2)^{s_{i-1} z_\tau} \cdot S_i^{w_{x_i^*,\tau}}, S_i, S_i^{z_{1-\tau}} \cdot g_1^{s_{i+1} w_{x_{i+1}^*,1-\tau}}, \ldots\ ) & \text{if } 1 < i < \ell \\ (\ \ldots, (g_1 g_2)^{s_{\ell-1} z_{\bar{\ell}}} \cdot S_\ell^{w_{x_\ell^*,\bar{\ell}}}, S_\ell, S_\ell^{w_{\text{end}}}, \mathsf{H}(e(S_\ell, h^\alpha)) \cdot m_\beta\ ) & \text{if } i = \ell \end{cases}$$

Here we use the fact that the ciphertext contains no term with $s_i z_\tau$ in the exponent (cf. Remark 1). All omitted terms can be honestly computed from aux and exponents $\{s_j\}_{j\neq i}$ sampled by ourselves. Clearly, when $S_i = g_1^{s_i}$, the output is identical to $\mathsf{ct}_{x^*}^{i-1}$; when $S_i = g_1^{s_i} \cdot g_2^{s_i}$, the output is identical to $\mathsf{ct}_{x^*}^{i-1,i}$. This completes the proof. $\square$

Lemma 11 ($\mathsf{G}_{2.i.3} \approx_c \mathsf{G}_{2.i.4}$)**.** *For $i = 1, \ldots, \ell$, there exists $\mathcal{B}_1, \mathcal{B}_2$ with $\mathsf{Time}(\mathcal{B}_1)$, $\mathsf{Time}(\mathcal{B}_2) \approx \mathsf{Time}(\mathcal{A})$ such that*

$$|\mathsf{Adv}_{\mathcal{A}}^{2.i.3}(\lambda) - \mathsf{Adv}_{\mathcal{A}}^{2.i.4}(\lambda)| \le \mathsf{Adv}_{\mathcal{B}_1}^{\mathrm{SWITCH}}(\lambda) + 4(|\Sigma| - 1) \cdot \mathsf{Adv}_{\mathcal{B}_2}^{\mathrm{DDH}_{p_2}^{H_N}}(\lambda).$$

Proof. This roughly means that

$$(\,\mathsf{mpk},\ \boxed{\mathsf{ct}_{x^*}^{i-1,i}},\ \mathsf{sk}_f^i\,) \approx_c (\,\mathsf{mpk},\ \boxed{\mathsf{ct}_{x^*}^{i}},\ \mathsf{sk}_f^i\,)$$

We prove the lemma using $(s_{i-1}, w_{x_i^*,\tau})$-transition lemma (see Lemma 2). Recall that $\tau = i \bmod 2$. The reduction is analogous to that for Lemma 10: On input

$$\mathsf{aux},\ S_{i-1},\ \{h^{w_{x_i^*,\tau}\bar{r}_u} \cdot h_2^{\bar{\Delta}},\ h^{\bar{r}_u}\}_{u\in[Q]}$$

with $\mathsf{aux} = (g_1, g_2, h, h^{w_{x_i^*,\tau}}, g_1^{w_{x_i^*,\tau}}, g_2^{w_{x_i^*,\tau}})$ and

$$S_{i-1} = g_1^{s_{i-1}} \ \text{ or } \ S_{i-1} = g_1^{s_{i-1}} \cdot g_2^{s_{i-1}}$$

where $w_{x_i^*,\tau}, s_{i-1}, \bar{\Delta}, \bar{r}_u \leftarrow \mathbb{Z}_N$ for all $u \in [Q]$, we sample α, w_{start}, w_{end}, z_0, z_1, $w_{\sigma,1-\tau} \leftarrow \mathbb{Z}_N$ for all $\sigma \in \Sigma$, $w_{\sigma,\tau} \leftarrow \mathbb{Z}_N$ for all $\sigma \neq x_i^*$ and $s_j \leftarrow \mathbb{Z}_N$ for all $j \neq i-1$; then we can simulate mpk and the challenge ciphertext analogously. The main difference locates at the simulation of secret key.

(Simulating key for f) We want to simulate sk_f^i in the form:

$$\mathsf{sk}_f^i = \left(\begin{array}{c} h^{d_1 + w_{\text{start}} r_1},\, h^{r_1}, \\ \{h^{-d_u + z_\tau r_u},\, \boxed{h^{d_{\delta(u,x_i^*)} + w_{x_i^*,\tau} r_u} \cdot h_2^{\Delta_{i,\delta(u,x_i^*)}},\, h^{r_u}}\}_{u\in[Q]}, \\ \boxed{\{h^{d_v + w_{\sigma,\tau} r_u} \cdot h_2^{\Delta_{i,v}}\}_{u\in[Q],\sigma\neq x_i^*, v=\delta(u,\sigma)}} \\ \{h^{-d_u + z_{1-\tau} r_u},\, h^{d_v + w_{\sigma,1-\tau} r_u},\, h^{r_u}\}_{u\in[Q],\sigma\in\Sigma,v=\delta(u,\sigma)}, \\ \{h^{\alpha - d_u + w_{\text{end}} r_u},\, h^{r_u}\}_{u\in F} \end{array}\right).$$

On input f, we sample $d_u \leftarrow \mathbb{Z}_N$ for all $u \in [Q]$ and implicitly set $\Delta = \bar{\Delta}$ as before but we set $\{r_u\}_{u\in[Q]}$ as follows:

- We build $F_{i,x^*} \subseteq [Q]$, sample $r_u \leftarrow \mathbb{Z}_N$ for all u such that $\delta(u, x_i^*) \notin F_{i,x^*}$ and implicitly set $r_u = \bar{r}_u$ for all u such that $\delta(u, x_i^*) \in F_{i,x^*}$.

Then we simulate sk_f^i as follows:

- By the definition of $\{\Delta_{i,u}\}_u$ and our implicit setting, we can rewrite all terms in the dashed box as below

$$\begin{cases} h^{r_u},\, h^{d_{\delta(u,x_i^*)} + w_{x_i^*,\tau} r_u} & \text{if } \delta(u, x_i^*) \notin F_{i,x^*} \\ h^{\bar{r}_u},\, h^{d_{\delta(u,x_i^*)} + w_{x_i^*,\tau} \bar{r}_u} \cdot h_2^{\bar{\Delta}} & \text{if } \delta(u, x_i^*) \in F_{i,x^*} \end{cases}$$

  and simulate them from either $\{r_u\}_{\delta(u,x_i^*)\notin F_{i,x^*}}$ or $\{h^{w_{x_i^*,\tau}\bar{r}_u} \cdot h_2^{\bar{\Delta}},\ h^{\bar{r}_u}\}_{\delta(u,x_i^*)\in F_{i,x^*}}$ with the help of $\{d_u\}_{u\in[Q]}$ and aux. This is similar to the simulation of terms in the dashed boxes in the proof for Lemma 10.

– The terms in the gray box are computationally simulated in the following form

$$\{h^{d_v+w_{\sigma,\tau}r_u}\cdot \cancel{h_2^{\Delta_{i,v}}}\}_{u\in[Q],\sigma\neq x_i^*,v=\delta(u,\sigma)}$$

using $\{d_u\}_{u\in[Q]}, \{w_{\sigma,\tau}\}_{\sigma\neq x_i^*}$ we sampled and $\{h^{r_u}\}_{u\in[Q]}$ we have simulated. This follows from $\mathrm{DDH}_{p_2}^{H_N}$ assumption w.r.t $w_{\sigma,\tau} \bmod p_2$ with $\sigma\neq x_i^*$ which implies that: for all $\sigma\neq x_i^*$ and $\Delta\in\mathbb{Z}_N$, we have

$$\{h_2^{r_u}, h_2^{w_{\sigma,\tau}r_u}\}_{u\in[Q]} \approx_c \{h_2^{r_u}, h_2^{\Delta+w_{\sigma,\tau}r_u}\}_{u\in[Q]}$$

given g_1,g_2,h_1,h_2,h_3 and $h_2^{w_{\sigma,\tau}}$ where $w_{\sigma,\tau}, r_u\leftarrow\mathbb{Z}_N$ for all $u\in[Q]$. Here we use the fact that both $\mathsf{ct}_{x^*}^{i-1,i}$ and $\mathsf{ct}_{x^*}^{i}$ does not leak $w_{\sigma,\tau} \bmod p_2$ with $\sigma\neq x_i^*$.

– All remaining terms can be easily handled as in the proof of Lemma 10.

This completes the proof. $\square$

3.7 Switching key II: $\mathsf{G}_{2.i.2}\mapsto\mathsf{G}_{2.i.3}$

In this section we prove the following lemma.

Lemma 12 **($\mathsf{G}_{2.i.2}\approx_c\mathsf{G}_{2.i.3}$).** *For all $i=1,\dots,\ell$, there exists $\mathcal{B}_1,\mathcal{B}_2$ with $\mathsf{Time}(\mathcal{B}_1)$, $\mathsf{Time}(\mathcal{B}_2)\approx\mathsf{Time}(\mathcal{A})$ such that*

$$|\mathsf{Adv}_{\mathcal{A}}^{2.i.2}(\lambda)-\mathsf{Adv}_{\mathcal{A}}^{2.i.3}(\lambda)|\leq\mathsf{Adv}_{\mathcal{B}_1}^{\mathrm{TRANS}}(\lambda)+2(|\Sigma|-1)\cdot\mathsf{Adv}_{\mathcal{B}_2}^{\mathrm{DDH}_{p_2}^{H_N}}(\lambda).$$

Proof. Recall $\tau=i \bmod 2$. By the Chinese Reminder Theorem, it suffices to focus on the p_2-components; concretely we prove

$$\begin{aligned}
\mathsf{sk}_f^{i-1,i}[2] &= \begin{pmatrix} h_2^{d_1+w_{\mathrm{start}}r_1}, h_2^{r_1}, \\ \{h_2^{-d_u+\boxed{\Delta_{i-1,u}}+z_\tau r_u}, h_2^{d_{\delta(u,x_i^*)}+w_{x_i^*,\tau}r_u}, h_2^{r_u}\}_{u\in[Q]}, \\ \{h_2^{d_v+w_{\sigma,\tau}r_u}\}_{u\in[Q],\sigma\neq x_i^*,v=\delta(u,\sigma)}, \\ \{h_2^{-d_u+z_{1-\tau}r_u}, h_2^{d_v+w_{\sigma,1-\tau}r_u}, h_2^{r_u}\}_{u\in[Q],\sigma\in\Sigma,v=\delta(u,\sigma)}, \\ \{h_2^{\alpha-d_u+w_{\mathrm{end}}r_u}, h_2^{r}\}_{u\in F} \end{pmatrix} \\
&\approx_c \begin{pmatrix} h_2^{d_1+w_{\mathrm{start}}r_1}, h_2^{r_1}, \\ \{h_2^{-d_u+z_\tau r_u}, h_2^{d_{\delta(u,x_i^*)}+\boxed{\Delta_{i,\delta(u,x_i^*)}}+w_{x_i^*,\tau}r_u}, h_2^{r_u}\}_{u\in[Q]}, \\ \{h_2^{d_v+w_{\sigma,\tau}r_u}\}_{u\in[Q],\sigma\neq x_i^*,v=\delta(u,\sigma)}, \\ \{h_2^{-d_u+z_{1-\tau}r_u}, h_2^{d_v+w_{\sigma,1-\tau}r_u}, h_2^{r_u}\}_{u\in[Q],\sigma\in\Sigma,v=\delta(u,\sigma)}, \\ \{h_2^{\alpha-d_u+w_{\mathrm{end}}r_u}, h_2^{r_u}\}_{u\in F} \end{pmatrix} \\
&\approx_c \begin{pmatrix} h_2^{d_1+w_{\mathrm{start}}r_1}, h_2^{r_1}, \\ \{h_2^{-d_u+z_\tau r_u}, h_2^{d_{\delta(u,x_i^*)}+\Delta_{i,\delta(u,x_i^*)}+w_{x_i^*,\tau}r_u}, h_2^{r_u}\}_{u\in[Q]}, \\ \{h_2^{d_v+\boxed{\Delta_{i,v}}+w_{\sigma,\tau}r_u}\}_{u\in[Q],\sigma\neq x_i^*,v=\delta(u,\sigma)}, \\ \{h_2^{-d_u+z_{1-\tau}r_u}, h_2^{d_v+w_{\sigma,1-\tau}r_u}, h_2^{r_u}\}_{u\in[Q],\sigma\in\Sigma,v=\delta(u,\sigma)}, \\ \{h_2^{\alpha-d_u+w_{\mathrm{end}}r_u}, h_2^{r_u}\}_{u\in F} \end{pmatrix} = \mathsf{sk}_f^{i}[2]
\end{aligned}$$

given g_1, h_1, h_3 and

$$\mathsf{ct}_{x^*}^{i-1,i}[2] = \begin{cases} g_2^{s_0 w_{\text{start}}}, g_2^{s_0}, g_2^{s_0 z_1 + s_1 w_{x_1^*,1}}, g_2^{s_1}, g_2^{s_1 z_0} & \text{if } i = 1 \\ g_2^{s_{i-1} w_{x_{i-1}^*, 1-\tau}}, g_2^{s_{i-1}}, g_2^{s_{i-1} z_\tau + s_i w_{x_i^*,\tau}}, g_2^{s_i}, g_2^{s_i z_{1-\tau}} & \text{if } 1 < i < \ell \\ g_2^{s_{\ell-1} w_{x_{\ell-1}^*, 1-\bar{\ell}}}, g_2^{s_{\ell-1}}, g_2^{s_{\ell-1} z_{\bar{\ell}} + s_\ell w_{x_\ell^*,\bar{\ell}}}, g_2^{s_\ell}, g_2^{s_\ell w_{\text{end}}}, e(g_2^{s_\ell}, h_2^{\alpha}) & \text{if } i = \ell \end{cases}$$

Here terms g_1, h_1, h_3 allow us to simulate the p_1- and p_3-components of $\mathsf{ct}_{x^*}^{i-1,i}$ and $\mathsf{sk}_f^{i-1,i}$ (or sk_f^i) as well as mpk, which is sufficient for proving the lemma. We then proceed as follows:

- The first $\approx_c$ relies on $(z_\tau, w_{x_i^*,\tau})$-transition lemma (see Lemma 3). On input

$$\mathsf{aux}, s_{i-1} z_\tau + s_i w_{x_i^*,\tau}, \{h_2^{\hat{\Delta}_0 + z_\tau \bar{r}_u}, h_2^{\hat{\Delta}_1 + w_{x_i^*,\tau} \bar{r}_u}, h_2^{\bar{r}_u}\}_{u \in [Q]}$$

  with $\mathsf{aux} = (g_1, g_2, h_1, h_2, h_3, s_{i-1}, s_i, h_2^{z_\tau}, h_2^{w_{x_i^*,\tau}})$ where $z_\tau, w_{x_i^*,\tau}, \bar{r}_u \leftarrow \mathbb{Z}_N$ for all $u \in [Q]$ and

$$(\hat{\Delta}_0, \hat{\Delta}_1) \in \{(s_i \bar{\Delta}, 0), (0, s_{i-1} \bar{\Delta})\} \quad \text{with} \quad \bar{\Delta} \leftarrow \mathbb{Z}_N,$$

  we simulate p_2-components of the ciphertext and keys as follows:

  (Simulating ciphertext) We sample $\alpha, w_{\text{start}}, w_{\text{end}}, z_{1-\tau}, w_{\sigma,1-\tau} \leftarrow \mathbb{Z}_N$ for all $\sigma \in \Sigma$, and $w_{\sigma,\tau} \leftarrow \mathbb{Z}_N$ for $\sigma \neq x_i^*$. It is straight-forward to simulate $\mathsf{ct}_{x^*}^{i-1,i}[2]$ from $g_2, s_{i-1}, s_i, s_{i-1} z_\tau + s_i w_{x_i^*,\tau}$. This relies on the fact that neither $z_\tau \bmod p_2$ nor $w_{x_i^*,\tau} \bmod p_2$ appear elsewhere in $\mathsf{ct}_{x^*}^{i-1,i}[2]$.

  (Simulating key for f) We want to generate a challenge key which is either $\mathsf{sk}_f^{i-1,i}[2]$ on the LHS or the key on the RHS depending on $(\hat{\Delta}_0, \hat{\Delta}_1)$. On input f, we build $F_{i-1,x^*} \subseteq [Q]$ from f and sample $d_u \leftarrow \mathbb{Z}_N$ for all $u \in [Q]$ and $r_u \leftarrow \mathbb{Z}_N$ for all $u \notin F_{i-1,x^*}$. We implicitly set

$$\Delta = \begin{cases} s_i \bar{\Delta} & \text{for the LHS} \\ s_{i-1} \bar{\Delta} & \text{for the RHS} \end{cases} \quad \text{and} \quad r_u = \bar{r}_u \;\; \text{for all} \;\; u \in F_{i-1,x^*}$$

  and proceed as follows:
  - We rewrite all terms in the second row of keys on the two sides in terms of $s_{i-1}, s_i, \bar{\Delta}, \bar{r}_u$:

$$\text{LHS}_{\text{row 2}} = \begin{cases} h_2^{-d_u + \boxed{s_i \bar{\Delta}} + z_\tau \bar{r}_u}, h_2^{d_{\delta(u,x_i^*)} + w_{x_i^*,\tau} \bar{r}_u}, h_2^{\bar{r}_u} & \text{if } u \in F_{i-1,x^*} \\ h_2^{-d_u + z_\tau r_u}, \quad h_2^{d_{\delta(u,x_i^*)} + w_{x_i^*,\tau} r_u}, h_2^{r_u} & \text{if } u \notin F_{i-1,x^*} \end{cases}$$

$$\text{RHS}_{\text{row 2}} = \begin{cases} h_2^{-d_u + z_\tau \bar{r}_u}, h_2^{d_{\delta(u,x_i^*)} + \boxed{s_{i-1} \bar{\Delta}} + w_{x_i^*,\tau} \bar{r}_u}, h_2^{\bar{r}_u} & \text{if } \delta(u, x_i^*) \in F_{i,x^*} \\ h_2^{-d_u + z_\tau r_u}, h_2^{d_{\delta(u,x_i^*)} + w_{x_i^*,\tau} r_u}, \quad h_2^{r_u} & \text{if } \delta(u, x_i^*) \notin F_{i,x^*} \end{cases}$$

and generate the second row of the challenge key as

$$\begin{cases} h_2^{-d_u+\boxed{\hat{\Delta}_0}+z_\tau \bar{r}_u}, \ h_2^{d_{\delta(u,x_i^*)}+\boxed{\hat{\Delta}_1}+w_{x_i^*,\tau}\bar{r}_u}, \ h_2^{\bar{r}_u} & \text{if } u \in F_{i-1,x^*} \\ h_2^{-d_u+z_\tau r_u}, \qquad h_2^{d_{\delta(u,x_i^*)}+w_{x_i^*,\tau} r_u}, \qquad h_2^{r_u} & \text{if } u \notin F_{i-1,x^*} \end{cases}$$

where, with $\{d_u\}_{u\in[Q]}$, all terms for $u \in F_{i-1,x^*}$ can be built from terms $\{h_2^{\hat{\Delta}_0+z_\tau \bar{r}_u}, h_2^{\hat{\Delta}_1+w_{x_i^*,\tau}\bar{r}_u}, h_2^{\bar{r}_u}\}_{u\in F_{i-1,x^*}}$ provided in the input; all terms for $u \notin F_{i-1,x^*}$ can be built from $h_2, h_2^{z_\tau}, h_2^{w_{x_i^*,\tau}}$ in aux and $\{r_u\}_{u\notin F_{i-1,x^*}}$ we sampled.

- ◦ We can trivially generate all remaining terms in the challenge key which are identical to $\mathsf{sk}_f^{i-1,i}[2]$ (and also the key on the RHS) using $\{r_u\}_{u\notin F_{i-1,x^*}}$ and $\{h_2^{r_u} = h_2^{\bar{r}_u}\}_{u\in F_{i-1,x^*}}$ as well as α, w_{start}, $z_{1-\tau}$, $\{w_{\sigma,\tau}\}_{\sigma\neq x_i^*}$, $\{w_{\sigma,1-\tau}\}_{\sigma\in\Sigma}$, w_{end}.

Observe that,

- ◦ when $(\hat{\Delta}_0, \hat{\Delta}_1) = (s_i\bar{\Delta}, 0)$, the output distribution is identical to the LHS;
- ◦ when $(\hat{\Delta}_0, \hat{\Delta}_1) = (0, s_{i-1}\bar{\Delta})$, the output distribution is identical to the RHS; here we rely on the fact that $u \in F_{i-1,x^*} \iff \delta(u, x_i^*) \in F_{i,x^*}$ for all $u \in [Q]$, see Lemma 1.

This is sufficient for the proof of the first $\approx_c$.

- – The second $\approx_c$ follows from $\text{DDH}_{p_2}^{H_N}$ assumption w.r.t. $w_{\sigma,\tau} \bmod p_2$ with $\sigma \neq x_i^*$, which implies that: for all $\sigma \neq x_i^*$ and $\Delta \in \mathbb{Z}_N$, we have

$$\left\{h_2^{r_u}, h_2^{w_{\sigma,\tau} r_u}\right\}_{u\in[Q]} \approx_c \left\{h_2^{r_u}, h_2^{\Delta + w_{\sigma,\tau} r_u}\right\}_{u\in[Q]}$$

given g_1, g_2, h_1, h_2, h_3 and $h_2^{w_{\sigma,\tau}}$ where $w_{\sigma,\tau}, r_u \leftarrow \mathbb{Z}_N$ for all $u \in [Q]$. This relies on the fact that $\mathsf{ct}_{x^*}^{i-1,i}[2]$ does not leak $w_{\sigma,\tau} \bmod p_2$ with $\sigma \neq x_i^*$.

Combining the two steps proves the lemma. □

3.8 Finalize: $\mathsf{G}_{2.\ell.4} \mapsto \mathsf{G}_3$

We first describe the following lemma. The proof is analogous to the proof for Lemma 6 and we defer more details to the full paper due to the lack of space.

Lemma 13 **($\mathsf{G}_{2.\ell.4} \approx \mathsf{G}_3$).** *There exists $\mathcal{B}$ with $\mathsf{Time}(\mathcal{B}) \approx \mathsf{Time}(\mathcal{A})$ such that*

$$|\mathsf{Adv}_{\mathcal{A}}^{2.\ell.4}(\lambda) - \mathsf{Adv}_{\mathcal{A}}^{3}(\lambda)| \leq 2(|\Sigma| + 3) \cdot \mathsf{Adv}_{\mathcal{B}}^{\text{DDH}_{p_2}^{H_N}}(\lambda).$$

Finally we prove the last lemma evaluating adversary's advantage in G_3. Combining this lemma with Lemma 2,3 and Lemma 4,5,6,10,11,12,13 proves Theorem 1.

Lemma 14 **(Advantage in G_3).** *For all $\mathcal{A}$, we have $\mathsf{Adv}_{\mathcal{A}}^{3}(\lambda) \approx 0$.*

Proof. The definition of $\{\Delta_{\ell,u}\}_{u\in F}$ and $F_{\ell,x^*} = F$ imply that sk_f^* only leak $\alpha + \Delta \bmod p_2$. This means that secret keys perfectly hide $\alpha \bmod p_2$. Therefore, the term $e(g_2, h)^{s_\ell \alpha}$ in $\mathsf{ct}_{x^*}^{\ell}$ is independently and uniformly distributed and message m_β is statistically hidden by $\mathsf{H}(e(g_1, h)^{s_\ell \alpha} e(g_2, h)^{s_\ell \alpha})$ by the leftover hash lemma. Hence, $\mathsf{Adv}_{\mathcal{A}}^{3}(\lambda) \approx 0$. □

3.9 Towards Many-key Setting

Our proof for the one-key setting can be extended to the many-key setting in a straightforward way. Without loss of generality, we assume that all key queries $f_1, \ldots, f_q$ share the same state space $[Q]$ and alphabet Σ, and extend notations δ, F and F_{i,x^*}, d_u, r_u, $\Delta_{i,u}$ for f_κ with an additional subscript κ. Then we sketch the changes that are needed to handle the many-key setting:

Game sequence. We still employ the game sequence described in Section 3.2 except

– secret keys in $\mathsf{G}_{2.i.0}$, $\mathsf{G}_{2.i.1}$, $\mathsf{G}_{2.i.3}$ and G_3 are $\mathsf{sk}_{f_\kappa}^{i-1}$, $\mathsf{sk}_{f_\kappa}^{i-1,i}$, $\mathsf{sk}_{f_\kappa}^{i}$ and $\mathsf{sk}_{f_\kappa}^{*}$, respectively, for *all* $\kappa \in [q]$;
– in each game, $\{\Delta_{i,u,\kappa}\}_{u\in[Q]}$ for all $\kappa \in [q]$ are defined using the same $\Delta \leftarrow \mathbb{Z}_N$.

Useful lemmas. All lemmas in Section 3.3 can be trivially extended to the many-key setting; in fact, the (s,w)-switching lemma (Lemma 2) and (z,w)-transition lemma (Lemma 3) hold when we replace index $u \in [Q]$ with $(u,\kappa) \in [Q] \times [q]$.

Lemmas and Proofs. Lemma 4,5,6,10,11,12,13,14 all hold in the many-key setting:

– The proof for Lemma 4 can be trivially extended to the many-key setting.
– The proofs for Lemma 5,6,13 can work in the many-key setting due to the fact that
  ◦ $\{d_{u,\kappa}\}_{u\in[Q]}$ are fresh for each $\kappa \in [q]$; this ensures that all changes of variables still hold with multiple keys;
  ◦ $\{r_{u,\kappa}\}_{u\in[Q]}$ are fresh for each $\kappa \in [q]$; this ensures that all DDH-based arguments still hold with multiple keys.
– The proofs for Lemma 10,11,12 can be extended using the many-key version of (s,w)-switching lemma or (z,w)-transition lemma; here we also need the fact that $\{r_{u,\kappa}\}_{u\in[Q]}$ are fresh for each $\kappa \in [q]$.
– To prove Lemma 14 with many keys, we argue that *all* secret keys $\mathsf{sk}_{f_1}^{*}, \ldots, \mathsf{sk}_{f_q}^{*}$ only leak $\alpha + \Delta \bmod p_2$.

References

1. S. Agrawal and M. Chase. Simplifying design and analysis of complex predicate encryption schemes. In J. Coron and J. B. Nielsen, editors, *EUROCRYPT 2017, Part I*, volume 10210 of *LNCS*, pages 627–656. Springer, Heidelberg, Apr. / May 2017.
2. N. Attrapadung. Dual system encryption via doubly selective security: Framework, fully secure functional encryption for regular languages, and more. In P. Q. Nguyen and E. Oswald, editors, *EUROCRYPT 2014*, volume 8441 of *LNCS*, pages 557–577. Springer, Heidelberg, May 2014.
3. N. Attrapadung. Dual system encryption framework in prime-order groups via computational pair encodings. In J. H. Cheon and T. Takagi, editors, *ASIACRYPT 2016, Part II*, volume 10032 of *LNCS*, pages 591–623. Springer, Heidelberg, Dec. 2016.
4. O. Blazy, E. Kiltz, and J. Pan. (Hierarchical) identity-based encryption from affine message authentication. In J. A. Garay and R. Gennaro, editors, *CRYPTO 2014, Part I*, volume 8616 of *LNCS*, pages 408–425. Springer, Heidelberg, Aug. 2014.
5. J. Chen, R. Gay, and H. Wee. Improved dual system ABE in prime-order groups via predicate encodings. In E. Oswald and M. Fischlin, editors, *EUROCRYPT 2015, Part II*, volume 9057 of *LNCS*, pages 595–624. Springer, Heidelberg, Apr. 2015.

6. J. Chen, J. Gong, L. Kowalczyk, and H. Wee. Unbounded ABE via bilinear entropy expansion, revisited. In J. B. Nielsen and V. Rijmen, editors, *EUROCRYPT 2018, Part I*, volume 10820 of *LNCS*, pages 503–534. Springer, Heidelberg, Apr. / May 2018.
7. J. Chen and H. Wee. Fully, (almost) tightly secure IBE and dual system groups. In R. Canetti and J. A. Garay, editors, *CRYPTO 2013, Part II*, volume 8043 of *LNCS*, pages 435–460. Springer, Heidelberg, Aug. 2013.
8. J. Chen and H. Wee. Semi-adaptive attribute-based encryption and improved delegation for Boolean formula. In M. Abdalla and R. D. Prisco, editors, *SCN 14*, volume 8642 of *LNCS*, pages 277–297. Springer, Heidelberg, Sept. 2014.
9. A. Escala, G. Herold, E. Kiltz, C. Ràfols, and J. Villar. An algebraic framework for Diffie-Hellman assumptions. In R. Canetti and J. A. Garay, editors, *CRYPTO 2013, Part II*, volume 8043 of *LNCS*, pages 129–147. Springer, Heidelberg, Aug. 2013.
10. J. Gong, X. Dong, J. Chen, and Z. Cao. Efficient IBE with tight reduction to standard assumption in the multi-challenge setting. In J. H. Cheon and T. Takagi, editors, *ASIACRYPT 2016, Part II*, volume 10032 of *LNCS*, pages 624–654. Springer, Heidelberg, Dec. 2016.
11. V. Goyal, O. Pandey, A. Sahai, and B. Waters. Attribute-based encryption for fine-grained access control of encrypted data. In A. Juels, R. N. Wright, and S. Vimercati, editors, *ACM CCS 06*, pages 89–98. ACM Press, Oct. / Nov. 2006. Available as Cryptology ePrint Archive Report 2006/309.
12. D. Hofheinz, J. Koch, and C. Striecks. Identity-based encryption with (almost) tight security in the multi-instance, multi-ciphertext setting. In J. Katz, editor, *PKC 2015*, volume 9020 of *LNCS*, pages 799–822. Springer, Heidelberg, Mar. / Apr. 2015.
13. Z. Jafargholi, C. Kamath, K. Klein, I. Komargodski, K. Pietrzak, and D. Wichs. Be adaptive, avoid overcommitting. In J. Katz and H. Shacham, editors, *CRYPTO 2017, Part I*, volume 10401 of *LNCS*, pages 133–163. Springer, Heidelberg, Aug. 2017.
14. L. Kowalczyk and H. Wee. Compact adaptively secure ABE from k-lin. In *EUROCRYPT*, 2019.
15. A. B. Lewko and B. Waters. New techniques for dual system encryption and fully secure HIBE with short ciphertexts. In D. Micciancio, editor, *TCC 2010*, volume 5978 of *LNCS*, pages 455–479. Springer, Heidelberg, Feb. 2010.
16. A. B. Lewko and B. Waters. Unbounded HIBE and attribute-based encryption. In K. G. Paterson, editor, *EUROCRYPT 2011*, volume 6632 of *LNCS*, pages 547–567. Springer, Heidelberg, May 2011.
17. A. B. Lewko and B. Waters. New proof methods for attribute-based encryption: Achieving full security through selective techniques. In R. Safavi-Naini and R. Canetti, editors, *CRYPTO 2012*, volume 7417 of *LNCS*, pages 180–198. Springer, Heidelberg, Aug. 2012.
18. T. Okamoto and K. Takashima. Fully secure unbounded inner-product and attribute-based encryption. In X. Wang and K. Sako, editors, *ASIACRYPT 2012*, volume 7658 of *LNCS*, pages 349–366. Springer, Heidelberg, Dec. 2012.
19. A. Sahai and B. R. Waters. Fuzzy identity-based encryption. In R. Cramer, editor, *EUROCRYPT 2005*, volume 3494 of *LNCS*, pages 457–473. Springer, Heidelberg, May 2005.
20. B. Waters. Dual system encryption: Realizing fully secure IBE and HIBE under simple assumptions. In S. Halevi, editor, *CRYPTO 2009*, volume 5677 of *LNCS*, pages 619–636. Springer, Heidelberg, Aug. 2009.
21. B. Waters. Functional encryption for regular languages. In R. Safavi-Naini and R. Canetti, editors, *CRYPTO 2012*, volume 7417 of *LNCS*, pages 218–235. Springer, Heidelberg, Aug. 2012.
22. H. Wee. Dual system encryption via predicate encodings. In Y. Lindell, editor, *TCC 2014*, volume 8349 of *LNCS*, pages 616–637. Springer, Heidelberg, Feb. 2014.