Déjà Q: Encore! Un Petit IBE

Hoeteck Wee[⋆]

ENS, Paris, France

Abstract. We present an identity-based encryption (IBE) scheme in composite-order bilinear groups with essentially optimal parameters: the ciphertext overhead and the secret key are *one* group element each and decryption requires only *one* pairing. Our scheme achieves adaptive security and anonymity under standard decisional subgroup assumptions as used in Lewko and Waters (TCC '10). Our construction relies on a novel extension to the Deja Q framework of Chase and Meiklejohn (Eurocrypt '14).

1 Introduction

In identity-based encryption (IBE) [24, 5], ciphertexts and secret keys are associated with identities, and decryption is possible only when the identities match. IBE has been studied extensively over the last decade, with a major focus on obtaining constructions that simultanously achieve short parameters and full adaptive security under static assumptions in the standard model. This was first achieved in the works of Lewko and Waters [25, 20], which also introduced the powerful dual system encryption methodology. The design of the Lewko-Waters IBE and the underlying proof techniques have since had a profound impact on both attribute-based encryption and pairing-based cryptography.

1.1 Our Contributions

In this work, we obtain the first efficiency improvement to the Lewko-Waters IBE in composite-order bilinear groups. We present an adaptively secure and anonymous identity-based encryption (IBE) scheme with essentially optimal parameters: the ciphertext overhead and the secret key are *one* group element each, and decryption only requires *one* pairing; this improves upon the Lewko-Waters IBE [20] in three ways: shorter parameters, faster decryption, and anonymity. Via Naor's transformation, we obtain a fully secure signature scheme where the signature is again only *one* group element. We stress that we achieve all of these improvements while relying on the same computational subgroup assumptions as in the Lewko-Waters IBE, notably in composite-order groups whose order is the product of three primes. We refer to Fig 1 for a comparison with prior works.

The Lewko-Waters IBE has played a foundational role in recent developments of IBE and more generally attribute-based encryption (ABE). Indeed, virtually all of the state-of-the-art prime-order IBE schemes in [19, 2] —along with the subsequent extensions to ABE [21, 26, 1, 11]— follow the basic design and proof strategy introduced in the Lewko-Waters IBE. For this reason, we are optimistic that our improvement to the Lewko-Waters IBE will lead to further advances in IBE and ABE. In fact, our improved composite-order IBE already hints at the potential of a more efficient prime-order IBE that subsumes all known schemes; we defer further discussion to Section 1.3.

We also present a selectively secure broadcast encryption scheme for n users where the ciphertext overhead is two group elements (independent of the number of recipients) and the user private

[⋆] `wee@di.ens.fr`. CNRS (UMR 8548), INRIA and Columbia University. Supported in part by ERC Project aSCEND (639554) and NSF Award CNS-1445424.

Scheme	$\lvert$mpk$\rvert$	$\lvert$sk$\rvert$	$\lvert$ct$\rvert$	decryption	anonymous	number of primes
LW10 [20]	$3\lvert G_N\rvert + \lvert G_T\rvert$	$2\lvert G_N\rvert$	$2\lvert G_N\rvert + \lvert G_T\rvert$	2 pairings	no	3
DIP10 [9]	$3\lvert G_N\rvert + \lvert G_T\rvert$	$2\lvert G_N\rvert$	$2\lvert G_N\rvert + \lvert G_T\rvert$	2 pairings	✓	4
YCZY14 [27]	$3\lvert G_N\rvert + \lvert G_T\rvert$	$2\lvert G_N\rvert$	$2\lvert G_N\rvert + \lvert G_T\rvert$	2 pairings	✓	4
this work (Fig 2)	$2\lvert G_N\rvert + \lvert G_T\rvert$	$\lvert G_N\rvert$	$\lvert G_N\rvert + \lvert G_T\rvert$	1 pairing	✓	3

Fig. 1. Comparison amongst adaptively secure IBEs in composite-order bilinear groups $e : G_N \times G_N \to G_T$.

key is a single group element.[1] To the best of our knowledge, this is the first broadcast encryption scheme to achieve constant-size ciphertext overhead, constant-size user private keys and linear-size public parameters under static assumptions; previously, such schemes were only known under q-type assumptions [6].

1.2 Our Techniques

The starting point of our constructions is the Deja Q framework introduced by Chase and Meiklejohn [10]; this is an extension of Waters' dual system techniques to eliminate the use of q-type assumptions in settings beyond the reach of previous techniques. These settings include deterministic primitives such as pseudo-random functions (PRF) and —quite remarkably— schemes based on the inversion framework [23, 4, 8]. However, the Deja Q framework is also limited in that it cannot be applied to advanced encryption systems such as identity-based and broadcast encryption, where certain secret exponents appear in both ciphertexts and secret keys on both sides of the pairing. We show how to overcome this limitation using several simple ideas.

IBE Overview. We describe our IBE scheme and the security proof next. We present a simplified variant of the constructions, suppressing many details pertaining to randomization and subgroups. Following the Lewko-Waters IBE [20], we rely on composite-order bilinear groups whose order N is the product of three primes p_1, p_2, p_3. We will use the subgroup G_{p_1} of order p_1 for functionality, and the subgroup G_{p_2} of order p_2 in the proof of security. The third subgroup corresponding to p_3 is used for additional randomization.

Recall that the Lewko-Waters IBE has the following form:

$$\mathsf{mpk} := (g, g^{\beta}, g^{\gamma}, e(g,u)),\ \mathsf{ct}_{\mathsf{id}} := (g^{s}, g^{(\beta+\gamma\mathsf{id})s}, e(g,u)^{s}\cdot m),\ \mathsf{sk}_{\mathsf{id}} := (u\cdot g^{(\beta+\gamma\mathsf{id})r}, g^{r}))$$

Our IBE scheme has the following form:

$$\mathsf{mpk} := (g, g^{\alpha}, e(g,u)),\ \mathsf{ct}_{\mathsf{id}} := (g^{(\alpha+\mathsf{id})s}, e(g,u)^{s}\cdot m),\ \mathsf{sk}_{\mathsf{id}} := (u^{\frac{1}{\alpha+\mathsf{id}}})$$

Note that our scheme uses the "exponent inversion" framework [8], which has traditionally eluded a proof of security under static assumptions. In both schemes, g, u are random group elements of order p_1, and α, β, γ are random exponents over $\mathbb{Z}_N$. It is easy to see that decryption in our scheme only requires a single pairing to compute $e(g^{(\alpha+\mathsf{id})s}, u^{\frac{1}{\alpha+\mathsf{id}}}) = e(g,u)^{s}$.

IBE security proof. We rely on the same assumption as the Lewko-Waters IBE in [20], namely the $(p_1 \mapsto p_1p_2)$-subgroup assumption, which asserts that random elements of order p_1 and those of order p_1p_2

[1] Here, we ignore the additional overhead from specifying the set of recipients in the ciphertext, which requires n *bits*; decrypting also requires knowing some public parameters, which are not considered part of the user private keys.

are computationally indistinguishable. In the proof of security, we rely on the assumption to introduce random G_{p_2}-components to the ciphertext and the secret keys.

We begin with the secret keys. We introduce a random G_{p_2}-component to the secret key $\mathsf{sk}_{\mathsf{id}}$ following the Deja Q framework [10] as follows:

$$\mathsf{sk}_{\mathsf{id}} = u^{\frac{1}{\alpha+\mathsf{id}}} \xrightarrow{\text{subgroup}} u^{\frac{1}{\alpha+\mathsf{id}}} g_2^{\frac{r_1}{\alpha+\mathsf{id}}} \xrightarrow{\text{CRT}} u^{\frac{1}{\alpha+\mathsf{id}}} g_2^{\frac{r_1}{\alpha_1+\mathsf{id}}}, \tag{1}$$

where $\alpha_1 \leftarrow \mathbb{Z}_N$. In the first transition, we use the $(p_1 \mapsto p_1 p_2)$-subgroup assumption which says that $u \approx_c u g_2^{r_1}, r_1 \leftarrow_{\mathrm{R}} \mathbb{Z}_N$, where g_2 is a generator of order p_2. In the second transition, we use the Chinese Reminder Theorem (CRT), which tell us $\alpha \bmod p_1$ and $\alpha \bmod p_2$ are independently random values, so we may replace $\alpha \bmod p_2$ with $\alpha_1 \bmod p_2$ for a fresh $\alpha_1 \leftarrow_{\mathrm{R}} \mathbb{Z}_N$, as long as the challenge ciphertext and mpk reveal no information about $\alpha \bmod p_2$. We may now repeat this transition q more times:

$$\begin{array}{lclcl} u^{\frac{1}{\alpha+\mathsf{id}}} & \xrightarrow{\text{subgroup}} & u^{\frac{1}{\alpha+\mathsf{id}}} g_2^{\frac{r_1}{\alpha+\mathsf{id}}} & \xrightarrow{\text{CRT}} & u^{\frac{1}{\alpha+\mathsf{id}}} g_2^{\frac{r_1}{\alpha_1+\mathsf{id}}} \\ & \xrightarrow{\text{subgroup}} & u^{\frac{1}{\alpha+\mathsf{id}}} g_2^{\frac{r_2}{\alpha+\mathsf{id}}} g_2^{\frac{r_1}{\alpha_1+\mathsf{id}}} & \xrightarrow{\text{CRT}} & u^{\frac{1}{\alpha+\mathsf{id}}} g_2^{\frac{r_2}{\alpha_2+\mathsf{id}}+\frac{r_1}{\alpha_1+\mathsf{id}}} \\ & \longrightarrow & \cdots & \xrightarrow{\text{CRT}} & u^{\frac{1}{\alpha+\mathsf{id}}} g_2^{\frac{r_{q+1}}{\alpha_{q+1}+\mathsf{id}}+\cdots+\frac{r_2}{\alpha_2+\mathsf{id}}+\frac{r_1}{\alpha_1+\mathsf{id}}} \end{array}$$

where $r_1, \ldots, r_{q+1}, \alpha_1, \ldots, \alpha_{q+1} \leftarrow_{\mathrm{R}} \mathbb{Z}_N$, and q is an upper bound on the number of key queries made by the adversary.[2]

Next, we show that for distinct $x_1, \ldots, x_q$, the following matrix

$$\begin{pmatrix} \frac{1}{\alpha_1+x_1} & \frac{1}{\alpha_1+x_2} & \cdots & \frac{1}{\alpha_1+x_q} \\ \vdots & \vdots & \ddots & \vdots \\ \frac{1}{\alpha_q+x_1} & \frac{1}{\alpha_q+x_2} & \cdots & \frac{1}{\alpha_q+x_q} \end{pmatrix} \tag{2}$$

is invertible with overwhelming probability over $\alpha_1, \ldots, \alpha_q \leftarrow_{\mathrm{R}} \mathbb{Z}_p$. We provide an explicit formula for the determinant of this matrix in Section 3.1; this is the only place in the proof where we crucially exploit the "exponent inversion" structure. We can then replace

$$\mathsf{id} \mapsto \frac{r_{q+1}}{\alpha_{q+1}+\mathsf{id}} + \cdots + \frac{r_2}{\alpha_2+\mathsf{id}} + \frac{r_1}{\alpha_1+\mathsf{id}}$$

by a truly random function $\mathsf{RF}(\cdot)$. Indeed, $\mathsf{sk}_{\mathsf{id}}$ can now be written as $u^{\frac{1}{\alpha+\mathsf{id}}} g_2^{\mathsf{RF}(\mathsf{id})}$, which have independently random G_{p_2}-components.

So far, what we have done is the same as the use of Deja Q framework for showing that $x \mapsto u^{\frac{1}{x+\alpha}}$ yields a PRF [10] (the explicit formula for the matrix determinant is new), and this is where the similarity ends. At this point, we still need to hide the message m in the ciphertext $(g^{(\alpha+\mathsf{id})s}, e(g,u)^s \cdot m)$. Towards this goal, we want to introduce a G_{p_2}-component into the ciphertext, which will then interact with newly random G_{p_2}-component in the keys to generate extra statistical entropy to hide m. At the same time, we need to ensure that the ciphertext still hides $\alpha \bmod p_2$ so that we may carry out the transition of the secret keys in (1). Indeed, naively applying the $(p_1 \mapsto p_1 p_2)$-subgroup assumption to g^s in the ciphertext would leak $\alpha \bmod p_2$.

To circumvent this difficulty, note that we can rewrite the ciphertext in terms of $\mathsf{sk}_{\mathsf{id}}$ as

$$\mathsf{ct}_{\mathsf{id}} = (g^{(\alpha+\mathsf{id})s}, e(g^{(\alpha+\mathsf{id})s}, \mathsf{sk}_{\mathsf{id}}) \cdot m)$$

[2] We use $q+1$ values to account for the q key queries plus the challenge identity.

Moreover, as long as $\alpha + \mathsf{id} \neq 0$, we can replace $(\alpha+\mathsf{id})s$ with s without changing the distribution, which allows us to rewrite the challenge ciphertext as

$$\mathsf{ct}_{\mathsf{id}} = (g^s, e(g^s, \mathsf{sk}_{\mathsf{id}}) \cdot m).$$

This means that the challenge ciphertext leaks no information about α except through $\mathsf{sk}_{\mathsf{id}}$. In addition, the challenge ciphertext also leaks no information about id, which allows us to prove anonymity. In contrast, the Lewko-Waters IBE is not anonymous, and anonymous variants there-of in [9, 27] requires the use of 4 primes and additional assumptions.

We can now apply the $(p_1 \mapsto p_1p_2)$-subgroup assumption to the ciphertext to replace g^s with $g^s g_2^{r'}$. Now, the ciphertext distribution is completely independent of α except what is leaked through $\mathsf{sk}_{\mathsf{id}}$, so we can apply the secret key transitions as before, at the end of which the challenge ciphertext is given by:

$$(g^s g_2^{r'}, e(g^s g_2^{r'}, u^{\frac{1}{\alpha+\mathsf{id}}} g_2^{\mathsf{RF}(\mathsf{id})}) \cdot m) = (g^s g_2^{r'}, e(g^s, u^{\frac{1}{\alpha+\mathsf{id}}}) \cdot \boxed{e(g_2^{r'}, g_2^{\mathsf{RF}(\mathsf{id})})} \cdot m)$$

We can now use the $\log p_2$ bits of entropy from $\mathsf{RF}(\mathsf{id})$ over G_{p_2} to hide m; this requires modifying the original scheme so that an encryption of m is given by $(g^{(\alpha+\mathsf{id})s}, \mathsf{H}(e(g,u)^s) \cdot m)$, where H denotes a strong randomness extractor whose seed is specified in mpk.

Broadcast encryption. By rewriting the challenge ciphertext in terms of $\mathsf{sk}_{\mathsf{id}}$ in order to hide α, our technique for IBE seems inherently limited to IBE. We show how to extend our techniques to broadcast encryption in Section 4; however, we only achieve selective and not adaptive security. We briefly note that our broadcast encryption scheme is derived from Boneh-Gentry-Waters (BGW) scheme [6] based on the q-DBDHE assumption. This is the first scheme to asymptotically match the parameters of the BGW broadcast encryption scheme under static assumptions.

1.3 Discussion

Comparison with Deja Q framework [10]. The core of the Deja Q framework is a beautiful technique which translates linear independence (and thus computational independence in the generic group model) amongst a set of monomials "in the exponent" into statistical independence, upon which security can be established using a purely information-theoretic argument. There are however three caveats to the prior instantiation in [10]: first, these monomials must appear on the same side of the pairing, which means the techniques cannot be applied to advanced encryption primitives where the same term often appears in the ciphertext and the secret key on both sides of the pairing; second, the statistical independence only holds within certain subgroups, and another subgroup assumption was used to spread this localized entropy over the entire group; third, the prior instantiation is limited to asymmetric composite-order groups. In this work, we showed how to overcome all of these three caveats.

In particular, we rely only on the $(p_1 \mapsto p_1p_2)$-subgroup assumption and eliminated the additional use of the $(p_2 \mapsto p_1p_2)$-subgroup assumption. This technique can also be applied to the PRF in [10]. We note that while simulating subgroup decisional assumptions in composite-order groups using the k-LIN assumption in prime-order groups, we can simulate the $(p_1 \mapsto p_1p_2)$-subgroup assumption using $k+1$ group elements whereas simulating both subgroup assumption requires $2k$ group elements.

Candidate prime-order IBE. As noted earlier, our composite-order IBE scheme constitutes the first evidence for an adaptively IBE based on SXDH with two group elements in the ciphertext and in the secret keys and constant-size public parameters, which would be a significant improvement over the state of the art, subsuming a long series of incomparable constructions, and giving us adaptive security at essentially the same cost as selective security! Moreover, such a IBE would in turn also yield a fully secure signature scheme based on SXDH with two group elements in the signature and constant-size public key. To reach two elements, it is important that we rely only on the $(p_1 \mapsto p_1 p_2)$-subgroup assumption and eliminated the additional use of the $(p_2 \mapsto p_1 p_2)$-subgroup assumption. The optimism comes from combining our composite-order IBE scheme with the huge success we have had in converting composite-order schemes to prime-order ones [14, 22, 19, 11]. In fact, we present a concrete candidate for a prime-order IBE in Section 3.3; we stress that we do not have a security proof for the scheme. We note that an improved SXDH-based signature scheme would likely yield further improvements to other related primitives, such as group signatures and structure-preserving signatures. These applications further motivate the open problem highlighted in [10] of finding prime-order analogues for the Deja Q framework.

Perspective. We presented new constructions of "optimal" IBE and signatures and new IBE candidates that improve upon a long line of work; moreover, we achieve these via an extended Deja Q framework which avoid the limitations of widely used techniques. We are optimistic and excited about challenges and possibilities that lie ahead.

2 Preliminaries

Notation. We denote by $s \leftarrow_{\mathrm{R}} S$ the fact that s is picked uniformly at random from a finite set S. By PPT, we denote a probabilistic polynomial-time algorithm. Throughout, we use 1^λ as the security parameter.

2.1 Composite-Order Bilinear Groups and Cryptographic Assumptions

We instantiate our system in composite-order bilinear groups, which were introduced in [7] and used in [18, 20, 21]. A generator $\mathcal{G}$ takes as input a security parameter λ and outputs a description $\mathbb{G} := (N, G, G_T, e)$, where N is product of distinct primes of $\Theta(\lambda)$ bits, G and G_T are cyclic groups of order N, and $e : G \times G \to G_T$ is a non-degenerate bilinear map. We require that the group operations in G and G_T as well the bilinear map e are computable in deterministic polynomial time.We consider bilinear groups whose orders N are products of three distinct primes p_1, p_2, p_3 (that is, $N = p_1 p_2 p_3$). We can write $G = G_{p_1} G_{p_2} G_{p_3}$ where $G_{p_1}, G_{p_2}, G_{p_3}$ are subgroups of G of order p_1, p_2 and p_3 respectively. In addition, we use $G^*_{p_i}$ to denote $G_{p_i} \setminus \{1\}$. We will often write g_1, g_2, g_3 to denote random generators for the subgroups $G_{p_1}, G_{p_2}, G_{p_3}$.

Cryptographic assumptions. Our construction relies on the following two decisional subgroup assumptions (also known as subgroup hiding assumptions). We define the following two advantage functions:

$$
\begin{aligned}
&\mathsf{Adv}^{\mathrm{SD1}}_{\mathcal{G},\mathcal{A}}(\lambda) := |\Pr[\mathcal{A}(D, T_0) = 1] - \Pr[\mathcal{A}(D, T_1) = 1]| \\
&\quad \text{where } \mathbb{G} \leftarrow \mathcal{G}, T_0 \leftarrow \boxed{G_{p_1}}, T_1 \leftarrow_{\mathrm{R}} \boxed{G_{p_1} G_{p_2}} \qquad\qquad (p_1 \mapsto p_1 p_2) \\
&\qquad \text{and } D := (g_1, g_3, g_{\{1,2\}}), g_1 \leftarrow_{\mathrm{R}} G^*_{p_1}, g_3 \leftarrow_{\mathrm{R}} G^*_{p_3}, g_{\{1,2\}} \leftarrow_{\mathrm{R}} G_{p_1} G_{p_2} \\
&\mathsf{Adv}^{\mathrm{SD2}}_{\mathcal{G},\mathcal{A}}(\lambda) := |\Pr[\mathcal{A}(D, T_0) = 1] - \Pr[\mathcal{A}(D, T_1) = 1]| \\
&\quad \text{where } \mathbb{G} \leftarrow \mathcal{G}, T_0 \leftarrow \boxed{G_{p_1} G_{p_3}}, T_1 \leftarrow_{\mathrm{R}} \boxed{G_{p_1} G_{p_2} G_{p_3}} \qquad\qquad (p_1 p_3 \mapsto N) \\
&\qquad \text{and } D := (g_1, g_3, g_{\{1,2\}}, g_{\{2,3\}}), g_1 \leftarrow_{\mathrm{R}} G^*_{p_1}, g_3 \leftarrow_{\mathrm{R}} G^*_{p_3}, g_{\{1,2\}} \leftarrow_{\mathrm{R}} G_{p_1} G_{p_2}, g_{\{2,3\}} \leftarrow_{\mathrm{R}} G_{p_2} G_{p_3}
\end{aligned}
$$

The decisional subgroup assumptions assert that that for all PPT adversaries $\mathcal{A}$, the advantages $\mathsf{Adv}^{\mathrm{SD1}}_{\mathcal{G},\mathcal{A}}(\lambda)$ and $\mathsf{Adv}^{\mathrm{SD2}}_{\mathcal{G},\mathcal{A}}(\lambda)$ are negligible functions in λ.

2.2 Anonymous Identity-Based Encryption

We define identity-based encryption (IBE) in the framework of key encapsulation. An identity-based encryption scheme consists of four algorithms $(\mathsf{Setup}, \mathsf{Enc}, \mathsf{KeyGen}, \mathsf{Dec})$:

$\mathsf{Setup}(1^\lambda) \to (\mathsf{mpk}, \mathsf{msk})$. The setup algorithm gets as input the security parameter λ and outputs the public parameter mpk, and the master key msk. All the other algorithms get mpk as part of its input.

$\mathsf{Enc}(\mathsf{mpk}, \mathsf{id}) \to (\mathsf{ct}, \kappa)$. The encryption algorithm gets as input mpk and an identity $\mathsf{id} \in \{0,1\}^\lambda$. It outputs a ciphertext ct and a symmetric key $\kappa \in \{0,1\}^\lambda$.

$\mathsf{KeyGen}(\mathsf{msk}, \mathsf{id}) \to \mathsf{sk}_{\mathsf{id}}$. The key generation algorithm gets as input msk and an identity $\mathsf{id} \in \{0,1\}^\lambda$. It outputs a secret key $\mathsf{sk}_{\mathsf{id}}$.

$\mathsf{Dec}(\mathsf{sk}_{\mathsf{id}}, \mathsf{ct}) \to \kappa$. The decryption algorithm gets as input $\mathsf{sk}_{\mathsf{id}}$ and ct. It outputs a symmetric key κ.

Correctness. We require that for all $\mathsf{id} \in \{0,1\}^\lambda$,

$$\Pr[(\mathsf{ct}, \kappa) \leftarrow \mathsf{Enc}(\mathsf{mpk}, \mathsf{id});\ \mathsf{Dec}(\mathsf{sk}_{\mathsf{id}}, \mathsf{ct}) = \kappa)] = 1,$$

where the probability is taken over $(\mathsf{mpk}, \mathsf{msk}) \leftarrow \mathsf{Setup}(1^\lambda)$ and the coins of Enc.

Security definition. We require pseudorandom ciphertexts against adaptively chosen plaintext and identity attacks, which implies both anonymity and adaptive security. For a stateful adversary $\mathcal{A}$, we define the advantage function

$$\mathsf{Adv}_{\mathcal{A}}^{\text{A-IBE}}(\lambda) := \Pr\left[b = b' : \begin{array}{l} (\mathsf{mpk}, \mathsf{msk}) \leftarrow \mathsf{Setup}(1^\lambda); \\ \mathsf{id}^* \leftarrow \mathcal{A}^{\mathsf{KeyGen}(\mathsf{msk}, \cdot)}(\mathsf{mpk}); \\ b \leftarrow_{\mathrm{R}} \{0,1\}; \mathsf{ct}_1 \leftarrow_{\mathrm{R}} \mathcal{C}; \kappa_1 \leftarrow_{\mathrm{R}} \{0,1\}^\lambda; \\ (\mathsf{ct}_0, \kappa_0) \leftarrow \mathsf{Enc}(\mathsf{mpk}, \mathsf{id}^*); \\ b' \leftarrow \mathcal{A}^{\mathsf{KeyGen}(\mathsf{msk}, \cdot)}(\mathsf{ct}_b, \kappa_b) \end{array} \right] - \frac{1}{2}$$

with the restriction that all queries id that $\mathcal{A}$ makes to $\mathsf{KeyGen}(\mathsf{msk}, \cdot)$ satisfies $\mathsf{id} \neq \mathsf{id}^*$, and where $\mathsf{ct}_1 \leftarrow_{\mathrm{R}} \mathcal{C}$ denotes a random element from the ciphertext space.[3] An identity-based encryption (IBE) scheme is *adaptively secure and anonymous* if for all PPT adversaries $\mathcal{A}$, the advantage $\mathsf{Adv}_{\mathcal{A}}^{\text{A-IBE}}(\lambda)$ is a negligible function in λ.

2.3 Broadcast Encryption

A broadcast encryption scheme consists of three algorithms $(\mathsf{Setup}, \mathsf{Enc}, \mathsf{Dec})$:

$\mathsf{Setup}(1^\lambda, 1^n) \to (\mathsf{mpk}, (\mathsf{sk}_1, \ldots, \mathsf{sk}_n))$. The setup algorithm gets as input the security parameter λ and 1^n specifying the number of users and outputs the public parameter mpk, and secret keys $\mathsf{sk}_1, \ldots, \mathsf{sk}_n$.

$\mathsf{Enc}(\mathsf{mpk}, \Gamma) \to (\mathsf{ct}_\Gamma, \kappa)$. The encryption algorithm gets as input mpk and a subset $\Gamma \subseteq [n]$. It outputs a ciphertext ct_Γ and a symmetric key $\kappa \in \{0,1\}^\lambda$. Here, Γ is public given ct_Γ.

$\mathsf{Dec}(\mathsf{mpk}, \mathsf{sk}_y, \mathsf{ct}_\Gamma) \to \kappa$. The decryption algorithm gets as input $\mathsf{mpk}, \mathsf{sk}_y$ and ct_Γ. It outputs a symmetric key κ.

[3] This means that the distribution of ct_1 is independent of id^*, which implies anonymity.

Correctness. We require that for all $\Gamma \subseteq [n]$ and all $y \in [n]$ for which $y \in \Gamma$,

$$\Pr[(\mathsf{ct}_\Gamma, \kappa) \leftarrow \mathsf{Enc}(\mathsf{mpk}, \Gamma);\ \mathsf{Dec}(\mathsf{mpk}, \mathsf{sk}_y, \mathsf{ct}_\Gamma) = \kappa)] = 1,$$

where the probability is taken over $(\mathsf{mpk}, (\mathsf{sk}_1, \ldots, \mathsf{sk}_n)) \leftarrow \mathsf{Setup}(1^\lambda, 1^n)$ and the coins of Enc.

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

$$\mathsf{Adv}^{\text{S-BCE}}_{\mathcal{A}}(\lambda) := \Pr\left[b = b' : \begin{array}{l} \Gamma^* \leftarrow \mathcal{A}(1^\lambda); \\ (\mathsf{mpk}, (\mathsf{sk}_1, \ldots, \mathsf{sk}_n)) \leftarrow \mathsf{Setup}(1^\lambda); \\ b \leftarrow_{\mathrm{R}} \{0,1\}; \kappa_1 \leftarrow_{\mathrm{R}} \{0,1\}^\lambda; \\ (\mathsf{ct}_{\Gamma^*}, \kappa_0) \leftarrow \mathsf{Enc}(\mathsf{mpk}, \Gamma^*); \\ b' \leftarrow \mathcal{A}(\mathsf{ct}_{\Gamma^*}, \kappa_b, \{\mathsf{sk}_y : y \notin \Gamma^*\}) \end{array} \right] - \frac{1}{2}$$

A broadcast encryption scheme is *selectively secure* if for all PPT adversaries $\mathcal{A}$, the advantage $\mathsf{Adv}^{\text{S-BCE}}_{\mathcal{A}}(\lambda)$ is a negligible function in λ.

3 Identity-Based Encryption

We present an adaptively secure and anonymous IBE scheme in Fig 2, and a fully secure signature scheme in Fig 3. The schemes here refer to symmetric composite-order bilinear groups; we present the variant for asymmetric composite-bilinear groups in Section A. The schemes and the proofs are the same as in the overview in the introduction (Section 1.2), except the secret keys in both the scheme and the proof have an extra random G_{p_3}-component and we will use the $(p_1 p_3 \mapsto N)$-subgroup assumption to switch the secret keys.

Comparison with prior schemes. We recall several IBE and signature schemes in the inversion framework which share a similar structure to our IBE and signature scheme. All of these schemes require an additional scalar in the key/signature, and both of the IBE schemes require an additional group element in the ciphertext.

BB_2 IBE [4]. The BB_2 IBE is selectively secure under the q-DBDHI assumption:

$$\mathsf{ct}_{\mathsf{id}} := (g^{(\alpha+\mathsf{id})s}, g^{\beta s}, e(g,u)^s \cdot m),\ \mathsf{sk}_{\mathsf{id}} := (u^{\frac{1}{\alpha+\mathsf{id}+\beta r}}, r)$$

Gentry's IBE [16]. Gentry's IBE is adaptively secure and anonymous under the q-ADBDHE assumption:

$$\mathsf{ct}_{\mathsf{id}} := (g^{(\alpha+\mathsf{id})s}, e(g,g)^s, e(g,u)^s \cdot m),\ \mathsf{sk}_{\mathsf{id}} := ((u \cdot g^{-r})^{\frac{1}{\alpha+\mathsf{id}}}, r)$$

Boneh-Boyen signatures [3, 10]. The Deja Q analogue [10] of the Boneh-Boyen signatures is given by:

$$\mathsf{pk} := (g, g^\alpha, g^\beta, e(g,u)),\ \sigma := (u^{\frac{1}{\alpha+M+\beta r}}, r) \in \mathbb{G}_N \times \mathbb{Z}_N.$$

Our signature scheme in Fig 3 is simpler and shorter, and the scheme can be also be instantiated in symmetric composite-order groups. In fact, our signature scheme may be viewed as applying the Deja Q framework to the Boneh-Boyen weak signatures, which both "upgrades" the security from weak to full, and removes the use of q-type assumptions.

3.1 Core lemma

The following lemma is implicit in the analysis of the PRF in [10, Theorem 4.2, Equation 8].

Lemma 1. *Fix a prime p and define $\mathsf{F}^q_{r_1,\dots,r_q,\alpha_1,\dots,\alpha_q}:\mathbb{Z}_p\to\mathbb{Z}_p$ to be*

$$\mathsf{F}^q_{r_1,\dots,r_q,\alpha_1,\dots,\alpha_q}(x) := \sum_{i=1}^{q}\frac{r_i}{\alpha_i+x}$$

Then, for any (possibly unbounded) adversary $\mathcal{A}$ that makes at most q queries, we have

$$\left|\Pr_{r_1,\dots,r_q,\alpha_1,\dots,\alpha_q\leftarrow_{\mathrm{R}}\mathbb{Z}_p}\left[\mathcal{A}^{\mathsf{F}^q_{r_1,\dots,r_q,\alpha_1,\dots,\alpha_q}(\cdot)}(1^q)=1\right]-\Pr\left[\mathcal{A}^{\mathsf{RF}(\cdot)}(1^q)=1\right]\right|\le\frac{q^2}{p}$$

where $\mathsf{RF}:\mathbb{Z}_p\to\mathbb{Z}_p$ is a truly random function.

The proof in [10] directly rewrites the function $\mathsf{F}^q_{r_1,\dots,r_q,\alpha_1,\dots,\alpha_q}$ with a common denominator and then relates the numerator to the Lagrange interpolating polynomial for an appropriate choice of q points. We sketch an alternative proof which better explains the choice of the function $(\alpha,\mathsf{id})\mapsto\frac{1}{\alpha+\mathsf{id}}$. We first consider the case where the queries $x_1,\dots,x_q$ made by $\mathcal{A}$ are chosen non-adaptively. WLOG, we may assume that these queries are distinct. Then, it suffices to show that the following matrix

$$\begin{pmatrix}\frac{1}{\alpha_1+x_1} & \frac{1}{\alpha_1+x_2} & \cdots & \frac{1}{\alpha_1+x_q}\\ \vdots & \vdots & \ddots & \vdots\\ \frac{1}{\alpha_q+x_1} & \frac{1}{\alpha_q+x_2} & \cdots & \frac{1}{\alpha_q+x_q}\end{pmatrix}$$

is invertible with overwhelming probability over $\alpha_1,\dots,\alpha_q\leftarrow_{\mathrm{R}}\mathbb{Z}_p$. (Such a statement follows from the proof in [10] but was not pointed out explicitly.) As it turns out, we can write the determinant of this matrix explicitly as:

$$\frac{\Pi_{1\le i<j\le q}(x_i-x_j)(\alpha_i-\alpha_j)}{\Pi_{1\le i,j\le q}(\alpha_i+x_j)}$$

which is non-zero as long as $\alpha_1,\dots,\alpha_q$ are distinct, $x_1,\dots,x_q$ are distinct, and the α_i+x_j's are all non-zero.

That is, we want to show that

$$\Pi_{1\le i,j\le q}(\alpha_i+x_j)\cdot\det\begin{pmatrix}\frac{1}{\alpha_1+x_1} & \frac{1}{\alpha_1+x_2} & \cdots & \frac{1}{\alpha_1+x_q}\\ \vdots & \vdots & \ddots & \vdots\\ \frac{1}{\alpha_q+x_1} & \frac{1}{\alpha_q+x_2} & \cdots & \frac{1}{\alpha_q+x_q}\end{pmatrix}=\Pi_{1\le i<j\le q}(x_i-x_j)(\alpha_i-\alpha_j)$$

Using the standard formula for the determinant of the matrix, we can write the determinant above as a sum of inverses of homogenous polynomials of degree q in $x_1,\dots,x_q,\alpha_1,\dots,\alpha_q$. Upon multiplying by $\Pi_{1\le i,j\le q}(\alpha_i+x_j)$, we would "clear the denominators" to obtain a homogeneous polynomial P in $x_1,\dots,x_q,\alpha_1,\dots,\alpha_q$ of degree q^2-q. Moreover, the matrix has two equal rows (resp. columns) whenever we have $\alpha_i=\alpha_j$ (resp. $x_i=x_j$); when this happens, the matrix has determinant 0 and thus P vanishes. Therefore, the polynomial P must be a multiple of $\Pi_{1\le i<j\le q}(x_i-x_j)(\alpha_i-\alpha_j)$, which also has degree q^2-q. This means that P must be a constant multiple of $\Pi_{1\le i<j\le q}(x_i-x_j)(\alpha_i-\alpha_j)$, and it is easy to check that the constant is 1.

To handle adaptive queries, observe that this corresponds to building the matrix one column at a time. As long as the partial selection of columns have full rank, the output of F is uniformly random, which then completely hides $\alpha_1,\dots,\alpha_q$. Therefore, the probability that $\alpha_1,\dots,\alpha_q$ are distinct, and that α_i+x_j's are all non-zero is at least $1-q^2/p$, even for adaptive choices of distinct $x_1,\dots,x_q$.

Setup($\mathbb{G}$): msk := $(\alpha, u, g_3) \leftarrow_{\mathrm{R}} \mathbb{Z}_N \times G_{p_1} \times G_{p_3}^*$; mpk := $(g_1, g_1^\alpha, e(g_1, u), \mathsf{H})$; return (mpk, msk) KeyGen(msk, id $\in \mathbb{Z}_N$): pick $R_3 \leftarrow_{\mathrm{R}} G_{p_3}$; return $\mathsf{sk}_{\mathsf{id}} := u^{\frac{1}{\alpha+\mathsf{id}}} R_3$	Enc(mpk, id $\in \mathbb{Z}_N$): pick $s \leftarrow_{\mathrm{R}} \mathbb{Z}_N$; return $(\mathsf{ct}, \kappa) := (g_1^{(\alpha+\mathsf{id})s}, \mathsf{H}(e(g_1, u)^s))$ Dec($\mathsf{sk}_{\mathsf{id}}$, ct): return $\mathsf{H}(e(\mathsf{ct}, \mathsf{sk}_{\mathsf{id}}))$

Fig. 2. Adaptively secure anonymous IBE w.r.t. a composite-order bilinear group $\mathbb{G}$. Here, $\mathsf{H} : G_T \to \{0,1\}^\lambda$ is drawn from a family of pairwise-independent hash functions. In asymmetric groups, randomization with R_3 in KeyGen is not necessary (i.e., KeyGen is deterministic).

Setup($\mathbb{G}$): sk := $(\alpha, u, g_3) \leftarrow_{\mathrm{R}} \mathbb{Z}_N \times G_{p_1} \times G_{p_3}^*$; pk := $(g_1, g_1^\alpha, e(g_1, u))$; return (pk, sk)	**sign**(sk, $M \in \mathbb{Z}_N$): pick $R_3 \leftarrow_{\mathrm{R}} G_{p_3}$; return $\sigma := u^{\frac{1}{\alpha+M}} R_3$ **verify**(pk, M, σ): check $e(g_1^M \cdot g_1^\alpha, \sigma) = e(g_1, u)$

Fig. 3. Fully secure signature scheme, obtained by applying Naor's transformation to the IBE scheme in Fig 2. In asymmetric groups, randomization with R_3 in **sign** is not necessary (i.e., **sign** is deterministic).

3.2 Our IBE Scheme

Theorem 1. *The scheme in Figure 2 is an adaptively secure anonymous IBE under the decisional subgroup assumption in* $\mathbb{G}$.

Proof. Correctness follows readily from the equation

$$e(g_1^{(\alpha+\mathsf{id})s}, u^{\frac{1}{\alpha+\mathsf{id}}} R_3) = e(g_1, u)^s.$$

We show that for any adversary $\mathcal{A}$ that makes at most q queries against the IBE, there exist adversaries $\mathcal{A}_1, \mathcal{A}_2$ whose running times are essentially the same as that of $\mathcal{A}$, such that

$$\mathsf{Adv}_{\mathcal{A}}^{\text{A-IBE}}(\lambda) \leq \mathsf{Adv}_{\mathcal{G},\mathcal{A}_1}^{\text{SD1}}(\lambda) + (q+1) \cdot \mathsf{Adv}_{\mathcal{G},\mathcal{A}_2}^{\text{SD2}}(\lambda) + 2^{-\Omega(\lambda)}$$

We proceed via a series of games and we use Adv_i to denote the advantage of $\mathcal{A}$ in Game i.

Game 0. This is the real experiment from Definition 2.2. We will also make the following simplifying assumptions:

- We never encounter an identity id such that id $= \alpha \bmod p_1$; such an identity constitutes the discrete log of g_1^α and trivially breaks the subgroup assumption.
- The adversary's queries $\mathsf{id}_1, \ldots, \mathsf{id}_q \in \mathbb{Z}_N$ are distinct, since we can perfectly randomize the secret key $\mathsf{sk}_{\mathsf{id}} = u^{\frac{1}{\alpha+\mathsf{id}}} R_3$ given g_3 (we can add g_3 to mpk without affecting the security proof).
- $\mathsf{id}_1, \ldots, \mathsf{id}_q$ are distinct mod p_2; given $\mathsf{id}_i \neq \mathsf{id}_j \in \mathbb{Z}_N$ such that $\mathsf{id}_i = \mathsf{id}_j \bmod p_2$, computing $\gcd(\mathsf{id}_i - \mathsf{id}_j, N)$ would allow us to factor N.

We can incorporate these simplifying assumptions by introducing an extra hybrid before Game 1 that aborts if the first or third condition is violated, and uses randomization to handle repeated key queries.

Game 1. We change $(\mathsf{ct}_0, \kappa_0) \leftarrow_{\mathrm{R}} \mathsf{Enc}(\mathsf{mpk}, \mathsf{id}^*)$ as follows: pick $C \leftarrow_{\mathrm{R}} G_{p_1}$, output

$$(\mathsf{ct}_0, \kappa_0) := (C, H(e(C, \mathsf{sk}_{\mathsf{id}^*}))).$$

We claim that $\mathsf{Adv}_0 = \mathsf{Adv}_1$. This follows readily from the following two observations:

i. for all id, $e(g_1, u)^s = e(g_1^{(\alpha+\mathsf{id})s}, u^{\frac{1}{\alpha+\mathsf{id}}}) = e(g_1^{(\alpha+\mathsf{id})s}, \mathsf{sk}_{\mathsf{id}})$;

ii. if $\alpha + \mathsf{id} \neq 0$, $g_1^{(\alpha+\mathsf{id})s}$ and C are identically distributed.

Game 2. We change the distribution of C in $(\mathsf{ct}_0, \kappa_0)$ from $C \leftarrow_{\mathrm{R}} G_{p_1}$ to $C \leftarrow_{\mathrm{R}} G_{p_1} G_{p_2}$. We now construct $\mathcal{A}_1$ for which

$$\mathsf{Adv}_0 - \mathsf{Adv}_1 \leq \mathsf{Adv}^{\mathrm{SD1}}_{\mathcal{G},\mathcal{A}_1}(\lambda).$$

$\mathcal{A}_1$ on input (g_1, g_3, C) where either $C \leftarrow_{\mathrm{R}} G_{p_1}$ or $C \leftarrow_{\mathrm{R}} G_{p_1} G_{p_2}$, simulates the experiment in Game 1 with the adversary $\mathcal{A}$ as follows: runs $\mathsf{Setup}(\mathbb{G})$ honestly to obtain (α, u), then uses (α, u) to answer all key queries honestly and to compute (ct, κ_0) as $(C, H(e(C, \mathsf{sk}_{\mathsf{id}^*})))$.

Game 3. We change the distribution of $\mathsf{sk}_{\mathsf{id}}$ from $u^{\frac{1}{\alpha+\mathsf{id}}} R_3$ to $u^{\frac{1}{\alpha+\mathsf{id}}} g_2^{\sum_{i=1}^{q+1} \frac{r_i}{\alpha_i+\mathsf{id}}} R_3$, where $r_1, \ldots, r_{q+1}, \alpha_1, \ldots, \alpha_{q+1} \leftarrow_{\mathrm{R}} \mathbb{Z}_N$, as outlined in Section 1.1. We proceed via a series of sub-games $3.j.0$ and $3.j.1$ for $j = 1, 2, \ldots, q+1$, where

- In Sub-Game $3.j.0$, $\mathsf{sk}_{\mathsf{id}}$ is given by $u^{\frac{1}{\alpha+\mathsf{id}}} g_2^{\frac{r_j}{\alpha+\mathsf{id}} + \sum_{i=1}^{j-1} \frac{r_i}{\alpha_i+\mathsf{id}}} R_3$;
- In Sub-Game $3.j.1$, $\mathsf{sk}_{\mathsf{id}}$ is given by $u^{\frac{1}{\alpha+\mathsf{id}}} g_2^{\sum_{i=1}^{j} \frac{r_i}{\alpha_i+\mathsf{id}}} R_3$. Game 2 corresponds to Sub-Game 3.0.1, and Game 3 corresponds to Sub-Game $3.q+1.1$.

First, observe that $\mathsf{Adv}_{3.j.0} = \mathsf{Adv}_{3.j.1}$. This follows readily from the fact that $\alpha \bmod p_2$ is completely hidden given mpk and the challenge ciphertext, and therefore we may replace $\alpha \bmod p_2$ with $\alpha_j \bmod p_2$. Next, for $j = 1, \ldots, q+1$, we construct $\mathcal{A}_2$ for which

$$\mathsf{Adv}_{3.(j-1).1} - \mathsf{Adv}_{3.j.0} \leq \mathsf{Adv}^{\mathrm{SD2}}_{\mathcal{G},\mathcal{A}_2}(\lambda).$$

$\mathcal{A}_2$ on input $(\mathbb{G}, g_1, g_{\{2,3\}}, g_3, C, T)$ where $C \leftarrow_{\mathrm{R}} G_{p_1} G_{p_2}$ and either $T = uR_3 \leftarrow_{\mathrm{R}} G_{p_1} G_{p_3}$ or $T = ug_2^{r_j} R_3 \leftarrow_{\mathrm{R}} G_{p_1} G_{p_2} G_{p_3}$, simulates the experiment in Game 3 with the adversary $\mathcal{A}$ as follows:

- picks $\alpha \leftarrow_{\mathrm{R}} \mathbb{Z}_N$ and publishes $\mathsf{mpk} := (g_1, g_1^{\alpha}, e(g_1, T), H)$, where $e(g_1, T) = e(g_1, u)$;
- picks $\alpha_1, \ldots, \alpha_{j-1}, r_1, \ldots, r_{j-1} \leftarrow_{\mathrm{R}} \mathbb{Z}_N$;
- simulates KeyGen on input id by choosing $R_3' \leftarrow_{\mathrm{R}} G_{p_3}$ and outputting $T^{\frac{1}{\alpha+\mathsf{id}}} g_{2,3}^{\sum_{i=1}^{j-1} \frac{r_i}{\alpha_i+\mathsf{id}}} R_3'$
- uses C to compute $(\mathsf{ct}_0, \kappa_0)$;

Observe that if $T = uR_3$, then this is exactly Game $3.j-1.1$, and if $T = ug_2^{r_j} R_3$, then this is exactly Game $3.j.0$. It follows readily that

$$\mathsf{Adv}_2 - \mathsf{Adv}_3 \leq (q+1) \cdot \mathsf{Adv}^{\mathrm{SD2}}_{\mathcal{G},\mathcal{A}_2}(\lambda).$$

Game 4. We replace $\sum_{i=1}^{q+1} \frac{r_i}{\alpha_i+\mathsf{id}}$ in $\mathsf{sk}_{\mathsf{id}}$ with $\mathsf{RF}(\mathsf{id})$ where $\mathsf{RF} : \mathbb{Z}_N \to \mathbb{Z}_{p_2}$ is a truly random function; that is, $\mathsf{sk}_{\mathsf{id}}$ is now given by $u^{\frac{1}{\alpha+\mathsf{id}}} g_2^{\mathsf{RF}(\mathsf{id})} R_3$. It follows readily from Lemma 1 that

$$\mathsf{Adv}_3 - \mathsf{Adv}_4 \leq O(q^2/p_2).$$

$\underline{\mathsf{Setup}(\mathbb{G})}$: $\mathsf{msk} := (\mathbf{W}, \mathbf{u}) \leftarrow_{\mathrm{R}} \mathbb{Z}_p^{(k+1)\times(k+1)} \times \mathbb{Z}_p^k$; $\mathsf{mpk} := ([\mathbf{A}]_1, [\mathbf{A}^\top \mathbf{W}]_1, [\mathbf{A}^\top \mathbf{Bu}]_T)$; return $(\mathsf{mpk}, \mathsf{msk})$ $\underline{\mathsf{KeyGen}(\mathsf{msk}, \mathsf{id} \in \mathbb{Z}_p)}$: return $\mathsf{sk}_{\mathsf{id}} := [(\mathbf{W} + \mathsf{id}\mathbf{I}_{k+1})^{-1}\mathbf{Bu}]_2$	$\underline{\mathsf{Enc}(\mathsf{mpk}, \mathsf{id} \in \mathbb{Z}_p)}$: pick $\mathbf{s} \leftarrow_{\mathrm{R}} \mathbb{Z}_p^k$; return $(\mathsf{ct}, \kappa) := ([\mathbf{s}^\top \mathbf{A}^\top (\mathbf{W} + \mathsf{id}\mathbf{I}_{k+1})]_1, [\mathbf{s}^\top \mathbf{A}^\top \mathbf{Bu}]_T)$; $\underline{\mathsf{Dec}(\mathsf{sk}_{\mathsf{id}}, \mathsf{ct})}$: return $e(\mathsf{ct}, \mathsf{sk}_{\mathsf{id}})$

Fig. 4. Candidate IBE in prime-order bilinear groups under the k-LIN assumption, following the Diffie-Hellman framework and notation in [12]. Here, $\mathbf{A}, \mathbf{B} \in \mathbb{Z}_p^{k\times(k+1)}$ denote the matrices for the k-LIN assumptions in G_1 and G_2 respectively. Both the keys and the ciphertext contain $k+1$ group elements, i.e. 2 elements under SXDH = 1-LIN.

Game 5. We replace $\kappa_0 = \mathsf{H}(e(C, \mathsf{sk}_{\mathsf{id}^*}))$ with $\kappa_0 \leftarrow_{\mathrm{R}} \{0,1\}^\lambda$. Observe that the quantity (from which κ_0 is derived)

$$e(C, \mathsf{sk}_{\mathsf{id}^*}) = e(C, u^{\frac{1}{\alpha+\mathsf{id}^*}} g_2^{\mathsf{RF}(\mathsf{id}^*)}) = e(C, u^{\frac{1}{\alpha+\mathsf{id}^*}}) \cdot \boxed{e(C, g_2^{\mathsf{RF}(\mathsf{id}^*)})}$$

has $\log p_2 = \Theta(\lambda)$ bits of min-entropy coming from $\mathsf{RF}(\mathsf{id}^*)$, since $\mathsf{id}^* \notin \{\mathsf{id}_1, \ldots, \mathsf{id}_q\}$; this holds as long as the G_{p_2}-component of C is not 1, which happens with probability $1 - 1/p_2$. Then, by the left-over hash lemma, $\kappa_0 = \mathsf{H}(e(C, \mathsf{sk}_{\mathsf{id}^*}))$ is $2^{-\Omega(\lambda)}$-close to the uniform distribution over $\{0,1\}^\lambda$, even given $\mathsf{ct}_0 = C$.

In Game 5, the joint distribution of $(\kappa_0, \mathsf{ct}_0)$ is uniformly random over $\{0,1\}^\lambda \times \mathcal{C}$, where $\mathcal{C} := G_{p_1} G_{p_2}$. Therefore, the view of the adversary $\mathcal{A}$ is statistically independent of the challenge bit b. Hence, $\mathsf{Adv}_5 = 0$. This completes the proof. □

3.3 A Candidate Prime-order Scheme

In Fig 4, we present a *candidate* prime-order scheme obtained by applying the transformation in [11] to our composite-order IBE scheme; concretely, the transformation was used to obtain prime-order dual-system ABE schemes starting from composite-order ones based on the same decisional subgroup assumptions as used in this work. The ciphertext and secret keys in the candidate scheme contain $k+1$ group elements, which is a substantial improvement over the state-of-the-art. Applying Naor's transformation then yields a signature scheme with signature size $k+1$ group elements. In contrast, a scheme that uses both the $(p_1 \mapsto p_1 p_2)$-subgroup and $(p_2 \mapsto p_1 p_2)$-subgroup assumptions as in [10] would likely require at least $2k+1$ group elements, which is another reason to eliminate the use of the $(p_2 \mapsto p_1 p_2)$-subgroup assumption.

We stress that we do not have a proof of security for this scheme. The main technical difficulties arise from having to understand the matrix inverse $(\mathbf{W} + \mathsf{id}\mathbf{I}_{k+1})^{-1}$ for general matrices $\mathbf{W}$. For this specific scheme, it appears that we can completely recover $\mathbf{W} \in \mathbb{Z}_p^{k\times k}$ given $(\mathbf{W} + \mathsf{id}\mathbf{I}_{k+1})^{-1}\mathbf{B} \in \mathbb{Z}_p^k$ for many choices of id, which ruins parameter-hiding in the secret key space. On the other hand, in the composite-order scheme, given $\frac{1}{\alpha+\mathsf{id}} \bmod p_1$ for an unbounded number of id still completely hides $\alpha \bmod p_2$. Nonetheless, we conjecture that a more judicious choice of a matrix distribution for $\mathbf{W}$ would yield a variant of this scheme which is adaptively secure under the k-linear assumption. We quickly point out here that diagonal matrices don't work.

4 Broadcast Encryption

In broadcast encryption [13], a sender broadcasts encrypted content in such a way that only a specified set of authorized receivers may decrypt the message. In this section, we present a selectively secure broadcast encryption scheme for n users, where the ciphertext overhead and the secret keys are a constant number of group elements, and security is based on the decisional subgroup assumption in composite-order groups. Previous dual-system broadcast encryption schemes [17, 25, 15] achieve adaptive security under static assumptions, but never better than a $(t, n/t)$-type trade-off between ciphertext overhead and key size.

4.1 Overview

We begin with an informal description of the scheme, ignoring randomization in the G_{p_3}-subgroup. The scheme is derived from the Boneh-Gentry-Waters (BGW) broadcast encryption scheme [6], which is also selectively secure under the q-DBDHE assumption. The public parameters in our scheme are given by

$$\mathsf{mpk} := (g_1^{\gamma}, g_1^{\alpha}, g_1^{\alpha^2}, \ldots, g_1^{\alpha^n}, u^{\alpha}, u^{\alpha^2}, \ldots, u^{\alpha^n}, u^{\alpha^{n+2}}, \ldots, u^{\alpha^{2n}})$$

The ciphertext for a subset $\Gamma \subseteq [n]$ and the key for a user $y \in [n]$ are given by

$$\mathsf{ct}_\Gamma := (g_1^s, g_1^{(\gamma+\sum_{k\in\Gamma}\alpha^k)s}, e(g_1, u^{\alpha^{n+1}})^s \cdot m),\ \mathsf{sk}_y := u^{\alpha^{n-y+1}\gamma}$$

Decryption proceeds analogously to the BGW scheme, and requires a judicious choice of pairing-product equation to recover $e(g_1, u^{\alpha^{n+1}})^s$. We note that $u^{\alpha^{n+1}}$ is omitted from mpk. Indeed, given g_1^s and mpk, it is easy to compute $e(g_1, u^{\alpha^k})^s$ for any $k \neq n+1$. We also note that the BGW scheme uses $u = g_1$.

To establish security, we will introduce random G_{p_2}-components to the $2n$ terms $u^{\alpha}, u^{\alpha^2}, \ldots, u^{\alpha^{2n}}$ (including $u^{\alpha^{n+1}}$), and the extra entropy from $u^{\alpha^{n+1}}$ will be used to hide the message m. That is, we apply the Deja Q framework to the set of $2n$ linearly independent monomials $\{\alpha, \alpha^2, \ldots, \alpha^{2n}\}$, as encoded "in the exponent of u" in the secret keys. To achieve this, we proceed as follows:

$$\begin{array}{cccccc}
u^{\alpha^k} & \overset{\text{subgroup}}{\longrightarrow} & u^{\alpha^k} g_2^{r_1\alpha^k} & \overset{\text{CRT}}{\longrightarrow} & u^{\alpha^k} g_2^{r_1\alpha_1^k} \\
 & \overset{\text{subgroup}}{\longrightarrow} & u^{\alpha^k} g_2^{r_2\alpha^k} g_2^{r_1\alpha_1^k} & \overset{\text{CRT}}{\longrightarrow} & u^{\alpha^k} g_2^{r_2\alpha_2^k + r_1\alpha_1^k} \\
 & \longrightarrow & \cdots & \overset{\text{CRT}}{\longrightarrow} & u^{\alpha^k} g_2^{r_{2n}\alpha_{2n}^k + \cdots + r_2\alpha_2^k + r_1\alpha_1^k}
\end{array}$$

where $r_1, \ldots, r_{2n}, \alpha_1, \ldots, \alpha_{2n} \leftarrow_{\mathrm{R}} \mathbb{Z}_N$. We can then replace

$$k \mapsto r_{2n}\alpha_{2n}^k + \cdots + r_2\alpha_2^k + r_1\alpha_1^k$$

by a truly random function $\mathsf{RF}(\cdot)$. As with the IBE scheme, we need to avoid leaking $\alpha \bmod p_2$ in the ciphertext in order to carry out the transformation to the secret keys above. That is, we need to eliminate all occurrences of α in the polynomial $\gamma + \sum_{k\in\Gamma}\alpha^k$ which shows up in the ciphertext. Unfortunately, we do not know a transformation to the ciphertext distribution analogous to that for the IBE. Instead, we will need to settle for selective security where the adversary announces the subset Γ at the very beginning, so that we can use γ as a one-time pad. We will then select $\tilde{\gamma}$ at random (which is treated as a known scalar) and program γ so that $\tilde{\gamma} = \gamma + \sum_{k\in\Gamma}\alpha^k$. We can then rewrite the ciphertext and key as

$$\mathsf{ct}_\Gamma := (g^s, g^{\tilde{\gamma}s}, e(g, u^{\alpha^{n+1}})^s \cdot m),\ \mathsf{sk}_y := (u^{\alpha^{n-y+1}\tilde{\gamma} - \sum_{k\in\Gamma}\alpha^{n+1-y+k}})$$

Now, the monomials in α only show up on the same side of the pairing in both the ciphertext and the secret keys in the exponents of u. As in the security proof for the BGW scheme, we will later use the

Setup$(\mathbb{G}, 1^n)$:	$\mathsf{Enc}(\mathsf{mpk}, \Gamma \subseteq [n])$:
$(\alpha,\gamma,u) \leftarrow_{\mathrm{R}} \mathbb{Z}_N^2 \times G_{p_1}$; pick $R'_{3,k} \leftarrow_{\mathrm{R}} G_{p_3}$; $u'_k := u^{\alpha^k} R_{3,k}$, for $k = 1,\ldots,2n$; pick $R_{3,y} \leftarrow_{\mathrm{R}} G_{p_3}$; $\mathsf{sk}_y := u^{\alpha^{n-y+1}\gamma} R_{3,y}$, for $y = 1,\ldots,n$; $\mathsf{mpk} := (g_1, g_1^{\gamma}, e(g_1, u'_{n+1}), \mathsf{H},$ $g_1^{\alpha},\ldots,g_1^{\alpha^n},$ $u'_1, u'_2,\ldots,u'_n, u'_{n+2},\ldots,u'_{2n})$; return $(\mathsf{mpk}, (\mathsf{sk}_1,\ldots,\mathsf{sk}_n))$	pick $s \leftarrow_{\mathrm{R}} \mathbb{Z}_N$; $\mathsf{ct}_\Gamma := (g_1^s, g_1^{(\gamma+\sum_{k\in\Gamma}\alpha^k)s})$; $\kappa := \mathsf{H}(e(g_1, u^{\alpha^{n+1}})^s)$; return $(\mathsf{ct}_\Gamma, \kappa)$ $\mathsf{Dec}(\mathsf{mpk}, \mathsf{sk}_y, \mathsf{ct}_\Gamma = (c_0, c_1))$: $\kappa' := e(c_1, u'_{n-y+1}) \cdot e(c_0, \mathsf{sk}_y \prod_{k\in\Gamma, k\neq y} u'_{n+1+(k-y)})$; return $\mathsf{H}(\kappa')$

Fig. 5. Broadcast encryption w.r.t. a composite-order bilinear group $\mathbb{G}$. Here, $\mathsf{H} : G_T \to \{0,1\}^\lambda$ is drawn from a family of pairwise-independent hash functions.

fact that the monomial α^{n+1} does not show up in any sk_y for which $y \notin \Gamma$. We note that in the proof of security, the distribution of mpk changes, which is quite unusual for a proof based on the dual system methodology.

4.2 Our broadcast encryption scheme

Theorem 2. *The scheme in Figure 5 is a selectively secure broadcast encryption scheme under the decisional subgroup assumption in* $\mathbb{G}$.

Proof. Correctness follows readily from the fact that for all $y \in \Gamma$,

$$e\big(g_1^{(\gamma+\sum_{k\in\Gamma}\alpha^k)s}, u^{\alpha^{n-y+1}}\big) \cdot e\big(g_1^s, u^{\alpha^{n-y+1}\gamma} \prod_{k\in\Gamma, k\neq y} u^{\alpha^{n+1+(k-y)}}\big) = e(g_1, u^{\alpha^{n+1}})^s.$$

Note that for all $k \neq y$, $n+1+(k-y) \in \{2,\ldots,n,n+2,\ldots,2n\}$, which means we can compute $u^{\alpha^{n+1+(k-y)}}$ given mpk. Next, we show that for any adversary $\mathcal{A}$ against the broadcast encryption scheme, there exist adversaries $\mathcal{A}_1, \mathcal{A}_2$ whose running times are essentially the same as that of $\mathcal{A}$, such that

$$\mathsf{Adv}_{\mathcal{A}}^{\text{S-BCE}}(\lambda) \leq \mathsf{Adv}_{\mathcal{G},\mathcal{A}_1}^{\text{SD1}}(\lambda) + 2n \cdot \mathsf{Adv}_{\mathcal{G},\mathcal{A}_2}^{\text{SD2}}(\lambda) + 2^{-\Omega(\lambda)}$$

We proceed via a series of games and we use Adv_i to denote the advantage of $\mathcal{A}$ in Game i.

Game 0. This is the real experiment from Definition 2.3.

Game 1. Pick $(\alpha, \tilde{\gamma}, u) \leftarrow_{\mathrm{R}} \mathbb{Z}_N^2 \times G_{p_1}$ and set $\gamma := \tilde{\gamma} - \sum_{k\in\Gamma^*} \alpha^k$, where Γ^* is the selective challenge output by $\mathcal{A}$. Then,

- compute $u'_1,\ldots,u'_{2n}$ as in the honest Setup;
- compute mpk as in the honest Setup.
- compute $\mathsf{ct}_{\Gamma^*} = (g_1^s, (g_1^s)^{\tilde{\gamma}})$ and $\kappa_0 = \mathsf{H}(e(g_1^s, u'_{n+1}))$;
- simulate $\{\mathsf{sk}_y : y \notin \Gamma^*\}$ using $\tilde{\gamma}$ and $(u'_1,\ldots,u'_n, u'_{n+2},\ldots,u'_{2n})$, by computing

$$\mathsf{sk}_y = (u'_{n-y+1})^{\tilde{\gamma}} \cdot \big(\prod_{k\in\Gamma^*, k\neq y} u'_{n+1+(k-y)}\big)^{-1} \cdot R_{3,y}$$

Clearly, Game 0 and 1 are identically distributed, so $\mathsf{Adv}_0 = \mathsf{Adv}_1$.

Game 2. We change the distribution of $(\mathsf{ct}_{\Gamma^*}, \kappa_0)$ by replacing g_1^s with $C \leftarrow_R G_{p_1} G_{p_2}$, that is

$$(\mathsf{ct}_{\Gamma^*}, \kappa_0) := ((C, C^{\tilde{\gamma}}), \mathsf{H}(e(C, u'_{n+1}))$$

It is straight-forward to construct $\mathcal{A}_1$ (following the proof for Theorem 1) for which

$$\mathsf{Adv}_1 - \mathsf{Adv}_2 \le \mathsf{Adv}^{\mathrm{SD1}}_{\mathcal{G},\mathcal{A}_1}(\lambda).$$

Game 3. We change the distribution of $u'_1, \ldots, u'_{2n}$ from $u^{\alpha^k} R'_{3,k}$ to $u^{\alpha^k} g_2^{\sum_{i=1}^{2n} r_i \alpha_i^k} R'_{3,k}$, where $r_1, \ldots, r_{2n}, \alpha_1, \ldots, \alpha_{2n} \leftarrow_R \mathbb{Z}_N$, as outlined in Section 4.1; this in turn affects the distribution of mpk, κ_0 and $\{\mathsf{sk}_y : y \notin \Gamma^*\}$. We proceed via a series of sub-games $3.j.0$ and $3.j.1$ for $j = 1, 2, \ldots, 2n$, where

- In Sub-Game $3.j.0$, u'_k is given by $u^{\alpha^k} g_2^{r_j \alpha^k + \sum_{i=1}^{j-1} r_i \alpha_i^k} R'_{3,k}$ for $k = 1, \ldots, 2n$;
- In Sub-Game $3.j.1$, u'_k is given by $u^{\alpha^k} g_2^{\sum_{i=1}^{j} r_i \alpha_i^k} R'_{3,k}$ for $k = 1, \ldots, 2n$. Game 2 corresponds to Sub-Game $3.0.1$, and Game 3 corresponds to Sub-Game $3.2n.1$.

First, observe that $\mathsf{Adv}_{3.j.0} = \mathsf{Adv}_{3.j.1}$ as before. Next, for $j = 1, \ldots, 2n$, we construct $\mathcal{A}_2$ for which

$$\mathsf{Adv}_{3.(j-1).1} - \mathsf{Adv}_{3.j.0} \le \mathsf{Adv}^{\mathrm{SD2}}_{\mathcal{G},\mathcal{A}_2}(\lambda).$$

$\mathcal{A}_2$ on input $(g_1, g_{\{2,3\}}, g_3, C, T)$ where $C \leftarrow_R G_{p_1} G_{p_2}$ and either $T = u R'_{3,k} \leftarrow_R G_{p_1} G_{p_3}$ or $T = u g_2^{r_j} R'_{3,k} \leftarrow_R G_{p_1} G_{p_2} G_{p_3}$, simulates the experiment in Game 2 with the adversary $\mathcal{A}$ as follows:

- picks $\alpha, \alpha_1, \ldots, \alpha_{j-1}, r_1, \ldots, r_{j-1} \leftarrow_R \mathbb{Z}_N$;
- for $k = 1, \ldots, 2n$, computes u'_k by choosing $R'_{3,k} \leftarrow_R G_{p_3}$ and outputting $T^{\alpha^k} g_{2,3}^{\sum_{i=1}^{j-1} r_i \alpha_i^k} R'_{3,k}$
- proceed as in Game 2 using $\alpha, u'_1, \ldots, u'_{2n}$ as computed above to compute mpk and $\{\mathsf{sk}_y : y \notin \Gamma^*\}$, and using C as provided and u'_{n_1} as computed above to compute $(\mathsf{ct}_{\Gamma^*}, \kappa_0)$.

Observe that if $T = u R'_{3,k}$, then this is exactly Game $3.j-1.1$, and if $T = u g_2^{r_j} R'_{3,k}$, then this is exactly Game $3.j.0$. It follows readily that

$$\mathsf{Adv}_2 - \mathsf{Adv}_3 \le 2n \cdot \mathsf{Adv}^{\mathrm{SD2}}_{\mathcal{G},\mathcal{A}_2}(\lambda).$$

Game 4. We replace $\sum_{i=1}^{2n} r_i \alpha_i^k$ in u'_k with $\mathsf{RF}(k)$ where $\mathsf{RF} : [2n] \to \mathbb{Z}_{p_2}$ is a truly random function; that is, u'_k is now given by $u^{\alpha^k} g_2^{\mathsf{RF}(k)} R'_{3,k}$, for $k = 1, \ldots, 2n$. Now, we exploit the fact that the Vandermonde matrix

$$\begin{pmatrix} \alpha_1 & \alpha_2 & \cdots & \alpha_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_1^{2n} & \alpha_2^{2n} & \cdots & \alpha_{2n}^{2n} \end{pmatrix}$$

is invertible as long as $\alpha_1, \ldots, \alpha_{2n} \bmod p_2$ are distinct, which happens with overwhelming probability over $\alpha_1, \ldots, \alpha_{2n} \leftarrow_R \mathbb{Z}_N$. It follows readily that

$$\mathsf{Adv}_3 - \mathsf{Adv}_4 \le O(n^2 / p_2).$$

Game 5. We replace $\kappa_0 = \mathsf{H}(e(C, u'_{n+1}))$ with $\kappa_0 \leftarrow_R \{0,1\}^\lambda$. First, recall from Game 1 that $\{\mathsf{sk}_y : y \notin \Gamma^*\}$ only depend on $u'_1, \ldots, u'_n, u'_{n+2}, \ldots, u'_{2n}$; therefore, they only depend on $\mathsf{RF}(1), \ldots, \mathsf{RF}(n), \mathsf{RF}(n+2), \ldots, \mathsf{RF}(2n)$ and do not reveal any information about $\mathsf{RF}(n+1)$. Then, the quantity (from which κ_0 is derived)

$$e(C, u'_{n+1}) = e(C, u^{\alpha^{n+1}} g_2^{\mathsf{RF}(n+1)}) = e(C, u^{\alpha^{n+1}}) \cdot \boxed{e(C, g_2^{\mathsf{RF}(n+1)})}$$

has $\log p_2 = \Theta(\lambda)$ bits of min-entropy coming from $\mathsf{RF}(n+1)$; this holds as long as the G_{p_2}-component of C is not 1, which happens with probability $1-1/p_2$. Then, by the left-over hash lemma, $\kappa_0 = \mathsf{H}(e(C, u'_{n+1}))$ is $2^{-\Omega(\lambda)}$-close to the uniform distribution over $\{0,1\}^\lambda$.

In Game 5, both κ_0, κ_1 are uniformly random over $\{0,1\}^\lambda$. Therefore, the view of the adversary $\mathcal{A}$ is statistically independent of the challenge bit b. Hence, $\mathsf{Adv}_5 = 0$. This completes the proof. $\square$

Acknowledgments. I would like to thank Allison Bishop, Dan Boneh, Melissa Chase, Jie Chen, Sarah Meiklejohn and Alain Passelègue for helpful discussions.

References

[1] N. Attrapadung. Dual system encryption via doubly selective security: Framework, fully secure functional encryption for regular languages, and more. In *EUROCRYPT*, pages 557–577, 2014.

[2] O. Blazy, E. Kiltz, and J. Pan. (Hierarchical) identity-based encryption from affine message authentication. In *CRYPTO*, pages 408–425, 2014.

[3] D. Boneh and X. Boyen. Short signatures without random oracles. In *EUROCRYPT*, pages 56–73, 2004.

[4] D. Boneh and X. Boyen. Efficient selective-ID secure identity-based encryption without random oracles. In *EUROCRYPT*, pages 223–238, 2004.

[5] D. Boneh and M. K. Franklin. Identity-based encryption from the Weil pairing. *SIAM J. Comput.*, 32(3):586–615, 2003.

[6] D. Boneh, C. Gentry, and B. Waters. Collusion resistant broadcast encryption with short ciphertexts and private keys. In *CRYPTO*, pages 258–275, 2005.

[7] D. Boneh, E.-J. Goh, and K. Nissim. Evaluating 2-DNF formulas on ciphertexts. In *TCC*, pages 325–341, 2005.

[8] X. Boyen. General *Ad Hoc* encryption from exponent inversion IBE. In *EUROCRYPT*, pages 394–411, 2007.

[9] A. D. Caro, V. Iovino, and G. Persiano. Fully secure anonymous HIBE and secret-key anonymous IBE with short ciphertexts. In *Pairing-Based Cryptography - Pairing 2010*, pages 347–366, 2010.

[10] M. Chase and S. Meiklejohn. Déjà Q: using dual systems to revisit q-type assumptions. In *EUROCRYPT*, pages 622–639, 2014. Cryptology ePrint Archive, Report 2014/570.

[11] J. Chen, R. Gay, and H. Wee. Improved dual system ABE in prime-order groups via predicate encodings. In *Eurocrypt*, pages 595–624, 2015.

[12] A. Escala, G. Herold, E. Kiltz, C. Ràfols, and J. Villar. An algebraic framework for Diffie-Hellman assumptions. In *CRYPTO (2)*, pages 129–147, 2013.

[13] A. Fiat and M. Naor. Broadcast encryption. In *CRYPTO*, pages 480–491, 1993.

[14] D. M. Freeman. Converting pairing-based cryptosystems from composite-order groups to prime-order groups. In *EUROCRYPT*, pages 44–61, 2010.

[15] S. Garg, A. Kumarasubramanian, A. Sahai, and B. Waters. Building efficient fully collusion-resilient traitor tracing and revocation schemes. In *ACM Conference on Computer and Communications Security*, pages 121–130, 2010.

[16] C. Gentry. Practical identity-based encryption without random oracles. In *EUROCRYPT*, pages 445–464, 2006.

[17] C. Gentry and B. Waters. Adaptive security in broadcast encryption systems (with short ciphertexts). In *EUROCRYPT*, pages 171–188, 2009.

[18] J. Katz, A. Sahai, and B. Waters. Predicate encryption supporting disjunctions, polynomial equations, and inner products. In *EUROCRYPT*, pages 146–162, 2008.

[19] A. B. Lewko. Tools for simulating features of composite order bilinear groups in the prime order setting. In *EUROCRYPT*, pages 318–335, 2012. Also Cryptology ePrint Archive, Report 2011/490.

[20] A. B. Lewko and B. Waters. New techniques for dual system encryption and fully secure HIBE with short ciphertexts. In *TCC*, pages 455–479, 2010.

[21] A. B. Lewko, T. Okamoto, A. Sahai, K. Takashima, and B. Waters. Fully secure functional encryption: Attribute-based encryption and (hierarchical) inner product encryption. In *EUROCRYPT*, pages 62–91, 2010.

[22] T. Okamoto and K. Takashima. Hierarchical predicate encryption for inner-products. In *ASIACRYPT*, pages 214–231, 2009.

[23] R. Sakai and M. Kasahara. ID based cryptosystems with pairing on elliptic curve. Cryptology ePrint Archive, Report 2003/054, 2003.

[24] A. Shamir. Identity-based cryptosystems and signature schemes. In *CRYPTO*, pages 47–53, 1984.

[25] B. Waters. Dual system encryption: Realizing fully secure IBE and HIBE under simple assumptions. In *CRYPTO*, pages 619–636, 2009.

[26] H. Wee. Dual system encryption via predicate encodings. In *TCC*, pages 616–637, 2014.

[27] T. H. Yuen, S. S. Chow, C. Zhang, and S. M. Yiu. Exponent-inversion signatures and IBE under static assumptions. Cryptology ePrint Archive, Report 2014/311, 2014.

A Asymmetric Composite-Order Bilinear Groups

In this section, we outline the extension of our result to asymmetric composite-order bilinear groups. Here, we can work with groups whose group order is the product of two primes, and we obtain IBE and signature schemes (shown in Fig 6 and 7) where the key generation and signing algorithms are deterministic. We state the underlying decisional subgroup assumptions, and the proofs are exactly analogously to the ones from before.

Asymmetric composite-Order bilinear groups. The generator $\mathcal{G}$ takes as input a security parameter λ and outputs a description $\mathbb{G} := (N, G, H, G_T, e)$, where N is product of distinct primes of $\Theta(\lambda)$ bits, G, H and G_T are cyclic groups of order N, and $e : G \times H \to G_T$ is a non-degenerate bilinear map. We consider bilinear groups where N is the product of two distinct primes p_1, p_2 (that is, $N = p_1 p_2$). We can write $G = G_{p_1} G_{p_2}$ where G_{p_1}, G_{p_2} are subgroups of G of order p_1 and p_2 respectively. In addition, we use $G^*_{p_i}$ to denote $G_{p_i} \setminus \{1\}$. We will often write g_1, g_2 to denote random generators for the subgroups G_{p_1}, G_{p_2}. We can also write $H = H_{p_1} H_{p_2}$, where $H_{p_1}, H_{p_2}, h_1, h_2$ are defined analogously.

Cryptographic assumptions. Our construction relies on the following two subgroup decisional assumptions. We define the following two advantage functions:

$$
\begin{aligned}
&\mathsf{Adv}^{\mathrm{SD1}}_{\mathcal{G},\mathcal{A}}(\lambda) := |\Pr[\mathcal{A}(D, T_0) = 1] - \Pr[\mathcal{A}(D, T_1) = 1]| \\
&\quad \text{where } \mathbb{G} \leftarrow \mathcal{G}, T_0 \leftarrow \boxed{G_{p_1}}, T_1 \leftarrow_{\mathrm{R}} \boxed{G_{p_1} G_{p_2}} \\
&\qquad \text{and } D := (g_1, g_{\{1,2\}}, h_1, h_{\{1,2\}}), g_1 \leftarrow_{\mathrm{R}} G^*_{p_1}, g_{\{1,2\}} \leftarrow_{\mathrm{R}} G_{p_1} G_{p_2}, \\
&\qquad\quad h_1 \leftarrow_{\mathrm{R}} H^*_{p_1}, h_{\{1,2\}} \leftarrow_{\mathrm{R}} H_{p_1} H_{p_2} \\
&\mathsf{Adv}^{\mathrm{SD2}}_{\mathcal{G},\mathcal{A}}(\lambda) := |\Pr[\mathcal{A}(D, T_0) = 1] - \Pr[\mathcal{A}(D, T_1) = 1]| \\
&\quad \text{where } \mathbb{G} \leftarrow \mathcal{G}, T_0 \leftarrow \boxed{H_{p_1}}, T_1 \leftarrow_{\mathrm{R}} \boxed{H_{p_1} H_{p_2}} \\
&\qquad \text{and } D := (h_1, h_2, h_{\{1,2\}}, g_1, g_{\{1,2\}}), h_1 \leftarrow_{\mathrm{R}} H^*_{p_1}, h_2 \leftarrow_{\mathrm{R}} H^*_{p_2}, \\
&\qquad\quad h_{\{1,2\}} \leftarrow_{\mathrm{R}} H_{p_1} H_{p_2}, g_1 \leftarrow_{\mathrm{R}} G^*_{p_1}, g_{\{1,2\}} \leftarrow_{\mathrm{R}} G_{p_1} G_{p_2}
\end{aligned}
$$

The decisional subgroup assumptions assert that that for all PPT adversaries $\mathcal{A}$, the advantages $\mathsf{Adv}^{\mathrm{SD1}}_{\mathcal{G},\mathcal{A}}(\lambda)$ and $\mathsf{Adv}^{\mathrm{SD2}}_{\mathcal{G},\mathcal{A}}(\lambda)$ are negligible functions in λ.

Remark 1. Note that Assumption 2 is false if the pairing is symmetric (i.e., there exists an efficiently computable isomorphism between G and H) since we can pair with h_2 to distinguish between T_0 and T_1. The term h_2 will play the role of $g_{2,3}$ in the transitions from Game 3.$(j-1)$.1 to 3.j.0 in the proofs of Theorems 1 and 2.

$\underline{\mathsf{Setup}(\mathbb{G})\text{:}}$ $\mathsf{msk} := (\alpha, u) \leftarrow_{\mathrm{R}} \mathbb{Z}_N \times H_{p_1}$; $\mathsf{mpk} := (g_1, g_1^{\alpha}, e(g_1, u), \mathsf{H})$; return $(\mathsf{mpk}, \mathsf{msk})$ $\underline{\mathsf{KeyGen}(\mathsf{msk}, \mathsf{id} \in \mathbb{Z}_N)\text{:}}$ return $\mathsf{sk}_{\mathsf{id}} := u^{\frac{1}{\alpha+\mathsf{id}}}$	$\underline{\mathsf{Enc}(\mathsf{mpk}, \mathsf{id} \in \mathbb{Z}_N)\text{:}}$ pick $s \leftarrow_{\mathrm{R}} \mathbb{Z}_N$; return $(\mathsf{ct}, \kappa) := (g_1^{(\alpha+\mathsf{id})s}, \mathsf{H}(e(g_1, u)^s))$ $\underline{\mathsf{Dec}(\mathsf{sk}_{\mathsf{id}}, \mathsf{ct})\text{:}}$ return $\mathsf{H}(e(\mathsf{ct}, \mathsf{sk}_{\mathsf{id}}))$

Fig. 6. Adaptively secure anonymous IBE w.r.t. an asymmetric composite-order bilinear group $\mathbb{G}$. Here, $\mathsf{H} : G_T \to \{0,1\}^{\lambda}$ is drawn from a family of pairwise-independent hash functions.

$\underline{\mathsf{Setup}(\mathbb{G})\text{:}}$ $\mathsf{sk} := (\alpha, u) \leftarrow_{\mathrm{R}} \mathbb{Z}_N \times H_{p_1}$; $\mathsf{pk} := (g_1, g_1^{\alpha}, e(g_1, u))$; return $(\mathsf{pk}, \mathsf{sk})$	$\underline{\textbf{sign}(\mathsf{sk}, M \in \mathbb{Z}_N)\text{:}}$ return $\sigma := u^{\frac{1}{\alpha+M}}$ $\underline{\textbf{verify}(\mathsf{pk}, M, \sigma)\text{:}}$ check $e(g_1^M \cdot g_1^{\alpha}, \sigma) = e(g_1, u)$

Fig. 7. Fully secure signature scheme w.r.t. an asymmetric composite-order bilinear group $\mathbb{G}$.