Attribute-Based Encryption in the Generic Group Model: Automated Proofs and New Constructions

Miguel Ambrona
IMDEA Software Institute, Madrid, Spain
Universidad Politécnica de Madrid, Spain

Gilles Barthe
IMDEA Software Institute, Madrid, Spain

Romain Gay
ENS, Paris, France

Hoeteck Wee
CNRS, France
ENS, Paris, France

ABSTRACT

Attribute-based encryption (ABE) is a cryptographic primitive which supports fine-grained access control on encrypted data, making it an appealing building block for many applications. In this paper, we propose, implement, and evaluate fully automated methods for proving security of ABE in the Generic Bilinear Group Model (Boneh, Boyen, and Goh, 2005, Boyen, 2008), an idealized model which admits simpler and more efficient constructions, and can also be used to find attacks. Our method is applicable to Rational-Fraction Induced ABE, a large class of ABE that contains most of the schemes from the literature, and relies on a Master Theorem, which reduces security in the GGM to a (new) notion of symbolic security, which is amenable to automated verification using constraint-based techniques. We relate our notion of symbolic security for Rational-Fraction Induced ABE to prior notions for Pair Encodings. Finally, we present several applications, including automated proofs for new schemes.

CCS CONCEPTS

•Security and privacy → Mathematical foundations of cryptography; Formal security models; Logic and verification;

KEYWORDS

automated proofs, symbolic security, attribute-based encryption, generic group model

1 INTRODUCTION

Computer-aided cryptography [18] is an emerging approach that advocates using automated tools based on formal methods for analyzing the security of cryptographic schemes and their implementation. The high level of assurance provided by computer-aided cryptography is particularly important for cryptographic schemes that are already deployed in real-world systems, such as RSA-OAEP and TLS, but also for schemes that are required in many applications and hold the promise of widespread deployment. One such example is provided by Attribute-Based Encryption [41, 58], a novel form of public-key encryption. ABE supports fine-grained access control on encrypted data, and has many applications including electronic medical records [9], messaging systems [50], online social networks [15] and information-centric networking [44]. These applications make ABE an ideal application domain for computer-aided cryptography.

Approach. In this paper, we propose, implement, and evaluate automated methods for proving security of ABE in the Generic (Bilinear) Group Model, an idealized model defined in [28, 32] for analyzing the security of cryptographic assumptions and pairing-based schemes. While we do not advocate proving security in the GGM over the standard model, there are several reasons for our approach. First, the GGM captures most algebraic attacks, making automated analysis in the GGM desirable for providing cryptographers early feedback during the design of new constructions. Second, the Generic Group Model often admits schemes that are simpler, more efficient, and ultimately more likely to be deployed in real-world systems. Third, existing proofs of adaptive security of ABE in the standard model are very challenging and full automation remains beyond the state-of-the-art, despite recent progress [24]. In contrast, there exists a promising line of work [10, 20] that develops fully automated tools for proving security in the GGM. Finally, GGM proofs are generally considered to be fairly mechanical and sometimes claims are made without proofs, e.g. [43, footnote 1 (Chapter 6)]; this makes GGM proofs a useful target and test-bed for automated proofs.

Concretely, we introduce the class of Rational-Fraction Induced ABE, which includes many constructions from the literature, and prove for every ABE in this class that their security in the GGM is equivalent to security in a symbolic model, where the experiments are purely algebraic. Then, we introduce a notion of symbolic security for RFI-ABE, and prove that every symbolically secure RFI-ABE is secure in the symbolic model. Leveraging the fact that symbolic security suffices to conclude security of a Rational-Fraction Induced ABE in the GGM, we develop a constraint-solving method for proving symbolic security. Informally, the constraint-solving method can automatically (dis)prove the existence of solutions for systems of (in)equations between rational fractions. We implement the constraint-solving method and use it to evaluate several schemes, including schemes from the literature, various new schemes of independent interest, and some subtly insecure schemes. Our tool finds automated proofs for most constructions, and attacks for the insecure schemes.

CCS'17, Oct. 30–Nov. 3, 2017, Dallas, TX, USA.
© 2016 ACM. ISBN 978-1-4503-4946-8/17/10…$15.00
DOI: https://doi.org/10.1145/3133956.3134088

Our results and tools are specialized to prime order, asymmetric (Type III) bilinear groups, with a pairing function $e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$, where $\mathbb{G}_1$, $\mathbb{G}_2$, and $\mathbb{G}_T$ are prime order groups. This setting is a natural choice to consider because it supports more efficient and compact implementations.

Outline of contributions. For the clarity of exposition, we distinguish between new results about security of ABE in the GGM, and new results about automated proofs in the GGM. However, we stress that our main contribution resides precisely in developing an approach that is rigorously justified and is amenable to automated verification.

ABE. In ABE, ciphertexts are associated with descriptive values x in addition to a plaintext, secret keys are associated with descriptive values y, and a secret key decrypts the ciphertext if and only if $\mathsf{P}(x, y) = 1$ for some boolean predicate P. Here, y together with P may express an arbitrarily complex access policy, which is in stark contrast to traditional public-key encryption, where access is all or nothing. The simplest example of ABE is identity-based encryption (IBE) [29, 39, 59] where x and y are identities and P corresponds to equality. The security requirement for ABE enforces resilience to collusion attacks, namely any group of users holding secret keys for different values learns nothing about the plaintext if none of them is individually authorized to decrypt the ciphertext. This should hold even if the adversary *adaptively* decides which secret keys to ask for, as is inevitable in real-world scenarios.

Following several recent works [12, 63], we focus on schemes where the ciphertext for x is of the form $g_1^{c_x(s,b)}, g_T^{sa} \cdot M$ and the secret key for y is of the form $g_2^{k_y(a,b,r)}$. For correctness, we require that whenever $P(x, y) = 1$, there should exist a degree 2 function of $c_x(S, B), k_y(A, B, R)$ that outputs SA, where S, B, A, R are formal variables corresponding to the inputs s, b, a, r of c_x, k_y; the degree 2 function allows us to compute g_T^{sa} given $g_1^{c_x(s,b)}, g_2^{k_y(a,b,r)}$.

We propose ABE schemes based on encodings c_x, k_y defined in terms of rational fractions of polynomials, which allows us to capture larger classes of schemes. An example is the "petit IBE" [64], where $c_x(S, B) = (B + x)S, k_y(A, B, R) = \frac{A}{B+y}$ and P corresponds to the equality predicate. To prove adaptive security of these ABE in GGM, we require that the ABE satisfy a strengthening of the symbolic security from Agrawal-Chase [6] to the many-key setting, namely that there exists no degree two function of $c_x(S, B), \{k_y(A, B, R) : P(x, y) = 0\}$ that outputs SA. Looking ahead, note that many-key symbolic security is a purely algebraic criterion, and therefore particularly amenable to analysis using automated tools.

Next, we prove that if we restrict c_x, k_y to polynomials that satisfy some structural requirements as in prior works [6, 13] and that the ABE satisfies the (one-key) symbolic security from [6], then the ABE is adaptively secure in GGM. This means that it suffices for the automated tool to check the one-key symbolic security criterion instead of the many-key variant. We note that a similar result was shown in Agrawal-Chase [6], where they first apply a transformation to the ABE scheme which blows up the ciphertext and key sizes by a factor of 2, and showed that the ensuing ABE is adaptively secure in the standard model; in contrast, we prove adaptive security of the ABE "as is" in GGM. Compared to the latter schemes, our schemes are simpler and twice as efficient in terms of encryption time, decryption time, ciphertext and key sizes, but we only achieve security in the idealized GGM model. We note that all known non-trivial attacks on bilinear groups in use today are captured by GGM. For this reason, we believe that our ABE schemes provide a compelling alternative to less efficient standard model schemes in practical applications where performance is paramount.

Formally, we obtain both results in a unified manner by showing that for ABE captured by restricted polynomials c_x, k_y as in the latter, symbolic security implies many-key symbolic security. We note that a few of the ABE schemes captured by our framework have been informally claimed to be adaptively secure in GGM (e.g. [43, footnote 1 (Chapter 6)]), but to the best of our knowledge, our work provides the first formal treatment of adaptive security in GGM for a broad class of schemes satisfying a simple algebraic criterion.

En route, we prove a "Master Theorem" relating security in the GGM to security in a symbolic model. The main technical difference with prior work is that our Master Theorem handle rational fractions instead of polynomials [16, 17, 28].

Automated proofs. Our main theorem establishes that every RFI ABE which satisfies symbolic security is also secure in the GGM, and justifies using automated methods for proving symbolic security. Informally, our notion of symbolic security asserts the (non-)existence of a solution to a system of equations between rational fractions; one specificity is that these equations may include so-called big operators, i.e. expressions of the form $\sum_{i=1}^{n} e_i$ or $\prod_{i=1}^{n} e_i$, where n can take arbitrary values. Because neither symbolic computation nor algorithmic verification tools can deal with big operators (the former do not support big operators and the latter operate on a bounded state space), we develop constraint-solving methods that can successfully analyze the systems of equations representing cryptographic constructions. Broadly speaking, the algorithms combine simplification rules, which turn systems into simpler ones and case distinctions, which transform one single system into a system of equations, adding to each new system new equations that can trigger further simplifications. In contrast to prior works, the main novelty of our tool is to consider systems of equations between rational fractions, rather than polynomial expressions. We stress that our tool achieves soundness but does not constitute a decision procedure; this means that our tool never makes mistakes but can sometimes fail to produce an output.

Related work. Our work builds upon several areas, including ABE, GGM, and computer-aided cryptography.

ABE. Designing adaptively secure and efficient attribute-based encryption schemes is hard, and has been the focus of many prior works [47, 48, 54, 55, 61]. In 2014, Wee [63] and Attrapadung [12] propose simpler primitives called encoding and cryptographic compilers that turn secure encodings into adaptively secure attribute-based encryption schemes for a broad range of predicates. Their work is initially carried in the composite-order setting; in, Chen, Gay and Wee [36], Agrawal Chase [5], and Attrapadung [13] adapt the compiler to the prime order setting, using the notion of Dual System Groups (DSG) [37, 38]. More recently, Agrawal and Chase

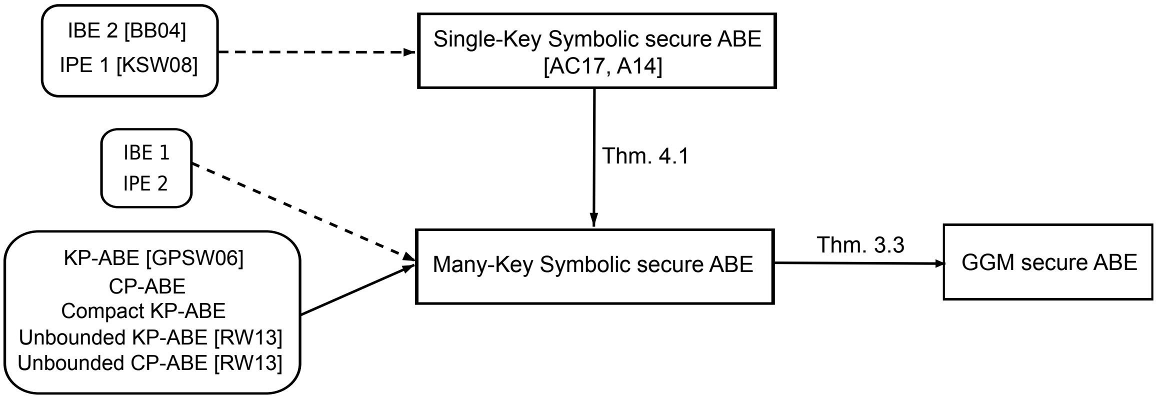

Figure 1: Roadmap of our results. The statements marked with dotted arrows were performed fully automatically with our tool (see Section 6), while plain arrows denotes proofs by hand. We provide proofs in the Appendix for all the results.

[6] propose a notion of symbolic security for pair encodings, and show that every symbolically secure pair encoding is compiled to an attribute-based encryption scheme that achieves full security under a q-type assumption. Ambrona, Barthe, and Schmidt [11] provide an algebraic characterization of the information-theoretic notion of α-privacy for predicate encodings. Both works leave open the possibility of building fully automated tools for checking symbolic security or the algebraic characterization of privacy.

GGM. The Generic Group Model was introduced in [53, 60] to reason about lower bounds for computing discrete logarithms and related problems. Maurer [51] gives an alternative presentation; while the two presentations are essentially equivalent, Maurer's presentation is more convenient for formalizing the Master Theorem and as a basis for formal verification. The GGM has been used for analyzing a broad variety of assumptions and constructions.

Master Theorems for bilinear groups were introduced by Boneh, Boyen and Goh in [28, 32]. There exist many others instances of Master Theorems; in particular, previous works on automated analyses in the GGM (detailed below) come with their own Master Theorem.

Computer-aided proofs. Barthe, Cederquist and Tarento [19] use the Coq proof assistant for building machine-checked proofs of security in the Generic Group Model. Their formalization is restricted to very simple examples.

Barthe and co-workers [20] develop an automated tool for analyzing security assumptions in the GGM. Their tool is justified by a Master Theorem which reduces security in the Generic Group Model to a weaker notion of symbolic security. However, their Master Theorem and their tool is primarily targetted to analyze assumptions, rather than schemes. A follow-up [21] considers the case of structure-preserving signatures [1–4, 22, 35] and harnesses the automated analyzer with a synthesis algorithm, which is used to discover new schemes. However, the tool is limited to prove security against a restricted class of adversaries. Ambrona and co-workers [10] extend prior Master Theorems to a more general class of security experiments and provide constraint-solving for proving symbolic security. However, their work does not consider rational functions.

Beyond this, prime focus of computer-aided cryptography is to support proofs in the standard model. Prior work uses a highly automated tool called AutoGP for proving security of several IBE in the standard model [24]. However, we are not aware of any prior work that uses computer-aided tools for reasoning about ABE. It could be possible to use existing computer-aided tools such as EasyCrypt [23] for building machine-checked proofs of security of ABE in the standard model; however, it would be very challenging to automate existing proofs for the composite order case, and even more so for the prime order case.

Finally, there have been efforts to integrate formal verification in tool-assisted cryptographic engineerings approaches for pairing-based cryptography [8]. There exist some similarities between our constraint-based method for proving symbolic security and the techniques they use. However, the goals of the two methods, and their justification, are fundamentally different.

2 PRELIMINARIES

Here we give relevant notations and definitions.

2.1 Lists

We denote by $\emptyset$ the empty list, by $\text{append}(L, x)$ the act of adding an element x to the list L, and for any $i \in \mathbb{N}$, we denote by $L[i]$ the i'th element of the L if it exists (lists are indexed from index 1 on), or $\perp$ otherwise.

2.2 Rational fractions

Polynomials. Let p be a prime, $n \in \mathbb{N}$. The set of multi-variate polynomials over $\mathbb{Z}_p$ with indeterminates $X_1, \dots, X_n$ is denoted by $\mathbb{Z}_p[X_1, \dots, X_n]$. The following lemma is a standard tool used for proving security in the Generic Group Model.

Lemma 2.1 (Schwartz-Zippel). *For any prime p, $t \in \mathbb{N}^*$, any polynomial $P \in \mathbb{Z}_p[X_1, \dots, X_t]$ of degree $d > 0$,*

$$\Pr[P(\vec{v}) = 0] \leq \frac{d}{p},$$

where the probability is taken over $\vec{v} \leftarrow_R \mathbb{Z}_p^t$.

For a polynomial $P \in \mathbb{Z}_p[X]$ and a formal variable Y, we write $P[X \rightarrow Y]$ to denote the polynomial in $\mathbb{Z}_p[Y]$ where X is replaced by Y. We generalize this notation for multivariate polynomials.

Rational fractions. Let p be a prime, $n \in \mathbb{N}$. A rational fraction is a pair $(f, g) \in \mathbb{Z}_p[X_1, \ldots, X_n] \times \mathbb{Z}_p[X_1, \ldots, X_n]^*$. We use f/g to denote the rational fraction (f, g) and we use f to denote $f/1$. For any $\vec{x} \in \mathbb{Z}_p^n$ such that $g(\vec{x}) = 0$, we denote $\frac{f(\vec{x})}{g(\vec{x})} = \perp$. We define for all $v \in \mathbb{Z}_p$, $\perp + v = v + \perp = \perp$, and $v \cdot \perp = \perp \cdot v = \perp$. We define the degree of a rational fraction f/g as $\deg(f/g) := \max\{\deg(f), \deg(g)\}$, where $\deg(f)$ and $\deg(g)$ denote the degree of polynomials f and g, respectively.

Equivalence relation. We define an equivalence relation $\sim_{\mathrm{rf}}$ between rational fractions by the clause $f/g \sim_{\mathrm{rf}} f'/g'$ iff $f \cdot g' = f' \cdot g$, where f/g and f'/g' are arbitrary rational fractions.

Operators. For any two rational fractions $f/g, f'/g'$, we define

- Addition: $f/g +_{\mathrm{rf}} f'/g' := (f \cdot \frac{\widehat{g}}{g} + f' \cdot \frac{\widehat{g}}{g'})/\widehat{g}$, where $\widehat{g} = \mathsf{lcm}(g, g')$ denotes the least common multiple of polynomials g and g'. Note that $\deg(f/g +_{\mathrm{rf}} f'/g') \leq \deg(f/g) + \deg(f'/g')$.
- Scalar multiplication: for any $\alpha \in \mathbb{Z}_p$, and rational fraction f/g, $\alpha \cdot (f/g) := (\alpha \cdot f)/g$.
- Product: $f/g \cdot_{\mathrm{rf}} f'/g'$ as $(f \cdot f')/(g \cdot g')$.

Note that the set of rational fractions equipped with addition, scalar multiplication and product is an algebra over $\mathbb{Z}_p$. In particular, rational fractions verify the associative property with $+_{\mathrm{rf}}$, we write $\sum_{i \in [n]}^{\mathrm{rf}} \alpha_i \cdot f_i/g_i := \alpha_1 \cdot f_1/g_1 +_{\mathrm{rf}} \ldots +_{\mathrm{rf}} \alpha_n \cdot f_n/g_n$, for $\alpha_1, \ldots, \alpha_n \in \mathbb{Z}_p$, and rational fractions $f_1/g_1, \ldots, f_n/g_n$. This is called a linear combination of the rational fractions $f_1/g_1, \ldots, f_n/g_n$. For any set of rational fractions Γ, we denote by $\langle \Gamma \rangle$ the set of all linear combinations of rational fractions in Γ.

For any set of formal variables S and S', $f/g \in \mathbb{Z}_p[S]$, and $f'/g' \in \mathbb{Z}_p[S']$, we naturally extend the operators $f/g +_{\mathrm{rf}} f'/g'$ and $f/g \cdot_{\mathrm{rf}} f'/g'$ to obtain rational fractions in $\mathbb{Z}_p[S \cup S']$.

2.3 Pairing groups

Let GGen be a probabilistic polynomial time (PPT) algorithm that on input the security parameter 1^λ, returns a description $\mathcal{PG} = (p, \mathbb{G}_1, \mathbb{G}_2, g_1, g_2, \mathbb{G}_T, e)$ of pairing groups where $\mathbb{G}_1$, $\mathbb{G}_2$, $\mathbb{G}_T$ are cyclic group of order p for a 2λ-bit prime p, g_1, g_2 are generators of $\mathbb{G}_1$, $\mathbb{G}_2$, respectively, and $e : \mathbb{G}_1 \times \mathbb{G}_2 \rightarrow \mathbb{G}_T$ is an efficiently computable (non-degenerate) bilinear map. Define $g_T := e(g_1, g_2)$, which is a generator of $\mathbb{G}_T$. We use implicit representation of group elements: for $a \in \mathbb{Z}_p$, define $[a]_s = g_s^a \in \mathbb{G}_s$ as the implicit representation of a in $\mathbb{G}_s$, for $s \in \{1, 2, T\}$. Given $[a]_1$ and $[b]_2$, one can efficiently compute $[ab]_T$ using the pairing e. For any $s \in \{1, 2, T\}$, we adopt the convention $[\perp]_s = \perp$.

2.4 Attribute-Based Encryption

We recall the definition of Attribute Based Encryption (in short: ABE) from [58] for predicate $\mathsf{P} : \mathcal{X} \times \mathcal{Y} \rightarrow \{0, 1\}$. It consists of the the following PPT algorithms:

- $\mathsf{Setup}(1^\lambda, \mathcal{X}, \mathcal{Y}) \rightarrow (\mathsf{mpk}, \mathsf{msk})$. The setup algorithm gets as input the security parameter 1^λ, the attribute universe $\mathcal{X}$, the predicate universe $\mathcal{Y}$. It outputs a master secret key msk and a master public key mpk, which defines a key space $\mathcal{K}$.
- $\mathsf{Enc}(\mathsf{mpk}, x) \rightarrow (\mathsf{ct}_x, \kappa)$. The encryption algorithm gets as input mpk and an attribute $x \in \mathcal{X}$. It outputs a ciphertext ct_x and a symmetric encryption key $\kappa \in \mathcal{K}$.
- $\mathsf{KeyGen}(\mathsf{mpk}, \mathsf{msk}, y) \rightarrow \mathsf{sk}_y$. The key generation algorithm gets as input mpk, msk and a value $y \in \mathcal{Y}$. It outputs the secret key: sk_y.
- $\mathsf{Dec}(\mathsf{mpk}, \mathsf{sk}_y, \mathsf{ct}_x, x) \rightarrow \kappa$. The decryption algorithm gets as input sk_y and ct_x such that $\mathsf{P}(x, y) = 1$. It outputs a symmetric key κ.

Correctness. For all $x \in \mathcal{X}, y \in \mathcal{Y}$ such that $\mathsf{P}(x, y) = 1$,

$$\Pr[\mathsf{Dec}(\mathsf{mpk}, \mathsf{sk}_y, \mathsf{ct}_x, x) = \kappa] = 1 - \mathsf{negl}(\lambda),$$

where the probability is taken over $(\mathsf{msk}, \mathsf{mpk}) \leftarrow \mathsf{Setup}(1^\lambda, \mathcal{X}, \mathcal{Y})$, $(\mathsf{ct}_s, \kappa) \leftarrow \mathsf{Enc}(\mathsf{mpk}, x)$, and $\mathsf{sk}_y \leftarrow \mathsf{KeyGen}(\mathsf{mpk}, \mathsf{msk}, y)$.

Adaptive Security. For any stateful adversary $\mathcal{A}$, Attribute Based Encryption ABE, and security parameter λ, we define the advantage function:

$$\mathsf{Adv}_{\mathcal{A}}^{\mathsf{ABE}}(\lambda) :=$$

$$\Pr\left[\beta' = \beta : \begin{array}{c} (\mathsf{mpk}, \mathsf{msk}) \leftarrow \mathsf{Setup}(1^\lambda, \mathcal{X}, \mathcal{Y}, \mathcal{M}) \\ (x^\star) \leftarrow \mathcal{A}^{\mathsf{KeyGen}(\mathsf{msk}, \cdot)}(\mathsf{mpk}) \\ (\mathsf{ct}_{x^\star}, \kappa) \leftarrow \mathsf{Enc}(\mathsf{mpk}, x^\star) \\ \beta \leftarrow_{\mathrm{R}} \{0, 1\}; K_0 := \kappa; K_1 \leftarrow_{\mathrm{R}} \mathcal{K} \\ \beta' \leftarrow \mathcal{A}^{\mathsf{KeyGen}(\mathsf{msk}, \cdot)}(\mathsf{ct}_{x^\star}, K_\beta) \end{array}\right] - \frac{1}{2}$$

with the restriction that all queries y that $\mathcal{A}$ makes to $\mathsf{KeyGen}(\mathsf{msk}, \cdot)$ must satisfy $\mathsf{P}(x^\star, y) = 0$ (that is, the secret keys cannot decrypt the challenge ciphertext). ABE is *adaptively secure* if for all PPT adversaries $\mathcal{A}$ and security parameter λ, the advantage $\mathsf{Adv}_{\mathcal{A}}^{\mathsf{ABE}}(\lambda) = \mathsf{negl}(\lambda)$.

3 RATIONAL-FRACTION INDUCED ABE

In this section we define a special class of so called Rational-Fraction Induced ABE (RFI-ABE), that captures all previous dual system ABE, but also allows inversion in the exponent, thereby capturing ABE's that fall out of the scope of dual system encryption, most notably the IBE from [64], as well as new ABE described in Section 5.

We prove the adaptive security of RFI-ABE in the generic group model, where it is assumed that no attack can make use of the algebraic structure of the particular bilinear group that is used. As it is common in the literature, we prove security in two steps. First, we prove a Master Theorem (Theorem 3.3) that bounds the probability of distinguishing between the *generic* and the *symbolic* models. Second (Lemma 3.2), we show that the advantage of any adversary in the symbolic model is zero, provided some algebraic condition on the ABE is satisfied (this condition is defined as the symbolic security of the ABE). For the sake of simplicity, our Master Theorem is specialized to capture the security experiment of RFI-ABE, however, it can be generalized to capture more general security games[1].

[1] Note that a more general master theorem could require a looser bound.

More precisely, we adopt the *generic model* by Maurer [51], where a third party implements the group and gives access to the adversary via handles, providing also equality checking. In the *symbolic model*, however, the third party does not implement an actual group, but keeps track of abstract expressions[2].

```
Setup$(1^\lambda, \mathcal{X}, \mathcal{Y})$:
$\mathcal{PG} \leftarrow \mathsf{GGen}(1^\lambda)$; $\vec{b} \leftarrow_R \mathbb{Z}_p^n$, $\alpha \leftarrow_R \mathbb{Z}_p$
Outputs $\mathsf{msk} := (\vec{b}, \alpha)$, $\mathsf{mpk} := ([\vec{b}]_1, [\alpha]_T) \in \mathbb{G}_1^n \times \mathbb{G}_T$.

Enc$(\mathsf{mpk}, x \in \mathcal{X})$:
$\vec{c}(\vec{S}, \vec{B}) \leftarrow \mathsf{sE}(x)$, $\vec{s} := (s_0, \dots, s_{w_1}) \leftarrow_R \mathbb{Z}_p^{w_1+1}$. Outputs
$\mathsf{ct}_x := [\vec{c}(\vec{b}, \vec{s})]_1 \in \mathbb{G}_1^{|\mathsf{ct}_x|}$, $\kappa := [\alpha s_0]_T \in \mathbb{G}_T$.

KeyGen$(\mathsf{mpk}, \mathsf{msk}, y \in \mathcal{Y})$:
$\vec{k}(\vec{R}, \vec{B}, A) \leftarrow \mathsf{rE}(y)$, $\vec{r} \leftarrow_R \mathbb{Z}_p^m$. Outputs $\mathsf{sk}_y := [\vec{k}(\vec{b}, \vec{r})]_2 \in$
$\mathbb{G}_2^{|\mathsf{sk}_y|}$.

Dec$(\mathsf{mpk}, \mathsf{ct}_x := [\vec{c}]_1, \mathsf{sk}_y := [\vec{k}]_2)$:
$\mathbf{E} \leftarrow \mathsf{Pair}(x, y)$. Outputs $[\vec{c}^\top \mathbf{E} \vec{k}]_T$.
```

Figure 2: $(p, n, \mathsf{sE}, \mathsf{rE}, \mathsf{Pair})$-**RFI ABE.**

RFI-ABE. Let $\mathsf{P} : \mathcal{X} \times \mathcal{Y} \to \{0, 1\}$ be predicate, p be a prime, $n \in \mathbb{N}$ and the following deterministic poly-time algorithms (rational fractions are considered over $\mathbb{Z}_p$):

- $\mathsf{sE}(x) \to \vec{c}(\vec{S}, \vec{B})$. On input $x \in \mathcal{X}$, the sender encoding algorithm sE outputs a vector of polynomials $\vec{c} = (c_1, \dots, c_{|\mathsf{ct}_x|})$ in the variables $\vec{S} = (S_0, \dots, S_w)$ and the common variables $\vec{B} = (B_1, \dots, B_n)$. Wlog. we assume that the polynomials do not contain any monomial B_i or any constant term.
- $\mathsf{rE}(y) \to \vec{k}(\vec{R}, \vec{B}, A)$. On input $y \in \mathcal{Y}$, the receiver encoding algorithm rE outputs a vector of rational fractions $\vec{k} = (k_1, \dots, k_{|\mathsf{sk}_y|})$ in the variables $\vec{R} = (R_1, \dots, R_m)$, A, and the common variables $\vec{B}$.
- $\mathsf{Pair}(x, y) \to \mathbf{E}$. On input $x \in \mathcal{X}$, $y \in \mathcal{Y}$, the Pair algorithm outputs a matrix $\mathbf{E} \in \mathbb{Z}_p^{|\mathsf{ct}_x| \times |\mathsf{sk}_y|}$,

We say an ABE is $(p, n, \mathsf{sE}, \mathsf{rE}, \mathsf{Pair})$-RFI if it is as described in Figure 2.

Degree of a RFI ABE. We define the degree of a RFI ABE as the maximum degree over all the polynomials that can be created by multiplying a polynomial from $\mathsf{sE}(x)$ with a polynomial from $\mathsf{rE}(y)$ for any $x \in \mathcal{X}$ and $y \in \mathcal{Y}$. The degree of a RFI ABE allows to bound the probability[3] of inconsistent equality check between the generic model and the symbolic model. More formally, given a $(p, n, \mathsf{sE}, \mathsf{rE}, \mathsf{Pair})$-RFI ABE, let $d_c := \max\{\deg(c_i) | i \in [|\mathsf{ct}_x|], \vec{c} \leftarrow \mathsf{sE}(x), x \in \mathcal{X}\}$ and let $d_k := \max\{\deg(k_i) | i \in [|\mathsf{sk}_y|], \vec{k} \leftarrow \mathsf{rE}(y), y \in \mathcal{Y}\}$. The degree of the pair encoding is defined by $d = d_c \cdot d_k$.

Correctness. The following theorem gives a sufficient condition for a RFI-ABE to be correct according to the definition of correctness from Section 2.4.

Theorem 3.1 (Correctness). *Let* ABE *be a* $(p, n, \mathsf{rE}, \mathsf{sE}, \mathsf{Pair})$-*RFI ABE for* $\mathsf{P} : \mathcal{X} \times \mathcal{Y} \to \{0, 1\}$. *If for all* $x \in \mathcal{X}, y \in \mathcal{Y}$ *such that* $\mathsf{P}(x, y) = 1$, $\vec{c}^\top \mathbf{E} \vec{k} \sim_{\mathsf{rf}} AS_0$, *where* $\vec{c} = \mathsf{sE}(x)$, $\vec{k} = \mathsf{rE}(y)$, $\mathbf{E} = \mathsf{Pair}(x, y)$, *then,* ABE *is correct, that is, for all* $x \in \mathcal{X}$, $y \in \mathcal{Y}$, $\Pr[\mathsf{Dec}(\mathsf{mpk}, \mathsf{sk}_y, \mathsf{ct}_x) \neq \kappa] \leq \frac{d|\mathsf{sk}_y|}{p}$, *where* d *is the degree of* ABE.

Symbolic security. We present an algebraic condition on RFI ABE that is sufficient to make it secure in the generic group model, as shown in Lemma 3.2 and Theorem 3.3.

We say a $(p, n, \mathsf{sE}, \mathsf{rE}, \mathsf{Pair})$-RFI ABE is symbolically secure if for all $x \in \mathcal{X}$, there does not exist $\{\mathbf{E}_y^*\}_{y \in \mathcal{Y}_x}$ such that $\sum_{y \in \mathcal{Y}_x} \vec{c}(\vec{S}, \vec{B})^\top \mathbf{E}_y^* \vec{k}_y(\vec{R}_y, \vec{B}, A) \sim_{\mathsf{rf}} AS_0$, where $\vec{c}(\vec{S}, \vec{B}) = \mathsf{sE}(x)$, $\mathcal{Y}_x \subseteq \mathcal{Y}$ is the set of all $y \in \mathcal{Y}$ such that $\mathsf{P}(x, y) = 0$, and for all $y \in \mathcal{Y}_x$, $\vec{R}_y := (R_{y,1}, \dots, R_{y,m_1})$, $\vec{k}_y(\vec{R}_y, \vec{B}, A) := \mathsf{rE}(y)(\vec{R} \to \vec{R}_y)$.

We show in the following lemma that the symbolic security above implies a seemingly stronger security notion, which allows to go from security in the private-key setting, to a public key setting.

Lemma 3.2 (From public to private key). *Let* ABE *be a* $(p, n, \mathsf{sE}, \mathsf{rE}, \mathsf{Pair})$-*RFI ABE. The symbolic security of* ABE *implies that for all* $x \in \mathcal{X}$, *there does not exist* $\{\mathbf{E}_y^*\}_{y \in \mathcal{Y}_x}$ *and* $\gamma \in \mathbb{Z}_p$ *such that* $\sum_{y \in \mathcal{Y}_x} (\vec{B}, \vec{c}(\vec{S}, \vec{B}))^\top \mathbf{E}_y^* \vec{k}_y(\vec{R}_y, \vec{B}, A) + \gamma A \sim_{\mathsf{rf}} AS_0$ *where* $\vec{c}(\vec{S}, \vec{B}) = \mathsf{sE}(x)$, $\mathcal{Y}_x \subseteq \mathcal{Y}$ *is the set of all* $y \in \mathcal{Y}$ *such that* $\mathsf{P}(x, y) = 0$, *and for all* $y \in \mathcal{Y}_x$, $\vec{R}_y := (R_{y,1}, \dots, R_{y,m_1})$, $\vec{k}_y(\vec{R}_y, \vec{B}, A) := \mathsf{rE}(y)(\vec{R} \to \vec{R}_y)$.

Security in the generic group model. Let ABE be a $(p, n, \mathsf{sE}, \mathsf{rE}, \mathsf{Pair})$-RFI ABE for $\mathsf{P} : \mathcal{X} \times \mathcal{Y} \to \{0, 1\}$, and $\mathcal{A}$ be an adversary. For $\mathsf{xxx} \in \{\mathsf{GGM}, \mathsf{SM}\}$, we define the experiments $\mathsf{Exp}_{\mathsf{ABE}}^{\mathsf{xxx}}(1^\lambda, \mathcal{A})$ in Figure 3. We define the advantages:

$$\mathsf{Adv}_{\mathsf{ABE}, \mathcal{A}}^{\mathsf{xxx}}(\lambda) := \left| \frac{1}{2} - \Pr\left[\mathsf{Exp}_{\mathsf{ABE}}^{\mathsf{xxx}}(1^\lambda, \mathcal{A}) \to 1)\right] \right|.$$

We say ABE is adaptively secure in the generic group model if for all PPT adversaries $\mathcal{A}$: $\mathsf{Adv}_{\mathsf{ABE}, \mathcal{A}}^{\mathsf{GGM}}(\lambda) = \mathsf{negl}(\lambda)$.

Very roughly, experiment $\mathsf{Exp}^{\mathsf{xxx}}(1^\lambda, \mathcal{A})$ is the security game where adversary $\mathcal{A}$ is trying to break the *ABE*[4]. However, there is a third party who implements the group, so that the adversary can only access to the group via handles. Internally, this third party keeps track of both, a symbolic representation of group elements

[2] For example, consider an experiment where values x, y are sampled from $\mathbb{Z}_p$ and the adversary gets handles to g^x and g^y. In the generic model, the third party will choose a group of order p, for example $(\mathbb{Z}_p, +)$, will sample values $x, y \leftarrow_R \mathbb{Z}_p$ and will give handles to x and y. On the other hand, in the symbolic model the sampling won't be performed and the third party will output handles to X and Y, where X and Y are abstract variables. Now, if the adversary asks for equality of the elements associated to the two handles, the answer will be negative in the symbolic model, since abstract variable X is different from abstract variable Y, but there is a small chance the equality check succeeds in the generic model (only when the sampling of x and y coincides).

[3] Note that, by Schwartz-Zippel, the probability that two different polynomials over $\mathbb{Z}_p$, evaluated uniformly at random, give the same output is bounded by the maximum degree of the two, divided by p.

[4] In this experiment, $\mathcal{A}$ is given the public parameters and access to a key generation oracle that returns valid keys for values y of its choice. Eventually, $\mathcal{A}$ will choose two messages m_0 and m_1 and a target value x. After a random sampling $b \leftarrow_R \{0, 1\}$, message m_b will be encrypted under attribute x and sent to $\mathcal{A}$. Now, the adversary is allowed to keep asking for secret keys and we say $\mathcal{A}$ wins the experiment if it can guess b correctly.

$\underline{\mathsf{Exp}_{\mathsf{ABE}}^{\boxed{\mathrm{GGM}}\ \boxed{\mathrm{SM}}}(1^\lambda, \mathcal{A})\text{:}}$

$\mathsf{cnt} = \mathsf{gen} := 0$, $L_1^{\mathsf{eq}} = L_2^{\mathsf{eq}} = L_T^{\mathsf{eq}} = L_1^{\sim} = L_2^{\sim} = L_T^{\sim} := \emptyset$, $\mathcal{Q}_{\mathsf{chal}} = \mathcal{Q}_{\mathsf{sk}} := \emptyset$, $\mathsf{append}(L_1^{\sim}, \vec{B})$, $\mathsf{append}(L_T^{\sim}, A)$, $\vec{b} \leftarrow_{\mathrm{R}} \mathbb{Z}_p^n$, $\alpha \leftarrow_{\mathrm{R}} \mathbb{Z}_p$, $\mathsf{append}(L_1^{\mathsf{eq}}, \vec{b})$, $\beta \leftarrow_{\mathrm{R}} \{0,1\}$. $\beta' \leftarrow \mathcal{A}^{\mathcal{O}_{\mathsf{add}}, \mathcal{O}_{\mathsf{pair}}, \boxed{\mathcal{O}_{\mathsf{eq}}}, \boxed{\mathcal{O}_{\sim}}, \mathcal{O}_{\mathsf{chal}}, \mathcal{O}_{\mathsf{sk}}}(1^\lambda, p)$. If $\beta' = \beta$, and for all $x \in \mathcal{Q}_{\mathsf{chal}}$, $y \in \mathcal{Q}_{\mathsf{sk}}$, $\mathsf{P}(x,y) = 0$, output 1. Otherwise, output 0.

$\underline{\mathcal{O}_{\mathsf{add}}(s \in \{1,2,T\}, i, j \in \mathbb{N})\text{:}}$

$\mathsf{append}(L_s^{\sim}, L_s^{\sim}[i] +_{\mathsf{rf}} L_s^{\sim}[j])$, $\mathsf{append}(L_s^{\mathsf{eq}}, L_s^{\mathsf{eq}}[i] + L_s^{\mathsf{eq}}[j])$.

$\underline{\mathcal{O}_{\mathsf{pair}}(i, j \in \mathbb{N})\text{:}}$

$\mathsf{append}(L_s^{\sim}, L_s^{\sim}[i] \cdot_{\mathsf{rf}} L_s^{\sim}[j])$, $\mathsf{append}(L_s^{\mathsf{eq}}, L_s^{\mathsf{eq}}[i] \cdot L_s^{\mathsf{eq}}[j])$.

$\underline{\mathcal{O}_{\mathsf{chal}}(x \in \mathcal{X})\text{:}}$

$\vec{c}(\vec{S}, \vec{B}) \leftarrow \mathsf{sE}(x)$, $\vec{S} := (S_0, \ldots, S_{w_1})$, $f_0^\star := AS_0$, $f_1^\star := U$, where U is a fresh formal variable, $\vec{s} \leftarrow_{\mathrm{R}} \mathbb{Z}_p^{w_1}$, $v_0^\star := \alpha s_0$, $v_1^\star := u \leftarrow_{\mathrm{R}} \mathbb{Z}_p$, $\mathsf{append}\big(L_1^{\sim}, \vec{c}(\vec{B}, \vec{S})\big)$, $\mathsf{append}(L_T^{\sim}, f_\beta^\star)$, $\mathsf{append}\big(L_1^{\mathsf{eq}}, \vec{c}(\vec{b}, \vec{s})\big)$, $\mathsf{append}(L_s^{\mathsf{eq}}, v^\star)$, $\mathcal{Q}_{\mathsf{chal}} := \mathcal{Q}_{\mathsf{chal}} \cup \{x\}$.

$\underline{\mathcal{O}_{\mathsf{sk}}(y \in \mathcal{Y})\text{:}}$

$\vec{R}_{\mathsf{cnt}} := (R_{\mathsf{cnt},1}, \ldots, R_{\mathsf{cnt},m_1})$, $\vec{k}(\vec{R}_{\mathsf{cnt}}, \vec{B}, A) \leftarrow \mathsf{rE}(y)(\vec{R} \to \vec{R}_{\mathsf{cnt}})$, $\vec{r}_{\mathsf{cnt}} \leftarrow_{\mathrm{R}} \mathbb{Z}_p^{m_1}$, $\mathsf{append}(L_2^{\sim}, \vec{k})$, $\mathsf{append}\big(L_2^{\mathsf{eq}}, \vec{k}(\vec{r}_{\mathsf{cnt}}, \vec{b}, \alpha)\big)$, $\mathsf{cnt} := \mathsf{cnt} + 1$, $\mathcal{Q}_{\mathsf{sk}} := \mathcal{Q}_{\mathsf{sk}} \cup \{y\}$.

$\underline{\mathcal{O}_{\mathsf{eq}}(s \in \{1,2,T\}, i, j \in \mathbb{N})\text{:}}$

Output 1 if $L_s^{\mathsf{eq}}[i] = L_s^{\mathsf{eq}}[j]$, 0 otherwise

$\underline{\mathcal{O}_{\sim}(s \in \{1,2,T\}, i, j \in \mathbb{N})\text{:}}$

Output 1 if $L_s^{\sim}[i] \sim_{\mathsf{rf}} L_s^{\sim}[j]$, 0 otherwise.

Figure 3: Experiments $\mathsf{Exp}_{\mathsf{ABE}}^{\boxed{\mathrm{GGM}}\ \boxed{\mathrm{SM}}}(1^\lambda, \mathcal{A})$. We require that $\mathcal{A}$ queries $\mathcal{O}_{\mathsf{chal}}$ at most once, and that for $x \in \mathcal{Q}_{\mathsf{chal}}$ and all $y \in \mathcal{Q}_{\mathsf{sk}}$, $\mathsf{P}(x,y) = 0$. In each procedure, the components inside a light gray (dark gray) frame are only present in the games marked by a light gray (dark gray) frame. Wlog. we assume no query contains indices $i, j \in \mathbb{N}$ that exceed the size of the involved lists.

and a real one (by sampling random values when required). The difference between $\mathsf{Exp}^{\mathsf{GGM}}$ and $\mathsf{Exp}^{\mathsf{SM}}$ is in equality checks that are answered by using the generic representation and the symbolic representation of group elements respectively. Our next theorem bounds the probability of any distinguisher between $\mathsf{Exp}^{\mathsf{GGM}}$ and $\mathsf{Exp}^{\mathsf{SM}}$. Approximately, the only chance of distinguishing is that an *bad event*[5] occurs. Theorem 3.3 bounds the probability of a bad event happening.

Security proof of the generic construction. Our next result establishes that symbolically secure RFI ABE are also secure in the GGM.

Theorem 3.3 (From symbolic to generic security). *Let* ABE *be a symbolically secure* $(p, n, \mathsf{sE}, \mathsf{rE}, \mathsf{Pair})$*-RFI ABE for* $\mathsf{P} : \mathcal{X} \times \mathcal{Y} \to \{0,1\}$. *Let* $\lambda \in \mathbb{N}$ *be the security parameter, and* $\mathcal{A}$ *be an adversary that on input* $(1^\lambda, p)$*, makes* Q_{sk}, Q_{add}, Q_{pair} *calls to the oracles* $\mathcal{O}_{\mathsf{sk}}$, $\mathcal{O}_{\mathsf{add}}$, $\mathcal{O}_{\mathsf{pair}}$*, respectively, and* 1 *call to* $\mathcal{O}_{\mathsf{chal}}$. *We have:*

$$\mathsf{Adv}_{\mathsf{ABE},\mathcal{A}}^{\mathsf{GGM}}(\lambda) \leq \frac{2d(n + |\mathsf{ct}| + Q_{\mathsf{sk}}|\mathsf{sk}| + Q_{\mathsf{add}} + Q_{\mathsf{pair}})^4}{p},$$

where d is the degree of ABE, $|\mathsf{ct}| := \max\{|\mathsf{ct}_x| : x \in \mathcal{Q}_{\mathsf{chal}}\}$*, and* $|\mathsf{sk}| := \max\{|\mathsf{sk}_y| : y \in \mathcal{Q}_{\mathsf{sk}}\}$

4 PAIR ENCODINGS

In this section, we recall the definition of pair encodings, which have been originally introduced in [12, 63] as a useful abstraction to build ABE whose security proof rely on the Dual System Encryption techniques [61] (roughly speaking, a pair encoding is a private-key, one-time secure variant of ABE). We show in Theorem 4.1 that any pair encoding that is symbolically secure, as defined in [6] (this is the weakest possible notion of security for pair encoding), yields a symbolically secure RFI-ABE via the construction presented in Figure 2. The RFI-ABE obtained are roughly twice more efficient that those obtained via previous dual system frameworks, albeit relying on the generic group model.

[5] Equality checks in the symbolic representation and the generic representation differ.

Pair encodings. Let p be a prime, $n \in \mathbb{N}$. A (p, n) pair encoding for predicate $\mathsf{P} : \mathcal{X} \times \mathcal{Y} \rightarrow \{0, 1\}$ consists of the following deterministic poly-time algorithms (polynomials are considered over $\mathbb{Z}_p$):

- $\mathsf{sE}(x) \rightarrow \big(\vec{S}, \vec{c}(\vec{S}, \vec{S}', \vec{B})\big)$. On input $x \in \mathcal{X}$, the sender encoding algorithm sE outputs $(\vec{S}, \vec{c})$, where $\vec{c} = (c_1, \ldots, c_{w_3})$ is a vector of polynomials in the non-lone variables $\vec{S} = (S_0, \ldots, S_{w_1})$, the lone variables $\vec{S}' = (S'_1, \ldots, S'_{w_2})$, and the common variables $\vec{B} = (B_1, \ldots, B_n)$ where for all $i \in [w_3]$, c_i is a linear combination of the monomials $\{S'_i, S_j B_\ell | i \in [w_2], j \in [0, w_1], \ell \in [n]\}$.
- $\mathsf{rE}(y) \rightarrow (\vec{R}, \vec{k}(\vec{R}, \vec{R}', \vec{B}, A))$. On input $y \in \mathcal{Y}$, the receiver encoding algorithm rE outputs $(\vec{R}, \vec{k}(\vec{R}, \vec{R}', \vec{B}, A))$, where $\vec{k} = (k_1, \ldots, k_{m_3})$ is a vector of polynomials in the non-lone variables $\vec{R} = (R_1, \ldots, R_{m_1})$, the lone variables $\vec{R}' = (R'_1, \ldots, R'_{m_2})$, A, and the common variables $\vec{B}$, where for all $i \in [m_3]$, k_i is a linear combination of the monomials $\{A, R'_i, R_j B_\ell | i \in [m_2], j \in [m_1], \ell \in [n]\}$.
- $\mathsf{Pair}(x, y) \rightarrow \mathbf{E}, \mathbf{E}'$. On input $x \in \mathcal{X}$, $y \in \mathcal{Y}$, the Pair algorithm outputs matrices $\mathbf{E} \in \mathbb{Z}_p^{(w_1+1)\times m_3}$, and $\mathbf{E}' \in \mathbb{Z}_p^{w_3 \times m_1}$.

Correctness. For all $x \in \mathcal{X}, y \in \mathcal{Y}$ such that $\mathsf{P}(x, y) = 1$, $\vec{S}^\top \mathbf{E} \vec{k} + \vec{c}^\top \mathbf{E}' \vec{R} = AS_0$, where $(\vec{S}, \vec{c}) = \mathsf{sE}(x)$, $(\vec{R}, \vec{k}) = \mathsf{rE}(y)$, $(\mathbf{E}, \mathbf{E}') \leftarrow \mathsf{Pair}(x, y)$.

Symbolic security [6]. For all $x \in \mathcal{X}$ and $y \in \mathcal{Y}$ such that $\mathsf{P}(x, y) = 0$, there is no matrix $\mathbf{E}^* \in \mathbb{Z}_p^{(1+w_1+w_3)\times(m_1+m_3)}$ such that $\vec{c}^\top \mathbf{E}^* \vec{k} = AS_0$, where $\vec{c} = \mathsf{sE}(x)$, $\vec{k} = \mathsf{rE}(y)$.

Our next theorem shows that any symbolically secure (p, n) pair encoding $(\mathsf{sE}, \mathsf{rE}, \mathsf{Pair})$ [6] yields a symbolically secure $(p, n, \mathsf{sE}, \mathsf{rE}, \mathsf{Pair})$-RFI ABE.

Theorem 4.1. *[Symbolically secure pair encoding ⇒ symbolically secure RFI-ABE] Let* $(\mathsf{sE}, \mathsf{rE}, \mathsf{Pair})$ *be a* (p, n) *pair encoding for predicate* $\mathsf{P} : \mathcal{X} \times \mathcal{Y} \rightarrow \{0, 1\}$*. The construction described in Figure 2 is a symbolically secure,* $(p, n, \mathsf{sE}, \mathsf{rE}, \mathsf{Pair})$*-RFI ABE.*

5 CONCRETE RFI-ABE

Focusing on the generic group model allowed us to build schemes that are often simpler and more efficient compared to existing schemes from the literature (see table in Figure 4 for a comparison amongst the most efficient ABE). In this section, we show a selection of schemes that illustrate the versatility of our framework. Our contribution here is threefold:

(1) we design new pair encodings, which give new, more efficient RFI-ABE via our framework (cf. Figure 2). This is the case of IPE 2, compact KP-ABE, unbounded KP-ABE, CP-ABE, and unbounded CP-ABE.
(2) we use our framework on existing pair encodings, to obtain new, more efficient RFI-ABE, albeit relying on a stronger assumption. This is the case of IBE 1 and IPE 1, whose underlying pair encoding are implicit in the work of [64] and [46] respectively.
(3) we use our framework on existing pair encodings, to prove new security guarantees on existing RFI-ABE. This is the case of IBE 2 from [27] and KP-ABE from [41]. Here, our framework, when input on the pair encodings implicitly given in [27, 41], outputs exactly the same RFI-ABE present in those papers: there is no efficiency gain. However, we can prove these RFI-ABE *adaptively* secure, under GGM, while they were proved only *selectively* secure, based on standard assumptions.

Overall, our new framework captures previous schemes (contribution (3)), and improves upon many others (contribution (1) and (2)), at the price of a strong assumption, namely GGM.

5.1 Identity-Based Encryption (IBE)

IBE is the simplest example of ABE, introduced by [59], where Alice can send a message to Bob only using some public parameters and Bob's identity (a pre-existing identifier, e.g. an email address), unlike traditional public-key encryption, where Bob would need to communicate his public key to Alice. In general, IBE simplifies the key management of certificate-based public-key infrastructure. A major use case for IBE is email encryption, where it allows pairwise email encryption, that is, Alice can send an encrypted email directly to Bob without Bob's involvement. This technology is being adopted in real-life applications. In fact, early IBE schemes are being standardized in IEEE P1363.3 and RFC 5091.

For IBE, we have $\mathcal{X} = \mathcal{Y} = \mathbb{Z}_p$, and the predicate P is defined as: $\mathsf{P}(x, y) = 1$ iff $x = y$.

IBE 1 [64]

- $n = 1, \vec{B} := B; w_1 = 0, \vec{S} := S; m_1 = 0; w_2 = m_2 = 1.$
- $\mathsf{sE}(x) \rightarrow S(B + x)$.
- $\mathsf{rE}(y) \rightarrow A/(B + y)$.
- $\mathsf{Pair}(x, y) \rightarrow 1$

IBE 1 is the prime-order version of the IBE from [64], which uses the Déjà Q framework, introduced in [34]. It is an open problem to translate this framework, which uses *composite-order* bilinear groups, to the more efficient [42] prime order setting. This yields one of the most efficient IBE, as illustrated in the benchmark Figure 7. Note that an unpublished manuscript from Eike Kiltz and Gregory Neven, cited in [31, citation 35], already proves adaptive security of IBE 1 in the GGM.

IBE 2 [27]

- $n = 2, \vec{B} := (B_1, B_2); w_1 = 0, \vec{S} := S; m_1 = 1, \vec{R} := R; w_2 = m_2 = 2.$
- $\mathsf{sE}(x) \rightarrow \big(S, S(B_1 + xB_2)\big)$
- $\mathsf{rE}(y) \rightarrow \big(R, A + R(B_1 + yB_2)\big)$
- $\mathsf{Pair}(x, y) \rightarrow \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$

IBE 2 is [27], which we prove adaptively secure in the GGM ([27] proved it selectively secure based on DBDH).

5.2 Inner Product Encryption (IPE)

IPE generalizes IBE, and captures useful classes of predicates, such as CNF and DNF formulas, or predicates that can expressed as polynomials (see [46] for more details).

For IPE, we have $\mathcal{X} = \mathcal{Y} = \mathbb{Z}_p^d$ and for any $z \in \mathbb{Z}_p^*$, the predicate P_z is defined as: $\mathsf{P}_z(\vec{x}, \vec{y}) = 1$ iff $\vec{x}^\top \vec{y} = z$.

KP-ABE:	$\lvert\mathsf{mpk}\rvert$	$\lvert\mathsf{sk}\rvert$	$\lvert\mathsf{ct}\rvert$	T_{Dec}	(assumption,sec)
GPSW06 [41]	$U\lvert\mathbb{G}\rvert + \lvert\mathbb{G}_T\rvert$	$\ell\lvert\mathbb{G}\rvert$	$\lvert\Gamma\rvert \cdot \lvert\mathbb{G}\rvert + \lvert\mathbb{G}_T\rvert$	$\lvert\Gamma\rvert \cdot P + \ell E$	(DBDH,sel.) (GGM,ad.)
RW13 [57]	$3\lvert\mathbb{G}\rvert + \lvert\mathbb{G}_T\rvert$	$3\ell\lvert\mathbb{G}\rvert$	$(2\lvert\Gamma\rvert + 1)\lvert\mathbb{G}\rvert + \lvert\mathbb{G}_T\rvert$	$(2\lvert\Gamma\rvert + 1)P + 3\ell E$	(Q-type,sel.)
Our unbounded KP-ABE	$2\lvert\mathbb{G}\rvert + \lvert\mathbb{G}_T\rvert$	$2\ell\lvert\mathbb{G}\rvert$	$2\lvert\Gamma\rvert \cdot \lvert\mathbb{G}\rvert + \lvert\mathbb{G}_T\rvert$	$2\lvert\Gamma\rvert \cdot P + 2\ell E$	(GGM,ad.)
ALP11 [14]	$d\lvert\mathbb{G}\rvert + \lvert\mathbb{G}_T\rvert$	$(d+1)\ell\lvert\mathbb{G}\rvert$	$2\lvert\mathbb{G}\rvert + \lvert\mathbb{G}_T\rvert$	$2P + \lvert\Gamma\rvert \cdot \ell E$	(Q-type,sel.)
Our compact KP-ABE	$U\lvert\mathbb{G}\rvert + \lvert\mathbb{G}_T\rvert$	$\ell U\lvert\mathbb{G}\rvert$	$2\lvert\mathbb{G}\rvert + \lvert\mathbb{G}_T\rvert$	$2P + \lvert\Gamma\rvert \cdot \ell E$	(GGM,ad.)

CP-ABE:	$\lvert\mathsf{mpk}\rvert$	$\lvert\mathsf{sk}\rvert$	$\lvert\mathsf{ct}\rvert$	T_{Dec}	(assumption,sec)
W11 [62]	$(U+1)\lvert\mathbb{G}\rvert + \lvert\mathbb{G}_T\rvert$	$(\lvert\Gamma\rvert + 2)\lvert\mathbb{G}\rvert$	$(2\ell + 1)\lvert\mathbb{G}\rvert + \lvert\mathbb{G}_T\rvert$	$(\lvert\Gamma\rvert + 2)P + 2\ell E$	(Q-type,sel.)
Our CP-ABE	$U\lvert\mathbb{G}\rvert + \lvert\mathbb{G}_T\rvert$	$(\lvert\Gamma\rvert + 1)\lvert\mathbb{G}\rvert$	$(\ell + 1)\lvert\mathbb{G}\rvert + \lvert\mathbb{G}_T\rvert$	$(\lvert\Gamma\rvert + 1)P + \ell E$	(GGM,ad.)
RW13 [57]	$4\lvert\mathbb{G}\rvert + \lvert\mathbb{G}_T\rvert$	$(2\lvert\Gamma\rvert + 2)\lvert\mathbb{G}\rvert$	$(3\ell + 1)\lvert\mathbb{G}\rvert + \lvert\mathbb{G}_T\rvert$	$(2\lvert\Gamma\rvert + 2)P + 3\ell E$	(Q-type,sel.)
Our unbounded CP-ABE	$4\lvert\mathbb{G}\rvert + \lvert\mathbb{G}_T\rvert$	$(\lvert\Gamma\rvert + 2)\lvert\mathbb{G}\rvert$	$3\ell\lvert\mathbb{G}\rvert + \lvert\mathbb{G}_T\rvert$	$(\lvert\Gamma\rvert + 2)P + 3\ell E$	(GGM,ad.)

Figure 4: Comparison of the most efficient existing KP-ABE and CP-ABE schemes for (monotone) boolean span programs, based on prime-order bilinear groups. We denote by $|\Gamma|$ the attribute set size, d the maximum size for Γ (if bounded), U the size of the attribute universe (if bounded small-universe), ℓ is the size of the access structure. For CT, we omit the additive overhead of $O(|\Gamma|)$ *bits* in order to transmit the attribute vector (for KP-ABE), or $O(\ell)$ *bits* in order to transmit the access structure. We use T_{Dec} to denote the decryption time, $|\mathbb{G}|$ the size of the source groups, $|\mathbb{G}_T|$ the size of the target group, E exponentiation in the source groups, and P to denote a pairing. Decryption algorithms have been optimized taking into account that $P > E$. Gray boxes indicate new results.

IPE 1 [46]

- $n = d + 1, \vec{B} := (U, \vec{V}); w_1 = 0, \vec{S} := S; m_1 = 1, \vec{R} := R; w_2 = m_2 = 2.$
- $\mathsf{sE}(\vec{x}) \to \big(S, S(U\vec{x} + \vec{V})\big)$
- $\mathsf{rE}(\vec{y}) \to \big(R, A + R(Uz + \vec{V}^\top \vec{y})\big)$
- $\mathsf{Pair}(x, y) \to \begin{pmatrix} 0 & 1 \\ -\vec{y} & 0 \end{pmatrix}$

IPE 1 is a prime-order version [46], which, via our framework described in Figure 2, gives an IPE that is twice shorter than the already existing prime-order version of [46], namely [56]. This is expected, since we use a stronger assumption, GGM, while the cited works use standard assumptions.

IPE 2

- $n = d; w_1 = 0, \vec{S} := S; m_1 = 0; w_2 = m_2 = 1.$
- $\mathsf{sE}(\vec{x}) \to S(\vec{x} + \vec{B})$
- $\mathsf{rE}(\vec{y}) \to A/(z + \vec{B}^\top \vec{y})$
- $\mathsf{Pair}(\vec{x}, \vec{y}) \to \vec{y}$

IPE 2 is a new and shorter IPE that relies on inversions in the exponent, which were not captured by previous framework.

5.3 ABE for boolean span programs.

We define (monotone) access structures using the language of (monotone) span programs [45]. They capture boolean formulas, thereby generalizing IBE and IPE, by allowing to embed more complex access policies in ciphertexts (such ABE are called Ciphertext Policy ABE, or CP-ABE) or in keys (such ABE are called Key Policy ABE, or KP-ABE).

Definition 5.1 (access structure [25, 45]). A *(monotone) access structure* for attribute universe $\mathcal{U}$ is a pair $(\mathbf{M}, \rho)$ where $\mathbf{M} \in \mathbb{Z}_p^{\ell \times \ell'}$ and $\rho : [\ell] \to \mathcal{U}$. Given $\Gamma \subseteq \mathcal{U}$, we say that

$$\Gamma \text{ satisfies } (\mathbf{M}, \rho) \text{ iff } \vec{1}^\top \in \mathsf{span}_{\mathsf{row}}(\mathbf{M}_\Gamma),$$

Here, $\vec{1} := (1, 0, \ldots, 0) \in \mathbb{Z}^{\ell'}$ is a row vector; $\mathbf{M}_S$ denotes the collection of vectors $\{\mathbf{M}_j : \rho(j) \in \Gamma\}$ where $\mathbf{M}_i$ denotes the i'th row of $\mathbf{M}$; and $\mathsf{span}_{\mathsf{row}}$ refers to linear span of collection of (row) vectors over $\mathbb{Z}_p$.

That is, Γ satisfies $(\mathbf{M}, \rho)$ iff there exists constants $\omega_1, \ldots, \omega_\ell \in \mathbb{Z}_p$ such that

$$\sum_{\rho(j) \in S} \omega_j \mathbf{M}_j = \vec{1}^\top \tag{1}$$

Observe that the constants $\{\omega_i\}$ can be computed in time polynomial in the size of the matrix $\mathbf{M}$ via Gaussian elimination.

Large universe, Unbounded ABE. When $\mathcal{U}$ is of polynomial size, we write $\mathcal{U} := [d]$, and we describe sets $\Gamma \subseteq [d]$ by their characteristic vectors $\vec{x} \in \{0,1\}^n$, where for all $i \in [d]$, $x_i = 1$ if $i \in \Gamma$, and 0 otherwise. If an ABE supports universes $\mathcal{U}$ of exponential size, we call it *large universe*. If additionally, it does not introduce a bound on the number of attributes per ciphertext, we use the term *unbounded ABE*. For practical purposes, unbounded ABE [49] are preferable, since the setup does not put a bound on the number of attributes per ciphertext, and they allow for more versatility since any bit string (once hashed into $\mathbb{Z}_p$) can be used as an attribute.

Using GGM, we prove the adaptive security of the KP-ABE from [41], arguably one of the most efficient KP-ABE, while [41] proved its selective security based on DBDH.

KP-ABE [41]

Here, $\mathcal{U} := [d]$, $\mathcal{X} := \{0,1\}^d$, $\mathcal{Y} := \mathbb{Z}_p^{\ell \times \ell'} \times ([\ell] \to [d])$.

- $n = d, \vec{B} := (B_1, \ldots, B_d); w_1 = 0, \vec{S} := S; m_1 := \ell' - 1.$
- $\mathsf{sE}(\vec{x}) \to (x_1 S B_1, \ldots, x_d S B_d)$
- $\mathsf{rE}(\mathbf{M}, \rho) \to \big(\mathbf{M}_1^\top (A, \vec{R})/B_{\rho(1)}, \ldots, \mathbf{M}_\ell^\top (A, \vec{R})/B_{\rho(\ell)}\big)$
- $\mathsf{Pair}(\vec{x}, (\mathbf{M}, \rho)) \to \mathbf{E} \in \mathbb{Z}_p^{d \times \ell}$, where for all $i \in [d]$, $j \in [\ell]$, $E_{i,j} = \omega_j$ if $\rho(j) = i$, 0 otherwise.

We now give a new compact KP-ABE, where the ciphertexts contain 2 group elements, regardless of the number of attribute.

This is more efficient that state of the art [14] for which ciphertexts contain 3 group element (although the latter is for large universe, and ours small).

Compact KP-ABE

Here, $\mathcal{U} := [d]$, $\mathcal{X} := \{0,1\}^d$, $\mathcal{Y} := \mathbb{Z}_p^{\ell \times \ell'} \times ([\ell] \to [d])$.

- $n = d$, $\vec{B} := (B_1, \ldots, B_d)$; $w_1 = 0$, $\vec{S} := S$; $m_1 := \ell' - 1$.
- $\mathsf{sE}(\vec{x}) \to (c_1, c_2)$, where $c_1 := S \sum_{i=1}^{d} x_i B_i$, and $c_2 := S$
- $\mathsf{rE}(\mathbf{M}, \rho) \to \big((k_j)_{j\in[\ell]}, (k_{i,j})_{i\in[d], j\in[\ell], \rho(j)\neq i}\big)$, where $k_j := \mathbf{M}_j^\top(A, \vec{R})/B_{\rho(j)}$, $k_{i,j} := \mathbf{M}_j^\top(A, \vec{R})B_i/B_{\rho(j)}$
- $\mathsf{Pair}(\vec{x}, (\mathbf{M}, \rho)) \to \mathbf{E} \in \mathbb{Z}_p^{2\times\ell\cdot d}$ such that $(c_1, c_2)^\top \mathbf{E}\big((k_j)_{j\in[\ell]}, (k_{i,j})_{i\in[d], j\in[\ell], \rho(j)\neq i}\big) = c_1 \cdot_{\mathrm{rf}} \sum^{\mathrm{rf}}_{j\in[\ell]} \omega_j k_j +_{\mathrm{rf}} c_2 \cdot_{\mathrm{rf}} \sum^{\mathrm{rf}}_{j\in[\ell], i\in[d], i\neq\rho(j)} x_i \omega_j k_{i,j}$.

Then, we give an unbounded KP-ABE that improves upon [57] (which is proved selectively secure under Q-type assumption), and thereby gives the most efficient unbounded KP-ABE to our knowledge (see the table Figure 4 for a precise comparison).

Unbounded KP-ABE

Here, $\mathcal{U} := \mathbb{Z}_p$, $\mathcal{X} := \{\Gamma \subseteq \mathbb{Z}_p\}$, $\mathcal{Y} := \mathbb{Z}_p^{\ell\times\ell'} \times ([\ell] \to \mathbb{Z}_p)$.

- $n = 2$, $\vec{B} := (B_1, B_2)$; $w_1 = |\Gamma|$, $\vec{S} := (S, S_i)_{i\in\Gamma}$; $m_1 := \ell' - 1$.
- $\mathsf{sE}(\Gamma) \to \Big(\big(S_i(B_1 + iB_2)\big)_{i\in\Gamma}, \big(S - S_i\big)_{i\in\Gamma}\Big)$
- $\mathsf{rE}(\mathbf{M}, \rho) \to \Big(\big(\mathbf{M}_j^\top(A, \vec{R})/(B_1 + \rho(j)B_2)\big)_{j\in[\ell]}, \big(\mathbf{M}_j^\top(A, \vec{R})\big)_{j\in[\ell]}\Big)$
- $\mathsf{Pair}(\vec{x}, (\mathbf{M}, \rho)) \to \begin{pmatrix} \mathbf{E} & \mathbf{0} \\ \mathbf{0} & \mathbf{E} \end{pmatrix} \in \mathbb{Z}_p^{2|\Gamma|\times 2\ell}$, where for all $i \in \Gamma$ and all $j \in [\ell]$ the element of the row associated to i in $\mathbf{E} \in \mathbb{Z}_p^{|\Gamma|\times\ell}$ and column j equals ω_j if $i = \rho(j)$ and 0 otherwise.

We also give a new adaptively secure CP-ABE where ciphertexts are half the size of [62], while the latter prove selective security based on Q-type assumptions.

CP-ABE

Here, $\mathcal{U} := [d]$, $\mathcal{X} := \mathbb{Z}_p^{\ell\times\ell'} \times ([\ell] \to [d])$, $\mathcal{Y} := \{0,1\}^d$.

- $n = d$, $\vec{B} := (B_1, \ldots, B_d)$; $w_1 = \ell' - 1$, $\vec{S} := (S, \vec{U})$; $m_1 := 1$, $\vec{R} := R$.
- $\mathsf{sE}(\mathbf{M}, \rho) \to \Big(\big(\mathbf{M}_i^\top(S, \vec{U})B_{\rho(i)}\big)_{i\in[\ell]}, S\Big)$
- $\mathsf{rE}(\vec{x}) \to \big((x_j R/B_j)_{j\in[d]}, A - R\big)$
- $\mathsf{Pair}((\mathbf{M}, \rho), \vec{x}) \to \begin{pmatrix} \mathbf{E} & \vec{0} \\ \vec{0}^\top & 1 \end{pmatrix} \in \mathbb{Z}_p^{(\ell+1)\times(d+1)}$, where for all $i \in [\ell]$, $j \in [d]$, $E_{i,j} = \omega_i$ if $\rho(i) = j$, 0 otherwise.

Finally, we give an new, adaptively secure, unbounded CP-ABE where secret key size and decryption time are roughly half that state of the art [57], whose selective security is based on Q-type assumptions.

Unbounded CP-ABE

Here, $\mathcal{U} := \mathbb{Z}_p$, $\mathcal{X} := \mathbb{Z}_p^{\ell\times\ell'} \times ([\ell] \to \mathbb{Z}_p)$, $\mathcal{Y} := \{\Gamma \subseteq \mathbb{Z}_p\}$.

- $n = 4$, $\vec{B} := (B_1, B_2, V, W)$; $w_1 = (\ell' - 1) + |\Gamma|$, $\vec{S} := (S, \vec{U}, S_i)_{i\in\Gamma}$; $m_1 := 1$, $\vec{R} := R$.
- $\mathsf{sE}(\mathbf{M}, \rho) \to \Big(S_i(B_1 + \rho(i)B_2), -VS_i + W\mathbf{M}_i^\top(S, \vec{U}), \mathbf{M}_i^\top(S, \vec{U})\Big)_{i\in[\ell]}\Big)$
- $\mathsf{rE}(\Gamma) \to \Big(\big(RV/(B_1 + jB_2)\big)_{j\in\Gamma}, R, A - WR\Big)$
- $\mathsf{Pair}((\mathbf{M}, \rho), \Gamma) \to \begin{pmatrix} \mathbf{E} & \vec{0} & \vec{0} \\ \vec{0} & \vec{e} & \vec{0} \\ \vec{0} & \vec{0} & \vec{e} \end{pmatrix} \in \mathbb{Z}_p^{3\ell\times(|\Gamma|+2)}$, where for all $i \in [\ell]$, $j \in [d]$, $E_{i,j} = \omega_i$ if $\rho(i) = j$, 0 otherwise. For all $i \in [\ell]$, $e_i = \omega_i$ if $\rho(i) \in \Gamma$, 0 otherwise.

6 AUTOMATED PROOFS

Our main result entails that symbolic security implies security in the GGM for every RFI ABE. Conversely, an attack against symbolic security usually represents a generic attack.[6] In this section, we present a constraint-solving method for (dis)proving symbolic security of RFI ABE. Our method proceeds in two steps: we encode symbolic security as a constraint (written in a fragment of first-order logic); then we use proof rules for proving its (non-)validity. In this section, we present the syntax of constraints and give some proof rules. Then, we show how our method can be used to obtain a proof of symbolic security of the IBE1 example, and to find a subtle attack. Finally, we present an implementation of the tool, and summarize some experimental results.

Technically, the main difficulty is to reason about equations and inequations that combine rational fractions and big operators, i.e. expressions of the form $\sum_{i\in Q} e_i$ or $\prod_{i\in Q} e_i$, where Q is a set of arbitrary size—informally, corresponding to adversary queries. Because neither symbolic computation nor algorithmic verification tools can deal with big operators (the former do not support big operators and the latter operate on a bounded state space), we develop deductive methods for solving systems of equations.

Constraints. We use a rich language of constraints that can express the existence of solutions of systems of equations and inequations between rational expressions. In order to accommodate case analysis, the language also features disjunction at top level. Thus constraints are of the form

$$\exists\vec{x_1}.\, C_1 \vee \ldots \vee \exists\vec{x_k}.\, C_k$$

where each C is a finite conjunction of (in-)equations. Due to the presence of big operators, (in-)equations may be universally quantified over arbitrary sets Q. Therefore, and without loss of generality, each C is a finite conjunction of atoms of the following form:

- equation: $\mathcal{E} = 0$;
- inequation: $\mathcal{E} \neq 0$;
- universal equation: $\forall\, k \in \mathcal{K}.\, \mathcal{E} = 0$;
- universal inequation: $\forall\, k \in \mathcal{K}.\, \mathcal{E} \neq 0$.

where $\mathcal{E}$ ranges over expressions. The syntax of expressions is presented in Figure 6. Expressions $\mathcal{E}$ must be well-typed, which we enforce by declaring a type for each variable, and imposing a simple typing discipline on expressions. For example, matrices appearing in our equations are typed with a dimension and we require that these dimensions are consistent for matrix addition and

[6] An attack against symbolic security could potentially require an exponential number of keys, and in that case, it would not correspond to an efficient attack on the scheme.

com-den	$\sum_{i \in K} \mathcal{E}_i / \mathcal{E}'_i \rightsquigarrow \dfrac{\sum_{i \in K} \mathcal{E}_i \times \prod_{j \in K \setminus \{i\}} \mathcal{E}'_j}{\prod_{i \in K} \mathcal{E}'_i}$
mul-split	$\mathcal{E} * \mathcal{E}' = 0 \rightsquigarrow \mathcal{E} = 0 \lor \mathcal{E}' = 0$
div-split	$\mathcal{E} / \mathcal{E}' = 0 \rightsquigarrow \mathcal{E} = 0 \land \mathcal{E}' \neq 0$
eval-var	$\mathcal{E} = 0 \rightsquigarrow \mathcal{E} = 0 \land \mathcal{E}[v \mapsto \mathcal{E}'] = 0$ for variable v and a closed (variable-free) expression $\mathcal{E}'$
extr-coeff	$\mathcal{E} * v + \mathcal{E}' = 0 \rightsquigarrow \mathcal{E} = 0 \land \mathcal{E}' = 0$ where v is a variable and $\mathcal{E}, \mathcal{E}'$ do not contain v
zero-prod	$\prod_{i \in K} \mathcal{E}_i = 0 \rightsquigarrow \exists j \in K : \mathcal{E}_j = 0$
non-zero-sum	$\sum_{i \in K} \mathcal{E}_i \neq 0 \rightsquigarrow \exists j \in K : \mathcal{E}_j \neq 0$
idx-split	$\exists i \in K. \mathcal{S}_i \rightsquigarrow (\exists i \in K \setminus \{j\}. \mathcal{S}_i) \lor \mathcal{S}_j$

Table 1: Selected constraint-solving rules

sets $\quad Q = [q].$
params $\quad x^*, y_i, a_i \in \mathbb{Z}_p \; \forall i \in Q.$
vars $\quad S, B, A \in \mathbb{Z}_p.$

$$\begin{aligned} &\forall i \in Q : y_i \neq x^* && \land \\ &\sum_{i \in Q} a_i \frac{S(B + x^*)A}{B + y_i} = AS \end{aligned}$$

Figure 5: Input file for the symbolic security of IBE 1

multiplication. Additionally, operators like ∘ (pair-wise product) and diag (diagonal matrix) are enforced to be applied to vectors only (matrices with dimension $n \times 1$ or $1 \times n$).

Constraint-solving system. The constraint-solving system consists of two parts: proof rules and proof search.

Proof rules are of the form $\mathcal{D} \rightsquigarrow \mathcal{D}'$. Rules can either be simplification rules or case distinction rules. Simplification rules turn systems into simpler ones. The rules are *sound* in the sense that they preserve solutions, i.e., if the new system contains a contradictory equation like $1 = 0$ or $0 \neq 0$, it is guaranteed that the original system is unsatisfiable. Case distinctions transform one single system into several systems of equations. Soundness is guaranteed because these transformations are such that if the original system has a solution, at least one of the derived new systems will have a solution. In turn, the new equations can trigger further simplifications. Table 1 contains some key rules: com-den can be used to push the division operation outermost, by multiplying and dividing by the common denominator of the summation terms; eval-var exploits the fact that if a polynomial equation is zero, it has to be zero for every evaluation of its variables; eval-coeff uses similar ideas than the previous rule, but is applied to expressions that do not include divisions; zero-prod is semantically sound because $\mathbb{Z}_p$ is an integral domain; finally div-split, mul-split and idx-split (the last two are examples of case-distinction rules) allow to split the system into more restricted cases.

Proof search is a series of heuristics that repeatedly selects and applies rules until it is shown that the system has no solution (or on the contrary is solvable). Since all rules are sound, the proof search algorithm is trivially sound.

Example. We illustrate our constraints solving methodology with an example. Consider the system of equations in Figure 5, that corresponds to the symbolic security of the IBE1 from Section 5.1. A solution to such a system consists of concrete values for $q \in \mathbb{N}$ and the parameters $x^*, y_i, a_i \in \mathbb{Z}_p$ for every $i \in [q]$ such that all the equations hold simultaneously treating S, B, A as formal variables (note that equality must be treated as the equivalence relation $\sim_{\mathrm{rf}}$ defined in Section 2).

The first step consists of getting rid of divisions. To do so, we apply rules com-div and div-split in this case. These rules, combined with other standard simplification rules will transform the system into:

$$\begin{aligned} &\forall i \in y_i - x^* \neq 0 && \land \\ &\prod_{i \in Q} (B + y_i) = \sum_{i \in Q} \Big(\prod_{j \in Q \setminus \{i\}} B + y_j \Big) a_i (B + x^*) && \land \\ &\forall i \in Q : B + y_i \neq 0 \end{aligned}$$

Now, the application of the rule eval-var to the second equation with variable B and $\mathcal{E}' = -x^*$ will add the equation $\prod_{i \in Q}(-x^* + y_i) = 0$ to the system, which can be further simplified by zero-prod. The system becomes:

$$\begin{aligned} &\exists k \in Q : \\ &\qquad \forall i \in Q : y_i - x^* \neq 0 && \land \\ &\qquad \prod_{i \in Q} (B + y_i) = \sum_{i \in Q} \Big(\prod_{j \in Q \setminus \{i\}} B + y_j \Big) a_i (B + x^*) && \land \\ &\qquad \forall i \in Q : B + y_i \neq 0 && \land \\ &\qquad - x^* + y_k = 0 \end{aligned}$$

which will be reduced to a contradiction after applying standard simplification rules, because the first and the fourth equations are contradictory.

Finding Attacks. Our tool can be used to find attacks for primitives that *look secure.* We present an attack (found by our tool) for the candidate Unbounded KP-ABE$^{\triangle}$ below:

$$\mathcal{U} := \mathbb{Z}_p, \mathcal{X} := \{\Gamma \subseteq \mathbb{Z}_p\}, \mathcal{Y} := \mathbb{Z}_p^{\ell \times \ell'} \times ([\ell] \to \mathbb{Z}_p).$$

- $n = 1, \vec{B} := B; w_1 = 0, \vec{S} := S; m_1 := \ell' - 1$
- $\mathsf{sE}(\Gamma) \longrightarrow \big(S_i(B + i), S - S_i\big)_{i \in S}$
- $\mathsf{rE}(\mathbf{M}, \rho) \longrightarrow \big(\mathbf{M}_j^\top (A, \vec{R})/(B + \rho(j)), \mathbf{M}_j^\top (A, \vec{R})\big)_{j \in [\ell]}$

The attack works as follows: first, the challenger samples $b, a \overset{R}{\leftarrow} \mathbb{Z}_p$ and makes $[b]_1, [a]_T$ public. The adversary queries a secret key for policy $\mathbf{M} = (1, 0, \ldots, 0), \rho(1) = 3$ which is satisfied iff the set of attributes contains attribute 3. The adversary will be given $\mathsf{sk} = (\mathsf{sk}_1, \mathsf{sk}_2) = ([a/(b + 3)]_2, [a]_2)$. Then, it picks two messages at

$$\begin{array}{ll}
\mathcal{D} ::= \mathcal{D} \vee \mathcal{D} \mid \mathcal{S} & \text{disjunction} \\
\mathcal{S} ::= \exists k \in \mathcal{K}.\, \mathcal{S} \mid C & \text{symbolic constraint } (k \in \mathsf{Idx}) \\
C ::= C \wedge C \mid \forall\, k \in \mathcal{K}.\, C & \text{conjunction } (k \in \mathsf{Idx}) \\
\quad \mid \mathcal{E} = 0 \mid \mathcal{E} \neq 0 & \\
\mathcal{E} ::= \mathcal{E} + \mathcal{E} \mid \mathcal{E} * \mathcal{E} \mid \mathcal{E}/\mathcal{E} & \text{expression } (k \in \mathsf{Idx}) \\
\quad \mid \mathcal{E} \circ \mathcal{E} \mid \mathsf{diag}(\mathcal{E}) & \\
\quad \mid \sum_{k \in \mathcal{K}} \mathcal{E} \mid \prod_{k \in \mathcal{K}} \mathcal{E} & \\
\quad \mid -\mathcal{E} \mid \mathcal{E}^{\top} \mid \mathcal{M} \mid S & \text{atom } (S \in \mathbb{Z}) \\
\mathcal{K} ::= \Gamma \mid \mathcal{K} \setminus \{k\} & \text{index set } (k \in \mathsf{Idx}, \Gamma \in \mathsf{Set})
\end{array}$$

We assume given sets Var, Par, Idx, Set of *variables*, *parameters*, *indices* and *index sets* respectively. Matrices $\mathcal{M}$ are associated to a name $\rho \in$ Var $\cup$ Par, a dimension $m \times n$ ($m, n \in \mathbb{N}$) and a domain $\mathbb{Z}_p$ or $\{0,1\} \subset \mathbb{Z}_p$. Our syntax $\circ$ stands for pair-wise product between vectors. Additionally, for a vector $v \in \mathbb{Z}_p^n$, $\mathsf{diag}(\vec{v})$ represents the null matrix in $\mathbb{Z}_p^{n \times n}$, where the main diagonal is replaced by vector $\vec{v}$.

Figure 6: Grammar for symbolic constraints

random and sends them together with the target set for attributes $\Gamma = \{1,2\}$. It will receive

$$\mathsf{ct} = (\mathsf{ct}_1, \mathsf{ct}_2, \mathsf{ct}_3, \mathsf{ct}_4) = ([s_1(b+1)]_1, [s-s1]_1, [s_2(b+2)]_1, [s-s2]_1)$$

where s, s_1, s_2 are fresh random values in $\mathbb{Z}_p$. Now, the following linear combination

$$\begin{gathered}
-e(\mathsf{ct}_1, \mathsf{sk}_1) + 2e(\mathsf{ct}_2, \mathsf{sk}_1) - e(\mathsf{ct}_2, \mathsf{sk}_2) + \\
2e(\mathsf{ct}_3, \mathsf{sk}_1) - 2e(\mathsf{ct}_4, \mathsf{sk}_1) + 2e(\mathsf{ct}_4, \mathsf{sk}_2)
\end{gathered}$$

equals the symmetric key $\kappa = [as]_T$ derived from encryption. This allows the adversary to fully recover the plaintext and win the experiment. This is because

$$\begin{gathered}
-S_1 A \frac{B+1}{B+3} + 2A \frac{S-S_1}{B+3} - A(S-S_1) + \\
2S_2 A \frac{B+2}{B+3} - 2A \frac{S-S_2}{B+3} + 2A(S-S_2) =_{\mathrm{rf}} AS.
\end{gathered}$$

The above attack can be easily missed when designing the primitive, since it involves a linear combination of six terms on a primitive that at a first sight, looks secure. This is an evidence of the subtleties that inversion in the exponent and the GGM may involve and it justifies the need of rigorous formalization and the design of automated methods for verification.

Implementation and case studies. We have implemented our method in a tool[7] and used the tool on several case studies. Table 2 summarizes the results. Our tool is able to prove automatically the symbolic security of our encodings IBE 1, IBE 2, IPE 1, IPE 2 and several encodings from the literature, like CP-ABE's and KP-ABE's from [36], or the CP-ABE for negated boolean formulas from [11]. For the most complex examples, like our CP-ABE and KP-ABE, our tool is only able to prove security for fixed-size dimensions. In some cases this is because it is hard to express the security of the full scheme with our grammar, while in others, our heuristics do not succeed in finding a proof. The tool is also able to find the attack against the candidate Unbounded KP-ABE$^{\triangle}$ automatically.

Scheme	Time (s)	Proof	Security
IBE 1 [64]	0.016	✓	Many-key
IBE 2 [27]	0.001	✓	One-key*
IPE 1 [46]	0.001	✓	One-key*
IPE 2 (New)	0.027	✓	Many-key
KP-ABE [41]	-	×	-
Compact KP-ABE (New)	-	×	-
Unbounded KP-ABE (New)	-	×	-
KP-ABE [41]	-	×	-
(fixed-size $d = \ell = \ell' = 2$)	0.046	✓	One-key
(fixed-size $d = \ell = \ell' = 3$)	1.52	✓	One-key
CP-ABE (New)	-	×	-
(fixed-size $d = \ell = \ell' = 2$)	0.212	✓	One-key
(fixed-size $d = \ell = \ell' = 3$)	5.75	✓	One-key
Spatial Encryption [36]	0.005	✓	One-key*
Doubly Spatial Enc. [36]	0.013	✓	One-key*
KP-ABE [36]	0.256	✓	One-key*
CP-ABE [36]	0.206	✓	One-key*
NIPE,ZIPE [36]	0.003	✓	One-key*
CP-ABE for negated bf. [11]	0.084	✓	One-key*
Unbounded KP-ABE$^{\triangle}$	0.006	Attack	Insecure

Table 2: Encodings analyzed with our automatic tool. The first group corresponds to the encodings from this paper (Section 5). ✓ means the tool fully proved the scheme, × means it could not prove the scheme. For every scheme we provide the level of symbolic security that was analyzed. For the schemes marked with *, one-key symbolic security is enough to achieve many-key security in the GGM (see Theorem 4.1).

Comparison with previous work. We note that our tool follows the approach of the Generic Group Analyzer, gga [20] and the Generic Group Analyzer Unbounded, gga$^{\infty}$ [10], and as the later our tool can express systems of equations depending on an unbounded number of terms, which allows to handle many security experiments of interest. Additionally, our tool is defined over a new grammar (described in Figure 6) and therefore, it complements previous tools and broadens the class of schemes than can be analyzed with computer-assistance. In particular, our handling of division / and big products $\prod$ suffices to handle many of the primitives proposed in this work.

7 PERFORMANCE EVALUATION

We have implemented the schemes introduced in the previous section, as well as several Identity-Based Encryption from the literature. Our implementation uses Charm [7] for pairings with a prime-order

[7] Source code available at https://github.com/miguel-ambrona/ggm-symbolic-solver.

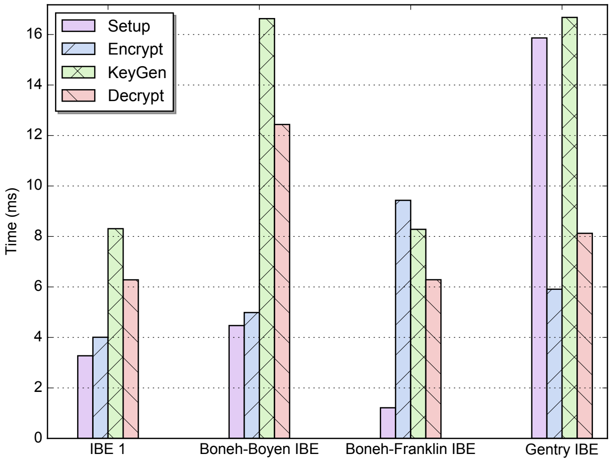

Figure 7: Execution time for different IBE schemes

IBE	mpk	msk	ct	sk
IBE 1	$\mathbb{G}_1 \times \mathbb{G}_T$	$\mathbb{Z}_p^2$	$\mathbb{G}_1$	$\mathbb{G}_2$
BonBoy [26]	$\mathbb{G}_1^2 \times \mathbb{G}_T$	$\mathbb{Z}_p^3$	$\mathbb{G}_1^2$	$\mathbb{G}_2^2$
BonFra [30]	$\mathbb{G}_1 \times (\mathbb{Z}_p \to \mathbb{G}_2)$	$\mathbb{Z}_p$	$\mathbb{G}_1$	$\mathbb{G}_2$
Gentry [40]	$\mathbb{G}_1 \times \mathbb{G}_2 \times \mathbb{G}_T$	$\mathbb{Z}_p$	$\mathbb{G}_1 \times \mathbb{G}_T$	$\mathbb{Z}_p \times \mathbb{G}_2$

Table 3: Key and ciphertext sizes of IBE algorithms

224-bits Miyaji, Nakabayashi and Takano Curve [52]. The experiments were executed on a 2.40GHz Intel Core i7-3630QM CPU with 8GB of RAM. We use our implementations to compare the performance between the different schemes (see Figure 7). Expectedly, IBE1 outperforms other constructions, highlighting the usual trade-off between efficiency and security in the standard model. We provide more details below.

For every construction, we evaluate the performance of *setup*, *encryption*, *key generation* and *decryption* on 100 executions, displaying the average time (in milliseconds). *Encryption* and *key generation* take an identity as input, which is chosen uniformly at random (in $\mathbb{Z}_p$) in every execution (this is not considered part of the execution time). We also include the IBE of Boneh and Franklin [29], arguably on of the most efficient IBE (which is proven secure in the Random Oracle Model). Note that the encryption in IBE 1 is more efficient that in [29], since contrary to the latter, IBE 1 does not require to hash into the source group $\mathbb{G}_1$, and it does not require to compute a pairing. To make the comparison more fair, in our implementation of [29], we consider a naive and efficient hashing from $\mathbb{Z}_p$ into $\mathbb{G}_1$ (performed once in encryption and once in key generation). Note, however, that for security, this hashing cannot be done naively (see [33] for instance).

8 CONCLUDING REMARKS

We have presented an automated method for analyzing security of ABE in the Generic Group Model. Our work significantly broadens the scope of automated analyses in the Generic Group Model, and nicely complements prior works on proving security of ABE in the standard model. We have shown how our tool can be used for proving automatically security of several schemes, including some variants of previous schemes or new schemes, and for discovering subtle attacks.

There are many directions for further work. On the theoretical side, it would be interesting to prove that RFI ABE are selectively secure in the standard model, under a strong Q-type assumption. On the practical side, it would be very interesting to develop synthesis techniques for exploring the space of RFI ABE. As in prior works using synthesis [10, 22], we plan to explore large classes of constructions systematically, using our tool for finding attacks and proofs. In order to achieve broader coverage (in other words minimize the number of schemes for which the tool times out), we intend to improve the efficiency of the tool both for finding attacks and proofs. Moreover, it would be desirable to establish mathematical theorems that justify focusing on more restricted, tractable, classes of constructions—else the search space far exceeds current computing capabilities. Beyond ABE, it seems appealing to explore whether our tool could be used for Structure-Preserving Signatures and in particular to synthesize Structure-Preserving Signatures based on rational fractions.

Acknowledgments. This work is partially supported by ONR Grants N000141210914 and N000141512750 (Barthe), a Google PhD Fellowship (Gay), and ERC Project aSCEND (H2020 639554) and NSF Award CNS-1445424 (Wee).

REFERENCES

[1] M. Abe, G. Fuchsbauer, J. Groth, K. Haralambiev, and M. Ohkubo. Structure-preserving signatures and commitments to group elements. In T. Rabin, editor, *CRYPTO 2010*, volume 6223 of *LNCS*, pages 209–236. Springer, Heidelberg, Aug. 2010.

[2] M. Abe, J. Groth, K. Haralambiev, and M. Ohkubo. Optimal structure-preserving signatures in asymmetric bilinear groups. In P. Rogaway, editor, *CRYPTO 2011*, volume 6841 of *LNCS*, pages 649–666. Springer, Heidelberg, Aug. 2011.

[3] M. Abe, J. Groth, and M. Ohkubo. Separating short structure-preserving signatures from non-interactive assumptions. In D. H. Lee and X. Wang, editors, *ASIACRYPT 2011*, volume 7073 of *LNCS*, pages 628–646. Springer, Heidelberg, Dec. 2011.

[4] M. Abe, J. Groth, M. Ohkubo, and M. Tibouchi. Unified, minimal and selectively randomizable structure-preserving signatures. In Y. Lindell, editor, *TCC 2014*, volume 8349 of *LNCS*, pages 688–712. Springer, Heidelberg, Feb. 2014.

[5] S. Agrawal and M. Chase. A study of pair encodings: Predicate encryption in prime order groups. In E. Kushilevitz and T. Malkin, editors, *TCC 2016-A, Part II*, volume 9563 of *LNCS*, pages 259–288. Springer, Heidelberg, Jan. 2016.

[6] S. Agrawal and M. Chase. Simplifying design and analysis of complex predicate encryption schemes. In J.-S. Coron and J. B. Nielsen, editors, *Advances in Cryptology – EUROCRYPT 2017: 36th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Paris, France, April 30 – May 4, 2017, Proceedings, Part I*, pages 627–656, Cham, 2017. Springer International Publishing.

[7] J. A. Akinyele, C. Garman, I. Miers, M. W. Pagano, M. Rushanan, M. Green, and A. D. Rubin. Charm: a framework for rapidly prototyping cryptosystems. *Journal of Cryptographic Engineering*, 3(2):111–128, 2013.

[8] J. A. Akinyele, M. Green, and S. Hohenberger. Using SMT solvers to automate design tasks for encryption and signature schemes. In A.-R. Sadeghi, V. D. Gligor, and M. Yung, editors, *ACM CCS 13*, pages 399–410. ACM Press, Nov. 2013.

[9] J. A. Akinyele, M. W. Pagano, M. D. Green, C. U. Lehmann, Z. N. J. Peterson, and A. D. Rubin. Securing electronic medical records using attribute-based encryption on mobile devices. In X. Jiang, A. Bhattacharya, P. Dasgupta, and W. Enck, editors, *SPSM'11, Proceedings of the 1st ACM Workshop Security and Privacy in Smartphones and Mobile Devices, Co-located with CCS 2011, October 17, 2011, Chicago, IL, USA*, pages 75–86. ACM, 2011.

[10] M. Ambrona, G. Barthe, and B. Schmidt. Automated unbounded analysis of cryptographic constructions in the generic group model. In M. Fischlin and J.-S. Coron, editors, *EUROCRYPT 2016, Part II*, volume 9666 of *LNCS*, pages 822–851. Springer, Heidelberg, May 2016.

[11] M. Ambrona, G. Barthe, and B. Schmidt. Generic transformations of predicate encodings: Constructions and applications. In *CRYPTO*, 2017.

[12] 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.

[13] 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.

[14] N. Attrapadung, B. Libert, and E. de Panafieu. Expressive key-policy attribute-based encryption with constant-size ciphertexts. In D. Catalano, N. Fazio, R. Gennaro, and A. Nicolosi, editors, *PKC 2011*, volume 6571 of *LNCS*, pages 90–108. Springer, Heidelberg, Mar. 2011.

[15] R. Baden, A. Bender, N. Spring, B. Bhattacharjee, and D. Starin. Persona: An online social network with user-defined privacy. In *Proceedings of the ACM SIGCOMM 2009 Conference on Data Communication*, SIGCOMM '09, pages 135–146, New York, NY, USA, 2009. ACM.

[16] C. E. Z. Baltico, D. Catalano, and D. Fiore. Practical functional encryption for bilinear forms. *IACR Cryptology ePrint Archive*, 2016:1104, 2016.

[17] C. E. Z. Baltico, D. Catalano, D. Fiore, and R. Gay. Practical functional encryption for quadratic functions with applications to predicate encryption. *IACR Cryptology ePrint Archive*, 2017:151, 2017.

[18] G. Barthe. High-assurance cryptography: Cryptographic software we can trust. *IEEE Security & Privacy*, 13(5):86–89, 2015.

[19] G. Barthe, J. Cederquist, and S. Tarento. A machine-checked formalization of the generic model and the random oracle model. In D. A. Basin and M. Rusinowitch, editors, *Automated Reasoning - Second International Joint Conference, IJCAR 2004, Cork, Ireland, July 4-8, 2004, Proceedings*, volume 3097 of *Lecture Notes in Computer Science*, pages 385–399. Springer, 2004.

[20] G. Barthe, E. Fagerholm, D. Fiore, J. C. Mitchell, A. Scedrov, and B. Schmidt. Automated analysis of cryptographic assumptions in generic group models. In J. A. Garay and R. Gennaro, editors, *CRYPTO 2014, Part I*, volume 8616 of *LNCS*, pages 95–112. Springer, Heidelberg, Aug. 2014.

[21] G. Barthe, E. Fagerholm, D. Fiore, A. Scedrov, B. Schmidt, and M. Tibouchi. Strongly-optimal structure preserving signatures from type II pairings: Synthesis and lower bounds. In J. Katz, editor, *Public-Key Cryptography - PKC 2015 - 18th IACR International Conference on Practice and Theory in Public-Key Cryptography, Gaithersburg, MD, USA, March 30 - April 1, 2015, Proceedings*, volume 9020 of *Lecture Notes in Computer Science*, pages 355–376. Springer, 2015.

[22] G. Barthe, E. Fagerholm, D. Fiore, A. Scedrov, B. Schmidt, and M. Tibouchi. Strongly-optimal structure preserving signatures from type II pairings: Synthesis and lower bounds. In J. Katz, editor, *PKC 2015*, volume 9020 of *LNCS*, pages 355–376. Springer, Heidelberg, Mar. / Apr. 2015.

[23] G. Barthe, B. Grégoire, S. Heraud, and S. Zanella Béguelin. Computer-aided security proofs for the working cryptographer. In P. Rogaway, editor, *CRYPTO 2011*, volume 6841 of *LNCS*, pages 71–90. Springer, Heidelberg, Aug. 2011.

[24] G. Barthe, B. Grégoire, and B. Schmidt. Automated proofs of pairing-based cryptography. In I. Ray, N. Li, and C. Kruegel:, editors, *ACM CCS 15*, pages 1156–1168. ACM Press, Oct. 2015.

[25] A. Beimel. *Secure Schemes for Secret Sharing and Key Distribution*. Ph.D., Technion - Israel Institute of Technology, 1996.

[26] D. Boneh and X. Boyen. Efficient selective-ID secure identity based encryption without random oracles. In C. Cachin and J. Camenisch, editors, *EUROCRYPT 2004*, volume 3027 of *LNCS*, pages 223–238. Springer, Heidelberg, May 2004.

[27] D. Boneh and X. Boyen. Secure identity based encryption without random oracles. In M. Franklin, editor, *CRYPTO 2004*, volume 3152 of *LNCS*, pages 443–459. Springer, Heidelberg, Aug. 2004.

[28] D. Boneh, X. Boyen, and E.-J. Goh. Hierarchical identity based encryption with constant size ciphertext. In R. Cramer, editor, *EUROCRYPT 2005*, volume 3494 of *LNCS*, pages 440–456. Springer, Heidelberg, May 2005.

[29] D. Boneh and M. K. Franklin. Identity-based encryption from the Weil pairing. In J. Kilian, editor, *CRYPTO 2001*, volume 2139 of *LNCS*, pages 213–229. Springer, Heidelberg, Aug. 2001.

[30] D. Boneh and M. K. Franklin. Identity based encryption from the Weil pairing. *SIAM Journal on Computing*, 32(3):586–615, 2003.

[31] X. Boyen. Miniature CCA2 PK encryption: Tight security without redundancy. In K. Kurosawa, editor, *ASIACRYPT 2007*, volume 4833 of *LNCS*, pages 485–501. Springer, Heidelberg, Dec. 2007.

[32] X. Boyen. The uber-assumption family (invited talk). In S. D. Galbraith and K. G. Paterson, editors, *PAIRING 2008*, volume 5209 of *LNCS*, pages 39–56. Springer, Heidelberg, Sept. 2008.

[33] E. Brier, J.-S. Coron, T. Icart, D. Madore, H. Randriam, and M. Tibouchi. Efficient indifferentiable hashing into ordinary elliptic curves. In T. Rabin, editor, *CRYPTO 2010*, volume 6223 of *LNCS*, pages 237–254. Springer, Heidelberg, Aug. 2010.

[34] M. Chase and S. Meiklejohn. Déjà Q: Using dual systems to revisit q-type assumptions. In P. Q. Nguyen and E. Oswald, editors, *EUROCRYPT 2014*, volume 8441 of *LNCS*, pages 622–639. Springer, Heidelberg, May 2014.

[35] S. Chatterjee and A. Menezes. Type 2 structure-preserving signature schemes revisited. In T. Iwata and J. H. Cheon, editors, *ASIACRYPT 2015, Part I*, volume 9452 of *LNCS*, pages 286–310. Springer, Heidelberg, Nov. / Dec. 2015.

[36] 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.

[37] 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.

[38] J. Chen and H. Wee. Dual system groups and its applications — compact hibe and more. Cryptology ePrint Archive, Report 2014/265, 2014. http://eprint.iacr.org/2014/265.

[39] C. Cocks. An identity based encryption scheme based on quadratic residues. In B. Honary, editor, *Cryptography and Coding, 8th IMA International Conference*, volume 2260 of *LNCS*, pages 360–363, Cirencester, UK, Dec. 17–19, 2001. Springer, Heidelberg.

[40] C. Gentry. Practical identity-based encryption without random oracles. In S. Vaudenay, editor, *EUROCRYPT 2006*, volume 4004 of *LNCS*, pages 445–464. Springer, Heidelberg, May / June 2006.

[41] 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.

[42] A. Guillevic. Comparing the pairing efficiency over composite-order and prime-order elliptic curves. In M. J. Jacobson Jr., M. E. Locasto, P. Mohassel, and R. Safavi-Naini, editors, *ACNS 13*, volume 7954 of *LNCS*, pages 357–372. Springer, Heidelberg, June 2013.

[43] M. Hamburg. *Spatial Encryption*. Ph.D. Thesis, Stanford University, California, 2011.

[44] M. Ion, J. Zhang, and E. M. Schooler. Toward content-centric privacy in ICN: attribute-based encryption and routing. In B. Ohlman, G. C. Polyzos, and L. Zhang, editors, *ICN'13, Proceedings of the 3rd, 2013 ACM SIGCOMM Workshop on Information-Centric Networking, August 12, 2013, Hong Kong, China*, pages 39–40. ACM, 2013.

[45] M. Karchmer and A. Wigderson. On span programs. In *Structure in Complexity Theory Conference, 1993., Proceedings of the Eighth Annual*, pages 102–111, May 1993.

[46] J. Katz, A. Sahai, and B. Waters. Predicate encryption supporting disjunctions, polynomial equations, and inner products. In N. P. Smart, editor, *EUROCRYPT 2008*, volume 4965 of *LNCS*, pages 146–162. Springer, Heidelberg, Apr. 2008.

[47] 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 H. Gilbert, editor, *EUROCRYPT 2010*, volume 6110 of *LNCS*, pages 62–91. Springer, Heidelberg, May 2010.

[48] 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.

[49] 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.

[50] J. Li, M. H. Au, W. Susilo, D. Xie, and K. Ren. Attribute-based signature and its applications. In D. Feng, D. A. Basin, and P. Liu, editors, *ASIACCS 10*, pages 60–69. ACM Press, Apr. 2010.

[51] U. M. Maurer. Abstract models of computation in cryptography (invited paper). In N. P. Smart, editor, *10th IMA International Conference on Cryptography and Coding*, volume 3796 of *LNCS*, pages 1–12. Springer, Heidelberg, Dec. 2005.

[52] A. Miyaji, M. Nakabayashi, and S. TAKANO. New explicit conditions of elliptic curve traces for fr-reduction, 2001.

[53] V. I. Nechaev. Complexity of a determinate algorithm for the discrete logarithm. *Mathematical Notes*, 55(2):165–172, 1994.

[54] T. Okamoto and K. Takashima. Hierarchical predicate encryption for inner-products. In M. Matsui, editor, *ASIACRYPT 2009*, volume 5912 of *LNCS*, pages 214–231. Springer, Heidelberg, Dec. 2009.

[55] T. Okamoto and K. Takashima. Fully secure functional encryption with general relations from the decisional linear assumption. In T. Rabin, editor, *CRYPTO 2010*, volume 6223 of *LNCS*, pages 191–208. Springer, Heidelberg, Aug. 2010.

[56] T. Okamoto and K. Takashima. Adaptively attribute-hiding (hierarchical) inner product encryption. In D. Pointcheval and T. Johansson, editors, *EUROCRYPT 2012*, volume 7237 of *LNCS*, pages 591–608. Springer, Heidelberg, Apr. 2012.

[57] Y. Rouselakis and B. Waters. Practical constructions and new proof methods for large universe attribute-based encryption. In A.-R. Sadeghi, V. D. Gligor, and M. Yung, editors, *ACM CCS 13*, pages 463–474. ACM Press, Nov. 2013.

[58] 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.

[59] A. Shamir. Identity-based cryptosystems and signature schemes. In G. R. Blakley and D. Chaum, editors, *CRYPTO'84*, volume 196 of *LNCS*, pages 47–53. Springer, Heidelberg, Aug. 1984.

[60] V. Shoup. Lower bounds for discrete logarithms and related problems. In W. Fumy, editor, *EUROCRYPT'97*, volume 1233 of *LNCS*, pages 256–266. Springer, Heidelberg, May 1997.

[61] 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.

[62] B. Waters. Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization. In D. Catalano, N. Fazio, R. Gennaro, and A. Nicolosi, editors, *PKC 2011*, volume 6571 of *LNCS*, pages 53–70. Springer, Heidelberg, Mar. 2011.

[63] 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.

[64] H. Wee. Déjà Q: Encore! Un petit IBE. In E. Kushilevitz and T. Malkin, editors, *TCC 2016-A, Part II*, volume 9563 of *LNCS*, pages 237–258. Springer, Heidelberg, Jan. 2016.

A PROOFS OF THE MAIN BODY

A.1 Proof of Theorem 3.1

Proof. For all $x \in \mathcal{X}, y \in \mathcal{Y}$ such that $\mathsf{P}(x, y) = 1$, we have: $f/g \sim_{\mathrm{rf}} AS_0$, where $\vec{c} := \mathsf{sE}(x)$, $\vec{k} := \mathsf{rE}(y)$, $\mathbf{E} := \mathsf{Pair}(x, y)$, and $f/g := \vec{c}^{\top}\mathbf{E}\vec{k}$. In particular, for all $\alpha \in \mathbb{Z}_p, \vec{b} \in \mathbb{Z}_p^n, \vec{r} \in \mathbb{Z}_p^{m_1}, \vec{s} \in \mathbb{Z}_p^{w+1}$ such that $g(\alpha, \vec{b}, \vec{r}) \neq 0$, we have $f(\alpha, \vec{b}, \vec{s}, \vec{r})/g(\alpha, \vec{b}, \vec{r}) = \alpha s_0$, and the key computed by Dec corresponds to the key computed by Enc on x. Thus, we simply have to bound the probability that g evaluates to 0 on a random point. To do so, we use the fact that $\deg(g) \leq d|\mathsf{sk}_y|$, where d is the degree of ABE. Therefore, by Lemma 2.1 (Schwartz-Zippel), the probability of a failed decryption is bounded by $\leq \frac{d|\mathsf{sk}_y|}{p}$. □

A.2 Proof of Lemma 3.2

Proof. The proof goes by contradiction. Suppose there is $x \in \mathcal{X}$, $\{\mathbf{E}_y^*\}_{y \in \mathcal{Y}_x}$ and $\gamma \in \mathbb{Z}_p$ such that $\sum_{y \in \mathcal{Y}_x} (\vec{B}, \vec{c}(\vec{S}, \vec{B}))^{\top} \mathbf{E}_y^* \vec{k}_y(\vec{R}_y, \vec{B}, A) + \gamma A \sim_{\mathrm{rf}} AS_0$. By evaluating the formal variable S_i for $i \in [0, w]$ to 0, we obtain

$$\sum_{y \in \mathcal{Y}_x} (\vec{B}, \vec{0})^{\top} \mathbf{E}_y^* \vec{k}_y(\vec{R}_y, \vec{B}, A) + \gamma A \sim_{\mathrm{rf}} 0.$$

Thus, $\sum_{y \in \mathcal{Y}_x} (\vec{0}, \vec{c}(\vec{S}, \vec{B}))^{\top} \mathbf{E}_y^* \vec{k}_y(\vec{R}_y, \vec{B}, A) \sim_{\mathrm{rf}} AS_0$. That is, the matrices $\{\underline{\mathbf{E}_y^*} \in \mathbb{Z}_p^{|\mathsf{ct}_x| \times q|\mathsf{sk}_y|}\}$, which comprise the $|\mathsf{ct}_x|$ lower rows of $\{\mathbf{E}_y^* \in \mathbb{Z}_p^{w+|\mathsf{ct}_x| \times q|\mathsf{sk}_y|}\}$, are such that $\sum_{y \in \mathcal{Y}_x} \vec{c}(\vec{S}, \vec{B})^{\top} \underline{\mathbf{E}_y^*} \vec{k}_y(\vec{R}_y, \vec{B}, A) \sim_{\mathrm{rf}} AS_0$, which contradicts the symbolic security of $\overline{\mathsf{ABE}}$. □

A.3 Proof of Theorem 3.3

The proof of Theorem 3.3 proceeds in two steps, first, it shows that the advantages $\mathsf{Adv}_{\mathsf{ABE},\mathcal{A}}^{\mathsf{GGM}}(\lambda)$ and $\mathsf{Adv}_{\mathsf{ABE},\mathcal{A}}^{\mathsf{SM}}(\lambda)$ are negligibly different. Then, it shows that $\mathsf{Adv}_{\mathsf{ABE},\mathcal{A}}^{\mathsf{SM}}(\lambda) = 0$, using the symbolic security of ABE.

Proof. We proceed via a hybrid argument, using Game_i for $i \in [0, Q_{\mathrm{eq}}]$, defined in Figure 8, and we denote by Adv_i the advantage of $\mathcal{A}$ in Game_i. It is clear that Game_0 is the same as $\mathsf{Exp}_{\mathsf{ABE}}^{\mathsf{GGM}}(1^{\lambda}, \mathcal{A})$, and $\mathsf{Game}_{Q_{\mathrm{eq}}}$ is the same as $\mathsf{Exp}_{\mathsf{ABE}}^{\mathsf{SM}}(1^{\lambda}, \mathcal{A})$. We show how to transition from Game_i to Game_{i+1} for all $i \in [0, Q_{\mathrm{eq}} - 1]$ in the following lemma.

Lemma A.1. *For all $i \in [0, Q_{\mathrm{eq}}]$,*

$$|\mathsf{Adv}_{i+1} - \mathsf{Adv}_i| \leq \frac{6d\big(2 + (n + |\mathsf{ct}|)Q_{\mathsf{sk}}|\mathsf{sk}|\big)}{p}.$$

Proof of Lemma A.1. First, in Lemma A.2, we give a bound on the degree of the rational fractions in the lists $L_s^{\sim}$ for $s \in \{1, 2, T\}$. Then, we apply Lemma 2.1 (Schwartz Zippel) to bound $|\mathsf{Adv}_{i+1} - \mathsf{Adv}_i|$.

Lemma A.2. *For all $s \in \{1, 2, T\}$, $f/g \in L_s^{\sim}$,*

$$\deg(f/g) \leq d\big(2 + (n + |\mathsf{ct}|)Q_{\mathsf{sk}}|\mathsf{sk}|\big).$$

Proof of Lemma A.2. First, note that for all $s \in \{1, 2, T\}$, $f/g \in L_s^{\sim}$ is a linear combination of rational fractions in $\widehat{L}_s$ where $\widehat{L}_1 := \{B_j | j \in [n]\} \cup \{\mathsf{sE}(x) | x \in \mathcal{Q}_{\mathrm{chal}}\}$, $\widehat{L}_2 := \{\mathsf{rE}(y) | y \in \mathcal{Q}_{\mathsf{sk}}\}$, $\widehat{L}_T := \{A, f_{\beta}^{\star}\} \cup \{f_1/g_1 \cdot_{\mathrm{rf}} f_2/g_2 | f_1/g_1 \in \widehat{L}_1, f_2/g_2 \in \widehat{L}_2\}$.

Thus, $s \in \{1, 2, T\}$, $f/g \in L_s^{\sim}$, $\deg(f/g) \leq d \cdot |\widehat{L}_s|$. We conclude the proof using the fact that

- $|\widehat{L}_1| \leq n + |\mathsf{ct}|$,
- $|\widehat{L}_2| \leq Q_{\mathsf{sk}}|\mathsf{sk}|$,
- $|\widehat{L}_s| \leq 2 + |\widehat{L}_1| \cdot |\widehat{L}_2|$.

□

Now, we bound $|\mathsf{Adv}_{i+1} - \mathsf{Adv}_i|$, using the fact that Game_{i+1} and Game_i only differs on the $i + 1$'st query to $\mathcal{O}_{\mathrm{eq}}$. In particular, the output of $\mathcal{O}_{\mathrm{eq}}(s, i', j')$, is different in these two games if (1) $L_s^{\sim}[i'] \sim_r f L_s^{\sim}[j']$ but $L_s^{\mathrm{eq}}[i'] \neq L_s^{\mathrm{eq}}[j']$, or (2) $L_s^{\mathrm{eq}}[i'] = L_s^{\mathrm{eq}}[j']$ but $L_s^{\sim}[i']$ not $\sim_r f L_s^{\sim}[j']$.

Let's consider the event (1). We write $L_s^{\sim}[i'] = f/g$ and $L_s^{\sim}[j'] = f'/g'$. Since $f/g \sim_{\mathrm{rf}} f'/g'$, we have for all points $\vec{x}$: $f(\vec{x}) \cdot g'(\vec{x}) = f(\vec{x}) \cdot g'(\vec{x})$. Moreover, if $g(\vec{x}), g'(\vec{x}) \neq 0$, then $f/g(\vec{x}) = f'/g'(\vec{x})$, that is, $L_s^{\mathrm{eq}}[i'] = L_s^{\mathrm{eq}}[j']$. Therefore, it suffices to bound the probability of the event: g or g' evaluates to 0 on a random point. By Lemma 2.1 (Schwartz Zippel), and Lemma A.2, we know this happens with probability at most: $\frac{2d\left(2+(n+|\mathsf{ct}|)Q_{\mathsf{sk}}|\mathsf{sk}|\right)}{p}$.

Let's now consider the event (2). If $L_s^{\mathrm{eq}}[i'] = L_s^{\mathrm{eq}}[j'] \neq \perp$, event (2) corresponds to the case where $fg' - fg' \neq 0$, and $(fg' - fg')(\vec{x}) = 0$, for a random point $\vec{x}$. By Lemma 2.1 (Schwartz Zippel), and Lemma A.2, we know this happens with probability at most: $\frac{2d\left(2+(n+|\mathsf{ct}|)Q_{\mathsf{sk}}|\mathsf{sk}|\right)}{p}$. Finally, using the same argument as for event (1), we can bound the probability that $L_s^{\mathrm{eq}}[i'] = L_s^{\mathrm{eq}}[j'] = \perp$ by $\frac{2d\left(2+(n+|\mathsf{ct}|)Q_{\mathsf{sk}}|\mathsf{sk}|\right)}{p}$.

Summing up, we obtain the lemma. □

Lemma A.3. $\mathsf{Adv}_{\mathsf{ABE},\mathcal{A}}^{\mathsf{SM}}(\lambda) = 0$.

Proof of Lemma A.3. We show that the view of any adversary $\mathcal{A}$ against $\mathsf{Exp}_{\mathsf{ABE}}^{\mathsf{SM}}(1^{\lambda}, \mathcal{A})$ is independent of β.

The only information that leaks about α is the output of $\mathcal{O}_{\sim}$ one queries of the form (T, i, j), for $i, j \in \mathbb{N}$. By Lemma A.2, we know that $L_T[i]$ and $L_T[j]$ are linear combinations of rational fractions in $\widehat{L}_T$, where $\widehat{L}_T$ is defined as in Lemma A.2. Namely, we write: $L_T[i] = \sum_{i \in [|\widehat{L}_T|]}^{\mathrm{rf}} \alpha_i \cdot f_i/g_i$, and $L_T[j] = \sum_{i \in [|\widehat{L}_T|]}^{\mathrm{rf}} \alpha'_i \cdot f_i/g_i$, for

$\underline{\mathrm{Game}_i(1^\lambda, \mathcal{A})}$:

$\mathsf{cnt} = \mathsf{gen} := 0$, $L_1^{\mathrm{eq}} = L_2^{\mathrm{eq}} = L_T^{\mathrm{eq}} = L_1^{\sim} = L_2^{\sim} = L_T^{\sim} := \emptyset$, $\mathcal{Q}_{\mathsf{chal}} = \mathcal{Q}_{\mathsf{sk}} := \emptyset$, $\mathsf{append}(L_1^{\sim}, \vec{B})$, $\mathsf{append}(L_T^{\sim}, A)$, $\beta \leftarrow_{\mathrm{R}} \{0,1\}$.
$\beta' \leftarrow \mathcal{A}^{\mathcal{O}_{\mathsf{add}}, \mathcal{O}_{\mathsf{pair}}, \mathcal{O}_{\mathsf{eq}}, \mathcal{O}_{\mathsf{chal}}, \mathcal{O}_{\mathsf{sk}}}(1^\lambda, p)$. If $\beta' = \beta$, and for all $x \in \mathcal{Q}_{\mathsf{chal}}$, $y \in \mathcal{Q}_{\mathsf{sk}}$, $\mathsf{P}(x,y) = 0$, output 1. Otherwise, output 0.

$\underline{\mathcal{O}_{\mathsf{add}}(s \in \{1,2,T\}, i, j \in \mathbb{N})}$:
If gen = 0, $\mathsf{append}(L_s^{\sim}, L_s^{\sim}[i] +_{\mathsf{rf}} L_s^{\sim}[j])$.
If gen = 1, $\mathsf{append}(L_s^{\mathrm{eq}}, L_s^{\mathrm{eq}}[i] +_{\mathsf{rf}} L_s^{\mathrm{eq}}[j])$.

$\underline{\mathcal{O}_{\mathsf{pair}}(i, j \in \mathbb{N})}$:
If gen = 0, $\mathsf{append}(L_s^{\sim}, L_s^{\sim}[i] \cdot_{\mathsf{rf}} L_s^{\sim}[j])$.
If gen = 1, $\mathsf{append}(L_s^{\mathrm{eq}}, L_s^{\mathrm{eq}}[i] \cdot_{\mathsf{rf}} L_s^{\mathrm{eq}}[j])$.

$\underline{\mathcal{O}_{\mathsf{chal}}(x \in \mathcal{X})}$:
$\vec{c}(\vec{S}, \vec{B}) \leftarrow \mathsf{sE}(x)$, $\vec{S} := (S_0, \dots, S_w)$, $f_0^\star := AS_0$, $f_1^\star := U$, where U is a fresh formal variable.
If gen = 0, $\mathsf{append}\big(L_1^{\sim}, \vec{c}(\vec{B}, \vec{S})\big)$, $\mathsf{append}(L_T^{\sim}, f_\beta^\star)$.
If gen = 1, $\vec{s} \leftarrow_{\mathrm{R}} \mathbb{Z}_p^{w_1}$, $\mathsf{append}\big(L_1^{\mathrm{eq}}, \vec{c}(\vec{b}, \vec{s})\big)$, $v_0^\star := \alpha s_0$, $v_1^\star := u \leftarrow_{\mathrm{R}} \mathbb{Z}_p$, $\mathsf{append}(L_T^{\mathrm{eq}}, v_\beta^\star)$.
$\mathcal{Q}_{\mathsf{chal}} := \mathcal{Q}_{\mathsf{chal}} \cup \{x\}$.

$\underline{\mathcal{O}_{\mathsf{sk}}(y \in \mathcal{Y})}$:
$\vec{R}_{\mathsf{cnt}} := (R_{\mathsf{cnt},1}, \dots, R_{\mathsf{cnt},m_1})$, $\vec{k}_{\mathsf{cnt}} \leftarrow \mathsf{rE}(y)(\vec{R} \rightarrow \vec{R}_{\mathsf{cnt}})$.
If gen = 0, $\mathsf{append}(L_2^{\sim}, \vec{k}_{\mathsf{cnt}})$.
If gen = 1, $\vec{r}_{\mathsf{cnt}} \leftarrow_{\mathrm{R}} \mathbb{Z}_p^{m_1}$, $\mathsf{append}\big(L_2^{\mathrm{eq}}, \vec{k}(\vec{r}_{\mathsf{cnt}}, \vec{b}, \alpha)\big)$.
$\mathsf{cnt} := \mathsf{cnt} + 1$, $\mathcal{Q}_{\mathsf{sk}} := \mathcal{Q}_{\mathsf{sk}} \cup \{y\}$.

$\underline{\mathcal{O}_{\mathsf{eq}}(s \in \{1,2,T\}, i', j' \in \mathbb{N})}$:
On the ν'th query:

- if $\nu < i+1$: Output 1 if $L_s^{\sim}[i] \sim_{\mathsf{rf}} L_s^{\sim}[j]$, 0 otherwise.
- if $\nu = i+1$: $\mathsf{gen} := 1$, $\vec{b} \leftarrow_{\mathrm{R}} \mathbb{Z}_p$, $\mathsf{append}(L_1^{\mathrm{eq}}, \vec{b})$, for $x \in \mathcal{Q}_{\mathsf{chal}}$, $\vec{c}(\vec{S}, \vec{B}) \leftarrow \mathsf{sE}(x)$, $\vec{s} \leftarrow_{\mathrm{R}} \mathbb{Z}_p^{w_1}$, $\mathsf{append}\big(L_1^{\mathrm{eq}}, \vec{c}(\vec{s}, \vec{b})\big)$, $\alpha \leftarrow_{\mathrm{R}} \mathbb{Z}_p$, for all $j \in [\mathsf{cnt}]$, $\vec{r}_{\mathsf{cnt}} \leftarrow_{\mathrm{R}} \mathbb{Z}_p^{m_1}$, $\mathsf{append}\big(L_2^{\mathrm{eq}}, \vec{k}_{\mathsf{cnt}}(\vec{r}_{\mathsf{cnt}}, \vec{b}, \alpha)\big)$, output 1 if $L_s^{\mathrm{eq}}[i'] = L_s^{\mathrm{eq}}[j']$, 0 otherwise.
- if $\nu > i+1$: Output 1 if $L_s^{\mathrm{eq}}[i] = L_s^{\mathrm{eq}}[j]$, 0 otherwise.

Figure 8: Game$_i$ for $i \in [0, Q_{\mathrm{eq}}]$, for the proof of Theorem 3.3. We require that $\mathcal{A}$ queries $\mathcal{O}_{\mathsf{chal}}$ at most once, and that for $x \in \mathcal{Q}_{\mathsf{chal}}$ and all $y \in \mathcal{Q}_{\mathsf{sk}}$, $\mathsf{P}(x,y) = 0$. Wlog. we assume no query contains indices $i, j \in \mathbb{N}$ that exceed the size of the involved lists.

$\alpha_1, \alpha_1', \dots, \alpha_{|\widehat{L}_T|}, \alpha'_{|\widehat{L}_T|} \in \mathbb{Z}_p$, where for all $i \in [|\widehat{L}_T|]$, $\widehat{L}_T[i] := f_i/g_i$. Let $i^\star \in \mathbb{N}^*$ such that $f_{i^\star}/g_{i^\star} = f_\beta^\star$.

- If $\alpha_{i^\star} = \alpha'_{i^\star}$, then $L_T[i] \sim_{\mathsf{rf}} L_T[j] \Leftrightarrow \sum_{i \neq i^\star}^{\mathsf{rf}} \alpha_i \cdot f_i/g_i \sim_{\mathsf{rf}} \sum_{i \neq i^\star}^{\mathsf{rf}} \alpha_i' \cdot f_i/g_i$, which is independent of β.
- If $\alpha_{i^\star} \neq \alpha'_{i^\star}$, then $L_T[i] \sim_{\mathsf{rf}} L_T[j] \Rightarrow f_\beta^\star \sim_{\mathsf{rf}} \sum_{i \neq i^\star}^{\mathsf{rf}} \frac{\alpha_i' - \alpha_i}{\alpha_{i^\star} - \alpha'_{i^\star}} \cdot f_i/g_i$, thus, there exist $x \in \mathcal{X}$, $\{\mathbf{E}_y^*\}_{y \in \mathcal{Y}_x}$ and $\gamma \in \mathbb{Z}_p$ such that $\sum_{y \in \mathcal{Y}_x} (\vec{B}, \vec{c}(\vec{S}, \vec{B}))^\top \mathbf{E}_y^* \vec{k}_y(\vec{R}_y, \vec{B}, A) + \gamma A \sim_{\mathsf{rf}} f_\beta^\star$.

When $\beta = 0$, $f_0^\star = AS_0$, which, together with Lemma 3.2, contradicts the symbolic security of ABE. When $\beta = 1$, $f_1^\star = U$, which cannot be a linear combination of rational fractions on a disjoint set of formal variables. To sum up, $L_T[i]$ not $\sim_{\mathsf{rf}} L_T[j]$, regardless of β.

□

Summing everything up, we obtain: $\mathsf{Adv}_{\mathsf{ABE},\mathcal{A}}^{\mathsf{GGM}}(\lambda) \leq \frac{6dQ_{\mathrm{eq}}\left(2+(n+|\mathsf{ct}|)Q_{\mathsf{sk}}|\mathsf{sk}|\right)}{p}$ We conclude the proof of Theorem 3.3 using the fact that $Q_{\mathrm{eq}} \leq \frac{\left(|L_1^{\mathrm{eq}}|+|L_2^{\mathrm{eq}}|+|L_T^{\mathrm{eq}}|\right)^2}{2} \leq \frac{\left(2+n+Q_{\mathrm{add}}+|\mathsf{ct}|+Q_{\mathsf{sk}}|\mathsf{sk}|+Q_{\mathrm{pair}}\right)^2}{2}$. □

A.4 Proof of Theorem 4.1

Proof. We prove the symbolic security of the ABE by contradiction. Suppose there is $x \in \mathcal{X}$, and matrices $\{\mathbf{E}_y^*\}_{y \in \mathcal{Y}_x}$ such that

$$\sum_{y \in \mathcal{Y}_x} \big(\vec{S}, \vec{c}(\vec{S}, \vec{S}', \vec{B})\big)^\top \mathbf{E}_y^* \big(\vec{R}_y, \vec{k}_y(\vec{R}_y, \vec{R}_y', \vec{B}, A)\big) = AS_0, \qquad (2)$$

where $\big(\vec{S}, \vec{c}(\vec{S}, \vec{S}', \vec{B})\big) = \mathsf{sE}(x)$, $\mathcal{Y}_x \subseteq \mathcal{Y}$ is the set of all $y \in \mathcal{Y}$ such that $\mathsf{P}(x,y) = 0$, and for all $y \in \mathcal{Y}_x$, $\vec{R}_y := (R_{y,1}, \dots, R_{y,m_1})$, $\vec{R}_y' :=$

$(R'_{y,1},\dots,R'_{y,m_1})$, $\big(\vec{R}_y, \vec{k}_y(\vec{R}_y, \vec{R}'_y, \vec{B}, A)\big) = \mathsf{rE}(y)(\vec{R} \to \vec{R}_y, \vec{R}' \to \vec{R}'_y)$.

For all $y \in \mathcal{Y}_x$, we evaluate the polynomials in Equation (2) on $\vec{R}_{y'} = \vec{0}$ and $\vec{R}'_{y'} = \vec{0}$, for all $y' \in \mathcal{Y}_x \setminus \{y\}$, and $A = 0$, to obtain:

$$\big(\vec{S}, \vec{c}(\vec{S}, \vec{S}', \vec{B})\big)^\top \mathbf{E}^*_y\big(\vec{R}_y, \vec{k}_y(\vec{R}_y, \vec{R}'_y, \vec{B}, 0)\big) = 0 \qquad (3)$$

Now, we show that there exists $y^\star \in \mathcal{Y}_x$ and a constant $\rho \in \mathbb{Z}_p^*$ such that $\big(\vec{S}, \vec{c}(\vec{S}, \vec{S}', \vec{B})\big)^\top \rho\mathbf{E}^*_{y^\star}\big(\vec{0}, \vec{k}_{y^\star}(\vec{0}, \vec{0}, \vec{0}, A)\big) = AS_0$, which, together with Equation (3), implies: $\big(\vec{S}, \vec{c}(\vec{S}, \vec{S}', \vec{B})\big)^\top \rho\mathbf{E}^*_{y^\star}\big(\vec{R}_{y^\star}, \vec{k}_{y^\star}(\vec{R}_{y^\star}, \vec{R}'_{y^\star}, \vec{B}, A)\big) = AS_0$, thereby contradicting the symbolic security of $(\mathsf{sE}, \mathsf{rE}, \mathsf{Pair})$. We do so in two steps, where in Step 1. (Lemma A.4) we show that for all $y \in \mathcal{Y}_x$, we can assume some structural properties of the matrix $\mathbf{E}^*_y$. In step 2. we use this structural properties with Equations (2) and (3) to derive the desired $y^\star \in \mathcal{Y}_x$.

Lemma A.4 (Step 1.). *For all $x \in \mathcal{X}$, $y \in \mathcal{Y}_x$, and $\mathbf{E}^*_y := \begin{pmatrix} \mathbf{E}^{(1)}_y & \mathbf{E}^{(2)}_y \\ \mathbf{E}^{(3)}_y & \mathbf{E}^{(4)}_y \end{pmatrix}$ with $\mathbf{E}^{(1)}_y \in \mathbb{Z}_p^{(1+w)\times m_1}$, $\mathbf{E}^{(2)}_y \in \mathbb{Z}_p^{(1+w)\times m_3}$, $\mathbf{E}^{(3)}_y \in \mathbb{Z}_p^{w_3\times m_1}$, $\mathbf{E}^{(4)}_y \in \mathbb{Z}_p^{w_3\times m_3}$ that satisfies Equation* (3), *we have: $\big(\vec{S}, \vec{c}(\vec{S}, \vec{S}', \vec{B})\big)^\top \begin{pmatrix} \mathbf{0} & \mathbf{E}^{(2)}_y \\ \mathbf{E}^{(3)}_y & \mathbf{0} \end{pmatrix} \big(\vec{R}_y, \vec{k}_y(\vec{R}_y, \vec{R}'_y, \vec{B}, 0)\big) = 0$.*

Proof of Lemma A.4. We first show that $\vec{c}(\vec{S}, \vec{S}', \vec{B})^\top \mathbf{E}^{(4)}_y \vec{k}_y(\vec{R}_y, \vec{R}'_y, \vec{B}, 0) = 0$. Suppose this is not the case. Then, by definition of a pair encoding (see Section 4), the polynomial $\vec{c}(\vec{S}, \vec{S}', \vec{B})^\top \mathbf{E}^{(4)}_y \vec{k}_y(\vec{R}_y, \vec{R}'_y, \vec{B}, 0)$ is a linear combinations of monomials of the form: $S'_{i'}R'_{y,j'}$, $S'_{i'}B_\ell R_{y,j}$, $S_i B_\ell R'_{y,j'}$, or $S_i B_\ell B_{\ell'} R_j$, where $i \in [w_1], i' \in [w_2], j \in [m_1], j' \in [m_2], \ell, \ell' \in [n]$. This is in contradiction with the fact that $\vec{c}(\vec{S}, \vec{S}', \vec{B})^\top \mathbf{E}^{(4)}_y \vec{k}_y(\vec{R}_y, \vec{R}'_y, \vec{B}, 0) = -\vec{S}^\top \mathbf{E}^{(1)}_y \vec{R}_y - \vec{S}^\top \mathbf{E}^{(2)}_y \vec{k}_y(\vec{R}_y, \vec{R}'_y, \vec{B}, A) - \vec{C}(\vec{S}, \vec{S}', \vec{B})^\top \mathbf{E}^{(3)}_y \vec{R}_y$ (Equation (3)).

Then, by evaluating Equation (3) on $\vec{S}' = \vec{0}, \vec{R}' = \vec{0}, \vec{B} = \vec{0}$, we obtain: $\vec{S}^\top \mathbf{E}^{(1)}_y \vec{R} = 0$. □

Step 2. Combining Equation (2) and (3), we obtain:

$$\sum_{y \in \mathcal{Y}_x} \big(\vec{S}, \vec{c}(\vec{S}, \vec{S}', \vec{B})\big)^\top \mathbf{E}^*_y\big(\vec{0}, \vec{k}_y(\vec{0}, \vec{0}, \vec{0}, A)\big) = AS_0.$$

Evaluating the above equation on $B_i = 0$ and $S'_j = 0$ for all $i \in [n]$ and $j \in [w]$, we obtain:

$$\sum_{y \in \mathcal{Y}_x} \vec{S}^\top \mathbf{E}^{(2)}_y \vec{k}_{y^\star}(\vec{0}, \vec{0}, \vec{0}, A) = AS_0.$$

Then, we use the fact that $\vec{k}_{y^\star}$ is a vector of polynomials that are linear in A, and that $\vec{S} := S_0$ (since we assumed $w_1 = 0$) thus, we have:

$$\sum_{y \in \mathcal{Y}_x} \mathbf{E}^{(2)}_y \vec{k}_{y^\star}(\vec{0}, \vec{0}, \vec{0}, 1) = 1.$$

In particular, that means there exists $y^\star \in \mathcal{Y}_x$ such that $\mathbf{E}^{(2)}_{y^\star} \vec{k}_{y^\star}(\vec{0}, \vec{0}, \vec{0}, 1) = \mu \neq 0$. Consequently, the matrix $\widetilde{\mathbf{E}} := 1/\mu \begin{pmatrix} \mathbf{0} & \mathbf{E}^{(2)}_y \\ \mathbf{E}^{(3)}_y & \mathbf{0} \end{pmatrix}$ is such that:

$$\big(\vec{S}, \vec{c}(\vec{S}, \vec{S}', \vec{B})\big)^\top \widetilde{\mathbf{E}}\big(\vec{0}, \vec{k}_{y^\star}(\vec{0}, \vec{0}, \vec{0}, A)\big) = AS_0.$$

Combining this fact with Lemma A.4 leads to a contradiction of the symbolic security of $(\mathsf{sE}, \mathsf{rE}, \mathsf{Pair})$. □

B SYMBOLIC SECURITY OF CONCRETE ABE

B.1 Symbolic security of IBE 1 [64]

By contradiction, suppose there exist $x \in \mathbb{Z}_p$, and $\{e_y \in \mathbb{Z}_p\}_{y \in \mathcal{Y}_x}$ such that $\sum^{\mathsf{rf}}_{y \in \mathcal{Y}_x} S(B+x)e_y A/(B+y) \sim_{\mathsf{rf}} AS$. Since for all $y \in \mathcal{Y}_x$, $y \neq x$, we can evaluate the above rational fraction on $B = -x$, to obtain: $0 \sim_{\mathsf{rf}} AS$, which is a contradiction. More formally, this corresponds to the application of rules **com-den**, **div-split**, **eval-var** on $B = -x$, and **zero-prod**, as explained in the example of Section 6.

B.2 Symbolic security of IBE 2 [27]

The underlying pair encoding of IBE 2 falls under the definition of [6]. Thus, by Theorem 4.1 (symbolically secure pair encoding ⇒ symbolically secure RFI-ABE), we only have to show that the pair encoding is symbolically secure, as defined [6] (recalled in Section 4). This is proven by contradiction, and using the Lemma A.4 (additional structure on the bilinear map): suppose there exist $x, y \in \mathbb{Z}_p$ such that $x \neq y$, and $e_1, e_2 \in \mathbb{Z}_p$ such that: $e_1 S\big(A + R(B_1 + yB_2)\big) + e_2 S(B_1 + xB_2)R = AS$. Evaluating the polynomials on $B_2 = u$ and $B_1 = -xu$, for an arbitrary $u \in \mathbb{Z}_p^*$, we obtain: $e_1 S\big(A + u(y-x)R\big) = AS$. Then, using the rule **extr-coeff** on R, we obtain $(y - x) = 0$, which contradicts $x \neq y$.

B.3 Symbolic security of IPE 1 [46]

The underlying pair encoding of IPE 1 falls under the definition of [6]. Thus, by Theorem 4.1 (symbolically secure pair encoding ⇒ symbolically secure RFI-ABE), we only have to show that the pair encoding is symbolically secure, as defined [6] (recalled in Section 4). This is proven by contradiction, and using the Lemma A.4 (additional structure on the bilinear map): suppose there exist $\vec{x}, \vec{y} \in \mathbb{Z}_p$ such that $\vec{x}^\top \vec{y} \neq z$, $e_1 \in \mathbb{Z}_p$, and $\vec{e}_2 \in \mathbb{Z}_p^d$ such that: $e_1 S\big(A + R(Uz + \vec{V}^\top \vec{y})\big) + S(U\vec{x} + \vec{V})^\top \vec{e}_2 R = AS$. Evaluating the polynomials on $U = u$ and $\vec{V} = -\vec{x}u$, for an arbitrary $u \in \mathbb{Z}_p^*$, we obtain: $e_1 S\big(A + u(z + \vec{x}^\top \vec{y})R\big) = AS$. Then, using the rule **extr-coeff** on R, we obtain $(z + \vec{x}^\top \vec{y}) = 0$, which contradicts $(z + \vec{x}^\top \vec{y}) \neq 0$.

B.4 Symbolic security of IPE 2

By contradiction, suppose there exist $\vec{x} \in \mathbb{Z}_p^d$, and $\{\vec{e}_{\vec{y}} \in \mathbb{Z}_p^d\}_{\vec{y} \in \mathcal{Y}_x}$ such that $\sum^{\mathsf{rf}}_{\vec{y} \in \mathcal{Y}_{\vec{x}}} S(\vec{x} + \vec{B})^\top \vec{e}_{\vec{y}} A/(z + \vec{B}^\top \vec{y}) \sim_{\mathsf{rf}} AS$. Since for all $\vec{y} \in \mathcal{Y}_x$, $\vec{x}^\top \vec{y} \neq z$, we can evaluate the above rational fraction on $\vec{B} = -\vec{x}$, to obtain: $0 \sim_{\mathsf{rf}} AS$, which is a contradiction. As for the proof of symbolic security of IBE 1 above, this can be handle by our automatic tool, using the rules **com-den**, **div-split**, **eval-var** on $\vec{B} = -\vec{x}$, and **zero-prod**.

From the Appendix B.5 on, we use a generalized **extr-coeff** rule, namely, for every polynomials P, Q, R, such that $Q \neq 0$, and $R \notin I \setminus \{0\}$ where I is the ideal generated by Q, and 0 denotes the zero polynomial, we have: $PQ + R = 0$ implies $P = 0$ and $R = 0$.

B.5 Symbolic security of KP-ABE [41]

By contradiction, suppose there exist $\vec{x} \in \{0,1\}^d$, and $\{\mathbf{E}_{(\mathbf{M},\rho)} \in \mathbb{Z}_p^{d \times \ell}\}_{(\mathbf{M},\rho) \in \mathcal{Y}_{\vec{x}}}$ such that $\sum := \sum^{\mathsf{rf}}_{(\mathbf{M},\rho) \in \mathcal{Y}_{\vec{x}}} \mathsf{sE}(\vec{x})^\top \mathbf{E}_{(\mathbf{M},\rho)} \mathsf{rE}(\mathbf{M},\rho)(\vec{R} \to \vec{R}_{(\mathbf{M},\rho)}) \sim_{\mathsf{rf}} AS$.

We write $\sum = \sum_1 +_{\mathsf{rf}} \sum_2$, where for all $t \in [2]$, $\sum_t \in \langle S_t \rangle$, with:

- $S_1 := \{x_{\rho(j)} S \mathbf{M}_j^\top (A, \vec{R}_{(\mathbf{M},\rho)}) : (\mathbf{M},\rho) \in \mathcal{Y}_{\vec{x}}, j \in [\ell]\}$
- $S_2 := \{x_i S \mathbf{M}_j^\top (A, \vec{R}_{(\mathbf{M},\rho)}) B_i / B_{\rho(j)} : (\mathbf{M},\rho) \in \mathcal{Y}_{\vec{x}}, j \in [\ell], i \in [d], \rho(j) \neq i\}$

We use the rules **com-den**, **div-split** and **extr-coeff** on the monomial $\prod_{t \in \mathcal{V}} B_t$ where $\mathcal{V} := \{\rho(j) : (\mathbf{M},\rho) \in \mathcal{Y}_{\vec{x}}, j \in [\ell], i \in [d], \rho(j) \neq i\}$, in the equation $\sum_1 +_{\mathsf{rf}} \sum_2 \sim_{\mathsf{rf}} AS$, to obtain $\sum_1 \sim_{\mathsf{rf}} AS$.

Then, we write $\sum_1 := \sum_{(\mathbf{M},\rho) \in \mathcal{Y}_{\vec{x}}, j \in [\ell]} \gamma_{(\mathbf{M},\rho),j} x_{\rho(j)} S \mathbf{M}_j^\top (A, \vec{R}_{(\mathbf{M},\rho)})$, and for all $(\mathbf{M},\rho) \in \mathcal{Y}_{\vec{x}}$, we evaluate the equation $\sum_1 \sim_{\mathsf{rf}} AS$ on $A = 0$, $S = 1$, and $\vec{R}_{(\mathbf{M}',\rho')} = \vec{0}$ for all $(\mathbf{M}',\rho') \in \mathcal{Y}_{\vec{x}} \setminus \{(\mathbf{M},\rho)\}$, to obtain:

$$\forall (\mathbf{M},\rho) \in \mathcal{Y}_{\vec{x}} : \sum_{j \in [\ell]} \gamma_{(\mathbf{M},\rho),j} x_{\rho(j)} \mathbf{M}_j^\top (0, \vec{R}_{(\mathbf{M},\rho)}) \sim_{\mathsf{rf}} 0 \qquad (4)$$

Then, we evaluate the equation $\sum_1 \sim_{\mathsf{rf}} AS$ on $A = 1$, $S = 1$, and $\vec{R}_{(\mathbf{M},\rho)} = \vec{0}$ for all $(\mathbf{M},\rho) \in \mathcal{Y}_{\vec{x}}$, to obtain: $\sum^{\mathsf{rf}}_{(\mathbf{M},\rho) \in \mathcal{Y}_{\vec{x}}, j \in [\ell]} \gamma_{(\mathbf{M},\rho),j} x_{\rho(j)} \mathbf{M}_j^\top (1, \vec{0}) \sim_{\mathsf{rf}} 1$. Using the rule **non-zero-sum**, there exists $(\mathbf{M}^\star, \rho^\star) \in \mathcal{Y}_{\vec{x}}$ such that

$$\sum_{j \in [\ell]} \gamma_{(\mathbf{M}^\star,\rho^\star),j} x_{\rho^\star(j)} \mathbf{M}_j^{\star\top} (1, \vec{0}) = \mu \neq 0 \qquad (5)$$

Combining Equation (4) and (5), we have: $\frac{1}{\mu} \sum_{j \in [\ell]} \gamma_{(\mathbf{M},\rho),j} x_{\rho^\star(j)} \mathbf{M}_j^{\star\top} (1, \vec{R}_{(\mathbf{M}^\star,\rho^\star)}) \sim_{\mathsf{rf}} 1$. Then, using the rule **extr-coeff** on each variable of $\vec{R}_{(\mathbf{M}^\star,\rho^\star)}$, we obtain $\frac{1}{\mu} \sum_{j \in [\ell]} \gamma_{(\mathbf{M},\rho),j} x_{\rho^\star(j)} \mathbf{M}_j^{\star\top} = \vec{1}$, which contradicts $\mathsf{P}(\vec{x}, (\mathbf{M}^\star, \rho^\star))$.

B.6 Symbolic security of compact KP-ABE

By contradiction, suppose there exist $\vec{x} \in \{0,1\}^d$, and $\{\mathbf{E}_{(\mathbf{M},\rho)} \in \mathbb{Z}_p^{2 \times d\ell}\}_{(\mathbf{M},\rho) \in \mathcal{Y}_{\vec{x}}}$ such that $\sum := \sum^{\mathsf{rf}}_{(\mathbf{M},\rho) \in \mathcal{Y}_{\vec{x}}} \mathsf{sE}(\vec{x})^\top \mathbf{E}_{(\mathbf{M},\rho)} \mathsf{rE}(\mathbf{M},\rho)(\vec{R} \to \vec{R}_{(\mathbf{M},\rho)}) \sim_{\mathsf{rf}} AS$.

We write $\sum = \sum_1 +_{\mathsf{rf}} \sum_2 +_{\mathsf{rf}} \sum_3$, where for all $t \in [3]$, $\sum_t \in \langle S_t \rangle$, with:

- $S_1 := \{x_{\rho(j)} S \mathbf{M}_j^\top (A, \vec{R}_{(\mathbf{M},\rho)}) : (\mathbf{M},\rho) \in \mathcal{Y}_{\vec{x}}, j \in [\ell]\}$
- $S_2 := \{S \mathbf{M}_j^\top (A, \vec{R}_{(\mathbf{M},\rho)}) / B_{\rho(j)}, S \mathbf{M}_j^\top (A, \vec{R}_{(\mathbf{M},\rho)}) B_i / B_{\rho(j)}, x_i S \mathbf{M}_j^\top (A, \vec{R}_{(\mathbf{M},\rho)}) B_i B_{i'} / B_{\rho(j)} : i, i' \in [d], j \in [\ell] s.t. \rho(j) \neq i, \rho(j) \neq i', (\mathbf{M},\rho) \in \mathcal{Y}_{\vec{x}}\}$
- $S_3 := \{x_{\rho(j)} S B_i \mathbf{M}_j^\top (A, \vec{R}_{(\mathbf{M},\rho)}) : (\mathbf{M},\rho) \in \mathcal{Y}_{\vec{x}}, i \in [d], j \in [\ell]\}$

We use the rules **com-den**, **div-split** and **extr-coeff** on the monomial $\prod_{t \in \mathcal{V}} B_t$ where $\mathcal{V} := \{\rho(j) : (\mathbf{M},\rho) \in \mathcal{Y}_{\vec{x}}, j \in [\ell]\}$, to obtain $\sum_1 +_{\mathsf{rf}} \sum_3 \sim_{\mathsf{rf}} AS$.

Then, we obtain $\sum_3 \sim_{\mathsf{rf}} 0$ using the rule **extr-coeff** on the monomial B_i for all $i \in [d]$, in the equation $\sum_1 +_{\mathsf{rf}} \sum_3 \sim_{\mathsf{rf}} AS$. Thus, we get: $\sum_1 \sim_{\mathsf{rf}} AS$.

The rest of the proof goes exactly as for the proof of te KP-ABE[41]. See Section B.5 for further details.

B.7 Symbolic security of Unbounded KP-ABE

By contradiction, suppose there exist $\Gamma \subset \mathbb{Z}_p$, and $\{\mathbf{E}_{(\mathbf{M},\rho)} \in \mathbb{Z}_p^{2|\Gamma| \times 2\ell}\}_{(\mathbf{M},\rho) \in \mathcal{Y}_\Gamma}$ such that $\sum := \sum^{\mathsf{rf}}_{(\mathbf{M},\rho) \in \mathcal{Y}_\Gamma} \mathsf{sE}(\Gamma)^\top \mathbf{E}_{(\mathbf{M},\rho)} \mathsf{rE}(\mathbf{M},\rho)(\vec{R} \to \vec{R}_{(\mathbf{M},\rho)}) \sim_{\mathsf{rf}} AS$.

We write $\sum := \sum_1 +_{\mathsf{rf}} \sum_2 +_{\mathsf{rf}} \sum_3$, where for all $t \in [3]$, $\sum_t \in \langle S_t \rangle$, with:

- $S_1 := \{(S - S_i) \mathbf{M}(A, \vec{R}_{(\mathbf{M},\rho)}), S_{\rho(j)} \mathbf{M}_j^\top (A, \vec{R}_{(\mathbf{M},\rho)}) : (\mathbf{M},\rho) \in \mathcal{Y}_\Gamma, j \in [\ell]\}$
- $S_2 := \{S_i (B_1 + i B_2) \mathbf{M}(A, \vec{R}_{(\mathbf{M},\rho)}) : (\mathbf{M},\rho) \in \mathcal{Y}_\Gamma, i \in \Gamma\}$
- $S_3 := \{S_i (B_1 + i B_2) \mathbf{M}_j^\top (A, \vec{R}_{(\mathbf{M},\rho)}) / (B_1 + \rho(j) B_2) : (\mathbf{M},\rho) \in \mathcal{Y}_\Gamma, i \in \Gamma, j \in [\ell], \rho(j) \neq i\} \cup \{(S - S_i) \mathbf{M}_j^\top (A, \vec{R}_{(\mathbf{M},\rho)}) / (B_1 + \rho(j) B_2) : (\mathbf{M},\rho) \in \mathcal{Y}_\Gamma, i \in \Gamma, j \in [\ell]\}$

We show that:

- $\sum_2 \sim_{\mathsf{rf}} 0$: evaluating the equation $\sum \sim_{\mathsf{rf}} AS$ on $B_2 = 0$, then multiplying it by B_1, and using the rule **extr-coeff** on $S_i B_1^2$ for all $i \in \Gamma$.
- $\sum_1 \sim_{\mathsf{rf}} AS$: using the rule **com-den** on the equation $\sum_1 +_{\mathsf{rf}} \sum_3 \sim_{\mathsf{rf}} AS$, then **div-split**, and applying the rules **extr-coeff** on the polynomial $B_1 + \rho(j) B_2$ sequentially for each value $\rho(j)$ such that $(\mathbf{M},\rho) \in \mathcal{Y}_\Gamma$, and $j \in [\ell]$.

Then, we write $\sum_1 := \sum_{1.1} + \sum_{1.2}$, where

$$\sum_{1.1} := \sum_{(\mathbf{M},\rho) \in \mathcal{Y}_\Gamma, j : \rho(j) \in \Gamma} \sigma_{(\mathbf{M},\rho),j} S \mathbf{M}_j^\top (A, \vec{R}_{(\mathbf{M},\rho)})$$

and

$$\sum_{1.2} := \sum_{(\mathbf{M},\rho) \in \mathcal{Y}_\Gamma, i \in \Gamma, j \in [\ell]} \sigma_{(\mathbf{M},\rho),j,i} (S - S_i) \mathbf{M}_j^\top (A, \vec{R}_{(\mathbf{M},\rho)}).$$

We have $\sum_{1.2} \sim_{\mathsf{rf}} 0$ using **extr-coeff** on S_i for all $i \in \Gamma$.

Finally, we reach a contradiction from $\sum_{1.1} \sim_{\mathsf{rf}} AS$ exactly as in the proof of symbolic security of the KP-ABE [41]. We defer to Section B.5 for further details.

B.8 Symbolic security of CP-ABE

By contradiction, suppose there exist $(\mathbf{M},\rho) \in \mathbb{Z}_p^{\ell \times \ell'} \times ([\ell] \to [d])$, and $\{\mathbf{E}_{\vec{x}} \in \mathbb{Z}_p^{(\ell+1) \times (d+1)}\}_{\vec{x} \in \mathcal{Y}_{(\mathbf{M},\rho)}}$ such that $\sum := \sum^{\mathsf{rf}}_{\vec{x} \in \mathcal{Y}_{(\mathbf{M},\rho)}} \mathsf{sE}(\mathbf{M},\rho)^\top \mathbf{E}_{\vec{x}} \mathsf{rE}(\vec{x})(R \to R_{\vec{x}}) \sim_{\mathsf{rf}} AS$.

We write $\sum := \sum_1 +_{\mathsf{rf}} \sum_2 +_{\mathsf{rf}} \sum_3$, where for all $t \in [3]$, $\sum_t \in \langle S_t \rangle$, with:

- $S_1 := \{S(A - R_{\vec{x}}), x_{\rho(i)} R_{\vec{x}} \mathbf{M}_i^\top (S, \vec{U}) : \vec{x} \in \mathcal{Y}_{(\mathbf{M},\rho)}, i \in [\ell]\}$
- $S_2 := \{x_j S R_{\vec{x}} / B_j, x_j R_{\vec{x}} B_{\rho(i)} \mathbf{M}_i^\top (S, \vec{U}) / B_j : \vec{x} \in \mathcal{Y}_{(\mathbf{M},\rho)}, j \in [d], i \in [\ell], \rho(i) \neq j\}$
- $S_3 := \{(A - R_{\vec{x}}) B_{\rho(i)} \mathbf{M}_i^\top (S, \vec{U}) : i \in [\ell]\}$

We use the rules **com-den**, **div-split** and **extr-coeff** on the monomial $\prod_{j \in [d]} B_j$, to obtain $\sum_1 +_{\mathsf{rf}} \sum_3 \sim_{\mathsf{rf}} AS$.

Then, we obtain $\sum_3 \sim_{\mathrm{rf}} 0$ using the rule **extr-coeff** on the monomial $B_{\rho(i)}$ for all $i \in [\ell]$, in the equation $\sum_1 +_{\mathrm{rf}} \sum_3 \sim_{\mathrm{rf}} AS$. Thus, we get: $\sum_1 \sim_{\mathrm{rf}} AS$.

Then, we write

$$\sum_1 := \sum_{\vec{x} \in \mathcal{Y}_{(\mathbf{M},\rho)}, i \in [\ell]} \gamma_{\vec{x},i} x_{\rho(i)} \mathbf{M}_i^\top (S, \vec{U}) R_{\vec{x}} + \gamma_{\vec{x}} S (A - R_{\vec{x}}),$$

and for all $\vec{x} \in \mathcal{Y}_{(\mathbf{M},\rho)}$, we evaluate the equation $\sum_1 \sim_{\mathrm{rf}} AS$ on $A = 0$, $S = 1$, and $R_{\vec{x}'} = \vec{0}$ for all $\vec{x}' \in \mathcal{Y}_{(\mathbf{M},\rho)} \setminus \{\vec{x}\}$, to obtain:

$$\sum_{i \in [\ell]} \left(\gamma_{\vec{x},i} x_{\rho(i)} \mathbf{M}_i^\top (S, \vec{U}) R_{\vec{x}} \right) - \gamma_{\vec{x}} R_{\vec{x}} S \sim_{\mathrm{rf}} 0 \qquad (6)$$

Suppose $\gamma_{\vec{x}} \neq 0$. Then, evaluating Equation (6) on $R_{\vec{x}} = 1$, we have: $\sum_{i \in [\ell]} \left(\frac{\gamma_{\vec{x},i}}{\gamma_{\vec{x}}} x_{\rho(i)} \mathbf{M}_i^\top (S, \vec{U}) \right) \sim_{\mathrm{rf}} S$. Then, using the rule **extr-coeff** on S and all the variables in $\vec{U}$, we obtain: $\sum_{i \in [\ell]} \frac{\gamma_{\vec{x},i}}{\gamma_{\vec{x}}} x_{\rho(i)} \mathbf{M}_i^\top = \vec{1}$, which contradicts $\mathsf{P}(\vec{x}, (\mathbf{M}, \rho))$. Therefore, for all $\vec{x} \in \mathcal{Y}_{(\mathbf{M},\rho)}$, we have $\gamma_{\vec{x}} = 0$. In particular, $\sum_1$ does not contain the formal variable A, which contradicts $\sum_1 \sim_{\mathrm{rf}} AS$ (the contradiction is obtained using the rule **extr-coeff** on A).

B.9 Symbolic security of Unbounded CP-ABE

By contradiction, suppose there exist $(\mathbf{M}, \rho) \in \mathbb{Z}_p^{\ell \times \ell'} \times ([\ell] \to \mathbb{Z}_p)$, and $\{\mathbf{E}_\Gamma \in \mathbb{Z}_p^{3\ell \times (|\Gamma|+2)}\}_{\Gamma \in \mathcal{Y}_{(\mathbf{M},\rho)}}$ such that $\sum := \sum^{\mathrm{rf}}_{\Gamma \in \mathcal{Y}_{(\mathbf{M},\rho)}} \mathsf{sE}(\mathbf{M}, \rho)^\top \mathbf{E}_\Gamma \mathsf{rE}(\vec{x})(R \to R_\Gamma) \sim_{\mathrm{rf}} AS$.

We write $\sum := \sum_1 +_{\mathrm{rf}} \sum_2 +_{\mathrm{rf}} \sum_3 +_{\mathrm{rf}} \sum_4$, where for all $t \in [4]$, $\sum_t \in \langle S_t \rangle$, with:

- $S_1 := \{S_i R_\Gamma V : \Gamma \in \mathcal{Y}_{(\mathbf{M},\rho)}, i \in [\ell], \rho(i) \in \Gamma\} \cup \big\{\big(- VS_i + W\mathbf{M}_i^\top (S, \vec{U})\big) R_\Gamma, \mathbf{M}_i^\top (S, \vec{U})(A - WR_\Gamma) : \Gamma \in \mathcal{Y}_{(\mathbf{M},\rho)}, i \in [\ell]\big\}$
- $S_2 := \{-VS_i + W\mathbf{M}_i^\top (S, \vec{U})(A - WR_\Gamma), \mathbf{M}_i^\top (S, \vec{U}) R_\Gamma : \Gamma \in \mathcal{Y}_{(\mathbf{M},\rho)}, i \in [\ell]\}$
- $S_3 := \{S_i (B_1 + \rho(i) B_2) R_\Gamma, S_i (B_1 + \rho(i) B_2)(A - WR_\Gamma) : \Gamma \in \mathcal{Y}_{(\mathbf{M},\rho)}, i \in [\ell]\}$
- $S_4 := \big\{\big(-VS_i + W\mathbf{M}_i^\top (S, \vec{U})\big) R_\Gamma V/(B_1 + jB_2), \mathbf{M}_i^\top (S, \vec{U}) R_\Gamma V/(B_1 + jB_2) : \Gamma \in \mathcal{Y}_{(\mathbf{M},\rho)}, i \in [\ell], j \in \Gamma\big\} \cup \{S_i (B_1 + \rho(i) B_2) R_\Gamma V/(B_1 + jB_2) : \Gamma \in \mathcal{Y}_{(\mathbf{M},\rho)}, i \in [\ell], j \in \Gamma, \rho(i) \neq j\}$

We show that:

- $\sum_3 \sim_{\mathrm{rf}} 0$: evaluating the equation $\sum \sim_{\mathrm{rf}} AS$ on $B_2 = 0$, then multiplying it by B_1, and using the rule **extr-coeff** on $S_i B_1^2$.
- $\sum_1 +_{\mathrm{rf}} \sum_2 \sim_{\mathrm{rf}} AS$: using the rule **com-den** on the equation $\sum_1 +_{\mathrm{rf}} \sum_2 +_{\mathrm{rf}} \sum_4 \sim_{\mathrm{rf}} AS$, then **div-split**, and applying the rules **extr-coeff** on the polynomial $B_1 + jB_2$ sequentially for each value $j \in \Gamma$.
- $\sum_2 \sim_{\mathrm{rf}} AS$: first, we use the rule **extr-coeff** on WA and W^2 in the equation $\sum_1 +_{\mathrm{rf}} \sum_2 \sim_{\mathrm{rf}} 0$. Then, we evaluate the equation $\sum_1 +_{\mathrm{rf}} \sum_2 \sim_{\mathrm{rf}} AS$ on $W = 0$, $V = 0$, $A = 0$, and use the rule **extr-coeff** on R_Γ for all $\Gamma \in \mathcal{Y}_{(\mathbf{M},\rho)}$. Finally, we evaluate the equation $\sum_1 +_{\mathrm{rf}} \sum_2 \sim_{\mathrm{rf}} AS$, on $R_\Gamma = 0$ for all $\Gamma \in \mathcal{Y}_{(\mathbf{M},\rho)}$ and $A = 0$, and we use the rule **extr-coeff** on VS_i for all $i \in [\ell]$.

Summing up, we get: $\sum_1 \sim_{\mathrm{rf}} 0$.

We write $\sum_1 := \sum_{1.1} +_{\mathrm{rf}} \sum_{1.2} +_{\mathrm{rf}} \sum_{1.3}$, where

$$\sum_{1.1} := \sum_{\Gamma \in \mathcal{Y}_{(\mathbf{M},\rho)}, i : \rho(i) \in \Gamma} \gamma_i^\Gamma A \mathbf{M}_i^\top (S, \vec{U}),$$

$$\sum_{1.2} := \sum_{\Gamma \in \mathcal{Y}_{(\mathbf{M},\rho)}, i \in [\ell]} \big(VS_i + W\mathbf{M}_i^\top (S, \vec{U})\big)\big(\sigma_i^\Gamma R_\Gamma + \delta_i^\Gamma (A - WR_\Gamma)\big),$$

$$\sum_{1.3} := \sum_{\Gamma \in \mathcal{Y}_{(\mathbf{M},\rho)}, i \in [\ell]} \mathbf{M}_i^\top (S, \vec{U})\big(\eta_i^\Gamma R_\Gamma + \mu_i^\gamma (A - WR_\Gamma)\big).$$

We have, for all $\Gamma \in \mathcal{Y}_{(\mathbf{M},\rho)}$, $i \in [\ell]$:

- $\sigma_i^\Gamma = 0$, using **extr-coeff** on $VS_i R_\Gamma$,
- $\delta_i^\Gamma = 0$, using **extr-coeff** on AVS_i.

This implies $\sum_{1.2} \sim_{\mathrm{rf}} 0$.

Next, we show that for all $\Gamma \in \mathcal{Y}_{(\mathbf{M},\rho)}$, $i \in [\ell]$:

- $\sum_{\Gamma, i} \eta_i^\Gamma \mathbf{M}_i^\top = \vec{0}^\top$, using **extr-coeff** on $R_\Gamma S$ and $R_\Gamma \vec{U}$,
- $\sum_{\Gamma, i} \mu_i^\Gamma \mathbf{M}_i^\top = \vec{0}^\top$, using **extr-coeff** on $WR_\Gamma S$ and $WR_\Gamma \vec{U}$.

This implies $\sum_{1.3} \sim_{\mathrm{rf}} 0$. Finally, we have: $\sum_{1.1} \sim_{\mathrm{rf}} AS$, which leads to a contradiction, as argued in Section B.8, for the proof of symbolic security of the CP-ABE.