CARIBE: Cascaded IBE for Maximum Flexibility and User-side Control

Abstract. Mass surveillance and a lack of end-user encryption, coupled with a growing demand for key escrow under legal oversight and certificate authority security concerns, raise the question of the appropriateness of continued general dependency on PKI. Under this context, we examine Identity-Based Encryption (IBE) as an alternative to public-key encryption. Cascade encryption, or sequential multiple encryption, is the concept of layering encryption such that the ciphertext from one encryption step is the plaintext of the next. We describe CARIBE, a cascaded IBE scheme, for which we also provide a cascaded CCA security experiment, IND-ID-C.CCA, and prove its security in the computational model. CARIBE combines the ease-of-use of IBE with key escrow, limited to the case when the entire set of participating PKGs collaborate. Furthermore, we describe a particular CARIBE scheme, CARIBE-S, where the receiver is a self-PKG – one of the several PKGs included in the cascade. CARIBE-S inherits IND-ID-C.CCA from CARIBE, and avoids key escrow entirely. In essence, CARIBE-S offers the maximum flexibility of the IBE paradigm and gives the users complete control without the key escrow problem.

1 Introduction

Mass surveillance has undoubtedly formed one of the most contentious turning points in modern Internet history. Fueled by the revelation of the **PRISM** surveillance program in 2013 [19], which collected Internet data from some of the biggest operators, including Microsoft™, Google™, and Yahoo™, and subsequent knowledge of programs such as **xkeyscore** [18] for collecting data en-mass as it is transferred, the essential need for encryption has never been more salient. Simultaneously, the case for *back-doored* encryption is also being argued, as governments fight for control of, potentially vital, information for stanching terrorist threats. Under this context we raise the question of optimal key management infrastructure, comparing identity-based encryption (IBE) as an alternative to the current public key infrastructure (PKI) to increase the ease of encryption use, while also presenting a new prospective on IBE – CARIBE – which provides limited key escrow and allows for end-user control of encryption.

Fundamentally, a PKI system relies upon the receiver's precaution; whether or not they have set up a public/private key pair with the public key listed securely online for access by others who wish to communicate with them. Since powerful organizations can subvert these *secure* key directories [27] and most end users demonstrate a general apathy for

establishing such keys to begin with [41], there is a clear need for a change to the conventional method. What the exigency of the situation demands is a system that provides secure ease-of-use encryption, does not rely upon a trusted third party, and yet allows for limited key escrow subject to the constraints of law. Notably, the need for limited key escrow is an axiomatically oblique path from the hither-to performed mass surveillance and pressure for backdoored products. As was recently stated in an open letter by U.S. congressmen Hurd and Lieu to the James Comey, Director of the FBI, "There is a difference between private companies assisting law enforcement and the government compelling companies to weaken their products..." [21].

Historically, IBE has been proposed and discussed as a means of encryption that is particularly user-friendly, as it is not necessary to have public or private keys established [37], yet it traditionally demands a trusted third party, namely a private-key generator (PKG). As with a CA in PKI, it is necessary to establish trusted parameters for the PKG, although it has been argued that this should not be as formidable a task as in PKI [17]. Developments in IBE have allowed for some preventative measures against a malicious PKG by distributing the key generation duties among multiple PKGs [25], but these designs demand that all involved PKGs must use the same IBE scheme which in turn could lead to a monopoly of the system. Realistically, it is even possible for groups of PKGs with the same IBE schemes in common to form coalitions, making collusion between PKGs easier and consequently increasing the risk of exposure for encrypted data. To our knowledge, no existing adaptation realizes the IBE ease-of-use, eliminates the demand for trust in a single third party, allows free choice in the combination of PKGs and thereby encryption schemes, and only provides key escrow under collaboration of the entire set of PKGs involved – all of which we address with CARIBE. Furthermore, if any receiver entity has offered itself as a PKG, a message sender may select that entity as one of the chosen PKGs, thereby bypassing escrow entirely on the message (CARIBE-S). Thus, for example, if various governments with sufficient resources offer themselves as PKGs under CARIBE-S, they also allow the option for communication partners to send escrow-prohibited messages to the selected government PKG entities; meanwhile messages to third parties can only be accessed under the combined agreement of all PKGs (for example, when legally required).

In order to address cogent issues in key management for data encryption, we propose applying IBE through the interface of cascade encryp-

tion, galvanizing it into a realistic scheme for response to modern issues. Even while allowing key escrow in the most extreme circumstances, and demanding no less than the participation of all key generators to achieve it, the freshly-interfaced IBE provides far greater power to the end user for selecting a trust model than has been previously proposed. Merging such varied cryptographic areas precisely reflects the spirit of the IACR *Copenhagen Resolution* [22]:

> Population-wide surveillance threatens democracy and human dignity. We call for expediting research and deployment of effective techniques to protect personal privacy against governmental and corporate overreach.

Markedly other, similar, infrastructures also exist, such as attribute-based encryption (anyone in possession of the correct set of attributes can decrypt) and, more generally, predicate-based encryption (anyone in possession of the correct set of attributes and a decryption key corresponding to a certain predicate can decrypt). While these are certainly interesting, we focus on IBE due to its resemblance to PKI, with encryption based upon fixed identities. However, it is straightforward to envisage that our results can be adapted for both attribute-based encryption and predicate-based encryption, with the same freedom-of-choice benefit of the trust model maintained for the end user.

1.1 Related Work

Identity-Based Cryptography Identity-based cryptography has seen a considerable amount of development since it was first envisaged by Shamir in the mid 1980's [37]. Initial examples of schemes for identity-based cryptography are due to Cocks [11], Boneh and Franklin [5], and Sakai, Ohgishi and Kasahara [35]. Today, there are entire books devoted to the subject [24, 8], as well as an extensive amount of research in various aspects of the field (for example, [5–7, 11, 12, 17, 20, 25, 35, 37, 42]).

Shamir argued for a public key encryption system conceptually similar to the postal system, albeit idealized, where a sender needs only the name and address of the recipient [37]. "IBE is a kind of public key encryption scheme where the public key of a user can be any arbitrary string – typically the e-mail address" [8], i.e. the recipient's identity, such as name, location, etc., becomes their public key. Enticingly, this approach offers some substantial advantages over the traditional PKI. One of the attributes that make IBE advantageous is its suitability for situations

where network access is not continuous. Furthermore, and perhaps one of the more notable advantages of identity-based cryptography, is the nullification of the need for certificates and thereby the instantaneousness with which encryption can be performed without the requirement to obtain such a certificate. Joux [23] provides a broad, non-specific introduction to identity-based cryptography, relating it with other common public key practices. Examples of current IBE frameworks for scheme proposals include Full-Domain-Hash IBE, Exponent-Inversion IBE, and Commutative-Blinding IBE [6].

In 2008, some research was performed into the security of IBE when decryption keys are generated under the same ID from multiple PKGs [33]. Those security results are highly relevant to this work, and support the security analysis of our schemes. However, we do not limit our cascades to the use of one encryption scheme.

While the wider field of identity-based cryptography is of great interest, throughout this paper our focus will be on key management in the context and, in particular, identity-based encryption. Thus, we will generically refer to IBE and key management for IBE schemes. Identity-based signatures and the problem with the key escrow have been addressed in [43].

Cascade Encryption Cascade encryption, or sequential multiple encryption, is the concept of layering encryption such that the ciphertext from one encryption step is the plaintext of the next. Essentially, an n-fold cipher cascade of Encrypt algorithms takes in a message m and outputs

$$(\text{Encrypt}_{k_n} \circ \cdots \circ \text{Encrypt}_{k_1})(m) \ .$$

Ways of realizing a cascade cipher include increasing the number of rounds of a cipher, cascading encryption under different keys, and cascading actual ciphers. In the context of IBE in this paper, the latter is of particular interest due to the potential benefits of employing various PKGs. Essentially, while multiple cipher rounds may be generally beneficial for security, it is the benefit of key escrow without mandatory trust in one PKG that makes cascade encryption attractive in the context of IBE.

Previous work focusing on cascade encryption includes that of Even and Goldreich [15] which proved that in a 2-fold block-cipher cascade, the security of the cascade was reducible to the security of either of the component ciphers. Later work showed that the security of an n-cipher cascade was reducible to that of the first cipher in the cascade [30] (using weaker security assumptions about the individual ciphers than [15]),

that triple-encryption (3-fold cipher cascade) for block ciphers provides a security improvement over single- or double-encryption [4, 16], and describe generic CCA security for multiple encryption [13]. Furthermore, it has been information-theoretically demonstrated that an n-fold cascade of pseudo-random permutations (PRPs), for which the computational distinguishing advantage is bounded by $\epsilon < 1$ (ϵ-PRP), yields a $((n-(n-1)\epsilon)\epsilon^n + \nu)$-PRP for negligible function ν [39].

Despite the extensive research on multiple and cascade encryption, the application of an n-fold IBE-cipher cascade has not been addressed, nor have security considerations (CCA, etc.) been considered in this context. Since IBE already presents a possible alternative to PKI with some alluring benefits, the security of cascade encryption composed of IBE schemes, and the exact manner in which such a cascade can be realized, is particularly interesting. Moreover, cascade encryption with IBE goes beyond the encryption itself – in such a context, it is essential to consider collusion among the private key generators (PKGs) involved.

1.2 Our Contributions

We propose CARIBE, an IBE scheme that addresses the ease-of-use, eliminates the demand for trust in a single third party, allows free choice in the combination of PKGs and thereby encryption schemes, and only provides key escrow under collaboration of the entire set of PKGs involved. CARIBE addresses the cogent issues in key management for data encryption by applying IBE through the interface of cascade encryption. Even while allowing key escrow in the most extreme circumstances, and demanding no less than the participation of all key generators to achieve it, CARIBE provides far greater power to the end user for selecting a trust model than has been previously proposed.

Furthermore, we define IND-ID-CCA security, IND-ID-C.CCA, for the CARIBE environment. The experiment game for IND-ID-C.CCA expands on IND-ID-CCA by allowing for scheme cascades. Handling of the ID-based indistinguishability experiment presents special challenges in a cascade, and is therefore presented in formalized pseudo-code, as opposed to the ad-hoc discussion definitions historically presented for IND-ID-CCA.

We highlight a special instance of CARIBE, CARIBE-S, which inherits security from CARIBE but completely avoids key escrow. This is accomplished with a simple addition that was present in some earlier schemes [12, §1.1.2]: namely, that recipients of encrypted messages are

themselves one of several cascaded PKGs. However, in contrast to previous proposals where recipients are also PKGs, our proposal argues that there is no need for involvement of any part of a public key infrastructure.

All CARIBE schemes apply a cascade of encryptions via multiple PKGs to eliminate the single point of failure that is inherent in traditional IBE. However, while generally with CARIBE there is a possibility for the principle of the key escrow to be realized under the assumption that all PKGs collude, in CARIBE-S that possibility is void due to the fact that one of the PKGs is the recipient itself. CARIBE schemes are not limited by the selection choice of concrete schemes involved. Unlike distributed IBE where all PKGs must operate under the same scheme, CARIBEs allow for the interaction of multiple IBE schemes. Notably, the benefit of this should not be under-estimated in the modern real-world context. Even as each PKG has freedom to use whatever IBE scheme it desires, a sender may either select PKGs based upon the combination of options given or upon a trust (or mutual distrust) foundation without regard to the corresponding IBE schemes being used. Thus, a sender may feasibly select rival PKGs to reduce the chances of collusion; for instance, PKGs implemented by, and operating under, the standards of competitive world powers [32, 34].

2 Background and Preliminaries

Identity-based cryptography falls within the scope of public key cryptography. Currently, public key systems rely almost completely on *certificate authorities* (CAs), employing certificate chaining to distribute, assert, and prove ownership of public keys. Popularly, this system is referred to as PKI [26]. Mao [29], as well as Katz and Lindell [26], offers a good foundational overview of PKI.

Structurally, identity-based cryptography diverges considerably from PKI and, as such, comes with certain advantages and disadvantages, particularly relating to key management. For a good introduction, Joux, via Joye and Neven [24], gives a clean and concise introduction to identity-based cryptography, relating it with the certificated system encompassed within public key infrastructure.

2.1 IBE schemes with more than one PKG

This section examines current proposals for IBE schemes employing more than one PKG, providing an overview of these architectures and highlighting the properties they possess.

Architecture	PKI	IBE
Key management authority	CA	PKG
Key Escrow	No	Yes
Certificate management	Yes	No
Non-interactive authentication	No	Yes
Always encrypt	No	Yes
Compromise of management authority is fatal	No	Yes

Table 1: Comparison of properties between PKI and IBE.

Hierarchical IBE Originally envisaged by Horwitz and Lynn, HIBE has parallels with the hierarchical nature of current PKI [20]. Like PKI it is comprised of root nodes, intermediate nodes, and users. Informally, the root PKG holds the master secret key $\mathsf{masterkey}$, while an intermediate PKG holds its own identity ($\mathsf{ID}_{\text{PKG.i}}$) and must request their own secret key from the root PKG. Similarly, the user has an identity ($\mathsf{ID}_{\text{user}}$) and requests its secret key from the intermediate node. Keys at each stage are derived from functions on the keys at the higher level, as demonstrated in the following generalization for a hierarchy of n PKGs [20].

$$
\begin{aligned}
&\text{Root}: && f_1(\mathsf{masterkey}, \mathsf{ID}_{\text{PKG.2}}) = dkey_2 \rightarrow \text{PKG.2} \\
&\text{PKG.2}: && f_2(dkey_2, \mathsf{ID}_{\text{PKG.3}}) = dkey_3 \rightarrow \text{PKG.3} \\
&\vdots \\
&\text{PKG.}n: && f_n(dkey_n, \mathsf{ID}_{\text{User}}) = dkey_{\text{User}} \rightarrow \text{User}
\end{aligned}
$$

It is worth noting that the functions f_i, for $i \in \{1, n\}$, are known and that every intermediate PKG_i in the hierarchy, excepting the user, may have multiple descendants.

Gentry and Silverberg offered an improved HIBE scheme, presenting an instantiation of HIBE that is CCA-secure under the Bilinear Diffie-Hellman Problem and collusion resistant [17].

Other extensions of hierarchical IBE schemes exist, such as Multi-HIBE and Anonymous-HIBE. Multi-hierarchical offers forward security

[42] and anonymous-hierarchical offers anonymous communication between sender and receiver [7].

Certificateless Public Key Cryptography Certificateless public key cryptography (CL-PKC) (see [1] and [10]), was developed with the aim of finding public key schemes that are not dependent on certificates and do not have the key escrow property. As CL-PKC is claimed as an intermediate between standard PKI and the identity-based variant, we describe how it works on a high level.

CL-PKC requires two parties to generate public and private keys, where one is the end user. The PKG in this instance has a known public key $\mathsf{ID}_{\mathrm{PKG}}$ and a master secret key. The user U has an identity $\mathsf{ID}_{\mathrm{User}}$ and some secret information SecInfo–U known only to themselves, with the public key and the secret key generated from these parameters.

$$\begin{aligned} \text{PKG}: &\quad f_1(\mathsf{masterkey}, \mathsf{ID}_{\mathrm{User}}) = dkey_{\tilde{U}} \rightarrow \text{User} \\ \text{User}: &\quad f_2(dkey_{\tilde{U}}, \text{SecInfo–}U) = dkey_U \\ \text{User}: &\quad f_3(\text{SecInfo–}U, \mathsf{ID}_{\mathrm{PKG}}) = pkey_U \end{aligned}$$

Again, the functions f_i are assumed to be known for all i, and $dkey_{\tilde{U}}$ represents the partial decryption key for user U, which must be combined with the users secret information to form the decryption key.

Generation of the public key can still be done prior to generation of the private key. Note that the public key is not computable from the identity of the user and therefore must also be pre-computed and made available publicly (though verification of the public key is no longer required). Consequently, due to the nature of this public key derivation, CL-PKC is no longer identity-based [1] and lacks the major advantage of the identity-based paradigm which allows any-time encryption without the receiver having to preform any set up.

Distributed IBE Joux [23] advocates for a system with many, independent PKGs for nullifying the issue of compromise of a single PKG: "Such a scheme could mitigate the trust issues, at the cost of making the private key generation step heavier ..." Distributed IBE, as formally defined by Kate and Goldberg [25] does precisely that, with a form of threshold trust. Informally, an IBE scheme of n PKGs is (n, t)-distributed if no collusion of $x \leq t$ of the PKGs can compute the master key, for some threshold value $t \leq n$, where all n PKGs contain a share of a user's private key. In the distribution model, the n PKGs share parts of one master secret key.

An approach that is complementary to the distributed IBE approach was proposed by Chow in [9].

2.2 Identity-Based Encryption

Formally, we present the definition of an IBE scheme which serves as a grounding point for the work in this section. From IBE schemes, we build CARIBE – the scheme contribution of this paper – using generic, yet unspecified, number of n PKG.

Definition 1 (Identity-Based Encryption [12]). *Under a Private Key Generator (PKG), an identity-based encryption scheme $IBE.\mathcal{E}$ is a tuple of algorithms:*

- $\text{Setup}(\lambda) \xrightarrow{\$} (\mathsf{params}, \mathsf{masterkey})$*: A probabilistic setup generation algorithm that takes as input a security parameter λ and outputs parameters* params *and a PKG master key* masterkey*.*
- $\text{Extract}(\mathsf{params}, \mathsf{masterkey}, \mathsf{ID}) \xrightarrow{\$} dkey$*: A probabilistic extraction algorithm that takes as input system parameters* params*, a PKG master key* masterkey*, and a public identity string* ID*, and outputs a decryption key dkey.*
- $\text{Encrypt}(\mathsf{params}, \mathsf{ID}, m) \xrightarrow{\$} c$*: A probabilistic encryption algorithm that takes as input system parameters* params*, a public identity string* ID*, and a message $m \in \mathcal{M}$, and outputs a ciphertext $c \in \mathcal{C}$.*
- $\text{Decrypt}(\mathsf{params}, c, dkey) \xrightarrow{\$} m$*: A possibly probabilistic decryption algorithm that takes as input system parameters* params*, a ciphertext $c \in C$, and a private decryption key dkey, and outputs either a message $m \in \mathcal{M}$ or an error symbol $\perp$.*

In addition, it is required that if $dkey \leftarrow \text{Extract}(\mathsf{params}, \mathsf{masterkey}, \mathsf{ID})$*, then*

$$\forall m \in \mathcal{M} : \text{Decrypt}(\mathsf{params}, \text{Encrypt}(\mathsf{params}, \mathsf{ID}, m), dkey) = m \ .$$

As an accepted assessment of security for public key encryption schemes, IND-CCA is also the criterion for security in the layered PKG setting. While IND-CCA security has been extensively handled before [3], and even the particular case of IND-ID-CCA for IBE described [12], a clear, formalized, pseudo-code definition for IND-ID-CCA has been lacking. Consequently, we unambiguously delineate the IND-ID-CCA experiment and adversary win conditions, corresponding to Definition 2, in Fig. 1. Notationally, we let Π denote the protocol employed by the PKG.

Definition 2. *Let Π be an identity-based encryption scheme according to Definition 1 and let $\mathcal{A}$ be an adversary algorithm. Then, for the IND-ID-CCA experiment given in Fig. 1,*

$$\mathsf{Adv}^{\text{IND-ID-CCA}}_{\Pi,\mathcal{A}} = |\Pr[b = b'] - {}^1\!/_2| \ .$$

$\underline{\mathsf{Exp}^{IND-ID-CCA}_{\Pi,\mathcal{A}}():}$

1: $(\mathsf{params}, \mathsf{masterkey}) \xleftarrow{\$} \text{Setup}(\lambda)$
2: $\mathsf{ID.list_{ext}} \leftarrow \perp$
3: $\mathsf{ID.list_{enc}} \leftarrow \perp$
4: $S \leftarrow \emptyset$
5: $b \xleftarrow{\$} \{0,1\}$
6: $\mathcal{A}^{\text{Extract}(\cdot),\text{Encrypt}(\cdot),\text{Decrypt}(\cdot),\mathsf{params}}()$
7: $b' \xleftarrow{\$} \mathcal{A}^{\text{Extract}(\cdot),\text{Encrypt}(\cdot),\text{Decrypt}(\cdot),\mathsf{params}}$

$\underline{\text{Oracle } \mathsf{Extract}(\mathsf{ID}_i):}$

1: **if** $\mathsf{ID}_i \in \mathsf{ID.list_{enc}}$ **then**
2: **return** $\perp$
3: $dkey_i \leftarrow \text{Extract}(\mathsf{params}, \mathsf{masterkey}, \mathsf{ID}_i)$
4: $\mathsf{ID.list_{ext}} \leftarrow \mathsf{ID.list_{ext}}|\mathsf{ID}_i$
5: **return** $dkey_i$

$\underline{\text{Oracle } \mathsf{Decrypt}(\mathsf{ID}_i, c_i):}$

1: **if** $(\mathsf{ID}_i, c_i) \in S$ **then**
2: **return** $\perp$
3: $dkey_i \leftarrow \text{Extract}(\mathsf{params}, \mathsf{masterkey}, \mathsf{ID}_i)$
4: $m_i \leftarrow \text{Decrypt}(\mathsf{params}, c_i, dkey_i)$
5: **return** m_i

$\underline{\text{Oracle } \mathsf{Encrypt}(\mathsf{ID}, m_0, m_1):}$

1: **if** $\mathsf{ID} \in \mathsf{ID.list_{ext}}$ **then**
2: **return** $\perp$
3: $c^{(0)} \leftarrow \text{Encrypt}(\mathsf{params}, \mathsf{ID}, m_0)$
4: $c^{(1)} \leftarrow \text{Encrypt}(\mathsf{params}, \mathsf{ID}, m_1)$
5: **if** $c^{(0)} = \perp$ or $c^{(1)} = \perp$ **then**
6: **return** $\perp$
7: $c_u := c^{(b)}$
8: $S \leftarrow S \cup \{(\mathsf{ID}, c_u)\}$
9: $\mathsf{ID.list_{enc}} \leftarrow \mathsf{ID.list_{enc}}|\mathsf{ID}$
10: **return** c_u

Fig. 1: IND-ID-CCA Experiment for $IBE.\mathcal{E}$.

3 Cascade-realized IBE – CARIBE

Employing a generic, finite number of n IBE schemes, as defined above, we describe Cascade-realized Identity-Based Encryption (CARIBE), an n-fold IBE-cipher cascade, in Definition 3. Saliently, the CARIBE definition

does not restrict the type of encryption schemes being used. As a result, a CARIBE scheme $CARIBE.\mathcal{E}$ could literally consist of PKGs using n distinct IBE schemes, if such variation is desired or deemed necessary. Essentially, a CARIBE scheme works with cascaded encryption; however, unlike general cascade encryption schemes, multiple PKGs are involved and encryption is sequentially performed using the parameters params generated by each of them.

In the following definition it is required that each generated ciphertext is in the plaintext space of the next cipher in the encryption cascade. We make the practical assumption that the selected IBE schemes are compatible in this manner, either directly using the plaintext space as ciphertext space, or indirectly, by applying some transformation before encryption, which is known to all parties. Note that, as the outputs of all schemes can be interpreted as a sequence of bits, the composition of IBE schemes defined on different algebraic domains is possible.

Definition 3 (Cascade-realized Identity-Based Encryption). *Under n Private Key Generators (PKG), a cascade-realized identity-based encryption scheme $CARIBE.\mathcal{E}$ is a tuple of algorithms that takes n IBE encryption schemes Π_i, for $i \in \{1, \dots n\}$ where $n \geq 2$, with the restriction that $\mathcal{C}_i \subseteq \mathcal{M}_{i+1}$ for $i \in \{1, \dots n-1\}$, i.e. that the ciphertext of each IBE scheme is in the plaintext space of the next IBE scheme in the cascade. Algorithms for $CARIBE.\mathcal{E} := C(\Pi_1, \dots, \Pi_n)$ are as follows:*

- $\text{Setup}_S(\lambda_1, \dots, \lambda_n)$:

  1: **for** $i \in \{1, \dots, n\}$ **do**
  2: $\quad(\mathsf{params}_i, \mathsf{masterkey}_i) \leftarrow \text{Setup}_i(\lambda_i)$
  3: **return** $(\{\mathsf{params}_i\}, \{\mathsf{masterkey}_i\})$

  A probabilistic setup generation algorithm that takes as input an ordered sequence of n security parameters λ_i and outputs an ordered set of n parameters $\{\mathsf{params}_i\}$ and an ordered set of n PKG master keys $\{\mathsf{masterkey}_i\}$, for $i \in \{1, \dots n\}$.
- $\text{Extract}_S((\{\mathsf{params}_i\}, \{\mathsf{masterkey}_i\}), \mathsf{ID})$:

  1: **for** $i \in \{1, \dots, n\}$ **do**
  2: $\quad dkey_i \leftarrow \text{Extract}_i(\mathsf{params}_i, \mathsf{masterkey}_i, \mathsf{ID})$
  3: **return** $\{dkey_i\}$

  A probabilistic extraction algorithm that takes as input a set of n system parameters $\{\mathsf{params}_i\}$, a set of n PKG master keys $\{\mathsf{masterkey}_i\}$, and a public identity string ID, and outputs a set of n decryption keys $\{dkey_i\}$, for $i \in \{1, \dots n\}$.
- $\text{Encrypt}_S(\{\mathsf{params}_i\}, \mathsf{ID}, m)$:

1: $c_2 \leftarrow \text{Encrypt}_1(\mathsf{params}_1, \mathsf{ID}, m)$
2: **for** $i \in \{2, \ldots, n\}$ **do**
3: $\quad c_{i+1} \leftarrow \text{Encrypt}_i(\mathsf{params}_i, \mathsf{ID}, c_i)$
4: $c \leftarrow c_{n+1}$
5: **return** c

A probabilistic encryption algorithm that takes as input an ordered set of n system parameters $\{\mathsf{params}_i\}$, for $i \in \{1, \ldots n\}$, a public identity string ID, and a message $m \in \mathcal{M}$, and outputs a ciphertext $c \in \mathcal{C}$. The plaintext space of Encrypt_S is $\mathcal{M} := \mathcal{M}_1$, the plaintext space of Encrypt_1, while the ciphertext space of Encrypt_S is $\mathcal{C} := \mathcal{C}_n$, the ciphertext space of Encrypt_n.

– $\text{Decrypt}_S(\{\mathsf{params}_i\}, c, \{dkey_i\})$:

1: $c_n \leftarrow c$
2: $i \leftarrow n$
3: **while** $i > 0$ **do**
4: $\quad c_{i-1} \leftarrow \text{Decrypt}_i(\mathsf{params}_i, c_i, dkey_i)$
5: $\quad i \leftarrow i - 1$
6: $m \leftarrow c_0$
7: **return** m

A possibly probabilistic decryption algorithm that takes as input an ordered set of n system parameters $\{\mathsf{params}_i\}$, a ciphertext $c \in C$, and an ordered set of n private decryption keys $\{dkey_i\}$, and outputs either a message $m \in \mathcal{M}$ or an error symbol $\perp$.

In addition, it is required that if $\{dkey_i\} \leftarrow \text{Extract}_S(\{\mathsf{params}_i\}, \{\mathsf{masterkey}_i\}, \mathsf{ID})$, *then*

$$\forall m \in \mathcal{M} : \text{Decrypt}_S(\{\mathsf{params}_i\}, \text{Encrypt}(\{\mathsf{params}_i\}, \mathsf{ID}, m), \{dkey_i\}) = m \ .$$

Remark 1. Note that while we require at least two PKGs ($n \geq 2$), we do not *require* unique encryption schemes. Indeed, it is possible for any two PKGs, PKG_i and PKG_j with encryption schemes Π_i and Π_j, respectively, that $\Pi_i = \Pi_j$.

3.1 Security of CARIBE

CARIBE is essentially a type of cascade encryption scheme and as such presents a challenge in the context of CCA security. As noted in [13], any encryption cascade fails to provide CCA security, since an adversary that is in possession of the key of the outermost encryption layer could simply decrypt that layer and re-encrypt, yielding a new ciphertext to call

the decryption oracle on, trivially breaking the CCA security. However, this is based upon the assumption that an adversary already has the key for the outermost encryption, and assuming such key possession is generally non-standard when considering CCA security. To avoid this fairly trivial break, we propose the following assumption when analyzing the CCA security of cascade schemes; a CCA security game based upon this assumption will be termed Cascade CCA (C.CCA):

C.CCA Assumption for Cascaded Encryption *For a cascaded encryption scheme, with ciphertexts generated as* $c := \mathrm{E}_{K_n}(\ldots(\mathrm{E}_{K_2}(\mathrm{E}_{K_1}(m))))$*, and an adversary* $\mathcal{A}$*, CCA security is analyzed under the assumption that* $\mathcal{A}$ *does not possess* K_n*.*

Note that if $\mathcal{A}$ possesses the encryption keys for the outermost r layers, and can win a CCA security game on an encryption scheme cascade of the remaining $n - r$ layers, then $\mathcal{A}$ can certainly win the CCA game on the entire scheme. Thus, the layers can be "peeled back" until $\mathcal{A}$ does not possess the outermost decryption key. While making this assumption is not ideal for security analysis, it is necessary to avoid the trivial break mentioned above and allows for realistic analyses to still be performed for cascaded schemes.

In addition to the CARIBE scheme description, we present the tailored IND-ID-C.CCA experiment in Fig. 2. While most schemes are analyzed under a general security experiment, an experiment for CARIBE itself is required as any CARIBE scheme is in fact a particular cascade selection of other IBE schemes. Adversarial advantage for the experiment is described in Definition 4.

Definition 4. *Let* C *be an algorithm taking as input* n *identity-based encryption schemes* Π_j*, for* $j \in \{1, \ldots, n\}$ *where* $n \geq 2$*, according to Definition 1 and yielding a cascade-realized identity-based encryption scheme* $C(\Pi_1, \ldots, \Pi_n)$*, per Definition 3, comprised of a new tuple of algorithms* $(\mathrm{Setup}_S, \mathrm{Extract}_S, \mathrm{Encrypt}_S, \mathrm{Decrypt}_S)$*. Let* $\mathcal{A}$ *be an adversary algorithm. Then, for the IND-ID-C.CCA experiment given in Fig. 2,*

$$\mathsf{Adv}^{\text{IND-ID-C.CCA}}_{C(\Pi_1,\ldots,\Pi_n),\mathcal{A}} = |\Pr[b = b'] - {}^1\!/_2| \ .$$

As noted in Remark 1, we do not *require* unique encryption schemes Π, although at least two PKGs ($n \geq 2$) are required for the cascaded IND-ID-C.CCA definition.

$\underline{\mathsf{Exp}^{IND-ID-C.CCA}_{C(\Pi_1,\ldots,\Pi_n),\mathcal{A}}():}$

1: $(\{\mathsf{params}_j\}, \{\mathsf{masterkey}_j\}) \xleftarrow{\$} \mathrm{Setup}(\lambda_1, \ldots, \lambda_n)$
2: $\mathsf{ID.list_{ext}} \leftarrow \perp$
3: $\mathsf{ID.list_{enc}} \leftarrow \perp$
4: $S \leftarrow \emptyset$
5: $b \xleftarrow{\$} \{0, 1\}$
6: $\mathcal{A}^{\mathrm{Extract}_S(\cdot),\mathrm{Encrypt}_S(\cdot),\mathrm{Decrypt}_S(\cdot),\{\mathsf{params}_j\}}()$
7: $b' \xleftarrow{\$} \mathcal{A}^{\mathrm{Extract}_S(\cdot),\mathrm{Encrypt}_S(\cdot),\mathrm{Decrypt}_S(\cdot),\{\mathsf{params}_j\}}$

$\underline{\text{Oracle } \mathsf{Extract}_S(\mathsf{ID}_i, \{1, \ldots, n\}):}$

1: **if** $\mathsf{ID}_i \in \mathsf{ID.list_{enc}}$ **then**
2: **return** $\perp$
3: $\{dkey_j\} \leftarrow \mathrm{Extract}_S(\{\mathsf{params}_j\}, \{\mathsf{masterkey}_j\}, \mathsf{ID}_i)$
4: $\mathsf{ID.list_{ext}} \leftarrow \mathsf{ID.list_{ext}}|\mathsf{ID}_i$
5: **return** $\{dkey_j\}_i$

$\underline{\text{Oracle } \mathsf{Decrypt}_S(\mathsf{ID}_i, c_i, \{1, \ldots, n\}):}$

1: **if** $(\mathsf{ID}_i, c_i) \in S$ **then**
2: **return** $\perp$
3: $\{dkey_j\}$
$\leftarrow \mathrm{Extract}_S(\{\mathsf{params}_j\}, \{\mathsf{masterkey}_j\}, \mathsf{ID}_i)$
4: $m_i \leftarrow \mathrm{Decrypt}_S(\{\mathsf{params}_j\}, c_i, \{dkey_j\})$
5: **return** m_i

$\underline{\text{Oracle } \mathsf{Encrypt}_S(\mathsf{ID}, m_0, m_1, \{1, \ldots, n\}):}$

1: **if** $\mathsf{ID} \in \mathsf{ID.list_{ext}}$ **then**
2: **return** $\perp$
3: $c^{(0)} \leftarrow \mathrm{Encrypt}_S(\{\mathsf{params}_j\}, \mathsf{ID}, m_0)$
4: $c^{(1)} \leftarrow \mathrm{Encrypt}_S(\{\mathsf{params}_j\}, \mathsf{ID}, m_1)$
5: **if** $c^{(0)} = \perp$ or $c^{(1)} = \perp$ **then**
6: **return** $\perp$
7: $c := c^{(b)}$
8: $S \leftarrow S \cup \{(\mathsf{ID}, c)\}$
9: $\mathsf{ID.list_{enc}} \leftarrow \mathsf{ID.list_{enc}}|\mathsf{ID}$
10: **return** c

Fig. 2: IND-ID-C.CCA Experiment for $CARIBE.\mathcal{E}$.

Security for CARIBE depends upon the constituent IBE schemes involved, as each contributes to the security of the final ciphertext. As previously mentioned, it has been shown that the encryption security of a 2-fold cascade is reducible to the security of either of the composite ciphers [14, 15]. Consequently, not only do we focus on the expanded n-fold case, but take into consideration the possibility of collusion. On a logical level, the ciphertext cannot be decrypted even if $n-1$ of the n PKGs collude, so long as one PKG is honest. Essentially, this worst-case scenario would then be precisely equivalent to a basic, secure IBE scheme under an honest PKG. Thus, the distinction between a CARIBE and IBE scheme becomes one of existence; for IBE we demand that the IBE scheme in use is secure with an honest PKG, while for CARIBE it is only required that one such IBE scheme exists in the cascade. Succinctly, Theorem 1 provides a proof of this analysis, similar to that of [15] yet given in detail for IBE.

To enable the analysis, we operate in an execution environment with the following standard list of allowed adversarial queries:

- $\mathsf{Extract}_S(\mathsf{ID}_i, \{1, \ldots, n\})$: Operates as in Fig. 2.
- $\mathsf{Encrypt}_S(\mathsf{ID}, m_0, m_1, \{1, \ldots, n\})$: Operates as in Fig. 2.
- $\mathsf{Decrypt}_S(\mathsf{ID}_i, c_i, \{1, \ldots, n\})$: Operates as in Fig. 2.
- $\mathsf{Corrupt}_S(\Pi_j)$: This query returns $\mathsf{masterkey}_j$. As an adversary $\mathcal{A}$ already has access to params_j, corrupting Π_j allows $\mathcal{A}$ to extract decryption keys $dkey_j$ for any ID_i. This query models $\mathcal{A}$'s ability to request the collusion of the PKG operating Π_j.

Note that we prove Theorem 1 for a static adversary which, although it may adaptively corrupt nodes at will, must commit to at least one honest PKG before the protocol run. Notably, this follows similarly to the chain of past IBE work, where a static adversarial model is common [25]. Our theorem, and its accompanying proof, are IBE-specific adaptions of a more general approach by Dodis and Katz for cascade encryption [13]. The proof is given in detail here to elucidate the adversarial power in the inter-workings of IBE, and how a challenger answers adversarial queries.

Theorem 1. *If $IBE.\mathcal{E}$ protocols Π_j, for $j \in \{0, \ldots, n\}$, are combined to form $CARIBE.\mathcal{E} = C(\Pi_1, \ldots, \Pi_n)$, the resulting $CARIBE.\mathcal{E}$ protocol will be IND-ID-C.CCA provided that there exists $\Pi_t \in \{\Pi_j\}$ that is IND-ID-CCA secure.*

Specifically, for any efficient adversary $\mathcal{A}$ that runs in time $\mathtt{t}$ and asks $q = q_{ext} + q_{enc} + q_{dec}$ queries, where q_{ext} are extraction queries,

q_{enc} are encryption queries, and q_{dec} are decryption queries, there exists adversaries $\mathcal{B}_j$ that run in time $\mathtt{t}_{\mathcal{B}} \approx \mathtt{t}$ and asks $q_{\mathcal{B}}$ queries, such that

$$\mathsf{Adv}^{\text{IND-ID-C.CCA}}_{C(\Pi_1,\ldots,\Pi_n)}(\mathcal{A}) \leq \mathsf{Adv}^{\text{IND-ID-CCA}}_{\Pi_t}(\mathcal{B}_t) \ .$$

Proof. Let $\mathcal{A}$ be an challenger against the IND-ID-C.CCA security of $CARIBE.\mathcal{E} = C(\Pi_1, \ldots, \Pi_n)$ and let $\mathcal{B}$ be an adversary against the IND-ID-C.CCA of $IBE.\mathcal{E}$ for Π_t, with $\mathsf{Extract}_t$, $\mathsf{Encrypt}_t$, and $\mathsf{Decrypt}_t$ oracles running on params_t and $\mathsf{masterkey}_t$, corresponding to Π_t, as well as Extract_j, Encrypt_j, and Decrypt_j algorithms running on params_j and $\mathsf{masterkey}_j$ for $j \in \{1, \ldots, n\}/\{t\}$ which he uses to answer $\mathcal{A}$'s queries. Let $S_{\mathcal{B}}$ be a list of pairs (ID, c) which $\mathcal{B}$ sends back to $\mathcal{A}$ in response to $\mathsf{Encrypt}_S$ queries, maintained by $\mathcal{B}$ and initialized to $\perp$. If at any time $\mathcal{A}$ makes a $\mathsf{Corrupt}(\Pi_t)$ query, $\mathcal{B}$ gives up.

When $\mathcal{A}$ asks an $\mathsf{Extract}_S$ query on $(\mathsf{ID}_i, \{1, \ldots, n\})$, $\mathcal{B}$ calls his $\mathsf{Extract}_t$ oracle and Extract_j algorithms, and sends the agglomerated responses $\{dkey_j\}$ to $\mathcal{A}$.

When $\mathcal{A}$ asks a $\mathsf{Decrypt}_S$ query on a ciphertext c, $\mathcal{B}$ sequentially uses his Decrypt_j algorithms – starting with Decrypt_n on c, followed with Decrypt_{n-1} on the output of Decrypt_n, and so forth for $t < j$. $\mathcal{B}$ then call $\mathsf{Decrypt}_t$ on the output of Decrypt_{t+1}. Thereafter, $\mathcal{B}$ continues with his Decrypt_j calculations, starting with Decrypt_{t-1} on the output of $\mathsf{Decrypt}_t$, for $j < t$. Finally, the result of Decrypt_1 is returned to $\mathcal{A}$.

Should $\mathcal{A}$ query $\mathsf{Encrypt}_S$ on $(\mathsf{ID}, m_0, m_1, \{1, \ldots, n\})$, $\mathcal{B}$ behaves as follows: $\mathcal{B}$ calculates $\text{Encrypt}_1(\mathsf{params}_1, \mathsf{ID}, m_0) = c_1^{(0)}$ and $\text{Encrypt}_1(\mathsf{params}_1, \mathsf{ID}, m_1) = c_1^{(1)}$, then $\text{Encrypt}_j(\mathsf{params}_j, \mathsf{ID}, c_{j-1}^{(0)}) = c_j^{(0)}$ and $\text{Encrypt}_j(\mathsf{params}_j, \mathsf{ID}, c_{j-1}^{(1)}) = c_j^{(1)}$ for $1 < j < t$. Then, $\mathcal{B}$ calls $\mathsf{Encrypt}_t(\mathsf{ID}, c_{t-1}^{(0)}, c_{t-1}^{(1)})$ to get c_t. Thereafter $\mathcal{B}$ continues calculating $\text{Encrypt}_j(\mathsf{params}_j, \mathsf{ID}, c_{j-1}) = c_i$ for $t < j \leq n$. Finally, $\mathcal{B}$ sets $c := c_n$, $S \leftarrow S \cup (\mathsf{ID}, c)$, and passes c back to $\mathcal{A}$.

By the IND-ID-C.CCA success of $\mathcal{A}$ against $CARIBE.\mathcal{E}$, at some point $\mathcal{A}$ returns a correct bit guess b'. Hence, $\mathcal{B}$ also wins the IND-ID-CCA game against the $IBE.\mathcal{E}$ protocol Π_t with b'. □

From Theorem 1 it can be observed that the CARIBE scheme is at least as secure as the strongest IBE protocol in the cascade. As mentioned before, should multiple PKG collude to determine the decryption key or plaintext, this implies that a CARIBE scheme is secure as long as at most $n - 1$ of the n PKGs collude.

4 Cascade-Realized IBE with Self-PKG – CARIBE-S

While the PKGs used in CARIBE would naturally be expected to be separate from the users, special security considerations arise when we consider the possibility of a *self-PKG*, where a receiver also acts in the role of a PKG. This could be desirable in real-world implementation, for example, if the receiver is a government organisation with both the capabilities and legal authority to be a self-PKG. Although the receiver may trust its PKG, and even demand its use for all in-coming messages, the sender may not. In response to this situation, the sender may include the receiver's PKG along with other (trusted) PKGs under CARIBE-S, creating a mutually satisfactory trust relationship. Thus, while avoiding key escrow, CARIBE-S allows for a trust balance between sender and receiver.

Definition 5 (CARIBE-S). *We say that an entity is a member of a CARIBE-S scheme if it is one of n PKGs in the Definition 3.*

Naturally, a receiver cannot force a self-selection as a PKG under CARIBE. This is to be expected. As in CARIBE, the decision to use a CARIBE-S and avoid key-escrow is completely the sender's choice. However, it is dependent on the *a priori* action on a receiver's part to arrange PKG functionality. Consequently, the option of a CARIBE-S is also restricted to those receivers with the resources and forethought to form self-PKGs.

4.1 Security of CARIBE-S

From the security of CARIBE we have the following theorem.

Theorem 2 (Security of CARIBE-S). *If $IBE.\mathcal{E}$ protocols Π_j, for $j \in \{0, \ldots, n\}$, are combined to form $CARIBE.\mathcal{E} = C(\Pi_1, \ldots, \Pi_n)$, the resulting $CARIBE.\mathcal{E}$ protocol will be IND-ID-C.CCA provided that there exists $\Pi_t \in \{\Pi_j\}$ that is IND-ID-CCA secure.*

Specifically, for any efficient adversary $\mathcal{A}$ that runs in time $\mathtt{t}$ and asks $q = q_{ext} + q_{enc} + q_{dec}$ queries, where q_{ext} are extraction queries, q_{enc} are encryption queries, and q_{dec} are decryption queries, there exists adversaries $\mathcal{B}_j$ that run in time $\mathtt{t}_{\mathcal{B}} \approx \mathtt{t}$ and asks $q_{\mathcal{B}}$ queries, such that

$$\mathsf{Adv}^{\text{IND-ID-C.CCA}}_{C(\Pi_1,\ldots,\Pi_n)}(\mathcal{A}) \leq \mathsf{Adv}^{\text{IND-ID-CCA}}_{\Pi_t}(\mathcal{B}_t) \ .$$

Whilst a CARIBE scheme is secure as long as at most $n-1$ of the n PKGs collude, in CARIBE-S, one of the PKGs which has joined the

infrastructure, having provided its PKG parameters, is also the intended recipient of the encrypted messages. Thus, Corollary 1 follows directly from Theorem 2.

Corollary 1 (Security against Collusion of CARIBE-S). *A CARIBE-S scheme is secure against collusion and thus is not a key escrow scheme.*

Table 3 in Appendix A presents a comparison of CARIBE and CARIBE-S with other IBE-composite schemes discussed in §2.1, under standard structure. Both CARIBE and CARIBE-S allow for composition across multiple IBE platforms – namely, each PKG can use a different IBE scheme for extraction, encryption, etc. In the interest of security, this yields logical real-world benefits in the case where preferred PKGs, known to be adverse to mutual collusion, insist on utilizing different IBE schemes.

4.2 Ciphertext Expansion in CARIBE/CARIBE-S

One natural consequence of cascaded encryption is the amplification of ciphertext expansion. Historically, ciphertext expansion would be a concern under slow transmission rates, and since it is already common in IBE schemes, further expansion from cascades would hardly have been welcomed. However, with increasing improvements in IBE scheme developments involving less expansion, as well as faster transmission rates than were previously available, this issue is not as imposing as it once was. Moreover, in the context of modern internet privacy concerns, it is more likely that users will be willing to trade factors like the convenience of fast transmission times, for increased privacy and security.

Since CARIBE is a composition of ciphers of the sender's choice, it is not possible to predict the relative ciphertext expansion in advance without knowing which ciphers, and in what order, the sender will select. Still, some basic observations can be noted. Unquestionably, the expansion involved in a CARIBE of several compositions of Cocks' IBE schemes [11] would be enormous, as ciphertext length in under single encryption is already several times larger than the plaintext length. Yet the ciphertext expansion for a regular, single Cocks scheme is daunting enough at the outset to be naturally prohibitive in practice. Meanwhile, in a CARIBE of n Boneh–Franklin [12] ciphers, a plaintext length $|m|$ would expand to $n \cdot |P| + |m|$, where $|P|$ is the length of a pre-selected element of a group $\mathbb{G}$, of large prime order q, which is part of a bilinear map. Markedly, such a linear expansion is hardly imposing. Aside from classic IBE ciphers, ciphertext expansion in modern IBE proposals lie spread on the scale

between these examples, yet far closer to Boneh–Franklin efficiency than Cocks. With simultaneously increasing efficiency and security awareness, it is reasonable that expansion for CARIBE will be of limited concern.

5 Software libraries for implementation of CARIBE and CARIBE-S

Our proposals for CARIBE and CARIBE-S collect widely known and tested concepts and combine them in a novel way, expanding the horizons of IBE. This is not a new approach. We can refer to the well known concept of Bitcoin that had a similar approach [31] in the beginning.

In the modern Internet era, the crucial moment for a collection of concepts to become a widely used paradigm is linked to the existence of publicly available (preferably free) software tools and libraries. We argue that these types of conditions are maturing for CARIBE and CARIBE-S. In Table 2 we give a list of tools, packages or libraries that can perform the operations for Pairing-Based Cryptography – these are described in more detail below.

Name	License	Language
PBCl	GNU GPL	C
MIRACL	Free non noncommercial	C/C++
SAGE	GNU GPL	Python
PARI/GP	GNU GPL	C/GP
RELIC	GNU Lesser GPL	C
HP IBE	Yes	C/C++

Table 2: Software libraries and packages for Pairing-Based Cryptography

- The Pairing-Based Cryptography Library [28] is a free portable C library for rapid prototyping of pairing-based cryptosystems. It provides an interface to a cyclic group with a bilinear pairing. It has also Perl, Python, Java and C++ wrappers and bindings.
- MIRACL [36] is a C/C++ library that provides pairing-based cryptography primitives. It runs on different OS and CPU platforms but is especially efficient on x86 platforms due to hand-optimized assembly code for low-level arithmetic. It is free for noncommercial use.

– SAGE [38] is a powerful open-source computer algebra system. Its interface is Python based. It has huge number of cryptographic functions including some of the worlds fastest implementations of operations with elliptical curves.
– PARI/GP [40] is a computer algebra system designed for fast computations in number theory. It is implemented in C but it has also a script language called GP.
– RELIC [2] is a modern cryptographic meta-toolkit with emphasis on efficiency and flexibility. RELIC implements Elliptic curves over prime and binary fields (NIST curves and pairing-friendly curves), Bilinear maps and related extension fields. Its portable C produces very efficient codes in a range from tiny micro-controllers to powerful modern 64-bit CPUs.
– In February 2015, HP announced that they will acquire Voltage Security Inc. that previously offered the IBE Toolkit. Now that toolkit is commercially available as HP Identity-Based Encryption.

6 Conclusion

CARIBE-S is a completely key escrow-free variant of a CARIBE, combining IBE and cascade encryption. It synthesizes diverse ideas to provide more benefits and a higher level of security than have been achieved in other schemes.

Even though there is an inherent time-cost in multiple encryptions for CARIBE and CARIBE-S, the added security coupled with ever-increasing computing power, and publicly available open source or commercial software libraries, dilutes this drawback. Additionally, while the onus is on the receiver to obtain decryption keys from multiple authorities, the sender's ability to virtually select a security level for encryption through the PKGs of their choice – possibly based on the encryption type provided by the PKG – may commonly be seen as a sufficient time/security trade-off.

In comparison with other multi-PKG IBE variations, this end-user security selection power provides the catalyst for re-visiting cascade encryption in a previous un-investigated context. In terms of the modern world, where desire to legally access encrypted messages is paired with hostility among internet powers, the consolidation or avoidance of key escrow and leveraged distrust makes CARIBE – and therefore CARIBE-S – a viable option.

Acknowledgements

We would like to thank the anonymous reviewers of Mycrypt 2016 for their valuable comments and suggestions.

References

1. Sattam S. Al-Riyami and K. G. Paterson. Certificateless public key cryptography. In *Advances in Cryptology-ASIACRYPT 2003*, pages 452–473. Springer, 2003.
2. D. F. Aranha and C. P. L. Gouvêa. RELIC is an Efficient LIbrary for Cryptography. `http://code.google.com/p/relic-toolkit/`.
3. M. Bellare, A. Desai, D. Pointcheval, and P. Rogaway. Relations among Notions of Security for Public-Key Encryption Schemes. In *In Proceedings of CRYPTO'98, Lecture Notes in Computer Science, vol. 1462*, pages 26–45. Springer–Berlin–Heidelberg, 1998.
4. M. Bellare and P. Rogaway. The Security of Triple Encryption and a Framework for Code-Based Game-Playing Proofs. In *Advances in Cryptology - EUROCRYPT 2006, Lecture Notes in Computer Science vol. 4004*, pages 409–426. Springer Berlin Heidelberg, 2006.
5. D. Boneh and M. Franklin. Identity-Based Encryption from the Weil Pairing. *SIAM Journal on Computing*, 32(3):586–615, 2003.
6. X. Boyen. A Tapestry of Identity-Based Encryption: Practical Frameworks Compared. *International Journal of Applied Cryptography, vol.1, number 1*, pages 3–21, 2008.
7. X. Boyen and B. Waters. Anonymous Hierarchical Identity-Based Encryption (without Random Oracles). In *Advances in Cryptology-CRYPTO 2006*, pages 290–307. Springer, 2006.
8. S. Chatterjee and P. Sarkar. *Identity-Based Encryption*. Springer Science & Business Media, 2011.
9. Sherman SM Chow. Removing escrow from identity-based encryption. In *International Workshop on Public Key Cryptography*, pages 256–276. Springer, 2009.
10. Sherman SM Chow, Colin Boyd, and Juan Manuel González Nieto. Security-mediated certificateless cryptography. In *International Workshop on Public Key Cryptography*, pages 508–524. Springer, 2006.
11. C. Cocks. An Identity Based Encryption Scheme Based on Quadratic Residues. In *Cryptography and Coding*, pages 360–363. Springer, 2001.
12. D. Boneh and M. Franklin. Identity-Based Encryption from the Weil Pairing. In *SIAM Journal of Computing, vol. 32, issue 3*, pages 586–615. Society for Industrial and Applied Mathematics, 2003.
13. Y. Dodis and J. Katz. Chosen-Ciphertext Security of Multiple Encryption. In *In Proceedings of TCC 2005, Lecture Notes in Computer Science, vol. 3378*, pages 188–209. Springer–Berlin–Heidelberg, 2005.
14. S. Even and O. Goldreich. On the Power of Cascade Ciphers. Technical Report Tech. Rep. No. 275, Computer Science Dept., Technion, Haifa, Israel., May 1983.
15. S. Even and O. Goldreich. On the Power of Cascade Ciphers. In *In Proceedings of CRYPTO'83, Advances in Cryptology*, pages 43–50. Springer–Verlag US, 1984.
16. P. Gaži and U. Maurer. Cascade Encryption Revisited. In *Advances in Cryptology – Proceedings of ASIACRYPT 2009, Lecture Notes in Computer Science, vol. 5912*, pages 37–51. Springer–Verlag–Berlin–Heidelberg, 2009.
17. C. Gentry and A. Silverberg. Hierarchical ID-Based Cryptography. In *Proceedings of the 8th International Conference on the Theory and Application of Cryptology and Information Security: Advances in Cryptology*, ASIACRYPT '02, pages 548–566. Springer-Verlag, 2002.
18. G. Greenwald. XKeyscore: NSA tool collects 'nearly everything a user does on the internet'. http://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data, July 31, 2013 Accessed 2 June, 2015.

19. G. Greenwald and E. MacAskill. NSA Prism program taps in to user data of Apple, Google and others. http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data, June 7, 2013. Accessed 2 June, 2015.
20. J. Horwitz and B. Lynn. Toward Hierarchical Identity-Based Encryption. In *Advances in Cryptology—EUROCRYPT 2002*, pages 466–481. Springer, 2002.
21. W. Hurd and T.W. Lieu. Congressman Lieu Letter to FBI Director Comey on Encryption "Backdoor" Proposal. https://lieu.house.gov/media-center/, June 1, 2015 Accessed 2 June, 2015.
22. IACR. IACR Statement On Mass Surveillance: Copenhagen Resolution. http://www.iacr.org/misc/statement-May2014.html, May 14, 2014. Accessed 2 June, 2015.
23. A. Joux. Introduction to Identity-Based Cryptography. *Identity- Based Cryptography*, 2009.
24. M. Joye and G. Neven. *Identity-Based Cryptography*, volume 2. IOS press, 2009.
25. A. Kate and I. Goldberg. Distributed private-key generators for identity-based cryptography. In *Security and Cryptography for Networks*, volume 6280 of *Lecture Notes in Computer Science*, pages 436–453. Springer Berlin Heidelberg, 2010.
26. J. Katz and Y. Lindell. *Introduction to Modern Cryptography*. CRC Press, 2014.
27. N. Leavitt. Internet Security under Attack: The Undermining of Digital Certificates. *Computer*, 44(12):17–20, Dec 2011.
28. Ben Lynn. Pbc library manual 0.5. 11, 2006.
29. W. Mao. *Modern Cryptography: Theory and Practice*. Prentice Hall PTR, 2004.
30. M. Maurer and J. Massey. Cascade Ciphers: The Importance of Being First. In *Journal of Cryptology, vol. 6, Issue 1*, pages 55–61. Springer–Verlag, 1993.
31. Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system. *Consulted*, 1(2012):28, 2008.
32. National Institute of Standards and Technology. http://www.nist.gov/, Accessed 2 June, 2015.
33. K. G. Paterson and S. Srinivasan. Security and Anonymity of Identity-Based Encryption with Multiple Trusted Authorities. In *In Proceedings of Pairing-Based Cryptography–Pairing 2008, Lecture Notes in Computer Science, vol. 5209*, pages 354–375. Springer–Berlin–Heidelberg, 2008.
34. V. Popov, I. Kurepkin, and S. Leontiev. RFC 4357: Additional Cryptographic Algorithms for Use with GOST 28147-89, GOST R 34.10-94, GOST R 34.10-2001, and GOST R 34.11-94 Algorithms, January 2006.
35. R. Sakai, K. Ohgishi, and M Kasahara. Cryptosystems Based on Pairing. In *The 2000 Symposium on Cryptography and Information Security, Okinawa, Japan*, pages 135–148, 2000.
36. M. Scott. MIRACL – Multiprecision Integer and Rational Arithmetic C/C++ Library, 2007.
37. A. Shamir. Identity-Based Cryptosystems and Signature Schemes. In *Advances in cryptology*, pages 47–53. Springer, 1985.
38. William Stein and David Joyner. Sage: System for algebra and geometry experimentation. *Communications in Computer Algebra (SIGSAM Bulletin)(July 2005), http://sage. sourceforge. net*, 2005.
39. S. Tessaro. Security Amplification for the Cascade of Arbitrarily Weak PRPs: Tight Bounds via the Interactive Hardcore Lemma. In *In Proceedings of Theory of Cryptography TCC 2011, Lecture Notes in Computer Science vol. 6597*, pages 37–54. Springer Berlin Heidelberg, 2011.

40. The PARI Group, Bordeaux. *PARI/GP version* `2.7.0`, 2014. available from `http://pari.math.u-bordeaux.fr/`.
41. A. Whitten and J.D. Tygar. Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0. In *Usenix Security*, volume 1999, 1999.
42. D. Yao, N. Fazio, Y. Dodis, and A. Lysyanskaya. ID-Based Encryption for Complex Hierarchies with Applications to forward Security and Broadcast Encryption. In *Proceedings of the 11th ACM conference on Computer and communications security*, pages 354–363. ACM, 2004.
43. Tsz Hon Yuen, Willy Susilo, and Yi Mu. How to construct identity-based signatures without the key escrow problem. *International Journal of Information Security*, 9(4):297–311, 2010.

A Scheme Comparison

Topic	H-IBE	D-IBE	CARIBE	CARIBE-S
Key management authority	n PKGs, hierarchy	n PKGs, t-threshold	n PKGs	n PKGs
Key Escrow	Yes	Limited to $t+1$ collusions	Limited n collusions	No
Certificates	No	No	No	No
Ciphertext Expansion	Yes	Yes	Yes	Yes
Management authority has access to private keys	Yes for all PKGs	Under $t+1 \leq n$ collusions	Under n collusions	No
Compromise of management authority is fatal	Yes for any PKG in hierarchy	Under $t+1 \leq n$ collusions	Under n collusions	No
Incorporation of various encryption methods across PKGs possible	No	No	Yes	Yes

Table 3: Comparison of properties among composition IBE schemes including CARIBE and CARIBE-S.