VIBE, an Authenticated IBE solution Analysis

Olivier Blazy *

1 Introduction and State of the Art

Since its apparition four decades ago, public key cryptography has evolved considerably and today everyone is likely to be either a direct user or at least affected by its use. In such a context, with cryptographic solutions being deployed everywhere, key management has become the base of every deployed cryptographic solutions. While developing theoretical schemes, cryptographers usually dismissed the drawbacks of key management, as public keys are assumed to be available all the time, easily stored at no cost, without any kind of corruptions. However, in practice those assumptions are often violated and a large body of research is concerned with this proper key management, both theoretically and for practical purposes.

The cryptography literature usually pays close to no attention to the fact that in practice proper key management is quite difficult to set up and that it is really resource-consuming both in terms of space and time. Moreover, since the standard approach assumes that keys are never corrupted, and always available, it is interesting to see what happens and what problems arise with improper key management (either by partial corruption and/or unavailability) and how identity-based cryptography helps alleviate those issues.

Quite often in practice, the public keys used in cryptographic protocols are stored in a central database certified by a master authority. When this is done, the security of the scheme depends in a crucial way on the trust in this certification authority. Recent events have shown that certification authorities may not always be trusted, not necessarily because they misbehave on purpose but by weaknesses in their certification process. There exists some techniques to control the authorities behavior. Unfortunately, these are often still not efficient enough for real-world use, and many real-world protocols rely on "ad-hoc" constructions. It is therefore interesting to propose more efficient secure constructions, to analyse the security of existing ones and of specific cryptographic constructions that use a central authority for identity management.

*Olivier Blazy is an Associate Professor at the University of Limoges in France. He did his Ph.D. in 2012. Since then, he leads the master level security program in Limoges, and has a french national grant on identity-based cryptography.

The VIBE solution is inscribed in the trend of so-called Identity-based Cryptography introduced by Adi Shamir in 1984 [Sha84]. The approach adopted will be both theoretical and practical, since we will provide security results in mathematical frameworks (information theoretic or computational) with the aim to design protocols among the most efficient known. The project will notably involve discrete mathematical structures to model information security problems and mathematical analysis of cryptographic constructions, and development and instantiation of usable solutions.

2 Context, Position and Objectives of the proposal

Modern cryptography has seen the proposal of many suitable algorithmic problems and the design of many cryptographic schemes, together with more or less heuristic proofs of their respective security relative to the intractability of the underlying problems (potentially ad-hoc). Many schemes that were originally thought as secure have since been successfully cryptanalysed, which clearly indicates the need of mathematical security assurance. Nowadays, public-key cryptographic primitives or protocols without a rigorous proof cannot be regarded as secure in practice, and are quickly dismissed. A significant line of research has tried to provide proofs in the framework of complexity theory (a.k.a. "reductionist" security proofs): the proofs provide reductions from an attack against a cryptographic protocol to a well-studied number-theoretic problem. Since there is no absolute proof of security, it is also essential to study cryptanalysis and to analyse the underlying mathematical problems.

Identity Based Encryption (IBE), introduced by Shamir in 1984 [Sha84], provides a way to allow a sender to encrypt a message with the receiver's identity as a public key. A practical example of such identity would be an e-mail address, it is easily memorable by a human, and with very few exceptions, there is no entropy that could be used to pre-embed in a cryptographic secret. The decryption is done by a key tied to the user identity id usually called $\mathsf{usk}[\mathsf{id}]$, this key is generated by a trusted authority thanks to a master key msk.

First proposals for such an IBE were given in 2001 by Boneh and Franklin [BF01] and Cocks [Coc01]. The first one is based on Weil pairings and the second one relies on the quadratic residuosity problem. These elegant schemes felt into the random oracle model. Academic proposals have followed since then, four years later, Waters proposed the first adaptively secure construction in the standard model [Wat05], where adaptive security means that an adversary may select the challenge identity id^* after seeing the public key and arbitrarily many user secret keys for identities of his choice. The quality of security reduction to the underlying hard problem was then considered as, beside the theoretical interest, the security loss makes the construction less efficient. Chen and Wee [CW13] proposed the first IBE scheme with tight security in the standard model.

However while those solutions answer theoretical questions, they fail to find a widespread application in real life scenarios.

2.1 Context, Social issues

For the last decade, the unceasing evolution of information technology has offered users access to powerful online services. Pay-TV, mobile phone, Internet, credit cards are well-known examples of such facilities millions of people use every day all over the world. We all want to make the most of these new powerful technologies, but we have a requirement: having some guarantee about the security of these systems. We all share this fear of making sensitive information accessible to potential attackers, but the issues of intrusion scenarios are, of course, very different depending on which class of users one belongs to : regular users, enterprises, or state agencies. For a regular user who, for instance, buys some items on the Internet using his personal credit card, the concern is to use a system for which he knows that his personal data will stay protected against potential intrusions and in particular be sure he is interacting with the correct interlocutor. From the enterprise point of view, the damages caused by a failure in a security system could have larger-scale consequences. Indeed, in the context of industrial spying, any sensitive information that ends up in the hand of an industrial adversary could lead to an economic disaster. For state agencies, the level of security required to decide that a system is sufficiently trustworthy is very high. Indeed, such agencies deal every day with sensitive information related to the defense of the nation and thus such data should strongly be kept secure against potential threats coming from foreign countries. If such a scenario happened, it could have severe implications in political, financial, and even military operations (e.g. the Wikileaks US diplomatic cables leak). In the context of protecting individual digital information, it becomes essential to study the robustness of existing systems by analysing their resistance to potential threats, and reducing the attack surface by lowering the trust required in every person involved in each protocol.

2.2 The VIBE Proposal

The solution of VIBE arises in the context of Identity-Based Encryption. The contribution is two-fold.

- First, the point of on identity-based encryption is to alleviate the complicated key management. In a context with several n users (Internet of Things), a classical public key solution would require $O(n^2)$ interactions. Here, the fact that VIBE is an IBE allows to remove those complicated operations.
- Then, contrarily to most IBE solution, VIBE propose verifiability that allows the receiver to check who is the person that sent the message. The solution proposed to send an extra authenticating information with the ciphertext, this is done in such a way that nobody can know which of the sender or the receiver has generated the ciphertext. This is concept that appears in designated verifier signature [JSI96], and that was sketched in authenticated identity-based encryptions [Lyn02]. Such approach allows the recipient to be sure of who wrote him (as he knows, he did not generate the message), while not being able to prove to someone else who did: an outsider is not able (even having access

to the recipient secret keys) to know whether a ciphertext was sent by Alice to Bob, or if Bob crafted it pretending it was generated by Alice, this allows deniability.

This combination makes vibe an elegant design to provide both encryption and authentication in modern context, especially IoT environments, without superfluous additional communications / computations.

As is, the identity is an abstract concept, allowing to dissociate the cryptographic component from the object. The trusted center, as in every IBE, does not have to protect several items besides his master secret key, registering a new object can be done on the fly, without further communication to other registered items.

The solution proposed rely on a classical cryptographical assumption close to the bilinear computational Diffie Hellman problem, but in an asymmetric setting. Most of the time, this type of curves lead to faster instantiation with more compact objects.

3 References

[ACHdM05] Giuseppe Ateniese, Jan Camenisch, Susan Hohenberger, and Breno de Medeiros. Practical group signatures without random oracles. Cryptology ePrint Archive, Report 2005/385, 2005. `http://eprint.iacr.org/2005/385`.

[BBS04] Dan Boneh, Xavier Boyen, and Hovav Shacham. Short group signatures. In Matthew Franklin, editor, *Advances in Cryptology – CRYPTO 2004*, volume 3152 of *Lecture Notes in Computer Science*, pages 41–55, Santa Barbara, CA, USA, August 15–19, 2004. Springer, Heidelberg, Germany.

[BF01] Dan Boneh and Matthew K. Franklin. Identity-based encryption from the Weil pairing. In Joe Kilian, editor, *Advances in Cryptology – CRYPTO 2001*, volume 2139 of *Lecture Notes in Computer Science*, pages 213–229, Santa Barbara, CA, USA, August 19–23, 2001. Springer, Heidelberg, Germany.

[BFPV11] Olivier Blazy, Georg Fuchsbauer, David Pointcheval, and Damien Vergnaud. Signatures on randomizable ciphertexts. In Dario Catalano, Nelly Fazio, Rosario Gennaro, and Antonio Nicolosi, editors, *PKC 2011: 14th International Conference on Theory and Practice of Public Key Cryptography*, volume 6571 of *Lecture Notes in Computer Science*, pages 403–422, Taormina, Italy, March 6–9, 2011. Springer, Heidelberg, Germany.

[Bon98] Dan Boneh. The decision Diffie-Hellman problem. In *Third Algorithmic Number Theory Symposium (ANTS)*, volume 1423 of *Lecture Notes in Computer Science*. Springer, Heidelberg, Germany, 1998. Invited paper.

[Coc01] Clifford Cocks. An identity based encryption scheme based on quadratic residues. In Bahram Honary, editor, *8th IMA International Conference on Cryptography and Coding*, volume 2260 of *Lecture Notes in Computer Science*, pages 360–363, Cirencester, UK, December 17–19, 2001. Springer, Heidelberg, Germany.

[CW13] Jie Chen and Hoeteck Wee. Fully, (almost) tightly secure IBE and dual system groups. In Ran Canetti and Juan A. Garay, editors, *Advances in Cryptology – CRYPTO 2013, Part II*, volume 8043 of *Lecture Notes in Computer Science*, pages 435–460, Santa Barbara, CA, USA, August 18–22, 2013. Springer, Heidelberg, Germany.

[DH76] Whitfield Diffie and Martin E. Hellman. New directions in cryptography. *IEEE Transactions on Information Theory*, 22(6):644–654, 1976.

[GPS08] Steven D. Galbraith, Kenneth G. Paterson, and Nigel P. Smart. Pairings for cryptographers. *Discrete Applied Mathematics*, 156(16):3113 – 3121, 2008.

[JSI96] Markus Jakobsson, Kazue Sako, and Russell Impagliazzo. Designated verifier proofs and their applications. In Ueli M. Maurer, editor, *Advances in Cryptology – EUROCRYPT'96*, volume 1070 of *Lecture Notes in Computer Science*, pages 143–154, Saragossa, Spain, May 12–16, 1996. Springer, Heidelberg, Germany.

[Lyn02] Ben Lynn. Authenticated identity-based encryption. Cryptology ePrint Archive, Report 2002/072, 2002. `https://eprint.iacr.org/2002/072`.

[Sha84] Adi Shamir. Identity-based cryptosystems and signature schemes. In G. R. Blakley and David Chaum, editors, *Advances in Cryptology – CRYPTO'84*, volume 196 of *Lecture Notes in Computer Science*, pages 47–53, Santa Barbara, CA, USA, August 19–23, 1984. Springer, Heidelberg, Germany.

[Wat05] Brent R. Waters. Efficient identity-based encryption without random oracles. In Ronald Cramer, editor, *Advances in Cryptology – EUROCRYPT 2005*, volume 3494 of *Lecture Notes in Computer Science*, pages 114–127, Aarhus, Denmark, May 22–26, 2005. Springer, Heidelberg, Germany.

A Security Definition

A.1 Generalities

Hard problem A function $f : \mathbb{N} \to \mathcal{R}$ is said to be negligible, if $\forall c \in \mathbb{N}, \exists k_0 \in \mathbb{N}, \forall k \geq k_0 : |f(k)| < k^{-c}$. A problem is said to be hard, if there exists no polynomial time algorithm solving it with non-negligible probability.

Cyclic Group A cyclic group is a tuple $(p, \mathbb{G}, g)$ where $\mathbb{G}$ is a group entirely generated by g where $g^p = 1_{\mathbb{G}}$. (The neutral element of $\mathbb{G}$)

Bilinear Groups A bilinear group is a tuple $(p, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, e, g_1, g_2)$ where $\mathbb{G}_1, \mathbb{G}_2$ et $\mathbb{G}_T$ are cyclic groups of prime order p, generated respectively by g_1,g_2 and $e(g_1, g_2)$, $e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$ is a non-degenerated bilinear form, *i.e.*:

$$\forall X \in \mathbb{G}_1, \forall Y \in \mathbb{G}_2, \forall \lambda, \mu \in \mathbb{Z}_p : e(X^\lambda, Y^\mu) = e(X, Y)^{\lambda\mu}$$

and $e(g_1, g_2)$ does indeed generate the prime order group $\mathbb{G}_T$. In the following we will suppose there exists a polynomial time algorithm GrpGen which takes $1^{\mathfrak{K}}$ as input, and which outputs such bilinear groups. In this case p is a prime order of $\mathfrak{K}$ bits.

Such groups are commonly instantiated on elliptic curves on which such pairings can be defined as bilinear forms. Galbraith *et al.* [GPS08] have split such instantiations in three main types:

- Type I, where $\mathbb{G}_1 = \mathbb{G}_2$, and $g_1 = g_2$, those groups are said to be symmetric and can be simplified in $(p, \mathbb{G}, \mathbb{G}_T, e, g)$. This first case often leads to problems based on the DLin hypothesis,
- Type II, if there exists a computationally efficient homomorphism from $\mathbb{G}_2$ in $\mathbb{G}_1$, but none from $\mathbb{G}_1$ to $\mathbb{G}_2$. This case often leads to problems based on the XDH hypothesis,
- Type III, if such efficient homomorphism does not exist in either way. This last case often leads to problems based on the SXDH hypothesis.

In the following, we will focus on Type III curves.

A.2 Security Hypotheses

Decisional Diffie Hellman (DDH [Bon98]) The Decisional Diffie-Hellman hypothesis states that in a multiplicative group $(p, \mathbb{G}, g)$, given (g^μ, g^ν, g^ψ) for unknown $\mu, \nu \xleftarrow{\$} \mathbb{Z}_p$, it is hard to decide whether $\psi = \mu\nu$.

External Diffie Hellman in $\mathbb{G}_1$ (XDH [BBS04]) This variant of the previous hypothesis states that in a type II bilinear group, given $(g_1^\mu, g_1^\nu, g_1^\psi)$ for unknown $\mu, \nu \xleftarrow{\$} \mathbb{Z}_p$, it is hard to decide whether $\psi = \mu\nu$. (In other words DDH is hard in $\mathbb{G}_1$.) A variant can say that DDH is hard in $\mathbb{G}_2$.

Symmetric External Diffie Hellman (SXDH [ACHdM05]) This last variant, used mostly in type III bilinear groups, states that DDH is hard in both $\mathbb{G}_1$ and $\mathbb{G}_2$.

We also describe two computational hypotheses related to the DDH:

Computational Diffie Hellman (CDH [DH76]) The Computational Diffie-Hellman hypothesis states that in a multiplicative group $(p, \mathbb{G}, g)$, given (g^μ, g^ν) for unknown $\mu, \nu \xleftarrow{\$} \mathbb{Z}_p$, it is hard compute $g^{\mu\nu}$.

Advanced Computational Diffie-Hellman problem (CDH^+ [BFPV11]): Let us be given two (multiplicative) groups $(\mathbb{G}_1, \mathbb{G}_2)$ of prime order p with (g_1, g_2) as respective generators. The CDH^+ assumption states that given $(g_1, g_2, g_1^{\mu}, g_2^{\mu}, g_1^{\nu})$, for random $\mu, \nu \in \mathbb{Z}_p$, it is hard to compute $g_1^{\mu\nu}$.

New Assumptions:

Trilinear eXternal Diffie Hellman Assumption (TXDH) Let us be given two (multiplicative) groups $(\mathbb{G}_1, \mathbb{G}_2)$ of prime order p with (g_1, g_2) as respective generators. The TXDH assumption states that given $g_1, g_2, g_1^a, g_2^a, g_1^b, g_2^c$, for random $a, b, c \in \mathbb{Z}_p$, it is hard to distinguish $e(g_1, g_2)^{abc}$ from $e(g_1, g_2)^d$ with d random in $\mathbb{Z}_p$

Trilinear Computational Diffie Hellman Assumption (TCDH) Let us be given two (multiplicative) groups $(\mathbb{G}_1, \mathbb{G}_2)$ of prime order p with (g_1, g_2) as respective generators. The TCDH assumption states that given $g_1, g_2, g_1^a, g_2^a, g_1^b, g_2^c$, for random $a, b, c \in \mathbb{Z}_p$, it is hard to compute $e(g_1, g_2)^{abc}$.

Those assumptions are slightly easier that the classical SXDH assumptions, but harder than the CDH^+ one.

A.3 Security Experiments

We now recall syntax and security of IBE in terms of an Authenticated ID-based encryption.

Authenticated Identity-based Encryption An Authenticated identity-based encryption scheme consists of four PPT algorithms $\mathsf{IBE} = (\mathsf{Gen}, \mathsf{USKGen}, \mathsf{Enc}, \mathsf{Dec})$ with the following properties.

- The probabilistic key generation algorithm $\mathsf{Gen}(\mathfrak{K})$ returns the (master) public/secret key $(\mathsf{mpk}, \mathsf{msk})$. We assume that mpk implicitly defines a message space $\mathcal{M}$, an identity space ID, a key space $\mathcal{K}$, and ciphertext space CS.
- The probabilistic user secret key generation algorithm $\mathsf{USKGen}(\mathsf{msk}, \mathsf{id})$ returns the user secret-key $\mathsf{usk}[\mathsf{id}]$ for identity $\mathsf{id} \in \mathsf{ID}$.
- The probabilistic encapsulation algorithm $\mathsf{Enc}(\mathsf{mpk}, M, \mathsf{id}_R, \mathsf{usk}[\mathsf{id}_S])$ returns the ciphertext $\mathsf{C} = (C, A)$ of a message M for the user id_R authenticated with respect to the user id_S.
- The deterministic decapsulation algorithm $\mathsf{Dec}(\mathsf{usk}[\mathsf{id}_R], \mathsf{id}_S, \mathsf{C})$ returns the plaintext M associated with C if the authentication holds or the reject symbol $\perp$.

For perfect correctness we require that for all $\mathfrak{K} \in \mathbb{N}$, all pairs $(\mathsf{mpk}, \mathsf{msk})$ honestly generated by $\mathsf{Gen}(\mathfrak{K})$, all identities $\mathsf{id}_R, \mathsf{id}_S \in \mathsf{ID}$, all $\mathsf{usk}[\mathsf{id}_R], \mathsf{usk}[\mathsf{id}_S]$ generated by $\mathsf{USKGen}(\mathsf{msk}, \mathsf{id})$, all messages $M \in \mathcal{M}$ and all C output by $\mathsf{Enc}(\mathsf{mpk}, M, \mathsf{id}_R, \mathsf{usk}[\mathsf{id}_S])$:

$$\Pr[\mathsf{Dec}(\mathsf{usk}[\mathsf{id}_R], \mathsf{id}_S, \mathsf{C} = M) = \mathsf{sk}] = 1.$$

Procedure Initialize:
$(\mathsf{mpk}, \mathsf{msk}) \xleftarrow{\$} \mathsf{Gen}(\mathfrak{K})$
Return mpk

Procedure USKGenO(id):
$\mathcal{Q}_{\mathsf{ID}} = \mathcal{Q}_{\mathsf{ID}} \cup \{\mathsf{id}\}$
Return $\mathsf{usk}[\mathsf{id}] \xleftarrow{\$} \mathsf{USKGen}(\mathsf{msk}, \mathsf{id})$

Procedure $\mathsf{Enc}(\mathsf{mpk}, M, \mathsf{id}^*_R, \mathsf{id}_S)$: | 1 query
$(\mathsf{sk}^*, \mathsf{C}^*) \xleftarrow{\$} \mathsf{Enc}(\mathsf{mpk}, M, \mathsf{id}^*_R, \mathsf{usk}[\mathsf{id}_S])$
$\boxed{\mathsf{sk}^* \xleftarrow{\$} \mathcal{K}; \mathsf{C}^* = (C^* \xleftarrow{\$} \mathsf{CS}, \mathsf{Sign}(\mathsf{usk}[\mathsf{id}_S], C^*))}$
Return $(\mathsf{sk}^*, \mathsf{C}^*))$

Procedure $\mathsf{Finalize}(\beta)$:
Return $(\mathsf{id}^*_R \notin \mathcal{Q}_{\mathsf{ID}}) \wedge \beta$

Figure 1: Security Games $\mathsf{PR\text{-}ID\text{-}CPA}_{\mathsf{real}}$ and $\boxed{\mathsf{PR\text{-}ID\text{-}CPA}_{\mathsf{rand}}}$ for defining PR-ID-CPA-security.

The main security requirements we consider here are indistinguishability and anonymity against chosen plaintext and identity attacks (IND-ID-CPA and ANON-ID-CPA). Instead of defining both security notions separately, we define pseudorandom ciphertexts against chosen plaintext and identity attacks (PR-ID-CPA) which means that challenge key and ciphertext are both pseudorandom. Note that PR-ID-CPA trivially implies IND-ID-CPA and ANON-ID-CPA. We define PR-ID-CPA-security of IBKEM formally via the games given in Figure 1. In addition, we are also going to consider unforgeability in Figure 2.

PR-ID-CPA **Security** An identity-based encryption is PR-ID-CPA-secure if for all PPT $\mathcal{A}$, $\mathsf{Adv}^{\mathsf{pr\text{-}id\text{-}cpa}}_{\mathsf{IBE}}(\mathcal{A}) := |\Pr[\mathsf{PR\text{-}ID\text{-}CPA}^{\mathcal{A}}_{\mathsf{real}} \Rightarrow 1] - \Pr[\mathsf{PR\text{-}ID\text{-}CPA}^{\mathcal{A}}_{\mathsf{rand}} \Rightarrow 1]|$ is negligible.

Unforgeability. This experiment encompasses the proper authentication of the ciphertext. The adversary has to generate a new valid ciphertext by an uncorrupted user, even after having seen several valid ones.

Procedure Initialize:
$(\mathsf{mpk}, \mathsf{msk}) \xleftarrow{\$} \mathsf{Gen}(\mathfrak{K})$
Return mpk

Procedure USKGenO(id):
$\mathcal{Q}_{\mathsf{ID}} = \mathcal{Q}_{\mathsf{ID}} \cup \{\mathsf{id}\}$
Return $\mathsf{usk}[\mathsf{id}] \xleftarrow{\$} \mathsf{USKGen}(\mathsf{msk}, \mathsf{id})$

Procedure $\mathsf{Enc}(\mathsf{mpk}, M, \mathsf{id}_R, \mathsf{id}^*_S)$:
$\mathcal{SM} = \mathcal{SM} \cup \{\mathsf{id}_R, M\} \cup \{\mathsf{id}^*_S, M\}$
$(\mathsf{sk}^*, \mathsf{C}^*) \xleftarrow{\$} \mathsf{Enc}(\mathsf{mpk}, M, \mathsf{id}_R, \mathsf{usk}[\mathsf{id}^*_S])$ Return $(\mathsf{sk}^*, \mathsf{C}^*)$

Procedure $\mathsf{Finalize}(\mathsf{C}^*, M^*, \mathsf{id}^*_R, \mathsf{id}^*_S)$:
Return $(\mathsf{id}_{S^*} \notin \mathcal{Q}_{\mathsf{ID}}) \wedge ((\mathsf{id}^*, M^*) \notin \mathcal{M}_{\mathsf{ID}}) \wedge M^* = \mathsf{Dec}(\mathsf{mpk}, \mathsf{C}^*, \mathsf{usk}[\mathsf{id}^*_R], \mathsf{id}^*_S)$

Figure 2: Security Games defining unforgeability.

UF-ID-CPA **Security** An identity-based encryption is UF-ID-CPA-secure if for all PPT $\mathcal{A}$, $\mathsf{Adv}^{\mathsf{pr\text{-}id\text{-}cpa}}_{\mathsf{IBE}}(\mathcal{A})$ is negligible.

B VIBE Proposal, and Security Analysis

VIBE

- $\underline{\mathsf{Setup}(\mathfrak{K})}$
  $\mathsf{crs} = (p, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, e, g_1, g_2) \xleftarrow{\$} \mathsf{ggen}_s$
  Choose $\mathcal{H}_i$ two hash functions from $\{0,1\}^*$ to $\mathbb{G}_i$
  Choose $\mathcal{H}_3$ a hash function from $\{0,1\}^*$ to $\mathbb{Z}_p^*$
  Choose $\mathcal{H}'$ a hash function from $\mathbb{G}_T$ to $\{0,1\}^*$
  Return $\mathsf{param} = (\mathsf{crs}, \mathcal{H}_1, \mathcal{H}_2, \mathcal{H}_3, \mathcal{H}_4)$

- $\underline{\mathsf{Gen}(\mathsf{param})}$
  $s \xleftarrow{\$} \mathbb{Z}_p^*, h_1 \leftarrow s \cdot \mathcal{H}_1(\mathsf{id}_{\mathsf{TC}})$
  Return $(\mathsf{mpk} = h_1, \mathsf{msk} = s)$

- $\underline{\mathsf{USKGen}(\mathsf{msk}, \mathsf{id})}$
  Return $\mathsf{usk}[\mathsf{id}] = (s^{-1} \cdot \mathcal{H}_1(\mathsf{id}), s^{-1} \cdot \mathcal{H}_2(\mathsf{id}))$

- $\underline{\mathsf{Verify}_{\mathsf{param}}(\mathsf{mpk}, \mathsf{usk}[\mathsf{id}])}$
  Return $e(h_1, \mathsf{usk}[\mathsf{id}]_2) == e(\mathcal{H}_1(\mathsf{id}_{\mathsf{TC}}), \mathcal{H}_2(\mathsf{id}))$

- $\underline{\mathsf{Enc}(\mathsf{mpk}, \mathsf{id}_R, \mathsf{id}_S, M)}$
  $r \leftarrow \mathcal{H}_3(M)$
  Compute $U = M \oplus \mathcal{H}'(e(\mathcal{H}_1(\mathsf{id}_{\mathsf{TC}}), \mathcal{H}_2(\mathsf{id}_R))^r)$
  And $Y = \mathcal{H}'(e(\mathcal{H}_1(\mathsf{id}_R), \mathsf{usk}[\mathsf{id}_S]_2)^r)$
  $V = r \cdot h_1$
  Return $\mathcal{C} = (U, V, Y)$

- $\underline{\mathsf{Dec}(\mathsf{mpk}, \mathsf{usk}[\mathsf{id}_R], \mathsf{id}_S, \mathcal{C})}$
  Parse $\mathcal{C}$ as (U, V, Y)
  $M = U \oplus \mathcal{H}'(e(V, \mathsf{usk}[\mathsf{id}_R]_2))$, $r \leftarrow \mathcal{H}_3(M)$
  Authenticated if and only if $Y == \mathcal{H}'(e(\mathsf{usk}[\mathsf{id}_R]_1, \mathcal{H}_2(\mathsf{id}_S))^r)$
  Return M

Figure 3: Write-up of the VIBE solution.

B.1 Presudo-Randomness (Enhanced Indistinguishability)

It should be noted that VIBE proposal uses a deterministic randomness generation for the encapsulation ($r \leftarrow \mathcal{H}_3(M)$) which do not allow IND-CPA. However due to

the use of the random oracle, one can achieve a similar security by considering a message space of high enough entropy.

In the remainder of this section, one will now consider that r is generated at random.

Theorem B.1 *Under the hardness of the* TXDH *assumption, the VIBE proposal achieves* PR-ID-CPA *in the Random Oracle Model.*

Proof We are going to proceed in a sequence of games. We are going to build a simulator $\mathcal{B}$ solving a decisional TXDH challenge. To do so, we start from the real game, and then we start by guessing the target identity id_R^*, and then we alter the values U, V in the challenge ciphertext so that it allows to solve an TXDH challenge.

We assume, the simulator receives a TXDH challenge of the form: $(g_1, g_2, a \cdot g_1, a \cdot g_2, b \cdot g_1, c \cdot g_2, d \cdot g_T)$.

- In game G_0, the simulator simply acts normally, especially he knows msk.
- In game G_0', the simulator simply acts normally, especially he knows msk, but tries to guess the challenge identity. It succeeds with probability $1/q$ where q is the number of identities queries to the system (in particular this is upper-bounded by the number of ROM queries). Hence $|\mathsf{Adv}(G_0') - \mathsf{Adv}(G_0)| \leq 1/q$
- In game G_1, the simulator forgets msk and sets $h_1 = g_1, \mathcal{H}_{1,2}(\mathsf{id}_{\mathsf{TC}}) = \beta_{1,2} \cdot a \cdot g_{1,2}$ and $\mathcal{H}_1(\mathsf{id}^*) = \gamma_1 \cdot g_1$ for $\beta, \gamma \xleftarrow{\$} \mathbb{Z}_p$ while $\mathcal{H}_2(\mathsf{id}^*) = c \cdot g_2$.
  - To answer key queries, the simulator picks $\alpha_{1,2} \in \mathbb{Z}_p^2$ and sets, $\mathsf{usk}[\mathsf{id}] = \alpha_1 \cdot g_1, \alpha_2 \cdot g_2$ (setting $\mathcal{H}_b(\mathsf{id}) = \alpha_b \cdot a \cdot g_b$).
  - For the challenge ciphertext, it sets $V = b \cdot g_1$, and sets
    - $Y = \mathcal{H}'(e(\mathcal{H}_1(\mathsf{id}^*), \mathsf{usk}[\mathsf{id}_S]_2)^r) = \mathcal{H}'(e(\gamma \cdot V, \mathsf{usk}[\mathsf{id}_S]_2))$
    - $U = M \oplus \mathcal{H}'(e(\mathcal{H}_1(\mathsf{id}_{\mathsf{TC}}), \mathcal{H}_2(\mathsf{id}^*))^r) = M \oplus \mathcal{H}'(d \cdot g_T)$

We hence have $|\mathsf{Adv}(G_1) - \mathsf{Adv}(G_0')| \leq \mathsf{Adv}(\mathsf{TXDH})$

If $d \cdot g_T = e(g_1, g_2)^{abc}$ this corresponds to the real game, otherwise this corresponds to the random one. Hence $\mathsf{Adv}_{\mathsf{IBE}}^{\mathsf{pr\text{-}id\text{-}cpa}}(\mathcal{A}) \leq 1/q + \mathsf{Adv}(\mathsf{TXDH})$ which leads to the conclusion. ∎

Remark This means, that assuming a high entropy in the message space, the scheme achieves both the classical notion of **indistinguishability** (hiding the message encrypted), and **anonymity** (hiding the expected recipient).

B.2 Unforgeability

We are now going to show that the scheme proposes proper ciphertext authentication.

Theorem B.2 *Under the hardness of the* TCDH *assumption, the VIBE proposal achieves* UF-ID-CPA *in the Random Oracle Model.*

Proof Once again, we are going to proceed in a sequence of games, by showing how to answer authentication queries without knowing neither the user key, nor the master key. The proof is similar to the previous one. It should be noted that, the adversary only sees the value $Y = \mathcal{H}'(D^r)$ and but not the preimage, hence generating a new value, is equivalent to generating the first one without any other signing queries. Hence, he has to find a way to compute $e(\mathcal{H}_1(\mathsf{id}_R), \mathsf{usk}[\mathsf{id}_S])$ without knowing neither user secret keys nor the master secret keys. Hence the computational Diffie Hellman. ∎

Remark Here the unforgeability argument is simplified by the deterministic randomness generation, in case of further applications where r is generated purely at random, one could add M as an extra argument to $\mathcal{H}'$ in Y to leverage the same security argument.

B.3 An Additional feature: Deniability

Authentication is a wonderful feature, to allow secure message transmission. However, in some context, one wants to prevent the receiver from proving the message comes from a given sender.

The VIBE protocol provides such feature. The *Authentication* part Y of the cipher can be generated equally using the randomness r and the sender private key as $\mathcal{H}'(e(\mathcal{H}_1(\mathsf{id}_R), \mathsf{uskid}_{S2}))$ or using the randomness r and the receiver private key $\mathcal{H}'(e(\mathsf{usk}[\mathsf{id}_R]_1, \mathcal{H}_2(\mathsf{id}_S)))$. (which is the process used in the verification).

As those two values are strictly equal, this means that the receiver is not able to prove to an outsider that the sender did indeed send a given message.

Such features normally appears in designated verifier signatures [JSI96], and is expected from authenticated Identity-Based Encryption [Lyn02], and here comes at no cost/security hypothesis.

Theorem B.3 *The VIBE protocol achieves sender deniability*

C Conclusion

There are several IBE protocols existing nowadays. VIBE manages to be one of the only one combining several security properties under classical cryptographic hypotheses. It provides both indistinguishability (or even pseudo-random indistinguishability which is strictly stronger), and deniable authentication (unforgeability+ deniability), all the while it manages to keep the ciphertexts very short, with few pairing computations.