Concurrently-Secure Credential Ownership Proofs [*]

Siamak F Shahandshti $^\diamond$ Reihaneh Safavi-Naini $^{\diamond\,\dagger}$ Joonsang Baek $^\triangle$

$^\diamond$ Centre for Information Security
School of IT and CS, University of Wollongong, Australia
http://www.uow.edu.au/∼sfs166 and http://www.uow.edu.au/∼rei

$^\triangle$ Institute for InfoComm Research (I^{2}R), Singapore
http://www1.i2r.a-star.edu.sg/∼jsbaek

September 2, 2008

Abstract. We address the case in credential systems where a credential owner wants to show her credential to a verifier without taking the risk that the ability to prove ownership of the same (and any other) credential is transferred to the verifier. We define *credential ownership proof* protocols for credentials signed by standard signature schemes. We also propose proper security definitions for the protocol, aiming to protect the security of both the credential issuer and the credential owner against concurrent attacks. We give two generic constructions of credential ownership proofs based on identity-based encryption and identity-based identification schemes. Furthermore, we show that signatures with credential ownership proofs are equivalent to identity-based identification schemes, in the sense that any secure construction of each implies a secure construction of the other. Finally, we show that the GQ identification protocol yields an efficient credential ownership proof for credentials signed by the RSA-FDH signature scheme of Bellare and Rogaway and prove the protocol concurrently-secure.

Keywords: Credential Systems, Signature Schemes, Designated-Verifier Signatures, Identification Schemes, Identity-Based Cryptography

1 Introduction

Consider the following scenario. A club wants to issue electronic tickets, entitling users to watch either a single game, multiple games, or all games in a season. In the latter two cases, although the same ticket can be used multiple times, the system must ensure that for each game the ticket is used only once.

A basic credential system based on digital signatures can closely satisfy these requirements. The electronic ticket will have a text m that states the entitlement of the user, and the signature σ of the club on m. When

[*] An abridged version of this paper appears in F. Bao and S. Miller (Eds.): Proceedings of the 2007 ACM Symposium on Information, Computer and Communications Security (ASIACCS'07), pp. 161–172, ACM, 2007. This is the full version.

[†] Now at *i*CORE Information Security Lab (*i*CIS), Department of Computer Science, University of Calgary, Canada, http://www.cpsc.ucalgary.ca/∼rei

the ticket is presented to a ticket controller, the signature of the club is verified, and if valid, the statement m will be honored. Tickets should not be linked to individuals' identities and users should have the flexibility to give their tickets to others as long as 'one user one ticket' per game is enforced. Not including user-specific information in tickets and allowing tickets to be circulated among users, implies that there is no direct link between the user and the ticket and so users' privacy will be protected.

The system looks very attractive: it appears *secure* assuming the signature system provides unforgeability; it is *efficient* and requires one signature generation and verification for ticket generation and checking, respectively; and uses *standard cryptography*, so is easy to implement.

This basic system, however, is completely insecure against *ticket cloning*. The ticket can be illegally copied (cloned) by (i) legitimate ticket holders (who have legally purchased the ticket), and (ii) ticket controllers during ticket verification phase. Protection against the former can be easily enforced by adding a checking stage for the serial number of the presented tickets against a log of the serial numbers of already-shown tickets and so effectively prevent 'double spending' of the ticket. However, the system is still vulnerable to copying by a (real or fake) ticket controller. A malicious controller will make a copy of the ticket during a showing by an honest user, and then successfully use it for future games, simply by making sure that he is the first to present the ticket to the system. This way, the user will effectively lose the privilege that the ticket needs to guarantee.

An immediate solution would be to require ticket holders to prove ownership of the ticket without directly showing it to the controller. A user can show her claimed privilege m and then prove in *zero knowledge (ZK)* [GMR89] that she knows the club's signature on the message. That is, she can use a ZK protocol for *proof of knowledge (PoK)* [BG92] of a signature on the claimed message, i.e. a ZK-PoK of a member of the NP language $L_{(pk,m)} = \{\sigma : \mathsf{Verify}(pk, m, \sigma)\}$. The zero-knowledge property, however, although guaranteeing that no information other than the validity of the signature is revealed to the controller, is computationally expensive and requires many rounds of communication. Therefore, the question is: "Is there a more efficient way of implementing a credential system with the above requirements?"

In this paper we give a positive answer to the above question by proposing an extension to signature schemes which we call *Credential Ownership Proof (COP)*, that captures the required security property. We also give generic and concrete constructions for COP protocols with provable security.

A COP for a signature scheme is an interactive protocol attached to the scheme, that allows a credential holder to prove interactively the ownership of a claimed credential to a verifier. A secure COP must ensure security of credential holders and credential issuer, both. That is, prover's interaction with multiple verifiers should not allow mis-use of the system by enabling successful run of the protocol without having the required credentials. We show that COPs can be much more efficient than zero-knowledge proofs (see Table 3). In particular, the COP for RSA-based credentials that we construct, is based on the GQ protocol [GQ88], which is known to be only *honest verifier zero knowledge* [GQ88]. This makes COPs and their secure construction of immediate practical importance. We note the following remarks with respect to users' privacy in the above credential system:

- In the above credential system, showings of a ticket are linkable through the value of m, which, as mentioned before, must be unique to prevent double spending. However users cannot be traced as the tickets can be purchased by any user. Such linkability property enables conducting (anonymous) statistical analyses on the behavior of users.
- The system allows users to make 'clones' of their tickets and share them with their trusted friends. The 'double spending' protection of the ticket controlling system ensures that for each game only a single user will actually use the ticket. The users, however, have higher flexibility with the tickets and are able to share their tickets, which is a very attractive property.

1.1 Related Work

Credential systems and their vast range of security properties in different applications have been intensively studied in recent years. The closest work to ours is *Universal Designated Verifier Signature Proofs (UDVSP)* introduced by Baek et al. [BSS05]. A UDVSP is similar to a COP as it enables a signature holder to prove the ownership of a signature to a verifier, however, the security properties of the two are very different. In UDVSP the goal is to remove a restriction of *Universal Designated Verifier Signature (UDVS)* proposed by Steinfeld et al. [SBWP03] and the security model is mainly geared to ensure security of a single credential holder and with no concern about security of the credential issuer. In particular, in their security model, there is no security guarantee against an adversary who corrupts a number of credential holders and gets to know their credentials (e.g. ticket controller who collects many copies of tickets) or possibly can obtain tickets of his choice by directly asking the credential issuer. Baek et al's definition of security is one-sided and resembles security definition of an identification protocol. It focuses on the security of a single credential holder (corresponding to the owner of the secret in identification protocols), but not the issuing authority, and does not address a system of different credential holders. In Section 3.1, we further elaborate on these definitions and show that our security requirements captures all the requirements of the above scenario.

In the following we outline other most relevant systems in relation to our work.

Anonymous Credentials. Anonymous credential systems (a.k.a. *pseudonym systems*) ensure privacy of users in securely accessing services of organizations. Organizations issue credentials on users' pseudonyms, and hence the name 'pseudonym systems'. Pseudonym systems were introduced by Chaum [Cha85, CE86] and more recently further formalized and studied in [LRSW99, Lys02]. The aim of these systems is to simultaneously guarantee anonymity of credential holders, unlinkability of credential showings, and non-transferability of credentials. These property ensure ultimate users' privacy and organizations' security at a high computation and communication cost. Indeed, most of such systems use multiple zero knowledge protocols for issuing and verifying credentials (see e.g. [Bra00, Lys02]). In many real life applications, such as our motivating scenario above, a more moderate level of security is considered sufficient as long as much higher efficiency can be provided. It is however crucial to clearly state the required security properties and prove it is achievable for the proposed constructions. Our work is an step in this direction.

Identification Protocols. One of the security goals of a COP protocol, protection of the secret of the credential holder, can be seen as parallel to the security goal of an identification protocol, if authority's signature is the prover's *secret* in the identification protocol. Security requirement of COP with regard to credential holder is in line with that of identification protocols as defined in [FFS88], with attacker's goal being impersonation of the prover, without having her secret. The strongest attack model for identification protocols allows the adversary to pose as a verifier and run arbitrary-interleaved (i.e. concurrent) sessions [BP02] with the prover before taking up the role of a malicious prover. We model a similar attacker for COP (having concurrent sessions with prover) and also allow the attacker to have access to signing oracle that models the credential issuer. COP security also requires security for credential issuer, which is not required in identification protocols.

DMA and NTS Schemes. Deniable Message Authentication (DMA) [DDN00] and Non-Transitive Signature (NTS) [Des88, OO90] schemes enable a sender to construct an authenticated message for a receiver such that the receiver cannot convince a third party about the origin of the message. In other words, they provide unforgeability guarantee of a digital signature but the message can be repudiated as the receiver can simulate the transcript of the protocol. The security goals in DMA and NTS schemes are complementary to a basic credential system as described above. That is, the credential holder may require that his credential ownership proof be repudiable. Although in a COP protocol the proof is interactive, but the proof transcript may not be simulatable and so in this sense, non-repudiable. DMA and NTS systems use zero knowledge proofs to provide repudiation property. Such proofs are costly and we wish to avoid them in simple credential systems, like the ones discussed above. In fact this (avoiding ZK proofs) has been one of the motivation of our work.

1.2 Our Contributions

We formalize the security model of a credential system, consisting of credential issuers, credential holders, and verifiers, with emphasis on security of credential showing. A credential issuer signs a credential using a secure (i.e. unforgeable against chosen message attack) signature scheme. A credential holder wants to prove to a verifier that he has a credential but would like to make sure that the credential cannot be copied. This protection against copying is crucial in scenarios as described above and so it is imperative that the credential holder only provide 'proof' for ownership of the credential and not the actual credential. An immediate question is what properties such a proof should have, and if efficient constructions exist.

In this paper, we define *credential ownership proof (COP)* protocols for signature schemes. We give security notions for COPs that capture precisely the security requirements of the scenario given earlier, and guarantees security of credential holders and issuers both. COPs have also the desirable property that they provide some level of control for the credential holders over unwanted distribution of their credentials. This, however, is not in the strongest sense of repudiability of the credential, but as a side effect of employing proofs.

Next we consider construction of COPs. We provide two generic constructions for signature schemes and their associated secure COPs. The first construction is based on identity-based encryption (IBE) [Sha84]. It has been observed that a secure identity-based encryption scheme can be utilized to construct a secure signature scheme[1]. We show that it is possible to define a secure COP for this scheme in a natural way. We reduce security of this COP to one-wayness of the underlying IBE under chosen-ciphertext attacks (denoted OWE-ID-CCA). This is a new security notion for IBE, that is, in terms of strength, in between the two (folklore standard) notions of one-wayness (under chosen-plaintext attacks, denoted OWE-ID) and indistinguishability under chosen-ciphertext attacks (denoted IND-ID-CCA), introduced in [BF01]. We show that this generic construction results in a scheme provably-secure based on standard computational assumptions in the *standard model* (i.e. not in the *random oracle mpodel*).

The second generic construction is based on identity-based identification (IBI) [BNN04]. We show an equivalence between a signature that is EUF-CMA (i.e. existentially unforgeable under chosen-message attacks [GMR88]) plus an associated COP that is secure in our model, and an IBI that is secure against impersonation under concurrent attacks (in the sense of [BNN04]). We show a one-to-one relationship between entities and algorithms, and give a bilateral translation of security notions of the two.

An interesting observation in this context with regard to COPs is their application in construction of secure IBIs. Kurosawa and Heng [KH04] gave a generic construction for an IBI from a signature scheme and an HVZK proof of knowledge (PoK) protocol. Security of their construction however was proved only against a *passive* adversary. We show that replacing PoK protocol with a COP protocol in their construction will result in security against *active* and *concurrent* attacks. This results in a generic construction of secure IBI schemes from COP schemes.

Both generic constructions above use identity-based cryptography, which could be considered as less traditional and requiring more advanced knowledge of cryptography. It is desirable to have a signature scheme with an associated COP that are provably secure and use standard (textbook) cryptography. We show that, for a credential system based on RSA signature, a secure COP can be obtained based on the GQ identification protocol [GQ88]. GQ, as an identification protocol, is proved to be secure against impersonation under concurrent attacks [BP02]. It is also widely known that GQ can be used to prove knowledge of RSA-FDH

[1] This is attributed to Moni Naor [BF01, p. 226].

Table 1: Notation used in the paper

$\mathsf{Sans\ Serif}$	algorithm	$x \leftarrow \mathsf{X}^{\mathcal{O}}(a)$	X with access to $\mathcal{O}$ and input a is run and outputs x
$\textsc{Small Caps}$	security notion		
$\mathcal{C}alligraphic$	oracle	$\mathsf{A} \xrightarrow{a} \mathsf{B}$	a is sent from A to B
$x \leftarrow a$	a is assigned to x	$\mathsf{X}(a)$ description $x \lrcorner$	algorithm description: X takes a as input and returns x as output
$x \overset{N}{\leftarrow} a$	a mod N is assigned to x		
$x \overset{\$}{\leftarrow} X$	x is chosen randomly from X		
$y \leftarrow [\mathsf{X}(x) \leftrightarrow \mathsf{Y}](a)$	interactive protocol between X with private input x and Y is run with public input a, and y is the output of Y ($\overset{\triangle}{=}$ output of the protocol)		

signatures, although adequate formalization of this does not seem to exist in the literature. We prove that the COP protocol based on GQ is secure in our model under concurrent attacks.

Combining RSA-FDH signature scheme of [BR96] with the GQ based COP, results in a very efficient and provably-secure credential system that can be easily implemented using commonly used cryptographic libraries. Security of the system relies, in the random oracle model, on security of GQ as an identification protocol, which is, in turn, proved in [BP02] assuming *one-more RSA inversion* [BNPS01] is hard. An interesting open question is construction of secure COPs for other traditional signature schemes.

The paper is organized as follows. In Section 2 we introduce the notations used through the paper. Section 3 formalizes the proposed security model for COPs. We propose our IBE-based and IBI-based constructions in Sections 4 and 5. Then, in Section 6, an efficient RSA-based scheme based on GQ is proposed, and finally, Section 7 concludes the paper.

2 Notation

The notation we use throughout the paper is summarized in Table 1. We also denote the internal state information of algorithm X by St_{X}, the set of all algorithms poly-time in k by $\mathcal{P}oly(k)$, and the empty string by ε.

3 Definitions

A credential system consists of users and organizations. Organizations issue credentials to users. Users can later show their credentials to (the same or) other organizations to enjoy the privileges they are entitled to. A credential is of the form (m, σ), where m is the text of the credential and σ is the issuer's signature on m, generated using the standard signature scheme $\mathsf{SS} = \mathsf{SS}.(\mathsf{KeyGen}, \mathsf{Sign}, \mathsf{Verify})$. To prove ownership of such a credential, we associate an interactive proof protocol with the signature scheme SS, through which the credential-holder (prover) convinces the verifier that she owns a credential signed by an issuer that employs the signature SS.

Definition 1 *Associated with a standard signature* SS*, we define a* credential ownership proof (equiv. COP) *protocol* $\mathsf{SS\text{-}COP} = \mathsf{SS\text{-}COP}.(\mathsf{P}, \mathsf{V})$*, consisting of a pair of algorithms: the* prover $\mathsf{SS\text{-}COP.P}$ *and the* verifier

$\mathsf{SS\text{-}COP.V}$. *Prover's private input is a signature σ and protocol's public inputs are the signature verification key pk and a message m. After the interaction with the prover, the verifier outputs a binary decision b. The protocol's output is the verifier's output and the protocol run is denoted by:*

$$b \leftarrow [\mathsf{SS\text{-}COP.P}\,(\sigma) \leftrightarrow \mathsf{SS\text{-}COP.V}]\,(pk, m) \quad .$$

The working scenario for $\mathsf{SS\text{-}COP}$ would be as follows: first the signer issues a credential (m, σ), which is given to the credential holder, using $\mathsf{SS.KeyGen}$ and $\mathsf{SS.Sign}$ algorithms. When the credential-holder wants to 'securely' show her credential to a verifier, she first sends to the verifier the identity of the issuer, from which the verifier can securely obtain the issuer's public key (for example through PKI), and the text of the credential (i.e. the message) m, on which she claims to have the issuer's signature. The credential-holder and the verifier then interact with each other running $\mathsf{SS\text{-}COP.P}$ and $\mathsf{SS\text{-}COP.V}$, respectively. At the end of this interaction, either the verifier accepts the prover's claim of credential ownership or not. This is reflected in the protocol's output b as a 1 if the verifier is convinced, and a 0 otherwise.

We require that an honest credential-holder can always convince the verifier, i.e. it must be guaranteed that if the signature σ is a valid signature on m with respect to pk, then the COP protocol run must return 1. Hence, we define the completeness of the COP protocol as follows.

Definition 2 *We say that the above credential ownership proof* $\mathsf{SS\text{-}COP}$ *is complete iff*

$$\Pr\Big[b = 1 : b \leftarrow [\mathsf{SS\text{-}COP.P}\,(\sigma) \leftrightarrow \mathsf{SS\text{-}COP.V}]\,(pk, m) \;\Big|\; \mathsf{SS.Verify}\,(pk, m, \sigma)\Big] = 1 \quad .$$

3.1 Defining COP Security

A COP-IMP-CA adversary $\mathsf{A} = \mathsf{A}.(\hat{\mathsf{V}}, \hat{\mathsf{P}})$ is a pair of randomized poly-time algorithms: the *cheating verifier* and the *cheating prover*, respectively. The attack is mounted in two phases. Throughout both phases, the adversary is provided with a signing oracle, which enables it to have a signature on any message of its choice.

At the beginning of the first phase, the cheating verifier is given the public key, which has been generated through the signature key generation. Then it starts requesting interactions with clones of honest provers who own a signature on messages of its choice in an arbitrary interleaved way (i.e. *concurrent* way). When an interaction with a new clone is requested, the message provided by the adversary is signed, the signature is given to a new honest prover clone, and an interaction between the honest prover and the cheating verifier is initialized. On the other hand, if the adversary asks for the next round of interaction with an already existing honest prover clone, the appropriate clone is provoked. Multiple clones are allowed to exist simultaneously. At some point, the cheating verifier declares that the first phase is complete and decides on an impersonation target message (denoted $\dot{m}$). This target message and the state information of the cheating verifier is given to the cheating prover in the beginning of the second phase.

In the second phase, the target message is given to an honest verifier along with the public key, and an interaction between the cheating prover and the honest verifier is initiated. During this interaction, the cheating prover has access to the same oracles as did the cheating verifier during the first phase. The adversary is said to win if at the end of this interaction the honest verifier is convinced that the adversary is in possession of a signature on the target message, given the condition that the target message have not been queried to the signing oracle.

Definition 3 *For an adversary* A *and a protocol* $\mathsf{SS\text{-}COP}$*, we define the following experiment:*

```
$\mathsf{Expt}^{\text{COP-IMP-CA}}_{\mathsf{SS\text{-}COP}}(\mathsf{A}, k)$
    $(pk, sk) \leftarrow \mathsf{SS.KeyGen}(k)$
    $(\dot{m}, St_{\mathsf{A}}) \leftarrow \mathsf{A}.\hat{\mathsf{V}}^{\mathcal{O}}(k, pk)$
    $b \leftarrow \left[\mathsf{A}.\hat{\mathsf{P}}^{\mathcal{S}ign(\cdot)}(St_{\mathsf{A}}) \leftrightarrow \mathsf{SS\text{-}COP.V}\right](pk, \dot{m})$
    $b \hookleftarrow$
```

```
$\mathcal{O} \triangleq \left(\mathcal{I}nteract(\cdot,\cdot,\cdot), \mathcal{S}ign(\cdot)\right)$

$\mathcal{I}nteract(m, sid, M_{\text{in}})$
    If $(m, sid)$ new
        Then $St[m, sid] \leftarrow \left(pk, \mathsf{SS.Sign}(sk, m)\right)$
    $(M_{\text{out}}, St[m, sid]) \leftarrow \mathsf{P}(M_{\text{in}}, St[m, sid])$
    $M_{\text{out}} \hookleftarrow$

$\mathcal{S}ign(m) \triangleq \mathsf{SS.Sign}(sk, m)$
```

Moreover, the advantage *of* A *in a* COP-IMP-CA *attack on* $\mathsf{SS\text{-}COP}$ *is defined as:*

$$\mathrm{Adv}^{\text{COP-IMP-CA}}_{\mathsf{SS\text{-}COP},\mathsf{A}}(k) \triangleq \Pr\left[\mathsf{Expt}^{\text{COP-IMP-CA}}_{\mathsf{SS\text{-}COP},\mathsf{A}}(k) = 1 \,|\, no\mathcal{S}ign(\dot{m})\ query\right]$$

Finally, we define the COP-IMP-CA insecurity *of* $\mathsf{SS\text{-}COP}$ *as the maximum advantage a poly-time* COP-IMP-CA *adversary can achieve, i.e.*

$$\mathrm{Insec}^{\text{COP-IMP-CA}}_{\mathsf{SS\text{-}COP}}(k) \triangleq \max_{\mathsf{A}\in\mathcal{P}oly(k)}\left[\mathrm{Adv}^{\text{COP-IMP-CA}}_{\mathsf{SS\text{-}COP},\mathsf{A}}(k)\right] \quad .$$

We say that $\mathsf{SS\text{-}COP}$ *is* COP-IMP-CA-secure *if its* COP-IMP-CA *insecurity is negligible in k.*

Credential-Holder Protection. The COP-IMP-CA security guarantees that an adversary interacting with many different credential-holders is not able to impersonate one of them in a COP protocol and prove ownership of one of their credentials to another entity. This property is reflected in the defined experiment as the case where the adversary interacts with a clone holding the credential on the target message during the attack. It is also worth to mention that COP-IMP-CA security is stronger than both notions of security in [BSS05], i.e. IMP-1 and IMP-2, aiming to capture credential-holder protection. In fact, COP-IMP-CA security can be seen as an extension of these two notions, in which the adversary has extra capabilities of corrupting credential-holders of its choice (i.e. access to the signing oracle), interacting with credential-holders of its choice, arbitrarily interleaving such interactions (i.e. concurrent attack), and deciding on the credential text that it will claim ownership of the signature on.

Credential-Issuer Protection. The credential-issuer is protected in the definition as the adversary who can have the signatures on arbitrary messages of its choice and can interact with arbitrary credential-holders of its choice, cannot even prove ownership of a new credential, let alone forging one. This property is reflected in the defined experiment, as the case where the adversary does not interact with a clone holding the credential on the target message during the attack and the target message presents a new credential. We note that COP-IMP-CA security implies existential unforgeability of the underlying signature scheme under chosen-message attack (i.e. being EUF-CMA [GMR88]). This is true because if the signature is not EUF-CMA, the adversary will be able to forge a new message-signature pair (i.e. a new credential) by properly querying the signing oracle in the first phase of the COP-IMP-CA attack, and successfully prove ownership of the credential in the second phase.

It is easy to see that a ZK proof of knowledge of a member of the NP language $L_{(pk,m)} = \{\sigma : \mathsf{Verify}(pk, m, \sigma)\}$ is a COP-IMP-CA-secure COP given that the underlying signature is EUF-CMA. To prove this, one can construct a signature forger out of a COP impersonator as follows. Honest credential-holders can be simulated without knowing a signature in the first phase since the protocol is zero knowledge. In the second phase, a valid signature can be extracted from the cheating prover since the protocol is a proof of knowledge. The obtained signature constitutes a forgery for the signature scheme. In the following sections though, we seek more efficient ways to realize COP-IMP-CA-secure COPs.

4 Generic Construction from IBE

As stated before, it is known that a secure signature scheme can be constructed based on a secure *identity-based encryption (IBE)*. In this section, we give a generic construction of a COP associated to the mentioned signature scheme based on any IBE scheme and prove it COP-IMP-CA-secure assuming *one-wayness* of the IBE under *chosen ciphertext attacks* (denoted by OWE-ID-CCA). OWE-ID-CCA is a new security notion for IBE schemes which is weaker than *indistinguishability* under *chosen ciphertext attacks* (i.e. IND-ID-CCA), a widely-accepted security notion for IBE schemes formalized in [BF01, BF03]. Our results in this section provides constructions for signature schemes and associated COPs provably-secure based on *standard assumptions* such as BDH, in the *standard model* (i.e. not in the *random oracle model*).

4.1 IBE and Its Security

An identity-based encryption scheme IBE consists of four algorithms $\mathsf{IBE} = \mathsf{IBE}.(\mathsf{Set}, \mathsf{Ext}, \mathsf{Enc}, \mathsf{Dec})$ [BF01], where The *setup* algorithm $\mathsf{IBE.Set}$ takes input the security parameter k and returns the system parameters par and the master key mk, denoted $(par, mk) \leftarrow \mathsf{IBE.Set}(k)$, the *extraction* algorithm $\mathsf{IBE.Ext}$ is given input par, mk, and an identity ID and outputs the decryption key dk corresponding to ID, denoted $dk \leftarrow \mathsf{IBE.Ext}(par, mk, ID)$, the *encryption* algorithm $\mathsf{IBE.Enc}$ on input par, ID, and some plaintext P outputs the ciphertext C, denoted $C \leftarrow \mathsf{IBE.Enc}(par, ID, P)$, and finally, the *decryption* algorithm $\mathsf{IBE.Dec}$ takes inputs par, dk, and C and outputs P, denoted $P \leftarrow \mathsf{IBE.Dec}(par, dk, C)$.

We introduce a new notion of security for IBE schemes in analogy with the notions in [BF01] and [BF03]. Boneh and Franklin define three notions of security for IBEs: OWE-ID, IND-ID-CPA, and IND-ID-CCA. The resources of the adversary is the same in the first two notions: having access to an extraction oracle. On the other hand, the goal of the adversary is the same in the last two notions: distinguishing the ciphertexts of two chosen plaintexts. We introduce a new notion OWE-ID-CCA in which the resources of the adversary is the same as the last notion: having access to both extraction and decryption oracles, and the goal of the adversary is the same as the first notion: decrypting a challenge ciphertext. It is clear that the security level guaranteed by this notion is higher than OWE-ID, but lower than IND-ID-CCA.

Definition 4 *An IBE is called* OWE-ID-CCA *if the value*

$$\Pr\left[P = R : \begin{array}{l} (par, mk) \leftarrow \mathsf{IBE.Set}(k) \\ \left(\dot{ID}, St_{\mathsf{A}}\right) \leftarrow \mathsf{A}^{\mathcal{E}xt(\cdot),\mathcal{D}ec_1(\cdot,\cdot)}(par) \\ P \xleftarrow{\$} \{0,1\}^* \\ C \leftarrow \mathsf{IBE.Enc}\left(par, \dot{ID}, P\right) \\ R \leftarrow \mathsf{A}^{\mathcal{E}xt(\cdot),\mathcal{D}ec_2(\cdot,\cdot)}(C, St_{\mathsf{A}}) \end{array}\right]$$

is negligible in k for any poly-time adversary A given that there is neither a $\mathcal{E}xt\left(\dot{ID}\right)$ nor a $\mathcal{D}ec_2\left(\dot{ID}, C\right)$ query by the adversary, where $\mathcal{E}xt(\cdot)$, $\mathcal{D}ec_1(\cdot,\cdot)$, and $\mathcal{D}ec_2(\cdot,\cdot)$ are the extraction oracle, decryption oracle in phase 1, and decryption oracle in phase 2, respectively.

4.2 IBE-Based Signature and IBE-Based COP

Given an IBE scheme, a signature scheme IBESig can be constructed [BF01, p. 226]. The key generation, signing, and *randomized* verification algorithms are as follows:

```
IBESig.KeyGen $(k)$
    $(par, mk) \leftarrow$ IBE.Set $(k)$
    $pk \leftarrow par$
    $sk \leftarrow (par, mk)$
    $(pk, sk) \lrcorner$
```

```
IBESig.Sign $(sk, m)$
    $dk \leftarrow$ IBE.Ext $(par, mk, m)$
    $\sigma \leftarrow dk$
    $\sigma \lrcorner$
```

```
IBESig.Verify $(pk, m, \sigma)$
    $P \xleftarrow{\$} \{0,1\}^*$
    $C \leftarrow$ IBE.Enc $(pk, m, P)$
    $R \leftarrow$ IBE.Dec $(par, \sigma, C)$
    $b \leftarrow (P = R)$
    $b \lrcorner$
```

As one may notice, the verification algorithm in IBESig inherently has a challenge-response structure. We use this structure to define the IBE-based credential ownership proof IBE-COP as follows:

```
[IBE-COP.P $(\sigma) \leftrightarrow$ IBE-COP.V] $(pk, m)$
    $St_{\mathsf{P}} \leftarrow (\sigma, pk, m)$ ,    $St_{\mathsf{V}} \leftarrow (pk, m)$

                                                 IBE-COP.V $(\varepsilon, St_{\mathsf{V}})$
                                                     $P \xleftarrow{\$} \{0,1\}^*$ , $St_{\mathsf{V}} \leftarrow P$
                                                     $C \leftarrow$ IBE.Enc $(pk, m, P)$
IBE-COP.P $(C, St_{\mathsf{P}})$      $\xleftarrow{C}$          $(C, St_{\mathsf{V}}) \lrcorner$
    $R \leftarrow$ IBE.Dec $(pk, \sigma, C)$
    $R \lrcorner$                      $\xrightarrow{R}$          IBE-COP.V $(R, St_{\mathsf{V}})$
                                                     $d \leftarrow (P = R)$
                                                     $d \lrcorner$
```

In other words, the verifier sends the prover a challenge ciphertext, obtained using encryption of a random plaintext, and expects the prover to be able to decrypt it using the signature she knows and reply with a response equal to the plaintext. We prove that this construction is COP-IMP-CA-secure.

Theorem 1 IBE-COP *is a* COP-IMP-CA*-secure credential ownership proof if* IBE *is an* OWE-ID-CCA *identity-based encryption.*

The proof is given in Appendix D. We note that this theorem is also of theoretical interest. Waters [Wat05], constructed efficient IBE schemes secure under the standard BDH assumption and without random oracle. Combining this result with Theorem 1 implies that a secure signature with associated COP can be constructed in standard model, without requiring random oracle or strong assumptions (such as one-more RSA).

As noted before, COP-IMP-CA security implies EUF-CMA. Hence, we have the following as a corollary. Note that this result is stronger than the previous observation, which claimed EUF-CMA security for IBESig given that the underlying IBE is IND-ID-CCA.

Corollary 1 IBESig *is* EUF-CMA *assuming that* IBE *is* OWE-ID-CCA*.*

Table 2: Equivalence between SS+COPs and IBIs

scheme	entity			algorithm				parameter			
SS+COP	issuer	holder	verifier	KeyGen	Sign	P	V	pk	sk	σ	m
⦀	⦀	⦀	⦀	⦀	⦀	⦀	⦀	⦀	⦀	⦀	⦀
IBI	authority	user	verifier	$\mathsf{MKeyGen}$	$\mathsf{UKeyGen}$	P	V	mpk	msk	usk	ID

5 Equivalence with IBI

An *identity-based identification scheme (IBI)* is a scheme through which an entity can identify herself to a verifier who only knows the claimed identity and a public key of an authority. The widely-accepted framework of security for such schemes is security against *impersonation* under *passive*, *active*, or *concurrent* attacks formalized in [BNN04]. In the same paper, Bellare, Namprempre, and Neven show that there exists a trivial general construction of IBI schemes with building blocks of standard identification and signature schemes, called *certificate-based* IBI. They also prove that if the underlying standard identification and signature schemes are secure, then the resulted certificate-based IBI is also secure. Hence, IBIs achieving high levels of security such as security against impersonation under concurrent attacks (which we denote by id-imp-ca) can be constructed.

In an independent work, Kurosawa and Heng [KH04] introduced a new general construction of IBI using signature schemes with honest-verifier zero-knowledge protocols for proof of knowledge of a signature on a mutually-known message. However, their IBI only achieves security against impersonation under *passive* attacks assuming that the underlying signature scheme is secure and the protocol is HVZK-PoK. Interestingly, in this section we show that security against impersonation under *concurrent* attacks (id-imp-ca) can be achieved if their construction is applied to a signature with an associated credential ownership proof (henceforth SS+COP), instead of a signature with their requirements! Furthermore, we show that SS+COPs and IBIs are actually equivalent, i.e. each of them can be employed instead of the other only by renaming the entities, algorithms and parameters in use. Such equivalence implies yet another generic construction for secure COPs.

The Equivalence between Schemes. A SS+COP is a scheme through which a credential-issuer generates signatures on messages and later on, a credential-holder proves to a verifier, who only knows the credential-issuer's public key, that she is in possession of a signature on a mutually-known message. Similarly, an IBI is a scheme through which an authority generates user secret keys for user identities and later on, a user proves to a verifier, who only knows the authority's master public key, that she is in possession of a user secret key of a mutually-known identity. From this simple comparison, the equivalence shown in Table 2 between the entities, algorithms and parameters in the two schemes, i.e. SS+COP scheme $\mathsf{SS}.(\mathsf{KeyGen}, \mathsf{Sign}, \mathsf{Verify})$ + $\mathsf{SS\text{-}COP}.(\mathsf{P}, \mathsf{V})$ and IBI scheme $\mathsf{IBI}.\big(\mathsf{MKeyGen}, \mathsf{UKeyGen}, (\mathsf{P}, \mathsf{V})\big)$ becomes apparent. Note that, similar to signatures, a user secret key is also publicly verifiable (at least by simulating the identification protocol).

We call the transform which uses Table 2 to rename entities, algorithms and parameters in a given SS+COP to convert it to an IBI scheme, $\mathsf{COP\text{-}2\text{-}IBI}$ *transform.* The corresponding reverse transform is likewise denoted $\mathsf{IBI\text{-}2\text{-}COP}$ *transform.* In what follows, we show that if these transforms are applied to secure input schemes, they will yield secure output schemes. This fact enables us to construct each of the schemes from an implementation of the other.

Theorem 2 *The scheme* $\mathsf{COP\text{-}2\text{-}IBI}\,(\mathsf{SS}, \mathsf{SS\text{-}COP})$ *is an* id-imp-ca*-secure identity-based identification assuming that* $\mathsf{SS\text{-}COP}$ *is a* cop-imp-ca*-secure credential ownership proof, and vice versa, i.e. the construction* $\mathsf{IBI\text{-}2\text{-}COP}\,(\mathsf{IBI})$ *is a* euf-cma *signature with an associated* cop-imp-ca*-secure credential ownership proof assuming that* IBI *is an* id-imp-ca*-secure identity-based encryption.*

Proof. (Sketch) Security in a SS+COP scheme translates into a guarantee that no poly-time adversary is able to impersonate a credential-holder, even if it can have a signature on any message it wishes (i.e. corrupt any credential holder it wants) and can interact concurrently with clones of credential-holders on messages of its choice. Likewise, security in an IBI scheme translates into a guarantee that no poly-time adversary is able to impersonate a user, even if it can have the user secret key of any identity it wishes (i.e. corrupt any identity it wants) and can interact concurrently with clones of users with identities of its choice. A thorough examination of the two security definitions, i.e. the definition of our COP-IMP-CA notion in Definition 3 and the ID-IMP-CA notion in [BNN04, p. 275], shows that (barring notation and some minor details[2]) they *are* indeed equivalent if the entities, algorithms, and parameters are properly renamed according to Table 2. □

Note that the second part of Theorem 2 particularly enables one to construct several COP-IMP-CA-secure COP protocols (plus several EUF-CMA signatures) out of the many ID-IMP-CA-secure IBI schemes proposed to date, based on a range of different computational assumptions. For a collection of provably-secure IBI schemes, please refer to [BNN04]. Another implication of this equivalence is the construction of secure IBI schemes from secure IBE schemes.

6 Efficient COP from GQ

The mentioned two generic constructions result in several COP protocols based on a range of different security assumptions. However, the cryptography involved in implementing IBE and IBI schemes is complex. For instance, a notable proportion of such schemes requires implementation of bilinear maps. In this section we show that the GQ identification scheme [GQ88] yields a COP-IMP-CA-secure credential ownership proof protocol (that we call RSA-COP) for the popular RSA-FDH signature [BR96]. Such a construction only exploits simple RSA cryptography and can be implemented efficiently. Particularly, RSA-COP can be easily integrated into credential systems already using the popular RSA-FDH signature to issue credentials. First we briefly review the GQ scheme and then prove that it yields a secure COP protocol. Finally, a simple comparison is shown between RSA-COP and some ZK solutions to our motivating problem, in terms of computational and communicational complexity. The comparison provides clear justification why COPs are preferable to ZK solutions.

6.1 The GQ Identification Scheme

This scheme was proposed by Guillou and Quisquater [GQ88], and proved to have both the *honest verifier zero knowledge (HVZK)* and the *proof of knowledge (PoK)* properties. The scheme enables the prover to prove knowledge of x to the verifier such that $X = x^e \bmod N$ holds for some mutually-known $pk_{\mathsf{GQ}} = (N, e, X)$. To identify herself, the prover first sends a *commitment* Y to the receiver which is then replied by a *challenge* c from the verifier. Finally, the prover answers with a *response* z. The verifier then makes the decision d by testing whether or not the equation $z^e = Y \cdot X^c \bmod N$ holds. The scheme is transcribed in Appendix A.

Bellare and Palacio prove that this identification scheme is secure against concurrent impersonation attacks [BP02] (called IMP-CA, see Appendix B for definition) provided that the *challenge length* is super-logarithmic and the *one-more RSA inversion problem* [BNPS01] is hard.

[2] [BNN04] adds an initialization oracle to the two oracles that we have. The adversary there must first initialize each identity, which causes a secret key to be generated for that identity. We do not require the adversary to initialize the credentials, i.e. to cause a certain message to be signed. Instead, the credentials are automatically initialized upon calling the interaction oracle. The difference stems from two ways of formalizing the same concept, and as our goal here is to show an inherent equivalence, rather than a precisely formal one, we do not address the difference.

6.2 RSA-FDH Credential Ownership Proof

The $\mathsf{RSA\text{-}FDH}$ signature scheme is proposed and proved existentially unforgeable under chosen message attack by Bellare and Rogaway [BR96]. Briefly, the scheme uses an RSA modulus generator $\mathsf{Gen}_{\mathsf{RSA}}$ to generate keys, assigns a signature of the form $[H(m)]^d \bmod N$ to a message m, and a verifies a candidate signature σ by checking whether or not $\sigma^e = H(m) \bmod N$. The complete transcription of the scheme comes in Appendix C. We define the COP protocol $\mathsf{RSA\text{-}COP}$ as follows.

```
$[\mathsf{RSA\text{-}COP.P}\,(\sigma) \leftrightarrow \mathsf{RSA\text{-}COP.V}]\,(pk, m)$
  $pk_{\mathsf{GQ}} \leftarrow \big(N, e, H(m)\big)$
  $sk_{\mathsf{GQ}} \leftarrow (N, \sigma)$
  $b \leftarrow [\mathsf{GQ.P}\,(sk_{\mathsf{GQ}}) \leftrightarrow \mathsf{GQ.V}]\,(pk_{\mathsf{GQ}})$
  $b$ ↲
```

Note that in analogy with GQ, in $\mathsf{RSA\text{-}COP}$ the prover proves knowledge of a value σ to the verifier such that $H(m) = \sigma^e \bmod N$ holds for some mutually-known N, $H(m)$, and e.

Proving completeness of the protocol is straightforward: Completeness of GQ translates into the equation $\sigma^e = H(m) \bmod N$, which holds given the validity of the RSA-FDH signature. We prove security of the protocol against COP-IMP-CA attacks.

Theorem 3 $\mathsf{RSA\text{-}COP}$ *is* COP-IMP-CA*-secure in the random oracle model assuming that* GQ *is secure against concurrent impersonation attack. Quantitatively speaking, we have*

$$\mathrm{Insec}^{\text{COP-IMP-CA}}_{\mathsf{RSA\text{-}COP}}(k) \le O\left(q_s\right) \cdot \mathrm{Insec}^{\text{IMP-CA}}_{\mathsf{GQ}}(k) \quad ,$$

where q_s is the number of credentials the issuer signs.

Proof. (Sketch) We present a construction of an IMP-CA adversary A_{GQ} for GQ which uses a successful COP-IMP-CA adversary A for $\mathsf{RSA\text{-}COP}$ as a subroutine. A_{GQ}, given $pk_{\mathsf{GQ}} = (N, e, X)$ as input, simulates A's hash and signing oracle queries following Coron's method [Cor00], i.e. embeds X in the hash values of some hash queries ($H(m_i) = X \cdot r_i^e \bmod N$) and answers others randomly ($H(m_i) = r_i^e \bmod N$). This way, A_{GQ} is also able to answer signing oracle queries m_i, if X is not embedded in $H(m_i)$, as $\sigma_i = [H(m_i)]^d = r_i$. However, A_{GQ} fails whenever it is asked a signing oracle query m_i, if X is embedded in $H(m_i)$. Furthermore, A_{GQ} is able to properly respond to *all* the interaction requests of A: when A asks to interact with a clone holding a signature on a message m, where X is not embedded in $H(m)$, since A_{GQ} already knows the signature on the message ($\sigma = r$), it is able to play the role of the requested clone for A. On the other hand, if A asks to interact with a clone holding a signature on a message m, where X is embedded in $H(m)$, A_{GQ} will use its ability to request interaction with an honest GQ prover clone to simulate the interaction for A. Since the honest GQ prover clone supplies A_{GQ} with a z, such that $z^e = Y \cdot X^c \bmod N$, by relaying the same Y and c, A_{GQ} will be able to respond to A with $\zeta \leftarrow r^c \cdot z \bmod N$, such that $\zeta^e = Y \cdot X^c \cdot r^{ec} = Y \cdot [H(m)]^c \bmod N$, which convinces A. When A declares that the first phase of the attack is over and enters the second phase, again similar to Coron's method, if A chooses a target message $\dot{m}$, where X is not embedded in $H(\dot{m})$, A_{GQ} fails. But if A chooses a target message, where X is embedded in $H(\dot{m})$, A_{GQ} will be able to impersonate the GQ prover using a similar method as before: since A is able to provide A_{GQ} a ζ, such that $\zeta^e = Y \cdot [H(\dot{m})]^c \bmod N$, by relaying the same Y and c, A_{GQ} will be able to respond with $z \leftarrow \zeta / \dot{r}^c \bmod N$, such that

$$z^e = \frac{\zeta^e}{\dot{r}^{ce}} = \frac{Y \cdot [H(\dot{m})]^c}{\dot{r}^{ce}} = \frac{Y \cdot (X^c \cdot \dot{r}^{ce})}{\dot{r}^{ce}} = Y \cdot X^c \mod N,$$

which convinces the honest GQ verifier. Similar to Coron's analysis, here A's success probability can be calculated and the claimed bound can be proved. The full proof is presented in Appendix E. □

Table 3: Comparison of $\mathsf{RSA\text{-}COP}$ Costs with other ZK Solutions

protocol	rounds	prover cost	verifier cost
		(group op.)	(group op.)
ZK-PoK-RSA from [DK99]	5	5	5
ZK-PoK-DL from [DK99]	5	4	5
ZK-PoK-DL from [CDM00]	4	4	6
RSA-COP	3	2	2

Combining this theorem and [BP02, Theorem 4.1], we will simply have the following.

Corollary 2 *In the random oracle model,* $\mathsf{RSA\text{-}COP}$ *is* COP-IMP-CA*-secure if one-more RSA inversion problem is hard for moduli generated by* $\mathsf{Gen}_{\mathrm{RSA}}$ *and the challenge space . Quantitatively speaking, we have*

$$\mathrm{Insec}^{\text{COP-IMP-CA}}_{\mathsf{RSA\text{-}COP}}(k) \leq O(q_s) \cdot \left(2^{-\ell(k)} + \sqrt{\mathrm{Insec}^{\text{RSA-OMI}}_{\mathsf{Gen}_{\mathrm{RSA}}}(k)}\right) \quad ,$$

where q_s *is the number of credentials the issuer signs and* ℓ *is the challenge length in* $\mathsf{RSA\text{-}COP}$.

6.3 Efficiency of the Scheme

We have showed that GQ provides a COP-IMP-CA-secure credential ownership proof for RSA-FDH credentials. As mentioned before, GQ is only known to be HVZK. This can be considered as a clue that $\mathsf{RSA\text{-}COP}$ fulfills our motivating initial to design COP protocols that can be implemented more efficiently than ZK proofs. A thorough examination of the scheme reveals that this indeed is the case. In Table 3 $\mathsf{RSA\text{-}COP}$ is compared with some of the most efficient constructions of ZK for widely-used cryptographic relations, to the best of our knowledge. The compared protocols are two ZK proofs of knowledge of discrete logarithm (denoted ZK-PoK-DL) and one ZK proof of knowledge of eth root (denoted ZK-PoK-RSA) from [DK99, CDM00]. As the table shows, ZK solution to our problem takes up to four rounds of interaction and costs the credential holder up to four group operations, while employing GQ as $\mathsf{RSA\text{-}COP}$ reduces the interaction rounds to three and credential holder cost to only two group operations. This property makes our solution desirable for light-weight implementations of credential systems with the mentioned security requirements.

7 Concluding Remarks

In this paper we have introduced the concept of secure credential ownership proofs and proposed several schemes for it. We have shown general constructions based on identity-based encryption and identification schemes. Plenty of secure schemes for each of those schemes has been proposed in the literature, offering a wide range of options to implement secure credential ownership proofs. Furthermore, the equality we have shown between credential ownership proofs and identity-based identifications introduces new scheme designs for the latter (and hence for identity-based signatures through the Fiat-Shamir paradigm [FS86, BNN04]) as well. Our result on the security of the GQ protocol for proving ownership of RSA-FDH credentials enables current credential systems which use such signatures to integrate GQ easily with guaranteed security, while all the previously issued credentials can be still used in the new system.

This paper can be seen as an attempt to fill a part of the gap between the two ends of the credential systems spectrum, namely standard signatures and pseudonym systems, with the former offering merely the basic security properties and the latter offering ultimate security and privacy protection. For many purposes, the full protection guaranteed in pseudonym systems are not needed. Hence, properly defining and securely designing new schemes which give up parts of such full protection for better efficiency still remains a challenging open problem.

References

[BF01] Dan Boneh and Matthew K. Franklin. Identity-Based Encryption from the Weil Pairing. In Joe Kilian, editor, *CRYPTO*, volume 2139 of *Lecture Notes in Computer Science*, pages 213–229. Springer, 2001. (Cited on pages 4, 8 and 9.)

[BF03] Dan Boneh and Matthew K. Franklin. Identity-Based Encryption from the Weil Pairing. *SIAM J. Comput.*, 32(3):586–615, 2003. (Cited on page 8.)

[BG92] Mihir Bellare and Oded Goldreich. On Defining Proofs of Knowledge. In Ernest F. Brickell, editor, *CRYPTO*, volume 740 of *Lecture Notes in Computer Science*, pages 390–420. Springer, 1992. (Cited on page 2.)

[BNN04] Mihir Bellare, Chanathip Namprempre, and Gregory Neven. Security Proofs for Identity-Based Identification and Signature Schemes. In Christian Cachin and Jan Camenisch, editors, *EUROCRYPT*, volume 3027 of *Lecture Notes in Computer Science*, pages 268–286. Springer, 2004. (Cited on pages 4, 10, 11 and 13.)

[BNPS01] Mihir Bellare, Chanathip Namprempre, David Pointcheval, and Michael Semanko. The Power of RSA Inversion Oracles and the Security of Chaum's RSA-Based Blind Signature Scheme. In Paul F. Syverson, editor, *Financial Cryptography*, volume 2339 of *Lecture Notes in Computer Science*, pages 319–338. Springer, 2001. (Cited on pages 5 and 11.)

[BP02] Mihir Bellare and Adriana Palacio. GQ and Schnorr Identification Schemes: Proofs of Security against Impersonation under Active and Concurrent Attacks. In Moti Yung, editor, *CRYPTO*, volume 2442 of *Lecture Notes in Computer Science*, pages 162–177. Springer, 2002. (Cited on pages 3, 4, 5, 11, 13, 16 and 18.)

[BR96] Mihir Bellare and Phillip Rogaway. The Exact Security of Digital Signatures - How to Sign with RSA and Rabin. In *EUROCRYPT*, pages 399–416, 1996. (Cited on pages 5, 11 and 12.)

[Bra00] Stefan Brands. *Rethinking Public Key Infrastructures and Digital Certificates: Building in Privacy.* MIT Press, 2000. (Cited on page 3.)

[BSS05] Joonsang Baek, Reihaneh Safavi-Naini, and Willy Susilo. Universal Designated Verifier Signature Proof (or How to Efficiently Prove Knowledge of a Signature). In Bimal K. Roy, editor, *ASIACRYPT*, volume 3788 of *Lecture Notes in Computer Science*, pages 644–661. Springer, 2005. (Cited on pages 3 and 7.)

[CDM00] Ronald Cramer, Ivan Damgård, and Philip D. MacKenzie. Efficient Zero-Knowledge Proofs of Knowledge Without Intractability Assumptions. In Hideki Imai and Yuliang Zheng, editors, *Public Key Cryptography*, volume 1751 of *Lecture Notes in Computer Science*, pages 354–372. Springer, 2000. (Cited on page 13.)

[CE86] David Chaum and Jan-Hendrik Evertse. A Secure and Privacy-protecting Protocol for Transmitting Personal Information Between Organizations. In Odlyzko [Odl87], pages 118–167. (Cited on page 3.)

[Cha85] David Chaum. Security Without Identification: Transaction Systems to Make Big Brother Obsolete. *Commun. ACM*, 28(10):1030–1044, 1985. (Cited on page 3.)

[Cor00] Jean-Sébastien Coron. On the Exact Security of Full Domain Hash. In Mihir Bellare, editor, *CRYPTO*, volume 1880 of *Lecture Notes in Computer Science*, pages 229–235. Springer, 2000. (Cited on pages 12, 18 and 19.)

[DDN00] Danny Dolev, Cynthia Dwork, and Moni Naor. Nonmalleable Cryptography. *SIAM J. Comput.*, 30(2):391–437, 2000. (Cited on page 3.)

[Des88] Yvo Desmedt. Subliminal-Free Authentication and Signature (Extended Abstract). In *EUROCRYPT*, pages 23–33, 1988. (Cited on page 3.)

[DK99] Yvo Desmedt and Kaoru Kurosawa. Practical and Proven Zero-Knowledge Constant Round Variants of GQ and Schnorr. *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, 82(1):69–76, 1999. (Cited on page 13.)

[FFS88] Uriel Feige, Amos Fiat, and Adi Shamir. Zero-Knowledge Proofs of Identity. *J. Cryptology*, 1(2):77–94, 1988. (Cited on page 3.)

[FS86] Amos Fiat and Adi Shamir. How to Prove Yourself: Practical Solutions to Identification and Signature Problems. In Odlyzko [Odl87], pages 186–194. (Cited on page 13.)

[GMR88] Shafi Goldwasser, Silvio Micali, and Ronald L. Rivest. A Digital Signature Scheme Secure Against Adaptive Chosen-Message Attacks. *SIAM J. Comput.*, 17(2):281–308, 1988. (Cited on pages 4 and 7.)

[GMR89] Shafi Goldwasser, Silvio Micali, and Charles Rackoff. The Knowledge Complexity of Interactive Proof Systems. *SIAM J. Comput.*, 18(1):186–208, 1989. (Cited on page 2.)

[GQ88] Louis C. Guillou and Jean-Jacques Quisquater. A "Paradoxical" Indentity-Based Signature Scheme Resulting from Zero-Knowledge. In Shafi Goldwasser, editor, *CRYPTO*, volume 403 of *Lecture Notes in Computer Science*, pages 216–231. Springer, 1988. (Cited on pages 2, 4 and 11.)

[KH04] Kaoru Kurosawa and Swee-Huay Heng. From Digital Signature to ID-based Identification/Signature. In Feng Bao, Robert H. Deng, and Jianying Zhou, editors, *Public Key Cryptography*, volume 2947 of *Lecture Notes in Computer Science*, pages 248–261. Springer, 2004. (Cited on pages 4 and 10.)

[LRSW99] Anna Lysyanskaya, Ronald L. Rivest, Amit Sahai, and Stefan Wolf. Pseudonym Systems. In Howard M. Heys and Carlisle M. Adams, editors, *Selected Areas in Cryptography*, volume 1758 of *Lecture Notes in Computer Science*, pages 184–199. Springer, 1999. (Cited on page 3.)

[Lys02] Anna Lysyanskaya. *Signature Schemes and Applications to Cryptographic Protocol Design*. PhD thesis, Massachusetts Institute of Technology, 2002. (Cited on page 3.)

[Odl87] Andrew M. Odlyzko, editor. *Advances in Cryptology - CRYPTO '86, Santa Barbara, California, USA, 1986, Proceedings*, volume 263 of *Lecture Notes in Computer Science*. Springer, 1987. (Cited on pages 14 and 15.)

[OO90] Tatsuaki Okamoto and Kazuo Ohta. How to Utilize the Randomness of Zero-Knowledge Proofs. In Alfred Menezes and Scott A. Vanstone, editors, *CRYPTO*, volume 537 of *Lecture Notes in Computer Science*, pages 456–475. Springer, 1990. (Cited on page 3.)

[SBWP03] Ron Steinfeld, Laurence Bull, Huaxiong Wang, and Josef Pieprzyk. Universal Designated-Verifier Signatures. In Chi-Sung Laih, editor, *ASIACRYPT*, volume 2894 of *Lecture Notes in Computer Science*, pages 523–542. Springer, 2003. (Cited on page 3.)

[Sha84] Adi Shamir. Identity-Based Cryptosystems and Signature Schemes. In *CRYPTO*, pages 47–53, 1984. (Cited on page 4.)

[Wat05] Brent Waters. Efficient Identity-Based Encryption Without Random Oracles. In Ronald Cramer, editor, *EUROCRYPT*, volume 3494 of *Lecture Notes in Computer Science*, pages 114–127. Springer, 2005. (Cited on page 9.)

A The GQ Identification Scheme

```
$\mathsf{GQ.KeyGen}(k)$
    $(N, e, d) \leftarrow \mathsf{Gen}_{\mathrm{RSA}}(k)$
    $x \xleftarrow{\$} \mathbb{Z}_N^*, X \xleftarrow{N} x^e$
    $pk_{\mathsf{GQ}} \leftarrow (N, e, X)$
    $sk_{\mathsf{GQ}} \leftarrow (N, x)$
    $(pk_{\mathsf{GQ}}, sk_{\mathsf{GQ}}) \hookleftarrow$
```

```
$[\mathsf{GQ.P}(sk_{\mathsf{GQ}}) \leftrightarrow \mathsf{GQ.V}](pk_{\mathsf{GQ}})$
    $St_{\mathsf{P}} \leftarrow (sk_{\mathsf{GQ}}, pk_{\mathsf{GQ}})$
    $St_{\mathsf{V}} \leftarrow pk_{\mathsf{GQ}}$

$\mathsf{GQ.P}(\varepsilon, St_{\mathsf{P}})$
    $y \xleftarrow{\$} \mathbb{Z}_N^*, Y \xleftarrow{N} y^e$
    $St_{\mathsf{P}} \leftarrow (sk_{\mathsf{GQ}}, y)$
    $(Y, St_{\mathsf{P}}) \hookleftarrow$
                                $\xrightarrow{Y}$
                                                    $\mathsf{GQ.V}(Y, St_{\mathsf{V}})$
                                                        $c \xleftarrow{\$} \{0,1\}^{\ell(k)}$
                                                        $St_{\mathsf{V}} \leftarrow (pk_{\mathsf{GQ}}, Y, c)$
                                                        $(c, St_{\mathsf{V}}) \hookleftarrow$
                                $\xleftarrow{c}$
$\mathsf{GQ.P}(c, St_{\mathsf{P}})$
    $z \xleftarrow{N} y \cdot x^c$
    $z \hookleftarrow$
                                $\xrightarrow{z}$
                                                    $\mathsf{GQ.V}(z, St_{\mathsf{V}})$
                                                        $d \leftarrow \left(z^e \overset{N}{=} Y \cdot X^c\right)$
                                                        $d \hookleftarrow$
```

B Definition of Security against Impersonation

The widely accepted formal security notion for identification schemes is security against impersonation under passive, active, and concurrent attacks. We rephrase the definition of [BP02] for security under concurrent attacks here.

Definition 5 *For an adversary* A_{ID} *and an identification scheme* ID*, the following experiment is defined:*

```
$\mathsf{Expt}^{\text{IMP-CA}}_{\mathsf{ID}}(\mathsf{A}_{\mathsf{ID}}, k)$
    $(pk_{\mathsf{ID}}, sk_{\mathsf{ID}}) \leftarrow \mathsf{ID.K}(k)$
    $(St_{\mathsf{A}_{\mathsf{ID}}}) \leftarrow \mathsf{A}_{\mathsf{ID}}.\hat{\mathsf{V}}^{\mathcal{Interact}(\cdot,\cdot)}(k, pk)$
    $b \leftarrow \left[\mathsf{A}_{\mathsf{ID}}.\hat{\mathsf{P}}(St_{\mathsf{A}_{\mathsf{ID}}}) \leftrightarrow \mathsf{ID.V}\right](pk)$
    $b \hookleftarrow$
```

```
$\mathcal{Interact}(sid, M_{\mathrm{in}})$
    If $sid$ new
        Then $St_{sid} \leftarrow (pk_{\mathsf{ID}}, sk_{\mathsf{ID}})$
    $(M_{\mathrm{out}}, St_{sid}) \leftarrow \mathsf{P}(M_{\mathrm{in}}, St_{sid})$
    $M_{\mathrm{out}} \hookleftarrow$
```

The advantage *of* A_{ID} *in a* IMP-CA *attack on* ID *and the* IMP-CA insecurity *of* ID *are respectively defined as:*

$$\mathrm{Adv}^{\text{IMP-CA}}_{\mathsf{ID},\mathsf{A}_{\mathsf{ID}}}(k) \triangleq \Pr\left[\mathsf{Expt}^{\text{IMP-CA}}_{\mathsf{ID},\mathsf{A}_{\mathsf{ID}}}(k) = 1\right] \quad \textit{and} \quad \mathrm{Insec}^{\text{IMP-CA}}_{\mathsf{ID}}(k) \triangleq \max_{\mathsf{A}_{\mathsf{ID}} \in \mathcal{Poly}(k)} \left[\mathrm{Adv}^{\text{IMP-CA}}_{\mathsf{ID},\mathsf{A}_{\mathsf{ID}}}(k)\right] .$$

ID *is said to be* IMP-CA-secure *if* $\mathrm{Insec}_{\mathsf{ID}}^{\text{IMP-CA}}(k)$ *is negligible in* k.

C The RSA-FDH Signature Scheme

The scheme assumes oracle access to a *full-domain hash* function $H : \{0,1\}^* \to \mathbb{Z}_N^*$, where $N = pq$ is an RSA modulus.

```
RSA-FDH.KeyGen $(k)$
    $(N, e, d) \leftarrow \mathsf{Gen}_{\mathsf{RSA}}(k)$
    $pk \leftarrow (N, e)$
    $sk \leftarrow (N, d)$
    $(pk, sk)$ ↲

RSA-FDH.Sign $(sk, m)$
    $\sigma \overset{N}{\leftarrow} [H(m)]^d$
    $\sigma$ ↲

RSA-FDH.Verify $(pk, m, \sigma)$
    $b \leftarrow \left(\sigma^e \overset{N}{=} H(m)\right)$
    $b$ ↲
```

Here, $\mathsf{Gen}_{\mathsf{RSA}}$ is an RSA modulus generator, which produces an RSA modulus N and two values e and d such that $e \cdot d = 1 \mod \varphi(N)$, where φ is the Euler function.

D Proof of Theorem 1

Proof. We construct an OWE-ID-CCA adversary $\mathsf{A}_{\mathsf{IBE}}$ attacking IBE from a COP-IMP-CA adversary $\mathsf{A} = \mathsf{A}.\left(\hat{\mathsf{P}}, \hat{\mathsf{V}}\right)$ attacking $\mathsf{IBE\text{-}COP}$ and show that $\mathsf{A}_{\mathsf{IBE}}$ is able to mount a successful attack if A succeeds.

In the first phase of the OWE-ID-CCA attack, $\mathsf{A}_{\mathsf{IBE}}$ is given the public parameters of IBE and oracle access to the extraction and decryption oracles. At the end of this phase, $\mathsf{A}_{\mathsf{IBE}}$ is expected to decide on the identity it is going to attack. $\mathsf{A}_{\mathsf{IBE}}$ does this running A as a subroutine.

$\mathsf{A}_{\mathsf{IBE}}$ first runs $\mathsf{A}.\hat{\mathsf{V}}$ on the public parameters given to it as input. While running, $\mathsf{A}.\hat{\mathsf{V}}$ will make two kinds of requests: signing oracle queries and requests to interact with a clone of honest prover holding a signature on a message of $\mathsf{A}.\hat{\mathsf{V}}$'s choice. $\mathsf{A}_{\mathsf{IBE}}$ answers the signing oracle queries using the extraction oracle provided to it, as signing in $\mathsf{IBE\text{-}COP}$ is in correspondence with extraction in IBE.

When $\mathsf{A}.\hat{\mathsf{V}}$ asks to have an interaction with a signature holder clone on a message m_i, $\mathsf{A}_{\mathsf{IBE}}$ sets $ID_i \leftarrow m_i$ and waits for the first message of interaction. $\mathsf{A}.\hat{\mathsf{V}}$ will send an encrypted challenge and expect to receive the correct decryption. $\mathsf{A}_{\mathsf{IBE}}$ answers to the challenge C_i using its decryption oracle, i.e. queries (ID_i, C_i) to the decryption oracle and relays the oracle response back to $\mathsf{A}.\hat{\mathsf{V}}$. This way, $\mathsf{A}.\hat{\mathsf{V}}$ will receive what it expects, i.e. the decryption of C_i.

After $\mathsf{A}.\hat{\mathsf{V}}$ has gathered enough information to be able to impersonate, it decides on a target message $\dot{m}$, declaring that it wants to impersonate a prover holding a signature on the message $\dot{m}$. $\mathsf{A}_{\mathsf{IBE}}$ now sets $\dot{ID} \leftarrow \dot{m}$, outputs $\dot{ID}$ as the target identity it wishes to attack, and declares that the first phase of the OWE-ID-CCA attack is over.

In the second phase of the OWE-ID-CCA attack, $\mathsf{A}_{\mathsf{IBE}}$ is given a challenge ciphertext C and oracle access to the extraction and decryption oracles and is expected to be able to decrypt the challenge. To do so, $\mathsf{A}_{\mathsf{IBE}}$ runs $\mathsf{A}.\hat{\mathsf{P}}$ in the second phase of the (simulated) COP-IMP-CA attack. At this stage, the successful $\mathsf{A}.\hat{\mathsf{P}}$ is supposed to be able to impersonate, i.e. to be able to properly respond to a challenge given to it. $\mathsf{A}_{\mathsf{IBE}}$ simply sends the challenge ciphertext C to $\mathsf{A}.\hat{\mathsf{P}}$ and outputs the obtained response R. If $\mathsf{A}.\hat{\mathsf{P}}$ is successful in impersonation, this response must be the correct decryption of C, which in turn means that $\mathsf{A}_{\mathsf{IBE}}$ will be successful in the OWE-ID-CCA attack.

$\mathsf{A}_{\mathsf{IBE}}$ does not query the decryption oracle in the second phase of the attack, hence there is no $\mathcal{D}ec_2\left(\dot{ID}, C\right)$ query. Besides, it only queries the extraction oracle when A asks a sugning oracle query. Therefore, it can be easily seen that the success probability of $\mathsf{A}_{\mathsf{IBE}}$ is equal to that of A. Furthermore, the running times of $\mathsf{A}_{\mathsf{IBE}}$ and A are equal. Hence, $\mathsf{A}_{\mathsf{IBE}}$ is also poly-time and we have:

$$\mathrm{Adv}_{\mathsf{IBE},\mathsf{A}_{\mathsf{IBE}}}^{\text{OWE-ID-CCA}}(k) = \mathrm{Adv}_{\mathsf{IBE\text{-}COP},\mathsf{A}}^{\text{COP-IMP-CA}}(k) \quad .$$

Denoting the COP-IMP-CA adversary achieving the highest advantage by A^* and the corresponding OWE-ID-CCA adversary constructed from A^* by $\mathsf{A}_{\mathsf{IBE}}^*$ we get

$$\mathrm{Insec}_{\mathsf{IBE\text{-}COP}}^{\text{COP-IMP-CA}}(k) = \mathrm{Adv}_{\mathsf{IBE\text{-}COP},\mathsf{A}^*}^{\text{COP-IMP-CA}}(k) = \mathrm{Adv}_{\mathsf{IBE},\mathsf{A}_{\mathsf{IBE}}^*}^{\text{OWE-ID-CCA}}(k) \leq \mathrm{Insec}_{\mathsf{IBE}}^{\text{OWE-ID-CCA}}(k) \quad ,$$

which completes the proof. □

E Proof of Theorem 3

Proof. We prove that if a successful COP-IMP-CA adversary A for $\mathsf{RSA\text{-}COP}$ exists, then, in the random oracle model, a successful IMP-CA (in the sense of [BP02]) adversary A_{GQ} for GQ can be constructed. Description of such a construction follows.

Our assumption, i.e. the existence of a successful COP-IMP-CA adversary A for $\mathsf{RSA\text{-}COP}$, means that there exists a pair of algorithms $\mathsf{A} = \mathsf{A}.\left(\hat{\mathsf{V}}, \hat{\mathsf{P}}\right)$, which is able to carry out a successful COP-IMP-CA attack on $\mathsf{RSA\text{-}COP}$ protocol. A_{GQ} uses these algorithms to mount an IMP-CA attack on GQ. Besides, working in the random oracle model implies that A_{GQ} must also simulate hash oracle query responses.

In the first phase of the IMP-CA attack, A_{GQ} is given pk_{GQ} and can request to interact concurrently with different *clones* of honest prover $\mathsf{GQ.P}$. In the second phase, A_{GQ} is supposed to play the role of a prover and convince an honest verifier$\mathsf{GQ.V}$ in an interaction.

To answer new hash oracle queries, A_{GQ} follows the well-known Coron's method [Cor00], i.e. to answer the ith new query m_i, it picks a random value r_i from $\mathbb{Z}_N^*$ and answers with hash value $r_i^e \bmod N$ with probability p_0 and with hash value $X \cdot r_i^e \bmod N$ with probability $(1 - p_0)$. In the former case we say X is *not* embedded in the hash of m_i and in the latter case we say X *is* embedded in the hash of m_i. Note that p_0 is a fixed probability which will be determined later, X is a value obtained from parsing pk_{GQ}, and all repeated queries will be answered the same as was answered before.

In the first phase of the attack, A_{GQ} must play the role of a cheating verifier $\mathsf{A}_{\mathsf{GQ}}.\hat{\mathsf{V}}$ to extract needed information out of concurrent interactions with clones of honest GQ prover. A_{GQ} does this using the cheating verifier $\mathsf{A}.\hat{\mathsf{V}}$ as a subroutine. Given the public key $pk_{\mathsf{GQ}} = (N, e, X)$, A_{GQ} runs $\mathsf{A}.\hat{\mathsf{V}}$ on input $pk = (N, e)$. $\mathsf{A}.\hat{\mathsf{V}}$ will then adaptively make two kinds of requests: requests to have $\mathsf{RSA\text{-}FDH}$ signature on an arbitrary message ($\mathcal{S}ign$ oracle queries) and requests to interact concurrently with clones of $\mathsf{RSA\text{-}COP}$ prover. We describe bellow how to properly respond to these requests ($\mathcal{I}nteract$ oracle queries).

On a $\mathcal{S}ign$ oracle query m_i, A_{GQ} again follows Coron's method, i.e. is only able to answer the queries, in the hash of which X is not embedded, with simulated signature r_i (because $\sigma = [H(m_i)]^d = \left(r_i^e\right)^d = r_i \bmod N$) . Otherwise, i.e. if X is embedded in the hash of m_i, A_{GQ} will not be able to answer the query and fails as a result.

On an $\mathcal{I}nteract$ oracle query (m, sid, M_{in}), A_{GQ} simulates the interaction as follows. First, it queries the hash oracle on m, and then, distinguishes the following two cases:

1. If X is not embedded in the hash of m (i.e. $H(m) = r^e \bmod N$), A_{GQ} has an easy work ahead. The signature on m is r (because $\sigma = [H(m)]^d = (r^e)^d = r \bmod N$). So A_{GQ} can play the role of a prover in possession of the signature by just running the algorithm $\mathsf{RSA\text{-}COP.P}$.

2. On the other hand, if X is embedded in the hash of m (i.e. $H(m) = X \cdot r^e \bmod N$), A_{GQ} uses its ability to request interaction with $\mathsf{GQ.P}$ to simulate the interaction with an honest $\mathsf{RSA\text{-}COP}$ prover, as follows. If (m, sid) is new (i.e. $\mathsf{A}.\hat{\mathsf{V}}$ is asking for the clone to begin the interaction), A_{GQ} issues an interaction query $(\varepsilon, m||sid)$ to its GQ interaction oracle and receives a Y as response. It simply outputs Y as the response to $\mathsf{A}.\hat{\mathsf{V}}$'s query. On the other hand, if (m, sid) is not new (i.e. $\mathsf{A}.\hat{\mathsf{V}}$ is asking for the clone to respond to a challenge $c = M_{\text{in}}$), A_{GQ} issues an interaction query $(M_{\text{in}}, m||sid)$ to its GQ interaction oracle and receives a z as response, such that

   $$z^e = Y \cdot X^c \mod N \ .$$

   A_{GQ} then outputs $\zeta \leftarrow r_i^c \cdot z \bmod N$ as the response to $\mathsf{A}.\hat{\mathsf{V}}$'s query. Using the above equation and considering the fact that $H(m) = X \cdot r^e \bmod N$ we will have:

   $$\zeta^e = r^{ce} \cdot z^e = r^{ce} \cdot Y \cdot X^c = Y \cdot (X \cdot r^e)^c = Y \cdot [H(m)]^c \mod N \ ,$$

   which means that ζ is the convincing response with respect to the commitment Y given previously to $\mathsf{A}.\hat{\mathsf{V}}$ by the clone with ID (m, sid) and the challenge $c = M_{\text{in}}$ received from $\mathsf{A}.\hat{\mathsf{V}}$. This, in turn means that A_{GQ} has simulated the interaction for $\mathsf{A}.\hat{\mathsf{V}}$ correctly.

A_{GQ} continues to simulate the responses to the signing and interaction requests of $\mathsf{A}.\hat{\mathsf{V}}$ as above until at some point $\mathsf{A}.\hat{\mathsf{V}}$ halts and outputs a pair $(\dot{m}, St_{\mathsf{A}})$. Similar to what Coron had in [Cor00], here A_{GQ} will be able to impersonate the GQ prover in the next phase if X is embedded in the hash value of $\dot{m}$ and fails otherwise.

In the second phase, A_{GQ} must play the role of a GQ prover and convince an honest GQ verifier that it knows the GQ secret key. To achieve this goal, A_{GQ} uses $\mathsf{A}.\hat{\mathsf{P}}$ as a subroutine. A_{GQ} runs $\mathsf{A}.\hat{\mathsf{P}}$ on input St_{A}, simulating $\mathsf{A}.\hat{\mathsf{P}}$'s signing and interaction oracle queries as in phase one. At some point, $\mathsf{A}.\hat{\mathsf{P}}$ outputs a commitment Y. A_{GQ} simply sends Y as the first message to the honest verifier. The honest verifier then chooses a challenge c and sends it back. A_{GQ} relays this c as challenge to $\mathsf{A}.\hat{\mathsf{P}}$. Then $\mathsf{A}.\hat{\mathsf{P}}$ will output a ζ such that:

$$\zeta^e = Y \cdot [H(\dot{m})]^c \mod N \ .$$

A_{GQ} calculates $z \leftarrow \zeta / \dot{r}^c \bmod N$ and sends it to the honest verifier as the final message. Considering that X is embedded in the hash value of $\dot{m}$ (i.e. $H(\dot{m}) = X \cdot \dot{r}^e \bmod N$), We have:

$$z^e = \frac{\zeta^e}{\dot{r}^{ce}} = \frac{Y \cdot [H(\dot{m})]^c}{\dot{r}^{ce}} = \frac{Y \cdot (X^c \cdot \dot{r}^{ce})}{\dot{r}^{ce}} = Y \cdot X^c \mod N \ ,$$

which means that the honest verifier will be convinced with the response z. Hence, whenever $\mathsf{A}.\hat{\mathsf{V}}$ selects an $\dot{m}$, in hash of which X is embedded, A_{GQ} will be able to impersonate.

It can be easily seen that if A is a poly-time algorithm, then so is A_{GQ}. In fact, A_{GQ}'s running time is equal to that of A plus at most an exponentiation for each hash, sign, and interaction query. Moreover, a similar analysis to [Cor00] for calculating the success probability of the constructed adversary can be carried out as follows. A_{GQ} succeeds if A never asks a sign oracle query on a message in the hash of which X is embedded, chooses the target message $\dot{m}$ such that in the hash of it X is embedded, and succeeds in impersonating a COP prover. The first condition happens with probability at least $p_0^{q_s}$, where q_s is the total number of issued credentials (which is in turn bigger that the total number of signing oracle queries). The second condition is met with probability at least $(1 - p_0)$, which in turn leads us to the equation:

$$\mathrm{Adv}^{\text{IMP-CA}}_{\mathsf{GQ},\mathsf{A}_{\mathsf{GQ}}}(k) \geq p_0^{q_s} \cdot (1 - p_0) \cdot \mathrm{Adv}^{\text{COP-IMP-CA}}_{\mathsf{RSA\text{-}COP},\mathsf{A}}(k) \ .$$

The optimum p_0 which maximizes the success probability of A_{GQ} is then calculated as

$$p_0^* = 1 - \frac{1}{q_s + 1} \quad ,$$

which in turn yields the following equation:

$$\mathrm{Adv}_{\mathsf{GQ},\mathsf{A}_{\mathsf{GQ}}}^{\text{IMP-CA}}(k) \geq \frac{1}{q_s} \cdot \left(1 - \frac{1}{q_s + 1}\right)^{q_s+1} \cdot \mathrm{Adv}_{\mathsf{RSA\text{-}COP},\mathsf{A}}^{\text{COP-IMP-CA}}(k) \quad .$$

Considering the fact that

$$\frac{q_s}{\left(1 - \frac{1}{q_s+1}\right)^{q_s+1}} = O(q_s) \quad ,$$

we will obtain:

$$\mathrm{Adv}_{\mathsf{RSA\text{-}COP},\mathsf{A}}^{\text{COP-IMP-CA}}(k) \leq O(q_s) \cdot \mathrm{Adv}_{\mathsf{GQ},\mathsf{A}_{\mathsf{GQ}}}^{\text{IMP-CA}}(k) \quad .$$

We have shown that for any COP adversary A, a GQ adversary A_{GQ} exists, such that the above equation holds. Denoting the COP adversary with the highest advantage by A^* and the corresponding constructed GQ adversary by $\mathsf{A}_{\mathsf{GQ}}^*$ we get

$$\mathrm{Insec}_{\mathsf{RSA\text{-}COP}}^{\text{COP-IMP-CA}}(k) = \mathrm{Adv}_{\mathsf{RSA\text{-}COP},\mathsf{A}^*}^{\text{COP-IMP-CA}}(k) \leq O(q_s) \cdot \mathrm{Adv}_{\mathsf{GQ},\mathsf{A}_{\mathsf{GQ}}^*}^{\text{IMP-CA}}(k) \leq O(q_s) \cdot \mathrm{Insec}_{\mathsf{GQ}}^{\text{IMP-CA}}(k) \quad ,$$

which proves the claimed bound. □