A previous version of this paper is to be published in ProvSec 2009 Proceedings. This is the full version.

Anonymous Signatures Revisited

Vishal Saraswat and Aaram Yun[⋆]

University of Minnesota — Twin Cities
{vishal,aaram}@cs.umn.edu

September 2009

Abstract. We revisit the notion of the anonymous signature, first formalized by Yang, Wong, Deng and Wang [12], and then further developed by Fischlin [6] and Zhang and Imai [13]. We present a new formalism of anonymous signature, where instead of the message, a part of the signature is withheld to maintain anonymity. We introduce the notion *unpretendability* to guarantee infeasibility for someone other than the correct signer to pretend authorship of the message and signature. Our definition retains applicability for all previous applications of the anonymous signature, provides stronger security, and is conceptually simpler. We give a generic construction from any ordinary signature scheme, and also show that the short signature scheme by Boneh and Boyen [4] can be naturally regarded as such a secure anonymous signature scheme according to our formalism.

Keywords: anonymous signature, signature, anonymity, unpretendability, commitment, Boneh-Boyen signature scheme

1 Introduction

An anonymous signature is a signature scheme where the signature σ of a message m does not reveal the identity of the signer. Yang et al. [12] discussed the usefulness of anonymous signatures in many applications where anonymity is needed, including key exchange protocols, auction systems, and anonymous paper reviewing.

The notion of the anonymous signature was formalized much later than that of the anonymous encryption. Bellare et al. [1] had already defined in Asiacrypt 2001 key-privacy, or anonymity of an encryption scheme, as indistinguishability of ciphertexts encrypted by different public keys, that is, an eavesdropper cannot obtain any information about the recipient (corresponding to the public key) from the ciphertext. However, one problem for introducing the idea of anonymity to digital signatures is that a signature is publicly verifiable;

[⋆] The second author is supported in part by the US National Science Foundation (grant no. CCF 0621462).

if there are only a few candidate signers, the adversary of anonymity can simply try verification of the message-signature pair with respect to all candidate public keys to break anonymity. Therefore, as long as the adversary obtains both the message and the signature, it seems that anonymity is impossible.

Yang et al. resolved the paradox by guaranteeing the anonymity only when the adversary obtains the signature and not the message, or when there is some randomness in the message not revealed to the adversary. In fact, there are many applications where not revealing the complete message is justifiable; for example, in the key transport example given by Yang et al., Bob already knows what Alice's message should be from previous communication, so Alice may send only the anonymous signature without the message, and this authenticates Alice while protecting Alice's anonymity from eavesdroppers. In the case of an auction, a bidder may append some random string r to a message m, which is his bid, and sign it. After the auction ends, only the winner may reveal the randomness r and thus his identity, and the other participants remain anonymous.

This idea of hidden randomness in the message is used by Fischlin [6] to propose an elegant generic transform for anonymous signatures out of ordinary signatures, by applying the idea of randomness extractor to extract the hidden randomness and use it for anonymizing the signature. Fischlin's formulation of anonymous signatures is slightly different, but essentially captures the same idea as that of Yang et al. Also in [13], Zhang and Imai suggested the notion of 'strong anonymous signatures', where they considered the case when there is not much uncertainty in the message.

1.1 Limits of the previous formalism

We revisit the formal definition of anonymous signature and show that previous formalisms of anonymous signature are not completely satisfactory in that, they fail to capture the intuition fully, and actually are inconsistent with some of the suggested applications. Also, we claim that a slightly different formalism captures the intuition better, retains the applicability, more consistently models the application scenarios, enables simpler constructions, and gives better security guarantee.

As explained, in the current formalism, the signer anonymity is based on hidden residual randomness of the message. As long as there is enough such randomness, the signer maintains anonymity, but of course the signature cannot be verified. Eventually the randomness in message is revealed explicitly or implicitly, and whoever has the complete message-signature pair can verify the signature.

In order to model this, Yang et al. and Fischlin formalize that each signer, having public key pk, has certain message distribution $\mathcal{M}(pk)$. Then, two key pairs (pk_0, sk_0), (pk_1, sk_1) are chosen and pk_0 and pk_1 are given to the adversary. Also, a message m is chosen from $\mathcal{M}(pk_b)$ with respect to a random bit

$b \in \{0,1\}$, and the signature $\sigma = \mathrm{Sig}(sk_b, m)$ is computed and given to the adversary. If the adversary cannot guess the random bit b with probability not much greater than $1/2$, then the signature scheme is considered anonymous.

But this formalism is not completely satisfactory in some aspects. First, this is in fact *inconsistent* to the suggested application of anonymous auction, or anonymous paper review. In these cases, if m is the original intended message, then the signer adds some random string r to form appended message $m\|r$, and releases the message m, together with the signature σ of the appended message $m\|r$. From the point of view of an eavesdropper, different original message m gives different message distribution of the whole appended message $m\|r$; the message distribution cannot be a function of only the public key pk, and in fact also depends on the partially revealed portion (m) of the message.

Second, this definition does not formally give a guarantee of infeasibility for someone other than the correct signer to come later and pretend that the signature is his. We call this property *unpretendability*. For an ordinary signature for which complete message-signature pair is released at once, this problem may be less crucial; the pair is publicly verifiable and the authorship can be attributed to the signer. But for an anonymous signature, where only a part of the message-signature pair is released initially, there is theoretical possibility that someone other than the signer may come and claim the authorship of the message and signature. For example, in the anonymous paper review example, the author A of a paper $paper_A$ picks a random string r, computes $\sigma \leftarrow \mathrm{Sig}(sk_A, paper_A\|r)$, and releases $(paper_A, \sigma)$ initially, and only later reveals r when the paper is accepted. Now, if the anonymous signature is not unpretendable, then another author, B, may be able to compute r' satisfying $\mathrm{Vf}(pk_B, paper_A\|r', \sigma) = \mathsf{true}$ and use such an r' to claim authorship of $paper_A$.

Hence, we argue that this unpretendability should be an essential feature of an anonymous signature; otherwise anonymous signature is in fact not applicable for quite a few of originally proposed applications.

Note that we are not claiming that any of the actual schemes proposed in previous papers fails to satisfy unpretendability. But, still this notion should be formally defined and guaranteed for each anonymous scheme. In fact, later we will give an example of an unforgeable signature scheme which provides complete anonymity but is not at all unpretendable. This means that, unpretendability does not follow directly from unforgeability and/or anonymity, and warrants separate definition.

Third, we feel that the idea of a signature of an unknown message is somewhat counter-intuitive. Intuitively, a signature is a proof of authorship for a given document. If we do not know the document in question, or if we are not sure whether the document ends with 'Therefore you should . . . ,' or 'Therefore you should not . . . ,' then the meaning of a signature for such uncertain document is at least debatable.

1.2 Our formalism

Discarding hidden randomness in the message. For these reasons, we propose a new definition of anonymous signatures as follows: first, instead of relying on the hidden residual randomness of the message, we introduce hidden randomness to the signature. Second, we formalize not only the notion of anonymity, but also give explicit formalization of unpretendability.

In traditional digital signatures, signature generation is considered as a randomized algorithm in general, therefore this strategy of explicit randomness is applicable no matter how much entropy (or lack thereof) the distribution of the message has.

This enables us to disregard the randomness in the message altogether, and use the provided randomness directly to anonymize the public key. In fact, even when there is enough entropy in the message distribution, often the randomness is not diffused in the whole message but well-separated from the rest of the message and controllable by the signer. For example, in the bidding example where the bidder appends some random string r to the message m and then sign the appended message $m \| r$, certainly the distribution of this appended message has enough entropy which can be extracted back, but we feel this is artificial; the original message was m, and intuitively, the signer is not really interested in protecting the integrity of r, which is not part of his message m which he *really* wanted to sign. Hence, it is more natural to regard this r as a part of the signature, instead of regarding this as a part of the message which needs to be signed and protected.

Surfacing the verification token. Therefore, in our formalism, we split a digital signature $\tilde{\sigma}$ into two parts, $\tilde{\sigma} = (\sigma, \tau)$. We call τ a *verification token*, or a token in short. Then σ, the rest of $\tilde{\sigma}$, is now just called a *signature*. The signature σ and the token τ are computed by the signature generation algorithm which takes the signer's secret key and the message m as inputs, and when m, σ, and τ are presented, then anyone can verify the validity of the signature using the public key of the signer. But as long as τ is hidden, the adversary cannot break the anonymity of the signer just from the message m and the signature σ. Meanwhile, anyone to whom the token τ (along with the identity of the signer) is revealed may verify the signature.

Note that our formalism is just a specialization of the traditional formalism of digital signature, and not something incompatible; (σ, τ) together serves as a signature which is publicly verifiable, and unforgeable according to the usual definition. We only enforce our signature to have this special format, and to have anonymity and unpretendability in addition to the unforgeability.

In short, we surfaced the hidden randomness of the anonymous signature explicit as the verification token, and moved it from the message to the signature itself. Also we identified and formalized the unpretendability as another property an anonymous signature should have.

Enhanced notion of security. Not only separating the randomness extraction from the anonymous signature results in a conceptually cleaner formalism, but also it enables us to guarantee better notion of security. Because in previous formalisms the verification token was 'diffused' in the message itself, the adversary of anonymity could not choose the challenge message by himself, and a random challenge message had to be chosen out of some message distribution. But in our formalism, there is no problem for the adversary to adaptively choose the challenge message by himself, and indeed we give this stronger notion of anonymity, which all of our schemes meet.

Our contribution. In this paper, we give a new formalism for an anonymous signature following the outline given in the introduction. Also, we present some examples of efficient anonymous signature schemes. We first give a generic construction out of any ordinary unforgeable signature scheme and a commitment scheme. Also, we show that the short signature scheme by Boneh and Boyen [4] can be naturally regarded as such a secure anonymous signature scheme according to our formalism with essentially no modification.

2 Related work

The notion of anonymous signature was first formalized by Yang et al. in [12], and explored further by Fischlin in [6]. Our work revisits this notion, and provides an alternative formalism.

Zhang and Imai [13] proposed a very similar approach as ours. Their idea is to define 'strong anonymous signature', which maintains anonymity even when there is not much uncertainty in the message distribution. Though their definition of strong anonymity is essentially the same as our anonymity, they do not discuss unpretendability, which we argue as central to the notion of anonymous signatures.

Independently from us, Bellare and Duan also presented [2] a formalism of anonymous signatures similar to ours, but with somewhat stronger notions of unforgeability and unpretendability (their 'unambiguity'). They also gave a through investigation of random oracle based anonymous signature schemes, starting from a commitment-based generic transform.

There are pre-existing security notions closely related to unpretendability; Menezes and Smart [9] studied security against the key substitution attack for signature schemes, where an adversary produces a public key (and the corresponding secret key, in their formulation) to claim the ownership of a message-signature pair generated by someone else. Also Hu et al. [8] introduced key replacement attack, which is the similar notion in context of certificateless signatures.

Galbraith and Mao [7] introduced the notion of anonymity to undeniable and confirmer signatures. Our definition of anonymity of an anonymous signature is similar to theirs, and also the fact that the signer has to provide the verification token later to let others verify the signature looks similar to the case of undeniable signatures. But an anonymous signature is not an undeniable signature; anyone who obtained the token of the signature can in fact let others verify the signature, without involvement of the signer. In general, an anonymous signature is much simpler than an anonymous undeniable signature.

Also, there are notions of anonymity in group and ring signatures, but these are anonymity within the group or ring in question, on the other hand the anonymous signature in our formalism or in previous formalism is essentially a conventional signature scheme with some additional properties.

3 Definitions

3.1 Notations and conventions

We denote by $v \leftarrow A(x, y, z, \ldots)$ the operation of running a randomized algorithm $A(x, y, z, \ldots)$ and storing the output to the variable v. If X is a set, then $v \overset{\text{R}}{\leftarrow} X$ denotes the operation of choosing an element v of X according to the uniform random distribution on X. Unless stated otherwise, all algorithms in this paper are probabilistic algorithms.

3.2 Anonymous signature

We define an *anonymous signature* Σ as a triple of algorithms $\Sigma = (\mathrm{Gen}, \mathrm{Sig}, \mathrm{Vf})$, where the key generation algorithm $\mathrm{Gen}()$ outputs a key pair $(pk, sk) \leftarrow \mathrm{Gen}()$, signature generation algorithm $\mathrm{Sig}()$ outputs a pair of a signature and a verification token $\tilde{\sigma} = (\sigma, \tau) \leftarrow \mathrm{Sig}(sk, m)$ with respect to the secret key sk and a message $m \in \{0,1\}^*$, and the deterministic, signature verification algorithm $\mathrm{Vf}(pk, m, \sigma, \tau)$ outputs true or false.

For consistency, we require the following:

$$\mathrm{Vf}(pk, m, \mathrm{Sig}(sk, m)) = \mathsf{true},$$

for $(pk, sk) \leftarrow \mathrm{Gen}()$, and for any $m \in \{0,1\}^*$.

3.3 Unforgeability

For an anonymous signature scheme $\Sigma = (\mathrm{Gen}, \mathrm{Sig}, \mathrm{Vf})$ and an adversary $\mathcal{A}$, we define the *unforgeability* advantage of $\mathcal{A}$ with respect to Σ as

$$\mathbf{Adv}_{\Sigma}^{\mathsf{uf\text{-}cma}}(\mathcal{A}) \overset{\text{def}}{=} \mathbf{Pr}\left[\mathbf{Expr}_{\Sigma}^{\mathsf{uf\text{-}cma}}(\mathcal{A}) = \mathsf{true}\right]$$

in the following experiment:

```
Experiment $\mathbf{Expr}_{\Sigma}^{\mathsf{uf\text{-}cma}}(\mathcal{A})$
    $(pk, sk) \leftarrow \mathrm{Gen}()$
    $(m^*, \sigma^*, \tau^*) \leftarrow \mathcal{A}^{\mathrm{Sig}(sk,\cdot)}(pk)$
    return $\mathrm{Vf}(pk, m^*, \sigma^*, \tau^*)$
```

where the adversary $\mathcal{A}$ has access to the signing oracle $\mathrm{Sig}(sk,\cdot)$ with respect to the secret key *sk* with the requirement that $\mathcal{A}$ is not allowed to query the signing oracle with m^*.

Similarly, we define *strong unforgeability* advantage of $\mathcal{A}$ as

$$\mathbf{Adv}_{\Sigma}^{\mathsf{suf\text{-}cma}}(\mathcal{A}) \overset{\text{def}}{=} \mathbf{Pr}\left[\mathbf{Expr}_{\Sigma}^{\mathsf{suf\text{-}cma}}(\mathcal{A}) = \mathsf{true}\right]$$

in the experiment $\mathbf{Expr}_{\Sigma}^{\mathsf{suf\text{-}cma}}(\mathcal{A})$, which is identical to $\mathbf{Expr}_{\Sigma}^{\mathsf{uf\text{-}cma}}(\mathcal{A})$, except that we require $\mathcal{A}$ not to have received (σ^*, τ^*) as an answer to any query of form m^* to the signing oracle.

Remark 1. In this definition and in the following ones, we define only the advantage of an adversary in a security experiment, and would not explicitly define the security notion itself. Informally, Σ is unforgeable if for any efficient adversary $\mathcal{A}$, the advantage $\mathbf{Adv}_{\Sigma}^{\mathsf{uf\text{-}cma}}(\mathcal{A})$ is negligible. But unlike in the asymptotic setting, there is no clear-cut definition of 'efficient' or 'negligible' and it depends on particular applications.

3.4 Anonymity

Consider an adversary which is a pair of algorithms $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$. Let *st* be the state information which $\mathcal{A}_1$ passes to $\mathcal{A}_2$. We define the *anonymity* advantage of $\mathcal{A}$ with respect to Σ as

$$\mathbf{Adv}_{\Sigma}^{\mathsf{anon}}(\mathcal{A}) \overset{\text{def}}{=} \left|\mathbf{Pr}[\mathbf{Expr}_{\Sigma}^{\mathsf{anon\text{-}1}}(\mathcal{A}) = 1] - \mathbf{Pr}[\mathbf{Expr}_{\Sigma}^{\mathsf{anon\text{-}0}}(\mathcal{A}) = 1]\right|,$$

where experiments $\mathbf{Expr}_{\Sigma}^{\mathsf{anon\text{-}}b}(\mathcal{A})$ $(b = 0, 1)$ are defined as follows:

```
Experiment $\mathbf{Expr}_{\Sigma}^{\mathsf{anon\text{-}}b}(\mathcal{A})$
    $(pk_0, sk_0) \leftarrow \mathrm{Gen}();\ (pk_1, sk_1) \leftarrow \mathrm{Gen}()$
    $(m^*, st) \leftarrow \mathcal{A}_1^{\mathrm{Sig}(sk_0,\cdot),\mathrm{Sig}(sk_1,\cdot)}(pk_0, pk_1)$
    $(\sigma^*, \tau^*) \leftarrow \mathrm{Sig}(sk_b, m^*)$
    $b' \leftarrow \mathcal{A}_2^{\mathrm{Sig}(sk_0,\cdot),\mathrm{Sig}(sk_1,\cdot)}(\sigma^*, st)$
    return $b'$
```

We call Σ anonymous with respect to *full key exposure*, when the advantage of any adversary is still negligible even if the adversary also gets the secret keys sk_0, sk_1 as additional input. We denote by $\mathbf{Adv}_{\Sigma}^{\mathsf{anon\text{-}fke}}(\mathcal{A})$ the advantage of an adversary in the anonymity experiment with full key exposure.

3.5 Unpretendability

For any adversary $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$, we define the *unpretendability* advantage of $\mathcal{A}$ with respect to Σ as

$$\mathbf{Adv}_{\Sigma}^{\mathsf{up}}(\mathcal{A}) \stackrel{\text{def}}{=} \mathbf{Pr}\left[\mathbf{Expr}_{\Sigma}^{\mathsf{up}}(\mathcal{A}) = \mathsf{true}\right]$$

in the experiment $\mathbf{Expr}_{\Sigma}^{\mathsf{up}}(\mathcal{A})$ in Figure 1.

Intuitively, the adversary is trying to claim the authorship of (m^*, σ^*), which is signed by the target secret key sk^*. The adversary tries to produce an appropriate τ so that the signature is verified with his own public key pk, which could be freshly chosen, and the definition guarantees that the success probability for this attempt is negligible.

Also, we define a weaker version of unpretendability: for any adversary $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2, \mathcal{A}_3)$, we define the *weak unpretendability* advantage of $\mathcal{A}$ with respect to Σ as

$$\mathbf{Adv}_{\Sigma}^{\mathsf{wup}}(\mathcal{A}) \stackrel{\text{def}}{=} \mathbf{Pr}\left[\mathbf{Expr}_{\Sigma}^{\mathsf{wup}}(\mathcal{A}) = \mathsf{true}\right]$$

in the experiment $\mathbf{Expr}_{\Sigma}^{\mathsf{wup}}(\mathcal{A})$ in Figure 1.

The difference between the unpretendability and the weak unpretendability is that, in the unpretendability, the adversary is allowed to choose his public key adaptively, but that is not allowed in the case of weak unpretendability. The notion of weak unpretendability is applicable for example in situations where there is trustable PKI under which every party registers his public key to his identity, possibly timestamped and with proof of secret key possession; in such cases the adversary cannot adaptively choose his public key after seeing the signature, and claim the ownership under the fresh key/identity. Many applications like anonymous paper review or anonymous auction could fall into this category, but this depends on how the public keys are managed. The unpretendability is stronger in that the adversary cannot claim the ownership of the signature even when he is allowed to freshly create a new public key.

Like the case of anonymity, we say that Σ is (weakly) unpretendable with respect to full key exposure, when the advantage of any adversary is still negligible even if the adversary also gets the target secret key sk^* as additional input. We denote the advantage of an adversary in the (weak) unpretendability experiment with full key exposure by $(\mathbf{Adv}_{\Sigma}^{\mathsf{wup\text{-}fke}}(\mathcal{A}))$ $\mathbf{Adv}_{\Sigma}^{\mathsf{up\text{-}fke}}(\mathcal{A})$.

3.6 Security of an anonymous signature

Suppose that $\Sigma = (\mathrm{Gen}, \mathrm{Sig}, \mathrm{Vf})$ is an anonymous signature scheme. We say that Σ is a *secure* anonymous signature, if Σ is unforgeable, anonymous, and at least weakly unpretendable.

We emphasize that the unpretendability is a crucial property that an anonymous signature should have. Already we showed that if an anonymous signature is not unpretendable, then it cannot be used for some of the suggested

```
Experiment $\mathbf{Expr}^{\mathsf{up}}_{\Sigma}(\mathcal{A})$
    $(pk^*, sk^*) \leftarrow \mathrm{Gen}()$
    $(m^*, st) \leftarrow \mathcal{A}_1^{\mathrm{Sig}(sk^*,\cdot)}(pk^*)$
    $(\sigma^*, \tau^*) \leftarrow \mathrm{Sig}(sk^*, m^*)$
    $(\tau, pk) \leftarrow \mathcal{A}_2^{\mathrm{Sig}(sk^*,\cdot)}(\sigma^*, \tau^*, st)$
    return $\mathrm{Vf}(pk, m^*, \sigma^*, \tau) \wedge (pk \neq pk^*)$
```

```
Experiment $\mathbf{Expr}^{\mathsf{wup}}_{\Sigma}(\mathcal{A})$
    $(pk, st) \leftarrow \mathcal{A}_1()$
    $(pk^*, sk^*) \leftarrow \mathrm{Gen}()$
    $(m^*, st') \leftarrow \mathcal{A}_2^{\mathrm{Sig}(sk^*,\cdot)}(pk^*, st)$
    $(\sigma^*, \tau^*) \leftarrow \mathrm{Sig}(sk^*, m^*)$
    $\tau \leftarrow \mathcal{A}_3^{\mathrm{Sig}(sk^*,\cdot)}(\sigma^*, \tau^*, st')$
    return $\mathrm{Vf}(pk, m^*, \sigma^*, \tau)$
```

Fig. 1. Experiments $\mathbf{Expr}^{\mathsf{up}}_{\Sigma}(\mathcal{A})$ and $\mathbf{Expr}^{\mathsf{wup}}_{\Sigma}(\mathcal{A})$

applications like anonymous paper review. Here, we show an example of an anonymous signature which is unforgeable, anonymous, but not weakly unpretendable.

Suppose $\Sigma = (\mathrm{Gen}, \mathrm{Sig}, \mathrm{Vf})$ is an ordinary unforgeable signature scheme. We then construct an anonymous signature scheme $\Sigma' = (\mathrm{Gen}', \mathrm{Sig}', \mathrm{Vf}')$ as follows: $\mathrm{Gen}'()$ is the same as $\mathrm{Gen}()$. $\mathrm{Sig}'(sk, m)$ is defined as

$$\mathrm{Sig}'(sk, m) = (\sigma, \tau) \stackrel{\mathrm{def}}{=} (\mathrm{Sig}(sk, m) \oplus \tau, \tau)$$

where the verification token τ is a bitstring of the same bit-length as the signature $\mathrm{Sig}(sk, m)$ and is chosen uniform randomly. Finally, $\mathrm{Vf}'(sk, m, \sigma, \tau)$ is defined as

$$\mathrm{Vf}'(pk, m, \sigma, \tau) \stackrel{\mathrm{def}}{=} \mathrm{Vf}(pk, m, \sigma \oplus \tau).$$

It is clear that the anonymous signature Σ' is both unforgeable and anonymous; because the signature $\mathrm{Sig}(sk, m)$ is masked with random bitstring τ in $\mathrm{Sig}'(sk, m)$, essentially the adversary has no information about the signature. Only later when τ is revealed, the signature σ is revealed and signature can be verified. Thus, this is equivalent to deferring the signing to the last minute when the token τ has to be revealed. Hence the scheme is unforgeable, and unless τ is revealed, the signer anonymity is guaranteed.

But, it is trivial to break unpretendability of this scheme; if $(m^*, \sigma^* = \mathrm{Sig}(sk^*, m^*) \oplus \tau^*)$ is given, then the adversary may compute $\mathrm{Sig}(sk, m^*)$ using his own secret key sk, and compute τ as

$$\tau \stackrel{\mathrm{def}}{=} \mathrm{Sig}(sk, m^*) \oplus \sigma^*.$$

Then,

$$\mathrm{Vf}'(pk, m^*, \sigma^*, \tau) = \mathrm{Vf}(pk, m^*, \sigma^* \oplus \tau) = \mathrm{Vf}(pk, m^*, \mathrm{Sig}(sk, m^*)) = \mathsf{true}.$$

3.7 Commitment schemes

A *commitment scheme* Γ consists of a pair of algorithms $(\mathrm{Com}, \mathrm{CVf})$ satisfying the following:

Correctness: For any message $m \in \{0,1\}^*$, $\mathrm{CVf}(\mathsf{com}, \mathsf{dec}, m) = \mathsf{true}$ holds, whenever $(\mathsf{com}, \mathsf{dec}) \leftarrow \mathrm{Com}(m)$.

Hiding: For any adversary $\mathcal{A}$ which is a pair of algorithms $(\mathcal{A}_1, \mathcal{A}_2)$, the *hiding* advantage with respect to Γ is defined as

$$\mathbf{Adv}_{\Gamma}^{\mathsf{hide}}(\mathcal{A}) \overset{\text{def}}{=} \left|\mathbf{Pr}[\mathbf{Expr}_{\Gamma}^{\mathsf{hide}\text{-}1}(\mathcal{A}) = 1] - \mathbf{Pr}[\mathbf{Expr}_{\Gamma}^{\mathsf{hide}\text{-}0}(\mathcal{A}) = 1]\right|$$

where experiments $\mathbf{Expr}_{\Gamma}^{\mathsf{hide}\text{-}b}(\mathcal{A})$ $(b = 0, 1)$ are defined in Figure 2. Also, we require the adversary $\mathcal{A}$ to output m_0, m_1 of the same length.

Binding: For any adversary $\mathcal{A}$, the *binding* advantage with respect to Γ is defined as

$$\mathbf{Adv}_{\Gamma}^{\mathsf{bind}}(\mathcal{A}) \overset{\text{def}}{=} \mathbf{Pr}\left[\mathbf{Expr}_{\Gamma}^{\mathsf{bind}}(\mathcal{A}) = \mathsf{true}\right]$$

in the experiment $\mathbf{Expr}_{\Gamma}^{\mathsf{bind}}(\mathcal{A})$ in Figure 2.

```
Experiment $\mathbf{Expr}_{\Gamma}^{\mathsf{hide}\text{-}b}(\mathcal{A})$
    $(m_0, m_1, st) \leftarrow \mathcal{A}_1()$
    $(\mathsf{com}, \mathsf{dec}) \leftarrow \mathrm{Com}(m_b)$
    $b' \leftarrow \mathcal{A}_2(\mathsf{com}, st)$
    return $b'$
```

```
Experiment $\mathbf{Expr}_{\Gamma}^{\mathsf{bind}}(\mathcal{A})$
    $(\mathsf{com}, \mathsf{dec}, m, \mathsf{dec}', m') \leftarrow \mathcal{A}()$
    $p \leftarrow \mathrm{CVf}(\mathsf{com}, \mathsf{dec}, m)$
    $p' \leftarrow \mathrm{CVf}(\mathsf{com}, \mathsf{dec}', m')$
    return $p \wedge p' \wedge (m \neq m')$
```

Fig. 2. Experiments $\mathbf{Expr}_{\Gamma}^{\mathsf{hide}\text{-}b}(\mathcal{A})$ and $\mathbf{Expr}_{\Gamma}^{\mathsf{bind}}(\mathcal{A})$

3.8 'Unique' commitment schemes

In order to construct a strongly unforgeable anonymous signature from a strongly unforgeable signature, we define a commitment scheme with a special property, which we call *uniqueness*.

A *'unique' commitment scheme* Γ consists of a pair of algorithms $(\mathrm{Prep}, \mathrm{Com}, \mathrm{CVf})$ satisfying the following:

Correctness: For any message $m \in \{0,1\}^*$, $\mathrm{CVf}(\mathsf{com}, \omega, \mathsf{dec}, m) = \mathsf{true}$ holds, whenever $(\omega, \rho) \leftarrow \mathrm{Prep}()$ and $(\mathsf{com}, \mathsf{dec}) \leftarrow \mathrm{Com}(m, \rho)$.

Hiding: For any adversary $\mathcal{A}$ which is a pair of algorithms $(\mathcal{A}_1, \mathcal{A}_2)$, the hiding advantage with respect to Γ is defined as

$$\mathbf{Adv}_{\Gamma}^{\mathsf{hide}}(\mathcal{A}) \overset{\text{def}}{=} \left|\mathbf{Pr}[\mathbf{Expr}_{\Gamma}^{\mathsf{hide}\text{-}1}(\mathcal{A}) = 1] - \mathbf{Pr}[\mathbf{Expr}_{\Gamma}^{\mathsf{hide}\text{-}0}(\mathcal{A}) = 1]\right|$$

where experiments $\mathbf{Expr}_{\Gamma}^{\mathsf{hide}\text{-}b}(\mathcal{A})$ $(b = 0, 1)$ are defined in Figure 3. Also, we require the adversary $\mathcal{A}$ to output m_0, m_1 of the same length.

```
Experiment $\mathbf{Expr}_{\Gamma}^{\mathsf{hide}\text{-}b}(\mathcal{A})$
    $(\omega, \rho) \leftarrow \mathrm{Prep}()$
    $(m_0, m_1, st) \leftarrow \mathcal{A}_1(\omega)$
    $(\mathsf{com}, \mathsf{dec}) \leftarrow \mathrm{Com}(m_b, \rho)$
    $b' \leftarrow \mathcal{A}_2(\mathsf{com}, st)$
    return $b'$
```

```
Experiment $\mathbf{Expr}_{\Gamma}^{\mathsf{bind}}(\mathcal{A})$
    $(\mathsf{com}, \omega, \mathsf{dec}, m, \mathsf{dec}', m') \leftarrow \mathcal{A}()$
    $p \leftarrow \mathrm{CVf}(\mathsf{com}, \omega, \mathsf{dec}, m)$
    $p' \leftarrow \mathrm{CVf}(\mathsf{com}, \omega, \mathsf{dec}', m')$
    return $p \wedge p' \wedge (m \neq m')$
```

Fig. 3. Experiments $\mathbf{Expr}_{\Gamma}^{\mathsf{hide}\text{-}b}(\mathcal{A})$ and $\mathbf{Expr}_{\Gamma}^{\mathsf{bind}}(\mathcal{A})$

Binding: For any adversary $\mathcal{A}$, the binding advantage with respect to Γ is defined as

$$\mathbf{Adv}_{\Gamma}^{\mathsf{bind}}(\mathcal{A}) \overset{\text{def}}{=} \mathbf{Pr}\left[\mathbf{Expr}_{\Gamma}^{\mathsf{bind}}(\mathcal{A}) = \mathsf{true}\right]$$

in the experiment $\mathbf{Expr}_{\Gamma}^{\mathsf{bind}}(\mathcal{A})$ in Figure 3.

Uniqueness: For any adversary $\mathcal{A}$, the uniqueness advantage with respect to Γ is defined as

$$\mathbf{Adv}_{\Gamma}^{\mathsf{uniq}}(\mathcal{A}) \overset{\text{def}}{=} \mathbf{Pr}\left[\mathbf{Expr}_{\Gamma}^{\mathsf{uniq}}(\mathcal{A}) = \mathsf{true}\right]$$

in the following experiment:

```
Experiment $\mathbf{Expr}_{\Gamma}^{\mathsf{uniq}}(\mathcal{A})$
    $(\omega, m, \mathsf{com}, \mathsf{com}', \mathsf{dec}, \mathsf{dec}') \leftarrow \mathcal{A}()$
    $p \leftarrow \mathrm{CVf}(\mathsf{com}, \omega, \mathsf{dec}, m)$
    $p' \leftarrow \mathrm{CVf}(\mathsf{com}', \omega, \mathsf{dec}', m)$
    return $p \wedge p' \wedge (\mathsf{com}, \mathsf{dec}) \neq (\mathsf{com}', \mathsf{dec}')$
```

Intuitively, before each commitment, a 'help string' ω is chosen, and the commitment and the decommitment processes are controlled by ω. The committer sends (com, ω), and the hiding property holds even if the messages are chosen with the knowledge of ω. Finally, the uniqueness says that given ω and m, computationally there should be at most one way to create a valid commitment and decommitment with respect to (ω, m).

A unique commitment scheme can be trivially built in the random oracle model: in order to commit a message m, pick a random bitstring r, compute $\omega \leftarrow H(r)$, and define $(\mathsf{com}, \mathsf{dec}) \overset{\text{def}}{=} (H(r, \omega, m), r)$. The decommitment can be done by revealing r and m.

In the standard model, one way to construct a unique commitment scheme is to use the standard Blum-Micali construction [3]: given a one-way permutation π and its hard-core bit b, in order to commit a k-bit message m, we pick a random string ρ and compute $\omega \leftarrow \pi^{k+1}(\rho)$, and define

$$(\mathsf{com}, \mathsf{dec}) \overset{\text{def}}{=} (b(\pi^k(\rho)) \| b(\pi^{k-1}(\rho)) \| \cdots \| b(\pi^2(\rho)) \| b(\pi(\rho)) \oplus m, \rho).$$

It is well known that $\omega \| b(\pi^k(\rho)) \| b(\pi^{k-1}(\rho)) \| \cdots \| b(\pi^2(\rho)) \| b(\pi(\rho))$ itself is computationally indistinguishable from a uniform random bitstring, so for any message m, which might have been chosen with knowledge of $\omega = \pi^{k+1}(\rho)$, the commitment com is computationally indistinguishable from a uniform random bitstring, from which follows the hiding property. Also, in order to decommit to a different value, one has to find $\rho' \neq \rho$ with $\omega = \pi^{k+1}(\rho) = \pi^{k+1}(\rho')$, but since π is a permutation, it is not possible. Hence the binding property holds perfectly. Also, ω uniquely determines ρ, therefore given any ω and m, $(\mathsf{com}, \mathsf{dec})$ is unique.

Using stronger assumptions, we may construct more efficient schemes. For example, one can use decisional Diffie-Hellman assumption or its hashed variants: let $\mathbb{G}$ be a cyclic group of order p, and let g be a random generator of $\mathbb{G}$ and h a random element of $\mathbb{G}$. If the decisional Diffie-Hellman assumption holds, then (g, h, g^r, h^r) for a random $r \overset{\text{R}}{\leftarrow} \mathbb{Z}_p$ and (g, h, g^r, k) for a uniformly and independently chosen $k \overset{\text{R}}{\leftarrow} \mathbb{G}$ are indistinguishable. Then $\omega \overset{\text{def}}{=} h^r$, $(\mathsf{com}, \mathsf{dec}) \overset{\text{def}}{=} (m \cdot g^r, r)$ satisfies the required properties, for any message $m \in \mathbb{G}$.

4 Secure anonymous signature schemes

In this section, first we show how to construct an anonymous signature scheme generically from any ordinary unforgeable signature scheme. Then, we show that the short signature scheme of Boneh and Boyen [4] can be naturally considered as a secure anonymous signature according to our formalism, with essentially no modification. To be precise, it is a weakly unpretendable anonymous signature.

4.1 Generic construction from an unforgeable signature

Here we present a generic construction of an anonymous signature scheme using an ordinary signature scheme and a commitment scheme. It is required that the signature scheme is unforgeable, and the public key size and the signature size are the same for all users.

Let $\Sigma = (\mathrm{Gen}, \mathrm{Sig}, \mathrm{Vf})$ be a signature scheme, and let $\Gamma = (\mathrm{Com}, \mathrm{CVf})$ be a commitment scheme. We construct an anonymous signature $\Sigma' = (\mathrm{Gen}', \mathrm{Sig}', \mathrm{Vf}')$ using these as follows:

```
function $\mathrm{Gen}'()$
    $(pk, sk) \leftarrow \mathrm{Gen}()$
    $pk' \leftarrow pk$
    $sk' \leftarrow sk \| pk$
    return $(pk', sk')$

function $\mathrm{Vf}'(pk', m, \sigma, \tau)$
    Parse $\tau$ as $\tau_1 \| \tau_2$
    return $\mathrm{CVf}(\sigma, \tau_1, pk' \| \tau_2) \wedge \mathrm{Vf}(pk', m, \tau_2)$

function $\mathrm{Sig}'(sk', m)$
    Parse $sk'$ as $sk \| pk$
    $\sigma' \leftarrow \mathrm{Sig}(sk, m)$
    $(\mathsf{com}, \mathsf{dec}) \leftarrow \mathrm{Com}(pk \| \sigma')$
    $\sigma \leftarrow \mathsf{com}$; $\tau \leftarrow \mathsf{dec} \| \sigma'$
    return $(\sigma, \tau)$
```

Theorem 1. *Given an ordinary signature scheme Σ, consider the scheme Σ' defined in the above. If Σ is unforgeable, then Σ' is a secure unforgeable anonymous signature. Moreover, Σ' is both anonymous and unpretendable with respect to full key exposure.*

Proof. First, we prove the unforgeability of Σ'.

Suppose that $\mathcal{A}$ is an adversary attacking the unforgeability of Σ'. Then using $\mathcal{A}$, we construct an adversary $\mathcal{B}$ which attacks the unforgeability of Σ, and satisfying

$$\mathbf{Adv}_{\Sigma'}^{\text{uf-cma}}(\mathcal{A}) \leq \mathbf{Adv}_{\Sigma}^{\text{uf-cma}}(\mathcal{B}).$$

The adversary $\mathcal{B}$ is given a public key pk of Σ, and the corresponding signing oracle $\mathrm{Sig}(sk, \cdot)$. $\mathcal{B}$ sets $pk' = pk$, and gives it to $\mathcal{A}$ and answers the signing query of $\mathcal{A}$ as follows: for signing query of m, $\mathcal{B}$ calls its own signing oracle with query m to obtain σ', computes $(\mathsf{com}, \mathsf{dec}) \leftarrow \mathrm{Com}(pk, \sigma')$ and returns $(\sigma = \mathsf{com}, \tau = \mathsf{dec} \| \sigma')$ to $\mathcal{A}$. Note that this simulation of the unforgeability experiment for $\mathcal{A}$ by $\mathcal{B}$ is perfectly done according to the description of Σ'.

Suppose that $\mathcal{A}$ halts with output (m^*, σ^*, τ^*). Then $\mathcal{B}$ parses τ^* as $\tau_1 \| \tau_2$, and halts with output (m^*, τ_2).

Whenever the output (m^*, σ^*, τ^*) of $\mathcal{A}$ is a successful forgery for Σ', then $\mathcal{B}$ outputs a successful forgery (m^*, τ_2) for Σ since from the definition of Vf', $\mathrm{Vf}'(pk', m^*, \sigma^*, \tau^*) = \mathsf{true}$ holds only if $\mathrm{Vf}(pk, m^*, \tau_2) = \mathsf{true}$ holds. This proves the claimed inequality.

Also, the time complexity of $\mathcal{B}$ is essentially at most that of $\mathcal{A}$ plus $q \cdot T_c(l_p + l_s)$, where q is the number of signature queries $\mathcal{A}$ makes, $T_c(l)$ is the time complexity for committing a bitstring of length l, and l_p and l_s are lengths of public keys and signatures of Σ, respectively. $\mathcal{B}$ also makes at most q signature queries.

Next, we show that Σ' satisfies anonymity with respect to full key exposure. Suppose that $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$ is an adversary attacking anonymity of Σ'. Using $\mathcal{A}$, we construct $\mathcal{B}$ attacking the hiding property of the commitment scheme Γ, satisfying

$$\mathbf{Adv}_{\Sigma'}^{\text{anon-fke}}(\mathcal{A}) \leq \mathbf{Adv}_{\Gamma}^{\text{hide}}(\mathcal{B}).$$

Also, $\mathcal{B}$ has essentially the same time complexity as that of $\mathcal{A}$.

Consider the experiment $\mathbf{Expr}_{\Gamma}^{\text{hide-}b}(\mathcal{B})$ with respect to this adversary $\mathcal{B}$. $\mathcal{B}$ generates two key pairs (pk'_0, sk'_0) and (pk'_1, sk'_1). $\mathcal{B}$ then runs $\mathcal{A}_1(pk'_0, pk'_1, sk'_0, sk'_1)$

to obtain an output (m^*, st) and gives $s_0 = pk_0 \| \mathrm{Sig}(sk_0, m^*)$ and $s_1 = pk_1 \| \mathrm{Sig}(sk_1, m^*)$ to the challenger. The challenger computes $(\mathsf{com}, \mathsf{dec}) \leftarrow \mathsf{Com}(s_b)$, and gives $\sigma^* = \mathsf{com}$ to $\mathcal{B}$. $\mathcal{B}$ now runs $\mathcal{A}_2(\sigma^*, st)$ to obtain an output b' and then halts with output b'.

Note that this simulation of the full-key exposure anonymity experiment for $\mathcal{A}$ by $\mathcal{B}$ is perfect, and the output of $\mathcal{B}$ is the same as the output of $\mathcal{A}$. Hence, $\mathbf{Pr}[\mathbf{Expr}_{\Gamma}^{\mathsf{hide}\text{-}b}(\mathcal{B})] = \mathbf{Pr}[\mathbf{Expr}_{\Sigma'}^{\mathsf{anon}\text{-}\mathsf{fke}\text{-}b}(\mathcal{A})]$, for $b = 0, 1$. Therefore,

$$\begin{aligned}
\mathbf{Adv}_{\Sigma'}^{\mathsf{anon}\text{-}\mathsf{fke}}(\mathcal{A}) &= \left|\mathbf{Pr}[\mathbf{Expr}_{\Sigma'}^{\mathsf{anon}\text{-}\mathsf{fke}\text{-}1}(\mathcal{A}) = 1] - \mathbf{Pr}[\mathbf{Expr}_{\Sigma'}^{\mathsf{anon}\text{-}\mathsf{fke}\text{-}0}(\mathcal{A}) = 1]\right| \\
&= \left|\mathbf{Pr}[\mathbf{Expr}_{\Gamma}^{\mathsf{hide}\text{-}1}(\mathcal{B}) = 1] - \mathbf{Pr}[\mathbf{Expr}_{\Gamma}^{\mathsf{hide}\text{-}0}(\mathcal{B}) = 1]\right| \\
&= \mathbf{Adv}_{\Gamma}^{\mathsf{hide}}(\mathcal{B}).
\end{aligned}$$

Finally, we show that Σ' satisfies unpretendability with respect to full key exposure. Suppose that $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$ is an adversary attacking unpretendability of Σ'. Using $\mathcal{A}$, we construct an adversary $\mathcal{B}$ attacking the binding property of the commitment scheme Γ, satisfying

$$\mathbf{Adv}_{\Sigma'}^{\mathsf{up}\text{-}\mathsf{fke}}(\mathcal{A}) \le \mathbf{Adv}_{\Gamma}^{\mathsf{bind}}(\mathcal{B}).$$

Also, $\mathcal{B}$ has time complexity essentially the same as $\mathcal{A}$.

$\mathcal{B}$ generates a key pair (pk'^*, sk'^*), and runs $\mathcal{A}_1(pk'^*, sk'^*)$ to obtain an output (m^*, st). $\mathcal{B}$ then computes $(\sigma^*, \tau^*) \leftarrow \mathrm{Sig}'(sk'^*, m^*)$, and runs $\mathcal{A}_2(\sigma^*, \tau^*, st)$ to obtain an output (τ, pk'). Then $\mathcal{B}$ parses τ as $\tau_1 \| \tau_2$ and τ^* as $\tau_1^* \| \tau_2^*$ and halts with output $(\sigma^*, \tau_1^*, pk'^* \| \tau_2^*, \tau_1, pk' \| \tau_2)$. This simulation of the full-key exposure unpretendability experiment for $\mathcal{A}$ by $\mathcal{B}$ is perfect.

We claim that, in the above simulation, whenever $\mathcal{A}$ succeeds at breaking the unpretendability of Σ', that is, $\mathrm{Vf}'(pk', m^*, \sigma^*, \tau) = \mathsf{true}$ and $pk' \neq pk'^*$, then $\mathcal{B}$ also succeeds in breaking the binding property of Γ. From the definition of Vf', in order that $\mathrm{Vf}'(pk', m^*, \sigma^*, \tau) = \mathsf{true}$, it is necessary that $\mathrm{CVf}(\sigma^*, \tau_1, pk' \| \tau_2)$ is also true. Moreover, since $(\sigma^*, \tau^*) = \mathrm{Sig}'(sk'^*, m^*)$, also $\mathrm{Vf}'(pk'^*, m^*, \sigma^*, \tau^*) = \mathsf{true}$ holds, and from this it follows that $\mathrm{CVf}(\sigma^*, \tau_1^*, pk'^* \| \tau_2^*) = \mathsf{true}$. Now, $pk'^* \neq pk'$ so that $pk'^* \| \tau_2^* \neq pk' \| \tau_2$ and hence $\mathcal{B}$ has successfully violated the binding property of Γ. □

4.2 Generic construction from a strongly unforgeable signature

If the underlying signature scheme Σ is strongly unforgeable, we may construct a strongly unforgeable anonymous signature generically from Σ. However, in contrast to the case of an unforgeable signature, we could not find an efficient, generic construction using any secure commitment scheme. Instead, we show a generic construction using any *unique* commitment scheme, which was defined in Section 3.8. Similarly as before, it is required that the signature scheme is strongly unforgeable, and the public key size and the signature size are the same for all users.

Let $\Sigma = (\mathrm{Gen}, \mathrm{Sig}, \mathrm{Vf})$ be a signature scheme, and let $\Gamma = (\mathrm{Prep}, \mathrm{Com}, \mathrm{CVf})$ be a unique commitment scheme. We construct an anonymous signature $\Sigma' = (\mathrm{Gen}', \mathrm{Sig}', \mathrm{Vf}')$ using these as follows:

```
function $\mathrm{Gen}'()$
    $(pk, sk) \leftarrow \mathrm{Gen}()$
    $pk' \leftarrow pk$
    $sk' \leftarrow sk \| pk$
    return $(pk', sk')$

function $\mathrm{Vf}'(pk', m, \sigma, \tau)$
    Parse $\sigma$ as $\sigma_1 \| \sigma_2$
    Parse $\tau$ as $\tau_1 \| \tau_2$
    return $\mathrm{CVf}(\sigma_1, \sigma_2, \tau_1, pk' \| \tau_2) \wedge \mathrm{Vf}(pk', m \| \sigma_2, \tau_2)$

function $\mathrm{Sig}'(sk', m)$
    Parse $sk'$ as $sk \| pk$
    $(\omega, \rho) \leftarrow \mathrm{Prep}()$
    $\sigma' \leftarrow \mathrm{Sig}(sk, m \| \omega)$
    $(\mathsf{com}, \mathsf{dec}) \leftarrow \mathrm{Com}(pk \| \sigma', \rho)$
    $\sigma \leftarrow \mathsf{com} \| \omega$; $\tau \leftarrow \mathsf{dec} \| \sigma'$
    return $(\sigma, \tau)$
```

Theorem 2. *Given an ordinary signature scheme Σ, consider the scheme Σ' defined in the above. If Σ is unforgeable, then Σ' is a secure unforgeable anonymous signature. Moreover, Σ' is both anonymous and unpretendable with respect to full key exposure. Also, if Σ is strongly unforgeable, then Σ' is also a secure strongly unforgeable anonymous signature.*

Proof. We only give proof for the case when the underlying signature scheme Σ is strongly unforgeable, because the other case can be proved similarly.

First, let us prove the strong unforgeability of Σ'. Suppose that $\mathcal{A}$ is an adversary attacking strong unforgeability of Σ'. Then using $\mathcal{A}$, we construct an adversary $\mathcal{B}$ which attacks strong unforgeability of Σ, and an adversary $\mathcal{C}$ attacking uniqueness of Γ, and together satisfying

$$\mathbf{Adv}^{\mathsf{suf\text{-}cma}}_{\Sigma'}(\mathcal{A}) \leq \mathbf{Adv}^{\mathsf{suf\text{-}cma}}_{\Sigma}(\mathcal{B}) + \mathbf{Adv}^{\mathsf{uniq}}_{\Gamma}(\mathcal{C}).$$

The adversary $\mathcal{B}$ is given a public key pk of Σ, and the corresponding signing oracle $\mathrm{Sig}(sk, \cdot)$. $\mathcal{B}$ then gives $pk' = pk$ to $\mathcal{A}$. $\mathcal{B}$ keeps an associative array L whose entries are initially all set to $\perp$. And, $\mathcal{B}$ answers the signing query of $\mathcal{A}$ as follows: for signing query for message m, $\mathcal{B}$ computes $(\omega, \rho) \leftarrow \mathrm{Prep}()$, calls its own signing oracle with query $m \| \omega$. When it obtains its answer σ', $\mathcal{B}$ computes $(\mathsf{com}, \mathsf{dec}) \leftarrow \mathrm{Com}(pk \| \sigma', \rho)$, updates $L[(m \| \omega, \sigma')] \leftarrow (\mathsf{com}, \mathsf{dec})$, and returns $(\sigma, \tau) \overset{\mathrm{def}}{=} (\mathsf{com} \| \omega, \mathsf{dec} \| \sigma')$ to $\mathcal{A}$. Note that the simulation is perfectly done according to the description of Σ'.

Suppose that $\mathcal{A}$ halts with output (m^*, σ^*, τ^*). Let $\sigma^* = \sigma_1^* \| \sigma_2^*$ and $\tau^* = \tau_1^* \| \tau_2^*$. $\mathcal{B}$ then checks if $L[(m^* \| \sigma_2^*, \tau_2^*)] = \perp$. If so, then $\mathcal{B}$ halts with output $(m^* \| \sigma_2^*, \tau_2^*)$. If not, then $\mathcal{B}$ aborts.

Now, the description of $\mathcal{C}$ is almost identical to that of $\mathcal{B}$: $\mathcal{C}$ provides the same simulation for $\mathcal{A}$ as $\mathcal{B}$, but up to the step where $\mathcal{A}$ halts with output

(m^*, σ^*, τ^*). The difference between $\mathcal{C}$ and $\mathcal{B}$ is that, since the signing oracle for Σ is not available to $\mathcal{C}$, instead $\mathcal{C}$ generates a key pair (pk, sk), gives pk to $\mathcal{A}$, and answers the signing queries of $\mathcal{A}$ using sk. $\mathcal{C}$ also checks if $L[(m^* \| \sigma_2^*, \tau_2^*)] = \bot$. If so, then $\mathcal{C}$ aborts. If not, then let $(\mathsf{com}, \mathsf{dec}) = L[(m^* \| \sigma_2^*, \tau_2^*)]$. Then $\mathcal{C}$ halts with output $(\sigma_2^*, m^*, \sigma_1^*, \mathsf{com}, \tau_1^*, \mathsf{dec})$.

Suppose that the output (m^*, σ^*, τ^*) of $\mathcal{A}$ is a successful strong forgery for Σ'. Then, from the definition of Σ', we have $\mathrm{CVf}(\sigma_1^*, \sigma_2^*, \tau_1^*, pk \| \tau_2^*) = \mathsf{true}$ and $\mathrm{Vf}(pk, m^* \| \sigma_2^*, \tau_2^*) = \mathsf{true}$. Suppose that in the run of $\mathcal{B}$, at the end $L[(m^* \| \sigma_2^*, \tau_2^*)] = \bot$ happened. This means that $(m^* \| \sigma_2^*, \tau_2^*)$ is a valid strong forgery of Σ, and in that case $\mathcal{B}$ succeeds.

But the probability that $L[(m^* \| \sigma_2^*, \tau_2^*)] = \bot$ happens in the simulation of $\mathcal{B}$ for $\mathcal{A}$ is identical to the probability that the same event happens in the simulation of $\mathcal{C}$ for $\mathcal{A}$, since up to the point $\mathcal{A}$ outputs a forgery attempt, both $\mathcal{B}$ and $\mathcal{C}$ provides the identical, perfect simulation of the original security game.

Now consider the case that the output (m^*, σ^*, τ^*) of $\mathcal{A}$ is a successful strong forgery for Σ' in the simulation of $\mathcal{C}$, and $L[(m^* \| \sigma_2^*, \tau_2^*)] = (\mathsf{com}, \mathsf{dec}) \neq \bot$. This means that, $\mathcal{A}$ has made a signature query for m^*, $\mathcal{C}$ computed $\mathrm{Prep}()$ with output (σ_2^*, ρ) for some ρ, $\mathcal{C}$ queried its own oracle for $m^* \| \sigma_2^*$ to obtain τ_2^*, computed $(\mathsf{com}, \mathsf{dec}) \leftarrow \mathrm{Com}(pk \| \tau_2^*, \rho)$, and returned $(\mathsf{com} \| \sigma_2^*, \mathsf{dec} \| \tau_2^*)$ as the signature-token pair for the message m^*.

From the correctness of commitment, $\mathrm{CVf}(\mathsf{com}, \sigma_2^*, \mathsf{dec}, pk \| \tau_2^*) = \mathsf{true}$. Suppose that $(\mathsf{com}, \mathsf{dec}) = (\sigma_1^*, \tau_1^*)$. Then,

$$(m^*, \sigma^*, \tau^*) = (m^*, \sigma_1^* \| \sigma_2^*, \tau_1^* \| \tau_2^*) = (m^*, \mathsf{com} \| \sigma_2^*, \mathsf{dec} \| \tau_2^*),$$

which contradicts the assumption that (m^*, σ^*, τ^*) is a successful strong forgery for Σ'. Hence, it follows that $(\mathsf{com}, \mathsf{dec}) \neq (\sigma_1^*, \tau_1^*)$. But this means that the output $(\sigma_2^*, m^*, \sigma_1^*, \mathsf{com}, \tau_1^*, \mathsf{dec})$ of $\mathcal{C}$ is a successful attack on uniqueness of Γ. This proves the claimed inequality.

Also, the time complexity of $\mathcal{B}$ is essentially at most that of $\mathcal{A}$ plus $q \cdot (T_c(l_p + l_s) + T_p + T_a(q))$, where q is the number of signature queries $\mathcal{A}$ makes, $T_c(l)$ is the time complexity for committing a bitstring of length l, T_p is the time complexity for computing $\mathrm{Prep}()$, $T_a(q)$ is the time complexity for one operation of associative array of size at most q, and l_p and l_s are lengths of public keys and signatures of Σ, respectively. $\mathcal{B}$ also makes at most q signature queries.

The time complexity of $\mathcal{C}$ is that of $\mathcal{B}$, plus $q \cdot T_s(l_\omega + l_m)$, where $T_s(l)$ is the time complexity for signing one l-bit message, l_ω is the bit length of ω for $(\omega, \rho) \leftarrow \mathrm{Prep}()$, and l_m is the maximum length of messages that $\mathcal{A}$ queries.

Next, we show that Σ' satisfies anonymity with respect to full key exposure. Suppose that $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$ is an adversary attacking anonymity of Σ'. Using $\mathcal{A}$, we construct $\mathcal{B}$ attacking the hiding property of the commitment scheme Γ, satisfying

$$\mathbf{Adv}^{\textsf{anon-fke}}_{\Sigma'}(\mathcal{A}) \leq \mathbf{Adv}^{\textsf{hide}}_{\Gamma}(\mathcal{B}).$$

Also, $\mathcal{B}$ has time complexity essentially the same as $\mathcal{A}$.

Consider the experiment $\mathbf{Expr}^{\textsf{hide-}b}_{\Gamma}(\mathcal{B})$ with respect to this adversary $\mathcal{B}$. The challenger computes $(\omega, \rho) \leftarrow \mathrm{Prep}()$ and runs $\mathcal{B}$ with ω as input. $\mathcal{B}$ generates two key pairs (pk'_0, sk'_0) and (pk'_1, sk'_1). $\mathcal{B}$ then runs $\mathcal{A}_1(pk'_0, pk'_1, sk'_0, sk'_1)$ to obtain an output (m^*, st) and gives $s_0 = pk_0 \| \mathrm{Sig}(sk_0, m^* \| \omega)$ and $s_1 = pk_1 \| \mathrm{Sig}(sk_1, m^* \| \omega)$ to the challenger. The challenger computes $(\mathsf{com}, \mathsf{dec}) \leftarrow \mathrm{Com}(s_b, \rho)$, and gives com to $\mathcal{B}$. $\mathcal{B}$ now runs $\mathcal{A}_2(\mathsf{com} \| \omega, st)$ to obtain an output b' and then halts with output b'.

Note that this simulation of the full-key exposure anonymity experiment for $\mathcal{A}$ by $\mathcal{B}$ is perfect, and the output of $\mathcal{B}$ is the same as the output of $\mathcal{A}$. Hence, $\mathbf{Pr}[\mathbf{Expr}^{\textsf{hide-}b}_{\Gamma}(\mathcal{B})] = \mathbf{Pr}[\mathbf{Expr}^{\textsf{anon-fke-}b}_{\Sigma'}(\mathcal{A})]$, for $b = 0, 1$. Therefore,

$$\begin{aligned}
\mathbf{Adv}^{\textsf{anon-fke}}_{\Sigma'}(\mathcal{A}) &= \left| \mathbf{Pr}[\mathbf{Expr}^{\textsf{anon-fke-1}}_{\Sigma'}(\mathcal{A}) = 1] - \mathbf{Pr}[\mathbf{Expr}^{\textsf{anon-fke-0}}_{\Sigma'}(\mathcal{A}) = 1] \right| \\
&= \left| \mathbf{Pr}[\mathbf{Expr}^{\textsf{hide-1}}_{\Gamma}(\mathcal{B}) = 1] - \mathbf{Pr}[\mathbf{Expr}^{\textsf{hide-0}}_{\Gamma}(\mathcal{B}) = 1] \right| \\
&= \mathbf{Adv}^{\textsf{hide}}_{\Gamma}(\mathcal{B}).
\end{aligned}$$

Finally, we show that Σ' satisfies unpretendability with respect to full key exposure. Suppose that $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$ is an adversary attacking unpretendability of Σ'. Using $\mathcal{A}$, we construct an adversary $\mathcal{B}$ attacking the binding property of the commitment scheme Γ, satisfying

$$\mathbf{Adv}^{\textsf{up-fke}}_{\Sigma'}(\mathcal{A}) \leq \mathbf{Adv}^{\textsf{bind}}_{\Gamma}(\mathcal{B}).$$

Also, $\mathcal{B}$ has essentially the same time complexity as $\mathcal{A}$.

$\mathcal{B}$ generates a key pair $(pk'^*, sk'^*) = (pk^*, sk^* \| pk^*)$, and runs $\mathcal{A}_1(pk'^*, sk'^*)$ to obtain an output (m^*, st). $\mathcal{B}$ then computes $(\omega, \rho) \leftarrow \mathrm{Prep}()$, $\sigma^* \leftarrow \mathrm{Sig}(sk^*, m^* \| \omega)$, $(\mathsf{com}, \mathsf{dec}) \leftarrow \mathrm{Com}(pk^* \| \sigma^*, \rho)$, and then runs $\mathcal{A}_2(\mathsf{com} \| \omega, \mathsf{dec} \| \sigma^*, st)$ to obtain an output $(\tau, pk') = (\tau_1 \| \tau_2, pk)$. Then $\mathcal{B}$ outputs $(\mathsf{com}, \omega, \mathsf{dec}, pk^* \| \sigma^*, \tau_1, pk \| \tau_2)$ and halts. This simulation of the full-key exposure unpretendability experiment for $\mathcal{A}$ by $\mathcal{B}$ is perfect.

We claim that, in the above simulation, whenever $\mathcal{A}$ succeeds at breaking the unpretendability of Σ', that is, $\mathrm{Vf}'(pk, m^*, \mathsf{com} \| \omega, \tau_1 \| \tau_2) = \mathsf{true}$ and $pk \neq pk^*$, then $\mathcal{B}$ also succeeds in breaking the binding property of Γ. From the definition of Vf', in order that $\mathrm{Vf}'(pk, m^*, \mathsf{com} \| \omega, \tau_1 \| \tau_2) = \mathsf{true}$, it is necessary that $\mathrm{CVf}(\mathsf{com}, \omega, \tau_1, pk \| \tau_2) = \mathsf{true}$. Moreover, since $(\mathsf{com}, \mathsf{dec}) = \mathrm{Com}(pk^* \| \sigma^*, \rho)$, also $\mathrm{CVf}(\mathsf{com}, \omega, \mathsf{dec}, pk^* \| \sigma^*) = \mathsf{true}$ holds. Now, $pk^* \neq pk$ so that $pk^* \| \sigma^* \neq pk \| \tau_2$ and hence $\mathcal{B}$ has successfully violated the binding property of Γ. □

Remark 2. If we instantiate the unique commitment scheme using ideas of Section 3.8, the resulting construction would look like

$$(\sigma, \tau) \leftarrow (((pk \| \mathrm{Sig}(sk, m \| H(\tau))) \oplus G(\tau)) \| H(\tau), \tau),$$

where $H(\tau)$ is a collision resistant function, and $G(\tau)$ is a pseudorandom generator which remains pseudorandom when $H(\tau)$ is exposed. (For example, $H(\tau) = \pi^{k+1}(\tau)$, $G(\tau) = b(\pi^k(\tau))\|b(\pi^{k-1}(\tau))\| \cdots \|b(\pi^2(\tau))\|b(\pi(\tau))$, following Blum-Micali construction.) This is similar to the construction given by Zhang and Imai in Section 4.2 of [13]. We note that care is needed for that construction: in our notation, they defined $\mathrm{Sig}'(sk', m, \tau)$ to be $\mathrm{Sig}(sk, m\|\tau) \oplus G(\tau)$. In their construction, it is not sufficient for G to be a pseudorandom generator. This is because $\mathrm{Sig}(sk, m\|\tau)$ and $G(\tau)$ are correlated by the hidden variable τ. In order to prove anonymity of this construction, G has to look pseudorandom even when $\mathrm{Sig}(sk, m\|\tau)$ is exposed: for example, suppose we are given an unforgeable signature $\overline{\mathrm{Sig}}()$. Using this, we construct $\mathrm{Sig}(sk, m\|\tau) \overset{\text{def}}{=} \overline{\mathrm{Sig}}(sk, m\|\tau) \oplus G(\tau)$, i.e., in order to sign a message with length larger than or equal to l_0, which is the length of τ, sign the message and xor it with the output of the pseudorandom generator for the last l_0 bits of the message. In that case, the construction of Zhang and Imai gives $\mathrm{Sig}'(sk', m, \tau) = \mathrm{Sig}(sk, m\|\tau) \oplus G(\tau) = \overline{\mathrm{Sig}}(sk, m\|\tau)$. If $\overline{\mathrm{Sig}}$ leaks information about pk corresponding to sk, then so does Sig'.

Note that in contrast to our construction, they allow G to be different between different users, so this example is not directly applicable. But still G has to be a pseudorandom generator satisfying the stronger property.

4.3 Boneh-Boyen short signature

Here we give a brief description of the Boneh-Boyen signature scheme [4] for completeness.

Parameter generation A bilinear group $(\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T)$ with a pairing $e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$, where $|\mathbb{G}_1| = |\mathbb{G}_2| = |\mathbb{G}_T| = p$ for some prime p, is chosen. The message space is $\mathbb{Z}_p$, which gives no essential problem since the domain can be extended by using a (target) collision resistant hash function.

Key generation Key generation algorithm chooses random generators g_1 and g_2 of $\mathbb{G}_1$ and $\mathbb{G}_2$, respectively, and chooses $x, y \overset{\mathrm{R}}{\leftarrow} \mathbb{Z}_p^*$, computes $u \leftarrow g_2^x \in \mathbb{G}_2$, $v \leftarrow g_2^y \in \mathbb{G}_2$. Then, $pk \overset{\text{def}}{=} (g_1, g_2, u, v)$, and $sk \overset{\text{def}}{=} (g_1, x, y)$.

Signing For a secret key (g_1, x, y) and a message $m \in \mathbb{Z}_p$, the signing algorithm chooses $\tau \overset{\mathrm{R}}{\leftarrow} \mathbb{Z}_p \setminus \{-\frac{x+m}{y}\}$, and computes $\sigma \leftarrow g_1^{1/(x+m+y\tau)} \in \mathbb{G}_1$. Then the signature is the pair (σ, τ).

Verification For a public key (g_1, g_2, u, v), a message m, and a signature (σ, τ), the verification can be done by checking whether $e(\sigma, u \cdot g_2^m \cdot v^\tau) = e(g_1, g_2)$.

4.4 Security of Boneh-Boyen as an anonymous signature

The Boneh-Boyen short signature can be naturally considered as an anonymous signature, by regarding τ in $(\sigma = g_1^{1/(x+m+y\tau)}, \tau)$ as the verification token. To be precise, because τ should not be equal to $-(x+m)/y$ modulo p, we need to make slight modifications both to the signature scheme and to the formalism itself; for example, instead of choosing τ uniformly from $\mathbb{Z}_p \setminus \{-(x+m)/y\}$, τ may be chosen uniformly from $\mathbb{Z}_p$, and instead the signing algorithm may be allowed to fail in the negligible possibility that $\tau = -(x+m)/y$.

Then, the Boneh-Boyen short signature scheme becomes a secure anonymous signature scheme; we show that it is strongly unforgeable, anonymous with full key exposure, and *weakly* unpretendable with full key exposure.

Strong unforgeability Because our definition of strong unforgeability for anonymous signatures is identical to the ordinary definition of strong unforgeability, the proof of Boneh and Boyen for the strong unforgeability of the short signature scheme is directly applicable. Their proof is based on the SDH assumption on bilinear groups $(\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T)$.

Anonymity with full key exposure For a message $m \in \mathbb{Z}_p$ chosen by the adversary, consider the distribution of the signature σ, where $\sigma = g_1^{1/(x+m+y\tau)}$, for uniformly chosen token $\tau \overset{\text{R}}{\leftarrow} \mathbb{Z}_p$, when the secret key (g_1, x, y) is given to the adversary. Then, even conditioned on g_1, x, m, and y, still $1/(x+m+y\tau)$ has uniform distribution on $\mathbb{Z}_p^* \cup \{\perp\}$, and σ has uniform distribution on $(\mathbb{G}_1 \setminus \{1\}) \cup \{\perp\}$. Because this is true for any secret key (g_1, x, y), we conclude that the Boneh-Boyen short signature scheme is anonymous with full key exposure.

Weak unpretendability with full key exposure We prove weak unpretendability of Boneh-Boyen signature with full key exposure, under the following assumption on the bilinear groups $(\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T)$ which we call 'adversarial pairing inversion assumption':

> With respect to any adversarially chosen $h \in \mathbb{G}_T \setminus \{1\}$, it is infeasible to find $X \in \mathbb{G}_2$ satisfying $e(g, X) = h$, for $g \overset{\text{R}}{\leftarrow} \mathbb{G}_1 \setminus \{1\}$.

It is a nonstandard variant of pairing inversion problem; it is known that some versions of pairing inversion problem is as hard as the computational Diffie-Hellman problem [5,11], but here h is allowed to be chosen by the adversary, and it is not known whether this assumption can be derived from more traditional assumptions. Note also that this is an interactive assumption. But, the adversarial choice of h does not seem to allow any obvious attacks, and as a partial justification of the assumption, it can be shown that this assumption holds in generic bilinear groups.

Let $\mathcal{A}$ be an adversary of weak unpretendability of the Boneh-Boyen signature, with key exposure. Using $\mathcal{A}$, we construct the adversary $\mathcal{B}$ of the adversarial pairing inversion problem. $\mathcal{B}$ runs $\mathcal{A}$, which would output its public key

$(g_1, g_2, u, v) \in \mathbb{G}_1 \times \mathbb{G}_2 \times \mathbb{G}_2 \times \mathbb{G}_2$ of $\mathcal{A}$, $\mathcal{B}$ outputs $h \leftarrow e(g_1, g_2)$ as his chosen instance for the adversarial pairing inversion to the challenger.

Then, the challenger sends $\mathcal{B}$ a random $g \overset{\text{R}}{\leftarrow} \mathbb{G}_1 \setminus \{1\}$. $\mathcal{B}$ defines $g_1^* \overset{\text{def}}{=} g$, and randomly chooses $g_2^* \overset{\text{R}}{\leftarrow} \mathbb{G}_2 \setminus \{1\}$, $x^*, y^* \overset{\text{R}}{\leftarrow} \mathbb{Z}_p$, and sends g_1^*, g_2^*, x^*, y^* to $\mathcal{A}$. $\mathcal{A}$ then outputs the challenge message m^*. $\mathcal{B}$ randomly chooses $\tau^* \overset{\text{R}}{\leftarrow} \mathbb{Z}_p$, computes $\sigma^* \leftarrow (g_1^*)^{1/(x^*+m^*+y^*\tau^*)}$, and sends (σ^*, τ^*) to $\mathcal{A}$. $\mathcal{A}$ eventually halts with some τ. Using τ, $\mathcal{B}$ outputs X, where X is defined as

$$X \overset{\text{def}}{=} (u g_2^{m^*} v^{\tau})^{1/(x^*+m^*+y^*\tau^*)}.$$

In the above, $\mathcal{B}$ provides perfect simulation for $\mathcal{A}$. Suppose that the attack of $\mathcal{A}$ is successful: then

$$e(g_1, g_2) = e(\sigma^*, u g_2^{m^*} v^{\tau})$$

holds. Since $\sigma^* = (g_1^*)^{1/(x^*+m^*+y^*\tau^*)} = g^{1/(x^*+m^*+y^*\tau^*)}$, the above equation is equivalent to $e(g, X) = e(g_1, g_2) = h$, which shows that $\mathcal{B}$ solves the pairing inversion, whenever the weak unpretendability attack of $\mathcal{A}$ is successful.

On unpretendability of Boneh-Boyen The Boneh-Boyen signature scheme satisfies weak unpretendability with full key exposure, but it is *not* unpretendable; it is easy to break unpretendability when the adversary is allowed to choose his public key adaptively.

Acknowledgements

We thank anonymous reviewers for many constructive and helpful comments. Especially, we revised notions of the unpretendability, following criticisms on our previous definition. Also, a reviewer suggested possibility of commitment-based generic construction of anonymous signatures. In a previous version of our manuscript on ePrint archive [10], we had presented a pseudorandom generator based construction which was a special case of commitment based construction, but we generalized it based on any commitment scheme, following the reviewer's suggestion.

References

1. Mihir Bellare, Alexandra Boldyreva, Anand Desai, and David Pointcheval. Key-privacy in public-key encryption. In Colin Boyd, editor, *ASIACRYPT*, volume 2248, pages 566–582. Springer, 2001.
2. Mihir Bellare and Shanshan Duan. New definitions and designs for anonymous signatures. Cryptology ePrint Archive, Report 2009/336, 2009.

3. Manuel Blum and Silvio Micali. How to generate cryptographically strong sequences of pseudo-random bits. *SIAM Journal on Computing*, 13(4):850–864, 1984.
4. Dan Boneh and Xavier Boyen. Short signatures without random oracles and the SDH assumption in bilinear groups. *Journal of Cryptology*, 21(2):149–177, 2008.
5. Jung Hee Cheon and Dong Hoon Lee. Diffie-Hellman problems and bilinear maps. Cryptology ePrint Archive, Report 2002/117, 2002.
6. Marc Fischlin. Anonymous signatures made easy. In Tatsuaki Okamoto and Xiaoyun Wang, editors, *Public Key Cryptography*, volume 4450, pages 31–42. Springer, 2007.
7. Steven D. Galbraith and Wenbo Mao. Invisibility and anonymity of undeniable and confirmer signatures. In Marc Joye, editor, *CT-RSA*, volume 2612, pages 80–97. Springer, 2003.
8. Bessie C. Hu, Duncan S. Wong, Zhenfeng Zhang, and Xiaotie Deng. Certificateless signature: a new security model and an improved generic construction. *Designs, Codes and Cryptography*, 42(2):109–126, 2007.
9. Alfred Menezes and Nigel P. Smart. Security of signature schemes in a multi-user setting. *Designs, Codes and Cryptography*, 33(3):261–274, 2004.
10. Vishal Saraswat and Aaram Yun. Anonymous signatures revisited. Cryptology ePrint Archive, Report 2009/307, 2009.
11. Takakazu Satoh. On pairing inversion problems. In Tsuyoshi Takagi, Tatsuaki Okamoto, Eiji Okamoto, and Takeshi Okamoto, editors, *Pairing*, volume 4575, pages 317–328. Springer, 2007.
12. Guomin Yang, Duncan S. Wong, Xiaotie Deng, and Huaxiong Wang. Anonymous signature schemes. In Moti Yung, Yevgeniy Dodis, Aggelos Kiayias, and Tal Malkin, editors, *Public Key Cryptography*, volume 3958, pages 347–363. Springer, 2006.
13. Rui Zhang and Hideki Imai. Strong anonymous signatures. In Moti Yung, Peng Liu, and Dongdai Lin, editors, *Inscrypt*, volume 5487, pages 60–71. Springer, 2008.