Pseudorandom Signatures[⋆]

Nils Fleischhacker[1], Felix Günther[2], Franziskus Kiefer[3], Mark Manulis[3], and Bertram Poettering[4]

[1] Cryptographic Algorithms Group, Saarland University, Germany
fleischhacker@cs.uni-saarland.de
[2] Cryptographic Protocols Group, Technische Universität Darmstadt, Germany
guenther@cs.tu-darmstadt.de
[3] Department of Computing, University of Surrey, United Kingdom
f.kiefer@surrey.ac.uk, mark@manulis.eu
[4] Information Security Group, Royal Holloway, University of London, United Kingdom
bertram.poettering@rhul.ac.uk

Abstract. We develop a three-level hierarchy of privacy notions for (unforgeable) digital signature schemes. We first prove mutual independence of existing notions of anonymity and confidentiality, and then show that these are implied by higher privacy goals. The top notion in our hierarchy is *pseudorandomness*: signatures with this property hide the entire information about the signing process and cannot be recognized as signatures when transmitted over a public network. This implies very strong unlinkability guarantees across different signers and even different signing algorithms, and gives rise to new forms of private public-key authentication.

We show that one way towards pseudorandom signatures leads over our mid-level notion, called *indistinguishability*: such signatures can be simulated using only the public parameters of the scheme. As we reveal, indistinguishable signatures exist in different cryptographic settings (e.g. based on RSA, discrete logarithms, pairings) and can be efficiently lifted to pseudorandomness deploying general transformations using appropriate encoding techniques. We also examine a more direct way for obtaining pseudorandomness for any unforgeable signature scheme. All our transformations work in the standard model. We keep public verifiability of signatures in the setting of system-wide known public keys. Some results even hold if signing keys are disclosed to the adversary — given that signed messages have high entropy.

1 Introduction

A digital signature σ on a message m is generated using a private key sk and is verified in respect to the corresponding public key pk. Digital signatures shall be unforgeable and offer authenticity of signers and integrity of signed messages. In the 90's, however, with the advent of public key infrastructures (PKIs), digital signatures were criticized for being a threat to user's *privacy* [19]. For instance, with system-wide known (PKI-certified) public keys, and due to the public verifiability of signatures, any transmission of (m, σ) over a public network such as the Internet implicitly reveals to all intermediate parties the identity of the signer, i.e. owner of (certified) pk — and not only to the intended recipients/verifiers. Considering public availability of both σ and pk, we can hope to obtain privacy only by restricting the amount of publicly available information about message m. Indeed, messages might be delivered through a different communication channel (e.g. in an online banking scenario with two-factor authentication) or at some earlier or later point in time (e.g. in anonymous auctions), and thus still remain out of reach of the adversary that obtains signatures and public keys. Further on, verifiers might expect signatures on messages that need not be transmitted at all: for example, private outputs computed with secure multi-party computation techniques or in (anonymous) key exchange protocols can be viewed as messages for which parties may wish to exchange signatures.

[⋆] A shortened version of this paper appears in the proceedings of the 8th ACM Symposium on Information, Computer and Communications Security (ASIACCS 2013), May 8–10, 2013, Hangzhou, China. This is the full version.

Current Privacy Notions and Open Issues. Privacy of digital signatures, where signatures σ are revealed but associated messages m are not disclosed, has found attention in definitions and security models of *anonymous signatures* by Yang et al. [28] and Fischlin [17], and in the notion of *confidential signatures* by Dent et al. [16]. These schemes aim at either hiding the identities/public keys of signers (anonymity) or the content of signed messages (confidentiality). Both privacy notions were defined for high-entropy message spaces, which is a necessary requirement, presuming the system-wide knowledge of public keys and signatures. This conceptual similarity raises a question on the possible relationship between anonymity and confidentiality, and triggers interest in a deeper study on the limits of privacy achievable with traditional signature schemes: Are there schemes whose signatures σ hide signer's identity/public key and simultaneously keep signed messages secret? What are the differences between deterministic and probabilistic schemes in terms of these goals? Is the property of 'message recovery' damaging for privacy? Answers to these questions would clarify the relationship among the existing notions of privacy for signature schemes, shed light on their privacy-enabling properties, and possibly pave the way for more sophisticated privacy guarantees. We give answers to many such questions.

Pseudorandom Signatures and Applications. In fact, the most interesting question in respect to privacy of signature schemes is whether signatures can look (to observers) completely random. On the one hand, this property would repel attention of intermediate parties, possibly performing traffic analysis, to the transmission of signatures. Those parties could not learn whether a given datagram represents something potentially valuable (in this case a signature) or not. On the other hand, and more importantly, signatures that cannot be distinguished from random strings (of some fixed length) also hide which signing algorithm its signer was using — this knowledge alone is often sufficient to identify signers (even if the signature scheme itself is anonymous).

We give some examples where signers, or groups of signers, naturally use different parameters settings for (potentially) the same signing algorithm.

For instance, in the new European travel documents, the selection of specific (elliptic curve) parameters is the priority of respective states [9]. Many banks and health insurance companies issue smart cards to their customers, initialized with different signing algorithms and parameters. We observe that distinguishing among different settings, implementations, or instantiations of the same signature scheme S can be seen as a privacy problem, e.g. if signatures can be used to derive which citizenship or which customer relationship to which bank or insurance company the signer has. Now assume that different signature schemes S_1, S_2, ... (unforgeable, possibly under different hardness assumptions or with varying levels of security) output signatures σ_1, σ_2, ..., respectively, of fixed length L. If *all* these signatures looked random to observers, then σ_i would hide the applied scheme S_i, i.e. only the possession of m and (the expected signer's) pk would allow to verify σ_i. In contrast, any other party (even with knowledge of the keys of the whole system) would remain totally clueless whether σ_i represents a signature or not, and, if so, which signing algorithm was used.

Furthermore, pseudorandom signatures give rise to *covert public-key authentication*, offering cryptographic protection to covert channels, i.e. channels that appear random to any entity other than the communication partner (as defined, e.g. in [10, 20, 27]). With pseudorandom signatures, it would be possible to perform public-key authentication and execute authenticated key exchange over covert channels without loosing covertness. For example, parties could first run an unauthenticated key exchange protocol that has random-looking messages (those can easily be constructed using the Diffie-Hellman approach in various groups based on techniques used in our work (cf. Lemma 13)) and then exchange pseudorandom signatures on the protocol transcript and an additional high-entropy confirmation token derived from the established shared key material. Since all exchanged messages are random-looking, the established secure channel between the two mutually authenticated parties would remain covert. Moreover, if pseudorandomness of signatures can be preserved even in the unfortunate case where the signing key sk is leaked, then the above protocol would guarantee 'forward covertness' (akin to forward secrecy, e.g. [13]). More generally, pseudorandom signatures seem to offer very strong and useful privacy guarantees in communication protocols and applications where authentication should remain unobservable by traffic analysis [22].

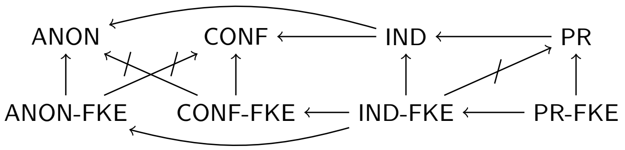

Fig. 1. Privacy Hierarchy for Digital Signatures.
Notation: $X \rightarrow Y$ means that X is a strictly stronger privacy notion than Y. $X \nrightarrow Y$ means that X does not imply Y. X-FKE stands for X defined with of full key exposure.

1.1 Our Results and Techniques

Privacy Hierarchy for Digital Signatures. We develop a three-level hierarchy of privacy notions for digital signatures, starting our work with the investigation of the relationship between anonymity and confidentiality, two previously established privacy notions for signatures. Definitions of anonymity were first given by Yang et al. [28], with later refinements by Fischlin [17]. These definitions presume messages with high entropy (unlike Bellare and Duan [2] and Saraswat and Yun [24], who regard a more restrictive form of signatures[5]). For confidentiality, we use the original definitions by Dent et al. [16] (in its strongest variant). We show that anonymous signatures and confidential signatures are independent privacy notions[6]. For this reason, *anonymity* (ANON) and *confidentiality* (CONF) are located at the lowest level of our privacy hierarchy.

At the mid-level of our hierarchy we have *indistinguishability* (IND), expressing that signatures can be simulated from the public parameters of the scheme. We prove that such signatures offer stronger privacy guarantees than purely anonymous and purely confidential schemes. In particular, any transmission of an IND signature simultaneously hides both the signer *and* the associated message. The IND property is thus a generalization of both ANON and CONF and is sufficient for obtaining privacy in anticipated applications of both schemes. IND signatures may, however, leak some recognizable structure about the signature scheme in use.

The strongest privacy notion in our arsenal lets signatures appear to privacy adversaries as (structureless) strings of random bits, and is hence termed *pseudorandom* (PR). We show why this property is sufficient to hide *all* information about the signing process, including the signature scheme itself. The introduced privacy hierarchy with the intuitively strongest notion of pseudorandomness on top is thus likely to close the subject of privacy-preserving signatures.

Each of our privacy notions is defined in two variants, reflecting that adversaries might of might not have a copy of the signing key. That is, we also address security with *full key exposure* (FKE), which has been formalized for anonymous schemes by Fischlin [17] (and is also considered in [2, 24], but did not find formal treatment in the definitions of confidentiality in [16]). In our privacy hierarchy, we further distinguish between probabilistic and deterministic schemes. Within other, we show that with full key exposure, obtaining any form of privacy for deterministic schemes is hopeless.

The universe of privacy notions considered in this paper and their relationships is illustrated in Figure 1.

[5] Anonymity definitions in [2, 24] assume that σ consists of two parts — signature σ_1 and a value σ_2 (called *de-anonymizer* in [2] or *verification token* in [24]), both of which are needed to perform the verification. Transmission of the entire $\sigma = (\sigma_1, \sigma_2)$, that is amenable to verification, becomes a two-stage process, with σ_1 (together with m) being disclosed in the first stage, and σ_2 in the second stage. Anonymity of the signer is then defined with respect to an adversary that knows σ_1 but not σ_2. As discussed in [2, 24], this definition essentially implies anonymity from [17, 28], allowing also low-entropy message spaces. Since we look on privacy from a more general perspective (e.g. consider confidentiality as another privacy goal), it appears more advisable to work with high-entropy messages and use conceptually simpler anonymity definitions from [17, 28].

[6] Interestingly, Dent et al. [16] mention similarities between the notions but do not formally investigate their relationship. They only expect it to be similar to the relationship between anonymous (key-private) encryption schemes [1] and traditional public-key encryption schemes. Arguably, these notions do not seem to be independent, unless anonymous encryption schemes that do not offer secrecy of encrypted messages are interesting on their own.

Setting	Example scheme	IND with FKE	PR with FKE	Model
RSA	FDH-RSA [4]	randomized hash with padding	IND-to-PR compiler	ROM
DL	Schnorr [25]	✓	IND-to-PR compiler	ROM
Pairings	Boneh-Boyen [5]	for random ℓ-bit m / hash-then-sign	IND-to-PR compiler	STD / ROM
any unforgeable signature scheme		inherited from PR compiler	direct PR compiler	STD

Table 1. Indistinguishable and Pseudorandom Signatures (Settings, Techniques, Compilers)

Constructions and Transformations. For a selection of existing signature schemes, we investigate indistinguishability and pseudorandomness properties and, where appropriate, propose modifications and generic transformations to achieve these goals. We build privacy-preserving signatures in three different cryptographic settings, namely using RSA parameters on the example of the full-domain hash RSA (FDH-RSA) scheme [4], using cyclic prime-order groups on the example of Schnorr's scheme [25], and using pairings on the example of the Boneh-Boyen (BB) scheme [5]. These results are summarized in Table 1 and detailed in the following.

Indistinguishable Signatures. We formalize the notion of *information recovering signatures* (as a generalization of the known concept of 'message recovery') and discuss its negative impact on confidentiality, and hence on indistinguishability and pseudorandomness. We show that not only known message recovering schemes (e.g. 'text-book' RSA and Nyberg-Rueppel [21], together with their 'hash-then-sign'-based transformations), but also several other schemes (in different cryptographic contexts) fall under our more general notion of 'information recovery' and thus do not offer indistinguishability. Examples include schemes by Cramer and Shoup (CS) [15], Camenisch and Lysyanskaya (CL) [11], and Boneh, Lynn, and Shacham (BLS) [7]. That is, signatures in these schemes leak information even if they do not allow full recovery of signed messages.

We then focus on three cryptographic settings — RSA, discrete logarithms (DL), and pairings — and provide examples of indistinguishable schemes. In particular, we show that, using appropriate randomization and padding techniques, FDH-RSA becomes indistinguishable. In DL setting we prove that the (generalized) signature scheme by Schnorr [25] offers indistinguishability 'off the shelf', yet assuming that its cyclic group is shared among all signers. We notice that anonymity of FDH-RSA and Schnorr's schemes was previously analyzed in [28], their confidentiality in [16]. Our analysis essentially shows that both schemes admit much stronger privacy guarantees. Finally, we prove that the pairing-based Boneh-Boyen (BB) [5] scheme is indistinguishable in the standard model, yet for uniformly distributed (fixed-length) messages only. As suggested in [5], the 'hash-then-sign' approach can be used in standard model to sign longer messages. We show that in the random oracle model this method readily offers indistinguishability for arbitrary long high-entropy messages. We note that indistinguishability of all analyzed schemes holds in the presence of full key exposure (FKE). Bottom line, we show existence of IND schemes in different cryptographic settings, paving the way towards pseudorandom signature schemes (based on different hardness assumptions).

Pseudorandom Signatures. PR signatures, which cannot be distinguished from random bit strings of the same length, offer the highest form of privacy that signatures can provide.

Our first result on PR signatures is a generic transformation that strengthens IND signatures to obtain the PR property (we call it IND-to-PR compiler in Table 1). It uses *admissible encodings*, introduced in a different context by Boneh and Franklin [6] for elliptic curves, generalized later by Brier et al. [8], and also used to preserve privacy in the password-based authentication protocol by Bringer, Chabanne and Icart [9] (we thus show another interesting application of this primitive). By finding appropriate admissible encodings for different types of sets, we can immediately obtain the PR property for the IND versions of FDH-RSA, Schnorr, and BB schemes. We also prove that the obtained PR property holds in the presence of full key exposure.

Our next result is a second generic transformation that achieves the PR property directly for any (unforgeable) digital signature scheme. This PR compiler is powerful enough to guarantee the PR property also for information recovering schemes and works irrespective of whether the original scheme is probabilistic or deterministic. Moreover, the PR property is guaranteed even if secret signing keys are exposed (FKE). This compiler uses randomness extractors and its techniques have been previously developed by Fischlin [17] to construct anonymous signatures. We thus prove formally that Fischlin's anonymous signature admits a general transformation, which is strong enough to convert any unforgeable signature scheme into a scheme satisfying the strongest[7] privacy property. This direct PR compiler, however, is slightly less efficient than our IND-to-PR compiler.

1.2 Related Work on Signature Privacy

Anonymity of signers assuming high-entropy messages was initially defined by Yang et al. [28], who analyzed anonymity of 'text-book' RSA, PSS, and Schnorr signatures, after applying some necessary modifications. Their definition was simplified by Fischlin [17] (and relaxed to full key exposure), who showed how to obtain anonymity using randomness extractors. Anonymity definitions for arbitrary messages, yet with specific restrictions on the format of disclosed signatures, were formulated independently by Bellare and Duan [2], Saraswat and Yun [24], and Zhang and Imai [29]. Using the 'sign-then-commit' approach, Bellare and Duan [2] gave four constructions: Their first scheme (also presented in [24]) uses commitments as black-box to produce anonymous signatures in the standard model. The second scheme uses randomized hash functions and can be applied to deterministic signature schemes. Their third solution relies on deterministic hash functions and can be used with probabilistic signature schemes. The fourth scheme from [2], termed 'splitting construction' follows closely the design of Schnorr signatures in the discrete logarithm setting. Saraswat and Yun [24] proved anonymity of the signature scheme by Boneh and Boyen [5]. Furthermore, both [2] and [24] formalize another requirement (called unambiguity in [2] and unpretendability in [24]) that prevents the adversary from claiming the ownership of an anonymous signature at a later stage. Note that this requirement is orthogonal to privacy and can be handled separately. The anonymous scheme by Zhang and Imai [29] uses what they call 'collision-resistant exposure-free functions' which are instantiated with randomized hash functions in the random oracle model. Confidentiality of signature schemes has been considered so far formally by Dent et al. [16] for messages with high entropy, inspired by the definitional treatment of confidentiality for deterministic public-key encryption [3]. They defined three flavors (weak, mezzo, and strong) with increasing strength and addressed both deterministic and probabilistic schemes (without full key exposure). Confidentiality of several schemes used in practice was analyzed as well, including those that use full-domain hash constructions (for which [16] defined confidentiality of hash functions, following earlier ideas from [12]), those obtained from Fiat-Shamir transformation, and those based on randomness extractors. Manifold solutions for obtaining privacy were also proposed with more advanced signing techniques. For example, in group signatures [14], users obtain membership certificates from the manager of a group and issue signatures that identify the signer as a valid group member without revealing its actual identity. The latter can be recovered from the signature only by the group manager. Ring signatures [23] allow the signer to form 'ad-hoc' groups and so hide its own identity (in an unrevocable way) from a potential verifier, who only learns that the signer belongs to the formed group. As discussed in [17], ring signatures differ substantially from anonymous signatures as, in the former, anonymity is bound to a (presumably small) group, and in the latter it is guaranteed as long as some information needed for the public verification of signatures remains secret. Anonymity notions have also been considered for other signature types, e.g. undeniable and confirmer signatures by Galbraith and Mao [18]; as discussed in [24], these notions differ from anonymity in ordinary signature schemes.

2 Previous Privacy Notions

We recall the syntax of digital signatures in Definition 1 and the notion of existential unforgeability in Definition 2. Note that all schemes used in this work are existentially unforgeable.

[7] Fischlin [17] mentioned informally that his anonymous signature scheme offers pseudorandomness, although this notion was not yet defined. Our hierarchy clarifies his intuition formally and further implies indistinguishability and confidentiality of his scheme (in presence of full key exposure).

Definition 1 (Digital Signature Scheme). *A* digital signature scheme $\mathsf{S} = (\mathsf{KGen}, \mathsf{Sign}, \mathsf{Ver})$ *is given by three algorithms: The key generation algorithm* KGen*, on input security parameter* 1^λ*, generates a key pair* $(sk, pk) \leftarrow \mathsf{KGen}(1^\lambda)$*, the signing algorithm* Sign*, on input a secret key sk and a message* $m \in \{0,1\}^*$*, outputs a signature* $\sigma \leftarrow \mathsf{Sign}(sk, m)$*, and the (deterministic) verification algorithm* Ver*, on input a public key pk, a message m, and a candidate signature* σ*, outputs a bit* $d \leftarrow \mathsf{Ver}(pk, m, \sigma)$*. The scheme* S *is* correct *if for all* $\lambda \in \mathbb{N}$*,* $(sk, pk) \leftarrow \mathsf{KGen}(1^\lambda)$*,* $m \in \{0,1\}^*$*, and* $\sigma \leftarrow \mathsf{Sign}(sk, m)$*, we have* $\mathsf{Ver}(pk, m, \sigma) = 1$*. The scheme* S *is* deterministic *if every two invocations of* $\mathsf{Sign}(sk, \cdot)$ *on the same input message m result in the same signature* σ*.*

Definition 2 (Existential Unforgeability). *A signature scheme* S *is* existentially unforgeable under adaptive chosen-message attacks ($\mathsf{EUF\text{-}CMA}$) *if all PPT adversaries* $\mathcal{A}$ *have negligible probability to output* $(m^*, \sigma^*) \leftarrow \mathcal{A}^{\mathsf{Sign}(sk,\cdot)}(pk)$ *(where* $(sk, pk) \leftarrow \mathsf{KGen}(1^\lambda)$ *and* $\mathsf{Sign}(sk, \cdot)$ *is a signature oracle) such that* $\mathsf{Ver}(pk, m^*, \sigma^*) = 1$*, provided that* m^* *was not queried to* $\mathsf{Sign}(sk, \cdot)$ *oracle.*

We focus in the main part of this paper on privacy of probabilistic schemes in a setting with system-wide known public keys. Please refer to Appendix A for a discussion of restrictions and impossibility results on privacy for *deterministic* schemes.

2.1 Anonymous Signatures

Anonymity of signatures for high-entropy messages [17, 28] hides which signer (presuming the system-wide knowledge of public keys) generated a given challenge signature σ. Definition 3 is essentially from [17], where we also let the adversary $\mathcal{A}$ choose the challenge message m (similar to [2]). In case of full key exposure, $\mathcal{A}$ receives secret keys, which obsoletes the signing oracle.

Definition 3 (Anonymous Signatures). *A signature scheme* S *is* anonymous (ANON)*, possibly* with full key exposure ($\mathsf{ANON\text{-}FKE}$)*, if for all PPT adversaries* $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$ *the advantage function*

$$\mathsf{Adv}^{\mathsf{ANON[\text{-}FKE]}}_{\mathsf{S},\mathcal{A}}(\lambda) := \left| \Pr\left[\mathsf{Exp}^{\mathsf{ANON[\text{-}FKE]},0}_{\mathsf{S},\mathcal{A}}(\lambda) = 1\right] - \Pr\left[\mathsf{Exp}^{\mathsf{ANON[\text{-}FKE]},1}_{\mathsf{S},\mathcal{A}}(\lambda) = 1\right] \right|$$

is negligible in λ*, where* $\mathsf{Exp}^{\mathsf{ANON[\text{-}FKE]},b}_{\mathsf{S},\mathcal{A}}(\lambda)$*,* $b \in \{0,1\}$*, are the* anonymity experiments *from Figure 2, and where the following* high entropy constraint *holds: The function* $\mu(\lambda) = \max_{M \in \{0,1\}^*} \Pr[M = m : m \leftarrow \mathcal{A}_1]$ *is negligible in* λ*, assuming that* $\mathcal{A}_1$ *is provided with all admissible inputs and oracles as specified in the respective anonymity experiment. The* minimum entropy *of* $\mathcal{A}$ *is then given by* $-\log_2 \mu(\lambda)$*.*

```
$\mathsf{Exp}^{\mathsf{ANON},b}_{\mathsf{S},\mathcal{A}}(\lambda)$ :
  $(sk_0, pk_0) \leftarrow \mathsf{KGen}(1^\lambda)$
  $(sk_1, pk_1) \leftarrow \mathsf{KGen}(1^\lambda)$
  $m \leftarrow \mathcal{A}_1^{\mathsf{Sign}(sk_0,\cdot),\mathsf{Sign}(sk_1,\cdot)}(pk_0, pk_1)$
  $\sigma \leftarrow \mathsf{Sign}(sk_b, m)$
  $d \leftarrow \mathcal{A}_2^{\mathsf{Sign}(sk_0,\cdot),\mathsf{Sign}(sk_1,\cdot)}(pk_0, pk_1, \sigma)$
  output $d$
```

```
$\mathsf{Exp}^{\mathsf{ANON\text{-}FKE},b}_{\mathsf{S},\mathcal{A}}(\lambda)$ :
  $(sk_0, pk_0) \leftarrow \mathsf{KGen}(1^\lambda)$
  $(sk_1, pk_1) \leftarrow \mathsf{KGen}(1^\lambda)$
  $m \leftarrow \mathcal{A}_1(sk_0, pk_0, sk_1, pk_1)$
  $\sigma \leftarrow \mathsf{Sign}(sk_b, m)$
  $d \leftarrow \mathcal{A}_2(sk_0, pk_0, sk_1, pk_1, \sigma)$
  output $d$
```

Fig. 2. Anonymity Experiments (without and with Full Key Exposure)

2.2 Confidential Signatures

Confidentiality of digital signatures, formalized by Dent et al. in [16], hides information about the message m that was signed. Definition 4 corresponds to *strong confidentiality* from [16], the strongest among the three notions (weak, mezzo, strong) proposed there.

Definition 4 (Confidential Signatures). *A signature scheme* S *is* confidential (CONF)*, possibly* with full key exposure ($\mathsf{CONF\text{-}FKE}$)*, if for all PPT adversaries* $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$ *the following advantage function*

$$\mathsf{Adv}_{\mathsf{S},\mathcal{A}}^{\mathsf{CONF[\text{-}FKE]}}(\lambda) := \left|\Pr\left[\mathsf{Exp}_{\mathsf{S},\mathcal{A}}^{\mathsf{CONF[\text{-}FKE]},0}(\lambda) = 1\right] - \Pr\left[\mathsf{Exp}_{\mathsf{S},\mathcal{A}}^{\mathsf{CONF[\text{-}FKE]},1}(\lambda) = 1\right]\right|$$

is negligible in λ*, where* $\mathsf{Exp}_{\mathsf{S},\mathcal{A}}^{\mathsf{CONF[\text{-}FKE]},b}(\lambda)$*,* $b \in \{0,1\}$*, are the* confidentiality experiments *from Figure 3, and where the following* high entropy constraint *holds: The function* $\mu(\lambda) = \max_{M\in\{0,1\}^*} \Pr[M \in \boldsymbol{m} : (\boldsymbol{m}, t) \leftarrow \mathcal{A}_1]$ *is negligible in* λ*, assuming* $\mathcal{A}_1$ *is provided with all admissible inputs and oracles as specified in the resp. confidentiality experiment. The* minimum entropy *of* $\mathcal{A}$ *is then given by* $-\log_2 \mu(\lambda)$*.*

```
$\mathsf{Exp}_{\mathsf{S},\mathcal{A}}^{\mathsf{CONF},b}(\lambda)$ :
    $(sk, pk) \leftarrow \mathsf{KGen}(1^\lambda)$
    $(\boldsymbol{m}_0, t_0) \leftarrow \mathcal{A}_1^{\mathsf{Sign}(sk,\cdot)}(pk)$
    $(\boldsymbol{m}_1, t_1) \leftarrow \mathcal{A}_1^{\mathsf{Sign}(sk,\cdot)}(pk)$
    if $|\boldsymbol{m}_0| \neq |\boldsymbol{m}_1|$ then output 0
    $\boldsymbol{\sigma}^* \leftarrow \mathsf{Sign}(sk, \boldsymbol{m}_b)$
    $t' \leftarrow \mathcal{A}_2^{\mathsf{Sign}(sk,\cdot)}(pk, \boldsymbol{\sigma}^*)$
    if $t' = t_0$ then output 1, else output 0
```

```
$\mathsf{Exp}_{\mathsf{S},\mathcal{A}}^{\mathsf{CONF\text{-}FKE},b}(\lambda)$ :
    $(sk, pk) \leftarrow \mathsf{KGen}(1^\lambda)$
    $(\boldsymbol{m}_0, t_0) \leftarrow \mathcal{A}_1(sk, pk)$
    $(\boldsymbol{m}_1, t_1) \leftarrow \mathcal{A}_1(sk, pk)$
    if $|\boldsymbol{m}_0| \neq |\boldsymbol{m}_1|$ then output 0
    $\boldsymbol{\sigma}^* \leftarrow \mathsf{Sign}(sk, \boldsymbol{m}_b)$
    $t' \leftarrow \mathcal{A}_2(sk, pk, \boldsymbol{\sigma}^*)$
    if $t' = t_0$ then output 1, else output 0
```

Fig. 3. Confidentiality Experiments (without and with Full Key Exposure).[8]

Observe that, in the confidentiality experiments from Figure 3, the first-stage adversary $\mathcal{A}_1$ outputs a vector $\boldsymbol{m}$ of messages, each of high entropy, and an additional token t. This token models the intuition that confidential signatures shouldn't leak 'any information' about signed messages.[9]

2.3 Independence of ANON and CONF

Lemmas 1 and 2 separate the two notions ANON and CONF. Their independence follows then from the fact that some unforgeable schemes are neither anonymous nor confidential and that for other schemes both notions hold simultaneously (cf. Section 4).

Lemma 1 ($\mathsf{CONF[\text{-}FKE]} \not\Rightarrow \mathsf{ANON}$)**.** *Confidential signature schemes (with full key exposure) are not necessarily anonymous.*

Proof. Let S be a confidential signature scheme. We construct a confidential but not anonymous signature scheme S' from S as follows.

$\mathsf{KGen}'(1^\lambda)$: Output $(sk, pk) \leftarrow \mathsf{KGen}(1^\lambda)$.

[8] Values $\boldsymbol{m}$ output by (stateless) $\mathcal{A}_1$ are *vectors* of messages in $\{0,1\}^*$ and $|\boldsymbol{m}|$ denotes the number of elements in $\boldsymbol{m}$. Accordingly, by $\boldsymbol{\sigma} \leftarrow \mathsf{Sign}(sk, \boldsymbol{m})$ we denote the process of signing the messages in $\boldsymbol{m}$ *element-wise* and *independently* of each other, resulting in a vector $\boldsymbol{\sigma}$ of corresponding signatures.

[9] We stick here to the confidentiality definition introduced by Dent et al. in [16] using two separate calls of $\mathcal{A}_1$.

$\mathsf{Sign}'(sk, m):$ $\sigma \leftarrow \mathsf{Sign}(sk, m)$. Output $\sigma' := (\sigma, pk)$.
$\mathsf{Ver}'(pk, m, \sigma'):$ Parse σ' as (σ, pk'). Return 1 iff $\big(\mathsf{Ver}(pk, m, \sigma) = 1 \wedge pk = pk'\big)$.

As the public verification key pk is extractable from a signature σ', S' is not anonymous. Yet, S' remains confidential (as the CONF adversary knows pk anyway). Clearly, the construction preserves unforgeability. □

Lemma 2 (ANON[-FKE] $\not\Rightarrow$ CONF). *Anonymous signature schemes (with full key exposure) are not necessarily confidential.*

Proof. Let S be an anonymous signature scheme and $\texttt{last} : \{0,1\}^* \to \{0,1\}$ denote the function that outputs the last bit of its argument. We construct an anonymous but not confidential signature scheme S' from S as follows.

$\mathsf{KGen}'(1^\lambda):$ Output $(sk, pk) \leftarrow \mathsf{KGen}(1^\lambda)$.
$\mathsf{Sign}'(sk, m):$ $\sigma \leftarrow \mathsf{Sign}(sk, m)$. Output $\sigma' := (\sigma, \texttt{last}(m))$.
$\mathsf{Ver}'(pk, m, \sigma'):$ Parse σ' as (σ, b). Return 1 iff $\big(\mathsf{Ver}(pk, m, \sigma) = 1 \wedge \texttt{last}(m) = b\big)$.

To see that S' is not confidential, consider the following confidentiality adversary $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$. $\mathcal{A}_1$ outputs $(\boldsymbol{m}_0, t_0)$ (resp. $(\boldsymbol{m}_1, t_1)$), where $\boldsymbol{m}_i = (M_i)$ for $M_i \in_R \{0,1\}^\lambda$, and $t_i = \texttt{last}(M_i)$. $\mathcal{A}_2$ parses $\boldsymbol{\sigma}^*$ as $\boldsymbol{\sigma}^* = ((\sigma, b))$ and outputs b. So $\mathsf{Adv}^{\mathsf{CONF}}_{\mathsf{S}',\mathcal{A}}(\lambda) = |\Pr[\mathsf{Exp}^{\mathsf{CONF},0}_{\mathsf{S}',\mathcal{A}}(\lambda) = 1] - \Pr[\mathsf{Exp}^{\mathsf{CONF},1}_{\mathsf{S}',\mathcal{A}}(\lambda) = 1]| = \big|1 - \frac{1}{2}\big| = \frac{1}{2}$.

To show anonymity of S', consider any adversary $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$ against ANON of S'. Flip a coin $\beta \in_R \{0,1\}$ and define ANON adversary $\mathcal{B} = (\mathcal{B}_1, \mathcal{B}_2)$ against S as follows: On input pk_0, pk_1, $\mathcal{B}_1$ runs $\mathcal{A}_1(pk_0, pk_1)$ as a black-box and receives a message m. If $\texttt{last}(m) = \beta$, m is output, otherwise the simulation aborts which is modeled by letting $\mathcal{B}$'s simulator output 0, i.e. $\Pr[\mathsf{Exp}^{\mathsf{ANON},b}_{\mathsf{S},\mathcal{B}}(\lambda) = 1 | \mathtt{A}] = 0$ for $b \in \{0,1\}$. The "abort" event $\mathtt{A}$ will occur with probability $\frac{1}{2}$. Now, on input pk_0, pk_1, σ, algorithm $\mathcal{B}_2$ appends β to σ, runs $d \leftarrow \mathcal{A}_2(pk_0, pk_1, (\sigma, \beta))$ and outputs d. Then

$$\begin{aligned}\Pr[\mathsf{Exp}^{\mathsf{ANON},b}_{\mathsf{S},\mathcal{B}}(\lambda) = 1] &= \Pr[\mathsf{Exp}^{\mathsf{ANON},b}_{\mathsf{S},\mathcal{B}}(\lambda) = 1 | \neg\mathtt{A}] \cdot \Pr[\neg\mathtt{A}] + \Pr[\mathsf{Exp}^{\mathsf{ANON},b}_{\mathsf{S},\mathcal{B}}(\lambda) = 1 | \mathtt{A}] \cdot \Pr[\mathtt{A}] \\ &= \Pr[\mathsf{Exp}^{\mathsf{ANON},b}_{\mathsf{S}',\mathcal{A}}(\lambda) = 1] \cdot \tfrac{1}{2} + 0 \cdot \tfrac{1}{2}\end{aligned}$$

and hence $\mathsf{Adv}^{\mathsf{ANON}}_{\mathsf{S},\mathcal{B}}(\lambda) = \frac{1}{2} \cdot \mathsf{Adv}^{\mathsf{ANON}}_{\mathsf{S}',\mathcal{A}}(\lambda)$. Thus S' is anonymous, as the left hand side is negligible by assumption. □

3 Digital Signatures with Information Recovery

The following definition of 'information recovery', where in the verification procedure signer's public key is used together with the signature to compute some information that is then compared to information determined by the public key and the message, generalizes the known concept of 'message recovery'.

Definition 5 (Information Recovering Signatures). *A digital signature scheme* $\mathsf{S} = (\mathsf{KGen}, \mathsf{Sign}, \mathsf{Ver})$ *is called* information recovering *if there exist two polynomial-time algorithms* Inf *and* Rec *such that for all* $(sk, pk) \leftarrow \mathsf{KGen}(1^\lambda)$*,* $m \in \{0,1\}^*$*, and* $\sigma \leftarrow \mathsf{Sign}(sk, m)$*, the verification algorithm* $\mathsf{Ver}(pk, m, \sigma)$ *outputs 1 if and only if* $\mathsf{Inf}(pk, m) = \mathsf{Rec}(pk, \sigma)$*.*

Remark 1. Note that information recovering signature schemes with $\mathsf{Inf}(pk, \cdot) = pk = \mathsf{Rec}(pk, \cdot)$ might be correct, but are necessarily forgeable. More precisely, if $\mathsf{Inf}(pk, m_0) = \mathsf{Inf}(pk, m_1)$ happens with noticeable probability (for independently drawn $m_0, m_1 \in_R \{0,1\}^\lambda$), an adversary $\mathcal{A}$ against unforgeability can be constructed by letting $\mathcal{A}$ request a signature σ_0 on a random message m_0 and output (m_1, σ_0), for random m_1, as a forgery. To see that $\mathcal{A}$ has non-negligible success probability, observe that σ_0 will verify successfully for m_1 if we have $\mathsf{Rec}(pk, \sigma_0) = \mathsf{Inf}(pk, m_1) = \mathsf{Inf}(pk, m_0)$, what happens with non-negligible probability by assumption.

3.1 Examples of Schemes with Information Recovery

Classical examples of information recovering schemes include “text-book” RSA and Nyberg-Rueppel [21], whose signatures can be used to recover messages. Observe that if the “hash-then-sign” approach is used, e.g. FDH-RSA [4], then signatures computed on hash values $H(m)$ (rather than on messages m) are still information recovering, even if H is modeled as a random oracle, i.e. the corresponding algorithm $\mathsf{Inf}(pk, m)$ would simply output $H(m)$. This property can also be found amongst signature schemes that are not message recovering or where messages need not be hashed to compute (unforgeable) signatures, as shown in the following.

Cramer-Shoup (CS) [15]. The Strong RSA-based CS scheme outputs signatures of the form $\sigma = (e, s, \sigma_1', \sigma_2')$ and its verification algorithm checks whether e is an odd integer of certain length, followed by two checks of the form $\sigma_1'^e \equiv th^{H(s)} \bmod N$ and $\sigma_2'^{\tilde{e}} \equiv sh^m \bmod N$ with $\tilde{e}$, t, h, and N being part of the public key pk. These equation can be rewritten to $\mathsf{Inf}(pk, m) = \mathsf{Rec}(pk, \sigma)$ using $\mathsf{Inf}(pk, m)$ that outputs a pair $(t, h^m \bmod N)$ and $\mathsf{Rec}(pk, \sigma)$ returning a pair $(\sigma_1'^e \cdot h^{-H(s)}, \sigma_2'^{\tilde{e}} \cdot s^{-1} \bmod N)$ after verifying the appropriate form for e. The equality of the outputs of Inf and Rec can then be tested component-wise to verify the signature.

Camenisch-Lysyanskaya (CL) [11]. The Strong RSA-based CL scheme outputs signatures of the form $\sigma = (e, s, \sigma')$ and its verification algorithm checks if e is in the appropriate range and $\sigma'^e \equiv a^m b^s c \bmod N$ with a, b, c, and N being part of the public key pk. By rewriting the verification equation to $a^m \equiv \sigma'^e/(b^s c) \bmod N$ we can define algorithm $\mathsf{Inf}(pk, m)$ to output $a^m \bmod N$ and $\mathsf{Rec}(pk, \sigma)$ to output $\sigma'^e \cdot (b^s c)^{-1} \bmod N$ if e is in the appropriate range.

Boneh-Lynn-Shacham (BLS) [7]. The pairing-based BLS scheme, which can be initialized for example in cyclic groups $G = \langle g \rangle$ of prime order q with a suitable bilinear map $e : G \times G \mapsto G_T$, outputs signatures of the form $\sigma = H(m)^x$ where $H : \mathbb{Z}_q^* \mapsto G$ is a random oracle and x is a secret key. Its verification equation $e(H(m), y) = e(\sigma, g)$ with g, y belonging to pk, immediately defines $\mathsf{Inf}(pk, m)$ and $\mathsf{Rec}(pk, \sigma)$.

3.2 Information Recovery Limits Privacy

The property of information recovery of a scheme can be immediately used to break the scheme’s confidentiality by including information derived via algorithm Inf from messages in $\boldsymbol{m}$ into t, as shown in the following lemma.

Lemma 3. *There is no unforgeable information recovering signature scheme that provides confidentiality.*

Proof. Let $\mathsf{S} = (\mathsf{KGen}, \mathsf{Sign}, \mathsf{Ver})$ be an information recovering signature scheme. Consider the following adversary $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$ against confidentiality of S: $\mathcal{A}_1$ on input pk picks a random λ-bit message m, computes $t \leftarrow \mathsf{Inf}(pk, m)$, and outputs (m, t). $\mathcal{A}_2$ on input (pk, σ^*) outputs $t' \leftarrow \mathsf{Rec}(pk, \sigma^*)$. In this setting, we observe that correctness of S and the construction of Ver from Inf and Rec implies $\Pr[\mathsf{Exp}_{\mathsf{S},\mathcal{A}}^{\mathsf{CONF},0}(\lambda) = 1] = 1$. We now consider $\mathsf{Exp}_{\mathsf{S},\mathcal{A}}^{\mathsf{CONF},1}(\lambda)$, where we use σ_1 to denote the challenge signature $\sigma^* \leftarrow \mathsf{Sign}(sk, m_1)$. Note that by construction of $\mathcal{A}_2$ we have $t' = \mathsf{Rec}(pk, \sigma_1)$. We see that

$$\Pr[\mathsf{Exp}_{\mathsf{S},\mathcal{A}}^{\mathsf{CONF},1}(\lambda) = 1] = \Pr[t' = t_0] = \Pr[\mathsf{Rec}(pk, \sigma_1) = \mathsf{Inf}(pk, m_0)] = \Pr[\mathsf{Inf}(pk, m_1) = \mathsf{Inf}(pk, m_0)],$$

which, as S is unforgeable, is negligible (cf. Remark 1). For $\mathcal{A}$ we thus proved non-negligible advantage $\mathsf{Adv}_{\mathsf{S},\mathcal{A}}^{\mathsf{CONF[\text{-}FKE]}}(\lambda)$ against confidentiality of signature scheme S. □

4 Indistinguishable Signatures

The independence of the notions of anonymity and confidentiality of digital signature schemes places these concepts at the bottom level of our privacy hierarchy and puts forward the question on the existence of a more general privacy property that implies both of them. We call this property *indistinguishability* and formalize it in Definition 6. We use a simulation-based approach, following the intuition that anonymity and confidentiality are implied if all information that can be extracted from a real signature can also be extracted from a 'signature' that was *simulated* without knowledge of keys and messages.[10]

Definition 6 (Indistinguishable Signatures). *A signature scheme* S *is* indistinguishable (IND)*, possibly* with full key exposure ($\mathsf{IND\text{-}FKE}$)*, if there exists a PPT* simulator Sim *such that for all PPT adversaries* $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$ *the following advantage function*

$$\mathsf{Adv}^{\mathsf{IND[\text{-}FKE]}}_{\mathsf{S,Sim},\mathcal{A}}(\lambda) := \left|\Pr\left[\mathsf{Exp}^{\mathsf{IND[\text{-}FKE]},0}_{\mathsf{S,Sim},\mathcal{A}}(\lambda) = 1\right] - \Pr\left[\mathsf{Exp}^{\mathsf{IND[\text{-}FKE]},1}_{\mathsf{S,Sim},\mathcal{A}}(\lambda) = 1\right]\right|$$

is negligible in λ*, where* $\mathsf{Exp}^{\mathsf{IND[\text{-}FKE]},b}_{\mathsf{S,Sim},\mathcal{A}}(\lambda)$*,* $b \in \{0,1\}$*, are the* indistinguishability experiments *from Figure 4, and where the following* high entropy constraint *holds: The function* $\mu(\lambda) = \max_{M\in\{0,1\}^*} \Pr[M \in \boldsymbol{m} : (\boldsymbol{m}, t) \leftarrow \mathcal{A}_1]$ *is negligible in* λ*, assuming* $\mathcal{A}_1$ *is provided with all admissible inputs and oracles as specified in the resp. indistinguishability experiment. The* minimum entropy *of* $\mathcal{A}$ *is given by* $-\log_2 \mu(\lambda)$*.*

```
$\mathsf{Exp}^{\mathsf{IND},b}_{\mathsf{S,Sim},\mathcal{A}}(\lambda)$ :
    $(sk, pk) \leftarrow \mathsf{KGen}(1^\lambda)$
    $(\boldsymbol{m}, t) \leftarrow \mathcal{A}_1^{\mathsf{Sign}(sk,\cdot)}(pk)$
    $\boldsymbol{\sigma}_0 \leftarrow \mathsf{Sign}(sk, \boldsymbol{m})$
    $\boldsymbol{\sigma}_1 \leftarrow \mathsf{Sim}(1^\lambda, |\boldsymbol{m}|)$
    $t' \leftarrow \mathcal{A}_2^{\mathsf{Sign}(sk,\cdot)}(pk, \boldsymbol{\sigma}_b)$
    if $t' = t$ then output 1, else output 0
```

```
$\mathsf{Exp}^{\mathsf{IND\text{-}FKE},b}_{\mathsf{S,Sim},\mathcal{A}}(\lambda)$ :
    $(sk, pk) \leftarrow \mathsf{KGen}(1^\lambda)$
    $(\boldsymbol{m}, t) \leftarrow \mathcal{A}_1(sk, pk)$
    $\boldsymbol{\sigma}_0 \leftarrow \mathsf{Sign}(sk, \boldsymbol{m})$
    $\boldsymbol{\sigma}_1 \leftarrow \mathsf{Sim}(1^\lambda, |\boldsymbol{m}|)$
    $t' \leftarrow \mathcal{A}_2(sk, pk, \boldsymbol{\sigma}_b)$
    if $t' = t$ then output 1, else output 0
```

Fig. 4. Indistinguishability Experiments (without and with Full Key Exposure).

Lemmas 4 and 5 confirm the intuition that indistinguishable signatures are also anonymous and confidential (even in presence of full key exposure).

Lemma 4 ($\mathsf{IND} \Rightarrow \mathsf{ANON}$, $\mathsf{IND\text{-}FKE} \Rightarrow \mathsf{ANON\text{-}FKE}$). *Every indistinguishable signature scheme is anonymous. The same implication holds in presence of full key exposure.*

Proof. Let S be an indistinguishable signature scheme with simulator Sim. For an ANON-adversary $\mathcal{A}$ consider experiment $\mathsf{Exp}^*_{\mathsf{S,Sim},\mathcal{A}}(\lambda)$, which is like $\mathsf{Exp}^{\mathsf{ANON},0}_{\mathsf{S},\mathcal{A}}(\lambda)$, except that challenge signature σ is computed as $\sigma \leftarrow \mathsf{Sim}(1^\lambda, 1)$. Construct IND-adversary $\mathcal{B}$ by generating random $(sk', pk') \leftarrow \mathsf{KGen}(1^\lambda)$ and defining $\mathcal{B}_1$ and $\mathcal{B}_2$ as follows: $\mathcal{B}_1$, on input pk and having oracle access to $\mathsf{Sign}(sk, \cdot)$, runs $m \leftarrow \mathcal{A}_1^{\mathsf{Sign}(sk,\cdot),\mathsf{Sign}(sk',\cdot)}(pk, pk')$ as a black-box, relaying oracle queries to $\mathsf{Sign}(sk, \cdot)$, and answering $\mathsf{Sign}(sk', \cdot)$ queries itself. After receiving m, $\mathcal{B}_1$ outputs $(\boldsymbol{m}, t) = ((m), 1)$ and stops. $\mathcal{B}_2$, on input pk and challenge signature $\boldsymbol{\sigma} = (\sigma)$, feeds σ into $\mathcal{A}_2$

[10] Since our IND definition involves a simulator Sim that generates signatures in $\boldsymbol{\sigma}$ without knowledge of (sk, m), one may ask about the relationship to zero-knowledge proofs, which also, by definition, are simulatable without knowledge of the secret. We observe that indistinguishable signatures are not zero-knowledge proofs — simulated IND signatures need not to be convincing (as opposed to simulated proofs), i.e. they do not need to pass the regular signature verification.

(together with pk and pk'). Value d output by $\mathcal{A}_2$ is used as return value t' of $\mathcal{B}_2$. Careful inspection results in

$$\begin{aligned}\left|\Pr\left[\mathsf{Exp}^{\mathsf{ANON},0}_{\mathsf{S},\mathcal{A}}(\lambda)=1\right]-\Pr\left[\mathsf{Exp}^{*}_{\mathsf{S},\mathsf{Sim},\mathcal{A}}(\lambda)=1\right]\right| &= \left|\Pr\left[\mathsf{Exp}^{\mathsf{IND},0}_{\mathsf{S},\mathsf{Sim},\mathcal{B}}(\lambda)=1\right]-\Pr\left[\mathsf{Exp}^{\mathsf{IND},1}_{\mathsf{S},\mathsf{Sim},\mathcal{B}}(\lambda)=1\right]\right|\\ &= \mathsf{Adv}^{\mathsf{IND}}_{\mathsf{S},\mathsf{Sim},\mathcal{B}}(\lambda).\end{aligned}$$

Equality $\left|\Pr[\mathsf{Exp}^{\mathsf{ANON},1}_{\mathsf{S},\mathcal{A}}(\lambda)=1]-\Pr[\mathsf{Exp}^{*}_{\mathsf{S},\mathsf{Sim},\mathcal{A}}(\lambda)=1]\right| = \mathsf{Adv}^{\mathsf{IND}}_{\mathsf{S},\mathsf{Sim},\mathcal{B}}(\lambda)$ can be shown similarly (by swapping pk and pk' in the construction of $\mathcal{B}$). All in all we have shown $\mathsf{Adv}^{\mathsf{ANON}}_{\mathsf{S},\mathcal{A}}(\lambda) \leq 2\cdot\mathsf{Adv}^{\mathsf{IND}}_{\mathsf{S},\mathsf{Sim},\mathcal{B}}(\lambda)$, which is negligible by assumption. The implication IND-FKE ⇒ ANON-FKE is shown analogously. □

Lemma 5 **(IND ⇒ CONF, IND-FKE ⇒ CONF-FKE).** *Every indistinguishable signature scheme is confidential. The same implication holds in presence of full key exposure.*

Proof. Let S be an indistinguishable signature scheme with simulator Sim. For a CONF-adversary $\mathcal{A}$ consider experiment $\mathsf{Exp}^{*}_{\mathsf{S},\mathsf{Sim},\mathcal{A}}(\lambda)$, which is like $\mathsf{Exp}^{\mathsf{CONF},0}_{\mathsf{S},\mathcal{A}}(\lambda)$, except challenge signatures $\boldsymbol{\sigma}^*$ are computed as $\boldsymbol{\sigma}^* \leftarrow \mathsf{Sim}(1^\lambda, |\boldsymbol{m}_0|)$. Construct IND-adversary $\mathcal{B}$ defining $\mathcal{B}_1,\mathcal{B}_2$ as follows: $\mathcal{B}_1$, on input pk and with oracle $\mathsf{Sign}(sk,\cdot)$, runs $\mathcal{A}_1^{\mathsf{Sign}(sk,\cdot),\mathsf{Sign}(sk',\cdot)}(pk)$ twice as a black-box, relaying oracle queries to $\mathsf{Sign}(sk,\cdot)$ and answering $\mathsf{Sign}(sk',\cdot)$ queries itself, to obtain $(\boldsymbol{m}_0,t_0)$ and $(\boldsymbol{m}_1,t_1)$, respectively. Algorithm $\mathcal{B}_1$ aborts if $|\boldsymbol{m}_0| \neq |\boldsymbol{m}_1|$. Else it outputs $(\boldsymbol{m}_0,t_0)$ and stops. $\mathcal{B}_2$, on input pk and challenge signatures $\boldsymbol{\sigma}$, feeds $\boldsymbol{\sigma}$ into $\mathcal{A}_2$ (together with pk). Value t' output by $\mathcal{A}_2$ is used as return value t' of $\mathcal{B}_2$. Now we have

$$\begin{aligned}\left|\Pr\left[\mathsf{Exp}^{\mathsf{CONF},0}_{\mathsf{S},\mathcal{A}}(\lambda)=1\right]-\Pr\left[\mathsf{Exp}^{*}_{\mathsf{S},\mathsf{Sim},\mathcal{A}}(\lambda)=1\right]\right| &= \left|\Pr\left[\mathsf{Exp}^{\mathsf{IND},0}_{\mathsf{S},\mathsf{Sim},\mathcal{B}}(\lambda)=1\right]-\Pr\left[\mathsf{Exp}^{\mathsf{IND},1}_{\mathsf{S},\mathsf{Sim},\mathcal{B}}(\lambda)=1\right]\right|\\ &= \mathsf{Adv}^{\mathsf{IND}}_{\mathsf{S},\mathsf{Sim},\mathcal{B}}(\lambda).\end{aligned}$$

Equality $\left|\Pr[\mathsf{Exp}^{\mathsf{CONF},1}_{\mathsf{S},\mathcal{A}}(\lambda)=1]-\Pr[\mathsf{Exp}^{*}_{\mathsf{S},\mathsf{Sim},\mathcal{A}}(\lambda)=1]\right| = \mathsf{Adv}^{\mathsf{IND}}_{\mathsf{S},\mathsf{Sim},\mathcal{B}}(\lambda)$ can be shown similarly (by letting $\mathcal{B}_1$ output $(\boldsymbol{m}_1,t_1)$ instead of $(\boldsymbol{m}_0,t_0)$). All in all we have shown $\mathsf{Adv}^{\mathsf{CONF}}_{\mathsf{S},\mathcal{A}}(\lambda) \leq 2\cdot\mathsf{Adv}^{\mathsf{IND}}_{\mathsf{S},\mathsf{Sim},\mathcal{B}}(\lambda)$, which is negligible by assumption. The implication IND-FKE ⇒ CONF-FKE is shown analogously. □

4.1 Techniques and Examples

We now exemplify IND constructions using three known signature schemes: FDH-RSA [4], Schnorr [25], and Boneh-Boyen [5]. That is, we show that indistinguishable schemes can be obtained in different cryptographic setting, i.e. RSA, discrete logarithms (DL), and pairings. We notice that our techniques can be applied to many existing schemes that either fulfill this privacy notion directly or can be slightly modified to become indistinguishable.

RSA-based Construction. On the example of FDH-RSA [4], which is neither confidential nor anonymous, we demonstrate two techniques to obtain indistinguishability. First, we apply a *randomized hash* [2], where a message m is hashed together with some randomness r, which is chosen within the signing procedure. The hash value $H(m,r)$ is then used in the signing algorithm (instead of m), and r is appended to the resulting signature. This method eliminates information recovery since the output of $\mathsf{Inf}(pk,m)$ depends now on $H(m,r)$ (and not only on m), and the probability that the first stage IND adversary learns information about $H(m,r)$ is negligible (given that r is sufficiently long and chosen in the challenge phase). We can then apply *padding* to hide the length of signature components that are elements of $\mathbb{Z}_N$, and by this protect anonymity [28]. These methods turn out to be sufficient for the indistinguishability of the scheme.

Randomized FDH-RSA with Padding. Let $\mathsf{GenRSA}(1^\lambda)$ denote an algorithm that outputs tuples (N,e,d) where N is an RSA modulus, i.e. $N=pq$ for two prime numbers p and q of length $\lambda/2$, and $e,d\in\mathbb{Z}^\times_{\varphi(N)}$ with $ed = 1 \bmod \varphi(N)$, where $\varphi(N)=(p-1)(q-1)$. Let $H_N:\{0,1\}^*\to\mathbb{Z}_N$ be a hash function modeled as random oracle and Z_λ be a fixed number of 2λ bits, independently of N. The randomized FDH-RSA scheme with padding is defined as follows.

$\mathsf{FDH\text{-}RSA.KGen}(1^\lambda)$: Let $(N,e,d) \leftarrow \mathsf{GenRSA}(1^\lambda)$, $pk := (N,e)$, and $sk := d$. Output (sk,pk).
$\mathsf{FDH\text{-}RSA.Sign}(sk,m)$: Choose $r \in_R \{0,1\}^\lambda$ and $k \in_R [0, \lfloor Z_\lambda/N \rfloor - 1]$. Let $\sigma' := H_N(m \parallel r)^d \bmod N$. Output $\sigma := (\sigma' + kN, r)$.
$\mathsf{FDH\text{-}RSA.Ver}(pk,m,\sigma)$: Parse σ as (σ', r). Let $h' \leftarrow H_N(m \parallel r)$ and $h := (\sigma')^e \bmod N$. Output $h = h'$.

Observe that on each signature σ' a probabilistic padding is applied, computing $k \in_R [0, \lfloor Z_\lambda/N \rfloor - 1], \sigma := \sigma' + kN$, which can be reversed by computing $\sigma' := \sigma \bmod N$. It maps uniformly distributed integers from $[0, N-1]$ to (nearly) uniformly distributed integers in $[0, Z_\lambda - 1]$ (cf. Lemma 13).

Lemma 6. *The probabilistic FDH-RSA scheme with padding is indistinguishable with full key exposure, in the random oracle model.*

Proof. We will consider the simulator Sim that, on input security parameter 1^λ and message number ℓ, outputs a vector of ℓ integers in $[0, Z_\lambda - 1]$, drawn uniformly at random. Let $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$ be any indistinguishability adversary against the modified FDH-RSA scheme. Consider experiments $\mathsf{Exp}^{\mathsf{IND},0,j}_{\mathsf{FDH\text{-}RSA},\mathsf{Sim},\mathcal{A}}(\lambda)$, similar to $\mathsf{Exp}^{\mathsf{IND},0}_{\mathsf{FDH\text{-}RSA},\mathsf{Sim},\mathcal{A}}(\lambda)$, except that the first j signatures in $\boldsymbol{\sigma}^*$ are simulated using $\mathsf{Sim}(1^\lambda, j)$, i.e. $\mathsf{Exp}^{\mathsf{IND},0}_{\mathsf{FDH\text{-}RSA},\mathsf{Sim},\mathcal{A}}(\lambda) = \mathsf{Exp}^{\mathsf{IND},0,0}_{\mathsf{FDH\text{-}RSA},\mathsf{Sim},\mathcal{A}}(\lambda)$ and $\mathsf{Exp}^{\mathsf{IND},1}_{\mathsf{FDH\text{-}RSA},\mathsf{Sim},\mathcal{A}}(\lambda) = \mathsf{Exp}^{\mathsf{IND},0,\ell}_{\mathsf{FDH\text{-}RSA},\mathsf{Sim},\mathcal{A}}(\lambda)$ for some ℓ polynomially bounded by λ. It will suffice to prove that

$$\left| \Pr\left[\mathsf{Exp}^{\mathsf{IND},0,j}_{\mathsf{FDH\text{-}RSA},\mathsf{Sim},\mathcal{A}}(\lambda) = 1\right] - \Pr\left[\mathsf{Exp}^{\mathsf{IND},0,j+1}_{\mathsf{FDH\text{-}RSA},\mathsf{Sim},\mathcal{A}}(\lambda) = 1\right] \right|$$

is negligible for all j.

Let Exp be the experiment which is like $\mathsf{Exp}^{\mathsf{IND},0,j}_{\mathsf{FDH\text{-}RSA},\mathsf{Sim},\mathcal{A}}(\lambda)$ except that, in the generation of the $(j+1)$th signature of $\boldsymbol{\sigma}^*$, we replace the output of hash function H_N by a value $h \in_R \mathbb{Z}_N$, picked uniformly at random (or, equivalently, we use the value h^d, for $h \in_R \mathbb{Z}_N$). By the Random Oracle Model, this change can only be detected by adversaries that correctly guess both: message m and randomizer r. But this will happen only with negligible probability, since $\mathcal{A}_1$ would have to guess $r \in \{0,1\}^\lambda$, and $\mathcal{A}_2$ would have to guess m, which has large entropy. Consider now the hop to experiment $\mathsf{Exp}^{\mathsf{IND},0,j+1}_{\mathsf{FDH\text{-}RSA},\mathsf{Sim},\mathcal{A}}(\lambda)$, which is exactly like Exp, except that the returned $(j+1)$th 'signature' is not computed via the padding, i.e. $\sigma = (h + kN, r)$, but instead via $\sigma = (h', r)$, where $h' \in_R [0, Z_\lambda - 1]$. We will show in Lemma 13 (1) that this introduces only a negligible statistical difference between the output distributions of Exp and $\mathsf{Exp}^{\mathsf{IND},0,j+1}_{\mathsf{FDH\text{-}RSA},\mathsf{Sim},\mathcal{A}}(\lambda)$. □

DL and Pairing-Based Constructions. We now move to the DL and pairing-based settings and focus on the signature schemes by Schnorr [25] and by Boneh and Boyen [5], respectively.

Schnorr Signature Scheme. Let $G = \langle g \rangle$ be a cyclic group of prime order q, where $|q| = \lambda$, and $H : \{0,1\}^* \to \mathbb{Z}_q$ be a hash function modeled as random oracle. Schnorr's signature scheme is specified as follows.

$\mathsf{SCH.KGen}(1^\lambda)$: Choose $x \in_R \mathbb{Z}_q$. Output $(sk, pk) := (x, g^x)$.
$\mathsf{SCH.Sign}(sk, m)$: Choose $r \in_R \mathbb{Z}_q$. Let $c \leftarrow H(g^r \parallel m)$ and $s := sk \cdot c + r \bmod q$. Output $\sigma := (c, s)$.
$\mathsf{SCH.Ver}(pk, m, \sigma)$: Parse σ as (c, s). Compute $c' \leftarrow H(pk^{-c} \cdot g^s \parallel m)$. Output $c = c'$.

In the indistinguishability analysis (akin to prior work on anonymity and confidentiality of the scheme [16,28]) we assume that all signers use the same group G.

Lemma 7. *The (generalized) Schnorr signature scheme is indistinguishable with full key exposure, in the random oracle model.*

Proof. Consider the following simulator Sim: On input security parameter 1^λ and message number ℓ, Sim independently samples ℓ random pairs $(c'_1, s'_1), \ldots, (c'_\ell, s'_\ell) \in_R \mathbb{Z}_q \times \mathbb{Z}_q$ and outputs $\boldsymbol{\sigma}^* = (\sigma_i)_{1 \le i \le \ell}$, where $\sigma_i = (c'_i, s'_i)$. Let $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$ be any indistinguishability adversary against the Schnorr signature scheme. Denote by $\mathsf{Exp}^{\mathsf{IND},0,j}_{\mathsf{SCH},\mathsf{Sim},\mathcal{A}}(\lambda)$ the experiment that is like $\mathsf{Exp}^{\mathsf{IND},0}_{\mathsf{SCH},\mathsf{Sim},\mathcal{A}}(\lambda)$, except that the first j signatures in $\boldsymbol{\sigma}^*$

are simulated using $\mathsf{Sim}(1^\lambda, j)$, i.e. $\mathsf{Exp}^{\mathsf{IND},0}_{\mathsf{SCH},\mathsf{Sim},\mathcal{A}}(\lambda) = \mathsf{Exp}^{\mathsf{IND},0,0}_{\mathsf{SCH},\mathsf{Sim},\mathcal{A}}(\lambda)$ and $\mathsf{Exp}^{\mathsf{IND},1}_{\mathsf{SCH},\mathsf{Sim},\mathcal{A}}(\lambda) = \mathsf{Exp}^{\mathsf{IND},0,\ell}_{\mathsf{SCH},\mathsf{Sim},\mathcal{A}}(\lambda)$ for some ℓ polynomially bounded by λ. It suffices to prove that, for all j,

$$\left|\Pr\left[\mathsf{Exp}^{\mathsf{IND},0,j}_{\mathsf{SCH},\mathsf{Sim},\mathcal{A}}(\lambda) = 1\right] - \Pr\left[\mathsf{Exp}^{\mathsf{IND},0,j+1}_{\mathsf{SCH},\mathsf{Sim},\mathcal{A}}(\lambda) = 1\right]\right|$$

is negligible.

Denote by Exp the experiment which is like $\mathsf{Exp}^{\mathsf{IND},0,j}_{\mathsf{SCH},\mathsf{Sim},\mathcal{A}}(\lambda)$ except that, in the generation of the $(j+1)$th signature of $\boldsymbol{\sigma}^*$, we replace the output of hash function H by a value $c' \in_R \mathbb{Z}_q$, picked uniformly at random. By the Random Oracle Model, this change can only be detected by adversaries that correctly guess both: group element g^r and message m. This will happen only with negligible probability, since $\mathcal{A}_1$ would have to guess g^r (with success probability $\frac{1}{q} \approx 2^{-\lambda}$), and $\mathcal{A}_2$ would have to guess m, which has large entropy. Note that c is now independent of r, i.e., in the calculation of $s := sk \cdot c + r$, variable r acts like a one-time pad on $sk \cdot c$. It follows that also s can be replaced by a uniformly random value $s' \in_R \mathbb{Z}_q$, without $\mathcal{A}$ noticing it. We have just shown that $|\Pr[\mathsf{Exp}^{\mathsf{IND},0,j}_{\mathsf{SCH},\mathsf{Sim},\mathcal{A}}(\lambda) = 1] - \Pr[\mathsf{Exp} = 1]|$ is negligible, and that $|\Pr[\mathsf{Exp} = 1] - \Pr[\mathsf{Exp}^{\mathsf{IND},0,j+1}_{\mathsf{SCH},\mathsf{Sim},\mathcal{A}}(\lambda) = 1]| = 0$. This concludes the proof. □

Boneh-Boyen Signature Scheme. The signature scheme by Boneh and Boyen [5] based on pairings works over cyclic groups G_1, G_2, G_T of prime order q (with $|q| = \lambda$) for which an efficient bilinear map $e : G_1 \times G_2 \to G_T$ is known. Let g_1 and g_2 be generators of G_1 and G_2, respectively. The scheme is specified for message space $\mathbb{Z}_q$ as follows.

$\mathsf{BB.KGen}(1^\lambda)$: Choose $x, y \in_R \mathbb{Z}_q \setminus \{0\}$. Let $sk := (x, y)$ and $pk := (u, v) = (g_2^x, g_2^y)$. Output (sk, pk).
$\mathsf{BB.Sign}(sk, m)$: Choose $r \in_R \mathbb{Z}_q \setminus \{-\frac{x+m}{y}\}$. Let $\sigma' := g_1^{1/(x+m+yr)}$. Output $\sigma := (\sigma', r)$.
$\mathsf{BB.Ver}(pk, m, \sigma)$: Parse σ as (σ', r). Output $e(\sigma, u g_2^m v^r) = e(g_1, g_2)$.

Lemma 8. *The "hash-then-sign" version of the signature scheme by Boneh and Boyen is indistinguishable with full key exposure, in the random oracle model.*

We first prove that this construction is indistinguishable (in the standard model), yet for uniform message distributions only, and then generalize this result to arbitrary distributions in $\{0,1\}^*$ (in the random oracle model).

Lemma 9. *Signature scheme* BB *is (perfectly) indistinguishable with respect to full key exposure, for* uniformly *distributed messages.*

Proof. Consider the following simulator Sim: On input security parameter 1^λ and message number ℓ, Sim independently samples ℓ random pairs $(\sigma', r) \in_R (G_1 \setminus \{1\}) \times \mathbb{Z}_q$. Let $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$ be any indistinguishability adversary against the BB signature scheme such that $\mathcal{A}_1$ outputs uniformly distributed messages in $\mathbb{Z}_q$. Denote by $\mathsf{Exp}^{\mathsf{IND},0,j}_{\mathsf{BB},\mathsf{Sim},\mathcal{A}}(\lambda)$ the experiment that is like $\mathsf{Exp}^{\mathsf{IND},0}_{\mathsf{BB},\mathsf{Sim},\mathcal{A}}(\lambda)$, except that the first j signatures in $\boldsymbol{\sigma}^*$ are simulated using $\mathsf{Sim}(1^\lambda, j)$, i.e. $\mathsf{Exp}^{\mathsf{IND},0}_{\mathsf{BB},\mathsf{Sim},\mathcal{A}}(\lambda) = \mathsf{Exp}^{\mathsf{IND},0,0}_{\mathsf{BB},\mathsf{Sim},\mathcal{A}}(\lambda)$ and finally $\mathsf{Exp}^{\mathsf{IND},1}_{\mathsf{BB},\mathsf{Sim},\mathcal{A}}(\lambda) = \mathsf{Exp}^{\mathsf{IND},0,\ell}_{\mathsf{BB},\mathsf{Sim},\mathcal{A}}(\lambda)$ for some ℓ polynomially bounded by λ.

Note that in $\mathsf{BB.Sign}$ the mapping $r \mapsto \sigma' = g_1^{1/(x+m+yr)}$ is one-to-one between domain $\mathbb{Z}_q \setminus \{-\frac{x+m}{y}\}$ and range $G_1 \setminus \{1\}$. Basically, this is due to the fact that $\mathbb{Z}_q$ is a finite field, in which all elements but zero can be multiplicatively inverted. It follows that, if r is picked uniformly at random from the given domain, then r acts like a one-time pad on m and makes σ' uniformly distributed, in $\mathcal{A}_1$'s eyes. The analog holds for $\mathcal{A}_2$: This time, it is uniformly distributed message m that makes σ' look uniform. This shows that $\Pr[\mathsf{Exp}^{\mathsf{IND},0,j}_{\mathsf{BB},\mathsf{Sim},\mathcal{A}}(\lambda) = 1] = \Pr[\mathsf{Exp}^{\mathsf{IND},0,j+1}_{\mathsf{BB},\mathsf{Sim},\mathcal{A}}(\lambda) = 1]$ for all j, and hence concludes the proof. □

In general, digital signature schemes are expected to support arbitrary message spaces, i.e. messages $m \in \{0,1\}^*$. As pointed out by Boneh and Boyen [5], their scheme can be converted into an unforgeable signature scheme for arbitrary long messages by using the "hash-then-sign" approach, for a suitable hash function $H : \{0,1\}^* \to \mathbb{Z}_q$. Such 'hybrid' version of BB can still be proven unforgeable in the standard model, as the only condition posed on H is that of collision-resistance. If, on the other hand, the hash function H is additionally modeled as a random oracle (that smoothes the entropy in the message space to a uniform distribution) the proof of Lemma 8 follows directly from Lemma 9.

5 Pseudorandom Signatures

Although indistinguishability is already a strong privacy notion it still has one important limitation: The simulator Sim used to define the IND property depends on the signature scheme S; in particular, it simulates signatures using public parameters of S. Although both the signer and the message are successfully hidden in IND signatures, the very scheme that was used to create a given signature might not be, e.g. IND signatures may have characteristic lengths or follow specific formats, like element representation of the components of Schnorr signatures, and so on. In practice, usage of some S in an application or network protocol can be prescribed via standards. However, instantiations with concrete parameters (e.g. prime modulus p in a Schnorr group $G \subseteq \mathbb{Z}_p^\times$) is often left unspecified. Different parameter choices may introduce a unique pattern that can be (mis)used to distinguish among the signing algorithms and by this obtain more information about signers and about the context in which the signatures were produced.

We address this limitation in Definition 7 with the property of *pseudorandomness*, where we require that signatures output by S are indistinguishable from randomly chosen binary strings of length $L(\lambda) = L_{\mathsf{S}}(\lambda)$. This simpler definition is sufficient to obtain pseudorandom signatures of some fixed length L^*, viewed as a global upper bound on the individual lengths $L_{\mathsf{S}}(\lambda)$ for all signature schemes S in the system, using a simple *padding with random bits*. That is, *all* signatures in the system would be L^* bits long and look completely random, no matter how they were produced. It would hence become impossible, for some given signature σ to derive any information about the scheme S that was used to generate it. This seems to be the highest level of privacy that can be offered by a signature scheme.

Definition 7 (Pseudorandom Signatures). *A signature scheme* S *is* pseudorandom (PR)*, possibly* with full key exposure ($\mathsf{PR\text{-}FKE}$)*, if there is a polynomially bounded function* $L(\lambda)$ *such that for all PPT adversaries* $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$ *the advantage function*

$$\mathsf{Adv}_{\mathsf{S},\mathcal{A}}^{\mathsf{PR[\text{-}FKE]}}(\lambda) := \left| \Pr\left[\mathsf{Exp}_{\mathsf{S},\mathcal{A}}^{\mathsf{PR[\text{-}FKE]},0}(\lambda) = 1\right] - \Pr\left[\mathsf{Exp}_{\mathsf{S},\mathcal{A}}^{\mathsf{PR[\text{-}FKE]},1}(\lambda) = 1\right] \right|$$

is negligible in λ*, where* $\mathsf{Exp}_{\mathsf{S},\mathcal{A}}^{\mathsf{PR[\text{-}FKE]},b}(\lambda)$*,* $b \in \{0,1\}$*, are the* pseudorandomness experiments *from Figure 5, and where the following* high entropy constraint *holds: The function* $\mu(\lambda) = \max_{M \in \{0,1\}^*} \Pr[M \in \boldsymbol{m} : (\boldsymbol{m}, t) \leftarrow \mathcal{A}_1]$ *is negligible in* λ*, assuming that* $\mathcal{A}_1$ *is provided with all admissible inputs and oracles as specified in the respective pseudorandomness experiment. The* minimum entropy *of* $\mathcal{A}$ *is then given by* $-\log_2 \mu(\lambda)$*.*

```
$\mathsf{Exp}_{\mathsf{S},\mathcal{A}}^{\mathsf{PR},b}(\lambda)$ :
    $(sk, pk) \leftarrow \mathsf{KGen}(1^\lambda)$
    $(\boldsymbol{m}, t) \leftarrow \mathcal{A}_1^{\mathsf{Sign}(sk,\cdot)}(pk)$
    $\boldsymbol{\sigma}_0 \leftarrow \mathsf{Sign}(sk, \boldsymbol{m})$
    $\boldsymbol{\sigma}_1 \in_R \{0,1\}^{L(\lambda) \times |\boldsymbol{m}|}$
    $t' \leftarrow \mathcal{A}_2^{\mathsf{Sign}(sk,\cdot)}(pk, \boldsymbol{\sigma}_b)$
    if $t' = t$ then output 1, else output 0
```

```
$\mathsf{Exp}_{\mathsf{S},\mathcal{A}}^{\mathsf{PR\text{-}FKE},b}(\lambda)$ :
    $(sk, pk) \leftarrow \mathsf{KGen}(1^\lambda)$
    $(\boldsymbol{m}, t) \leftarrow \mathcal{A}_1(sk, pk)$
    $\boldsymbol{\sigma}_0 \leftarrow \mathsf{Sign}(sk, \boldsymbol{m})$
    $\boldsymbol{\sigma}_1 \in_R \{0,1\}^{L(\lambda) \times |\boldsymbol{m}|}$
    $t' \leftarrow \mathcal{A}_2(sk, pk, \boldsymbol{\sigma}_b)$
    if $t' = t$ then output 1, else output 0
```

Fig. 5. Pseudorandomness Experiments (without and with Full Key Exposure).[11]

Pseudorandomness is as a special case of indistinguishability, where simulator Sim draws at random from $\{0,1\}^{L(\lambda)}$. However, PR is strictly stronger than IND, i.e. Lemmas 10 and 11 settle the PR notion at the top of the privacy hierarchy:

[11] We denote by $\boldsymbol{\sigma} \in_R \{0,1\}^{L \times |\boldsymbol{m}|}$ the process of picking $|\boldsymbol{m}|$ strings independently at random from $\{0,1\}^L$. We comprehend $L(\lambda)$ as the fixed length of signatures conforming to security level λ.

Lemma 10 ($\mathsf{PR} \Rightarrow \mathsf{IND}$, $\mathsf{PR\text{-}FKE} \Rightarrow \mathsf{IND\text{-}FKE}$)**.** *Every pseudorandom signature scheme is indistinguishable. The same implication holds with full key exposure.*

Proof. The lemma follows directly from Definitions 6 and 7 by choosing the simulator Sim that draws signatures at random from $\{0,1\}^{L(\lambda)}$ in the indistinguishability experiment.

Lemma 11 ($\mathsf{IND[\text{-}FKE]} \not\Rightarrow \mathsf{PR}$)**.** *Indistinguishable signature schemes (with full key exposure) are not necessarily pseudorandom.*

Proof. Let S be an indistinguishable signature scheme, with simulator Sim. We construct an indistinguishable but not pseudorandom signature scheme S' from S as follows.

$\mathsf{KGen}'(1^\lambda)$: Output $(sk, pk) \leftarrow \mathsf{KGen}(1^\lambda)$.
$\mathsf{Sign}'(sk, m)$: $\sigma \leftarrow \mathsf{Sign}(sk, m)$. Output $\sigma' := \sigma \,\|\, 1$.
$\mathsf{Ver}'(pk, m, \sigma')$: Parse σ' as $\sigma \,\|\, b$. Return 1 iff $\big(\mathsf{Ver}(pk, m, \sigma) = 1 \wedge b = 1\big)$.

Scheme S' is not pseudorandom: Define $\mathcal{A}_1$ to pick single random messages $m \in_R \{0,1\}^\lambda$, and output $(\boldsymbol{m}, 1)$, where $\boldsymbol{m} = (m)$. Let $\mathcal{A}_2$, on input $\boldsymbol{\sigma} = (\sigma)$, output the last bit of σ. We compute $\mathcal{A}$'s advantage as follows:

$$\mathsf{Adv}^{\mathsf{PR}}_{\mathsf{S}',\mathcal{A}}(\lambda) = \left|\Pr\left[\mathsf{Exp}^{\mathsf{PR},0}_{\mathsf{S}',\mathcal{A}}(\lambda) = 1\right] - \Pr\left[\mathsf{Exp}^{\mathsf{PR},1}_{\mathsf{S}',\mathcal{A}}(\lambda) = 1\right]\right| = \left|1 - \tfrac{1}{2}\right| = \tfrac{1}{2}.$$

However, S' is still indistinguishable: An appropriate simulator $\mathsf{Sim}'(1^\lambda)$ is given by $\mathsf{Sim}(1^\lambda) \,\|\, 1$. It is straightforward to show that any successful indistinguishability adversary for S' can be turned into a successful adversary against S. □

5.1 Two Pseudorandomness Compilers

We present two compilers for pseudorandomness of digital signatures. Our first compiler assumes that the underlying scheme is indistinguishable (with some additional constraints), while our second compiler offers pseudorandomness for arbitrary (unforgeable) signature schemes. Both transformations work *without* random oracles.

IND-to-PR Compiler: From Indistinguishability to Pseudorandomness. Our IND-to-PR compiler converts any indistinguishable signature scheme into a pseudorandom one. This is done by considering the different elements that form the signature component-wise (e.g., in case of Schnorr signatures, the elements $c \in \mathbb{Z}_q$ and $s \in \mathbb{Z}_q$), and encoding them as binary strings via appropriate *admissible encodings*. Resulting strings are concatenated to obtain the pseudorandom signature. The concept of admissible encodings was created for the main purpose of hashing into elliptic curves in the IBE scheme of Boneh and Franklin [6]. Their definition was later generalized to arbitrary sets by Brier et al. [8], and used recently in the construction of a privacy-preserving authentication protocol by Bringer, Chabanne and Icart [9].

Definition 8 (Admissible Encoding [8]). *Let S, R denote finite sets with $|S| > |R|$. A function $F : S \to R$ is called* ϵ-admissible encoding *for (S, R) if it satisfies the following properties:*

1. *Computable: F is computable in deterministic polynomial time.*
2. *Invertible: There exists a PPT algorithm $\mathcal{I}_F$ such that $\mathcal{I}_F(r) \in F^{-1}(r) \cup \{\perp\}$ for all $r \in R$, and for r uniformly distributed in R the distribution of $\mathcal{I}_F(r)$ is ϵ-statistically indistinguishable from the uniform distribution in S.*

If ϵ is a negligible function of the security parameter then F is called an admissible encoding*.*

Intuitively, an admissible encoding $F : S \to R$ shifts the process of picking elements uniformly at random in S to the process of picking elements uniformly at random in R, and vice versa. Not surprisingly, the following aggregation lemma holds.

Lemma 12 (Aggregation of Admissible Encodings). *Let $\mathcal{S} = S_1 \times \ldots \times S_n$ and $\mathcal{R} = R_1 \times \ldots \times R_n$ denote Cartesian products of finite sets. For each $1 \leq i \leq n$, let $F_i : S_i \to R_i$ denote an ϵ_i-admissible encoding. Then $F : \mathcal{S} \to \mathcal{R}$; $(s_1, \ldots, s_n) \mapsto (F_1(s_1), \ldots, F_n(s_n))$ is an ϵ-admissible encoding, for $\epsilon = \sum_{i=1}^{n} \epsilon_i$.* □

In our compiler, we will use admissible encodings $F : S \to R$, where $S = \{0,1\}^{L(\lambda)}$ and R is the 'signature space' of the scheme. Note that w. l. o. g. it would even suffice to have $S = \{0,1\}^{\ell}$ for $\ell < L(\lambda)$ as we can always pad[12] with $L(\lambda) - \ell$ random bits at the end in $\mathcal{I}_F$, and ignore the last $L(\lambda) - \ell$ bits when evaluating F. Thus, if σ is indistinguishable then $\sigma' := \mathcal{I}_F(\sigma) \in \{0,1\}^{L(\lambda)}$ is pseudorandom. This admissible encoding-based compiler works as follows, where the input signature scheme S is assumed to be indistinguishable with a regular simulator and $(F, \mathcal{I}_F)$ denotes an appropriate admissible encoding that maps strings in $\{0,1\}^{L(\lambda)}$ into the signature space.

$\mathsf{AEC.KGen}(1^{\lambda})$: Output $(sk, pk) \leftarrow \mathsf{S.KGen}(1^{\lambda})$.
$\mathsf{AEC.Sign}(sk, m)$: Let $\sigma \leftarrow \mathsf{S.Sign}(sk, m)$. Output $\sigma' \leftarrow \mathcal{I}_F(\sigma)$.
$\mathsf{AEC.Ver}(pk, m, \sigma')$: Let $\sigma \leftarrow F(\sigma')$. Output $\mathsf{S.Ver}(pk, m, \sigma)$.

The pseudorandomness of the resulting scheme AEC is proven in Theorem 1. This proof requires the following notion of *regular simulators* that can be found in our proofs of IND signature schemes from Section 4.1 and exist for many other schemes.

Definition 9 (Regular Simulators). *A simulator* Sim *in the indistinguishability experiment (cf. Figure 4) is called* regular *if it samples uniformly at random from the 'signature space' $\mathcal{S}(\lambda)$, i.e. the range of the* Sign *algorithm. That is, for regular simulators* Sim*, running $\boldsymbol{\sigma}^* \leftarrow \mathsf{Sim}(1^{\lambda}, \ell)$ and $\boldsymbol{\sigma}^* \in_R \mathcal{S}(\lambda)^{\ell}$ are identical.*

Theorem 1. *If* S *is an indistinguishable signature scheme with a regular simulator* Sim *and F is an ϵ-admissible encoding that maps $\{0,1\}^{L(\lambda)}$ into the signature space of* S *then the* AEC *signature scheme, obtained via* IND*-to-*PR *compiler, is pseudorandom.*

Proof. Let $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$ be any pseudorandomness adversary against AEC signature scheme. Denote by Exp the experiment that is like $\mathsf{Exp}^{\mathsf{PR},0}_{\mathsf{AEC},\mathcal{A}}(\lambda)$, except that the signatures in $\boldsymbol{\sigma}^*$ are not computed individually as $\sigma := \mathcal{I}_F(\mathsf{S.Sign}(sk, m))$, but as $\boldsymbol{\sigma}^* := \mathcal{I}_F(\mathsf{Sim}(1^{\lambda}, |\boldsymbol{m}|))$, where $\mathcal{I}_F$ is executed component-wise. As S is indistinguishable by assumption, we know that $\left|\Pr\left[\mathsf{Exp}^{\mathsf{PR},0}_{\mathsf{AEC},\mathcal{A}}(\lambda) = 1\right] - \Pr\left[\mathsf{Exp} = 1\right]\right|$ is negligible. Consider now experiment Exp^j, which is like Exp except that the first j values in $\boldsymbol{\sigma}^*$ are randomly picked strings in $\{0,1\}^{L(\lambda)}$, i.e. $\mathsf{Exp} = \mathsf{Exp}^0$ and $\mathsf{Exp}^{\mathsf{PR},1}_{\mathsf{AEC},\mathcal{A}}(\lambda) = \mathsf{Exp}^{\ell}$ for some ℓ polynomially bounded by λ. As Sim is regular, the distribution of $\mathcal{I}_F(\mathsf{Sim}(1^{\lambda}, 1))$ is ϵ-close to the uniform distribution over $\{0,1\}^{L(\lambda)}$. That is, we proved that $\left|\Pr\left[\mathsf{Exp}^j = 1\right] - \Pr\left[\mathsf{Exp}^{j+1} = 1\right]\right| \leq \epsilon$ is negligible for all j. All in all, we showed $\mathsf{Adv}^{\mathsf{PR}}_{\mathsf{AEC},\mathcal{A}}(\lambda) = \left|\Pr\left[\mathsf{Exp}^{\mathsf{PR},0}_{\mathsf{AEC},\mathcal{A}}(\lambda) = 1\right] - \Pr\left[\mathsf{Exp}^{\mathsf{PR},1}_{\mathsf{AEC},\mathcal{A}}(\lambda) = 1\right]\right|$ is negligible. Note that AEC preserves the unforgeability of scheme S. □

As shown above, general transformation of indistinguishable signatures into pseudorandom becomes straightforward — once appropriate admissible encodings are identified. If signatures are formed by tuples of elements of certain sets then by the aggregation lemma it will suffice to identify encodings for these particular sets. Lemma 13 shows existence of admissible encodings for a variety of algebraic sets that are often used in practical cryptography, including sets behind the indistinguishable versions of FDH-RSA, Schnorr, and Boneh-Boyen schemes from Section 4.1.

Lemma 13 (Sets with Admissible Encodings). *For the following sets R there exist polynomials $\ell(\lambda)$ and admissible encodings $F : \{0,1\}^{\ell(\lambda)} \to R$:*

(1) Ranges $R = \{0, \ldots, N-1\} = \mathbb{Z}_N$ of natural numbers, for arbitrary $N \in \mathbb{N}$.

[12] Such pad/ignore steps can also be seen as the aggregation of F with the canonical admissible encoding for $\{0,1\}^{L(\lambda)-\ell} \to \{0,1\}^0$ (where $\{0,1\}^0$ denotes the language that contains only the empty word).

(2) The set of quadratic residues modulo safe primes p, i.e. $R = QR(p) \subseteq \mathbb{Z}_p^\times$.
(3) Arbitrary subgroups $G_q \subseteq \mathbb{Z}_p^\times$ of prime order q.
(4) The set $R = E(\mathbb{F})$ of rational points on (certain) elliptic curves, defined over a finite field.

Proof. The set $\{0,1\}^{\ell(\lambda)}$ can be canonically identified with $T^{\ell(\lambda)} := \mathbb{Z}_{2^{\ell(\lambda)}}$. It will hence, for all considered sets R, suffice to indicate admissible encodings $T^{\ell(\lambda)} \to R$.

(1) Let $N \in \mathbb{N}$ be a natural number, and $\lambda = |N|$ its length. Consider polynomial $\ell(\lambda) = 2\lambda$, function $F \colon T^{\ell(\lambda)} \to \mathbb{Z}_N; a \mapsto a \bmod N$, and the probabilistic mapping $\mathcal{I}_F \colon \mathbb{Z}_N \to T^{\ell(\lambda)};\ b \mapsto b + kN$ for random $k \in_R [0, \lfloor 2^{\ell(\lambda)}/N \rfloor - 1]$. It is easy to see that $\mathcal{I}_F$ inverts F. According to [26, Section 8.8], the statistical distance ϵ between $\mathcal{I}_F(r)$ for $r \in_R \mathbb{Z}_N$ and the uniform distribution in $T^{\ell(\lambda)}$ is bounded by $\epsilon < N/2^{\ell(\lambda)} \approx 2^\lambda/2^{2\lambda} = 2^{-\lambda}$, and hence negligible.

(2) and (3) Let $p = \alpha q + 1$ with primes p, q such that $\gcd(\alpha, q) = 1$ and $|p| = \lambda$ (if $\alpha = 2$ we have the safe prime setting). Let g be a generator of $G = \mathbb{Z}_p^\times$. Consider the probabilistic $\mathcal{I}_F \colon G_q \to \mathbb{Z}_p^\times;\ a \mapsto (g^q)^r a^{\alpha^{-1} \bmod q} \bmod p$ for $r \in_R \mathbb{Z}_\alpha$ together with its inversion $F \colon \mathbb{Z}_p^\times \to G_q;\ b \mapsto b^\alpha \bmod p$. As g^q and also $(g^q)^r$ have order α, it is easy to see that F perfectly 'inverts' $\mathcal{I}_F$. The encoding is 0-admissible as for every $h \in G$ we have $h = g^t = (g^q)^x (g^\alpha)^y$ for some t, x, y (by CRT or Euclid), i.e. every element in G is the (unique) product of the power of an order-α and the power of an order-q element. In above construction, the role of the former is taken by $(g^q)^r$, while element $a^{\alpha^{-1}} \in G_q$ corresponds to the latter. This encoding can be composed with (1) for $N = p$ to obtain the desired $F \colon \{0,1\}^{\ell(\lambda)} \to R$.

(4) We refer to Brier et al. [8] for an overview of (pairing-friendly) curves with suitable admissible encodings. □

Direct PR Compiler. The PR compiler introduced below outputs pseudorandom signatures (with full key exposure) for any signature scheme S; underlying techniques were proposed in [17] for building anonymous signatures. Its main building block is a pair of *associated randomness extractor $\mathcal{E}$ and hash function H*. Here, we only recall the properties of such a pair $(\mathcal{E}, H)$ and refer to [17] for a rigorous treatment. Basically, a randomized hash function H takes a message m and some randomness $r \in_R \{0,1\}^{t(\lambda)}$ and outputs $h = H(m; r)$. H is called *collision-intractable* if it is difficult to find $m \neq m'$ and $r \in \{0,1\}^{t(\lambda)}$ with $H(m; r) = H(m', r)$, for the same randomness r. The task of the randomness extractor $\mathcal{E}$ is to distill uniformly distributed strings of fixed length from inputs $x \leftarrow \mathcal{X}$ whose distribution is unknown but where a certain minimum level of entropy is assumed. As auxiliary input, $\mathcal{E}$ gets a uniformly distributed randomness $u \in \{0,1\}^{d(\lambda)}$. The extracted value is denoted by $\mathcal{E}(m; u)$. A pair $(\mathcal{E}, H)$ is called *pseudorandom* if tuples (r, y, u, e) and (r, y, u, v) are computationally indistinguishable, where $r \in_R \{0,1\}^{t(\lambda)}$, $y \leftarrow H(x; r)$, $u \in_R \{0,1\}^{d(\lambda)}$, $e \leftarrow \mathcal{E}(x; u)$, and $v \in_R \{0,1\}^{|e|}$, for $x \leftarrow \mathcal{X}$. Fischlin [17] offers an efficient instantiation for such primitive in the standard model[13]. Our analysis shows that this primitive gives rise to the following compiler for pseudorandom signatures, which are also indistinguishable and confidential (by Lemmas 10 and 5). We notice that this compiler results in somewhat less efficient schemes as opposed to our IND-to-PR compiler (e.g. when used with our IND examples).

DPRC.KGen(1^λ) : Output $(sk, pk) \leftarrow$ S.KGen(1^λ).
DPRC.Sign(sk, m) : Choose $r \in_R \{0,1\}^{t(\lambda)}$ and $u \in_R \{0,1\}^{d(\lambda)}$. Let $h \leftarrow H(m; r)$ and $\sigma \leftarrow$ S.Sign(sk, h). Compute $\tau := \sigma \oplus \mathcal{E}(m; u)$ and output $\sigma' := \tau \,\|\, r \,\|\, u$.
DPRC.Ver(pk, m, σ') : Parse σ' as $\sigma' = \tau \,\|\, r \,\|\, u$. Let $\sigma := \tau \oplus \mathcal{E}(m; u)$ and $h \leftarrow H(m; r)$. Output S.Ver(pk, h, σ).

Theorem 2. *If $(\mathcal{E}, H)$ is a pseudorandom pair of an associated randomness extractor $\mathcal{E}$ and a hash function H then for any signature scheme* S *the* DPRC *signature scheme, obtained using our direct* PR *compiler, is pseudorandom with respect to full key exposure (in the standard model).*

[13] In the random oracle model $H(x; r) := H^{\#}(0 \,\|\, x \,\|\, r)$ and $\mathcal{E}(x; u) := H^{\#}(1 \,\|\, x \,\|\, r)$ for a hash function $H^{\#}$ is an efficient instantiation of a pseudorandom associated pair $(\mathcal{E}, H)$.

Proof (Sketch). Anonymity of DPRC is shown in [17] by presenting a game-hopping proof that, in the first hop, modifies ANON game such that challenge signature σ^* is computed as specified in DPRC, except that τ is replaced by $\tau := \sigma \oplus v$ for random $v \in_R \{0,1\}^{|\mathcal{E}(m;u)|}$. As v acts as a one-time pad on σ, component τ is uniformly distributed in $\{0,1\}^{|\sigma|}$. Obviously, the concatenation $\sigma' = \tau \,\|\, r \,\|\, u$ is uniformly distributed as well, in $\{0,1\}^{|\sigma|+t(\lambda)+d(\lambda)}$. This shows pseudorandomness of DPRC. Note that the transformed scheme inherits its unforgeability from S under standard assumptions as proven in [17]. □

6 Conclusion

In this paper we gave a detailed account on the privacy hierarchy for ordinary signature schemes, taking into account earlier definitions of anonymity and confidentiality in the setting of high-entropic message spaces and system-wide known public keys. Our major result are pseudorandom signatures that cannot be distinguished from random strings and thus hide the entire information about message, signer, and signing algorithm. To obtain such fully private signatures we gave two compilers: the more efficient one adds pseudorandomness to indistinguishable signature schemes and we have shown that such schemes exist in different cryptographic settings; our second compiler, based on Fischlin's work [17], adds pseudorandomness to any unforgeable signature scheme but is less efficient (though in the standard model). In summary, with our hierarchy of privacy notions and generic transformations we showed how to efficiently achieve an ultimate form of privacy for arbitrary signature schemes, both in the random oracle and the standard model.

Acknowledgments.

The majority of work on this paper was performed while all its authors were in the Cryptographic Protocols Group at TU Darmstadt. This research was supported by the German Science Foundation (DFG) through the project PRIMAKE (MA 4957).

References

1. M. Bellare, A. Boldyreva, A. Desai, and D. Pointcheval. Key-Privacy in Public-Key Encryption. In *ASIACRYPT 2001*, *LNCS* 2248, pp. 566–582. 2001.
2. M. Bellare and S. Duan. Partial Signatures and their Applications. Cryptology ePrint Archive, Report 2009/336, 2009. `http://eprint.iacr.org/2009/336`.
3. M. Bellare, M. Fischlin, A. O'Neill, and T. Ristenpart. Deterministic Encryption: Definitional Equivalences and Constructions without Random Oracles. In *CRYPTO 2008*, *LNCS* 5157, pp. 360–378. 2008.
4. M. Bellare and P. Rogaway. Random Oracles are Practical: A Paradigm for Designing Efficient Protocols. In *CCS 1993*, pp. 62–73. 1993.
5. D. Boneh and X. Boyen. Short Signatures Without Random Oracles and the SDH Assumption in Bilinear Groups. *J. of Cryptology*, 21(2):149–177, 2008.
6. D. Boneh and M. Franklin. Identity-Based Encryption from the Weil Pairing. In *CRYPTO 2001*, *LNCS* 2139, pp. 213–229. 2001.
7. D. Boneh, B. Lynn, and H. Shacham. Short Signatures From the Weil Pairing. *J. of Cryptology*, 17(4):297–319, 2004.
8. E. Brier, J.-S. Coron, T. Icart, D. Madore, H. Randriam, and M. Tibouchi. Efficient Indifferentiable Hashing into Ordinary Elliptic Curves. In *CRYPTO 2010*, *LNCS* 6223, pp. 237–254. 2010.
9. J. Bringer, H. Chabanne, and T. Icart. Password Based Key Exchange Protocols on Elliptic Curves Which Conceal the Public Parameters. In *ACNS 2010*, *LNCS* 6123, pp. 291–308. 2010.
10. C. Cachin. An Information-Theoretic Model for Steganography. In *Information Hiding 1998*, *LNCS* 1525, pp. 306–318. 1998.
11. J. Camenisch and A. Lysyanskaya. A Signature Scheme with Efficient Protocols. In *Security in Communication Networks 2002*, *LNCS* 2576, pp. 268–289. 2003.
12. R. Canetti. Towards Realizing Random Oracles: Hash Functions That Hide All Partial Information. In *CRYPTO 1997*, *LNCS* 1294, pp. 455–469. 1997.

13. R. Canetti and H. Krawczyk. Security Analysis of IKE's Signature-Based Key-Exchange Protocol. In *CRYPTO 2002*, *LNCS* 2442, pp. 143–161. 2002.
14. D. Chaum and E. van Heyst. Group Signatures. In *EUROCRYPT 1991*, *LNCS* 547, pp. 257–265. 1991.
15. R. Cramer and V. Shoup. Signature Schemes Based on the Strong RSA Assumption. *ACM TISSEC*, 3(3):161–185, 2000.
16. A. W. Dent, M. Fischlin, M. Manulis, M. Stam, and D. Schröder. Confidential Signatures and Deterministic Signcryption. In *PKC 2010*, *LNCS* 6056, pp. 462–479. 2010.
17. M. Fischlin. Anonymous Signatures Made Easy. In *PKC 2007*, *LNCS* 4450, pp. 31–42. 2007.
18. S. D. Galbraith and W. Mao. Invisibility and Anonymity of Undeniable and Confirmer Signatures. In *CT-RSA 2003*, *LNCS* 2612, pp. 80–97. 2003.
19. G. Greenleaf and R. Clarke. Privacy Implications of Digital Signatures. IBC Conference on Digital Signatures, 1997. Available at `http://www.anu.edu.au/people/Roger.Clarke/DV/DigSig.html`.
20. N. J. Hopper, J. Langford, and L. von Ahn. Provably Secure Steganography. In *CRYPTO 2002*, *LNCS* 2442, pp. 77–92. 2002.
21. K. Nyberg and R. Rueppel. Message Recovery for Signature Schemes Based on the Discrete Logarithm Problem. In *EUROCRYPT 1994*, *LNCS* 950, pp. 182–193. 1995.
22. J.-F. Raymond. Traffic Analysis: Protocols, Attacks, Design Issues, and Open Problems. In *Workshop on Design Issues in Anonymity and Unobservability 2000*, *LNCS* 2009, pp. 10–29. 2000.
23. R. L. Rivest, A. Shamir, and Y. Tauman. How to Leak a Secret. In *ASIACRYPT 2001*, *LNCS* 2248, pp. 552–565. 2001.
24. V. Saraswat and A. Yun. Anonymous Signatures Revisited. In *Provable Security 2009*, *LNCS* 5848, pp. 140–153. 2009.
25. C.-P. Schnorr. Efficient Identification and Signatures for Smart Cards. In *CRYPTO 1989*, *LNCS* 435, pp. 239–252. 1990.
26. V. Shoup. *A Computational Introduction to Number Theory and Algebra.* Cambridge Uni Press, 2008.
27. G. J. Simmons. The Prisoners' Problem and the Subliminal Channel. In *CRYPTO 1983*, pp. 51–67. 1983.
28. G. Yang, D. S. Wong, X. Deng, and H. Wang. Anonymous Signature Schemes. In *PKC 2006*, *LNCS* 3958, pp. 347–363. 2006.
29. R. Zhang and H. Imai. Strong Anonymous Signatures. In *Inscrypt 2008*, *LNCS* 5487, pp. 60–71. 2009.

A Privacy and Impossibility Results for Deterministic Signature Schemes

In the following, we discuss why the privacy properties anonymity, confidentiality, indistinguishability, and pseudorandomness from Definitions 3, 4, 6, and 7, respectively, can only be achieved by probabilistic signature schemes. By specifying further definitional constraints on the respective experiments, we obtain meaningful notions of these privacy properties for deterministic schemes. In addition, we give several impossibility results in case of full key exposure.

A.1 Anonymity of Deterministic Signature Schemes.

A trivial attack against anonymity of any deterministic signature scheme S works as follows: Let $P(\cdot)$ be some efficiently computable non-trivial predicate (e.g. the last bit of its argument) that is hard-coded into both $\mathcal{A}_1$ and $\mathcal{A}_2$. By random sampling and testing, $\mathcal{A}_1$ picks a message m for which $P(\sigma_0) = 0$ and $P(\sigma_1) = 1$, where $\sigma_0 \leftarrow \mathsf{Sign}(sk_0, m)$ and $\sigma_1 \leftarrow \mathsf{Sign}(sk_1, m)$. Adversary $\mathcal{A}_2$ outputs $P(\sigma)$ and clearly breaks the anonymity of the deterministic scheme S. Hence, any meaningful definition of anonymity for deterministic signature schemes will require at least the following additional constraint (whose name was coined for confidential signatures by Dent et al. [16]):

- *Signature free:* $\mathcal{A}_1$ may not output m that has been queried to the signing oracle before.

If we also allow full key exposure, where $\mathcal{A}_1$ learns both sk_0 and sk_1 and can sign messages on its own, then obviously the above constraint does not help:

Lemma 14. *There is no deterministic signature scheme that provides anonymity with full key exposure.*

Note that neither Yang et al. [28] nor Fischlin [17] addressed anonymity of deterministic schemes. In particular, their anonymity notions, used as a basis in Definition 3, did not reflect possible determinism of schemes.

A.2 Confidentiality of Deterministic Signature Schemes.

A trivial attack against confidentiality of deterministic signature schemes proceeds as follows: On each invocation, $\mathcal{A}_1$ outputs $(\boldsymbol{m}, t)$, where $\boldsymbol{m} = (M)$ consists of a single random high-entropy message M, and $t = \mathsf{Sign}(sk, M)$. $\mathcal{A}_2$ receives $\boldsymbol{\sigma}^* = (\sigma)$, outputs σ, and "wins" the experiment with advantage $1/2$. This and similar more sophisticated attacks can, again, be ruled out by a 'signature free' restriction, similar to the one stated on anonymous schemes, yet extended to message vectors:

– *Signature free:* $\mathcal{A}_1$ may not output $\boldsymbol{m}$ that contains a message m that has been queried to the signing oracle before.

Note that this constraint was also marked by Dent et al. [16] as being relevant to deterministic signature schemes in their definition of strong confidentiality.

As in the case of anonymity, the 'signature free' restriction cannot prevent the above attack against confidentiality of deterministic schemes if private signing keys are exposed, as the adversary could always sign $\boldsymbol{m}$ on its own.

Lemma 15. *There is no deterministic signature scheme that provides confidentiality with full key exposure.*

Yet, 'signature free' is not the only restriction that is necessary to define confidentiality of deterministic schemes in a reasonable way. In particular, we present another trivial attack against Definition 4: $\mathcal{A}_1$ flips a coin and outputs either $(\boldsymbol{m}, 0)$, where $\boldsymbol{m} = (M, M)$ for a random message M, or outputs $(\boldsymbol{m}, 1)$ with $\boldsymbol{m} = (M, M')$, $M \neq M'$. Adversary $\mathcal{A}_2$ just compares the two signatures in $\boldsymbol{\sigma}^*$ and outputs 0 or 1, accordingly. It seems that the following 'message uniqueness' constraint is sufficient to exclude this attack.

– *Message uniqueness:* for each $(\boldsymbol{m}, t) \leftarrow \mathcal{A}_1$ (where $\mathcal{A}_1$ is provided admissible inputs and oracles) and all $1 \leq i, j \leq |\boldsymbol{m}|$, we have $i \neq j \Rightarrow m_i \neq m_j$, i.e. no message is present twice in $\boldsymbol{m}$.

Intuitively, this is a rather natural constraint: The adversary would not gain any additional knowledge from asking the same message $m \in \{0,1\}^*$ twice to a *deterministic* signing oracle. Interestingly, Dent et al. [16] used the equivalent 'pattern preservation' constraint[14] in their definition, yet without marking it as being relevant for deterministic schemes only. We could not identify any reason why this constraint should be relevant for probabilistic schemes: Probabilistic signatures should not carry patterns existing within $\boldsymbol{m}$ over to $\boldsymbol{\sigma}^*$. Posing the constraint on such schemes would thus weaken the general confidentiality definition unnecessarily.

A.3 Indistinguishability of Deterministic Signature Schemes.

As in the case of deterministic anonymous and confidential signatures, we need additional constraints on the definition of indistinguishability for deterministic schemes:

– *Signature free:* $\mathcal{A}_1$ may not output $\boldsymbol{m}$ that contains a message m that has been queried to the signing oracle before.
– *Message uniqueness:* $\mathcal{A}_1$ may not output $\boldsymbol{m}$ that contains a single message twice

Basing on Lemmas 4 and 5 ($\mathsf{IND} \Rightarrow \mathsf{ANON}$ and $\mathsf{IND} \Rightarrow \mathsf{CONF}$, respectively), the following two impossibility results with regard to information recovering and deterministic signature schemes are implied immediately by Lemma 3 resp. Lemmas 14 and 15:

Corollary 1. *There is no information recovering signature scheme that provides indistinguishability.*

Corollary 2. *There is no deterministic signature scheme that provides indistinguishability with full key exposure.*

[14] The 'pattern preservation' constraint is defined as follows [16]: For any adversary $\mathcal{A}_1$ there exists a length function $\ell(\lambda)$ and relations $\diamond_{ij} \in \{=, \neq\}$ $(1 \leq i, j \leq \ell(\lambda))$ such that for all possible $(\boldsymbol{m}, t) \leftarrow \mathcal{A}_1$ (where $\mathcal{A}_1$ is provided admissible inputs and oracles) it is required that $|\boldsymbol{m}| = \ell(\lambda)$ and $m_i \diamond_{ij} m_j \, \forall i, j$. In other words: If some of the messages output by $\mathcal{A}_1$ are equal to each other (and hence form an "equality pattern"), then this pattern occurs in all vectors output by $\mathcal{A}_1$. For deterministic signature schemes, the notions of pattern preservation and message uniqueness are clearly equivalent.

A.4 Pseudorandomness of Deterministic Signature Schemes.

Not surprisingly, we also have to restrict the definition of pseudorandomness to fit deterministic signatures schemes. As for indistinguishability, the *'signature free'* and *'message uniqueness'* constraints have to be added. Clearly, the impossibility of obtaining deterministic IND schemes in case where secret keys are exposed (cf. Corollary 2) also applies to PR schemes, as Lemma 10 establishes '$\mathsf{PR} \Rightarrow \mathsf{IND}$'.

Corollary 3. *There is no deterministic signature scheme that provides pseudorandomness with full key exposure.*