Pseudorandom Signatures

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

[1]Cryptographic Protocols Group, Technische Universität Darmstadt, Germany
[2]Department of Computing, University of Surrey, United Kingdom
[3]Information Security Group, Royal Holloway, University of London, United Kingdom

Abstract. We develop a three-level hierarchy of privacy notions for (unforgeable) digital signatures, starting with existing notions of anonymity and confidentiality, whose independence we prove formally. The ultimate privacy goal in our hierarchy is *pseudorandomness*: signatures with this property hide the entire information about the signing process and they 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 prove that one way towards pseudorandom signatures leads over the mid-level notion, called *indistinguishability*: these signatures can be simulated using only the public parameters of the scheme. Indistinguishable signatures exist in different cryptographic settings (e.g. based on RSA, discrete logarithms, pairings) and can be efficiently lifted to the highest privacy level using general transformations based on appropriate encoding techniques. We also show a more direct way for obtaining pseudorandomness from any unforgeable signature scheme. Our transformations work in the standard model. We keep public verifiability of signatures in the setting of system-wide known public keys and we allow full disclosure of signatures, and even of secret signing keys, while working with messages of high entropy.

1 Introduction

A digital signature σ on a message m is generated by the signer in possession of the private key sk and is verified using the corresponding public key pk. Digital signatures are unforgeable and offer authenticity of signers and integrity of signed messages. In late 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 besides m also the identity of the signer — and owner of (certified) pk — to all intermediate parties and not only to the intended recipients/verifiers. Considering full disclosure of σ and that public keys are traditionally known to everyone we can hope to obtain privacy only by restricting the amount of publicly available information about the message m. In fact, messages can be delivered out-of-band, at some earlier or later point in time, or through a different communication channel, and thus, under reasonable assumptions, still remain out of reach of the adversary that obtains signatures and public keys. Further, verifiers may expect signatures on messages that need not be transmitted at all: for example, private outputs computed with secure multi-party computation techniques could be viewed as messages for which parties may also wish to exchange signatures.

Current Privacy Notions and Open Issues. Privacy of digital signatures in security models, where σ is revealed but associated m is not disclosed has found attention in the definitions of *anonymous signatures* by Yang et al. [28] and Fischlin [17], and in the recent 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 restriction, presuming the system-wide knowledge of public keys and full disclosure of 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 while also keeping 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 relationships amongst 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.

Pseudorandom Signatures and Applications. In fact, the most interesting question is whether signatures can look 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 would not know, whether a given datagram represents something potentially valuable (in this case signature) or not. On the other hand and more importantly, signatures that cannot be distinguished from random strings (of some fixed length) can be used to hide, which signing algorithm its signer was using — this knowledge alone is often sufficient to identify the signer (even if the signature scheme itself is anonymous).

For example, selection of elliptic curve parameters for use in the authentication protocols in the new European travel documents is the priority of respective states [9]; similarly, for security reasons, many banks and health insurance companies prefer to instantiate signing algorithms in customers' smart cards with their own parameters. In this case, even distinguishing amongst different settings/implementations/instantiations of the same 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 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, ... of length L^*. If *all* these signatures are random-looking then σ_i would hide the applied scheme S_i, i.e. only the verifier in possession of m (and the expected signer's pk) would be able to check validity of σ_i, while any other party (even with system-wide known public keys) would remain completely clueless whether σ_i represents a signature and, if so, which of the signing algorithms was used.

Furthermore, pseudorandom signatures would give rise to *covert public-key authentication* that can in turn be used for cryptographic protection of 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 be easily constructed using Diffie-Hellman approach in various groups based on techniques used in our work (cf. Lemma 12)) and then exchange pseudorandom signatures on the protocol transcript and the 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].

1.1 Our Results and Techniques

Privacy Hierarchy for Digital Signatures. We develop a three-level hierarchy of privacy notions for digital signatures and start our work with the investigation of the relationship between anonymity and confidentiality (the two previously established privacy notions for signatures). We use anonymity definitions of Yang et al. [28] with later refinements by Fischlin [17]. These definitions presume messages with high entropy (unlike definitions by Bellare and Duan [2] and by Saraswat and Yun [24], who regard a more restrictive form of signatures[1]). For confidentiality we use the original definitions by Dent et al. [16] (in its

[1] Anonymity definitions in [2, 24] assume that σ consists of two parts — signature σ_1 and some 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 does not learn σ_2. As discussed in [2, 24], this definition essentially implies anonymity

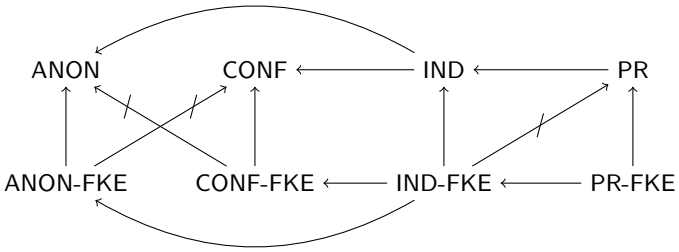


Fig. 1. Privacy Hierarchy for Ordinary Digital Signatures.
Notation: $X \to Y$ means that X is a strictly stronger privacy notion than Y. $X \nrightarrow Y$ means that X does not imply Y. X-FKE stands for the privacy notion X defined in the presence of full key exposure.

strongest version). We show that anonymous signatures and confidential signatures are independent privacy notions[2]. 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 put *indistinguishability* (IND) for signatures that can be simulated from the public parameters of the scheme. We prove that such signatures offer stronger privacy guarantees when compared to purely anonymous and purely confidential schemes. In particular, any transmission of an IND signature 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 the reasonable level of privacy in anticipated applications of both schemes. IND signatures may, however, leak some recognizable structure, which could be of potential interest to privacy attackers.

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.

All our privacy notions are additionally defined with respect to stronger privacy adversaries that are in possession of secret signing keys of users. That is, we also address security with *full key exposure* (FKE), which has been formalized for anonymous schemes by Fischlin [17] (and 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.

Along the path 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 by this on indistinguishability and pseudorandomness.

The resulting privacy hierarchy and relationships amongst its notions are illustrated in Figure 1.

Constructions and Transformations. On the practical side, we investigate indistinguishability and pseudorandomness of existing signature schemes and propose appropriate modifications and generic transformations. Essentially, we construct such 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

from [17, 28], allowing at the same time for low-entropy messages. Since we look on privacy from a more general perspective (e.g. consider confidentiality as another privacy goal) it appears for us more advisable to work with high-entropy messages and use conceptually simpler anonymity definitions from [17, 28].

[2] 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.

cyclic prime order groups on the example of Schnorr's scheme [25], and using parings on the example of the Boneh-Boyen (BB) scheme [5].

These results are summarized in Table 1 and detailed in the following.

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-and-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)

Indistinguishable Signatures. We first illustrate that in addition to known message recovering schemes (e.g. "text-book" RSA and Nyberg-Rueppel [21], together with their "hash-and-sign"-based transformations) several other schemes, which are widely used in different cryptographic contexts, fall under our more general notion of "information recovery" and thus do not offer indistinguishability, e.g. Cramer-Shoup (CS) [15], Camenisch-Lysyanskaya (CL) [11], and Boneh-Lynn-Shacham (BLS) [7]. That is, information can be leaked by signature schemes even if they do not let to recover 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 amongst all the 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-and-sign" approach can be used in the 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 is proven 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 protection that signature schemes can provide.

Our first result on PR signatures is a general transformation that strengthens IND signatures with 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 considering existence of 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 second result is another general 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, PR property is guaranteed even if secret signing keys are exposed. 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 general transformation, which is strong enough to convert any unforgeable signature scheme into a scheme satisfying the

strongest[3] privacy property. This direct PR compiler, however, is slightly less efficient than our IND-to-PR compiler.

1.2 Related Work on Privacy in Digital Signatures

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, proposing 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 from [2] uses randomized hash functions and can be applied to deterministic schemes. Their third solution relies on deterministic hash functions and can be used with probabilistic 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 unrevokable way) from a potential verifier, who would only learn that the signer is someone from 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. for undeniable and confirmer signatures by Galbraith and Mao [18]; as discussed in [24], these notions and goals differ from anonymity in ordinary signature schemes.

2 Previous Privacy Notions: Anonymity and Confidentiality

We recall the syntax of digital signatures in Definition 1. Note that all schemes used in this work are also unforgeable (cf. Appendix A). In the main part we focus on privacy of probabilistic[4] schemes in a setting with system-wide known public keys.

[3] Fischlin [17] mentioned informally that his anonymous signature scheme offers pseudorandomness, although the notion was not defined at that time. Our work clarifies his intuition formally and our privacy hierarchy further implies indistinguishability and confidentiality of his scheme (in presence of full key exposure).

[4] Due to space limitations all (impossibility) results on privacy for *deterministic* schemes have been moved to Appendix B.

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*.*

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 2 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 2 (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 3 corresponds to *strong confidentiality* from [16], the strongest amongst the three notions (weak, mezzo, strong) proposed there.

Definition 3 (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*

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

$\mathsf{Exp}^{\mathsf{CONF},b}_{\mathsf{S},\mathcal{A}}(\lambda)$:

$(sk, pk) \leftarrow \mathsf{KGen}(1^\lambda)$
$(\boldsymbol{m}_0, t_0) \leftarrow \mathcal{A}_1^{\mathsf{Sign}(sk,\cdot)}(pk)$
$(\boldsymbol{m}_1, t_1) \leftarrow \mathcal{A}_1^{\mathsf{Sign}(sk,\cdot)}(pk)$
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

$\mathsf{Exp}^{\mathsf{CONF\text{-}FKE},b}_{\mathsf{S},\mathcal{A}}(\lambda)$:

$(sk, pk) \leftarrow \mathsf{KGen}(1^\lambda)$
$(\boldsymbol{m}_0, t_0) \leftarrow \mathcal{A}_1(sk, pk)$
$(\boldsymbol{m}_1, t_1) \leftarrow \mathcal{A}_1(sk, pk)$
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). 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.

is negligible in λ, where $\mathsf{Exp}^{\mathsf{CONF[\text{-}FKE]},b}_{\mathsf{S},\mathcal{A}}(\lambda)$, $b \in \{0,1\}$, *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 that $\mathcal{A}_1$ is provided with all admissible inputs and oracles as specified in the respective confidentiality experiment. The* minimum entropy *of $\mathcal{A}$ is then given by* $-\log_2 \mu(\lambda)$.

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.[5]

2.3 Independence of Anonymity and Confidentiality

Lemmas 1 and 2, proven in Appendix C, 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 4.1).

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

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

3 Digital Signatures with Information Recovery

The following definition of 'information recovery', where in the verification procedure signer's public key is used to compute some information that is then compared to the information determined by the public key and the message, generalizes the known concept of 'message recovery' which can be obtained by viewing Inf as an algorithm which outputs its second argument.

Definition 4 (Information Recovering Signatures). *An (unforgeable) 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* $\mathsf{Inf}(pk, m) = \mathsf{Rec}(pk, \sigma)$.

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

3.1 Examples of Schemes with Information Recovery

Classical examples of schemes with information recovering include "text-book" RSA and Nyberg-Rueppel [21] whose signatures can be used to recover messages. Observe that if "hash-and-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 to be hashed for the computation of (unforgeable) signatures (as shown in Appendix D).

3.2 Information Recovery Limits Privacy

The property of information recovery can be immediately used to break confidentiality of the scheme by including information derived via algorithm Inf from messages in $\boldsymbol{m}$ into t (cf. Definition 3):

Lemma 3. *Information recovering signature schemes are not confidential (according to Definition 3).* □

4 Indistinguishability — Central Privacy Notion for Digital 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 5. 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.[6]

4.1 Definition and Implications of Indistinguishable Signatures

Definition 5 (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*

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

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

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

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

Lemma 5 ($\mathsf{IND} \Rightarrow \mathsf{CONF}$ and $\mathsf{IND\text{-}FKE} \Rightarrow \mathsf{CONF\text{-}FKE}$). *Every indistinguishable signature scheme is confidential. The corresponding implication holds in presence of full key exposure.*

[6] 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 procedure.

$\mathsf{Exp}^{\mathsf{IND},b}_{\mathsf{S},\mathsf{Sim},\mathcal{A}}(\lambda)$:

$(sk, pk) \leftarrow \mathsf{KGen}(1^\lambda)$

$(\boldsymbol{m}, t) \leftarrow \mathcal{A}_1^{\mathsf{Sign}(sk,\cdot)}(pk)$

$\boldsymbol{\sigma}_0 \leftarrow \mathsf{Sign}(sk, \boldsymbol{m})$

$\boldsymbol{\sigma}_1 \leftarrow \mathsf{Sim}(1^\lambda, |\boldsymbol{m}|)$

$t' \leftarrow \mathcal{A}_2^{\mathsf{Sign}(sk,\cdot)}(pk, \boldsymbol{\sigma}_b)$

if $t' = t$ then output 1

else output 0

$\mathsf{Exp}^{\mathsf{IND\text{-}FKE},b}_{\mathsf{S},\mathsf{Sim},\mathcal{A}}(\lambda)$:

$(sk, pk) \leftarrow \mathsf{KGen}(1^\lambda)$

$(\boldsymbol{m}, t) \leftarrow \mathcal{A}_1(sk, pk)$

$\boldsymbol{\sigma}_0 \leftarrow \mathsf{Sign}(sk, \boldsymbol{m})$

$\boldsymbol{\sigma}_1 \leftarrow \mathsf{Sim}(1^\lambda, |\boldsymbol{m}|)$

$t' \leftarrow \mathcal{A}_2(sk, pk, \boldsymbol{\sigma}_b)$

if $t' = t$ then output 1

else output 0

Fig. 4. Indistinguishability Experiments (without and with Full Key Exposure). As in Figure 3, $\boldsymbol{m}$ and $\boldsymbol{\sigma}$ are understood as *vectors* of messages and signatures, respectively.

4.2 Techniques and Examples of Indistinguishable Signature Schemes

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 fulfil this privacy notion directly or can be slightly modified to become indistinguishable. Here we summarize our results; the actual specification of the three schemes with corresponding proofs of Lemmas 6–8 are given in Appendix F.

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.

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

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. We come to the following results:

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

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

5 Pseudorandomness — Top Privacy Notion for Digital 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 amongst 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 6 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 the highest level of privacy that can be offered by a signature scheme.

Definition 6 (Pseudorandom Signatures). *A signature scheme* S *is* pseudorandom (PR)*, possibly* with full key exposure (PR-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*

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

is negligible in λ*, where* $\mathsf{Exp}^{\mathsf{PR[\text{-}FKE]},b}_{\mathsf{S},\mathcal{A}}(\lambda)$*,* $b \in \{0,1\}$*, 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* $-\log_2 \mu(\lambda)$*.*

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

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

Fig. 5. Pseudorandomness Experiments. 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.

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 9 and 10, proven in Appendix G, settle the PR notion at the top of the privacy hierarchy:

Lemma 9 (PR $\Rightarrow$ IND and PR-FKE $\Rightarrow$ IND-FKE). *Every pseudorandom signature scheme is indistinguishable. The same implication holds in the presence of full key exposure.*

Lemma 10 (IND[-FKE] $\not\Rightarrow$ PR). *Indistinguishable signature schemes (with full key exposure) are not necessarily pseudorandom.*

5.1 Two Pseudorandomness Compilers for Digital Signatures

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. (The corresponding proofs of Lemma 12 and Theorems 1 and 2 can be found in Appendix H.)

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 7 (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 11 (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[7] 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 is illustrated in Figure 6 and its pseudorandomness 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 4.2 and exist for many other schemes.

Definition 8 (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 in Figure 6, is pseudorandom.*

[7] 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).

$\mathsf{AEC.KGen}(1^\lambda)$:
$(sk, pk) \leftarrow \mathsf{S.KGen}(1^\lambda)$
output (sk, pk)

$\mathsf{AEC.Sign}(sk, m)$:
$\sigma \leftarrow \mathsf{S.Sign}(sk, m)$
$\sigma' \leftarrow \mathcal{I}_F(\sigma)$
output σ'

$\mathsf{AEC.Ver}(pk, m, \sigma')$:
$\sigma \leftarrow F(\sigma')$
output $\mathsf{S.Ver}(pk, m, \sigma)$

Fig. 6. IND-to-PR Compiler and Resulting AEC Signature Scheme. The input signature scheme S is assumed to be indistinguishable with a regular simulator. $(F, \mathcal{I}_F)$ denotes an appropriate admissible encoding that maps strings in $\{0,1\}^{L(\lambda)}$ into the signature space.

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 12 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 4.2.

Lemma 12 (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 $N \in \mathbb{N}$.
(2) The set of quadratic residues modulo safe primes p, i.e. $R = QR(p) \subseteq \mathbb{Z}_p^\times$.
(3) The set $R = E(\mathbb{F})$ of rational points on (certain) elliptic curves, defined over a finite field.

Direct PR Compiler. The PR compiler from Figure 7 outputs pseudorandom signatures (with full key exposure) for any signature scheme S; underlying techniques were proposed by Fischlin [17]. 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 $(\mathcal{E}, H)$ pair 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 $(\mathcal{E}, H)$ of associated randomness extractor and hash function 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[8]. Our analysis shows that this primitive gives rise to a compiler for pseudorandom signatures, which are also indistinguishable (by Lemma 9) and confidential (by Lemma 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).

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 in Figure 7, is pseudorandom with respect to full key exposure (in the standard model).*

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

[8] 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 $H^\#$ gives an efficient instantiation of a pseudorandom associated pair $(\mathcal{E}, H)$.

$\mathsf{DPRC.KGen}(1^\lambda)$:

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

output (sk, pk)

$\mathsf{DPRC.Sign}(sk, m)$:

$r \in_R \{0,1\}^{t(\lambda)}$

$u \in_R \{0,1\}^{d(\lambda)}$

$h \leftarrow H(m; r)$

$\sigma \leftarrow \mathsf{S.Sign}(sk, h)$

$\tau := \sigma \oplus \mathcal{E}(m; u)$

$\sigma' := \tau \,\|\, r \,\|\, u$

output σ'

$\mathsf{DPRC.Ver}(pk, m, \sigma')$:

parse σ' as $\sigma' = \tau \,\|\, r \,\|\, u$

$\sigma := \tau \oplus \mathcal{E}(m; u)$

$h \leftarrow H(m; r)$

output $\mathsf{S.Ver}(pk, h, \sigma)$

Fig. 7. Direct PR Compiler and Resulting DPRC Signature Scheme

system-wide known public keys. Our major result are pseudorandom signatures that cannot be distinguished from random strings and by this hide the entire information about the message, the signer, and the signing algorithm. To obtain such fully private signatures we gave two compilers: our most efficient compiler 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 (especially 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.

References

1. M. Bellare, A. Boldyreva, A. Desai, and D. Pointcheval. Key-Privacy in Public-Key Encryption. In *ASIACRYPT 2001*, volume 2248 of *LNCS*, pages 566–582. Springer, 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*, volume 5157 of *LNCS*, pages 360–378. Springer, 2008.
4. M. Bellare and P. Rogaway. Random Oracles are Practical: A Paradigm for Designing Efficient Protocols. In *ACM Conference on Computer and Communications Security (ACM CCS 1993)*, pages 62–73. ACM, 1993.
5. D. Boneh and X. Boyen. Short Signatures Without Random Oracles and the SDH Assumption in Bilinear Groups. *Journal of Cryptology*, 21(2):149–177, 2008.
6. D. Boneh and M. Franklin. Identity-based encryption from the weil pairing. In J. Kilian, editor, *Advances in Cryptology CRYPTO 2001*, volume 2139 of *Lecture Notes in Computer Science*, pages 213–229. Springer Heidelberg, 2001.
7. D. Boneh, B. Lynn, and H. Shacham. Short Signatures From the Weil Pairing. *Journal 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 T. Rabin, editor, *CRYPTO*, volume 6223 of *Lecture Notes in Computer Science*, pages 237–254. Springer, 2010.
9. J. Bringer, H. Chabanne, and T. Icart. Password based key exchange protocols on elliptic curves which conceal the public parameters. In J. Zhou and M. Yung, editors, *Applied Cryptography and Network Security*, volume 6123 of *Lecture Notes in Computer Science*, pages 291–308. Springer Heidelberg, 2010.
10. C. Cachin. An Information-Theoretic Model for Steganography. In *Information Hiding*, volume 1525 of *LNCS*, pages 306–318. Springer, 1998.
11. J. Camenisch and A. Lysyanskaya. A Signature Scheme with Efficient Protocols. In *3rd International Conference on Security in Communication Networks (SCN 2002)*, LNCS, pages 268–289. Springer, 2003.
12. R. Canetti. Towards Realizing Random Oracles: Hash Functions That Hide All Partial Information. In *CRYPTO 1997*, volume 1294 of *LNCS*, pages 455–469. Springer, 1997.
13. R. Canetti and H. Krawczyk. Security Analysis of IKE's Signature-Based Key-Exchange Protocol. In *CRYPTO 2002*, volume 2442 of *LNCS*, pages 143–161. Springer, 2002.

14. D. Chaum and E. van Heyst. Group Signatures. In *EUROCRYPT 1991*, volume 547 of *LNCS*, pages 257–265. Springer, 1991.
15. R. Cramer and V. Shoup. Signature Schemes Based on the Strong RSA Assumption. *ACM Transactions on Information and System Security*, 3(3):161–185, 2000.
16. A. W. Dent, M. Fischlin, M. Manulis, M. Stam, and D. Schröder. Confidential signatures and deterministic signcryption. In P. Q. Nguyen and D. Pointcheval, editors, *Public Key Cryptography*, volume 6056 of *Lecture Notes in Computer Science*, pages 462–479. Springer, 2010.
17. M. Fischlin. Anonymous signatures made easy. In T. Okamoto and X. Wang, editors, *Public Key Cryptography*, volume 4450 of *Lecture Notes in Computer Science*, pages 31–42. Springer, 2007.
18. S. D. Galbraith and W. Mao. Invisibility and Anonymity of Undeniable and Confirmer Signatures. In *CT-RSA 2003*, volume 2612 of *LNCS*, pages 80–97. Springer, 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*, volume 2442 of *LNCS*, pages 77–92. Springer, 2002.
21. K. Nyberg and R. Rueppel. Message Recovery for Signature Schemes Based on the Discrete Logarithm Problem. In *EUROCRYPT 1994*, volume 950 of *LNCS*, pages 182–193. Springer, 1995.
22. J.-F. Raymond. Traffic Analysis: Protocols, Attacks, Design Issues, and Open Problems. In *Workshop on Design Issues in Anonymity and Unobservability*, volume 2009 of *LNCS*, pages 10–29. Springer, 2000.
23. R. L. Rivest, A. Shamir, and Y. Tauman. How to Leak a Secret. In *ASIACRYPT 2001*, volume 2248 of *LNCS*, pages 552–565. Springer, 2001.
24. V. Saraswat and A. Yun. Anonymous signatures revisited. In *Proceedings of the 3rd International Conference on Provable Security*, ProvSec '09, pages 140–153, Berlin, Heidelberg, 2009. Springer-Verlag.
25. C.-P. Schnorr. Efficient Identification and Signatures for Smart Cards. In *CRYPTO 1989*, volume 435 of *LNCS*, pages 239–252. Springer, 1989.
26. V. Shoup. *A Computational Introduction to Number Theory and Algebra*. Cambridge University Press, New York, NY, USA, 2008.
27. G. J. Simmons. The Prisoners' Problem and the Subliminal Channel. In *CRYPTO 1983*, pages 51–67. Plenum Press, NY, 1983.
28. G. Yang, D. S. Wong, X. Deng, and H. Wang. Anonymous signature schemes. In M. Yung, Y. Dodis, A. Kiayias, and T. Malkin, editors, *Public Key Cryptography*, volume 3958 of *Lecture Notes in Computer Science*, pages 347–363. Springer, 2006.
29. R. Zhang and H. Imai. Strong anonymous signatures. In M. Yung, P. Liu, and D. Lin, editors, *Information Security and Cryptology*, pages 60–71. Springer-Verlag, Berlin, Heidelberg, 2009.

A Definition of Unforgeability

Definition 9 (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.*

B Privacy and Impossibility Results for Deterministic Signature Schemes

In the following, we discuss why the privacy properties anonymity, confidentiality, indistinguishability, and pseudorandomness from Definitions 2, 3, 5, and 6, 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.

B.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 anonymity of deterministic 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, see [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 the above constraint does not help:

Lemma 13. *There exists no deterministic signature scheme that is anonymous with full key exposure.* □

Note that neither [28] nor [17] addressed anonymity of deterministic schemes. In particular, their anonymity notions, used as a basis in Definition 2, did not reflect possible determinism of schemes.

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. This shows the following lemma.

Lemma 14. *There exists no deterministic signature scheme that is confidential 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 3: $\mathcal{A}_1$ 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 constraint on 'message uniqueness' 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 in* $\boldsymbol{m}$ *twice.*

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[9] 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 weaken the general confidentiality definition unnecessarily.

[9] 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.

Indistinguishability of Deterministic Signature Schemes. As in the case of deterministic anonymous and confidential signatures, we have to put an additional constraint on the definition of indistinguishability (Definition 5): For deterministic schemes S we will again need *'signature free'* — $\mathcal{A}_1$ may not output $\boldsymbol{m}$ that contains a message m that has been queried to the signing oracle before — and *'message uniqueness'* constraints — $\mathcal{A}_1$ 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 13 and 14:

Corollary 1. *There exists no information recovering signature scheme that is indistinguishable.*

Corollary 2. *There exists no deterministic signature scheme that is indistinguishable with full key exposure.*

Pseudorandomness of Deterministic Signature Schemes. Again, it is necessary to slightly modify definition of pseudorandomness to fit deterministic signatures schemes: For deterministic signature schemes S, we introduce the *'signature free' constraint*: $\mathcal{A}_1$ may not output m that has been queried to the signing oracle before. 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 9 establishes '$\mathsf{PR} \Rightarrow \mathsf{IND}$'.

Corollary 3. *There exists no deterministic signature scheme that is pseudorandom with full key exposure.* □

C Proofs of Lemmas 1 and 2 (Separating Anonymity and Confidentiality)

Proof of Lemma 1 (CONF[-FKE] $\not\Rightarrow$ ANON): We give an example of a signature scheme S' that is confidential but not anonymous. Let S be an arbitrary confidential signature scheme. We construct signature scheme S' from S as follows:

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

Since public keys can readily be extracted from signatures σ', the obtained scheme S' is not anonymous. Yet, S' remains confidential (as confidentiality adversaries $\mathcal{A}_1, \mathcal{A}_2$ know the public verification key pk anyway). Obviously, this construction preserves unforgeability. □

Proof of Lemma 2 (ANON[-FKE] $\not\Rightarrow$ CONF): We give an example of a signature scheme S' that is anonymous but not confidential. Let S be an arbitrary anonymous signature scheme and let $\mathtt{last} : \{0,1\}^* \to \{0,1\}$ denote the function that outputs the last bit of its argument. We construct signature scheme S' from S as follows:

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

To see that S' is not confidential, consider the following confidentiality adversary $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$. Algorithm $\mathcal{A}_1$ 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 $t_i = \mathtt{last}(M_i)$. Note that the $\boldsymbol{m}_i$ have high entropy according to Definition 3. Algorithm $\mathcal{A}_2$ parses $\boldsymbol{\sigma}^*$ as $\boldsymbol{\sigma}^* = ((\sigma, b))$ and outputs b. We have

$$\mathsf{Adv}^{\mathsf{CONF}}_{\mathsf{S}',\mathcal{A}}(\lambda) = \Big|\Pr\Big[\mathsf{Exp}^{\mathsf{CONF},0}_{\mathsf{S}',\mathcal{A}}(\lambda) = 1\Big] - \Pr\Big[\mathsf{Exp}^{\mathsf{CONF},1}_{\mathsf{S}',\mathcal{A}}(\lambda) = 1\Big]\Big| = \big|1 - 1/2\big| = 1/2.$$

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, algorithm $\mathcal{B}_1$ runs

$\mathcal{A}_1(pk_0, pk_1)$ as a black-box and receives message m. In case $\texttt{last}(m) = \beta$, this message is output. However, in case $\texttt{last}(m) \neq \beta$, the simulation aborts. This is modeled by letting $\mathcal{B}$'s simulator output 0 in this case, i.e. $\Pr[\mathsf{Exp}^{\mathsf{ANON},b}_{\mathsf{S},\mathcal{B}}(\lambda) = 1 | \texttt{ABORT}] = 0$ for $b \in \{0,1\}$. Note that event ABORT will occur with probability exactly $1/2$. Now, on input pk_0, pk_1, σ, algorithm $\mathcal{B}_2$ appends bit β to σ and runs $d \leftarrow \mathcal{A}_2(pk_0, pk_1, (\sigma, \beta))$. Bit d is the output of $\mathcal{B}_2$. We now have

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

and hence

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

This shows anonymity of S', as the left hand side of the equation is negligible by assumption. □

D Examples of Information Recovering Signature Schemes

D.1 Cramer-Shoup (CS) [15].

The Strong RSA-based CS schemes 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 $\sigma_1'^e \equiv t h^{H(s)} \bmod N$ and $\sigma_2'^{\tilde{e}} \equiv s h^m \bmod N$ 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 $\mathsf{Rec}(pk, \sigma)$ that returns 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 componentwise to verify the signature.

D.2 Camenisch-Lysyanskaya (CL) [11].

The Strong RSA-based CL scheme outputs signatures of the form $\sigma = (e, s, \sigma')$ and its verification algorithm checks whether e is in the appropriate range and if $\sigma'^e \equiv a^m b^s c \bmod N$ with a, b, c, and N being part of the public key pk. By rewriting this 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 algorithm $\mathsf{Rec}(pk, \sigma)$ to first check whether e is in the appropriate range and if so output $\sigma'^e \cdot (b^s c)^{-1} \bmod N$.

D.3 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 being in the public key pk, immediately defines algorithms $\mathsf{Inf}(pk, m)$ and $\mathsf{Rec}(pk, \sigma)$.

E Proofs of Lemmas 4 and 5 (Indistinguishability implies Anonymity and Confidentiality)

Proof of Lemma 4 ($\mathsf{IND} \Rightarrow \mathsf{ANON}$ and $\mathsf{IND\text{-}FKE} \Rightarrow \mathsf{ANON\text{-}FKE}$): Let S be an indistinguishable signature scheme, with simulator Sim. For an ANON-adversary $\mathcal{A}$ consider experiment $\mathsf{Exp}^{*}_{\mathsf{S},\mathsf{Sim},\mathcal{A}}(\lambda)$, 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 message m, algorithm $\mathcal{B}_1$ outputs $(\boldsymbol{m},t) = ((m),1)$ and stops. $\mathcal{B}_2$, on input pk and challenge signature $\boldsymbol{\sigma} = (\sigma)$, feeds σ into $\mathcal{A}_2$ (together with pk and pk'). Value d output by $\mathcal{A}_2$ is used as return value t' of $\mathcal{B}_2$. Careful inspection shows that

$$\Big|\Pr\big[\mathsf{Exp}^{\mathsf{ANON},0}_{\mathsf{S},\mathcal{A}}(\lambda)=1\big]-\Pr\big[\mathsf{Exp}^{*}_{\mathsf{S},\mathsf{Sim},\mathcal{A}}(\lambda)=1\big]\Big| =$$
$$\Big|\Pr\big[\mathsf{Exp}^{\mathsf{IND},0}_{\mathsf{S},\mathsf{Sim},\mathcal{B}}(\lambda)=1\big]-\Pr\big[\mathsf{Exp}^{\mathsf{IND},1}_{\mathsf{S},\mathsf{Sim},\mathcal{B}}(\lambda)=1\big]\Big| = \mathsf{Adv}^{\mathsf{IND}}_{\mathsf{S},\mathsf{Sim},\mathcal{B}}(\lambda)$$

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

Proof of Lemma 5 (IND $\Rightarrow$ CONF and IND-FKE $\Rightarrow$ CONF-FKE): 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 that challenge signatures $\boldsymbol{\sigma}^*$ are computed as $\boldsymbol{\sigma}^* \leftarrow \mathsf{Sim}(1^\lambda,|\boldsymbol{m}_0|)$. Construct IND-adversary $\mathcal{B}$ by 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 $\mathcal{A}_1^{\mathsf{Sign}(sk,\cdot),\mathsf{Sign}(sk',\cdot)}(pk)$ 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 $\mathcal{B}_2$. Careful inspection shows that

$$\Big|\Pr\big[\mathsf{Exp}^{\mathsf{CONF},0}_{\mathsf{S},\mathcal{A}}(\lambda)=1\big]-\Pr\big[\mathsf{Exp}^{*}_{\mathsf{S},\mathsf{Sim},\mathcal{A}}(\lambda)=1\big]\Big| =$$
$$\Big|\Pr\big[\mathsf{Exp}^{\mathsf{IND},0}_{\mathsf{S},\mathsf{Sim},\mathcal{B}}(\lambda)=1\big]-\Pr\big[\mathsf{Exp}^{\mathsf{IND},1}_{\mathsf{S},\mathsf{Sim},\mathcal{B}}(\lambda)=1\big]\Big| = \mathsf{Adv}^{\mathsf{IND}}_{\mathsf{S},\mathsf{Sim},\mathcal{B}}(\lambda)$$

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

F Indistinguishable Signature Schemes: Constructions and Proofs

F.1 Randomized FDH-RSA Signature Scheme with Padding and Proof of Lemma 6

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. Moreover, let Z_λ be a fixed number of 2λ bits, independently of N. The randomized FDH-RSA scheme with padding is presented in Figure 8. Observe that on each signature σ' a probabilistic padding is applied, computing $k \in_R [0,\ldots,\lfloor Z_\lambda/N\rfloor - 1]; \sigma := \sigma' + kN$, which can be reversed by computing $\sigma' := \sigma \bmod N$. This padding maps uniformly distributed integers from $[0,N-1]$ to (nearly) uniformly distributed integers in $[0,Z_\lambda-1]$ (cf. Lemma 12).

Proof of Lemma 6 (Randomized FDH-RSA with Padding is Indistinguishable). 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 $\mathsf{Exp}^{\mathsf{IND},0,j}_{\mathsf{FDH\text{-}RSA},\mathsf{Sim},\mathcal{A}}(\lambda)$, which are like $\mathsf{Exp}^{\mathsf{IND},0}_{\mathsf{FDH\text{-}RSA},\mathsf{Sim},\mathcal{A}}(\lambda)$, except that the first j signatures in $\boldsymbol{\sigma}^*$ are simulated using $\mathsf{Sim}(1^\lambda,j)$, i.e.

$\mathsf{FDH\text{-}RSA.KGen}(1^\lambda)$:

$(N, e, d) \leftarrow \mathsf{GenRSA}(1^\lambda)$

$pk := (N, e)$

$sk := d$

output (sk, pk)

$\mathsf{FDH\text{-}RSA.Sign}(sk, m)$:

$r \in_R \{0,1\}^\lambda$

$\sigma' := H_N(m \,\|\, r)^d \bmod N$

$k \in_R [0, \lfloor Z_\lambda / N \rfloor - 1]$

$\sigma := (\sigma' + kN, r)$

output σ

$\mathsf{FDH\text{-}RSA.Ver}(pk, m, \sigma)$:

parse σ as (σ', r)

$h' \leftarrow H_N(m \,\|\, r)$

$h := (\sigma')^e \bmod N$

output $h = h'$

Fig. 8. Randomized FDH-RSA Signature Scheme with Padding

$\mathsf{Exp}^{\mathsf{IND},0}_{\mathsf{FDH\text{-}RSA},\mathsf{Sim},\mathcal{A}}(\lambda) = \mathsf{Exp}^{\mathsf{IND},0,0}_{\mathsf{FDH\text{-}RSA},\mathsf{Sim},\mathcal{A}}(\lambda)$ 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.

Denote by Exp 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 12.(1) that this introduces only a negligible statistical difference between the output distributions of Exp and $\mathsf{Exp}^{\mathsf{IND},0,j+1}_{\mathsf{FDH\text{-}RSA},\mathsf{Sim},\mathcal{A}}(\lambda)$. □

F.2 Indistinguishability of Schnorr Signatures and Proof of Lemma 7

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 in Figure 9. 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.

$\mathsf{SCH.KGen}(1^\lambda)$:

$x \in_R \mathbb{Z}_q$

output $(sk, pk) := (x, g^x)$

$\mathsf{SCH.Sign}(sk, m)$:

$r \in_R \mathbb{Z}_q$

$c \leftarrow H(g^r \,\|\, m)$

$s := sk \cdot c + r \bmod q$

output $\sigma := (c, s)$

$\mathsf{SCH.Ver}(pk, m, \sigma)$:

parse σ as (c, s)

$c' \leftarrow H(pk^{-c} \cdot g^s \,\|\, m)$

output $c = c'$

Fig. 9. Schnorr Signature Scheme

Proof of Lemma 7 (Indistinguishability of Schnorr Signatures). 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 $|\Pr[\mathsf{Exp}^{\mathsf{IND},0,j}_{\mathsf{SCH},\mathsf{Sim},\mathcal{A}}(\lambda) = 1] - \Pr[\mathsf{Exp}^{\mathsf{IND},0,j+1}_{\mathsf{SCH},\mathsf{Sim},\mathcal{A}}(\lambda) = 1]|$ is negligible for all j.

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. □

F.3 Indistinguishability of Boneh-Boyen Signatures and Proof of Lemma 8

The pairing-based signature scheme by Boneh and Boyen [5] 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 in Figure 10, for message space $\mathbb{Z}_q$. 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).

$\mathsf{BB.KGen}(1^\lambda)$:
- $x, y \in_R \mathbb{Z}_q \setminus \{0\}$
- $sk := (x, y)$
- $pk := (u, v) = (g_2^x, g_2^y)$
- output (sk, pk)

$\mathsf{BB.Sign}(sk, m)$:
- $r \in_R \mathbb{Z}_q \setminus \{-\frac{x+m}{y}\}$
- $\sigma' := g_1^{1/(x+m+yr)}$
- output $\sigma := (\sigma', r)$

$\mathsf{BB.Ver}(pk, m, \sigma)$:
- parse σ as (σ', r)
- output $e(\sigma, ug_2^m v^r) = e(g_1, g_2)$

Fig. 10. Boneh-Boyen Scheme

In order to prove Lemma 8 we first prove the following lemma (which holds in the standard model).

Lemma 15. *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 $\mathsf{Exp}^{\mathsf{IND},1}_{\mathsf{BB},\mathsf{Sim},\mathcal{A}}(\lambda) = \mathsf{Exp}^{\mathsf{IND},0,\ell}_{\mathsf{BB},\mathsf{Sim},\mathcal{A}}(\lambda)$ for some ℓ polynomially bounded by λ.

Observe 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 15.

G Proofs of Lemmas 9 and 10 (Pseudorandomness implies Indistinguishability)

The proof of Lemma 9 ($\mathsf{PR} \Rightarrow \mathsf{IND}$ and $\mathsf{PR\text{-}FKE} \Rightarrow \mathsf{IND\text{-}FKE}$) follows directly from Definitions 5 and 6.

Proof of Lemma 10 ($\mathsf{IND}[\text{-}\mathsf{FKE}] \not\Rightarrow \mathsf{PR}$): We give an example of a signature scheme S' that is indistinguishable but not pseudorandom. Let S be an arbitrary indistinguishable signature scheme, with simulator Sim. We construct signature scheme S' from S as follows:

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

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

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

H Our Pseudorandomness Compilers: Proofs of Theorem 1, Lemma 12, and Theorem 2

Proof of Theorem 1 (Pseudorandomness of IND-to-PR Compiler). 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 that $\mathsf{Adv}^{\mathsf{PR}}_{\mathsf{AEC},\mathcal{A}}(\lambda) = \left|\Pr\left[\mathsf{Exp}^{\mathsf{PR},0}_{\mathsf{AEC},\mathcal{A}}(\lambda) = 1\right] - \Pr\left[\mathsf{Exp}^{\mathsf{PR},1}_{\mathsf{AEC},\mathcal{A}}(\lambda) = 1\right]\right|$ is negligible. Note that AEC preserves unforgeability of scheme S. □

Proof of Lemma 12 (Sets with Admissible Encodings). 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 $F : T^{\ell(\lambda)} \to \mathbb{Z}_N;\ a \mapsto a \bmod N$, and the probabilistic mapping $\mathcal{I}_F : \mathbb{Z}_N \to T^{\ell(\lambda)};\ b \mapsto b + kN$ 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) Let $p = 2p' + 1$ be a safe prime of length $|p| = \lambda$. It is known that $|\mathbb{Z}_p^{\times}| = 2|QR(p)|$. In addition, safe primes are always $p \equiv 3 \bmod 4$ (since p' is prime and hence odd) so that Legendre symbol $\left(\frac{-1}{p}\right)$ is negative, i.e. $-1 \notin QR(p)$. It follows that $\mathbb{Z}_p^{\times} = \langle -1 \rangle \times QR(p)$ and that the probabilistic mapping $\mathcal{I}_F : QR(p) \to \mathbb{Z}_p^{\times};\ a \mapsto (-1)^b a$ for random $b \in_R \{0,1\}$ together with its inversion $\mathbb{Z}_p^{\times} \to QR(p);\ b \mapsto b \cdot \left(\frac{b}{p}\right)$ is a (perfect) 0-admissible encoding. We compose this encoding with the one presented in (1), for $N = p$, to obtain the desired $F : \{0,1\}^{\ell(\lambda)} \to QR(p)$.
(3) We refer to Brier et al. [8] for an overview of (pairing-friendly) elliptic curves with suitable admissible encodings. □

Proof of Theorem 2 (Pseudorandomness of Direct PR Compiler). (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 [17]. □