Attribute-Based Signatures*

Hemanta K. Maji† Manoj Prabhakaran† Mike Rosulek‡

November 22, 2010

Abstract

We introduce *Attribute-Based Signatures (ABS)*, a versatile primitive that allows a party to sign a message with fine-grained control over identifying information. In ABS, a signer, who possesses a set of attributes from the authority, can sign a message with a predicate that is satisfied by his attributes. The signature reveals no more than the fact that a single user with some set of attributes satisfying the predicate has attested to the message. In particular, the signature hides the attributes used to satisfy the predicate and any identifying information about the signer (that could link multiple signatures as being from the same signer). Furthermore, users cannot collude to pool their attributes together.

We give a general framework for constructing ABS schemes, and then show several practical instantiations based on groups with bilinear pairing operations, under standard assumptions. Further, we give a construction which is secure even against a malicious attribute authority, but the security for this scheme is proven in the generic group model. We describe several practical problems that motivated this work, and how ABS can be used to solve them. Also, we show how our techniques allow us to extend Groth-Sahai NIZK proofs to be simulation-extractable and identity-based with low overhead.

1 Introduction

Alice, a finance manager in a big corporation, while going through her company's financial records, has learned about a major international scandal. She decides to send these records to a major newspaper, retaining her anonymity, but with a proof that she indeed has access to the records in question. It turns out that several people, due to a combination of reasons, may have access to these records: those in the New York, London or Tokyo office who are either finance managers associated with project Skam, or internal auditors. Alice considers using a *ring signature* [30] to endorse her message anonymously, but realizes that it is infeasible not only because of the large number of people involved, but also because she does not know who these people are. She realizes she cannot use a *group signature* [17] either, because the set of people Alice needs to refer to here is idiosyncratic to her purposes, and may not have been already collected into a group.[1] She is also aware of *mesh signatures* [11], but mesh signatures provide no way to convince the newspaper that the financial record was endorsed by a single person, not, say, a programmer in the New York office colluding with an internal auditor in the Smalltown office.

Alice's needs in this story reflect the challenges in a system where the roles of the users depend on the *combination* of attributes they possess. In such systems, users obtain multiple attributes from

*Partially supported by NSF grants CNS 07-16626 and CNS 07-47027.

†Department of Computer Science, University of Illinois, Urbana-Champaign. {hmaji2,mmp}@uiuc.edu.

‡Department of Computer Science, University of Montana. mikero@cs.umt.edu.

[1] Even if a group exists, the group manager could identify Alice as the informant.

one or more *attribute authorities*, and a user's capabilities in the system (e.g., sending or receiving messages, access to a resource) depend on their attributes. While offering several advantages, attribute-based systems also present fundamental cryptographic challenges. For instance, suppose Alice wants to simply send a message to the above group of people using an "attribute-based messaging" system; then to provide *end-to-end* secure communication, it must be possible for her to encrypt a message using attribute-keys (rather than individual users' keys). Recently cryptographic tools have emerged to tackle some of these challenges for encryption [33, 20, 4, 37]. In this work, we provide a solution for authentication, which among other things, will let Alice in the above example leak the financial records anonymously, but with the appropriate claim regarding her credentials.

Why attribute-based signatures?

The kind of authentication required in an attribute-based system differs from that offered by digital signatures, in much the same way public-key encryption does not fit the bill for attribute-based encryption. An attribute-based solution requires a richer semantics, including anonymity requirements, similar to signature variants like group signatures [17], ring signatures [30], and mesh signatures [11]. The common theme in all these signature primitives is that they provide a guarantees of *unforgeability* and *signer anonymity*. A valid signature can only be generated in particular ways, but the signature does not reveal any further information about which of those ways was actually used to generate it.

More specifically, group and ring signatures reveal only the fact that a message was endorsed by one of a list of possible signers. In a ring signature, the list is public, chosen by the signer *ad hoc*, and given explicitly. In a group signature, the group must be prepared in advance by a group manager, who can revoke the anonymity of any signer. In mesh signatures, a valid signature describes an access structure and a list of pairs (m_i, vk_i), where each vk_i is the verification key of a standard signature scheme. A valid mesh signature can only be generated by someone in posession of enough standard signatures σ_i, each valid under vk_i, to satisfy the given access structure.

In this work we introduce *attribute-based signatures (ABS)*. Signatures in an ABS scheme describe a message and a predicate over the universe of attributes. A valid ABS signature attests to the fact that "a single user, whose attributes satisfy the predicate, endorsed the message." We emphasize the word "single" in this informal security guarantee; ABS signatures, as in most attribute-based systems, require that colluding parties not be able to pool their attributes together.[2] Furthermore, attribute signatures do not reveal more than the claim being made regarding the attributes, even in the presence of other signatures.

Ring and group signatures are then comparable to special cases of ABS, in which the only allowed predicates are *disjunctions* over the universe of attributes (identities). Only one attribute is required to satisfy a disjunctive predicate, so in these cases collusion is not a concern. As in ring signatures, ABS signatures use *ad hoc* predicates. Mesh signatures allow more fine-grained predicates, but do not provide hiding of signature data that would be needed in an ABS scheme. A straight-forward application of mesh signatures as an ABS scheme would either allow collusion (as in the previous example, a New York programmer colluding with a Smalltown auditor to satisfy the "New York auditor" predicate) or allow signatures to be associated with a pseudonym of the signer (thus linking several signatures as originating from the same signer).

[2]Note that for attribute-based *encryption*, if collusion is allowed there are fairly easy solutions; but for ABS, even after allowing collusion (for instance by considering all users to have the same identity while generating keys), the residual primitive is essentially a mesh signature, which is already a non-trivial cryptographic problem.

Applications

Attribute-based signatures have natural applications in many systems where users' capabilities depend on possibly complex combinations of attributes. ABS is a natural choice for simple authentication in such systems. One of our motivations for developing such schemes comes from the authentication requirements in an Attribute-Based Messaging (ABM) system. In addition to the "leaking secrets" application described above, in Section 6 we also identify applications in trust negotiation systems.

Overview of Our Results

We introduce the concept of Attribute-Based Signatures (ABS) as a powerful primitive with several applications and several efficient instantiations. Our main technical contributions in this work are the following:

- A formal security definition for ABS, that includes the guarantees of unforgeability (even in the presence of collusion) and privacy for the signer.
- A general framework for constructing ABS schemes. Our framework consists of a "credential bundle" representing the attributes associated with a single user and a non-interactive proof of credential ownership that can be bound to a message. The credential bundle must have the property that multiple users should not be able to collude and combine their credentials. The proof system must have some zero-knowledge-like guarantee so that the signature does not leak information about the signer's identity or attributes.

  We instantiate this framework using Boneh-Boyen [8] or Waters [36] signatures as the credential bundle, and Groth-Sahai NIZK proofs [22] as the efficient non-interactive proof system. These instantiations provide practical ABS schemes secure under standard assumptions in bilinear groups.
- We present a practical ABS scheme suitable for high throughput systems. This construction deviates from our framework of credential bundles and proof of credential ownership. In this scheme we do employ a credential bundle scheme (same as the one in the last item above), but use a novel randomization technique to blind the actual attributes. This gives the best efficiency among our schemes. Further, this scheme remains secure even against a corrupt attribute-authority. However, the security of this scheme is proven in the heuristic generic-group model (augmented to handle groups with bilinear pairings).
- One of the most striking features of our construction is that it is very easily amenable to natural multi-authority settings. We describe practical considerations related to such a deployment.
- In Appendix E we show how our techniques of incorporating digital signatures and non-interactive proofs can be used to add *simulation-extractability* to the Groth-Sahai proof system, several orders of magnitude more efficiently than the only other comparable scheme, constucted by Groth in [21].

Which among the above schemes will suit an application will depend on the specific efficiency and security requirements in the system. In all these schemes, the privacy is unconditional, and it is only the unforgeability that depends on computational assumptions. Within a large enterprise setting (with pre-authenticated users) where the threat of forgery may be limited but the volume of signatures may be large, the final scheme may be the most suited. In more susceptible systems with a high security requirement, one of the schemes based on the Groth-Sahai proof systems maybe more suitable (at the expense of efficiency). The choice also depends on whether the application demands high-volume real-time performance (as in a messaging system) or involves only offline signing and verification (as in leaking a secret).

All of our instantiations depend on expressing the attribute predicate as a monotone-span program, which is the state of the art for attribute-based cryptography [20, 4, 37]. We remark that unlike in many constructions of attribute-based encryption schemes, we achieve "full security" in all our constructions. That is, we do not weaken the definition in the manner of "selective-ID" security. Nor do we need to limit our construction to a small universe of attributes. In all our instantiations, attributes can be arbitrary strings: given a collision-resistant hash function, an *a priori* unbounded attribute universe can be used.

Further Related Work

Groups with bilinear pairings have been used to construct identity-based (e.g., [10]) and attribute-based encryption schemes [33, 20, 4]. Non-interactive zero-knowledge proofs (including identity-based proofs) have previously been used in the context of efficient constructions of signature primitives [2, 24, 12, 21].

Khader [26, 25] proposes a notion called *attribute-based group signatures*. This primitive hides only the identity of the signer, but reveals which attributes the signer used to satisfy the predicate. It also allows a group manager to identify the signer of any signature (which is similar to the semantics of group signatures [17]); in contrast we require signer privacy to hold against everyone, including all authorities.

Subsequent to a preliminary (unpublished) version of this work, Li and Kim [28] gave an ABS scheme that supports predicates which are solely conjunctions of attributes (hence privacy is required only for the identity of the signer and not for the attributes used in satisfying the predicate), and is restricted to a "selective" unforgeability definition. Guo and Zeng [23] construct an attribute-based signature scheme, although their definition of security did not include any privacy for the signer. Shahandashti and Safavi-Naini [34] and Li et al. [27] construct efficient ABS schemes that support predicates consisting of a single threshold gate.

Binding a non-interactive proof to a message, as we do, is also a feature of *identity-based* proofs [24], in which every proof is bound to some identity, and proofs under one identity cannot be used to forge any proofs under a different identity. Indeed, such ID-based proofs have been used to construct signature-like primitives; however the construction from [24] does not have all the properties we need.

Anonymous credentials [16] is one primitive that has some parallels with ABS, but with goals that differ from ABS in several important ways. ABS could be considered as providing some of the functionality of AC as a very special case, but with a weaker anonymity guarantee. Conversely, some of the techniques used to construct efficient AC systems bear some resemblance to some of our efficient ABS constructions. In Appendix B we discuss these similarities and differences in more detail.

Another related primitive (but much simpler than ABS) is identity-based signatures (IBS) [35]. It is well-known that a simple scheme using traditional certificates realizes IBS, but dedicated schemes aimed at achieving better efficiency have been widely studied. We refer the reader to a comprehensive survey by Bellare et al. [3] for details.

Supporting multiple attribute-authorities is crucial to many attribute-based systems. Previously, there has been much interest on this aspect for attribute-based *encryption* schemes; see Chase et al. [14, 15]. The constructions in this paper readily generalize to the multi-authority setting.

2 Preliminaries

2.1 Groups with Bilinear Pairings

Let $\mathbb{G}, \mathbb{H}, \mathbb{G}_T$ be cyclic (multiplicative) groups of order p, where p is a prime. Let g be a generator of $\mathbb{G}$, and h be a generator of $\mathbb{H}$. Then $e : \mathbb{G} \times \mathbb{H} \to \mathbb{G}_T$ is a *bilinear pairing* if $e(g, h)$ is a generator of $\mathbb{G}_T$, and $e(g^a, h^b) = e(g, h)^{ab}$ for all a, b. We review several standard cryptographic assumptions in such groups:

Definition 1 (q-SDH assumption [8])**.** *Let $\mathbb{G}$, $\mathbb{H}$, and $\mathbb{G}_T$ be as above. The* q-Strong Diffie-Hellman (q-SDH) assumption *holds in $(\mathbb{G}, \mathbb{H})$ if, given the elements $(g, g^x, g^{x^2}, \ldots, g^{x^q}, h, h^x) \in \mathbb{G}^{q+1} \times \mathbb{H}^2$, for random choice of $x \leftarrow \mathbb{Z}_p$ and random generators $g \in \mathbb{G}, h \in \mathbb{H}$, it is computationally infeasible to compute any pair of the form $\left(c, g^{\frac{1}{x+c}}\right) \in \mathbb{Z}_p \times \mathbb{G}$.*

Definition 2 (SXDH assumption [22])**.** *Let $\mathbb{G}$, $\mathbb{H}$, and $\mathbb{G}_T$ be as above. The* Symmetric External Diffie-Hellman (SXDH) assumption *holds in $(\mathbb{G}, \mathbb{H})$ if the standard Decisional Diffie-Hellman (DDH) assumption holds simultaneously in $\mathbb{G}$ and $\mathbb{H}$.*

Definition 3 (DLIN assumption [9])**.** *Let $\mathbb{G}$, $\mathbb{H}$, and $\mathbb{G}_T$ be as above, but with $\mathbb{G} = \mathbb{H}$. The* Decision-Linear (DLIN) assumption *holds in $\mathbb{G}$ if, given the elements $(g^x, g^y, g^{rx}, g^{sy}, g^t) \in \mathbb{G}^5$, for a random choice of $x, y, r, s \leftarrow \mathbb{Z}_p$, it is computationally infeasible to determine whether $t = r + s$ or t is random in $\mathbb{Z}_p$.*

2.2 Monotone Span Programs

Let $\Upsilon : \{0,1\}^n \to \{0,1\}$ be a monotone boolean function. A *monotone span program for* Υ over a field $\mathbb{F}$ is an $\ell \times t$ matrix $\mathbf{M}$ with entries in $\mathbb{F}$, along with a labeling function $a : [\ell] \to [n]$ that associates each row of $\mathbf{M}$ with an input variable of Υ, that, for every $(x_1, \ldots, x_n) \in \{0,1\}^n$, satisfies the following:

$$\Upsilon(x_1, \ldots, x_n) = 1 \iff \exists\, \vec{v} \in \mathbb{F}^{1 \times \ell} : \vec{v}\mathbf{M} = [1, 0, 0, \ldots, 0] \text{ and } (\forall i : x_{a(i)} = 0 \Rightarrow v_i = 0)$$

In other words, $\Upsilon(x_1, \ldots, x_n) = 1$ if and only if the rows of $\mathbf{M}$ indexed by $\{i \mid x_{a(i)} = 1\}$ span the vector $[1, 0, 0, \ldots, 0]$.

We call ℓ the *length* and t the *width* of the span program, and $\ell + t$ the *size* of the span program. Every monotone boolean function can be represented by some monotone span program, and a large class do have compact monotone span programs. In particular, given a circuit expressed using *threshold gates*, with the i-th gate being an $\binom{\ell_i}{t_i}$ threshold gate, it is easy to recursively construct a monotone span program with length $\sum_i (\ell_i - 1) + 1$ and width $\sum_i (t_i - 1) + 1$.

2.3 Non-Interactive Proofs

We refer the reader to [22] for detailed definitions of non-interactive witness-indistinguishable (NIWI) proofs, but give a brief overview of the necessary definitions here. A NIWI scheme is comprised of the following main algorithms:

- NIWI.Setup: Outputs a reference string crs.
- NIWI.Prove: On input $(crs; \Phi; x)$, where Φ is a boolean formula and $\Phi(x) = 1$, outputs a proof π.
- NIWI.Verify: On input $(crs; \Phi; \pi)$, outputs a boolean.

The completeness requirement is that $\mathsf{NIWI.Verify}(crs; \Phi; \mathsf{NIWI.Prove}(crs; \Phi; x)) = 1$, if $\Phi(x) = 1$ (i.e., x is a *witness* for Φ). The (perfect) witness indistinguishability requirement is that the distributions $\mathsf{NIWI.Prove}(crs; \Phi; x_1)$ and $\mathsf{NIWI.Prove}(crs; \Phi; x_2)$ are identical when x_1 and x_2 are witnesses for Φ. For the soundness/proof of knowledge requirement, we require the following additional algorithms:

- $\mathsf{NIWI.SimSetup}$: Outputs a simulated reference string crs and trapdoor ψ.
- $\mathsf{NIWI.Extract}$: On input $(crs, \psi; \Phi; \pi)$, outputs a witness x.

We require that the crs output by $\mathsf{NIWI.SimSetup}$ is indistinguishable to that of $\mathsf{NIWI.Setup}$. Further, we require that for every $(crs, \psi) \leftarrow \mathsf{NIWI.SimSetup}$, if $\mathsf{NIWI.Verify}(crs; \Phi; \pi) = 1$ then $\mathsf{NIWI.Extract}(crs, \psi; \Phi; \pi)$ outputs a valid witness for Φ, with overwhelming probability.

3 Attribute-Based Signatures: Definitions and Security

We present the formal definitions of attribute-based signatures (ABS). An overview of how ABS can be used in an attribute-based system can be found in Appendix A

Let $\mathbb{A}$ be the universe of possible attributes. A *claim-predicate* over $\mathbb{A}$ is a monotone boolean function, whose inputs are associated with attributes of $\mathbb{A}$. We say that an attribute set $\mathcal{A} \subseteq \mathbb{A}$ *satisfies* a claim-predicate Υ if $\Upsilon(\mathcal{A}) = 1$ (where an input is set to be true if its corresponding attribute is present in $\mathcal{A}$).

Definition 4 (ABS)**.** *An* Attribute-Based Signature (ABS) scheme *is parameterized by a universe of possible attributes $\mathbb{A}$ and message space $\mathbb{M}$, and consists of the following four algorithms.*

- $\mathsf{ABS.TSetup}$ *(to be run by a* signature trustee*: Generates public reference information TPK.*
- $\mathsf{ABS.ASetup}$ *(to be run by an* attribute-issuing authority*): generates a key pair $APK, ASK \leftarrow \mathsf{ABS.ASetup}$.*
- $\mathsf{ABS.AttrGen}$*: On input $(ASK, \mathcal{A} \subseteq \mathbb{A})$, outputs a signing key $SK_{\mathcal{A}}$.*[3]
- $\mathsf{ABS.Sign}$*: On input $(PK = (TPK, APK), SK_{\mathcal{A}}, m \in \mathbb{M}, \Upsilon)$, where $\Upsilon(\mathcal{A}) = 1$, outputs a signature σ.*
- $\mathsf{ABS.Ver}$*: On input $(PK = (TPK, APK), m, \Upsilon, \sigma)$, outputs a boolean value.*

Definition 5 (Correctness)**.** *We call an ABS scheme* correct *if for all $TPK \leftarrow \mathsf{ABS.TSetup}$, all purported APK, all messages m, all attribute sets $\mathcal{A}$, all signing keys $SK_{\mathcal{A}} \leftarrow \mathsf{ABS.AttrGen}(ASK, \mathcal{A})$, all claim-predicates Υ such that $\Upsilon(\mathcal{A}) = 1$, and all signatures $\sigma \leftarrow \mathsf{ABS.Sign}\big(PK = (TPK, APK), SK_{\mathcal{A}}, m, \Upsilon\big)$, we have $\mathsf{ABS.Ver}(PK = (TPK, APK), m, \Upsilon, \sigma) = 1$.*

We present two formal definitions that together capture our desired notions of security. Slightly weaker security requirements may also be useful for most applications, but we use the stronger ones because our constructions satisfy them and because they are much easier to work with.

For simplicity, we only present definitions for the simpler case of a single attribute-issuing authority. The definitions for multiple authorities are analogous, and we discuss this case in Section 5.

Definition 6 (Perfect Privacy)**.** *An ABS scheme is* perfectly private *if, for all honestly generated $TPK \leftarrow \mathsf{ABS.TSetup}$, all purported APK, all attribute sets $\mathcal{A}_1, \mathcal{A}_2$, all*

[3] For simplicity, we treat the signing key as a monolithic quantity. However, in our construction the signing key consists of separate components for each attribute in $\mathcal{A}$, and the $\mathsf{ABS.Sign}$ algorithm needs only as much of $SK_{\mathcal{A}}$ as is relevant to the claim-predicate.

$SK_1 \leftarrow \mathsf{ABS.AttrGen}(ASK, \mathcal{A}_1)$, $SK_2 \leftarrow \mathsf{ABS.AttrGen}(ASK, \mathcal{A}_2)$, *all messages* m, *and all claim-predicates* Υ *such that* $\Upsilon(\mathcal{A}_1) = \Upsilon(\mathcal{A}_2) = 1$, *the distributions* $\mathsf{ABS.Sign}(PK, SK_1, m, \Upsilon)$ *and* $\mathsf{ABS.Sign}(PK, SK_2, m, \Upsilon)$ *are equal.*

In other words, the signer's privacy relies only on the signature trustee, and not the attribute-issuing authority. Even a malicious and computationally unbounded attribute-issuing authority cannot link a signature to a set of attributes or the signing key used to generate it.

We slightly overload notation and write $\mathsf{ABS.Sign}(ASK, m, \Upsilon)$ (i.e., with the attribute authority's private key ASK instead of PK and $SK_{\mathcal{A}}$) to denote the following procedure: first, run $SK_{\mathcal{A}} \leftarrow \mathsf{ABS.AttrGen}(ASK, \mathcal{A})$ for any arbitrary $\mathcal{A}$ satisfying Υ; then output the result of $\mathsf{ABS.Sign}(PK, SK_{\mathcal{A}}, m, \Upsilon)$. For convenience in the experiment below we use $\mathsf{ABS.Sign}(ASK, \cdot, \cdot)$ to generate signatures requested by the adversary. This is reasonable when the scheme satisfies perfect privacy, since any other way of letting the adversary obtain signatures will result in the same distribution.

Definition 7 (Unforgeability)**.** *An ABS scheme is* unforgeable *if the success probability of any polynomial-time adversary in the following experiment is negligible:*

1. *Run* $TPK \leftarrow \mathsf{ABS.TSetup}$ *and* $(APK, ASK) \leftarrow \mathsf{ABS.ASetup}$. *Give* $PK = (TPK, APK)$ *to the adversary.*
2. *The adversary is given access to two oracles:* $\mathsf{ABS.AttrGen}(ASK, \cdot)$ *and* $\mathsf{ABS.Sign}(ASK, \cdot, \cdot)$.
3. *At the end the adversary outputs* $(m^*, \Upsilon^*, \sigma^*)$.

We say the adversary succeeds if (m^*, Υ^*) *was never queried to the* ABS.Sign *oracle, and* $\mathsf{ABS.Ver}(PK, m^*, \Upsilon^*, \sigma^*) = 1$, *and* $\Upsilon^*(\mathcal{A}) = 0$ *for all* $\mathcal{A}$ *queried to the* ABS.AttrGen *oracle.*

Thus any signature which could not have been legitimately made by a *single* one of the adversary's signing keys is considered a forgery. Note that we do not consider it a forgery if the adversary can produce a *different* signature on (m, Υ) than the one he received from the signing oracle.

4 Constructing ABS Schemes

4.1 Credential Bundles

We introduce a new generic primitive called *credential bundles*, which we use in our ABS constructions. Credential bundles model the intuitive requirements of publicly verifiable attributes that resist collusion.

Definition 8 (Credential bundle scheme)**.** *A* credential bundle scheme *is parameterized by a message space* $\mathbb{M}$, *and consists of the following three algorithms.*

- CB.Setup*: Outputs a verification key* vk *and a secret key* sk.
- CB.Gen*: On input* $(sk, \{m_1, \ldots, m_n\} \subseteq \mathbb{M})$, *outputs a tag* τ *and values* $\sigma_1, \ldots, \sigma_n$.
- CB.Ver*: On input* $(vk, m, (\tau, \sigma))$, *outputs a boolean value.*

The scheme is correct *if, for all* $(\tau, \sigma_1, \ldots, \sigma_n) \leftarrow \mathsf{CB.Gen}(sk, m_1, \ldots, m_n)$, *we have* $\mathsf{CB.Ver}(vk, m_i, (\tau, \sigma_i)) = 1$ *for all* i.

Clearly by excluding some of the σ_i's from an existing bundle, one can generate a new bundle on a subset of attributes. Our main security definition requires that taking a subset of a *single* bundle is the only way to obtain a new bundle from existing bundles; in particular, attributes from several bundles cannot be combined.

Definition 9. *A credential bundle scheme is* secure *if the success probability of any polynomial-time adversary in the following experiment is negligible:*

1. *Run* $(vk, sk) \leftarrow \mathsf{CB.Setup}$*, and give* vk *to the adversary.*
2. *The adversary is given access to an oracle* $\mathsf{CB.Gen}(sk, \cdot)$*.*
3. *At the end the adversary outputs* $(\tau^*, (m_1^*, \sigma_1^*), \ldots, (m_n^*, \sigma_n^*))$*.*

We say the adversary succeeds *if* $\mathsf{CB.Ver}(vk, m_i^*, (\tau^*, \sigma_i^*)) = 1$ *for all* $i \leq n$*, and if no superset of* $\{m_1^*, \ldots, m_n^*\}$ *was ever queried (in a single query) to the* $\mathsf{CB.Gen}$ *oracle.*

From any plain digital signature scheme we can easily construct a credential bundle scheme in which the bundle is a collection of signatures of messages "$\tau \| m_i$", where each m_i is the name of an attribute and τ is an identifier that is unique to each user (e.g., an email address). Conversely, when a credential bundle scheme is restricted to singleton sets of messages, its unforgeability definition is equivalent to normal digital signature unforgeability. Despite this equivalence under black-box reductions, the syntax of credential bundles more closely models our desired semantics for ABS.

4.2 A Framework for ABS

Our generic ABS construction for the case of a *single attribute authority* is given in Figure 1. The construction generalizes easily to the multiple attribute authority case (Section 5). At a high level, to sign a message m with claim-predicate Υ, the signer proves that she possesses either a credential bundle containing either sufficient attributes to satisfy Υ, or a "pseudo-attribute" identified with the pair (m, Υ). Only the signature trustee is capable of generating bundles involving pseudo-attributes (these are verified against the trustee's verification key tvk), but it never does so. Thus the proof is convincing that the signer satisfied Υ. However, in the security reduction, the pseudo-attribute provides a mechanism to bind the NIWI proof to a message and give simulated signatures. In Appendix C.1 we prove the following:

Theorem 1. *Given a NIWI argument of knowledge scheme and any secure credential bundle scheme (equivalently, any digital signature scheme), the construction in Figure 1 is a secure ABS scheme. Further, if the NIWI argument is perfectly hiding, the ABS scheme is perfectly private.*

4.3 Practical Instantiation 1

Our first practical instantiation uses Groth-Sahai proofs [22] as the NIWI component and Boneh-Boyen signatures [7] as the credential bundle component. One notable feature of this choice is that attributes in the scheme are simply Boneh-Boyen signatures on messages of the form "userid$\|$attr".

This instantiation requires cyclic groups of prime order equipped with bilinear pairings (Section 2.1). The Groth-Sahai system can prove satisfiability of *pairing-product equations* in such groups, and the main challenge in this instantiation is expressing the logic of the claim-predicate and the Boneh-Boyen signature verification in this limited vocabulary. We identify $\mathbb{Z}_p^*$ with the universe of attributes, where p is the size of the cyclic group used in the scheme.[4]

Boneh-Boyen signatures We briefly review the Boneh-Boyen digital signature scheme [8]. As before, we suppose there is a bilinear pairing $e : \mathbb{G} \times \mathbb{H} \to \mathbb{G}_T$, where $\mathbb{G}$ and $\mathbb{H}$ have prime order p, and where g is a generator of $\mathbb{G}$, and h is a generator of $\mathbb{H}$. The scheme, described below, is strongly unforgeable under the q-SDH assumpion (Definition 1).

[4] More precisely $\mathbb{A} \cup \mathbb{A}' \subseteq \mathbb{Z}_p^*$ where $\mathbb{A}'$ is the universe of pseudo-attributes. As is standard, the universe of (pseudo-)attributes can be extended to $\{0,1\}^*$ by applying a collision-resistant hash with range $\mathbb{Z}_p^*$.

Let $\mathbb{A}$ be the desired universe of ABS attributes. Let $\mathbb{A}'$ denote a space of *pseudo-attributes*, where $\mathbb{A} \cap \mathbb{A}' = \emptyset$. For every message m and claim-predicate Υ we associate a psuedo-attribute $a_{m,\Upsilon} \in \mathbb{A}'$. Let CB be a secure credential bundle scheme, with message space $\mathbb{A} \cup \mathbb{A}'$, and let NIWI be a perfect NIWI proof of knowledge scheme. Our ABS construction is as follows:

$\mathsf{ABS.TSetup}$**:** The signature trustee runs $crs \leftarrow \mathsf{NIWI.Setup}$ as well as $(tvk, tsk) \leftarrow \mathsf{CB.Setup}$ and publishes $TPK = (crs, tvk)$.

$\mathsf{ABS.ASetup}$**:** The attribute-issuing authority runs $(avk, ask) \leftarrow \mathsf{CB.Setup}$ and publishes $APK = avk$ and sets $ASK = ask$.

$\mathsf{ABS.AttrGen}(ASK, \mathcal{A})$**:** Ensure that $\mathcal{A}$ contains no pseudo-attributes. Then output the result of $\mathsf{CB.Gen}(ask, \mathcal{A})$.

$\mathsf{ABS.Sign}(PK, SK_{\mathcal{A}}, m, \Upsilon)$**:** Assume that $\Upsilon(\mathcal{A}) = 1$. Parse $SK_{\mathcal{A}}$ as $(\tau, \{\sigma_a \mid a \in \mathcal{A}\})$. Υ is a formula over formal variables $\mathbb{A}$. Define $\widetilde{\Upsilon} := \Upsilon \vee a_{m,\Upsilon}$, where $a_{m,\Upsilon} \in \mathbb{A}'$ is the pseudo-attribute associated with (m, Υ). Thus, we still have $\widetilde{\Upsilon}(\mathcal{A}) = 1$. Let $\{a_1, \ldots, a_n\}$ denote the attributes appearing in $\widetilde{\Upsilon}$. Let vk_i be avk if attribute a_i is a pseudo-attribute, and tvk otherwise. Finally, let $\Phi[vk, m, \Upsilon]$ denote the following boolean expression:

$$\exists\, \tau, \sigma_1, \ldots, \sigma_n : \widetilde{\Upsilon}\Big(\big\{a_i \;\big|\; \mathsf{CB.Ver}\big(vk_i, a_i, (\tau, \sigma_i)\big) = 1\big\}\Big) = 1 \tag{1}$$

For each i, set $\hat{\sigma}_i = \sigma_{a_i}$ from $SK_{\mathcal{A}}$ if it is present, and to any arbitrary value otherwise (since then its value does not matter). Compute $\pi \leftarrow \mathsf{NIWI.Prove}\big(crs; \Phi[vk, m, \Upsilon]; (\tau, \hat{\sigma}_1, \ldots, \hat{\sigma}_n)\big)$. Output π as the ABS signature.

$\mathsf{ABS.Ver}(PK, m, \Upsilon, \pi)$**:** Output the result of $\mathsf{NIWI.Verify}(crs; \Phi[vk, m, \Upsilon]; \pi)$.

Figure 1: General framework for an ABS scheme.

$\mathsf{DS.KeyGen}$**:** Choose random $b, c, d \leftarrow \mathbb{Z}_p$ and compute $B = g^b$, $C = g^c$, $D = g^d$. The verification key is $(B, C, D) \in \mathbb{G}^3$, and the signing key is $(b, c, d) \in (\mathbb{Z}_p)^3$.

$\mathsf{DS.Sign}(sk, m \in \mathbb{Z}_p)$**:** Choose random $r \leftarrow \mathbb{Z}_p$; output $\sigma = \left(h^{1/(b+cm+dr)}, t\right) \in \mathbb{H} \times \mathbb{Z}_p$.

$\mathsf{DS.Ver}(vk, m, \sigma = (S, r))$**:** Output 1 if $e(BC^m D^r, S) = e(g, h)$, and 0 otherwise.

Expressing the Non-Interactive Proof using Pairing Equations We use the notation introduced in Figure 1. We must show how the statement $\Phi[vk, m, \Upsilon]$ (equation 1) can be efficiently encoded in the Groth-Sahai system when the credential bundles use Boneh-Boyen signatures.

Groth-Sahai proofs work by first giving a commitment to the values of the witness, and then proving that the commited values satisfy given pairing equations. Suppose we commit to a group element Z (where the group $\mathbb{G}$ or $\mathbb{H}$ will be clear from context), then we will let $\langle Z \rangle$ denote the formal variable corresponding to that commitment. Thus, we express the statements to be proven as pairing equations whose formal variables we will write in the $\langle Z \rangle$ notation.

Suppose the modified predicate $\widetilde{\Upsilon}$ has a canonical monotone span program $\mathbf{M}$ of size $\ell \times t$, where the ith row corresponds to the $a(i)$-th attribute mentioned in $\widetilde{\Upsilon}$. To establish $\Phi[vk, m, \Upsilon]$,

we prove the following equation, which implies it:

$$\exists\ \tau, \sigma_1, \ldots, \sigma_n, v_1, \ldots, v_n : \vec{v}\mathbf{M} = [1, 0, \ldots, 0] \\ \wedge \bigwedge_{i=1}^{\ell} \Big[v_i \neq 0 \Rightarrow \mathsf{CB.Ver}(vk, a_{a(i)}, (\tau, \sigma_{a(i)})) = 1 \Big]$$

Then, in addition to $\tau, \{\sigma_i\}$, we will have the signer commit to the vector $\vec{v}$ which can be canonically computed from his satisfying assignment of $\widetilde{\Upsilon}$.

This new boolean expression is a conjunction of two kinds of clauses: The first has the form $\exists \vec{v} : \vec{v}\mathbf{M} = [1, \ldots, 0]$. To prove it, we commit to the values g^{v_i} and prove the following pairing equations (for each $j \in [t]$):

$$\prod_{i=1}^{\ell} e(\langle g^{v_i} \rangle, h^{\mathbf{M}_{i,j}}) = \begin{cases} e(g,h) & \text{if } j = 1 \\ e(g^0, h) & \text{otherwise} \end{cases}$$

The other clauses have the form $\exists\ \tau, \sigma, v : \big[v \neq 0 \Rightarrow \mathsf{CB.Ver}(vk, m, (\tau, \sigma)) = 1 \big]$. When we use Boneh-Boyen signatures as the instantiation of credential bundles, these clauses can be simplified to

$$\exists\ \tau, \sigma, v : \big[v \neq 0 \Rightarrow \mathsf{DS.Ver}(vk, \tau \| m, \sigma) = 1 \big]$$

where $\mathsf{DS.Ver}$ is the Boneh-Boyen signature verification.

It is crucial that the proof is a proof *of knowledge*, so the simulator can extract the credential bundles. Thus we commit to τ and r *bitwise*, since they are elements of $\mathbb{Z}_p$and could not otherwise be efficiently extracted in the Groth-Sahai scheme. In this way, the extractor can extract the bits and reconstruct the entire witness τ and r.[5] Let $(\tau, \sigma = (S, r), v)$ be a witness to the above expression. Express τ bitwise as $\tau = \sum_i \tau_i 2^i$. Then $\tau \| m$ may be identified with a number $m 2^{|\tau|} + \sum_i \tau_i 2^i$. Similarly, interperet r bitwise as $r = \sum_i r_i 2^i$.

Using the same notation as before, we can prove satisfiability of the clause as follows. We commit to each r_i and τ_i in both groups, as $g^{r_i}, h^{r_i}, g^{\tau_i}, h^{\tau_i}$, and then prove that each is indeed a single bit, using the following pairing equations for all i:

$$e(\langle g^{r_i} \rangle, h) = e(g, \langle h^{r_i} \rangle); \qquad e(\langle g^{\tau_i} \rangle, h) = e(g, \langle h^{\tau_i} \rangle);$$
$$e(\langle g^{r_i} \rangle, \langle h^{r_i} \rangle) = e(\langle g^{r_i} \rangle, h); \qquad e(\langle g^{\tau_i} \rangle, \langle h^{\tau_i} \rangle) = e(\langle g^{\tau_i} \rangle, h).$$

Next, observe that the pairing equation $e(BC^{\tau \| m} D^r, S^v) = e(g^v, h)$ is logically equivalent to the expression $v \neq 0 \Rightarrow \mathsf{DS.Ver}(vk, \tau \| m, (S, r)) = 1$, which we need to prove. However, the prover cannot directly compute $BC^{\tau \| m} D^r$ or S^v given the committed values. Thus the prover commits to some additional intermediate values $S^v \in \mathbb{H}$ and $C^\tau, D^r \in \mathbb{G}$, and proves the following equations:

$$e(\langle D^r \rangle, h) = \textstyle\prod_i e(D^{2^i}, \langle h^{r_i} \rangle); \qquad e(\langle g^v \rangle, \langle S \rangle) = e(g, \langle S^v \rangle);$$
$$e(\langle C^\tau \rangle, h) = \textstyle\prod_i e(C^{2^i}, \langle h^{\tau_i} \rangle);$$
$$e(\langle g^v \rangle, h) = e(BC^{2^{|\tau|} m}, \langle S^v \rangle)\ e(\langle C^\tau \rangle, \langle S^v \rangle)\ e(\langle D^r \rangle, \langle S^v \rangle).$$

Note that since m and $|\tau|$ are public, all the coefficients in these equations can be publicly computed. This completes the description of how we encode the required logic into the Groth-Sahai proof system.

[5] We remark that the proof need not be a proof of knowledge with respect to $\vec{v}$, so it was safe to use these values directly in $\mathbb{Z}_p$.

There are two instantiations of the Groth-Sahai proof system over prime order groups, based on the DLIN and SXDH assumptions, both of which are suitable for our purposes. Using these we obtain the following (a more detailed analysis of the efficiency is given in Appendix C.2).

Theorem 2. *Under the q-SDH and either DLIN or SXDH assumptions, there is an ABS scheme supporting claim-predicates represented as monotone span programs, with signatures consisting of $O(ks)$ group elements, where s is the size of the monotone span program.*

4.4 Practical Instantiation 2

We can also instantiate our framework using the same approach as above, but with the signature scheme of Waters [36]. Signatures in Waters' scheme do not include any elements of $\mathbb{Z}_p$. This fact allows us to avoid the inefficiency of committing to many components of the Boneh-Boyen signatures in a bitwise fashion. Furthermore, Waters signatures are secure under the much weaker BDH assumption, which is implied by the assumptions required for Groth-Sahai proofs. Thus this instantiation does not require the additional q-SDH assumption. However, as a tradeoff, the Waters instantiation requires larger public parameters: a linear (in the security parameter) number of group elements, not the constant number of group elements needed by the Boneh-Boyen instantiation.

The details of this instantiation follow a similar approach as the previous one, incorporating the verification equation of the Waters signature. In Appendix C.3 we prove the following:

Theorem 3. *Under either the DLIN or SXDH assumptions, there is an ABS scheme supporting claim-predicates represented as monotone span programs, with signatures consisting of $O(k + s)$ group elements, where s is the size of the monotone span program.*

4.5 Practical Instantiation 3

We now present an ABS scheme which is our most practical. Signatures in the scheme consist of *exactly* $s + 2$ group elements, where s is the size of the claim-predicate's monotone span program. This scheme does not use the Groth-Sahai proof system; we use our own randomization techniques to blind the attributes that are used in signing. One additional advantage of avoiding a NIZK proof system is that the privacy of the signers is provided even against a malicious signature trustee; in contrast the above NIZK-based constructions rely on the signature trustee to set up a common reference string honestly.

Our approach is motivated by the construction of mesh signatures [11], but incorporates the efficient credential bundles of the previous construction, as well as the concept of "pseudo-attributes" to bind a message to the signature. In Appendix D, we give a high-level motivation of the details of this scheme. Below we give a description of the construction:

This construction supports all claim-predicates whose monotone span programs have width at most t_{max}, where t_{max} is an arbitrary parameter. We treat $\mathbb{A} = \mathbb{Z}_p^*$ as the universe of attributes, where p is the size of the cyclic group used in the scheme.[6]

ABS.TSetup: Choose suitable cyclic groups G and H of prime order p, equipped with a bilinear pairing $e : G \times H \to G_T$. Choose a collision-resistant hash function $\mathcal{H} : \{0,1\}^* \to \mathbb{Z}_p^*$. Choose random generators: $g \leftarrow G$; $h_0, \ldots h_{t_{\mathsf{max}}} \leftarrow H$. The trustee public key is $TPK = (G, H, \mathcal{H}, g, h_0, \ldots, h_{t_{\mathsf{max}}})$.

[6] As always, the universe of attributes can be further extended to $\{0,1\}^*$ by applying a collision-resistant hash having range $\mathbb{Z}_p^*$. For simplicity of presentation, we do not include this modification.

ABS.ASetup: Choose random $a_0, a, b, c \leftarrow \mathbb{Z}_p^*$ and set:

$$C = g^c; \qquad A_0 = h_0^{a_0}; \qquad A_j = h_j^a \text{ and } B_j = h_j^b \quad (\forall j \in [t_{\mathsf{max}}]).$$

The master key is $ASK = (a_0, a, b)$. The public key APK is $(A_0, \ldots, A_{t_{\mathsf{max}}}, B_1, \ldots, B_{t_{\mathsf{max}}}, C)$

ABS.AttrGen: On input ASK as above and attribute set $\mathcal{A} \subseteq \mathbb{A}$, Choose random generator $K_{\mathsf{base}} \leftarrow G$. Set:

$$K_0 = K_{\mathsf{base}}^{1/a_0}; \qquad K_u = K_{\mathsf{base}}^{1/(a+bu)} \quad (\forall u \in \mathcal{A})$$

The signing key is then $SK_{\mathcal{A}} = (K_{\mathsf{base}}, K_0, \{K_u \mid u \in \mathcal{A}\})$.

ABS.Sign: On input $(PK, SK_{\mathcal{A}}, m, \Upsilon)$ such that $\Upsilon(\mathcal{A}) = 1$, first convert Υ to its corresponding monotone span program $\mathbf{M} \in (\mathbb{Z}_p)^{\ell \times t}$, with row labeling $u : [\ell] \to \mathbb{A}$. Also compute the vector $\vec{v}$ that corresponds to the satisfying assignment $\mathcal{A}$. Compute $\mu = \mathcal{H}(m \| \Upsilon)$.

Pick random $r_0 \leftarrow \mathbb{Z}_p^*$ and $r_1, \ldots r_\ell \leftarrow \mathbb{Z}_p$ and compute:

$$Y = K_{\mathsf{base}}^{r_0}; \qquad S_i = (K_{u(i)}^{v_i})^{r_0} \cdot (Cg^{\mu})^{r_i} \quad (\forall i \in [\ell]);$$

$$W = K_0^{r_0}; \qquad P_j = \prod_{i=1}^{\ell} (A_j B_j^{u(i)})^{\mathbf{M}_{ij} \cdot r_i} \quad (\forall j \in [t]).$$

We note that the signer may not have $K_{u(i)}$ for every attribute $u(i)$ mentioned in the claim-predicate. But when this is the case, $v_i = 0$, and so the value is not needed. The signature is $\sigma = (Y, W, S_1, \ldots, S_\ell, P_1, \ldots, P_t)$.

ABS.Ver: On input $(PK, \sigma = (Y, W, S_1, \ldots, S_\ell, P_1, \ldots, P_t), m, \Upsilon)$, first convert Υ to its corresponding monotone span program $\mathbf{M} \in (\mathbb{Z}_p)^{\ell \times t}$, with row labeling $u : [\ell] \to \mathbb{A}$. Compute $\mu = \mathcal{H}(m \| \Upsilon)$. If $Y = 1$, then output reject. Otherwise check the following constraints:

$$e(W, A_0) \stackrel{?}{=} e(Y, h_0)$$

$$\prod_{i=1}^{\ell} e\Big(S_i, (A_j B_j^{u(i)})^{\mathbf{M}_{ij}}\Big) \stackrel{?}{=} \begin{cases} e(Y, h_1)\, e(Cg^{\mu}, P_1), & j = 1 \\ e(Cg^{\mu}, P_j), & j > 1, \end{cases}$$

for $j \in [t]$. Return accept if all the above checks succeed, and reject otherwise.

The security proof of this scheme is given in Appendix D.1.

Theorem 4. *In the generic group model, there is an ABS scheme supporting claim-predicates represented as monotone span programs, with signatures consisting of $s + 2$ group elements, where s is the size of the monotone span program.*

5 Multiple Attribute-Authorities

Our first two intantiations of ABS (indeed, our general framework) can be easily extended for use in an environment with multiple attribute-issuing authorities. Except in a centralized enterprise setting, a single user would acquire her attributes from different authorities (e.g., different government agencies, different commercial services she has subscribed to, different social networks she is registered with and so on). These different attribute authorities may not trust each other, nor even be aware of each other. Indeed, some attribute authorities may be untrustworthy, and this should not affect the trustworthiness of attributes acquired from other authorities, or of ABS signatures involving trustworthy attributes.

Apart from these mutually distrusting attribute authorities, we still require a (possibly separate) *signature trustee* to set up the various public parameters of the ABS signature scheme itself. A signature trustee does not have to trust any attribute authority. The attribute authorities use only the public keys from the signature trustee. As long as the signature trustee is trusted, then the ABS signatures are secure and leak no information about the identity or attributes of the signer. The only requirement for compatibility among attribute authorities is that they all have a mechanism for agreeing on a user's userid (say, an email address) so that a user's bundle of credentials may contain compatible attributes from several authorities.

Finally, the claim-predicate in the ABS signature must carry the identity of the attribute-authorities who *own* the various attributes (possibly as meta-data attached to the attribute description). Given this information, the statement proven in the non-interactive proof can be modified to refer to the appropriate digital signature verification keys corresponding to each attribute, including the pseudo-attribute. If one attribute authority's signatures are compromised, then an ABS verifier should not give much importance to attributes from that authority. However, the ABS signatures themselves are still valid (in that they indeed attest to the given claim-predicate being satisfied) as long as the trustee is uncorrupted.

6 Applications

We identify several natural applications of ABS schemes:

Attribute-based messaging Attribute-Based Messaging, or ABM, (e.g., [5]) provides an example of a quintessential attribute-based system. In an ABM system, messages are addressed not by the identities of the recipients, but by a predicate on users' attributes which the recipients must satisfy. The users need not be aware of each other's identities or attributes. To provide *end-to-end* message privacy (against users whose attributes do not satisfy the sender's policy), one can use *ciphertext-policy attribute-based encryption*, as proposed by Bethencourt, Sahai and Waters [4]. However, there was no satisfactory way to achieve *authentication* (i.e., for the receiver to verify that the sender also satisfied a particular policy) in an ABM system until now. Existing cryptographic technology, including certificates and mesh signatures, would not provide an adequate level of anonymity for the senders while simultaneously preventing collusions.

In a typical ABM system, a certain degree of authorization is required to send messages to certain groups of users. That is, an attribute-based access control mechanism must decide whether to allow a messaging attempt from a sender, depending on both the attributes of the sender and the attribute-based address attached to the message. ABS can be used to authenticate a sender to the ABM system itself (as opposed to the scenario above, where the sender was authenticating to the message recipient). As the messaging system can publicly verify the ABS signature, this solution eliminates the need for the messaging system to query the attribute database to determine the sender's authorization. Indeed, the messaging system need not know the sender's identity at all.

Finally, because our construction is so readily suited for multi-authority settings, ABS is a natural choice for inter-domain ABM systems. However, there are many engineering and cryptographic challenges involved in other aspects of a truly inter-domain ABM system. For example, Chase's proposal [14] for multi-authority attribute-based encryption (originally for the schemes in [33, 20], but can be extended to the one in [4]) requires all the attribute-authorities to share secret keys with a central authority, thereby requiring the central authority to trust all the attribute authorities. In contrast, our ABS system requires no such trust between the signature

trustee and attribute authorities. As such, ABS is much better suited to practical inter-domain attribute-based systems than its encryption counterparts.

Attribute-based authentication and trust-negotiation ABS can also be used as a more general fine-grained authentication mechanism. For instance, a server can publish its access policy for a particular resource along with its encryption public key. When a client wishes to access the resource, the server issues a random challenge string. The client can then generate a session key for (private-key) communication, generate an ABS signature of $(challenge, sessionkey)$ under the server's policy, and send these to the server encrypted under the server's public key. Thereafter, the client and server can communicate using the shared session key. This simple protocol is robust even against a man in the middle.

This technique can be extended to multiple rounds as a simple *trust negotiation* protocol, in which two parties progressively reveal more about their attributes over several rounds of interaction. Several recent works also consider cryptographic approaches to trust negotiation that give more privacy to users than is achieved when they simply take turns revealing their attributes [29, 19]. Instead of these techniques, ABS can provide a sophisticated way to reveal partial information about one's attributes that is natural for this setting. Being able to bind a message to such a proof about one's attributes, as ABS permits, also allows one to protect the trust negotiation from outside attack, using an approach as above. At each step of the negotiation, the active party can choose an "ephemeral key" for secure (private-key) communication and sign it using ABS. This approach prevents a man-in-the-middle attacks by an adversary who has enough attributes to intercept the first few steps of the negotiation.

Leaking secrets The classical application for which the notion of ring-signatures was developed by Rivest, Shamir and Tauman [30] is "leaking secrets," that we used as the motivating example in the opening of this paper. Ring signatures support only claim-predicates which are disjunctions. Mesh signatures are an extension of this concept which allow more sophisticated claim-predicates, but permit multiple parties to pool their attributes (atomic signatures). This is not necessarily the intended semantics in natural secret-leaking environment. ABS, on the other hand, provides the semantics that a *single* user (not a coalition) whose attributes satisfy the stated predicate attests to the secret.

References

[1] M. Belenkiy, M. Chase, M. Kohlweiss, and A. Lysyanskaya. P-signatures and noninteractive anonymous credentials. In R. Canetti, editor, *TCC*, volume 4948 of *Lecture Notes in Computer Science*, pages 356–374. Springer, 2008.

[2] M. Bellare, D. Micciancio, and B. Warinschi. Foundations of group signatures: Formal definitions, simplified requirements, and a construction based on general assumptions. In E. Biham, editor, *EUROCRYPT*, volume 2656 of *Lecture Notes in Computer Science*, pages 614–629. Springer, 2003.

[3] M. Bellare, C. Namprempre, and G. Neven. Security proofs for identity-based identification and signature schemes. *Journal of Cryptology*, 22(1):1–61, January 2009. Preliminary version appeared in Eurocrypt 2004.

[4] J. Bethencourt, A. Sahai, and B. Waters. Ciphertext-policy attribute-based encryption. In *IEEE Symposium on Security and Privacy*, pages 321–334, 2007.

[5] R. Bobba, O. Fatemieh, F. Khan, C. A. Gunter, and H. Khurana. Using attribute-based access control to enable attribute-based messaging. In *ACSAC*, pages 403–413. IEEE Computer Society, 2006.

[6] R. Bobba, O. Fatemieh, F. Khan, A. Khan, C. Gunter, H. Khurana, and M. Prabhakaran. Attribute based messaging: Access control and confidentiality. Manuscript (under submission), 2008.

[7] D. Boneh and X. Boyen. Secure identity based encryption without random oracles. In M. K. Franklin, editor, *CRYPTO*, volume 3152 of *Lecture Notes in Computer Science*, pages 443–459. Springer, 2004.

[8] D. Boneh and X. Boyen. Short signatures without random oracles. In C. Cachin and J. Camenisch, editors, *EUROCRYPT*, volume 3027 of *Lecture Notes in Computer Science*, pages 56–73. Springer, 2004.

[9] D. Boneh, X. Boyen, and H. Shacham. Short group signatures. In M. K. Franklin, editor, *CRYPTO*, volume 3152 of *Lecture Notes in Computer Science*, pages 41–55. Springer, 2004.

[10] D. Boneh and M. K. Franklin. Identity-based encryption from the Weil pairing. *SIAM J. Comput.*, 32(3):586–615, 2003.

[11] X. Boyen. Mesh signatures. In M. Naor, editor, *EUROCRYPT*, volume 4515 of *Lecture Notes in Computer Science*, pages 210–227. Springer, 2007.

[12] X. Boyen and B. Waters. Compact group signatures without random oracles. In S. Vaudenay, editor, *EUROCRYPT*, volume 4004 of *Lecture Notes in Computer Science*, pages 427–444. Springer, 2006.

[13] J. Camenisch and T. Groß. Efficient attributes for anonymous credentials. In P. Ning, P. F. Syverson, and S. Jha, editors, *ACM Conference on Computer and Communications Security*, pages 345–356. ACM, 2008.

[14] M. Chase. Multi-authority attribute based encryption. In S. P. Vadhan, editor, *TCC*, volume 4392 of *Lecture Notes in Computer Science*, pages 515–534. Springer, 2007.

[15] M. Chase and S. S. M. Chow. Improving privacy and security in multi-authority attribute-based encryption. In E. Al-Shaer, S. Jha, and A. D. Keromytis, editors, *ACM Conference on Computer and Communications Security*, pages 121–130. ACM, 2009.

[16] D. Chaum. Security without identification: Transaction systems to make big brother obsolete. *Commun. ACM*, 28(10):1030–1044, 1985.

[17] D. Chaum and E. van Heyst. Group signatures. In *EUROCRYPT*, pages 257–265, 1991.

[18] A. De Santis and G. Persiano. Zero-knowledge proofs of knowledge without interaction. In *33rd FOCS*, pages 427–436. IEEE Computer Society Press, 1992.

[19] K. B. Frikken, J. Li, and M. J. Atallah. Trust negotiation with hidden credentials, hidden policies, and policy cycles. In *NDSS*. The Internet Society, 2006.

[20] V. Goyal, O. Pandey, A. Sahai, and B. Waters. Attribute-based encryption for fine-grained access control of encrypted data. In A. Juels, R. N. Wright, and S. D. C. di Vimercati, editors, *ACM Conference on Computer and Communications Security*, pages 89–98. ACM, 2006.

[21] J. Groth. Simulation-sound NIZK proofs for a practical language and constant size group signatures. In X. Lai and K. Chen, editors, *ASIACRYPT*, volume 4284 of *Lecture Notes in Computer Science*, pages 444–459. Springer, 2006.

[22] J. Groth and A. Sahai. Efficient non-interactive proof systems for bilinear groups. In N. P. Smart, editor, *EUROCRYPT*, volume 4965 of *Lecture Notes in Computer Science*, pages 415–432. Springer, 2008.

[23] S. Guo and Y. Zeng. Attribute-based signature scheme. In *International Conference on Information Security and Assurance*, pages 509–511. IEEE, 2008.

[24] J. Katz, R. Ostrovsky, and M. O. Rabin. Identity-based zero knowledge. In C. Blundo and S. Cimato, editors, *SCN*, volume 3352 of *Lecture Notes in Computer Science*, pages 180–192. Springer, 2004.

[25] D. Khader. Attribute based group signature with revocation. Cryptology ePrint Archive, Report 2007/241, 2007. `http://eprint.iacr.org/2007/241`.

[26] D. Khader. Attribute based group signatures. Cryptology ePrint Archive, Report 2007/159, 2007. http://eprint.iacr.org/2007/159.

[27] J. Li, M. H. Au, W. Susilo, D. Xie, and K. Ren. Attribute-based signature and its applications. In D. Feng, D. A. Basin, and P. Liu, editors, *ASIACCS*, pages 60–69. ACM, 2010.

[28] J. Li and K. Kim. Attribute-based ring signatures. Cryptology ePrint Archive, Report 2008/394, 2008. http://eprint.iacr.org/2008/394.

[29] N. Li, W. Du, and D. Boneh. Oblivious signature-based envelope. *Distributed Computing*, 17(4):293–302, 2005.

[30] R. L. Rivest, A. Shamir, and Y. Tauman. How to leak a secret. In C. Boyd, editor, *ASIACRYPT*, volume 2248 of *Lecture Notes in Computer Science*, pages 552–565. Springer, 2001.

[31] J. Rompel. One-way functions are necessary and sufficient for secure signatures. In *Proc. 22nd STOC*, pages 387–394. ACM, 1990.

[32] A. Sahai. Non-malleable non-interactive zero knowledge and adaptive chosen-ciphertext security. In *FOCS*, pages 543–553, 1999.

[33] A. Sahai and B. Waters. Fuzzy identity-based encryption. In R. Cramer, editor, *EUROCRYPT*, volume 3494 of *Lecture Notes in Computer Science*, pages 457–473. Springer, 2005.

[34] S. F. Shahandashti and R. Safavi-Naini. Threshold attribute-based signatures and their application to anonymous credential systems. In B. Preneel, editor, *AFRICACRYPT*, volume 5580 of *Lecture Notes in Computer Science*, pages 198–216. Springer, 2009.

[35] A. Shamir. Identity-based cryptosystems and signature schemes. In *CRYPTO*, pages 47–53, 1984.

[36] B. Waters. Efficient identity-based encryption without random oracles. In R. Cramer, editor, *EUROCRYPT*, volume 3494 of *Lecture Notes in Computer Science*, pages 114–127. Springer, 2005.

[37] B. Waters. Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization. Cryptology ePrint Archive, Report 2008/290, 2008. http://eprint.iacr.org/2008/290.

A Using ABS

Attribute-based signatures are just a cryptographic primitive fully defined by the above described algorithms and the security and correctness guarantees. To be useful in a system, ABS has to be used appropriately. Here we describe the typical usage scenario for ABS.

For the sake of expositional clarity, in this section we consider a setting with a single authority who sets up the system parameters and public keys, and also issues private keys for each user, for each of the user's attributes.[7]

Mapping Attributes Before describing the operation of the system, we need to relate the attributes as used in ABS with the attributes that occur in a real-life system. In a typical system one encounters attributes which have a *name* and optionally a *value*. For instance a user may possess an attribute named `age`, with a numerical value 25. On the other hand, some attributes may not have any value attached to them; for instance a user could possess an attribute named `student`. ABS, as described above, supports only the latter kind of attributes. Nevertheless, since the names supported by ABS are free-form strings, one could encode a (name, value) pair into a single string using an appropriate (standardized) encoding scheme.

[7] We do not consider the technical issues of how the authority establishes the identity of a user before handing it any keys. Also, we consider it the authority's prerogative to determine which attributes should be given to each requesting user.

But it is not enough to encode the attributes; one must also translate the predicates involving the (name, value) pair into predicates in terms of the encoded string. The above encoding is sufficient if the predicates involve only equality conditions. But for numerical attributes, other comparisons (like "$\geq$", "$\leq$") are also important. This can be taken care of by representing a single numerical attribute by a few value-less attributes, as has been already pointed out in [20, 4]. We remark that at the cost of increasing the number of value-less attributes used (thereby increasing private-key size of the user), one can reduce the size of the predicate representing a comparison condition, leading to faster operations (signing and verification, in our case).

Another issue regarding mapping real-life attributes to ABS attributes relates to attribute expiry and revocation issues. As discussed below, the collusion-resistance property of ABS provides suitable flexibility to support revocation. But the exact manner in which this flexibility is used is a design decision that trades off efficiency and security parameters.

Typical System with ABS In a typical institutional setting, the signature trustee and attribute-issuing authority coincide. In that case, the authority runs the $\mathsf{ABS.TSetup}$ and $\mathsf{ABS.ASetup}$ routines to generate a global key pair for the scheme, and publishes the public key PK. This public-key will be picked up by all users who need to create or verify signatures in the system.

Later, each user visits the authority to obtain private keys corresponding to her attributes. Let $\mathcal{A} \subseteq \mathbb{A}$ be the set of attributes that the authority wants to give to this user. Then the authority runs $\mathsf{ABS.AttrGen}$ to generate a signing key $SK_{\mathcal{A}}$ corresponding to the set of attributes possessed by that user.

After this, parties can sign and verify messages without further interaction with the authority. As long as the authority is uncorrupted, the unforgeability guarantee holds. Further, even if the authority is corrupt, the perfect privacy guarantee holds for the signer.[8]

Changing Attributes In the scenario above the authority issued a single key $SK_{\mathcal{A}}$ for the set of attributes $\mathcal{A}$. Once issued this attribute set is never changed. This is usually not satisfactory. There are two possible solutions that ABS offers.

When a user's attribute set changes, the authority can reissue an entire new set of signing keys, generated via $\mathsf{ABS.AttrGen}$. This is akin to establishing a new user with new set of attributes. By the collusion-resistance the user cannot combine keys in the new set with keys in the old set (or any other set for that matter). The user can of course still create signatures using the old set of attributes, so the attributes should be designed to include expiry information if the system requires revoking the old attributes.

Alternately, if the user simply acquires new attributes, it is not necessary to issue a totally new key set. Though not apparent from the syntax presented above, in fact our ABS construction allows the authority to augment a key $SK_{\mathcal{A}}$ to $SK_{\mathcal{A}\cup\mathcal{A}'}$. (The syntax for this operation is made explicit in our definitions for multi-authority ABS in the full-version, where keys are issued for one attribute at a time.) To allow for augmenting signing keys with new attributes, the authority could either maintain some state per user (to remember the randomness used to generate the key $SK_{\mathcal{A}}$), or provide a signed certificate of some public randomness that the user can keep and must bring back when requesting each new attribute, or more practically use a pseudorandom function such as AES to obtain this randomness as a function of the user's identity. In the latter case, the authority only needs to remember just one additional pseudorandom function seed (or AES key).

[8] Of course, if the authority wishes to reveal the user's attributes, it can; but irrespective of what the authority reveals, the signer has the guarantee that creating a signature reveals no *further* information about its attributes (beyond the fact that its attributes satisfied the claim-predicate).

B Comparison with Anonymous Credentials

It is useful to compare and contrast ABS with the widely studied notion of anonymous credentials (AC) [16]. Like ABS, anonymous credential systems allow users to anonymously demonstrate posession of attributes. Further, a recent AC scheme [1] uses similar basic tools as a couple of our ABS schemes, namely Groth-Sahai NIZK schemes. However, the goals of AC differ from ABS in several important ways.

To understand the difference between AC and ABS, consider using a *multi-authority* ABS system to approximate an AC scheme: a user will use an attribute each from the different attribute authorities as her credentials from them. The user can then use signatures from an ABS scheme to prove the possession of credential from any authority, in an anonymous manner (for instance, by signing a challenge nonce and a signature key used for further communication).

On the positive side, the ABS approach extends to using an unbounded number of attributes from each authority, and further revealing only a predicate of the attributes possessed, rather than the individual attributes themselves. Note that the former requires that with a small, fixed amount of public key material, the attribute-issuing authority in an ABS scheme can manage an unbounded universe of attributes. In contrast, an authority in an AC scheme (including the one in [1]) is typically considered to be responsible for only a single attribute. Put differently, in AC schemes, the public key material scales linearly with the number of attributes in the system, whereas in ABS the public key scales with the number of authorities, but is independent of the number of attributes in the system. More recently, [13] considers allowing an unbounded universe of attributes, without suffering a corresponding blowup in the public key, but their construction allows only a single level of disjunctions or conjunctions of attributes.

On the flip side, ABS does not provide the kind of anonymity against authorities that an AC system provides. Indeed, a significant complication that arises in constructing an AC scheme has to do with ensuring that when the same user registers with multiple authorities, her multiple registrations cannot be linked with each other. However, multi-authority ABS, as we have proposed, does not provide this kind of anonymity against the authorities; it allows colluding attribute authorities to find out which attributes a particular user has. Nevertheless, this information from the registration phase is the only information that an ABS system leaks; in particular, when a user proves the possession of credentials, even colluding authorities cannot identify the user. This provides sufficient anonymity in many access control applications, especially if anonymity is required against entities who do not themselves issue credentials.

The simpler anonymity guarantee in an ABS scheme comes with the advantage that an ABS scheme is significantly more efficient during attribute acquisition. In particular, AC schemes involve a zero-knowledge proof protocol during this phase, whereas for ABS, this phase can be implemented using little more than standard digital signatures.

Finally, ABS is a signature scheme as opposed to AC. While a signature scheme can be used for proving credentials and setting up an authenticated channel based on that, it has many more applications, and perhaps has a more intuitive semantics than an AC scheme.

In short, ABS is in some ways a simpler primitive compared to AC, with less demanding anonymity requirements, but with a richer and more expressive functionality, more efficient implementations, and several new applications.

C Proofs and Details of our ABS Constructions

C.1 General Framework

Proof of Theorem 1. Perfect privacy follows directly from the perfect witness hiding of the NIWI scheme, which our ABS scheme instantiates using the perfectly hiding setup.

Assuming that the NIWI scheme is sound, we show that any adversary A that violates ABS unforgeability can be converted into an adversary A^* that violates the security of the underlying credential bundle scheme, with comparable advantage. Let A^* simulate a copy of A, and perform one of the following two simulations in the bundle security experiment:

Simulator 1: Receive from the experiment tvk and run $(crs, \psi) \leftarrow$ NIWI.SimSetup. Give $TPK = (crs, tvk)$ to A as the simulated result of ABS.TSetup. Run $(APK, ASK) \leftarrow$ ABS.ASetup honestly and give APK to A. Whenever A makes a query $\mathcal{A} \subseteq \mathbb{A}$ to the ABS.AttrGen oracle, compute the response honestly.

Whenever A makes a query (m, Υ) to the ABS.Sign oracle, request from the CB.Gen oracle a singleton bundle for the pseudo-attribute associated with (m, Υ). Use the result as a witness to generate a NIWI proof of $\Phi[vk, m, \Upsilon]$ to use as the simulated ABS signature.

Whenever A outputs a valid forgery (m^*, Υ^*, π^*), use NIWI.Extract with the trapdoor ψ to extract a witness for $\Phi[vk, m^*, \Upsilon^*]$. Extraction succeeds with overwhelming probability, thus we obtain a bundle that contains the pseudo-attribute associated with (m^*, Υ^*) or sufficient attributes to satisfy Υ^*. If the bundle contains the pseudo-attribute, then it represents a forgery against tvk from the external forgery experiment, since A^* has never requested (m^*, Υ^*) from its CB.Gen oracle.

Simulator 2: Similar to above, except receive a bundle signature verification key from the experiment and treat it as avk instead of tvk. Then generate tvk honestly, and give simulated ABS signatures to A by generating bundle signatures on the pseudo-attribute. Relay all of A's queries on its ABS.AttrGen oracle to the external CB.Gen oracle. Then when A outputs an ABS forgery, extract it. If the extracted bundle satisfies Υ^* (rather than contains the associated pseudo-attribute), then the bundle is a forgery in the external experimant.

Both simulations induce identical views for A, and the key observation is that any valid forgery by A must be extracted to give a forgery suitable for one of the two simulations.

By applying the security of the NIWI scheme in a straight-forward series of hybrids (first replace legitimate signatures with simulated signatures, then replace NIWI.Setup with NIWI.SimSetup), we see that the advantage of one of the two simulations in its unforgeability game is comparable to that of A in the ABS forgery game (losing only a factor of 1/2). □

From this theorem and the constructions in [31, 18], we see that polynomial-time ABS schemes exist if enhanced trapdoor permutations exist.

C.2 Efficiency of Instantiation 1

We simplify the following efficiency analysis by noting that $n \leq \ell$.

The proof requires $\ell(5 + 4k)$ variables: for each $i \in [\ell]$, the prover must commit to $g^{v_i}, S, S^{v_i}, D^r, C^\tau$ as well as all k of the bits of τ, r in both groups (if $\mathbb{G} = \mathbb{H}$, then only $\ell(5 + 2k)$ variables are needed).

There are $t + 4\ell k$ quadratic $\mathbb{Z}_p$ equations (these are equations where both the variables and the coefficients have known discrete logs): t to perform the matrix multiplication and $4\ell k$ to establish

$\tau_j, r_i \in \{0,1\}$. The t matrix multiplication equations are of a special form (all variables are in $\mathbb{G}$) that some instantiations of Groth-Sahai can optimize. When $\mathbb{G} = \mathbb{H}$, $2\ell k$ of these equations are not needed.

There are 3ℓ multi-scalar product equations (these are equations where all variables and coefficients in one of the two groups have known discrete logs): for each $i \in [\ell]$, the equations involving S, D^r, and C^τ.

Finally, there are ℓ pairing-product equations (the most general form supported by Groth-Sahai): the equations that verify the main pairing equation for each $i \in [\ell]$.

Depending on the instantiation of Groth-Sahai used (based on either the SXDH or DLIN assumptions), the entire size of the ABS signature (measured in number of group elements) is given in the following table:

# of group elts	SXDH	DLIN ($\mathbb{G} = \mathbb{H}$)
$(5+4k)\ell$ vars	$10\ell + 8\ell k$	$15\ell + 6\ell k$
$t + 4\ell k$ quadratic	$2t + 16\ell k$	$2t + 12\ell k$
3ℓ multi-scalar	18ℓ	27ℓ
ℓ pairing-prod	8ℓ	9ℓ
signature size	$36\ell + 2t + 24\ell k$	$51\ell + 2t + 18\ell k$

We remark that the most efficient Groth-Sahai proof instantiation uses a composite subgroup decision problem, but working in a prime order subgroup of unknown size within a composite order group is incompatible with our approach. First, users must be able to compute $\vec{v}$ and matrix $\mathbf{M}$ given a description of Υ and a satisfying assignment. This may not always be possible if the linear algebra is in a field of unknown size. Second, Boneh-Boyen signatures are only known to be useful in groups of prime order.

C.3 Instantiation 2 Details

We can also instantiate our framework using the same approach as above, but with the signature scheme of Waters [36]. Signatures in Waters' scheme do not include any elements of $\mathbb{Z}_p$. This fact allows us to avoid the inefficiency of committing to many components of the Boneh-Boyen signatures in a bitwise fashion (though one bitwise commitment is needed for the tag τ of the credential bundle). Furthermore, Waters signatures are secure under the much weaker BDH assumption, which is implied by the assumptions required for Groth-Sahai proofs. Thus this instantiation does not require the additional q-SDH assumption. However, as a tradeoff, the Waters instantiation requires larger public parameters: a linear (in the security parameter) number of group elements, not the constant number of group elements needed by the Boneh-Boyen instantiation.

Waters signatures We briefly review the Waters digital signature scheme [36]. As before, we suppose there is a bilinear pairing $e : \mathbb{G} \times \mathbb{H} \to \mathbb{G}_T$, where $\mathbb{G}$ and $\mathbb{H}$ have prime order p, and where g is a random generator of $\mathbb{G}$, and h is a random generator of $\mathbb{H}$ (it is important that g and h are chosen independently at random, in the case where $\mathbb{G} = \mathbb{H}$).

DS.KeyGen: Choose random $a, v_0, \ldots, v_n \leftarrow \mathbb{Z}_p$ and compute $A = h^a$, $V_i = g^{v_i}$. The verification key is $(A, V_0, \ldots, V_n)$, and the signing key is $g^a \in \mathbb{G}$.

DS.Sign($sk, m \in \mathbb{Z}_p$): Choose random $r \leftarrow \mathbb{Z}_p$. Set

$$\sigma_1 = \left(V_0 \prod_{i=1}^{n} V_i^{m_i} \right)^r g^a; \qquad \sigma_2 = h^r$$

where m_i is the ith bit of m. Output $\sigma = (\sigma_1, \sigma_2) \in \mathbb{G} \times \mathbb{H}$.

$\mathsf{DS.Ver}(vk, m, \sigma = (\sigma_1, \sigma_2))$**:** Output 1 if

$$e\left(V_0 \prod_{i=1}^{n} V_i^{m_i},\ \sigma_2\right) e(g, A) = e(\sigma_1, h)$$

and output 0 otherwise.

The Waters scheme is strongly unforgeable under the BDH assumpion, which is implied by either of the SXDH or DLIN assumptions (see [36]).

Expressing the Non-Interactive Proof using Pairing Equations We use the same approach as above to express the desired logic using pairing equations. The only significant difference is in how we encode clauses of the form

$$\exists\ \tau, \sigma, v : \left[v \neq 0 \Rightarrow \mathsf{DS.Ver}(vk, \tau \| m, \sigma) = 1\right]$$

where $\mathsf{DS.Ver}$ is now the Waters signature verification.

Since the Waters scheme treats $\tau \| m$ bitwise, we must commit to τ bitwise, as before (m is an attribute name, and therefore public in all of our proof clauses). In this way, we ensure that the extractor can extract the bits and reconstruct the entire witness τ.

Let $(\tau, \sigma = (\sigma_1, \sigma_2), v)$ be a witness to the above expression. Express τ bitwise as $\tau = \tau_1 \cdots \tau_k$ and m as $m_1 \cdots m_k$. As before, we commit to τ_i in both groups, as g^{τ_i}, h^{τ_i}, and then first prove that each is indeed a single bit. This is done exactly as in the previous instantiation.

Next, observe that the pairing equation

$$e\left(V_0 \prod_{i=1}^{k} V_i^{\tau_i} \prod_{i=1}^{k} V_{k+i}^{m_i},\ \sigma_2\right) e(g^v, A) = e(\sigma_1, h^v)$$

is logically equivalent to the desired expression $[v \neq 0 \Rightarrow \mathsf{DS.Ver}(vk, \tau \| m, (\sigma_1, \sigma_2)) = 1]$, provided that the prover sets $\sigma_2 = h^0$ when $v = 0$.

The prover cannot directly compute $\prod_i V_i^{\tau_i}$ given the committed values. Thus we let the prover commit to this intermediate value, and prove consistency via the following equations:

$$e\left(\left\langle \prod_{i=1}^{k} V_i^{\tau_i} \right\rangle, h\right) = \prod_{i=1}^{k} e(V_i, \langle h^{\tau_i} \rangle);$$

$$e(\langle \sigma_1 \rangle, \langle h^v \rangle) = e\left(V_0 \prod_{i=1}^{k} V_{k+i}^{m_i}, \langle \sigma_2 \rangle\right) \cdot\ e\left(\left\langle \prod_{i=1}^{k} V_i^{\tau_k} \right\rangle, \langle \sigma_2 \rangle\right)\ e(\langle g^v \rangle, A).$$

Note that since m, A, B, V_i are public, all the coefficients in these equations can be publicly computed. Thus we have:

Theorem 5. *Under either the DLIN or SXDH assumptions, there is an ABS scheme supporting claim-predicates represented as monotone span programs, with signatures consisting of $O(k + s)$ group elements, where s is the size of the monotone span program.*

Efficiency Again we simplify the following efficiency analysis by noting that $n \leq \ell$.

The proof requires $5\ell + 2k + 1$ variables: Each of the k bits of τ, in both groups (unless $\mathbb{G} = \mathbb{H}$), plus the product $\prod_i V_i^{tau_i}$, which is shared among several clauses. Then for each $i \in [\ell]$, the prover must commit to $g^{v_i}, h^{v_i}, \sigma_1, \sigma_2, A^{v_i}$.

There are $t + 2k + \ell$ quadratic $\mathbb{Z}_p$ equations (these are equations where both the variables and the coefficients have known discrete logs): t to perform the matrix multiplication, $2k$ to establish $\tau_j \in \{0, 1\}$, and ℓ to ensure consistency between g^{v_i} and h^{v_i}. The t matrix multiplication equations are of a special form (all variables are in $\mathbb{G}$) that some instantiations of Groth-Sahai can optimize. When $\mathbb{G} = \mathbb{H}$, the $2k$ equations involving τ_j are not needed.

There are $\ell + 1$ multi-scalar product equations (these are equations where all variables and coefficients in one of the two groups have known discrete logs): one equation involving each A^{v_i}, and one overall involving $\prod_i V_i^{\tau_i}$.

Finally, there are ℓ pairing-product equations (the most general form supported by Groth-Sahai): the equations that verify the main pairing equation for each $i \in [\ell]$.

Depending on the instantiation of Groth-Sahai used (based on either the SXDH or DLIN assumptions), the entire size of the ABS signature (measured in number of group elements) is given in the following table:

# of group elts	SXDH	DLIN ($\mathbb{G} = \mathbb{H}$)
$5\ell + 2k + 1$ vars	$10\ell + 4k + 2$	$15\ell + 3k + 3$
$t + 2k + \ell$ quad	$2t + 8k + 4\ell$	$2t + 6k + 3\ell$
$\ell + 1$ multi-scalar	$6\ell + 6$	$9\ell + 9$
ℓ pairing-prod	8ℓ	9ℓ
signature size	$28\ell + 2t + 12k + 8$	$36\ell + 2t + 9k + 12$

Compared to the instantiation using Boneh-Boyen signatures, this instantiation is much more efficient. Each Boneh-Boyen signature involves bitwise operations on an element of $\mathbb{Z}_p$, but Waters signatures avoid this, thus eliminating the dominating $O(nk)$ factor in the total Groth-Sahai proof size. We note that this improvement comes at the cost of having $O(k)$ group elements in the verification key, instead of $O(1)$ group elements as in the Boneh-Boyen instantiation.

D Notes on Instantiation 3

Our construction from Section 4.5 is perhaps the best choice in a typical attribute-based system, especially if the system already involves attribute-based encryption schemes whose security is proven in the generic-group model. We make a few notes about the efficiency and extensions of the scheme.

Delegation This scheme supports delegation of attributes in a natural way. Suppose a party has a signing key for $\mathcal{A}$, say, $(K_{\mathsf{base}}, K_0, \{K_u \mid u \in \mathcal{A}\})$. Then for any $\mathcal{A}' \subseteq \mathcal{A}$, when choosing random $r \leftarrow \mathbb{Z}_p^*$, the quantity $((K_{\mathsf{base}})^r, (K_0)^r, \{(K_u)^r \mid u \in \mathcal{A}'\})$ is a valid, correctly distributed signing key for attribute set $\mathcal{A}'$.

Probabilistic Verification Using a standard technique, signatures in this scheme can be verified probabilistically with only $\ell + 4$ pairings instead of $\ell t + 2$, at the cost of additional exponentiations and a very small probability of false positives.

To probabilistically verify a signature, proceed as in the normal verification algorithm, but replace the final t checks with the following random one: Choose random $r_1, \ldots r_t \leftarrow \mathbb{Z}_p^*$, and check

the single constraint:

$$\prod_{i=1}^{\ell} e\left(S_i, \prod_{j=1}^{t} (A_j B_j^{u(i)})^{\mathbf{M}_{ij} \cdot r_j}\right) \stackrel{?}{=} e(Y, h_1^{r_1})\, e\left(Cg^{\mu}, \prod_{j=1}^{t} P_j^{r_j}\right)$$

This is essentially a random linear combination of the t original constraints. Legitimate signatures pass such a check with probability 1, while invalid signatures pass with probability at most $1/p$.

Efficiency The total public key data consists of $3(t_{\mathsf{max}}+1)$ group elements, which we emphasize is independent of the number of possible attributes in the system. Signatures have linear size, consisting of $\ell + t + 2$ group elements, where ℓ and t are the dimensions of the claim-predicate's monotone span program. Signing can be done using a maximum of $2w+\ell(1+2t)+3$ exponentiations in G and H, where w is the minimum number of attributes needed for the signer to satisfy Υ.

D.1 Security Proof

In this section we prove the following theorem.

Theorem 6. *Instantiation 3 is a secure ABS scheme in the generic group model.*

We break the security proof into the following two lemmas.

Lemma 1. *Instantiation 3 is a correct (Definition 5) and perfectly private (Definition 6) ABS scheme.*

Proof. Correctness can be seen by straight-forward substitutions. To prove perfect privacy it suffices to show that for any claim-predicate Υ and any attribute set $\mathcal{A}$ that satisfies Υ, the output of $\mathsf{ABS.Sign}(PK, SK_{\mathcal{A}}, m, \Upsilon)$ is uniformly distributed among signatures σ, subject to the constraint that $\mathsf{ABS.Ver}(PK, m, \Upsilon, \sigma) = 1$. For $\sigma = (Y, W, S_1, \ldots, S_n, P_1, \ldots, P_t)$ it is easy to see that for any setting of $Y \neq 1$ and $S_1, \ldots, S_n$, there is a unique value of $W, P_1, \ldots, P_t$ for which the signature successfully verifies. We conclude by observing that Y and $S_1, \ldots, S_n$ output by $\mathsf{ABS.Sign}$ are distributed uniformly in their respective domains and that the signature output by $\mathsf{ABS.Sign}$ successfully verifies. □

Lemma 2. *Instantiation 3 is unforgeable (Definition 7) in the generic group model.*

Proof. We first observe that the distribution $\mathsf{AltSign}(ASK, m, \Upsilon)$ can be sampled in the following way:

Let $\mathbf{M} \in (\mathbb{Z}_p)^{l \times t}$ be the monotone span program for Υ, with row labeling $u : [l] \to \mathbb{A}$; let $\mu = \mathcal{H}(m \| \Upsilon)$.

1. Pick random $s_1, \ldots, s_l \leftarrow \mathbb{Z}_p$ and $y \leftarrow \mathbb{Z}_p^*$
2. For all $j \in [t]$, compute

$$p_j = \frac{1}{(c+\mu)} \left[\sum_{i=1}^{l} s_i (a + u(i)b) \mathbf{M}_{i,j} - y z_j\right],$$

   where $\vec{z} = [1, 0, \ldots, 0]$.
3. Output $\sigma = (g^y, g^{y/a_0}, g^{s_1}, \ldots, g^{s_l}, h_1^{p_1}, \ldots, h_t^{p_t})$

It is straight-forward to check that this distribution matches $\mathsf{AltSign}(ASK, m, \Upsilon)$. WLOG, we assume that in the security experiment, responses to signature queries are generated in this way.

We now proceed with the proof of unforgeability, following the standard approach for generic groups. Let $\mathtt{Lin}(S)$ be the set of functions that are linear in the terms in the set S. Let $\mathtt{Hom}(S)$ be the subset of $\mathtt{Lin}(S)$ of homogenous functions whose constant coefficient is zero. In the generic group model, the forgery generated by the adversary is a fixed function of the inputs given in the security experiment.

Since it can only benefit an adversary, we assume that the groups G and H coincide. Suppose the adversary outputs a purported forgery signature σ^* on a policy Υ^* and message m^* such that $(m^*, \Upsilon^*) \neq (m^{(q)}, \Upsilon^{(q)})$ for all q. Let $\mathbf{M}^* \in \mathbb{Z}_p^{l^* \times t^*}$ be the corresponding monotone span program with row labeling $u^*(\cdot)$. Let $\mu^* = \mathcal{H}(m^* \| \Upsilon^*)$, and suppose the signature has the form $\sigma^* = (g^{y^*}, g^{w^*}, g^{s_1^*}, \ldots, g^{s_{l^*}^*}, g^{p_1^*}, \ldots, g^{p_{t^*}^*})$.

To be a forgery, we need $y^* \neq 0$, and $w^* = y^*/a_0$, and

$$\sum_{i=1}^{l^*} s_i^* \mathbf{M}_{i,j}^* (a + u^*(i) b) \Delta_j = y^* z_j \Delta_j + (c + \mu^*) p_j^* \quad (\forall j \in [t^*])$$

WLOG we can assume that these constraints are functionally satisfied (when viewing y^*, w^*, s_i^*, etc. as appropriate functions in the random variables generated in the experiment); otherwise equality holds only with negligible probability. The rest of our proof proceeds by assuming these constraints are functionally equivalent, and eventually obtaining a contradiction: that there exists a $k_0 \in [n]$ such that $\Upsilon(\mathcal{A}_{k_0}) = 1$. In other words, the adversary could have generated a signature legitimately with the signing key for $\mathcal{A}_{k_0}$, and thus the output is not a forgery.

We know that $y^*, w^*, s_1^*, \ldots, s_{l^*}^*, p_1^*, \ldots, p_{t^*}^* \in \mathtt{Lin}(\Gamma)$, where

$$\begin{aligned}\Gamma =& \{1, a_0, \Delta_0, c\} \cup \{\Delta_j, a\Delta_j, b\Delta_j \mid j \in [t_{\mathsf{max}}]\} \\ & \cup \{x_k, x_k/a_0, x_k/(a + bu) \mid k \in [n], u \in \mathcal{A}_k\} \\ & \cup \{s_i^{(q)}, y^{(q)}, w^{(q)}, p_j^{(q)} \mid q \in [\nu], i \in [l^{(q)}], j \in [t^{(q)}]\}\end{aligned}$$

The rest of our analysis proceeds by comparing terms in these constraints. We can show that the multilinear functions given by the adversary's forgery cannot contain terms of certain kinds. Since $y^* = w^* a_0$, we get that:

$$y^* \in \mathtt{Hom}\left(\{\Delta_0 a_0\} \cup \{x_k : k \in [n]\} \cup \{y^{(q)} : q \in [\nu]\}\right)$$

It is easy to see that $\Delta_j | (c + \mu^*) p_j^*$ and hence $\Delta_j | p_j^*$. So,

$$p_j^* \in \mathtt{Hom}\left(\{\Delta_j, \Delta_j a, \Delta_j b\} \cup \{p_j^{(q)} : q \in [\nu]\}\right)$$

Consider j_0 such that $z_{j_0} \neq 0$. Then suppose y^* has a $\Delta_0 a_0$ term. Then there is a $\Delta_0 a_0 \Delta_{j_0}$ monomial in $y^* z_j \Delta_{j_0}$. This monomial cannot occur in $(c + \mu^*) p_{j_0}^*$, nor can it occur in $\sum_i^{l^*} s_i^* \mathbf{M}_{i,j_0} (a + u^*(i) b) \Delta_{j_0}$, since all monomials from the sum have a factor of a or b. Hence,

$$y^* \in \mathtt{Hom}\left(\{x_k : k \in [n]\} \cup \{y^{(q)} : q \in [\nu]\}\right)$$

Suppose p_j^* has Δ_j term. Then the right hand side contributes monomials Δ_j and $b\Delta_j$. Because y^* has no constant term, $y^* z_j \Delta_j$ can not contribute a Δ_j monomial. And similar to above, $\sum_i^{l^*} s_i^* \mathbf{M}_{i,j} (a + u^*(i) b) \Delta_j$ can not contribute a monomial with Δ_j alone, hence

$$p_j^* \in \mathtt{Hom}\left(\{\Delta_j a, \Delta_j b\} \cup \{p_j^{(q)} : q \in [\nu]\}\right)$$

Suppose p_j^* has a $p_j^{(q)}$ term. Then on the right hand side we will have a contribution of $(c+\mu^*)p_j^*$, producing a term with a factor of $(c+\mu^*)/(c+\mu^{(q)})$. Since $\mu^* \neq \mu^{(q)}$ for any q, this is a proper rational. No setting of y^* or $\{s_i^*\}_{i\in[l^*]}$ can yield terms in the final equation with a factor of $(c+\mu^*)/(c+\mu^{(q)})$. Hence:

$$p_j^* \in \mathtt{Hom}\left(\{\Delta_j a, \Delta_j b\}\right)$$

Consider j_0 such that $z_{j_0} \neq 0$. Now, y^* can not have a $y^{(q)}$ term, because neither $(c+\mu^*)p_{j_0}^*$ nor $\sum_i^{l^*} s_i^* \mathbf{M}_{i,j_0}(a+u^*(i)b)\Delta_{j_0}$ can contribute a monomial of this form. Hence:

$$y^* \in \mathtt{Hom}\left(\{x_k : k \in [n]\}\right)$$

Finally we conclude that:

$$p_j^* \in \mathtt{Hom}\left(\{\Delta_j a, \Delta_j b\}\right) \quad \text{and} \quad y^* \in \mathtt{Hom}(\{x_k : k \in [n]\})$$

Observe that any term which appears in y^* must also be contributed from the left hand side, to make the expression equal. So, we can split s_i^* into two parts; one whose terms involve x_k variables, and one which does not. Let

$$s_i^* = t_i^*\left(X_i\right) + \delta^*(\Gamma \setminus X_i)$$

where $X_i = \left\{\frac{x_k}{(a+u^*(i)b)} : u(i) \in \mathcal{A}_k, k \in [n]\right\}$. Observe that $t_i^* \in \mathtt{Hom}(X_i)$, and satisfies the following equation for all $j \in [t]$:

$$\sum_{i=1}^{l^*} t_i^* \mathbf{M}_{i,j}^*(a+u^*(i)b) = y^* z_j$$

Consider any x_{k_0} such that it has a non-zero coefficient in y^*. Construct v_i^*, for $i \in [l]$, by defining

$$v_i^* = \frac{1}{[x_{k_0}]y^*}\left[\frac{x_{k_0}}{a+u^*(i)b}\right] t_i^*$$

where the $[x]\pi$ notation denotes the coefficient of the term x in π. We see that v^* is a vector of constant coefficients which satisfies the equation $v^*M^* = [z_1 \ldots z_t] = [1, 0 \ldots, 0]$. Further, in every position where $v_i^* \neq 0$, the set $\mathcal{A}_{k_0}$ surely contained the attribute $u^*(i)$. By the properties of the monotone span program, it must be the case that $\Upsilon^*(\mathcal{A}_{k_0}) = 1$, and thus the signature is not a forgery. □

E Simulation-Extractable Identity-Based NIZK and ABS

Our technique of augmenting a NIWI proof with a digital signature scheme can be used to make any NIWI argument of knowledge into a *simulation-extractable*, identity-based NIZK argument of knowledge. Identity-based NIZK was defined in [24] as a NIZK proof with an associated identity. The soundness definition requires that seeing a proof under one identity does not help one to construct proofs under another identity (even proofs of the same statement).

Simulation-soundness [32], informally, requires that seeing a *simulated* proof does not help one to violate the soundness property of a proof system. In the case of proofs (or arguments) of knowledge, the corresponding notion is termed "simulation-extractability." We are interested in incorporating simulation-extractability into identity-based NIZK arguments of knowledge. We note that the identity-based NIZK from [24] is not simulation-sound.

Theorem 7. *Any statement provable in via Groth-Sahai proofs can be made an identity-based, simulation extractable, NIZK argument of knowledge, with overhead linear in the number of variables (independent of the number of constraints).*

Proof. The identity-based, simulation extractable NIZK scheme in the above theorem is described as follows:

ID-NIZK.Setup**:** Run $crs \leftarrow$ ID-NIZK.Setup and $(vk, sk) \leftarrow$ DS.KeyGen. Publish $crs' = (crs, vk)$.

ID-NIZK.SimSetup**:** Run $(crs, \psi) \leftarrow$ ID-NIZK.SimSetup and $(vk, sk) \leftarrow$ DS.KeyGen. Publish $crs' = (crs, vk)$, and use $\psi' = (\psi, sk)$ as the trapdoor.

ID-NIZK.Prove$(crs'; \Phi; id; w)$**:** Define $\Phi'_{vk,id} := \exists\ w, \sigma : \Phi(w) \vee \mathsf{DS.Ver}(vk, \mu, \sigma) = 1$, where μ is an encoding of (id, Φ). Output the result of NIWI.Prove$(crs; \Phi'_{vk,id}; w)$.

ID-NIZK.Verify$(crs'; \Phi; id; \pi)$**:** Define $\Phi'_{vk,id}$ as above, then output the result of NIWI.Verify$(crs; \Phi'_{vk,id}; \pi)$.

ID-NIZK.Extract(crs', ψ', π)**:** Output the result of NIWI.Extract$(crs, \psi; \pi)$.

ID-NIZK.Simulate$(crs', \psi'; id; \Phi)$**:** Define $\Phi'_{vk,id}$ as above, then compute $\sigma \leftarrow \mathsf{DS.Sign}(sk, \mu = (id, \Phi))$. Output the result of NIWI.Prove$(crs; \Phi'_{vk,id}; \sigma)$.

Now we argue that the above construction indeed gives an ID-NIZK.

First, the crs' output by ID-NIZK.Setup is indistinguishable from that of ID-NIZK.SimSetup, directly by the security of NIWI.Setup, NIWI.SimSetup. Next, simulated proofs are indistinguishable from legitimate proofs by the witness indistinguishability of NIWI.Prove.

Finally, we must show that if an adversary has access to an oracle for ID-NIZK.Simulate and outputs a valid (verifying) proof π^* on Φ^* under id^*, where (id^*, Φ^*) have never been queried to ID-NIZK.Simulate, then ID-NIZK.Extract outputs a witness for Φ^* with overwhelming probability. This is easy to see by simulating such an experiment within the signature scheme's unforgeability experiment. Each time a simulated proof is needed, we request a signature on (id, Φ) and use it to generate a simulated signature. By the correctness of NIWI.Extract, when the adversary outputs π^*, we obtain a witness for $(\Phi^*)'_{vk,id^*}$ with overwhelming probability. This is either a witness for Φ^*, or a signature on (id^*, Φ^*). However, the latter would constitute a signature forgery, thus with overwhelming probability we do in fact obtain a witness for Φ^*, as desired.

Finally, to prove Theorem 7, we describe an efficient application of the above construction, using Groth-Sahai proofs and Waters signatures. Groth-Sahai proofs are zero-knowledge only for statements that can be expressed (perhaps after adding extra variables) as pairing equations of the form:

$$\textstyle\prod_i e(\mathcal{X}_i, B_i) \prod_j e(A_j, \mathcal{Y}_j) \prod_{i,j} e(\mathcal{X}_i, \mathcal{Y}_j)^{\gamma_{ij}} = e(g, h)$$

where $\mathcal{X}_i, \mathcal{Y}_j$ are the formal variables, and A_i, B_j, γ_{ij} are public coefficients.

Suppose $(A, V_0, \ldots, V_n)$ is the Waters public key, and let $(\sigma_1, \sigma_2) \in \mathbb{G} \times \mathbb{H}$ be a candidate signature. Our approach is to develop a proof of the following statment:

$$\begin{aligned}\prod_i e(\mathcal{X}_i^\beta, B_i) \prod_j e(A_j, \mathcal{Y}_j^\beta) \prod_{i,j} e(\mathcal{X}_i^\beta, \mathcal{Y}_j^\beta)^{\gamma_{ij}} \\ \times\ e(V^*, \sigma_2^{1-\beta})\ e(g^{1-\beta}, A) = e(g^\beta, h)\ e(\sigma_1, h^{1-\beta}) \\ \wedge\ \beta \in \{0, 1\}\end{aligned}$$

In the above expression, $V^* = V_0 \prod_i V_i^{\mu_i}$, a public coefficient when μ is known. This new statement says that either the original statement was satisfied, or (σ_1, σ_2) is a valid signature on μ, as desired. We can rewrite any term of the form $e(C, z^{1-\beta})$ as $e(C, z) \cdot e(C^{-1}, z^\beta)$, and thus we must commit

to additional values: each $\mathcal{X}_i^\beta$ and $\mathcal{Y}_j^\beta$, as well as $g^\beta, h^\beta, \sigma_1, \sigma_1^\beta, \sigma_2, \sigma_2^\beta$. We prove the expression above, using the commitments to these values.

Finally, we add additional pairing equations to prove that $\beta \in \{0, 1\}$. First, equations $e(\langle g^\beta \rangle, \langle h^\beta \rangle) = e(\langle g^\beta \rangle, h)$ and $e(\langle g^\beta \rangle, h) = e(g, \langle h^\beta \rangle)$. We must also prove that the commitments to $\mathcal{X}_i^\beta, \mathcal{Y}_j^\beta, \sigma_1^\beta, \sigma_2^\beta$ are consistent with β, using equations of the form:

$$e(\langle \mathcal{X}_i \rangle, \left\langle h^\beta \right\rangle) = e(\left\langle \mathcal{X}_i^\beta \right\rangle, h); \qquad e(\left\langle g^\beta \right\rangle, \langle \mathcal{Y}_j \rangle) = e(g, \left\langle \mathcal{Y}_j^\beta \right\rangle).$$

We note that this transformation can be applied to every pairing equation in the Groth-Sahai proof, re-using the same $\beta, \sigma_1, \sigma_2$, and shared $\mathcal{X}_i^\beta, \mathcal{Y}_j^\beta$ variables. Thus the overhead of the transformation is linear in the number of variables, and independent of the number of pairing equations proven on those variables. □

F Multiple Attribute Authorities

When an attribute-based system is in an enterprise setting (say, an attribute-based messaging system for communications within a corporation), there would be a single authority issuing attributes to the users and setting up the ABS scheme. However, for many practically interesting settings, it is important to allow users to obtain attributes from different attribute authorities who may not trust each other, or may not even be aware of each other. Indeed, some of the attribute authorities may be corrupt, and this should not affect the attributes issued by other authorities.

As a simple illustrative example, suppose Alice wishes to anonymously publish an anecdote on user experience in online social networks. To give credibility to her story she decides to use the following claim to endorse her message:

(Facebook user for 2 years AND Has 100 Facebook friends)
OR (Has 100 Orkut friends AND Participated in 100 Orkut discussion forums)
OR ((Princeton professor OR Yale professor) AND Expert on online social networks).

Alice wants to endorse her anecdote using this claim, without having to reveal how she satisfies the claim. These attributes are owned by different attribute authorities like Facebook, Orkut, Princeton University, Yale University and the American Sociological Association, who may not trust each other, or may not even be aware of each other. Nor might all these authorities trust a common central agency. To satisfy the claim Alice may need to use attributes she acquired from different authorities, say Yale and the ASA. To make matters more challenging, Alice may have never interacted with Facebook's attribute-authority, and yet she wishes to use an arbitrary attribute string from Facebook as part of her claim.

In the following we extend the notion of ABS to such a multi-authority setting. Then in Appendix F.2 we will illustrate how Alice can use multi-authority ABS to solve her problem.

In a multi-authority ABS scheme, apart from (mutually distrusting) attribute authorities, there needs to be an entity to set up the various public parameters of the signature system. We call this entity the **signature trustee**. However, *we shall require that the signature trustee does not have to trust any attribute authority.* In particular, the attribute authorities use only the public keys from the signature trustee.

Finally, we shall also allow there to be multiple signature trustees. In this case, the attribute authorities would issue attribute keys to a user for all the signature trustees she wishes to work with. Here, an attribute authority or a signer need not trust the signature trustee.

Below we give a summary of the modifications in the syntax and security definitions of the ABS primitive for the multi-authority setting, followed by the formal definition.

Modified syntax. Our main changes in syntax involve separating the key material into pieces originating from different authorities. Further, the syntax must now include new safety checks on the key material, since (a) the authorities depend on the user to provide key material from the trustees, and (b) the users no longer consider all authorities as trusted entities.

The claim-predicates in the signatures are now required to carry the identity of the attribute-authorities who *own* the various attributes (possibly as meta-data attached to the attribute description). Note that if for any attribute appearing in the claim-predicate the verifier uses a different attribute-authority than what the signer used, the verification will simply fail. So it is in the interest of the signer to point to the correct attribute-authorities.

Definition 10 (Multi-Authority ABS)**.** *A* multi-authority ABS scheme *consists of the following algorithms/protocols:*

ABS.TSetup**:** *The signature trustee runs the algorithm* ABS.TSetup *which produces a* trustee public key PK *and* trustee secret key TSK*. The trustee publishes PK and stores TSK.*

ABS.TRegister**:** *When a user with user id* uid *registers with the signature trustee, the trustee runs* $\mathsf{ABS.TRegister}(TSK, \mathsf{uid})$ *which outputs a public* user-token τ*. The trustee gives τ to the user.*

ABS.ASetup**:** *An attribute authority who wishes to issue attributes runs* $\mathsf{ABS.ASetup}(PK)$ *which outputs an* attribute-authority public key APK *and an* attribute-authority secret key ASK*. The attribute authority publishes APK and stores ASK.*

ABS.AttrGen**:** *When an attribute authority needs to issue an attribute $u \in \mathbb{A}$ to a user* uid*, first it obtains (from the user) her user-token τ, and runs a token verification algorithm* $\mathsf{ABS.TokenVerify}(PK, \mathsf{uid}, \tau)$*. If the token is verified, then it runs* $\mathsf{ABS.AttrGen}(ASK, \tau, u)$ *which outputs an* attribute key K_u*. The attribute authority gives K_u to the user.*

The user checks this key using $\mathsf{ABS.KeyCheck}(PK, APK, \tau, K_u)$ *and accepts this attribute key only if it passes the check.*

ABS.Sign**:** *A user signs a message m with a claim-predicate Υ, only if there is a set of attributes $\mathcal{A}$ such that $\Upsilon(\mathcal{A}) = 1$, the user has obtained a set of keys $\{K_u \mid u \in \mathcal{A}\}$ from the attribute authorities, and they have all passed* ABS.KeyCheck*. Then the signature σ can be generated using*

$$\mathsf{ABS.Sign}\left(PK, \{APK_{\mathsf{auth}(u)} \mid u \in \mathbb{A}_\Upsilon\}, \tau, \{K_u \mid u \in \mathcal{A}\}, m, \Upsilon\right).$$

Here $\mathsf{auth}(u)$ *stands for the authority who owns the attribute u (as described in u), and $\mathbb{A}_\Upsilon$ is the set of attributes appearing in Υ. (m, Υ, σ) can be given out for verification.*

ABS.Ver**:** *To verify a signature σ on a message m with a claim-predicate Υ, a user runs*

$$\mathsf{ABS.Ver}\left(PK, \{APK_{\mathsf{auth}(u)} \mid u \in \mathbb{A}_\Upsilon\}, m, \Upsilon, \sigma\right)$$

which outputs a boolean value, accept *or* reject*.*

Security Definitions The security definitions are now a little more elaborate to accommodate for the different cases corresponding to different entities (signers, verifiers, attribute-authorities and signature-trustees) being corrupt.

The privacy requirement is formulated as a perfect information-theoretic property: for every PK, m, and Υ, the output distribution of $\mathsf{ABS.Sign}(PK, \{APK_{\mathsf{auth}(u)} \mid u \in \mathbb{A}_\Upsilon\}, \cdot, \cdot, m, \Upsilon)$ is the same no matter which τ, and attribute signing keys $\{K_u\}$ are used, as long as the keys $\{K_u\}$ have

all passed ABS.KeyCheck. In other words, there is a (computationally infeasible) procedure AltSign such that $\mathsf{AltSign}(PK, m, \Upsilon, \{APK_{\mathsf{auth}(u)} \mid u \in \mathbb{A}_\Upsilon\})$ is distributed exactly as a valid signature on m with claim-predicate Υ.

The unforgeability definition is modified to account for the case where some of the attribute authorities, and some signature trustees are corrupt. The unforgeability requirement is with respect to an uncorrupted signature trustee (whose setup is carried out by the experimenter in the security experiment).

Definition 11. *A multi-authority ABS scheme is* unforgeable *if the success probability of every polynomial-time adversary is negligible in the following experiment:*

1. *Run* $(PK, TSK) \leftarrow$ ABS.TSetup. *The adversary is given* PK *and access to the* $\mathsf{ABS.TRegister}(TSK, \cdot)$ *oracle.*
2. *The adversary can ask for honest attribute authorities to be instantiated using* ABS.ASetup. *For each of these, the adversary receives only the public key* APK *and gets access to a* $\mathsf{ABS.AttrGen}(ASK, \cdot, \cdot)$ *oracle. The adversary can also instantiate (corrupt) attribute authorities and publish public keys for them.*
3. *The adversary gets access to the alternate signing oracle* $\mathsf{AltSign}(PK, \cdot, \cdot, \cdot)$.
4. *At the end the adversary outputs* (m, Υ, σ).

Let $\mathcal{A}_{\mathsf{uid}}$ *be the set of* $u \in \mathbb{A}$ *such that the adversary queried the* ABS.AttrGen *oracle on* (uid, u). *Let* $\mathcal{A}_0$ *be the set of possible attributes corresponding to corrupt attribute authorities. Then the adversary succeeds if* σ *verifies as a valid signature on* (m, Υ), *and* (m, Υ) *was never queried to the signing oracle, and* $\Upsilon(\mathcal{A}_0 \cup \mathcal{A}_{\mathsf{uid}}) = 0$ *for all* uid *queried to the* ABS.TRegister *oracle.*

F.1 Construction

All our constructions generalize to the multi-authority setting. In the case of Schemes 1, 2 and 3, recall that the credential-bundles are implemented as signatures by the attribute authority on (nonce,attribute) pairs. In the multi-authority setting each attribute authority publishes their own signature verification key. The nonce will be derived deterministically (using a collision-resistant hash function) from the identity uid of the user, so that all authorities agree on the same nonce. The signature trustee publishes its own signature verification key and a CRS for the NIWI argument of knowledge. The NIWI system will be used to prove possession of sufficient attributes (valid signatures, under different verification keys) or a signature on the (message, predicate) pair under the the verification key of the signature trustee. With this modification, the rest of the construction is almost identical to that in the case of the single authority setting.

Our final scheme, which is secure in the generic group model, also extends to the multi-authority setting. Below we sketch in more detail the modifications required for this.

ABS.TSetup: Here the signature trustee selects the cyclic groups G and H, generators $g, C, h_0, \ldots, h_{t_{\mathsf{max}}}$, hash function $\mathcal{H}$, and $A_0 = h_0^{a_0}$, as in the single-authority setting. In addition, it generates a signature key-pair $(TSig, TVer)$ for a (conventional) digital signature scheme. The private key is $TSK := (a_0, TSig)$, and the public key is $PK := ((G, H), \mathcal{H}, g, A_0, h_0, \ldots, h_{t_{\mathsf{max}}}, C, TVer)$.

ABS.TRegister: Given uid, draw at random $K_{\mathsf{base}} \leftarrow G$. Let $K_0 := K_{\mathsf{base}}^{1/a_0}$, where a_0 is retrieved from TSK. Output $\tau := (\mathsf{uid}, K_{\mathsf{base}}, K_0, \rho)$ where ρ is (conventional) signature on $\mathsf{uid} \| K_{\mathsf{base}}$ using the signing key $TSig$ (also retrieved from TSK).

ABS.ASetup: Choose $a, b \leftarrow \mathbb{Z}_p$ and compute $A_j = h_j^a$, $B_j = h_j^b$ for $j \in [t_{\mathsf{max}}]$. The private key is $ASK := (a, b)$ and the public key is $APK := \{A_j, B_j \mid j \in [t_{\mathsf{max}}]\}$.

ABS.AttrGen: The token verification $\mathsf{ABS.TokenVerify}(PK, \mathsf{uid}, \tau)$ verifies the signature contained in τ using the signature verification $TVer$ in PK. $\mathsf{ABS.AttrGen}(ASK, \tau, u)$ extracts K_{base} from τ, and using (a, b) from ASK, computes $K_u := K_{\mathsf{base}}^{1/(a+bu)}$.

The key K_u can be checked for consistency using $\mathsf{ABS.KeyCheck}(PK, APK, \tau, K_u)$, which checks that $e(K_u, A_j B_j^u) = e(K_{\mathsf{base}}, h_j)$ for all $j \in [t_{\mathsf{max}}]$, where A_j and B_j are from APK.

ABS.Sign, ABS.Ver: These algorithms proceed verbatim as before, except where $(A_j B_j^{u(i)})$ is used (corresponding to the attribute $u(i)$ associated with the ith row of the monotone span program), we use $A_{ij} B_{ij}^{u(i)}$ where A_{ij} and B_{ij} are A_j and B_j from APK (as described in ABS.ASetup above) published by the authority $\mathsf{auth}(u(i))$ who owns the attribute $u(i)$.

In the above construction we used a τ which contained a certificate from the signature trustee binding K_{base} to uid. The need for this certificate can be avoided if we derive K_{base} as $K_{\mathsf{base}} = R(\mathsf{uid})$, where $R : \{0,1\}^* \to G$ is a hash function modeled as a random oracle. We use a random oracle because it is important that users have no advantage in computing the discrete logarithms of their K_{base} values. This eliminates the need for a user to present the token to the attribute authorities, and the need for token verification, because the attribute authorities could themselves derive the K_{base}. We stress that in our construction, we do not employ a random oracle anywhere, except for this optional efficiency improvement.

F.2 Using Multi-Authority ABS

As described above, ABS can support multiple, mutually independent (and possibly distrusting) agents who can set up their own signature infrastructure, and multiple agents who can issue their own attributes to users. To illustrate how ABS operates in such a setting, we return to the example introduced in the beginning of this section. Recall that Alice wishes to endorse her message with a claim which includes attributes owned by different attribute authorities like Facebook, Orkut, Princeton University, Yale University and the American Sociological Association. Alice needs to choose one or more signature trustees under whose system she will provide the signatures. Suppose Alice is aware that most of her potential readers use Google or the Department of Motor Vehicles (DMV) as trusted signature-trustees. Then Alice can go about endorsing her story as follows:

1. Alice registers herself with Google and the DMV (using ABS.TRegister). These trustees would use their idiosyncratic ways to bind the user with a user ID. For instance the DMV could use the user's driver's licence number and Google could use the user's social security number. Alice gets two tokens τ_{Google} and τ_{DMV} this way. We stress that the tokens issued by the trustees are *public*. As such it is not important for the trustees to verify the identity of a user while registering.

2. Alice happens to be a professor at Yale, and is certified by the American Sociological Association as an expert on online social networks. To obtain appropriate attributes, first she approaches Yale's attribute authority, and presents her tokens from Google and the DMV. For Yale to be able to issue her attributes under these trustees, Yale needs to have the trustee's public-keys. Further, Yale should be satisfied that Alice is indeed the person who possesses the user ID mentioned in the tokens. We shall assume that the Yale can verify the social security number and licence number of all Yale faculty. After verifying Alice's identity and the tokens she presented, using Google and DMV's trustee public-keys, Yale can issue corresponding attribute keys on the attribute "Professor at Yale" (for simplicity we ignore the

fact that Alice is untenured, and Yale would only issue an attribute saying Professor at Yale in 2008). Similarly the American Sociological Association will issue Alice keys for the attribute "Expert on online social networks" under the two trustees. Again, the ASA will need to be able to verify Alice's social security number and driver's licence for this, and have access to Google and the DMV's public trustee keys.

3. Alice has already registered herself with Google and the DMV and obtained her tokens. Later, when she has prepared her anecdote — which we shall denote simply by m — she can decide what claim to attach to it. As mentioned above, she decides on the claim (which we shall call Υ) involving additional attributes owned by the attribute authorities Facebook, Orkut and Princeton (from whom she does not have any attributes). Using her attributes from Yale and the American Sociological Association, she can successfully prepare a pair of signatures σ_{Google} and σ_{DMV} on m using Υ. For this she will need access to the public keys of Facebook, Orkut and Princeton (but need not have interacted with them otherwise). In describing Υ, each attribute is clearly marked as owned by the corresponding attribute authority, so that a verifier knows which public keys are to be used. Further, σ_{Google} and σ_{DMV} include the information that the signature trustee for that signature is Google and the DMV respectively.

4. Suppose Alice has anonymously published $(m, \Upsilon, \sigma_{\text{Google}}, \sigma_{\text{DMV}})$ on the internet. A user in India who trusts Google (but does not know if DMV can be trusted) can verify σ_{Google} and be convinced that the message was endorsed by someone possessing adequate attributes as claimed. For this she should have access to the public keys issued by all the attribute authorities (Facebook, Orkut, Princeton, Yale and the American Sociological Association).

   As an orthogonal issue, this user might believe that Princeton University's attribute authority has been hacked, and an attribute from that authority should not be trusted. In this case she does not attach any significance to the part of the claim (Professor at Princeton OR Professor at Yale).

In this example, Alice herself need not have trusted all the signature trustees. Indeed, she could be concerned that Google is interested in knowing who signed the message, or which attributes were used to sign them. Further, Orkut's attribute authority could be colluding with Google's signature trustee. But even so, the perfect privacy guarantee assures Alice that her signature does not contain any information other than the message and the claim-predicate (and other public information).

Finally, we point out that it is important to use user IDs (social security number or licence number) which cannot be shared among multiple individuals. To see this, suppose Google used an e-mail address as the user ID. Also suppose Alice and her friend Bob shared the e-mail address alice.and.bob@gmail.com . Yale could verify that the e-mail address indeed belongs to Alice. But, meanwhile Bob, who happens to be a professional chess player, can get an attribute Top-100 Chess Player from the World Chess Federation, also under the same user ID and token from Google, because the World Chess Federation verifies that the user ID indeed belongs to Bob. Thus, if they could share a user ID, Alice and Bob would be able to pool their attributes together and endorse messages claiming to have attributes satisfying Professor at Yale AND Top-100 Chess Player.

G Applications

G.1 Attribute-Based Messaging

Attribute-Based Messaging or ABM (e.g. [5]) provides an example of a quintessential attribute-based system which demands new cryptographic primitives for achieving its natural security goals. In an ABM system, the set of users to whom a message is addressed is not specified by their identities, but by an "attribute-based address": that is, a predicate on the attributes, such that the intended receivers are the users whose attributes satisfy the predicate. An ABM system can also ensure that only users whose attributes satisfy certain conditions can send messages to certain other users. All this must be facilitated without requiring the users to be aware of each other's identities or attributes.

End-to-End guarantees in ABM The goals of an ABM system can be achieved using trusted entities. But as in other communication systems, the users may require an *end-to-end* guarantee on these properties, independent of the entities involved in delivering the messages. That is, (1) senders would like to encrypt their messages so that only users with appropriate attributes can decrypt them, and (2) receivers would like to verify signatures on messages such that only users with appropriate attributes could have signed them; the signer should not be forced to reveal more details about its attributes or identity than what is relevant to the receiver. Note that here the users would be willing to trust the authority that issues the attributes, as a compromised attribute-authority could give all attributes to any user, thereby rendering the above guarantees meaningless.[9]

The first of these issues can be elegantly handled using attribute-based encryption: in particular the *ciphertext-policy attribute-based encryption* of Bethencourt, Sahai and Waters [4] provides just the right cryptographic tool. Their implementation of this encryption scheme was integrated into the ABM system of Bobba et al. [6] and demonstrated to be practical.

However, the second issue of authentication did not have a satisfactory solution until now. To highlight some of the issues involved, we point out shortcomings of some natural proposals using existing cryptographic tools:

- *Using certificates:* For each attribute that a user has, the attribute authority gives the user a new signing key and a certificate binding the attribute to the corresponding signature verification key. Then, to sign a message using her attributes, a user simply signs it using the signing key from the attribute authority and presents (a subset of) the certificates it received.

This achieves the goal of users not having to be *a priori* aware of other users or their attributes. But this "solution" has at least two drawbacks. First, the user has to reveal (a subset of) its attributes, rather than just some predicate of the attributes. Second, even though the user's identity is not directly revealed by the signature, multiple signatures can be linked together as coming from the same user.

- *Using mesh signatures:* To allow signing with non-trivial predicates of attributes, one could consider using the recently developed tool of mesh-signatures [11]. This does indeed provide a perfect privacy guarantee. However, this approach fails a crucial unforgeability requirement: multiple users can pool their attributes together and create signatures which none of them could have by themselves produced.

[9] In an ABM system, the entities in the message path are significantly more vulnerable than the attribute authority, because they need to stay online and be involved in every message delivery. The attribute authority interacts with users only when issuing them attributes.

• As a "fix" to the above collusion problem, one might consider using disjoint attribute universes for different parties. This would indeed prevent collusion, and would still retain the privacy guarantee that the signature does not reveal how the claim-predicate was satisfied. However this is also not a satisfactory solution, as it allows multiple signatures to be identified as being generated by the same user.

Using an ABS scheme simultaneously overcomes all these problems, and achieves (a) perfect privacy and unlinkability, and (b) collusion resistant unforgeability. In integrating ABS into ABM, the message path of the ABM need not be altered. But in the attribute keying path, during registration the users should obtain keys for signing and verification as well (in addition to keys for encryption and decryption). An implementation would follow the description in Section A.

ABS for Access Control in ABM As suggested above, the primary application of ABS in an ABM system would be to obtain end-to-end authentication guarantees. But in addition, ABS could be used by the system to implement access control: a typical ABM system will require that messages to some addresses be not delivered unless the sender has attributes satisfying a certain policy. That is, an attribute-based access control mechanism must decide whether to allow a messaging attempt from a sender or not, depending on the attributes of the sender and the attribute-based address of the message.

In the current implementations this is achieved by the sender authenticating itself to a central server in the message path, who then consults the attribute database to determine whether the sender's attributes satisfy the requisite predicate. This requires this central server having access to the user's identity as well as attributes. This in general is not considered a serious issue, because anyway the attribute database has to be queried for obtaining the list of recipients.

However, it is possible that the attributes of the receivers used in the addresses are not the same (and may not be as sensitive) as the attributes of the sender used to determine access privileges. In such a scenario, using ABS can completely eliminate the need to query the database regarding the more sensitive attributes. Instead, for each message, a sender can decide what predicate regarding its attributes is to be revealed, then sign the message with that predicate using ABS. A server in the message path can ensure that the claimed predicate satisfies the system's sending policy, and if the signature verifies, deliver the message. Note that since this signature verification can be carried out using public keys, it can be done at one of the many points in the message path, instead of at a centralized server.

In a complex ABM system one might require the senders to include two ABS tags with every message — one intended for the message delivery agents, and one for the end recipient. The former would typically involve a claim-predicate that is independent of the contents of the message, and simpler (and hence faster to verify). The signature intended for the receiver could be dependent on the message and more complex; note that this signature is verified by the individual users locally, without putting load on central servers.

ABS for inter-domain ABM There are several engineering and cryptographic challenges in implementing a truly inter-domain ABM system. Neither the current implementations of ABM nor attribute-based encryption schemes known today fully support multiple attribute authorities (so that a user can use attributes from different attribute-authorities in the same message). For instance, Chase's proposal [14] for multi-authority attribute-based encryption (originally for the schemes in [33, 20], but can be extended to the one in [4]) requires all the attribute-authorities to share secret keys with a central authority, thereby requiring the central authority to trust all the attribute authorities.

Remarkably, however, the multi-authority version of our ABS scheme is readily amenable to a full-fledged inter-domain setting. There can be multiple attribute-authorities and signature-trustees who need not trust each other. It is safe for a signer to produce signatures using keys from untrusted trustees, and it is possible to form signatures involving attributes from multiple (untrusted) attribute-authorities; the verifier needs to trust just one of the signature-trustees used.

G.2 Other Applications

ABS offers a unique combination of features that makes it suitable for several other scenarios as well. We point out a few potential applications. These are only meant to illustrate different possibilities of ABS, and not claimed to be solutions for these problems in their most general setting.

Attribute-Based Authentication Consider a server which allows clients to connect to it and carry out transactions depending only on the client's attributes. A client who wishes to carry out a transaction may wish to reveal only minimal information about its identity of attributes as required by the system policy. ABS provides an immediate solution: to establish an authenticated session, the server sends a unique *session-id* to the client. The client responds to the server over an encrypted channel with an ABS signature on (*session-id*, *session-key*), where *session-key* consists of freshly generated keys for symmetric-key encryption (with semantic security) and MAC. After verifying the ABS signature, the server grants the client access depending on the claim-predicate of the ABS tag. All further communication in the session is carried out using the session-key.

Leaking Secrets The classical application for which the notion of ring-signatures was developed by Rivest, Shamir and Tauman [30] is "leaking secrets." In a ring signature the signer can endorse a message and attach a claim that it is one of the identities (or attributes, in our case) in some set. This is indeed an instance of ABS, with a particularly simple class of claim-predicates, namely disjunctions. *Mesh signatures* [11] are an extension of this concept that allow a rich class of claim-predicates (the same class of claim-predicates supported in our construction). However, when allowing this larger class of predicates an issue arises which is not present in the ring signature setting — namely, the possibility of multiple users colluding to pool their attributes together. Note that when restricted to disjunction, having any one attribute is enough to satisfy the claim, and pooling attributes does not allow a coalition to satisfy any new disjunctions. But for any claim-predicate other than a disjunction, collusion can indeed help. In [11] collusion is considered legitimate: indeed attributes there are considered to be individual identities, and multiple users *must* collude to obtain multiple attributes.

ABS goes beyond mesh signatures and provides collusion-resistance. (If certain groups of users must be allowed to collude, an ABS scheme would treat them as a single user; indeed if there is only one user in the system, an ABS scheme degenerates to a mesh signature scheme.) In that sense ABS is a more appropriate generalization of ring signatures to complex claim-predicates in many settings.

The semantics of leaking a secret with an ABS signature is that a *single entity* who has attributes satisfying a certain claim has endorsed the message. Here it is important that the ABS allows claims to be in terms of some arbitrary attributes *chosen* by the signer (presumably designed to obscure their identity), as well as some attributes the signer might indeed possess.

Trust Negotiations Trust-negotiation between two parties is a well-studied problem in the setting of an attribute-based system. From a theoretical point of view, the problem is a special case of secure two-party computation. However much of the research on this problem focuses on

obtaining very efficient solutions when possible. A standard approach to such an efficient protocol is a carefully designed sequence of rounds in which the two parties progressively reveal more and more of their attributes. At its simplest, this can mean simply revealing one or more of one's own attributes in a verifiable manner. However, several recent works also consider cryptographic approaches to trust negotiation that give more privacy to users than is achieved when they simply take turns revealing their attributes [29, 19]. ABS permits a sophisticated way to reveal partial information about one's attributes that is natural for this setting: one party can prove to the other party that her attributes satisfy some complex predicate.

Being able to bind a message with such a proof about one's attributes, as ABS permits, allows for a robust turn-based trust negotiation protocol. At every step of the negotiation, there is an "ephemeral key" for secure communication (private-key encryption and MAC). At each step, the active party picks a new ephemeral key, signs it using ABS with the claim that he or she wants to reveal at that step, and sends it securely (using the ephemeral key from the previous step) to the other party, who verifies the signature. Using new ephemeral keys at each step prevents man-in-the-middle attacks by an adversary who has enough attributes to carry out only the first few steps of the negotiation.