Abstract
There are many different types of digital signature schemes and each type has its own characteristics, usage benefits, and drawbacks. Some of these signature schemes can be described as anonymous digital signatures, and they all differ in some way from the types of signatures we may be most familiar with. Those familiar types could be described as “ordinary signatures.” They are associated with X.509 digital certificates and the SignedData type defined in the Cryptographic Message Syntax (CMS) standards widely used in the financial services (X9.73), in the IETF to implement secure electronic mail, or more recently as the new ITU Recommendation X.894 that standardizes CMS for the telecommunications industry. Though anonymous digital signatures have been around for quite a while and implemented in many products, there is now a renewed interest of their application in new and emerging technologies such as electronic voting, cryptocurrencies, blockchains, distributed ledgers, payments, and smart contracts.

R
ecently, there has been increased interest in Bitcoin,1 zCash,2 Ether,3 and other cryptocurrencies. Along with this interest there has been a rise in the number of blockchain and distributed ledger technology (DLT) use cases, prototypes, and pilots. Though some of these involve cryptocurrencies, while others do not, it seems that nearly every day we learn of another use case or blockchain initiative being started.

Beyond the fear of being disintermediated and left behind as markets respond to change and evolve, a primary attraction of adopting blockchain technology by existing industries is the promise of this new technology to reduce costs4 and increase transparency. Competitive upstarts believe that blockchains will allow them to sweep away the old vanguard of entrenched market leaders as they revolutionize the way business is being conducted. Through the decentralization of trust5 that blockchain offers, some of its proponents hope that blockchain can even “provide a new lever to unseat today’s status quo of censorship and entrenched monopolies.”6

The drive by organizations to move from private, in-house blockchain experimentation to more flexible, public platforms seeks to bring greater transparency to their operations and business practices. While greater transparency may be beneficial in some cases, the public exposure of an organization’s detailed business information that is currently treated as internal use only may also serve to benefit competitors. This exposure creates business risk that must be managed in order for organizations to exploit the advantages that may be found in this new technology.

1 https://bitcoin.org/.
2 https://z.cash/.
3 https://www.ethereum.org/.

Though there is a need to protect personally identifiable and other sensitive information posted to a blockchain or other public store, security controls that provide data confidentiality are not sufficient for addressing all of these transparency risks. The use of tokenization or encryption can provide data confidentiality services to address some of these concerns. However, these types of security techniques may not adequately mask the identities of those who sign transactions publicly in a blockchain or distributed ledger environment, or mask the aggregated information made available about the signers’ organizations.

Though the terms confidentiality, privacy and anonymity have different meanings, these terms are popularly used interchangeably. In the case of a blockchain participant, it is the need for anonymity in its activities that is required. At the same time it is necessary to preserve the benefits that blockchain can bring to transparent transactions and open business operations. These conflicting requirements have brought about a resurgence of interest in security techniques that support data integrity and origin authenticity along with some degree of anonymity.

Anonymous signature schemes

The ISO/IEC 20008 standard specifies two categories of mechanisms that provide anonymous digital signatures. One category verifies signatures using a single group public key. The other category verifies signatures using a set of public keys, including the public key of the actual signer. The first category is referred to as group signatures, and the second as ring signatures. In practice, both group and ring signature schemes have many variations.

These variations have evolved from the original signature scheme definitions over time. Each derivative has added new characteristics to the techniques as initially defined. As an example, one variation on group signatures specified in ISO/IEC 20008-2 is Direct Anonymous Attestation (DAA), a special digital signature that balances “signer authentication and privacy” [4]. DAA applications have been used in mobile phone applications that rely on an embedded trusted platform module (TPM), as well as on other popular personal computer platforms.

However, in general, there are just three basic categories of signature primitives depending on which type of public keys is used for signature verification” [4]. These categories are illustrated in table 1. The ring and group anonymous digital signature schemes differ from the “ordinary”signature schemes that are commonly used to provide security for electronic mail systems and to sign X.509 certificates and certificate revocation lists (CRLs).

<table>
<thead>
<tr>
<th>SIGNATURE SCHEME</th>
<th>SIGNATURE VERIFICATION</th>
<th>SIGNER PRIVACY PROVIDED</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ordinary</td>
<td>Single-signer public key</td>
<td>None</td>
</tr>
<tr>
<td>Ring</td>
<td>Set of public keys</td>
<td>Depends on number of keys</td>
</tr>
<tr>
<td>Group and DAA</td>
<td>Group public key</td>
<td>Depends on group size</td>
</tr>
</tbody>
</table>

Table 1 – Categories of digital signature schemes

In ordinary signature verification, the signer public key reveals the signer’s unique information. Therefore, an ordinary signature does not provide signer privacy. For ring signatures,
signature verification uses a set of public keys, each binding to one potential signer. Here the level of privacy provided is dependent on the size of the public key set. For group and DAA signature verification, which makes use of a group public key, the level of privacy is dependent on the size of the group [4]. When used in blockchain and distributed ledger technology (DLT) environments, group signatures seem intuitively to be more suitable for use in private or permissioned implementations. Ringsignatures may be more suitable for use cases that are implemented in public or permissionless environments. Group signatures require a group manager, a central authority that manages group keys, while ring signature schemes do not. Still, there are some usage contexts in both public and private environments where each signature scheme category could be applied.

Group signatures

In their 1991 “Group Signatures” paper, Chaum and Van Heyst presented a new type of signature for a group of persons [3]. The group has numerous members and a single manager, all associated with a single signature-verification key, the group public key [1]. For all of the mechanisms specified in the 1991 paper, a trusted authority establishes the group scheme, and group membership is “fixed in advance” [3]. Each group member has his own secret signing key with which digital signatures that can be verified using the group public key can be produced [1], as illustrated in figure 1.

Figure 1 – Group: Shared signature verification key

Group signature schemes involve a group manager, an entity “who is able to open any group signature by showing which group member issued it” [2]. Signatures that are created by different group members are “indistinguishable to their verifiers, but not to the group manager” who can disclose the identity of any member of the group [8]. Due to this characteristic, group signature schemes are sometimes used in “applications such as electronic cash and electronic voting” where it is necessary to detect or “prevent payers from spending the same coin twice” (i.e., double spend) or “voters from casting more than one ballot” [2]. As described by Chaum and Van Heyst, the group manager has a secret master key with which it can “extract the identity of the group member” from a given signature instance [1]. This capability provides the property of signer traceability, in what are sometimes referred to “traceable signatures” [2]. Given a group signature instance, no one that is without possession of the secret master key held by the group manager should be able to determine which group member was the signer. This capability provides the property of signer anonymity, where the larger the size of the group, the more anonymity for each group member will be provided.

Group signatures are anonymous digital signature mechanisms in which a relying party uses “a group public key to verify a digital signature” on a message signed by a group member [6]. Some group mechanisms are capable of revealing by a designated signature verifier information about the signer. These mechanisms provide the capability of linking “two signatures signed by the same signer” or the capability of a “special entity to reveal the identity of the signer” by opening a signature [6]. Some group mechanisms have both a linking and an opening capability.

Group mechanisms may provide additional properties such as revocation. For some mechanisms, three levels of revocation may be performed by a group manager. The entire group may be revoked, a single group member may be revoked, or specific signing capabilities of one member may be revoked.
Up to four possible revocation types are described for the group signature mechanisms defined in part two of the ISO/IEC 20008 standard. The number of revocation types available in the standard vary by group mechanism. These mechanisms include private key revocation, verifier blacklist, signature revocation, and credential update. In contrast to group signatures, ring signature schemes do not support revocation.

**Ring signatures**

Ring signature schemes were first introduced in 2001 in a paper titled, “How to Leak a Secret” by Rivest, Shamir, and Tauman, that was then published again in 2006 [8]. These schemes do not have group managers, require a prearranged groups of users, or need any of the management procedures for setting, changing, or deleting groups [8]. Due to these characteristics, ring signatures are considered a “light-weight alternative to group signatures” [2].

As ring signatures were originally conceived, since there is no group manager, it should be possible to determine the identity of the ring signer only from self-disclosure. There is no group setup procedure, so ring signatures schemes can be initiated at any time. Signers only require the private key of the actual signer and the public keys of an arbitrary set of the possible signers (i.e., the non-signers) that includes the public key of the signer. The non-signer public keys are chosen by the signer to form a ring as shown in figure 2.

All a signer needs to create a ring signature is to choose the other ring members. This choice of ring members is dynamic, since the signer forms a new set of members with each signature. No permission is required to use the public keys of the other ring members or to include them in the ring. The signer needs no assistance or cooperation from these non-signers to create a ring signature, just access to their public keys. Since the signer is also included as a member of the ring, along with the other non-signer members, the signer should send the signed message through an anonymizer, such as Tor, to mask its origin.

Later ring signature innovations would show that it is possible to construct ring signature schemes that have “an opening mechanism, in which case they become group signatures with vastly simplified group management” [2]. There are other associated constructions with group and ring signatures. These others include “identity-escrow, anonymous credentials, concurrent signatures,” as well as list signature schemes, “traceable signatures, and direct anonymous attestation” (DAA) [2].

**Associated constructions**

Traceable signatures were first introduced as “a new privacy primitive” back in 2004 by Kiayias, Tsiounis, and Yung [7]. They are similar in their functionality to the group signatures described by Chaum and Van Heyst, but they include additional capabilities. These capabilities are described as “tracing and claiming” [2]. While tracing is also a characteristic of group signatures, traceable signatures allow “tracing of all signatures of a single (misbehaving) party without opening signatures and revealing identities of any other user in the system” [7]. In contrast, to perform similar tracing of all signatures of a group member would require examining the signatures of all group members, violating the privacy of all users if it were possible to do so at all to any scale [7].

Fujisaki and Suzuki described a traceable ring signature in 2008 that provides a means to overcome the anonymity of “malicious or irresponsible signers” [5]. Their ring signature variation uses a “tag that consists of a list of ring members and an issue” that refers to some event, such as perhaps “a social affair or an election” [5]. In their scheme, a ring member can sign a message related to an issue anonymously, but only one time per tag. This approach can provide the ability to comment anonymously, but can provide a deterrent to trolling since the tag cannot be reused without loss of anonymity. When applied to an election system, an anonymous individual attempting to vote more than once can be detected.

**Conclusion**

This article has described several anonymous digital signature schemes and has detailed some important similarities and differences in their characteristics. These characteristics help to distinguish where and how these security techniques can be applied in emerging technologies such as blockchain and smart contract environments. Traceable variations of the initial group and ring signature schemes have an important role to play in striking the balance between the benefits of anonymity to the individual and the traceability of the actions of an individual required to protect society from bad actors.

However, not everyone lives in a perfect world in which governments, business entities, and powerful individuals can be trusted to always act nobly and in their best interest. It is still sometimes in the best interests of society for an individual to be able to “leak a secret” without being imperiled. Even in a country like the United States, where we are purportedly protected by the constitution from unwarranted government surveillance, we are afforded very little protection against online stalking, against what has been fairly termed surveillance capitalism. Until we all can live in the perfect world, there will be a need for onion routers, identity mixers, and anonymous digital signature techniques.


Anonymous Digital Signatures | Phillip H. Griffin

References


About the Author

Phillip, CISM, has over 20 years of information assurance experience. He has served as a trusted security adviser, security architect, and consultant with leading corporations, and acted as committee chair, editor, and head of delegation in the development of US national and international security standards. Phillip has served on the ISSA Educational Advisory Council and the ISSA Journal Editorial Advisory Board, and actively participates in ITU-T SG17 Security, ISO TC68/SC2 Security, ISO/IEC JTC1/SC27 Security techniques, and X9 Financial Services standards development. He may be reached at phil@philipgriffin.com.

LOOKING AHEAD – JOURNAL THEMES

May: Cryptography
Today, multiple cryptographic technologies lie at the center of our daily interactions. In the corporate world, cryptography is a critical component of any mature corporate information security program to secure information that we access, process, transport, store, or retrieve. This is also true in personal lives, where we rely upon cryptography to protect our daily communications, entertainment, financial transactions, and transportation. We are seeking articles on all aspects of cryptography. Topics of interest include, but are not limited to, theory, technology, and application of blockchain technology, cryptography, digital signatures, digital rights management, email security, hashing, payment systems, personnel identifiers, quantum cryptography, and virtual private networks. What are the difficulties when implementing new cryptographic policies and procedures? How do you remain current on new cryptographic developments and technologies? How do you evaluate new cryptographic security technologies?

June: Privacy
The 2016 US election and Facebook data analytics scandal revealed that average people truly don’t know their rights in regards to information and data privacy, and the privacy we give up as we engage more and more with the Internet. Information privacy is an intertwined relationship between collecting, protecting, and sharing data, technology, and the expectation that our privacy is protected. Every data breach, engagement with social media, search history, smart appliances, and even the much-loved Amazon Echo reveal that our control over privacy has weakened even though privacy rights have grown stronger. Privacy has emerged as the most significant consumer protection issue. How little or how much do we have? What are our privacy rights? Should we demand more? Are we giving up too much privacy by living life on the Internet?

SUBMIT ARTICLES TO
EDITOR@ISSA.ORG.