Digital signatures: “What you are” versus “Who you are”

James H. Davenport and Dalia Khader

1 Introduction

“What you are” versus “Who you are” is a grand **challenge** in todays world. Authorizing people to do certain tasks relays these days on identifying the person while the actual need is to recognize their attributes. For example, to enter a certain secure building, technologies like checking fingerprints, showing ID cards, etc, are used and the information is checked against a database that has the information of all authorized users. This not only breaches privacy of people, it is also hard to scale for global use (i.e. using driving license all around globe). Furthermore, if some unauthorized user corrupts the database, the security of the whole system collapses. The **challenge** is to move away from identifying the *person* to extracting his *properties.* If the system can derive that the person owns enough attributes to enter the building then it does not need to know who (s)he is (e.g. To access building prove that you are an employee in company ’A’, who is a manager in the IT department). Another **challenge** that arises in attribute based systems is revocation, because “What you are” changes rapidly while “Who you are” does not. Cryptography began as the science of confidentiality and en/decryption was its main focus for a long time. Since the invention(s) of public-key cryptography, cryptography expanded to include the concept of digital signatures [4, Ch. 20]. Digital signatures are equivalent to handwritten signatures and fingerprints in the analog world. Nowadays, cryptography includes many concepts and ideas other than these two, however this document will raise grand **challenges** in the field of cryptography using digital signatures as our example.

2 Identity-based or Attribute-based?

Signatures have existed as a means of authentication for ages. Taking different formats according to the application. It started as a handwritten signature and later evolved to include seals/stamps and fingerprints. In the 70’s, *algorithms* (not complete *systems*) were provided in order to digitally sign documents. Until that point signing a document meant identifying the person. Signatures have been very useful in creating certified documents, *but* it has generally been necessary to rely on external evidence that the persons signing the document are *qualified* to do so. This is today’s **challenge**.

In the early days of digital signatures, signers owned a pair of keys, a public key known to everyone used as an input for the verification process and a private key known by the signer and used in the signature process. Shamir (see [4, p.115-116]) suggested identity-based cryptography which allows the user to verify a signature given the identity of the signer (rather than a public key), where ‘identity’ can be a passport number, email, address, etc. Identity based cryptography and digital signatures are very good for some issues, e.g. “is this the Mr X who is allowed to board the plane”, but not for others, like “is this signed by a competent authority certifying that these are legitimate chemical samples”. For such situations, cryptographers proposed attribute based signatures which is a set of algorithms that allow verifiers to extract attributes of the signer, (e.g. manager, professor, citizen of a certain country, student etc.) rather than identifying him, answering a real life **challenge**.

3 What is known about Attribute-based Signatures

Research in Attribute based signatures followed a certain trend. Cryptographers would identify an application that requires attribute signatures where that application would require certain properties that no existing cryptosystem provides. They would propose a totally new scheme with new security notions that serve such properties. The result was several schemes each serving a very specific application making it hard to employ in any other. The following are two examples of such schemes:

- Anonymous Credentials: Such systems (introduced by Chaum) have users and organizations. Organizations know the users by their pseudonyms and they issue credentials to these pseudonyms. Users, anonymously, can prove possession of a credential even to organizations that know them with a different pseudonym while unforgeablity of credentials is guaranteed [2, p. 63-64].

- Attribute based signatures: A system that is very similar in concept with anonymous credentials, however, it can mix more than one attribute in one query(i.e. signature) [2, 3].

Designing a scheme for a specific purpose lead to overlooking common problems. One of the most **challenging** problems is revocation and finding a standard infrastructure.

4 Revocation of Attributes

Revocation — "this is no longer valid" — is an issue of peculiar importance in the digital world. In the analog world, we might wish to supply a new signature, or even a new fingerprint after an accident, but the old one does not cease to be valid. In the digital world, revocation of "who one is" is generally assumed to be a rare process, as it is linked to theft (or forgery) of digital keys. Revocation of "what one is" is a much more common process: people change jobs (or get sacked!) all the time. People in authority are mortal, and the breaking of, say, a pope's seal on his death is akin to revocation.

Existing research on revocation focuses on three kinds of solution [2, pp. 128-129]: time stamps (akin to a passport's expiry date); revocation (or "stop") lists; and explicit re-calculation. The time stamp idea deals well with, say, company directors who are elected for fixed terms, but even here a stop list would be needed to deal with unforeseen events (takeovers or boardroom coups). For other kinds of attributes, other solutions may be more appropriate. One **challenge** is converting the existing research ideas into practicable solutions that meet real-world requirements.

5 We Need a Standard Infrastructure

While there is a significant public-key infrastructure that supports SSL certificates for web browsing, the equivalent is far from existing here, and the problem is more complex.

The attributes of a single person may be issued by many trusted authorities, (e.g. a university gives student id cards while the government gives passports and ID cards). The trusted authorities may be independent institutions or dependent. For example, universities and the ministry of education might be considered hierarchal authorities which implies that a student in university X is a student in general. Furthermore trusted authorities can be considered separable. A student ID and a driving license are given by two independent authorities, *but* both are needed to hire a car at student rates. Having a strong infrastructure for attribute based cryptography that includes such relations will help in making the system more scalable. In other words, one can produce one query that includes many attributes from different authorities instead of many queries for each attribute needed (e.g. A British resident who is a student, and that owns a driving license can get discount on petrol). The **challenge** is to be able to create one signature proving that you own all the various attributes because that is more efficient than having to provide a set.

6 Conclusion

Ever since the paper of Goyal *et al.* [1] in 2006, research in the area of attribute based cryptography has been of an interest to cryptographers. The importance of such schemes was realized and the IACR archive[1] alone has twenty papers or more around that topic (as of the day this document was written). The papers focused on proposing different cryptosystems that had various properties to serve the variety of applications that exist. None of the existing approaches have been deployed because of the grand **challenges** we propose in this document. It would be nice to try address these problems in order to use the schemes in real life. One can start with trying to apply solutions of similar problems in cryptography to attribute based cryptography.

References

[1] V. Goyal, O. Pandeyy, A. Sahaiz, and B. Waters. Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data. In *13th ACM CCS*, pages 89–98, 2006.

[2] D. Khader. *PhD Thesis.* University of Bath, 2009. `http://opus.bath.ac.uk/16738`.

[3] D. Khader, L. Chen, and J. Davenport. Certificate-free attribute authentication. In *Cryptography and Coding*, volume 5921 of *Lecture Notes in Computer Science*, pages 301–325. Springer, 2009.

[4] B. Schneier. *Applied Cryptography: Protocols, Algorithms, and Source Code in C.* Wiley, New York, 2nd edition, 1996.

[1] IACR is the most famous technical report archive for cryptography.