PRIVACY–ENHANCING CRYPTOGRAPHY–BASED MATERIALS

Almudena Alcaide[1], Esther Palomar[1], Israel Barroso-Perez[1] and Ali E. Abdallah[2]
[1]*Department of Computer Science, University Carlos III, Avda. Universidad 30, 28911 Leganés, Spain*
[2]*The Faculty of Business, Department of Informatics, London South Bank University*
90 London Road, SE1 6LN, London, U.K.

Keywords: Privacy–Enhancing schemes, Protocols and systems, Cryptography, Privacy, Anonymity.

Abstract: In this paper, we offer a comprehensible survey and classification on cryptographic schemes which serve as the building blocks for most privacy–enhancing protocols and systems being deployed nowadays. For each cryptography material here described we offer a brief description of its foundations, the privacy–related features it possesses and an illustration of its application to some real life scenarios. The classification proposed is, to the best of our knowledge, pioneer in collecting all cryptography material with regard to privacy.

1 INTRODUCTION

Formally, different types of cryptographic material can be viewed according to the following three-level general model (IEEE-P1363, 2009): (1) *Primitives* - Basic mathematical operations that are based on number-theoretic hard problems. Primitives are not meant to achieve security or privacy just by themselves, but they serve as building blocks for schemes. (2) *Schemes* - A collection of related operations combining primitives and additional methods. Schemes can provide complexity-theoretic security which is enhanced when they are appropriately applied in protocols. (3) *Protocols* - Sequences of operations to be performed by multiple parties to achieve specific goals. Additionally, in this work we consider *Systems* as a set of protocols which are implemented and integrated to achieve a common set of goals.

1.1 Overview of our Work

In this paper[1] we offer a brief survey and classification of cryptographic schemes, protocols and systems which assist or enhance privacy aspects of electronic operations. Most privacy–enhancing software and system architectures being deployed nowadays are based on the mechanisms described in this work. We present all cryptography material in chronological order, offering a brief description of its foundations. The privacy related issues being addressed are concerned with anonymity of the sender/recipient of some digital data, anonymity of the signer of some digital data, unlinkability of online transactions, unobservability of entities' online activities and the selective and minimal disclosure of information.

[1]The poster shows further graphs and tables which summarize the scope and content of our original work.

2 PRIVACY–ENHANCING SCHEMES

Blind Signature Schemes. To perform a blind signature (Chaum, 1983) over a message *m*, the user *U* must first blind *m*, typically by combining it in some way with a random blinding factor. The blinded message is passed to a signer *O*, who then signs it using a standard signing algorithm and its private key. The resulting message can be *unblinded* and can be later on verified against *O*'s public key.

Zero–Knowledge Proofs. Zero knowledge proofs (ZKPs) were first introduced by Feige et al. in 1987 (Fiege et al., 1987). A ZKP involves two parties who share an input to an NP problem. One of the entities called the *prover* wants to convince the other entity, the *verifier*, that he, the prover, knows a valid solution for the problem on that input, while making sure that no other information about such a solution leaks. ZKPs must satisfy the properties of *completeness*, *soundness* and *zero–knowledge* (that is, the verifier must learn nothing about the content of the proof).

Group Signature Schemes. Group signature, introduced by Chaum and Heyst (Chaum and van Heyst,

Alcaide A., Palomar E., Barroso-Perez I. and E. Abdallah A..
PRIVACY–ENHANCING CRYPTOGRAPHY–BASED MATERIALS.
DOI: 10.5220/0003517803790382
In *Proceedings of the International Conference on Security and Cryptography* (SECRYPT-2011), pages 379-382
ISBN: 978-989-8425-71-3

1991), provides the authentication of a signer within a certain group, at the same time as it protects the anonymity of the signer. Each member in the group can generate valid signatures on behalf of the group. Verifiers can verify that the signature is from the given group, but they do not know who within the group computed the signature. When necessary, say, if an abuse has occurred, the group manager can determine the signer's identity (anonymity revocation).

Dual Signature Schemes. Secure Electronic Transaction (SET) is designed to protect credit card transactions on the Internet (SETCo., 1998). An important innovation introduced in SET were the dual signatures applied in the following scenario: A user U constructs an *Order Information* token, denoted as OI, describing the concept of a purchase, quantity, price, etc. User U also generates a *Payment Information* token denoted by PI, including the card details and the amount to be paid. Item OI is destined to the Merchant M and item PI is destined to the user's Bank B. Both items are linked to the same transaction, however, OI is kept secret from B and PI is kept secret from the merchant M.

Commitment Schemes. A commitment scheme (Brassard et al., 1988), consists of a sender and a receiver, satisfying the following constraints: at the end of a *Commit phase* the sender is committed to a tuple of secret values (a single bit, a pseudonym, random values, etc.) which cannot be changed at a later stage. Additionally, the commitment should not reveal any information, to the receiver, about the content of the committed tuple. In a *Reveal phase*, the sender sends extra information to the receiver that allows him to determine the values that were concealed by the commitment.

Ring Signature Schemes. Ring signatures (Rivest et al., 2001) make it possible to specify a set of possible signers without revealing which member does actually produce a signature. Anyone can check the validity of a ring signature. A ring signature differs from a group signature scheme in two different factors. (1) Groups are not prearranged and, (2) Anonymity of the signer cannot be revoked. More recently, *Verifiable* ring signatures and *Deniable* ring signatures include the property of anonymity revocation by a predesignated verifier.

Identity–based Signature/Encryption Schemes. Although the concept was first introduced by Shamir in 1985 (Shamir, 1985), it was a much later work (Boneh and Franklin, 2001) where such a paradigm was finally efficiently realized. In a basic identity–based *encryption* (IBE) scheme, a sender Alice can use any identifier information from the receiver Bob (such as an email address, an IP address, etc.) to encrypt a message. In a similar way, an identity–based *signature* (IBS) scheme allows Alice to sign a message, using private information such that certain public identifier information (such as an email address, an IP address, etc.) serve to verify such signature. Identity–based cryptography eliminates the need for a public key infrastructure (PKI), although a Trusted Third Party (the PKG, private Key Generator), must be part of the scheme.

CL–Signature Schemes. Two new signature schemes SRSA–CL (Strong RSA assumption–based Camenisch–Lysyanskaya scheme (Camenisch and Lysyanskaya, 2003)) and BL–CL (Lysyanskaya, 2004) allow proofs to be performed on the messages being signed. They support signing several structured blocks of a message, instead of signing a message as an unstructured string of bits. They allow signatures to be issued on commitments of a message and, allow efficient ZKP of knowledge of a signature and of relations between signatures and commitments.

Verifiable Encryption/Decryption Schemes. In *Verifiable encryption* (Camenisch and Shoup, 2003), a party T has a public/private key pair (e_T, d_T). Party A encrypts, using T's public key e_T, a secret message m that satisfies a publicly-defined property Θ, and gives the resulting ciphertext c to another party B. The latter party demands that A proves that c is an encryption of a message satisfying property Θ. Verifiable encryption allows A to the proof with zero–knowledge, that m satisfies Θ. In *Verifiable decryption*, another party B' might obtain the ciphertext c, and may request that T proves that c decrypts under d_T to a message m satisfying a publicly-defined property Θ'; in this situation T simply gives m to B', and proves (with zero knowledge) to B' that the decryption was performed correctly.

Anonymous Biometric Schemes. Some unique characteristics of a biometric sample are extracted to form a *biometric template* which is stored in a database for subsequent comparison purposes. By providing an authentication constant value (the biometric template), although anonymity is preserved, the linkability across many databases and the traceability of transactions involving the same user result in a lost of privacy. The goal of *anonymous* biometric, also called untraceable biometrics (UB) is to securely extract a digital key from a biometrical template of a person in such a way that, neither the key nor the biometric template can ever be compromised or linked to any other stored biometric template database (untraceable databases).

3 PRIVACY–AWARE PROTOCOLS AND SYSTEMS

This section outlines the main protocols and systems which are built upon the aforementioned privacy-enhancing schemes.

One–pass Certificates. *One–show* certificates (Brands, 2000) offer privacy related features such as: (1) The certificate owner has control over what attributes from the certificates are shown to others and, (2) It is possible for a user to give interactive or non-interactive proofs that the attributes encoded in the certificate enjoy a given property, as encoded by a linear boolean formula. This is done without revealing the actual attribute value. The main drawback of Brands certificates is that using the same certificate twice makes the two transactions linkable even though the attributes are still hidden. It is applicable, for example, in anonymous electronic ticketing for access control purposes.

Multi–show Certificates. *Multi–show* digital certificates (Verheul, 2001) can be used several times and still guarantee unlinkability. The owner of a multi–show certificate can himself construct another ad-hoc certificates, with one or more of the same attributes from the original certificate such that they are unlinkable. However, Verheul's certificates do not allow the user to prove, in a zero–knowledge fashion, properties of the attributes of his certificate. In 2003, Persiano et al. introduced the concept of a *chameleon certificate* (Persiano and Visconti, 2003a). Chameleon certificates offer two important properties: (1) The owner of the certificate has complete control over the amount of information about its attributes that it is released, and (2) Different uses of the same certificate are unlinkable (multi–show property).

Anonymous Credentials. Globally, in an anonymous credential system users are allowed to (1) anonymously obtain credentials from authorities, (2) anonymously prove possession of those credentials and, (3) make different uses of the same credential unlinkable such that, verifier entities, not even if they joined forces, will be able to distinguish one user from another. Furthermore, in some cases, these credentials allow users to obtain other types of credentials. However, in anonymous credential systems, there is an inherent danger that dishonest users may transfer their credentials to other illegitimate parties.

Non–transferable Anonymous Credentials. In 1986, Chaum and Evertse presented the first non–transferable anonymous credential system (Chaum and Evertse, 1986). The system was based on the use of pseudonyms. More recently, in 2001, a more efficient and practical anonymous credential system was proposed by Camenisch and Lysyanskaya in (Camenisch and Lysyanskaya, 2001). Most anonymous credential systems rely on deterrents to credential delegation by tying the credential to any set of user's valuable secrets. However, some applications require a stronger guarantee of non–transferability, for example, anonymous credentials for country's citizenship. Anonymous biometric authentication is one way to confirm an individual's identity with a strong non–transferability guarantee.

Delegable Anonymous Credentials. Often in practice, a user is authenticated using some credential chain. i.e.: a root organization gives a credential to an intermediate party who can in turn use this to issue credentials to other users. A user can prove possession of a valid chain of credentials of a given length without revealing any other identifying information or attributes. In (Belenkiy et al., 2009), authors extended the Camenisch and Lysyanskaya anonymous credential system previously described, to allow credential delegation.

Privacy–enhanced PKI. Privacy–enhanced PKI (pPKI) can attain user authentication and yet protect user privacy. pPKI was first conceived by Jan Camenisch et al. (Camenisch et al., 2006). In their framework, authors propose to modify the standard $X.509$ certificates, to allow the implementation of a series of protocols based on ZKP of possession of such new $X.509$ certificates, using the same paradigm as in anonymous credential systems aforementioned. Other pPKI implementations are based on group signatures (Calandriello et al., 2007; Ren et al., 2008). Finally, a privacy-aware PKI is also obtained by the use of above mentioned chameleon certificates (Persiano and Visconti, 2003b).

Anonymous Routing. The Onion Router Protocol consists of a fixed infrastructure of *onion routers*. During a *Setup* phase, the initiator application, opens a socket connection with an onion router and establishes a path to the destination in the onion routing infrastructure, then sends *an onion* to the first router of the path. The onion is a layered data structure such that it is necessary to decrypt all outer layers of the onion in order to reach an inner layer. Since each router peels off a layer, the messages are unlinkable and untraceable.

Finally, Figure 1 summarizes the privacy properties considered by the described schemes, protocols and systems according to whether they are assured (✓), or deficient (−). The work has focused on giving an overview on the foundations of these materi-

Table 1: Summary of the privacy properties according to whether they are assured (✓), or deficient (–).

	Anonymity	Unlinkabilt.	Observabilt.	Control. Info. Disclosure
Blind Sig.	–	✓	✓	✓
ZKPs	✓	–	–	✓
Group Sig.	✓	✓	✓	–
Dual Sig.	–	–	–	✓
Ring Sig.	✓	✓	✓	–
IBE	of recipient	✓	✓	–
IBS	of signer	✓	✓	–
One–pass Credentials	✓	–	–	✓
Multiple–pass Credentials	✓	✓	✓	✓
Anonymous Credentials	✓	✓	✓	✓
pPKI	✓	✓	✓	✓
Rand. ZKPs	✓	✓	✓	✓
Anonym. Bio.	✓	✓	✓	–
Tor Routing	✓	✓	✓	–

als, escaping from the technical details of the actual implementations. The accompanied poster shows further illustrations summarizing the scope and content of our work.

REFERENCES

Belenkiy, M., Camenisch, J., Chase, M., Kohlweiss, M., Lysyanskaya, A., and Shacham, H. (2009). Randomizable proofs and delegatable anonymous credentials. In *Advances in Cryptology - CRYPTO 2009*, volume 5677, pages 108–125.

Boneh, D. and Franklin, M. (2001). Identity-based encryption from the weil pairing. In *Advances in Cryptology CRYPTO*, volume 2139, pages 213–229.

Brands, S. (2000). *Rethinking Public Key Infrastructures and Digital Certificates; Building in Privacy*. MIT Press.

Brassard, G., Chaum, D., and Crépeau, C. (1988). Minimum disclosure proofs of knowledge. *J. Comput. Syst. Sci.*, 37:156–189.

Calandriello, G., Papadimitratos, P., Hubaux, J.-P., and Lioy, A. (2007). Efficient and robust pseudonymous authentication in vanet. In *Proc. of the fourth ACM Int. workshop on Vehicular ad hoc networks*, VANET '07, pages 19–28.

Camenisch, J. and Lysyanskaya, A. (2001). An efficient system for non-transferable anonymous credentials with optional anonymity revocation. In *Proc. of the Int. Conf. on the Theory and Application of Cryptographic Techniques (EUROCRYPT '01)*, pages 93–118, London, UK. Springer-Verlag.

Camenisch, J. and Lysyanskaya, A. (2003). A signature scheme with efficient protocols. In *Proc. of the 3rd Int. Conf. on Security in communication networks*, SCN'02, pages 268–289.

Camenisch, J. and Shoup, V. (2003). Practical verifiable encryption and decryption of discrete logarithms. In *Proc. of Crypto 2003*, pages 126–144. Springer-Verlag.

Camenisch, J., Sommer, D., and Zimmermann, R. (2006). A general certification framework with applications to privacy-enhancing certificate infrastructures. In *Security and Privacy in Dynamic Environments*, volume 201 of *IFIP Int. Federation for Information Processing*, pages 25–37. Springer Boston.

Chaum, D. (1983). Blind signatures for untraceable payments. In *Advances in Cryptology, Crypto '82*, pages 199–203. Springer-Verlag.

Chaum, D. and Evertse, J. (1986). A secure and privacy-protecting protocol for transmitting personal information between organizations. In *Advances in CryptologyEurocrypt*, volume 263, pages 118–167.

Chaum, D. and van Heyst, E. (1991). Group signatures. In *Eurocrypt*, volume 547, pages 257–265.

Fiege, U., Fiat, A., and Shamir, A. (1987). Zero knowledge proofs of identity. In *STOC '87: Proceedings of the nineteenth annual ACM symposium on Theory of computing*, pages 210–217. ACM.

IEEE-P1363 (2009). Standard specifications for public-key cryptography. Technical report.

Lysyanskaya, A. (2004). Signature schemes and anonymous credentials from bilinear maps. In *Proc. of Crypto 2004*, pages 56–72. Springer-Verlag.

Persiano, P. and Visconti, I. (2003a). An anonymous credential system and a privacy-aware pki. In *Proc. of the Australasian Conf. on information security and privacy, ACISP*, pages 27–38.

Persiano, P. and Visconti, I. (2003b). An anonymous credential system and a privacy-aware pki. LNCS, 2003.

Ren, W., Ren, K., Lou, W., and Zhang, Y. (2008). Efficient user revocation for privacy-aware pki. In *Proc. of the 5th Int. ICST Conf. on Heterogeneous Networking for Quality, Reliability, Security and Robustness*, QShine '08, pages 11:1–11:7.

Rivest, R., Shamir, A., and Tauman, Y. (2001). How to leak a secret. In *Advances in Cryptology ASIACRYPT 2001*, volume 2248 of *LNCS*, pages 552–565. Springer Berlin / Heidelberg.

SETCo. (1998). Secure electronic transactions http://www.setco.org. In *SET Co. Protocol SET Bulletin 1998 Technical Proposal-1*.

Shamir, A. (1985). Identity-based cryptosystems and signature schemes. *Advances in Cryptology*, pages 47–53.

Verheul, E. R. (2001). Self-blindable credential certificates from the weil pairing. In *ASIACRYPT '01: Proceedings of the 7th Int. Conf. on the Theory and Application of Cryptology and Information Security*, pages 533–551. Springer-Verlag.