Identity(ID)-Based Signature from Pairings

Public key cryptography (PKC): This is the domain of cryptography, where techniques of secure communication are studied in presence of public key(s) in the system. The PKC can be viewed as a field of study of design and analysis of encryption schemes and digital signatures. There are fundamental objectives, aimed to achieve for a secure communiaction by the means of of cryptography. They are- privacy, authentication, integrity and non-repudiation. In a less formal way, digital signature is a public key cryptographic primitive which provides properties like authentication and non-repudiation. The main algorithms of a digital sigtaure are *signing*- where user signs a message, for the receiver, using her private key, and *verification*- where the receiver verifies the validity of the signature on the intended message, using signer's public key. Observing the importance and need of digital signature, variety of signature schemes have been proposed till date. In many revolution to this journey of signature in cryptography the seminal work of *identity (ID)-based cryptography* by Shamir [10] was one of the significant paradigms.

ID-Based Cryptography (IBC): In the conventional public key infrastructure (PKI) there is a certificate authority (CA) who certifies the public key(s). Shamir's work [10] eliminated the need of CA in PKC, hence reduced the overhead of key management in the system. In the IBC, the public key of a user is an easily computable function from his/her identity and the corresponding private key is generated by a trusted authority (TA). The first practical realization of ID-based encryption (IBE) was observed by Boneh and Franklin [1] in 2001. The functionality in their scheme was due to the amazing properties of bilinear pairing (aka bilinear map or pairing). This application of pairing attracted a huge number of cryptographers in the following years and consequently hundreds of public key primitives were proposed from pairings. Though, parallel to this technique, there are other constructions of IBE, for example using quadratic residuosity [4] and lattice [6]. But there are isuues with the size of public key and ciphertexts, which makes them less popular for practical implementation.

ID-Based Signature from Pairings: For the authentication, efficiency and other obvious reasons, the construction of ID-based signature schemes were also desired. Similar to the IBE, majority of ID-based signatures have been constructed from bilinear pairing. In more particular way, as they have been useful in the cryptographic constructions, the pairing is a bilinear map defined over the points of elliptic curve. Hence study of elliptic curves are inherently associated with the study of pairings for cryptographic purpose. Other than the functionality, the bilinear pairings have been popular choice also due to the new security notions they brough in the scheme, for example bilinear Diffie-Hellman problems [5]. Though the usage of pairing in signature was first realised in construction of a (non ID-based) Short signature [2], but the elementary signatures of Paterson, Hess and Choon-Cheon [9, 7, 3] opened doors to the possibilities of construction of efficient signatures on the ID-based setting from bilinear pairings. Following these works, there has been cluster of ID-based signature schemes since the last 3 decades which can be studied by categorising them in different classes, for example- efficiency, security notion (random oracle/standard model),... etc. On the other hand there are variety of digital signatures, constructed for different objectives, for example- Ring signature, Group signature, Blind signature (to achieve annonimity), Proxy signature (for delegation of signing rights), Designated verifier signature (for only authorized verification) etc. For a short thesis, one of the signature schemes can be studied and/or implemented in the view of its construction on the ID-based setting and using bilinear pairing.

Bilinear Pairing: Let G_1, G_2 and G_T be multiplicative cyclic groups of the same (large) prime order q. A map $e : G_1 \times G_2 \to G_T$ is called a *cryptographic bilinear map* or a *pairing* if it satisfies the following properties:

Bilinearity: For all $(g_1, g_2) \in G_1 \times G_2$ and for all $a, b \in \mathbb{Z}_q$, $(g_1^a, g_2^b) = e(g_1, g_2)^{ab}$.

Non-Degeneracy: There exists $(g_1, g_2) \in G_1 \times G_2$ such that $(g_1, g_2) \neq 1$ where 1 is the identity of G_T.

Computability: There exists an efficient algorithm to compute $e(g_1, g_2) \in G_T$ for all $(g_1, g_2) \in G_1 \times G_2$.

Remarks:

- A pairing $e : G_1 \times G_2 \to G_T$ is called *symmetric* or *Type 1* pairing if $G_1 = G_2$, otherwise it is called *asymmetric*, which is further categorized into Type 2 and Type 3 pairings.
- For additive cyclic group G_1 and symmetric pairing $e : G_1 \times G_1 \to G_T$ the bilinearity property is
$$e(ag_1, bg_2) = e(g_1, g_2)^{ab}.$$
- There are algorithms, for example Miller's algorithm [8] for computation of certain bilinear pairings.

ID-Based Signature: A generic framework of an ID-based signature scheme is as follows:

- $\boldsymbol{PP} \leftarrow$ **Setup**(λ)**.** On input of a security parameter λ it outputs the public parameters PP for the system, which is usually an implicit input to the further algorithms.
- $(Q_{ID}, S_{ID}) \leftarrow$ **KeyGen**(ID, s)**.** On input of user's identity and master secret this key generation algorithm outputs public key Q_{ID} and private key S_{ID} of the user.
- $\sigma \leftarrow$ **Sign**(m, S_{ID})**.** This probablistic algorithm produces signature on message m, using the private key S_{ID}.
- $(1$ **or** $0) \leftarrow$ **Verify**(m, σ)**.** This deterministic verification algorithm checks the validity of the signature σ on message m.

References

[1] Dan Boneh and Matt Franklin. Identity-based encryption from the weil pairing. In *Annual international cryptology conference*, pages 213–229. Springer, 2001.

[2] Dan Boneh, Ben Lynn, and Hovav Shacham. Short signatures from the weil pairing. In *International Conference on the Theory and Application of Cryptology and Information Security*, pages 514–532. Springer, 2001.

[3] Jae Cha Choon and Jung Hee Cheon. An identity-based signature from gap diffie-hellman groups. In *International workshop on public key cryptography*, pages 18–30. Springer, 2003.

[4] Clifford Cocks. An identity based encryption scheme based on quadratic residues. In *IMA International Conference on Cryptography and Coding*, pages 360–363. Springer, 2001.

[5] Ratna Dutta, Rana Barua, and Palash Sarkar. Pairing-based cryptography: A survey. 2004.

[6] Craig Gentry, Chris Peikert, and Vinod Vaikuntanathan. Trapdoors for hard lattices and new cryptographic constructions. In *Proceedings of the fortieth annual ACM symposium on Theory of computing*, pages 197–206. ACM, 2008.

[7] Florian Hess. Efficient identity based signature schemes based on pairings. In *International Workshop on Selected Areas in Cryptography*, pages 310–324. Springer, 2002.

[8] Victor S Miller. Use of elliptic curves in cryptography. In *Conference on the theory and application of cryptographic techniques*, pages 417–426. Springer, 1985.

[9] Kenneth G Paterson. Id-based signatures from pairings on elliptic curves. *Electronics Letters*, 38(18):1025–1026, 2002.

[10] Adi Shamir. Identity-based cryptosystems and signature schemes. In *Workshop on the theory and application of cryptographic techniques*, pages 47–53. Springer, 1984.