Chapter 11
Biometric Identity Based Encryption: Security, Efficiency and Implementation Challenges

Neyire Deniz Sarier
Bonn-Aachen International Center for Information Technology, Germany

EXECUTIVE SUMMARY

In this chapter, we evaluate the security properties and different applications of Identity Based Encryption (IBE) systems. Particularly, we consider biometric identities for IBE, which is a new encryption system defined as fuzzy IBE. Next, we analyze the security aspects of fuzzy IBE in terms of the security notions it must achieve and the prevention of collusion attacks, which is an attack scenario specific to fuzzy IBE. In this context, we present a new method that avoids the collusion attacks and describe the currently most efficient biometric IBE scheme that implements this new method. Also, we investigate implementation challenges for biometric IBE systems, where fuzzy IBE could be a potential cryptographic primitive for biometric smartcards. Due to the limited computational power of these devices, a different solution for biometric IBE is considered, which is the encryption analogue of the biometric identity based signature system of Burnett et al. (2007). Finally, we state the future trends for biometric IBE systems and conclude our results.

INTRODUCTION

Cryptography consists of set of mathematical techniques to achieve the goals of confidentiality, data integrity, entity authentication, and data origin authentication in order to provide information security in theory and in practice. These cryptographic goals can be summarized as follows (Sarier, 2007).

- *Confidentiality:* Confidentiality is the protection of transmitted data from passive attacks. Other aspect of confidentiality is the protection of traffic flow from analysis.
- *Authentication:* It is concerned with assurance of identity. It ensures that the origin of a message or electronic document is

DOI: 10.4018/978-1-60960-015-0.ch011

correctly identified, and the identity is not false. When a sales clerk compares the signature on the back of a credit card with the signature on a sales slip, the clerk is using the handwritten signatures as an authentication mechanism, to verify the person presenting the credit card is the person the card was sent to by the issuing bank.

- *Data Integrity*: assures that data has not been modified since the signature was applied. In other words, it ensures that only authorized parties are able to modify computer system assets and transmitted information. While a handwritten signature does not in itself provide data integrity services, digital signatures provide excellent data integrity services by virtue of the digital signature value being a function of the message digest; even the slightest modification of digitally signed messages will always result in signature verification failure.
- *Non-repudiation*: It prevents either sender or receiver from denying a transmitted message and could provide evidence to a third-party (like a judge, or jury, for example). The buyer's signature on the credit card sales slip provides evidence of the buyer's participation in the transaction, and protects the store and the card-issuing bank from false denials of participation in the transaction by the buyer.
- *Access Control:* It is the ability to limit and control the access to host systems and applications via communications links.
- *Availability:* It requires that computer system assets be available to authorized parties when needed.

Encryption tries to solve the problem of secure communication over an insecure channel, where apart from the sender and the receiver, an adversary may involve controlling the channel. The two types of encryption schemes are called as symmetric and asymmetric encryption, where the basic difference is the same secret key that is shared in the former one, whereas a pair of keys called public and secret key take part in the latter one. In addition, in symmetric encryption, the shared secret key must be transferred through a secure channel while asymmetric encryption does not require a secure channel to pass the encryption key at the cost of *authentication of public* keys. This way the sender A is sure that he is encrypting under the legitimate public key of the receiver.

The setting of public-key cryptography (PKC) is asymmetric in key information held by the parties, since one party (Bob) has a secret key while another (Alice) uses the public key that matches this secret key. This is in contrast to symmetric encryption, where both parties share the same key. Asymmetric encryption is thus another name for public-key encryption. Bob generates the pair of public/secret keys that belong to him and sends his public key over an authenticated channel to Alice, so that Alice can encrypt a message with Bob´s public key to be sent to him. The only person, who is able to read the message, is Bob, since only he possesses the secret key, which cannot be recovered in polynomial time. The authenticated channel is necessary to assure Alice that the public key of Bob really belongs to Bob. One difference between the symmetric and the asymmetric setting is the channel over which the keys are distributed. Instead of a secure channel, an authenticated channel is sufficient for PKC. On the other hand, PKC requires much more computational resources as the number-theoretic operations in these schemes are computationally costly relative to symmetric key cryptography (SKC), which should considered for energy-constrained ad hoc network devices. Hence, to minimize the amount of data to which these number-theoretic operations are applied, public key cryptography is used only to encrypt small data (short strings), namely symmetric encryption keys and digital signatures.

Besides, key management is easier in PKC since authenticity of public key through certifi-