Chapter 17
Secure Dynamic Signature–Crypto Key Computation

Andrew Teoh Beng Jin
Yonsei University, Korea

Yip Wai Kuan
Multimedia University, Malaysia

ABSTRACT

Biometric-key computation is a process of converting a piece of live biometric data into a key. Among the various biometrics available today, the hand signature has the highest level of social acceptance. The general masses are familiar with the use of handwritten signature by means of verification and acknowledgement. On the other hand, cryptography is used in multitude applications present in technologically advanced society. Examples include the security of ATM cards, computer networks, and e-commerce. The signature crypto-key computation is hence of highly interesting as it is a way to integrate behavioral biometrics with the existing cryptographic framework. In this chapter, we report a dynamic hand signatures-key generation scheme which is based on a randomized biometric helper. This scheme consists of a randomized feature discretization process and a code redundancy construction. The former enables one to control the intraclass variations of dynamic hand signatures to the minimal level and the latter will further reduce the errors. Randomized biometric helper ensures that a signature-key is easy to be revoked when the key is compromised. The proposed scheme is evaluated based on the 2004 signature verification competition (SVC) database. We found that the proposed methods are able to produce keys that are stable, distinguishable, and secure.

INTRODUCTION

With widespread information exchange and access to resources over public network, cryptography has become an important and necessary mechanism for secure channel access and authentication. According to Schneier (1996), the aim of cryptography is to provide secure transmission of messages, in the sense that two or more persons can communicate in a way that guarantees to meet the desired subset of the following four goals - confidentiality, data integrity, authentication and non-repudiation.

DOI: 10.4018/978-1-60566-725-6.ch017

However, there are some practical problems associated with the use of cryptosystem since the current methods authenticate the key instead of the user. The need for a proper and reliable key management mechanism is required in order to confirm that the listed keys actually belong to the given entities.

Currently, a manual method of authentication using identification card, company number or license, is required for enrolment of keys. In addition, the security depends on the large size of a cryptographic secret key generated, and it is not feasible to require user to remember such a long key. Thus a simple password is still required for key encryption which in turn leads to continuing potential hacker attack on the password to retrieve the cryptographic keys. Both passwords and cryptographic keys do not necessarily require the user to be present, leading to identity frauds.

Biometrics is the science of using unique human characteristics for personal authentication based on a person's biological and behavioral characteristics (Jain, A. K., Hong, L. & Pankanti, S. 2000). By incorporating biometrics technologies which utilize the uniqueness of personal characteristics, the keys can be placed in a secure storage and be protected by biometrics, instead of password. The keys will be released if a query biometrics matches the stored template. The security of cryptosystems could be strengthened as authentication now requires the presence of the user. Traditionally, biometrics based authentication for access into systems has always been yes/no decision model depending on how "close" the test biometrics is to a stored template. The decision is determined empirically and entails tuning of a threshold. This may open to systematic attack where a test biometrics is repeatedly presented to retrieve system threshold and hence leads to keys disclosure. This is more vulnerable to behavioral biometrics such as hand signature, due to existence of skilled forgery which is unlikely found in physiological biometric. To avoid the storage of the template, one alternative solution is biometrics on-the-fly using the help of some information about the biometrics. An unique and compact bit string of the biometric input can be used instead of just a simple threshold-based decision. Keys that could be generated directly from biometrics data are crucial for seamless integration between biometrics and cryptography.

Motivations and Contributions

In reality, direct biometrics to key transformation is not favorable. This is because biometrics suffers from privacy invasion and it is not replaceable. To make the matter worse, a new template cannot be assigned when compromised, and the only solution is to replace with another biometric feature. Yet, a person has only a limited number of biometric features which can be utilized, and thus, the replacement of biometric feature is not a feasible solution. Furthermore, inherent high variability of biometric data hinders it to be directly transformed into deterministic bit strings. Hence new frameworks and formalisms related to integrating biometrics into cryptosystems need to be considered.

Among various biometrics available today, hand signature is an ideal candidate for biometric-key computation. This is of particular important as wide array of cryptographic applications are remote and unattended over an unsecure public network. Hand signature has several advantages such as socially and generally well-accepted, more cost effective in terms of capturing equipment (e.g. PDAs, smartphones and mouse-pen) and non-intrusive. In online applications, dynamic hand signatures is preferable than just off line hand signatures due to higher security concern. Dynamic hand signatures are more difficult to copy as they require the capture of timing information from the signing action and other behavioral characteristics such as the pressure imposed, altitude of the pen and azimuth.

In this chapter, a dynamic hand signatures crypto-key computation scheme is discussed.