Chapter 2
Design Aspects of Secure Biometric Systems and Biometrics in the Encrypted Domain

Claus Vielhauer, Jana Dittmann, and Stefan Katzenbeisser

Abstract This chapter introduces the main security requirements for the biometric processing pipeline and summarizes general design principles and approaches. General IT security principles are reflected and selected paradigms such as template protection by biometric hashing, fuzzy commitment schemes, and fuzzy extractors are reviewed. Further, we discuss the design principles of biometric matching algorithms that operate in the encrypted domain. The overall algorithm design, implementation, and configuration issues are summarized and discussed in an exemplary manner for the case of face biometrics.

2.1 Security Requirements for the Biometric Processing Pipeline

Recently security has become one of the most significant and challenging problems during the introduction of new information technology. It therefore plays an important role for biometric systems and applications. Since digital biometric data can easily be copied without information loss, manipulated at will or forged without noticeable traces, security solutions are required to counter these threats. In order to judge and evaluate the overall trustworthiness, security criteria need to be defined, e.g. taken from the Europe-wide valid ITSEC catalogue of criteria [16], and applied to biometrics.

In general we can notice a rising awareness of security for biometric solutions. In which way security mechanisms can be applied to biometric data and their applica-

C. Vielhauer (✉)
Brandenburg University of Applied Sciences, Potsdam, Germany
e-mail: claus.vielhauer@fh-brandenburg.de

C. Vielhauer · J. Dittmann
Otto-von-Guericke University Magdeburg, Magdeburg, Germany

J. Dittmann
e-mail: jana.dittmann@iti.cs.uni-magdeburg.de

S. Katzenbeisser
Technische Universität Darmstadt, Darmstadt, Germany
e-mail: skatzenbeisser@acm.org

P. Campisi (ed.), *Security and Privacy in Biometrics*,
DOI 10.1007/978-1-4471-5230-9_2,

tions needs to be analyzed individually for each application and biometric modality. This is mainly due to the structure and complexity of biometric data as well as the privacy requirements derived from the right of all individuals to protect person-related data and information, as codified in data protection laws. Based on the central issues of IT-security, this chapter introduces the most important security requirements, which must be fulfilled by today's biometric systems. We first provide an overview of the basic security requirements (also called security aspects) in general by enumerating five generally known security aspects (confidentiality, integrity, authenticity, non-repudiation, and availability) and proceed with a discussion of privacy issues (unlinkability, unobservability, anonymity, and pseudonymity) that are commonly linked to biometric applications.

The security requirements of confidentiality, integrity, authenticity, non-repudiation, and availability are essential for computer and network systems (see for example [3] and [7, 27] or [20]). In the case of biometrics we consider as security target under investigation the involved resources such as humans (subjects), entities (such as components or processes) and biometric data (information).

Confidentiality refers to the secrecy or prohibition of unauthorized disclosure of resources. In cases of a biometric system it mainly refers to biometric and related authentication information, which needs to be kept secret from unauthorized entities. Confidentiality may ensure secrecy of user's biometric data when it is captured, transferred or stored. Particularly biometric information should only be accessible in full quality to the person it belongs. Beside this issue, during biometric verification or identification the accessing party needs to be restricted with appropriate security measures. This ensures that nobody apart from the allowed parties can use the measurement. An attack goal could be the unauthorized access to and copying of reference data, such as fingerprints. Biometric data is highly sensitive and personal, because any illegitimate possession and use of stolen data may lead to uncontrollable subsequent illicit use. For example, a stolen fingerprint reference can be used to construct artificial silicon fingerprints [24] for identity theft or even to lay fake fingerprint traces by printing the fingerprint patterns with amino acids as described in [21]. Some biometric modalities even reveal medical patterns that potentially indicate diseases [15].

Integrity of a biometric system refers to the overall integrity of all resources such as biometric and related authentication information and all software and hardware components involved in the biometric processing pipeline. Integrity is the quality or condition of being whole and unaltered (resource is not altered or manipulated) and refers to its consistency, accuracy, and correctness. Security measures offering integrity usually ensure that modifications are detectable. Different integrity degrees such as *low*, *middle*, *high* can be defined, see for example the International Electrotechnical Commission safety standard IEC-Standard 61508 (see the website http://www.iec.ch, 2011). Appropriate levels need to be defined and integrity policies for the overall system design, implementation, and configurations need to be imposed. For a biometric system the integrity should be defined as "high" for all

components, which means that any malicious manipulations during operation and storage should be avoided or at least detected including its notification and correction.

Authenticity: two aspects of authenticity play an important role in a biometric system, namely entity authenticity and data origin authenticity:

- *Entity authenticity* ensures that all entities involved in the overall processing are the ones they claim to be. For example, humans need to be correctly identified as originator or system entities such as sensors or processes need to be identified as sender or receiver. Here for example the following threat occurs: an attacker can try to gain unauthorized access, without possessing copies of biometric reference data. Obviously, the security risk in this case is entity authenticity of legitimate users of a biometric system. This category has apparently attracted most scientific and non-scientific work recently, with numerous publications addressing techniques to attack biometric authentication systems without any or with little knowledge about the original biometric trait of the subject under attack. Recent works in this domain include, for example, reverse engineering and hill-climbing attacks to handwriting modality attacks, see for example [13] and [22].
- *Data origin authenticity* ensures the origin, genuineness, originality, truth, and realness of data. For example, for biometric data captured with sensor devices, data origin authenticity ensures that the captured data comes from a genuine sensor and is not spoofed from a previous recording.

Non-repudiation involves an identification of involved parties such as entities and used components, and binds all actions to these parties. It either proves that the involved parties performed a certain action or that an event occurred. Furthermore, this fact can be proven to third parties. For example an event or action can be the biometric identification or verification of humans including the used system entities and components, the capturing and sampling of biometric traits, the creation or generation and sending of a derived message, the receipt of this message and the submission or transport of this message. Non-repudiation also can refer to so-called accountability ensuring that, for example, a sender of biometric information and recipients of this information cannot successfully deny having sent or received biometric information. With respect to third parties, legal enforceability can be achieved, ensuring that a user can be held liable to fulfill his or her legal responsibilities.

Availability: a resource has the property of availability with respect to a set of entities if all members of the set can access the resource. A further aspect is the so-called reachability to ensure that an entity such as a human or a system process either can or cannot be contacted, depending on user interests. Attackers might be interested to set the system in an inoperable state for rightful users, thus preventing them from using authenticated applications and services. Such attacks clearly target the availability and represent a Denial-of-Service (DoS) attack variant to biometric systems, in analogy to DoS attacks to other IT systems such as Web applications.

Due to the private nature of biometrics, besides the classical five security aspects from common IT security definitions discussed before, additional *privacy* requirements become important especially if the biometric data is associated to a certain situation, place, belief, action, and so on. Privacy summarizes the ability of a human to determine and control her- or himself which personal information is revealed during data collection, usage, storage, modification, transfer, and deletion. The classification into personal relevant information depends often on society, culture and individual preferences and is subject to change. Therefore subjects have the right to request corrections, locking or deletion. Sometimes privacy is related to confidentiality and anonymity to describe that the information is personally sensitive and should not be attributed to a specific person. However, privacy itself is much broader than confidentiality and anonymity and covers all security aspects mentioned including the concepts of appropriate usage with transparent rules for each individual, minimal principle, and appropriation as well as protection and deletion strategies.

With respect to user privacy, confidentiality, and entity authenticity of the user (human) during his or her actions, further security requirements (such as anonymity, unobservability, unlinkability, and pseudonymity) can be defined, see also the terminology in [17] and [29]: Here we understand anonymity as the state of being not identifiable and therefore indistinguishable within a set of subjects, the so-called anonymity set. It can also be seen as unknown authorship or origin, lacking individuality, distinction, or recognizability within the anonymity set by reducing the likelihood to be identified as originator. The definition can, of course, be also applied to the recipients and the overall communication. Anonymity does not mean that a person cannot be identified, rather that he is indistinguishable within some particular group. In the literature [31], so-called degrees of anonymity are defined such as *provably exposed*, *exposed*, *possible innocence*, *probable innocence*, *beyond suspicion*, and *absolute privacy*. Applied to biometric systems these different degrees can be used to describe and provide anonymity properties to the users involved and further to select appropriate security mechanisms.

Unobservability covers the infeasibility of observation of a resource and service usage by humans or entities (parties). Parties not involved should not be able to observe the participation, such as the act of sending or receiving of messages (state of being indistinguishable). From the summary of [29] and [30], unobservability covers undetectability against all subjects uninvolved and anonymity even against the other subject(s) involved.

Unlinkability addresses the relation between two or more humans and entities (e.g., subjects, messages, events, actions). In an unlinkable biometric system it should not be possible to derive any further information on the relation between two entities than is available through a-priori knowledge, see further discussions in [29].

Pseudonyms (also called Nyms in its shortened form) are identifiers that cannot with confidence be associated with any particular human or entity. This is achieved by a mapping between real identities and fictitious identities. Re-identification is only possible by knowing the mapping function. More details about pseudonymity with respect to accountability and authorization can be found in [29].

In the following we sketch which of the five security aspects and the discussed privacy issues are particularly important in the biometric processing pipeline. Here

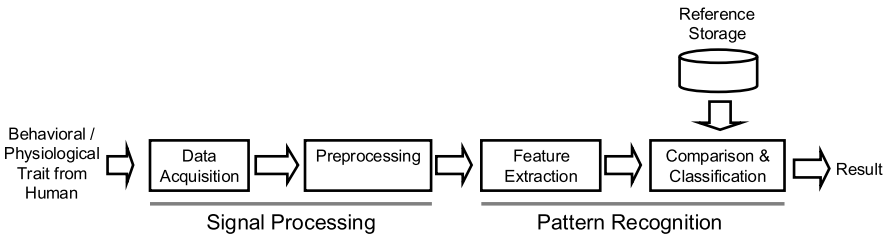

Fig. 2.1 Biometric authentication pipeline as a signal processing and pattern recognition model [37]

we consider the biometric systems as a generalized chain of signal processing and pattern recognition primitives, as suggested by [37]. This idea is motivated by the fact that the origin of any biometric recognition process is the collection of physical phenomena by means of a sensor (*data acquisition*), resulting in some form of electronic measurement. This initial process is followed by analog-digital (A/D) conversion and subsequent digital signal processing steps for conditioning (*preprocessing*) of the raw data. From the pre-processed data, characteristics are determined by *feature extraction* and finally, the authentication is performed by *comparison* of the extracted features to stored *references* through some *classification* method. Figure 2.1 from [37] illustrates this model for biometric authentication.

The following figures briefly illustrate, based this the model-oriented view, the impact of the above mentioned security and privacy aspects on the biometric processing pipeline.

As seen in Fig. 2.2, in each step itself and in the communication between the steps of the biometric pipeline, authenticity of all entities such as the subject and all processing parties including all running processes, data authenticity and data integrity needs to be ensured. Furthermore for the reference storage, it needs to be ensured that the reference storage in its hardware and software itself and all related application processes are authentic and integer (e.g. not spoofed or manipulated entities) as well as the stored data has authenticity and integrity (e.g. is not spoofed or manipulated). Two examples should illustrate the protection goals:

(a) During acquisition it needs to be ensured that the data comes from a human and is captured by a sensor with genuine hardware and software (otherwise a replay of recorded human traits cannot be prevented).
(b) Furthermore after data acquisition, all subsequent processing steps need to be checked for entity authenticity, data authenticity and integrity to avoid that e.g. malicious software is injected and can manipulate the overall processing steps.

The security aspect of confidentiality (see Fig. 2.3) plays an important role when data is acquired and further processed; it needs to be ensured in each step of the processing pipeline, for the communication of all processes (inter-process communication) and in the reference storage. As person related data is usually involved, privacy requirements such as anonymity or pseudonymity, unobservability, and unlinkability become important (see also Fig. 2.3). Privacy is hereby a mandatory aspect derived

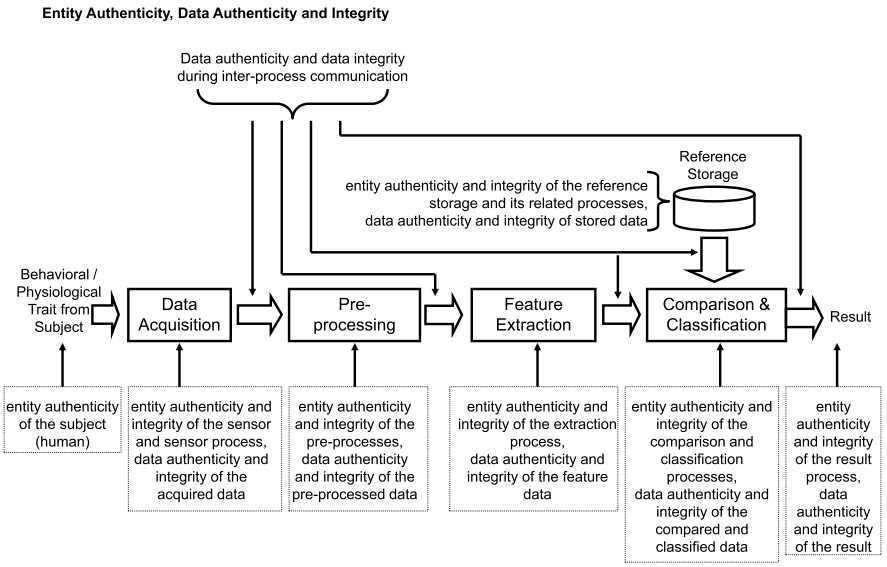

Fig. 2.2 Entity authenticity, data authenticity and integrity for the biometric authentication pipeline

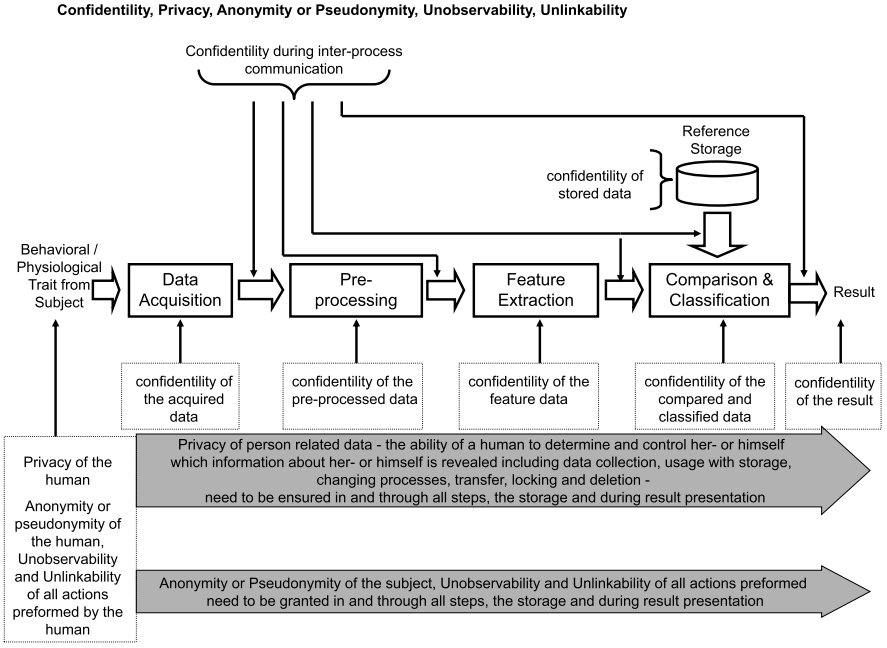

Fig. 2.3 Confidentility, privacy, anonymity or pseudonymity, unobservability, unlinkability for the biometric authentication pipeline

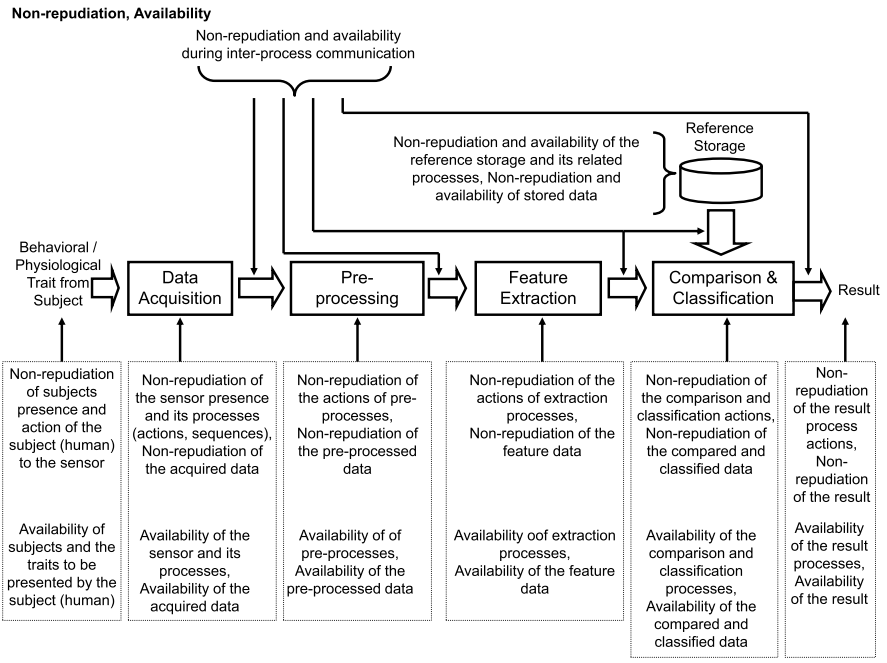

Fig. 2.4 Non-repudiation and availability for the biometric authentication pipeline

from related privacy laws of the. For an anonymous, unobserved or unlikable communication, specific protocols needs to be used in all actions performed in each step and between steps of the pipeline.

If biometric systems are used to ensure a certain provable service or action, then usually non-repudiation plays an important role and needs to be ensured from the subject of investigation (non-repudiation of the subject presence and actions itself) through and between all steps (with non-repudiations of sensor presence and all related processes, as well as of all actions and processes of and between preprocessing, feature extraction, comparison and classification, storage) in the biometric pipeline including the reference storage (see Fig. 2.4). Availability aspects include the availability of the subjects and the required traits, the corresponding sensor technology, and the availability of all processes and building blocks of the biometric pipeline, including the storage of references (see also Fig. 2.4).

2.2 Summary of General Design Principles and Approaches

In this section we start with a brief summary of terminology and a definition of risk as well as basic design principles known for example from discussions in [2] for a biometric system derived from overall IT security principles. We further briefly introduce exemplary organizational and technical security measures and mechanisms.

Furthermore selected measures and mechanisms specifically tailored towards biometric measurements are summarized.

Regarding terminology, security aspects (requirements) are met by security measures, and security measures consist of several security mechanisms and security services (sometimes also called methods of defense). The goal is to prevent, detect or recover from a malicious incident that violates security. From [2], prevention involves that the implemented mechanisms cannot be overridden by users and can be trusted to be implemented in correct and unalterable ways. In particular, detection tries to determine that a malicious incident is under way (or has occurred) and provides mechanisms to report it. Recovery resumes correct operation either after a malicious incident or even while a malicious incident is under way.

From an abstract point of view, the risk of a malicious incident depends mainly on the expected loss (vulnerabilities) and the probability of occurrence of the incidents. For a biometric system it is therefore important to reduce the number of vulnerabilities and potential threats by performing an adequate risk management. To avoid inherent vulnerabilities, biometric systems should be designed based on the common rules of simplicity (make design and interactions easy so that its security can be evaluated) and restrictions (minimize the power of entities, "Need To Know" principle and compartmentalization). Further design principles can be found in [3] and [33] such as the principle of least privilege, principle of fail-safe (secure) defaults, principle of economy of mechanism, principle of complete mediation, principle of open design, principle of separation of privilege, principle of least common mechanism, and principle of psychological acceptability.

We distinguish between organizational and technical measures and mechanisms. For a biometric system, organizational aspects should be defined a priori in terms of security policies, i.e., statements of what is, and is not, allowed. Policies can be expressed mathematically or in natural language as a list of allowed and non-allowed actions, also including the required non-technical or technical security mechanisms of enforcing the described security policy. If several policies exist, the policies need to be combined by composition. Attention needs to be paid to policy conflicts, as discrepancies may create subtle security vulnerabilities. Therefore policy composition requires checking and resolving for inconsistencies among policies.

In the following we give examples of technical security measures [7], which can be divided further in active and passive approaches, transforming the overall security target with or without changes. For example, general methods for data authentication to ensure data origin authenticity and/or data integrity can be applied a priori by actively introducing authenticity or integrity labels, e.g. by watermarking. This label changes the original target and allows tracing and verifying either or both security properties integrity or authenticity. Different design strategies such as robust and fragile watermark patterns are know today to describe the level of authenticity or integrity of multimedia data, which can be potentially applied to biometric data as well. These concepts are based on the assumption that (at least) two parties are involved in the authentication process: at the origin, an entity who performs the transformation of the data and communicates it to a set of receivers. At the recipient side, (at least) one verifier inspects the received data and checks its authenticity and/or integrity.

For example, by embedding a label, known to the verifier and a secret symmetric key, mutually shared between the origin entity and the verifier, data origin authenticity verification can be achieved in the following way:

- The origin entity embeds a label in a key-dependent manner using some watermarking algorithm and the shared key into the biometric data and subsequently communicates it,
- The verifier receives the biometric data and attempts to retrieve the known label using the shared key. If retrieved successfully, the verifier can assume origin authenticity; if not, authenticity is not ensured.

Additional aspects for the application of watermarking to biometric data are robustness, i.e. the possibility to perform authentication even after transformations such as image processing (e.g. cropping/scaling/compression), and/or integrity verification by so-called fragile watermarks. The latter kind of watermarks is designed in such way that even minor modifications of the cover media lead to dissolving of the embedded label, indicating any kind of modification to the verifier. For further details on the concept of using watermarking for authentication and integrity verification, see for example [7] or [6].

In comparison to active changes of the target, *passive cryptography* transforms the target without changing the target at the recipient side itself (encryption functions ensure confidentiality) or transforms and compresses the target from arbitrary length to a fixed length as one way function (hashing). *Cryptography* can be used to ensure the security aspects summarized in Fig. 2.2 for integrity and authenticity and Fig. 2.3 for confidentiality in this chapter. As commonly known, see for example in [2], encryption is in general the process of transforming data to conceal content without concealing the existence of data, i.e. the transformed data is visible but cannot be understood. It is implemented by use of cryptosystems consisting of a set of (keyed) invertible functions. Private-key cryptosystems use shared secret keys, whereas public-key cryptosystems make use of pairs of a public and private key, where the public key is used for encryption and the secret key for decryption. An authentic link between the public key and its owner with the corresponding secret key is needed to achieve the overall security goals. Such a link is provided by so-called public-key certificates issued by a so-called Trust Center (TC), as summarized for example in [7]. Thereby trust centers authenticate the link of users (also our users of the biometric system) to their public keys by means of certificates and provide further services like non-repudiation (such as summarized in Fig. 2.4 in this chapter), revocation handling, timestamping, auditing, and directory service.

Besides ensuring confidentiality with symmetric or asymmetric encryption schemes, *cryptography* as *a priori passive protection* helps to ensure *integrity* by means of *cryptographic hash functions* (as verifiable code). As stated before, hash functions are functions that transform input data of arbitrary length into output data of fixed length, preserving the following properties as commonly known, see also for example in [2]:

- Reproducibility: for any two identical input data, the hash functions outputs identical values.

- Collision Resistance: for any two different input data, it is very unlikely for the function to produce identical values.
- Irreversibility: it is computationally very hard to reproduce original input to any given output.
- Bit-Sensitivity: Minor changes in input data (e.g. single bit flipping) cause severe changes in the output.

Given these properties, hash functions provide building blocks for preservation of integrity in systems, by attaching reference hash value to targets as known and widely applied, see also in [2]. Any malicious or non-malicious change during processing or communication can then be detected by re-calculating the hash values at the end of the process pipeline and comparing it to the reference values. Further, hash functions can be applied to achieve authenticity by introducing the knowledge of keys and binding of hash function to keys (then called Message Authentication Codes, MAC) or symmetric ciphers with symmetric keys or asymmetric ciphers as digital signatures with private and corresponding public keys.

Finally, as widely known, cryptographic hash functions can be useful to preserve confidentiality of reference data in authentication applications. Password-based authentication, for example, requires the comparison of a reference password with an actual one during every login. For security reasons, it is unwise to store such reference passwords in clear text (as a potential intruder could get hold of all passwords of all users). To overcome this problem, passwords (extended by other data) are generally transformed by hash functions prior to storage and comparison during login takes place in the transformed, hash domain.

In summary, cryptographic methods can be used for the following purposes in system design:

- Data Confidentiality: symmetric/asymmetric encryption
- Data Integrity and Reference Data Confidentiality: hash functions
- Data origin authenticity: symmetric key encryption
- Data origin authenticity and Data integrity: MAC (hash functions using symmetric keys), Digital Signatures (hash functions plus asymmetric keys)

However, as we discuss further on in this chapter, there are specific requirements to biometric systems, which may limit the usefulness of cryptographic schemes. For example, cryptographic hash functions commonly cannot be used for reference data protection, due to the intra-class variability of biometric data (which obviously stands in conflict to the property of bit-sensitivity).

In the biometric domain, the need for specific methods and designs towards increased security of biometric systems has been recognized and addressed by several new concepts. Specific key problems here address all security aspects of biometric reference data, as discussed in this section. Generally, as can be seen from the variety of approaches found in the literature, the methods can be categorized in two classes: *Template Protection* methods focus on securing biometric reference data and often suggest transformations of biometric data in such way that it is made unusable in case of theft by potential intruders. This includes aspects such as non-reversibility, cancelation, and renewal of template information. *Crypto-Biometrics* aspires to inte-

grate biometric data and cryptographic functions, for example by derivation of cryptographic keys from biometrics. In the following, we briefly outline some concepts; in the subsequent section, we focus on one additional concept (Biometrics in the encrypted domain) in more detail and give a description based on a practical example.

Template Protection by Transformation: the goal here is to maintain confidentiality of biometric references (templates), by applying techniques to avoid the necessity of keeping original biometric in the Reference Storage (see Fig. 2.1). Rather than original biometric data, only selected features from the reference samples are stored during enrollment. These features need to be selected in such way that reconstruction of original data from them is next to impossible. For example, a signature verification system could store significant statistical properties of reference signatures, such as writing duration and velocity, number of pen lifts, aspect ratio etc. during enrollment. Provided that these features possess sufficient discriminatory power, it will be sufficient, for a later verification, to calculate the same features from every newly acquired sample and compare them to the stored values. However, it will be hard for an attacker to reconstruct the original data given the template. Generally speaking, this protection scheme is based on *non-reversible transformations* of biometric raw data during enrollment and authentication. Selected early examples for such transformations are Biometric key generation from speech [25], Biometric Hashes for handwriting [38] and [37], Fuzzy Commitments [18] and Secure Sketches [8] and [34]; meanwhile numerous additional approaches for literally all biometric modalities have been suggested. A review of additional related concepts from the literature is provided in [19].

Note that typically, these concepts are purely transformations by means of transform function and optionally some additional public information (for example denoted as helper data). They do not consider any dependency on additional credentials such as keys or other secrets. Typically, these protection schemes assume that transformation takes place within a protected process of the biometrics processing chain (e.g. as part of feature extraction) prior to reference storage or comparison, but also concepts for on-device transformations have been suggested [23]. The analysis of the non-reversibility property of the transformation function, i.e. attempts of generating sets artificial biometric raw data raw from transformed templates, leading to close matches these templates, is a relatively recent area of interest related to Transformation techniques, see for example [14, 22] and [26].

Cancelable Biometrics: the goal of cancelable biometrics is to provide means to make biometric references unusable, even after data theft occurred. Cancelation can be performed either alone by the owner or system operator, respectively, or as a joint operation. Most concepts suggested for Cancelable Biometrics are based on the principle to link fuzzy biometric data, sometimes along with some public helper data, to secret information, in order to from some authentication information. Only if both secret knowledge and biometric information are present, the biometric matching can be performed. For cancelation, principals need to withdraw, i.e. “forget” their secret knowledge parts. Such concepts are also often referred to as *Revocable Biometrics*,

for the case when cancelation is initiated solely by the users. Examples of methods from the variety include Fuzzy Extractors [8], anonymous, and cancelable fingerprint biometrics [4] and application of BioHash for cancelable biometrics [35].

Renewable Biometrics: there are two main reasons for the necessity of Renewable Biometrics: Firstly, since biometric properties are subject to biological and mechanical changes (e.g. aging, injuries), the accuracy of biometric authentication may decrease over time. Particularly for behavioral biometrics such as speech or handwriting, it is quite obvious that aging impacts the way people speak or write. Similar observations can be made for physiological traits such as face. From the perspective of biometric systems, this observation leads to the tendency of potential increase of false non-matches, i.e. legitimate users of biometric systems are more frequently rejected. This effect is commonly referred and has been addressed in research, see for example [5] and [12]. Secondly, compromised or stolen Biometric data are problems for biometric systems. Once any original biometric raw data has been compromised, it may be potentially used for replay attacks. For example, it has been shown that gummy fingerprints can be produced from digital fingerprint images and used gain illegitimate authentication by fingerprint systems [24].

For both reasons, it may be desirable to renew biometric reference data: one goal is to maintain the recognition performance for individual subjects over time of operation of biometric systems, by frequently updating reference data. The second aim is to be able to replace compromised biometric data in such ways that after renewal any attacker in possession of stolen biometric references is unable to achieve illegitimate access, while the owner of the stolen data (victim) can still be authenticated. In this sense, Renewable Biometrics can be seen as a derivative of Cancelable Biometrics with an additional requirement for re-enrollment. In order to renew biometric references for any given user, the biometric system will cancel the previous reference and, in a second step, acquire a new biometric reference from the user. This concept obviously implies that the newly acquired sample needs to be considerably different from the previously canceled one in such way that the compromised data cannot be misused for false authentication. This can be achieved for example by using a different finger in physiological biometrics, different writing or speech content in behavioral systems or by simply involving a new secret in systems that combine secret knowledge and biometric information. Consequently, potentially all concepts for cancelable biometrics, which are based on withdrawal of secret information, appear particularly appropriate for renewable biometrics.

Encrypted Biometrics: in this scenario, protection of biometric data is ensured by encryption of sensitive data using cryptographic encryption and decryption functions and keys. Access to biometric information thus is only possible for entities in possession of the appropriate key. In general, protection can be applied straightforward to biometric systems, e.g. by cryptographically protecting all communication channels and storage components of the biometric pipeline, as suggested earlier in this chapter. However, usually any data processing (such as feature extraction or comparison) is performed in clear text domain, requiring decryption of data at run time; an alternative solution is described in the next section.

Table 2.1 Summary of main security concepts and their properties towards security of biometric systems with respect to reference data

Security concept	Key properties
Template protection by transformation	Non-reversible transformations on original data
	Optionally additional public helper data for the transforms
	Maintaining some similarity or identity property in the transformed domain
	Authentication by comparison in transformed domain, without necessity of processing sensitive biometric raw data
Cancelable biometrics	Means to make biometric references unusable after data theft
	Cancelation alone by the owner, system operator or jointly
	Mostly based on link fuzzy biometric data in combination with secret information
	Special case: *Revocable* Biometrics, when cancelation process is initiated solely by users
Renewable biometrics	See Cancelable Biometrics
	In addition: replacement of compromised biometric data, i.e. attacker is unable to achieve access, while owner can still be authenticated after replacement
Encrypted biometrics	Use of using cryptographic encryption and decryption for protection of biometric data
	Biometric data/signal processing requires prior decryption
Biometric key management	Controlled access to a key management system by means of biometrics
	User-related keys are released upon successful biometric authentication from trusted systems
	No intrinsic binding between keys and biometrics

Biometric Key Management: methods in the domain of biometric key management are based on controlled access to a key management system by means of biometric user authentication, as discussed for example in [36]. User-related keys are stored in protected and trusted system environments and keys are only released after successful biometric authentication. This concept can be categorized as Crypto-Biometrics, although in a narrow sense, it is not related to the security of biometric systems themselves, as no intrinsic binding between the keys and biometric data exists.

To summarize common security principles specific for biometrics, Table 2.1 provides an selected overview of the security concepts discussed in this section, along with their key properties. In summary, it can be stated that cryptographic methods are important building blocks to secure biometric systems and should be implemented throughout the biometric processing pipeline. However, the methods discussed above come to a limit whenever the processing of biometric data requires availability of the original biometric data in the clear. To overcome this problem, biometric matching "in the encrypted domain" can be applied.

2.3 Biometrics in the Encrypted Domain

All approaches that match a newly measured biometry against a protected template are only able to provide security of templates while they are stored in a database or on a server, and make the assumption that the matching process itself is performed in a secure environment (such as on a trusted server or directly on a smart card). This is important since the device that performs the matching operation has access to the newly collected biometrics in the clear. In some applications this assumption is questionable. Consider, for example, an authentication scenario, where a biometric measurement is obtained by a client device, which submits the measurement (or a template derived thereof) to an authentication server that performs matching against a large set of templates in a database. In case the server is compromised (for example through malware), it can collect biometric templates of all clients who request an authentication. In order to avoid this leak, biometric verification can be performed in such a way that a protected template is matched against an encrypted biometric measurement—we speak of matching in the encrypted domain.

The overall design of a system that performs matching in the encrypted domain consists of a client and a server; the client has access to a new biometric measurement, and the server wants to match this measurement against a set of templates. Depending on the application scenario, these templates can either be stored in the clear or in protected/encrypted form. The former case is, for instance, applicable to surveillance scenarios, where a large number of people are matched against a small list of known suspects, and where the privacy of all checked people should be protected. The latter case is relevant for authentication scenarios, where biometric templates stored at the server need to be protected against misuse, such as identity theft or cross-matching. We can also distinguish between scenarios where the matching result is available to the server or the client. The former is relevant in authentication scenarios, whereas the latter can be of interest in applications that use biometric services on a large scale and where cross-matching between individual service requests should be prohibited (such as a service that matches surveillance images against a small set of "suspects").

In both cases techniques of *signal processing in the encrypted domain* [9] can be applied, which provides methods to manipulate signals that are encrypted through semantically secure homomorphic encryption schemes. Using this specific class of encryption schemes, algebraic operations can be performed on ciphertexts without decryption: more precisely, for additively homomorphic encryption schemes, an encryption $[x + y]$ of a sum can be computed from encryptions $[x]$ and $[y]$ of the individual terms (we use square brackets to denote encryptions), without knowledge of the secret cryptographic key in use and without learning the result or the two factors in the clear. Since multiplication with a constant can be seen as a repeated addition, an encryption $[x]$ can also be multiplied by a constant a available in the clear to obtain an encryption of $[ax]$, again without learning the value of x. Thus, linear operations can directly be performed on ciphertexts without decryption. More complex operations (such as multiplications of two encrypted values or equality tests) can be implemented by adopting concepts from secure-two-party computation, which provides interactive protocols between a party that performs the computations and a

party that has access to the secret key. Still, the protocols are designed in such a way that both parties do not gain information on the data they operate on; details on the utilized protocols can be found in [9].

Note again that most protocols used to compute with encrypted values require interaction. Due to the employed homomorphic encryption scheme, the communication overhead can be substantial: if instantiated with the common Paillier encryption scheme, every ciphertext will require 2048 bits or more to obtain security comparable to state-of-the-art RSA. Thus, there may be a significant communication overhead compared to a biometric matching process implementation in the plain; this is particularly pronounced in case a biometric signal (such as an image or a time series of measurements) needs to be encrypted sample by sample: each encrypted sample may then take thousands of bits instead of just a few. This drawback can be mitigated by "packing" several samples into one encryption [1].

We illustrate the concept of matching biometrics in the encrypted domain by the example of a face recognition service [10]. Suppose that a client (Alice) and a server (Bob) jointly want to execute a standard biometric face recognition algorithm in a privacy-friendly manner. In this scenario, Alice owns a face image, while Bob owns a database containing a collection of face images (or corresponding feature vectors) from individuals. Both parties are interested in running a face recognition algorithm in order to determine whether the picture owned by Alice shows a person whose biometric data is in Bob's database. While it is acceptable that Alice learns the basic setup of the face recognition algorithm (i.e., the algorithm employed as well as some parameters of the matching process), the content of Bob's database is considered private data that he is not willing to reveal. Alice trusts Bob to execute the face recognition algorithm correctly, but is neither willing to share the image nor the detection result with Bob. This ensures that Bob, who does the biometric matching, cannot relate subsequent matching results, as he cannot see which person was identified on the image. After termination of the protocol, Alice will only learn if a match occurred or, alternatively, the identity of the matched person. The full protocol can be found in [9]. Subsequent research considered optimizations of both cryptographic protocols in use in "private face recognition" as well as the basic face recognition algorithm [28, 32].

As example, we provide some details on [9], which considered private face recognition based on the Eigenface recognition algorithm, where face images are represented as vectors in a subspace, which is determined by Principal Component Analysis of training images. Before the protocol starts, Alice generates a public/private key pair of a homomorphic encryption algorithm (such as Paillier); the public key is distributed between both parties, while the private key is kept secret by Alice. Alice furthermore possesses an input image as private data, which shows a face that she wants to identify with help of Bob. On the other hand, Bob knows all data computed during the enrollment process: the basis vectors of the face space and biometric templates of all enrolled people (images projected onto the face space).

When describing the protocol we make the design decision of not publishing the face space basis vectors. This is due to the fact that these vectors inevitably leak some information on the training or enrollment images used to derive them. Since it

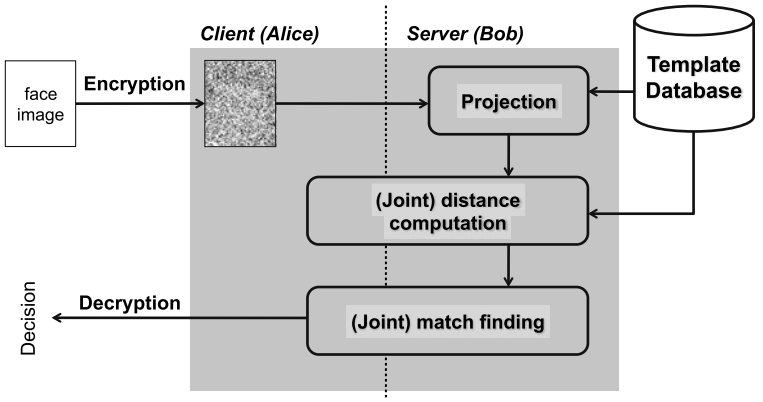

Fig. 2.5 Schematic description of face recognition in the encrypted domain

is difficult to quantify this potential information leak, we consider the basis vectors private to the server; this ensures that *no* information on the training data is leaked to the client. If the basis vectors are computed from a public source of face images (and are independent of enrollment data), the protocol can be simplified by publishing the basis vectors, see below.

In order to jointly run the algorithm, all steps of the face recognition system must be performed securely "under encryption" (see Fig. 2.5):

- *Projection*: In a first step, the input image is encrypted pixel-by-pixel by Alice and sent over to Bob, who has to project the image onto the face space. Since Bob has access to the basis vectors of the face space in the clear, and projection is a linear operation, he can directly compute (by use of the homomorphic properties of the encryption scheme) an encryption of the biometric template of the face to be recognized.

  If we assume that the basis vectors of the face space are independent of the enrollment data, we can drastically simplify this step: Alice herself can project the face image onto the publicly available basis vectors, encrypt the result and send it to Bob. This saves both computation (since each operation on encrypted values corresponds to an operation in a finite ring) and communication (transmitting the encrypted face image pixel-by-pixel is rather costly compared to the transmission of the encrypted template).
- *Distance computation*: Subsequently, Alice and Bob jointly compute encrypted distances between the encrypted face template obtained in the first step and all templates stored in the database by Bob. Since computing the (squared) Euclidean distance between two vectors is not a linear operation, this step requires interaction between Alice and Bob. In particular, one requires to compute the square of an encrypted number, which cannot be done by homomorphic encryption alone. For this purpose, they can run a small two-party protocol.
- *Match finding*: After the second step is finished, Bob has access to encryptions containing distances between the newly obtained biometrics and all templates of

the database. As a third step, both parties have to pick the encryption that contains the smallest distance, and compare this against the threshold. If the smallest encrypted distance is smaller than the threshold, a match is achieved.

Technically, this step can be performed by repeatedly running cryptographic protocols for solving Yao's millionaire's problem (see Sect. 5 of [9]), which allows picking the minimum of two encrypted values. Given the set of encrypted distances, the protocol is run iteratively: during each iteration two distances are compared and the smaller distance is retained (in a way that the server does not "see" which encryption is kept, this can be realized by re-randomizing the encryption). This process is iterated until only one distance is left. Finally, this distance is (again using the protocol to solve Yao's Millionaire problem) compared to the threshold, and the encrypted binary answer is sent to the client, who can decrypt and interpret the result.

This way, the client learns the result of the matching process, while the server is completely oblivious about the computations: he does not obtain the input values, the output values or intermediate values during computation. The price to pay is a higher computation and communication effort.

The solution sketched above works in a scenario where the server (Bob) has access to all templates in the clear. However, in situations where the actual templates should be hidden from the server, signal processing in the encrypted domain can be applied as well. To this end, template protection can be combined with encrypted processing in a way that the server matches an encrypted newly measured biometric against a set of encrypted templates in an interactive fashion. Details of the construction can be found in [11].

2.4 Conclusions

In this chapter we discussed the basic security requirements of biometric identification. We showed that security considerations must be an integral part of the entire biometric processing pipeline, starting from the acquisition of the biometric through a sensor down to the comparison with stored templates. Furthermore we showed that biometric matching "under encryption" is possible so that the party that does the computation does not learn the biometrics or the matching result. This enables implementation of biometric technologies even on hostile or untrusted devices.

References

1. Bianchi T, Piva A, Barni M (2010) Composite signal representation for fast and storage-efficient processing of encrypted signals. IEEE Transactions on Information Forensics and Security 5(1):180–187
2. Bishop M (2002) Computer Security: Art and Science. Addison–Wesley, Reading
3. Bishop M (2005) Introduction to Computer Security. Addison–Wesley, Reading

4. Bringer J, Chabanne H, Kindarji B (2009) Anonymous identification with cancelable biometrics. In: Proceedings of the 6th International Symposium on Image and Signal Processing and Analysis, Salzburg, Austria, pp 494–499
5. Carls JW (2011) A Framework for Analyzing Biometric Template Aging and Renewal Prediction. ProQuest, UMI Dissertation Publishing, Cambridge
6. Cox I, Miller M, Bloom J, Fridrich J, Kalker T (2008) Digital Watermarking and Steganography, 2nd edn. Morgan Kaufmann, San Mateo
7. Dittmann J, Wohlmacher P, Nahrstedt K (2001) Multimedia and security—using cryptographic and watermarking algorithms. IEEE Multimedia 8(4):54–65
8. Dodis Y, Reyzin L, Smith A (2004) Fuzzy extractors: how to generate strong keys from biometrics and other noisy data. In: Cachin C, Camenisch J (eds) Advances in Cryptology—Eurocrypt 2004. Lecture Notes in Computer Science, vol 3027. Springer, Berlin, pp 523–540
9. Erkin Z, Piva A, Katzenbeisser S, Lagendijk R, Shokrollahi J, Neven G (2007) Protection and retrieval of encrypted multimedia content: when cryptography meets signal processing. EURASIP Journal on Information Security
10. Erkin Z, Franz M, Guajardo J, Katzenbeisser S, Lagendijk I, Toft T (2009) Privacy-preserving face recognition. In: Privacy Enhancing Technologies Symposium (PET 2009). Lecture Notes in Computer Science, vol 5672, pp 235–253. Springer, Berlin
11. Failla P, Sutcu Y, Barni M (2010) ESketch: a privacy-preserving fuzzy commitment scheme for authentication using encrypted biometrics In: ACM Workshop on Multimedia Security, MMSect 2010. ACM, New York
12. Fenker SP, Bowyer KW (2012) Analysis of template aging in iris biometrics. In: Proceedings of IEEE Computer Vision and Pattern Recognition Workshops (CVPRW), pp 45–51
13. Galbally J, Fiérrez-Aguilar J, Ortega-Garcia J (2007) Bayesian hill-climbing attack and its application to signature verification. ICB 386–395.
14. Galbally J, Cappelli R, Lumini A, Maltoni D, Fierrez J (2008) Fake fingertip generation from a minutiae template. In: Proc Intl Conf on Pattern Recognition, ICPR, Tampa, USA
15. Gupta UK, Prakash S (2003) Dermatoglyphics: a study of finger tip patterns in bronchial asthma and its genetic disposition. Kathmandu University Medical Journal 1(4):267–271
16. Information Technology Security Evaluation Criteria (ITSEC): provisional harmonised criteria. V 1.2, Jun 1991
17. ISO99 ISO/IEC IS 15408 (1999). http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=50341. Website request 24.5.2013
18. Juels A, Wattenberg M (1999) A fuzzy commitment scheme. In: Proceedings of the 6th ACM Conference on Computer and Communications Security, CCS'99. ACM, New York, pp 28–36
19. Kanade SG, Petrovska-Delacrétaz D, Dorizzi B (2012) Enhancing Information Security and Privacy by Combining Biometrics with Cryptography. Morgan & Claypool Publishers, San Rafael
20. Kiltz S, Lang A, Dittmann J (2007) Taxonomy for computer security incidents. In: Janczewski LJ, Colarik AM (eds) Cyber Warfare and Cyber Terrorism. Information Science Reference (IGI Global), Hershey. ISBN 978-1-59140-991-5
21. Kiltz S, Hildebrandt M, Dittmann J, Vielhauer C, Kraetzer C (2011) Printed fingerprints: a framework and first results towards detection of artificially printed latent fingerprints for forensics. In: Proc of SPIE: Image Quality and System Performance VIII, San Francisco, USA. doi:10.1117/12.872329
22. Kümmel K, Vielhauer C (2010) Reverse-engineering methods on a biometric hash algorithm for dynamic handwriting. In: Proceedings of the 12th ACM Workshop on Multimedia and Security. ACM, New York, pp 62–72
23. Kümmel K, Vielhauer C (2011) Biometric Hash algorithm for dynamic handwriting embedded on a Java card. In: Biometrics and ID Managements. Lecture Notes in Computer Science, vol 6583. Springer, Heidelberg, pp 61–72
24. Matsumoto T, Matsumoto H, Yamada K, Hoshino S (2002) Impact of artificial "Gummy" fingers on fingerprint systems. In: Proceedings of SPIE Conference on Optical Security and Counterfeit Deterrence Techniques IV, vol 4677

25. Monrose F, Reiter MK, Li Q, Wetzel S (2001) Using voice to generate cryptographic keys. In: Proceedings of Odyssey 2001. Proceedings of the Speaker Verification Workshop
26. Nagar A, Nandakumar K, Jain AK (2010) Biometric template transformation: a security analysis. In: Proceedigns of SPIE Conference on Media Forensics and Security II, vol 7541. doi:10.1117/12.839976
27. Oermann A, Dittmann J (2006) Trust in e-technologies. In: Khosrow-Pour M (ed) Encyclopedia of E-Commerce, E-Government and Mobile Commerce, vol 2. Idea Group Reference, Hershey, pp 1101–1108
28. Osadchy M, Pinkas B, Jarrous A, Moskovich B (2010) SCiFI—a system for secure face identification. In: IEEE Symposium on Security and Privacy 2010. IEEE Press, New York, pp 239–254
29. Pfitzmann A, Hansen M A terminology for talking about privacy by data minimization: anonymity, unlinkability, undetectability, unobservability, pseudonymity, and identity management. (Version v0.34, 10 Aug 2010). http://dud.inf.tu-dresden.de/literatur/Anon_Terminology_v0.34.pdf. Web request from 15th February 2011
30. Pfitzmann A, Waidner M (1986) Networks without user observability—design options. In: Pichler F (ed) Advances in Cryptology—EUROCRYPT'85. Lecture Notes in Computer Science, vol 219, pp 245–253
31. Reiter MK, Rubin AD (1998) Crowds: anonymity for web transactions. ACM Transactions on Information and System Security 1(1):66–92
32. Sadeghi A, Schneider T, Wehrenberg I (2009) Efficient privacy-preserving face recognition. In: Information, Security and Cryptology—ICISC 2009. Lecture Notes in Computer Science, vol 5984. Springer, Berlin, pp 229–244
33. Saltzer JH, Schroeder MD (1975) The protection of information in computer systems. Proceedings of the IEEE 63(9):1278–1308
34. Sutcu Y, Li Q, Memon N (2007) Protecting biometric templates with sketch: theory and practice. IEEE Transactions on Information Forensics and Security 2(3):503–512
35. Teoh A, Kuan Y, Lee S (2007) Cancelable biometrics and annotations on BioHash. Pattern Recognition 41(6):2034–2044
36. Uludag U, Pankanti S, Prabhakar S, Jain AK (2004) Biometric cryptosystems: issues and challenges. Proceedings of the IEEE 948–960
37. Vielhauer C (2006) Biometric User Authentication for IT Security: From Fundamentals to Handwriting. Springer, New York
38. Vielhauer C, Steinmetz R, Mayerhöfer A (2002) Biometric Hash based on statistical features of online signatures. In: Proceedings of the IEEE International Conference on Pattern Recognition (ICPR), Quebec City, Canada, vol 1, pp 123–126

http://www.springer.com/978-1-4471-5229-3

Security and Privacy in Biometrics
Campisi, P. (Ed.)
2013, X, 438 p., Hardcover
ISBN: 978-1-4471-5229-3