Biometric Encryption: Technology for Strong Authentication, Security and Privacy

Ann Cavoukian, Alex Stoianov and Fred Carter

Office of the Information and Privacy Commissioner, Toronto, Ontario, Canada
{commissioner, Alex.Stoianov, Fred.Carter}@ipc.on.ca

Abstract. This paper looks at privacy-enhanced uses of biometrics, with a particular focus on the privacy and security advantages of Biometric Encryption (BE). It considers the merits of Biometric Encryption for verifying identity, protecting privacy, and ensuring security. In doing so, it argues that BE technologies can help to overcome the prevailing "zero-sum" mentality, which posits that adding privacy to identification and information systems will necessarily weaken security and functionality. It explains how and why BE technology promises a "win-win" scenario for all stakeholders.

1 Biometrics and Privacy

During the past decade we have witnessed a rapid evolution and maturation of biometric (and other) information technologies. Biometric technologies are now being deployed in a wide range of public and private sector uses and applications, including: physical and logical access controls, attendance recording, payment systems, crime and fraud prevention/detection, and border security controls.

Biometric technologies are now reaching an important threshold in terms of general awareness, acceptance and widespread use.

Biometric technologies promise many benefits, including stronger user authentication, greater user convenience, and improved security and operational efficiencies.

Biometric technologies are not, however, without their challenges and their risks. These include some important technological challenges (such as accuracy, reliability, data security, user acceptance, cost, and interoperability), as well as challenges associated with ensuring effective privacy protections.

Of particular concern when we talk about biometrics is the concept of informational privacy, referring generally to an individual's *personal* control over the collection, use and disclosure of recorded information about them, as well as to an organization's responsibility for data protection and the safeguarding of personally identifiable information (PII), in its custody or control.

A lack of informational privacy can have profound negative impacts on user confidence, trust, and the usage of a given information technology, specific application or deployment, or even an entire industry.

Please use the following format when citing this chapter:

Cavoukian, A., Stoianov, A. and Carter, F., 2008, in IFIP International Federation for Information Processing, Volume 261; *Policies and Research in Identity Management*; Eds. E. de Leeuw, Fischer-Hübner, S., Tseng, J., Borking, J.; (Boston: Springer), pp. 57–77.

The privacy concerns associated with biometric technologies and the collection, use, and retention of biometric data have been extensively documented[i], and include:

- unauthorized secondary uses of biometric data (function creep);
- expanded surveillance tracking, profiling, and potential discrimination;
- data misuse (data breach, identity fraud and theft);
- negative personal impacts of false matches, non-matches, system errors and failures;
- diminished oversight, accountability, and openness of biometric data systems;
- absence of individual knowledge and consent; loss of personal control.

Many responses to these privacy concerns and risks have been proposed, including strengthening legal and regulatory oversight mechanisms, developing and operationalizing clear data usage policies, and improving education and awareness efforts. The general intent of these approaches is to minimize identified risks to acceptable levels and to encourage user confidence.

Some critics have gone further to advocate more structural approaches to protecting privacy in biometric systems, for example, by limiting the design and operation of biometric technologies to authentication (1:1) only, rather than identification (1:n) purposes[ii].

International data protection commissioners, for example, have consistently argued against creating large, centralized databases of biometric data[iii]. They have also encouraged the development and use of privacy-enhancing technologies (PETs) that express internationally accepted fair information principles directly into the information system. PETs enable individuals to manage their own personally identifiable information (PII) and minimize privacy risks at an earlier, more granular level.[iv] They do this by:

- actively engaging the individual in managing and controlling their own PII (e.g., consent, accuracy, access, challenging compliance);
- minimizing the collection, use, disclosure and retention of PII by others (e.g., limiting purposes, collection, use, retention, etc.); and
- enhancing data security (e.g., safeguards).[v]

Some critics suggest that deploying PETs would hinder the objectives and functions of biometric-enabled information systems and applications. This is based on the common assumption, belief or argument that individual privacy must necessarily be sacrificed to broader societal, programmatic and operational needs, for example, accountability and security.

In our view, engineering privacy into (biometric) information systems is not only desirable and possible, but can also be accomplished in a manner that achieves positive-sum results for all stakeholders. Biometric Encryption (BE) technologies – the particular PETs that we will explore here in detail – are a good example of how privacy and security can both be increased in a positive-sum model.

BE is, in our view, worthy of consideration for a wide range of private and public sector uses, where user confidence and trust are critical success factors.

2 Security Vulnerabilities of a Biometric System

Biometric systems, especially those based on one-to-one authentication, are vulnerable to potential attacks.[vi] Vulnerabilities include:

- **Spoofing**. It has been demonstrated that a biometric system sometimes can be fooled by applying fake fingerprints, face or iris image, etc.
- **Replay attacks**, e.g. circumventing the sensor by injecting a recorded image in the system input, which is much easier than attacking the sensor.
- **Substitution attack**: The biometric template must be stored to allow user verification. If an attacker gets access to the storage, either locally or remotely, he can overwrite the legitimate user's template with his/her own – in essence, stealing their identity.
- **Tampering**: Feature sets on verification or in the templates can be modified in order to obtain a high verification score, no matter which image is presented to the system, or, alternatively, to bring the system down by making the score low for legitimate users.
- **Masquerade attack**. It was demonstrated[vii, viii] that a digital "artefact" image can be created from a fingerprint template, so that this artefact, if submitted to the system, will produce a match. The artefact may not even resemble the original image. This attack poses a real threat to the remote authentication systems (e.g. via the Web), since an attacker does not even have to bother to acquire a genuine biometric sample. All he needs is just to gain an access to the templates stored on a remote server.
- **Trojan horse attacks**: Some parts of the system, such as a matcher, can be replaced by a Trojan horse program that always outputs high verification scores.
- **Overriding Yes/No response**. An inherent flaw of existing biometric systems is that the output of the system is always a binary Yes/No (i.e., match/no match) response. In other words, there is a fundamental disconnect between the biometric and applications, which makes the system open to potential attacks. For example, if an attacker were able to interject a false Yes response at a proper point of the communication between the biometrics and the application, he could pose as a legitimate user to any of the applications, thus bypassing the biometric part.
- **Insufficient accuracy** of many commercial biometric systems, both in terms of False Rejection Rate (FRR) and False Acceptance Rate (FAR). High FRR causes inconvenience for legitimate users and prompts the system administrator to lower a verification threshold. This inevitably gives rise to FAR, which, in turn, lowers the security level of the system.

The privacy and security issues of a biometric system outlined in this section are illustrated in Fig. 1 below:

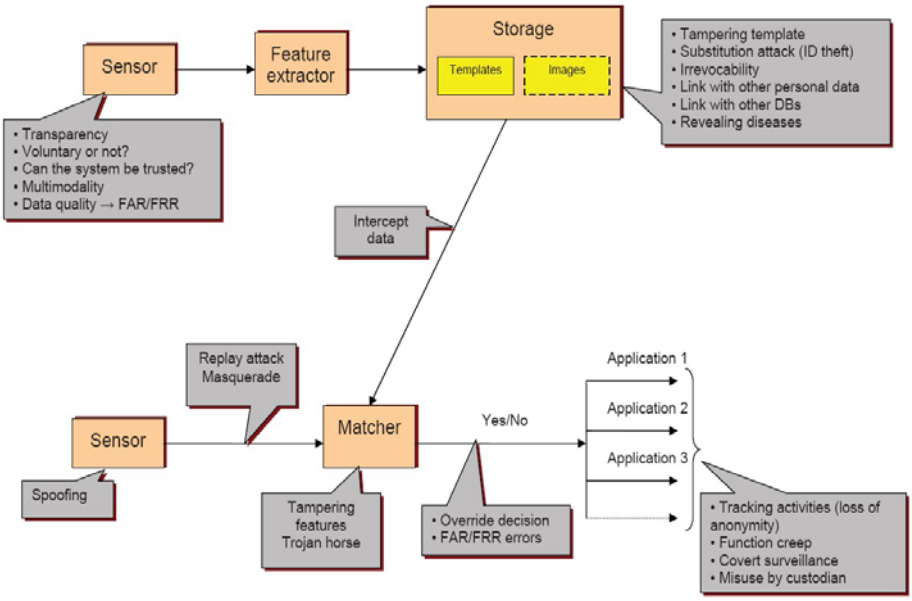

Fig. 1. Privacy and security issues in a biometric system

The enrolment part of any conventional biometric system consists of at least three blocks: a biometric sensor which acquires an image, a feature extractor that creates a biometric template, and storage for the templates, or images, or both. The storage can be either a database or a distributed medium.

The verification or identification part contains (at a minimum) a sensor to acquire a new image sample, and a matcher, which compares the image with the previously enrolled template(s) received from the storage. The output of the matcher is a Yes/No (i.e., match/no match) response that may go to the variety of applications.

A user of the system faces several privacy issues immediately at enrolment:

- Transparency, i.e., if the purpose of the system is clear to the user;
- If the enrolment is voluntary, and what are the consequences of not getting enrolled (for a variety of reasons);
- If the system can be trusted, i.e., if the personal data are adequately protected;
- Quality of biometric data: poor quality may lead to higher FRR and FAR. While FAR increases security risks for the system, a false rejection often causes some follow-up procedures which can be privacy-invasive to the individual.

3 Biometrics and Cryptography

Conventional cryptography uses encryption keys, which are just long bit strings, usually 128 bits or more. These keys – which can be symmetric, public, or private— are an essential part of any cryptosystem, for example, Public Key Infrastructure

(PKI). A person cannot memorize such a long random key, so the key is generated, using several steps, from a password or a PIN that can be memorized. The password management is the weakest point of any cryptosystem, as the password can be guessed, found with a brute force search, or stolen by an attacker.

Biometrics, on the other hand, are unique characteristics that are always there. Can they be used as a cryptographic key? Unfortunately, the answer is negative: biometric images or templates are variable by nature, which means that each new biometric sample is different. And conventional cryptography cannot tolerate a single bit error.

A biometric system always produces a Yes/No response, which is essentially one bit of information. Therefore, an obvious role for biometrics in the conventional cryptosystem is password management, as mentioned by Bruce Schneier[ix]. Upon receiving Yes response, the system unlocks a password or a key. The key must be stored in a secure location (so called "trusted" device). This scheme is still prone to the security vulnerabilities noted in Fig. 1, however, since the biometric system and the password are connected via one bit only.

Biometric templates or images stored in a database can be encrypted by conventional cryptographic means. This would improve the level of system security, since an attacker must gain the access to the encryption keys first. However, most privacy issues associated with a large database remain, since the keys and, therefore, the biometric data, are controlled by a custodian.[x]

A comprehensive review of the issues involving biometrics and cryptography can be found elsewhere.[xi]

4 What is Biometric Encryption (BE)?

Because of its variability, the biometric image or template itself cannot serve as a cryptographic key. However, the amount of information contained in a biometric image is quite large: for example, a typical image of 300x400 pixel size, encoded with eight bits per pixel has 300x400x8 = 960,000 bits of information. Of course, this information is highly redundant. One can ask a question: Is it possible to consistently extract a relatively small number of bits, say 128, out of these 960,000 bits without storage of any additional data? Or, is it possible to bind a 128-bit key to the biometric information, so that the key could be consistently regenerated? While the answer to the first question is problematic, the second question has given rise to the new area of research, called Biometric Encryption (BE).[1]

Biometric Encryption is a process that securely binds a PIN or a cryptographic key to a biometric, so that neither the key nor the biometric can be retrieved from the

[1] Other terms used for these technologies: biometric cryptosystem, private template, fuzzy commitment scheme, fuzzy vault, fuzzy extractor, secure sketch, biometric locking, biometric key binding, biometric key generation, virtual PIN, biometrically hardened passwords, biometric signature, etc. We use the term "Biometric Encryption" in a broad sense to include all the foregoing technologies.

stored template. The key is re-created only if the correct live biometric sample is presented on verification.

The digital key (password, PIN, etc.) is randomly generated on enrolment, so that nobody, including the user, knows it. The key itself is completely independent of biometrics and, therefore, can always be changed or updated. After a biometric sample is acquired, the BE algorithm securely and consistently binds the key to the biometric to create a protected BE template, also called a "private template." In essence, the key is encrypted with the biometric. The BE template provides an excellent privacy protection and can be stored either in a database or locally (on a smart card, token, laptop, cell phone, or other device.). At the end of the enrolment, both the key and the biometric are discarded.

On verification, the user presents her fresh biometric sample, which, when applied to the legitimate BE template, will let the BE algorithm retrieve the same key/password. So the biometric serves as a decryption key. At the end of verification, the biometric sample is discarded once again.

The BE algorithm is designed to account for acceptable variations in the input biometric. Nevertheless, an attacker whose biometric sample is different enough will not be able to retrieve the password. This encryption/decryption scheme is fuzzy, as the biometric sample is different each time, unlike an encryption key in conventional cryptography. Of course, it is a big technological challenge to make the system work.

After the digital key, password, PIN, etc., is retrieved, it can be used as the basis for any physical or logical application. The most obvious way lies in the conventional cryptosystem, such as a PKI, where the password will generate a pair of public and private keys.

Overall, Biometric Encryption is an effective, secure, and privacy friendly tool for biometric password management, since the biometric and the password are bound on a fundamental level.

5 Advantages of Biometric Encryption

Biometric Encryption technologies have enormous potential to enhance privacy and security. Some of the key benefits and advantages of this technology include:

5.1 NO retention of the biometric image or template

Most privacy and security concerns derive from storage and misuse of the biometric data.

A common concern is that "if you build it (the database), they will come (for the data)." The top-line privacy and security concerns include fears of potential data matching, surveillance, profiling, interception, data security breaches, and identity theft by others. Misuse and mismanagement of biometric data by others invokes negative externalities and costs that fall primarily upon individuals rather than the

collecting organization. But the accountability and credibility of the collecting organization are also at stake and, with them, the viability of the entire program.

From a privacy perspective, the best practice is to collect little or no personally identifiable information (PII) at all in the first place. This is referred to as "data minimization" — minimizing the amount of personal data collected and retained, thus eliminating the possibility of subsequent abuse.

Biometric Encryption directly addresses these risks, threats and concerns. Users retain complete (local) control and use of their own biometrics. Local control enhances confidence and trust in the system, which ultimately promotes greater enrolment and use.

5.2 2. Multiple/cancelable/revocable identifiers

Biometric Encryption allows individuals to use a single biometric for multiple accounts and purposes without fear that these separate identifiers or uses will be linked together by a single biometric image or template. If a single account identifier becomes compromised, there is far less risk that all the other accounts will also be compromised. Even better, Biometric Encryption technologies make it possible to change or recompute account identifiers. That is, identifiers may be revoked or cancelled, and substituted for newly generated ones calculated from the same biometric! Traditional biometric systems simply cannot do this.

5.3 3. Improved authentication security: stronger binding of user biometric and identifier

Account identifiers are bound with the biometric and recomputed directly from it on verification. This results in much stronger account identifiers (passwords) that are longer and more complex, don't need to be memorized, and are less susceptible to security attacks. Many security vulnerabilities of a biometric system listed in Fig. 1 are also addressed by BE:

No substitution attack: An attacker cannot create his own template since neither he, nor anybody else, know the digital key and other transitory data used to create the legitimate template.

No tampering: Since the extracted features are not stored, the attacker has no way to modify them.

No high level masquerade attack: Again, the system does not store the biometric template, so that the attacker cannot create a digital artefact to submit to the system[2]. BE provides an effective protection for remote authentication systems.

[2] A masquerade attack may still be possible on a low level, which requires thorough knowledge of BE algorithm from an attacker. See, for example, "Hill Climbing" attack against an early BE system with insufficient protection[xxi].

No Trojan horse attacks: A BE algorithm does not use any score, either final or intermediate, to make a decision, it just retrieves (or does not retrieve) a key. Therefore, the attacker cannot fool the system by outputting a high score.

No overriding Yes/No response: The output of BE algorithm is a 128-bit (or longer) digital key, as opposed to the binary Yes/No response. The attacker cannot obtain the key from a private template.

The security of Biometric Encryption technology can be augmented by the use of tokens (e.g. smart cards, PDA) and additional passwords, if needed[xii].

5.4 Improved security of personal data and communications

As an added bonus, users can take advantage of the convenience and ease of BE technologies to encrypt their own personal or sensitive data. See Use Case Scenario #1 for an example. Since the key is one's own biometric, used locally, this technology could place a powerful tool directly in the hands of individuals. Biometric Encryption could be viewed as encryption for the masses, made easy!

5.5 Greater public confidence, acceptance, and use; greater compliance with privacy laws

Public confidence and trust are necessary ingredients for the success of any biometric system deployment. One major data breach involving a large centralized database of biometric templates could set back the entire industry for years.

Data governance policies and procedures can only go so far to foster public trust. However, if privacy, security and trust can be built directly into the biometric system, then the public and data protection authorities are far more likely to accept the privacy claims being made.

Putting biometric data firmly under the exclusive control of the individual, in a way that benefits that individual and minimizes risk of surveillance and identity theft, will go a long way towards satisfying the requirements of privacy and data protection laws, and will promote broader acceptance and use of biometrics.

5.6 Suitable for large-scale applications

BE technologies speak directly to the clear preference and recommendations of international privacy and data protection authorities for using biometrics to authenticate or verify identity, rather than for identification purposes alone.

We prefer to see biometrics used to positively link the bearer to a card or token, avoiding the creation of systems that rely upon centralized storage and remote access/lookup of biometric data. An important reason for this view is that it is not known if biometric technology is sufficiently accurate and reliable to permit real time identification in large n samples, where n is of an order of several million or higher. Nevertheless, many large-scale one-to-many public biometric projects are being proposed and are well underway.

Often the biometric data in these systems are actually used for authentication purposes and not identification, but the lines between these two concepts can be blurred when multiple data items are collected and transmitted to a database for comparison. The distinction between the identifier and the authenticator can be somewhat arbitrary.

From a privacy point of view, transmitting biometric image or template data to a central database to be authenticated is risky enough without compounding the risks by sending more and more personal identifiers with it. Multimodal biometric solutions depend on collecting and comparing more than one biometric. It should be noted that the main reason for using multimodal solutions, besides providing a fallback for problem users, is insufficient accuracy/speed/security of existing biometrics. So the technical solution to using biometrics for authentication seems to be to collect more and more biometric and other personal data.

The European Data Protection Supervisor (EDPS) Peter Hustinx has warned, in his commentaries and formal opinions, of the privacy dangers of using biometric images or templates as an index or key to interoperable databases.[xiii]

Fortunately, BE technologies make possible database applications, minimizing the risks of traditional biometric systems (although we still prefer one-to-one applications with local template storage). It is possible to create secure and local biometric-enabled bindings of users to some other token identifiers without the need to reveal the actual biometric image or data.

It is further possible to create a so-called "anonymous database" where a link between an anonymous identifier and encrypted (by conventional cryptographic means) user's record is controlled by a BE process. This is very useful for a database containing sensitive information, such as medical records (see Use Case Scenario #2).

Another promising application of BE is a privacy-protected one-to-many database for preventing "double dipping." The database is multimodal: it contains conventional but anonymous templates for one biometric (e.g. fingerprints) and private templates (e.g. for iris) that control the link with the user's encrypted records. A user's record would only be decrypted and displayed if there was a positive match on both conventional and private templates. Otherwise, all the information is inaccessible even to the system administrator.

With Biometric Encryption, users would be empowered by the ability to securely prove who they are to anyone, for any purpose, using their own biometrics, without having to disclose the biometric data itself.

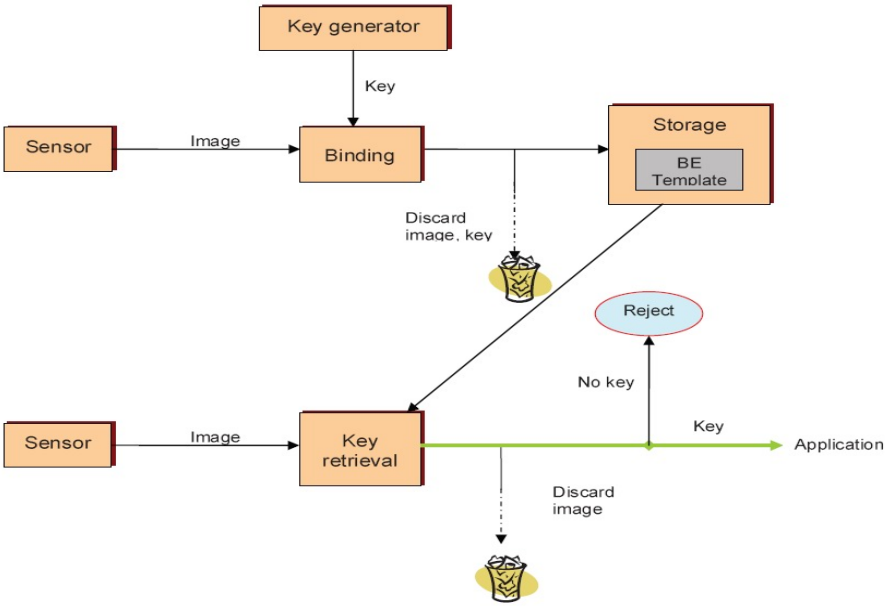

Fig. 2. High level diagram of a Biometric Encryption process

The enrolment part of a BE system consists of at least four blocks: a biometric sensor, a key generator that normally outputs a random key, a binding algorithm that creates a BE (private) template, and a storage for the BE template. Neither the key nor the image can be recovered from the BE template. The key, the image, and some transitory data are discarded at the end of the enrolment process.

The verification part contains at least a sensor to acquire a new image sample, and a key retrieval algorithm, which applies the image to the previously enrolled BE template received from the storage. The algorithm either retrieves the key, if the image on verification is close enough to the one enrolled, or fails to do so, in which case the user is rejected. The key enters an application, such as a PKI. Each application has its unique key. The biometric image is discarded at the end of the verification process.

6 Current State of Biometric Encryption

The original concept of Biometric Encryption for fingerprints was pioneered in 1994 by Dr. George Tomko, founder of Mytec Technologies (Toronto, Canada). Since then, many research groups have taken part in the development of BE and related technologies. There is substantial number of articles and patents published to date, most of which have appeared since 2002.[i]

BE and related technologies have drawn attention from major academic research groups specializing in biometrics and industry leaders..

Virtually all types of biometrics have been tested to bind (or generate) a digital key: fingerprints, iris, face, keystroke dynamics, voice, handwritten signatures, and palm prints. The most promising results have been achieved with iris, where FRR = 0.47%, FAR = 0 (or at least less than one in 200,000) to generate a 140-bit key[xiv]. These error rates are only marginally higher than for a conventional iris-based biometric system with the same input images.[3]

The use of fingerprints is also feasible in terms of accuracy for BE, with FRR greater than 10% at present[xii]. Unlike an iris, there is a noticeable degradation in accuracy from a conventional fingerprint system. This is understandable since fingerprints are more prone to distortions and other factors that degrade accuracy. It is more difficult to compensate those factors in the case of Biometric Encryption, since BE works in a "blind" mode (the enrolled fingerprint or its minutiae template are not seen). There are several ways to overcome this problem, for example, by using a free air (i.e., contactless) fingerprint sensor, or by using more than one finger from the same person, or by combining several biometrics. Note that even a 10% – 20% false rejection rate may still be acceptable for some applications with relatively low traffic and cooperative users: it simply means that a person would be rejected each fifth or tenth time on average and asked by the system to place the finger on the reader again.

Face recognition, which is usually considered third (after irises and fingerprints) in terms of accuracy in conventional biometrics, has shown a significant improvement of performance over the last few years. This allowed Philips Research to create a working BE system using a face biometric. The published results range from FRR = 3.5% for a face database with low to medium variability of images to FRR = 35% for a database with high variability; FAR = 0 (or at least less than 1 in 100,000) in both cases. The key size used is 58 bits, which may be sufficient as a password replacement. The Philips technology, called privID™, is a part of a European 3D Face project [xv].

It is not clear if other biometrics have enough entropy (i.e., the amount of non-redundant information) to bind a sufficiently long key (e.g. 128 bit). This is an area of future research.

Some works published since 2002 provide a general theoretical foundation for BE technologies from a cryptographic point of view. They prove that the system can be made secure against "brute force" search attacks. In other words, an attacker checks at random all possible combinations in order to retrieve a key (or a biometric). Like conventional cryptography, it is assumed that the attacker is fully familiar with the algorithm, and may have a template in hand, but does not have a proper biometric to unlock the secret (i.e., the key bound to the biometric).

However, the attacker may try more sophisticated attacks exploiting inherent weaknesses (if any) of the BE system and biometrics in general. This area of research has been largely overlooked. If such an attack were successful, the effective security of the system would be reduced from 128 bits to, perhaps, 69, 44, or an even lower number of bits. "This may seem an alarmingly small number to the crypto purist."[xiv]

[3] The iris images were acquired in close to ideal conditions of a laboratory environment. In real life systems, some degradation of performance is expected, which is always the case with biometrics.

On the other hand, BE is not just another cryptographic algorithm; it is rather a key/password management scheme. Key management has always been the weakest part of any cryptosystem, as it relies on passwords that may be forgotten, stolen, guessed, shared, etc. Biometric Encryption binds the key/password with the biometric and, thus, makes the system more secure.

It is interesting to note that breaking a biometrically encrypted key exposes that key, but not necessarily the biometric, let alone the entire BE database, making it a more secure system.

With the notable exception of Philips privID™, to the best of our knowledge, there is no commercially available BE system being used to date. The reason for this lies in both the technological challenges and market conditions. Not only the general public, but most hi-tech developers, are unaware of this emerging technology. Consequently, resources and funding in this area have, to date, been poor. We believe that the technological challenges have been overcome to a large extent using an iris, and partially for face and fingerprints, so that the BE technology is very close to the prototype development stage and could soon be ready for testing in pilot projects.

7 Related Technologies

7.1 Storing a key in a trusted system

There have been some products that store a cryptographic key or a PIN in a so-called trusted system (e.g. a computer or a Digital Signal Processor (DSP)). The key is released upon successful biometric verification and then enters a conventional cryptosystem, e.g. Public Key Infrastructure (PKI). The biometric template (or image) is also stored somewhere, often in encrypted (by conventional means) form.

If properly implemented, such systems may offer some security benefits. However, most problems outlined in the foregoing sections remain. For example, a binary Yes/No response is still required to release the key – this part of the algorithm is just hidden better. Most privacy issues associated with the template storage are also there.

Note that these systems often use the same terminology and/or claim the same benefits as BE, while in fact they do not provide a true binding between a key and a biometric.

7.2 Cancelable biometrics

A new area of research, closely related to BE, is cancelable biometrics. It has been developed by IBM T.J. Watson Research Center, and by some academic groups[xvi]. In this privacy-protecting technology, a distortion transform (preferably, irreversible) is applied to a biometric template. Only those distorted templates are stored, and they are matched also in the distorted form. If a distorted template is compromised, it can

be "cancelled" by choosing just another distortion transform (i.e., the biometric is not lost). The transforms are application-dependent, meaning that the templates cannot be reused by another applications (so function creep is prevented).

Cancelable biometrics has some other similarities with BE, for example, a technique called bioHashing can be used for both technologies. But unlike BE, a key is not generated or released in cancelable biometrics, so that the system still produces a binary Yes/No response and is more vulnerable to attacks. The distortion transform should be truly irreversible (i.e., one way only) and kept secret. Otherwise, an attacker can either reconstruct the original biometric or create his own impostor template for a substitution attack, or even create an "artefact" image for a masquerade attack. Since the key is not generated, the variety of potential applications is narrower than for BE; for example, an anonymous database cannot be created. On the other hand, BE possesses all the functionality of cancelable biometrics. Both technologies face similar accuracy/security challenges.

7.3 Fuzzy Identity Based Encryption

Another related technology, called Fuzzy Identity Based Encryption (FIBE), was proposed by A. Sahai and B. Waters in 2005[xvii]. This technology also combines biometrics and cryptography on a fundamental level. Unlike BE, the user's biometric is made somewhat public. In an example provided by D. Nali, C. Adams and A. Miri[xviii], a user (A) could go to a Driver Licensing Agency (D), and identify herself via an iris scan, under the ongoing surveillance of a trained agent. D could then use this scan to encrypt A's information (e.g. an annual driver's license), when this information needs to be securely sent to A (e.g. via the Web). In order to obtain her biometric private keys, A would have to go in-person to a trusted third party (e.g. a state agency) that would deliver keys via the same authenticating procedure as that used by D. A could then decrypt the message addressed to her using FIBE. She does not need a biometric reading at that point. In other words, A leaves her biometrics in at least two places, D and the trusted third party (often called Trusted Authority (TA)).

This scheme prevents impersonation of A by surreptitious capturing of her biometric sample, such as an iris photograph or latent fingerprints. "FIBE allows biometric measurements to be public"[xviii] and, therefore, those surreptitious samples would become useless. While interesting from a scientific point of view, this technology is not privacy protecting, as biometric data are considered personal information. There are also problems in handling a false rejection: user A may not have a chance to present another biometric sample if the false rejection occurs during decryption.

8 Scientific, Technological, and Privacy-Related Merits

Encryption with a fuzzy key (such as a biometric) was only recently introduced in conventional cryptography. Beyond such trivial things like accepting a few spelling errors in a password, or letting Alice partially share a list of her favourite movies with Bob, Biometric Encryption technologies are by far the most important application of those theoretical works. Market demand for such a technology would provide a great incentive to this promising area of modern mathematics and cryptography.

BE results in tougher requirements for distortion tolerance, discrimination, and the security of a biometric system. Solving these problems would be a significant scientific breakthrough both in the area of biometrics and cryptography. This would accelerate research and development of better biometric sensors and other hardware, as well as new, more accurate algorithms and software. No doubt this would bring technological benefits for the entire field of biometrics.

BE overcomes many security vulnerabilities of a biometric system, especially in a distributed environment. This could facilitate deployment of biometric systems on portable and handheld devices (laptops, cellphones, PDAs, etc.).

It would not be an overstatement to say that biometrics is perceived, in general, as a privacy-invasive technology. As we have shown, this perception is not baseless. Biometric Encryption, on the other hand, is a privacy-enhancing technology. It allows a user to retain full control over her biometric and, at the same time, to stay anonymous in many applications, i.e., to be represented only by a randomly generated (and cancelable) identifier linked to her biometric. No other personal data, e.g. address, telephone, date of birth, have to be revealed.

BE can render databases privacy-protected, as they will comprise "private templates." While such databases cannot be used for a background check, they are perfectly suitable for one-to-one access control systems or even for systems that prevent multiple registrations and related fraud. The user retains control over his or her sensitive information, such as medical or financial records, stored in the database.

Proliferation of BE technology may ultimately change the public's perception of biometrics. This would raise the benchmark for biometric technologies, such that the industry would be prompted to develop and adopt new privacy-friendly solutions. If the "private templates" generated by BE make a significant presence in the market, this could reshape the entire biometric industry. Increased user acceptance and confidence would be extremely beneficial for the industry.

8.1 Use Case Scenario #1: Small-scale use of BE

To demonstrate the power of BE, we will briefly present a biometric authentication protocol (remote or local) with third party certification. We use a simplified and reworded description from Boyen's paper on fuzzy extractors.[xix]

Suppose that Alice wishes to authenticate herself to Bob using biometrics. Due to privacy concerns, she does not wish to reveal any biometric information to Bob. Conversely, for the authentication to be meaningful, Bob wants some assurance that Alice is, in fact, in possession of her purported biometrics at the time the

authentication is taking place (i.e., that no one is impersonating her). We assume that there is a third party (often called the Trusted Authority), Trent, whom Bob trusts to honestly certify Alice's biometrics, and to whom Alice will temporarily grant access to her biometrics for the purpose of generating such a certificate. Alice will want to be able to obtain as many or as few of those certificates as she wants, and to reuse as many of them with multiple Bobs, some of whom may even be dishonest, without fear of privacy leaks or impersonation. The protocol is as follows:

Enrolment and certification takes place under Trent's supervision and using Alice's own biometric, as follows:

1. Alice creates a BE template from her biometric and a randomly selected PIN. Neither the biometric nor the PIN can be recovered from the template.
2. The PIN is used to generate a pair of keys called public and private keys.
3. The biometric, the PIN, and the private key are discarded.
4. If Trent is satisfied that Alice has executed the steps honestly, he certifies the binding between Alice's name and the public key, i.e., he digitally signs the pair ["Alice," public key]. At this point, Alice may send the public key to Bob, or even publish it for all to see.

A challenge/response scheme is used to verify Alice:

1. At any time when appropriate (e.g. whenever Alice desires to authenticate herself to Bob), Bob sends Alice a fresh random challenge.
2. By obtaining her new biometric sample and applying it to her BE template, Alice recovers her PIN on the fly, which, in turn, regenerates her private key.
3. Alice signs the challenge with her private key and gives Bob the signature.
4. Bob authenticates Alice by checking the validity of the signature under her authentic public key.

The protocol does not require Alice to remember or store her PIN or her private key. The BE template may be stored on a smart card or in Alice's laptop that also has a biometric sensor. For different applications ("multiple Bobs"), a new pair of public and private keys is generated from the PIN. Those keys are periodically updated. Some applications may require different PINs, in which case several BE templates can be stored. A proper template can be automatically recognized by the application.

The system based on digital signatures may be adopted both for a remote and local access. The important point is that the most critical part of any cryptosystem, the PIN (or a password), is securely bound to the biometrics.

To summarize, Alice has in her possession and under her control as many BE templates as necessary. She can use them to digitally sign in, either for remote authentication or for logical or physical access. The authentication is done simply by checking the validity of her digital signature using standard cryptographic means. Neither Alice's biometric nor her PIN are stored or revealed. As a result, the system is both secure and highly privacy-protective.

8.2 Use Case Scenario #2: Anonymous database; large or medium-scale applications

Suppose that a clinic, a hospital, or a network of hospitals maintains a database of medical records. Alice does not want her record to be accessed by unauthorized personnel or third parties, even for statistical purposes. For that the latter, her record is made anonymous and encrypted (by conventional means). The only public entry in the database is her personal identifier, which may be her real name or, in certain cases (e.g. drug addiction clinic), an alias ("Jane Doe"). The link between Alice's identifier and her medical record is controlled by Biometric Encryption.

On enrolment, a BE template is created from Alice's biometric and a randomly-generated PIN (Alice does not even know the PIN). The PIN is used to generate a pointer to Alice's medical record and a crypto-key that encrypts the record, and also a pair of keys called public and private keys (similar to Use Case Scenario #1). The BE template and the public key are associated with Alice's ID and stored in the database (they can be also stored on Alice's smart card). Other temporary data, such as Alice's biometric, the PIN, the private key, the pointer, and the crypto-key, are discarded.

Suppose that Alice visits a doctor, to whom she wants to grant remote access to her medical record, or part of it, if the record is structured. From the doctor's office, Alice makes a request to the database administrator, Bob. The authentication procedure using challenge/response scheme is similar to that in use case scenario #1:

1. If Alice does not have her smart card with her (e.g. in the case of an emergency), Bob sends Alice's BE template to the doctor's office.
2. Alice applies her new biometric sample to the BE template and recovers her PIN on the fly.
3. The PIN is used to regenerate her private key, the pointer to her medical record, and the crypto-key.
4. Bob sends Alice a fresh random challenge.
5. Alice signs the challenge with her private key and gives Bob the signature.
6. Bob authenticates Alice by checking the validity of the signature under her public key.
7. Alice securely sends Bob the pointer to her medical record.
8. Bob recovers Alice's encrypted medical record (or a part of it, also encrypted) and sends it to Alice.
9. Using her crypto-key, which was regenerated from her PIN, Alice decrypts her medical record for the doctor.
10. Alice's biometric, the PIN, the private key, the pointer, and the crypto-key, are discarded.

In summary, Bob (the database administrator) has an assurance that Alice is, in fact, who she claims to be (she was able to unlock her BE template in the doctor's office); he is also assured that her medical record was sent to the right person. At the same time, Alice retains full control over her medical record, so that even Bob (the database administrator) has no access to it, since he does not have the crypto-key to decrypt it. The privacy protection is embedded into the system at a very basic technological level.

8.3 Use Case Scenario #3: Travel documents; large-scale database applications

Using biometrics for travel documents has been a hot topic of discussion of late. To illustrate how BE can protect the user's privacy and, at the same time, improve the level of security, we will consider a system proposed by Van der Veen et al.[xx]

The International Civil Aviation Organization (ICAO) dictates international standards for Machine Readable Travel Documents (MRTD), including those for ePassports. Among the recommendations is the "three-way-check" for secure verification at a border crossing. This involves comparing data originating from (i) the biometric sensor, (ii) the biometric image stored on the ePassport, and (iii) biometric data stored in external (centralized) databases.

BE technology provides the opportunity to do this in a privacy preserving manner. In addition to the biometric templates stored on the ePassport, their secure versions, namely, the BE templates, are also stored in a third-party database. The biometric images or conventional templates are not stored in the database. A "three-way check" is then performed by matching the BE template from the database to that appearing on the ePassport, and the live biometric measurement scanned at the kiosk. So border passage now involves the following steps:

1. At a kiosk, a user claims his identity (ID), and presents his biometric (e.g. facial image, fingerprint or iris) for measurements.
2. The ID is sent to the third-party database to extract the corresponding BE template.
3. The BE template is transmitted to the kiosk.
4. The BE template and the biometric measurement are combined to derive a hashed version of the cryptographic key.
5. The image of the iris, face or fingerprint is extracted from the ePassport and used together with the BE template to derive another hashed version of the cryptographic key. This will validate the biometric stored on the ePassport.
6. Both hashed versions of the key derived in Steps 4 and 5 are transmitted to the border control authority and verified against the database version. A positive authentication is achieved when all three versions are identical.

The user's privacy is protected since the biometric image or template is not stored in a central database; instead, a secure BE template is stored. The database is inherently secure, meaning there is no need for complicated encryption and key management protocols. The ePassport is protected against tampering, since neither a potential attacker nor anybody else know the cryptographic key that was used to create the BE template.

9 Next Steps for Bringing BE to the Prototype Stage

Biometric Encryption has been researched since the mid-90s. Technologically, this area is much more challenging than conventional biometrics. But now, BE is fast

approaching the next phase, i.e., the creation and testing of a prototype. The following issues still need to be addressed:

9.1 Selecting a Proper Biometric

The most promising results in terms of accuracy have been obtained for irises. Low variability of image samples, and the presence of a natural alignment feature (the pupil), make this biometric the number one candidate for BE.

Face recognition is the most publicly acceptable type of biometric. Recent advances in the technology made it possible to use face biometric for BE. At the present time, one of the drawbacks of the face-based BE system, however, is the relatively small size (~ 58 bits) of the encryption key that may be securely bound to the biometric. Using high resolution or 3D face recognition would likely improve the system performance.

Fingerprints, for which the BE was originally pioneered, are also a prime choice. The fingerprint biometric is used more widely than the iris, and most privacy concerns relate to fingerprints. At the same time, using fingerprints for BE turns out to be much more challenging. The reasons are that high skin distortions can be introduced when the finger presses upon the sensor, and the difficulty of aligning a fingerprint on verification with the one enrolled. As mentioned before, the situation is more difficult for BE than for a conventional fingerprint verification, since most BE schemes work in a "blind" mode (the enrolled fingerprint or its minutiae template are not seen). Some of these issues can be overcome with a free-air image. Although this would present other optical issues, we believe they could be resolved by current technology. In general, face and especially iris are less vulnerable to distortion and alignment problems.

Other biometrics, e.g. voice, signature, palmprints, etc., may not have enough entropy (i.e., the amount of non-redundant information to support a long enough cryptographic key). They could be possibly put on the list of "auxiliary" biometrics, i.e., used for BE in combination with irises, faces, or fingerprints or, perhaps, with conventional passwords (which is called "hardening").

9.2 Improving the Image Acquisition Process

For fingerprints, this means choosing a proper fingerprint sensor that is less susceptible to skin distortions (e.g. a free air sensor), or changing the existing sensor ergonomics to keep the distortions under control. Image quality can also be improved at the algorithm level (i.e., through software). In general, the requirements for the image quality are tougher for BE than for conventional biometrics.

9.3 Making BE Resilient Against Attacks

This area of research — the analysis of potential vulnerability of BE against attacks— has been largely overlooked. By that we mean that a sophisticated attacker could gain

access to both the BE templates and the algorithm. The only thing he cannot obtain is a user's biometric. Such an attacker, fully familiar with the algorithm and exploiting its weaknesses, will not be doing just a brute force search (i.e., about 2128 computations for a 128 bit key) in order to break the BE template. Instead, he will devise various attacks that can be run in a realistic time frame. The BE algorithm must be resilient against those off-line attacks[xxi]. The same approach (i.e., resilience against attacks) is adopted in conventional cryptography.

9.4 Improving Accuracy and Security of BE Algorithm

There have been substantial advances in algorithm development in conventional biometrics in the past few years, as demonstrated by a series of international competitions. Many of those advances are applicable to BE.

For BE, a crucial step, both in terms of accuracy and security, is selection of a proper *Error Correcting Code* (ECC). For the past 10-13 years, there have been major advances in the area of ECC. Some of them have been already applied to BE with promising results[xxii].

9.5 Exploiting Multimodal Approaches

This has been a hot area of research and development in conventional biometrics. The performance of a biometric system is significantly improved when different algorithms, or different fingers, or different biometrics (e.g. fingerprints and face) are combined. The modes that are combined should be "orthogonal" i.e., statistically independent. It is reasonable to expect that the multimodal approach would also work for BE.

9.6 Developing BE Applications

The applications, such as those described in the case studies, should clearly demonstrate the benefits for privacy and security brought about by the use of BE.

10 Summary and Conclusions

Biometric Encryption technology is a fruitful area for research and has become sufficiently mature for broader public policy consideration, prototype development, and consideration of applications.

This paper has explored the possibilities and privacy-enhancing benefits of Biometric Encryption technologies for meeting the needs of businesses and government agencies.

We believe that BE technology exemplifies the fundamental privacy and data protection principles endorsed around the world, such as data minimization, user

empowerment and security, better than any other biometric technology solution in existence.

We hope that our paper will form a valuable contribution to current national and international discussions regarding the most appropriate methods to achieve, in a privacy-enhanced manner, strong identification and authentication protocols.

While introducing biometrics into information systems may result in considerable benefits, it can also introduce many new security and privacy vulnerabilities, risks, and concerns, as discussed above. However, novel Biometric Encryption techniques have been developed that can overcome many, if not most, of those risks and vulnerabilities, resulting in a win-win, positive-sum scenario.

One can only hope that the biometric portion is done well, and preferably not modeled on a zero-sum paradigm, where there must always be a loser. A positive-sum model, in the form of Biometric Encryption, presents distinct advantages to both security and privacy.

References

---

[i] See list of resources in appendices of: Ann Cavoukian and Alex Stoianov, *Biometric Encryption: A Positive-Sum Technology that Achieves Strong Authentication, Security AND Privacy* (March 2007) at www.ipc.on.ca/images/Resources/up-1bio_encryp.pdf, and: Organization for Economic Co-operation and Development (OECD), Directorate for Science, Technology and Industry (DSTI), Committee for Information, Computer and Communications Policy (ICCP): *Biometric-Based Technologies* DSTI/ICCP/REG(2003)2/FINAL (June 2004); and
International Biometric Group BioPrivacy Initiative at www.Bioprivacy.org

[ii] See the 27th International Conference of Data Protection and Privacy Commissioners, Montreux, Switzerland, *Resolution on the use of biometrics in passports, identity cards and travel documents* (16 Sept 2005).

[iii] See European Union Article 29 Working Party, *Working document on biometrics* (Aug 2003)

[iv] See: UK Information Commissioner, *Data Protection Technical Guidance Note: Privacy enhancing technologies* (Nov 2006);
European Commission, Communication: Promoting Data Protection by Privacy Enhancing Technologies (PETs) (COM(2007) 228 final) (May 02, 2007); and
Information and Privacy Commissioner of Ontario & Dutch Registratierkamer, *Privacy-Enhancing Technologies: The Path to Anonymity* (Vols I & II - August 1995)

[v] For excellent overviews and discussions of PETs, see:
OECD DSTI/ICCP, *Inventory of Privacy-Enhancing Technologies (PETs)* (Jan 2003)
Dutch Interior Ministry, *Privacy-Enhancing Technologies. White paper for decision-makers* (2004)
R. Leenes, J. Schallaböck and M. Hansen, Privacy and Identity Management for Europe (PRIME) Project, *PRIME White paper v2* (June 2007)
Future of Identity in the Information Society (FIDIS) Project, *D13.1: Identity and impact of privacy enhancing technologies* (2007)

[vi] N. K. Ratha, J. H. Connell, R. M. Bolle. Enhancing security and privacy in biometrics-based authentication systems. IBM Systems Journal, vol. 40, NO 3, p.p. 614 – 634, 2001

[vii] C.J. Hill, "Risk of masquerade arising from the storage of biometrics," B.S. Thesis, Australian National University, 2001 (supervisor Dr. Roger Clarke).

[viii] R. Cappelli, A. Lumini, D. Maio, and D. Maltoni, "Fingerprint Image Reconstruction from Standard Templates". IEEE Transactions On Pattern Analysis And Machine Intelligence, v. 29, No. 9, pp. 1489 - 1503, 2007

[ix] B. Schneier, "The Uses and Abuses of Biometrics," Comm. ACM, vol. 42, no. 8, p. 136, Aug. 1999

[x] There has been recent activity of International Organization for Standardization in order to support the confidentiality and integrity of the biometric template by using cryptographic means (ISO/IEC WD 24745, "Biometric Template Protection").

[xi] FIDIS report, "D3.2: A study on PKI and biometrics," 2005

[xii] K. Nandakumar, A. Nagar, and A. K. Jain, "Hardening Fingerprint Fuzzy Vault Using Password", Proceedings of ICB 2007, Seoul, Korea, August 27-29, 2007. Lecture Notes in Computer Science, Springer, v. 4642, pp. 927-937, 2007

[xiii] See EDPS, Comments on the Communication of the Commission on interoperability of European Databases (10 March 2006)

[xiv] F. Hao, R. Anderson, and J. Daugman. "Combining Crypto with Biometrics Effectively". IEEE Transactions on Computers, v. 55, No.9, pp. 1081-1088, 2006

[xv] www.3Dface.org

[xvi] N. K. Ratha, S. Chikkerur, J. H. Connell, and R. M. Bolle, "Generating Cancelable Fingerprint Templates". IEEE Transactions On Pattern Analysis And Machine Intelligence, v. 29, No. 4, pp. 561-572, 2007; and the references cited there.

[xvii] A. Sahai and B. Waters, "Fuzzy identity based encryption," in Proceedings of EUROCRYPT'05 on Advances in Cryptology, LNCS 3494, pp. 457–473, Springer-Verlag, 2005

[xviii] D. Nali, C. Adams, and A. Miri. Using Threshold Attribute-Based Encryption for Practical Biometric-Based Access Control. International Journal of Network Security, Vol.1, No.3, pp.173–182, Nov. 2005

[xix] X. Boyen, "Reusable cryptographic fuzzy extractors," CCS 2004, pp. 82–91, ACM Press.

[xx] M. van der Veen, T. Kevenaar, G.-J. Schrijen, T. H. Akkermans, and Fei Zuo, "Face Biometrics with Renewable Templates". Proceedings of SPIE, Volume 6072: Security, Steganography, and Watermarking of Multimedia Contents VIII, 2006.

[xxi] A. Adler, "Vulnerabilities in biometric encryption systems". NATO RTA Workshop: Enhancing Information Systems Security - Biometrics (IST-044-RWS-007), 2004

[xxii] S. C. Draper, A. Khisti, E. Martinian, A. Vetro and J. S. Yedidia, "Using Distributed Source Coding to Secure Fingerprint Biometrics". *Proc. of IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP),* v. 2, pp. 129-132, April 2007