# Achieving Privacy, Security, and Interoperability among Biometric Networks using Symmetric Encryption

Eduardo M. Lacerda Filho and Vinicius P. Gonçalves
*Department of Electrical Engineering, University of Brasilia, Brazil*

Keywords: Privacy, Encryption, Biometric Security, Communication Protocol, Interoperability.

Abstract: Privacy, security, and interoperability of biometrics systems are fundamental for any segment of a society that uses it. In this work, we developed a network that uses a symmetric encryption scheme, to ensure the anonymous index data exchange and registration of a person, and an interoperability communication protocol to process identification requests between different biometric systems. Our main contribution is the construction of a non-reversible encryption index that can safely traverse, without decrypting it, the network of connections between different biometric systems with an interoperability and data integrity communication protocol. The advantages of our work are the mitigation of known encryption and network attacks, the creation of a random initialization vector, without sending it over the network, but feasible to be calculated for all the accredited Biometric Service Providers, the increased security of biometric database, that not only relies about templates, and the improvement of IEEE Biometric Open Protocol Standard. The security analysis of the scheme and the results confirm that the network holds anonymity of a person and that it is possible to interoperate this data with an enhanced integrity protocol.

## 1 INTRODUCTION

Biometric Service Providers (BSP) are used in various segments of society (Jain et al., 2016). For many years the typical approach for the security and privacy of a biometric system has been template protection (Jain et al., 2016; Ngo et al., 2015; Campisi, 2013). When it was proof that a vector minutiae representation of a fingerprint could be retrieved (Ross et al., 2007), many works have been developed to deal with the security and privacy of biometric networks.

Enhanced schemes have been created. They are based on cancelable biometric (feature transformations) (Kaur and Khanna, 2019) and biometric cryptosystems (Toli and Preneel, 2018; Kumar and Kumar, 2016; Li et al., 2015; Nasir and Perumal, 2013). Those efforts over the years have some improvements, but also some problems, which include linkage attacks, brute force attacks, side-channel attacks, the problem of level privacy against False Acceptance Rate (FAR), and others (Natgunanathan et al., 2016; Hirano et al., 2016; Quan et al., 2008; Kocher, 1996). Furthermore, it was not shown how to use each of these schemes on different biometric databases and make them communicate with reasonable security evidence.

From this exposition, one issue arises. How to ensure that the identity of one person is not revealed but can be processed and used for different systems interoperation, preserving privacy? This work resolves this problem with a novel approach that does not focus on the biometric template. We build a scheme that anonymizes the records in the BSP databases, enhancing security, holding privacy, and a set of communications techniques for interoperability and integrity.

The contribution of this paper can be summarized as follows:

- A scheme which produces an encrypted register based on AES-CBC algorithm (Dworkin, 2001), with 256-bit symmetric secret key `k`, a random and locally calculated initialization vector `iv`, and on the one-way functions SHA-2 (Dang, 2015), for checksum, calculated into Hardware Security Module (HSM) (Wenqian Yu et al., 2016), embedded in a safe and audit environment;
- A communication protocol based on HTTPS (Rescorla, 2000), JSON (Bray, 2017), and ANSI/NIST (Mangold, 2016) packages, that improves the IEEE BOPS (Biometric Open Protocol Standard) (IEEE, 2019) method.

The cryptographic scheme proposed turns a record based on a unique biographical identification of a person, such as the social number `SN` into an IDN anonymous register. Anonymous register means that no biographical index data is stored or exchanged, not either

the biometric raw images. So, one IDN represents only one owner associated with SN. All the BSP in the network can calculate locally the same IDN string representing one person of that biometrics unequivocally, without exchange iv. The goals of this scheme are: 1. guarantee that it is impossible to use known attacks to link IDN to the biographical SN identity; 2. security and privacy of a person in the network it is not maintained only by using biometric templates; 3. usage of an anonymous register to exchange biometric information of the same person among different systems, without revealing who the person is.

The communication protocol uses HTTPS and JSON protocols, and ANSI/NIST packages. It is possible to achieve interoperability and integrity between the biometric systems that handle the encrypted IDN without decrypting it. As an improvement to the IEEE BOPS, we implemented one flow of identification (1:n) of a record, with biometric base integrity assurance procedures. The goal of this protocol is that any biometric network can use this method to address any request for identification without tampering with the recognition technology. A network is created where different system technologies have a hub and directory services to authenticate and fulfill the requests for identification between biometric systems.

This paper is divided into the following parts. In Section 2, we will discuss the related works, highlighting the technical issues involved. We introduce the proposed scheme of our contributions, in section 3. In Section 4 and 5, the security analysis and the results of a running instance of the proposed framework evaluation are reported, respectively. Finally, in Section 6, we will conclude indicating future works.

# 2 RELATED WORK

## 2.1 Privacy and Security Concerns

Achieving data privacy and security is a challenge. The Dwork's differential privacy work (Dwork, 2006) shows that there is much auxiliary information that an adversary ($\mathcal{A}$) can obtain without accessing the database. Therefore, it is essential to delimit what a method intends to establish security and privacy (Campisi, 2013). For biometric systems security and privacy, many cryptography techniques are used.

The work of Nassir and Perumal (Nasir and Perumal, 2013) uses symmetric and RSA algorithms. The work encrypts and signs the user ID and password with the biometric data extracted into one package. Some performance evaluation is done without security analysis.

Li et al. (Li et al., 2015) describe a new security analysis, proposing a multibiometric construction. By combining information-theory and security, the work uses features extraction and two levels of encryption, one with hash functions and fuzzy vaults to bind the transformed fingerprint template, and the other use Shamir's secret sharing scheme to split and store the hash values. A decision-level fused obtains the identity of a sample.

The paper from Kumar and Kumar (Kumar and Kumar, 2016) proposed a multimodal biometric cryptosystem based on feature-mode and decision-mode. The construction consists of three phases, i.e., a Bose Chaudhuri Hocquenghem (BCH) applied in the biometrics, creating parity-code, a locking stage hash code computation performed on the biometric modalities, and an unlock stage where the parity-code is regenerated using XORCoding. Experimental analysis confirms the superiority of multimodal cryptosystems and decision-level fusion.

The Toli and Preneel (Toli and Preneel, 2018) work uses a pseudo-identity authentication recorder of a bank's client. With a client's PIN code, the package is encrypted and stored in the device, being discarded the biometrics and the PIN. For secure requirements, the proposed use the ISO biometric, financial, and cryptographic device standards.

Kaur and Khanna (Kaur and Khanna, 2019) proposed a random distance method. Considering multimodal cancelable biometric template approach, it generates a *discriminative and privacy-preserving revocable pseudo-biometric identities*. The security analysis shows some resistant to some attacks.

## 2.2 Interoperability Network

Interoperability between biometric data is discussed in Tolosana et al. and Mason et al. (Tolosana et al., 2015; Mason et al., 2014). However, regarding system interoperability, the ANSI/NIST proposal (Mangold, 2016) and IEEE BOPS (IEEE, 2019) should be considered relevant references. For this paper, we will depart from the ANSI/NIST package and will improve the IEEE BOPS method.

The IEEE BOPS is a standard that enables interoperability independent of the underlying system. The proposed architecture is built using neutral languages. It is based on a client/server authentication with software running on a mobile system. There are some formats, including JSON requests and responses, that addresses the interoperability among those devices.

The fact that the IEEE BOPS mechanism is not complete about checking communication integrity is a problem. As IEEE BOPS, we will show that our sys-

tem has better security characteristics, and a complete workflow to address different biometric systems. That includes dealing with a time-out or bad connection among systems, check the status for the identification of biometric procedures, and message acknowledgments between the systems.

# 3 THE PROPOSED SCHEME

In this section, we describe our work. We will explain the IDN encrypted scheme, the biometric operating network running two different technologies, and the communication protocol. This network is currently operational in a real government system.

## 3.1 IDN: The Encrypted Index Register for Biometric Databases

The IDN generation scheme uses the SN, the k stored in a non-exportable HSM slot (|k| = 256 bits), the AES-256 algorithm in CBC mode, with a random, and locally calculated iv, and the SHA256 hash functions, for checksum, as follows:

- The SN is expanded by concatenation by itself until it gets a 256-bit length; we concatenate k and SN expanded, resulting 512-bit string (y); then, we get x = SHA256(y), a 256-bit string; after, we divide x in two halves, letting A be the first 128 bits and B the trailing ones; and finally iv = A⊕B;
- The SN padded with 128 bits is AES-256-CBC encrypted using k, feasible to be locally calculated for the BSP, as the iv is not transmitted over the network. This yields z, an encrypted 128-bit string;
- Then, SHA256(z) is calculated and concatenated with SHA256(SHA256(z)), for checksum; the previous result is BASE64-encoded (Josefsson, 2006) to generate the IDN.

Any BSP, with k, can reach the same IDN for only one SN, but the IDN becomes irreversible as soon it leaves the HSM. The premise of using the non-exportable key attribute, within HSM leased in an audit secure environment, makes it easy to identify any misuse or key compromised. There is also internal protection of the information, which benefits segments that have issues in sharing their client's information.

### 3.1.1 Export and Import the Secret Key

For this work, we generate a 256-bit random symmetric secret key k into a offline HSM. The exporting of k is done using an OpenSSL library[1]. We export k by wrapping it with the public keys of the BSP HSM in the network, producing one cryptographic envelope per each HSM, containing k. In this way, only the HSM that owns the respective private key can unwrap the envelope. A local audit ceremony imports the secret key into the HSM with the "no export" feature that guarantees it cannot be taken or copied from the slot anymore, just used. For this purpose we use the public key encryption RSA-2048-OAEP padding (Moriarty et al., 2016; Bellare and Rogaway, 1995) to export k.

## 3.2 The Biometric Network

The first step of Figure 1 is the *enrollment process*, which uses fingerprint and face sensors. The *enrollment process* prepares an ANSI/NIST Package 1, with a secure proprietary biometric template and the biographical information of the person. The Package 1 is sent through a mutually authenticated TLS/SSL channel for the system *Network 1*.

At the system *Network 1*, in the *client/server interface*, the biographical SN is replaced into the HSM by the encrypted index IDN. An ANSI/NIST Package 2 is built and includes a Transaction Code Number (TCN) based on Universal Time Coordinated (UTC). In the core of the system *Network 1* (*Bio API and Engine*) begins the local identification process. In the *directory service*, it is checked if the IDN is already in the base, without decrypting it. If IDN exists, the *Bio API and Engine* checks if there is only one owner or other. If it is only one, it performs the 1:1 verification process (if positive, ends the process with a "verification ok"; if not, performs the following); if not the only owner, it must inform the *enrollment processes* that there is something to be treated, possibly a fraud.

The *Bio API and Engine* initiates the identification 1:n process in case no IDN found. If there is some exception (biometric found associated with other IDN), it reports for the *enrollment process* that there is something to be treated, possibly a fraud. If not, the *HUB service* prepares a JSON message, attaching the encrypted ANSI/NIST IDE packet with the BSP receiver's public key and the IDN. The fingerprint and face images are not a proprietary biometric template anymore, but a wrap RSA-OAEP-2048-bit encrypted bits that can only be opened by the receiving BSP. Through a mutually authenticated SSL/TLS channel between the BSP, this encrypted packet is sent to *Network 2*, which initiates the same local biometric identification 1:n. If some irregularity is found, the receiving BSP sends back a JSON message with an

[1] https://www.openssl.org/

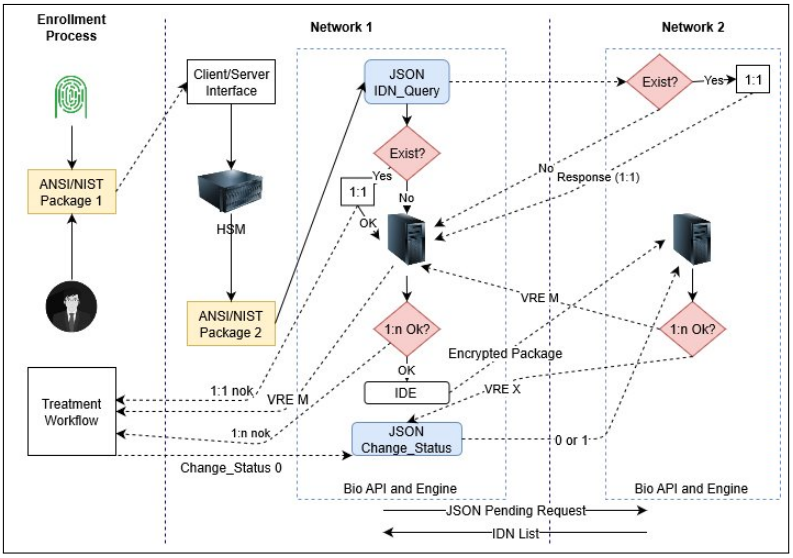


Figure 1: Biometric Service Providers Network Diagram.

ANSI/NIST `VRE` with `M` value, informing that there is something to be verified, possibly a fraud. If not, a JSON message with an ANSI/NIST `VRE` with `X` value is sent, informing that everything is "ok" and the IDN can be stored.

Shortly after receiving the "ok" information, the issuing BSP sends an acknowledgment JSON message `change_status` to the network, informing that the IDN can be stored. Also, the network have the `pending_operation` mechanism, that checks if one BSP has any process to be made, but for somehow was not able to performer it on-line.

## 3.3 The Communication Protocol

### 3.3.1 Network and HTTPS Messages

Requests for *HUB services* must follow the asynchronous pattern. All responses must be returned by the HUB that received the request when it has the available information. The requests must use the `POST` method, containing only the ANSI/NIST file in the request body.

Requests for *directory services* must follow the synchronous pattern. All responses must be returned in the same request/response. The requests must use the `POST` method.

### 3.3.2 JSON Messages Standards and Formats

The JSON messages will be described.

- JSON IDN query operation: Checks if IDN code is registered in the network. The response for the registered IDN is a JSON package, figuring out which fingerprints and face are registered (TRUE|FALSE), along with the related IDN.
- JSON Pending operations listing operation: It reveals, in the event of any contingency with a biometric system (time-out, bad connection or maintenance), a list of IDN that requires further processing. Hourly, a JSON type is sent to ensure that all processes have been executed, holding integrity through the network.
- JSON Change status notification operation: This operation notifies BSP if a record, with its IDN, was completed or there was some error.

## 3.4 Benchmarking

There are some works with security evidence and anonymity of the index register into a biometric database and network. As we showed, using cryptographic techniques along with biometrics systems is not new, but up to our best knowledge, shown in Table 1, it had not been used to guarantee privacy with security evidence and interoperability to the data. Our main contribution is the construction of a non-reversible cryptographic index that can safely traverse the network of connections between biometric systems.

Table 1: Benchmarking.

| Works | Security and privacy biometric data approach | Security and privacy biographical data approach | Security evidence against known database or network attacks | Interoperability |
|---|---|---|---|---|
| (Nasir and Perumal, 2013) | YES | YES | NO | NO |
| (Li et al., 2015) | YES | NO | YES | NO |
| (Kumar and Kumar, 2016) | YES | NO | YES | NO |
| (Toli and Preneel, 2018) | YES | YES | NO | NO |
| (Kaur and Khanna, 2019) | YES | NO | YES | NO |
| Our proposed scheme | YES | YES | YES | YES |

# 4 SECURITY ANALYSIS

This section is divided into three areas of security analysis (Katz and Lindell, 2007). The first and the second are focused on cryptoanalysis, mainly on the randomness of the secret key and semantic security. The third one is based on the operational security of the network.

## 4.1 Randomness of the Secret Key

For the first proof that the proposed scheme is secure, we tested the randomness of keys that are generated by HSM of the third reliable offline party. We use the NIST Special Publication 800-90B - Recommendation for Random Number Generation Using Deterministic Random Bit Generators (Turan et al., 2018). We compiled the "make iid" and "make non_iid" tests using the "libdivsufsort-dev / libbz2-dev" dependencies, with a Ubuntu 18.04 operation system.

The results are:

```
NIST IID test
./ea_iid -i keys.bin
Calculating baseline statistics...
H_original: 7.886548
H_bitstring: 0.998301
min(H_original, 8 X H_bitstring):
7.886548
** Passed chi square tests
** Passed length of longest
repeated substring test
Beginning initial tests...
Beginning permutation tests... these
may take some time
** Passed IID permutation tests

NIST Non-IID test
./ea_non_iid -i keys.bin
Running non-IID tests...
Running Most Common Value Estimate...
Running Entropic Statistic Estimates
(bit strings only)...
Running Tuple Estimates...
Running Predictor Estimates...
H_original: 7.718814
H_bitstring: 0.932005
min(H_original, 8 X H_bitstring): 7.456043
```

The result demonstrates that the official NIST test suite approves the randomness of the keys (k) that are generated from the proposed scheme.

## 4.2 Semantic Security

*Challenge:* The BSP must find a secure way to generate the same IDN for the same SN.

Supposing that we do not have any random input of the block entrance, the birthday attack can be used against non-Feistel ciphers (Schramm et al., 2004). The encryption could be broken with not too much effort (e.g., exhaustion of fewer than 65,000 tests - 15-bit exhaustion - would lead to its probability of inferring any SN from the cipher to very high values).

To proof that the IDN scheme is secure enough for any $\mathcal{A}$, we must start by explaining the calculated iv created. First, we concatenate, for this research, the 88-bit SN string, which have 4-bit entropy for each octet block, until 256-bit length, with the 256-bit k, resulting in a 512-bit length. We use the entropy of SHA-256 to one way 256-bit string, leading a $log_2((1-1/e)*2^{256})$ outputs (Bellare and Kohno, 2004). A bitwise XOR-ed is used with equal parts of the SHA-256 result, leading a 128-bit random iv. Because $\mathcal{A}$ cannot have control of the input bits calculated on the iv, the computational cost effort to find a collision is around $2^{n/2}$ (Dobraunig et al., 2015), n = output bits, leading to unfeasible known polynomial-time attacks between the SN to IDN or IDN to SN.

Our 128-bit padding SN plaintext, it is XOR-ed with a 128-bit random iv. Instead of rebooting the encrypted AES-256-CBC with the previous outcome and an initialization public vector (IV), we recalculate the block entrance of the AES-256-CBC encryp-

tion with a 128-bit random and local iv, derived from known parameters (K and SN) only for the BSP. This leads to an entropy effort of $256 + log_2(1e9)$ bits. These random bits scattering on the input makes the system unfeasible to known polynomial-time attacks, holding anonymity.

There are others attacks in the literature that are avoided:

- Padding Oracle Attacks (Kang et al., 2016): all the SN padded block is XOR with 128-bit string, local and random iv created, avoiding this attack;
- Chosen Ciphertext Attacks (Rogaway, 2011): the proposed iv is not sent over the network, it works only within the cryptography module of the HSM. So, $\mathcal{A}(\texttt{iv} \oplus t, AES(\texttt{SN}))$ cannot be enforcement;
- Chosen Plaintext Attacks (Rogaway, 2011): the iv can not be predictable by $\mathcal{A}$, i.e., the proposed AES-256-CBC cannot be attacked in polynomial-time, as shown. Because the calculations are done into accredited HSM, this also avoids adaptive-CPA (Ding et al., 2019).
- Timing Attacks (Kocher, 1996): the HSM of the BSP implements cryptographic calculations in a constant-time, accredited with FIPS test suite (Schaffer, 2019).

For exporting k from the offline HSM, we use RSA-2048-OAEP-wrap operation. Each BSP sends its own HSM public key for these operations. By the known literature, this RSA-2048-OAEP calculus has IND-CPA-security and IND-CCA1/CCA2-security (Boldyreva and Fischlin, 2006), which makes the calculation semantically secure. Using index calculus NFS (Number Field Sieve), the published literature describes that the cost to break RSA-2048 is $2^{112}$ (Bernstein and Lange, 2014), which turns out to be unfeasible in polynomial-time for $\mathcal{A}$. We use the same wrap operation to the ANSI/NIST encrypted package between BSP, for additional security.

### 4.3 Operation Security

After the cryptoanalysis, we face the attacks that could be done in the network. It is essential to state that the wrapped k is imported in a local ceremony at the security environment of the BSP.

Accredited HSM (Schaffer, 2019) does not allow any copy or misuse of the non-exportable k. Other security features of the HSM embedded in the network are IDS (Intrusion Detection System), non-physical, mechanical, chemical violability, and SQL injection protection (Wenqian Yu et al., 2016). Within the biometric network, we use a TLS/SSL (RSA-2048-bit) mutually authenticated for all communication. A reliable entity informs for each BSP the certificates and URL end-points. Further, dedicated firewalls are only from the IPs of each BSP, also audit by a trusted reliable party. Each biometric file has the origin and destination name of the BSP given on the certificate.

Thereby, Distributed DoS attacks are mitigated in this network (Yan et al., 2016). In addition to every network part mentioned, BSP set one random session key per transaction and also have a timestamp for each file sent. This scenario mitigates any replays attacks (Ding et al., 2018).

## 5 RESULTS

The results were obtained using data acquired into the operational BSP network. First, we show the IDN scheme created, indicating the calculations needed to generate an IDN. Second, we demonstrate the communication protocol logs, working for an identification purpose ("IDE") between two distinct networks in a time interval.

### 5.1 The IDN Scheme

The IDN scheme:

Algorithm 1: IDN algorithm.

**Data:** SN, K
**Result:** IDN
$SNEXT =$ "$\$SNhex\$SNhex\$SNhex''$
$y =$ "$\$K\$SNEXT''$
$\mathsf{H}(y) = x$
$x \in \{0,1\}^{256}$
$A \in (x^0, x^1, ..., x^{127})$
$B \in (x^{128}, x^{129}, ..., x^{255})$
$iv = A \oplus B$
$DataHex = \$\{\#SNhex\}$
$BlockPadded = \$(((32 - \$DataHex)/2))$
$blockSN =$ "$\$SNhex''$
$tmp = \$(printf'\%02x'\$BlockPadded)$
**for** *((i=0; i < $BlockPadded; i++ ))* **do**
  $blockSN =$ "$\${blockSN}\${tmp}$"
**end**
$AES\text{-}256\text{-}CBC(blockSN, K, iv) = ID$
$\mathsf{H}(ID) = IDbase$
$\mathsf{H}(IDbase) = IDCheck$
$IDNhex = (\$IDbase\$IDCheck)$
$IDN = Encode64(IDNhex)$

Table 2 presents the IDN calculations, from Algorithm 1. Those are made, step by step, buy using a SN and k, generated from the HSM of the entity, for experimental purpose. It is possible to conclude from the calculations that only with k and SN it is possible

Table 2: IDN calculations.

| Parameter | Values and Results |
|---|---|
| K | ffd62502b336b5c5784813e310412438bb 91a45aade63aafff76154016d291fc |
| SN | 00000000001 |
| SHA256 (K\|\|(SN:SN:SN)) | b72c3caf4dfa7468b6db5752310939f0a5 67f084dd66c19b9e77e3ce3e76f43d |
| iv | 124bcc2b909cb5f328acb49c0f7fcdcd |
| Input Block | 30303030303030303030310505050505 (padding) |
| ID | f0de00ed3a0c0569243d6d1924d8be25 |
| IDbase | 8N4A7ToMBWkkPW0ZJNi+JQ== |
| SHA256(IDbase) | 4fc25d068b5661e7e5578ad4a20e3e3f ce0c6a86fc7b0772a3988ca20b0beebf |
| SHA256 (SHA256(IDbase)) | 27d3f2d0113b96d039f96401a431f189 ce52c2268e12bc9c86b08f0b986f9ead |
| IDN | T8JdBotWYeflV4rUog4+P84Maob8ewd yo5iMogsL7r8n0/LQETuW0Dn5Z AGkMfGJzlLCJo4SvJyGsI8LmG+erQ== |

to reach the IDN. In the next subsection, we will show a real `SN`, shown as IDN, in this operation biometric network.

## 5.2 The Operation Communication Protocol

Based on the protocol created, shown in Section 3, we present the network communications by following a log trail for an `IDE` (identification) purpose. This communication is extracted from a real operational network, between *Network 1* and *Network 2*, with a real and irreversible IDN.

### 5.2.1 Log Trail

We show the core of a communication protocol for a `pending_operation`, an `IDE`, and a `change_status` messages, suppressing some log messages to make it clearer to explain. The encrypted ANSI/NIST biometric package is attached, for identification purpose.

```
psbio-19-09-2019-10.log.gz:[2019-09-19
21:08:10.209] 3.1.12 INFO 187
server.service.DirectoryService -
[DIR:RECEIVED] FROM=``bsp2"; REQUEST=
{"requestType": "pending_operations"}
psbio-19-09-2019-10.log.gz:[2019-09-19
21:08:17.376] 3.1.12 INFO 187
server.service.DirectoryService
- [DIR:SENT] TO=``bsp2"; RESULT=
{"pendingOperationsList":[{"operationType":
"1_n_queue","idnList":,"idnList":[{"idn"
:"RekIJzYwMUwEE9RMSThy7kwV1SR884EC1g29VdPNzD
jM5yjAffg8X+To5tlm4p/7D/9/6W2FVJTavAORlYkAo
w==","tcn":"77a538fd-8ebe-4bdf-8d39-0ea517b1
f491"}]}]}
```

The `pending_operation` mechanism ensures that every service provider processes all data. By request, the issuing BSP receives from other providers all the IDN/TCN that were not processed. This command allows the network to be integrated all the time.

```
[2019-09-18 17:17:04.559] - [HUB:SENT]
TO=``bsp2";TRANSACTION={"transaction-type"
:"IDE","idn":"L3dipU0xsnNJ1qInrbh0QCcQH7QWDN
q6IquiMv1CBhSl5WsYwoyu3xe14TMojzwyJTNjH7xxI
ysA0ETyo6gW0g==","tcn":"9F925749-ADDE-408E-
B421-3C8374E33237","timestamp":"1568837824559"}

[2019-09-18 17:35:28.596] - [HUB:RECEIVED]
FROM=``bsp2";TRANSACTION=
{"transaction-type":"VRE","idn":"L3dipU0xsn
NJ1qInrbh0QCcQH7QWDNq6IquiMv1CBhSl5WsYwoyu
3xe14TMojzwyJTNjH7xxIysA0ETyo6gW0g==","tcn":
"02FA798D-D81F-43DB-9E44-32489389C470",
"timestamp":"1568838928596","reference-tcn":
"9F925749-ADDE-408E-B421-3C8374E33237","srf"
:"X"}

[2019-09-18 18:02:32.830] - [HUB:SENT]
TO=``bsp2"; REQUEST={"requestType":
"change_status","statusCode":"1","idn":
"L3dipU0xsnNJ1qInrbh0QCcQH7QWDNq6IquiMv1C
BhSl5WsYwoyu3xe14TMojzwyJTNjH7xxIysA0ETy
o6gW0g=="}
```

It is possible to interpret that the `IDE` request was made for the encrypted IDN "L3dipU...", which response was a `VRE` with `X` value, *i.e.*, no biometrics were found in the biometric database. Then, the issuing system sent a `change_status` acknowledge message, completing the registration process.

# 6 CONCLUSIONS

In this work, we proposed a new approach scheme that guarantees the anonymity of anyone within biometric databases and still allows them to communicate securely. Symmetric cryptography techniques and known communication protocols were used to

achieve privacy, with security evidence and interoperability integrity between biometric networks. We successfully showed that, for the same input data and secret key among systems, we produced an anonymous index register into all databases representing a person. Also, we improved the IEEE BOPS standard by constructing a framework for JSON messages between systems, including a way of networks to maintain operations regardless of the contingencies. As future works, we could generate IDN for any government database that needs privacy, security, and interoperability. This future work is an immediate outcome of the contributions we made to enhance the security, and also, of the shared anonymous record index we built.

# REFERENCES


Bellare, M. and Kohno, T. (2004). Hash function balance and its impact on birthday attacks. In Cachin, C. and Camenisch, J. L., editors, *Advances in Cryptology - EUROCRYPT 2004*, pages 401–418, Berlin, Heidelberg. Springer Berlin Heidelberg.

Bellare, M. and Rogaway, P. (1995). Optimal asymmetric encryption. In De Santis, A., editor, *Advances in Cryptology — EUROCRYPT'94*, pages 92–111, Berlin, Heidelberg. Springer Berlin Heidelberg.

Bernstein, D. and Lange, T. (2014). Batch NFS. In Joux, A. and Youssef, A., editors, *Selected Areas in Cryptography – SAC 2014: 21st International Conference, Montreal, QC, Canada, August 14-15, 2014, Revised Selected Papers*, Lecture Notes in Computer Science, pages 38–58, Germany. Springer.

Boldyreva, A. and Fischlin, M. (2006). On the security of oaep. In Lai, X. and Chen, K., editors, *Advances in Cryptology – ASIACRYPT 2006*, pages 210–225, Berlin, Heidelberg. Springer Berlin Heidelberg.

Bray, T. (2017). The JavaScript Object Notation (JSON) Data Interchange Format. RFC 8259.

Campisi, P. (2013). *Security and Privacy in Biometrics*. Springer Publishing Company, Incorporated.

Dang, Q. (2015). Secure Hash Standard (SHS). Federal Information Processing Standards Publication FIPS Pub 180-4, pub-NIST, pub-NIST:adr.

Ding, D., Han, Q.-L., Xiang, Y., Ge, X., and Zhang, X.-M. (2018). A survey on security control and attack detection for industrial cyber-physical systems. *Neurocomputing*, 275:1674–1683.

Ding, Y., Shi, Y., Wang, A., Zheng, X., Wang, Z., and Zhang, G. (2019). Adaptive Chosen-Plaintext Collision Attack on Masked AES in Edge Computing. *IEEE Access*, 7:63217–63229.

Dobraunig, C., Eichlseder, M., and Mendel, F. (2015). Analysis of SHA-512/224 and SHA-512/256. In *Proceedings, Part II, of the 21st International Conference on Advances in Cryptology — ASIACRYPT 2015 - Volume 9453*, pages 612–630, Berlin, Heidelberg. Springer-Verlag.

Dwork, C. (2006). Differential Privacy. In *Proceedings of the 33rd International Conference on Automata, Languages and Programming - Volume Part II*, ICALP'06, pages 1–12, Berlin, Heidelberg. Springer-Verlag.

Dworkin, M. J. (2001). SP 800-38A 2001 Edition. Recommendation for Block Cipher Modes of Operation: Methods and Techniques. Technical report, Gaithersburg, MD, United States.

Hirano, T., Ito, T., Kawai, Y., Matsuda, N., Yamamoto, T., and Munaka, T. (2016). A practical attack to AINA2014's countermeasure for cancelable biometric authentication protocols. In *2016 International Symposium on Information Theory and Its Applications (ISITA)*, pages 315–319.

IEEE (2019). IEEE Standard for Biometric Open Protocol, Redline. *IEEE Std 2410-2019 (Revision of IEEE Std 2410-2017), Redline*, pages 1–134.

Jain, A. K., Nandakumar, K., and Ross, A. (2016). 50 years of biometric research: Accomplishments, challenges, and opportunities. *Pattern Recognition Letters*, 79:80–105.

Josefsson, S. (2006). The Base16, Base32, and Base64 Data Encodings. RFC 4648.

Kang, H., Park, M., Moon, D., Lee, C., Kim, J., Kim, K., Kim, J., and Hong, S. (2016). New efficient padding methods secure against padding oracle attacks. In Kwon, S. and Yun, A., editors, *Information Security and Cryptology - ICISC 2015*, pages 329–342, Cham. Springer International Publishing.

Katz, J. and Lindell, Y. (2007). *Introduction to Modern Cryptography (Chapman & Hall/Crc Cryptography and Network Security Series)*. Chapman & Hall/CRC.

Kaur, H. and Khanna, P. (2019). Random Distance Method for Generating Unimodal and Multimodal Cancelable Biometric Features. *IEEE Transactions on Information Forensics and Security*, 14:709–719.

Kocher, P. C. (1996). Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems. In *Proceedings of the 16th Annual International Cryptology Conference on Advances in Cryptology*, CRYPTO '96, pages 104–113, London, UK, UK. Springer-Verlag.

Kumar, A. and Kumar, A. (2016). A Cell-Array-Based Multibiometric Cryptosystem. *IEEE Access*, 4:15–25.

Li, C., Hu, J., Pieprzyk, J., and Susilo, W. (2015). A New Biocryptosystem-Oriented Security Analysis Framework and Implementation of Multibiometric Cryptosystems Based on Decision Level Fusion. *IEEE Transactions on Information Forensics and Security*, 10(6):1193–1206.

Mangold, K. (2016). Data Format for the Interchange of Fingerprint, Facial and Other Biometric Information ANSI/NIST-ITL 1-2011 NIST Special Publication 500-290 Edition 3. Number 500-290e3.

Mason, S., Gashi, I., Lugini, L., Marasco, E., and Cukic, B. (2014). Interoperability between Fingerprint Biometric Systems: An Empirical Study. In *2014 44th*

*Annual IEEE/IFIP International Conference on Dependable Systems and Networks*, pages 586–597.

Moriarty, K., Kaliski, B., Jonsson, J., and Rusch, A. (2016). PKCS #1: RSA Cryptography Specifications Version 2.2. RFC 8017.

Nasir, M. and Perumal, P. (2013). Implementation of Biometric Security using Hybrid Combination of RSA and Simple Symmetric Key Algorithm. *International Journal of Innovative Research in Computer and Communication Engineering*, 3297.

Natgunanathan, I., Mehmood, A., Xiang, Y., Beliakov, G., and Yearwood, J. (2016). Protection of Privacy in Biometric Data. *IEEE Access*, 4:880–892.

Ngo, D. C. L., Teoh, A. B. J., and Hu, J. (2015). *Biometric Security*. Cambridge Scholars Publishing, United Kingdom.

Quan, F., Fei, S., Anni, C., and Feifei, Z. (2008). Cracking Cancelable Fingerprint Template of Ratha. In *2008 International Symposium on Computer Science and Computational Technology*, volume 2, pages 572–575.

Rescorla, E. (2000). HTTP Over TLS. RFC 2818.

Rogaway, P. (2011). Evaluation of Some Blockcipher Modes of Operation. Evaluation carried out for the Cryptography Research and Evaluation Committees (CRYPTREC) for the Government of Japan.

Ross, A., Shah, J., and Jain, A. K. (2007). From Template to Image: Reconstructing Fingerprints from Minutiae Points. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 29(4):544–560.

Schaffer, K. B. (2019). Security Requirements for Cryptographic Modules. Federal Information Processing Standards Publication FIPS Pub 140-3, pub-NIST, pub-NIST:adr.

Schramm, K., Leander, G., Felke, P., and Paar, C. (2004). A collision-attack on aes. In Joye, M. and Quisquater, J.-J., editors, *Cryptographic Hardware and Embedded Systems - CHES 2004*, pages 163–175, Berlin, Heidelberg. Springer Berlin Heidelberg.

Toli, C.-A. and Preneel, B. (2018). Privacy-preserving biometric authentication model for e-finance applications. In *ICISSP*.

Tolosana, R., Vera-Rodriguez, R., Ortega-Garcia, J., and Fierrez, J. (2015). Preprocessing and Feature Selection for Improved Sensor Interoperability in Online Biometric Signature Verification. *IEEE Access*, 3:478–489.

Turan, Meltem S.and Barker, E. B., Kelsey, J.and McKay, K., Baish, M., and Boyle, M. (2018). SP 800-90B Recommendation for the Entropy Sources Used for Random Bit Generation. Technical report, Gaithersburg, MD, United States.

Wenqian Yu, Weigang Li, Junyuan Wang, and Changzheng Wei (2016). A study of HSM based key protection in encryption file system. In *2016 IEEE Conference on Communications and Network Security (CNS)*, pages 352–353.

Yan, Q., Yu, F. R., Gong, Q., and Li, J. (2016). Software-Defined Networking (SDN) and Distributed Denial of Service (DDoS) Attacks in Cloud Computing Environments: A Survey, Some Research Issues, and Challenges. *IEEE Communications Surveys Tutorials*, 18(1):602–622.