Chapter 12

BLOCK CODING SCHEMES DESIGNED FOR BIOMETRIC AUTHENTICATION

Vladimir B. Balakirsky, Anahit R. Ghazaryan, A. J. Han Vinck*
Institute for Experimental Mathematics, Ellernstr. 29, 45326 Essen, Germany

Key Words: encoding, decoding, authentication, cryptography

1. Coding approaches to a general biometric authentication problem

Let us consider the following mathematical problem. Suppose that

$$\mathbf{b} = (b_1, \ldots, b_n),\ \mathbf{b}' = (b'_1, \ldots, b'_n) \in \{0,1\}^n$$

are given binary vectors of length n. The verifier has to make the acceptance decision if the Hamming distance between these vectors $d(\mathbf{b}, \mathbf{b}')$ does not exceed a given threshold T and the rejection decision otherwise:

– *if* $d(\mathbf{b}, \mathbf{b}') \le T$, *then accept the identity claim* (Y)*;*
if $d(\mathbf{b}, \mathbf{b}') > T$, *then reject the identity claim* (N)*,*

*E-mail address: v.b.balakirsky@rambler.ru

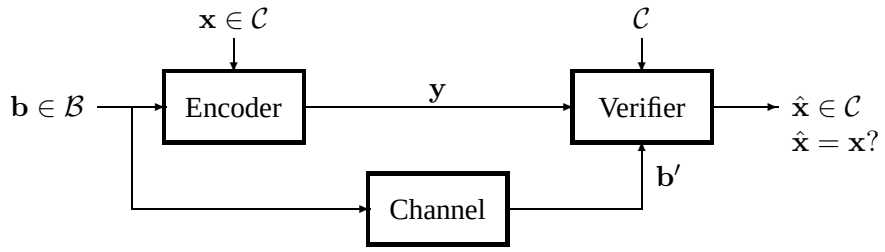


Figure 1. General authentication scheme.

"The identity claim" in the description above appears because we assume that the vectors $\mathbf{b}$ and $\mathbf{b}'$ contain outcomes of measurements of some biometric parameters of two people. The verification is understood as a procedure, which checks whether the difference between the results is caused by the observation noise or by the fact that people are different.

The difficulties in the implementation of the scheme above are due to the point that the vector $\mathbf{b}$ containing the outcomes of sample measurements of a person has to be hidden from an attacker, who tries to present a vector $\mathbf{b}'$ leading to the acceptance decision. A possible solution to the hiding problem is the use of a cryptographic "one–way" hash function Hash where we assume that the value of the function can be easily computed for a given argument, but the value of the argument is hard to get for a given value of the function. If only $\mathrm{Hash}(\mathbf{b})$ is known to the verifier, then he can compute the values of $\mathrm{Hash}(\mathbf{b}' \oplus \mathbf{e})$ for all binary vectors $\mathbf{e} \in \{0,1\}^n$ of the Hamming weight at most T and make the acceptance decision if one of them is equal to $\mathrm{Hash}(\mathbf{b})$, where $\oplus$ denotes the component–wise sum modulo 2. Such a scheme is secure up to the security of hashing, but requires the hash function to be defined over 2^n binary vectors and calculations with $\sum_{i=0}^{T} \binom{n}{i}$ noise vectors. The block coding schemes are introduced to relax these requirements.

The coding problem for biometric authentication can be presented as designing codes for the scheme in Figure 1. Let $\mathcal{B}$ and $\mathcal{C}$ be subsets of binary vectors of length n. The set $\mathcal{B}$ is the set of biometric vectors, and the probability distribution

$$(\Pr_{\text{bio}}\{\, B = \mathbf{b}\,\},\ \mathbf{b} \in \mathcal{B}\,)$$

is known. The entries of the set $\mathcal{C}$ are codewords assigned by the designer. The encoding is the transformation of a pair $(\mathbf{x}, \mathbf{b}) \in \mathcal{C} \times \mathcal{B}$, where the vector $\mathbf{b}$ is generated by the source and $\mathbf{x}$ is chosen according to a uniform probability distribution over the code $\mathcal{C}$, to another vector $\mathbf{y}$. This vector and the value of $\mathrm{Hash}(\mathbf{x})$ are stored in the database under the name of the person whose biometric characteristics are expressed by the vector $\mathbf{b}$. Having received a vector $\mathbf{b}'$ and the name of the person, the decoder reads $(\mathbf{y}, \mathrm{Hash}(\mathbf{x}))$ from the database and uses the error–correcting capabilities of the code to decode "the transmitted codeword" If $\mathrm{Hash}(\hat{\mathbf{x}}) = \mathrm{Hash}(\mathbf{x})$, where $\hat{\mathbf{x}} \in \mathcal{C}$ is the decoded codeword, then the identity claim is accepted; otherwise, the identity claim is rejected. The scheme satisfies the constraints

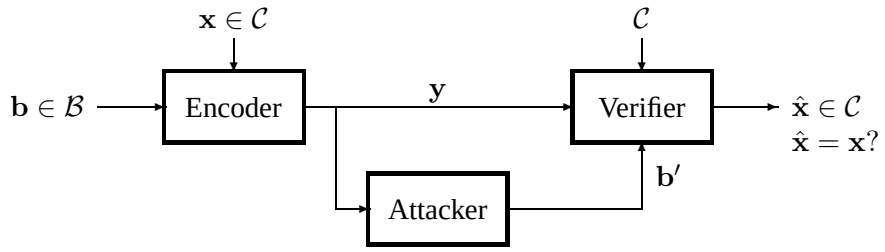


Figure 2. General authentication scheme from the attacker's prospective.

formulated above if, for all $\mathbf{b} \in \mathcal{B}$, $\mathbf{b}' \in \{0,1\}^n$, and $\mathbf{x} \in \mathcal{C}$,

$$\begin{cases} d(\mathbf{b}, \mathbf{b}') \le T & \Rightarrow \quad \hat{\mathbf{x}} = \mathbf{x}, \\ d(\mathbf{b}, \mathbf{b}') > T & \Rightarrow \quad \hat{\mathbf{x}} \ne \mathbf{x}. \end{cases} \tag{1}$$

From the attacker's prospective, the authentication scheme can be viewed as the scheme in Figure 2. The attacker reads the content of the database associated with a person, presents the name of the person and generates a vector $\mathbf{b}'$. The goal of the attacker is generating the vector leading to the verifier's acceptance decision. The coding problem can be formulated as constructing codes that simultaneously satisfy the constraints (1) and guarantee a low probability of the attacker's success. A more precise formulation of the problem will be presented in the corresponding subsections where we consider the additive and the permutation block coding schemes. Before this material is presented, we describe and analyze a direct authentication scheme, since its characteristics bring the best possible performance of the verifier.

In the following considerations, χ denotes the indicator function: $\chi\{\mathcal{S}\} = 1$ is the statement $\mathcal{S}$ is true and $\chi\{\mathcal{S}\} = 0$ otherwise. The Hamming weight of a binary vector $\mathbf{b}$ is denoted by $\mathrm{wt}(\mathbf{b})$.

2. Direct authentication scheme

2.1. Notation

Suppose that $\mathcal{B} = \{0,1\}^n$. For all $\mathbf{b} \in \{0,1\}^n$, let

$$\mathcal{D}^{(T)}(\mathbf{b}) \stackrel{\triangle}{=} \left\{ \mathbf{b}' \in \{0,1\}^n : \mathrm{wt}(\mathbf{b} \oplus \mathbf{b}') \le T \right\} \tag{2}$$

denote the set of biometric vectors located at distance T or less from the vector $\mathbf{b}$. If $\mathbf{b}$ and $\mathbf{b}'$ are the vectors processed at the enrollment and the authentication stages, respectively, and $\mathbf{b}' \in \mathcal{D}^{(T)}(\mathbf{b})$, then the verifier has to make the acceptance decision. The probability that the biometric vector generated independently of the vector $\mathbf{b}$ is equivalent to this vector

from the the verifier's point of view is equal to

$$Q_{\text{bio}}^{(T)}(\mathbf{b}) \stackrel{\triangle}{=} \sum_{\mathbf{b}' \in \mathcal{D}^{(T)}(\mathbf{b})} \Pr_{\text{bio}}\{B = \mathbf{b}'\}. \tag{3}$$

Let us denote

$$Q_{\text{bio}}^{(T)} \stackrel{\triangle}{=} \max_{\mathbf{b}} Q_{\text{bio}}^{(T)}(\mathbf{b}) \tag{4}$$

and introduce the sets

$$\mathcal{B}^{(T)} \stackrel{\triangle}{=} \left\{ \mathbf{b}^* : Q_{\text{bio}}^{(T)}(\mathbf{b}^*) = Q_{\text{bio}}^{(T)} \right\}, \tag{5}$$

$$\mathcal{D}^{(T)} \stackrel{\triangle}{=} \bigcup_{\mathbf{b}^* \in \mathcal{B}^{(T)}} \mathcal{D}^{(T)}(\mathbf{b}^*). \tag{6}$$

Let the noisy observations of the biometric vector $\mathbf{b}$ be specified by the conditional probability distribution

$$(\Pr_{\text{err}}\{ B' = \mathbf{b}' \,|\, B = \mathbf{b} \},\ \mathbf{b}' \in \{0,1\}^n)$$

in such a way that

$$\mathbf{b}' \notin \mathcal{D}^{(T)}(\mathbf{b}) \ \Rightarrow\ \Pr_{\text{err}}\{ B' = \mathbf{b}' \,|\, B = \mathbf{b} \} = 0. \tag{7}$$

Calculation of probabilities $Q_{\text{bio}}^{(T)}(\mathbf{b})$, $\mathbf{b} \in \{0,1\}^n$, is illustrated in Table 1 for $n = 4$. In this case, $\mathcal{B}^{(0)} = \{0000\}$ and $\mathcal{B}^{(1)} = \{1000, 1110\}$. Suppose that there is an attacker (a guesser), who wants to present a vector $\mathbf{b}'$ maximizing the probability that the verifier makes the acceptance decision considered as a success. If $T = 0$, then the guesser has to present the vector 0000, and the probability of success is equal to 0.25. If $T = 1$, then he has to present one of two vectors, 1000 or 1110, and the probability of success is equal to 0.48. Notice that the biometric vectors 1010 and 1100 are included into both guesses. Therefore, if the guesser would present both 1000 and 1110 as guesses, then the probability of success is computed as $0.96 - 0.07 - 0.13 = 0.76$.

2.2. Description of the scheme

Processing of a given biometric vector $\mathbf{b}$ at the enrollment stage and processing data at the authentication stage is illustrated in Figure 3.

The enrollment stage.

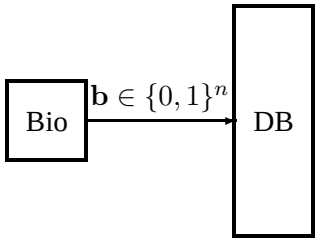
– *Store the biometric vector* $\mathbf{b}$ *in the database.*

The authentication stage.

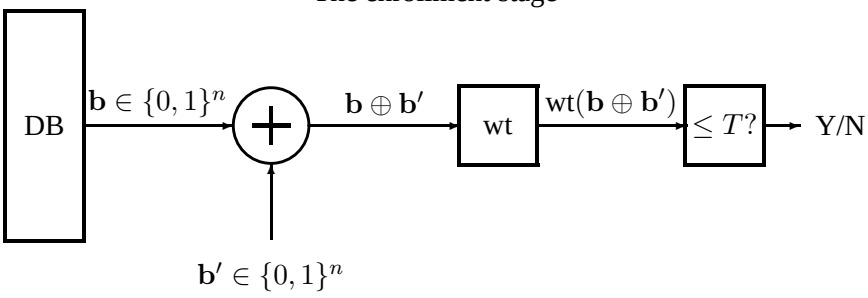
– *Read the biometric vector* $\mathbf{b}$ *associated with the claimed person from the database. If* $\text{wt}(\mathbf{b} \oplus \mathbf{b}') \le T$, *then make the acceptance decision* (Y). *If* $\text{wt}(\mathbf{b} \oplus \mathbf{b}') > T$, *then make the rejection decision* (N).

Table 1. Example of calculations of probabilities $Q_{\text{bio}}^{(T)}(\mathbf{b})$, $\mathbf{b} \in \{0,1\}^n$, where $n = 4$ and $T = 0, 1$.

$\mathbf{b}$	$Q_{\text{bio}}^{(0)}(\mathbf{b})$	$Q_{\text{bio}}^{(1)}(\mathbf{b})$
0000	**0.25**	$0.25 + 0.01 + 0.02 + 0.05 + 0.03 = 0.36$
0001	0.03	$0.03 + 0.02 + 0.01 + 0.01 + 0.25 = 0.32$
0010	0.05	$0.05 + 0.07 + 0.05 + 0.25 + 0.01 = 0.43$
0011	0.01	$0.01 + 0.03 + 0.08 + 0.03 + 0.05 = 0.20$
0100	0.02	$0.02 + 0.13 + 0.25 + 0.05 + 0.01 = 0.46$
0101	0.01	$0.01 + 0.01 + 0.03 + 0.08 + 0.02 = 0.15$
0110	0.05	$0.05 + 0.20 + 0.05 + 0.02 + 0.08 = 0.40$
0111	0.08	$0.08 + 0.03 + 0.01 + 0.01 + 0.05 = 0.18$
1000	0.01	$\mathbf{0.01 + 0.25 + 0.13 + 0.07 + 0.02 = 0.48}$
1001	0.02	$0.02 + 0.03 + 0.01 + 0.03 + 0.01 = 0.10$
1010	0.07	$0.07 + 0.05 + 0.20 + 0.01 + 0.03 = 0.36$
1011	0.03	$0.03 + 0.01 + 0.03 + 0.02 + 0.07 = 0.16$
1100	0.13	$0.13 + 0.02 + 0.01 + 0.20 + 0.01 = 0.37$
1101	0.01	$0.01 + 0.01 + 0.02 + 0.03 + 0.13 = 0.20$
1110	0.20	$\mathbf{0.20 + 0.05 + 0.07 + 0.13 + 0.03 = 0.48}$
1111	0.03	$0.03 + 0.08 + 0.03 + 0.01 + 0.20 = 0.35$



The enrollment stage



The authentication stage

Figure 3. Processing data by a direct authentication scheme.

Let Λ_+ and Λ_- denote the probability of the correct acceptance and the probability of the incorrect acceptance of the identity claim by the verifier,

$$\begin{aligned}\Lambda_+ &= \sum_{\mathbf{b}} \sum_{\mathbf{b}' \in \mathcal{D}^{(T)}(\mathbf{b})} \Pr_{\text{bio}}\{ B = \mathbf{b} \} \Pr_{\text{err}}\{ B' = \mathbf{b}' \mid B = \mathbf{b} \},\\ \Lambda_- &= \sum_{\mathbf{b}} \sum_{\mathbf{b}' \in \mathcal{D}^{(T)}(\mathbf{b})} \Pr_{\text{bio}}\{ B = \mathbf{b} \} \Pr_{\text{bio}}\{ B = \mathbf{b}' \}.\end{aligned}$$

Then using (7) and notation (3), (4) we obtain

$$\begin{aligned}\Lambda_+ &= 1,\\ \Lambda_- &= \sum_{\mathbf{b}} \Pr_{\text{bio}}\{ B = \mathbf{b} \} Q^{(T)}_{\text{bio}}(\mathbf{b}),\end{aligned}$$

where $Q^{(T)}_{\text{bio}}(\mathbf{b})$ is defined in (3).

2.3. Secrecy of the scheme

Let $\Lambda(\mathbf{b}')$ denote the probability of success for the attacker, who does not know the content of the database and presents the vector $\mathbf{b}'$ to the verifier as his guess. Then

$$\begin{aligned}\Lambda(\mathbf{b}') &= \sum_{\mathbf{b}} \Pr_{\text{bio}}\{ B = \mathbf{b} \} \chi\{ \mathbf{b} \in \mathcal{D}^{(T)}(\mathbf{b}') \}\\ &= Q^{(T)}_{\text{bio}}(\mathbf{b}').\end{aligned}$$

Therefore, the maximum probability of success is equal to

$$\Lambda \stackrel{\triangle}{=} \max_{\mathbf{b}'} \Lambda(\mathbf{b}') = Q^{(T)}_{\text{bio}},$$

and optimum guess is a vector $\mathbf{b}' \in \mathcal{B}^{(T)}$, where the set $\mathcal{B}^{(T)}$ is defined in (5).

2.4. Conclusion

We conclude that the probability of successful attack in the case when the attacker does not know the content of the database can be very small. However, the main problem with the direct authentication scheme is caused by the point that the biometric vector itself is stored in the database. If an attacker would have an access to the database, then he does not have any difficulties with the passing through the authentication stage with the acceptance decision. Moreover, the biometrics, being compromized, is compromized forever and it can be also used for any other purposes.

3. Additive block coding scheme

3.1. Description of the scheme

One of possible realizations of the scheme in Figure 1 is an additive block coding scheme. In this case, the biometric vector $\mathbf{b}$ is considered as an additive noise that corrupts the

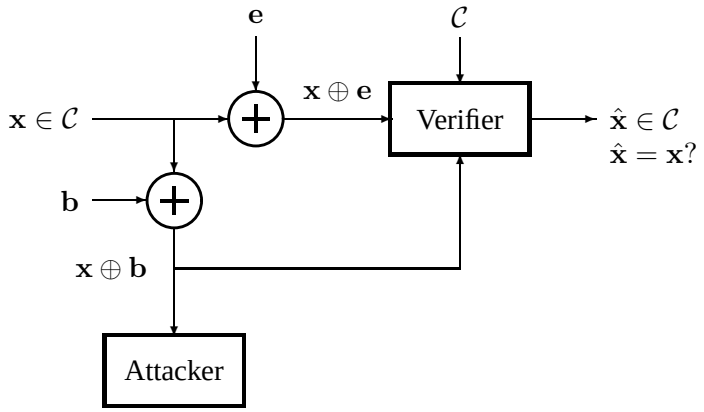


Figure 4. Wiretap-type additive block coding scheme.

transmitted codeword $\mathbf{x}$ and $\mathbf{y} = \mathbf{x} \oplus \mathbf{b}$. The decoding is based on the observations:

$$\left.\begin{array}{l} \mathbf{y} = \mathbf{x} \oplus \mathbf{b} \\ \mathbf{b}' = \mathbf{b} \oplus \mathbf{e} \end{array}\right\} \Rightarrow \left\{\begin{array}{l} \mathbf{x} \oplus \mathbf{e} = \mathbf{y} \oplus \mathbf{b}', \\ \mathbf{x} \oplus \mathbf{b} = \mathbf{y}. \end{array}\right.$$

Thus, the verifier analyzes the outcomes of transmission of the codeword $\mathbf{x}$ over two parallel channels, called the observation channel, $\mathbf{x} \to \mathbf{x} \oplus \mathbf{e}$, and the biometric channel, $\mathbf{x} \to \mathbf{x} \oplus \mathbf{b}$, while the attacker analyzes the output of the biometric channel (see Figure 4).

Let us restrict our attention to the case when $\mathcal{C}$ is a linear binary block code consisting of M different codewords of length n, i.e., $\mathcal{C} \subseteq \{0,1\}^n$ and $|\,\mathcal{C}\,| = M$. Then

$$\mathbf{x}, \mathbf{x}' \in \mathcal{C} \;\Rightarrow\; \mathbf{x} \oplus \mathbf{x}' \in \mathcal{C}. \tag{8}$$

Let

$$\mathcal{C} \oplus \mathbf{s} \stackrel{\triangle}{=} \bigcup_{\mathbf{x} \in \mathcal{C}} \{\mathbf{x} \oplus \mathbf{s}\} \tag{9}$$

denote the shift of the code by the vector $\mathbf{s} \in \{0,1\}^n$.

A basic property of a linear code is the existence of a set $\mathcal{S}_{\mathcal{C}} \subset \{0,1\}^n$, called the set of coset representatives of the code $\mathcal{C}$, such that

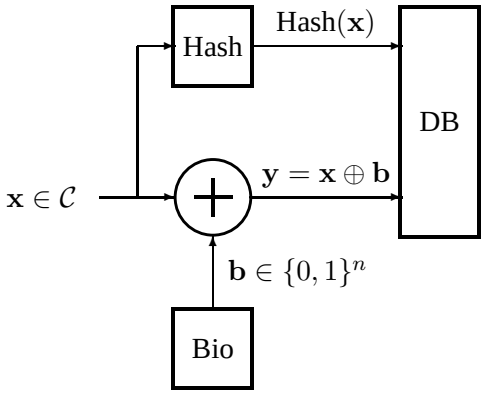
$$|\,\mathcal{S}_{\mathcal{C}}\,| = \frac{2^n}{M} \tag{10}$$

and

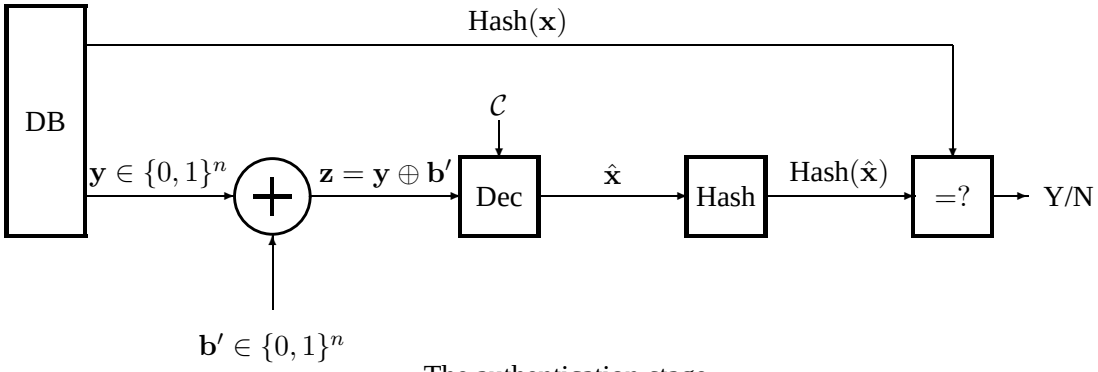
$$\{0,1\}^n = \bigcup_{\mathbf{s} \in \mathcal{S}_{\mathcal{C}}} (\mathcal{C} \oplus \mathbf{s}). \tag{11}$$

Thus, for any binary vector $\mathbf{y}$, there is a uniquely determined pair of vectors $(\mathbf{x}, \mathbf{s}) \in \mathcal{C} \times \mathcal{S}_{\mathcal{C}}$ such that $\mathbf{x} \oplus \mathbf{s} = \mathbf{y}$. Furthermore, if the minimum distance of the code $\mathcal{C}$ is at least $2T+1$, then all non–zero codewords have the weight at least $2T+1$,

$$\mathbf{x} \in \mathcal{C} \backslash \{(0, \ldots, 0)\} \;\Rightarrow\; \mathrm{wt}(\mathbf{x}) \geq 2T+1. \tag{12}$$



The enrollment stage



The authentication stage

Figure 5. Processing data by an additive block coding scheme when the verifier considers only output of the observation channel.

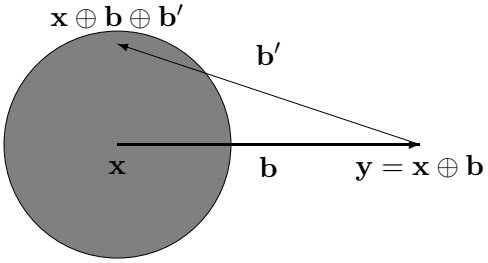


Figure 6. An illustration of transformations of the key codeword in an additive block coding scheme.

Processing of a given biometric vector $\mathbf{b}$ at the enrollment stage and processing data at the authentication stage when the verifier considers only the output of the observation channel is illustrated in Figure 5.

The enrollment stage.

– *Choose a key codeword* $\mathbf{x}$ *according to a uniform probability distribution over the code* $\mathcal{C}$ *and compute the value of* $\mathrm{Hash}(\mathbf{x})$.

– *Store* $(\mathrm{Hash}(\mathbf{x}), \mathbf{x} \oplus \mathbf{b})$ *in the database.*

The authentication stage.

– *Read the data* $(\mathrm{Hash}(\mathbf{x}), \mathbf{y})$ *associated with the claimed person from the database.*

– *Decode the key codeword, given a received vector* $\mathbf{z} = \mathbf{y} \oplus \mathbf{b}'$, *as* $\hat{\mathbf{x}}$. *If* $\mathrm{Hash}(\hat{\mathbf{x}}) = \mathrm{Hash}(\mathbf{x})$, *then make the acceptance decision* (Y). *If* $\mathrm{Hash}(\hat{\mathbf{x}}) \neq \mathrm{Hash}(\mathbf{x})$, *then make the rejection decision* (N).

The additive block coding scheme can be understood as follows (see Figure 6). The key codeword $\mathbf{x}$ chosen at random from the code $\mathcal{C}$ is corrupted by the biometric vector $\mathbf{b}$ at the enrollment stage, and the vector $\mathbf{y} = \mathbf{x} \oplus \mathbf{b}$ is stored in the database. Having received the vector $\mathbf{b}'$ at the authentication stage, the verifier adds it modulo 2 to the vector $\mathbf{y}$ and expects to receive a vector belonging to the decoding decision region for the codeword $\mathbf{x}$, because the distance between $\mathbf{x}$ and the vector $\mathbf{y} \oplus \mathbf{b}' = \mathbf{x} \oplus \mathbf{b} \oplus \mathbf{b}'$ is equal to the weight of the vector $\mathbf{b} \oplus \mathbf{b}'$.

Let us also illustrate the additive block coding by the numerical example. Let $n = 6, M = 8$. The codewords of the code $\mathcal{C}$ are given in the first column of Table 2. If $\mathbf{b} = 011011$ and $\mathbf{x} = 011110$, then the vector $\mathbf{y} = 000101$ is stored in the database. Having received another vector $\mathbf{b}' = 111011$, the verifier tries to find a codeword $\hat{\mathbf{x}}$ located at

Table 2. Example of processing data with the additive block coding scheme for $n = 6$ and $M = 8$. The vector $\mathbf{y}$ is stored in the database at the enrollment stage. The vector $\mathbf{z}$ is considered as the received word of the decoder at the authentication stage.

$\mathbf{x} \in \mathcal{C}$	$\longrightarrow$			$\mathbf{x} \oplus \mathbf{y}$	$\mathbf{x} \oplus \mathbf{z}$	$d(\mathbf{x}, \mathbf{z})$
000000	$\mathbf{x}$	$=$	011110	000101	111110	6
001011	$\mathbf{b}$	$=$	011011	001110	110101	4
010101	$\mathbf{y}$	$=$	$\mathbf{x} \oplus \mathbf{b}$	010000	101011	4
011110		$=$	000101	**011011**	**100000**	**1**
100110	$\mathbf{b}'$	$=$	111011	100011	011000	2
101101	$\mathbf{z}$	$=$	$\mathbf{y} \oplus \mathbf{b}'$	101011	010011	3
110011		$=$	111110	110110	001101	3
111000				111101	000110	2

distance at most 1 from the vector $\mathbf{y} \oplus \mathbf{b}' = 111110$. The result is $\hat{\mathbf{x}} = 011110$ and the acceptance decision is made, since $\hat{\mathbf{x}} = \mathbf{x}$ implies $\mathrm{Hash}(\hat{\mathbf{x}}) = \mathrm{Hash}(\mathbf{x})$. An attacker wants to submit some vector $\mathbf{b}'$, which also leads to the acceptance. He constructs the list of candidate biometric vectors as $\mathbf{x} \oplus \mathbf{y}$, $\mathbf{x} \in \mathcal{C}$, and outputs the vector $\mathbf{x}' \oplus \mathbf{y}$ having the maximum probability. In particular, if the probabilities $\Pr_{\text{bio}}\{B = \mathbf{b}\}$ decrease when the weight of the vector $\mathbf{b}$ increases, then this algorithm brings the vector $\mathbf{b}' = 010000$.

3.2. Secrecy of the scheme

The general description of the actions of an attacker can be presented in such a way that he applies a fixed function

$$\varphi : \{0,1\}^n \to \{0,1\}^n$$

to the vector $\mathbf{y}$, which is stored in the database, and submits the vector $\mathbf{b}' = \varphi(\mathbf{y})$ to the verifier.

For any vector $\mathbf{z} \in \{0,1\}^n$, let $\hat{\mathbf{x}}[\,\mathbf{z}\,]$ denote the codeword constructed by the following procedure. The decoder finds all codewords located at distance T or less from the vector $\mathbf{z}$. If there is only one codeword having this property, then $\hat{\mathbf{x}}[\,\mathbf{z}\,]$ is defined as this codeword. Otherwise, $\hat{\mathbf{x}}[\,\mathbf{z}\,]$ is a fixed vector (for example, the all–zero vector). Formally,

$$\hat{\mathbf{x}}[\,\mathbf{z}\,] \stackrel{\triangle}{=} \begin{cases} \mathbf{x}, & \text{if } \mathcal{D}^{(T)}(\mathbf{z}) \cap \mathcal{C} = \{\mathbf{x}\}, \\ (0, \ldots, 0), & \text{if } |\,\mathcal{D}^{(T)}(\mathbf{z}) \cap \mathcal{C}\,| \neq 1. \end{cases} \tag{13}$$

If the verifier decodes the key codeword as

$$\hat{\mathbf{x}} = \hat{\mathbf{x}}[\,\mathbf{y} \oplus \mathbf{b}'\,],$$

then the probability of successful attack can be expressed as

$$\Lambda_{\mathcal{C}}(\varphi) = \frac{1}{M} \sum_{\mathbf{x} \in \mathcal{C}} \sum_{\mathbf{y}} \Pr_{\text{bio}}\{B = \mathbf{x} \oplus \mathbf{y}\} \chi\{\,\hat{\mathbf{x}}[\,\mathbf{y} \oplus \varphi(\mathbf{y})\,] = \mathbf{x}\,\}. \tag{14}$$

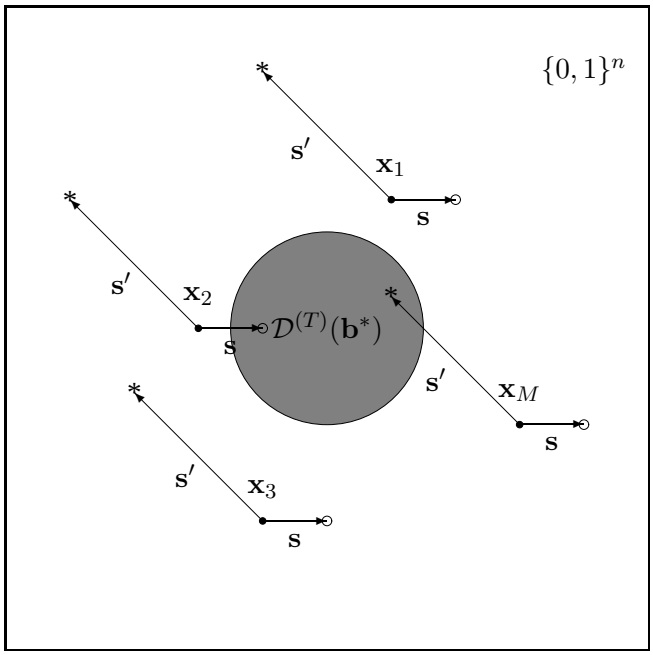


Figure 7. An illustration of the covering of the set $\{0,1\}^n$ by shifts of a linear code $\mathcal{C} = \{\mathbf{x}_1, \mathbf{x}_2, \mathbf{x}_3, \ldots, \mathbf{x}_M\}$.

Proposition 3.1 *The probability of successful attack is maximized when the maximum a posteriori probability decoding is used and* $\varphi = \varphi^{\text{MAP}}$, *where*

$$\varphi^{\text{MAP}}(\mathbf{y}) = \mathbf{y} \oplus \arg\max_{\mathbf{x}\in\mathcal{C}} \Pr_{\text{bio}}\{B = \mathbf{x} \oplus \mathbf{y}\}. \tag{15}$$

If $\mathcal{C}$ *is a linear code and* $\mathcal{E}_{\mathcal{C}}$ *denotes the set of coset representatives, then*

$$\Lambda_{\mathcal{C}}(\varphi^{\text{MAP}}) = \sum_{\mathbf{s}\in\mathcal{S}_{\mathcal{C}}} \max_{\mathbf{x}\in\mathcal{C}} \Pr_{\text{bio}}\{B = \mathbf{x} \oplus \mathbf{s}\}. \tag{16}$$

The claim of the Proposition 3.1 is illustrated in Figure 7. The set $\{0,1\}^n$ can be covered by shifts $\mathbf{s} \in \mathcal{S}_{\mathcal{C}}$. The shift can be discovered by the attacker using the rule: find the $\mathbf{s} \in \mathcal{S}_{\mathcal{C}}$ such that $\mathbf{y} \oplus \mathbf{s} \in \mathcal{C}$. The M biometric vectors $\mathbf{x} \oplus \mathbf{s}$, $\mathbf{x} \in \mathcal{C}$, are considered as candidates for the vector $\mathbf{b}$ processed at the enrollment stage. The vector having the maximum probability is the best guess, and the sum modulo 2 of this vector and the received vector $\mathbf{y}$ is the output of the attacker.

Instead of using the mapping φ^{MAP}, which requires running the decoding procedure for a given code $\mathcal{C}$, the attacker can use simpler options. Namely, he can 1) guess the key codeword with probability $1/M$ and submit the sum modulo 2 of this vector and the vector $\mathbf{y}$ stored in the database; 2) submit the sum modulo 2 of a biometric vector $\mathbf{b}^* \in \mathcal{B}^{(T)}$ and the vector $\mathbf{y}$. The strategies above bring the lower bound

$$\Lambda_{\mathcal{C}}(\varphi^{\text{MAP}}) \geq \max\Big\{\frac{1}{M},\, Q_{\text{bio}}^{(T)}\Big\}, \tag{17}$$

and the statement below establishes conditions under which the inequality (17) is tight.

Proposition 3.2

(1) The equality

$$\Lambda_{\mathcal{C}}(\varphi^{\text{MAP}}) = \frac{1}{M} \tag{18}$$

is valid if and only if

$$\left.\begin{array}{r}\mathbf{x}, \mathbf{x}' \in \mathcal{C} \\ \mathbf{s} \in \mathcal{S}_{\mathcal{C}}\end{array}\right\} \Rightarrow \Pr_{\text{bio}}\{B = \mathbf{x} \oplus \mathbf{s}\} = \Pr_{\text{bio}}\{B = \mathbf{x}' \oplus \mathbf{s}\}. \tag{19}$$

(2) The equality

$$\Lambda_{\mathcal{C}}(\varphi^{\text{MAP}}) = Q_{\text{bio}}^{(T)} \tag{20}$$

is valid if and only if

$$\mathbf{b} \in (\mathcal{C} \oplus \mathbf{s}) \bigcap \mathcal{D}^{(T)} \Rightarrow \Pr_{\text{bio}}\{B = \mathbf{b}\} = \max_{\mathbf{x} \in \mathcal{C}} \Pr_{\text{bio}}\{B = \mathbf{x} \oplus \mathbf{s}\} \tag{21}$$

and

$$(\mathcal{C} \oplus \mathbf{s}) \bigcap \mathcal{D}^{(T)} = \emptyset \Rightarrow \max_{\mathbf{x} \in \mathcal{C}} \Pr_{\text{bio}}\{B = \mathbf{x} \oplus \mathbf{s}\} = 0, \tag{22}$$

where the sets $\mathcal{D}^{(T)}$ and $\mathcal{C} \oplus \mathbf{s}$ are defined in (6) *and* (9)*, respectively.*

A special case of inequality (17) is received when $T = 0$,

$$\Lambda_{\mathcal{C}}(\varphi^{\text{MAP}}) \geq \max\Big\{\frac{1}{M}, Q_{\text{bio}}^{(0)}\Big\}, \tag{23}$$

where

$$Q_{\text{bio}}^{(0)} = \max_{\mathbf{b}} \Pr_{\text{bio}}\{B = \mathbf{b}\}.$$

Notice that the statement *(2)* of Proposition 3.2 for $T = 0$ is as follows: $\Lambda_{\mathcal{C}}(\varphi^{\text{MAP}}) = Q_{\text{bio}}^{(0)}$ if and only if the set, where the probabilities of biometric vectors are positive, coincides with one of shifts of the code $\mathcal{C}$, i.e.,

$$\exists \mathbf{s} \in \mathcal{S}_{\mathcal{C}} : \Pr_{\text{bio}}\{B = \mathbf{b}\} > 0 \Rightarrow \mathbf{b} \in \mathcal{C} \oplus \mathbf{s}.$$

3.3. Conclusion

A possible solution to the storing and the verification problems is based on the block cypher scheme. In this case, a secret vector $\mathbf{x}$ is added modulo 2 to the vector $\mathbf{b}$ at the enrollment stage. The same vector is also added to the vector $\mathbf{b}'$ at the verification stage, and the Hamming weight of the vector $(\mathbf{x} \oplus \mathbf{b}) \oplus (\mathbf{x} \oplus \mathbf{b}') = \mathbf{b} \oplus \mathbf{b}' = \mathbf{e}$ is then compared with the threshold. The feature of the block cypher scheme is the point that the secret vector $\mathbf{x}$ has to be known to the verifier. An additive block coding scheme can be viewed as an extension of the block cypher scheme where the verifier only knows the value of the "one–way" hash function at the key codeword used at the enrollment stage and checks whether the value of this function at the decoded codeword is the same or not. The secrecy of the scheme is completely determined by the probability distribution over the biometric vectors, and the constraints, under which the knowledge of the content of the database cannot be used by the attacker, are rather strong. These constraints are essentially relaxed in the permutation block coding scheme considered in the next section.

3.4. Proofs

Proof of Proposition 3.1

Let us rewrite (14) as

$$\Lambda_{\mathcal{C}}(\varphi) = \frac{1}{M} \sum_{\mathbf{y}} \lambda_{\mathcal{C}}(\varphi(\mathbf{y})),$$

where

$$\begin{aligned} \lambda_{\mathcal{C}}(\varphi(\mathbf{y})) &\stackrel{\triangle}{=} \sum_{\mathbf{x}\in\mathcal{C}} \Pr_{\text{bio}}\{B = \mathbf{x} \oplus \mathbf{y}\} \chi\{\, \hat{\mathbf{x}}[\mathbf{y} \oplus \varphi(\mathbf{y})] = \mathbf{x} \,\} \\ &= \Pr_{\text{bio}}\{B = \hat{\mathbf{x}}[\mathbf{y} \oplus \varphi(\mathbf{y})] \oplus \mathbf{y}\} \\ &\leq \max_{\mathbf{x}\in\mathcal{C}} \Pr_{\text{bio}}\{B = \mathbf{x} \oplus \mathbf{y}\} \end{aligned}$$

and the inequality follows from the observation that $\hat{\mathbf{x}}[\mathbf{y} \oplus \varphi(\mathbf{y})]$ is a codeword of the code $\mathcal{C}$. This inequality is tight if $\varphi(\mathbf{y}) = \varphi^{\text{MAP}}(\mathbf{y})$, where $\varphi^{\text{MAP}}(\mathbf{y})$ is defined in (15). Hence

$$\lambda_{\mathcal{C}}(\varphi(\mathbf{y})) \leq \lambda_{\mathcal{C}}(\varphi^{\text{MAP}}(\mathbf{y}))$$

and

$$\Lambda_{\mathcal{C}}(\varphi^{\text{MAP}}) = \frac{1}{M} \sum_{\mathbf{y}} \max_{\mathbf{x}\in\mathcal{C}} \Pr_{\text{bio}}\{B = \mathbf{x} \oplus \mathbf{y}\}.$$

Using linear properties of the code, we obtain

$$\begin{aligned} \frac{1}{M} \sum_{\mathbf{y}} \max_{\mathbf{x}\in\mathcal{C}} \Pr_{\text{bio}}\{B = \mathbf{x} \oplus \mathbf{y}\} &= \frac{1}{M} \sum_{\mathbf{x}'\in\mathcal{C}} \sum_{\mathbf{s}\in\mathcal{S}_{\mathcal{C}}} \max_{\mathbf{x}\in\mathcal{C}} \Pr_{\text{bio}}\{B = \mathbf{x} \oplus \mathbf{x}' \oplus \mathbf{s}\} \\ &= \frac{1}{M} \sum_{\mathbf{x}'\in\mathcal{C}} \sum_{\mathbf{s}\in\mathcal{S}_{\mathcal{C}}} \max_{\tilde{\mathbf{x}}\in\mathcal{C}} \Pr_{\text{bio}}\{B = \tilde{\mathbf{x}} \oplus \mathbf{s}\} \\ &= \sum_{\mathbf{s}\in\mathcal{S}_{\mathcal{C}}} \max_{\tilde{\mathbf{x}}\in\mathcal{C}} \Pr_{\text{bio}}\{B = \tilde{\mathbf{x}} \oplus \mathbf{s}\}, \end{aligned}$$

where the first two equalities follow from (8) and (11). The expression at the right-hand side coincides with (16), and the proof is complete.

Proof of Proposition 3.2

(1) We write

$$\begin{aligned} M\Lambda_{\mathcal{C}}(\varphi^{\text{MAP}}) &= \sum_{\mathbf{s}\in\mathcal{S}_{\mathcal{C}}} M \max_{\mathbf{x}\in\mathcal{C}} \Pr_{\text{bio}}\{B = \mathbf{x} \oplus \mathbf{s}\} \\ &\geq \sum_{\mathbf{s}\in\mathcal{S}_{\mathcal{C}}} \sum_{\mathbf{x}\in\mathcal{C}} \Pr_{\text{bio}}\{B = \mathbf{x} \oplus \mathbf{s}\} \\ &= \sum_{\mathbf{b}} \Pr_{\text{bio}}\{B = \mathbf{b}\}, \\ &= 1, \end{aligned}$$

where the inequality is tight if and only if

$$\mathbf{s} \in \mathcal{S}_{\mathcal{C}} \;\Rightarrow\; \max_{\mathbf{x}\in\mathcal{C}} \Pr_{\text{bio}}\{B = \mathbf{x} \oplus \mathbf{s}\} = \frac{1}{M} \sum_{\mathbf{x}\in\mathcal{C}} \Pr_{\text{bio}}\{B = \mathbf{x} \oplus \mathbf{s}\}.$$

One can easily see that this condition is equivalent to (19).

(2) Let us fix some vector $\mathbf{b}^* \in \mathcal{B}^{(T)}$, where the set $\mathcal{B}^{(T)}$ is defined in (5), and denote

$$\mathcal{S}_{\mathcal{C}}^{(T)}(\mathbf{b}^*) \stackrel{\triangle}{=} (\mathcal{C} \oplus \mathbf{s}) \bigcap \mathcal{D}^{(T)}(\mathbf{b}^*),$$

where the set $\mathcal{D}^{(T)}(\mathbf{b}^*)$ is defined by (2) for $\mathbf{b} = \mathbf{b}^*$. Then

$$\begin{aligned}
\Lambda_{\mathcal{C}}(\varphi^{\text{MAP}}) &= \sum_{\mathbf{s}\in\mathcal{S}_{\mathcal{C}}^{(T)}(\mathbf{b}^*)} \max_{\mathbf{x}\in\mathcal{C}} \Pr_{\text{bio}}\{B = \mathbf{x} \oplus \mathbf{s}\} + \sum_{\mathbf{s}\in\mathcal{S}_{\mathcal{C}}\setminus\mathcal{S}_{\mathcal{C}}^{(T)}(\mathbf{b}^*)} \max_{\mathbf{x}\in\mathcal{C}} \Pr_{\text{bio}}\{B = \mathbf{x} \oplus \mathbf{s}\} \\
&\geq \sum_{\mathbf{s}\in\mathcal{S}_{\mathcal{C}}^{(T)}(\mathbf{b}^*)} \max_{\mathbf{x}\in\mathcal{C}} \Pr_{\text{bio}}\{B = \mathbf{x} \oplus \mathbf{s}\}.
\end{aligned}$$

Suppose that there are two codewords, $\mathbf{x}', \mathbf{x}'' \in \mathcal{C}$ such that the vectors $\mathbf{x}' \oplus \mathbf{s}$ and $\mathbf{x}'' \oplus \mathbf{s}$ belong to the set $\mathcal{D}^{(T)}(\mathbf{b}^*)$ for some vector $\mathbf{s} \in \mathcal{S}_{\mathcal{C}}$. Then

$$\left.\begin{array}{rcl} \mathbf{x}' \oplus \mathbf{s} &=& \mathbf{b}^* \oplus \mathbf{e}' \\ \mathbf{x}'' \oplus \mathbf{s} &=& \mathbf{b}^* \oplus \mathbf{e}'' \end{array}\right\} \;\Rightarrow\; \mathbf{x}' \oplus \mathbf{x}'' = \mathbf{s} \oplus \mathbf{s}'' \;\Rightarrow\; \text{wt}(\mathbf{x}' \oplus \mathbf{x}'') = \text{wt}(\mathbf{e} \oplus \mathbf{e}'')$$

for some vectors $\mathbf{e}', \mathbf{e}''$ of weight at most T. However, since $\mathcal{C}$ is a linear code, $\mathbf{x}' \oplus \mathbf{x}'' \in \mathcal{C}$ and

$$\begin{aligned}
\text{wt}(\mathbf{e}'), \text{wt}(\mathbf{e}'') \leq T &\;\Rightarrow\; \text{wt}(\mathbf{e}' \oplus \mathbf{e}'') \leq 2T, \\
\mathbf{x}', \mathbf{x}'' \in \mathcal{C} &\;\Rightarrow\; \text{wt}(\mathbf{x}' \oplus \mathbf{x}'') \geq 2T + 1,
\end{aligned}$$

where the last inequality follows from (12). Thus, we conclude that, for any $\mathbf{s} \in \mathcal{S}_{\mathcal{C}}^{(T)}(\mathbf{b}^*)$, there is exactly one codeword $\mathbf{x}_{\mathbf{s}} \in \mathcal{C}$ such that $\mathbf{x}_{\mathbf{s}} \oplus \mathbf{s} \in \mathcal{D}^{(T)}(\mathbf{b}^*)$ and

$$|\,\mathcal{S}_{\mathcal{C}}^{(T)}(\mathbf{b}^*)\,| = |\,\mathcal{D}^{(T)}(\mathbf{b}^*)\,|.$$

As a result,

$$\begin{aligned}
\sum_{\mathbf{s}\in\mathcal{S}_{\mathcal{C}}^{(T)}(\mathbf{b}^*)} \max_{\mathbf{x}\in\mathcal{C}} \Pr_{\text{bio}}\{B = \mathbf{x} \oplus \mathbf{s}\} &\geq \sum_{\mathbf{s}\in\mathcal{S}_{\mathcal{C}}^{(T)}(\mathbf{b}^*)} \Pr_{\text{bio}}\{B = \mathbf{x}_{\mathbf{s}} \oplus \mathbf{s}\} \\
&= \sum_{\mathbf{b}'\in\mathcal{D}^{(T)}(\mathbf{b}^*)} \Pr_{\text{bio}}\{B = \mathbf{b}'\} \\
&= Q_{\text{bio}}^{(T)}.
\end{aligned}$$

One can easily see that the inequalities used in the proof are tight if and only if conditions (21) and (22) are satisfied.

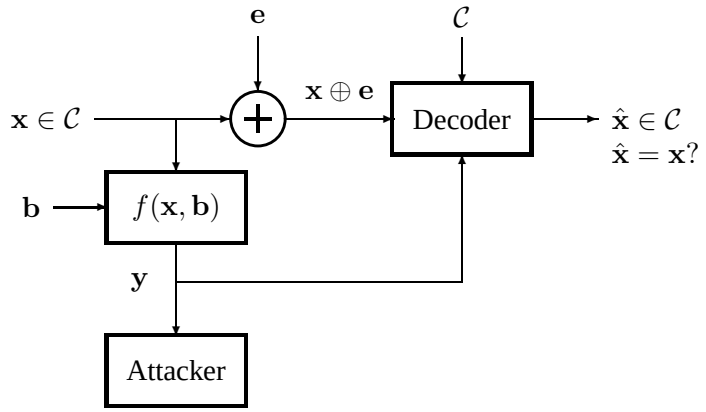


Figure 8. Modified wiretap-type block coding scheme.

4. Permutation block coding scheme

4.1. Description of the scheme

The permutation block coding scheme can be viewed as a modification of the scheme in Figure 4 where the sum modulo 2 in the link to the attacker is replaced by a stochastic mapping $f(\mathbf{x}, \mathbf{b})$, as it is shown in Figure 8. Such a modification is possible when both the vector $\mathbf{x}$ and $\mathbf{b}$ have equal weights and $f(\mathbf{x}, \mathbf{b})$ stands for the binary representation of a permutation $\boldsymbol{\pi}$ that transforms the vector $\mathbf{x}$ to the vector $\mathbf{b}$. Formally, let $\mathcal{B} = \{0,1\}_w^n$, where $\{0,1\}_w^n$ is the set consisting of binary vectors of the Hamming weight w. Thus, the biometric vector is a binary vector $\mathbf{b}$ of length n chosen by a combinatorial (n, w)-source, i.e.,

$$\mathrm{wt}(\mathbf{b}) \neq w \;\Rightarrow\; \Pr_{\text{bio}}\{B = \mathbf{b}\} = 0. \tag{24}$$

Let $\mathcal{C}$ denote a binary code consisting of M different codewords of length n and weight w, i.e., $\mathcal{C} \subseteq \{0,1\}_w^n$ and $|\,\mathcal{C}\,| = M$.

The permutation of components of some vector $\mathbf{x} = (x_1, \ldots, x_n) \in \{0,1\}_w^n$ is determined by a vector $\boldsymbol{\pi} \in \mathcal{P}$ in such a way that

$$\boldsymbol{\pi}(\mathbf{x}) = (x_{\pi_1}, \ldots, x_{\pi_n}),$$

where $\mathcal{P}$ is the set of all possible permutations of components of the vector $(1, \ldots, n)$. Given a vector $\mathbf{b} \in \{0,1\}_w^n$ and a permutation $\boldsymbol{\pi} \in \mathcal{P}$, let $\boldsymbol{\pi}^{-1} \in \mathcal{P}$ denote the inverse permutation, i.e.,

$$\boldsymbol{\pi}^{-1}(\mathbf{b}) = (b_{i_1(\boldsymbol{\pi})}, \ldots, b_{i_n(\boldsymbol{\pi})}),$$

where $i_j(\boldsymbol{\pi}) \in \{1, \ldots, n\}$ is the index determined by the equation $\pi_{i_j(\boldsymbol{\pi})} = j$.

For all vectors $\mathbf{x}, \mathbf{b} \in \{0,1\}_w^n$, let

$$\mathcal{P}(\mathbf{x} \to \mathbf{b}) \stackrel{\triangle}{=} \{\, \boldsymbol{\pi} \in \mathcal{P} :\; \boldsymbol{\pi}(\mathbf{x}) = \mathbf{b} \,\} \tag{25}$$

denote the set of permutations that transform the vector $\mathbf{x}$ to the vector $\mathbf{b}$. Let us introduce the probability distribution

$$\gamma_{\mathbf{x},\mathbf{b}} = (\,\gamma(\boldsymbol{\pi}|\mathbf{x},\mathbf{b}),\ \boldsymbol{\pi} \in \mathcal{P}\,)$$

in such a way that $\gamma(\boldsymbol{\pi}|\mathbf{x},\mathbf{b})$ can be positive only if $\boldsymbol{\pi} \in \mathcal{P}(\mathbf{x} \to \mathbf{b})$. Let us also denote a uniform probability distribution over the set $\mathcal{P}(\mathbf{x} \to \mathbf{b})$ by

$$\overline{\gamma}_{\mathbf{x},\mathbf{b}} = (\,\overline{\gamma}(\boldsymbol{\pi}|\mathbf{x},\mathbf{b}),\ \boldsymbol{\pi} \in \mathcal{P}\,),$$

where

$$\overline{\gamma}(\boldsymbol{\pi}|\mathbf{x},\mathbf{b}) \stackrel{\triangle}{=} \begin{cases} |\,\mathcal{P}(\mathbf{x},\mathbf{b})|^{-1}, & \text{if } \boldsymbol{\pi} \in \mathcal{P}(\mathbf{x} \to \mathbf{b}), \\ 0, & \text{if } \boldsymbol{\pi} \notin \mathcal{P}(\mathbf{x} \to \mathbf{b}). \end{cases}$$

For example, let $n = 4, k = 2$. The set $\{0,1\}_2^4$ consists of $\binom{4}{2} = 6$ binary vectors of length 4 having the weight 2 and $\mathcal{P}$ is the set consisting of $4! = 24$ permutations of components of the vector $(1,2,3,4)$. For all $\mathbf{x},\mathbf{b} \in \{0,1\}_2^4$, the set $\mathcal{P}(\mathbf{x} \to \mathbf{b})$ consists of $2!2! = 4$ permutations. In particular,

$$\mathcal{P}(1100 \to 1010) = \{\,1324, 1423, 2314, 2413\,\}.$$

Notice that

$$\left.\begin{array}{rcl} \mathbf{b} & = & \boldsymbol{\pi}(\mathbf{x}) \\ \mathbf{b}' & = & \mathbf{b} \oplus \mathbf{e} \end{array}\right\} \ \Rightarrow\ \boldsymbol{\pi}^{-1}(\mathbf{b}') = \boldsymbol{\pi}^{-1}(\mathbf{b}) \oplus \boldsymbol{\pi}^{-1}(\mathbf{e}) = \mathbf{x} \oplus \boldsymbol{\pi}^{-1}(\mathbf{e})$$

and

$$\mathrm{wt}(\boldsymbol{\pi}^{-1}(\mathbf{e})) = \mathrm{wt}(\mathbf{e}), \tag{26}$$

i.e., the decoder observes "the transmitted codeword" $\mathbf{x}$ as $\mathbf{x} \oplus \boldsymbol{\pi}^{-1}(\mathbf{e})$. If the source generating the noise vectors is assumed to be a memoryless source, then (26) implies that the presence of the permutation $\boldsymbol{\pi}^{-1}$ does not affect the decoding strategy, and the scheme is equivalent to the one in Figure 8.

Processing of a given biometric vector $\mathbf{b}$ at the enrollment stage and processing data at the authentication stage when the verifier considers only the output of the observation channel is illustrated in Figure 9.

The enrollment stage.

– *Choose a key codeword* $\mathbf{x}$ *according to a uniform probability distribution over the code* $\mathcal{C}$ *and compute the value of* $\mathrm{Hash}(\mathbf{x})$.

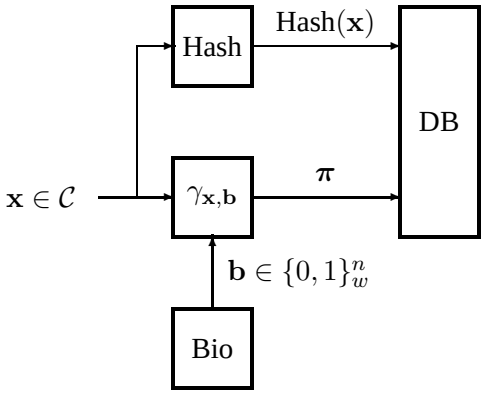
– *Given a pair of vectors* $(\mathbf{x},\mathbf{b}) \in \{0,1\}_w^n \times \{0,1\}_w^n$, *choose a permutation* $\boldsymbol{\pi} \in \mathcal{P}$ *according to the probability distribution* $\gamma_{\mathbf{x},\mathbf{b}}$.

– *Store* $(\mathrm{Hash}(\mathbf{x}), \boldsymbol{\pi})$ *in the database.*

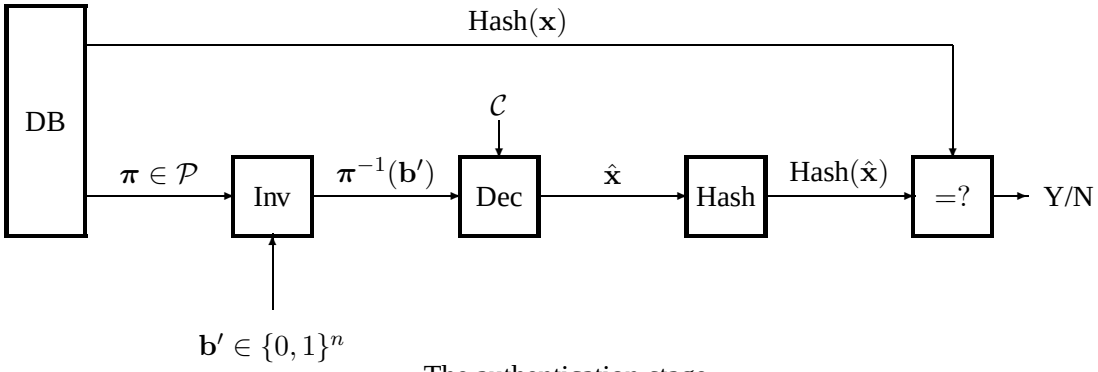
The authentication stage.

– *Read the data* $(\mathrm{Hash}(\mathbf{x}), \boldsymbol{\pi})$ *associated with the claimed person from the database.*

– *Apply the inverse permutation* $\boldsymbol{\pi}^{-1}$ *to the vector* $\mathbf{b}'$ *and decode the key codeword given a received vector* $\boldsymbol{\pi}^{-1}(\mathbf{b}')$ *as* $\hat{\mathbf{x}}$. *If* $\mathrm{Hash}(\hat{\mathbf{x}}) = \mathrm{Hash}(\mathbf{x})$, *then accept the identity claim* (Y). *If* $\mathrm{Hash}(\hat{\mathbf{x}}) \neq \mathrm{Hash}(\mathbf{x})$, *then reject the identity claim* (N).



The enrollment stage



The authentication stage

Figure 9. Processing data by a permutation block coding scheme.

4.2. Secrecy of the scheme

Let

$$\gamma = (\,\gamma_{\mathbf{x},\mathbf{b}},\, \mathbf{x}, \mathbf{b} \in \{0,1\}_w^n\,)$$

denote the list of conditional probability distributions over the set $\mathcal{P}$. In general, the attacker applies a fixed function

$$\psi:\ \mathcal{P}\ \to\ \{0,1\}^n$$

to the permutation $\boldsymbol{\pi}$ stored in the DB and submits the vector $\mathbf{b}' = \psi(\boldsymbol{\pi})$ to the verifier. Let us use the notation (13) and assume that the verifier decodes the key codeword as the vector

$$\hat{\mathbf{x}} = \hat{\mathbf{x}}[\boldsymbol{\pi}^{-1}(\mathbf{b}')].$$

Then the probability of successful attack is equal to

$$\Lambda_{\mathcal{C},\gamma}(\psi) = \frac{1}{M}\sum_{\mathbf{x}\in\mathcal{C}}\sum_{\mathbf{b}}\Pr_{\text{bio}}\{B=\mathbf{b}\}\sum_{\boldsymbol{\pi}\in\mathcal{P}}\gamma(\boldsymbol{\pi}|\mathbf{x},\mathbf{b})\chi\{\,\hat{\mathbf{x}}[\boldsymbol{\pi}^{-1}(\psi(\boldsymbol{\pi}))] = \mathbf{x}\,\}. \tag{27}$$

Proposition 4.1 *The probability of successful attack is maximized when the maximum a posteriori probability decoding is used and* $\psi = \psi^{\text{MAP}}$, *where*

$$\psi^{\text{MAP}}(\boldsymbol{\pi}) = \boldsymbol{\pi}\Big(\,\arg\max_{\mathbf{x}\in\mathcal{C}}\gamma_{\text{bio}}(\boldsymbol{\pi}|\mathbf{x})\,\Big) \tag{28}$$

and

$$\gamma_{\text{bio}}(\boldsymbol{\pi}|\mathbf{x}) \stackrel{\triangle}{=} \sum_{\mathbf{b}}\Pr_{\text{bio}}\{B=\mathbf{b}\}\gamma(\boldsymbol{\pi}|\mathbf{x},\mathbf{b}). \tag{29}$$

Furthermore,

$$\Lambda_{\mathcal{C},\gamma}(\psi^{\text{MAP}}) = \frac{1}{M}\sum_{\boldsymbol{\pi}\in\mathcal{P}}\max_{\mathbf{x}\in\mathcal{C}}\gamma_{\text{bio}}(\boldsymbol{\pi}|\mathbf{x}). \tag{30}$$

Notice that $(\,\gamma_{\text{bio}}(\boldsymbol{\pi}|\mathbf{x}),\ \boldsymbol{\pi}\in\mathcal{P}\,)$ is the conditional probability distribution over the set $\mathcal{P}$ and

$$\sum_{\boldsymbol{\pi}\in\mathcal{P}}\gamma_{\text{bio}}(\boldsymbol{\pi}|\mathbf{x}) = 1. \tag{31}$$

Notice also that the vector $\mathbf{x}\in\{0,1\}_w^n$ and the permutation $\boldsymbol{\pi}\in\mathcal{P}$ uniquely determine the vector $\mathbf{b}^0\in\{0,1\}_w^n$ such that $\boldsymbol{\pi}\in\mathcal{P}(\mathbf{x}\to\mathbf{b}^0)$. Namely, $\mathbf{b}^0 = \boldsymbol{\pi}(\mathbf{x})$, and the sum at the right-hand side of (29) contains at most one non–zero term.

The attacker has two simple possibilities: 1) fix a codeword $\mathbf{x}'\in\mathcal{C}$ and submit the vector $\mathbf{b}' = \boldsymbol{\pi}(\mathbf{x}')$; 2) submit a most likely biometric vector. In the first case, the attacker has to know the code $\mathcal{C}$ and the stored permutation $\boldsymbol{\pi}$. In the second case, he does not know these data and is equivalent to an attacker, who does not have access to the database and is ignorant about the code. One can easily see that the probabilities of successful attacks are equal to $1/M$ and Q^*_{bio}, respectively. Therefore the probability of successful attack under the maximum *a posteriori* probability decoding of the key codeword is bounded from below as follows:

$$\Lambda_{\mathcal{C},\gamma}(\psi^{\text{MAP}}) \geq \max\Big\{\frac{1}{M},\, Q^{(T)}_{\text{bio}}\Big\}.$$

We will present the formal proof to find under which conditions this inequality is tight.

Proposition 4.2

(1) The equality

$$\Lambda_{\mathcal{C},\gamma}(\psi^{\text{MAP}}) = \frac{1}{M} \tag{32}$$

is valid if and only if the probability distributions $\gamma_{\mathbf{x},\mathbf{b}}$ are assigned in such a way that the conditional probability distributions $(\gamma_{\text{bio}}(\boldsymbol{\pi}|\mathbf{x}),\ \boldsymbol{\pi} \in \mathcal{P}),\ \mathbf{x} \in \mathcal{C}$, coincide, i.e.,

$$\left.\begin{array}{r} \mathbf{x}, \mathbf{x}' \in \mathcal{C} \\ \boldsymbol{\pi} \in \mathcal{P} \end{array}\right\} \ \Rightarrow\ \gamma_{\text{bio}}(\boldsymbol{\pi}|\mathbf{x}) = \gamma_{\text{bio}}(\boldsymbol{\pi}|\mathbf{x}'). \tag{33}$$

(2) Suppose that the minimum disctance of the code $\mathcal{C}$ is at least $2T+1$. The equality

$$\Lambda_{\mathcal{C}}^{\text{MAP}}(\gamma) = Q_{\text{bio}}^{(T)} \tag{34}$$

is valid if and only if the probability distributions $\gamma_{\mathbf{x},\mathbf{b}}$ are assigned in such a way that there is a vector $\mathbf{b}^* \in \mathcal{B}^*$ with the following property: for all $\mathbf{b} \in \mathcal{D}^{(T)}(\mathbf{b}^*)$,

$$\mathbf{x}' = \boldsymbol{\pi}^{-1}(\mathbf{b}) \ \Rightarrow\ \max_{\mathbf{x}\in\mathcal{C}} \gamma_{\text{bio}}(\boldsymbol{\pi}|\mathbf{x}) = \Pr_{\text{bio}}\{B = \mathbf{b}\}\gamma(\boldsymbol{\pi}|\mathbf{x}', \mathbf{b}) \tag{35}$$

and

$$\bigcup_{\mathbf{b}\in\mathcal{D}^{(T)}(\mathbf{b}^*)} \{\boldsymbol{\pi}^{-1}(\mathbf{b})\} = \emptyset \ \Rightarrow\ \max_{\mathbf{x}\in\mathcal{C}} \gamma_{\text{bio}}(\boldsymbol{\pi}|\mathbf{x}) = 0. \tag{36}$$

4.3. Examples of specific schemes

Let $n = 8$, $w = 4$, $M = 4$, and let the codewords be specified by the matrix

$$\begin{bmatrix} \mathbf{x}_1 \\ \mathbf{x}_2 \\ \mathbf{x}_3 \\ \mathbf{x}_4 \end{bmatrix} = \begin{bmatrix} 00110011 \\ 01010101 \\ 10101010 \\ 11001100 \end{bmatrix}.$$

Suppose also that the biometric vector processed at the enrollment stage is one of rows of the matrix

$$\begin{bmatrix} \mathbf{b}_1 \\ . \\ . \\ \mathbf{b}_6 \end{bmatrix} = \begin{bmatrix} 00001111 \\ 00110011 \\ 01010101 \\ 10101010 \\ 11001100 \\ 11110000 \end{bmatrix}.$$

Denote $\mathcal{C} = \{\mathbf{x}_1, \mathbf{x}_2, \mathbf{x}_3, \mathbf{x}_4\}$ and $\mathcal{B} = \{\mathbf{b}_1, \ldots, \mathbf{b}_6\}$.

Proposition 4.3 *For all pairs of vectors $(\mathbf{x}, \mathbf{b}) \in \mathcal{C} \times \mathcal{B}$,*

$$|\,\mathcal{P}(\mathbf{x} \to \mathbf{b})\,| = (4!)^2 = 576 \tag{37}$$

and

$$|\,\mathcal{P}_{\mathcal{C}\to\mathcal{B}}(\mathbf{x}\to\mathbf{b})\,| = 4(2!)^4 = 64, \tag{38}$$

where $\mathcal{P}_{\mathcal{C}\to\mathcal{B}}(\mathbf{x}\to\mathbf{b})$ *denotes the set of permutations* $\boldsymbol{\pi}\in\mathcal{P}(\mathbf{x}\to\mathbf{b})$ *such that* $\boldsymbol{\pi}(\mathbf{x}')\in\mathcal{B}$ *for all* $\mathbf{x}'\in\mathcal{C}$.

Let us illustrate our considerations by the following examples:

$$\begin{bmatrix} \boldsymbol{\pi}' \\ \boldsymbol{\pi}'(\mathbf{x}_1) \\ \boldsymbol{\pi}'(\mathbf{x}_2) \end{bmatrix} = \begin{bmatrix} 1 & 2 & 5 & 6 & 3 & 4 & 7 & 8 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix},$$

$$\begin{bmatrix} \boldsymbol{\pi}'' \\ \boldsymbol{\pi}''(\mathbf{x}_1) \\ \boldsymbol{\pi}''(\mathbf{x}_2) \end{bmatrix} = \begin{bmatrix} 1 & 2 & 6 & 5 & 3 & 4 & 7 & 8 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 0 & 1 \end{bmatrix}.$$

The permutations $\boldsymbol{\pi}'$ and $\boldsymbol{\pi}''$ belong to the set $\mathcal{P}$. Furthermore, $\boldsymbol{\pi}'(\mathbf{x}_1)=\boldsymbol{\pi}''(\mathbf{x}_1)=\mathbf{b}_1$. However $\boldsymbol{\pi}'(\mathbf{x}_2)\in\mathcal{B}$, while $\boldsymbol{\pi}''(\mathbf{x}_2)\notin\mathcal{B}$. Suppose that $\boldsymbol{\pi}'$ is the permutation stored in the database. The attacker applies this permutation to all codewords of the code $\mathcal{C}$ and constructs the list $\boldsymbol{\pi}'(\mathbf{x}_1),\ldots,\boldsymbol{\pi}'(\mathbf{x}_4)$. All entries of this list are possible biometric vectors. If the permutation $\boldsymbol{\pi}''$ is stored in the database, then the list $\boldsymbol{\pi}'(\mathbf{x}_1),\ldots,\boldsymbol{\pi}'(\mathbf{x}_4)$ contains only 2 biometric vectors. The probability of successful attack is greater in the second case, and the permutation $\boldsymbol{\pi}'$ can be considered as a "bad" permutation.

The result of the Proposition 4.3 shows that most of the permutations are bad permutations. This fact leads to the statement that the uniform probability distribution over the set $\mathcal{P}(\mathbf{x}\to\mathbf{b})$, where $\mathbf{x}$ is the selected codeword and $\mathbf{b}$ is the biometric vector, brings a rather poor performance. Namely, suppose that the probability distribution over the set $\mathcal{B}$ is uniform, i.e.,

$$\Pr_{\text{bio}}\{B=\mathbf{b}\}=1/6,\ \mathbf{b}\in\mathcal{B}.$$

Let $\mathbf{x}$ be the codeword of the code $\mathcal{C}$ used at the enrollment stage. If $\gamma_{\mathbf{x},\mathbf{b}}=\overline{\gamma}_{\mathbf{x},\mathbf{b}}$, then the permutation is uniformly chosen from the set containing 576 entries. Only 64 of these permutations have the property that the set $\boldsymbol{\pi}(\mathbf{x})$, $\mathbf{x}\in\mathcal{C}$ contains 4 biometric vectors, and the probability of successful attack is equal to $1/4$. For the other 512 permutations, the set $\boldsymbol{\pi}(\mathbf{x})$, $\mathbf{x}\in\mathcal{C}$, contains 2 biometric vectors, and the probability of successful attack is equal to $1/2$. Thus

$$\Lambda_{\mathcal{C},\overline{\gamma}}(\psi^{\text{MAP}})=\frac{64}{576}(1/4)+\frac{512}{576}(1/2)=17/36.$$

Let us assign $\gamma_{\mathbf{x},\mathbf{b}}$ as a uniform probability distribution over the set $\mathcal{P}_{\mathcal{C}\to\mathcal{B}}(\mathbf{x}\to\mathbf{b})$ consisting of 64 entries. In all cases, the list $\boldsymbol{\pi}(\mathbf{x})$, $\mathbf{x}\in\mathcal{C}$, contains 4 biometric vectors, and the probability of successful attack is equal to $1/4$. As a result, the probability of successful attack is expressed as

$$\Lambda_{\mathcal{C},\gamma}(\psi^{\text{MAP}})=\frac{64}{64}(1/4)=1/4,$$

which is approximately twice less than $\Lambda_{\mathcal{C},\overline{\gamma}}(\psi^{\text{MAP}})$. Moreover, we obtain that the lower bound $1/M$ on the probability $\Lambda_{\mathcal{C},\gamma}(\psi^{\text{MAP}})$ is attained with the equality.

Let us consider a non–uniform probability distribution over the set $\mathcal{B}$. Namely, let $a \in [1/4, 1/2]$ be a fixed parameter and let

$$\Pr_{\text{bio}}\{B = \mathbf{b}\} = \begin{cases} a, & \text{if } \mathbf{b} \in \{00001111, 11110000\}, \\ 1/4 - a/2, & \text{if } \mathbf{b} \in \mathcal{B}\backslash\{00001111, 11110000\}. \end{cases}$$

Notice that the set $\mathcal{P}_{\mathcal{C}\to\mathcal{B}}(\mathbf{x}_1 \to \mathbf{b}_1)$ contains 32 permutations $\boldsymbol{\pi}$ such that

$$\{\boldsymbol{\pi}(\mathbf{x}_1), \boldsymbol{\pi}(\mathbf{x}_2), \boldsymbol{\pi}(\mathbf{x}_3), \boldsymbol{\pi}(\mathbf{x}_4)\} = \{\mathbf{b}_1, \mathbf{b}_2, \mathbf{b}_5, \mathbf{b}_6\}$$

and 32 permutations $\boldsymbol{\pi}$ such that

$$\{\boldsymbol{\pi}(\mathbf{x}_1), \boldsymbol{\pi}(\mathbf{x}_2), \boldsymbol{\pi}(\mathbf{x}_3), \boldsymbol{\pi}(\mathbf{x}_4)\} = \{\mathbf{b}_1, \mathbf{b}_3, \mathbf{b}_4, \mathbf{b}_6\}.$$

Let us denote the subsets of these permutations by $\mathcal{P}'_{\mathcal{C}\to\mathcal{B}}(\mathbf{x}_1 \to \mathbf{b}_1)$ and $\mathcal{P}''_{\mathcal{C}\to\mathcal{B}}(\mathbf{x}_1 \to \mathbf{b}_1)$, respectively. Let
(a) $\gamma_{\mathbf{x}_1,\mathbf{b}_1}, \gamma_{\mathbf{x}_1,\mathbf{b}_6}$ be uniform probability distributions over the set $\mathcal{P}_{\mathcal{C}\to\mathcal{B}}(\mathbf{x}_1 \to \mathbf{b}_1)$;
(b) $\gamma_{\mathbf{x}_1,\mathbf{b}_2}, \gamma_{\mathbf{x}_1,\mathbf{b}_5}$ be uniform probability distributions over the set $\mathcal{P}'_{\mathcal{C}\to\mathcal{B}}(\mathbf{x}_1 \to \mathbf{b}_1)$;
(c) $\gamma_{\mathbf{x}_1,\mathbf{b}_3}, \gamma_{\mathbf{x}_1,\mathbf{b}_4}$ be uniform probability distributions over the set $\mathcal{P}''_{\mathcal{C}\to\mathcal{B}}(\mathbf{x}_1 \to \mathbf{b}_1)$.
If $\boldsymbol{\pi} \in \mathcal{P}'_{\mathcal{C}\to\mathcal{B}}(\mathbf{x}_1 \to \mathbf{b}_1)$, then the *a posteriori* probabilities associated with the biometric vectors $\mathbf{b}_1, \mathbf{b}_2, \mathbf{b}_5, \mathbf{b}_6$ are equal to

$$\frac{1}{32}(a/2, 1/2 - a/2, 1/2 - a/2, a/2).$$

However $a/2 \geq 1/2 - a/2$, and the attacker outputs either the key codeword, which is mapped to the vector $\mathbf{b}_1$, or the key codeword, which is mapped to the vector $\mathbf{b}_6$. Similar considerations can be presented for the permutations belonging to the set $\mathcal{P}''_{\mathcal{C}\to\mathcal{B}}(\mathbf{x}_1 \to \mathbf{b}_1)$. As a result, we conclude that

$$\Lambda_{\mathcal{C},\gamma}(\psi^{\text{MAP}}) = 64(a/64) = a,$$

i.e., the lower bound Q^*_{bio} on the probability $\Lambda_{\mathcal{C},\gamma}(\psi^{\text{MAP}})$ is attained with the equality.

Let us consider the error–correcting capabilities of the verifier, who processes data of a legitimate user. Let P_w denote the probability that the vector $\mathbf{b}'$ differs from the vector $\mathbf{b}$ in w positions, $w = 0, \ldots, 8$. Then, assuming that the vectors $\mathbf{b}'$ are uniformly distributed over the set of vectors located at a fixed distance from the vector $\mathbf{b}$, we obtain that the probability of correct decoding for the code $\mathcal{C}$ and the threshold $T = 2$ is equal to $\tilde{\Lambda}^{(2)}_{\mathcal{C}} = P_0 + P_1 + (16/28)P_2$, since the decoder makes the correct decision for all error patterns of weight at most 1 and for 16 error patterns of weight 2 (the total number of error patterns of weight 2 is equal to 28). Suppose that the processed biometric vectors are constructed as a concatenation of L vectors $\mathbf{b}^{(1)}, \ldots, \mathbf{b}^{(L)} \in \mathcal{B}$, i.e., the total length of the vector is equal to $8L$. Suppose also that the vectors $\mathbf{b}^{(1)}, \ldots, \mathbf{b}^{(L)}$ are independently generated according to a uniform probability distribution over the set $\mathcal{B}$. Let the verifier make the acceptance decision if and only if such a decision is made for all L entries. Then the probability of correct decision is equal to $(\tilde{\Lambda}^{(2)}_{\mathcal{C}})^L$. On the other hand, the probability of successful attack, when the probability distributions $\gamma_{\mathbf{x},\mathbf{b}}$ are used is equal to $(1/4)^L$.

Table 3. Transformation of vectors of length $n = 4$ and weights 0,1,3,4 to balanced vectors, where $\tilde{w}, w$ are the Hamming weights of the vectors $\tilde{\mathbf{b}}, \mathbf{b}$ and i is the length of the prefix of the vector $\tilde{\mathbf{b}}$, which has to be inverted to obtain the vector $\mathbf{b}$.

$\tilde{\mathbf{b}}$	$\tilde{w}$	i	$\mathbf{b}$	w	$\tilde{\mathbf{b}}$	$\tilde{w}$	i	$\mathbf{b}$	w
0000	0	2	1100	2	1111	4	2	0011	2
0001	1	1	1001	2	1110	3	1	0110	2
0010	1	1	1010	2	1101	3	1	0101	2
0100	1	1	1100	2	1011	3	1	0011	2
1000	1	3	0110	2	0111	3	3	1001	2

4.4. Implementation of the permutation coding

The fixed Hamming weight of the possible biometric vectors is the constraint that has to be satisfied to implement the permutation block coding scheme. It can be done if the observer takes into account only a fixed number of the most reliable biometric parameters. For example, in the case of processing fingerprints, one can put an $n_1 \times n_2$ grid on the 2-dimensional plane (in this case, $n = n_1 n_2$) and register the w most reliable minutiae points in the cells of that grid. In general case, the biometric binary vector of length n can be viewed as a vector of n features where positions of 1's index the features that are present in the outcomes of the measurements. The total number of the most reliable features taken into account by the authentication scheme can be fixed in advance.

Another useful possibility is known as balancing arbitrary binary vector by the inversion of its prefix in such a way that the obtained vector has weight $\lfloor n/2 \rfloor$. The corresponding statement is presented below, and the examples of the transformation are given in Table 3.

Proposition 4.4 *For any binary vector $\tilde{\mathbf{b}} \in \{0,1\}^n$, one can find an index $i \in \{0,\dots,n\}$ in such a way that the vector $\tilde{\mathbf{b}}$ is transformed to a balanced vector by the inversion of the first i components, i.e.,*

$$(i - \tilde{w}_i) + \tilde{w} - \tilde{w}_i = \lfloor n/2 \rfloor,$$

where $\tilde{w}$ and $\tilde{w}_i$ denote the Hamming weight of the vector $\tilde{\mathbf{b}}$ and the Hamming weight of the prefix of length i of the vector $\tilde{\mathbf{b}}$, respectively.

The proof directly follows from the observation that the path on the plane whose coordinates are defined as $(j, \tilde{w}_j)$, $j = 0,\dots,n$, starts at the point $(0, \mathrm{wt}(\mathbf{b}))$, ends at the point $(n, n - \mathrm{wt}(\mathbf{b}))$, and has increments ± 1. Therefore, there is at least one index i such that $\tilde{w}_i = \lfloor n/2 \rfloor$.

Notice that the case $w = \lfloor n/2 \rfloor$ can be viewed as the most interesting one meaning the characteristics of the permutation block coding scheme. The claim of the Proposition 4.4 shows that an additional storing of the value of the parameter i used to transform an arbitrary binary vector to a vector belonging to the set $\{0,1\}^n_{\lfloor n/2 \rfloor}$ makes the implementation of such a scheme possible in general.

4.5. Conclusion

The mapping of the pair $(\mathbf{x}, \mathbf{b})$ to a binary string stored in the database can be viewed as the encryption of the message $\mathbf{b}$, which is parameterized by a key codeword $\mathbf{x} \in \mathcal{C}$ chosen at random. An interesting point is the possibility of decreasing the probability of successful attack, when an attacker tries to pass through the authentication stage with the acceptance decision, by using a randomized mapping, although *the values of additional random parameters are public*. In the permutation block coding scheme, a randomly chosen permutation that transforms the vector $\mathbf{x}$ to the vector $\mathbf{b}$ is used for these purposes. As the set of possible permutations has the cardinality, which is exponential in the length of the vectors, a designer has good chances to hide many of biometric vectors that differ from the most likely vector $\mathbf{b}^*$ into the information that can correspond to the vector $\mathbf{b}^*$. Thus, one can even reach exactly the same secrecy of the coded system as the secrecy of the blind guessing of the biometric vector, when the attacker does not have access to the database and is ignorant about the code. In other words, one can talk about the possibility of constructing permutation block coding schemes that have *a perfect algorithmic secrecy*. This notion is different from the usual definition of perfectness, which is understood as the point that the conditional entropy of the probability distribution over the key codewords, given the content of the database, is equal to $\log M$. In our example presented in the previous subsection, the *a posteriori* probability distribution over the key codewords certainly depends on a particular permutation, and the conditional entropies of these distributions can be much less than the entropy of a uniform probability distribution. Nevertheless, an optimum attacker cannot use this fact, and his observations do not introduce changes in the decoding algorithm.

4.6. Proofs

Proof of Proposition 4.1

Let us rewrite (27) as

$$\Lambda_{\mathcal{C},\gamma}(\psi) = \frac{1}{M} \sum_{\boldsymbol{\pi} \in \mathcal{P}} \lambda_{\mathcal{C},\gamma}(\psi(\boldsymbol{\pi})),$$

where

$$\begin{aligned} \lambda_{\mathcal{C},\gamma}(\psi(\boldsymbol{\pi})) &\stackrel{\triangle}{=} \sum_{\mathbf{x} \in \mathcal{C}} \sum_{\mathbf{b}} \Pr_{\text{bio}}\{B = \mathbf{b}\} \gamma(\boldsymbol{\pi}|\mathbf{x}, \mathbf{b}) \chi\{\, \hat{\mathbf{x}}[\boldsymbol{\pi}^{-1}(\psi(\boldsymbol{\pi}))] = \mathbf{x} \,\}. \\ &= \sum_{\mathbf{x} \in \mathcal{C}} \gamma_{\text{bio}}(\boldsymbol{\pi}|\mathbf{x}) \chi\{\, \hat{\mathbf{x}}[\boldsymbol{\pi}^{-1}(\psi(\boldsymbol{\pi}))] = \mathbf{x} \,\}. \\ &\leq \max_{\mathbf{x} \in \mathcal{C}} \gamma_{\text{bio}}(\boldsymbol{\pi}|\mathbf{x}). \end{aligned}$$

and the inequality follows from the observation that $\hat{\mathbf{x}}[\boldsymbol{\pi}^{-1}(\psi(\boldsymbol{\pi}))]$ is a codeword of the code $\mathcal{C}$. This inequality is tight if $\psi(\boldsymbol{\pi}) = \psi^{\text{MAP}}(\boldsymbol{\pi})$, where $\psi^{\text{MAP}}(\boldsymbol{\pi})$ is defined in (28). Hence,

$$\lambda_{\mathcal{C},\gamma}(\psi(\boldsymbol{\pi})) \leq \lambda_{\mathcal{C},\gamma}(\psi^{\text{MAP}}(\boldsymbol{\pi}))$$

and $\Lambda_{\mathcal{C},\gamma}(\psi^{\text{MAP}})$ is expressed by (30).

Proof of Proposition 4.2

(1): We write

$$\sum_{\boldsymbol{\pi}\in\mathcal{P}} \max_{\mathbf{x}\in\mathcal{C}} \gamma_{\text{bio}}(\boldsymbol{\pi}|\mathbf{x}) \geq \max_{\mathbf{x}\in\mathcal{C}} \sum_{\boldsymbol{\pi}\in\mathcal{P}} \gamma_{\text{bio}}(\boldsymbol{\pi}|\mathbf{x}) = 1, \tag{39}$$

where the equality follows from (31). By (30), this inequality implies

$$\Lambda_{\mathcal{C},\gamma}(\psi^{\text{MAP}}) \geq \frac{1}{M}$$

with the equality if and only if the inequality (39) is tight. The latter condition is satisfied when the maximum of $\gamma_{\text{bio}}(\boldsymbol{\pi}|\mathbf{x})$ is attained at the same codeword for all permutations $\boldsymbol{\pi} \in \mathcal{P}$, which is equivalent to (33).

(2): Let us fix a vector $\mathbf{b}^* \in \mathcal{B}^*$ and denote

$$\mathcal{P}_{\mathcal{C}}(\mathbf{b}^*) \stackrel{\triangle}{=} \bigcup_{\mathbf{x}\in\mathcal{C}} \bigcup_{\mathbf{b}\in\mathcal{D}^{(T)}(\mathbf{b}^*)} \mathcal{P}(\mathbf{x}\to\mathbf{b}).$$

Then

$$\begin{aligned}
\sum_{\boldsymbol{\pi}\in\mathcal{P}} \max_{\mathbf{x}\in\mathcal{C}} \gamma_{\text{bio}}(\boldsymbol{\pi}|\mathbf{x}) &\stackrel{\text{(a)}}{\geq} \sum_{\boldsymbol{\pi}\in\mathcal{P}_{\mathcal{C}}(\mathbf{b}^*)} \max_{\mathbf{x}\in\mathcal{C}} \gamma_{\text{bio}}(\boldsymbol{\pi}|\mathbf{x}) \\
&\stackrel{\text{(b)}}{=} \sum_{\mathbf{x}'\in\mathcal{C}} \sum_{\mathbf{b}\in\mathcal{D}^{(T)}(\mathbf{b}^*)} \sum_{\boldsymbol{\pi}\in\mathcal{P}(\mathbf{x}'\to\mathbf{b})} \max_{\mathbf{x}\in\mathcal{C}} \gamma_{\text{bio}}(\boldsymbol{\pi}|\mathbf{x}) \\
&\stackrel{\text{(c)}}{\geq} \sum_{\mathbf{x}'\in\mathcal{C}} \sum_{\mathbf{b}\in\mathcal{D}^{(T)}(\mathbf{b}^*)} \sum_{\boldsymbol{\pi}\in\mathcal{P}(\mathbf{x}'\to\mathbf{b})} \gamma_{\text{bio}}(\boldsymbol{\pi}|\mathbf{x}') \\
&\stackrel{\text{(d)}}{=} \sum_{\mathbf{x}'\in\mathcal{C}} \sum_{\mathbf{b}\in\mathcal{D}^{(T)}(\mathbf{b}^*)} \sum_{\boldsymbol{\pi}\in\mathcal{P}(\mathbf{x}'\to\mathbf{b})} \Pr_{\text{bio}}\{B=\mathbf{b}\}\gamma(\boldsymbol{\pi}|\mathbf{x}',\mathbf{b}) \\
&\stackrel{\text{(e)}}{=} \sum_{\mathbf{x}'\in\mathcal{C}} \sum_{\mathbf{b}\in\mathcal{D}^{(T)}(\mathbf{b}^*)} \Pr_{\text{bio}}\{B=\mathbf{b}\}Q^*_{\text{bio}} \\
&= MQ^{(T)}_{\text{bio}},
\end{aligned}$$

where (a) follows from $\mathcal{P}_{\mathcal{C}}(\mathbf{b}^*) \subset \mathcal{P}$; (b) follows from the observation that $\mathcal{P}(\mathbf{x}' \to \mathbf{b})$, $\mathbf{b} \in \mathcal{D}^{(T)}(\mathbf{b}^*)$, $\mathbf{x}' \in \mathcal{C}$, are pairwise disjoint sets; (c) $\max_{\mathbf{x}\in\mathcal{C}} \gamma_{\text{bio}}(\boldsymbol{\pi}|\mathbf{x}) \geq \gamma_{\text{bio}}(\boldsymbol{\pi}|\mathbf{x}')$; (d) substitution of (29); (e) follows from (31).

Proof of Proposition 4.3

Suppose that $(\mathbf{x},\mathbf{b}) = (\mathbf{x}_1,\mathbf{b}_1)$, i.e., $\mathbf{x} = 00110011$ and $\mathbf{b} = 00001111$. Equality (37) immediately follows from the fact that both $\mathbf{x}$ and $\mathbf{b}$ contain 4 zeroes and 4 ones. Notice that $\boldsymbol{\pi}(\mathbf{x}_1) \in \mathcal{B}$ implies $\boldsymbol{\pi}(\mathbf{x}_4) \in \mathcal{B}$, and $\boldsymbol{\pi}(\mathbf{x}_2) \in \mathcal{B}$ implies $\boldsymbol{\pi}(\mathbf{x}_3) \in \mathcal{B}$. Therefore,

$$\mathcal{P}_{\mathcal{C}\to\mathcal{B}}(\mathbf{x}\to\mathbf{b}) = \{\, \boldsymbol{\pi} \in \mathcal{P}(\mathbf{x}_1 \to \mathbf{b}_1) :\ \boldsymbol{\pi}(\mathbf{x}_2) \in \mathcal{B} \,\}.$$

If $\boldsymbol{\pi} \in \mathcal{P}(\mathbf{x}_1 \to \mathbf{b}_1)$ and $\boldsymbol{\pi} = (\pi_1, \ldots, \pi_8)$, then $(\pi_1, \ldots, \pi_4)$ is a permutation of components of the vector $(1, 2, 5, 6)$ and $(\pi_5, \ldots, \pi_8)$ is a permutation of components of the vector $(3, 4, 7, 8)$.

The condition $\pi(\mathbf{x}_2) \in \mathcal{B}$ is satisfied if and only if there is a vector $\mathbf{s} \in \{0011, 0101, 1010, 1100\}$ with the following property: the first 4 components of the vector $\boldsymbol{\pi}$ and the last 4 components of the vector $\boldsymbol{\pi}$ specify the permutations of columns of the matrices

$$\begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 \end{bmatrix} \text{ and } \begin{bmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 \end{bmatrix}$$

such that the 2-nd rows are equal to the vector $\mathbf{s}$. There are 4 possible vectors $\mathbf{s}$ and each vector can be constructed by $(2!)^4$ permutations. Therefore, this observation proves (38) for $(\mathbf{x}, \mathbf{b}) = (\mathbf{x}_1, \mathbf{b}_1)$. By the symmetric properties of the sets $\mathcal{C}$ and $\mathcal{B}$, one can see that considerations above also prove the statement for any fixed pair $(\mathbf{x}, \mathbf{b}) \in \mathcal{C} \times \mathcal{B}$.