Nonlinear Fuzzy Commitments with Kerdock Codes

Patrick Lacharme

Journées du GDR Securité

26 Juin 2023

Authentication of biometric templates

What is a biometric template ?

In this talk, a biometric template b is considered as a set of elements in $\mathbf{F}_2 = \{0, 1\}$ of fixed length n and the distance used for comparison of two templates is the Hamming distance d_H.

This assumption is not really restrictive : there exists binarization systems for many modalities as for iris, speaker or face recognition.

Authentication of a fresh template

The reference template b, acquired during enrolment, and the fresh template b' are compared with a threshold τ :
If $d_H(b, b') \leq \tau$, the authentication is successfull.

Encryption ? If the reference template is encrypted, it should be decrypted for comparison with the fresh template.
$\Longrightarrow$ Templates are not protected during the verification.

Errors correcting codes

Definition of a (block) code and minimum distance

A (n, K, d)-code is a subset of K elements of $\mathbf{F}_2^n$ such that the Hamming distance between two elements is $\geq d$.
In this case, d is called the minimum distance of the code.

Minimum distance decoding

1. A codeword c is transmitted on a noisy channel and is recovered as $x = c \oplus e \in (\mathbf{F}_2)^n$, where e is an error.
2. x is decoded into c, or an other codeword c' or FAILURE, depending if the Hamming weight $w_H(e)$ of e is small or large.

If $w_H(e)$ is small, there are no other codewords close to x.
Else, x can be close to c' or far from any codewords.

Consequence : a $(n, K, 2t + 1)$ code can correct t errors.

Fuzzy commitments (Juels and Wattenberg, 1999)

Enrolment

Let C be a (n, K, d) binary code with $d = 2t + 1$. The user sends $P = c \oplus b$ and $H(c)$ to the server, where b is the reference template, H is a hash function and $c \in C$ is a random secret codeword.

Authentication

The user sends his fresh template b' to the server, which computes $P \oplus b'$. The server decodes it in a codeword c' (or FAILURE) and controls if $c = c'$ by verifying $H(c) = H(c')$.

The threshold of comparison is related to the distance of the code : b' is accepted if and only if $d_H(b, b') \leq t$.

A key binding scheme : A secret key $K \in \{0, 1\}^k$ is encoded in a codeword c, masked with b and recovered with b' if $d_H(b, b') \leq t$.

Implementation of fuzzy commitments

The choice of the code strongly depends on the performance of the biometric data (intraclass and interclass rates) :

Linear codes used in fuzzy commitments

- Daugman *et al.* (2005), Rathgeb and Uhl (2009) : Reed Solomon and Hadamard Codes.
- Yang and Verbauwhede (2007), Maiorana and Campisi (2010), Bajaber *et al.* (2022) : BCH codes only.
- Bringer *et al.* (2007) : Reed-Mullers codes RM(1, m).

Two types of implementation are considered :

1. A code with length equal to the length of the template.
2. A combination of two codes.

Without loss of generalities, we consider in this talk the second one

Attack in undistinguishability (Simoens *et al.*, 2009)

Let C be a $[n, k, 2t+1]$ linear binary code, with $c_1, c_2 \in C$.
The attacker possesses $b_1 \oplus c_1, H(c_1)$ and $b_2 \oplus c_2$, $H(c_2)$.

Is it possible to know if the biometric templates b_1 and b_2 come from the same person or not ?

Description of the attack

The attacker computes $b_1 \oplus b_2 \oplus c_1 \oplus c_2 = e \oplus c_1 \oplus c_2$.

1. If $d_H(b_1, b_2) = e \leq t$, then $e \oplus c_1 \oplus c_2$ is decodable.
2. If $d_H(b_1, b_2) = e > t$, then $e \oplus c_1 \oplus c_2$ is decodable or not.

If $e \oplus c_1 \oplus c_2$ is decodable, the attacker cannot conclude (because $H(c_2 \oplus c2)$ is unknown). Nevertheless, if $e \oplus c_1 \oplus c_2$ is not decodable, then the attacker can conclude that $d_H(b_1, b_2) = e > t$.

A linear code with an high minimum distance is vulnerable.

Consequence on the attack in undistinguishability

A non linear code as solution ?

The previous attacks works because $c_1 \oplus c_2$ is a codeword, due to the linearity of the code. **Could we use a non linear code ?**

First problem

In a non linear code C the properties $\forall c_1, c_2 \in C, c_1 \oplus c_2 \in C$ is false, but it does not garanties that it doesn't exist some c_1 and $c_2 \in C$ such that $c_1 \oplus c_2 \in C$.

Second problem

Even if $c_1 \oplus c_2$ is not in C, if $w_H(c_1 \oplus c_2)$ is low, the attack could be again successfull.
The attack is not possible if $d_H(c_1 \oplus c_2, C) \geq t = \lfloor (d-1)/2 \rfloor$.

Non-linearity of random codes

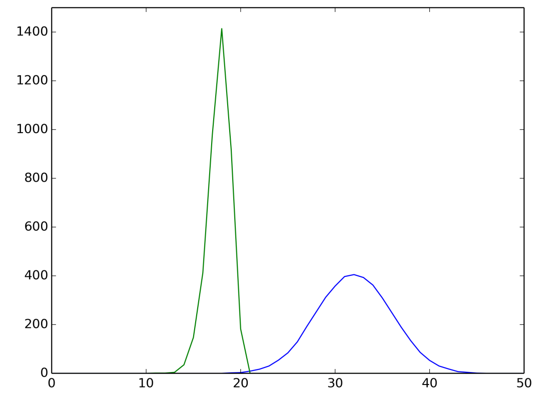

FIGURE – Distance and non-linearity of [64, 4096] random codes

Non-linearity distribution

Non-linearity distribution

Let C be a (n, K, d) code. The non-linearity distribution $D = (D_0 \dots, D_n)$ of the code C is defined by

$$D_i = \frac{1}{K} \sharp \{(c_1, c_2) \in C \mid d_H(c_1 \oplus c_2, C) = i\},$$

where $d_H(c_1 \oplus c_2, C) = \min_{c \in C} d_H(c_1 \oplus c_2, c)$.

Problem : decoding algorithms of random codes are not efficient.

Kerdock codes as solution ?

Kerdock codes are non linear codes which have an efficient decoding algorithm. Whats about their non linearity distribution ?

Boolean functions

Definition of Boolean functions and ANF

A Boolean function with n variables is a map from $(\mathbf{F}_2)^n$ to $\mathbf{F}_2$. It is defined either by a truth table or by a multivariate polynomial (called ANF) in the set $\mathbf{F}_2[x_1, \dots x_n]/(x_1^2 + x_1, \dots, x_n^2 + x_n)$.

Example : let $f : (\mathbf{F}_2)^3 \rightarrow \mathbf{F}_2$ defined by the ANF $f(x_1, x_2, x_3) = x_1x_2 + x_2x_3 + x_3$. The truth table is 11100010 because $f(0,0,0) = 0$, $f(0,0,1) = 1$, $f(0,1,0) = 0$, $f(0,1,1) = 0$, ...

Definition of bent functions

A Boolean function f with m variables is *bent* if and only if m is even and if the Hamming distance between f and linear functions is $2^{m-1} - 2^{\frac{m}{2}-1}$ or $2^{m-1} + 2^{\frac{m}{2}-1}$

Construction of Kerdock codes

Definition : $RM(1, m)$ is the set of linear Boolean functions and $RM(2, m)$ is the set of linear or quadratic Boolean functions.

Kerdock Set

Let $N = 2^{m-1} - 1$ and $f_1, \dots, f_N$ be quadratic bent functions with m variables, such that the sum of any pair of functions $f_i \oplus f_j$ is bent. Then the set $\{f_1, \dots, f_N\}$ is called a *Kerdock set*.

Kerdock code

The Kerdock code $K(m)$, with m even, is the subcode of $RM(2, m)$ defined by $RM(1, m) \cup (f_1 \oplus RM(1, m)) \cup \dots \cup (f_N \oplus RM(1, m))$.

$K(m)$ is a $(2^m, 2^{2m}, 2^{m-1} - 2^{\frac{m}{2}-1})$ nonlinear code, with parameters close to the linear Hadamard code or RM(1,m).

Non linearity distribution of Kerdock codes

Let m be an even number and the Kerdock set $\{f_1, \dots, f_{2^{m-1}-1}\}$, of $2^{m-1} - 1$ bent functions, defining the Kerdock code $K(m)$.

Theorem

The nonlinearity distribution of the Kerdock code is given by $D_0, \dots, D_K$ where all coefficients between D_1 and $D_{2^{m-2}-1}$ are null. Moreover if the sum of two bent functions of the Kerdock set is not in the Kerdock set, then we have $D_0 = 2^{m+1} + 2^{m+2} - 8$ and $\sum_{i \geq 2^{m-2}} D_i = (2^m - 2)(2^m - 4)$.

Interpretation

D_0 comes mainly from the linear subcode $RM(1, m)$. But 2^{m-2} is greater than the error-correcting capacity of the code !
D_0 is asymptotically negligeable compared to $\sum_{i \geq 2^{m-2}} D_i$.

Application to the (16, 64) code $K(4)$

There exist 28 *cosets* $f_i \oplus RM(1,4)$ in $RM(2,4)$, where f_i are quadratic bent functions with 4 variables (without linear part).

Let $G(4)$ be the graphe composed of 28 vertices f_i, where an edge between two vertices f_i and f_j means that $f_i \oplus f_j$ is bent.

An exhaustive search of cliques in this graphe provides a lot of cliques of order 3 and 8 cliques of order 7 :

- Cliques of order 3 are just composed by $(f_i, f_j, f_i \oplus f_j)$
- Each cliques of order 7 provide a Kerdock set (of cardinal $7 = 2^{4-1} - 1$) for Kerdock codes $K(4)$, verifying in all cases the distribution $D_0 = 88$ and $D_4 = 168$.

Interpretation

The previous theorem is incomplete, the non linearity distribution of all $K(4)$ has only two weights !
For $K(6)$ we also have $D_0 = 374$ and $D_{16} = 3720$.

Linear construction (Hammons *et al.*, 1992)

A Kerdock code can be seen as an image of a cyclic (linear) code on $\mathbb{Z}_4$, by the Gray map : $\mathbb{Z}_4 \to \mathbf{F}_2^2$. This cyclicity provides an efficient encoding/decoding procedure, based on LFSR on $\mathbb{Z}_4$.

It is not exactly the same Kerdock code than previously (for example codewords are not necessary quadratic).

Experiments

Our experiments on $K(4)$ and $K(6)$, constructed from these $\mathbb{Z}_4$ linear codes, provide the same nonlinearity distribution.

Parameters and numerical results :

$H(6)$ and $RM(1,6)$ are $(64, 128, 32)$ code, whereas $K(6)$ is a $(64, 4096, 28)$ code.
Success probability by block : $p_{H(6)} \simeq 0.998$ by block for $H(6)$ and $RM(1,6)$ against $p_{K(6)} \simeq 0.09$ by block for $K(6)$.

Conclusion

Parameters similar to linear codes.

Parameters of $K(m)$ are close to Hadamard codes $H(m)$ or Reed Muller $RM(1,m)$, used in fuzzy commitment schemes.

Resistance against undistinguishability.

Kerdock codes provide a good resistance against attacks in undistinguishability, due to their non linearity distribution.

Efficiency of the construction.

The construction of Hammons *et al.* provides an efficient decoding procedure, as for any cyclic linear codes.

Thank you ! Questions ?