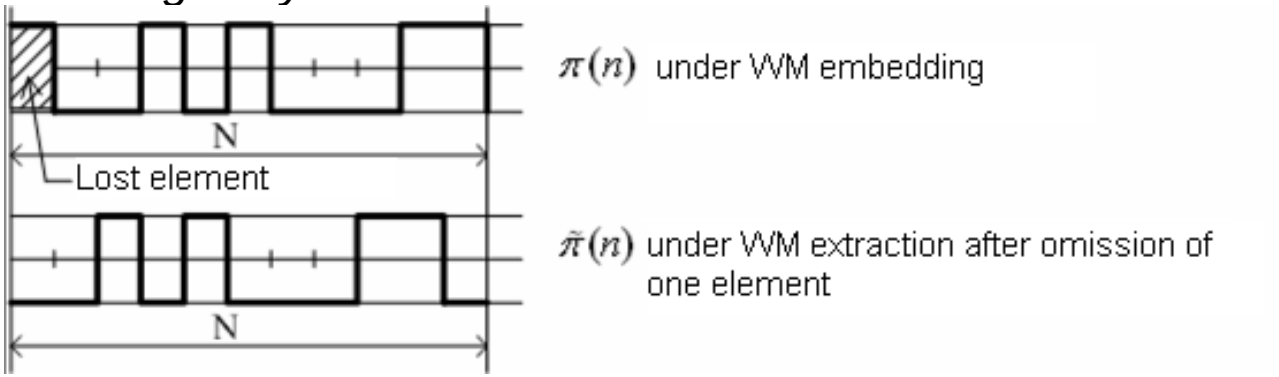
Lecture 12. Breaking of WM synchronization

The needs of synchronization*:*

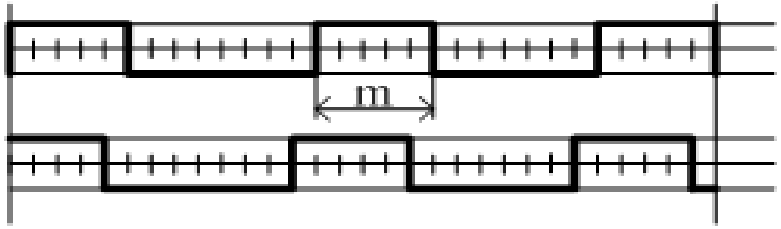
- PRS *π(n), n=1,2…* for additive embedding in CO,
- PRS *π(n), n=1,2…* for WM embedding based on FH concept.

Breaking of synchronization:



Decoder: $\frac{1}{N}\sum_{n=1}^{N}\pi(n)\tilde{\pi}(n)\approx 0$ (WM is not extracted).

Commonly used protection method (block repetition code):



$$\left.\begin{matrix}\pi(n)\\ \tilde{\pi}(n)\end{matrix}\right\}\frac{1}{N}\sum_{n=1}^{N}\pi(n)\tilde{\pi}(n)\approx 1$$

Defects:

- reducing of embedding rate at *m* times,
- degradation of WM robustness against estimation attack.

The main attacks breaking WM synchronization:

1) Resizing of images
2) Cropping of images
3) Rotation of images
4) Warping of images
5) Row -column copy attack for images .Sample repetition for audio CO
6) Row-column blanking for images and removal of samples for audio CO.

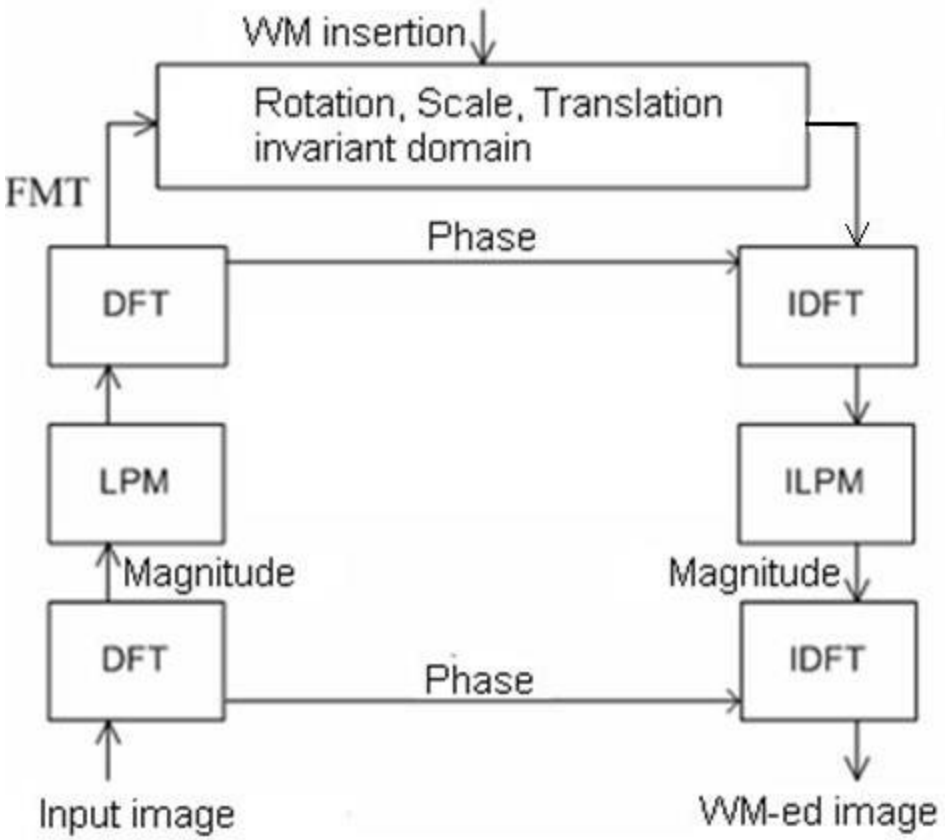
General principle of WM protection against desynchronization attacks.

1. Resizing attack.
Initially the image is resized as it is needed to extract WM and next the image is recovered by the use interpolation technique
WM occurs robust against such attack if it is used an embedding of redundant WM (like binary Logo see Lecture 8)

2. Cropping of image parts.
Image cannot be interpolated . WM is robust as well as in the first attack for redundant messages [20]. (See also Lecture 9)

3. Image rotation.
Under the rotation at 90 and 180 degree , WM can be extracted reliable if it was embedded in DWT coefficients [20].
For small rotation degree and for embedding in pixel domain the attack degree can be found and then original image can be recovered with the used of special pilot signal embedded in CO and determined by stegokey. (See also Lecture 9)

It can be used also transforms that are invariant to rotation (embedding WM in DFT amplitude). If both rotation and scaling along axis is applied in attack then WM occurs robust with embedding after *Fourier-Mellin transform* shown below.



LPM – Log-polar mapping
FMT – Fourier Mellin Transform

But our experience says that after application of LPM and next ILPM images are corrupted even without WM embedding.

4. Image warping. (see “Checkmark Benchmarking Tool.”)
WM can be extracted reliably if it has large redundancy and with embedding after DWT where is used Haar function
[20].

5*. Removal of audio CO samples.*
Let us consider common protection against such attacks.

Selection of so called "silent points " - SP [20].
The main idea – to find such samples of audio signal that after their removal very large distortion of CO arises. These points (SP) are used later in order to synchronize PRS in embedding of SS-based WM.

The main criterion to find SP – sharp increasing of WM sample energy :

If $\frac{E_a(n_0)}{E_b(n_0)} \geq \lambda_1$ and $E_a \geq \lambda_2$, where $E_b(n_0) = \sum_{i=-r}^{-1} C^2(n_0 + i), E_a(n_0) = \sum_{i=0}^{r-1} C^2(n_0 + i),$

where λ_1, λ_2, r – some parameters, then n_0 is assumed as "a candidate" in SP set.

Next a group of candidates in a set of SP is produced and it is selected as real SP such sample n_0, that has maximum *energy increasing* $E_a(n_0)/E_b(n_0)$.

Collusion attacks. Fingerprinting.

Two main types of collusion attacks:

1. If the same WM was used with different CO
2. If different WMs were used with the same CO (Fingerprinting).

1. The same WM with different CO.

$$\left.\begin{aligned} C_{w1}(n) &= C_1(n) + w(n) \\ C_{w2}(n) &= C_2(n) + w(n) \\ &\dots \\ C_{wL}(n) &= C_L(n) + w(n) \end{aligned}\right\}$$

$$n = 1,2,\dots N; w(n) \in \{-1,1\}, i.i.d.$$

Attack:

$$C'_{wi}(n) = C_{wi}(n) - \tilde{w}(n) + \varepsilon(n), \quad (23)$$

where $\tilde{w}(n) = \frac{1}{K}\sum_{j \in S_c} C_{wj}(n)$,

S_c – the set of user's number belonging to collusion group of the size K,

$\varepsilon(n)$ – additive noise.

where K – is the number of user which take part in collusion attack.

Attack's goals:

1. Make impossible to extract WM .
2. Make impossible to trace the participants of collusion attack.

Performance evaluation to reach the first goal:

$$C'_{wi}(n) = C_{wi}(n) - \tilde{w}(n), \quad \text{where} \quad \tilde{w}(n) = \frac{1}{K}\sum_{j \in S_c} C_{wj}(n) = \frac{1}{K}\sum_{j \in S_c} C_j(n) + w(n)$$

$$\Lambda_i = \sum_n (C'_{wi}(n) - C_i(n))w(n) = \sum_n (C_{wi}(n) - \tilde{w}(n) - C_i(n))w(n) =$$

$$= \sum_n (C_i(n) + w(n) - w(n) - \frac{1}{K}\sum_{j \in S_c} C_j(n) - C_i(n))w(n) = \sum_n (\frac{1}{K}\sum_{j \in S_c} C_j(n))w(n) =$$

$$= \sum_n S(n)w(n), \quad \text{where} \quad S(n) = \frac{1}{K}\sum_{j \in S_c} C_j(n). \qquad (24)$$

Conclusion: Since *S(n), n=1,2,…N* is not connected with *w(n)* then extraction of WM is impossible.

Performance evaluation to reach the second goal:

$$\Lambda_{iK} = \sum_n (C'_{wi}(n) - C_i(n))C_k(n) = \sum_n (\frac{1}{K}\sum_{j \in S_c} C_j(n))C_k(n) \qquad (25)$$

If $K \in S_c$ (*k-th user takes part in attack*), then

$$E\{\Lambda_{ik}\} = \frac{N}{K}\sigma_c^2 > 0.$$

If $K \notin S_c$ (*k-th* user does not take part in attack), then $E\{\Lambda_{ik}\} = 0.$

Conclusion: Tracing of the *k-th* user that took part in attack is possible but the owner of WM is unable to prove in a court that his (her) WM has been in fact embedded namely in this CO.

Remark 1. The conclusion above keeps true regardless of the fact if the user took part in attack or his (her) watermarked CO has been used by attackers without his (her) permission.

Remark 2: If the owner applies blind decoder for tracing of the *k-th* user:

$$\Lambda'_{ik} = \sum_n C_{wi}(n)w(n) = \sum_n (C_i(n) - \frac{1}{K}\sum_{j \in S_c} C_j(n))C_{wi}(n),$$

Then WM also cannot be detected and besides of them the *i-th* user will be found as attacker always .

Ratio S/N after attack:

$$\eta_a = \frac{\sigma_c^2}{Var\{\frac{1}{K}\sum_{j \in S_c} C_j(n)\}} = K, \quad \text{(if } C_j(n) \text{ are mutual independent).} \qquad (26)$$

We can see from (26) that CO quality degenerates significantly for small *K*.

2. Attack for different 0-bit WM with the same CO.

$$\left.\begin{aligned} C_{w1}(n) &= C(n) + w_1(n) \\ C_{w2}(n) &= C(n) + w_2(n) \\ &\dots \\ C_{wL}(n) &= C(n) + w_L(n) \end{aligned}\right\}$$

$$n = 1,2,\dots N; w_i(n) \in \{-\alpha, \alpha\}$$

Attack:

$$C'_w(n) = \frac{1}{K}\sum_{j \in S_c} C_{wj}(n) + \varepsilon(n), |S_c| = K, \qquad (27)$$

$$\varepsilon(n) \notin i.i.d., E\{\varepsilon(n)\} = 0, Var\{\varepsilon(n)\} = \sigma_\varepsilon^2.$$

Informed decoder for tracing of the i-th attacker .

$$\left.\begin{aligned} \Lambda_i > \lambda &\Rightarrow i \in S_c \\ \Lambda_i < \lambda &\Rightarrow i \notin S_c \end{aligned}\right\} \Lambda_i = \sum_{n=1}^{N} (C'_w(n) - C(n)) w_i(n) = \sum_{n=1}^{N} (\frac{1}{K}\sum_{j \in S_c} w_i(n) + \varepsilon(n)) w_i(n), \qquad (28)$$

$$\Lambda_{i1} \in N(E\{\Lambda_{i1}\}, Var\{\Lambda_{i1}\}), \Lambda_{i0} \in N(E\{\Lambda_{i0}\}, Var\{\Lambda_{i0}\}),$$

where $\Lambda_{i1} \to i \in S_c, \Lambda_{i0} \to i \notin S_c.$

$$P_{mi} = Q\left(\frac{E\{\Lambda_{i1}\} - \lambda}{\sqrt{Var\{\Lambda_{i1}\}}}\right) -$$ *the probability of undetecting for i-th* user($i \in S_c$) (29)

$$P_{fai} = 1 - Q\left(\frac{E\{\Lambda_{i0}\} - \lambda}{\sqrt{Var\{\Lambda_{i0}\}}}\right) -$$ *the probability* of false detecting of *i-th* user ($i \notin S_c$) (30)

$$E\{\Lambda_{i1}\} = E\{\sum_{n=1}^{N}(((\frac{1}{K}\sum_{j\in S_c} w_j(n)) + \varepsilon(n))w_i(n))\} = \frac{\alpha^2 N}{K},$$

$$Var\{\Lambda_{i1}\} = N(\sigma_\varepsilon^2\alpha^2 + \frac{\alpha^4(K-1)}{K^2}),$$ (31)

$$E\{\Lambda_{i0}\} = 0, Var\{\Lambda_{i0}\} = N(\sigma_\varepsilon^2\alpha^2 + \frac{\alpha^4}{K}).$$

$$P_{mi} = Q(\frac{\frac{\alpha^2 N}{K} - \lambda}{\sqrt{N(\sigma_\varepsilon^2\alpha^2 + \frac{\alpha^4(K-1)}{K^2})}}),$$ (32)

$$P_{fai} = 1 - Q(\frac{-\lambda}{\sqrt{N(\sigma_\varepsilon^2\alpha^2 + \frac{\alpha^4}{K})}})$$ (33)

Threshold $\lambda = \lambda_0$, that gives $P_{mi} = P_{fai}$:

$$\lambda_o = \frac{\alpha^2 N / K}{\left(\sqrt{\frac{K^2\sigma_\varepsilon^2 + \alpha^2(K-1)}{K^2\sigma_\varepsilon^2 + K\alpha^2}}\right) + 1}.$$

If the size of coalition $K>>1$, then:

$$\lambda_o = \frac{\alpha^2 N}{2K}$$

A quality of CO just after WM embedding and after collusion attack in terms of *signal –to-noise ratio is* η_w and η_a, respectively:

$$\eta_w = \frac{\sigma_c^2}{\alpha^2}, \qquad (16) \qquad \eta_a = \frac{\sigma_c^2}{Var\{C(n) - C'_w(n)\}} = \frac{\sigma_c^2}{\sigma_\varepsilon^2 + \frac{\alpha^2}{K}}.$$

For optimal threshold and $K>>1$ we get the following relation for $P_e = P_{mi} = P_{fai}$:

$$P_e = Q\left(\frac{1}{2}\sqrt{\frac{N}{K^2\eta}}\right),$$

where $\eta = \frac{\eta_w}{\eta_a}$, it is naturally to take $\eta=1$, because $\eta<1$ be suspicious.

Important conclusion: A compensation of collusion attack by group of K «pirates» results in an increasing N at K^2 times.

The use of orthogonal signals $w_i(n)$, $n=1,2\ldots$

$$\sum_{n=1}^{N} w_i(n)w_j(n) = \begin{cases} \alpha^2 N, i = j, \\ 0, i \neq j. \end{cases}$$

$$E\{\Lambda_{i1}\} = \frac{\alpha^2 N}{K}, E\{\Lambda_{i0}\} = 0, Var\{\Lambda_{i1}\} = N\sigma_\varepsilon^2\alpha^2, Var\{\Lambda_{i0}\} = N\sigma_\varepsilon^2\alpha^2, \quad (36)$$

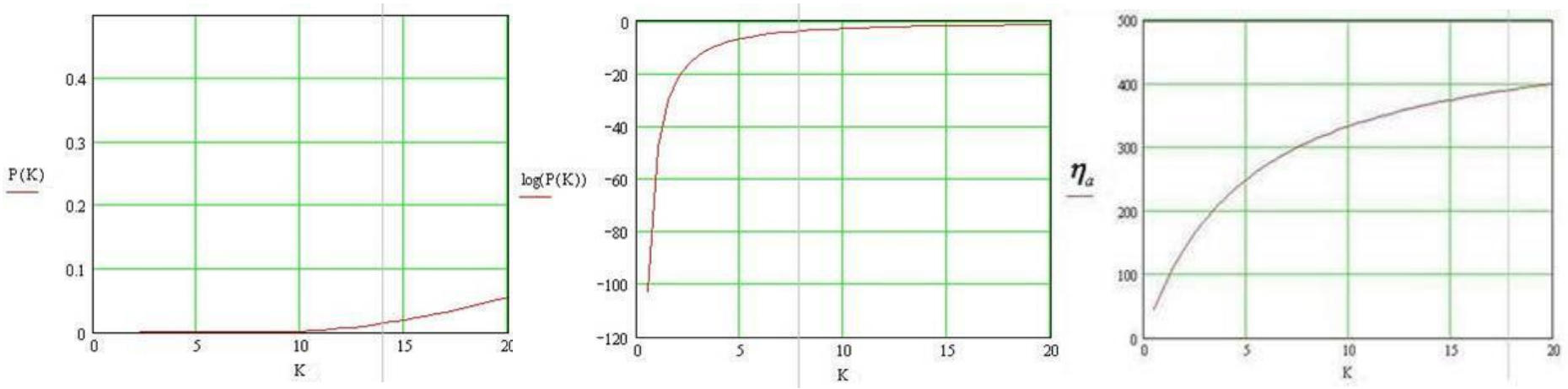
Substituting (36) in (34), we get

$$P = Q(\frac{1}{2}\sqrt{\frac{N}{K^2\eta_\varepsilon}}) = Q(\frac{1}{2}\sqrt{\frac{N}{K^2\eta - K}}),$$

where $\eta = \frac{\eta_w}{\eta_a}, \eta_w = \frac{\sigma_c^2}{\alpha^2}, \eta_a = \frac{\sigma_c^2}{\frac{\alpha^2}{K} + \sigma_\varepsilon^2}.$

Conclusion. The use of orthogonal WM signals improves slightly a detectability of attackers by WM owner but in comparison with collusion attack absent it is necessary to increase the number of PRS elements *N* at $4K^2$ times.

Example. $\sigma_c^2 = 2500, \alpha = 5, \sigma_\varepsilon^2 = 5, N = 1024.$ In Fig. below you can see dependences *p* and η_a versus size *K* of attacker's group calculated by eq. (34) and (35).



a) Input image

b) WM-ed image

c) WM-ed image after collusion attack with K=5

Remark 1. In a similar manner can be proved the formulas for reliability attacker's detecting with the use of blind decoder.

Remark 2. In place of *threshold decoder* considered above one can use so called *maximum decoder* that works as follows :

- i ("traitor "=attacker) = $argmax\Lambda_i$, if $argmax\Lambda_i \geq \lambda$,
- $i \in \varnothing$, if $argmax\Lambda_i < \lambda$ (e.g. "traitors" are not detected).

Comparison of these two decoders can be found in [28].

Remark 3. There are other types of collusion attacks (not necessary by averaging of WM as (27)) , for example :

- minimum attack: $C'_w(n) = \min_{i \in S_c} C_{wi}(n)$

- maximum attack: $C'_w(n) = \max_{i \in S_c} C_{wi}(n)$

- attack by “cropping and insertion ”: $C'_w(n) = C_{wi}(n), i \in S_i,$
where S_i – can be chosen deterministically (for the thing on half of the image for $K = 2$) or randomly
- other types of collusion attacks (see [28].)

However , as it was shown in [28], the efficiency of such attack in tracing traitors occurs approximately the same as it was for average attack.

Remark 4. Significantly improvement of traitor detecting can be obtained with the knowledge of the most likely groups of traitors (*Group oriented fingerprinting(FP)*[28]

Anticollusion-coded (ACC) fingerprinting

Defects of orthogonal-based FP:

- energy of each FP after attack is inverse proportional to the number of attackers $|S_c|$,
- the number of orthogonal signals is limited by their dimension *(N).*

The main idea of ACC:

Provide intentionally a correlation between FP signals .

Method of implementation of this idea:

Apply ACC based on construction known in combinatorial analysis *as balanced incomplete block designs - BIBDs.*

Definition. BIBD with parameters (*V, K, λ, r*) is called a set of blocks of the length *K*, where each digit of block belongs to the set *X* of the numbers (1, 2 … *V*) under the condition that each pair of the numbers from *X* occurs together in exactly λ blocks and each element of X occurs exactly in r blocks.

Example (7,3,1,3) BIBD: (124,136,157,235,267,347,456).
For every BIBDs the following relations hold:

$$\left.\begin{aligned} \lambda(V-1) &= r(K-1) \\ r &= \lambda(V-1)/(K-1) \\ n &= \lambda(V^2-V)/(K^2-K) \end{aligned}\right\}$$

n – the number of blocks,
r – the number of blocks which contain each of elements of *X.* (38)

Each BIBD can be described uniquely by its *VxV incidence matrix A = {a_{ij}},* in which a_{ij} *= 1,* if i^{-th} element of *X* belongs to the j^{th} block, otherwise a_{ij} *= 0.*

Incident matrix for (7,3,1)-BIBD provided in the earlier example :

$$A = \begin{pmatrix} 1110000 \\ 1001100 \\ 0101010 \\ 1000011 \\ 0011001 \\ 0100101 \\ 0010110 \end{pmatrix}$$

Example (7,3,1) BIBD –based ACC.

Let us construct the matrix *C* that is simply the bit complement matrix to the incidence matrix *A*:

$$C = \begin{pmatrix} 0001111 \\ 0110011 \\ 1010101 \\ 0111100 \\ 1100110 \\ 1011010 \\ 1101001 \end{pmatrix}$$

Select columns *C* as FP for every of 7th users, changing 0 to -1 and keeping 1. then we get :

$$w_1 = -1_1 - 1_2 + 1_3 - 1_4 + 1_5 + 1_6 + 1_7$$
$$w_2 = -1_1 + 1_2 - 1_3 + 1_4 + 1_5 - 1_6 + 1_7 \quad (39)$$
$$\ldots$$
$$w_7 = +1_1 + 1_2 + 1_3 - 1_4 - 1_5 - 1_6 - 1_7$$

Such system is able to detect colluders for any sets of the size $K \le 2$. In fact in the case of average attack for given $(w_i + w_j)/2$ it is always possible to find the numbers *i* and *j* of colluders by positions of +1 in the resulting vector. So if the users 1st and 2nd are colluders , then we get from (39) :

$$(w_1 + w_2)/2 = (-1,0,0,0,1,0,1),$$

where the position of +1s on 5th и 7th places are uniquely determined the 1st и 2nd users.

The methods of BIBD-based ACC design for large number of users and large number of colluders can be found in [28].

The use of superimposed code in real space (SIC) as anti-collision codes.

There are known so called Welch Bound Equality (WBE) sequences [46].
In order to provide good efficiency in traitor tracing it is necessary to use decoding based on minimizing Euclidean distance. However WBE sequences are able to provide only some known mean square correlation but not tight bounds for minimal Euclidean distance. Moreover , in order to avoid a trivial attack with WM subtraction from the versions of the WM content , it is necessary that WM be secure. WBE sequences and similar Kasami-Khamaletdinov sequences are not as large sets as desired.

It has been proposed in [47] to use so called *superimposed codes* in real space introduced before by Ericson and Gyorfi [50] for solution of other problems.

Definition: Let us C be a set of unit-norm vectors in R^N. For any subset A denote by $|A|$ its cardinality and by $f(A)$ sum of vector **x** in A $f(A)=\sum_{x\in A} x$.

For $m=0,1,...T$ let us define:

$A(m)=\{A\subseteq C:|A|\leq m\}$

$\varphi^{(m)}=\{f(A):A\in A(m)\}$

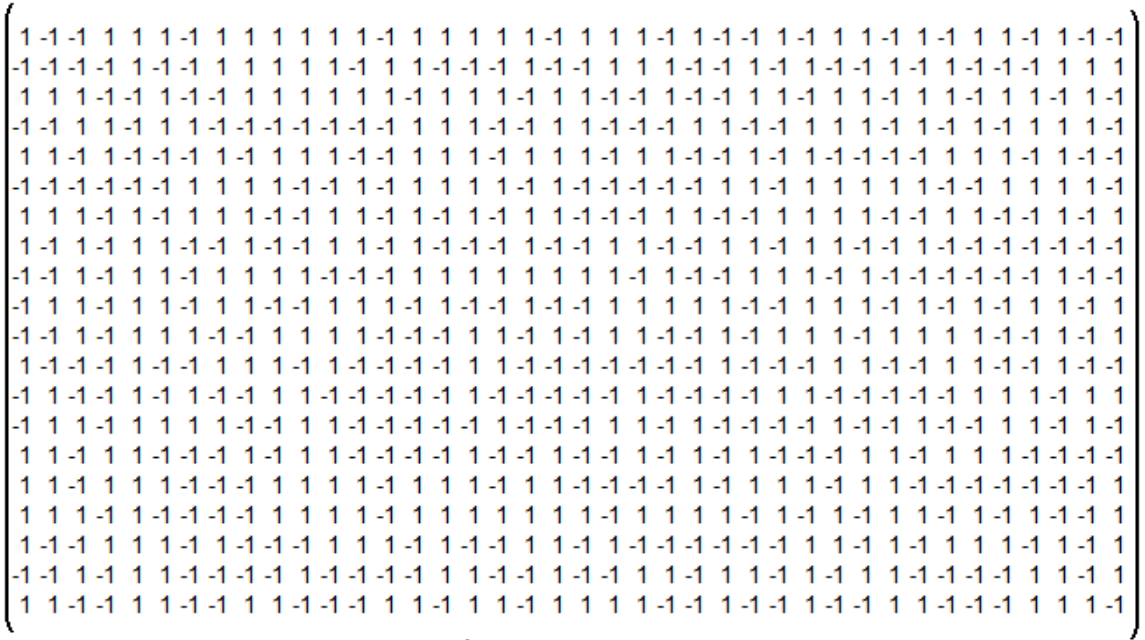
$d_E(\varphi^{(m)})=min||f(A)-f(B)||;$ (40)

$A\neq B, A,B\in A(m)$

Norm $||x||$ is conventional Euclidean norm $\left\|x^2\right\|=\sum_{i=1}^{N} x^2.$

A set C be called SIC with parameters (N, m, T, d), if $|C|=T$ and $d_E(\varphi^{(m)})\geq d$.

Simply speaking ,SIC is such code that provides some given Euclidean distance between conventional arithmetic sums of its vectors with given number of vectors in each sum.



Example of SIC 20x40

If SIC is chosen randomly , then minimal Euclidean distance $d_E(\varphi^{(m)})$ denoted as $\tilde{d}$ be connected with T and m=L as follows:

$$T = e^{NE(L,\tilde{d})},$$

where $E(L,\tilde{d}) \geq A(\tilde{d}) \min_{1 \leq l \leq L} \frac{log\sqrt{\pi l}}{2l}$, $A(\tilde{d}) = \max_{0 \leq x \leq 1} \frac{1-x}{1+x} x^{\tilde{d}/4}$.

For sequences $\left\{ \pm \frac{1}{\sqrt{N}} \right\}$ we have :

$$d = \frac{\sqrt{N}}{L} \tilde{d} \alpha$$

The bound above has been proved in [50] as a random-coding bound.
It is not surprising that randomly chosen codes give the best codes with large probability. This fact is well known from the theory of error correcting codes [35].The main drawback of these codes is the fact that they have no constructive error correcting algorithm because the number of code words is typically intractable.

In our case , the number of code words at SIC is equal to the number of users and therefore it is indeed tractable value. But the number of coalitions can be very large.

Fortunately , there does exist the sphere decoding algorithm (SDA) providing a polynomial complexity for the cases important for practice.

The optimal informed collusion decoder is the decoder on minimum Euclidean distance in real space:

$$\tilde{S}_c = \arg\min_{S_c} \left\| C'_w - C - \frac{1}{L} \sum_{i \in S_c} w_i \right\|, \qquad (41)$$

where L is the size of coalition.

The probability of error in a finding of incorrect coalition $S`_c$ instead of valid coalition S_c:

$$\Pr\left\{S_c' / S_c\right\} \approx Q\left(\frac{1}{2}\sqrt{\frac{d(S_c, S_c')}{\sigma_\varepsilon^2}}\right) = Q\left(\frac{d(S_c, S_c')}{2\sigma_\varepsilon}\right),$$

where $d(S_c, S_c') = \left\| \frac{1}{L}\sum_{i \in S_c} w_i - \frac{1}{L}\sum_{i \in S_c'} w_i \right\|$, $Q(x) = \frac{1}{\sqrt{2\pi}}\int_x^\infty e^{-\frac{t^2}{2}} dt$

Let us minimal Euclidean distance d for a chosen SIC is:

$$d = \min_{S_c \neq S'} d(S_c, S_c')$$

Then the probability of error has the following upper bound:

$$Pe = \Pr\left\{S_c' / S_c\right\} \leq Q\left(\frac{d}{2\sigma_\varepsilon}\right)$$

or

$$Pe \geq Q\left(\frac{\sqrt{N}\tilde{d}}{2L}\right).$$

№	L	$\tilde{d}$	N	*Pe*
1	2	≈1	7	0.387
2	2	≈1	16	0.325
3	3	≈1	16	0.387
4	3	≈1	20	0.372
5	4	≈1	50	0.346
6	4	≈1	100	0.281
7	4	≈1	600	0.065
8	5	≈1	900	0.069

Sphere decoding algorithm

Let us matrix H of the size NxM, is a matrix of WM for M users, (in other words each j^{th} WM is j^{th} column of the H).

$$\underbrace{\begin{pmatrix} H_{11} & H_{12} & \dots & H_{1M} \\ H_{21} & H_{22} & \dots & H_{2M} \\ \dots & \dots & \dots & \dots \\ H_{N1} & H_{N2} & \dots & H_{NM} \end{pmatrix}}_{N \times M}$$

We let that M>N, because otherwise WM can be chosen as orthogonal signals and there is no sense to use decoding on Euclidean distance.

If a coalition $\bar{S} \in \{0,1\}^M$, then statistics for decoding is:

$$x = \frac{\alpha}{k} H \bar{S} + \varepsilon, \qquad (42)$$

where α – embedding coefficient,

ε – gaussian noise with variance σ_ε^2,

K - the number of users of a coalition

The problem to recognize a coalition with Gaussian noise is:

$$\tilde{S} = \arg\min_{\bar{S}} \left\| x - \frac{\alpha}{K} H \bar{S} \right\|, \qquad (43)$$

where $\| \ \|$- is a norm in Euclidean space,

$x \in R^N$ (result of attack),

$H \in R^{NxM}$ (WM matrix),

$\bar{S} \in z^M$ (coalition vector of the length M).

If M>N, then a problem is non-polynomial hard and its effective solution is unknown.

If however M<N and H has a full rank (e.g. rank S = N), then it is possible to apply sphere decoding algorithm (SDA) [47].

The feature of SDA is to find all S given , which satisfy an inequality:

$$\left\| x - HS \right\|^2 \le r^2, \qquad (44)$$

where r - is a radius of hypersphere.

Next it is necessary to find the solution that has minimal Euclidean distance to x that be coincide with the solution of (43).

First , let perform a QR factorization of the matrix H with the use of MxM matrix R that is an upper triangular matrix and NxN orthogonal matrix Q :

$$H = Q\begin{bmatrix} R \\ 0_{(N-M)xM} \end{bmatrix} \tag{45}$$

Next we present matrix H as :

$$H = \begin{bmatrix} Q_1 Q_2 \end{bmatrix}\begin{bmatrix} R \\ 0_{(N-M)xM} \end{bmatrix}, \tag{46}$$

where $\mathbf{Q_1}$ and $\mathbf{Q_2}$ are the first M and the last N-M columns of the matrix $\mathbf{Q}$, respectively.

Then substituting (46) into the left part of (44) we get :

$$\left\| x - HS \right\|^2 = \left\| x - \begin{bmatrix} Q_1 Q_2 \end{bmatrix}\begin{bmatrix} R \\ 0 \end{bmatrix} S \right\|^2 = \left\| Q^{-1}x - \begin{bmatrix} R \\ 0 \end{bmatrix} S \right\|^2 =$$

$$= \left\| Q^T x - \begin{bmatrix} R \\ 0 \end{bmatrix} S \right\|^2 = \left\| \begin{bmatrix} Q_1^T \\ Q_2^T \end{bmatrix} x - \begin{bmatrix} R \\ 0 \end{bmatrix} S \right\|^2 = \left\| Q_1^T x - RS \right\|^2 + \left\| Q_2^T x \right\|^2 .$$

$$\left\| x - HS \right\|^2 = \left\| Q_1^T x - RS \right\|^2 + \left\| Q_2^T x \right\|^2 . \tag{47}$$

It has been shown in [47] that r can be chosen as

$$r = \sqrt{N\sigma_\varepsilon^2}$$

where $\sigma_\varepsilon^2 = \mathrm{var}\{\varepsilon\}$.

Substituting (47) into (44) we have:

$$\left\| Q_1^T x - RS \right\|^2 \le r^2 - \left\| Q_2^T x \right\|^2 \qquad (48)$$

Next we define $x' = Q_1^T x$ è $r'^2 = r^2 - \left\| Q_2^T x \right\|^2$, then:

$$r'^2 \ge \left\| x' - RS \right\|^2, \qquad (49)$$

where x' and RS are M-dimensional vectors.

But one problem arises .In order to apply SDA it is necessary to be the following conditions : M<N and rank H = M. In reality we have an opposite condition (N<M) ,because otherwise it would be possible to use all M signals as orthogonal ones and we be able to use correlation decoder instead decoding on minimal Euclidean distance.

In order to solve this contradiction we can assume that the most "innocent" users which are not in a coalition give minimal values of

$$\left| \Lambda_i \right| = \sum_{k=1}^{N} \sum_{i \in S_C} C_{ik} \tilde{C}_k \le \lambda \qquad (50)$$

Then these M-N users can be removed from S and to find the reminder of users which can take part in a coalition by SDA.
Changing (48) and (49) in line with agreement above we get:

$$\left\| Q_1^T x - RS \right\|^2 \le r^2, \tag{51}$$

$$r^2 \ge \left\| x' - RS \right\|^2. \tag{52}$$

Since R is square matrix then (52) can be expressed as follows:

$$r^2 \ge \sum_{i=1}^{M} \left(x_i' - \sum_{j=i}^{M} R_{i,j} S_j \right)^2. \tag{53}$$

Next transforms are based on the fact that matrix R is an upper triangular one:

$$r^2 \ge \left(x_M' - R_{M,M} S_M \right)^2 + \left(x_{M-1}' - R_{M-1,M-1} S_{M-1} - R_{M-1,M} S_M \right)^2 + \ldots \tag{54}$$

(In fact $\sum_{j=1}^{M} R_{i,j} S_j$ for an upper triangular R is:

$$\begin{pmatrix} R_{1,1} & \ldots & \ldots & R_{1,M} \\ \ldots & \ldots & \ldots & \ldots \\ \ldots & \ldots & R_{M-1,M-1} & R_{M-1,M} \\ 0 & \ldots & \ldots & R_{M,M} \end{pmatrix} \times \begin{pmatrix} S_1 \\ \ldots \\ S_{M-1} \\ S_M \end{pmatrix} = \begin{pmatrix} \ldots \\ \ldots \\ R_{M-1,M-1} S_{M-1} + R_{M-1,M} S_M \\ R_{M,M} S_M \end{pmatrix}.)$$

The necessary condition to be (54) is:

$$r^2 \geq \left(x_M{}' - R_{M,M} S_M \right)^2 \qquad (55)$$

Inequality (55) is equivalent to the following:

$$\frac{r - x_M'}{R_{M,M}} \leq S_M \leq \frac{r + x_M'}{R_{M,M}} \qquad (56)$$

Since S_M takes only two values (0,1) we can select those of them , which satisfy to (55) or (56).

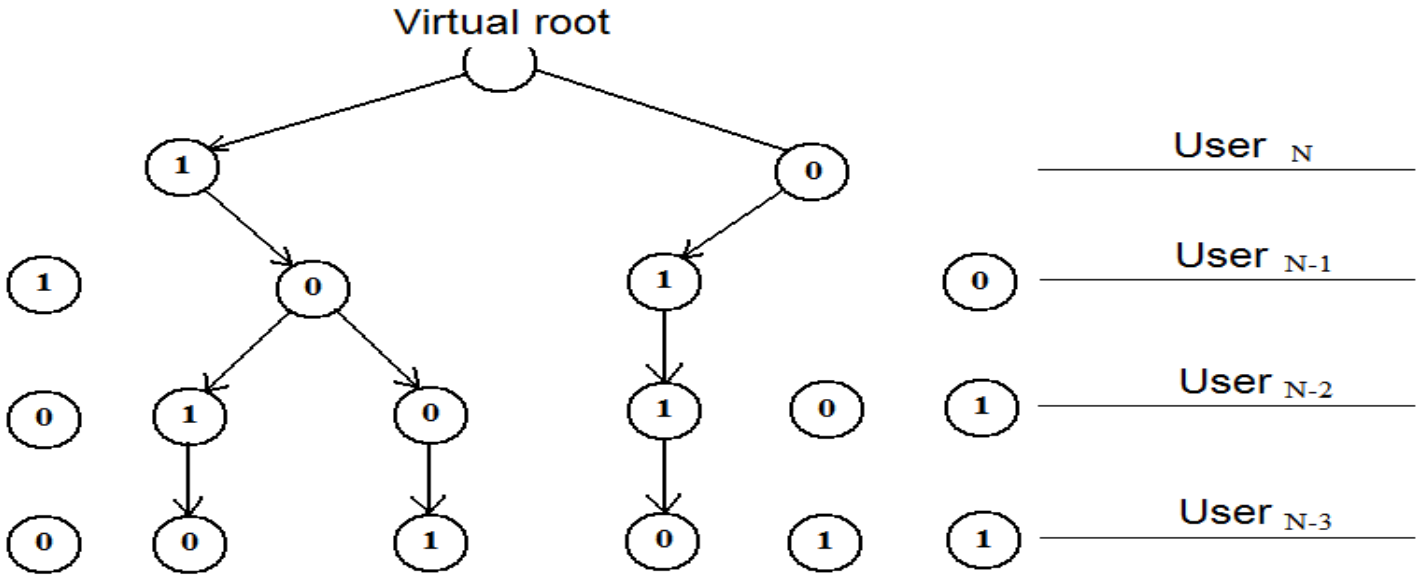
Substituting them into (48) we can get the condition for S_{M-1}:

$$r^2 - \left(x_M{}' - R_{M,M} \tilde{S}_M \right)^2 \geq \left(x_{M-1}{}' - R_{M-1,M-1} S_{M-1} - R_{M-1,M} \tilde{S}_M \right)^2 + \ldots \qquad (57)$$

Next we can find $S_{M-1} = \tilde{S}_{M-1}$ for which (57) holds.

Similar iterative procedure can be proceeded in order to find all coordinates of the vector S_c which lie inside of sphere of the radius r.
These process can be illustrated by search on the tree shown in Figure below.
Let us two decisions $\tilde{S}_M = 0$ and $\tilde{S}_M = 1$ satisfy to (55) (it is mapped in Fig. by two lines emerging from the virtual root of the tree.

If we let $\tilde{S}_M = 1$ into (57), then we get only one solution satisfying to (57), $\tilde{S}_{M-1} = 0$, whereas in the case $\tilde{S}_M = 0$ we get for $\tilde{S}_{M-1}$ only one solution – "1". Following to this way we can find a complete vector of coalition. For the example presented in Figure below we get tree ways.



A tree corresponding to SDA for N=4, $|S_c|=2$.

Now it is possible to compare Euclidean distances by (44) corresponding to three ways to the point $\bar{x}$ and take such a final decision S_C , which provides minimal Euclidean distance.