power level in the optical fibre was measured to be 16 μW. Fig. 3 demonstrates the isolation effects of the assembly experimented at a frequency of 30 MHz. Here, the linearity of the system using the assemblies is compared with the system using a cascade connection of three conventional isolators (3 × 30 dB). It is found that the linearity of the system using the assemblies is 20 dB and 40 dB wider than the one using the isolators at 0.001 dB and 0.01 dB deviation.

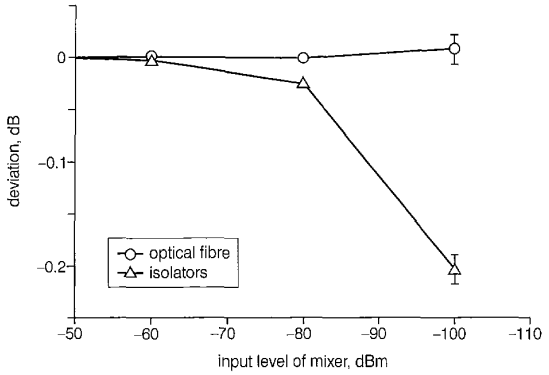

Fig. 3 *Isolation effects of LED-optical fibre-PD assemblies to attenuation measurement system*

Conclusions: The LED, optical fibre and PD assemblies were introduced to achieve a RF dual channel measurement system in high isolation. Isolation effects were verified in an experimental setup of a 10–100 MHz attenuation measurement system and satisfactory results were obtained. The assemblies also gave good flexibility to the structure of the system and minimised earth loop problems.

Acknowledgment: The authors wish to thank C. Siregar and Y. Setiady for many helpful discussions.

12 December 2001
Electronics Letters Online No: 20020686
DOI: 10.1049/el:20020686

A. Widarta and T. Kawakami (*National Metrology Institute of Japan, AIST-3, 1-1-1 Umezono, Tsukuba 305-8563, Japan*)

E-mail: anton-widarta@aist.go.jp

References

1 WARNER, F.L.: 'Microwave attenuation measurement' (Peter Peregrinus, London, 1977)
2 KAWAKAMI, T., NAGATSUKA, A., MAEDA, M., and IGARASHI, S.: 'RF attenuation measurement system with 1 kHz voltage ratio method', *IEEE Trans. Instrum. Meas.*, 1993, **42**, (6), pp. 1014–1019
3 KILBY, G.J., SMITH, T.A.J., and WARNER, F.L.: 'The accurate measurement of high attenuation at radio frequency', *IEEE Trans. Instrum. Meas.*, 1995, **44**, (2), pp. 308–311

Scattering codes to implement short 3-secure fingerprinting for copyright protection

F. Sebé and J. Domingo-Ferrer

Collusion attacks are a major issue in fingerprinting schemes for copyright protection. A new class of codes, called scattering codes, is presented which can be used to control colluders' strategy in collusions of size up to 3. Scattering codes can be combined with dual Hamming codes to obtain 3-secure fingerprinting codes much shorter than those resulting from Boneh–Shaw's general construction.

Successive failure of copy prevention systems has caused copy detection systems to become the most promising option for multimedia copyright protection. In copy detection, the merchant embeds an imperceptible mark into the content before selling it. There are two kinds of mark: watermarks and fingerprints. A watermark is a message that allows ownership of the marked content to be proven, whereas a fingerprint allows buyer identification.

Collusion attacks are a problem fingerprinting, because each copy being sold is different. In a collusion attack, a set of dishonest buyers compare their copies in order to locate differences between them and try to fabricate a new content whose mark is either no longer recoverable or does not allow identification of any of the colluders.

In [1], the concept of fingerprinting secure against buyer collusions is introduced. A general construction is given to obtain fingerprinting codes secure against collusions of up to c buyers (c-secure codes). For N possible buyers and given $\epsilon > 0$, $L = 2c\log(2N/\epsilon)$ and $d = 8c^2\log(8cL/\epsilon)$ a code with N codewords of length

$$l_{BS} = 2Ldc = 32c^4 \log(2N/\epsilon)\log(8cL/\epsilon) \quad (1)$$

is constructed which allows one of the colluders to be identified with probability $1-\epsilon$.

In [2] it is shown that, for $c = 2$, collusion security can be obtained using the error-correcting capacity of dual Hamming codes. In this way, 2-secure fingerprinting codes are obtained which are much shorter than 2-secure codes obtained via the general construction [1].

In [3] it is shown that, for $c = 3$, dual Hamming codes also offer collusion security, as long as the colluders' strategy can be controlled. This Letter describes how to control that strategy.

Definition 1: Let a^1, a^2, a^3 be three codewords of a binary code the codewords of which are N bits long, i.e. $a^i = a_1^i a_2^i \cdots a_N^i$. Define $inv(a^1, a^2, a^3)$ as the set of invariant positions between all three codewords, i.e. those bit positions in which all three codewords have the same bit value. Formally speaking,

$$inv(a^1, a^2, a^3) = \{i, 1 \le i \le N, a_i^1 = a_i^2 = a_i^3\}$$

Definition 2: Let a^1, a^2, a^3 be three codewords of a binary code the words of which are N bits long. Define minor (a^1; a^2, $a3$) as the set of bit positions in which a^1 has a value different from the values a^2 and a^3 (for such positions, $a_i^2 = a_i^3$). Formally speaking,

$$minor(a^1; a^2, a^3) = \{i, 1 \le i \le N, a_i^1 \ne a_i^2, a_i^1 \ne a_i^3\}$$

Let us assume that three dishonest buyers c^1, c^2, c^3 compare their copies of the same multimedia content. According to the marking assumption [1], they can only modify the embedded marks in those *detectable* positions where not all three marks take the same bit value. In those positions, the colluders can set the corresponding bit to 0, 1 or 'unreadable'. In this way, we conclude that, if three different buyers are assigned codewords a^1, a^2 and a^3 of a binary code, the result of their collusion will be a codeword a^{coll} where no bit has been modified in the positions in $inv(a^1, a^2, a^3)$. Conversely, colluders will be able to identify positions in $minor(a^1; a^2, a^3)$ as the bit positions corresponding to content fragments which are identical between the copies of c^2 and c^3 and different from the copy of c^1. In a similar way, $minor(a^2; a^1, a^3)$ and $minor(a^3; a^1, a^2)$ can be identified as well.

Definition 3: A p-majority collusion strategy is one in which colluders choose with probability p the majority bit value in positions $minor(a^i; a^j, a^k)$ (i.e. the bit values in a^j or a^k).

In [3] it is shown that dual Hamming codes offer security against collusions of up to three colluders, as long as a p-majority collusion strategy is used with a value p close to 1. The problem is that the parameter p defining the collusion strategy is chosen by the colluders, which implies they can take $p = 0$ to make sure they are not identified! To circumvent that shortcoming, we define below a new kind of codes called *scattering codes*.

Definition 4: A scattering codes $SC(d, t)$ with parameters (d, t) is a binary code consisting of $2t$ codewords of length $(2t+1)d$ constructed as follows:

1. Generate the codewords of $SC(1, t)$ as:
   (a) The ith codeword for $1 \le i \le t$ is constructed by setting the first and the $(i+1)$th bits of the codeword to '1'. The remaining bits are set to '0'.
   (b) The ith codeword for $t+1 \le i \le 2t$ is constructed by setting the $(i+1)$th bit of the codeword to '1'. The remaining bits are set to '0'.

2. The code $SC(d, t)$ is generated by replicating d times every bit in the codewords of $SC(1, t)$. Define a *block* to be a group of d replicated bits.

3. By convention, the first t codewords of $SC(d, t)$ are defined to encode a '1' and the last t codewords are defined to encode a '0'. The first block of the code is called 'Zone-A', the next t blocks are called 'Zone-B' and the last t blocks are called 'Zone-C'.

Using a scattering code, a '1' is encoded by randomly choosing one of the first t codewords and a '0' is encoded by randomly choosing one of the last t codewords.

A scattering code is decoded by using the first applicable rule among the following ordered list:

1. If all bits in 'Zone-A' are '1' and all bits in 'Zone-C' are '0', decode as '1'.
2. If all bits in 'Zone-A' are '0' and all bits in 'Zone-B' are '0', decode as '0'.
3. If in two blocks of 'Zone-B' there is at least one bit with value '1' in each one, decode as '1'.
4. If in two blocks of 'Zone-C' there is at least one bit with value '1' in each one, decode as '0'.
5. If there are more '1' bits than '0' bits in 'Zone-A', decode as '1'.
6. If there are more '0' bits than '1' bits in 'Zone-A', decode as '0'.
7. Decode as 'Unreadable'

Lemma 1 Let b^{coll} be a codeword generated by using a p-majority strategy between three codewords b^1, b^2, $b^3 \in SC(d, t)$ encoding the same bit value v. Then, b^{coll} decodes as v with probability 1.

Lemma 2 Let b^{coll} be a codeword generated using a p-majority strategy between three codewords b^1, b^2, $b^3 \in SC(d, t)$, with two of them (b^1 and b^2) encoding a value v and the other (b^3) a value $\bar{v}$. Then, the probability that b^{coll} decodes as v is given by

$$p(v) = \left(1 - \frac{1}{t}\right) p_{diff}(v) + \frac{1}{t} p_{same}(v)$$

where $p_{diff}(v)$ is the probability of decoding as v when $b^1 \neq b^2$ and can be computed as $p_{diff}(v) = 1 - p_{diff}(\bar{v})$ and

$$p_{diff}(\bar{v}) = (1-p)^d p^{2d} + 2 \cdot p^d (1-p^d) \sum_{k=0}^{\lfloor \frac{d-1}{2} \rfloor} b(k; d, p) + p^{2d} \sum_{k=1}^{\lfloor \frac{d-1}{2} \rfloor} b(k; d, p)$$

and $p_{same}(v)$ is the probability of decoding as v when $b^1 = b^2$ and can be computed as

$$p_{same}(v) = p^{2d} + (1-p^d) \sum_{k=\lfloor \frac{d+2}{2} \rfloor}^{d} b(k; d, p) + p^d \sum_{k=\lfloor \frac{d+2}{2} \rfloor}^{d-1} b(k; d, p)$$

Table 1 shows, for several codes $SC(d, t)$, the least probability $p(v)$ of decoding as the majority bit in a collusion of three codewords (two encoding v and one $\bar{v}$).

Table 1: Probability $p(v)$ of decoding as majority bit v in collusion of three buyers, for several parameter choices (d, t)

d	t	min $p(v)$
3	4	0.68
5	5	0.80
7	9	0.89
31	100	0.99

For $N = 2^n$ buyers, each buyer c^i is assigned a different codeword a^i of a dual Hamming code. Rather than directly embedding a^i in the content to be sold, the merchant generates a codeword A^i by composing a scattering code $SC(d, t)$ with a^i. Such a composition is performed by replacing each bit of a^i with a codeword in $SC(d, t)$ that encodes the value of the bit of a^i. In this way, the codeword A^i will have bitlength

$$l_{SD} = (N-1)(2t+1)d \quad (2)$$

The merchant then permutes the bits in A^i using a pseudorandom permutation seeded by a secret key known only to the merchant. Finally, the merchant embeds the permuted version of A^i in the content being sold.

What is achieved with the above composition is that, regardless of the p'-majority strategy used by colluders to generate codewords A^{coll}, the $p(v)$-majority strategy resulting from decoding A^{coll} as a^{coll} has a value $p(v)$ that can be controlled by the merchant by choosing appropriate values for parameters d and t.

Table 2 shows that, for fixed security level ϵ, the codes generated with our construction are much shorter than Boneh–Shaw's as long as the number of buyers stays moderate.

Table 2: Comparison of codeword length between our proposal and Boneh–Shaw's assuming $\epsilon = 10^{-10}$

Buyers	Our length (l_{SD})	Boneh–Shaw's length (l_{BS})
512	28,105	5,148,000
1,024	56,265	5,269,992
...	...	...
32,768	1,802,185	5,883,888
65,536	3,604,425	6,006,780
131,072	7,208,905	6,129,816

Acknowledgment: This work has been partly supported by the European Commission under project IST-2001-32012 'Co-Orthogonal Codes' and by the Spanish Ministry of Science and Technology and the European FEDER fund through Project No. TIC2001-0633-C03-01 'STREAMOBILE'.

11 May 2002
Electronics Letters Online No: 20020648
DOI: 10.1049/el:20020648

F. Sebé and J. Domingo-Ferrer (*Universitat Rovira i Virgili, Department of Computer Engineering and Mathematics, Av. Pasos Catalans 26, E-43007 Tarragona, Catalonia, Spain*)

E-mail: jdomingo@etse.urv.es

References

1 BONEH, D., and SHAW, J.: 'Collusion-secure fingerprinting for digital data' *in* 'Advances in cryptology—CRYPTO'95' (Springer LNCS 963, 1995), pp. 452–465. Journal version in *IEEE Trans. Inf. Theory*, 1998, **IT-44**, (5), pp. 1897–1905

2 DOMINGO-FERRER, J., and HERRERA-JOANCOMARTÍ, J.: 'Short collusion-secure fingerprints based on dual binary Hamming codes', *Electron. Lett.*, 2000, **36**, (20), pp. 1697–1699

3 SEBÉ, F., and DOMINGO-FERRER, J.: 'Short 3-secure fingerprinting codes for copyright protection' *in* 'ACISP'2002' (Springer LNCS (to appear))

Scheduling structure to achieve inter-layer optimisation in wireless IP networks

C. Wijting and R. Prasad

An inter-layer scheduling structure that achieves a coupling between the IP and data link layer is proposed. Based upon the QoS requirements from the network layer and the available resources at link layer the optimal bearer is selected. The combination of information from different layers in the protocol stack allows for a more optimised and accurate control of the traffic flows with different QoS requirements.

Introduction: Resource allocation deals with the assignment of shared resources to different tasks. This Letter introduces a novel structure that adapts the resources allocated to a service class depending on the requirements of the class, the arriving traffic and the available physical resources. The structure for this inter-layer approach is shown in Fig. 1.

Two main parts can be distinguished, a network part and a link layer part. The network part classifies the incoming traffic according to their requested service class [1]. The different classes can be serviced according to a queuing mechanism, e.g. priority queuing or weighted fair queuing.