Sequential and Dynamic Frameproof Codes

Maura Paterson
m.b.paterson@rhul.ac.uk
Department of Mathematics
Royal Holloway, University of London
Egham, Surrey TW20 0EX

Abstract

There are many schemes in the literature for protecting digital data from piracy by the use of digital fingerprinting, such as frameproof codes and traitor-tracing schemes. The concept of traitor tracing has been applied to a digital broadcast setting in the form of dynamic traitor-tracing schemes and sequential traitor-tracing schemes, which could be used to combat piracy of pay-TV broadcasts, for example. In this paper we extend the properties of frameproof codes to this dynamic model, defining and constructing both *l-sequential frameproof codes* and *l-dynamic c-frameproof codes*. We also give bounds on the number of users supported by such schemes.

Keywords: frameproof codes, dynamic traitor tracing, cryptography
Mathematics Subject Classification: 94A62, 05B30

1 Introduction

There are many schemes described in the literature that aim to discourage the piracy of digital data through the use of digital fingerprints (an extensive survey is given in [1]). Most of these schemes involve splitting the data into segments, each of which is marked in one of q possible ways. As in [6] we require that these marks satisfy the properties of *similarity*, namely that the presence of the mark should not be apparent when the data is used for its intended purpose, and *robustness*, whereby it should be impossible for a pirate to alter or remove the mark without causing a corresponding degradation in the actual data. In what follows we assume that it is possible to create marks with these properties; this is known as the *watermarking assumption*. For further discussion of issues surrounding watermarking see [9].

If the data is split into l segments that can be marked in q possible ways each marked copy of the data can be thought of as corresponding to a word $x = (x_1, x_2, \ldots, x_l) \in Q^l$ where Q is an alphabet of size q. The set of words corresponding to the marked copies distributed to the users forms a code $C \subseteq Q^l$. A user who makes illegal copies of the data can be identified by the codeword present on the illegal copies. It is possible that numerous users may cooperate in the production of illicit copies, however. A set of users, known as *traitors*, who collude to produce illegal copies of the data is known as a *pirate*. By combining the segments received by different traitors the pirate can attempt to produce

versions having different combinations of marks in an effort to avoid detection. If a pirate has access to a particular set $S \subset C$ of codewords then the set of new words it can form in such a manner is referred to as the *set of descendants of S*.

Definition 1.1. *Suppose* $S \subseteq Q^l$. *We define the* set of descendants of S, *denoted* $\mathrm{desc}(S)$, *by*

$$\mathrm{desc}(S) = \{x \in Q^l | \forall\ i = 1, 2, \ldots, l\ \exists y \in S \text{ with } x_i = y_i\}.$$

The descendants of a set of words are all those words that agree in each coordinate position with some word in that set.

Example 1.1 Suppose $S = \{(0,0,1), (2,0,0), (2,0,1)\}$. Then

$$\mathrm{desc}(S) = \{(0,0,0), (0,0,1), (2,0,0), (2,0,1)\}.$$

■

By altering properties of the code C such as the minimum distance, it is possible to affect the potential descendants of sets of codewords; this technique is used in many schemes for preventing piracy. An example of this is provided by *traitor-tracing schemes*, which consist of a code C and an algorithm that takes as input a descendant x of some set S of c or fewer codewords (*i.e.* a codeword produced by c or fewer colluding traitors) and outputs at least one of the codewords in S. Traitor-tracing schemes were first proposed by Chor, Fiat and Naor in [4].

If a descendant of the words belonging to a pirate set is a codeword corresponding to some innocent user then by producing a copy marked with that descendant the pirate can cause that user to be falsely incriminated. Conversely, a single traitor could distribute pirate copies of his or her version of the data and, if caught, claim to have been framed by some other coalition of users. *Frameproof codes* were proposed by Boneh and Shaw in order to solve this "toy problem" [3].

The following definition of a frameproof code appears in [1]; Boneh and Shaw's original definition differs slightly as they used different assumptions on the ability of the pirate to alter watermarks.

Definition 1.2. *A code* $C \subseteq Q^l$ *is a* c-frameproof code *if every set* $S \subset C$ *with* $|S| \leq c$ *satisfies* $\mathrm{desc}(S) \cap C = S$.

Thus when a c-frameproof code is used to fingerprint data no set of c or fewer traitors can collude to frame a user outside of that set. If a code is c-frameproof for all $c \geq 2$ we refer to it as a *frameproof code*.

Example 1.2 The following code Γ is a binary, length 3, 2-frameproof code.

$$\Gamma = \{(0,0,0), (1,1,0), (0,1,1), (1,0,1)\}$$

Any two words of Γ agree in at most one coordinate. Thus for any pair S of words from Γ and any word $x \in \Gamma \setminus S$ the word x has at least one coordinate position in which it differs from both words in S so $x \notin \mathrm{desc}(S)$. Hence no pair of words can frame a third word. ■

A result of Cohen and Encheva [5] provides a lower bound on the maximum number of words possible in a q-ary length l c-frameproof code: for $l \geq 2$

and $c \geq 2$ and prime-power $q \geq l$ they use error correcting codes to construct c-frameproof codes containing $q^{\lceil \frac{l}{c} \rceil}$ codewords. On the other hand, Staddon *et al.* show that for a q-ary length l c-frameproof code the number n of codewords is bounded by $n \leq cq^{\lceil \frac{l}{c} \rceil}$ [8]. For many choices of parameter better bounds are known (see [1] for details), although in many cases tight bounds have yet to be established. For the case of frameproof codes, however, Blackburn [2] gives a construction of q-ary length l frameproof codes containing $n = l(q-1)$ codewords and shows that no larger frameproof code exists for $q \geq 2$ and $l \geq 2$.

As in the case of traitor-tracing schemes the words of a frameproof code are embedded in the data, which is then distributed; any information about the pirates is obtained after the piracy has occurred, through the examination of the pirate copies of the data. We refer to this as the *static model*. In [6] Fiat and Tassa introduce *dynamic traitor-tracing schemes*, which make use of fingerprintinging in the digital broadcast setting where data is continuously broadcast to paying recipients. This could correspond to the output of a pay TV station, for example. In this dynamic setting the data is divided into segments, each corresponding to a few minutes of the broadcast. Digital fingerprints are added to each segment, with q differently-marked versions of each segment being produced. At a given time the appropriate segment is broadcast after being encrypted in such a way that each user can only decrypt a particular marked version so that different users receive differently-marked versions of each segment. We model this by using an alphabet Q of size q to represent the possible segments; a user u is therefore effectively allocated a symbol $M_j(u) \in Q$ during time segment j.

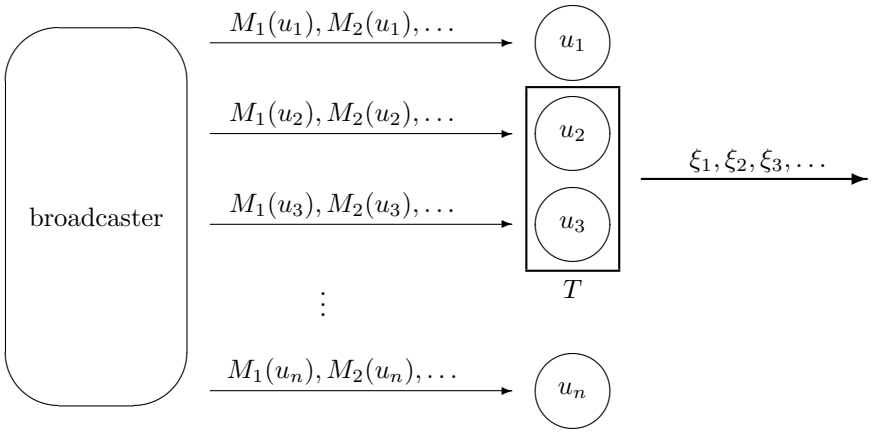

Figure 1: Piracy of a Fingerprinted Digital Broadcast

A set T of traitorous users who collaborate in piracy have the choice at each time i of broadcasting any segment with a mark received by one of the traitors at that time (*i.e.* a mark $\xi_i \in \{M_i(t) | t \in T\}$). We say that a *pirate broadcast sequence corresponding to* T is a sequence $\{\xi_i\}_{i=1}^{j}$ such that for each $i = 1, 2, \ldots, j$ the mark ξ_i is in the set $\{M_i(t) | t \in T\}$. If the legitimate broadcaster can intercept the pirate's broadcast it can detect the sequence of marks broadcast by the pirate and use it to determine how to distribute the differently marked versions

to the users at future times. For the sake of brevity we represent the pirate sequence $\{\xi_i\}_{i=1}^{j-1}$ by the word $\Xi_j = (\xi_1, \xi_2, \ldots, \xi_{j-1}) \in Q^{j-1}$.

A dynamic traitor-tracing scheme distributes the marks in such a way that the identities of the traitors are revealed by the pirate broadcast. In a *sequential traitor-tracing scheme*, as introduced by Safavi-Naini and Wang in [7], the mark distribution is not dependent on the pirate broadcast, which is used solely to identify the traitors.

It is shown in [6], however, that in order to trace even one traitor a deterministic dynamic traitor tracing scheme requires the use of at least $c+1$ differently marked variants, where c is the number of colluding traitors. If the number of traitors is high the broadcaster may not have the resources to produce the required number of versions. One approach in this situation would be to use a probabilistic scheme, as suggested in [10]; another option, which we explore here, is to consider a weaker model.

This paper examines the possibility of extending the properties of frameproof codes to the dynamic broadcast setting. In this setting we say that a pirate T who broadcasts a sequence $\{\xi_i\}_{i=1}^{j}$ has *framed* a user $u \in U \setminus T$ during time segment $i \leq j$ if $\xi_i = M_i(u)$. We say that T frames u over the interval $i, i+1, \ldots, i+l-1$ of length l if $\xi_\alpha = M_\alpha(u)$ for all $\alpha = i, i+1, \ldots, i+l-1$. We will investigate methods for preventing framing in the dynamic setting. The resulting schemes may be of less practical use than a corresponding traitor tracing scheme, but it is nonetheless interesting to study their behaviour in comparison with that of ordinary frameproof codes.

In Section 2 we define *l-sequential c-frameproof codes* that prevent the framing of innocent users by coalitions of up to c traitors over windows of l consecutive segments. These schemes do not depend on the pirate broadcast. We then show that these schemes are closely related to the static c-frameproof codes, and use this connection to bound the maximum number of users such schemes can support.

Section 3 contains an exploration of *l-dynamic c-frameproof codes*, which require l time segments to prevent coalitions of up to c traitors from framing innocent users. By exploiting the information present in the pirate broadcast these schemes can protect an exponentially greater number of users than an l-sequential c-frameproof code. We show that for $c \geq 2$ the maximum number of users that such a scheme can protect is equal to $q^{l-1}(q-1)$, and that when there is at most one traitor q^l users can be protected. We also describe constructions of schemes meeting each of these bounds.

2 Sequential Frameproof Codes

The aim of a sequential traitor tracing scheme is to distribute differently marked versions to the users in such a way that once the pirate broadcast is received a traitor can be identified. In the context of frameproof codes, however, our goal is to distribute segments so as to prevent the pirate from broadcasting a sequence of segments corresponding to that allocated to an innocent user. This concept is expressed formally in the following definition.

Definition 2.1. *Let U be a set of users. An* l-sequential c-frameproof code *is a function $\mathcal{M}$ mapping $\mathbb{N}^+ \times U$ to Q with $(j, u) \mapsto M_j(u)$, such that for any*

pirate $T \subset U$ with $|T| \leq c$, any $i \in \mathbb{N}^+$ and for any sequence of marks $\{\xi_j\}_{j=i}^{i+l-1}$ broadcast by that pirate over l consecutive time intervals there is no legitimate user $u \in U \setminus T$ with $M_j(u) = \xi_j$ for all $j = i, i+1, \ldots, i+l-1$.

During time section j the function $\mathcal{M}$ assigns to user u the segment marked with mark $M_j(u)$; the sequential c-frameproof property ensures that over the course of any l consecutive time segments, the sequence of marked segments broadcast by any pirate T with $|T| \leq c$ will differ from that allocated to any innocent user. If $\mathcal{M}$ is an l-sequential c-frameproof code for all $c \geq 2$ then we refer to it simply as an l-sequential frameproof code.

If at some time t a user u receives a mark that no other user received at that time we refer to it as a *unique* mark. If the pirate broadcast ξ_t is a unique mark, then we know that the user who received the mark must be part of the pirate coalition.

Example 2.1 Let $U = \{u_1, u_2, \ldots, u_n\}$ and $Q = \{1, 2, \ldots, n\}$, and define $\mathcal{M}$ by setting $\mathcal{M}(i, u_j) = j$ for all $i \in \mathbb{N}^+$. Then $\mathcal{M}$ is an l-sequential frameproof code for any $l \geq 1$, since the fact that no two users get the same mark at any time means that no user can be framed during any time interval. ■

The rather trivial code described above requires a mark alphabet of size n. If fewer marks are available then a more sophisticated construction is necessary in order to prevent framing. In fact l-sequential c-frameproof codes are essentially familiar objects in a new guise:

Theorem 2.2. *A q-ary l-sequential c-frameproof code supporting n users exists if and only if there exists a q-ary length l c-frameproof code containing n codewords.*

Proof. Suppose $\mathcal{M}$ is an l-sequential c-frameproof code over an alphabet Q of size q protecting a set U of users with $|U| = n$. Fix some integer $j \geq 1$ and associate a word $x^u = \big(M_j(u), M_{j+1}(u), \ldots, M_{j+l-1}(u)\big) \in Q^l$ with each user $u \in U$. Then it is straightforward to show that the set $\Gamma = \{x^u | u \in U\} \subset Q^l$ is a length l c-frameproof code over Q of size n. Conversely, for every q-ary length l c-frameproof code $\Gamma = \{x^1, x^2, \ldots, x^n\} \subset Q^l$ it is possible to construct an l-sequential c-frameproof code by letting $\mathcal{M}\colon \mathbb{N}^+ \times U \to Q$ be defined by setting $M_i(u_\alpha) = x^\alpha_{i'}$, where i' is the unique element of $\{1, 2, \ldots, l\}$ with $i \equiv i' \pmod{l}$. □

The above result implies that bounds on the number of words contained in a c-frameproof code translate into bounds on the number of users a sequential c-frameproof code can support. In particular, a previously mentioned result from [2] leads to the following bound.

Corollary 2.3. *An l-sequential frameproof code with $l \geq 2$ using an alphabet of size $q \geq 2$ can protect at most $l(q-1)$ users.*

This relationship with the static case is due to the fact that in the sequential setting neither the set of users nor the allocation of marked segments are affected by the broadcast, which enables known examples of c-frameproof codes to be effectively translated into the dynamic setting to yield sequential c-frameproof codes. This example illustrates how this works in practice.

Example 2.2 The code Γ of Example 1.2 is a binary, length 3, 2-frameproof code. We label the words as follows.

$$x^0 = (0,0,0),\ x^1 = (1,1,0),\ x^2 = (0,1,1),\ x^3 = (1,0,1)$$

As Γ contains four words, it can be turned into a 3-sequential 2-frameproof code for four users. Let $U = \{u_0, u_1, u_2, u_3\}$ and $Q = \{0,1\}$. Define a function $\mathcal{M}\colon \mathbb{N}^+ \times U \to Q$ by setting $M_i(u_j) = x^j_{i'}$, with $i' \in \{1,2,3\}$ and $i' \equiv i \pmod 3$. The following table indicates how the marks would be distributed according to $\mathcal{M}$ over the first nine time segments.

	1	2	3	4	5	6	7	8	9
u_0	0	0	0	0	0	0	0	0	0
u_1	1	1	0	1	1	0	1	1	0
u_2	0	1	1	0	1	1	0	1	1
u_3	1	0	1	1	0	1	1	0	1

If we consider any three consecutive time segments we observe that the marks received by each user correspond to words of Γ, therefore it is not possible for any two colluding users to frame a third user over any length 3 window of consecutive segments. Thus we conclude that $\mathcal{M}$ is indeed a 3-sequential 2-frameproof code. ■

3 Dynamic Frameproof Codes

The dynamic setting differs from the sequential case in that we wish in this instance to make use of the information present in the pirate's broadcast. Sequential frameproof codes are essentially equivalent to the ordinary frameproof codes but the greater flexibility of the dynamic setting suggests a potential for genuinely new constructions; in particular we would expect to find more-efficient ways of preventing framing. Indeed this is the case, as we will show.

We assume that at any given time j we know the pirate's previous broadcast Ξ_j and we use this information to determine the allocation of marks at that time. The pirate T responds by broadcasting a marked segment ξ_j received by a traitor $t \in T$; this mark is then taken into account when distributing the marks at time $j+1$. Our goal in this instance is to allocate marks so that after as short a time as possible we can be certain that no innocent user has been framed. We will therefore consider schemes that define a mark distribution over l segments and prevent any pirate set from framing an innocent user over that time period. We define this formally as follows:

Definition 3.1. *Let U be a set of users and Q a marking alphabet. An* l-dynamic c-frameproof code *is a finite family of functions $\{D_\alpha\}_{\alpha=1}^{l}$ where $D_1\colon U \to Q$ and $D_\alpha\colon Q^{\alpha-1} \times U \to Q$ for $\alpha > 1$, with the property that for any pirate broadcast sequence $\{\xi_j\}_{j=1}^{l}$ corresponding to a pirate T with $|T| \le c$ there is no user $u \in U \setminus T$ with $D_j(\Xi_j, u) = \xi_j$ for all $j = 1, 2, \ldots, l$.*

The function D_j associates each user u with a symbol $D_j(\Xi_j, u) \in Q$ that represents the marked version that will be distributed to the user u in time j; the marks Ξ_j previously broadcast by the pirate are used to determine how

the symbols are allocated. A family of such functions is a dynamic frameproof code if it distributes symbols in such a way that for any pirate set $T \subset U$ with $|T| \leq c$ and any innocent user $u \in U \setminus T$ no sequence $\{\xi_i\}_{i=1}^l$ corresponding to T will match the sequence $\{D_i(\Xi_i, u)\}_{i=1}^l$ received by u. In practice we wish l to be as small as possible, in order to minimise the duration for which framing can potentially occur. In the case where $\{D_\alpha\}_{\alpha=1}^l$ is an l-dynamic c-frameproof code for all $c \geq 2$ then we refer to it simply as an l-dynamic frameproof code.

Example 3.1 If $\mathcal{M}$ is an l-sequential c-frameproof code for user set U and alphabet Q we can define an l-dynamic c-frameproof code $\{D_\alpha\}_{\alpha=1}^l$by setting $D_\alpha(\Xi_\alpha, u) = \mathcal{M}(\alpha, u)$ for all $u \in U$ and $\alpha = 1, 2, \ldots, l$. ■

This is a somewhat trivial example of a dynamic c-frameproof code as the information contained in the pirate broadcast is not used; it is essentially equivalent to an ordinary frameproof code. The following construction yields l-dynamic frameproof codes that are significantly more efficient than those arising in this manner: they use an alphabet $Q = \{0, 1, \ldots, q-1\}$ to protect $q^{l-1}(q-1)$ users from framing in time l. We introduce the notation $S_1 = u$ and $S_j = \{u \in U | D_i(\Xi_i, u) = \xi_i \text{ for all } i = 1, 2, \ldots, j-1\}$ when $j > 1$, so S_j represents the set of all users who have been framed over the first $j-1$ time segments.

Construction 3.2. *For each $j \leq l-1$ divide S_j arbitrarily into q sets of equal size $S_j(0), S_j(1), \ldots, S_j(q-1)$ and define*

$$D_j(\Xi_j, u) = \begin{cases} i & \text{if } u \in S_j(i), \\ 0 & \text{otherwise.} \end{cases} \qquad \text{(for } j \leq l-1\text{)}$$

$$D_l(\Xi_l, u) = \begin{cases} i & \text{if } u \text{ is the } i^{th} \text{ member of } S_l \text{ for } 1 \leq i \leq \min\{|S_l|, q-1\}, \\ 0 & \text{otherwise.} \end{cases}$$

At each time prior to l the set of users who have been framed so far are divided into q groups that each receive a different symbol; at time l up to $q-1$ previously framed users receive unique marks and all other users receive 0. Note that the sets S_j satisfy

$$S_l \subseteq S_{l-1} \subseteq \cdots \subseteq S_1 = U,$$

and that for each $j > 1$ we have that $S_{j+1} = S_j(\xi_j)$, where ξ_j is the symbol broadcast by the pirate at time j.

We observe that this construction does not depend on the size of potential pirate coalitions: in fact it can prevent framing by coalitions of any size $2 \leq c \leq n-1$, as Theorem 3.3 shows. We observed previously that an l-sequential frameproof code can protect at most $l(q-1)$ users; this construction protects $q^{l-1}(q-1)$ users, an exponential increase due to the increased information available in the dynamic case. Indeed, even a length l 2-frameproof code (and hence an l-sequential 2-frameproof code) has size bounded by $2q^{\lceil \frac{l}{2} \rceil}$; this shows that there exist l-dynamic frameproof codes that are asymptotically more efficient than all l-sequential c-frameproof codes when $q \to \infty$, even when c is small.

Theorem 3.3. *The functions $\{D_i\}_{i=1}^l$ defined in Construction 3.2 constitute an l-dynamic frameproof code.*

Proof. During the first segment we have $|S_1| = q^{l-1}(q-1)$, so each set $S_1(i)$ contains $q^{l-2}(q-1)$ users. At time 2, since $S_2 = S_1(\xi_1)$ where ξ_1 is the symbol broadcast by the pirate at time 1 we have $|S_2| = q^{l-2}(q-1)$. Similarly, when $j \leq l-1$ we know $S_j = S_{j-1}(\xi_{j-1})$, so $|S_j| = |S_{j-1}(\xi_{j-1})|$, and $\left\lfloor \frac{|S_{j-1}|}{q} \right\rfloor \leq |S_{j-1}(\xi_{j-1})| \leq \left\lceil \frac{|S_{j-1}|}{q} \right\rceil$. This implies that for $j \leq l-1$ we have $|S_j| = q^{l-j}(q-1)$. In particular $|S_{l-1}| = q(q-1)$, so $|S_{l-1}(\xi_{l-1})| = q-1$, no matter what symbol ξ_{l-1} the pirate chooses to broadcast at time $l-1$. Thus $|S_l| = q-1$, so precisely $q-1$ users are framed over the first $l-1$ time segments. At time l these users are assigned the symbols $1, 2, \ldots, q-1$ and all other users receive 0. It is impossible for any user $u \in S_l$ to be framed at time l therefore, since no other users have received the same mark, hence no pirate set T with $u \notin T$ has the potential to broadcast $D_l(\Xi_l, u)$. Hence we conclude that no innocent user is framed over all l segments, no matter what the pirate broadcast. □

This example shows how this works in practice.

Example 3.2 Suppose $l = 3$ and $Q = \{0, 1, 2\}$. Then $q^{l-1}(q-1) = 18$. The following table shows how the marks are allocated to the users according to the above construction, in response to the particular pirate broadcast shown in row T.

	1	2	3
u_0	0	0	0
u_1	0	0	0
u_2	0	0	0
u_3	0	0	0
u_4	0	0	0
u_5	0	0	0
u_6	1	0	0
u_7	1	0	0
u_8	1	0	0
u_9	1	0	0
u_{10}	1	0	0
u_{11}	1	0	0
u_{12}	2	0	1
u_{13}	2	0	2
u_{14}	2	1	0
u_{15}	2	1	0
u_{16}	2	2	0
u_{17}	2	2	0
T	2	0	0

Here $\xi_1 = 2$, so $S_2 = \{u_{12}, u_{13}, \ldots, u_{17}\}$. At time 2 this set is divided into three sets of size 2, $S_2(0) = \{u_{12}, u_{13}\}$, $S_2(1) = \{u_{14}, u_{15}\}$ and $S_2(2) = \{u_{16}, u_{17}\}$; all other users receive 0 at this time. At time 3 we see that $S_3 = \{u_{12}, u_{13}\}$, so these users receive unique marks and all other users receive 0. Hence the only users who were framed over the first two segments (u_{12} and u_{13}) cannot be framed at time 3, so no user is framed over all $l = 3$ segments. ■

We have seen that the schemes arising from the above construction are more efficient than sequential schemes; now we would like to know whether more

efficient constructions exist. In the case of the sequential frameproof codes greater numbers of users can be protected when the number of traitors is limited, which leads to the question of whether bounding the number of colluding traitors could produce more efficient dynamic schemes. We will see, however, that once we suppose there is more than one traitor we do not in fact gain anything by considering limits on the number of traitors: two traitors can do as much damage as $n-1$ traitors. The following theorem gives precise bounds on the number of users that can be protected from framing by dynamic schemes.

Theorem 3.4. *Let $l \geq 2$ and $q \geq 2$. A q-ary l-dynamic c-frameproof code protecting n users exists if and only if*

1. *either $c = 1$ and $n \leq q^l$,*
2. *or $c \geq 2$ and $n \leq q^{l-1}(q-1)$.*

Proof. (1) Suppose there is only one traitor. If the marked segments are distributed so that each user receives a distinct sequence of l symbols then no user can frame another. There are exactly q^l length l sequences with symbols from an alphabet of size q; if there are no more than q^l users it is therefore possible to allocate a unique sequence to each user. The resulting mark distribution constitutes a q-ary l-dynamic 1-frameproof code protecting q^l users.
We prove the converse using induction on l.

Let $\mathcal{P}(l)$ be the proposition that the existence of an l-dynamic 1-frameproof code $\{D_j\}_{j=1}^{l}$ protecting a set U of users implies that $|U| \leq q^l$.

Then $\mathcal{P}(1)$ is true, since if there exists D_1 protecting more than q users there exist users $t, u \in U$ with $t \neq u$ who receive the same mark at time 1. Then t can frame u at this time, contradicting the 1-dynamic 1-frameproof nature of D_1.

Suppose $\mathcal{P}(k)$ is true for some k. Then every k-dynamic 1-frameproof code protects at most q^k users. Consider a $(k+1)$-dynamic 1-frameproof code $\{D_j\}_{j=1}^{k+1}$ and suppose it protects at least $q^{k+1}+1$ users. At time 1 there exists a mark that is received by at least $\left\lceil \frac{|U|}{q} \right\rceil \geq q^k + 1$ users. Suppose the pirate broadcast consists of this mark ξ_1; then $|S_2| \geq q^k + 1$. If Υ_α is the word $(\upsilon_1, \upsilon_2, \ldots, \upsilon_{\alpha-1}) \in Q^{\alpha-1}$ denote by $\Xi_{\alpha+1}$ the word $(\xi_1, \upsilon_1, \upsilon_2, \ldots, \upsilon_{\alpha-1}) \in Q^\alpha$. Define a family of functions $\{E_j\}_{j=1}^{k}$ with $E_1 \colon S_2 \to Q$ and $E_j \colon Q^{j-1} \times S_2 \to Q$ by setting $E_j(\Upsilon_j, u) = D_{j+1}(\Xi_{j+1}, u)$ for all $u \in S_2$. Then $\{E_j\}_{j=1}^{k}$ is a k-dynamic 1-frameproof code protecting the users in S_2, for if there exist users $t, u \in S_2$ with $t \neq u$ such that $E_j(\Upsilon_j, t) = E_j(\Upsilon_j, u)$ for all $j = 1, 2, \ldots, k$ it follows that $D_i(\Xi_i, t) = D_i(\Xi_i, u)$ for all $i = 2, 3, \ldots, k+1$. Since t and u are in S_2 we have $D_1(u) = D_1(t) = \xi_1$, hence t is capable of having produced the broadcast sequence that framed u over all $k+1$ segments, contradicting the assumption that $\{D_j\}_{j=1}^{k+1}$ is $(k+1)$-dynamic 1-frameproof. As $\{E_j\}_{j=1}^{k}$ is a k-dynamic 1-frameproof code protecting the users in S_2 it follows that $|S_2| \leq q^k$. This leads to a contradiction, hence we see that $\mathcal{P}(k) \Rightarrow \mathcal{P}(k+1)$, therefore $\mathcal{P}(l)$ is true for all $l \geq 1$.

(2) The existence of an l-dynamic c-frameproof code protecting $q^{l-1}(q-1)$ users is provided by Construction 3.2; the proof that $c \geq 2$ implies $n \leq q^{l-1}(q-1)$ is very similar to the above proof.

Let $\mathcal{P}(l)$ be the proposition that the existence of an l-dynamic 2-frameproof code $\{D_j\}_{j=1}^{l}$ protecting a set U of users implies that $|U| \leq q^{l-1}(q-1)$.

To show $\mathcal{P}(2)$ is true we suppose there exists a 2-dynamic 2-frameproof code protecting at least $q(q-1)+1$ users. At time 1 some symbol ξ_1 is received by at least q users; suppose the pirate broadcasts this symbol. At most $q-1$ users can receive a unique mark at time 2, so there exists some user $u \in S_2$ and some user $t \neq u$ who received the same mark at this time. Let $t' \in S_2 \setminus \{u\}$ and note that t and t' are not necessarily distinct. Then the set $T = \{t, t'\}$ is capable of having produced the broadcast that framed the user u over both time segments, contradicting our initial assumption. Hence $\mathcal{P}(2)$ is true.

Assume $\mathcal{P}(k)$ is true for some $k \geq 2$. Suppose there exists a $(k+1)$-dynamic 2-frameproof code protecting at least $q^k(q-1)+1$. Then some symbol ξ_1 is received at time 1 by at least $q^{k-1}(q-1)+1$ users. Defining functions $\{E_j\}_{j=1}^{k}$ as above we see that these functions constitute a k-dynamic 2-frameproof code, for any two users $t, t' \in S_2$ who can frame a third member u of S_2 from time 2 to $k+1$ also frame u at time 1 since all members of S_2 received the symbol ξ_1 broadcast by the pirate at that time. Thus we conclude that $|S_2| \leq q^{k-1}(q-1)$, which is a contradiction. Hence $\mathcal{P}(k) \Rightarrow \mathcal{P}(k+1)$ so $P(l)$ is true for all $l \geq 2$.

Thus any q-ary l-dynamic 2-frameproof code can protect at most $q^{l-1}(q-1)$ users, which implies that a q-ary l-dynamic c-frameproof code can protect at most $q^{l-1}(q-1)$ users when $c \geq 2$. □

We see therefore that framing can indeed be prevented in the dynamic setting, whether or not feedback from the pirate broadcast is available. In the case of l-dynamic c-frameproof codes the optimal number of users supported by such schemes has been shown to be $q^{l-1}(q-1)$ for $c \geq 2$ and q^l when $c = 1$. Further progress in the study of frameproof codes is necessary in order to establish optimal values in the sequential case.

Acknowledgements

I would like to thank Simon Blackburn and Peter Wild for helpful discussions on this topic. Thanks to Carlos Cid for some valuable feedback, and to the anonymous reviewer for some useful suggestions.

References

[1] S.R. Blackburn, Combinatorial schemes for protecting digital content, *Surveys in Combinatorics 2003*, LMS lecture notes series, Vol. 307 (2003) pp. 43–78.

[2] S.R. Blackburn. Frameproof codes. *SIAM Journal on Discrete Mathematics*, 16(3):499–510, 2003.

[3] D. Boneh and J. Shaw, Collusion-secure fingerprinting for digital data, *IEEE Transactions on Information Theory*, Vol. 44, No.5 (1998) pp. 1897–1905.

[4] B. Chor, A. Fiat, and M. Naor, Tracing traitors, *Advances in Cryptology -Crypto '94*, Lecture Notes in Computer Science, Vol. 839 (1994) pp. 257–270.

[5] G.D. Cohen and S.B. Encheva. Efficient constructions of frameproof codes. *Electronics Letters*, 36:1849–1842, 2000.

[6] A. Fiat and T. Tassa, Dynamic traitor tracing, *Advances in Cryptology -Crypto '99*, Lecture Notes in Computer Science, Vol. 1666 (1999) pp. 354–371.

[7] R. Safavi-Naini and Y. Wang, Sequential traitor tracing, *IEEE Transactions on Information Theory*, Vol. 49, No. 5 (2003) pp. 1319–1326.

[8] J.N. Staddon, D.R. Stinson and R. Wei. Combinatorial properties of frameproof and traceability codes. *IEEE Transactions on Information Theory*, 47:1024–1049, 2001.

[9] M.D. Swanson, M. Kobayashi, and A.H. Tewfik, Multimedia data-embedding and watermarking technologies, *Proceedings of the IEEE*, Vol. 86 (1998) pp. 1064–1087.

[10] T. Tassa. Low bandwidth dynamic traitor tracing schemes. *J. Cryptology*, 18(2):167–183, 2005.