Sliding-Window Dynamic Frameproof Codes

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

Abstract

A sliding-window dynamic frameproof code is a scheme for discouraging the piracy of digital broadcasts through the use of digital fingerprinting. In this paper we formally define sliding-window dynamic frameproof codes and provide optimal constructions for a certain class of these schemes. We also discuss bounds on the number of users such schemes can support.

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

1 Introduction

1.1 Schemes for the Prevention of Digital Piracy

Many different schemes have been proposed that make use of digital fingerprinting to prevent or discourage the illegal copying of digital material [2]. A digital fingerprint is created by embedding extra information into the data. For our purposes we require that the marked version be indistinguishable from the original when the data is used for its intended purpose, and also that the marks be robust in the sense that an adversary should not be able to remove or alter a mark without incurring a resulting degradation in the quality of the data. The assumption that it is possible to embed marks with these properties is known as the *watermark assumption*; a discussion of some of the technical issues surrounding this assumption can be found in [13].

Producing and distributing many variants of the data can be expensive, however. Several of the schemes discussed in the literature overcome this by dividing the data into separate segments, each of which is marked in a fixed number of ways. By producing q different variants of l different segments it is possible to create up to q^l different versions of the data as a whole. If we consider the variants of a particular section to correspond to the symbols of an alphabet Q of size q then each copy of the data will correspond to a word in Q^l.

If a single pirate distributes copies of some data that is marked in this fashion then the marks can be used to identify the culprit. However, two or more traitors possessing different versions may decide to collude, combining segments from their different versions in an attempt to produce copies that cannot be traced back to them. For example, if users t_1 and t_2 posses copies marked

$(0,0,1,1)$ and $(1,0,0,1)$ then by adjoining the first two segments of t_1's copy to the last two segments of t_2's copy they could produce a copy with the mark $(0,0,0,1)$. In a similar manner they could produce any of the marks in the set $\{(0,0,1,1,),(1,0,1,1),(0,0,0,1),(1,0,0,1)\}$. This capability is formalised in the following definition.

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

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

A pirate having a set S of different versions at its disposal can combine various segments to produce copies marked with any of the words in $\operatorname{desc}(S)$. Should one of those words correspond to the copy possessed by another user then the pirate could claim that that user was responsible for its creation, effectively framing him/her. For instance the users t_1 and t_2 above could frame a user u who possessed a copy marked $(1,0,1,1)$, since $(1,0,1,1) \in \operatorname{desc}(\{(0,0,1,1),(1,0,0,1)\})$. In order to combat the "toy problem" of a single traitor producing pirate copies yet potentially claiming to have been framed by a coalition of other users, Boneh and Shaw introduced *frameproof codes* in [4]. The following definition of a frameproof code appears in [3]; Boneh and Shaw use the same definition [4], but with a different definition of descendent.

Definition 1.2. *A code $C \subset Q^l$ is a* c-frameproof code *if every set $S \subset C$ with $|S| \leq c$ satisfies*

$$\operatorname{desc}(S) \cap C = S.$$

Suppose there is a set U of n users to whom copies of some data are to be distributed, and that each user is sent a fingerprinted version with marks corresponding to a unique word from a c-frameproof code C. In this case the only codewords that can be produced from a set S of words possessed by c or fewer collaborating traitors are those in S, hence no innocent user can be framed by a set of this size. Thus a c-frameproof code allows us to identify any single user who is illegally reproducing his/her copy of the data without falsely incriminating innocent users, provided no more than c traitors collaborate.

While perhaps being of greater theoretical than practical interest, frameproof codes have been extensively studied. An early result result arising from [4] is that a length l error correcting code with minimum distance d is a c-frameproof code if $d > \left(1 - \frac{1}{c}\right) l$. Cohen and Encheva [5] use error-correcting codes to construct c-frameproof codes of cardinality $q^{\left\lceil \frac{l}{c} \right\rceil}$ for $l \geq 2$ and $c \geq 2$ where $q \geq l$ is a prime power. Stinson and Wei construct them from t-designs and other combinatorial objects. Xing [15] uses a construction involving algebraic curves to obtain better parameters than those arising from error-correcting codes; Safavi-Naini and Wang use constant weight codes to construct binary c-frameproof codes of length l with at least $\frac{1}{l^r}\binom{l}{w}$ codeswords, where w is an integer with $1 \leq w \leq q$ and $r > 3$ is an integer satisfying $r > \left(1 - \frac{1}{c}\right) w$ [9]. An upper bound on the possible size of such codes has been given by Staddon *et al.* [11] who show that if a q-ary c-frameproof code of length l contains n codewords then n satisifies

$$n \leq cq^{\left\lceil \frac{l}{c} \right\rceil}.$$

Blackburn [3] gives a similar bound with an improved constant; the problem of determining a tight asymptotic bound as $q \to \infty$ with k and l fixed is still open, however.

If a code C is c-frameproof for all $c \geq 2$ then we refer to it simply as a *frameproof code.*

Example 1.3. Consider the following length 3 ternary code:

$$C = \{(1,0,0),(2,0,0),(0,1,0),(0,2,0),(0,0,1),(0,0,2)\}.$$

Each codeword has some coordinate position containing a *unique mark*: a symbol shared by no other word in that position. For example, only the first of the words has a 1 in the first position. Let $S \subseteq C$ be a set of size c for some $c \geq 2$. If there exists a word $x \in C \setminus S$ then there is some coordinate in which x has a unique mark, and hence no word in S matches x in that position. This implies that $x \notin \operatorname{desc}(S)$. Therefore $\operatorname{desc}(S) \cap C = S$ (since $S \subseteq \operatorname{desc}(S)$). Hence we conclude that C is a frameproof code.

The above example is a special case of Construction 2 of [3]; the following theorem is a direct consequence of Corollary 3 of that paper.

Theorem 1.4. *[3] Let C be a q-ary, length l frameproof code. Then*

$$|C| \leq l(q-1).$$

Frameproof codes can be used to protect media such as DVDs and CDs where the data is distributed to the users all at one time. In contrast to this is the situation of a TV broadcast, where information is received continuously by the users. A pay TV station will usually encrypt its broadcasts so that only paying users who are allocated the corresponding keys can decrypt the programs. Fiat and Tassa, in their paper on dynamic traitor tracing [6], introduced the scenario in which traitorous users set up a pirate TV station and rebroadcast the material in the clear. In their model the data is divided into segments, which here correspond to perhaps a few minutes of a TV program, and q different versions of each segment are produced then broadcast to different users. Thus each user $u \in U$ who receives the broadcast is effectively sent a sequence $\{M_i(u)\}_{i=1}^{\infty}$, with $M_i(u)$ being the symbol marking the i^{th} segment of the broadcast received by u.

We say that a set $T \subset U$ of users who collaborate to produce a pirate broadcast is a *pirate set.* At time i a pirate set T can choose to broadcast a segment with any of the marks $M_i(t)$ received by a member $t \in T$ of that pirate set. A *pirate broadcast sequence corresponding to a pirate* T is a sequence $\{\xi_i\}_{i=1}^{\infty}$ of marks such that for each i we have $\xi_i \in \{M_i(t) | t \in T\}$. We sometimes use the notation $\Xi_i = (\xi_1, \xi_2, \ldots, \xi_{i-1})$ to represent the $(i-1)$-tuple consisting of the first $i-1$ terms of the sequence $\{\xi_i\}_{i=1}^{\infty}$.

Example 1.5. Suppose a pay TV station has four users, u_1, u_2, u_3 and u_4, and suppose they receive the following sequences of marks:

$$\begin{aligned}
u_1 &: 0,0,0,0,0,0,0,0,\ldots \\
u_2 &: 1,1,1,1,1,1,1,1,\ldots \\
u_3 &: 0,0,1,1,0,0,1,1,\ldots \\
u_4 &: 0,0,0,1,0,0,0,1,\ldots\ .
\end{aligned}$$

Then the sequence $0, 0, 1, 0, 0, 0, 1, 0, \ldots$ is a pirate broadcast sequence corresponding to the pirate set $\{u_1, u_2\}$. It is also a pirate broadcast sequence corresponding to $\{u_1, u_3\}$, but could not be a sequence corresponding to $\{u_1, u_4\}$, since both u_1 and u_4 received the symbol 0 at time 3.

During a given time segment we say that a mark is *unique* if it is received by precisely one user at that time. If the pirate broadcasts a unique mark then it follows that the user who received that unique mark is necessary part of the pirate coalition. Once a user is identified as being guilty in this fashion then his/her subscription can be canceled and appropriate action taken against him/her. Throughout this paper we will be considering traitors that do not incriminate themselves in this fashion. We say that a pirate broadcast sequence $\{\xi_i\}_{i=1}^{\infty}$ is a *valid pirate broadcast sequence* if for each i we have that ξ_i is not a unique mark and hence has been received by at least two users.

The pirate broadcast sequence can thus potentially provide some information as to which users are involved in the piracy, and the pirate broadcast prior to time j can be used in deciding how to distribute the different versions among the users at that time. We refer to this as the *dynamic setting*, since the mark distribution can be determined dynamically in response to the pirate output (see [6, 1, 10, 14]). It was initially studied in the context of dynamic traitor tracing schemes, introduced by Fiat and Tassa [6], which can be used to identify individual members of a pirate coalition and provide evidence of their involvement in piracy. However, it is shown in [6] that a deterministic dynamic traitor scheme requires the use of a marking alphabet of size q that is greater than the number of colluding traitors. If the number of traitors is potentially large then it may be impractical for the broadcaster to produce sufficiently many versions of each segment to be able to implement such a scheme. One possible solution to this dilemma would be to consider probabilistic schemes, as in [14]. The other alternative, which is addressed in this paper, is to focus on the weaker concept of dynamic frameproof codes, which cannot be used to trace colluding traitors but will prevent innocent users from being framed by pirate coalitions.

The rest of this paper is devoted to examining ways of preventing framing of innocent users in this dynamic setting. Section 2 contains a discussion of the *sliding window model* of framing in a dynamic setting. We recall how length l frameproof codes can be applied in the dynamic setting to yield *l-sequential frameproof codes*, which prevent framing in the sliding-window model, and we mention the number of users protected by such codes.

In Section 3 we consider the potential for protecting a greater number of users if information from the pirate broadcast is used in determining the distribution of the marked versions to the users. We define *sliding-window l-dynamic frameproof codes*, which use this information to prevent framing in the sliding-window model, and provide an example of a construction of a sliding-window l-dynamic frameproof code that is more efficient than the schemes previously described.

We generalise this construction in Section 4 to provide a family of sliding-window l-dynamic frameproof codes depending on two parameters whose values can be selected in order to maximise the number of users protected for a given alphabet size and window length. We show that the number of users protected by these schemes is optimal for the given parameters, and we discuss some open problems relating to such schemes.

2 Sequential Frameproof Codes

If we wish to apply frameproof codes in a dynamic setting we must first consider what is meant by framing in a dynamic context. In the case of frameproof codes we were concerned with preventing pirate coalitions from reproducing codewords of length l corresponding to innocent users; in the dynamic case we extend this concept with the following definition.

Definition 2.1. *In the dynamic setting we will consider a user u to have been* framed *if a pirate coalition T broadcasts a sequence $\{\xi_i\}_{i=1}^{\infty}$ such that $u \notin T$ and there exists a time j with $\xi_i = M_i(u)$ for all $i = j, j+1, \dots, j+l-1$, in other words if T broadcasts marks corresponding to those received by u over l consecutive time segments.*

In the rest of this paper we will be concerned with schemes for distributing marks that ensure that coalitions of traitors cannot frame innocent users in this manner; we refer to this as the *sliding-window model*, since it requires that framing be prevented over every window of l consecutive time segments. The window length l is an important parameter in the schemes we discuss; essentially it bounds the maximum length of time over which an innocent user can be framed, hence it is desirable that it be kept as small as possible. If a broadcaster uses a scheme that is able to prevent framing over all windows of length l then after l segments have been broadcast it can be confident that no innocent user can have been framed throughout the entire broadcast, so any user who appears to have been framed over that time must in fact be a traitor.

In [7, 8] it was shown that ordinary frameproof codes can be adapted to prevent framing in the sliding-window model by means of the following construction. These schemes are not dynamic in the true sense of the word, since they do not make use of the information contained in the pirate's broadcast. In later sections we will see how fully dynamic schemes can be used to protect greater numbers of users.

Theorem 2.2. *Let $U = \{u_1, u_2, \dots, u_n\}$ be a set of users and let Q be the alphabet $Q = \{0, 1, \dots, q-1\}$. Suppose there exists a q-ary, length l frameproof code $C \subset Q^l$ with $|C| = n$, and let M be an $n \times l$ matrix with entries from Q whose rows are the words of C. Distributing marks to users such that at time j user u_i receives the segment marked with the symbol $M_{ij'}$ where $j' \in \{1, 2, \dots, l\}$ and $j' \equiv j \pmod{l}$ will prevent framing in the sliding-window model over windows of length l.*

Proof. We observe that if C is a q-ary length l frameproof code then so too is $\{(x_{\sigma^{-1}(1)}, x_{\sigma^{-1}(2)}, \dots, x_{\sigma^{-1}(l)}) | x \in C\}$ for any permutation $\sigma \in S_l$. Suppose there exists a pirate broadcast sequence $\{\xi_i\}_{i=1}^{\infty}$ corresponding to a pirate set $T \subset U$, a user $u \in U \setminus T$ and some time $j > 0$ with $\xi_i = M_i(u)$ for all $i = j, j+1, \dots, j+l-1$. Since for each i we have that $\xi_i = M_i(t)$ for some $t \in T$ it follows that

$$\begin{aligned}&\big(M_j(u), M_{j+1}(u), \dots, M_{j+l-1}(u)\big)\\ &\qquad\qquad \in \operatorname{desc}\Big(\Big\{\big(M_j(t), M_{j+1}(t), \dots, M_{j+l-1}(t)\big)\Big| t \in T\Big\}\Big).\end{aligned}$$

However, the words of $C' = \Big\{\big(M_j(x), M_{j+1}(x), \dots, M_{j+l-1}(x)\big)\Big| x \in U\Big\}$ are cyclic permutations of the words of C, by construction. Hence C' is a frameproof code, which contradicts the above assertion. Thus we conclude that there does not exists any pirate broadcast sequence corresponding to a pirate $T \subset U$ that permits T to frame a user $u \in U \setminus T$ over any l consecutive time segments. $\square$

In [7, 8] such mark distributions which prevent framing in the sliding-window model without recourse to information from the pirate broadcast were referred to as *l-sequential frameproof codes*, in an analogue of the sequential traitor tracing schemes of [10]. We have seen above that a length l frameproof code gives rise to an l-sequential frameproof code; in [7, 8] it was shown that the converse is also true, that the existence of a q-ary l-sequential frameproof code protecting n users implies the existence of a q-ary, length l frameproof code containing n words. Together with Theorem 1.4 this implies that a q-ary, l-sequential frameproof code can protect at most $l(q-1)$ users.

3 Sliding-Window Dynamic Frameproof Codes

We saw in the previous section that length l frameproof codes can be adapted for use in a dynamic setting, the resulting l-sequential frameproof codes enabling the prevention of framing over any l consecutive time segments. However the dynamic setting differs fundamentally from the static case as the information contained in the pirate broadcast is available throughout any given window, whereas in the static situation the pirate only responds after the entire length l word has been distributed. This suggests that in the dynamic setting it may be possible to devise schemes making use of the feedback from the pirate broadcast that are more efficient than those arising from frameproof codes. We propose the following definition of *sliding-window l-dynamic frameproof codes*:

Definition 3.1. *A* sliding-window l-dynamic frameproof code *is a countable family of functions $\{D_i\}_{i=1}^{\infty}$ where $D_1 \colon U \to Q$ and $D_i \colon Q^{i-1} \times U \to Q$ for $i > 1$ with the property that for any valid pirate broadcast sequence $\{\xi_i\}_{i=1}^{\infty}$ corresponding to a pirate T there is no legitimate user $u \in U \setminus T$ and time $j \geq l$ with $D_i(\Xi_i, u) = \xi_i$ for all $i = j-l+1, j-l+2, \dots j$.*

During time segment i the function D_i, which depends on the pirate broadcast prior to time i, is used to determine how the marks are distributed among the users.

The following construction provides an example of a sliding-window l-dynamic frameproof code. A user who is framed over $l-1$ consecutive segments receives a 0 in the subsequent segment; all other users receive the appropriate entry from M.

Construction 3.2. *Suppose there are $n = (q-1)^{l-1}$ users for some $q > 2$ and $l > 2$, and let $Q = \{0, 1, \dots, q-1\}$. Let M be an $n \times (l-1)$ matrix whose rows consist of the n distinct elements of $(Q \setminus \{0\})^{l-1}$. We define $\{D_i\}_{i=1}^{\infty}$ as follows:*

$$D_j(\Xi_j, u_t) = \begin{cases} 0 & \text{if } j \geq l \text{ and } \xi_i = D_i(\Xi_i, u_t) \text{ for all } i = j-l+1, \dots, j-1, \\ M_{t'j} & \text{otherwise, where } t' \in \{1, 2, \dots, l-1\} \\ & \text{and } t' \equiv t \pmod{l-1}. \end{cases}$$

We will prove that this construction does in fact yield a sliding-window l-dynamic frameproof code, but first we provide an example illustrating how it works in practice.

Example 3.3.

$$M = \begin{pmatrix} 1 & 1 \\ 1 & 2 \\ 1 & 3 \\ 1 & 4 \\ 2 & 1 \\ 2 & 2 \\ 2 & 3 \\ 2 & 4 \\ 3 & 1 \\ 3 & 2 \\ 3 & 3 \\ 3 & 4 \\ 4 & 1 \\ 4 & 2 \\ 4 & 3 \\ 4 & 4 \end{pmatrix}$$

	1	2	3	4	5	6	7	8	9
u_1	1	1	1	1	1	1	1	1	1
u_2	1	2	0	2	1	2	1	2	1
u_3	1	3	1	3	1	3	1	3	1
u_4	1	4	1	4	1	4	1	4	1
u_5	2	1	2	1	2	1	2	1	2
u_6	2	2	2	2	2	2	2	0	2
u_7	2	3	2	3	2	3	2	3	2
u_8	2	4	2	4	2	4	2	4	2
u_9	3	1	3	1	3	0	3	1	3
u_{10}	3	2	3	2	3	2	0	2	3
u_{11}	3	3	3	3	3	3	3	3	3
u_{12}	3	4	3	4	3	4	3	4	3
u_{13}	4	1	4	1	0	1	4	1	4
u_{14}	4	2	4	0	4	2	4	2	4
u_{15}	4	3	4	3	4	3	4	3	4
u_{16}	4	4	4	4	4	4	4	4	4
T	1	2	4	1	3	2	2	2	1

Suppose $q = 5$ and $l = 3$, with $n = 4^2 = 16$. The table above shows how the marks would be distributed according to Construction 3.2 over 9 time segments if the pirate were to broadcast the sequence listed in row T. Row k of the table shows the sequence of marks received by user u_k.

User u_2 is framed over the first two segments, and is thus allocated a 0 at time 3, preventing him/her from being framed at that time. Indeed, inspection of the table shows that no user has been framed over any three consecutive segments.

In order to prove that the scheme of Construction 3.2 results in a sliding-window l-dynamic frameproof code we require the following lemma.

Lemma 3.4. *When a scheme defined by Construction 3.2 is employed against any pirate coalition then at each time $j \geq l$ there will be at most one user who has been framed over the previous $l-1$ time segments.*

Proof. We prove this lemma by strong induction on j.
Let $\{D_i\}_{i=1}^{\infty}$ be defined as in Construction 3.2 and $T \subset U$ be a pirate coalition. Let $\mathcal{P}(j)$ be the proposition that for any valid pirate broadcast sequence $\{\xi_i\}_{i=1}^{\infty}$ corresponding to T then at time j there is at most one user u with $D_i(\Xi_i, u) = \xi_i$ for all $i = j-l+1, \ldots, j-1$.
Then $\mathcal{P}(l)$ is true, since over the first $l-1$ time segments user u_t receives a sequence corresponding to row t of M, and the rows of M are all distinct. This implies that at most one user will have received a sequence matching the pirate broadcast over this time.
Suppose $\mathcal{P}(j)$ is true for all $j \leq k$ for some $k \geq l$. This implies that at each time segment prior to k at most one user receives the symbol 0.
Now, over any $l-1$ consecutive time segments the sequences of marks received by user u_t form a cyclic shift of row t of M, with some marks possibly replaced by 0. By the inductive assumption, during the $l-1$ segments occurring prior to

time $k+1$ at most one user will have received a 0 in any given segment, hence no two users receive the same sequence over this time. Therefore at most one user can be framed over this interval, irrespective of the pirate broadcast. Therefore $\mathcal{P}(l), \ldots, \mathcal{P}(k) \Rightarrow \mathcal{P}(k+1)$ and so $\mathcal{P}(j)$ is true for all $j \geq l$ by the principle of mathematical induction. □

This result leads immediately to the following theorem:

Theorem 3.5. *Construction 3.2 results in a sliding-window l-dynamic frameproof code $\{D_i\}_{i=1}^{\infty}$.*

Proof. Let $\{D_i\}_{i=1}^{\infty}$ be defined as in Construction 3.2 and $\{\xi_i\}_{i=1}^{\infty}$ be a valid pirate broadcast sequence corresponding to a pirate coalition $T \subset U$. By Lemma 3.4 at most one user receives the mark 0 at any time, so $\xi_i \neq 0$ for all $i \geq 1$ as $\{\xi_i\}_{i=1}^{\infty}$ is a valid pirate broadcast sequence. Suppose some user u is framed over the $l-1$ consecutive segments prior to some time j. Then by construction u receives 0 at time j, but $\xi_j \neq 0$. Therefore we conclude that no user is framed over any l consecutive time segments, and so $\{D_i\}_{i=1}^{\infty}$ is a sliding-window l-dynamic frameproof code. □

The scheme arising from this construction protects $(q-1)^{l-1}$ users against framing by pirate coalitions of arbitrary size. In Section 2 we concluded that a q-ary l-sequential frameproof code could protect at most $(q-1)l$ users; in the case of Example 3.3 this would mean 12 users would be protected instead of 16. Thus we see that by taking into account the pirate broadcast it is possible to devise schemes that protect a number of users that is exponentially greater than those arising from frameproof codes. The scheme of Example 3.3 is a sliding-window 3-dynamic frameproof code; in the next section we will develop a more-general construction that can protect even more users for a given value of l.

4 Construction of a Family of Sliding-Window l-Dynamic Frameproof Codes

Construction 3.2 yields a q-ary sliding-window l-dynamic frameproof code protecting $(q-1)^{l-1}$ users. In an attempt to protect a greater number of users, given particular values for q and l, we will consider some more-general schemes.

In Construction 3.2 any user who was framed over $l-1$ consecutive time segments was protected in the subsequent segment by being allocated a unique symbol at that time. With an alphabet of size q it is possible to allocate up to $q-1$ unique marks at a given time. Thus instead of restricting ourselves to protecting 1 user we can consider schemes in which a users are protected at a time for any a with $1 \leq a \leq q-1$. However, once a users are given unique symbols only $q-a$ symbols remain to be distributed among the other users.

Furthermore, Construction 3.2 relied on the possibility of protecting a user in every single segment after $t = l$. In fact this is not necessary for the construction of a sliding-window l-dynamic frameproof code, as shown by the following example.

Example 4.1. Let $q = \{0, 1, 2\}$ and let $l = 3$. Suppose there are six users, $\{u_1, u_2, u_3, u_4, u_5, u_6\}$. At time segment j distribute marks as follows:

- If j is odd, distribute the mark 0 to u_1 and u_2, the mark 1 to u_3 and u_4 and the mark 2 to u_5 and u_6.
- If j is even then two users will have been framed in the previous segment. Give these users the symbols 0 and 1, with all other users receiving 2.

The following table shows an implementation of this scheme over five time segments, given a particular pirate broadcast.

	1	2	3	4	5
u_1	0	2	0	2	0
u_2	0	2	0	2	0
u_3	1	0	1	2	1
u_4	1	1	1	2	1
u_5	2	2	2	0	2
u_6	2	2	2	1	2
T	1	2	2	2	0

Any user who is framed in an odd segment is protected in the subsequent even segment. A window of three consecutive segments will necessarily include an odd segment followed by an even segment; as no user is framed over these two segments we see that no user can be framed over the whole window. This construction therefore results in a sliding-window 3-dynamic frameproof code.

The above example contained segments in which users were protected (the even segments) and segments in which no users were given unique marks (the odd segments). We will refer to segments in which users receive unique marks as *protection segments* and all other segments as *ordinary segments.* In this example exactly two users were protected in every protection segment, and there was one ordinary segment between every two protection segments.

In order to generalise the above example we will consider schemes in which α users are protected in every protection segment, with β ordinary segments occurring between subsequent protection segments for $1 \leq \alpha \leq q-1$ and $\beta \geq 0$.

4.1 Constructions with $\beta = 0$

For the sake of simplicity we begin by considering the case in which precisely α users receive unique marks in every segment. We find that it is possible to construct sliding-window l-dynamic frameproof codes with this property that protect up to $\alpha\big((q-\alpha)^{l-1}+(q-\alpha)^{l-2}+\cdots+(q-\alpha)+1\big)$ users. This construction relies on the trivial observation that if the pirate broadcast at time j is ξ_j then any user requiring protection at time $j+1$ must also have received the symbol ξ_j at time j. In later sections we generalise it to the case where $\beta > 0$. Before presenting the construction we define some notation that will help us to describe it more succinctly.

Definition 4.2. *Suppose $\{D_i\}_{i=1}^{\infty}$ is a sliding-window l-dynamic frameproof code and let $\{\xi_i\}_{i=1}^{\infty}$ be a valid pirate broadcast sequence corresponding to a pirate T. For $\gamma = 1, 2, \ldots, l-1$ and $j > \gamma$ we define*

$$S_j^{\gamma} = \{u \in U | D_i(\Xi_i, u) = \xi_i \textit{ for all } i = j-\gamma, j-\gamma+1 \ldots, j-1\}$$

and we set $S_j^0 = U$, $S_j^l = \emptyset$ and $S_j^j = \emptyset$ for $j \leq l$.

Then set S_j^γ contains those users who are framed over the γ segments prior to time j; these sets depend both on the code and on a particular pirate broadcast. For example, in the case of Example 3.3 we have $S_3^2 = \{u_2\}$ and $S_4^1 = \{u_{13}, u_{14}, u_{15}, u_{16}\}$. We note that

$$\phi = S_j^l \subseteq S_j^{l-1} \subseteq \dots S_j^1 \subseteq S_j^0 = U.$$

We also require the following definition:

Definition 4.3. *The* weight *of user u at time j is defined to be*

$$\text{weight}(u) = \max\{\gamma | u \in S_j^\gamma\}.$$

At time j a user of weight γ has been framed over precisely the previous γ segments. In Example 3.3 the user u_7 has weight 0 at time 7, and weight 1 at time 8. We are now in a position to describe the construction.

Construction 4.4. *This construction uses the alphabet $Q = \{0, 1, \dots, q-1\}$ to protect $n = \alpha\big((q-\alpha)^{l-1} + (q-\alpha)^{l-2} + \cdots + (q-\alpha) + 1\big)$ users over windows of size l, where $1 \leq \alpha \leq q-1$ and $l > 2$.*

```
for $j \geq 1$ do
    Order the users by decreasing weight and distribute the
    symbols $q-\alpha, q-\alpha+1, \dots, q-1$ to the first $\alpha$ users;

    for $\gamma = \min\{l-1, j-1\}..0$ do
        Distribute the symbols $0, 1, \dots, q-\alpha-1$ evenly among
        any remaining users in $S_j^\gamma \setminus S_j^{\gamma+1}$;
    end for;
end for;
```

Before proving that this construction yields a sliding-window l dynamic frameproof code we give an example to illustrate how it behaves.

Example 4.5.

	1	2	3	4	5	6	7
u_0	2	0	0	2	0	0	0
u_1	3	0	0	3	0	0	0
u_2	0	2	0	0	2	0	0
u_3	0	3	0	0	3	0	0
u_4	0	0	2	0	0	1	0
u_5	0	0	3	0	0	1	0
u_6	0	1	0	1	0	1	1
u_7	0	1	0	1	0	1	1
u_8	1	0	1	0	1	2	1
u_9	1	0	1	0	1	3	1
u_{10}	1	1	1	1	1	0	1
u_{11}	1	1	1	1	1	0	1
u_{12}	1	1	1	1	1	1	2
u_{13}	1	1	1	1	1	1	3
T	0	0	0	0	1	1	0

Let $l = 3$ and $q = 4$, with $\alpha = 2$. Then the resulting scheme will protect $2(2^2 + 2 + 1) = 14$ users. The above table shows an example of the above construction being applied over 7 segments given a particular choice of pirate broadcast.

At time $j = 1$ all users have weight 0, so the first two users are given unique marks, with half the remaining users receiving 0 and the rest receiving 1. At time $j = 2$ the users u_2 to u_7 are in S_2^1 and hence have weight 1. Thus unique marks a distributed to u_2 and u_3, half of the rest of these users receive 0 and half 1. The remaining users are all in $S_2^0 \setminus S_2^1$; 0 is received by half of them and 1 by the other half. At each time $j \geq 3$ there are precisely two users of weight 2, which implies that any user who is framed over two segments receives a unique mark in the subsequent segment and is hence protected.

The following theorem will be useful in showing that this construction works as claimed. For convenience we define $h_j^\gamma = |S_j^\gamma|$.

Theorem 4.6. *When the scheme of Construction 4.4 is applied to a valid pirate broadcast then for every $j \geq 1$ we have that*

$$h_j^\gamma = \alpha\big((q-\alpha)^{l-\gamma-1} + (q-\alpha)^{l-\gamma-2} + \cdots + (q-\alpha) + 1\big)$$

for every $\gamma = 0, 1, \ldots, l-1$ with $\gamma < j$.

Proof. We prove this result using induction on j.
Let $\mathcal{P}(j)$ be the proposition that

$$h_j^\gamma = \alpha\big((q-\alpha)^{l-\gamma-1} + (q-\alpha)^{l-\gamma-2} + \cdots + (q-\alpha) + 1\big)$$

for every $\gamma = 0, 1, \ldots, l-1$ with $\gamma < j$.
Then $\mathcal{P}(1)$ is true since by definition $S_1^0 = U$, so

$$h_1^0 = \alpha\big((q-\alpha)^{l-1} + (q-\alpha)^{l-2} + \cdots + (q-\alpha) + 1\big).$$

Suppose $\mathcal{P}(k)$ is true for some $k \geq 1$.
Consider h_{k+1}^γ. We know that $h_{k+1}^0 = \alpha\big((q-\alpha)^{l-1} + (q-\alpha)^{l-2} + \cdots + (q-\alpha) + 1\big)$. For $\gamma > 0$ we observe that the users in S_{k+1}^γ are precisely those users in $S_k^{\gamma-1}$ who are also framed at time k, and we have

$$h_k^{\gamma-1} = \alpha\big((q-\alpha)^{l-\gamma} + (q-\alpha)^{l-\gamma-1} + \cdots + (q-\alpha) + 1\big)$$

by the inductive assumption. Now α of the users in $S_k^{\gamma-1}$ will be assigned unique marks at time k (since $h_k^{\gamma-1} \geq \alpha$ for all $\gamma \leq l-1$); these marks cannot be part of a valid pirate broadcast. The remaining $q-\alpha$ symbols will be evenly distributed among the remaining $\alpha\big((q-\alpha)^{l-\gamma} + (q-\alpha)^{l-\gamma-1} + \cdots + (q-\alpha)\big)$ users in that set. Therefore, the mark the pirate broadcasts at time k will have been received by $\alpha\big((q-\alpha)^{l-\gamma-1} + (q-\alpha)^{l-\gamma-2} + \cdots + (q-\alpha) + 1\big)$ of the users in $S_k^{\gamma-1}$, hence

$$h_{k+1}^\gamma = \alpha\big((q-\alpha)^{l-\gamma-1} + (q-\alpha)^{l-\gamma-2} + \cdots + (q-\alpha) + 1\big).$$

Thus $\mathcal{P}(k) \Rightarrow \mathcal{P}(k+1)$, and therefore $\mathcal{P}(j)$ is true for all $j \geq 1$ by the principle of mathematical induction. □

The above theorem implies that $h_j^{l-1} = \alpha$ for every $j \geq l$. Thus precisely α users are framed over any $l-1$ consecutive segments; these users are given unique marks in the subsequent segment and hence protected. Thus we have the following useful corollary.

Corollary 4.7. *The scheme arising from Construction 4.4 is a sliding-window l-dynamic frameproof code.*

Construction 3.2 yields a code protecting $(q-1)^{l-1}$ users over windows of length l using an alphabet of size q. If we choose to use $\alpha = 1$ in Construction 4.4, however, we can protect $(q-1)^{l-1} + (q-1)^{l-2} + \cdots + (q-1) + 1$ users, which represents an improvement for all $q > 2$ and $l > 2$. In fact, of all possible schemes in which α users receive unique marks in each segment, the ones arising from the above Construction 4.4 are the most efficient, as we will see below.

In the case of ordinary c-frameproof codes it is possible to construct larger codes if we have a restriction on the maximum number c of traitors in a pirate coalition. It would be natural to wonder whether it is possible to consider sliding window l-dynamic c-frameproof codes in which at most c traitors collude in piracy. The following theorem shows that (at least in the case where α users are protected in each segment) we do not gain anything by doing so, in that no sliding-window l-dynamic c-frameproof code with $c \geq 2$ can protect more users than the codes of Construction 4.4.

Theorem 4.8. *Suppose that there exists a q-ary sliding-window l-dynamic 2-frameproof code protecting n users, in which α users receive unique marks during each segment, with $1 \leq \alpha \leq q-1$. Then n satisfies*

$$n \leq \alpha\big((q-\alpha)^{l-1} + (q-\alpha)^{l-2} + \cdots + (q-\alpha) + 1\big).$$

Proof. Suppose $\{D_i\}_{i=1}^{\infty}$ is a sliding-window l-dynamic 2-frameproof code protecting n users where $n \geq \alpha\big((q-\alpha)^{l-1} + (q-\alpha)^{l-2} + \cdots + (q-\alpha) + 1\big) + 1$. During the first time segment α users receive unique marks, which leaves $q-\alpha$ marks to be distributed among the remaining users. We observe that there exists such a mark that is received by at least $\alpha\big((q-\alpha)^{l-2} + (q-\alpha)^{l-3} + \cdots + (q-\alpha) + 1\big) + 1$ users; if we suppose this mark is broadcast by the pirate at this time then we have that

$$h_2^1 \geq \alpha\big((q-\alpha)^{l-2} + (q-\alpha)^{l-3} + \cdots + (q-\alpha) + 1\big) + 1.$$

In the second time segment, there exists some symbol that is received by at least $\lceil \frac{h_2^1 - \alpha}{q-\alpha} \rceil$ of the users in S_2^1, if the pirate broadcasts this symbol it ensures that

$$h_3^2 \geq \alpha\big((q-\alpha)^{l-3} + (q-\alpha)^{l-4} + \cdots + (q-\alpha) + 1\big) + 1.$$

Through applying this reasoning to the first $l-1$ time segments we can see that there exists a valid pirate broadcast sequence with

$$h_i^{i-1} \geq \alpha\big((q-\alpha)^{l-i-1} + (q-\alpha)^{l-i-2} + \cdots + (q-\alpha) + 1\big) + 1,$$

so $h_l^{l-1} \geq \alpha + 1$.

As only α users are protected in segment l, however, there exists at least one user who has been framed over the first $l-1$ segments yet is not protected at time l. If we denote that user by u then there exists some user $t \neq u$ with $D_l(\Xi_l, u) = D_l(\Xi_l, t)$; suppose that this is the mark broadcast by the pirate at this time. Also, there were at least $\alpha+1$ users in S_l^{l-1}, so there exists some user t' (not necessarily distinct from t) with $t' \in S_l^{l-1} \backslash \{u\}$. The set $T = \{t', t\}$ is then capable of having produced the relevant pirate broadcast and thus framing u, which contradicts our assumption that the code was sliding-window l-dynamic 2-frameproof.

Thus we conclude that for a sliding-window l-dynamic 2-frameproof code of the desired properties we have

$$n \leq \alpha\big((q-\alpha)^{l-1} + (q-\alpha)^{l-2} + \cdots + (q-\alpha) + 1\big).$$

□

4.2 General β

It is possible to generalise the above results to the case where $\beta > 0$. The following construction takes as a parameter $\beta \geq 0$, with $l \geq 2\beta + 1$. It is a generalisation of Construction 4.4, with which it coincides in the case where $\beta = 0$.

The codes arising from this construction protect α users during a protection segment, with β ordinary segments occurring between each protection segment. In this case every length l window necessarily contains a sequence of $l - \beta$ segments ending with a protection segment. By ensuring that no user is framed over any such sequence these codes guarantee that no user is framed over an entire window.

A sequence of $l - \beta$ segments ending with a protection segment will commence with $\big(l-(\beta+1)\lceil\frac{l-\beta}{\beta+1}\rceil\big)$ ordinary segments followed a protection segment; we denote this quantity by r. In the schemes produced by this construction segments in which $j \equiv (r+1) \pmod{\beta+1}$ will be protection segments, hence in these segments α users are given unique marks and the remaining $q - \alpha$ marks are allocated so that on each set S_j^γ they are distributed as evenly as possible. All other segments are ordinary segments, in which all q marks are distributed evenly among users in a similar fashion.

As we will prove in Theorem 4.12, during each protection segment all users who have been framed over the previous $l - b - 1$ segments are given unique marks and hence protected. During an ordinary segment occurring at time j the construction ensures that all q symbols are distributed evenly between users who have been framed over the previous γ segments for any γ satsifying $0 \leq \gamma \leq l - 2b + j'$; the segment $j - (1 - 2b + j')$ is the start of the sequence of $l - b$ segments that will conclude with the first protection segment to occur after time j.

Construction 4.9. *This construction is a modification of Construction 4.4. It protects* $\alpha q^r \Big(\big((q-\alpha)q^\beta\big)^{\lceil\frac{l-\beta}{\beta+1}\rceil-1} + \big((q-\alpha)q^\beta\big)^{\lceil\frac{l-\beta}{\beta+1}\rceil-2} + \cdots + (q-\alpha)q^\beta + 1\Big)$ *users where* $r = \big(l-(\beta+1)\lceil\frac{l-\beta}{\beta+1}\rceil\big)$, *for* $\alpha \leq q-1$ *and* $l \geq 2\beta+1$.

```
for $j \geq 1$ do
    $j' := j - r - 1 \pmod{\beta + 1}$;
    if $j' = 0$ then
```

```
        Order the users by decreasing weight and distribute the
        symbols $q-\alpha, q-\alpha+1, \ldots, q-1$ to the first $\alpha$ users;

        for $\gamma = \min\{l-\beta-1, j-1\}..0$ do
            Distribute the symbols $0, 1, \ldots, q-\alpha-1$ evenly among
            any remaining users in $S_j^\gamma \setminus S_j^{\gamma+1}$;
        end for;
    else
        for $\gamma = \min\{l-2\beta+j', j-1\}..0$ do
            Distribute the symbols $0, 1, \ldots, q-1$ evenly among
            any users in $S_j^\gamma \setminus S_j^{\gamma+1}$;
        end for;
    end if;
end for;
```

We now give an example of how the above construction works in practice.

Example 4.10. Let $l = 5$ and $\beta = 1$ with $\alpha = 1$ and $q = 3$. Then $\left\lceil \frac{l-\beta}{\beta+1} \right\rceil = 2$, so the code resulting from the above construction protects 21 users. The table below is an example of a mark distribution that results over six time segments.

	1	2	3	4	5	6
u_0	0	2	0	0	0	0
u_1	0	0	0	0	0	0
u_2	0	0	0	0	0	0
u_3	0	0	0	0	0	0
u_4	0	1	0	0	0	0
u_5	0	1	1	2	0	0
u_6	0	1	2	0	1	0
u_7	1	0	0	0	1	1
u_8	1	0	0	1	1	1
u_9	1	0	1	0	1	1
u_{10}	1	0	1	0	1	1
u_{11}	1	0	1	0	1	1
u_{12}	1	0	1	1	0	1
u_{13}	1	0	1	1	1	1
u_{14}	2	1	1	1	2	2
u_{15}	2	1	2	1	2	0
u_{16}	2	1	2	1	2	0
u_{17}	2	1	2	1	2	0
u_{18}	2	1	2	1	2	1
u_{19}	2	1	2	1	2	1
u_{20}	2	1	2	1	2	1
T	0	1	1	1	2	0

In segment 3 each of the three users u_4, u_5 and u_6 who have been framed over the first two segments gets a different symbol and then the symbols are distributed evenly among the rest of the users. In time 4 the unique user u_5 who was framed over the first three segments is protected, the symbols 0 and 1 are distributed evenly among the remaining users u_9 to u_{14} who were framed in segment 3, then they are distributed evenly among the remaining users.

In order to prove that these schemes work as claimed we require the following lemma.

Lemma 4.11. *When the scheme of Construction 4.9 is applied to a valid pirate broadcast then for every j that is not equivalent to $r+1 \pmod{\beta+1}$ we have that*

$$\left\lfloor \frac{h_j^\gamma}{q} \right\rfloor \leq h_{j+1}^{\gamma+1} \leq \left\lceil \frac{h_j^\gamma}{q} \right\rceil$$

for all $\gamma = 0, 1, \ldots, \min\{j-1, l-b-1\}$.

Proof. At time j the q symbols in the mark alphabet are distributed evenly among the users in the set S_j^γ; each symbol is thus received by $\left\lfloor \frac{h_j^\gamma}{q} \right\rfloor$ or $\left\lceil \frac{h_j^\gamma}{q} \right\rceil$ of those users. The users in $S_{j+1}^{\gamma+1}$, however, are precisely those users in S_j^γ who receive a mark matching the pirate broadcast at time j; the result follows. □

Theorem 4.12. *When the scheme of Construction 4.9 is applied to a valid pirate broadcast then for every $j \geq 1$ with $j \equiv r+1 \pmod{\beta+1}$ we have that*

$$h_j^\gamma = \alpha\Big(\big((q-\alpha)q^\beta\big)^{\left\lceil \frac{l-\beta}{\beta+1} \right\rceil - 1 - \delta} + \big((q-\alpha)q^\beta\big)^{\left\lceil \frac{l-\beta}{\beta+1} \right\rceil - 2 - \delta} + \cdots + (q-\alpha)q^\beta + 1\Big)$$

for every $\gamma < j$ with $\gamma = \delta(\beta+1) + r$ where $\delta \geq 0$.

Proof. Let $j = (\beta+1)j^* + r + 1$; we prove this result by induction on j^*. Let $\mathcal{P}(j^*)$ be the proposition that under the above conditions

$$h_j^\gamma = \alpha\Big(\big((q-\alpha)q^\beta\big)^{\left\lceil \frac{l-\beta}{\beta+1} \right\rceil - 1 - \delta} + \big((q-\alpha)q^\beta\big)^{\left\lceil \frac{l-\beta}{\beta+1} \right\rceil - 2 - \delta} + \cdots + (q-\alpha)q^\beta + 1\Big)$$

for every $\gamma < j$ with $\gamma = \delta(\beta+1) + r$ where $\delta \geq 0$.

Then $\mathcal{P}(0)$ is true, since the first r segments are ordinary segments and $h_1^0 = n$. Applying Lemma 4.11 r times we have

$$\begin{aligned} h_{r+1}^r &= \frac{h_1^0}{q^r} \\ &= \alpha\Big(\big((q-\alpha)q^\beta\big)^{\left\lceil \frac{l-\beta}{\beta+1} \right\rceil - 1} + \big((q-\alpha)q^\beta\big)^{\left\lceil \frac{l-\beta}{\beta+1} \right\rceil - 2} + \cdots + (q-\alpha)q^\beta + 1\Big). \end{aligned}$$

Suppose $\mathcal{P}(k)$ is true for some $k \geq 0$.
Consider time $(k+1)(\beta+1) + (r+1)$. The users in $S_{(k+1)(\beta+1)+(r+1)}^{\delta(\beta+1)+r+1}$ are those users in $S_{k(\beta+1)+(r+1)}^{(\delta-1)(\beta+1)+r+1}$ who have also been framed over time $k(\beta+1)+r+1$ to $(k+1)(\beta+1)+r$. During time segment $k(\beta+1)+r+1$ precisely α of the users in $S_{k(\beta+1)+(r+1)}^{(\delta-1)(\beta+1)+r+1}$ receive unique marks, with remaining symbols being distributed evenly among the other users in this set, hence

$$\begin{aligned} h_{k(\beta+1)+r+2}^{(\delta-1)(\beta+1)+r+1} &= \frac{h_{k(\beta+1)+r+1}^{(\delta-1)(\beta+1)+r} - \alpha}{q-\alpha} \\ &= \frac{\alpha}{q-\alpha}\Big(\big((q-\alpha)q^\beta\big)^{\left\lceil \frac{l-\beta}{\beta+1} \right\rceil - 1 - (\delta-1)} \\ &\qquad + \big((q-\alpha)q^\beta\big)^{\left\lceil \frac{l-\beta}{\beta+1} \right\rceil - 2 - (\delta-1)} + \cdots + (q-\alpha)q^\beta\Big). \end{aligned}$$

We now apply Lemma 4.11 β times to obtain

$$\begin{aligned} h^{(\delta)(\beta+1)+r}_{(k+1)(\beta+1)+r+1} &= \frac{h^{(\delta-1)(\beta+1)+r+1}_{k(\beta+1)+r+2}}{q^{\beta}} \\ &= \alpha\Big(\big((q-\alpha)q^{\beta}\big)^{\lceil \frac{l-\beta}{\beta+1}\rceil -1-\delta} \\ &\qquad + \big((q-\alpha)q^{\beta}\big)^{\lceil \frac{l-\beta}{\beta+1}\rceil -2-\delta} + \cdots + (q-\alpha)q^{\beta} + 1\Big). \end{aligned}$$

Thus $\mathcal{P}(k) \Rightarrow \mathcal{P}(k+1)$ and hence $\mathcal{P}(j)$ is true for all $j \geq 1$ by the principle of mathematical induction. □

In particular, this shows that at every ordinary segment j we have $h_j^{l-\beta-1} = \alpha$; all α users in $S_j^{l-\beta-1}$ are protected at time j, hence no user is framed over a sequence of $l-\beta$ segments ending in a protection segment. Every length l window contains such a sequence, from which we conclude:

Corollary 4.13. *Construction 4.9 yields a sliding-window l-dynamic frameproof code.*

As in the case for $\beta = 0$, this construction is optimal for the given parameters: the proof of Theorem 4.8 can be modified to give the following result.

Theorem 4.14. *Suppose that there exists a q-ary sliding-window l-dynamic 2-frameproof code in which every $\beta+1^{th}$ segment is a protection segment where α users receive unique marks and the remaining segments are ordinary segments. If this code supports n users then n satisfies*

$$n \leq \alpha q^{l-(\beta+1)\lceil \frac{l-\beta}{\beta+1}\rceil}\Big(\big((q-\alpha)q^{\beta}\big)^{\lceil \frac{l-\beta}{\beta+1}\rceil-1} + \big((q-\alpha)q^{\beta}\big)^{\lceil \frac{l-\beta}{\beta+1}\rceil-2} + \cdots + (q-\alpha)q^{\beta} + 1\Big).$$

If we consider the behaviour of the above upper bound as $q \to \infty$ we see that the degree of the leading term is $l-\beta-1$, which is maximised when $\beta = 0$, in which case the leading term reduces to $\alpha(q-\alpha)^{l-1}$. In the case where $q \mid l$ this is maximised by setting $\alpha = \frac{q}{l}$; this results in a leading term of size $\frac{(l-1)^{l-1}}{l^l}q^l$. Hence we have the following.

Theorem 4.15. *A sliding-window l-dynamic frameproof code that uses evenly-spaced protection segments and protects the same number of users in each protection segment with an alphabet of size q can protect at most n users, where*

$$n \leq \frac{(l-1)^{l-1}}{l^l}q^l + O(q^{l-1}),$$

as $q \to \infty$ with l fixed.

4.2.1 Further Possibilities

In order to study sliding-window dynamic frameproof codes of complete generality, it would be necessary to consider codes in which the value of α varied with each segment. By letting α range between 0 and $q-1$ this would encompass all possible sliding-window dynamic frameproof codes. There remains the open problem *do there exist q-ary sliding-window l-dynamic frameproof codes* *supporting more users than the ones discussed above?* Attempts to solve this question run into the problem that the behaviour of the mark distribution depends on the pirate's actions, which themselves depend on the distribution, so that it is hard to make progress in the absence of further assumptions about the behaviour of either the pirate or the mark distribution. The following bound, however, arises from Theorem 3.3 of [7, 8].

Theorem 4.16. *A sliding-window l-dynamic frameproof code using an alphabet of size q can support at most n users where*

$$n \leq q^l + O(q^{l-1}),$$

as $q \to \infty$ with l fixed.

There is a discrepancy between this asymptotic result and that given in the previous section: the degree of the leading term is the same in each case, but the coefficient differs. Thus we have the related question *do there exist q-ary sliding-window l-dynamic frameproof codes of size $cq^l + O(q^{l-1})$ where $c > \frac{(l-1)^{l-1}}{l^l}$?*

Acknowledgements

I'd like to thank Simon Blackburn and Peter Wild for their comments on this material, the Commonwealth Scholarship Commission and EPSRC for their support, and the anonymous reviewers for their helpful suggestions for improvements.

References

[1] O. Berkman, M. Parnas and J. Sgall. Efficient Dynamic Traitor Tracing. *SIAM Journal on Computing*, 30:1802–1828, 2001.

[2] S.R. Blackburn. Combinatorial schemes for protecting digital content. In C. D. Wensley, editor, *Surveys in Combinatorics 2003*, volume 307 of *LMS lecture notes series*, pages 43–78. Cambridge University Press, 2003.

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

[4] D. Boneh and J. Shaw. Collusion-secure fingerprinting for digital data. *IEEE Transactions on Information Theory*, 44(5):1897–1905, 1998.

[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. In *Advances in Cryptology -Crypto '99*, volume 1666 of *LNCS*, pages 354–371. Springer-Verlag, 1999.

[7] M.B. Paterson. Dynamic frameproof codes. *Ph.D. thesis, University of London*, 2005.

[8] M.B. Paterson. Sequential and dynamic frameproof codes. *Preprint, 2005.*

[9] R. Safavi-Naini and Y. Wang. New results on frameproof codes and traceability schemes *IEEE Transactions on Information Theory*, 47:3029–3033, 2001.

[10] R. Safavi-Naini and Y. Wang. Sequential traitor tracing. *IEEE Transactions on Information Theory*, 49:1319–1326, 2003.

[11] 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.

[12] D.R. Stinson and R. Wei. Combinatorial properties and constructions of traceability schemes and frameproof codes. *SIAM Journal on Discrete Mathematics*, 11:41–53, 1998.

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

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

[15] C. Xing. Asymptotic bounds on frameproof codes. *IEEE Transactions on Information Theory*, 48(11):2991–2995, 2002.