A New Construction for Sequential Traitor Tracing

Reihaneh Safavi-Naini and Yejing Wang
School of IT and CS, University of Wollongong,
Wollongong 2522, Australia
email: [rei,yejing]@uow.edu.au

October 2, 2001

Abstract

In a pay-TV system a subscriber uses a decoder to decrypt the broadcasted signal. Each decoder contains a unique set of decryption keys that can be used to identify the owner, and allows him/her to decrypt the data aimed at him/her. Traitor tracing schemes ensure that if up to c colluders construct a pirate decoder to access the data illegally, one of them can be identified. Sequential tracing schemes provide protection against colluders who *re-broadcast* the decrypted content to make it available for un-authorised users. A sequential tracing scheme ensures that all the colluders are identified and disconnected from the system.

In this paper we review the model of sequential tracing and propose a new construction.

1 Introduction

Protecting digital content against illegal copying and redistribution is one of the key problems facing the owners and distributors of digital content. Access control methods such as encryption schemes ensure that a digital object is only accessible to the person who owns the key information and so has paid the required fees. However when the content is decrypted, a malicious buyer can make illegal copies of the object and re-distribute it.

Traitor tracing schemes provide protection against illegal copying and redistribution of the digital data. A good example of application of traitor tracing is pay-TV systems. The TV station encrypts the content and broadcasts it to all the users. Each user has a decoder box with a set of keys that allows him/her to decrypt the content. However, some subscribers might collude to produce a pirate decoder by taking part of their keys. A traitor tracing scheme allows the broadcaster to identify at least one colluder by testing the keys inside a pirate decoder. Traitor tracing schemes were first introduced by Chor et al [4], and studied by various authors [10, 13, 14, 9, 3, 5, 12, 16].

Dynamic traitor tracing was introduced by Fiat et al [7]. This time traitors' aim is to bypass the security of the system by *re-broadcasting the content* after it is decoded. That is the colluders use their decoders to decrypt the content and then once it is in plain-text form, re-broadcast the plain-text to another group of users. To trace traitors

in this case, the content is broken into segments and for each segment different 'versions' is constructed. Users are divided into groups and each group receives a particular version. In this way a re-broadcasted message can be linked to the subgroup who had received that particular version. The two main characteristics of the new setting are (i) the plaintext content is marked and, (ii) there is a *feedback* from the channel which allows the traitor to become localised. An important feature of this system is that it allows *all* traitors to be traced. Efficient dynamic traitor tracing schemes have been proposed in [1, 2, 8].

Safavi-Naini and Wang [11] showed an attack on dynamic traitor tracing schemes and proposed a sequential traitor tracing that is secure against the attack. They gave a construction using an error-correcting code with minimum Hamming distance satisfying a particular lower bound. In this paper we construct an error-correcting code with this property that can be used as a sequential traitor tracing scheme.

The paper is organised as follows. In section 2 we review sequential traitor tracing schemes. Section 3 gives our construction. Section 4 concludes the paper.

2 Model and Definitions

We assume the *protected content* is divided into L *segments*, and there is a watermarking code $\mathcal{W} = \{1, \cdots, q\}$, that is used to mark segments and produce q *versions* of each segment. Let $U = \{u_1, u_2, \cdots, u_n\}$ denote the set of users. User u_i receives a sequence of marks in $\mathcal{W}$, denoted by u_i, that the content provider allocates to him according to a *mark allocation table* M. The table has N rows and L columns and $M(i,j)$ is the mark allocated to user i in segment j. There is a *feedback sequence* $F = ()$ which is initialised to the empty sequence. In segment j, the content provider sends the ℓ^{th} version to all users for whom $M(i,j)$ is ℓ and observes the feedback. The feedback signal $f_j \in \mathcal{W}$ is appended to F_{j-1} to construct $F_j = (f_1, \cdots, f_j)$ which is used to identify traitors. A feedback sequence F is called *c-consistent* if it can be generated by a colluder set of size at most c. Traitors are traced one by one, by examining the sequence of feedback signal and after d segments it is possible to trace all the traitors: that is the tracing algorithm *converges*. We assume that when a traitor is found, he is *disconnected*.

Definition 2.1 *A sequential $(c,d)_q$-traceability scheme consists of a mark allocation table M and a tracing algorithm A,*

1. *M is an $N \times L$ matrix with entries from $\mathcal{W}$;*

2. *A is a function*

$$A : \mathcal{W}^* \longrightarrow 2^U$$

with the property that for any c-consistent feedback sequence F, there exists a sequence of integers $0 < d_1 < d_2 < \cdots < d_k = d \leq \ell$ such that

$$A(F_j) = \begin{cases} T_j \neq \emptyset, & \text{for } j = d_1, d_2, \cdots, d_k \\ -, & \text{otherwise} \end{cases}$$

and $\bigcup_{j=1}^{k} T_{d_j} = C$, provided that C has produced F and $|C| \leq c$.

It is shown [11] that a sequential $(c,d)_q$-traceability scheme can be constructed via a q-ary error-correcting codes. We denote by $(L, N, D)_q$-ECC an error-correcting code over a q-ary alphabet with length L, minimum Hamming distance D having N codewords. A q-ary linear error-correcting code of dimension k is denoted by $[L, k, D]_q$.

Theorem 2.1 *Suppose there is an* $(L, N, D)_q$*-ECC,* Γ*. If*

$$D \geq (1 - \frac{1}{c^2})L + \frac{1}{c}, \tag{1}$$

then Γ *is a sequential* $(c, d)_q$*-traceability scheme in which* $d = c(L - D + 1)$*.*

From (1), in the case of equality we have

$$c = \lfloor \frac{-1 + \sqrt{1 + 4L(L-D)}}{2(L-D)} \rfloor.$$

Example of ECC that satisfy (1) are Reed-Solomon codes (RS-codes) or algebraic geometry codes (AG-codes). A RS-code is a linear q-ary code of length $L = q-1$, minimum Hamming distance $D = L - k + 1$, and dimension k, having $N = q^k$ codewords. It is well-known that $[L, k, D]_q$ RS-codes exist. An AG-code $[L, k, L + 1 - k - g]_q$ is a linear code of length L, dimension k and minimum Hamming distance $D = L + 1 - k - g$. It is known [15] that an AG-code $[L, k, L + 1 - k - g]_q$ exists if there exists an algebraic curve of genus g over $GF(q)$ having n rational points. In the next section we construct an ECC-code that satisfies (1).

3 A New Construction

Let F_q, F_{q^k} be fields of q and q^k elements, respectively. The trace function $Tr_{q^k|q} : F_{q^k} \to F_q$ of F_{q^k} over F_q is given by,

$$Tr_{q^k|q}(x) = x + x^q + x^{q^2} + \cdots + x^{q^{k-1}}.$$

When it is clear from the context we will use $Tr(x)$ instead of $Tr_{q^k|q}(x)$. The following proposition can be found in [6].

Proposition 3.1 *For any* $a \in F_q$*,*

$$|\{x \in F_{q^k} : Tr(x) = a\}| = q^{k-1}.$$

Let k, s be positive integers such that

$$k = 2t, s < q^{k/2}+1, \exists\, r \text{ s.t. } r \mid t,\ q^r = -1\ (mod\ s) \tag{2}$$

Note that when integers k and s are such that (2) is satisfied, then s is a divisor of $q^r + 1$ for some divisor r of t, and so is a divisor of $q^t + 1$. Hence s is a divisor of $q^k - 1 = (q^t + 1)(q^t - 1)$.

Let $x_1, x_2, \cdots, x_{q^k}$ be distinct elements of F_{q^k}. Consider the following vector

$$\Big(Tr(\alpha x_1^s + \beta),\ Tr(\alpha x_2^s + \beta),\ \cdots,\ Tr(\alpha x_{q^k}^s + \beta)\Big) \tag{3}$$

in which $\alpha \in F_{q^k}^*$, $\beta \in F_{q^k}$, and k and s satisfy the conditions in (2). For simplicity, we denote by (α, β, s) the vector (3). Denote by

$$z(\alpha, \beta, s) = |\{x \in F_{q^k} : Tr(\alpha x^s + \beta) = 0\}|.$$

Wolfmann showed the following theorem.

Theorem 3.1 *([17, 18]) Let* k *and* s *be integers satisfying (2) and* n *be such that* $ns = q^k - 1$*. Then* $z(\alpha, \beta, s)$ *is given by the following formulae*

1. *If* $\alpha^n = \sigma_1$ *and* $Tr(\beta) = 0$*, then* $z(\alpha, \beta, s) = q^{k-1} - \sigma(s-1)(q-1)q^{k/2-1}$*;*
2. *If* $\alpha^n = \sigma_1$ *and* $Tr(\beta) \neq 0$*, then* $z(\alpha, \beta, s) = q^{k-1} + \sigma(s-1)q^{k/2-1}$*;*
3. *If* $\alpha^n \neq \sigma_1$ *and* $Tr(\beta) = 0$*, then* $z(\alpha, \beta, s) = q^{k-1} + \sigma(q-1)q^{k/2-1}$*;*
4. *If* $\alpha^n \neq \sigma_1$ *and* $Tr(\beta) \neq 0$*, then* $z(\alpha, \beta, s) = q^{k-1} - \sigma q^{k/2-1}$*;*

where $\sigma = (-1)^{t/r}$ *and* $\sigma_1 = \sigma^u$ *with* $us = q^r + 1$*.*

Using Theorem 3.1 we have the following lemma about vectors of the form (3).

Lemma 3.1 *For any given integer* s *satisfying (2) and* $\alpha_1, \alpha_2 \in F_{q^k}^*$*, if* $\alpha_1 \neq \alpha_2$*, then* $(\alpha_1, \beta_1, s) \neq (\alpha_2, \beta_2, s)$ *for all* $\beta_1, \beta_2 \in F_{q^k}$*.*

Proof: Because of the following property of trace functions, $Tr(x+y) = Tr(x) + Tr(y)$, we have

$$\begin{aligned} & (\alpha_1, \beta_1, s) = (\alpha_2, \beta_2, s) \\ \text{iff} \quad & Tr(\alpha_1 x^s + \beta_1) = Tr(\alpha_2 x^s + \beta_2) = 0 \\ & \quad \text{for all } x \in F_{q^k} \\ \text{iff} \quad & Tr((\alpha_1 - \alpha_2)x^s + (\beta_1 - \beta_2)) = 0 \\ & \quad \text{for all } x \in F_{q^k} \end{aligned}$$

The last equality leads to a contradiction when $\alpha_1 - \alpha_2 \neq 0$. This is because according to Theorem 3.1 we have

$$|\{x \in F_{q^k} : Tr\left((\alpha_1 - \alpha_2)x^s + (\beta_1 - \beta_2)\right) = 0\}|$$

which is $< q^k$.

□

The following lemma can be easily proved.

Lemma 3.2 *For an integer s satisfying (2), $\alpha \in F^*_{q^k}$, and $\beta_1, \beta_2 \in F_{q^k}$, two vectors (α, β_1, s) and (α, β_2, s) are the same if and only if $Tr(\beta_1) = Tr(\beta_2)$.*

Now let s be an integer that satisfies (2). Define Γ to be a q-ary code consisting of vectors (α, β, s) of the form (3) such that for each $\alpha \in F^*_{q^k}$, $(\alpha, \beta_1, s), (\alpha, \beta_2, s) \in \Gamma$ if and only if $Tr(\beta_1) \neq Tr(\beta_2)$. Since

$$|\{Tr(\beta) : \beta \in F_{q^k}\}| = q,$$

for each α, there are q codewords (α, β_i, s) in Γ and hence $|\Gamma| = q(q^k - 1)$. The length of the codewords is $L = q^k$. The distance $D(v_1, v_2)$ between two codewords $v_1 = (\alpha_1, \beta_1, s)$ and $v_2 = (\alpha_2, \beta_2, s)$ is

$$\begin{aligned} & D(v_1, v_2) \\ &= |\{x \in F_{q^k} : Tr((\alpha_1 - \alpha_2)x^s + (\beta_1 - \beta_2)) \neq 0\}| \\ &= q^k - |\{x \in F_{q^k} : Tr((\alpha_1 - \alpha_2)x^s + (\beta_1 - \beta_2)) = 0\}| \end{aligned}$$

$$= \begin{cases} q^k - (q^{k-1} - \sigma(s-1)(q-1)q^{k/2-1}) \\ \qquad \text{if } \alpha^n = \sigma_1, Tr(\beta) = 0 \\ q^k - (q^{k-1} + \sigma(s-1)q^{k/2-1}) \\ \qquad \text{if } \alpha^n = \sigma_1, Tr(\beta) \neq 0 \\ q^k - (q^{k-1} + \sigma(q-1)q^{k/2-1}) \\ \qquad \text{if } \alpha^n \neq \sigma_1, Tr(\beta) = 0 \\ q^k - (q^{k-1} - \sigma q^{k/2-1}) \\ \qquad \text{if } \alpha^n \neq \sigma_1, Tr(\beta) \neq 0 \end{cases}$$

$$= \begin{cases} q^k - q^{k-1} + \sigma(s-1)(q-1)q^{k/2-1} \\ \qquad \text{if } \alpha^n = \sigma_1, Tr(\beta) = 0 \\ q^k - q^{k-1} - \sigma(s-1)q^{k/2-1} \\ \qquad \text{if } \alpha^n = \sigma_1, Tr(\beta) \neq 0 \\ q^k - q^{k-1} - \sigma(q-1)q^{k/2-1} \\ \qquad \text{if } \alpha^n \neq \sigma_1, Tr(\beta) = 0 \\ q^k - q^{k-1} + \sigma q^{k/2-1} \\ \qquad \text{if } \alpha^n \neq \sigma_1, Tr(\beta) \neq 0 \end{cases}$$

where $\alpha = \alpha_1 - \alpha_2, \beta = \beta_1 - \beta_2$, σ, σ_1 are the same as those in theorem 3.1. So the minimum distance D of the code satisfies

$$D \geq q^k - q^{k-1} - (s-1)(q-1)q^{k/2-1} \qquad (4)$$

Let

$$c = \lfloor \frac{-1 + \sqrt{1 + 4q^{3t-1}(q^t + (s-1)(q-1))}}{2q^{t-1}(q^t + (s-1)(q-1))} \rfloor. \qquad (5)$$

Because

$$\frac{-1 + \sqrt{1 + 4q^{3t-1}(q^t + (s-1)(q-1))}}{2q^{t-1}(q^t + (s-1)(q-1))}$$

is the positive zero of the quadratic equation

$$\left(q^{2t-1} + (s-1)(q-1)q^{t-1}\right)x^2 + x - q^{2t} = 0$$

we have

$$\left(q^{2t-1} + (s-1)(q-1)q^{t-1}\right)c^2 + c - q^{2t} \leq 0$$

and so

$$\begin{aligned} & c^2\left(q^{2t} - q^{2t-1} - (s-1)(q-1)q^{t-1}\right) \\ \geq \quad & \left(c^2 - 1\right)q^{2t} + c. \end{aligned}$$

That is

$$D \geq (1 - \frac{1}{c^2})L + \frac{1}{c}.$$

We summarize the above discussion in the following theorem.

Theorem 3.2 *For any prime power $q > 2$ and even k, there exists an $(L, N, D)_q$-ECC in which*

1. *$L = q^k$, $N = q(q^k - 1)$, and*
2. *D satisfies (1) with c given in (5).*

4 Trade-off and Concluding Remarks

For fixed q, the code obtained from the above Theorem has more codewords compared to the RS-code and AG-codes. This means that with the same number of marks, more users can be accomodated and hence the system is more efficient. However, the codewords are longer than RS-codes and AG-codes and it takes longer to detect all the colluders.

References

[1] O. Berkman, M. Parnas, and J. Sgall. Efficient dynamic traitor tracing. In *Proceedings of the 11^{th} annual ACM-SIAM symposium on discrete algorithms (SODA 2000)*, pages 586–595, 2000.

[2] O. Berkman, M. Parnas, and J. Sgall. Efficient dynamic traitor tracing. *SIAM Journal on Computing*, Vol. 30, No.6:1802–1828, 2001.

[3] D. Boneh and M. Franklin. An efficient public key traitor tracing scheme. In *Advances in Cryptology - CRYPTO'99, Lecture Notes in Computer Science*, volume 1666, pages 338–353. Springer-Verlag, Berlin, Heidelberg, New York, 1999.

[4] B. Chor, A. Fiat, and M. Naor. Tracing traitors. In *Advances in Cryptology - CRYPTO'94, Lecture Notes in Computer Science*, volume 839, pages 257–270. Springer-Verlag, Berlin, Heidelberg, New York, 1994.

[5] B. Chor, A. Fiat, M. Naor, and B. Pinkas. Tracing traitors. *IEEE Transactions on Information Theory*, Vol. 46, No. 3:893–910, 2000.

[6] A. J. Menezes (editor). *Applications of finite fields*. Kluwer Academic Publishers, 1993.

[7] A. Fiat and T. Tassa. Dynamic traitor tracing. In *Advances in Cryptology - CRYPTO'99, Lecture Notes in Computer Science*, volume 1666, pages 354–371. Springer-Verlag, Berlin, Heidelberg, New York, 1999.

[8] A. Fiat and T. Tassa. Dynamic traitor tracing. *Journal of Cryptology*, Vol. 14, No. 3:211–223, 2001.

[9] K. Kurosawa and Y. Desmedt. Optimum traitor tracing and asymmetric schemes. In *Advances in Cryptology - EUROCRYPT'98, Lecture Notes in Computer Science*, volume 1462, pages 502–517. Springer-Verlag, Berlin, Heidelberg, New York, 1998.

[10] B. Pfitzmann. Trials of traced traitors. In *Information Hiding, Lecture Notes in Computer Science,*, volume 1174, pages 49–64. Springer-Verlag, Berlin, Heidelberg, New York, 1996.

[11] R. Safavi-Naini and Y. Wang. Sequential traitor tracing. In *Advances in Cryptology - CRYPTO 2000, Lecture Notes in Computer Science*, volume 1880, pages 316–332. Springer-Verlag, Berlin, Heidelberg, New York, 2000.

[12] R. Safavi-Naini and Y. Wang. New results in frameproof codes, traceability schemes and secure codes. *IEEE transactions on information theory*, 2001.

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

[14] D. R. Stinson and R. Wei. Key preassigned traceability schemes for broadcast encryption. In *Proceedings of SAC'98, Lecture Notes in Computer Science*, volume 1556, pages 144–156. Springer-Verlag, Berlin, Heidelberg, New York, 1999.

[15] M. A. Tsfasman and S. G. Vladut. *Algebraic-geometric codes*. Kluwer Academic Publishers, 1991.

[16] Y. Wang. Contributions to traceability schemes. PhD Thesis, School of IT and CS, University of Wollongong, Australia, 2001.

[17] J. Wolfmann. The number of points on certain algebraic curves over finite fields. *Communications in Algebra*, 17(8):2055–2060, 1989.

[18] J. Wolfmann. Algebraic curves and varieties over finite fields and irreducible cyclic codes. In *Finite fields, coding theory, and advances in communications and computing, Lecture Notes in Pure and Applied Mathematics*, volume 141, pages 217–225. M. Dekker Inc. New York, 1993.