Authentication Codes and Algebraic Curves

Chaoping Xing

Abstract. We survey a recent application of algebraic curves over finite fields to the constructions of authentication codes.

1. Introduction

Authentication codes were invented by Gilbert, MacWilliams and Sloane [5]. The general theory of unconditional authentication has been developed by Simmons ([10, 11]) and has been extensively studied in recent years.

In the conventional model for unconditional authentication, there are three participants: a *transmitter*, a *receiver* and an *opponent*. The transmitter wants to communicate some information to the receiver using a public channel which is subject to active attack. That is, the opponent can either impersonate the transmitter and insert a message on the channel, or replace a transmitted message with another. To protect against these threats, the transmitter and the receiver share a secret key, the key is then used in an authentication code (A-code for short).

A *systematic* A-code (or A-code *without secrecy*) is a code where the *source state* (i.e. plain text) is concatenated with an *authenticator* (or a *tag*) to obtain a *message* which is sent through the channel. Such a code is a triple $(\mathcal{S}, \mathcal{E}, \mathcal{T})$ of finite sets together with a (authentication) mapping $f\colon \mathcal{S} \times \mathcal{E} \to \mathcal{T}$. Here $\mathcal{S}$ is the set of source states, $\mathcal{E}$ is the set of keys and $\mathcal{T}$ is the set of authenticators. When the transmitter wants to send the information $s \in \mathcal{S}$ using a key $e \in \mathcal{E}$, which is secretly shared with the receiver, he transmits the message $m = (s, t)$, where $s \in \mathcal{S}$ and $t = f(s, e) \in \mathcal{T}$. When the receiver receives a message $m = (s, t)$, she checks the authenticity by verifying whether $t = f(s, e)$ or not, using the secret key $e \in \mathcal{E}$. If the equality holds, the message m is called *valid*.

Suppose the opponent has the ability to insert messages into the channel and/or to modify existing messages. When the opponent inserts a new message $m' = (s', t')$ into the channel, this is called *impersonation attack*. When the opponent sees a message $m = (s, t)$ and changes it to a message $m' = (s', t')$ where $s \neq s'$, this is called *substitution attack*.

We assume that there is a probability distribution on the source states, which is known to all the participants. Given the probability distribution on the source

Research supported by the NUS grant RP3991621.

states, the receiver and the transmitter will choose a probability distribution for $\mathcal{E}$. We will denote the probability of success for the opponent when trying impersonation attack and substitution attack, by P_I and P_S, respectively, and $P(\cdot)$ and $P(\cdot|\cdot)$ specify probability and conditional probability distribution on the message space $\mathcal{M} := \mathcal{S} \times \mathcal{E}$. Then we have

$$P_I = \max_{(s,t)\in\mathcal{M}} P(m = (s,t) \text{ valid}) \qquad \text{and}$$
$$P_S = \max_{(s,t),(s',t')\in\mathcal{M},s\neq s'} P(m' = (s',t') \text{ valid} \mid m = (s,t) \text{ observed}).$$

If we further assume that the keys and the source states are uniformly distributed, then the deception probabilities can be expressed as

$$P_I = \max_{(s,t)\in\mathcal{M}} \frac{|\{e \in \mathcal{E}\colon\ t = f(s,e)\}|}{|\mathcal{E}|},$$

$$P_S = \max_{(s,t),(s',t')\in\mathcal{M},s\neq s'} \frac{|\{e \in \mathcal{E}\colon\ t = f(s,e), t' = f(s',e)\}|}{|\{e \in \mathcal{E}\colon\ t = f(s,e)\}|}.$$

In the remainder of the paper, we will always assume that the keys and the source states are uniformly distributed.

We observe that each parameter of an A-code $(\mathcal{S},\mathcal{E},\mathcal{T})$ plays a role:

- the size of $\mathcal{S}$ indicates how large the plain text could be;
- the size of $\mathcal{E}$ is the number of keys, which represents the number of users;
- the size of $\mathcal{T}$ is the number of authenticators, which represents the transmission rate;
- P_I is the security measure against the impersonation attack;
- P_S is the security measure against the substitution attack.

It is clear that for fixed sizes of $\mathcal{S},\mathcal{E}$ and $\mathcal{T}$, we want P_i and P_S to be as small as possible. In other words, if P_I, P_S and $|\mathcal{T}|$ are fixed, we are interested in A-codes $(\mathcal{S},\mathcal{E},\mathcal{T})$ with $|\mathcal{S}|$ and $|\mathcal{E}|$ as large as possible. In particular, the study of the asymptotic behaviour of $(\log|\mathcal{S}|)/|\mathcal{E}|$ for fixed $|\mathcal{T}|$, $P_I = 1/|\mathcal{T}|$ and P_S is one of the most important topics for A-codes. For a review of different bounds and constructions for A-codes, we refer to [7, 13, 8].

In this survey paper, we present an explicit construction of A-codes based on algebraic curves over finite fields.

2. Constructions

In this section, we describe a construction of authentication codes based on algebraic curves over finite fields.

Before starting our construction, we need to introduce some concepts and notations that are essential for the construction. For further results on algebraic curves over finite fields, we refer to [12, 16].

We fix some notations for this section.

ℓ: power of a prime;
$\mathbf{F}_\ell$: the finite field of ℓ elements;
$\mathcal{X}$: a projective, absolutely irreducible, complete algebraic curve defined over $\mathbf{F}_\ell$. We simply say that $\mathcal{X}$ is an algebraic curve;
$g = g(\mathcal{X})$: the genus of $\mathcal{X}$;
$\mathbf{F}_\ell(\mathcal{X})$: the function field of $\mathcal{X}$;
$\mathcal{X}(\mathbf{F}_\ell)$: the set of all $\mathbf{F}_\ell$-rational points on $\mathcal{X}$.

A *divisor* G of $\mathcal{X}/\mathbf{F}_q$ is a formal sum

$$G = \sum_{P \in S} \nu_P(G) P,$$

where S is a finite non-empty set of points of $\mathcal{X}$, and $\nu_P(G) \in \mathbf{Z}$ for all $P \in S$. A divisor G of $\mathcal{X}/\mathbf{F}_\ell$ is called $\mathbf{F}_\ell$-*rational* if

$$G^\sigma = G$$

for all automorphisms $\sigma \in \mathrm{Gal}(\overline{\mathbf{F}}_\ell/\mathbf{F}_\ell)$, where $\overline{\mathbf{F}}_\ell$ is a fixed algebraic closure of $\mathbf{F}_\ell$ and $\mathrm{Gal}(\overline{\mathbf{F}}_\ell/\mathbf{F}_\ell)$ is the Galois group of $\overline{\mathbf{F}}_\ell/\mathbf{F}_\ell$. In this paper we always mean a rational divisor whenever a divisor is mentioned.

We write ν_P for the normalized discrete valuation corresponding to the point P of $\mathcal{X}$.

For a divisor G we form the vector space

$$L(G) = \{x \in \mathbf{F}_\ell(\mathcal{X}) \backslash \{0\} \colon \mathrm{div}(x) + G \geq 0\} \cup \{0\}.$$

Then $L(G)$ is a finite-dimensional vector space over $\mathbf{F}_\ell$, and we denote its dimension by $l(G)$. By the Riemann-Roch theorem (see [12, 16]), we have

$$l(G) \geq \deg(G) + 1 - g,$$

and equality holds if $\deg(G) \geq 2g - 1$.

Now we are ready to describe the construction.

Let $\mathcal{P}$ be a subset of $\mathcal{X}(\mathbf{F}_\ell)$, i.e., $\mathcal{P}$ is a set of $\mathbf{F}_\ell$-rational points of $\mathcal{X}$. Let D be a positive divisor with $\mathcal{P} \cap \mathrm{Supp}(D) = \emptyset$. Choose an $\mathbf{F}_\ell$-rational point R in $\mathcal{P}$ and put $G = D - R$. Then $\deg(G) = \deg(D) - 1$, $L(G) \subset L(D)$ and $\mathbf{F}_\ell \cap L(G) = \{0\}$. Moreover, we have

$$L(D) = \mathbf{F}_\ell \oplus L(G) = \{\alpha + f | f \in L(G), \alpha \in \mathbf{F}_\ell\}.$$

Put

$$\mathcal{S} = L(G), \quad \mathcal{E} = \mathcal{P} \times \mathbf{F}_\ell, \quad \mathcal{T} = \mathbf{F}_\ell,$$

and consider the map f

$$\mathcal{S} \times \mathcal{E} \to \mathcal{T}, \quad (s, (P, \alpha)) \mapsto s(P) + \alpha.$$

It can be proved that $(\mathcal{S}, \mathcal{E}, \mathcal{T})$ constructed above together with f forms an A-code with the deception probabilities

$$P_I = \frac{1}{\ell}, \quad P_S = \frac{\deg(D)}{|\mathcal{P}|}$$

provided $\deg(D) \geq 2g+1$. More precisely, we have the following result.

Theorem 2.1. *Let $\mathcal{X}$ be an algebraic curve and $\mathcal{P}$ a set of $\mathbf{F}_\ell$-rational points on $\mathcal{X}$. Suppose that D is a positive divisor with $\deg(D) \geq 2g+1$ and $\mathcal{P} \cap \mathrm{Supp}(D) = \emptyset$. Then there exists an A-code $(\mathcal{S}, \mathcal{E}, \mathcal{T})$ with*

$$|\mathcal{S}| = \ell^{l(D)-1} = \ell^{\deg(D)-g}, \quad |\mathcal{E}| = \ell|\mathcal{P}|, \quad |\mathcal{T}| = \ell$$

$$P_I = \frac{1}{\ell}, \quad P_S = \frac{\deg(D)}{|\mathcal{P}|}.$$

Theorem 2.1 gives a construction of A-codes based on general algebraic curves over finite fields. In the examples below, we apply Theorem 2.1 to some special curves to obtain A-code with nice parameters.

Example 2.2. *Consider the projective line $\mathcal{X}/\mathbf{F}_\ell$. Then $g = g(\mathcal{X}) = 0$.*

(a) Let d be an integer between 1 and ℓ, and P an $\mathbf{F}_\ell$-rational point of $\mathcal{X}$. Put

$$D = dP, \quad \mathcal{P} = \mathcal{X}(\mathbf{F}_\ell) - \{P\}.$$

Then $\deg(D) = d \geq 2g+1$, $|\mathcal{P}| = \ell$ and $\mathcal{P} \cap \mathrm{Supp}(D) = \emptyset$. By Theorem 2.1, we obtain an A-code $(\mathcal{S}, \mathcal{E}, \mathcal{T})$ with

$$|\mathcal{S}| = \ell^d, \quad |\mathcal{E}| = \ell^2, \quad |\mathcal{T}| = \ell$$

$$P_I = \frac{1}{\ell}, \quad P_S = \frac{d}{\ell}.$$

The A-code $(\mathcal{S}, \mathcal{E}, \mathcal{T})$ with the above parameters can also be found in [2]*. It can be proved that the above A-code is optimal in the sense that*

(b) Let d be an integer between 2 and ℓ. Put $\mathcal{P} = \mathcal{X}(\mathbf{F}_\ell)$. As there always exists an irreducible polynomial of degree d over $\mathbf{F}_\ell$, we can find a positive divisor D such that $\deg(D) = d$ and $\mathcal{P} \cap \mathrm{Supp}(D) = \emptyset$. Then $\deg(D) = d \geq 2g+1$, $|\mathcal{P}| = \ell + 1$. By Theorem 4.1, we obtain an A-code $(\mathcal{S}, \mathcal{E}, \mathcal{T})$ with

$$|\mathcal{S}| = \ell^d, \quad |\mathcal{E}| = \ell(\ell+1), \quad |\mathcal{T}| = \ell$$

$$P_I = \frac{1}{\ell}, \quad P_S = \frac{d}{\ell+1}.$$

These A-codes had not been known before the construction in Theorem 2.1 was introduced (see [19]*).*

Example 2.3. *Let ℓ be a square and put $r = \sqrt{\ell}$. Consider a sequence of algebraic curves $\mathcal{X}_m/\mathbf{F}_\ell$ given in* [4] *as follows. Let $\mathcal{X}_1$ be the projective line with the function field $\mathbf{F}_\ell(\mathcal{X}) = \mathbf{F}_\ell(x_1)$. Let $\mathcal{X}_m$ be obtained by adjoining a new equation:*

$$x_m^r + x_m = \frac{x_{m-1}^r}{x_{m-1}^{r-1} + 1},$$

for all $m \geq 2$. Then the number of $\mathbf{F}_\ell$-rational points of $\mathcal{X}_m$ is more than $(r^2 - r)r^{m-1}$, and the genus g_m of $\mathcal{X}_m$ is less than r^m for all $m \geq 1$. Choose an integer

c between 2 *and* $\sqrt{\ell}-1$ *(c is independent of m) and an* $\mathbf{F}_\ell$*-rational point* P_m *of* $\mathcal{X}_m$ *and put* $D_m = c\ell^{m/2}P_m$*. Let* $\mathcal{P}_m$ *be a subset of* $\mathcal{X}_m(\mathbf{F}_\ell) - \{P_m\}$ *with*

$$|\mathcal{P}_m| = (r^2 - r)r^{m-1} = \ell^{m/2}(\sqrt{\ell} - 1).$$

By Theorem 2.1, we obtain a sequence of A-code $(\mathcal{S}_m, \mathcal{E}_m, \mathcal{T}_m)$ *with*

$$|\mathcal{S}_m| = \ell^{(c-1)\ell^{m/2}}, \quad |\mathcal{E}_m| = \ell^{m/2}(\ell\sqrt{\ell_m} - \ell), \quad |\mathcal{T}_m| = \ell,$$

and with deception probabilities

$$P_I = \frac{1}{\ell}, \qquad P_S = \frac{c}{\sqrt{\ell} - 1}.$$

The above example provides the first explicit construction of A-codes with $\lim_{|\mathcal{E}|\to 0}(\log|\mathcal{S}|)/|\mathcal{E}| > 0$ for fixed $|\mathcal{T}|$, $P_I = 1/|\mathcal{T}|$ and P_S.

References

[1] J. Bierbrauer, "Universal hashing and geometric codes", *Designs, Codes and Cryptography,* Vol.11, pp. 207–221, 1997.

[2] J. Bierbrauer, T. Johansson, G. Kabatianskii and B. Smeets, "On families of hash functions via geometric codes and concatenation", *Advances in Cryptology–CRYPTO'93, Lecture Notes in Computer Science*, **773**, pp. 331–342, 1994.

[3] J. L. Carter and M. N. Wegman, "Universal classes of hash functions", *J. Computer and System Sci.*, Vol.18, pp. 143–154, 1979.

[4] A. Garcia and H. Stichtenoth, "On the asymptotic behavior of some towers of function fields over finite fields", *J. of Number Theory*, Vol.61, pp. 248–273, 1996.

[5] E. N. Gilbert, F. J. MacWilliams and N. J. A. Sloane, "Codes which detect deception", *The Bell System Technical Journal*, Vol.33, No.3, pp. 405–424, 1974.

[6] T. Helleseth and T. Johansson, "Universal hash functions from exponential sums over finite fields and Galois Rings", *Advances in Cryptology–Crypto'96*, Lecture Notes in Computer Science, **1109**, pp. 31–44, 1996.

[7] T. Johansson, *Contributions to unconditionally secure authentication*, Ph.D. thesis, Lund, 1994.

[8] G. Kabatianskii, B. Smeets, and T. Johansson, "On the cardinality of systematic authentication codes via error correctings", *IEEE Trans. Inform. Theory*, Vol. 42, pp. 566–578, 1996.

[9] J. -P. Serre, *Rational points on curves over finite fields,* lecture notes, Harvard University, 1985.

[10] G. J. Simmons, "Authentication theory/coding theory", *Advances in Cryptology–Crypto '84*, Lecture Notes in Compute. Sci., **196**, pp. 411–431, 1984.

[11] G. J. Simmons, "A survey of information authentication", in *Contemporary Cryptology, The Science of Information Integrity*, G.J. Simmons, ed., IEEE Press, pp. 379–419, 1992.

[12] H. Stichtenoth, *Algebraic function fields and codes*, Berlin: Springer, 1993.

[13] D. R. Stinson, " Combinatorial characterization of authentication codes", *Designs, Codes and Cryptography*, Vol. 2, pp. 175–187, 1992.

[14] D. R. Stinson, "Universal hashing and authentication codes", *Designs, Codes and Cryptography*, Vol. 4, pp. 377–346, 1994. (also *Advances in Cryptology–CRYPTO '91*, Lecture Notes in Computer Sci. **576**, pp. 74–85, 1992.)

[15] D. R. Stinson, "On the connection between universal hashing, combinatorial designs and error-correcting codes, *Congressus Numerantium*, Vol. 114, pp. 7–27, 1996.

[16] M. A. Tsfasman and S. G. Vladut, *Algebraic-geometric codes*, Dordrecht: Kluwer, 1991.

[17] W. C. Waterhouse, "Abelian varieties over finite fields", *Ann. Sci. Ecole Norm. Sup.*, Vol. 2, pp. 521–560, 1969.

[18] M. N. Wegman and J. L. Carter, "New hash functions and their use in authentication and set equality", *Journal of Computer and System Sciences*, Vol. 22, pp. 265—279, 1981.

[19] C. P. Xing and H. X. Wang, "Constructions of authentication codes from algebraic curves over finite fields," IEEE Trans. Inform. Theory, to appear.

Department of Mathematics,
National University of Singapore,
2 Science Drive 2,
S117543, Singapore
E-mail address: matxcp@nus.edu.sg