Des Codes Crypt (2006) 41: 221–233
DOI 10.1007/s10623-006-9004-y

Explicit constructions of separating hash families from algebraic curves over finite fields

Lihua Liu · Hao Shen

Received: 9 December 2005 / Revised: 1 June 2006 /
Accepted 23 June 2006 / Published online: 19 September 2006

Abstract Let X be a set of order n and Y be a set of order m. An $(n, m, \{w_1, w_2\})$-separating hash family is a set $\mathcal{F}$ of N functions from X to Y such that for any X_1, $X_2 \subseteq X$ with $X_1 \cap X_2 = \emptyset$, $|X_1| = w_1$ and $|X_2| = w_2$, there exists an element $f \in \mathcal{F}$ such that $f(X_1) \cap f(X_2) = \emptyset$. In this paper, we provide explicit constructions of separating hash families using algebraic curves over finite fields. In particular, applying the Garcia–Stichtenoth curves, we obtain an infinite class of explicitly constructed $(n, m, \{w_1, w_2\})$–separating hash families with $N = \mathcal{O}(\log n)$ for fixed m, w_1, and w_2. Similar results for strong separating hash families are also obtained. As consequences of our main results, we present explicit constructions of infinite classes of frameproof codes, secure frameproof codes and identifiable parent property codes with length $N = \mathcal{O}(\log n)$ where n is the size of the codes. In fact, all the above explicit constructions of hash families and codes provide the best asymptotic behavior achieving the bound $N = \mathcal{O}(\log n)$, which substantially improve the results in [8, 15, 17] and give an answer to the fifth open problem presented in [11].

Keywords Algebraic curve · Separating hash family · Strong separating hash family · Frameproof (FP) code · Secure frameproof (SFP) code · Identifiable parent property (IPP) code

AMS Classification 05D05 · 05D40

Communicated by S. Galbraith.

L. Liu (✉)
Department of Information and Computation Science, Shanghai Maritime University, Shanghai, China
e-mail: eva@sjtu.edu.cn

L. Liu · H. Shen
Department of Mathematics, Shanghai Jiao Tong University, Shanghai 200240, China
email: haoshen@sjtu.edu.cn

1 Introduction

Definition 1.1 Let n and m be integers such that $2 \leq m \leq n$, X be a set of order n and Y be a set of order m. Let $\mathcal{F}$ be a family of N functions from X to Y, $\mathcal{F}$ is called an (N, n, m) hash family, denoted $HF(N; n, m)$. An (N, n, m) hash family $\mathcal{F}$ is called an $(N, n, m, \{w_1, w_2\})$–λ–*separating hash family*, denoted λ–$SHF(N; n, m, \{w_1, w_2\})$, if for any $X_1, X_2 \subseteq X, X_1 \cap X_2 = \emptyset, |X_1| = w_1$ and $|X_2| = w_2$, there exist at least λ functions $f \in \mathcal{F}$ such that $f(X_1) \cap f(X_2) = \emptyset$. When $\lambda = 1$, it is omitted from the notation.

Separating hash families have many applications to the constructions of cover–free families, FP codes, SFP codes, and IPP codes ([8,13–15]). The relationships among different types of codes and hash families are described in (11). Recently, Li et al. (6) consider the *optimal* separating hash families with $w_1 = 1$ and $w_2 = 2$ in order to construct cover–free families.

Let $N(n, m, \{w_1, w_2\})$ denote the least value N for which an $SHF(N; n, m, \{w_1, w_2\})$ exists. We are interested in determining the asymptotic behavior of $N(n, m, \{w_1, w_2\})$ as a function of n when m, w_1, and w_2 are fixed. Bounds on $N(n, m, \{w_1, w_2\})$ have been studied by numerous authors (3,11,13). We start with an upper bound for $N(n, m, \{w_1, w_2\})$ due to Stinson et al. (13) using the basic probabilistic method.

To present the theorem on the upper bound, we need the concept of chromatic polynomial. For a given graph $G = (V, E)$ and a positive integer m, let $\pi(G, m)$ denote the number of m-colorings of G. $\pi(G, m)$ as a polynomial of m of degree $|V|$ is called the *chromatic polynomial* of G. If the vertices of G are colored independently at random using m colors, then the probability that the result is an $m-$coloring is $\frac{\pi(G,m)}{m^{|V|}}$. We will use in this paper the complete bipartite graph with parts of size w_1 and w_2, denoted K_{w_1,w_2}. All logarithms in this paper are to the base 2, unless otherwise indicated.

Theorem 1.1 (13) *Suppose that n, m, w_1, and w_2 are positive integers. Then*

$$N(n, m, \{w_1, w_2\}) \leq \left\lceil \left(\frac{w_1 + w_2}{-\log q} \right) \log n \right\rceil,$$

where $q = 1 - \frac{\pi(K_{w_1,w_2},m)}{m^{w_1+w_2}}$ and $\lceil v \rceil$ denotes the least integer greater than or equal to the real number v.

On the other hand, we can derive a lower bound for $N(n, m, \{w_1, w_2\})$ from perfect hash families.

Definition 1.2 An (N, n, m) hash family $\mathcal{F}$ is called an (N, n, m, w)–perfect hash family, denoted $PHF(N; n, m, w)$, if for any $C \subseteq X$ with $|C| = w$, there exists an element $f \in \mathcal{F}$ such that f is injective on C.

The following theorem is helpful for deriving our lower bound:

Theorem 1.2 (12) *There is a $PHF(N; n, m, 2)$ if and only if*

$$n \leq m^N.$$

Theorem 1.3

$$N(n, m, \{w_1, w_2\}) \geq \frac{\log n}{\log m}.$$

Proof Since an $SHF(N;n,m,\{w_1,w_2\})$ is an $SHF(N;n,m,\{1,1\})$ and the latter is equivalent to a $PHF(N;n,m,2)$, we have $n \le m^N$ by Theorem 1.2. □

It follows from Theorems 1.1 and 1.3 that:

Corollary 1.1 *For given positive integers m, w_1, and w_2, $N(n,m,\{w_1,w_2\}) = \Theta(\log n)$.*

However, the proof is nonconstructive. To give explicit constructions that are asymptotically as good as the above result is of great interest and efforts have been made to provide explicit constructions (6,13,15). Especially, employing some combinatorial techniques, Stinson et al. (15) obtain the following result:

Theorem 1.4 (15) *For any positive integers m, w_1, and w_2, there exists an infinite class of $SHF(N;n,m,\{w_1,w_2\})$ for which*

$$N = \mathcal{O}((w_1w_2)^{\log^*(n)}(\log n)), \tag{1.1}$$

where the function $\log^*\colon \mathbb{Z}^+ \longrightarrow \mathbb{Z}^+$ *is defined recursively as follows:*

$$\log^*(1) = 1,$$
$$\log^*(n) = \log^*(\lceil \log n \rceil) + 1, \quad \text{if } n > 1.$$

The main purpose of this paper is to improve the above theorem by presenting an infinite class of explicitly constructed separating hash families achieving the bound $N = \mathcal{O}(\log n)$ from algebraic curves over finite fields. We present a method for explicit constructions of separating hash families from specific algebraic curves with many rational points. In particular, combining our construction based on the Garcia–Stichtenoth curves with a product type construction due to Stinson et al. (15), we provide an infinite class of explicitly constructed separating hash families with $N = \mathcal{O}(\log n)$ for any given integers m, w_1, and w_2.

Similar methods can be applied to obtain efficient constructions of strong separating hash families defined by Sarkar and Stinson (8), which turns out to be equivalent to the class of partially hashing property introduced in (1).

Definition 1.3 An (N,n,m) hash family $\mathcal{F}$ is called an $(N,n,m,\{w_1,w_2\})$–strong separating hash family, denoted $SSHF(N;n,m,\{w_1,w_2\})$, if for any two disjoint subsets $X_1, X_2 \subseteq X$ with $|X_1| = w_1$ and $|X_2| = w_2$, there is a function $f \in \mathcal{F}$ such that f is injective on X_1 and $f(X_1) \cap f(X_2) = \emptyset$.

Definition 1.4 An (N,n,m) hash family $\mathcal{F}$ is called an $(N,n,m,\{w_1,w_2\})$–partially hashing family, denoted $PAHF(N;n,m,\{w_1,w_2\})$, if for any two subsets $X_1, X_2 \subseteq X$ with $X_1 \subseteq X_2$, $|X_1| = w_1$ and $|X_2| = w_2$, there is a function $f \in \mathcal{F}$ such that for any $x_1 \in X_1$ and any $x_2 \in X_2$, if $x_1 \neq x_2$, we have $f(x_1) \neq f(x_2)$.

The equivalence of strong separating hash family and partially hashing family is presented in the following theorem.

Theorem 1.5 (8) *A hash family $\mathcal{F}$ is an $SSHF(N;n,m,\{w_1,w_2\})$ if and only if $\mathcal{F}$ is a $PAHF(N;n,m,\{w_1,w_1+w_2\})$.*

Based on the above result, we only consider the constructions of strong separating hash families.

Applying algebraic curves over finite fields, we obtain an infinite class of explicitly constructed strong separating hash families with $N = \mathcal{O}(\log n)$ for any given integers

m, w_1, and w_2. Applying our main constructions, for any given integers m and w, we obtain infinite classes of explicitly constructed FP codes, SFP codes, and IPP codes with length $N = \mathcal{O}(\log\, n)$ where n is the size of the codes.

In fact, comparing the known results, Sarkar and Stinson (8) obtain an infinite class of strong separating hash families for which

$$N = \mathcal{O}((w_1(w_1 + w_2))^{\log^*(n)}(\log\, n)) \tag{1.2}$$

for any positive integers m, w_1, and w_2, an infinite class of FP codes for which

$$N = \mathcal{O}(w^{\log^*(n)}(\log\, n)) \tag{1.3}$$

and an infinite class of IPP codes for which

$$N = \mathcal{O}((w^3)^{\log^*(n)}(\log\, n)) \tag{1.4}$$

for any positive integers m and w. In a recent paper (17), Trung and Martirosyan improve the result in (1.4) by presenting an infinite class of IPP codes for which

$$N = \mathcal{O}((w^2)^{\log^*(n)}(\log\, n)) \tag{1.5}$$

for any positive integers m and w.

It is worth noting that applying algebraic curves over finite fields, all our explicit constructions of separating hash families, strong separating hash families, FP codes, SFP codes, and IPP codes provide the best asymptotic behavior achieving the bound $N = \mathcal{O}(\log n)$, which substantially improve the results in (1.1)–(1.3), and (1.5). As consequences of our constructions, we present infinite classes of explicitly constructed 2–*FP* codes and 2–*SFP* codes achieving the bound $N = \mathcal{O}(\log\, n)$ for arbitrary m. This gives an answer to the fifth open problem presented in (11).

2 Preliminaries

In this section, we introduce some concepts and notations on algebraic curves over finite fields essential for the constructions. For further results on the aspect, we refer to (7,10,18).

Throughout, we let q be a prime power;
F_q–the finite field of q elements;
$\overline{F}_q$–a fixed algebraic closure of F_q;
Gal($\overline{F}_q/F_q$)–the Galois group of $\overline{F}_q/F_q$;
$\mathcal{X}$–a projective, absolutely irreducible, complete algebraic curve defined over F_q.

We simply call that $\mathcal{X}/F_q$ is an algebraic curve;

$g = g(\mathcal{X})$–the genus of $\mathcal{X}$;
$F_q(\mathcal{X})$–the function field of $\mathcal{X}$;
$\mathbb{P}_{F_q}$–the set of all the closed points on $\mathcal{X}$ over F_q;
$\mathcal{X}(F_q)$–the set of all F_q–rational points on $\mathcal{X}$ with all coordinates belonging to F_q.

A divisor G of $\mathcal{X}$ is called *rational* if

$$G^\sigma = G$$

for any automorphism $\sigma \in \mathrm{Gal}(\overline{F}_q/F_q)$. In this paper, we always mean a rational divisor whenever a divisor is mentioned.

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

Definition 2.1 For $x \in F_q(\mathcal{X})\backslash\{0\}$, let $Z(x)$ and $N(x)$ denote the set of zeros and the set of poles of x, respectively. The zero divisor of x is defined by

$$(x)_0 = \sum_{P \in Z(x)} v_P(x)P$$

and the pole divisor of x by

$$(x)_\infty = \sum_{P \in N(x)} (-v_P(x))P.$$

Then $(x)_0$ and $(x)_\infty$ are both rational divisors.

Definition 2.2 The principal divisor of x is given by

$$\mathrm{div}(x) = (x)_0 - (x)_\infty.$$

The degree of $\mathrm{div}(x)$ is equal to zero, i.e.,

$$\deg((x)_0) = \sum_{P \in Z(x)} v_P(x) = \sum_{P \in N(x)} (-v_P(x)) = \deg((x)_\infty).$$

For an arbitrary divisor $G = \sum m_P P$ of $\mathcal{X}$, we denote by $v_P(G)$ the coefficient m_P of P. Then

$$G = \sum v_P(G)P.$$

Definition 2.3 The support $Supp(G)$ of G is the set

$$Supp(G) = \{P \in \mathbb{P}_{F_q} : v_P(G) \neq 0\}.$$

Definition 2.4 (7) For a divisor G, we form the Riemann–Roch space

$$\mathcal{L}(G) = \{x \in F_q(\mathcal{X})\backslash\{0\} : \mathrm{div}(x) + G \geq 0\} \cup \{0\}.$$

Then $\mathcal{L}(G)$ is a finite–dimensional vector space over F_q. We denote the dimension of $\mathcal{L}(G)$ by $l(G)$.

Theorem 2.1 (*Riemann–Roch Theorem*) (7) *Let $\mathcal{X}$ be an algebraic curve with the genus g. Then for any divisor G of $\mathcal{X}$, we have*

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

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

Lemma 2.1 (10) *Let T be a subset of $\mathcal{X}(F_q)$, i.e., a set of F_q–rational points on $\mathcal{X}$. Then for any $t \geq 0$, there exists a divisor G such that $deg(G) = t$ and*

$$T \cap Supp(G) = \emptyset.$$

As we will show in Sect. 3, using algebraic curves over finite fields, for any fixed integers m, w_1, and w_2, we obtain explicit constructions of separating hash families $SHF(N; n, m, \{w_1, w_2\})$ and strong separating hash families $SSHF(N; n, m, \{w_1, w_2\})$ with $N = \mathcal{O}(\log n)$. As applications, in Sect. 4, for any fixed integers m and w, we obtain explicit constructions of (N, n, m) *w–FP* codes, *w–SFP* codes, and *w–IPP* codes with $N = \mathcal{O}(\log n)$.

3 Constructions of SHFs and SSHFs

In this section, we mainly describe the constructions of separating hash families based on algebraic curves over finite fields. Using a similar method, we also present the constructions of strong separating hash families.

Now we describe the constructions of separating hash families.

Let $T \subseteq \mathcal{X}(F_q)$ be a set of F_q–rational points on $\mathcal{X}$. Let G be a divisor with $T \cap \mathrm{Supp}(G) = \emptyset$. Each point $P \in T$ can be associated with a map h_P from $\mathcal{L}(G)$ to F_q defined by

$$h_P(f) = f(P).$$

The Riemann–Roch theorem leads to the following vital result.

Lemma 3.1 (7,19) *Let $\mathcal{F} = \{ h_P \mid P \in T \}$. If $deg(G) \geq 2g + 1$, then $|\mathcal{F}| = |\mathcal{T}|$.*

Theorem 3.1 *Let $\mathcal{X}/F_q$ be an algebraic curve and T a set of F_q–rational points of $\mathcal{X}$. Suppose that G is a divisor with $deg(G) \geq 2g+1$ and $T \cap Supp(G) = \emptyset$. Then there exists a separating hash family $SHF(|T|; q^{deg(G)-g+1}, q, \{w_1, w_2\})$ if $|T| > deg(G) \times w_1 w_2$.*

Proof Let $\mathcal{F}$ be as defined in Lemma 3.1. For any two subsets X_1 and X_2 of $\mathcal{L}(G)$ with $X_1 \cap X_2 = \emptyset$, $|X_1| = w_1$, and $|X_2| = w_2$, consider the set

$$\Phi_{X_1,X_2} := \{u - v \mid u \in X_1, v \in X_2\}.$$

Then Φ_{X_1,X_2} has at most $w_1 w_2$ elements and the number of zeros of an element $u - v$ is at most $\deg(G)$ since $u - v$ is an element of $\mathcal{L}(G)$. Therefore, the number of zeros of all functions in Φ_{X_1,X_2} is at most

$$\deg(G) \times |\Phi_{X_1,X_2}| \leq \deg(G) \times w_1 w_2.$$

By the condition $|T| > \deg(G) \times w_1 w_2$, we can find a point $R \in T$ such that R is not a zero for any function of Φ_{X_1,X_2}.

We claim that the function h_R satisfies the condition $h_R(X_1) \cap h_R(X_2) = \emptyset$. In fact, for any $u \in X_1$ and any $v \in X_2$, we have $u - v \in \Phi_{X_1,X_2}$. Thus R is not a zero of $u - v$, i.e., $u(R) \neq v(R)$ for any $u \in X_1$ and any $v \in X_2$. This is equivalent to $h_R(u) \neq h_R(v)$ for any $u \in X_1$ and any $v \in X_2$. The proof is completed. □

Remark 3.1 In fact, Theorem 3.1 presents a construction of λ–$SHF(|T|; q^{\deg(G)-g+1}, q, \{w_1, w_2\})$ based on algebraic curves over finite fields with $\lambda = |T| - \deg(G) \times w_1 w_2$, which is implied in the proof of Theorem 3.1.

In the following examples, we apply Theorem 3.1 to some special curves to get some separating hash families with nice parameters.

Example 3.1 Consider the projective line $\mathcal{X}/F_q$. Then the genus of $\mathcal{X}$ is $g(\mathcal{X}) = 0$.

Let N, t, w_1, and w_2 be positive integers with $tw_1 w_2 < N \leq q + 1$. Then there exist a subset T of rational points of $\mathcal{X}$ with $|T| = N$ and a divisor G of degree t with $T \cap \mathrm{Supp}(G) = \emptyset$. Applying Theorem 3.1, we obtain an $SHF\left(N; q^{t+1}, q, \{w_1, w_2\}\right)$. In particular, taking $N = q + 1$, we obtain an $SHF(q + 1; q^{t+1}, q, \{w_1, w_2\})$.

Example 3.2 Let $q = p^n$ for a prime p. Put

$$N_q(1) = \begin{cases} q + \lfloor 2\sqrt{q} \rfloor, & \text{if } p \mid \lfloor 2\sqrt{q} \rfloor \text{ and } n \geq 3 \\ q + \lfloor 2\sqrt{q} \rfloor + 1, & \text{otherwise.} \end{cases}$$

where $\lfloor \cdot \rfloor$ denotes the integral part of a real number. It is proved in (9) that there exists an elliptic curve $\mathcal{X}/F_q$ with $N_q(1)$ rational points and the genus of $\mathcal{X}$ is $g(\mathcal{X}) = 1$.

Let N, t, w_1, and w_2 be positive integers with $t \geq 3$ and $tw_1w_2 < N \leq N_q(1)$. Then there exist a subset T of rational points of $\mathcal{X}$ with $|T| = N$ and a divisor G of degree t such that $T \cap \mathrm{Supp}(G) = \emptyset$. Applying Theorem 3.1, we obtain an $SHF(N; q^t, q, \{w_1, w_2\})$. In particular, there exists an $SHF(N_q(1); q^t, q, \{w_1, w_2\})$.

Example 3.3 Let q be a prime power. Consider the Hermitian curve $\mathcal{X}/F_{q^2}$ (7,10) defined by

$$y^q + y = x^{q+1}.$$

Then the number of F_{q^2}–rational points of $\mathcal{X}$ is equal to $q^3 + 1$ and the genus of $\mathcal{X}$ is $g(\mathcal{X}) = q(q-1)/2$.

Let N, t, w_1, and w_2 be positive integers with $t \geq q(q-1) + 1$ and $tw_1w_2 < N \leq q^3 + 1$. Then there exist a subset T of rational points of $\mathcal{X}$ with $|T| = N$ and a divisor G of degree t such that $T \cap \mathrm{Supp}(G) = \emptyset$. Applying Theorem 3.1, we obtain an $SHF(N; q^{2t+2-q(q-1)}, q^2, \{w_1, w_2\})$. In particular, there exists an $SHF(q^3+1; q^{2t+2-q(q-1)}, q^2, \{w_1, w_2\})$.

The following infinite class of separating hash families is obtained from the Garcia–Stichtenoth curves.

Theorem 3.2 *Let q be a prime power and let $c_1, c_2 \geq 2$ be real numbers. Then there exists an*

$$SHF\left((q-1)q^i; \left\lceil q^{(c_1c_2-2)q^i} \right\rceil, q^2, \left\{ \left\lfloor \frac{\sqrt{2}}{c_1}(q^{\frac{1}{2}} - 1) \right\rfloor, \left\lfloor \frac{\sqrt{2}}{c_2}(q^{\frac{1}{2}} - 1) \right\rfloor \right\}\right)$$

for each $i \geq 1$. In particular, taking $c_1 = c_2 = 2$, we obtain an

$$SHF\left((q-1)q^i; q^{2q^i}, q^2, \left\{ \left\lfloor \frac{\sqrt{2}}{2}(q^{\frac{1}{2}} - 1) \right\rfloor, \left\lfloor \frac{\sqrt{2}}{2}(q^{\frac{1}{2}} - 1) \right\rfloor \right\}\right)$$

for each $i \geq 1$.

Proof Consider a sequence of algebraic curves $\mathcal{X}_i$ over F_{q^2} introduced by Garcia and Stichtenoth (4) as follows. Let $\mathcal{X}_1$ be the projective line with the function field $F_{q^2}(\mathcal{X}_1) = F_{q^2}(x_1)$. Let $\mathcal{X}_i$ be obtained by adjoining a new equation,

$$x_i^q + x_i = \frac{x_{i-1}^q}{x_{i-1}^{q-1} + 1}$$

for all $i \geq 2$. Then the number of F_{q^2}–rational points of $\mathcal{X}_i$ is more than $(q-1)q^i$, and the genus g_i of $\mathcal{X}_i$ is less than q^i for all $i \geq 1$. For each $i \geq 1$ put

$$N_i = (q-1)q^i, \qquad t_i = \left\lfloor \frac{c_1c_2}{2} q^i \right\rfloor,$$

$$w_1 = \left\lfloor \frac{\sqrt{2}}{c_1}(q^{\frac{1}{2}} - 1) \right\rfloor, \qquad w_2 = \left\lfloor \frac{\sqrt{2}}{c_2}(q^{\frac{1}{2}} - 1) \right\rfloor.$$

Then $t_i \geq 2g_i + 1$ since $c_1,\ c_2 \geq 2$ and we can check that

$$N_i > t_i w_1 w_2 \qquad \text{for all } i \geq 1.$$

We may choose a subset T_i of rational points of $\mathcal{X}_i$ with $|T_i| = N_i$ and a divisor G_i of degree t_i of $\mathcal{X}_i$ such that $T_i \cap \mathrm{Supp}(G_i) = \emptyset$. Applying Theorem 3.1, we obtain an

$$SHF\left((q-1)q^i; q^{2(t_i+1-g_i)}, q^2, \left\{\left\lfloor \frac{\sqrt{2}}{c_1}(q^{\frac{1}{2}} - 1) \right\rfloor, \left\lfloor \frac{\sqrt{2}}{c_2}(q^{\frac{1}{2}} - 1) \right\rfloor\right\}\right)$$

for each $i \geq 1$. The observation that

$$t_i + 1 - g_i > \frac{c_1 c_2}{2} q^i - q^i = \frac{(c_1 c_2 - 2)}{2} q^i$$

completes the proof. □

Before describing the next result, we first recall a product construction for separating hash families, due to Stinson et al. (15).

Lemma 3.2 (15) *Suppose there exist an $SHF(N; n, n_0, \{w_1, w_2\})$ and an $SHF(M; n_0, m, \{w_1, w_2\})$. Then there exists an $SHF(NM; n, m, \{w_1, w_2\})$.*

Combining Theorem 3.2 with Lemma 3.2, we are ready to prove our main theorem in this paper.

Theorem 3.3 *For any positive integers m, w_1, and w_2, there exists an infinite class of explicitly constructed separating hash families $SHF(N; n, m, \{w_1, w_2\})$ for which N is $\mathcal{O}(\log n)$.*

Proof For given positive integers m, w_1, and w_2, let q be the least prime power with $q^2 \geq m$, $q^{\frac{1}{2}} \geq \sqrt{2}w_1 + 1$, and $q^{\frac{1}{2}} \geq \sqrt{2}w_2 + 1$. We may choose $c_1, c_2 \in [2, \infty)$ such that $\frac{\sqrt{2}}{c_1}(q^{\frac{1}{2}} - 1) = w_1$ and $\frac{\sqrt{2}}{c_2}(q^{\frac{1}{2}} - 1) = w_2$. Then Theorem 3.2 implies the existence of an explicitly constructed

$$SHF\left((q-1)q^i; \left\lceil q^{(c_1c_2-2)q^i} \right\rceil, q^2, \{w_1, w_2\}\right) \quad \text{for each } i \geq 1.$$

For $q^2 \geq m$, we can explicitly construct an $SHF(M; q^2, m, \{w_1, w_2\})$ with M depending only on m, w_1 and w_2 as follows. Let X be a set of order q^2, Y be a set of order m and $y_1 \neq y_2 \in Y$. For any pair (X_1, X_2) of subsets of X with $X_1 \cap X_2 = \emptyset$, $|X_1| = w_1$ and $|X_2| = w_2$, we associate (X_1, X_2) with a function $f_{X_1X_2}$: $X \longrightarrow Y$ satisfying

$$f_{X_1X_2}\,|_{X_1} \equiv y_1, \quad f_{X_1X_2}\,|_{X_2} \equiv y_2.$$

Clearly, all such functions $\{f_{X_1X_2}\}$ form an $SHF(M; q^2, m, \{w_1, w_2\})$ with

$$M = \binom{q^2}{w_1}\binom{q^2 - w_1}{w_2}.$$

Hence, the parameter M can be effectively determined by m, w_1, and w_2. It follows from Lemma 3.2 that we get an explicit construction of an

$$SHF\left(M(q-1)q^i; \left\lceil q^{(c_1c_2-2)q^i} \right\rceil, m, \{w_1, w_2\}\right) \quad \text{for each } i \geq 1.$$

We thus obtain an infinite class of explicitly constructed $SHF(N; n, m, \{w_1, w_2\})$ with $N \leq C \log n$, where

$$C = \frac{M(q-1)}{(c_1c_2 - 2)\log q}$$

and all the parameters M, q, c_1, and c_2 depend only on m, w_1, and w_2. But n tends to ∞ as $i \to \infty$ since $n = \left\lceil q^{(c_1c_2-2)q^i} \right\rceil$. The desired result follows. □

Based on algebraic curves over finite fields, the similar method can be applied to obtain efficient constructions of strong separating hash families.

Theorem 3.4 *Let $\mathcal{X}/F_q$ be an algebraic curve and T a set of F_q–rational points of $\mathcal{X}$. Suppose that G is a divisor with $deg(G) \geq 2g+1$ and $T \cap Supp(G) = \emptyset$. Then there exists a strong separating hash family SSHF $(|T|; q^{deg(G)-g+1}, q, \{w_1, w_2\})$ if $|T| > deg(G) \times \left[\binom{w_1}{2} + w_1w_2\right]$.*

Proof Let $\mathcal{F}$ be as defined in Lemma 3.1. For any two subsets X_1 and X_2 of $\mathcal{L}(G)$ with $X_1 \cap X_2 = \emptyset$, $|X_1| = w_1$ and $|X_2| = w_2$, we only need to consider the set

$$\Phi_{X_1,X_2} := \left\{ (u-v)^2 |\, u \neq v \in X_1, \text{ or } u \in X_1 \text{ and } v \in X_2 \right\}.$$

□

By Theorem 3.4, the special curves in Examples 3.1–3.3 all can be applied to obtain some strong separating hash families replacing w_1w_2 by $\left[\binom{w_1}{2} + w_1w_2\right]$.

Applying the Garcia–Stichtenoth curves and selecting the parameters w_1 and w_2 appropriately lead to the following infinite class of strong separating hash families.

Theorem 3.5 *Let q be a prime power and let $c_1, c_2 \geq 2$ be real numbers. Then there exists an*

$$SSHF\left((q-1)q^i; \left\lceil q^{\frac{2(c_1^2c_2 - c_1 - c_2)}{(c_1+c_2)}q^i} \right\rceil, q^2, \left\{ \left\lfloor \frac{\sqrt{2q}}{2c_1} \right\rfloor, \left\lfloor \frac{\sqrt{2q}}{2c_2} \right\rfloor \right\}\right)$$

for each $i \geq 1$. In particular, taking $c_1 = c_2 = 2$, we obtain an

$$SSHF\left((q-1)q^i; q^{2q^i}, q^2, \left\{ \left\lfloor \frac{\sqrt{2q}}{4} \right\rfloor, \left\lfloor \frac{\sqrt{2q}}{4} \right\rfloor \right\}\right)$$

for each $i \geq 1$.

In order to apply our main method to give explicit constructions of an infinite class of strong separating hash families achieving the bound $N = \mathcal{O}(\log n)$, we also need a product construction of strong separating hash families.

Theorem 3.6 *Suppose there exist an $SSHF(N; n, n_0, \{w_1, w_2\})$ and an $SSHF(M; n_0, m, \{w_1, w_2\})$. Then there exists an SSHF $(NM; n, m, \{w_1, w_2\})$.*

Proof Let U, V, and W be sets with $|U| = n$, $|V| = n_0$, and $|W| = m$. We may regard S' as an $SSHF(N; n, n_0, \{w_1, w_2\})$ of functions of the form $\psi\colon U \to V$ and S'' as an $SSHF(M; n_0, m, \{w_1, w_2\})$ of functions of the form $\varphi\colon V \to W$. Let S be the family of functions from U to W produced by composing elements of S' with elements of S''. So

an element of S is a function ϕ: $U \to W$ that may be expressed in the form $\phi = \varphi\psi$ for some $\psi \in S^{'}$ and $\varphi \in S^{''}$.

It is clear that $|S| = |S^{'}||S^{''}|$. Furthermore, we have that S is an $SSHF(NM; n, m, \{w_1, w_2\})$. In fact, let X_1 and X_2 be any two subsets of U with $X_1 \cap X_2 = \emptyset$, $|X_1| = w_1$, and $|X_2| = w_2$. Since $S^{'}$ is an $SSHF(N; n, n_0, \{w_1, w_2\})$, there exists an element $\psi \in S^{'}$ such that ψ is injective on X_1 and $\psi(X_1) \cap \psi(X_2) = \emptyset$. Then $|\psi(X_1)| = w_1$ and $|\psi(X_2)| \leq w_2$. We can arbitrarily choose a subset X_3 of V with $|X_3| = w_2 - |\psi(X_2)|$, $\psi(X_1) \cap X_3 = \emptyset$, and $\psi(X_2) \cap X_3 = \emptyset$. We have $|\psi(X_2) \cup X_3| = w_2$ and $\psi(X_1) \cap (\psi(X_2) \cup X_3) = \emptyset$. Since $S^{''}$ is an $SSHF(M; n_0, m, \{w_1, w_2\})$, there exists an element $\varphi \in S^{''}$ such that φ is injective on $\psi(X_1)$ and $\varphi(\psi(X_1)) \cap \varphi(\psi(X_2)) = \emptyset$. Hence $\varphi\psi \in S$ satisfies the conditions that $\varphi\psi$ is injective on X_1 and $\varphi\psi(X_1) \cap \varphi\psi(X_2) = \emptyset$. Hence, S is an $SSHF(MN; n, m, \{w_1, w_2\})$. □

After the above preparations, combining Theorem 3.5 with Theorem 3.6 gives another main construction:

Theorem 3.7 *For any positive integers m, w_1 and w_2, there exists an infinite class of explicitly constructed strong separating hash families $SSHF(N; n, m, \{w_1, w_2\})$ for which N is $\mathcal{O}(\log n)$.*

4 Applications

In this section, we apply our main results to get explicit constructions of cover–free families, FP codes, SFP codes, and IPP codes with the best asymptotic behavior.

First, we give our application to cover–free families.

Definition 4.1 (14) Let w, r, and d be positive integers. A set system $(X, \mathcal{B})$, with $X = \{x_1, \ldots, x_N\}$ and $\mathcal{B} = \{B_i \subseteq X | i = 1, \ldots, T\}$, is called a $(w, r; d)$–cover–free family, denoted $(w, r; d)$–$CFF(N, T)$, provided that, for any w blocks $B_1, \ldots, B_w \in \mathcal{B}$, and any other r blocks $A_1, \ldots, A_r \in \mathcal{B}$, we have that

$$\left| \left(\bigcap_{i=1}^{w} B_i \right) \setminus \left(\bigcup_{j=1}^{r} A_j \right) \right| \geq d.$$

Less formally, the intersection of any w blocks contains at least d points that are not in the union of r other blocks.

Theorem 4.1 (14) *If there exists a $(w, r; d_1)$–$CFF(v, m)$ and a d_2–$SHF(N; n, m, \{w, r\})$, then there exists a $(w, r; d_1 d_2)$–$CFF(vN, n)$.*

Applying Theorems 3.3 and 4.1, we can **directly** derive the following result from separating hash families.

Theorem 4.2 (14) *For any positive integers w, r, and d, there exists an explicit construction for an infinite family of $(w, r; d)$–$CFF(d\binom{w+r}{w}N, T)$, where N is $\mathcal{O}(\log\ T)$.*

Proof For any w, r, and d, we can construct a $w + r$ by $d\binom{w+r}{w}$ matrix by taking d copies of every possible 0–1 column vector having Hamming weight equal to w. Then we obtain a $(w, r; d)$–CFF$(d\binom{w+r}{w}, w + r)$. By Theorem 3.3, for the above integers w and r, there exists an infinite class of explicitly constructed separating hash families $SHF(N; T, w + r, \{w, r\})$ for which N is $\mathcal{O}(\log\ T)$. Applying Theorem 4.1, the proof is completed. □

Remark 4.1 In (14), using Theorems 1.4 and 4.1, Stinson and Wei obtain the result for $(w,r;d)$–$CFF(d\binom{w+r}{w}N,T)$ with $N=\mathcal{O}((w_1w_2)^{\log^*(T)}(\log\ T))$. Then applying the best asymptotic behavior on perfect hash families (19), since any $PHF(N;\ n,\ m,\ w_1+w_2)$ is automatically an $SHF(N;n,m,\{w_1,w_2\})$, they **indirectly** obtain Theorem 4.2 from perfect hash families.

In the following, we will apply our main results to obtain explicit constructions of FP codes, SFP codes, and IPP codes with nice parameters. Before applications, we review the definitions of the codes first.

Consider a code $\mathcal{C}$ of length N on an alphabet Q with $|Q|=m$. Then $\mathcal{C}\subseteq Q^N$ and we will call it an (N,n,m)–code if $|\mathcal{C}|=n$. The elements of $\mathcal{C}$ are called codewords; each codeword has the form $x=(x_1,\ldots,x_N)$, where $x_i\in Q, 1\le i\le N$.

For any subset of codewords $\mathcal{C}_0\subseteq\mathcal{C}$, we define the set of descendants of $\mathcal{C}_0$, denoted $\mathsf{desc}(\mathcal{C}_0)$ by

$$\mathsf{desc}(\mathcal{C}_0)=\{x\in Q^N : x_i\in\{a_i : a\in\mathcal{C}_0\}, 1\le i\le N\}.$$

The set $\mathsf{desc}(\mathcal{C}_0)$ consists of the N–tuples that could be produced by a coalition holding the codewords in the set $\mathcal{C}_0$.

Now, let w be a positive integer. For a code $\mathcal{C}$, define the w–descendant code of $\mathcal{C}$, denoted $\mathsf{desc}_w(\mathcal{C})$, as follows:

$$\mathsf{desc}_w(\mathcal{C})=\bigcup_{\mathcal{C}_0\subseteq\mathcal{C},|\mathcal{C}_0|\le w}\mathsf{desc}(\mathcal{C}_0).$$

The set $\mathsf{desc}_w(\mathcal{C})$ consists of the N–tuples that could be produced by some coalition of size at most w.

Definition 4.2 Let $\mathcal{C}$ be an (N,n,m)–code and $w\ge 2$ be an integer.

1. **Frameproof Code:** (2) $\mathcal{C}$ is a *w–FP* code provided that for any subset $\mathcal{C}_0$ of $\mathcal{C}$ with cardinality at most w, $x\in\mathsf{desc}(\mathcal{C}_0)\cap\mathcal{C}$ implies $x\in\mathcal{C}_0$.
2. **Secure Frameproof Code:** (13) $\mathcal{C}$ is a *w–SFP* code provided that for any two subsets $\mathcal{C}_0$, $\mathcal{C}_1$ of $\mathcal{C}$ with cardinality at most w, $\mathsf{desc}(\mathcal{C}_0)\cap\mathsf{desc}(\mathcal{C}_1)\ne\emptyset$ implies $\mathcal{C}_0\cap\mathcal{C}_1\ne\emptyset$.
3. **Identifiable Parent Property Code:** (5) Let $\{\mathcal{C}_1,\mathcal{C}_2,\ldots,\mathcal{C}_\alpha\}$ be a family of subsets of $\mathcal{C}$ where each $\mathcal{C}_i$ is of cardinality at most w. We say that $\mathcal{C}$ is a *w–IPP* code provided that

$$\bigcap_{1\le i\le\alpha}\mathsf{desc}(\mathcal{C}_i)\ne\emptyset \text{ implies } \bigcap_{1\le i\le\alpha}\mathcal{C}_i\ne\emptyset.$$

We can depict an (N,n,m)–code $\mathcal{C}$ as an $n\times N$ matrix on m symbols, where each row of the matrix corresponds to one of the codewords. Similarly, we can represent an $HF(N;n,m)$ $\mathcal{F}$ as an $N\times n$ matrix on m symbols, where each row of the matrix corresponds to one of the functions in $\mathcal{F}$.

Given an (N,n,m)–code $\mathcal{C}$, we define $\mathcal{F}(\mathcal{C})$ to be the $HF(N;n,m)$ whose matrix representation is $\mathcal{C}^T$. Thus if $\mathcal{C}=\{x^1,x^2,\ldots,x^n\}$ and $1\le j\le N$, then the hash function $f_j\in\mathcal{F}(\mathcal{C})$ is defined by the rule $f_j(i)=x^i_j, 1\le i\le n$.

Based on the above analysis, we can apply our main constructions to the codes. The following equivalence theorems are of great importance for our applications.

Theorem 4.3 (13) *An (N,n,m)–code $\mathcal{C}$ is a w–FP code if and only if $\mathcal{F}(\mathcal{C})$ is an $SHF(N;n,m,\{w,1\})$.*

Theorem 4.4 (13) *An (N,n,m)–code $\mathcal{C}$ is a w–SFP code if and only if $\mathcal{F}(\mathcal{C})$ is an $SHF(N;n,m,\{w,w\})$ where $n \geq 2w$.*

By Theorem 4.4, as a consequence of Theorem 3.2, we present explicit constructions of an infinite class of *w–SFP* codes with special parameters.

Corollary 4.1 *Let q be a prime power. We obtain a*

$$\left((q-1)q^i, q^{2q^i}, q^2\right) \left\lfloor \frac{\sqrt{2}}{2}(q^{\frac{1}{2}}-1) \right\rfloor \text{–SFP code}$$

for each $i \geq 1$.

Combining Theorem 3.3 with Theorem 4.3, we obtain the following result.

Theorem 4.5 *For any positive integers m and w, there exists an infinite class of explicitly constructed (N,n,m) w–FP codes for which N is $\mathcal{O}(\log n)$.*

Applying Theorems 3.3 and 4.4 give an infinite class of *SFP* codes having the best asymptotic behavior, which is apparently novelty on the asymptotic behavior for *SFP* codes.

Theorem 4.6 *For any positive integers m and w, there exists an infinite class of explicitly constructed (N,n,m) w–SFP codes for which N is $\mathcal{O}(\log n)$.*

Staddon et al. (11) have ever arisen the problem: Can we find nice explicit constructions of 2–*FP* and 2–*SFP* codes for arbitrary m? In (16), Tonien and Safavi–Naini present several explicit constructions of m–ary 2–*SFP* codes. With appropriate choice of the parameters, they obtain 2–*SFP* codes with length $N = \mathcal{O}((\log n)^3)$.

In our paper, if we take $w = 2$ in Theorems 4.5 and 4.6, respectively, we can find nice explicit constructions of infinite classes of 2–*FP* and 2–*SFP* codes for arbitrary m with $N = \mathcal{O}(\log n)$.

Corollary 4.2 *For any positive integer m, there exists an infinite class of explicitly constructed (N,n,m) 2–FP codes for which N is $\mathcal{O}(\log n)$.*

Corollary 4.3 *For any positive integer m, there exists an infinite class of explicitly constructed (N,n,m) 2–SFP codes for which N is $\mathcal{O}(\log n)$.*

Applying our explicit constructions of strong separating hash families, we also obtain an infinite class of explicitly constructed *IPP* codes achieving the bound $N = \mathcal{O}(\log n)$. We review the relationship between strong separating hash families and *IPP* codes first.

Theorem 4.7 (1,8) *Let $\mathcal{C}$ be an (N,n,m)–code. If $\mathcal{F}(\mathcal{C})$ is an $SSHF(N;n,m,\{w, \left\lfloor \left(\frac{w+2}{2}\right)^2 \right\rfloor - w\})$, then $\mathcal{C}$ is an (N,n,m) w–IPP code.*

Applying Theorems 3.7 and 4.7 yields the following asymptotic result for *IPP* codes:

Theorem 4.8 *For any positive integers m and w, there exists an infinite class of explicitly constructed (N,n,m) w–IPP codes for which N is $\mathcal{O}(\log n)$.*

Acknowledgments The authors would like to express their sincere gratitude to Prof. Chaoping Xing for many enlightening discussions with the authors. The authors would also like to thank the referees for carefully reviewing the paper and for their valuable comments and suggestions.

References

1. Barg A, Cohen G, Encheva S, Kabatiansky G, Zémor G (2001) A hypergraph approach to the identifying parent property: the case of multiple parents. SIAM J Discrete Math 14:423–431
2. Boneh D, Shaw J (1998) Collusion–secure fingerprinting for digital data. IEEE Trans Inform Theor 44:1897–1905
3. Deng D, Stinson DR, Wei R (2004) The Lovász local lemma and its applications to some combinatorial arrays. Design Code Cryptogr 32:121–134
4. Garcia A, Stichtenoth H (1996) On the asymptotic behaviour of some towers of function fields over finite fields. J Number Theory 61:248–273
5. Hollmann HDL, van Lint JH (1998) Linnartz J-P, Tolhuizen LMGM (1998) On codes with identifiable parent property. J Comb Theory Ser A 82:121–133
6. Li PC, van Rees GHJ, Wei R (2006) Constructions of 2–cover–free families and related separating hash families. J Comb Design Published Online: 21 Apr. 2006
7. Niederreiter H, Xing C (2002) Rational points on curves over finite fields: theory and applications. Cambridge University Press, Cambridge, MA
8. Sarkar P, Stinson DR (2001) Frameproof and IPP Codes. In INDOCRYPT 2001. Lect Notes Comput Sci 2247:117–126
9. Serre J-P (1985) Rational points on curves over finite fields. Lecture Notes, Harvard University
10. Stichtenoth H, (1993) Algebraic function fields and codes. Springer–Verlag, Berlin
11. Staddon JN, Stinson DR, Wei R (2001) Combinatorial properties of frameproof and traceability codes. IEEE Trans Inform Theory. 47:1042–1049
12. Stinson DR (1997) On some methods for unconditionally secure key distribution and broadcast encryption. Design Code Cryptogr 12:215–243
13. Stinson DR, van Trung T, Wei R (2000) Secure frameproof codes, key distribution patterns, group testing algorithms and related structures. J Statist Plann Inference 86:595–617
14. Stinson DR, Wei R (2004) Generalized cover-free families. Discrete Math 279:463–477
15. Stinson DR, Wei R, Zhu L (2000) New constructions for perfect hash families and related structures using combinatorial designs and codes. J Comb Designs 8:189–200
16. Tonien D, Safavi–Naini R (2003) Explicit construction of secure frameproof codes. Int J Pure App Math 6:343–360
17. van Trung T, Martirosyan S (2005) New constructions for IPP codes. Design Code Cryptogr 35:227–239
18. Tsfasman MA, Vlădut SG (1991) Algebraic–geometric codes. Kluwer Academic, Dordrecht
19. Wang H, Xing C (2001) Explicit constructions of perfect hash families from algebraic curves over finite fields. J Comb Theory Ser A, 93:112–124