Recursive Constructions of Secure Codes and Hash Families Using *Difference Function Families*

Dongvu Tonien dong@uow.edu.au
Reihaneh Safavi-Naini rei@uow.edu.au

School of IT & CS, University of Wollongong, NSW, 2522, Australia

Abstract

To protect copyrighted digital data against piracy, codes with different secure properties such as frameproof codes, secure frameproof codes, codes with identifiable parent property (IPP codes), traceability codes (TA codes) are introduced. In this paper, we study these codes together with related combinatorial objects called separating and perfect hash families. We introduce for the first time the notion of *difference function families* and use these difference function families to give generalized recursive techniques that can be used for *any kind* of secure codes and hash families. We show that some previous recursive techniques are special cases of these new techniques.

1 Introduction

Codes with secure properties are used for copyright protection and piracy tracing [3, 2, 4, 5]. Since, for instance, in broadcast encryption, the number of users corresponds to the size of the code and the transmission bandwidth is proportional to the code length, it is desirable to construct codes with large size but relatively small length. Recursive techniques are the most effective way to construct large codes.

By recursive techniques, a larger code (hash family) is constructed from one or two smaller codes (hash families). Safavi-Naini and Wang [5] provide recursive constructions of frameproof codes and IPP codes. This technique uses a function family satisfying some special properties. Atici et al [1] technique is for perfect hash families and Stinson et al [7] technique is for separating hash families. These two techniques are very similar and they used difference matrices. Stinson et al [8] technique is also for perfect hash families and separating hash families. This technique uses difference matrices and mutually orthogonal Latin rectangles and squares. Tran van Trung and Martirosyan [9] technique uses code concatenation method to construct a new IPP code from two original IPP codes. They also present a recursive technique for perfect hash families.

In this paper, we generalize some of the above results using a uniformed technique. We introduce for the first time the notion of difference function families. An $(n; I, J)$-difference function family is a collection of IJ functions mapping $\{1, \ldots, n\}$ into itself that satisfy a special property. We present two recursive constructions using difference function families. These constructions can be used for any kind of secure codes: w-frameproof codes, w-secure frameproof codes, w-IPP codes, w-TA codes, and for any kind of hash families: $\{w_1, w_2\}$-separating hash families, w-perfect hash families.

In the first construction, with an original code of length ℓ and size n, under the action of an $(n; n, J)$-difference function family, we obtain a new code of length ℓJ and size n^2 with the same properties as the original codes. Similarly, with an (ℓ, n, m)-hash family, under the action of an $(n; n, J)$-difference function family, we obtain a new $(\ell J, n^2, m)$-hash family with the same properties as the original hash family. The parameter J is chosen depending on different properties of codes and hash families. Namely, $J = w + 1$ is for w-frameproof, $J = w^2 + 1$ is for w-secure frameproof, w-IPP and w-TA, $J = w_1 w_2$ is for $\{w_1, w_2\}$-separating hash and $J = \binom{w}{2}$ is for w-perfect hash.

In the second construction, a new code (hash family) is constructed from two existing codes (hash families). Starting with two codes of size n_1, length ℓ_1 and size n_2, length ℓ_2 with $n_1 \geq n_2$, an $(n_1; n_2, J)$-difference function family of bijective functions can be used to generate a new code of size $n_1 n_2$, length $\ell_1 J + \ell_2$ with the same properties as the original codes. For different properties of codes and hash families, similar values as in the first construction are used for the parameter J.

Importantly, we show that these two recursive techniques can be applied iteratedly, so that, for instance in the first construction, from an original code (hash family) of length ℓ and size n, under the actions of z difference function families, we have a code with size $n_z = n^{2^z}$ and length $\ell_z = \ell J^z = O(\log(n_z)^{\log_2 J})$.

The paper is organized as follows. In section 2, we give definitions of different secure codes, hash families, and basic relationships between them; we also introduce the notion of difference function families. In section 3, we present our new recursive techniques. Main results are stated in section 3.1. We give explicit constructions of difference function families in section 3.2. In section 3.3, we state main results on iterated application of our recursive techniques. Finally, we give the proofs of main results in section 4.

2 Definitions

In this section, we give definitions of different kinds of secure codes and hash families and discuss basic relationships between them. We also introduce for the first time the notion of *difference function families.*

2.1 Codes

Let $\mathcal{A}$ be an alphabet of size m. An (ℓ, n, m)-code Γ of length ℓ and size n over $\mathcal{A}$ is a collection of n elements, which are called *codewords*, of $\mathcal{A}^\ell$. Each $\alpha \in \mathcal{A}^\ell$ is written in the form $\alpha = (\alpha_1, \ldots, \alpha_\ell)$. The *matrix form* of Γ is an $n \times \ell$ matrix whose rows are codewords of Γ.

For a subset $X \subset \Gamma$ and a position $1 \leq i \leq \ell$, define the *projection* of X on the position i as

$$\pi_i(X) = \{x_i : x \in X\},$$

and the set of *descendants* of X as

$$desc(X) = \prod_{i=1}^{\ell} \pi_i(X) = \{\alpha \in \mathcal{A}^\ell : \alpha_i \in \pi_i(X),\ \forall 1 \leq i \leq \ell\}.$$

The set of descendants is a subset of $\mathcal{A}^\ell$ that can be constructed by a coalition of users who have the codewords in X. If $\alpha \in desc(X)$ then codewords in X are called *parents* of α.

Let w be a positive integer. Define the *w-descendant code*, denoted by $desc_w(\Gamma)$, as follows

$$desc_w(\Gamma) = \bigcup_{X \subset \Gamma,\ |X| \le w} desc(X).$$

Definition 1 *Let Γ be an (ℓ, n, m)-code and let w be a positive integer.*

*Γ is w-*frameproof *if for any $X \subset \Gamma$ such that $0 < |X| \le w$, we have*

$$desc(X) \cap \Gamma = X.$$

*Γ is w-*secure frameproof *if for any $X_1, X_2 \subset \Gamma$ such that $0 < |X_1| \le w$, $0 < |X_2| \le w$ and $X_1 \cap X_2 = \emptyset$, we have*

$$desc(X_1) \cap desc(X_2) = \emptyset.$$

For two subsets $X_1, X_2 \subset \Gamma$, if the two projection sets $\pi_i(X_1)$ and $\pi_i(X_2)$ are disjoint then the position i is said to *separate* X_1 and X_2.

It follows from Definition 1 that if Γ is a w-frameproof code then for any subset X of size up to w of Γ and any codeword $a \notin X$, there must exist a position i that separates X and $\{a\}$. Similarly, Γ is w-secure frameproof if for any two disjoint subsets X_1 and X_2 of size up to w of Γ, there exists a position i that separates them.

For $\alpha, \beta \in \mathcal{A}^\ell$, let $d(\alpha, \beta)$ denote the Hamming distance between α and β. For a code Γ, let d_Γ denote the minimum Hamming distance of Γ.

Definition 2 *Let Γ be an (ℓ, n, m)-code and let w be a positive integer.*

Γ is w-IPP (identifiable parent property) *if for any $\alpha \in desc_w(\Gamma)$, we have*

$$\bigcap_{X \subset \Gamma,\, |X| \le w,\, \alpha \in desc(X)} X \ne \emptyset.$$

Γ is w-TA (traceability) *if for any $X \subset \Gamma$ such that $0 < |X| \le w$ and for any $\alpha \in desc(X)$, there exists a codeword $x \in X$ such that for any $y \in \Gamma \setminus X$, we have $d(\alpha, x) < d(\alpha, y)$.*

A w-IPP code ensures that from a pirate word $\alpha \in desc_w(\Gamma)$ it is possible to find at least one of its parents. Clearly, a w-TA code is w-IPP. In a w-TA code, a codeword that has the shortest Hamming distance to the pirate word α must be one of its parents. There is a sufficient condition on the minimum Hamming distance for a code to be w-TA.

Theorem 1 ([6]) *Let Γ be an (ℓ, n, m)-code and let w be a positive integer. If the minimum Hamming distance $d_\Gamma > \ell\left(1 - \frac{1}{w^2}\right)$ then Γ is w-TA.*

Concatenated Codes. Let Γ be an (ℓ, n, m)-code and Ψ be an (L, N, n)-code. Let $\mathcal{A}$, Q denote the alphabet sets of Γ and Ψ then $|Q| = |\Gamma| = n$. Let $\imath : Q \to \Gamma$ be the bijective function mapping the ith symbol of Q to the ith codeword of Γ. The *concatenated code* $\Psi[\Gamma]$ over $\mathcal{A}$ is an $(L\ell, N, m)$-code defined as $\Psi[\Gamma] = \{(\imath(u_1), \ldots, \imath(u_L)) : u = (u_1, \ldots, u_L) \in \Psi\}$. Γ is called the *inner code* and Ψ is called the *outer code*. Each codeword of the concatenated code $\Psi[\Gamma]$ consists of L codewords of the inner code Γ.

Theorem 2 ([9]) *Let Γ, Ψ be two codes with parameters (ℓ, n, m) and (L, N, n), and w be a positive integer. If Γ and Ψ are both w-IPP then the concatenated code $\Psi[\Gamma]$ is also w-IPP.*

2.2 Hash Families

Let $[n] = \{1, \ldots, n\}$. Assume $|\mathcal{A}| = m$. An (ℓ, n, m)-hash family $\mathcal{H}$ is a collection of ℓ functions which map $[n]$ into $\mathcal{A}$. The *matrix form* of $\mathcal{H}$ is an $n \times \ell$ matrix whose columns represent functions of $\mathcal{H}$; that is, the matrix entry at row i and column j is $h(i)$ where h is the jth function of $\mathcal{H}$.

For a subset $X \subset [n]$ and $h \in \mathcal{H}$, denote $h(X) = \{h(x) : x \in X\}$.

Definition 3 *Let $\mathcal{H}$ be an (ℓ, n, m)-hash family and let w, w_1 and w_2 be positive integers.*

$\mathcal{H}$ is $\{w_1, w_2\}$-separating *if for any $X_1, X_2 \subset [n]$ such that $0 < |X_1| \le w_1$, $0 < |X_2| \le w_2$ and $X_1 \cap X_2 = \emptyset$, there exists a function $h \in \mathcal{H}$ satisfying*

$$h(X_1) \cap h(X_2) = \emptyset.$$

$\mathcal{H}$ is w-perfect *if for any $X \subset [n]$ such that $0 < |X| \le w$, there exists a function $h \in \mathcal{H}$ whose restriction on X is a one-to-one function.*

A function h in Definition 3 that satisfies $h(X_1) \cap h(X_2) = \emptyset$, is said to *separate* X_1 and X_2. In the matrix form of $\mathcal{H}$, the column corresponding to h is also said to separate the two sets of rows corresponding to X_1 and X_2.

An (ℓ, n, m)-code Γ and an (ℓ, n, m)-hash family $\mathcal{H}$ are *dual* of one another if they have the same matrix form $\mathcal{M}$. In this case, rows of $\mathcal{M}$ are codewords of Γ and columns of $\mathcal{M}$ are functions of $\mathcal{H}$. From now on, we abuse the language by using the same notation Γ to denote a code and its matrix form, and $\mathcal{H}$ to refer to a hash family and its matrix form.

There is a close connection between frameproof, secure frameproof codes with separating hash families, which is stated in Theorem 3.

Theorem 3 ([6]) *Let Γ be an (ℓ, n, m)-code and $\mathcal{H}$ be an (ℓ, n, m)-hash family. Assuming that Γ and $\mathcal{H}$ are dual then*

- *Γ is w-frameproof if and only if $\mathcal{H}$ is $\{1, w\}$-separating;*
- *Γ is w-secure frameproof if and only if $\mathcal{H}$ is $\{w, w\}$-separating.*

2.3 Difference Function Families

In this section, for the first time, we introduce the notion of *difference function families.* We first give the definition of difference matrices.

Definition 4 *An (n, k)-*difference matrix *is a $k \times n$ integer matrix $D = (d_{i,j})$ such that for any two different rows u and v, the n differences between entries on the two rows, $d_{u,1} - d_{v,1}$, $d_{u,2} - d_{v,2}$, $\ldots$, $d_{u,n} - d_{v,n}$, are distinct modulo n.*

Let $[n]^{[n]}$ denote the set of all functions mapping $[n]$ into itself. If a collection of functions $\Phi \subset [n]^{[n]}$ is indexed as $\Phi = \{\phi_{i,j} : 1 \le i \le I, 1 \le j \le J\}$ then Φ is said to be of size $I \times J$. If every member function $\phi_{i,j}$ is of the form $\phi_{i,j}(x) = x + \delta_{i,j} \pmod n$ for some constant $\delta_{i,j}$, then Φ is called a *rotating function family*, and the corresponding $I \times J$ matrix $\Delta = (\delta_{i,j})$ is called the *rotating coefficient matrix* of Φ.

If all functions $\phi_{i,j} : [n] \to [n]$ of Φ are bijective then the function family Φ is said to be *bijective.* Rotating function families are automatically bijective.

Difference function families are defined as follows.

Definition 5 *Let n, I and J be positive integers such that $J > 1$ and $I \leq n$. An $(n; I, J)$-*difference function family *is a function family $\Phi = \{\phi_{i,j}\} \subset [n]^{[n]}$ of size $I \times J$ which satisfies the following condition: for any $j_1 \neq j_2$, if $\phi_{i_1,j_1}(x) = \phi_{i_2,j_1}(y)$ and $\phi_{i_1,j_2}(x) = \phi_{i_2,j_2}(y)$ then $i_1 = i_2$ and $x = y$.*

It is not hard to show that, for any function family Φ of size $I \times J$ with $J > 1$, the condition on Φ in the Definition 5 implies $I \leq n$. Indeed, take any $1 \leq j_1 \neq j_2 \leq J$ and consider nI ordered pairs $(\phi_{i,j_1}(x), \phi_{i,j_2}(x))$ where $1 \leq i \leq I$ and $1 \leq x \leq n$. The condition on Φ implies that all these ordered pairs are distinct. Since these ordered pairs are elements of the set $[n] \times [n]$, it follows that $nI \leq n^2$, and thus, $I \leq n$. Difference function families are generalization of difference matrices by the following theorem.

Theorem 4 *Let $\Phi \in [n]^{[n]}$ be a rotating function family of size $n \times J$ with the rotating coefficient matrix $\Delta = (\delta_{i,j})$. Then Φ is an $(n; n, J)$-difference function family if and only if the transpose matrix of Δ is an (n, J)-difference matrix.*

Proof. Suppose that Φ is an $(n; n, J)$-difference function family, we prove that for any $1 \leq u \neq v \leq J$, the following differences $\delta_{1,u} - \delta_{1,v}$, $\delta_{2,u} - \delta_{2,v}$, $\ldots$, $\delta_{n,u} - \delta_{n,v}$ are distinct modulo n. Indeed, if $\delta_{i_1,u} - \delta_{i_1,v} = \delta_{i_2,u} - \delta_{i_2,v} \pmod n$ then $\delta_{i_1,u} - \delta_{i_2,u} = \delta_{i_1,v} - \delta_{i_2,v} = x - 1 \pmod n$ for some $x \in [n]$. Hence $\phi_{i_1,u}(1) = \phi_{i_2,u}(x)$ and $\phi_{i_1,v}(1) = \phi_{i_2,v}(x)$. It follows that $i_1 = i_2$.

Conversely, suppose that Δ^T is an (n, J)-difference matrix. Assume that $1 \leq j_1 \neq j_2 \leq J$, and $\phi_{i_1,j_1}(x) = \phi_{i_2,j_1}(y)$, $\phi_{i_1,j_2}(x) = \phi_{i_2,j_2}(y)$, we prove that $i_1 = i_2$ and $x = y$. Indeed, we have $\phi_{i_1,j_1}(x) - \phi_{i_1,j_2}(x) = \delta_{i_1,j_1} - \delta_{i_1,j_2} = \phi_{i_2,j_1}(y) - \phi_{i_2,j_2}(y) = \delta_{i_2,j_1} - \delta_{i_2,j_2} \pmod n$. Since Δ^T is an (n, J)-difference matrix, we must have $i_1 = i_2$, and thus, $x = y$. ■

3 Generalized Recursive Techniques

In this section, we present recursive techniques that generalize some of previous known techniques. We construct new codes or hash families from existing codes or hash families by letting some difference function families act on these existing codes or hash families. We prove that this action preserves the property of codes and hash families.

Let $\phi \in [n]^{[n]}$, then the matrix $\phi(\Gamma)$ is constructed as

$$\phi(\Gamma) = \begin{pmatrix} a_{\phi(1)} \\ \vdots \\ a_{\phi(n)} \end{pmatrix} \quad \text{where} \quad \Gamma = \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix}.$$

Consider the following two constructions.

The first construction. Let Γ be an (ℓ, n, m)-code (hash family). Let Φ be an $(n; n, J)$-difference function family. Then $\Phi(\Gamma)$ is a matrix of size $n^2 \times \ell J$ defined as

$$\Phi(\Gamma) = \begin{pmatrix} \phi_{1,1}(\Gamma) & \phi_{1,2}(\Gamma) & \dots & \phi_{1,J}(\Gamma) \\ \vdots & \vdots & & \vdots \\ \phi_{n,1}(\Gamma) & \phi_{n,2}(\Gamma) & \dots & \phi_{n,J}(\Gamma) \end{pmatrix}.$$

Under the action of function family Φ, from a code (hash family) Γ of parameters (ℓ, n, m) we obtain a new code (hash family) $\Phi(\Gamma)$ of parameters $(\ell J, n^2, m)$.

The second construction. Let Γ_1, Γ_2 be two codes (hash families) of parameters (ℓ_1, n_1, m_1) and (ℓ_2, n_2, m_2) where $n_1 \geq n_2$. Let Φ be a bijective $(n_1; n_2, J)$-difference function family. Then $\Phi(\Gamma_1, \Gamma_2)$ is a matrix of size $(n_1 n_2) \times (\ell_1 J + \ell_2)$ defined as

$$\Phi(\Gamma_1, \Gamma_2) = \begin{pmatrix} \phi_{1,1}(\Gamma_1) & \phi_{1,2}(\Gamma_1) & \dots & \phi_{1,J}(\Gamma_1) & \text{1st row of } \Gamma_2 \text{ repeated } n_1 \text{ times} \\ \vdots & \vdots & & \vdots & \vdots \\ \phi_{n_2,1}(\Gamma_1) & \phi_{n_2,2}(\Gamma_1) & \dots & \phi_{n_2,J}(\Gamma_1) & n_2\text{th row of } \Gamma_2 \text{ repeated } n_1 \text{ times} \end{pmatrix}.$$

Let $\mathcal{A}_1$ and $\mathcal{A}_2$ denote the alphabet sets of Γ_1 and Γ_2, respectively. If $m_1 \leq m_2$, by embedding $\mathcal{A}_1$ into $\mathcal{A}_2$, we can assume $\mathcal{A}_1 \subset \mathcal{A}_2$. Similarly, if $m_2 \leq m_1$, by embedding $\mathcal{A}_2$ into $\mathcal{A}_1$, we can assume $\mathcal{A}_2 \subset \mathcal{A}_1$. So the alphabet set of $\Phi(\Gamma_1, \Gamma_2)$ has $\max(m_1, m_2)$ number of symbols.

When $\Gamma_1 = \Gamma_2 = \Gamma$ is a code (hash family) of parameters (ℓ, n, m) and Φ is a bijective $(n; n, J)$-difference function family then the second construction gives a new code (hash family) $\Phi(\Gamma, \Gamma)$ of parameters $(\ell(J+1), n^2, m)$.

In section 3.1, we show that with certain choices of J, the two constructions will preserve properties of the codes (hash families).

3.1 Main Results

Frameproof Codes

Theorem 5 *If Γ is a w-frameproof (ℓ, n, m)-code and Φ is an $(n; n, w+1)$-difference function family, then $\Phi(\Gamma)$ is a w-frameproof $((w+1)\ell, n^2, m)$-code.*

Theorem 6 *If Γ_1, Γ_2 are two w-frameproof codes of parameters (ℓ_1, n_1, m_1), (ℓ_2, n_2, m_2), respectively, where $n_1 \geq n_2$, and Φ is a bijective $(n_1; n_2, w)$-difference function family, then $\Phi(\Gamma_1, \Gamma_2)$ is a w-frameproof $(w\ell_1 + \ell_2, n_1 n_2, \max(m_1, m_2))$-code.*

Secure Frameproof Codes

Theorem 7 *If Γ is a w-secure frameproof (ℓ, n, m)-code and Φ is an $(n; n, w^2+1)$-difference function family, then $\Phi(\Gamma)$ is a w-secure frameproof $((w^2+1)\ell, n^2, m)$-code.*

Theorem 8 *If Γ_1, Γ_2 are two w-secure frameproof codes of parameters (ℓ_1, n_1, m_1), (ℓ_2, n_2, m_2), respectively, where $n_1 \geq n_2$, and Φ is a bijective $(n_1; n_2, w^2)$-difference function family, then $\Phi(\Gamma_1, \Gamma_2)$ is a w-secure frameproof $(w^2\ell_1 + \ell_2, n_1 n_2, \max(m_1, m_2))$-code.*

IPP & TA Codes

Theorem 9 *If* Γ *is a* w*-IPP* (ℓ, n, m)*-code and* Φ *is an* $(n; n, w^2+1)$*-difference function family, then* $\Phi(\Gamma)$ *is a* w*-IPP* $((w^2+1)\ell, n^2, m)$*-code.*

Theorem 10 *If* Γ *is a* w*-TA* (ℓ, n, m)*-code with minimum Hamming distance* $d_\Gamma > \frac{J}{J-1}\ell\left(1 - \frac{1}{w^2}\right)$ *and* Φ *is an* $(n; n, J)$*-difference function family, then* $\Phi(\Gamma)$ *is a* w*-TA* $(J\ell, n^2, m)$*-code.*

Separating Hash Families

Theorem 11 *If* $\mathcal{H}$ *is a* $\{w_1, w_2\}$*-separating* (ℓ, n, m)*-hash family and* Φ *is an* $(n; n, w_1w_2+1)$*-difference function family, then* $\Phi(\mathcal{H})$ *is a* $\{w_1, w_2\}$*-separating* $((w_1w_2+1)\ell, n^2, m)$*-hash family.*

Theorem 12 *If* $\mathcal{H}_1$, $\mathcal{H}_2$ *are two* $\{w_1, w_2\}$*-separating hash families of parameters* (ℓ_1, n_1, m_1), (ℓ_2, n_2, m_2), *respectively, where* $n_1 \geq n_2$, *and* Φ *is a bijective* $(n_1; n_2, w_1w_2)$*-difference function family, then* $\Phi(\mathcal{H}_1, \mathcal{H}_2)$ *is a* $\{w_1, w_2\}$*-separating* $(w_1w_2\ell_1 + \ell_2, n_1n_2, \max(m_1, m_2))$*-hash family.*

Perfect Hash Families

Theorem 13 *If* $\mathcal{H}$ *is a* w*-perfect* (ℓ, n, m)*-hash family and* Φ *is an* $(n; n, \binom{w}{2}+1)$*-difference function family, then* $\Phi(\mathcal{H})$ *is a* w*-perfect* $((\binom{w}{2}+1)\ell, n^2, m)$*-hash family.*

Theorem 14 *If* $\mathcal{H}_1$, $\mathcal{H}_2$ *are two* w*-perfect hash families of parameters* (ℓ_1, n_1, m_1), (ℓ_2, n_2, m_2), *respectively, where* $n_1 \geq n_2$, *and* Φ *is a bijective* $(n_1; n_2, \binom{w}{2})$*-difference function family, then* $\Phi(\mathcal{H}_1, \mathcal{H}_2)$ *is a* w*-perfect* $(\binom{w}{2}\ell_1 + \ell_2, n_1n_2, \max(m_1, m_2))$*-hash family.*

Comparison with Previous Constructions. By Theorem 4, a difference matrix is equivalent to a *rotating* difference function family, the first recursive construction of perfect hash families by Atici et al [1] is, therefore, a special case of Theorem 13. Similarly, the recursive construction of separating hash families by Stinson et al [7] is a special case of Theorem 11.

Theorem 5 and Theorem 9 give better recursive constructions for frameproof codes and IPP codes compared to constructions by Safavi-Naini and Wang [5] since they generate codes with shorter lengths and larger sizes.

3.2 Explicit Construction of Difference Function Families

In this section, we give explicit constructions of difference function families and bijective difference function families.

Notation. An integer-valued function μ is called *one-to-one modulo* n if $\mu(x) \not\equiv \mu(y) \pmod{n}$ for any $x \neq y$.

Theorem 15 *Let* n, J, t *be positive integers such that* $J > 1$ *and* $\gcd(n, t) = \gcd(n, (J-1)!) = 1$. *Let* η, ξ, μ *be functions mapping* $[n]$ *into* $\mathbf{Z}$, *such that* μ *is one-to-one modulo* n. *Let* $\Phi = \{\phi_{i,j}\} \subset [n]^{[n]}$ *be a function family of size* $n \times J$ *constructed as* $\phi_{i,j}(x) \equiv tjx + \mu(i) + \eta(j) + \xi(x) \pmod{n}$ *then* Φ *is an* $(n; n, J)$*-difference function family.*

Proof. Suppose $\phi_{i_1,j_1}(x) = \phi_{i_2,j_1}(y)$ and $\phi_{i_1,j_2}(x) = \phi_{i_2,j_2}(y)$ for some $1 \leq j_1 \neq j_2 \leq J$, then $\phi_{i_1,j_1}(x) - \phi_{i_2,j_1}(y) + \phi_{i_2,j_2}(y) - \phi_{i_1,j_2}(x) \equiv t(j_1 - j_2)(x - y) \equiv 0 \pmod{n}$. Since $1 \leq x, y \leq n$, $0 < |j_1 - j_2| \leq J - 1$ and n is coprime to t and $(J-1)!$, it follows that $x = y$. Thus, $\phi_{i_1,j_1}(x) - \phi_{i_2,j_1}(y) \equiv \mu(i_1) - \mu(i_2) \equiv 0 \pmod{n}$. Since μ is one-to-one modulo n, we have $i_1 = i_2$. Therefore, Φ is an $(n; n, J)$-difference function family. ■

Corollary 1 *Let n be a prime. Let J, t, s be positive integers less than n and $J > 1$. Let η, ξ be two arbitrary functions mapping $[n]$ into $\mathbf{Z}$. Let $\Phi = \{\phi_{i,j}\} \subset [n]^{[n]}$ be a function family of size $n \times J$ constructed as $\phi_{i,j}(x) \equiv tjx + si + \eta(j) + \xi(x) \pmod{n}$, then Φ is an $(n; n, J)$-difference function family.*

The following theorem gives an explicit construction of bijective difference function families.

Theorem 16 *Let n, J, t be positive integers such that $J > 1$ and $\gcd(n, t) = \gcd(n, (J-1)!) = 1$. Let η, ξ, μ be functions mapping $[n]$ into $\mathbf{Z}$ such that ξ is one-to-one modulo n. Let $\Phi = \{\phi_{i,j}\} \subset [n]^{[n]}$ be a function family of size $n \times J$ constructed as $\phi_{i,j}(x) \equiv tij + \mu(i) + \eta(j) + \xi(x) \pmod{n}$, then Φ is a bijective $(n; n, J)$-difference function family.*

Proof. Φ is bijective because ξ is one-to-one modulo n. Now suppose that $\phi_{i_1,j_1}(x) = \phi_{i_2,j_1}(y)$ and $\phi_{i_1,j_2}(x) = \phi_{i_2,j_2}(y)$ for some $1 \leq j_1 \neq j_2 \leq J$, then $\phi_{i_1,j_1}(x) - \phi_{i_2,j_1}(y) + \phi_{i_2,j_2}(y) - \phi_{i_1,j_2}(x) \equiv t(i_1 - i_2)(j_1 - j_2) \equiv 0 \pmod{n}$. Since $1 \leq i_1, i_2 \leq n$, $0 < |j_1 - j_2| \leq J - 1$ and n is coprime to t and $(J-1)!$, it follows that $i_1 = i_2$. Thus, $\phi_{i_1,j_1}(x) - \phi_{i_2,j_1}(y) \equiv \xi(x) - \xi(y) \equiv 0 \pmod{n}$. Since ξ is one-to-one modulo n, we have $x = y$. Therefore, Φ is a bijective $(n; n, J)$-difference function family. ■

Corollary 2 *Let n be a prime. Let J, t, s be positive integers less than n and $J > 1$. Let η, ξ be two arbitrary functions mapping $[n]$ into $\mathbf{Z}$. Let $\Phi = \{\phi_{i,j}\} \subset [n]^{[n]}$ be a function family of size $n \times J$ constructed as $\phi_{i,j}(x) \equiv tij + sx + \mu(i) + \eta(j) \pmod{n}$, then Φ is a bijective $(n; n, J)$-difference function family.*

3.3 Iterated Recursive Constructions

An important property of our recursive techniques is that we can apply them unlimited number of times. To demonstrate, consider an application of Theorem 5 and Theorem 15 as follows.

Suppose we have a w-frameproof (ℓ, n, m)-code Γ. Using Theorem 15 to construct an $(n; n, w+1)$-difference function family $\Phi^{(1)}$, by Theorem 5, $\Phi^{(1)}(\Gamma)$ is a w-frameproof $((w+1)\ell, n^2, m)$-code. Using Theorem 15 again to construct an $(n^2; n^2, w+1)$-difference function family $\Phi^{(2)}$, by Theorem 5, $\Phi^{(2)}(\Phi^{(1)}(\Gamma))$ is a w-frameproof $((w+1)^2\ell, n^4, m)$-code. Eventually, after z times of doing this, we have a w-frameproof $((w+1)^z\ell, n^{2^z}, m)$-code as stated in Theorem 17.

Theorem 17 *Let n, w, z be positive integers such that $\gcd(n, w!) = 1$. For each $k = 1, \ldots, z$, let t_k be a positive integer and η_k, ξ_k, μ_k be functions mapping $[n^{2^{k-1}}]$ into $\mathbf{Z}$, such that $\gcd(n, t_k) = 1$ and μ_k is one-to-one modulo $n^{2^{k-1}}$.*

For each $k = 1, \ldots, z$, let $\Phi^{(k)} = \{\phi_{i,j}^{(k)}\} \subset [n^{2^{k-1}}]^{[n^{2^{k-1}}]}$ be a function family of size $n^{2^{k-1}} \times (w+1)$ constructed as $\phi_{i,j}^{(k)}(x) \equiv t_k jx + \mu_k(i) + \eta_k(j) + \xi_k(x) \pmod{n^{2^{k-1}}}$. Let Γ be a w-frameproof (ℓ, n, m)-code. Then the $((w+1)^z\ell, n^{2^z}, m)$-code $\Phi^{(z)}(\ldots(\Phi^{(2)}(\Phi^{(1)}(\Gamma)))\ldots)$ is w-frameproof.

Similarly, iteratedly applying the results in section 3.1 for w-secure frameproof codes, w-IPP codes, w-TA codes, w-perfect hash families, $\{w_1, w_2\}$-separating hash families using constructions of (bijective) difference function families in Theorem 15, Theorem 16, Corollary 1 and Corollary 2, we have:

Theorem 18 *If* $\gcd(n, (w^2)!) = 1$ *then from a w-secure frameproof (ℓ, n, m)-code it is possible to construct a new w-secure frameproof $((w^2+1)^z\ell, n^{2^z}, m)$-code for any positive integer z.*

Theorem 19 *If* $\gcd(n, (w^2)!) = 1$ *then from a w-IPP (ℓ, n, m)-code it is possible to construct a new w-IPP $((w^2+1)^z\ell, n^{2^z}, m)$-code for any positive integer z.*

Theorem 20 *If* $\gcd(n, (J-1)!) = 1$ *then for any positive integer z, from a w-TA (ℓ, n, m)-code with minimum Hamming distance $d > (\frac{J}{J-1})^z\ell\left(1 - \frac{1}{w^2}\right)$, it is possible to construct a new w-TA $(J^z\ell, n^{2^z}, m)$-code.*

Theorem 21 *If* $\gcd(n, (w_1w_2)!) = 1$ *then from a $\{w_1, w_2\}$-separating (ℓ, n, m)-hash family it is possible to construct a new $\{w_1, w_2\}$-separating $((w_1w_2+1)^z\ell, n^{2^z}, m)$-hash family for any positive integer z.*

Theorem 22 *If* $\gcd(n, \binom{w}{2}!) = 1$ *then from a w-perfect (ℓ, n, m)-hash family it is possible to construct a new w-perfect $((\binom{w}{2}+1)^z\ell, n^{2^z}, m)$-hash family for any positive integer z.*

4 Proofs of Main Results

For a function family $\Phi = \{\phi_{i,j}\} \subset [n]^{[n]}$ of size $n \times J$, let $\widehat{\Phi}$ denote the following (J, n^2, n)-code:

$$\widehat{\Phi} = \begin{pmatrix} \hat{\phi}_{1,1} & \hat{\phi}_{1,2} & \dots & \hat{\phi}_{1,J} \\ \hat{\phi}_{2,1} & \hat{\phi}_{2,2} & \dots & \hat{\phi}_{2,J} \\ \vdots & \vdots & & \vdots \\ \hat{\phi}_{n,1} & \hat{\phi}_{n,2} & \dots & \hat{\phi}_{n,J} \end{pmatrix} \text{ where } \hat{\phi}_{i,j} = \begin{pmatrix} \phi_{i,j}(1) \\ \phi_{i,j}(2) \\ \vdots \\ \phi_{i,j}(n) \end{pmatrix}.$$

Then for any (ℓ, n, m)-code Γ, the $(\ell J, n^2, m)$-code $\Phi(\Gamma)$ is exactly the concatenated code $\widehat{\Phi}[\Gamma]$ with Γ being its inner code and $\widehat{\Phi}$ its outer code. It follows from the definition that if Φ is an $(n; n, J)$-difference function family then the code $\widehat{\Phi}$ has minimum Hamming distance $d_{\widehat{\Phi}} \geq J - 1$. We use this observation to prove Theorem 9, Theorem 10 and Theorem 20.

Proof of Theorem 9. The corresponding (w^2+1, n^2, n)-code $\widehat{\Phi}$ of the $(n; n, w^2+1)$-difference function family Φ has minimum Hamming distance $d_{\widehat{\Phi}} \geq w^2$. Therefore, $d_{\widehat{\Phi}} > (w^2+1)\left(1 - \frac{1}{w^2}\right)$, by Theorem 1, the code $\widehat{\Phi}$ is w-TA, and thus, is w-IPP. Since Γ is w-IPP, by Theorem 2, the concatenated code $\widehat{\Phi}[\Gamma] = \Phi(\Gamma)$ is w-IPP. ■

Proof of Theorem 10. The code $\widehat{\Phi}$ has the minimum Hamming distance $d_{\widehat{\Phi}} \geq J - 1$. Since the minimum Hamming distance of a concatenated code is greater than or equal to the product of the minimum Hamming distances of its inner code and outer code, $d_{\Phi(\Gamma)} = d_{\widehat{\Phi}[\Gamma]} \geq d_{\widehat{\Phi}} d_\Gamma \geq (J-1)d_\Gamma > J\ell\left(1 - \frac{1}{w^2}\right)$. Therefore, by Theorem 1, $(J\ell, n^2, m)$-code $\Phi(\Gamma)$ is w-TA. ■

Proof of Theorem 20. Since $\gcd(n,(J-1)!)=1$, as in Theorem 17, for each $k=1,\ldots,z$, there exists an $(n^{2^{k-1}};n^{2^{k-1}},J)$-difference function family $\Phi^{(k)}$. Let $\Gamma_0=\Gamma$, for each $k=1,\ldots,z$, let $\Gamma_k=\Phi^{(k)}(\Gamma_{k-1})=\widehat{\Phi}^{(k)}[\Gamma_{k-1}]$. We will prove that the $(J^z\ell,n^{2^z},m)$-code Γ_z is w-TA.

Indeed, for each $k=1,\ldots,z$, the code $\widehat{\Phi}^{(k)}$ has the minimum Hamming distance $d_{\widehat{\Phi}^{(k)}}\geq J-1$. Thus, $d_{\Gamma_k}\geq d_{\widehat{\Phi}^{(k)}}d_{\Gamma_{k-1}}\geq(J-1)d_{\Gamma_{k-1}}$. Therefore, $d_{\Gamma_z}\geq(J-1)^z d_{\Gamma_0}=(J-1)^z d>J^z\ell\left(1-\frac{1}{w^2}\right)$, and by Theorem 1, $(J^z\ell,n^{2^z},m)$-code Γ_z is w-TA. ■

Theorem 5 and Theorem 7 follow from Theorem 11 and Theorem 3. Theorem 6 and Theorem 8 follow from Theorem 12 and Theorem 3. We now prove Theorem 11, Theorem 12, Theorem 13 and Theorem 14.

Proof of Theorem 11. The matrix $\Phi(\mathcal{H})$ contains n^2 rows divided into n blocks, each block contains n rows. With $1\leq b\leq n$, $1\leq t\leq n$, let $\langle b,t\rangle$ denote the t^{th} row in the b^{th} block of $\Phi(\mathcal{H})$. If a_i denotes the i^{th} row of $\mathcal{H}$ then $\langle b,t\rangle$ consists of w_1w_2+1 rows of $\mathcal{H}$ as follows

$$\langle b,t\rangle=(a_{\phi_{b,1}(t)},a_{\phi_{b,2}(t)},\ldots,a_{\phi_{b,w_1w_2+1}(t)}).$$

We prove that $\Phi(\mathcal{H})$ is $\{w_1,w_2\}$-separating by contradiction. Assume that $X_1=\{\langle b_1,t_1\rangle,\ldots,\langle b_u,t_u\rangle\}$ and $X_2=\{\langle d_1,s_1\rangle,\ldots,\langle d_v,s_v\rangle\}$ are two disjoint sets of rows of $\Phi(\mathcal{H})$ with $1\leq u\leq w_1$, $1\leq v\leq w_2$ and $desc(X_1)\cap desc(X_2)\neq\emptyset$.

$$\begin{array}{cccccc}
 & \langle b_1,t_1\rangle= & a_{\phi_{b_1,1}(t_1)} & a_{\phi_{b_1,2}(t_1)} & \cdots & a_{\phi_{b_1,w_1w_2+1}(t_1)}\\
 & \langle b_2,t_2\rangle= & a_{\phi_{b_2,1}(t_2)} & a_{\phi_{b_2,2}(t_2)} & \cdots & a_{\phi_{b_2,w_1w_2+1}(t_2)}\\
X_1 & \vdots & \vdots & \vdots & & \vdots\\
 & \langle b_u,t_u\rangle= & a_{\phi_{b_u,1}(t_u)} & a_{\phi_{b_u,2}(t_u)} & \cdots & a_{\phi_{b_u,w_1w_2+1}(t_u)}\\
\hline
 & \langle d_1,s_1\rangle= & a_{\phi_{d_1,1}(s_1)} & a_{\phi_{d_1,2}(s_1)} & \cdots & a_{\phi_{d_1,w_1w_2+1}(s_1)}\\
 & \langle d_2,s_2\rangle= & a_{\phi_{d_2,1}(s_2)} & a_{\phi_{d_2,2}(s_2)} & \cdots & a_{\phi_{d_2,w_1w_2+1}(s_2)}\\
X_2 & \vdots & \vdots & \vdots & & \vdots\\
 & \langle d_v,s_v\rangle= & a_{\phi_{d_v,1}(s_v)} & a_{\phi_{d_v,2}(s_v)} & \cdots & a_{\phi_{d_v,w_1w_2+1}(s_v)}
\end{array}$$

For each k, $1\leq k\leq w_1w_2+1$, the two sets of indices

$$\{\phi_{b_1,k}(t_1),\phi_{b_2,k}(t_2),\ldots,\phi_{b_u,k}(t_u)\}\text{ and }\{\phi_{d_1,k}(s_1),\phi_{d_2,k}(s_2),\ldots,\phi_{d_v,k}(s_v)\}$$

must have non-empty intersection since, if they are disjoint then from the $\{w_1,w_2\}$-separating property of $\mathcal{H}$, there exists a column that separates the following two sets of rows of $\mathcal{H}$:

$$\{a_{\phi_{b_1,k}(t_1)},a_{\phi_{b_2,k}(t_2)},\ldots,a_{\phi_{b_u,k}(t_u)}\}\text{ and }\{a_{\phi_{d_1,k}(s_1)},a_{\phi_{d_2,k}(s_2)},\ldots,a_{\phi_{d_v,k}(s_v)}\},$$

this column also separates the two sets of rows, X_1 and X_2, of $\Phi(\mathcal{H})$, which contradicts to the assumption that $desc(X_1)\cap desc(X_2)\neq\emptyset$.

For each k, $1\leq k\leq w_1w_2+1$, let S_k denote the set of all ordered pairs (p,q) with $1\leq p\leq u$ and $1\leq q\leq v$, such that $\phi_{b_p,k}(t_p)=\phi_{d_q,k}(s_q)$. From the above argument, S_k is not empty for any k.

Since there are w_1w_2+1 sets S_k and there are $uv\leq w_1w_2$ possible ordered pairs (p,q) with $1\leq p\leq u$ and $1\leq q\leq v$, it follows from Pigeon Hole Principle that there must exist a pair (p,q) that belongs two at least two sets, say S_{k_1} and S_{k_2} with $k_1\neq k_2$. We have,

$$\begin{cases}\phi_{b_p,k_1}(t_p) & = & \phi_{d_q,k_1}(s_q)\\ \phi_{b_p,k_2}(t_p) & = & \phi_{d_q,k_2}(s_q)\end{cases}$$

Thus, $t_p = s_q$ and $b_p = d_q$. Hence, $\langle b_p, t_p\rangle = \langle d_q, s_q\rangle \in X_1 \cap X_2$, contradiction. ■

Proof of Theorem 12. The matrix $\Phi(\mathcal{H}_1, \mathcal{H}_2)$ contains $n_1 n_2$ rows divided into n_2 blocks, each block contains n_1 rows. With $1 \le b \le n_2$, $1 \le t \le n_1$, let $\langle b, t\rangle$ denote the t^{th} row in the b^{th} block of $\Phi(\mathcal{H}_1, \mathcal{H}_2)$. If a_i, α_i denote the i^{th} rows of $\mathcal{H}_1$ and $\mathcal{H}_2$, respectively, then $\langle b, t\rangle$ consists of $w_1 w_2$ rows of $\mathcal{H}_1$ and one row of $\mathcal{H}_2$ as follows

$$\langle b, t\rangle = (a_{\phi_{b,1}(t)}, a_{\phi_{b,2}(t)}, \ldots, a_{\phi_{b,w_1 w_2}(t)}, \alpha_b).$$

We prove that $\Phi(\mathcal{H}_1, \mathcal{H}_2)$ is $\{w_1, w_2\}$-separating by contradiction. Assume that $X_1 = \{\langle b_1, t_1\rangle, \ldots, \langle b_u, t_u\rangle\}$ and $X_2 = \{\langle d_1, s_1\rangle, \ldots, \langle d_v, s_v\rangle\}$ are two disjoint sets of rows of $\Phi(\mathcal{H}_1, \mathcal{H}_2)$ with $1 \le u \le w_1$, $1 \le v \le w_2$ and $desc(X_1) \cap desc(X_2) \neq \emptyset$.

$$\begin{array}{cr|cccccc}
 & \langle b_1, t_1\rangle = & a_{\phi_{b_1,1}(t_1)} & a_{\phi_{b_1,2}(t_1)} & \cdots & a_{\phi_{b_1,w_1w_2}(t_1)} & \alpha_{b_1} \\
 & \langle b_2, t_2\rangle = & a_{\phi_{b_2,1}(t_2)} & a_{\phi_{b_2,2}(t_2)} & \cdots & a_{\phi_{b_2,w_1w_2}(t_2)} & \alpha_{b_2} \\
X_1 & \vdots & \vdots & \vdots & & \vdots & \vdots \\
 & \langle b_u, t_u\rangle = & a_{\phi_{b_u,1}(t_u)} & a_{\phi_{b_u,2}(t_u)} & \cdots & a_{\phi_{b_u,w_1w_2}(t_u)} & \alpha_{b_u} \\
\hline
 & \langle d_1, s_1\rangle = & a_{\phi_{d_1,1}(s_1)} & a_{\phi_{d_1,2}(s_1)} & \cdots & a_{\phi_{d_1,w_1w_2}(s_1)} & \alpha_{d_1} \\
 & \langle d_2, s_2\rangle = & a_{\phi_{d_2,1}(s_2)} & a_{\phi_{d_2,2}(s_2)} & \cdots & a_{\phi_{d_2,w_1w_2}(s_2)} & \alpha_{d_2} \\
X_2 & \vdots & \vdots & \vdots & & \vdots & \vdots \\
 & \langle d_v, s_v\rangle = & a_{\phi_{d_v,1}(s_v)} & a_{\phi_{d_v,2}(s_v)} & \cdots & a_{\phi_{d_v,w_1w_2}(s_v)} & \alpha_{d_v}
\end{array}$$

The two sets of indices

$$\{b_1, b_2, \ldots, b_u\} \text{ and } \{d_1, d_2, \ldots, d_v\}$$

must have non-empty intersection since, if they are disjoint then from the $\{w_1, w_2\}$-separating property of $\mathcal{H}_2$, there exists a column that separates the following two sets of rows of $\mathcal{H}_2$:

$$\{\alpha_{b_1}, \alpha_{b_2}, \ldots, \alpha_{b_u}\} \text{ and } \{\alpha_{d_1}, \alpha_{d_2}, \ldots, \alpha_{d_v}\},$$

this column also separates the two sets of rows, X_1 and X_2, of $\Phi(\mathcal{H}_1, \mathcal{H}_2)$, which contradicts to the assumption that $desc(X_1) \cap desc(X_2) \neq \emptyset$. Therefore, if S_0 denotes the set of all ordered pairs (p, q) with $1 \le p \le u$ and $1 \le q \le v$, such that $b_p = d_q$, then S_0 is not empty.

Similar argument as in the proof of Theorem 11 shows that for each k, $1 \le k \le w_1 w_2$, the following two sets of indices

$$\{\phi_{b_1,k}(t_1), \phi_{b_2,k}(t_2), \ldots, \phi_{b_u,k}(t_u)\} \text{ and } \{\phi_{d_1,k}(s_1), \phi_{d_2,k}(s_2), \ldots, \phi_{d_v,k}(s_v)\}$$

have non-empty intersection. So if S_k denotes the set of all ordered pairs (p, q) with $1 \le p \le u$, $1 \le q \le v$ such that $\phi_{b_p,k}(t_p) = \phi_{d_q,k}(s_q)$ then S_k is not empty for each k, $1 \le k \le w_1 w_2$.

By the Pigeon Hole Principle, there must exist a pair (p, q) that belongs to at least two sets, say S_{k_1} and S_{k_2} with $k_1 \neq k_2$. Consider two cases, k_1 and k_2 are both non-zero, or one of k_1, k_2 is equal to zero.

Case 1. If k_1 and k_2 are non-zero then

$$\left\{ \begin{array}{lcl} \phi_{b_p,k_1}(t_p) & = & \phi_{d_q,k_1}(s_q) \\ \phi_{b_p,k_2}(t_p) & = & \phi_{d_q,k_2}(s_q) \end{array} \right. .$$

Thus, $t_p = s_q$ and $b_p = d_q$. Hence, $\langle b_p, t_p\rangle = \langle d_q, s_q\rangle \in X_1 \cap X_2$, contradiction.

Case 2. If one of k_1, k_2 is zero. Assume that $k_2 = 0$, then

$$\begin{cases} \phi_{b_p,k_1}(t_p) & = & \phi_{d_q,k_1}(s_q) \\ b_p & = & d_q \end{cases}$$

Since Φ is bijective, we have $t_p = s_q$. Hence, $\langle b_p, t_p\rangle = \langle d_q, s_q\rangle \in X_1 \cap X_2$, contradiction. ∎

Proof of Theorem 13. In this proof, we use the same notation as in the proof of Theorem 11.

We prove that $\Phi(\mathcal{H})$ is w-perfect by contradiction. Assume that $X = \{\langle b_1, t_1\rangle, \ldots, \langle b_u, t_u\rangle\}$ is a set of u distinct rows of $\Phi(\mathcal{H})$ with $1 \le u \le w$ such that no column of $\Phi(\mathcal{H})$ is one-to-one on X.

$$X \quad \begin{array}{lllll} \langle b_1, t_1\rangle = & a_{\phi_{b_1,1}(t_1)} & a_{\phi_{b_1,2}(t_1)} & \cdots & a_{\phi_{b_1,\binom{w}{2}+1}(t_1)} \\ \langle b_2, t_2\rangle = & a_{\phi_{b_2,1}(t_2)} & a_{\phi_{b_2,2}(t_2)} & \cdots & a_{\phi_{b_2,\binom{w}{2}+1}(t_2)} \\ \vdots & \vdots & \vdots & & \vdots \\ \langle b_u, t_u\rangle = & a_{\phi_{b_u,1}(t_u)} & a_{\phi_{b_u,2}(t_u)} & \cdots & a_{\phi_{b_u,\binom{w}{2}+1}(t_u)} \end{array}$$

For each k, $1 \le k \le \binom{w}{2} + 1$, the following indices

$$\phi_{b_1,k}(t_1), \phi_{b_2,k}(t_2), \ldots, \phi_{b_u,k}(t_u)$$

must not be all distinct since, if they are all distinct then from the w-perfect property of $\mathcal{H}$, there exists a column that is one-to-one on the following set of rows of $\mathcal{H}$:

$$\{a_{\phi_{b_1,k}(t_1)}, a_{\phi_{b_2,k}(t_2)}, \ldots, a_{\phi_{b_u,k}(t_u)}\},$$

this column is also one-to-one on the set X of rows of $\Phi(\mathcal{H})$, which contradicts to the assumption we made earlier.

For each k, $1 \le k \le \binom{w}{2} + 1$, let S_k denote the set of all unordered pairs $\{p, q\}$ with $1 \le p \ne q \le u$, such that $\phi_{b_p,k}(t_p) = \phi_{b_q,k}(t_q)$. From the above argument, S_k is not empty for any k.

Since there are $\binom{w}{2} + 1$ sets S_k and there are $\binom{u}{2} \le \binom{w}{2}$ unordered pairs $\{p, q\}$ with $1 \le p \ne q \le u$, it follows from Pigeon Hole Principle that there must exist a pair $\{p, q\}$ that belongs to at least two sets, say S_{k_1} and S_{k_2} with $k_1 \ne k_2$. We have,

$$\begin{cases} \phi_{b_p,k_1}(t_p) & = & \phi_{b_q,k_1}(t_q) \\ \phi_{b_p,k_2}(t_p) & = & \phi_{b_q,k_2}(t_q) \end{cases}$$

Thus, $t_p = t_q$ and $b_p = b_q$. Hence, $\langle b_p, t_p\rangle = \langle b_q, t_q\rangle$, this contradicts to the assumption that X contains u distinct rows. ∎

Proof of Theorem 14. In this proof, we use the same notation as in the proof of Theorem 12.

We prove that $\Phi(\mathcal{H}_1, \mathcal{H}_2)$ is w-perfect by contradiction. Assume that $X = \{\langle b_1, t_1\rangle, \ldots, \langle b_u, t_u\rangle\}$ is a set of u distinct rows of $\Phi(\mathcal{H}_1, \mathcal{H}_2)$ with $1 \le u \le w$ such that no column of $\Phi(\mathcal{H}_1, \mathcal{H}_2)$ is one-to-one on X.

$$X \quad \begin{array}{llllll} \langle b_1, t_1\rangle = & a_{\phi_{b_1,1}(t_1)} & a_{\phi_{b_1,2}(t_1)} & \cdots & a_{\phi_{b_1,\binom{w}{2}}(t_1)} & \alpha_{b_1} \\ \langle b_2, t_2\rangle = & a_{\phi_{b_2,1}(t_2)} & a_{\phi_{b_2,2}(t_2)} & \cdots & a_{\phi_{b_2,\binom{w}{2}}(t_2)} & \alpha_{b_2} \\ \vdots & \vdots & \vdots & & \vdots & \vdots \\ \langle b_u, t_u\rangle = & a_{\phi_{b_u,1}(t_u)} & a_{\phi_{b_u,2}(t_u)} & \cdots & a_{\phi_{b_u,\binom{w}{2}}(t_u)} & \alpha_{b_u} \end{array}$$

The following indices

$$b_1, b_2, \ldots, b_u$$

must not be all distinct since, if they are all distinct then from the w-perfect property of $\mathcal{H}_2$, there exists a column that is one-to-one on the following set of rows of $\mathcal{H}_2$:

$$\{\alpha_{b_1}, \alpha_{b_2}, \ldots, \alpha_{b_u}\},$$

this column is also one-to-one on the set X of rows of $\Phi(\mathcal{H}_1, \mathcal{H}_2)$, which contradicts to the assumption we made earlier. Therefore, if S_0 denotes the set of all unordered pairs $\{p, q\}$ with $1 \leq p \neq q \leq u$ such that $b_p = b_q$, then S_0 is not empty.

Similar argument as in the proof of Theorem 13 shows that for each k, $1 \leq k \leq \binom{w}{2}$, the following indices

$$\phi_{b_1,k}(t_1), \phi_{b_2,k}(t_2), \ldots, \phi_{b_u,k}(t_u)$$

must not be all distinct. So if S_k denotes the set of all unordered pairs $\{p, q\}$ with $1 \leq p \neq q \leq u$ such that $\phi_{b_p,k}(t_p) = \phi_{b_q,k}(t_q)$ then S_k is not empty for each k, $1 \leq k \leq \binom{w}{2}$.

By the Pigeon Hole Principle, there must exist a pair $\{p, q\}$ that belongs to at least two sets, say S_{k_1} and S_{k_2} with $k_1 \neq k_2$. Consider two cases, k_1 and k_2 are both non-zero, or one of k_1, k_2 is equal to zero.

Case 1. If k_1 and k_2 are non-zero then

$$\begin{cases} \phi_{b_p,k_1}(t_p) &= \phi_{b_q,k_1}(t_q) \\ \phi_{b_p,k_2}(t_p) &= \phi_{b_q,k_2}(t_q) \end{cases}.$$

Thus, $t_p = t_q$ and $b_p = b_q$. Hence, $\langle b_p, t_p \rangle = \langle b_q, t_q \rangle$, contradiction.

Case 2. If one of k_1, k_2 is zero. Assume that $k_2 = 0$, then

$$\begin{cases} \phi_{b_p,k_1}(t_p) &= \phi_{b_q,k_1}(t_q) \\ b_p &= b_q \end{cases}$$

Since Φ is bijective, we have $t_p = t_q$. Hence, $\langle b_p, t_p \rangle = \langle b_q, t_q \rangle$, contradiction. ■

References

[1] M. Atici, S.S. Magliveras, D.R. Stinson and W.D. Wei, *Some recursive constructions for perfect hash families,* Journal of Combinatorial Designs, 4 (1996), pp. 353-363.

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

[3] B. Chor, A. Fiat, M. Naor and B. Pinkas, *Tracing traitors,* IEEE Transactions on Information Theory, 46 (2000), pp. 480–491.

[4] A. Fiat and T. Tassa, *Dynamic traitor tracing,* Journal of Cryptology, 14 (2001), pp. 211–223.

[5] R. Safavi-Naini and Y. Wang, *Sequential traitor tracing,* in Advances in Cryptology (CRYPTO'00), Lecture Notes in Computer Science 1880, 2000, pp. 316–332.

[6] J. Staddon, D.R. Stinson and R. Wei, *Combinatorial properties of frameproof and traceability codes,* IEEE Transaction on Information Theory, 47 (2001), pp. 1042–1049.

[7] D.R. Stinson, Tran van Trung and R. Wei, *Secure frameproof codes, key distribution patterns, group testing algorithms and related structures,* Journal of Statistical Planning and Inference, 86 (2000), pp. 595–617.

[8] D. R. Stinson, R. Wei and L. Zhu, *New constructions for perfect hash families and related structures using combinatorial designs and codes,* Journal of Combinatorial Designs, 8 (2000), pp. 189–200.

[9] Tran van Trung and S. Martinosyan, *New constructions for IPP codes,* Designs, Codes and Cryptography, 35 (2005), pp. 227–239.