Generalized mix functions and orthogonal equitable rectangles

D.R. Stinson*
David R. Cheriton School of Computer Science
University of Waterloo
Waterloo, Ontario N2L 3G1, Canada
dstinson@uwaterloo.ca

June 8, 2007

Abstract

Ristenpart and Rogaway defined "mix" functions, which are used to mix inputs from two sets of equal size, and produce outputs from the same two sets, in an optimal way. These functions have a cryptographic application in the context of extending the domain of a block cipher. It was observed that mix functions could be constructed from orthogonal latin squares.

In this paper, we give a simple, scalable construction for mix functions. We also consider a generalization of mix functions, in which the two sets need not be of equal size. These generalized mix functions turn out to be equivalent to an interesting type of combinatorial design which has not previously been studied. We term these "orthogonal equitable rectangles" and we construct them for all possible parameter situations, with a small number of exceptions and possible exceptions.

1 Mix Functions

Mix functions were defined by Ristenpart and Rogaway [4] as follows. Let $|X| = r$. Suppose $f : X \times X \to X \times X$, and denote $f(A, B) = (f_L(A, B), f_R(A, B))$ for all $A, B \in X$. Suppose that the following properties are satisfied:

1. $f(\cdot, \cdot)$ is a permutation of $X \times X$
2. if $A \in X$ is fixed, then $f_L(A, \cdot)$ is a permutation of X
3. if $A \in X$ is fixed, then $f_R(A, \cdot)$ is a permutation of X
4. if $B \in X$ is fixed, then $f_L(\cdot, B)$ is a permutation of X
5. if $B \in X$ is fixed, then $f_R(\cdot, B)$ is a permutation of X

Then we say that f is a $\mathsf{mix}(r)$ function.

Roughly speaking, a mix function takes two inputs A and B from a set X of cardinality r and produces two outputs from the same set, in such a way that that the entire output is "balanced",

*research supported by NSERC discovery grant 203114-06

and either of the two outputs is balanced when one input is fixed. These are useful properties to ensure that the function "mixes" the two inputs in an optimal way when it creates the two outputs. For more details on a specific application to encryption schemes, see [4].

Suppose r is a positive integer. A *latin square of order* r is an $r \times r$ array, say L, where every entry is chosen from a r-set X, such that the following two properties are satisfied:

1. every symbol $x \in X$ occurs exactly once in each row of L
2. every symbol $x \in X$ occurs exactly once in each column of L.

Suppose that L and R are latin squares of order r on symbol sets X and X', respectively. L and R are *orthogonal* provided that, for every ordered pair $(x, x') \in X \times X'$, there is a unique cell C such that $L(C) = x$ and $R(C) = x'$. (Equivalently, the superposition of L and R yields every ordered pair of symbols in $X \times X'$.)

It was observed in [4] that $\mathsf{mix}(r)$ functions can be constructed from a pair of orthogonal latin squares of order r. In fact, the converse is also true; we have the following result.

Theorem 1.1. *Suppose that* $|X| = r$ *and* $f : X \times X \to X \times X$. *Denote* $f(A, B) = (f_L(A, B), f_R(A, B))$ *for all* $A, B \in X$. *Define two* $n \times n$ *arrays* $L = (\lambda_{A,B})$ *and* $R = (\rho_{A,B})$ *by the rules* $\lambda_{A,B} = f_L(A, B)$ *and* $\rho_{A,B} = f_R(A, B)$ *for all* A, B. *Then* f *is a* $\mathsf{mix}(r)$ *function if and only if* L *and* R *are orthogonal latin squares of order* r.

Proof. It is clear that properties 2 and 4 of a mix function correspond to L being a latin square; properties 3 and 5 of a mix function correspond to R being a latin square; and property 1 corresponds to L and R being orthogonal. □

Corollary 1.2. *[4] Let* r *be a positive integer. Then there exists a* $\mathsf{mix}(r)$ *function if and only if* $r \neq 2, 6$.

Proof. Bose, Shrikhande and Parker [1, 2] showed that orthogonal latin squares of order $r \geq 1$ exist if and only if $r \neq 2, 6$ (for a short proof, see [5, Section 6.8]). Apply Theorem 1.1. □

Example 1.1. *A* $\mathsf{mix}(4)$ *function, which we present as orthogonal latin squares of order 4:*

$$L = \begin{array}{|c|c|c|c|}\hline 0&1&2&3\\\hline 1&0&3&2\\\hline 2&3&0&1\\\hline 3&2&1&0\\\hline\end{array} \qquad R = \begin{array}{|c|c|c|c|}\hline 0&2&3&1\\\hline 1&3&2&0\\\hline 2&0&1&3\\\hline 3&1&0&2\\\hline\end{array}.$$

2 A Simple General Construction

The case of greatest cryptographic interest is when r is a power of 2, say $r = 2^k$. Here we have the following special case of Corollary 1.2.

Corollary 2.1. *[4] Let* k *be a positive integer. Then there exists a* $\mathsf{mix}(2^k)$ *function if and only if* $k \neq 1$.

A $\mathsf{mix}(2^k)$ function defined on the set $X = \{0,1\}^k$ can be viewed as an optimal method of mixing two bitstrings of length k. For the purposes of the applications described in [4], it would be useful to have an efficient construction for $\mathsf{mix}(2^k)$ functions for all $k \geq 2$. It was observed in [4] that the usual finite field construction for orthogonal latin squares of order 2^k is not suitable, due to the need to store irreducible polynomials to generate finite fields $\mathbb{F}_{2^k}$ for various values of k.

We will give a completely general construction for $\mathsf{mix}(2^k)$ functions based on $\mathsf{mix}(4)$ and $\mathsf{mix}(8)$ functions. We use the following simple recursive construction for mix functions.

Construction 2.1. *For $i = 1, 2$, suppose that $|X_i| = r_i$, and suppose that $f^i : X_i \times X_i \to X_i \times X_i$ is a $\mathsf{mix}(r_i)$ function, where $f^i(A_i, B_i) = (f^i_L(A_i, B_i), f^i_R(A_i, B_i))$, $i = 1, 2$. Let $X = X_1 \times X_2$ and define a function $f = f_1 \otimes f_2$, where $f : X \times X \to X \times X$, by the following rule:*

$$\begin{aligned} f((A_1, A_2), (B_1, B_2)) &= (f_L((A_1, A_2), (B_1, B_2)), f_R((A_1, A_2), (B_1, B_2))) \\ f_L((A_1, A_2), (B_1, B_2)) &= (f^1_L(A_1, B_1), f^2_L(A_2, B_2)) \\ f_R((A_1, A_2), (B_1, B_2)) &= (f^1_R(A_1, B_1), f^2_R(A_2, B_2)). \end{aligned}$$

Then f is a $\mathsf{mix}(r_1 r_2)$ function.

Remark. Construction 2.1 is basically the classical direct (i.e., Kronecker) product construction for orthogonal latin squares (see, for example, [5, Theorem 6.27]), translated into the language of mix functions.

Now, we need to start with "nice" $\mathsf{mix}(4)$ and $\mathsf{mix}(8)$ functions. As observed in [4], it is easy to construct a $\mathsf{mix}(2^k)$ function defined on the finite field $\mathbb{F}_{2^k}$. Let $p(z) \in \mathbb{Z}_2[z]$ be an irreducible polynomial of degree k. Then $\mathbb{F}_{2^k} = \mathbb{Z}_2[z]/(p(z))$. Let $\alpha \in \mathbb{F}_{2^k}$ be a root of $p(z)$. Then the following formulas provide one way to obtain a mix function (where $x, y \in \mathbb{F}_{2^k}$):

$$f_L(x, y) = x + y \tag{1}$$
$$f_R(x, y) = x + \alpha y. \tag{2}$$

Note that all arithmetic is done in the field $\mathbb{F}_{2^k}$. Now, if we represent field elements with respect to the polynomial basis $\{\alpha^{k-1}, \ldots, \alpha^1, 1\}$, then we can define these mix function on bitstrings of length k.

In order to apply the formulas (1) and (2), it is necessary only to store the mapping $y \mapsto \alpha y$ as a mapping (actually a permutation) of the bitstrings of length k. The operation "+" in the field is the same as an exclusive-or operation performed on two bitstrings; we denote this operation by "$\oplus$".

We are building all possible mix functions from $\mathsf{mix}(4)$ and $\mathsf{mix}(8)$ functions, so only need to work out the relevant formulas in $\mathbb{F}_4$ and $\mathbb{F}_8$. We can generate $\mathbb{F}_4$ using the polynomial $z^2 + z + 1$, and $\mathbb{F}_8$ can be generated from the polynomial $z^3 + z + 1$. The permutations $y \mapsto \alpha y$ are recorded as the following permutations π_2 and π_3 of $\{0,1\}^2$ and $\{0,1\}^3$, respectively:

x	00	01	10	11
$\pi_2(x)$	00	10	11	01

x	000	001	010	011	100	101	110	111
$\pi_3(x)$	000	010	100	110	011	001	111	101

Now we can describe the resulting mix functions. Given $A = (A_1, \ldots, A_k) \in \{0,1\}^k$ and $B = (B_1, \ldots, B_k) \in \{0,1\}^k$, we show how to compute $(C, D) = (f_L(A,B), f_R(A,B))$, where $C = (C_1, \ldots, C_k) \in \{0,1\}^k$ and $D = (D_1, \ldots, D_k) \in \{0,1\}^k$.

First we consider the case where k is even, say $k = 2\ell$. Basically we "process" A and B two bits at a time using the $\mathsf{mix}(4)$ function based on π_2. For $1 \le i \le \ell$, we define

$$\begin{aligned} C_{2i-1}C_i &= A_{2i-1}A_i \oplus B_{2i-1}B_i \\ D_{2i-1}D_i &= A_{2i-1}A_i \oplus \pi_2(B_{2i-1}B_i). \end{aligned}$$

When k is odd, say $k = 2\ell + 1$, we proceed in much the same way, except that the last three bits are handled slightly differently, using the $\mathsf{mix}(8)$ function based on π_3. For $1 \le i \le \ell - 1$, we define

$$\begin{aligned} C_{2i-1}C_i &= A_{2i-1}A_i \oplus B_{2i-1}B_i \\ D_{2i-1}D_i &= A_{2i-1}A_i \oplus \pi_2(B_{2i-1}B_i). \end{aligned}$$

Then, define

$$\begin{aligned} C_{2\ell-1}C_{2\ell}C_{2\ell+1} &= A_{2\ell-1}A_{2\ell}A_{2\ell+1} \oplus B_{2\ell-1}B_{2\ell}B_{2\ell+1} \\ D_{2\ell-1}D_{2\ell}D_{2\ell+1} &= A_{2\ell-1}A_{2\ell}A_{2\ell+1} \oplus \pi_3(B_{2\ell-1}B_{2\ell}B_{2\ell+1}). \end{aligned}$$

The complexity of evaluating a $\mathsf{mix}(2^k)$ function using our approach is $O(k)$, and we require only $O(1)$ memory to do so. This is clearly optimal.

3 Generalized Mix Functions

In this section, we introduce a generalized type of mix function, where we mix inputs from two sets of (possibly) different sizes. Let $|X| = r$ and $|X'| = r'$. Suppose $f : X \times X' \to X \times X'$, and denote $f(A,B) = (f_L(A,B), f_R(A,B))$ for all $A, B \in X$. Suppose that the following properties are satisfied:

1. $f(\cdot,\cdot)$ is a permutation of $X \times X'$
2. if $A, C \in X$ are fixed, then $f_L(A,B) = C$ has either $\lceil \frac{r'}{r} \rceil$ or $\lfloor \frac{r'}{r} \rfloor$ solutions for $B \in X'$
3. if $A \in X$ is fixed, then $f_R(A,\cdot)$ is a permutation of X'
4. if $B \in X'$ is fixed, then $f_L(\cdot,B)$ is a permutation of X
5. if $B, D \in X'$ are fixed, $f_R(A,B) = D$ has either $\lceil \frac{r}{r'} \rceil$ or $\lfloor \frac{r}{r'} \rfloor$ solutions for $A \in X$.

Then we say that f is a $\mathsf{gmix}(r, r')$ function.

Suppose r, c and v are positive integers. We define an *equitable* $(r, c; v)$*-rectangle* to be an $r \times c$ array, say L, where every entry is chosen from a v-set X, such that the following two properties are satisfied:

1. every symbol $x \in X$ occurs either $\lceil \frac{c}{v} \rceil$ or $\lfloor \frac{c}{v} \rfloor$ times in each row of L
2. every symbol $x \in X$ occurs either $\lceil \frac{r}{v} \rceil$ or $\lfloor \frac{r}{v} \rfloor$ times in each column of L.

An equitable $(r, c; v)$-rectangle is *row-regular* if $v|c$, and it is *column-regular* if $v|r$. It is *regular* if it is both row- and column-regular. In a row-regular $(r, c; v)$-rectangle, every symbol occurs exactly c/v times in each row; in a column-regular $(r, c; v)$-rectangle, every symbol occurs exactly r/v times in each column.

An equitable $(r, c; c)$-rectangle with $r \leq c$ is known as a *latin rectangle*. A latin rectangle is row-regular. A latin rectangle with $r = c$ is the same thing as a latin square of order r. A latin square is regular.

Suppose that L is an equitable $(r, c; v)$-rectangle on symbol set X and R is an equitable $(r, c; v')$-rectangle on symbol set X', where $rc = vv'$. We say that L and R are *orthogonal* provided that, for every ordered pair $(x, x') \in X \times X'$, there is a unique cell C such that $L(C) = x$ and $R(C) = x'$. (Equivalently, the superposition of L and R yields every ordered pair of symbols in $X \times X'$.) It is easy to see that orthogonal equitable $(r, r; r)$-rectangles are identical to orthogonal latin squares of order r.

The next theorem is a straightforward generalization of Theorem 1.1.

Theorem 3.1. *Let $|X| = r$ and $|X'| = r'$, where $r \leq r'$. Suppose $f : X \times X' \to X \times X'$, and denote $f(A, B) = (f_L(A, B), f_R(A, B))$ for all $A, B \in X$. Define two $n \times n$ arrays $L = (\lambda_{A,B})$ and $R = (\rho_{A,B})$ by the rules $\lambda_{A,B} = f_L(A, B)$ and $\rho_{A,B} = f_R(A, B)$ for all A, B. Then f is a $\mathsf{gmix}(r, r')$ function if and only if L is an equitable $(r, r'; r)$-rectangle, R is an equitable $(r, r'; r')$-rectangle, and L and R are orthogonal.*

A $\mathsf{gmix}(r, r')$ function with $r \leq r'$ is said to be *row-regular* if the associated equitable $(r, r'; r)$-rectangle is row-regular (this is equivalent to the condition that $r|r'$).

Example 3.1. *A (row-regular) $\mathsf{gmix}(2, 4)$ function, which we present as an equitable $(2, 4; 2)$-rectangle and an equitable $(2, 4; 4)$-rectangle, such that the two rectangles are orthogonal:*

$$L = \begin{array}{|c|c|c|c|} \hline 0 & 1 & 0 & 1 \\ \hline 1 & 0 & 1 & 0 \\ \hline \end{array} \quad R = \begin{array}{|c|c|c|c|} \hline 0 & 1 & 2 & 3 \\ \hline 2 & 3 & 0 & 1 \\ \hline \end{array}.$$

The following simple lemma shows that it is sufficient to consider only $\mathsf{gmix}(r, r')$ functions with $r \leq r'$.

Lemma 3.2. *There exists a $\mathsf{gmix}(r, r')$ function if and only if there exists a $\mathsf{gmix}(r', r)$ function.*

It is easy to see that a $\mathsf{gmix}(r, r)$ function is the same thing as a $\mathsf{mix}(r)$ function. Therefore we have the following consequence of Corollary 1.2.

Lemma 3.3. *Suppose r is a positive integer. Then there exists a $\mathsf{gmix}(r, r)$ function if and only if $r \neq 2, 6$.*

3.1 Some Constructions

In this section, we present some recursive constructions for $\mathsf{gmix}(r, r')$ functions with $r < r'$. In most of these constructions, it will be fairly obvious that the required properties are satisfied. The only property that sometimes causes difficulty is the requirement that every symbol occurs either $\lceil \frac{r'}{r} \rceil$ or $\lfloor \frac{r'}{r} \rfloor$ times in each row of L, which is the equitable $(r, r'; r)$-rectangle that is being constructed. In order to ensure that this property is satisfied, we sometimes need to ensure that one or both of the hypothesized gmix functions used for a given construction are row-regular.

Construction 3.1 (Sum Construction). *Let r, r_1, r_2 be positive integers. Suppose there exists a $\mathsf{gmix}(r, r_1)$ function and a row-regular $\mathsf{gmix}(r, r_2)$ function. Then there exists a $\mathsf{gmix}(r, r_1 + r_2)$ function.*

Proof. Let L_i and R_i be the rectangles associated with a $\mathsf{gmix}(r, r_i)$ function, for $i = 1, 2$. We will stipulate that L_1 and L_2 are constructed in symbol set X of size r, R_1 is constructed on symbol set X_1 of size r_1, and R_2 is constructed on symbol set X_2 of size r_2, where $X_1 \cap X_2 = \emptyset$. Then define $X = X_1 \cup X_2$, $L = \boxed{L_1 \mid L_2}$ and $R = \boxed{R_1 \mid R_2}$. □

Suppose L is an equitable $(r, c; v)$-rectangle with $r \leq c$ and $r \leq v$. A *transversal* of L is a set T of r cells of L such that the following properties are satisfied:

1. each row of L contains one cell in T,
2. the cells in T occur in r distinct columns of L (this requires $r \leq c$), and
3. the cells in T contain r distinct symbols (this requires $r \leq v$).

Two transversals of L, say T and T', are said to be *disjoint* if T and T' contain no cells in common.

Suppose L is an equitable $(r, c; v)$-rectangle and R is an equitable $(r, c; v')$-rectangle, where $r \leq c$, $r \leq v$ and $r \leq v'$. A *common transversal* of L and R is a set T of r cells such that T is a transversal of both L and R.

Construction 3.2 (Projection Construction). *Suppose there are orthogonal latin squares of order r containing d disjoint common transversals. Then there exists a $\mathsf{gmix}(r, r + d)$ function.*

Proof. Let L and R be the hypothesized orthogonal latin squares of order r, and let $T_1, T_2, \ldots, T_d$ be the hypothesized common transversals. For $1 \leq j \leq d$, project each cell of T_d in L onto a new column and project each cell of T_j in R onto a new column. Then replace the contents of every cell of T_d in R by a new symbol ∞_j. □

Example 3.2. *We begin with the $\mathsf{mix}(4)$ function presented in Example 1.1:*

$$L = \begin{array}{|c|c|c|c|}\hline 0&1&2&3\\\hline 1&0&3&2\\\hline 2&3&0&1\\\hline 3&2&1&0\\\hline\end{array} \quad R = \begin{array}{|c|c|c|c|}\hline 0&2&3&1\\\hline 1&3&2&0\\\hline 2&0&1&3\\\hline 3&1&0&2\\\hline\end{array}.$$

These are orthogonal latin squares of order 4 that have four disjoint common transversals, which are indicated in the following array T:

$$T = \begin{array}{|c|c|c|c|}\hline 1&2&3&4\\\hline 3&4&1&2\\\hline 4&3&2&1\\\hline 2&1&4&3\\\hline\end{array}.$$

For $1 \le j \le 4$, T_j consists of all the cells in T containing the symbol j. Suppose we take $d = 2$, and project the transversals T_1 and T_2. Then we obtain a $\mathsf{gmix}(4,6)$ *function:*

0	1	2	3	0	1
1	0	3	2	3	2
2	3	0	1	1	0
3	2	1	0	2	3

∞_1	∞_2	3	1	0	2
1	3	∞_1	∞_2	2	0
2	0	∞_2	∞_1	3	1
∞_2	∞_1	0	2	1	3

The following result is well-known (see, for example, [3]).

Theorem 3.4. *There exist two orthogonal latin squares of order r containing r disjoint common transversals if and only if there exist three mutually orthogonal latin squares of order r.*

It is known that there exist three orthogonal latin squares of order r if $r \notin \{2, 3, 6, 10\}$ (see [6]). Thus we have the following corollary of Theorem 3.2.

Corollary 3.5. *Suppose that $r \ge 4$ is a positive integer, $r \neq 6, 10$. Then there exists a* $\mathsf{gmix}(r, r+d)$ *function for $0 \le d \le r$.*

Construction 3.2 can be generalized by starting with a row-regular generalized mix function, provided that the set of disjoint common transversals satisfies a suitable property. Suppose $T_1, \ldots, T_d$ are disjoint transversals in an equitable $(r, r'; r)$-rectangle L with $r \le r'$. These d transversals are *compatible* if, within any row of L, the cells in $T_1 \cup \cdots \cup T_d$ together contain every symbol either $\lceil \frac{d}{r} \rceil$ or $\lfloor \frac{d}{r} \rfloor$ times. A set of d compatible disjoint common transversals for a $\mathsf{gmix}(r, r')$ function is said to be *compatible* if the d transversals are compatible in the associated equitable $(r, r'; r)$-rectangle.

Construction 3.3 (Generalized Projection Construction). *Let r, r' be positive integers. Suppose there is a row-regular* $\mathsf{gmix}(r, r')$ *function having d compatible disjoint common transversals. Then there exists a* $\mathsf{gmix}(r, r' + d)$ *function.*

It is easy to verify that the standard direct (Kronecker) product of row-regular generalized mix functions will yield a generalized mix funciton.

Construction 3.4 (Direct Product Construction). *Suppose r_1, r_1', r_2 and r_2' are positive integers. Suppose there is a row-regular* $\mathsf{gmix}(r_i, r_i')$ *function, $i = 1, 2$. Then there is a row-regular* $\mathsf{gmix}(r_1 r_2, r_1' r_2')$ *function.*

Proof. For $i = 1, 2$, suppose that $|X_i| = r_i$, $|X_i'| = r_i'$ and $f^i : X_i \times X_i' \to X_i \times X_i'$ is a $\mathsf{gmix}(r_i, r_i')$ function, where $f^i(A_i, B_i) = (f_L^i(A_i, B_i), f_R^i(A_i, B_i))$, $i = 1, 2$. Let $X = X_1 \times X_2$, $X' = X_1' \times X_2'$ and define a function $f = f_1 \otimes f_2$, where $f : X \times X' \to X \times X'$, by the following rule:

$$\begin{aligned} f((A_1, A_2), (B_1, B_2)) &= (f_L((A_1, A_2), (B_1, B_2)), f_R((A_1, A_2), (B_1, B_2))) \\ f_L((A_1, A_2), (B_1, B_2)) &= (f_L^1(A_1, B_1), f_L^2(A_2, B_2)) \\ f_R((A_1, A_2), (B_1, B_2)) &= (f_R^1(A_1, B_1), f_R^2(A_2, B_2)). \end{aligned}$$

Then f is a $\mathsf{gmix}(r_1 r_2, r_1' r_2')$ function. □

4 Existence Results

In this section, we use the constructions from the previous section to construct all possible generalized mix functions, with a few exceptions and a few possible exceptions.

4.1 The Case $r = 1$

Theorem 4.1. *There exists a* $\mathsf{gmix}(1, r')$ *function for all* $r' \geq 1$.

Proof. Define L and R as follows:

$$L = \begin{array}{|c|c|c|c|} \hline 0 & 0 & \cdots & 0 \\ \hline \end{array} \quad R = \begin{array}{|c|c|c|c|} \hline 0 & 1 & \cdots & r'-1 \\ \hline \end{array}.$$

□

4.2 The Case $r = 2$

Lemma 4.2. *There does not exist a* $\mathsf{gmix}(2, 2)$ *or a* $\mathsf{gmix}(2, 3)$ *function.*

Proof. A $\mathsf{gmix}(2, 2)$ function does not exist (Lemma 3.3). Also, it is easy to verify that a $\mathsf{gmix}(2, 3)$ function does not exist. □

Lemma 4.3. *Suppose* $r' \geq 4$ *is an even integer. Then there exists a* $\mathsf{gmix}(2, r')$ *function.*

Proof. Define L and R as follows:

$$L = \begin{array}{|c|c|c|c|c|c|c|c|c|} \hline 0 & 1 & 0 & 1 & \cdots & 0 & 1 & 0 & 1 \\ \hline 1 & 0 & 1 & 0 & \cdots & 1 & 0 & 1 & 0 \\ \hline \end{array} \quad R = \begin{array}{|c|c|c|c|c|c|c|c|c|} \hline 0 & 1 & 2 & 3 & \cdots & r'-4 & r'-3 & r'-2 & r'-1 \\ \hline 2 & 3 & 4 & 5 & \cdots & r'-2 & r'-1 & 0 & 1 \\ \hline \end{array}.$$

□

Lemma 4.4. *Suppose* $r' \geq 5$ *is an odd integer. Then there exists a* $\mathsf{gmix}(2, r')$ *function.*

Proof. Define L and R as follows:

$$L = \begin{array}{|c|c|c|c|c|c|c|c|c|} \hline 0 & 1 & 0 & 1 & \cdots & 1 & 0 & 1 & 0 \\ \hline 1 & 0 & 1 & 0 & \cdots & 0 & 1 & 0 & 1 \\ \hline \end{array} \quad R = \begin{array}{|c|c|c|c|c|c|c|c|c|} \hline 0 & 1 & 2 & 3 & \cdots & r'-4 & r'-3 & r'-2 & r'-1 \\ \hline 2 & 3 & 4 & 5 & \cdots & r'-2 & r'-1 & 1 & 0 \\ \hline \end{array}.$$

□

Example 4.1. *A* $\mathsf{gmix}(2, 5)$ *function:*

$$L = \begin{array}{|c|c|c|c|c|} \hline 0 & 1 & 0 & 1 & 0 \\ \hline 1 & 0 & 1 & 0 & 1 \\ \hline \end{array} \quad R = \begin{array}{|c|c|c|c|c|} \hline 0 & 1 & 2 & 3 & 4 \\ \hline 2 & 3 & 4 & 1 & 0 \\ \hline \end{array}.$$

Combining the lemmas in this section, we obtain the following.

Theorem 4.5. *Suppose* $r' \geq 2$. *Then there exists a* $\mathsf{gmix}(2, r')$ *function if and only if* $r' \neq 2, 3$.

4.3 The Case $r = 3$

The following lemma can be verified by an exhaustive search.

Lemma 4.6. *There does not exist a* $\mathsf{gmix}(3,4)$ *function.*

Lemma 4.7. *There exists a* $\mathsf{gmix}(3,3)$*, a* $\mathsf{gmix}(3,5)$ *and a* $\mathsf{gmix}(3,7)$ *function.*

Proof. A a $\mathsf{gmix}(3,3)$ function is equivalent to orthogonal latin squares of order 3. We present examples of $\mathsf{gmix}(3,5)$ and $\mathsf{gmix}(3,7)$ functions now.

A $\mathsf{gmix}(3,5)$ function:

$$L = \begin{array}{|c|c|c|c|c|}\hline 0&0&1&1&2\\\hline 1&2&0&2&1\\\hline 2&1&2&0&0\\\hline\end{array} \quad R = \begin{array}{|c|c|c|c|c|}\hline 0&1&4&2&3\\\hline 3&4&2&0&1\\\hline 2&0&1&3&4\\\hline\end{array}.$$

A $\mathsf{gmix}(3,7)$ function:

$$L = \begin{array}{|c|c|c|c|c|c|c|}\hline 0&0&0&1&2&1&2\\\hline 1&1&2&0&0&2&1\\\hline 2&2&1&2&1&0&0\\\hline\end{array} \quad R = \begin{array}{|c|c|c|c|c|c|c|}\hline 0&1&2&4&5&6&3\\\hline 2&0&6&3&4&1&5\\\hline 4&2&1&0&3&5&6\\\hline\end{array}.$$

□

Theorem 4.8. *Suppose* $r' \geq 3$*. Then there exists a* $\mathsf{gmix}(3,r')$ *function if and only if* $r' \neq 4$*.*

Proof. We have already noted that a $\mathsf{gmix}(3,4)$ function does not exist. Suppose $r' \geq 3$, $r' \neq 4$. Write $r' = 3q + s$, where $q \geq 0$ and $s \in \{3,5,7\}$. Then apply the Sum Construction (Construction 3.1), using q copies of a $\mathsf{gmix}(3,3)$ function and one copy of a $\mathsf{gmix}(3,s)$ function (these exist by Lemma 4.7). □

4.4 The Case $r = 6$

First, we construct a row-regular $\mathsf{gmix}(6,12)$ function using Construction 3.4.

Example 4.2. *The direct product* $\mathsf{gmix}(3,3) \otimes \mathsf{gmix}(2,4)$ *yields a row-regular* $\mathsf{gmix}(6,12)$ *function:*

$$L = \begin{array}{|c|c|c|c|c|c|c|c|c|c|c|c|}\hline 0&1&2&3&4&5&0&1&2&3&4&5\\\hline 2&0&1&5&3&4&2&0&1&5&3&4\\\hline 1&2&0&4&5&3&1&2&0&4&5&3\\\hline 3&4&5&0&1&2&3&4&5&0&1&2\\\hline 5&3&4&2&0&1&5&3&4&2&0&1\\\hline 4&5&3&1&2&0&4&5&3&1&2&0\\\hline\end{array}$$

and

$$R = \begin{array}{|c|c|c|c|c|c|c|c|c|c|c|c|}\hline 0&1&2&9&10&11&6&7&8&3&4&5\\\hline 2&0&1&11&9&10&8&6&7&5&3&4\\\hline 1&2&0&10&11&9&7&8&6&4&5&3\\\hline 6&7&8&3&4&5&0&1&2&9&10&11\\\hline 8&6&7&5&3&4&2&0&1&11&9&10\\\hline 7&8&6&4&5&3&1&2&0&10&11&9\\\hline\end{array}.$$

This $\mathsf{gmix}(6,12)$ *function contains* 12 *disjoint common transversals:*

$$T = \begin{array}{|cccccccccccc|}\hline 1&2&3&4&5&6&7&8&9&10&11&12\\ 8&9&7&11&10&12&2&3&1&5&6&4\\ 10&11&12&1&2&3&4&5&6&7&8&9\\ 11&10&12&2&3&1&5&6&4&8&9&7\\ 7&8&9&10&11&12&1&2&3&4&5&6\\ 2&3&1&5&6&4&8&9&7&11&10&12\\ \hline\end{array}.$$

For $1 \le j \le 12$, T_j *consists of all the cells in* T *containing the symbol* j.

Theorem 4.9. *There does not exist a* $\mathsf{gmix}(6,6)$ *function. Further, there exists a* $\mathsf{gmix}(6,r')$ *function for all* $r' \ge 12$.

Proof. The nonexistence of a $\mathsf{gmix}(6,6)$ function was already noted in Lemma 3.3.

For $12 \le r' \le 24$, we will apply the Generalized Projection Construction (Construction 3.3), starting with the $\mathsf{gmix}(6,12)$ function constructed in Example 4.2. Note that it is straightforward to verify that the d transversals $T_1, \ldots, T_d$ defined in Example 4.2 are compatible, for any d such that $1 \le d \le 12$.

Finally, for $r' \ge 25$, write $r' = 12q + s$, where $q \ge 1$ and $12 \le s \le 23$. Then apply the Sum Construction (Construction 3.1), using q copies of a $\mathsf{gmix}(6,12)$ function and one copy of a $\mathsf{gmix}(6,s)$ function. □

4.5 The Case $r = 10$

Lemma 4.10. *There exists a* $\mathsf{gmix}(10,r')$ *function for* $10 \le r' \le 14$.

Proof. There exist orthogonal latin squares of order 10 containing four disjoint common transversals (see [3, p. 530]). Apply the Projection Construction (Construction 3.2). □

Next, we construct a row-regular $\mathsf{gmix}(10,20)$ function using Construction 3.4.

Example 4.3. *The direct product* $\mathsf{gmix}(5,5) \otimes \mathsf{gmix}(2,4)$ *yields a row-regular* $\mathsf{gmix}(10,20)$ *function:*

$$L = \begin{array}{|cccccccccccccccccccc|}\hline 0&1&2&3&4&5&6&7&8&9&0&1&2&3&4&5&6&7&8&9\\ 1&2&3&4&0&6&7&8&9&5&1&2&3&4&0&6&7&8&9&5\\ 2&3&4&0&1&7&8&9&5&6&2&3&4&0&1&7&8&9&5&6\\ 3&4&0&1&2&8&9&5&6&7&3&4&0&1&2&8&9&5&6&7\\ 4&0&1&2&3&9&5&6&7&8&4&0&1&2&3&9&5&6&7&8\\ 5&6&7&8&9&0&1&2&3&4&5&6&7&8&9&0&1&2&3&4\\ 6&7&8&9&5&1&2&3&4&0&6&7&8&9&5&1&2&3&4&0\\ 7&8&9&5&6&2&3&4&0&1&7&8&9&5&6&2&3&4&0&1\\ 8&9&5&6&7&3&4&0&1&2&8&9&5&6&7&3&4&0&1&2\\ 9&5&6&7&8&4&0&1&2&3&9&5&6&7&8&4&0&1&2&3\\ \hline\end{array}$$

and

$R =$

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
2	3	4	0	1	7	8	9	5	6	12	13	14	10	11	17	18	19	15	16
4	0	1	2	3	9	5	6	7	8	14	10	11	12	13	19	15	16	17	18
1	2	3	4	0	6	7	8	9	5	11	12	13	14	10	16	17	18	19	15
3	4	0	1	2	8	9	5	6	7	13	14	10	11	12	18	19	15	16	17
10	11	12	13	14	15	16	17	18	19	0	1	2	3	4	5	6	7	8	9
12	13	14	10	11	17	18	19	15	16	2	3	4	0	1	7	8	9	5	6
14	10	11	12	13	19	15	16	17	18	4	0	1	2	3	9	5	6	7	8
11	12	13	14	10	16	17	18	19	15	1	2	3	4	0	6	7	8	9	5
13	14	10	11	12	18	19	15	16	17	3	4	0	1	2	8	9	5	6	7

This $\mathsf{gmix}(10, 20)$ *function contains* 20 *disjoint common transversals:*

$T =$

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
5	1	2	3	4	10	6	7	8	9	15	11	12	13	14	20	16	17	18	19
15	11	12	13	14	20	16	17	18	19	5	1	2	3	4	10	6	7	8	9
19	20	16	17	18	4	5	1	2	3	9	10	6	7	8	14	15	11	12	13
6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	1	2	3	4	5
14	15	11	12	13	19	20	16	17	18	4	5	1	2	3	9	10	6	7	8
4	5	1	2	3	9	10	6	7	8	14	15	11	12	13	19	20	16	17	18
2	3	4	5	1	7	8	9	10	6	12	13	14	15	11	17	18	19	20	16
20	16	17	18	19	5	1	2	3	4	10	6	7	8	9	15	11	12	13	14
9	10	6	7	8	14	15	11	12	13	19	20	16	17	18	4	5	1	2	3

For $1 \leq j \leq 20$, T_j *consists of all the cells in* T *containing the symbol* j.

Lemma 4.11. *There exists a* $\mathsf{gmix}(10, r')$ *function for all* $r' \geq 20$.

Proof. For $20 \leq r' \leq 40$, apply the Generalized Projection Construction (Construction 3.3), starting with the $\mathsf{gmix}(10, 20)$ function constructed in Example 4.3. Note that it is straightforward to verify that the d transversals $T_1, \ldots, T_d$ defined in Example 4.3 are compatible, for any d such that $1 \leq d \leq 20$.

For $r' \geq 41$, write $r' = 20q + s$ with $q \geq 1$ and $20 \leq s \leq 39$. Then apply the Sum Construction (Construction 3.1), using q copies of a $\mathsf{gmix}(10, 20)$ function and one copy of a $\mathsf{gmix}(10, s)$ function. □

Combining Lemmas 4.10 and 4.11, we obtain the following.

Theorem 4.12. *Suppose* $r' \geq 10$. *If* $r' \notin \{15, 16, 17, 18, 19\}$, *then there is a* $\mathsf{gmix}(10, r')$ *function.*

4.6 The General Case

Theorem 4.13. *Suppose* $r' \geq r \geq 4$, $r \neq 6, 10$. *Then there exists a* $\mathsf{gmix}(r, r')$ *function.*

Proof. For $r \leq r' \leq 2r$, apply Corollary 3.5. For $r' \geq 2r + 1$, write $r' = qr + s$ with $q \geq 1$ and $r \leq s \leq 2r - 1$. Then apply the Sum Construction (Construction 3.1), using q copies of a $\mathsf{gmix}(r, r)$ function and one copy of a $\mathsf{gmix}(r, s)$ function. □

Gathering together all our results (Theorems 4.1, 4.5, 4.8, 4.9, 4.12 and 4.13), we have our Main Theorem. In this theorem, E denotes the set of (definite) exceptions and P denotes the set of possible exceptions.

Theorem 4.14 (Main Theorem). *Define*

$$E = \{(2,2), (2,3), (3,4), (6,6)\}$$

and

$$P = \{(6,j) : 7 \leq j \leq 11\} \cup \{(10,j) : 15 \leq j \leq 19\}.$$

Let $1 \leq r \leq r'$. Then there exists a $\mathsf{gmix}(r,r')$ function if $(r,r') \notin E \cup P$, and there does not exist a $\mathsf{gmix}(r,r')$ function if $(r,r') \in E$.

4.7 Parameters of Cryptographic Interest

The $\mathsf{gmix}(r,r')$ functions of potential cryptographic interest are those where r and r' are both powers of two. As a corollary of our existence results, we have the following theorem.

Corollary 4.15. *Let k, ℓ be positive integers. Then there exists a $\mathsf{gmix}(2^k, 2^\ell)$ function if and only if $(k,\ell) \neq (1,1)$.*

Even though the general existence results require several constructions, Corollary 4.15 can be proven using Corollary 2.1 and the Sum Construction (Construction 3.1) for the cases $k \geq 2$, and Lemma 4.3 for the case $k = 1$. It is easily seen that this leads to an efficient, scalable construction for these generalized mix functions.

5 Conclusion

The study of mix functions is motivated by a cryptographic application from [4]. We have defined generalized mix functions in this paper. These functions may have potential cryptographic applications, and they are of independent interest as a combinatorial problem. We have given an almost complete solution to the existence question for generalized mix functions (modulo a small number of possible exceptions).

An interesting open problem is to find necessary and sufficient conditions for there to exist an equitable $(r, c; v)$-rectangle and an equitable $(r, c; v')$-rectangle, such that the two rectangles are orthogonal.

References

[1] R.C. Bose and S.S. Shrikhande. On the construction of sets of mutually orthogonal Latin squares and the falsity of a conjecture of Euler. *Transactions of the American Mathematical Society* **95** (1960), 191–209.

[2] R.C. Bose, S.S. Shrikhande, and E.T. Parker. Further results on the construction of mutually orthogonal Latin squares and the falsity of Euler's conjecture. *Canadian Journal of Mathematics* **12** (1960), 189–203.

[3] C.J. Colbourn and J.H. Dinitz. *The CRC Handbook of Combinatorial Designs, Second Edition*, Chapman & Hall/CRC, 2007.

[4] T. Ristenpart and P. Rogaway. How to Enrich the Message Space of a Cipher. *Lecture Notes in Computer Science*, to appear (Fast Software Encryption, FSE 2007).

[5] D.R. Stinson. *Combinatorial Designs: Constructions and Analysis*, Springer, 2004.

[6] W.D. Wallis. Three orthogonal latin squares. *Congressus Numerantium* **42** (1984), 69–86.