Contents lists available at Science-Gate

International Journal of Advanced and Applied Sciences

Journal homepage: http://www.science-gate.com/IJAAS.html

# Fuzzy linear congruence and linear fuzzy integers

Frank Rogers *

*Department of Mathematics, University of West Alabama, Livingston, Alabama 35470, USA*

ARTICLE INFO

*Article history:*
Received 15 April 2016
Received in revised form
5 June 2016
Accepted 5 June 2016

*Keywords:*
Linear fuzzy real number
Liner fuzzy integers
Fuzzy linear congruence
Number theory
Cryptography

ABSTRACT

Uncertainty arises in fields such as computer science, physics, finance and engineering just to name a few such areas. Fuzzy sets, Fuzzy arithmetic, and Fuzzy operations are useful tools for dealing with uncertainty. This article presents the application of a system of a hybrid set of fuzzy numbers known as Linear Fuzzy Integers to the solution of Fuzzy Linear Congruence. The Linear Fuzzy Integers are presented after an illustration of the parent set, Linear Fuzzy Reals. Fuzzy Linear Congruences and the validity of its solution in the Linear Fuzzy Integer environment is shown by both illustration and verified by proof.



## 1. Introduction

Modular arithmetic is used in many applications. Linear congruence, a specific modulo equation, is often used in cryptography. Because of this, finding solutions to crisp linear congruence has been studied extensively. However, uncertainty arises because of human error, computer error or simply because of the unknown. According to Schjaer-Johnson (2002), when only uncertain information is available decision-making calls for more complex methods of representation and calculation. Thus in cryptography where uncertain information occurs, fuzzy numbers is a useful tool. In some cases, our use of fuzzy numbers may simply provide for greater efficiency. For instance, Golic (2005) states that linear recurring truncated integer sequences are predictable. This is natural since integers are a fully ordered set. Although predictability is welcomed in some areas of mathematics, it is an unwelcomed phenomenon in certain situations of cryptanalysis. In this paper we will present Linear Fuzzy Integers, a set of numbers with both properties of real numbers and of interval numbers. We will then find the solution(s) to a linear congruence using the hybrid numbers as an environment. The hybrid set of numbers are denoted as Linear Fuzzy Real numbers (LFR). Then we will briefly present the set of Linear Fuzzy Integers (LFZ). This set is a subset of LFR. Because of the hybrid nature of LFZ, fuzzy linear congruence can be solved in a similar way as its crisp counterpart.

Fuzzy sets were initially introduced by Bellman and Zadeh (1970). Neggers and Kim (2001) researched fuzzy posets. Neggers and Kim (2007) also created Linear Fuzzy Real numbers. Linear Fuzzy Real numbers were used by Monk (2001) and Prevo (2002) in the study of fuzzy random variables. Linear Fuzzy Real numbers were also used by Rogers (2008) to optimize the primal problems of linear programs with fuzzy constraints Rogers.

The set of LFR is a set that shows intermediate properties which are unique to the set and not to those of either the real numbers or the "general" fuzzy numbers. Because of the unique properties of LFR and thus LFZ, we can solve fuzzy linear congruences using known methods. This paper is outlined as follows. Operations on LFR are considered in Section 2. In Section 3, an introduction of the LFZ, a method of solution to fuzzy linear congruence and examples are considered. In Section 4, applications to cryptography and future research are considered.

## 2. Linear fuzzy real numbers

Considering the real numbers $R$, one way to associate a fuzzy number with a fuzzy subset of real numbers is as a function $\mu : R \to [0,1]$, where the value $\mu(x)$ is to represent a degree of belonging to the subset of R. The Linear Fuzzy Real numbers as described by Neggers and Kim (2001) is a triple of real numbers $(a,b,c)$ where $a \le b \le c$ of real numbers, See Fig. 1, such that:

$\mu(x) = 1$ if $x = b$;
$\mu(x) = 0$ if $x \le a$ or $x \ge c$;
$\mu(x) = (x - a)/(b - a)$ if $a < x < b$;
$\mu(x) = (c - x)/(c - b)$ if $b < x < c$.

For a real number $c$, we let $\epsilon(c) = \mu$ with associated triple $(c, c, c)$. Then $\mu$ is a linear fuzzy real number with $\mu(c) = 1$ and $\mu(x) = 0$ otherwise. As a linear

* Corresponding Author.
Email Address: frogers@uwa.edu (F. Rogers)

fuzzy real number we consider $\epsilon(c) = \mu$ to represent the real number $c$ itself. Thus by this interpretation we note that the set $R$ of all real numbers is a subset of the set containing the linear fuzzy real numbers. The set of the linear fuzzy real numbers is a hybrid set showing intermediate properties, which are unique to the set and not those of either the real numbers or the "general" fuzzy numbers.

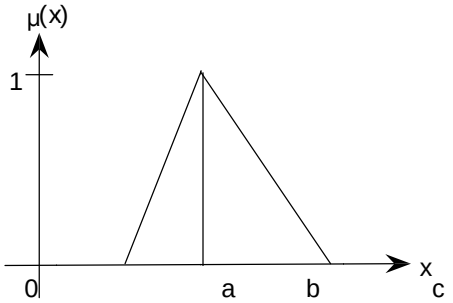


**Fig. 1:** Linear Fuzzy Real number $\mu$ $(a, b, c)$

Let $LFR = \{\mu : R \to [0,1] | \ \mu$ is a linear fuzzy real number$\}$. Each $\mu$ has a set of descriptive parameters. The base is defined as the triple $(a, b, c)$ that occurs in the definition of a linear fuzzy real number. Thus one may write an element of $LFR$ as $\mu = \mu\ (a, b, c)$.

## 3. Addition and subtraction

Given the linear fuzzy real numbers $\mu_1 = \mu\ (a_1, b_1, c_1)$ and $\mu_2 = \mu\ (a_2, b_2, c_2)$,

$\mu_1 + \mu_2$ is defined by

$\mu_1 + \mu_2 = \mu\ (a_1 + a_2, b_1 + b_2, c_1 + c_2)$.

This operation is not the usual definition of addition of functions. It is also clear that $\mu + \epsilon(0) = \mu$ for all $\mu \in LFR$. For subtraction, we have

$\mu_1 - \mu_2 = \mu\ (a_1 - c_2, b_1 - b_2, c_1 - a_2)$.

## 4. Law of trichotomy

A linear fuzzy real number $\mu\ (a, b, c)$ is defined to be positive if $a > 0$, negative if $c < 0$, and zeroic if $a \leq 0$ and $c \geq 0$. The following properties also hold:

1. If $\mu$ is positive , then $-\mu$ is negative;
2. If $\mu$ is negative, then $-\mu$ is positive;
3. If $\mu$ is zeroic, then $-\mu$ is also zeroic;
4. If $\mu_1$ and $\mu_2$ are positive, then so is $\mu_1 + \mu_2$;
5. If $\mu_1$ and $\mu_2$ are negative, then so is $\mu_1 + \mu_2$;
6. If $\mu_1$ and $\mu_2$ are zeroic, then so is $\mu_1 + \mu_2$;
7. For any $\mu$, $\mu - \mu$ is zeroic.

## 5. Multiplication and division

Given the linear fuzzy real numbers $\mu_1 = \mu\ (a_1, b_1, c_1)$ and $\mu_2 = \mu\ (a_2, b_2, c_2)$,

$\mu_1 \mu_2$ is defined by:

$\mu_1 \ \mu_2 = \mu\ (\min\{a_1a_2, a_1c_2, a_2c_1, c_1c_2\}, b_1b_2, \max\{a_1a_2, a_1c_2, a_2c_1, c_1c_2\})$.

Given the linear fuzzy real numbers $\mu_1 = \mu\ (a_1, b_1, c_1)$ and $\mu_2 = \mu\ (a_2, b_2, c_2)$, $\frac{\mu_1}{\mu_2}$ is defined by:

$$\frac{\mu_1}{\mu_2} = \mu_1 . \frac{1}{\mu_2},$$

where

$$\frac{1}{\mu_2} = \mu\left(\min\left\{\frac{1}{a_2}, \frac{1}{b_2}, \frac{1}{c_2}\right\}, \text{median}\left\{\frac{1}{a_2}, \frac{1}{b_2}, \frac{1}{c_2}\right\}, \max\left\{\frac{1}{a_2}, \frac{1}{b_2}, \frac{1}{c_2}\right\}\right)$$

## 6. Functions on LFR

Given a function $f: R \to R$ and $\mu\ (a, b, c) \in LFR$, $f^*(\mu): LFR \to LFR$ is defined as:

$f^*(\mu) = \mu\ (a^*, b^*, c^*)$,

where $a^* = \min\{f(a), f(b), f(c)\}$, $b^* = \text{median}\{f(a), f(b), f(c)\}$, $c^* = \max\{f(a), f(b), f(c)\}$. If $a = b$ or $b = c$, then $a^* = b^*$ or $b^* = c^*$. Therefore if $a = b = c$ then it follows that $a^* = b^* = c^*$, i.e., $f^*(\epsilon(b)) = \epsilon(f(b))$. Hence $f^*$ is an extension of the function $f$.

## 7. Ordering properties

Given $\mu_1, \mu_2 \in LFR$, $\mu_1 \leq \mu_2$ provided that $a_1 \leq a_2$, $b_1 \leq b_2$, $c_1 \leq c_2$. If $\epsilon(0) \leq \mu(a, b, c))$, then $0 \leq a \leq b \leq c$, hence $\mu$ is a non-negative linear fuzzy real number. Therefore if $\mu$ is non-negative and zeroic, then $a = 0$ precisely. If $\{\mu_i\}\ i \in I$ is a collection of linear fuzzy real numbers which is bounded above by a linear fuzzy real number $\mu$ where $\mu_i = \mu\ (a_i, b_i, c_i) \leq \mu = \mu\ (a, b, c)$, it follows that $\{a_i\}\ i \in I$, $\{b_i\}\ i \in I$, and $\{c_i\}\ i \in I$ are collections of real numbers bounded above by $a$, $b$, and $c$, respectively. By the completeness of $R$ there exist real numbers sup $(a_i)$, sup $(b_i)$, and sup $(c_i)$. Suppose that sup $(a_i)$ > sup $(b_i)$, then if $2\epsilon = \sup(a_i) - \sup(b_i) > 0$, there is an $a_j$ such that $a_j > \sup(a_i) - \epsilon > \sup(b_i) \geq b_j$, which leads to a contradiction. Therefore, sup $(a_i) \leq$ sup $(b_i)$ and by a similar argument, sup $(b_i) \leq$ sup $(c_i)$. It follows that sup $(a_i) \leq$ sup $(b_i) \leq$ sup $(c_i)$ and thus $\mu$ (sup $(a_i)$, sup $(b_i)$, sup $(c_i)$) is a linear fuzzy real number. Now suppose that $\mu < \mu$ (sup $(a_i)$, sup $(b_i)$ and sup $(c_i)$). Then $\mu = \mu\ (a, b, c)$ with $a \leq$ sup $(a_i)$, $b \leq$ sup $(b_i)$, and $c \leq$ sup $(c_i)$ where at least one of these is a strict inequality. Given without loss of generality that $a <$ sup $(a_i)$, there is an index $k$ such that $a_k > a$ so that it is not the case that $\mu_k \leq \mu$ and thus $\mu$ is not an upper bound for the collection $\{\mu_i\}\ i \in I$. If $\mu$ is such an upper bound, then $a \geq a_i$ implies $a \geq$ sup $(a_i)$, $b \geq$ sup $(b_i)$, and $c \geq$ sup $(c_i)$, so that $\mu$ (sup $(a_i)$, sup $(b_i)$, sup $(c_i)$) is the least upper bound. Therefore, $(LFR, \leq)$ is a complete ordered set. However, it is not linearly ordered. If we let $\mu_1 = \mu\ (3, 4, 5)$ and let $\mu_2 = \mu\ (a, 5, 6)$ and state that $a < 3$, then it is not true that $\mu_1 \leq \mu_2$ nor is it true that $\mu_1 \geq \mu_2$. Therefore, $\mu_1$ and $\mu_2$ are incomparable in this order.

## 8. Linear equations on LFR

Before discussing the Diophantine equation, we must discuss linear equations in the $LFR$ system. A linear equation over $LFR$ is an equation of the form

$\mu_1 \cdot \mu_x + \mu_2 = \mu_3 \cdot \mu_x + \mu_4$,

where the $\mu_i$ are $LFR$'s for $i = 1,2,3,4$ and $\mu_x$ is an unknown $LFR$ with a triple of unknown real numbers

($\alpha$, $\beta$, $\gamma$). The solution set of the general linear equation can be roughly classified as
1. Empty set,
2. singleton set,
3. not a singleton set but a bounded set:
$\beta_1 \leq \alpha \leq \beta \leq \gamma \leq \beta_2 \, for \, \beta_1, \beta_2 \in R$,,
4. an unbounded set but not all *LFR*'s are included,
5. all possible *LFR*'s are included.

A solution set that is bounded but not a singleton would imply that $\mu_x$ is not equal to the solution set in a crisp sense. Solving these equations through traditional means can be a daunting task. If we define a relation $\mu_1 \equiv \mu_2 \pmod{\theta}$ iff $\mu_1 - \mu_2$ is zeroic, then $\mu\,(a,b,c) \equiv \epsilon(b)\,(mod\ \theta)$ since $\mu\,(a,b,c) - \epsilon(b) = \mu(a-b, 0, c-b)$. Therefore if we define $[\mu_1] = \{\mu_2 | \mu_2 \equiv \mu_1 (mod\ \theta)$, then $[\mu\ (a,\ b,\ c)] = [\epsilon(b)]$. Furthermore, in order that $\epsilon(a) \equiv \epsilon\,(b)(mod\ \theta)$, we must have $\epsilon(a) - \epsilon(b) = \epsilon(a-b)$ zeroic, which can only happen if $a = b$. Hence, we have a mapping $\Phi$: $\mu \rightarrow [\mu]$ with the property that if we compose this with the mapping $b \rightarrow \epsilon(b)$ then we obtain the sequence $R \xrightarrow{\epsilon} LFR \xrightarrow{\varphi} LFR/Z$, where $Z$ is the set of zeroic elements of *LFR*, whence *LFR/Z* is seen to be isomorphic to itself. If: $Z \rightarrow LFR$ is the inclusion mapping and then we obtain a further diagram:

$$Z \xrightarrow{\sigma} LFR \xrightarrow{\varphi} LFR/Z \xrightarrow{\epsilon} LFR.$$

Thus $[\mu * \mu^{-1}] = [\mu] * [\mu^{-1}] = \epsilon(1)$, i.e., $[\mu]$ has a multiplicative inverse in *LFR/Z*. The properties of *LFR/Z* allow one to solve for the solution of fuzzy linear equations using the inverse order of operations.

## 9. Linear congruence in an LFZ environment

It has been shown by Neggers (2007) that arithmetic operations upon elements of LFR increase the area of $= \mu\ (a_i,\ b_i,\ c_i)$. This is also known as overestimation. It is a phenomenon typical of fuzzy operations. The overestimation effect is responsible for a more or less large discrepancy between the arithmetical solution of a problem and the calculated one. In an effort to avoid this, a combination of LFZ/Z unique properties and a re-imagining of the problem are implemented in some cases.

## 10. Crisp greatest common divisor and its applications

Because of overestimation we will define the Crisp GCD of *LFZ, CGCD*, as d = $\epsilon(b)$ such that d | $\mu_{i=} \mu(a_i,\ b_i,\ c_i)$ i= 1,2,3,4,5…and if there is an element w $\geq d \ and$ w | $\mu_{i=} \mu(a_i,\ b_i,\ c_i)$ i= 1,2,3,4,5… then d = w. The CGCD will essentially be the GCD of $\epsilon(b_i)$ for a given set of LFZ numbers. Note that for d|$\mu\ (a_i,\ b_i,\ c_i)$ where a, b, c, and d > 0 in LFZ, yields as expected in integer division.

$$\mu\left(floor\ \left(\frac{a_i}{d}\right), \frac{b_i}{d}, floor\ \left(\frac{c_i}{d}\right)\right),$$

Proposition 1: If d divides $\mu_a$ and $\mu_b$ then d divides $\mu_a$ *$\mu_x$ + $\mu_b$ *$\mu_y$ for all LFZ

Proof: If d divides $\mu_a$ then $\mu_a = \mu_m$ *d, likewise for $\mu_b$. Then it follows that

$\mu_a$ *$\mu_x$ + $\mu_b$ *$\mu_y$ = $\mu_m$ *d* $\mu_x$ + $\mu_n$ *d* $\mu_y$. Thus d divides $\mu_a$ *$\mu_x$ + $\mu_b$ *$\mu_y$ for all LFZ.□

Proposition 2: Let $\mu_a$ and $\mu_b$ be LFZ (not both zeroic) with CGCD *d*. Then an LFZ $\mu_c$ has the form $\mu_a$ *$\mu_x$ + $\mu_b$ *$\mu_y$ for some $\mu_x$ , $\mu_y$ ∈ LFZ iff $\mu_c$ is a multiple of *d*.

Proof: If $\mu_c = \mu_a$ *$\mu_x$ + $\mu_b$ *$\mu_y$ where $\mu_x$ , $\mu_y$ ∈ LFZ then since d divides $\mu_a$ and $\mu_b$, Proposition 1 implies that d divides $\mu_c$.

Proposition 2 implies that $\mu_c = \mu_a$ *$\mu_x$ + $\mu_b$ *$\mu_y$ has a Linear Fuzzy Integer solution if and only if d| $\mu_c$.

Let us observer the equation $\mu_c = \mu_a * \epsilon(x)_0 + \mu_b * \epsilon(y)_0$ and define $\frac{\mu_a}{d} = \mu_\alpha$ and $\frac{\mu_b}{d} = \mu_\beta$. If we set $\mu_x = \epsilon(x)_0 + \mu_\beta\, t$ and $\mu_y = \epsilon(y)_0 - \mu_\alpha\, t$ where t is any crisp integer, then $\mu_a$ *$\mu_x$ + $\mu_b$ *$\mu_y$ = $\mu_a * \epsilon(x)_0 + \mu_b * \epsilon(y)_0$ = $\mu_c$ therefore $\mu_x$ , $\mu_y$ is also a solution. This gives us infinitely many solutions for different integer's t.

## 11. Fuzzy Diophantine linear equations

Before discussing congruence, we must also discuss the Fuzzy Diophantine equations. They are equations of one or more variables, for which we seek integer solutions. One of the simplest of these is the Fuzzy Linear Diophantine equation $\mu_c = \mu_a$ *$\mu_x$ + $\mu_b$ *$\mu_y$. Derived from this is Bezout's identity d = $\mu_a$ *$\mu_x$ + $\mu_b$ *$\mu_y$. In fact, dividing by d, and defining $\frac{\mu_a}{d} = \mu_\alpha$ and $\frac{\mu_b}{d} = \mu_\beta$ produces the equation $\epsilon(1) = \mu_\alpha$ *$\mu_x$ + $\mu_\beta$ *$\mu_y$. It follows that a fuzzy solution to

$\epsilon(1) = \mu_\alpha$ *$\mu_x$ + $\mu_\beta$ *$\mu_y$ is

$\mu_x = \epsilon(x)_0 + \mu_y t$ and $\mu_y = \epsilon(y)_0 - \mu_x t$.

The Fuzzy Diophantine problem requires that the solution $\mu_x$ as well as $\mu_1$, $\mu_2$, $\mu_3$ and $\mu_4$ be elements such that $\mu_{i=} \mu\ (a_i,\ b_i,\ c_i)$ implies that $a_i,\ b_i,\ c_i \in Z$ for *i = 1, 2, 3, 4.* Thus $\mu\ (a,\ b,\ c) \in LFZ$ is an integral LFR and behaves much like *Z in R.* The mapping $Z \xrightarrow{\sigma} LFZ \xrightarrow{\varphi} LFZ/Z \xrightarrow{\epsilon} LFZ$,
where Z is the set of Zeroic elements and LFZ is the set of Linear Fuzzy Integers yields the same properties as the mapping of *LFR/Z*.

## 12. Fuzzy linear congruence

Congruence or in particular, fuzzy linear congruence has the form $\mu_a * \mu_x \equiv \mu_b \pmod{\mu_n}$ where $\mu_x$ is an unknown linear fuzzy integer. As is true of the crisp version of modulo congruence this also implies that $\mu_n$ divides the quantity ($\mu_a * \mu_x - \mu_b$).

Proposition 3: If d = gcd ($\mu_a$, $\mu_n$) then the fuzzy linear congruence is $\mu_a * \mu_x \equiv \mu_b \pmod{\mu_n}$ has a solution if and only if d divides $\mu_b$ and if $\epsilon(x)_0$ is any solution then the general solution is given by $\mu_x = \epsilon(x)_0 + \frac{\mu_n}{d} t$. Where t is an integer and the solution form exactly d congruence classes' mod ($\mu_n$).

Proof: This is equivalent to the Fuzzy Linear Diophantine Equation $\mu_b = \mu_a$ *$\mu_x$ - $\mu_n$ *$\mu_y$ thus $\mu_x = \epsilon(x)_0 + \mu_\alpha t$ and $\mu_y = \epsilon(y)_0 - \mu_\beta t$ where: $\frac{\mu_n}{d} = \mu_\alpha$ and $\frac{\mu_a}{d} = \mu_\beta$ ; note that, $\epsilon(x)_0 + \mu_\alpha t_1 \equiv \epsilon(x)_0 + \mu_\alpha t_2 \pmod{}$

($\mu_n$), if $\mu_n$ divides $\mu_\alpha\ (t_1 - t_2)$. Since $\frac{\mu_n}{d} = \mu_\alpha$ we arrive at the necessary statement d divides $(t_1 - t_2)$. This can only occur is if $(t_1 - t_2)$ a multiple of d is. So the congruence classes of solutions mod ($\mu_n$) are obtained by letting t range over a complete set of residues mod (d).

## 13. Examples of the solutions of fuzzy linear congruence with linear fuzzy integer components

The following examples illustrate the solutions of linear congruences in a LFZ environment.

Example 1

Solve $5*\mu_x \equiv \mu\ (6, 7, 8)*Mod\ [\mu(7, 8, 9)]$

Where d = 1. A reasonable $\epsilon(x)_0$ is 3.

Note:

$[5*(3) - \mu\ (6, 7, 8)] \div \mu\ (7, 8, 9) = [\mu\ (15, 15, 15) + \mu\ (-8, -7, -6)] \div \mu\ (7, 8, 9) = [\mu\ (7, 8, 9)] \div \mu\ (7, 8, 9)$.

Thus $\mu_x = 3 + [\mu\ (7, 8, 9)]/1$ implies that $\mu_x \equiv 3 \bmod [\mu\ (7, 8, 9)]$.

Example 2

Solve $5*\mu_x \equiv 6*Mod\ [\mu\ (17, 19, 20)]$

Where again d = 1. Let's suppose that a possible $\epsilon(x)_0$ is not obvious. We can use tradition Number Theory techniques to solve for an answer. Let us change the coefficient by adding multiples of $\mu_n$.

$6 \equiv 5*\mu_x \equiv \mu\ (22, 24, 25)] * \mu_x\ Mod\ [\mu\ (17, 19, 20)]$

$6 \equiv \mu\ (22, 24, 25) * \mu_x\ Mod\ [\mu\ (17, 19, 20)]$

$1 \equiv \mu\ (3, 4, 4) * \mu_x\ Mod\ [\mu\ (17, 19, 20)]$, note that the LFZ $\mu$ (a, *b, b*) or $\mu$ (b, *b, c*) is a right triangular fuzzy number or LFZ.

Here 5 are a reasonable $\epsilon(x)_0$. Thus $\mu_x \equiv 5 \bmod [\mu\ (17, 19, 20)]$.

Traditional number theory techniques such as the Euclidean Algorithm can also be used to solve LFZ linear congruences.

Example 3

Solve $\mu\ (12, 13, 13)*\mu_x \equiv -1 \bmod [\mu\ (13, 14, 14)]$.

Using the Euclidean Algorithm on the respective $\epsilon(b)$ values 13 and 14, we find that a reasonable $\epsilon(x)_0$ is 1 and thus $\mu_x \equiv 1 \bmod [\mu\ (13, 14, 14)]$.

## 14. Conclusion

We can find an interval solution by projecting the upper and lower bound $\mu\ (a, b, c) \rightarrow [a, c]$. We can find a crisp solution by projecting to the middle, $\mu\ (a, b, c) \rightarrow \epsilon(b)$. At the same time the method outlined produces a fuzzy solution in the form of an *LFZ* expression, which can be used directly as a fuzzy value or a fuzzy interval. In the future, *LFZ* may be used in cryptography to ensure stronger security. In cryptographic systems the messages can be encrypted using linear congruences in mere moments on a computer. Using linear congruences in LFZ for encryption is possible as well. For example, if X is the digital version of a plaintext letter and Y is the digital version of the corresponding ciphertext letter, then perhaps X and Y can be hidden in an LFZ triplet and coded via $\mu_x \equiv \mu_y + 3 \bmod [\mu\ (25, 26, 26)]$. A possibility here is a fuzzy Caesar Cipher where X and Y are hidden as upper bounds of the LFZ. Projecting to the middle is mathematically safer, but the upper or lower bound calculations may provide greater security. This of course, requires more study. However, it is a future goal to explore the possibility of using LFZ in the encryption processes to include the RSA and IBE cryptosystem.

## References


Bellman RE and Zadeh LA (1970). Decision-making in a fuzzy environment. Management science, 17(4): B-141. B141–B164.

Golić JD (1994). Linear cryptanalysis of stream ciphers. In Fast Software Encryption Springer Berlin Heidelberg, (1008): 154-169.

Monk B (2001). A Proposed Theory of Fuzzy Random Variables, Dissertation. University of Alabama.

Neggers J and Kim H (2007). On Linear Fuzzy Real Numbers. Manuscript for book under development.

Neggers J and Kim HS (2001). Fuzzy posets on sets. Fuzzy Sets and Systems, 117(3): 391-402.

Prevo R (2002). Entropies of Families of Fuzzy Random Variables: An Introduction to and an In-depth Exploration of Several Classes of Important Examples.

Rogers F, Neggers J and Jun Y (2008). Method for optimizing linear problems with fuzzy constraints. In International Mathematical Forum 3(23): 1141-1155.

Schjaer-Jacobsen H (2002). Representation and calculation of economic uncertainties: Intervals, fuzzy numbers, and probabilities. International Journal of Production Economics, 78(1): 91-98.