Filomat 32:5 (2018), 1679–1686
https://doi.org/10.2298/FIL1805679W

Published by Faculty of Sciences and Mathematics,
University of Niš, Serbia
Available at: http://www.pmf.ni.ac.rs/filomat

Solution to Open Problems on Fuzzy Filters in Logical algebras and Secure Communication Encoding Scheme on Filters

Wang Wei[a]

[a]*College of Sciences, Xi'an Shiyou University, Xi'an, 710065, China*

Abstract. We characterize fuzzy Boolean and implicative filters in pseudo *BCK* algebras, then get the essential equivalent relation between the two fuzzy filters. Based on this, we solve an open problem in pseudo *BCK* algebras. By constructing the Chinese remainder theorem with respect to filters in distributive lattice of polynomials, a new kind of communication encoding scheme is obtained, and we analyze the security of the scheme.

1. Introduction

Logical algebras are the algebraic counterpart of the fuzzy logics and the foundation of reasoning mechanism in information sciences, computer sciences, theory of control, artificial intelligence and other important fields[29]. For example, *BL* algebra, pseudo *MTL* algebra and residuated lattice correspond to monoidal t-norm-based logic and monoidal logic respectively[10, 27, 28].

Iséki and Imai introduced *BCK* algebra for *BCK* Logic[15, 17, 18]. Afterwards, Georgescu and Iorgulescu introduced notion of pseudo *BCK* algebra as extension of *BCK* algebra[4, 12]. Iorgulescu established connections between (pseudo)*BCK* algebra and (pseudo)*BL* algebra[3, 4]. In[22], Wang and Zhang presented the necessary and sufficient conditions for residuated lattice and bounded pseudo *BCK* algebra to be Boolean algebra.

Filter theory plays an important role both in algebraic structure research and non-classical logic and computer science[16, 19, 32]. From logical point of view, various filter corresponds to various set of provable formulae [31, 34]. For example, with the help of filter and prime filter in *BL* algebra, Hájek proved the completeness of Basic Logic[27]. In[9], Turunen defined implicative filter and Boolean filter and proved the equivalence of the two filters in *BL* algebra. In[1, 2, 8, 9, 13, 18, 20, 25, 33, 38, 42] different kinds of filters in in *BL* algebra, lattice implication algebra, pseudo *BL* algebra, pseudo effect algebra, pseudo hoop, residuated lattice, triangle algebra and the corresponding algebraic structures were further studied.

Fuzzy set was introduced by Zadeh[23]. Nowadays this idea has been applied to different algebraic structures. For example, fuzzy filter functions well in investigating algebraic structures. [39, 40, 42]

2010 *Mathematics Subject Classification*. Primary 03G10; Secondary 03B52
Keywords. Pseudo-*BCK* algebras; Fuzzy Boolean filters; Fuzzy implicative pseudo-filters; The Chinese remainder theorem.
Received: 25 September 2017; Accepted: 17 December 2018
Communicated by Hari M. Srivastava
Research supported by the National Natural Science Foundation of P. R. China (Grant No.11571281, 61673320); Foundation project of the National Key Laboratory of Aerospace Dynamics(Grant No. 202300006); the Fundamental Research Funds for the Central Universities(Grant No. 2682017ZT12).
Email address: wwmath@xsyu.edu.cn (Wang Wei)

introduced and characterized fuzzy positive implicative filters in lattice implication algebra. [21, 24] studied fuzzy filters in BL-algebra. Wang and Xin investigated fuzzy normal and Boolean filter as to solve an open problem in pseudo BL-algebra[31]. [14, 36, 37, 41]studied interval valued fuzzy filter in pseudo BL-algebra and MTL-algebra. Thus shows that fuzzy filter acts as a feasible tool to obtain results in logical algebra.

Upon the relation between implicative pseudo-filter and Boolean filter in pseudo BCK algebra or bounded pseudo BCK algebra, [35] proposed an open problem on the two filters and thus are the motivation of first part in this paper.

[29] explored the properties of fuzzy filter in pseudo BCK algebra, discussed the equivalent conditions of fuzzy normal filter in pseudo BCK algebra(pP), and proposed the relation between fuzzy implicative pseudo filter and Boolean filter of (bounded) pseudo BCK algebra(pP). Thus the open problem are partly solved.

Based on this, in this paper we further investigate the fuzzy Boolean and implicative filters in pseudo BCK algebra, and find essentially equivalent relation between them, then find the relation between them and implicative BCK algebras, then completely solve the open problem.

By constructing the Chinese remainder theorem with respect to filters in distributive lattice of polynomials, a new kind of communication encoding scheme is obtained.

2. Preliminaries

First we recall corresponding results which will be needed.

Definition 2.1. *[6]A nonempty set L with binary operations $\wedge$ and $\vee$ is called a lattice if for $x, y, z \in L$*
(1)$x \wedge x = x \vee x = x, x \wedge y = y \wedge x, x \vee y = y \vee x$,
(2)$(x \wedge y) \wedge z = x \wedge (y \wedge z), (x \vee y) \vee z = x \vee (y \vee z), (x \wedge y) \vee x = (x \vee y) \wedge x = x$.

A binary relation $\leq$ is defined as for $x, y \in L$, $x \leq y$ if $x \wedge y = x$ or $x \vee y = y$. Then we can find that binary relation $\leq$ is a partially ordered relation.

Definition 2.2. *[7]For $x, y, z \in L$,a lattice L is called*
(1)distributive if $x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)$ or $x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z)$;
(2)bounded if there exists $0, 1 \in L$, such that $0 \leq x \leq 1$.

Definition 2.3. *[15]A structure $(A, \rightharpoonup, 1)$ is called an BCK algebra if for $x, y, z \in A$*
(1) $(z \rightharpoonup x) \rightharpoonup (y \rightharpoonup x)) \geq (y \rightharpoonup z), (y \rightharpoonup x) \rightharpoonup x \geq y, x \geq x$,
(2) $x \geq y$ and $y \geq x$ imply $x = y$, and $x \rightharpoonup 1 = 1 (x \leq y \Leftrightarrow x \rightharpoonup y = 1)$.

Definition 2.4. *[5] A pseudo BCK algebra is a structure $(A, \geq, \rightarrow, \hookrightarrow, 1)$, if for $x, y, z \in A$*
(1) $(z \rightarrow x) \hookrightarrow (y \rightarrow x)) \geq y \rightarrow z, (z \hookrightarrow x) \rightarrow (y \hookrightarrow x)) \geq y \hookrightarrow z, (y \rightarrow x) \hookrightarrow x \geq y, (y \hookrightarrow x) \rightarrow x \geq y$,
(2) $x \geq x, 1 \geq x, x \geq y$ and $y \geq x$ imply $x = y, x \geq y$ iff $y \rightarrow x = 1$ iff $y \hookrightarrow x = 1$.

In a pseudo BCK algebra A, $x^{-} = x \rightarrow 0, x^{\sim} = x \hookrightarrow 0$ for $x \in A$ and A is called bounded if $0 \rightarrow x = 1$ or $0 \hookrightarrow x = 1$[12].

Proposition 2.5. *[4] In a pseudo BCK algebra A, the following properties hold for $x, y, z \in A$*
(1) $x \leq y \Rightarrow y \rightarrow z \leq x \rightarrow z$ and $y \hookrightarrow z \leq x \hookrightarrow z, x \leq y \Rightarrow z \rightarrow x \leq z \rightarrow y$ and $z \hookrightarrow x \leq z \hookrightarrow y$,
(2) $z \rightarrow x \leq (y \rightarrow z) \rightarrow (y \rightarrow x), z \hookrightarrow x \leq (y \hookrightarrow z) \hookrightarrow (y \hookrightarrow x), z \hookrightarrow (y \rightarrow x) = y \rightarrow (z \hookrightarrow x)$.

Definition 2.6. *[11] A pseudo BCK algebra(pP) is a pseudo BCK algebra A satisfying for $x, y \in A$, there exists $x \odot y = min\{z | x \leq y \rightarrow z\} = min\{z | y \leq x \hookrightarrow z\}$.*

Theorem 2.7. *[12]In a pseudo BCK algebra(pP) A, the followings hold*
(1) $(x \odot y) \rightarrow z = x \rightarrow (y \rightarrow z), (y \odot x) \hookrightarrow z = x \hookrightarrow (y \hookrightarrow z)$,
(2) $(x \rightarrow y) \odot x \leq x, y, x \odot (x \hookrightarrow y) \leq x, y, x \odot y \leq x \wedge y \leq x, y$.

The operations $\vee, \wedge, \odot$ have priority towards the operations $\rightarrow, \hookrightarrow$.

Definition 2.8. *[15] A BCK algebra A is called implicative if for* $x, y \in A$, $(x \rightharpoonup y) \rightharpoonup x = x$.

Definition 2.9. *[35] A pseudo BCK algebra A is called 1-type(2-type) implicative if for* $x, y \in A$, $(x \rightharpoonup y) \rightharpoonup x = (x \rightsquigarrow y) \rightsquigarrow x = x((x \rightsquigarrow y) \rightharpoonup x = (x \rightharpoonup y) \rightsquigarrow x = x)$.

Theorem 2.10. *[35]A pseudo BCK algebra A is a 1-type(2-type) implicative if and only if A is implicative.*

Definition 2.11. *(the Chinese remainder theorem)[26] Suppose* $n \geq 2$, *and* $m_1, m_2, \cdots, m_n$ *are n positive mutually prime integers. Let* $M = m_1 m_2 \cdots m_n = m_1 M_1 = m_2 M_2 = \cdots = m_n M_n$, *here* $M_i = \frac{M}{m_i}, i = 1, 2, \cdots, n$, *then for the following congruence equations group* $x \equiv b_i (mod m_i), i = 1, \cdots n$, *the minimum solution is* $x_0 = b_1 M_1' M_1 + b_2 M_2' M_2 + \cdots + b_n M_n' M_n mod M$, *here positive integer* M_i' *satisfying:* $M_i' M_i \equiv 1 (mod m_i), i = 1, \cdots n$, *i.e.,* M_i' *is the inverse element of* M_i *with respect to* m_i.

3. (fuzzy) pseudo-filters of pseudo *BCK* algebra

In this section, we recall the definitions of pseudo filter and fuzzy filter in pseudo *BCK* algebra A.

Definition 3.1. *[35]A subset F of A is called a pseudo-filter if*
(F1) $x \in F, y \in A, x \leq y \Rightarrow y \in F$,
(F2) $x \in F, x \rightarrow y \in F$ *or* $x \hookrightarrow y \in F \Rightarrow y \in F$.

Theorem 3.2. *[29]A subset F of A is a pseudo-filter if and only if*
(F3) $1 \in F$,
(F4) $x \in F, x \rightarrow y \in F$ *or* $x \hookrightarrow y \in F \Rightarrow y \in F$.

Definition 3.3. *[35]For* $x, y \in A$, *a filter F is called a(an)*
(1)Boolean if $(x \rightarrow y) \hookrightarrow x \in F$ *and* $(x \hookrightarrow y) \rightarrow x \in F$, *then* $x \in F$.
(2)implicative if $(x \rightarrow y) \rightarrow x \in F$ *and* $(x \hookrightarrow y) \hookrightarrow x \in F$, *then* $x \in F$.

Theorem 3.4. *[35]Let F be implicative of a bounded pseudo BCK algebra A. Then* $\forall x, y \in A$
(1)$((x \rightarrow 0) \rightarrow x) \hookrightarrow x \in F$, $((x \hookrightarrow 0) \hookrightarrow x) \rightarrow x \in F$,
(2)$((x \rightarrow y) \rightarrow x) \hookrightarrow x \in F$, $((x \hookrightarrow y) \hookrightarrow x) \rightarrow x \in F$,
(3)if $(x \rightarrow y) \rightarrow y \in F$, *then* $(y \rightarrow x) \hookrightarrow x \in F$, *if* $(x \hookrightarrow y) \hookrightarrow y \in F$, *then* $(y \hookrightarrow x) \rightarrow x \in F$,
(4)if $x \hookrightarrow y \in F$, *then* $((y \hookrightarrow x) \rightarrow x) \hookrightarrow y \in F$, *if* $x \rightarrow y \in F$, *then* $((y \rightarrow x) \hookrightarrow x) \rightarrow y \in F$.

Definition 3.5. *[29] A fuzzy subset f of A is called a fuzzy pseudo-filter if* f_t *is either empty or a pseudo-filter for* $t \in [0, 1]$.

F is a pseudo-filter iff χ_F is a fuzzy pseudo-filter, where χ_F is the characteristic function of *F*.
Inspired by[31], we get the following results.

Proposition 3.6. *[29] A fuzzy set f is a fuzzy pseudo-filter of A(or A(pP))if and only if for* $x, y, z \in A$, *one the followings holds*
(1)$f(1) \geq f(x)$, $f(y) \geq f(x) \wedge f(x \rightharpoonup y)$, $f(1) \geq f(x)$, $f(y) \geq f(x) \wedge f(x \rightsquigarrow y)$,
(2)f is order-preserving and $f(x \odot y) \geq f(x) \wedge f(y)$.

Definition 3.7. *[29] For* $x, y \in A$, *a fuzzy pseudo-filter f is called*
(1)implicative if $f((x \rightharpoonup y) \rightharpoonup x) = f(x)$, $f((x \rightsquigarrow y) \rightsquigarrow x) = f(x)$.
(2)Boolean if $f((x \rightharpoonup y) \rightsquigarrow x) = f((x \rightsquigarrow y) \rightharpoonup x) = f(x)$.

Theorem 3.8. *[29]For a fuzzy implicative pseudo-filter f of a bounded pseudo-BCK algebra A, then* $\forall x \in A$, $f((x^- \rightharpoonup x) \rightsquigarrow x) = f((x^\sim \rightsquigarrow x) \rightharpoonup x) = f((x^- \rightsquigarrow x) \rightharpoonup x) = f((x^\sim \rightharpoonup x) \rightsquigarrow x) = f(1)$.

Theorem 3.9. *[29] A fuzzy pseudo-filter f of A is implicative(Boolean) if and only if f_t is either empty or an implicative(Boolean) pseudo-filter for each $t \in [0, 1]$ if and only if $f_{f(1)}$ is an implicative(Boolean) pseudo-filter.*

Corollary 3.10. *[29] A subset F of A is an implicative(Boolean) pseudo-filter if and only if χ_F is implicative(Boolean).*

Theorem 3.11. *[29] A fuzzy pseudo-filter f of a bounded A is Boolean if and only if $f(x \rightharpoonup y) = f(x \rightharpoonup (y^- \rightsquigarrow y))$, $f(x \rightsquigarrow y) = f(x \rightsquigarrow (y^\sim \rightharpoonup y))$ if and only if $f((x^\sim \rightharpoonup x) \rightsquigarrow x) = f((x^- \rightsquigarrow x) \rightharpoonup x) = f(1)$ for $x, y \in A$.*

Corollary 3.12. *In a bounded pseudo-BCK algebra, every fuzzy implicative pseudo-filter is a fuzzy Boolean filter.*

Theorem 3.13. *[29]Let f be a fuzzy Boolean filter of a bounded A. Then $f((y \rightsquigarrow x) \rightharpoonup x) = f((x \rightharpoonup y) \rightsquigarrow y)$ for $x, y \in A$.*

Corollary 3.14. *Let f be a fuzzy Boolean filter of a bounded A. Then $f(x^{-\sim}) = f(x^{\sim -}) = f(x)$ for $x \in A$.*

4. The relation between implicative pseudo-filter and Boolean filter in pseudo-*BCK* algebras or bounded pseudo-*BCK* algebras

[35]proposed an open problem: "In pseudo *BCK* algebra or bounded pseudo *BCK* algebra, is the notion of implicative pseudo-filter equivalent to the notion of Boolean filter?" To solve the open problem, we recall the results of the relation between the two filters.

Theorem 4.1. *[35]Let F be normal of A. Then F is implicative if and only if F is Boolean.*

With the help of the equivalent condition of fuzzy normal filter of A(pP), inspired by [31], [29] get the following results and partly solve the open problem.

Theorem 4.2. *[29]In bounded pseudo BCK algebra, every implicative pseudo filter is a Boolean filter. In pseudo BCK algebras(pP), every Boolean filter is an implicative pseudo filter.*

We further investigate the properties of fuzzy Boolean filters and fuzzy implicative filters which make the relation between the two fuzzy filters much clear, and get the complete solution for the open problem.

Theorem 4.3. *Fuzzy implicative pseudo filters are fuzzy Boolean filters in pseudo BCK algebras.*

Proof. Let f be an fuzzy implicative pseudo filter of A. Then $\forall x \in A$, suppose $f((x \to y) \hookrightarrow x) = t$, then $(x \to y) \hookrightarrow x \in f_t$. From $x \leq ((x \to y) \hookrightarrow x) \to x$, so $(((x \to y) \hookrightarrow x) \to x) \to y \leq x \to y$ and $((((x \to y) \hookrightarrow x) \to x) \to y) \to (x \to y) = 1$. On the other hand, $x \to y \leq ((x \to y) \hookrightarrow x) \to x$, so we get $((((x \to y) \hookrightarrow x) \to x) \to y) \to (x \to y) \leq ((((x \to y) \hookrightarrow x) \to x) \to y) \to (((x \to y) \hookrightarrow x) \to x)$. Then $((((x \to y) \hookrightarrow x) \to x) \to y) \to (((x \to y) \hookrightarrow x) \to x) = 1 \in f_t$ and $((x \to y) \hookrightarrow x) \to x \in f_t$ since f is an fuzzy implicative filter. Combine that $(x \to y) \hookrightarrow x \in f_t$, according to the definition of filter, we get $x \in f_t$.

Similarly, suppose $f((x \hookrightarrow y) \to x) = t$, then $(x \hookrightarrow y) \to x \in f_t$. From From $x \leq ((x \hookrightarrow y) \to x) \hookrightarrow x$, so $(((x \hookrightarrow y) \to x) \hookrightarrow x) \hookrightarrow y \leq x \hookrightarrow y$ and $(((x \hookrightarrow y) \to x) \hookrightarrow x) \hookrightarrow y) \hookrightarrow (x \hookrightarrow y) = 1$, And $x \hookrightarrow y \leq ((x \hookrightarrow y) \to x) \hookrightarrow x$, so we get $((((x \hookrightarrow y) \to x) \hookrightarrow x) \hookrightarrow y) \hookrightarrow (x \hookrightarrow y) \leq ((((x \hookrightarrow y) \to x) \hookrightarrow x) \hookrightarrow y) \hookrightarrow (((x \hookrightarrow y) \to x) \hookrightarrow x)$. Then $((((x \hookrightarrow y) \to x) \hookrightarrow x) \hookrightarrow y) \hookrightarrow (((x \hookrightarrow y) \to x) \hookrightarrow x) = 1 \in f_t$ and $((x \hookrightarrow y) \to x) \hookrightarrow x \in f_t$ since f is a fuzzy implicative filter. Combine that $(x \hookrightarrow y) \to x \in f_t$, according to the definition of filter, then we get $x \in f_t$.

According to the definition, f is fuzzy Boolean. □

Similarly we can get

Theorem 4.4. *In pseudo BCK algebras, every fuzzy Boolean pseudo filter is a fuzzy implicative filter.*

Proof. Let f be a fuzzy Boolean filter of A. Then $\forall x \in A$, suppose $f((x \to y) \to x) \in f_t$, then $(x \to y) \to x \in f_t$. From $x \leq ((x \to y) \to x) \hookrightarrow x$, so $(((x \to y) \to x) \hookrightarrow x) \to y \leq x \to y$ and $(((x \to y) \to x) \hookrightarrow x) \to y) \hookrightarrow (x \to y) = 1$. On the other hand, $x \to y \leq ((x \to y) \to x) \hookrightarrow x$, so we get $((((x \to y) \to x) \hookrightarrow x) \to y) \hookrightarrow (x \to y) \leq ((((x \to y) \to x) \hookrightarrow x) \to y) \hookrightarrow ((x \to y) \to x) \hookrightarrow x)$. Then $((((x \to y) \to x) \hookrightarrow x) \to y) \hookrightarrow (((x \to y) \to x) \hookrightarrow x) = 1 \in f_t$ and $((x \to y) \to x) \hookrightarrow x \in f_t$ since f is a fuzzy implicative filter. Combine that $(x \to y) \to x \in f_t$, according to the definition of filter, then we get $x \in f_t$.

Similarly, suppose $f((x \hookrightarrow y) \hookrightarrow x))) \in f_t$, then $(x \hookrightarrow y) \hookrightarrow x \in f_t$. From $x \leq ((x \hookrightarrow y) \hookrightarrow x) \to x$, so $(((x \hookrightarrow y) \hookrightarrow x) \to x) \hookrightarrow y \leq x \hookrightarrow y$ and $(((x \hookrightarrow y) \hookrightarrow x) \to x) \hookrightarrow y) \to (x \hookrightarrow y) = 1$. On the other hand, $x \hookrightarrow y \leq ((x \hookrightarrow y) \hookrightarrow x) \to x$, so we get $((((x \hookrightarrow y) \hookrightarrow x) \to x) \hookrightarrow y) \to (x \hookrightarrow y) \leq ((((x \hookrightarrow y) \hookrightarrow x) \to x) \hookrightarrow y) \to ((x \hookrightarrow y) \hookrightarrow x) \to x)$. Then $((((x \hookrightarrow y) \hookrightarrow x) \to x) \hookrightarrow y) \to (((x \hookrightarrow y) \hookrightarrow x) \to x) = 1 \in f_t$ and $(x \hookrightarrow y) \hookrightarrow x) \to x \in f_t$ since f is a fuzzy Boolean filter. Combine that $(x \hookrightarrow y) \hookrightarrow x \in f_t$, according to the definition of filter, then we get $x \in f_t$.

According to the definition, f is fuzzy implicative. □

From the above results, we can get the following results as a solution for the open problem.

Theorem 4.5. *In pseudo BCK algebra or bounded pseudo BCK algebra, implicative pseudo filter is equivalent to Boolean filter.*

Remark 4.6. *The equivalent relation between the implicative pseudo filter and Boolean filter is of importance in the study of logical algebras. We discuss the properties of fuzzy implicative pseudo-filters and fuzzy Boolean filters in pseudo BCK algebras. Based on the results and previous work, we completely solve an open problem which is important in study of the algebraic structure of pseudo BCK algebras. For example, When studying of the relation between implicative pseudo-filter (Boolean filter) and implicative pseudo-BCK algebras, there is an open problem that "Prove or negate that pseudo BCK algebras is implicative BCK algebras if and only if every pseudo filters of them is implicative pseudo filters (or Boolean filter)[13]." Based on the results we have and some other results we obtained[29–31], we can completely solve the open problems like this.*

5. The Chinese Remainder Theorem in distributive lattice and its application

5.1. Congruence relation on filters of distributive lattice

Definition 5.1. *[6]A nonempty subset F of a lattice L is called a filter of L if it satisfies*
(1) $x \in F, y \in A, x \leq y \Rightarrow y \in F$,
(2) $x \in F, y \in F \Rightarrow x \wedge y \in F$.

Theorem 5.2. *Suppose F be a filter of a distributive lattice L. A binary relation $\equiv$ is defined as for $x, y \in L$, $x \equiv y(modF)$ if for some $z \in F$, $x \wedge z = y \wedge z$, then we can find that binary relation $\equiv$ is a congruence relation on L.*

Proof. It is easy to see that binary relation $\equiv$ has reflexivity and symmetry. Suppose for $x, y, z \in L$, $x \equiv y(modF)$ and $y \equiv z(modF)$, then there exist $h, t \in F$, such that $x \wedge h = y \wedge h$, $y \wedge t = z \wedge t$. So $x \wedge (h \wedge t) = y \wedge h \wedge t = y \wedge t \wedge h = z \wedge t \wedge h$, and $h \wedge t \in F$, then $x \equiv z(modF)$. Then binary relation $\equiv$ is an equivalent relation.

Suppose $x \equiv y(modF)$, then there exists some $z \in F$, such that $x \wedge z = y \wedge z$, then $\forall h \in L$, $(x \wedge z) \wedge h = (y \wedge z) \wedge h$, i.e., $(x \wedge h) \wedge z = (y \wedge h) \wedge z$, then $x \wedge h \equiv y \wedge h(modF)$.

In the same way, $x \equiv y(modF)$, then there exists some $z \in F$, such that $x \wedge z = y \wedge z$, then $\forall h \in L$, $(x \vee h) \wedge z = (x \wedge z) \vee (h \wedge z) = (y \wedge z) \vee (h \wedge z) = (y \vee h) \wedge z$, then $x \vee h \equiv y \vee h(modF)$.

Suppose $x \equiv y(modF)$ and $z \equiv h(modF)$, then $x \vee z \equiv y \vee z(modF)$ and $y \vee z \equiv y \vee h(modF)$, so $x \vee z \equiv y \vee h(modF)$.

In the same way, we can get $x \wedge z \equiv y \wedge h(modF)$. □

Remark 5.3. *Suppose F be a filter of a distributive lattice L. A congruence relation $\equiv$ can be induced by F. If we use $[x]_F$ to denote the equivalent class of x, i.e., $L/F = \{[x]_F | x \in F\}$. If we define $[x]_F \vee [y]_F = [x \vee y]_F$, $[x]_F \wedge [y]_F = [x \wedge y]_F$, then $(L/F, \vee, \wedge)$ is a distributive lattice.*

Theorem 5.4. *Suppose F be a filter of a distributive lattice L. If $x \in F$, then $[x]_F = F$.*

Proof. Suppose for $y \in [x]_F$, then there exist $h \in F$, such that $x \wedge h = y \wedge h$, since $x \wedge h = y \wedge h \in F, x \wedge h = y \wedge h \leq y$. So $y \in F$. On the other hand, if $y \in F$, then $x \wedge y \in F$, since $y \wedge (y \wedge x) = x \wedge (y \wedge x)$, then $y \equiv x(modF)$, i.e., $y \in [x]_F$. □

Corollary 5.5. *Suppose F be a filter of a distributive lattice L. If $x \in F$, then $\forall y \in L$, $x \equiv x \vee y(modF)$.*

Proof. $\forall y \in L$ and $x \in F$, $x \wedge x = (x \vee y) \wedge x$, so $x \equiv x \vee y(modF)$. □

Definition 5.6. *Suppose F_1, F_2 be two filters of a distributive lattice L. A filter F generated by $F_1 \cup F_2$ is called the sum of filters $F_1 and F_2$, denoted by $F = F_1 + F_2$.*

Lemma 5.7. *Suppose F_1, F_2 be two filters of a lattice L. Then $F_1 + F_2 = \{x | for some x_1 \in F_1, x_2 \in F_2, x \geq x_1 \wedge x_2\}$.*

Proof. Suppose $F = \{x | for some x_1 \in F_1, x_2 \in F_2, x \geq x_1 \wedge x_2$, so $F_1 \in F$ and $F_2 \in F$, then $F_1 + F_2 \subseteq F$. We have that any filter J containing F_1, F_2 must contain F: if $x \in F$, then for some $x_1 \in F_1$, $x_2 \in F_2$, $x \geq x_1 \wedge x_2$. And $x \geq x_1 \wedge x_2 \in J$, we get $x \in J$. i.e., $F \subseteq J$. And we have $F_1 + F_2 \supseteq F$.

Next we prove that F is a filter. Suppose $x_1 \wedge x_2 \leq y \leq x$, and $y \in F$, then $x \in F$. If $x, y \in F$, then for some $x_1, x' \in F_1$, $x_2, x'' \in F_2$, we have $x \geq x_1 \wedge x_2$, $y \geq x' \wedge x''$, so $x \wedge y \geq (x_1 \wedge x_2) \wedge (x' \wedge x'') = (x_1 \wedge x') \wedge (x_2 \wedge x'')$, and $x_1 \wedge x' \in F_1$, $x_2 \wedge x'' \in F_2$, we have $x \wedge y \in F$. □

Lemma 5.8. *Suppose F_1, F_2 be two filters of a distributive lattice L. Then $F_1 + F_2 = \{x \wedge y | for some x \in F_1, y \in F_2\}$.*

Proof. Suppose $x \in F_1 + F_2$, then for some $x_1 \in F_1$, $x_2 \in F_2$, we have $x \geq x_1 \wedge x_2$. And $x = x \vee (x_1 \wedge x_2) = (x \vee x_1) \wedge (x \wedge x_2)$, since $x_1 \leq x \vee x_1$, $x_2 \leq x \vee x_2$ and $x_1 \in F_1$, $x_2 \in F_2$, we get $x \vee x \vee x_1 \in F_1$, $x \vee x_2 \in F_2$. i.e., $F \subseteq J$. And we have $F_1 + F_2 \supseteq F$.

Next we prove that F is a filter. Suppose $x_1 \wedge x_2 \leq y \leq x$, and $y \in F$, then $x \in F$. If $x, y \in F$, then for some $x_1, x' \in F_1$, $x_2, x'' \in F_2$, we have $x \geq x_1 \wedge x_2$, $y \geq x' \wedge x''$, so $x \wedge y \geq (x_1 \wedge x_2) \wedge (x' \wedge x'') = (x_1 \wedge x') \wedge (x_2 \wedge x'')$, and $x_1 \wedge x' \in F_1$, $x_2 \wedge x'' \in F_2$, we have $x \wedge y \in F$. So $F_1 + F_2 \subseteq \{x \wedge y | for some x \in F_1, y \in F_2\}$, and $F_1 + F_2 \supseteq \{x \wedge y | for some x \in F_1, y \in F_2\}$ is obvious. □

5.2. The Chinese Remainder Theorem in distributive lattice

Theorem 5.9. *Suppose $F_i (i = 1 \cdots n)$ be filters of a distributive lattice L, such that $L = F_k + \bigcup_{i \neq k} F_i, k = 1, \cdots n$. If $b_1, b_2, \cdots b_n \in L$, then there exist $b \in L$, such that $b \equiv b_i(modF_i), i = 1, \cdots n$. And b is uniquely determined with respect to module filter $F_1 \wedge F_2 \wedge \cdots \wedge F_n$.*

Proof. for every k, $b_k \in L = F_k + \bigcup_{i \neq k} F_i, k = 1, \cdots n$. When $a_k \in F_k$, $r_k \in \bigcup_{i \neq k} F_i$, $b_k = a_k \wedge r_k$. On the other hand, $a_k \in F_k$, then $b_k \wedge a_k = a_k \wedge r_k \wedge a_k = r_k \wedge a_k$, so $b_k \equiv r_k(modF_i), i = 1, \cdots n$.

$r_k \in \bigcup_{i \neq k} F_i$, then $\forall d \in L$, $r_k \equiv r_k \vee d(modF_i), i = 1, \cdots n, i \neq k$. Let $d = r_i$, then $r_k \equiv r_k \vee r_i(modF_i), i = 1, \cdots n, i \neq k$. Let $b = r_1 \vee r_2 \vee \cdots \vee r_n \equiv (r_1 \vee r_k) \vee (r_2 \vee r_k) \vee \cdots \vee r_k \vee \cdots \vee (r_n \vee r_k)(modF_k) \equiv r_k(modF_k), k = 1, 2, \cdots, n$. So we get $b \equiv b_i(modF_i), i = 1, \cdots n$.

Then we prove the uniqueness. Suppose there exist $c \in L$, such that $c \equiv b_i(modF_i), i = 1, \cdots n$. Then $b \equiv c(modF_i), i = 1, \cdots n$. So there exists $d_k \in F_k$, such that $b \wedge d_k = c \wedge d_k, i = 1, \cdots n$. $(b \wedge d_1) \wedge (b \wedge d_2) \wedge \cdots \wedge (b \wedge d_n) = (c \wedge d_1) \wedge (c \wedge d_2) \wedge \cdots \wedge (c \wedge d_n)$, i.e., $b \wedge (d_1 \wedge d_2 \wedge \cdots \wedge d_n) = c \wedge (d_1 \wedge d_2 \wedge \cdots \wedge d_n)$, then we get $b \equiv c(modF_1 \wedge F_2 \wedge \cdots \wedge F_n)$. □

5.3. A new communication encoding scheme based on the Chinese Remainder Theorem in distributive lattice

Theorem 5.10. *Suppose L={the polynomial space on GF(2)}. A binary relation $\leq$ is defined as for $f(x), g(x) \in L$, $f(x) \leq g(x)$ if $f(x) | g(x)$, then $(L, \leq)$ is a partial ordered set.*

Theorem 5.11. *Suppose L=the polynomial space on GF(2). For $\forall f(x), g(x) \in L$, binary operations $\vee, \wedge$ are defined as $f(x) \vee g(x) = l.c.m.(f(x), g(x))$, $f(x) \wedge g(x) = g.c.d.(f(x), g(x))$, then $(L, \vee, \wedge)$ is a distributive lattice.*

Lemma 5.12. *Suppose F be a filter of a lattice L. Then $F = \{m(x)p(x) | m(x) \in L\}$, here $p(x)$ is the irreducible polynomial on L.*

Based on the Chinese remainder theorem of polynomials, we can design a secure communication scheme. Suppose L={the polynomial space on $GF(2)$}. For information flow "0 "or"1 ", the sender can separate it into several groups. For example, each group contains k code elements, which corresponds to a decimal number. Choose n modules (n different filters) on L: $F_1, F_2, \cdots, F_n$, by the Chinese remainder theorem in distributive lattice of polynomials, for the unique solution of the following congruence equations $F(x) \equiv f_i(x)(modF_i), i = 1, \cdots n$ can be obtained.

Based on the above analysis, a secure communication scheme can be designed as follows: after the sender and the receiver of the communication choose n modules (n different filters) on L: $F_1, F_2, \cdots, F_n$, the sender can send solution of the congruence equations group $F(x)$ directly through the channel, the receiver can obtain $f_i(x), i = 1, 2, \cdots, n$ by $F(x)modF_i$, then the receiver can get original information flow safely and effectively, so as to achieve the requirements of the secure communication.

5.4. Scheme analysis

In this paper, the secret communication scheme based on the Chinese remainder theorem of the polynomial has the following advantages:

(1) The original information sequence can be arbitrary separated;

(2) Module can be arbitrary chosen;

(3) System only need to transfer $F(x)$ secretly, transfer volume decreases. Even if $F(x)$ is obtained by an intruder, since he couldn't know the module and order, it is difficult to use $F(x)$ to get the original sequence;

(4) When the receiver needs to restore sequence, he only needs to perform modular operations, which is simpler and faster.By constructing the Chinese remainder theorem with respect to filters in distributive lattice of polynomials, a new kind of communication encoding scheme is obtained, and we analyze the security of the scheme.

References

[1] A. B. Saeid, S. Motamed, Normal filters in *BL*-algebras, World Applied Sciences Journal 7 (2009) 70–76.

[2] A. Dvurečenskij, R. Giuntini, T. Kowalski, On the structure of pseudo *BL*-algebras and pseudo Hoops in quantum logics, Foundations of Physics 40 (2010) 1519–1542.

[3] A. Iorgulescu, Iséki algebras, Connection with *BL*-algebras, Soft Comput 8 (2004) 449–463.

[4] A. Iorgulescu, Classes of Pseudo-*BCK* algebras : Part-I, J. Multiple Valued Logic and Soft Comput 12 (2006) 71–130.

[5] A. Iorgulescu, On pseudo-*BCK* algebras and porims, Scientiae Mathematicae Japonicae Online 10 (2004) 293–305.

[6] G. Birkhoof, Lattice theory, American Mathematical Society Colloquium, 1940.

[7] R. Balbes, P. Dwinger, Distributive lattices theory, University of Missouri Press, Columbia, America, 1974.

[8] B.V. Gasse, G. Deschrijver, C. Cornelis, E.E. Kerre, Filters of residuated lattices and triangle algebras, Information Sciences 180(16)(2010) 3006–3020.

[9] E. Turunen, Boolean deductive systems of *BL*-algebras, Arch. Math. Logic 40 (2001) 467–473.

[10] E. Turunen, Mathematics behind fuzzy logic, Physica-Verlag, Heidelberg, 1999.

[11] G. Georgescu, Bosbach states on fuzzy structures, Soft Comput 8 (2004) 217–230.

[12] G. Georgescu, A. Iorgulescu, Pseudo-BCK algebras: an extension of BCK algebras, Proceedings of DMTCS01: combinatorics, computability and logic, Springer, London (2001) 97–114.

[13] H. J. Gong, X. H. Zhang, Boolean filter and psMV-filter of pseudo-BCK algebras, Journal of Ningbo University 24(1)(2011) 49–53.

[14] J. M. Zhan, W. A. Dudek, Y.B. Jun, Interval valued $(\in, \in \vee q)$-fuzzy filters of pseudo BL-algebras, Soft Computing 13 (2009) 13–21.

[15] J. Meng, Y.B. Jun, *BCK*-algebras, Kyung Moon Sa Co., Seoul, Korea, 1994.

[16] J. Rachuảnek, D. Šalounová, Classes of filters in generalizations of commutative fuzzy structures 48 (2009) 93–107.

[17] K. Iséki, S. Tanaka, An introduction to the theory of *BCK*-algebras, Math Japon. 23 (1978) 1–26.

[18] K. Iséki, S. Tanaka, Ideal theory of *BCK*-algebras, Math. Japon. 21 (1976) 351–366.

[19] K. J. Lee, C. H. Park, Some ideals of pseudo BCI-algebras, J. Appl. Math. & Informatics 27 (2009) 217–231.

[20] L. C. Ciungu, Algebras on subintervals of pseudo-hoops, Fuzzy Sets and Systems 160 (2009) 1099–1113.

[21] L. Z. Liu, K. T. Li, Fuzzy filters of BL-algebras, Information Sciences 173 (2005) 141–154.

[22] L. L. Wang, X. H. Zhang, Necessary and sufficient conditions for residuated lattice and bounded psBCK-algebra to be Boolean algebra, Fuzzy Systems and Mathematics 24(5)(2010) 8–13.

[23] L. A. Zadeh, Fuzzy sets, Information and Control 8 (1965) 338–353.

[24] L. Z. Liu, K. T. Li, Fuzzy Boolean and positive implicative filters of *BL*-algebras, Fuzzy Sets and Systems 152 (2005) 333–348.

[25] M. Haveshki, A. Borumand Saeid, E. Eslami, Some types of filters in *BL* algebras, Soft Comput 10 (2006) 657–664.

[26] M. S. He, Y. S. Jian, Elementary number theory, Higher Education Press, Beijing, 2003.

[27] P. Hájek, Metamathematics of fuzzy logic, Kluwer, Dordrecht, 1998.

[28] P. Hájek, Observations on non-commutative fuzzy logic, Soft Computing 8 (2003) 38–43.

[29] W. Wang, H. Wan, K. Du, Y. Xu, On open problems based on fuzzy filters of pseudo BCK-algebras, Journal of Intelligent & Fuzzy Systems 29 (2015) 2387–2395.

[30] W. Wang, A. B. Saeid, Solutions to open problems on fuzzy filters of BL-algebras, International Journal of Computational Intelligence Systems 8(1)(2015) 106–113.

[31] W. Wang, X. L. Xin, On fuzzy filters of pseudo *BL*-algebras, Fuzzy Sets and Systems 162 (2011) 27–38.

[32] X. H. Zhang, W. H. Li, On pseudo-*BL* algebras and *BCC*-algebras, Soft Comput 10 (2006) 941–952.

[33] X. H. Zhang, X. S. Fan, Pseudo-*BL* algebras and pseudo-effect algebras, Fuzzy sets and systems 159(1)(2008) 95–106.

[34] X. H. Zhang, Y. B. Jun, Solution of three open problems on pseudo-filters (pseudo-ideals) of pseudo-*BCK* algebras, Proceedings of International Conference on Artificial Intelligence and Computational Intelligence (2011) 530–534.

[35] X. H. Zhang, H. J. Gong, Implicative pseudo-BCK algebras and implicative pseudo-Filters of pseudo-BCK algebras, 2010 IEEE International Conference on Granular Computing (2010) 615–619.

[36] X. H. Zhang, Y. B. Jun, M. I. Doh, On fuzzy filters and fuzzy ideals of BL-algebras, Fuzzy Systems and Mathematics 20 (2006) 8–20.

[37] X. L. Ma, J. M. Zhan, K. P. Shum, Interval valued $(\in, \in \vee q)$-fuzzy filters of MTL-algebras, Journal of Mathematical Research & Exposition 30 (2010) 265–276.

[38] Y. B. Jun, Implicative filters of lattice implication algebras, Bull. Korean Math. Soc. 34 (1997) 193–198.

[39] Y. B. Jun, Fuzzy positive implicative and fuzzy associative filters of lattice implication algebras, Fuzzy Sets and Systems 121 (2001) 353–357.

[40] Y. B. Jun, S. Z. Song, On fuzzy implicative filters of lattice implication algebras, The Journal of Fuzzy Mathematics 10 (2002) 893–900.

[41] Y. B. Jun, Y. Xu, X. H. Zhang, Fuzzy filters of *MTL*-algebras, Information Sciences 175 (2005) 120–138.

[42] Y. Xu, K. Y. Qin, On filters of lattice implication algebras, J. Fuzzy Math. 1 (1993) 251–260.