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

Wang Wei

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]
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 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 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 $\land$ and $\lor$ is called a lattice if for $x, y, z \in L$

1) $x \land x = x \lor x = x$, $x \land y = y \lor x$, $x \lor y = y \lor x$,
2) $(x \land y) \land z = x \land (y \lor z)$, $(x \lor y) \lor z = x \lor (y \lor z)$, $(x \land y) \lor x = (x \lor y) \land x = x$.

A binary relation $\leq$ is defined as for $x, y \in L$, $x \leq y$ if $x \land y = x \lor y = y$. 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 $x \land (y \lor z) = (x \land y) \lor (x \land z)$ or $x \lor (y \land z) = (x \lor y) \land (x \lor z)$;
2) bounded if there exists $0, 1 \in L$, such that $0 \leq x \leq 1$.

Definition 2.3. [15] A structure $(A, \to_1)$ is called an BCK algebra if for $x, y, z \in A$

1) $(x \to y) \to (y \to x)$ $\geq (y \to z)$, $(y \to x) \to x \geq y, x \geq x$,
2) $x \geq x$ and $y \geq x$ imply $x = y$, and $x \to 1 = 1(x \leq y \iff x \to y = 1)$.

Definition 2.4. [5] A pseudo BCK algebra is a structure $(A, \geq, \to, \rightarrow, 1)$, if for $x, y, z \in A$

1) $(x \to y) \rightarrow (y \to x)$ $\geq y \to z, (z \rightarrow x) \rightarrow (y \rightarrow x)$ $\geq y \to z, (y \to x) \rightarrow x \geq y, (y \to x) \rightarrow x \geq y, (y \to x) \rightarrow x \geq y$,
2) $x \geq x, 1 \geq x, x \geq y$ and $y \geq x$ imply $x = y, x \geq y$ if $y \to x = 1$ iff $y \rightarrow x = 1$.

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

Proposition 2.5. [4] In a pseudo BCK algebra $A$, the following properties hold for $x, y, z \in A$

1) $x \leq y \Rightarrow y \to z \leq x \to z$ and $y \rightarrow x \leq z \rightarrow y$ implies $x \leq z \to y$ and $z \to x \leq y$,
2) $z \to x \leq (y \to z) \rightarrow (y \to x)$, $z \rightarrow x \leq (y \to z) \rightarrow (y \to x)$, $z \rightarrow (y \to x) = y \rightarrow (z \to x)$.

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

Theorem 2.7. [12] In a pseudo BCK algebra(pP) $A$, the followings hold

1) $(x \land y) \rightarrow z = x \to (y \to z), (y \lor x) \rightarrow z = x \to (y \to z)$,
2) $(x \to y) \lor x \leq x, y \land (x \rightarrow y) \leq x, y \land y \leq x \land y \leq x, y.$
The operations $\lor, \land, \circ$ have priority towards the operations $\to, \leftrightarrow$.

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

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

**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 $x \equiv b_i (\text{mod } m_i), i = 1, \cdots, n$, the minimum solution is $x_0 = b_1 M_1 M_i + b_2 M_2 M_i + \cdots + b_n M_n M_i \text{mod } M$, here positive integer $M_i$ satisfying: $M_i M_i \equiv 1 (\text{mod } m_i), i = 1, \cdots, n$, 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

1. $x \in F, y \in A, x \leq y \Rightarrow y \in F$,
2. $x \to y \in F$ or $x \leftrightarrow y \in F \Rightarrow y \in F$.

**Theorem 3.2.** [29] A subset $F$ of $A$ is a pseudo-filter if and only if

1. $1 \in F$,
2. $x \in F, x \to y \in F$ or $x \leftrightarrow y \in F \Rightarrow y \in F$.

**Definition 3.3.** [35] For $x, y \in A$, a filter $F$ is called a(an)

1. Boolean if $(x \to y) \leftrightarrow x \in F$ and $(x \leftrightarrow y) \leftrightarrow x \in F$, then $x \in F$.
2. implicative if $(x \to y) \leftrightarrow x \in F$ and $(x \leftrightarrow y) \leftrightarrow x \in F$, 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. $(x \to 0) \to x \leftrightarrow x \in F, (0 \to x) \to x \leftrightarrow x \in F$,
2. $(x \to 0) \to x \leftrightarrow x \in F, (0 \to y) \to x \leftrightarrow x \in F$,
3. $(x \to y) \to y \in F$, then $(y \to x) \to x \leftrightarrow x \in F$, if $(x \to y) \leftrightarrow y \in F$, then $(y \to x) \to x \leftrightarrow x \in F$,
4. $(x \to y) \to y \in F$, then $(y \to x) \to x \leftrightarrow x \in F$, if $x \to y \in F$, then $(y \to x) \leftrightarrow x \to y \in F$.

**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 $\chi_f$ is a fuzzy pseudo-filter, where $\chi_f$ 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 $A(pP)$) iff and only if for $x, y, z \in A$, one the followings holds

1. $f(1) \geq f(x), f(y) \geq f(x) \land f(x \to y), f(1) \geq f(x), f(y) \geq f(x) \land f(x \to y), f(1)$, $f(1) \geq f(x) \land f(x \to y)$,
2. $f$ is order-preserving and $f(x \circ y) \geq f(x) \land f(y)$.

**Definition 3.7.** [29] For $x, y \in A$, a fuzzy pseudo-filter $f$ is called

1. implicative if $f((x \to y) \to x) = f(x), f((x \to y) \to x) = f(x), f((x \to y) \to x) = f(x)$.
2. Boolean if $f((x \to y) \to x) = f((x \to y) \to x) = f(x)$.

**Theorem 3.8.** [29] For a fuzzy implicative pseudo-filter $f$ of a bounded pseudo-BCK algebra $A$, then $\forall x \in A, f((x^- \to x) \to x) = f((x^- \to x) \to x) = f((x^- \to x) \to x) = f((x^- \to x) \to x) = f(1)$. 
Theorem 3.9. [29] A fuzzy pseudo-filter $f$ of $A$ is implicative(Boolean) if and only if $f_1$ is either empty or an implicative(Boolean) pseudo-filter for each $t \in [0, 1]$ if and only if $f_{1(1)}$ 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 $\chi_F$ is implicative(Boolean).

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

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 $f((y \rightsquigarrow x) \Rightarrow (x \rightsquigarrow x)) = 1$ for $x, y \in A$.

Corollary 3.14. Let $f$ be a fuzzy Boolean filter of a bounded $A$. Then $f((x \rightsquigarrow x)) = 1$ 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. 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 $f((x \Rightarrow y) \Leftrightarrow x) = 1$, then $(x \Rightarrow y) \Leftrightarrow x \in f_1$. From $x \leq ((x \Rightarrow y) \Leftrightarrow x) \Rightarrow x$, so $((x \Rightarrow y) \Leftrightarrow x) \Rightarrow y$ \leq $x \Rightarrow y$ and $(((x \Rightarrow y) \Leftrightarrow x) \Rightarrow y) \Rightarrow (x \Rightarrow y) = 1$. On the other hand, $x \Rightarrow y \leq ((x \Rightarrow y) \Leftrightarrow x) \Rightarrow x$, so we get $(((x \Rightarrow y) \Leftrightarrow x) \Rightarrow y) \Rightarrow (x \Rightarrow y) \leq (((x \Rightarrow y) \Leftrightarrow x) \Rightarrow y) \Rightarrow (((x \Rightarrow y) \Leftrightarrow x) \Rightarrow y) \Rightarrow (x \Rightarrow y) = 1$. Similarly, suppose $f((x \Rightarrow y) \Rightarrow x) = 1$, then $(x \Rightarrow y) \Rightarrow x \in f_1$. From $x \leq ((x \Rightarrow y) \Rightarrow x) \Rightarrow x$, so $((x \Rightarrow y) \Rightarrow x) \Rightarrow y \leq x \Rightarrow y$ and $(((x \Rightarrow y) \Rightarrow x) \Rightarrow y) \Rightarrow (x \Rightarrow y) = 1$. And $x \Rightarrow y \leq ((x \Rightarrow y) \Rightarrow x) \Rightarrow x$, so we get $(((x \Rightarrow y) \Rightarrow x) \Rightarrow y) \Rightarrow (x \Rightarrow y) \leq (((x \Rightarrow y) \Rightarrow x) \Rightarrow y) \Rightarrow (x \Rightarrow y) \Rightarrow (x \Rightarrow y) = 1$. Then $(((x \Rightarrow y) \Rightarrow x) \Rightarrow y) \Rightarrow (((x \Rightarrow y) \Rightarrow x) \Rightarrow y) \Rightarrow (x \Rightarrow y) = 1$. 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 \( f((x \rightarrow y) \rightarrow x) \in f \), then \((x \rightarrow y) \rightarrow x \in f \). From \( x \leq (x \rightarrow y) \rightarrow x \) \( \iff \), so \(((x \rightarrow y) \rightarrow x) \rightarrow y \leq x \rightarrow y \) and \(((x \rightarrow y) \rightarrow x) \rightarrow y \equiv (x \rightarrow y) = 1 \). On the other hand, \( x \rightarrow y \leq (x \rightarrow y) \rightarrow x \) \( \iff \), so we get \(((x \rightarrow y) \rightarrow x) \rightarrow y \equiv (x \rightarrow y) \leq (((x \rightarrow y) \rightarrow x) \rightarrow y) \equiv ((x \rightarrow y) \rightarrow x) \rightarrow x \). Then \(((x \rightarrow y) \rightarrow x) \rightarrow y \equiv (((x \rightarrow y) \rightarrow x) \rightarrow y) = 1 \in f \), and \(((x \rightarrow y) \rightarrow x) \rightarrow y \equiv (x \rightarrow y) \rightarrow x \in f \) since \( f \) is a fuzzy implicative filter. Combine that \((x \rightarrow y) \rightarrow x \in f \), according to the definition of filter, then we get \( x \in f \).

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

According to the definition, \( f \) is fuzzy implicative. \( \square \)

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 logic 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 the study of algebraic structures of pseudo BCK algebras. For example, when studying 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 filters)". 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. \( x \in F \), \( y \in F \) \( \Rightarrow \) \( x \wedge y \in F \),
2. \( x \in F \), \( y \in F \) \( \Rightarrow \) \( x \vee y \in F \).

**Theorem 5.2.** Suppose \( F \) be a filter of a distributive lattice \( L \). A binary relation \( \equiv \) is defined as for \( x, y \in L \), \( x \equiv y (mod F) \) 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 both relation \( \equiv \) has reflexility and symmetry. Suppose for \( x, y, z \in L \), \( x \equiv y (mod F) \) and \( y \equiv z (mod F) \), then there exist \( h, t \in F \), such that \( x \wedge h = y \wedge h \), \( y \wedge t = z \wedge t \). So \( x \wedge (h \wedge t) = y \wedge h \wedge t = y \wedge t = h = z \wedge t \). And \( h \wedge t \in F \), then \( x \equiv z (mod F) \). Then binary relation \( \equiv \) is an equivalent relation.

Suppose \( x \equiv y (mod F) \), 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 \( x \wedge h \equiv y \wedge h (mod F) \).

In the same way, \( x \equiv y (mod F) \), 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 h) \wedge (y \vee h) \wedge z = (y \wedge h) \wedge z , then \( x \vee h \equiv y \wedge h (mod F) \).

Suppose \( x \equiv y (mod F) \), then \( x \equiv y (mod F) \), and \( y \equiv z (mod F) \), then \( x \equiv y (mod F) \).

In the same way, we can get \( x \wedge z \equiv y \wedge z (mod F) \). \( \square \)

**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 \([x]_F \wedge [y]_F = [x \wedge y]_F \), \([x]_F \vee [y]_F = [x \vee y]_F \), 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 $y \equiv x (\bmod F)$, i.e., $y \in [x]_F$. □

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

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 $F_1 + F_2 = \{x | \text{forsome} x_1 \in F_1, x_2 \in F_2, x \geq x_1 \wedge x_2\}$.

Proof. Suppose $F = \{x | \text{forsome} x_1 \in F_1, x_2 \in F_2, x \geq x_1 \wedge x_2\}$, then $F_1 \cup F_2 \subseteq F$. 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 $x \geq x_1 \wedge x_2 \in J$, 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 $x_1, x_2' \in F_1, x_2 \in F_2$, we have $x \geq x_1 \wedge x_2 \leq x' \wedge x''$, 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 $F_1 + F_2 = \{x \wedge y | \text{forsome } x \in F_1, y \in F_2\}$.

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 $x = x \wedge (x_1 \wedge x_2) = (x \wedge x_1) \wedge (x \wedge x_2)$, since $x_1 \leq x \wedge x_1, x_2 \leq x \wedge x_2$ and $x_1, x_2 \in F_1, x_2 \in F_2$, we get $x \wedge x_1 \in F_1, x \wedge x_2 \in F_2$, 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 $x_1, x_2' \in F_1, x_2 \in F_2$, we have $x \geq x_1 \wedge x_2 \leq x' \wedge x''$, 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 $F_1 + F_2 \supseteq \{x \wedge y | \text{forsome } x \in F_1, y \in F_2\}$, and $F_1 + F_2 \supseteq \{x \wedge y | \text{forsome } x \in F_1, y \in F_2\}$ 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 $L = F_k \cup \bigcup_{k \neq 1} F_i, k = 1, \cdots n$. If $b_1, b_2, \cdots b_n \in L$, then there exist $b \in L$, such that $b \equiv b_i (\bmod F_i), i = 1, \cdots n$. And $b$ is uniquely determined with respect to module filter $F_1, F_2 \cdots F_n$.

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

$r_k \in \bigcup_{k \neq 1} F_i$, then $\forall d \in L, r_k \equiv r_k \vee d (\bmod F_i), i = 1, \cdots n, i \neq k$. Let $r = r_1 \lor r_2 \lor \cdots \lor r_n \equiv (r_1 \lor r_2) \lor (r_2 \lor r_3) \lor \cdots \lor (r_n \lor r_1) (\bmod F_i) \equiv r_1 (\bmod F_i), k = 1, 2, \cdots , n$. So we get $b \equiv b_i (\bmod F_i), i = 1, \cdots n$.

Then we prove the uniqueness. Suppose there exist $c \in L$, such that $c \equiv b_i (\bmod F_i), i = 1, \cdots n$. Then $b \equiv c (\bmod F_i), i = 1, \cdots n$. So there exists $d_k \in F_k$, such that $b \wedge d_k = c \wedge d_k, i = 1, \cdots n$. $(b \wedge d_1) \wedge (b \wedge d_2) \cdots \wedge (b \wedge d_n) = (c \wedge d_1) \wedge (c \wedge d_2) \cdots \wedge (c \wedge d_n)$, i.e., $b \wedge (d_1 \wedge d_2 \cdots \wedge d_n) = c \wedge (d_1 \wedge d_2 \cdots \wedge d_n)$, then we get $b \equiv c (\bmod F_1 \wedge F_2 \wedge \cdots \wedge F_n)$. □

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

Theorem 5.10. Suppose $L = \{\text{the polynomial space on } GF(2)\}$. 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 $L = \{\text{the polynomial space on } GF(2)\}$. For $f(x), g(x) \in L$, binary operations $\lor, \land$ are defined as $f(x) \lor g(x) = \text{l.c.m.}(f(x), g(x)), f(x) \land g(x) = \text{g.c.d.}(f(x), g(x))$, then $(L, \lor, \land)$ 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 reminder theorem of polynomials, we can design a secure communication scheme. Suppose \( L = \{ \text{the polynomial space on } GF(2) \} \). 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 \( L: F_1, F_2, \ldots, F_n \), by the Chinese remainder theorem in distributive lattice of polynomials, for the unique solution of the following congruence equations \( F(x) \equiv f_i(x)(mod F_i), i = 1, \ldots, n \) 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 \( L: F_1, F_2, \ldots, F_n \), the sender can send solution of the congruence equations group \( F(x) \) directly through the channel, the receiver can obtain \( f_i(x), i = 1, 2, \ldots, n \) by \( F(x) \mod F_i \), 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


