International Journal of Pure and Applied Mathematics

Volume 40 No. 3 2007, 439-447

POLYNOMIAL PERMUTATIONS ON FINITE LATTICES RELATED TO CRYPTOGRAPHY

Dietmar Dorninger[1], Helmut Länger[2] §

[1,2]Institute of Discrete Mathematics and Geometry
Vienna University of Technology
Wiedner Hauptstraße 8–10, Vienna, A–1040, AUSTRIA
[1]e-mail: d.dorninger@tuwien.ac.at
[2]e-mail: h.laenger@tuwien.ac.at

Abstract: Motivated by cryptography, permutations induced by polynomial functions on finite lattices $\mathcal{L} = (L, \vee, \wedge, ^*)$ with an antitone involution * are investigated. These permutations together with the operation of composition form a subgroup of the symmetric group on L. We describe the structure of this subgroup for different classes of lattices $\mathcal{L}$ and indicate possible applications by outlining a protocol for a symmetric cipher.

AMS Subject Classification: 06C15, 08A40, 06D30
Key Words: lattice, antitone involution, polynomial function, permutation, De Morgan algebra, polynomially complete, cryptographic protocol

1. Introduction

The procedure of encrypting and decrypting messages within cryptographic protocols is usually accomplished by means of mutually inverse bijections on a finite set which is endowed with an algebraic structure that serves to carry out the bijections effectively. Quite often, polynomial functions are employed for this end, like with RSA, where the underlying algebraic structure is a residue class ring of the integers and the bijections are realized by polynomial functions of the form $p(x) = x^r$.

In the following we suggest to make use of finite lattices for encoding and decoding messages. However, since any polynomial function on a lattice $(L, \vee, \wedge)$ is order preserving, we have to endow the lattice with an additional operation

Received: September 29, 2007

§Correspondence author

that makes it possible to build up appropriate polynomial functions. We agree to add an antitone involution * for this purpose. The algebra $\mathcal{L} = (L, \vee, \wedge, ^*)$ that arises this way will be called a **-lattice*. In case $\mathcal{L}$ is distributive, Boolean algebras and De Morgan algebras (Balbes et al [1]) are the best known examples, whereas in the non-distributive case ortholattices are exemplary. Yet we point out that $x \vee x^*$ has not to be the greatest element of $\mathcal{L}$ (or dually, $x \wedge x^*$ is not necessarily the least element of $\mathcal{L}$). We further agree that a polynomial function on a *-lattice $\mathcal{L}$ which is a permutation on L shall be called a *polynomial permutation* on $\mathcal{L}$.

The goal of this paper is to find and characterize polynomial permutations on $\mathcal{L}$ which can be used for cryptographic purposes.

After some preliminaries on *-lattices we describe a subgroup of the group of all polynomial permutations on an arbitrary *-lattice and prove that this subgroup exhausts all polynomial permutations if the lattice is a De Morgan algebra. Next we sort out *-lattices having only trivial polynomial permutations. Then we show that for every integer $n \geq 5$ there does exist a *-lattice $\mathcal{L}$ with n elements such that any permutation on L – even any one-place function on L – is a polynomial function, and we provide some further examples of lattices with non-trivial polynomial permutations. In Appendix a tentative cryptographic protocol is outlined.

2. Preliminaries about *-Lattices

We start with some straightforward generalizations of well-known properties of ortholattices. Since, with respect to cryptography, we only deal with finite algebras, we assume all lattices that occur to be finite (though most results in this paper carry over to the infinite case).

In the following let $\mathcal{L} = (L, \vee, \wedge, ^*)$ denote an arbitrary, but fixed finite *-lattice.

As with ortholattices we say that an element b of L *commutes* with an element a of L, in short $b \,\mathrm{C}\, a$, if $b = (b \wedge a) \vee (b \wedge a^*)$, and a is called a *central element* of $\mathcal{L}$ if every element of L commutes with a (cf. Kalmbach [5]). The set of all central elements of $\mathcal{L}$ will be called the *centre* of $\mathcal{L}$ and denoted by $\mathrm{C}(\mathcal{L})$. Since the greatest and smallest element of $\mathcal{L}$ always belong to $\mathrm{C}(\mathcal{L})$, $\mathrm{C}(\mathcal{L}) \neq \emptyset$.

Proposition 2.1. *Let $a \in \mathrm{C}(\mathcal{L})$ and put $x' := x^* \wedge a$ and $x^+ := x^* \wedge a^*$ for all $x \in L$. Then $\mathcal{L}_1 := ([0, a], \vee, \wedge, ')$ and $\mathcal{L}_2 := ([0, a^*], \vee, \wedge, ^+)$ are *-lattices, and $x \mapsto (x \wedge a, x \wedge a^*)$ and $(x, y) \mapsto x \vee y$ are mutually inverse isomorphisms between $\mathcal{L}$ and $\mathcal{L}_1 \times \mathcal{L}_2$.*

Proof. Let $b, c \in L$. Obviously, $'$ is an antitone mapping from $[0, a]$ to $[0, a]$. If $b \leq a$, then

$$(b')' = (b^* \wedge a)^* \wedge a = (b \vee a^*) \wedge (b \vee a) = b$$

which shows that $\mathcal{L}_1$ is a *-lattice. Analogously, it follows that $\mathcal{L}_2$ is a *-lattice.

Now $(b \wedge a) \vee (b \wedge a^*) = b$. If $(b, c) \in [0, a] \times [0, a^*]$ then

$$\begin{aligned}(b, c) \leq ((b \vee c) \wedge a, (b \vee c) \wedge a^*) \leq ((b \vee a^*) \wedge (b \vee a), (a \vee c) \wedge (a^* \vee c)) \\ = (b, c)\,,\end{aligned}$$

whence $((b \vee c) \wedge a, (b \vee c) \wedge a^*) = (b, c)$. Therefore the two mappings in Proposition 2.1 are mutually inverse bijections between L and $[0, a] \times [0, a^*]$.

If $b \leq c$ then $(b \wedge a, b \wedge a^*) \leq (c \wedge a, c \wedge a^*)$ and, conversely, if $(b \wedge a, b \wedge a^*) \leq (c \wedge a, c \wedge a^*)$ then

$$b = (b \wedge a) \vee (b \wedge a^*) \leq (c \wedge a) \vee (c \wedge a^*) = c.$$

From this and from $(b^* \wedge a, b^* \wedge a^*) = (b', b^+)$ we infer that $x \mapsto (x \wedge a, x \wedge a^*)$ is an isomorphism from $\mathcal{L}$ to $\mathcal{L}_1 \times \mathcal{L}_2$. □

In the following we make use of Proposition 2.1 without mentioning it explicitely.

Next we agree to call an element a of L *strongly distributive* if it is both distributive and standard (in the sense of Grätzer [4]), i.e. $(x \vee y) \wedge z = (x \wedge z) \vee (y \wedge z)$ and $(x \wedge y) \vee z = (x \vee z) \wedge (y \vee z)$ for all $x, y, z \in L$ with $a \in \{x, y, z\}$.

Lemma 2.1. *$\mathrm{C}(\mathcal{L})$ is the set of all strongly distributive elements a of $\mathcal{L}$ with $a \vee a^* = 1$.*

Proof. First assume $a \in \mathrm{C}(\mathcal{L})$. Then a is a strongly distributive element of $[0, a]$ and 0 is a strongly distributive element of $[0, a^*]$. Therefore $(a, 0)$ is a strongly distributive element of $[0, a] \times [0, a^*]$ and hence a a strongly distributive element of $\mathcal{L}$. Moreover, $a \vee a^* = (a \wedge 1) \vee (a^* \wedge 1) = 1$. If, conversely, a is strongly distributive and $a \vee a^* = 1$ then $(x \wedge a) \vee (x \wedge a^*) = x \wedge (a \vee a^*) = x \wedge 1 = x$ for all $x \in L$, i.e. $a \in \mathrm{C}(\mathcal{L})$. □

Lemma 2.2. *$(\mathrm{C}(\mathcal{L}), \vee, \wedge, ^*)$ is a subalgebra of $\mathcal{L}$ which is a Boolean algebra.*

Proof. Let $a, b \in \mathrm{C}(\mathcal{L})$. Then for all $c \in L$ we have by Lemma 2.1

$$\begin{aligned}&(c \wedge (a \vee b)) \vee (c \wedge (a \vee b)^*) \\ &\quad = (c \wedge a) \vee (c \wedge b) \vee (c \wedge a^* \wedge b^*)\end{aligned}$$

$$= (c \wedge a) \vee (c \wedge (a^* \wedge b^*)) \vee (c \wedge b) \vee (c \wedge (a^* \wedge b^*))$$
$$= (c \wedge (a \vee (a^* \wedge b^*))) \vee (c \wedge (b \vee (a^* \wedge b^*)))$$
$$= (c \wedge (a \vee b^*)) \vee (c \wedge (a^* \vee b)) = (c \wedge a) \vee (c \wedge b^*) \vee (c \wedge a^*) \vee (c \wedge b)$$
$$= (c \wedge a) \vee (c \wedge a^*) \vee (c \wedge b) \vee (c \wedge b^*) = c \vee c = c,$$

i.e., $a \vee b \in \mathrm{C}(\mathcal{L})$. Since $\mathrm{C}(\mathcal{L})$ is also closed with respect to *, the same is true for $\wedge$. The rest of the proof follows from Lemma 2.1. □

Generalizing the symmetric difference on Boolean algebras we define two binary operations $+_1$ and $+_2$ on L by

$$x +_1 y := (x \wedge y^*) \vee (x^* \wedge y) \quad \text{and} \quad x +_2 y := (x \vee y) \wedge (x^* \vee y^*)$$

for all $x, y \in L$. Obviously, $x +_1 0 = x +_2 0 = x$, $x +_1 1 = x +_2 1 = x^*$, $x +_1 x = x +_2 x = x \wedge x^*$, $x +_1 x^* = x +_2 x^* = x \vee x^*$, $(x +_1 y)^* = x +_2 y^* = x^* +_2 y$ and $(x +_2 y)^* = x +_1 y^* = x^* +_1 y$ for all $x, y \in L$.

Lemma 2.3. *For $a \in \mathrm{C}(\mathcal{L})$ and an arbitrary element c of L, $a +_1 c = a +_2 c$.*

Proof. In $[0, a] \times [0, a^*]$ we have

$$(a, 0) +_1 (c \wedge a, c \wedge a^*) = (a +_1 (c \wedge a), 0 +_1 (c \wedge a^*)) = ((c \wedge a)', c \wedge a^*)$$
$$= (a +_2 (c \wedge a), 0 +_2 (c \wedge a^*)) = (a, 0) +_2 (c \wedge a, c \wedge a^*). \quad \square$$

If, in the following $x, y \in L$ and $\{x, y\} \cap \mathrm{C}(\mathcal{L}) \neq \emptyset$, then we will write $x + y$ instead of $x +_1 y$ as well as instead of $x +_2 y$ (because then $x +_1 y = x +_2 y$ according to Lemma 2.3).

Lemma 2.4. *For $a, b \in \mathrm{C}(\mathcal{L})$ and $c \in L$, $a + b \in \mathrm{C}(\mathcal{L})$ and $(a + b) + c = a + (b + c)$.*

Proof. From Lemma 2.2 we infer that $\mathrm{C}(\mathcal{L})$ is closed with respect to $+$. Moreover, in $[0, a] \times [0, a^*]$ we have

$$((a, 0) + (b \wedge a, b \wedge a^*)) + (c \wedge a, c \wedge a^*)$$
$$= ((a + (b \wedge a)) + (c \wedge a), (0 + (b \wedge a^*)) + (c \wedge a^*))$$
$$= ((b \wedge a)' + (c \wedge a), (b \wedge a^*) + (c \wedge a^*))$$
$$= (((b \wedge a) + (c \wedge a))', (b \wedge a^*) + (c \wedge a^*))$$
$$= (a + ((b \wedge a) + (c \wedge a)), 0 + ((b \wedge a^*) + (c \wedge a^*)))$$
$$= (a, 0) + ((b \wedge a, b \wedge a^*) + (c \wedge a, c \wedge a^*)). \quad \square$$

Proposition 2.2. $(\mathrm{C}(\mathcal{L}), +)$ *is a group of exponent* 2.

Proof. This follows from Lemmata 2.4 and 2.1. □

3. Groups of Polynomial Permutations on *-Lattices

In the following let $\mathrm{P}(\mathcal{L})$ denote the set of all polynomial functions on $\mathcal{L}$ and $\mathrm{PP}(\mathcal{L})$ the set of all polynomial permutations on $\mathcal{L}$. Since L is finite, $p^{-1} = p^{|L|!-1}$ for all $p \in \mathrm{PP}(\mathcal{L})$ and hence $(\mathrm{PP}(\mathcal{L}), \circ)$ forms a subgroup of the symmetric group on L. For any $a \in \mathrm{C}(\mathcal{L})$ let p_a denote the mapping

$$x \mapsto a + x = (a^* \wedge x) \vee (a \wedge x^*) = (a \vee x) \wedge (a^* \vee x^*)$$

on L.

Theorem 3.1. *$(\{p_a \mid a \in \mathrm{C}(\mathcal{L})\}, \circ)$ is a subgroup of $(\mathrm{PP}(\mathcal{L}), \circ)$ of exponent 2 and $a \mapsto p_a$ is an isomorphism from $(\mathrm{C}(\mathcal{L}), +)$ to this subgroup.*

Proof. For $a, b \in \mathrm{C}(\mathcal{L})$ and $c \in L$ we have

$$(p_a \circ p_b)(c) = p_a(p_b(c)) = a + (b + c) = (a + b) + c = p_{a+b}(c)$$

and hence $(p_a \circ p_a)(c) = p_{a+a}(c) = p_0(c) = c$ according to Lemma 2.4, Proposition 2.2 and $p_a(0) = a$. The rest of the proof follows from Proposition 2.2. □

In general, $(\{p_a \mid a \in \mathrm{C}(\mathcal{L})\}, \circ)$ will be a proper subgroup of $(\mathrm{PP}(\mathcal{L}), \circ)$. This can be seen as follows:

Let $\mathcal{M}_k := (M_k, \vee, \wedge)$ for $k \geq 3$ denote the lattice with $k + 2$ elements and k atoms and $\mathcal{M}_k^*$ an arbitrary extension of $\mathcal{M}_k$ to a *-lattice. Since $\mathcal{M}_k$ is order polynomially complete, i.e. every order preserving function on M_k is a polynomial function on $\mathcal{M}_k$ (cf. Dorninger [2] or Wille [6]), every permutation on M_k fixing 0 and 1 is a polynomial permutation on $\mathcal{M}_k^*$. Therefore $\mathcal{M}_k^*$ possesses at least $k!$ polynomial permutations whereas at most $k + 2$ are of the form mentioned in Theorem 3.1.

We will generalize this example in Section 4.

A distributive *-lattice is called a *De Morgan algebra*.

Next we show that in case $\mathcal{L}$ is a De Morgan algebra (cf. Balbes et al [1]), $\mathrm{PP}(\mathcal{L}) = \{p_a \mid a \in \mathrm{C}(\mathcal{L})\}$.

Obviously, the central elements of a De Morgan algebra $\mathcal{L}$ are exactly the elements a of L satisfying $a \vee a^* = 1$.

Theorem 3.2. *If $\mathcal{L}$ is a De Morgan algebra then $\mathrm{PP}(\mathcal{L}) = \{p_a \mid a \in \mathrm{C}(\mathcal{L})\}$.*

Proof. From Dorninger et al [3] we know that any polynomial function on $\mathcal{L}$ has the form $p(x) = (a \wedge x \wedge x^*) \vee (b \wedge x) \vee (c \wedge x^*) \vee d$ with $a, b, c, d \in L$ satisfying $a \geq b \vee c$ and $b \wedge c \geq d$. If, in addition, p is a permutation, we must have: From $d \leq p(x) \leq a$ and $0, 1 \in p(L)$ it follows that $d = 0$ and $a = 1$, hence

$p(x) = (x \wedge x^*) \vee (b \wedge x) \vee (c \wedge x^*)$. Further, $p(b \vee b^*) = b = p(1)$ implies $b \vee b^* = 1$ and $p(c \wedge c^*) = c = p(0)$ yields $c \wedge c^* = 0$. Therefore $p(b^*) = b \wedge c = p(c)$, from which we infer $b^* = c$. Using distributivity we obtain

$$(b \wedge x) \vee (b^* \wedge x^*) = (b \vee x^*) \wedge (b^* \vee x) \wedge (x \vee x^*) \geq x \wedge x^*.$$

This implies

$$p(x) = (x \wedge x^*) \vee (b \wedge x) \vee (b^* \wedge x^*) = (b \wedge x) \vee (b^* \wedge x^*) = p_{b^*}(x). \qquad \square$$

Looking for *-lattices that could be useful in respect to cryptography we have to sort out all *-lattices that have exactly one atom, because of

Theorem 3.3. *If $\mathcal{L}$ has exactly one atom then* $\mathrm{PP}(\mathcal{L}) = \{x, x^*\}$.

Proof. If $|L| \leq 3$, $\mathcal{L}$ is a De Morgan algebra and the assertion of the theorem follows from Theorem 3.2. Now assume $|L| \geq 4$. Let $p \in \mathrm{P}(\mathcal{L})$ and $a \in L$. We show by induction on the shortest length $l^*(p)$ of the representation of p as a word in $L \cup \{x, x^*\}$ composed by $\vee$ and $\wedge$ that

$$\begin{array}{llll} (1) & p(0) = 0 \Rightarrow p(a) \leq a; & (2) & p(0) = 1 \Rightarrow p(a) \geq a^*; \\ (3) & p(1) = 0 \Rightarrow p(a) \leq a^*; & (4) & p(1) = 1 \Rightarrow p(a) \geq a. \end{array}$$

The assertions (1) – (4) are correct if $l^*(p) \leq 2$ since then p is of one of the forms b, x, x^*, $x \wedge b$, $x \vee b$, $x^* \wedge b$, $x^* \vee b$, $x \vee x^*$ or $x \wedge x^*$ with $b \in L$.

If $p = q \vee r$ with $l^*(q), l^*(r) < l^*(p)$ then

$$\begin{aligned} &p(0) = 0 \Rightarrow q(0) = r(0) = 0 \Rightarrow q(a), r(a) \leq a \Rightarrow p(a) \leq a, \\ &p(0) = 1 \Rightarrow q(0) = 1 \text{ or } r(0) = 1 \Rightarrow q(a) \geq a^* \text{ or } r(a) \geq a^* \Rightarrow p(a) \geq a^*, \\ &p(1) = 0 \Rightarrow q(1) = r(1) = 0 \Rightarrow q(a), r(a) \leq a^* \Rightarrow p(a) \leq a^* \text{ and} \\ &p(1) = 1 \Rightarrow q(1) = 1 \text{ or } r(1) = 1 \Rightarrow q(a) \geq a \text{ or } r(a) \geq a \Rightarrow p(a) \geq a. \end{aligned}$$

If $p = q \wedge r$ with $l^*(q), l^*(r) < l^*(p)$ then

$$\begin{aligned} &p(0) = 0 \Rightarrow q(0) = 0 \text{ or } r(0) = 0 \Rightarrow q(a) \leq a \text{ or } r(a) \leq a \Rightarrow p(a) \leq a, \\ &p(0) = 1 \Rightarrow q(0) = r(0) = 1 \Rightarrow q(a), r(a) \geq a^* \Rightarrow p(a) \geq a^*, \\ &p(1) = 0 \Rightarrow q(1) = 0 \text{ or } r(1) = 0 \Rightarrow q(a) \leq a^* \text{ or } r(a) \leq a^* \Rightarrow p(a) \leq a^* \\ &\quad \text{and} \\ &p(1) = 1 \Rightarrow q(1) = r(1) = 1 \Rightarrow q(a), r(a) \geq a \Rightarrow p(a) \geq a. \end{aligned}$$

Now let $p \in \mathrm{PP}(\mathcal{L})$ and let Θ denote the equivalence relation on L with the classes $\{0\}$, $\{1\}$ and $L \setminus \{0, 1\}$. Then Θ is a congruence on $\mathcal{L}$, and since every

polynomial function is compatible with every congruence, $p(\{0,1\}) = \{0,1\}$. Therefore there are two possibilities: Either $p(0) = 0$ and $p(1) = 1$ which implies $x \leq p(x) \leq x$ by (1) and (4) leaving $p(x)$ to be x, or $p(0) = 1$ and $p(1) = 0$ which implies $x^* \leq p(x) \leq x^*$ by (2) and (3), from which we infer $p(x) = x^*$. □

4. *-Lattices with Non-Trivial Polynomial Permutations

By Theorem 3.1 we obtained a group of involutory polynomial permutations which perfectly fit for symmetric chiffres (see Appendix). In the following we exemplarily construct a class of *-lattices that have polynomial permutations of order greater than two and could therefore be of interest in the non-symmetric case.

Example 4.1. Assume $\mathrm{C}(\mathcal{L}) \neq \{0,1\}$ and let $\overline{\mathcal{L}} = (\overline{L}, \vee, \wedge, ^*)$ be an extension of $\mathcal{L}$ obtained by adding an element $c = c^* \notin L$ to L which is incomparable to all elements of $L \setminus \{0,1\}$. Then $\overline{\mathcal{L}}$ is also a *-lattice. Let $a \in \mathrm{C}(\mathcal{L}) \setminus \{0,1\}$ and define $p_a(x) := (x \wedge a^*) \vee (x^* \wedge a)$ for all $x \in \overline{L}$. Obviously, $p_a | L \in \mathrm{PP}(\mathcal{L})$. Put $p(x) := p_a(x) \vee (p_a(x^*) \wedge c)$ for all $x \in \overline{L}$. Then p is a polynomial permutation on $\overline{\mathcal{L}}$ of order greater than two since $p = p_a$ on $L \setminus \{a\}$ and $p_a(a) = 0$ and hence $p(L \setminus \{a\}) = L \setminus \{0\}$, $p(a) = c$, $p(c) = 0$ and $p(p(a)) = p(c) = 0 \neq a$.

Theorem 4.1. *For any $n \geq 5$ there exists a *-lattice $\mathcal{L}$ with n elements such that any function on L and therefore any permutation of L is a polynomial function, i.e. $\mathcal{L}$ is polynomially complete.*

Proof. As already mentioned the lattice $\mathcal{M}_k$ we have defined above is order polynomially complete. Therefore, if f is an arbitrary function on M_k and one defines functions g, h, k, l on M_k by

$$g(x) := \left\{ \begin{array}{c} 0 \\ f(x) \\ 1 \end{array} \right\} \text{ if } x \left\{ \begin{array}{l} = 0 \\ \neq 0,1 \\ = 1 \end{array} \right. \qquad h(x) := \left\{ \begin{array}{c} 0 \\ f(x^*) \\ 1 \end{array} \right\} \text{ if } x \left\{ \begin{array}{l} = 0 \\ \neq 0,1 \\ = 1 \end{array} \right.$$

$$k(x) := \left\{ \begin{array}{c} 0 \\ f(0) \end{array} \right\} \text{ if } x \left\{ \begin{array}{l} \neq \\ = \end{array} \right\} 1 \qquad l(x) := \left\{ \begin{array}{c} 0 \\ f(1) \end{array} \right\} \text{ if } x \left\{ \begin{array}{l} \neq \\ = \end{array} \right\} 1.$$

then g, h, k, l are order preserving and hence polynomial functions on $\mathcal{M}_k$ and

$$f = (((h \wedge (g \circ x^*)) \vee k) \circ x^*) \vee ((g \wedge (h \circ x^*)) \vee l)$$

which shows that $f \in \mathrm{P}(\mathcal{M}_k^*)$. □

References

[1] R. Balbes, P. Dwinger, *Distributive Lattices*, Univ. of Missouri Press, Columbia (1974).

[2] D. Dorninger, A note on local polynomial functions over lattices, *Algebra Universalis*, **11** (1980), 135-138.

[3] D. Dorninger, D. Schweigert, Zur Darstellung von Polynomen auf De Morgan Algebren, *Czechoslovak Math. J.*, **30** (1980), 65-70.

[4] G. Grätzer, *General Lattice Theory*, Second Edition, Birkhäuser, Basel (1998).

[5] G. Kalmbach, *Orthomodular Lattices*, Academic Press, London (1983).

[6] R. Wille, Eine Charakterisierung endlicher, ordnungspolynomvollständiger Verbände, *Arch. Math.*, **28** (1977), 557-560.

Appendix

In the following we formulate a tentative protocol for a symmetric cipher based on *-lattices without discussing questions of complexity (and hence security) and problems of implementation. It can be easily seen how this protocol might be generalized to the non-symmetric case, for which questions of security are of even greater importance.

The study of such public key cryptosystems based on *-lattices together with problems of security and implementation will be the subject of future research, with the emphasis then on the computer science point of view.

A Symmetric Cipher

Given an index set $I = \{1, \dots, n\}$, n large, let $\mathbf{L} = \{\mathcal{L}_i \mid i \in I\}$ be a set of finite *-lattices $\mathcal{L}_i$ with the property that $|L_i| \geq |A|$ for any $i \in I$, where A is an alphabet that is represented by elements of L_i, not necessarily the same choice within every L_i (if e.g. A is the ASCII-Code, $|L_i| \geq 256$ for every $i \in I$).

Two participants who want to exchange secret information commonly agree on a selection of elements of I, repetitions allowed, in a well-defined order: $i_1, \dots, i_m$, and on a choice $a_k \in \mathrm{C}(\mathcal{L}_{i_k})$, for $k = 1, \dots, m$, m assumed to be large.

Put

$$\mathcal{L}' := \prod_{k=1}^{m} \mathcal{L}_{i_k} = (L', \vee, \wedge, ^*)\,,$$

$a := (a_1, \ldots, a_m)$ and $p_a := (p_{a_1}, \ldots, p_{a_m})$.

Then $(\mathcal{L}', p_a)$ can be taken as a common secret key, and blocks $x \in L'$ of the plain text are encoded by $y = p_a(x)$. The cipher text y is then recovered by $p_a(y) = p_a(p_a(x)) = x$.