l. 12, No. 1, 2001

PU.M.A.

Pure Mathematics and Applications

Volume 12, Number 2, 2001

Department of Mathematics, Budapest University of Economics
Department of Mathematics, University of Siena

Some applications of non-associative algebraic systems in cryptology

J. DÉNES
Csaba utca 10, Budapest H-1122, Hungary

and

A.D. KEEDWELL
Department of Mathematics and Statistics
University of Surrey, Guilford GU2 7XH, Surrey, U.K.

(Received: April 7, 2001)

Abstract. We survey applications of non-associative algebraic systems to cryptology in the past, present and future.

"The point of civilization is the exchange of ideas. And where is this exchange if everybody writes and nobody reads?" – Pope Gregory IX, 1227–1241.

Mathematics Subject Classifications (2000). 05B15, 20D99, 20N05, 94B60

1 Introduction

Hitherto, almost all constructions of error detecting and correcting codes and almost all cryptographic algorithms and enciphering systems have made use of associative algebraic structures such as groups and fields, the most-notable exceptions being those described in the work of R. Schauffler. The latter author was the first, and almost the only one to apply non-associative systems for the purposes both of constructing error detecting codes and of deciphering encrypted messages.

In this article, we shall draw attention by means of examples and suggestions for new constructions to the very considerable advantages of using non-associative algebraic systems particularly in connection with the design of cryptographic enciphering systems and decoding algorithms. However, we should like to emphasize that our purpose is not to provide ready-to-use cryptographic protocols but rather to describe past applications of such non-associative systems, mention recently implemented ones and indicate some of the ways in which we expect these systems to be used in the future.

2 Historical background

The earliest methods of enciphering messages involved the use of monoalphabetic ciphers. Later came polyalphabetic ciphers and, in particular, the Vigenère cipher (which in fact was invented somewhat earlier than Vigenère's lifetime by Trithemius). In effect, this makes use of a 26 × 26 square array containing the 26 letters of the alphabet (assuming that the language is English) arranged in a latin square. Different rows of this square array are used for enciphering the various letters of the plaintext in a manner prescribed by the keyword or keyphrase. (For more details of these early enciphering methods, see, for example, [B1] or [K1].) Since a latin square is the multiplication table of a quasigroup (see [D3] for details), this may be regarded as the earliest use of a non-associative algebraic structure in cryptography. Indeed, R. Schauffler in his Ph. D. dissertation [S1] of 1948 thought of it in exactly this way. He discussed the minimum amount of plaintext and corresponding ciphertext which would be required to break the Vigenère cipher (and the various mechanically produced extensions of it which were in use at that time). That is, he considered the minimum number of entries of a particular latin square which would determine the square completely. Recently, this problem has re-arisen as the problem of determining so-called critical sets in latin squares. (For a survey of recent work on critical sets, see [K6].)

More recent enciphering systems which may be regarded as extensions of Vigenère's (or Trithemius's) idea are the mechanical machines such as Jefferson's wheel and the M-209 Converter (used by the U.S. Army until the early 1950's) and the electronically produced stream ciphers of the present day.

In [K10] (and, in brief outline, in his earlier paper [K9]), C. Kościelny has shown how quasigroup/neofield-based stream ciphers may be produced which are both more efficient and more secure than those based on groups/fields. The present authors know of virtually no other serious attempts to employ non-associative algebraic systems as cryptographic tools. R.A. Rueppel's book [R3], for example, does not mention the use of non-associative systems at all despite the fact that, in the opinion of at least one of the present authors, it is the most comprehensive book on the subject of stream ciphers. However, it is worth noting that several of the early professional cryptographers, in particular A.A. Albert [A1], J.B. Rosser [R1], [R2] and E. Schönhardt [S4] (see also [D3]), were closely connected with the development of the theory of latin squares (quasigroups).

As regards the concept of error detecting and correcting codes, this is usually considered to have arisen from the work of M.J.E. Golay [G1] and of R.W. Hamming [H1], published in 1949 and 1950 respectively, and almost all subsequent developments have employed groups, fields and vector spaces. However, a short paper of much earlier date is that of W.F. Friedman and C.J. Mendelsohn [F4] who, in the early 1930's, worked in the mathematical branch of the U.S. cryptography service. Also, it is perhaps worthy of mention that, in a recent talk, P.J. Cameron [C1] drew attention to the fact that some of the work of R.A. Fisher [F2] and [F3] on minimal confounding (in the 1940's) uses mathematics which almost exactly parallels that used by Hamming for the construction of error correcting codes and so, in some sense, might be said to predate the latter's work. For a short description, see pages 79–82 of D.J. Finney [F1]. On this topic (that of error detecting and correcting codes) also, there have been a few very effective, but largely overlooked, alternative developments making use of non-associative algebraic systems. During the second World War while working for the German cryptography service, R. Schauffler developed a method of error detection based on the use of generalized identities (as they were later called by V.D. Belousov [B2]) in which the check digits are calculated by means of an associative system of quasigroups (latin squares). He pointed out that the resulting message would be more difficult to decode by an unauthorized receiver than is the case when a single associative operation is used for the calculation. (For more details, see [D3] especially page 365.). For obvious reasons, this work was kept secret at the time but, much later, in 1956, it was published (see [S2]). Despite the late publication date, it may well have pre-dated the work of Hamming. Later developments along the same lines have been made by A. Ecker and G. Poch [E1], R.H. Schulz [S5], [S6], [S7] and others. (Only Schulz has acknowledged the earlier work of Schauffler.)

Another, quite different, method of constructing (non-binary) error detecting and error correcting codes based on latin squares has been introduced by S.W. Golomb and E.C. Posner [G2] and further developed by J. Dénes et al in [D6]. The latter paper contains a detailed bibliography of recent results on Golomb-Posner codes and their generalizations while details of Golomb and Posner's early work and of a very few other constructions which use non-associative algebraic systems will be found in Section 10.1 of [D3]. Also, Chapter 9 of [D4] is devoted to this topic so, in the present paper, our main emphasis will be on cryptology. (A very recently published book which discusses the use of non-associative algebraic systems in coding theory and cryptography is [L2]. Also, [H2] contains a short chapter on this topic.)

3 Basic definitions

We assume that most of our readers will be familiar with the basic concepts of cryptology but that they may not be so familiar with some of the algebraic structures which we shall employ. Most basic is the structure called a quasigroup which we have already referred to in the preceding Section.

DEFINITION 3.1 A quasigroup $(Q, \circ)$ consists of a set Q of symbols on which a binary operation $(\circ)$ is defined such that (i) for all pairs of elements $a, b \in Q$, $a \circ b \in Q$ (*closure*) and (ii) for all pairs, $a, b \in Q$, there exist unique elements $x, y \in Q$, such that $x \circ a = b$ and $a \circ y = b$ (*unique solubility of equations*).

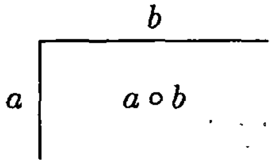

Figure 3.1.

When Q is finite (of (cardinal n), the quasigroup can be completely defined by means of its *multiplication table* (or *Cayley table*) which is an $n \times n$ square array bordered by the elements of Q in which the entry in the cell (a, b) is the element $a \circ b$ (see Figure 3.1). Because the equation $x \circ c = d$ is uniquely soluble for x, there is one and only one cell in the cth column which contains d. Similarly, because the equation $c \circ y = d$ is uniquely soluble for y, there is one and only one cell in the cth row which contains d. A square $n \times n$ array with the latter properties is called a *latin square* of order n.

A quasigroup may possess some or all of the following properties:

(i) for all $a, b, c \in Q$, $(a \circ b) \circ c = a \circ (b \circ c)$ (*the associative law*);

(ii) for all $a, b \in Q$, $a \circ b = b \circ a$ (*the commutative law*);

(iii) there exists an element $e \in Q$ such that, for all $a \in Q$, $e \circ a = a = a \circ e$. (*existence of a two-sided identity elemen*);

(iv) for each $a \in Q$, there exists an element $a_L^{-1} \in Q$ such that $a_L^{-1} \circ (a \circ b) = b$ for all $b \in Q$ (*the left inverse property*);

(v) for each $a \in Q$, there exists an element $a_R^{-1} \in Q$ such that $(b \circ a) \circ a_R^{-1} = b$ for all $b \in Q$ (*the right inverse property*);

(vi) for each $a \in Q$, there exists an element $a'_L \in Q$ such that $a'_L \circ (b \circ a) = b$ for all $b \in Q$ (*the left crossed-inverse property*);

(vii) for each $a \in Q$, there exists an element $a'_R \in Q$ such that $(a \circ b) \circ a'_R = b$ for all $b \in Q$ (*the right crossed-inverse property*).

A number of the above properties are inter-dependent. The most important of the connections for our purposes are the following:

(a) A quasigroup which satisfies (i) is called a *group*. If it also satisfies (ii), it is an *abelian group*. Every group satisfies (iii), (iv), (v). If and only if it is abelian, the group also satisfies (vi), (vii).

(b) A quasigroup which satisfies (iii) is called a *loop*. An associative loop is a group.

(c) A quasigroup which satisfies (iv) and (v) is called an *inverse-property quasigroup*. One which satisfies (vi) and (vii) is called a *crossed-inverse-property quasigroup*. For a quasigroup which is commutative, (iv) $\Leftrightarrow$ (vi) and (v) $\Leftrightarrow$ (vii) so the inverse and crossed inverse properties coincide.

LEMMA 3.1 *A quasigroup $(Q, \circ)$ of finite order which has the left crossed-inverse property also has the right crossed-inverse property; and conversely.*

Proof. The left crossed-inverse property states that, for every element $a \in Q$, there exists an element $a'_L \in Q$ such that $a'_L \circ (b \circ a) = b$ for every $b \in Q$. To each $a \in Q$, there corresponds a unique a'_L because the equation $x \circ (b \circ a) = b$ has a unique solution $x = a'_L$. Also, distinct elements $a_1, a_2 \in Q$ have distinct left inverses because $(a_1')_L = (a_2')_L = a_L'$ would imply $a_L' \circ (b \circ a_1) = b = a_L' \circ (b \circ a_2)$ and so, by the unique solubility of equations, $b \circ a_1 = b \circ a_2$ whence $a_1 = a_2$. It follows that, given $c \in Q$, there exists a unique $c' \in Q$ such that $c \circ (b \circ c') = b$ for all $b \in Q$. Let d be an arbitrary element of Q. By the solubility of equations, there exists an element $b \in Q$ such that $d = b \circ c'$. Then, $c \circ d = c \circ (b \circ c') = b$ and so $(c \circ d) \circ c' = b \circ c' = d$. That is, given $c \in Q$, there exists an element $c' \in Q$ such that $(c \circ d) \circ c' = d$ for all $d \in Q$. This is the right crossed-inverse property.

The proof of the converse is similar. □

In this paper, we shall be especially interested in non-commutative quasigroups of finite order which satisfy (vi) and consequently (by Lemma 3.1) also satisfy (vii). For brevity, we shall call them *CI-quasigroups* as, for example, in [A2] and [A3].

From now onwards, we shall write a' to denote the right crossed-inverse of the element a in a CI-quasigroup. Note that, from Lemma 3.1, $(c \circ b) \circ c' = b \Leftrightarrow c \circ (b \circ c') = b$ so, if c' is the right crossed-inverse of c, then c is the left crossed-inverse of c'.

LEMMA 3.2 *If a_L^{-1} is the left inverse of a in a quasigroup $(Q, \circ)$ which has the left inverse property, then a is the left inverse of a_L^{-1} for that quasigroup. An analogous result holds for right inverses.*

Proof. By the left inverse property, $a_L^{-1} \circ (a \circ c) = c$ for all $c \in Q$. Let b be an arbitrary element of Q. Then, by the solubility of equations, there exists an element $c \in Q$ such that $b = a \circ c$. So $a_L^{-1} \circ b = a_L^{-1} \circ (a \circ c) = c$, whence $a \circ (a_L^{-1} \circ b) = a \circ c = b$. This proves the result because b was arbitrarily chosen. □

In several of the applications to be described later in this paper, it is assumed that each piece of the message to be transmitted can be represented as a single element m of a quasigroup $(Q, \circ)$ and that this is enciphered by multiplying it by another element a of $(Q, \circ)$ so that the encoded message is $a \circ m$. (One important example is that of enciphering an authentication tag.) At the receiving end, the message is deciphered by multiplying by the inverse of a. If a right (or left) inverse property quasigroup is used and the right (left) inverse of a is a' say, then the right (left) inverse of a' is necessarily a. If a CI-quasigroup is used, this is not necessarily the case (as we shall show). This fact makes an attack on the system more difficult in the latter case.

DEFINITION 3.2 If $(Q, \circ)$ is a CI-quasigroup in which a' is the right crossed-inverse of a, a'' is that of a', a''' is that of a'', and so on, then the cycle $(a\ a'\ a'' \ldots)$ is called the *inverse cycle* associated with the element a.

Next we introduce algebraic structures useful in cryptology which involve two binary operations.

DEFINITION 3.3 A *left neofield* $(N, \oplus, .)$ of order n consists of a set N of n symbols on which two binary operations $(\oplus)$ and $(.)$ are defined such that $(N, \oplus)$ is a loop, with identity element 0 say, $(N \setminus \{0\}, .)$ is a group and $(.)$ distributes from the left over $(\oplus)$.

If the right distributive law $(a \oplus b)c = ac \oplus bc$ holds as well as the left distributive law, the system is called a *neofield.*

A neofield whose multiplication group is cyclic is called a *cyclic neofield.*

If the addition loop $(N, \oplus)$ is a group, the neofield is a *finite field* (or *Galois field*) and, in that case, the multiplicative group is necessarily cyclic (and the order is necessarily a prime power). So every finite field is a cyclic neofield.

Neofields were originally introduced by L.J. Paige [P1] who hoped to use them to construct new finite projective planes. Later, cyclic neofields with a particular divisibility property (called *property D neofields*) were studied in [K3] and [K4]. In particular, every finite field is a property D neofield. Also, inverse property cyclic neofields of prime power order were discussed in [J2]. Cyclic neofields whose addition loop is a CI-loop were studied in detail in [H4] under the name of XIP-neofields. Left neofields were introduced in [H5]. Quite recently the concept of a cyclic neofield was re-invented in [K9] and called a *spurious Galois field.*

It turns out that left neofields are particularly useful in cryptography because (i) they exist of all orders n (not only for prime powers) and (ii) their entire structure is determined by (and so can be computed with the aid of) a single mapping of the multiplication group: namely, either an orthomorphism or a near orthomorphism of that group.

DEFINITION 3.4 A one-to-one mapping $g \longrightarrow \phi(g)$ of a finite group $(G, .)$ onto itself is called an *orthomorphism* if the mapping $g \longrightarrow \theta(g)$, where $\theta(g) = g^{-1}\phi(g)$, is again a one-to-one mapping of G onto itself. The orthomorphism is said to be in *canonical form* if $\phi(1) = 1$, where 1 is the identity element of G.

An orthomorphism in canonical form may be regarded as a permutation

$$\phi = (1)\,(g_{11}g_{12}\cdots g_{1k_1})\,(g_{21}g_{22}\cdots g_{2k_2})\cdots(g_{s1}g_{s2}\cdots g_{sk_s})$$

of G such that the elements $g_{ij}^{-1}g_{i,j+1}$ (where $i = 1, 2, \ldots, s$ and the second suffix j is added modulo k_i) comprise the non-identity elements of G each counted once. Then $\phi(g_{ij}) = g_{i,j+1}$ and $\theta(g_{ij}) = g_{ij}^{-1}g_{i,j+1}$. The mapping θ is the *complete mapping* associated with the orthomorphism ϕ.

Suppose now that the elements of the finite group $(G, .)$ can be arranged in the form of a sequence $[g'_1\ g'_2\ g'_3 \cdots g'_h]$ followed by s cyclic sequences $(g_{11}g_{12}\cdots g_{1k_1})$, $(g_{21}g_{22}\cdots g_{2k_2}), \ldots, (g_{s1}g_{s2}\cdots g_{sk_s}$ such that the elements $g_j'^{-1}g'_{j+1}$ and $g_{ij}^{-1}g_{i,j+1}$ together with the elements $g_{ik_i}^{-1}g_{i1}$ comprise the non-identity elements of G each counted once. Then the mapping θ of $G \setminus \{g'_h\}$ onto $G \setminus \{g'_1\}$ given by $\theta(g'_j) = g_j'^{-1}g'_{j+1}$ for $j = 1, 2, \ldots, h-1$ and $\theta(g_{ij}) = g_{ij}^{-1}g_{i,j+1}$ (where arithmetic of second suffices is modulo k_i) is called a *near complete mapping* of G. The associated mapping $\phi : g \longrightarrow g\theta(g)$ of $G \setminus \{g'_h\}$ onto $G \setminus \{g'_1\}$ is called a *near orthomorphism* of G. It is said to be in *canonical form* if $g'_1 = 1$, where 1 is the identity element of G.

We shall represent a near orthomorphism ϕ in the following way:

$$\phi = [g'_1\, g'_2\, g'_3 \cdots g'_h](g_{11}g_{12}\cdots g_{1k_1})(g_{21}g_{22}\cdots g_{2k_2})\cdots(g_{s1}g_{s2}\cdots g_{sk_s})\,.$$

When the near orthomorphism is in canonical form so that $g'_1 = 1$, we shall denote the element g'_h which has no image under the mapping by η and call it the *ex-domain element.*

It is immediate to see from the definition of θ that

$$\eta = \left(\prod_{j=1}^{j=h-1} \theta(g'_j)\right)\left(\prod_{i=1}^{i=s}\prod_{j=1}^{j=k_s} \theta(g_{ij})\right).$$

That is, η is the product of all the elements of G in some appropriate order.

Remark An interesting direct application of group orthomorphisms to cryptography is described in [M2] and [M3].

The concepts of orthomorphism and near orthomorphism of a group enable us to characterize left neofilds in the following way:

Theorem 3.3 *Let $(N, \oplus, .)$ be a finite left neofield with multiplicative group $(G, .)$, where $G = N\backslash\{0\}$. Then, if $1\oplus 1 = 0$ in N, N defines an orthomorphism (and corresponding complete mapping) of $(G, .)$, which is in canonical form. If $1 \oplus 1 \neq 0$ but $1 \oplus \eta = 0$, N defines a near orthomorphism of G in canonical form and with η as ex-domain element.*

Conversely, let $(G, .)$ be a finite group with identity element 1 which possesses an orthomorphism ϕ (in canonical form). Let 0 be a symbol not in the set G and define $N = G \cup \{0\}$. Then $(N, \oplus, .)$ is a left neofield, where we define $\psi(\mathrm{w}) = 1\oplus w = \phi(\mathrm{w})$ for all $w \neq 0, 1$ and $\psi(0) = 1$, $\psi(1) = 0$. Also, $x\oplus y = x(1\oplus x^{-1}y)$ for $x \neq 0$, $0 \oplus y = y$ and $0.x = 0 = x.0$ for all $x \in N$.

Alternatively, let $(G, .)$ possess a near orthomorphism ϕ in canonical form. Then, with N defined as before, $(N, \oplus, .)$ is a left neofield, where we define $\psi(\mathrm{w}) = 1 \oplus w = \phi(\mathrm{w})$ for all $w \neq 0, \eta$, where η is the ex-domain element of ϕ and $\psi(0) = 1$, $\psi(\eta) = 0$. Also, $x \oplus y = x(1 \oplus x^{-1}y)$ for $x \neq 0$, as before, $0 \oplus y = y$ and $0.x = 0 = x.0$ for all $x \in N$.

Definition 3.5 The mapping $\varphi : w \longrightarrow 1 \oplus w$ is called the *presentation function* of the left neofield because it determines the complete addition table of the neofield by virtue of the fact that $x \oplus y = x(1 \oplus x^{-1}y)$.

In the case of a cyclic neofield with multiplicative group $\langle a\rangle$, the map $\varphi : v \longrightarrow w$ such that $1\oplus a^v = a^w$ determines the presentation function. The image w of v under this mapping is the *Jacobi algorithm* of v (see [J1]). We shall discuss the latter concept in more detail in Section 5 of this paper.

Theorem 3.3 was first given in [H5] and a detailed proof of the theorem together with a number of examples of the construction of left neofields from various groups will be found there.

It is of interest to note that every finite field of two-power order (say 2^r) has characteristic two (that is, $1+1=0$) and so it may be characterized by a particular orthomorphism of the cyclic group of odd order 2^r-1. Every finite field of odd prime power order (say p^r) has characteristic p (consequently, $1+1\neq 0$) and so it may be characterized by a particular near orthomorphism of the cyclic group of even order p^r-1. A cyclic (or any Abelian) group of odd order has no near orthomorphisms (because the product of all its elements is the identity) while a cyclic group of even order has no orthomorphisms (by a theorem of L.J. Paige [P1]). However, non-Abelian groups may have both orthomorphisms and near orthomorphisms. The reader seeking more information on this topic may consult Chapters 2 and 3 of [D4] and also [K8].

Looking again at Theorem 3.3, we see that, in a left neofield for which $1\oplus 1\neq 0$, the exdomain element η is the additive inverse of 1 (which, in the case of a finite field, is denoted by -1). It has been shown in [K5] that, in most left neofields, $\eta^2=1$. In particular, this is the case if the additive loop has either the left inverse property or the right inverse property. In [K5], a left neofield in which $\eta^2\neq 1$ has been called *pathological.* (See Theorem 8.2 for an application of such a left neofield.)

We end this Section with another structural lemma.

LEMMA 3.4 *If the additive loop of a left neofield $(N,\oplus,.)$ for which $1\oplus 1=0$ or of a two-sided neofield $(N,\oplus,.)$ has both the left and right inverse properties then the additive loop is commutative (and so N is two-sided in the former case as well).*

Proof. By the remark which precedes this lemma, $\eta^2=1$. We have $1\oplus\eta=0$ (where $\eta=1$ if $1\oplus 1=0$) and so, by the left distributive law, $\eta\oplus\eta^2=0$. That is, $\eta\oplus 1=0$. So, $a\oplus a\eta=0=a\eta\oplus a$ for every element $a\in N$.

By the left inverse property $a_L^{-1}\oplus(a\oplus b)=b$ for all $a,b\in N$. Putting $b=0$, we find that $a_L^{-1}=a\eta$. By the right-inverse property, $(c\oplus d)\oplus d_R^{-1}=c$ for all $c,d\in N$. Putting $c=0$, we find that $d_R^{-1}=d\eta$. In particular, $[a_L^{-1}\oplus(a\oplus b)]\oplus(a\oplus b)\eta=a_L^{-1}$. Thus, $b\oplus(a\oplus b)\eta=a\eta$. But, by the left inverse property, $b\eta\oplus(b\oplus a)=a$. So, in the case when $1\oplus 1=0$ and $\eta=1$, $a\oplus b=b\oplus a$ by the unique solubility of the equation $b\oplus x=a$. In the case when the neofield is two-sided, we can multiply the equation $b\oplus(a\oplus b)\eta=a\eta$ on the right by η to get $b\eta\oplus(a\oplus b)=a$. Comparing this with the equation $b\eta\oplus(b\oplus a)=a$, we again get $a\oplus b=b\oplus a$.

□

Note The special case of this Lemma which applies to cyclic neofields appears as Lemma I.14 of [H4].

4 Construction of CI-quasigroups

In the previous Section, we pointed out that CI-quasigroups are particularly suitable for enciphering schemes of the type $m \longrightarrow am$; and especially so for some applications if they have long inverse cycles. R. Artzy [A2] was the first to study the possible lengths of the inverse cycles of a CI-quasigroup (though the same idea was prósposed independently by A. Kotzig and developed to a limited extent in [D2]). Artzy proved, among other things, that if the inverse cycles of a CI-loop of order n consist of (e), where e is the identity element of the loop, and one other cycle (of length $n-1$) then $n = 2$ or 3. (In other words, only the cyclic groups C_2 and C_3 have this property. Compare Corollary I of our Theorem 4.3 below). He also showed that, if a CI-loop has an inverse cycle of length r, it has another inverse cycle distinct from (e) whose length is a (not-necessarily-proper) factor of r. The proofs are quite short and the results important for cryptology so, for completeness, we give them here.

THEOREM 4.1 *A CI-loop $(Q, \circ)$ (of order $m+1$) cannot consist of the identity element e and a single cycle $(x\ xJ\ xJ^2 \ldots xJ^{m-1})$ of length m except when $m = 1$ or 2.*

Proof. Each non-identity element of Q has the form xJ^i for some $i \in \mathbb{Z}_m$ so $x \circ xJ^{k+1} = xJ^{f(k)}$ where $k \neq 0$, $f(k) \neq 0$. [When $k = 0$, we have $x \circ xJ = e$ and, when $f(k) = 0$, $x \circ xJ^{k+1} = x$ so $xJ^{k+1} = e$.]

On multiplying both sides of the above inequality on the right by xJ and using the crossed inverse property, we get $xJ^{k+1} = xJ^{f(k)} \circ xJ$. Then, using the fact that $uJ^{-f(k)} \circ vJ^{-f(k)} = wJ^{-f(k)}$ for all $u, v, w \in Q$ such that $u \circ v = w$ because (see Theorem 4.4 below) J is an automorphism, we get $x \circ xJ^{1-f(k)} = xJ^{k+1-f(k)}$ so $f[-f(k)] = k + 1 - f(k)$.

Now, $\{f(1), f(2), \ldots, f(m-1)\} = \{1, 2, \ldots, m-1\}$ since neither $k = 0$ nor $f(k) = 0$ occurs in our first equality. Therefore, because $-f(i) = m - f(i)$ mod m,

$$\begin{aligned}\sum_{k=1}^{k=m-1} f[-f(k)] &= [\text{sum of } f(1), f(2), \ldots, f(m-1)] \\ &= [\text{sum of } 1, 2, \ldots, m-1] = \frac{1}{2}m(m-1)\end{aligned}$$

and

$$\begin{aligned}\sum_{k=1}^{k=m-1} [k + 1 - f(k)] &= \frac{1}{2}m(m-1) + (m-1) \\ &\quad -[\text{sum of } f(1), f(2), \ldots, f(m-1)] = m - 1\,.\end{aligned}$$

So we must have $\frac{1}{2}m(m-1) = (m-1)$ or $\left(\frac{1}{2}m - 1\right)(m-1) = 0$. Therefore, $m = 1$ or 2. □

THEOREM 4.2 *If a CI-loop $(Q, \circ)$ has an inverse cycle of length m, greater than 2, it has another inverse cycle whose length is a not-necessarily-proper factor of m.*

Proof. By Theorem 4.1, the elements of the inverse cycle of length m together with e cannot form a subloop. Thus, the inverse cycle contains at least one pair of (not necessarily distinct) elements x, y whose product is in a different inverse cycle. But $xJ^m = x$ and $yJ^m = y$ so $(x \circ y)J^m = xJ^m \circ yJ^m = x \circ y$ since J is an automorphism. Now, $(x \circ y)J^m = x \circ y$ implies that the length of the cycle in which the element $x \circ y$ lies divides m. □

As illustrations of the preceding result, Artzy gave a CI-loop of order 9 whose non-identity inverse cycles have lengths 2 and 6 and two non-isomorphic CI-loops of order 10 whose non-identity inverse cycles have lengths 1 and 8. The latter examples demonstrate the existence of CI-loops with inverse cycles of maximum possible length $n - 2$ (when $n > 3$). We reproduce one of these examples in Figure 4.1 below. The inverse cycles are (e), (1) and (2 3 4 5 6 7 8 9).

In [A3], Artzy proved that isotopic CI-loops are isomorphic. Later, in [B3], V.D. Belousov and B.V. Tzurkan showed that, if every loop isotopic to a given CI-loop is again a CI-loop, then the loop must in fact be an abelian group.

$(\circ)$	e	1	2	3	4	5	6	7	8	9
e	e	1	2	3	4	5	6	7	8	9
1	1	e	8	9	2	3	4	5	6	7
2	2	4	7	e	6	9	5	8	3	1
3	3	5	1	8	e	7	2	6	9	4
4	4	6	5	1	9	e	8	3	7	2
5	5	7	3	6	1	2	e	9	4	8
6	6	8	9	4	7	1	3	e	2	5
7	7	9	6	2	5	8	1	4	e	3
8	8	2	4	7	3	6	9	1	5	e
9	9	3	e	5	8	4	7	2	1	6

Figure 4.1.

The above facts concerning isomorphism suggest that CI-quasigroups which are not loops may be of most value in our cryptographic application. We shall now show how such quasigroups may be constructed. (The following constructions were first given in a forthcoming paper [K7] of the second author.)

THEOREM 4.3 *Let $(G, .)$ be an abelian group of order n such that $n + 1$ is composite. Define a binary operation $(\circ)$ on the elements of G by the relation $a \circ b = a^r b^s$, where $rs = n + 1$. Then $(G, \circ)$ is a CI-quasigroup and the right crossed inverse of the element a is a^u, where $u = (-r)^3$.*

COROLLARY I *If $(G, .)$ is the cyclic group C_p of prime order p and there exists a divisor r of $p + 1$ such that $(-r)^3$ is a primitive root of p, then the inverse* *cycles of $(G,\circ)$ are of lengths 1 and $p-1$. (An earlier conjecture of one of the authors was that such a divisor r exists whenever $p \equiv 2 \bmod 3$. However, for $p > 1000$, counterexamples exist. One obtained by R.K. Guy* [G3] *to whom the authors posed the problem is $p = 1181$. He does not guarantee that it is the smallest.)*

COROLLARY II *If $(G,.)$ is an elementary abelian group of order p^t (that is, an abelian group in which every element has the same prime order p) and there exists a divisor r of p^t+1 such that $(-r)^3$ is a primitive root of p, then the inverse cycles of $(G,\circ)$, excepting that of the identity element e of $(G,.)$, all have equal length $p-1$.*

Proof. We first show that $(G,\circ)$ is a quasigroup. Let $x\circ a = b$. Then $x^r a^s = b$ so $x^r = ba^{-s}$ and $x = x^{rs} = (ba^{-s})^s$ which is an element of G. Similarly, if $a\circ y = b$, then $a^r y^s = b$ so $y = y^{rs} = (a^{-r}b)^r$. Thus, equations are uniquely soluble and $(G,\circ)$ is a quasigroup. Also, $(a\circ b)\circ c = (a\circ b)^r c^s = (a^r b^s)^r c^s = b^{sr}a^{rr}c^s = b$ if $a^{rr}c^s = e$, the identity element of $(G,.)$: that is, if $c^s = a^{-rr}$ or if $c = c^{sr} = a^u$, where $u = (-r)^3$, as before. Thus, $(G,\circ)$ is CI-quasigroup and a^u, where $u = (-r)^3$, is the right crossed inverse of a. The result of the theorem follows.

Suppose next that $u = (-r)^3$ is a primitive root of p. Then $(a\ a^u\ a^{uu}\ \ldots)$, of length $p-1$, is the inverse cycle of $(G,\circ)$ which contains the element a since $u^{p-1} \equiv 1 \bmod p$ and $u^h \neq 1 \bmod p$ for $1 \leq h \leq p-2$. This proves both of the corollaries. □

Note. $(-r)^3$ can never be a primitive root of p when $p \equiv 1 \bmod 3$ since then $p-1$ is divisible by 3 and so the cube of an element has order at most $(p-1)/3$.

The above theorem provides a means of constructing CI-quasigroups with long inverse cycles and also proves the existence of CI-quasigroups all of whose non-identity cycles have equal length, thus answering for quasigroups the similar question discussed by Artzy for loops in [A2].

It is worth observing also that the CI-quasigroups so constructed are isotopes of the abelian group $(G,.)$. We may see this as follows: Since r and s are divisors of $n+1$, they are necessarily prime to the order n of $(G,.)$ and so the mappings $\alpha : x \longrightarrow x^r$ and $\beta : y \longrightarrow y^s$ are permutations of G. It follows immediately that $(G,\circ)$ is an isotope of $(G,.)$ because $x\circ y = x\alpha.y\beta$.

To illustrate the theorem, we choose the cardinal of G to be small and we give three examples as follows:

EXAMPLE 4.1 Let $(G,.)$ be the cyclic group $C_5 = \langle c : c^5 = e\rangle$ and define $a\circ b = a^3b^2$. We find that the multiplication table of the CI-quasigroup is as shown in Figure 4.2 and that the corresponding decomposition of G into inverse cycles is (0)(1 3 4 2). Here, the integers 0, 1, 2, 3, 4 represent the various powers of the generating element c of C_5.

EXAMPLE 4.2 Let $(G,.)$ be the cyclic group $C_{11} = \langle c : c^{11} = e\rangle$ and define $a \circ b = a^4b^3$. Then, $(-4)^3 \equiv 2 \bmod 11$ so it is a primitive root and the non-identity element inverse cycle has length 10.

EXAMPLE 4.3 Let $(G,.)$ be the elementary abelian group $C_5 \times C_5$ and define $a \circ b = a^2b^{13}$. Then, $(-2)^3 \equiv 2 \bmod 5$ which is a primitive root of 5. The six non-identity element inverse cycles each have length 4.

$(\circ)$	0	1	2	3	4
0	0	2	4	1	3
1	3	0	2	4	1
2	1	3	0	2	4
3	4	1	3	0	2
4	2	4	1	3	0

$(0 \circ 3) \circ 0 = 1 \circ 0 = 3$
$(2 \circ 4) \circ 1 = 4 \circ 1 = 4$
$(4 \circ 2) \circ 2 = 1 \circ 2 = 2$
$(3 \circ 3) \circ 4 = 0 \circ 4 = 3$
etc.

Figure 4.2

Note The CI-quasigroup obtained by the method of Theorem 4.4 is unipotent only if $r + s = n$: that is, only if $n = 5$.

When using an algebraic system for cryptographic purposes, economy of storage is important. We shall show that, in the case of a CI-loop with an inverse cycle of maximum length or of a CI-quasigroup with an inverse cycle of length one less than its order, very compact storage is possible because the structure of the entire quasigroup is determined by that of a single row of the Cayley table of the quasigroup. This is a consequence of the fact that the mapping J of an element to its right crossed-inverse is an automorphism of the quasigroup. Although the latter fact is well-known for the case of loops, the aforementioned implication does not seem to have been noticed until now. In our next theorem, we give a version of the result which is valid for CI-quasigroups as well as for CI-loops as in [B3]. (The result can also be regarded as a special case of Theorem 4.6 which we give later in this section.)

THEOREM 4.4 *For any CI-quasigroup $(Q,\circ)$, the mapping $J : a \longrightarrow a'$ from an element to its right crossed-inverse is an automorphism.*

Proof. For all pairs a, b of the elements of the quasigroup (or loop), we have $(a \circ b) \circ J = b$. Thus, $(c \circ d) \circ cJ = d$. Putting $c = a \circ b$ and $d = aJ$, we get $[(a \circ b) \circ aJ] \circ (a \circ b)J = aJ$. That is, $b \circ (a \circ b)J = aJ$. Then, putting $c = b$ and $d = (a \circ b)J$, we get $[b \circ (a \circ b)J] \circ bJ = (a \circ b)J$. That is $aJ \circ bJ = (a \circ b)J$. This proves the theorem. □

We apply this result first to the case of a CI-loop with e as identity element. As we remarked earlier, Artzy has proved that the maximum length of an inverse cycle is $n-2$ and that, when such a maximum length cycle exists, the loop has two self-inverse elements; namely e and another element which we shall denote by σ. Further, we shall suppose that the elements of the loop are denoted by $e, 0, 1, \ldots, n-3, \sigma$ and that the border elements of its Cayley table are written in that order. Also, we suppose that the notation is chosen so that $(0\ 1\ 2\ \ldots\ n-3)$ is the long inverse cycle. Thus, $eJ = e$, $\sigma J = \sigma$, and $aJ = (a+1)$ mod $(n-2)$ for $a = 0, 1, \ldots, n-3$.

Let us suppose that $0 \circ b = \sigma$. Then $0J^r \circ bJ^r = \sigma J^r$ for $r = 1, 2, \ldots, n-3$ since J is an automorphism. That is, $r \circ (b+r) = \sigma$ for $r = 0, 1, \ldots, n-3$, where addition is modulo $n-2$. Thus, the entries σ lie along a broken left-to-right diagonal of the $(n-2) \times (n-2)$ subsquare of the Cayley table which is formed by the second to $(n-1)$th rows and columns of the table. (See Figure 4.3 for an illustrative example with $n = 10$). Also, using the crossed inverse property, we find that $0 \circ b = \sigma \Rightarrow b = (0 \circ b) \circ 1 = \sigma \circ 1 \Rightarrow b \circ \sigma = (\sigma \circ 1) \circ \sigma = 1$ so $\sigma J^r \circ 1 J^r = bJ^r$ and $bJ^r \circ \sigma J^r = 1J^r$ for $r = 1, 2, \ldots, n-3$. Hence, $\sigma \circ r = b+r-1$ and $r \circ \sigma = 1 + r - b$ for $0, 1, \ldots, n-3$. Thus, the entries of the last row and column of the Cayley table of the loop are all determined by the cell of the second row which contains the entry σ (since this entry defines b).

Next, suppose that $0 \circ 0 = a$. Then, by the crossed inverse property, $0 = (0 \circ 0) \circ 1 = a \circ 1$ and $0 \circ (a+1) = (a \circ 1) \circ (a+1) = 1$, where addition is modulo $n-2$, as before. Since J is an automorphism, $a \circ 1 = 0 \Rightarrow 0 \circ (1-a) = -a$. Thus, $0 \circ 0 = a \Rightarrow 0 \circ (a+1) = 1$ and $0 \circ (-a+1) = -a$.

Similar reasoning shows that $0 \circ c = d \Rightarrow c = (0 \circ c) \circ 1 = d \circ 1$ and $c \circ (d+1) = (d \circ 1) \circ (d+1) = 1$. Thence, using the fact that J is an automorphism, $0 \circ c = d \Rightarrow 0 \circ (1-d) = c-d$ and $0 \circ (d-c+1) = 1-c$. So, since $0 \circ 1 = e$, it is sufficient to specify $\lceil (n-1)/3 \rceil$ of the entries of the second row of the Cayley table in order to determine the remainder. Moreover, because J is an automorphism, $0 \circ c = d \Rightarrow 0J^r \circ cJ^r = dJ^r \Rightarrow r \circ (c+r) = d+r$ for $r = 0, 1, \ldots, n-3$ and so these $\lceil (n-1)/3 \rceil$ entries determine the entire Cayley table.

$(\circ)$	e	0	1	2	3	4	5	6	7	σ
e	e	0	1	2	3	4	5	6	7	σ
0	0	5	e	4	7	3	6	1	σ	2
1	1	σ	6	e	5	0	4	7	2	3
2	2	3	σ	7	e	6	1	5	0	4
3	3	1	4	σ	0	e	7	2	6	5
4	4	7	2	5	σ	1	e	0	3	6
5	5	4	0	3	6	σ	2	e	1	7
6	6	2	5	1	4	7	σ	3	e	0
7	7	e	3	6	2	5	0	σ	4	1
σ	σ	6	7	0	1	2	3	4	5	e

Figure 4.3.

For example, the CI-loop whose Cayley table is given in Figure 4.3 above is completely determined by the statements that $n = 10$ and that $0 \circ 7 = \sigma$,

$0 \circ 0 = 5$ and $0 \circ 2 = 4$. The latter loop is isomorphic to that given in Figure 4.1 and can be obtained from it by the mapping

$$\phi = \begin{pmatrix} e\,1\,2\,3\,4\,5\,6\,7\,8\,9 \\ e\,\sigma\,0\,1\,2\,3\,4\,5\,6\,7 \end{pmatrix}.$$

Similarly, a CI-loop isomorphic to the second example of order 10 given by Artzy in [A2] is completely determined by the statements that $n = 10$ and that $0 \circ 7 = \sigma$, $0 \circ 0 = 5$ and $0 \circ 2 = 6$.

Next we consider the case of a CI-quasigroup of order n with elements $\sigma, 0, 1, \ldots, n-2$. We choose the notation so that σ is self-inverse and so that $(0\ 1\ 2 \ldots\ n-2)$ is the long inverse cycle.

Note We have shown the existence of such CI-quasigroups in Theorem 4.3. CI-quasigroups of order n with a single inverse cycle of length n also exist as has been shown recently by Simon Blackburn [B4]. We shall show how to construct these later in this Section.

We write the border elements of the Cayley table of our quasigroup in the order $0, 1, \ldots, n-2, \sigma$. Let us suppose that σ occurs in the $(b+1)$th column of the first row of the table so that $0 \circ b = \sigma$. Then $0J^r \circ bJ^r = \sigma J^r$ for $r = 1, 2, \ldots, n-2$ since J is an automorphism. That is, $r \circ (b+r) = \sigma$ for $r = 0, 1, \ldots, n-2$, where addition is modulo $n-1$. Thus, the entries σ lie along a broken left-to-right diagonal of the $(n-1) \times (n-1)$ subsquare of the Cayley table which is formed by its first $n-1$ rows and columns. (An illustrative example is given in Figure 4.4 with $n = 11$.) Also, using the crossed inverse property, we see that $0 \circ b = \sigma \Rightarrow b = (0 \circ b) \circ 1 = \sigma \circ 1 \Rightarrow b \circ \sigma = (\sigma \circ 1) \circ \sigma = 1$ so $\sigma J^r \circ 1J^r = bJ^r$ and $bJ^r \circ \sigma J^r = 1J^r$ for $r = 1, 2, \ldots, n-2$. Hence, $\sigma \circ r = b+r-1$ and $r \circ \sigma = 1+r-b$ for $r = 0, 1, \ldots, n-2$. Thus, the entries of the last row and column of the Cayley table of the quasigroup are all determined by the cell of the first row which contains the entry σ. (Compare the corresponding analysis for loops given above.)

Next, suppose that $0 \circ 0 = a$. By exactly the same reasoning as we used for the case of a CI-loop with a long inverse cycle, $0 \circ 0 = a \Rightarrow 0 \circ (a+1) = 1$ and $0 \circ (-a+1) = -a$. Also, if $0 \circ c = d$, then $0 \circ (1-d) = c-d$ and $0 \circ (d-c+1) = 1-c$. Moreover, each entry of the first row thus obtained determines the complete left-to-right broken diagonal on which it lies. We conclude that the entire CI-quasigroup is determined by the cell of the first row in which σ lies and by the contents of $\lceil (n-2)/3 \rceil$ other cells of the first row: that is, by a total of $\lceil (n+1)/3 \rceil$ cells.

$(\circ)$	0	1	2	3	4	5	6	7	8	9	σ
0	7	5	4	9	3	0	6	8	1	σ	2
1	σ	8	6	5	0	4	1	7	9	2	3
2	3	σ	9	7	6	1	5	2	8	0	4
3	1	4	σ	0	8	7	2	6	3	9	5
4	0	2	5	σ	1	9	8	3	7	4	6
5	5	1	3	6	σ	2	0	9	4	8	7
6	9	6	2	4	7	σ	3	1	0	5	8
7	6	0	7	3	5	8	σ	4	2	1	9
8	2	7	1	8	4	6	9	σ	5	3	0
9	4	3	8	2	9	5	7	0	σ	6	1
σ	8	9	0	1	2	3	4	5	6	7	σ

Figure 4.4.

For example, the CI-quasigroup whose Cayley table is given in Figure 4.4 is completely determined by the statements that $n = 11$ and that $0 \circ 9 = \sigma$, $0 \circ 0 = 7$, $0 \circ 1 = 5$ and $0 \circ 2 = 4$. This quasigroup is isomorphic to that described in Example 4.2 and can be obtained from it by the mapping

$$\phi = \begin{pmatrix} e & c & c^2 & c^4 & c^8 & c^5 & c^{10} & c^9 & c^7 & c^3 & c^6 \\ \sigma & 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \end{pmatrix}.$$

Before giving examples of possible applications of CI-quasigroups, let us point out that, in applications to cryptology, there are two types of key distributing centre. For public key systems, the role of the distributing centre is to provide a public key and a private key to each user of the system. These keys are then "fixed". They do not change for each new message or part message. For one-time pads and certain other applications, on the other hand, a new key is used for each message or each digit of a message and the role of the distributing centre (or centres, as in Example 4.7) is to arrange for this to occur.

EXAMPLE 4.4 A CI-quasigroup can be used to provide a one-time pad for key exchange (without the intervention of a key distributing centre).

The sender S selects arbitrarily (using a physical random number generator) an element $c^{(u)}$ of the CI-quasigroup $(Q, \circ)$ and sends both $c^{(u)}$ and the enciphered key (message) $c^{(u)} \circ m$. The receiver R uses his knowledge of the algorithm for obtaining $c^{(u)}J = c^{(u+1)}$ from $c^{(u)}$ (as in Theorem 4.3, for example) and hence he computes $(c^{(u)} \circ m) \circ c^{(u+1)} = m$.

EXAMPLE 4.5 A CI-quasigroup can be used to provide a new type of public key cryptographic system.

Let $(Q, \circ)$ be a CI-quasigroup with a long inverse cycle $(c\ c'\ c'' \ \ldots\ c^{(t-1)})$ of length t and suppose that all the users U_i $(i = 1, 2, \ldots)$ are provided with apparatus (for example, a chip card) which will compute $a \circ b$ for any given $a, b \in Q$. We assume that only the key distributing centre has a knowledge of the long inverse cycle which serves as a look-up table for keys. Each user U_i

has a public key $u_i \in Q$ and a private key u_iJ, both supplied in advance by the key distributing centre. User U_s wishes to send a message m to user U_t. He uses U_t's public key u_t to compute $u_t \circ m$ and sends that to U_t. U_t computes $(u_t \circ m) \circ u_tJ = m$.

EXAMPLE 4.6 A CI-quasigroup can be used to provide a common one-time key k for a particular communication between two users without the active intervention of a key distributing centre.

We assume that the set-up is as in Example 4.5. User U_s wishes to send a randomly chosen key k to user U_t and to obtain verification that U_t has received it. U_s first sends $u_t \circ k$ to U_t. U_t computes $(u_t \circ k) \circ u_tJ = k$ and sends back $u_s \circ k$ to U_s. U_s computes $(u_s \circ k) \circ u_sJ = k$ and hence verifies that U_t has received the key k.

EXAMPLE 4.7 We may use a system of CI-quasigroups to construct a blind-key distributing system from two distributing centres to a number of users.

Let D_a and D_b be the two distributing centres and $U_1, U_2, \ldots,$ be the users. Each user U_i is allocated two CI-quasigroups $(Q, {}^i\otimes_a)$ and $(Q, {}^i\otimes_b)$ defined on the same set Q and also has as public key an element u_i of Q. There is also a communal "public" quasigroup $(Q, \circ)$. The key for a particular communication is not known to either distributing centre and is in fact a "one-time pad".

The procedure is as follows: Suppose that U_s wishes to communicate with U_t. D_a selects an element k_a randomly (using a physical random number generator as before) from the set Q and sends $u_s({}^s \otimes {}_a)k_a$ to U_s and $u_t({}^t \otimes {}_a)k_a$ to U_t. D_b selects an element k_b randomly from the set Q and sends $u_s({}^s \otimes {}_b)k_b$ to U_s and $u_t({}^t \otimes {}_b)k_b$ to U_t. U_s decodes $u_s({}^s\otimes_a)k_a$ using the right crossed inverse of his public key u_s for the quasigroup $(Q, {}^s\otimes_a)$ to obtain k_a and he also decodes $u_s({}^s \otimes_b)k_b$ using the right crossed inverse of his public key u_s for the quasigroup $(Q, {}^s\otimes_b)$ to obtain k_b. He is then able to calculate $k = k_a \circ k_b$. U_t similarly is able to decode $u_t({}^t\otimes_a)k_a$ to obtain u_a and $u_t({}^t \otimes {}_b)k_b$ to obtain k_b and so he too is able to calculate $k = k_a \circ k_b$. U_s and U_t now have a common key k and so they are free to communicate with each other.

We may suppose, for this application, that each user has software (or, preferably, hardware) by which to compute kJ from k: for example, by using the algorithm of Theorem 4.3.

Note The examples given here and elsewhere in this paper are mostly somewhat simplistic for the purposes of illustration. Actual implementations would be (and, in some cases, already have been) carried out in a more sophisticated way. (cf. The earlier short paper [D5] of the authors to which the same remarks apply.)

The following Theorem 4.5 provides a construction for quasigroups of order n with a single inverse cycle of length n due to S. Blackburn and reproduced with his permission. The structure of such quasigroups is particularly simple and so it is not necessarily advantageous to use them for cryptography.

THEOREM 4.5 *CI-quasigroups of order n with a single inverse cycle of length n exist for infinitely many values of n.*

Proof. We suppose that $(Q, \circ)$, where $Q = \{0, 1, \ldots, n-1\}$, is a CI-quasigroup of order n of the required kind and that the notation is chosen so that $(0\ 1\ 2\ \ldots\ n-1)$ is its long inverse cycle. We let J denote the mapping of an element to its right crossed inverse so that $iJ = i + 1 \bmod n$. We define π to be the mapping of Q to Q such that $\pi(i) = 0 \circ i$.

Since, by assumption, J is an automorphism of the quasigroup,

$$i \circ j = (0J^i \circ (j-i)J^i) = (0 \circ (j-i))J^i = [\pi(j-i)]J^i = \pi(j-i) + i \bmod n\,.$$

Because $(Q, \circ)$ is a quasigroup, the equation $i \circ y = k$ has a unique solution y. So, in particular, $0 \circ i_1 = 0 \circ i_2 \Rightarrow i_1 = i_2$. That is, $\pi(i_1) = \pi(i_2) \Rightarrow i_1 = i_2$. Thus, since Q is a finite set, π is a permutation of Q.

Also, the equation $x \circ j = h$ has a unique solution for x. That is, $\pi(j-x) + x = h$ or, equivalently, $\pi(j-x) - (j-x) = (h-j)$ has a unique solution for x in $\mathbb{Z}_n$. Or, we may say that $\pi(z) - z = k$ has a unique solution for z in $\mathbb{Z}_n$.

Since $i+1$ (regarded as an element of $\mathbb{Z}_n$) is the right crossed inverse of i, we have $(i \circ x) \circ (i+1) = x$. That is, $[\pi(x-i) + i] \circ (i+1) = x$ in $\mathbb{Z}_n$ or $\pi\{(i+1) - [\pi(x-i) + i]\} + \pi(x-i) + i = x$ in $\mathbb{Z}_n$. This simplifies to $\pi[1 - \pi(x-i)] + \pi(x-i) = x - i$ or $\pi[1 - \pi(y)] + \pi(y) = y$ for all $y \in \mathbb{Z}_n$.

Let us suppose (as a special case) that a permutation π of $\mathbb{Z}_n$ with the above properties exists of the form $\pi(x) = \alpha x + \beta$, $\alpha, \beta \in \mathbb{Z}_n$.

The statement that $\pi(z) - z = k$ has a unique solution for z becomes $(\alpha - 1)z = k - \beta$ has a unique solution for z. Thus, $\alpha - 1$ must be a unit of $\mathbb{Z}_n$.

The statement that $\pi[1 - \pi(x)] + \pi(x) = x$ for all $x \in \mathbb{Z}_n$ becomes $\pi(1 - \alpha x - \beta) + \alpha x + \beta = x$ or $\alpha(1 - \alpha x - \beta) + \beta + \alpha x + \beta = x$ or $-\alpha\beta + 2\beta + \alpha = (\alpha^2 - \alpha + 1)x$ for all $x \in \mathbb{Z}_n$. So $-\alpha\beta + 2\beta + \alpha = 0$ and $\alpha^2 - \alpha + 1 = 0$.

Thus, the conditions for a permutation π of the above special form to exist are (i) $\alpha - 1$ is a unit of $\mathbb{Z}_n$; (ii) $\alpha - 2$ is a unit of $\mathbb{Z}_n$; (iii) $\alpha^2 - \alpha + 1 = 0$; and (iv) $\beta = \alpha/(\alpha - 2)$.

Equation (iii) can be written in the form $(\alpha - 2)^2 + 3(\alpha - 2) + 3 = 0$ or $(2\theta + 3)^2 = -3$, where $\theta = \alpha - 2$. Thence, $2\theta = -3 \pm \sqrt{-3}$. So, $\theta = \alpha - 2$ must be a unit and -3 must be a square in $\mathbb{Z}_n$. These conditions are both necessary and sufficient for (ii), (iii) and (iv) to hold.

In particular, if n is a prime, (i) and (ii) automatically hold. It is known that there are infinitely many primes p such that -3 is a square in $\mathbb{Z}_p$ and, for such primes, a permutation π which satisfies the required conditions exists.

If the conditions are satisfied when n is equal to a particular prime p, they are also satisfied when $n = p^r$. Further, using the Chinese remainder theorem, we can combine solutions for co-prime values of n into a solution for their product. Thus, since -3 is a square in $\mathbb{Z}_p$ when $p = 7, 13, 19, \ldots$, solutions exist for $n = 7^r 13^s 19^t \ldots$ etc. This proves the theorem. □

The simplest example of a CI-quasigroup obtained by the above method occurs when $n = 7$. Then $\theta = \alpha - 2 = 1$, $\alpha = 3$, $\beta = \alpha/(\alpha - 2) = 3$, so

$0 \circ x = \pi(x) = 3x + 3$. We illustrate the quasigroup so obtained in Figure 4.5.

$(\circ$	0	1	2	3	4	5	6
0	3	6	2	5	1	4	0
1	1	4	0	3	6	2	5
2	6	2	5	1	4	0	3
3	4	0	3	6	2	5	1
4	2	5	1	4	0	3	6
5	0	3	6	2	5	1	4
6	5	1	4	0	3	6	2

Figure 4.5.

In [K2], the concept of a CI-loop has been generalized. Let J denote the mapping of an element a of a loop $(L, \circ)$ to its right inverse so that $a \circ aJ = e$, where e is the identity element of the loop. We say that $(L, \circ)$ is an *m-inverse loop*, where m is a fixed positive or negative integer, if $(a \circ b)J^m \circ aJ^{m+1} = bJ^m$ for all elements, $a, b \in L$. Thus, in particular, a CI-loop is a 0-inverse loop.

We observe that, because J is an automorphism of a CI-loop, every 0-inverse loop is also an m-inverse loop for every positive integer m. (To see this, notice that $(aJ^r \circ bJ^r) \circ (aJ^r)J = bJ^r$ by the crossed inverse property, $r > 0$. Then, because J^r is an automorphism, we have $(a \circ b)J^r \circ aJ^{r+1} = bJ^r$ for every $r > 0$.) However, the converse is false. The authors of [K2] have given a 1-inverse loop of order 5 for which $J = (e)(0\ 1\ 2\ 3)$ and a 2-inverse loop of order 8 for which $J = (e)(0\ 1\ 2\ 3\ 4\ 5\ 6)$. We reproduce them (with notation changed from that of [K2] in Figures 4.6 and 4.7. Neither of these loops is a 0-inverse loop. Indeed, they show that, unlike the situation for CI-loops (0-inverse loops), m-inverse loops of order n with a single inverse cycle of length $n - 1$ do exist when $m > 0$.

$(\circ)$	e	0	1	2	3
e	e	0	1	2	3
0	0	1	e	3	2
1	1	2	3	e	0
2	2	3	0	1	e
3	3	e	2	0	1

Figure 4.6.

$(\circ)$	e	0	1	2	3	4	5	6
e	e	0	1	2	3	4	5	6
0	0	1	e	3	5	2	6	4
1	1	5	4	e	0	6	2	3
2	2	6	3	0	e	5	4	1
3	3	4	6	5	2	e	1	0
4	4	3	2	1	6	0	e	5
5	5	2	0	6	4	1	3	e
6	6	e	5	4	1	3	0	2

Figure 4.7.

It is also possible to define an m-inverse quasigroup: Let J be a permutation of the elements of a quasigroup $(Q, \circ)$ and m a fixed integer and suppose that $(a \circ b)J^m \circ aJ^{m+1} = bJ^m$ for all $a, b \in Q$. Then $(Q, \circ)$is an *m-inverse quasigroup* relative to the permutation J. (Clearly, J then defines the inverse cycles of the quasigroup.)

As in the case of loops, every CI-quasigroup is also an m-inverse quasigroup for every positive integer m. Until very recently, the present authors had not been able to construct any other examples of m-inverse quasigroups nor had they been able to find a general method for constructing m-inverse loops (ones that are not also CI-loops). However, quite recently the second author has found a method of construction but only so far for small orders so, at the present time, it is not possible to make use of such loops in cryptography.

EXAMPLE 4.8 A version of Example 4.6 which uses the fact that a CI-quasigroup is a 1-inverse quasigroup is the following:

With the same premises as before, user U_s chooses randomly an element $k \in Q$ and sends $(u_t \circ k)J$ to U_t. U_t computes $(u_t \circ k)J \circ u_t J^2 = kJ$ and sends back $u_s J \circ kJ = (u_s \circ k)J$ to U_s. U_s computes $(u_s \circ k)J \circ u_s J^2 = kJ$ and hence verifies that U_t has received the key k. He then sends $(k \circ m)J$ to U_t which U_t can now decipher by computing $(k \circ m)J \circ kJ^2 = mJ$ and thence obtain the message m.

We end our brief discussion of m-inverse loops with the following theorem (which, in the case of loops, is also Theorem 7 of [K2]):

THEOREM 4.6 *For every m-inverse loop or quasigroup, the mapping J^{3m+1} is an automorphism, where J is the permutation which defines the inverse cycles.*

COROLLARY *J is an automorphism for every CI-loop or CI-quasigroup* (cf. Theorem 4.4 above).

Proof. For all pairs a, b of the elements of the loop or quasigroup, we have $(a \circ b)J^m \circ aJ^{m+1} = bJ^m$. Thus, $(c \circ d)J^m \circ cJ^{m+1} = dJ^m$. Putting $c = (a \circ b)J^m$ and $d = aJ^{m+1}$, we get

$$[(a \circ b)J^m \circ aJ^{m+1}]J^m \circ [(a \circ b)J^m]J^{m+1} = aJ^{m+1}J^m .$$

That is, $bJ^{2m} \circ (a \circ b)J^{2m+1} = aJ^{2m+1}$. Then, putting $c = bJ^{2m}$ and $d = (a \circ b)J^{2m+1}$, we get

$$[bJ^{2m} \circ (a \circ b)J^{2m+1}]J^m \circ [bJ^{2m}]J^{m+1} = (a \circ b)J^{2m+1}J^m .$$

That is, $aJ^{3m+1} \circ bJ^{3m+1} = (a \circ b)J^{3m+1}$. This proves the theorem. □

Note 1. This theorem gives no information about the structures of the Cayley tables given in [K2] and exhibited in Figures 4.6 and 4.7 above because, in each case, J^{3m+1} turns out to be the identity mapping. The authors of [K2] have given no information as to how they constructed these tables.

Note 2. In [O2], J.M. Osborn has introduced the concept of a weak inverse loop and has shown (i) that weak inverse loops are examples of 1-inverse loops, and (ii) that, for a weak inverse loop, J^2 is an automorphism. This is not the case for a general 1-inverse loop as the example of Figure 4.6 shows. However, Theorem 4.6 shows that J^4 is an automorphism for every 1-inverse loop.

For completeness, we shall outline the proofs of the results mentioned in Note 2.

A loop $(L, \circ)$ is said to be a *weak inverse loop* if $b \circ (a \circ b)J = aJ$ for all elements $a, b \in L$, where J is the mapping of each element $a \in L$ to its right inverse as before.

Thus, $d \circ (c \circ d)J = cJ$. Putting $c = b$ and $d = (a \circ b)J$, we get $(a \circ b)J \circ [b \circ (a \circ b)J]J = bJ$. That is, $(a \circ b)J \circ aJ^2 = bJ$ so the loop is a 1-inverse loop, as claimed. Putting $c = (a \circ b)J$ and $d = aJ^2$, we get $aJ^2 \circ [(a \circ b)J \circ aJ^2]J = (a \circ b)J^2$. That is, $aJ^2 \circ bJ^2 = (a \circ b)J^2$ and so J^2 is an automorphism of the loop.

With Examples 4.4 to 4.8 to prompt him, the reader of this article will be able to see how to make use of CI-quasigroups in other kinds of cryptosystem which are of interest to him.

Just as quasigroups show superiority over groups for some cryptographic purposes, so finite neofields show superiority over finite fields. An outstanding example of this superiority is the enciphering system for stream ciphers devised by C. Kościelny (see [K9] and [K10] using so-called "spurious Galois fields". As we mentioned earlier, these are in fact neofields under another name.

We consider the application of neofields in cryptology in our next section and, in a later section, we discuss the existence of neofields whose additive structure is a CI-loop.

5 Using finite neofields in cryptology: discrete and Jacobi logarithms

A large number of enciphering systems have been proposed which depend for their security on the fact that computing logarithms in a finite field is believed to be difficult. See, for examples, [S10], pages 162–187; [S8], pages 310–316; [E2]; [C3]; and earlier papers cited therein. (The paper [L1] by B.A. LaMacchia and A.M. Odlyzko is especially interesting.) In many cases, an improvement to the security of such a scheme is obtained if the finite field is replaced by a cyclic neofield. Among other reasons, this is because (i) cyclic neofields exist of every positive integer order n, not just for prime power orders, and (ii) except for very small orders, there is more than one cyclic neofield of a particular order. We shall show that the concept of logarithm is just as valid in a cyclic neofield as it is in a Galois field. Moreover, the concept can be generalized to non-cyclic neofields.

Let $(N, \oplus, .)$ be a finite Galois field or a cyclic neofield. Then each non-zero element u of the additive group or loop $(N, \oplus)$ can be represented in the form $u = a^v$, where a is a generator of the multiplicative group $(N \setminus \{0\}, .)$. v is called the *discrete logarithm* of u to the base a or, sometimes, the *exponent* or *index* of u (see page 85 of [M1]). Given v and a, it is easy to compute u in a finite field but, if the order of the field is a sufficiently large prime p and also is appropriately chosen, it is believed to be difficult to compute v when u (as a residue modulo p) and a are given (see [O1]). Since the multiplicative structure of a cyclic neofield is the same as that of a finite field, the same remark applies to a cyclic neofield of the same prime order.

The following example shows one situation in which use of a neofield rather than a field is advantageous.

EXAMPLE 5.1 Let A,B,C, ..., be persons who wish to send each other encrypted messages, let p be a large prime number and let α be a primitive root of p. T. ElGamal in [E2] has proposed the following public key encryption scheme.

Each of A,B,C, ..., has a secret key $x(i)$, $i = a, b, c, \ldots$, and a public key, $y(i) = \alpha^{x(i)}$, $i = a, b, c, \ldots$. Suppose that A wishes to send B a block M_j of a message M, where $0 \leq M_j \leq p-1$. He chooses randomly a message key k, $0 < k < p-1$, and computes $y(b)^k = (\alpha^{x(b)})^k$ mod p. He then sends (C'_j, C_j), where $C'_j = \alpha^k$ mod p and $C_j = y(b)^k M_j$ or $y(b)^k + M_j$ according as multiplication or addition is used in the enciphering process.

On receipt of the enciphered message, B first computes $(C'_j)^{x(b)} = \alpha^{k.x(b)} = y(b)^k$ and hence he obtains $M_j = C_j/y(b)^k$ or $M_j = C_j - y(b)^k$.

ElGamal points out that it is not advisable to use the same key k for enciphering more than one block of the message since, if k is used more than once, knowledge of one block M_1 of the message would enable an intruder to compute other blocks because then $M_2/M_1 = C_2/C_1$ or $M_2 - M_1 = C_2 - C_1$ according as multiplication or addition is used. However, this problem does not arise if a cyclic neofield is used and $C_j = y(b)^k \oplus M_j$ since $\oplus$ does not satisfy the associative law and so $C_2 - C_1 = (y(b)^k \oplus M_2) - (y(b)^k \oplus M_1) \neq M_2 - M_1$.

Suppose, for example, that a cyclic neofield whose addition is a crossed-inverse loop is used. (We discuss the construction of such neofields in Section 8 below.) Then, since the order of the neofield is odd, each element g of the neofield has $g\eta = g\alpha^{(p-1)/2}$ as its crossed inverse (as we prove in Theorem 8.1). The modified ElGamal scheme is then as follows:

A chooses a key k, $0 < k < p-1$, and sends (C'_j, C_j), where $C'_j = \alpha^k$ mod p and $C_j = y(b)^k \oplus M_j$. On receipt of this encrypted block of the message, B computes $(C'_j)^{x(b)} = \alpha^{k.x(b)} = y(b)^k$ and thence $C_j \oplus (C'_j)^{x(b)}\eta = (y(b)^k \oplus M_1) \oplus y(b)^k \alpha^{(p-1)/2} = M_j$.

The same key k can now be used for each block of the message without providing any help to an intruder who acquires a knowledge of M_1 because

$$C_2 \oplus C_1\eta = (y(b)^k \oplus M_2) \oplus (y(b)^k \oplus M_1)\eta \neq M_2 \oplus M_1\eta .$$

Note Another solution to the problem of having to change the key k has been proposed by C.P. Schorr [S3].

As we remarked earlier (see Definition 3.5), the addition table of a left neofield is completely determined by its presentation function. We point out next that this is really only a generalization of an observation made by C.G.J. Jacobi about finite fields more than a century ago. We begin with a definition:

DEFINITION 5.1 Let $(N, \oplus, .)$ be a cyclic neofield (or Galois field) whose multiplicative group has a as a generating element. Every element of the loop (or group) $(N, \oplus)$, except 0, can be represented as a power of a and, because $x \oplus y = x(1 \oplus x^{-1}y)$, the entire loop is determined when the mapping $v \longrightarrow w$ such that $1 \oplus a^v = a^w$ is given. Then w is the *Jacobi logarithm* of v (or some authors may say that w is the Jacobi algorithm of $u = a^v$), see page 91 of [M1].

$p =$	7	11	13	17	19	23	29	31
$a =$	3	2	6	10	10	10	10	17
v								
0	2	1	5	10	17	8	11	12
1	4	8	7	13	6	3	23	8
2	1	4	11	8	4	18	3	29
3	*	6	4	2	13	14	17	18
4	5	9	2	7	12	5	8	6
5	3	*	8	9	16	9	26	9
6	.	5	*	1	3	21	24	26
7	.	3	3	5	14	13	9	23
8	.	2	10	*	9	20	13	22
9	.	7	1	14	*	19	15	28
10	.	.	9	11	1	17	20	5
11	.	.	6	4	7	*	27	21
12	.	.	.	3	15	7	19	13
13	.	.	.	15	11	10	25	24
14	.	.	.	6	8	12	*	17
15	.	.	.	12	10	6	12	*
16	.	.	.	.	2	15	7	3
17	.	.	.	.	5	4	16	11
18	.	.	.	.	.	1	10	1
19	.	.	.	.	.	11	6	10
20	.	.	.	.	.	16	5	25
21	.	.	.	.	.	2	2	19
22	.	.	.	.	.	.	.	etc

w (in the body of the table) is the Jacobi logarithm of v to base a in GF[p], where $1 \oplus a^v \equiv a^w \bmod p$. If $1 \oplus a^v \equiv 0 \bmod p$, we write (*) for w.

Figure 5.1.

In effect, the Jacobi logarithm defines the discrete logarithm of the sum of two elements expressed in exponent form since $a^x \oplus a^y = a^x(1 \oplus a^{y-x}) = a^{x+L(y-x)}$, where $L(y-x)$ is the Jacobi logarithm of $y - x$.

The Jacobi logarithm has also been called the *Zech logarithm*, see, for example, [C2], [H6], [H7], [K9] and [K10]; or *presentation function image*, see, for example, [H4], [H5] and [K4].

In his paper [J1] of 1846, C.G.J. Jacobi gave a table of such logarithms for all finite fields whose orders are primes p up to $p = 103$. We have reproduced part of his table as Figure 5.1. Although the Jacobi logarithm has been used very occasionally by cryptographers (for example, in [K9] and [K10]), the fact that it exists for every cyclic neofield seems not to have been exploited at all, nor has it been noticed that, whether the system is a field or a neofield, the relation $v \longrightarrow w$ can be readily obtained using the fact that the mapping $\phi : a^v \longrightarrow a^w$ is an orthomorphism or near orthomorphism of the cyclic multiplicative group $\langle a \rangle$. (See Theorem 3.3).

Note If the additive loop of a neofield $(N, \oplus, .)$ has the left inverse property, then the Jacobi logarithm can be deciphered using the fact that $\eta \oplus a^w = a^v$ if ϕ is a near orthomorphism or the fact that $1 \oplus a^w = a^v$ if ϕ is an orthomorphism. If the additive loop is a CI-loop, it can be deciphered using the fact that $a^w \oplus \eta = a^v$ or $a^w \oplus 1 = a^v$ in the above two cases respectively.

In Section 6 of the present paper, we show that some at least of the cyclic neofields can be completely specified by means of a short permutation polynomial or pseudo-permutation polynomial which defines the appropriate orthomorphism or near orthomorphism and this almost obviates the need for computer storage space. Indeed, the permutation polynomial may be made secure by installing it as hardware.

A second situation in which a cyclic neofield may be used advantageously is in the construction or encipherment of an authentication tag. We discuss this application in detail in Section 7.

The concepts of discrete logarithm and Jacobi logarithm can be generalized to apply to non-cyclic neofields.

We shall first illustrate this by means of a special case. Suppose that $(N, \oplus, .)$ is a left neofield whose multiplicative group is the non-abelian group H of order pq, where p, q are primes with $p < q$ (and necessarily p divides $q - 1$). (For a rather too simple example for our present purpose, see page 331 of [H5].) Each non-zero element u of the loop $(N, \oplus)$ can be represented as an element $a^v b^w \in H$, where a, b are generating elements of H and $0 \leq v \leq p-1$, $0 \leq w \leq q-1$. We may call the ordered pair (v, w) the *generalized discrete logarithm* of u. Also, if $1 \oplus a^v b^w = a^s b^t$ then (s, t) is the *generalized Jacobi logarithm* of (v, w).

More generally, if the multiplicative group of the left neofield $(N, \oplus)$ has generating sets of r elements, we may represent its elements by generalized discrete or Jacobi logarithms which are ordered r-tuples of integers.

Finally in this section, we draw the attention of the reader to the fact that the discrete logarithm concept can be extended in another way to apply to row-complete latin squares. In [L2], the discrete logarithm problem for the group

RL_n of all row-latin squares of order n is defined (see page 103) and, on pages 238 and 239, some illustrations of applications to cryptography are given.

6 Using pseudo-permutation polynomials as construction tools for neofields

We showed in Theorem 3.3 that a finite left neofield of order n is completely determined by its presentation function which is defined by an orthomorphism or near orthomorphism of the multiplicative group (of order $m = n - 1$). However, when one wants to use presentation functions in practice, it turns out that to store and handle them efficiently in a computer is not easy. For the case of cyclic neofields, in particular, one possible solution is to use a "pseudo permutation polynomial" of an algebraic structure containing the group which will enable easy calculation of $\phi(g)$ from g, where ϕ is the required orthomorphism or near orthomorphism.

Let $C_m = \langle a : a^m = e \rangle$. Then $C_m \cong (\mathbb{Z}_m, +)$ by the mapping $a^r \longrightarrow r$, $0 \le r \le m - 1$. Thus, to obtain an orthomorphism (m odd) or near orthomorphism (m even) of the multiplicative group C_m, we may use the following results (which we present as illustrations of this idea).

$(\mathbb{Z}_m, +), m$ odd.

$P(x) = rx$ is a permutation polynomial (of the ring $(\mathbb{Z}_m, +, .)$) which gives an orthomorphism of $(\mathbb{Z}_m, +)$ in canonical form whenever $r - 1$ and r are both relatively prime to m and $2 \le r \le m - 1$. (Under these conditions $P(x) - x$ also is a permutation of $(\mathbb{Z}_m, +)$.)

Note also that, if $g_i \longrightarrow \theta(g_i)$ is a complete mapping of a group $(G, .)$ and $g_i \longrightarrow \phi(g_i)$ is the corresponding orthomorphism, then $g_i \longrightarrow \theta(g_i)h$, where h is any fixed element of G, is another complete mapping and $g_i \longrightarrow \phi(g_i)h$ is the corresponding orthomorphism.

$(\mathbb{Z}_m, +), m = 2n$.

The following "pseudo-polynomials" of the ring $(\mathbb{Z}_m, +, .)$ define near orthomorphisms in canonical form (where all arithmetic is modulo m):

(i) $P(x) = 2n - 1 + \lfloor x/n \rfloor - x$, $x \neq n$,

(ii) $P(x) = 2x - \lfloor x/n \rfloor + 1$, $x \neq n$,

(iii) $P(x) = 2x + \alpha - 1$, $x \neq n$, where $\alpha = 1$ when $1 \le x \le n - 1$, and $\alpha = 0$ otherwise.

In the case when the order of the neofield is a prime power $q = p^h$ or is $q + 1$, we may sometimes be able to define orthomorphisms of the multiplicative structure of the neofield by means of permutation polynomials of the multiplicative or additive structures respectively of the field GF$[q]$. In particular, some of the permutation polynomials listed in Table 7.1 of [L3] are suitable.

(i) Orthomorphisms of the multiplicative structure of GF$[q]$ (cyclic group of order $q-1$) from which a neofield of order q can be constructed.

If $P(x)$ is a permutation polynomial such that $x^{-1}P(x)$ is also a permutation polynomial, then $P(x)$ defines an orthomorphism which is in canonical form provided that $P(1)=1$.

Of the polynomials listed in Table 7.1 of [L3], only the polynomials x^2 (valid if $q \equiv 0 \bmod 2$) and x^3 (valid if $q \equiv 0 \bmod 2$ and $q \not\equiv 1 \bmod 3$) satisfy these conditions. Thus, x^2 defines an orthomorphism in canonical form of a cyclic group $\langle a : a^{q-1} = 1\rangle$, where $q = 2^r$; and x^3 defines an orthomorphism in canonical form of a cyclic group $\langle a : a^{q-1} = 1\rangle$, provided that $q = 2^{2s+1}$.

Proof. $P(x) = x^2$ is a permutation polynomial of GF$[q]$ provided that $q \equiv 0 \bmod 2$ and clearly $x^{-1}P(x) = x$ is a permutation polynomial for any q. The first result follows since $P(1)=1$.

$P(x) = x^3$ is a permutation polynomial of GF$[q]$ provided that $q \not\equiv 1 \bmod 3$ and $x^{-1}P(x) = x^2$ is a permutation polynomial provided that $q \equiv 0 \bmod 2$. Thus, we require that $q = 2^r$ and that $2^r - 1$ is not divisible by 3.

Now $2^{2s}-1 = (2^2-1)(2^{2s-2}+2^{2s-4}+\ldots+2^2+1) = 3 \times (2^{2s-2}+2^{2s-4}+\ldots+2^2+1)$ so r cannot be even. Also, $2^{2s+1}-1 = (2-1)(2^{2s}+2^{2s-1}+2^{2s-2}+\ldots+2^2+2+1) = 2^{2s-1}(2+1)+2^{2s-3}(2+1)+\ldots+2(2+1)+1 = 3h+1$, where $h = 2^{2s-1}+2^{2s-3}+\ldots+2^3+2$, so 2^{2s+1} is never divisible by 3. □

EXAMPLE 6.1 GF$[2^3]$ has $\langle a : a^7 = 1\rangle$ as multiplicative group. The permutation polynomial $P(x) = x^3$ defines an orthomorphism of this group as shown below.

$$\begin{array}{rclllllll}
x & = & 1 & a & a^2 & a^3 & a^4 & a^5 & a^6 \\
P(x) & = & 1 & a^3 & a^6 & a^2 & a^5 & a & a^4 \\
x^{-1}P(x) & = & 1 & a^2 & a^4 & a^6 & a & a^3 & a^5.
\end{array}$$

(ii) Orthomorphisms of the additive structure of GF$[q]$ (elementary abelian group of type $p, p, \ldots, p$) from which a neofield of order $q+1$ can be constructed.

If $P(x)$ is a permutation polynomial such that $P(x)-x$ is also a permutation polynomial, then $P(x)$ defines an orthomorphism which is in canonical form provided that $P(0)=0$.

Of the polynomials listed in Table 7.1 of [L3] only the following may satisfy these conditions:

(a) cx for all q if c and $c-1$ are both non-zero in GF$[q]$;

(b) $x^3 - cx$ if $q \equiv 0 \bmod 3$ and both c and $c+1$ are non-squares in GF$[q]$;

(c) $x^4 + c_1x^2 + c_2x$ if $q \equiv 0 \bmod 2$ and c_1 and c_2 are chosen so that neither $P(x)$ nor $P(x) - x$ have any root in GF$[q]$ other than $x = 0$;

(d) $x^5 - cx$ if $q \equiv 0 \bmod 5$ and both c and $c-1$ are not fourth powers in GF$[q]$.

EXAMPLE 6.2 (case a)). Let a be a primitive root of GF$[3^2]$ such that $a^2 = a+1$. Then $a^3 = -a+1$, $a^4 = -1$, $a^5 = -a$, $a^6 = -a-1$, $a^7 = a-1$, $a^8 = 1$. Thus, $a \neq 0$ and $a - 1 = a^7 \neq 0$ so we may choose $c = a$. Then $P(x) = ax$

defines an orthomorphism of the group $C_3 \times C_3$ illustrated in Figure 6.1. We find that

$$\begin{array}{rclcccccccccc} & & x & = & 0 & 1 & a & a^2 & a^3 & a^4 & a^5 & a^6 & a^7 \\ P(x) & = & ax & = & 0 & a & a^2 & a^3 & a^4 & a^5 & a^6 & a^7 & 1 \\ P(x)-x & = & a^7x & = & 0 & a^7 & 1 & a & a^2 & a^3 & a^4 & a^5 & a^6 \end{array}$$

$(+)$	0	1	a	a^2	a^3	a^4	a^5	a^6	a^7
0	0	1	a	a^2	a^3	a^4	a^5	a^6	a^7
1	1	a^4	a^2	a^7	a^6	0	a^3	a^5	a
a	a	a^2	a^5	a^3	1	a^7	0	a^4	a^6
a^2	a^2	a^7	a^3	a^6	a^4	a	1	0	a^5
a^3	a^3	a^6	1	a^4	a^7	a^5	a^2	a	0
a^4	a^4	0	a^7	a	a^5	1	a^6	a^3	a^2
a^5	a^5	a^3	0	1	a^2	a^6	a	a^7	a^4
a^6	a^6	a^5	a^4	0	a	a^3	a^7	a^2	1
a^7	a^7	a	a^6	a^5	0	a^2	a^4	1	a^3

Figure 6.1.

EXAMPLE 6.3 (case (b)). Let a be a primitive root of GF$[3^2]$ such that $a^2 = a + 1$ as in the previous example. We may choose $c = -a = a^5$ and $c + 1 = -a + 1 = a^3$ since these are both non-squares. Then $P(x) = x^3 + ax$ defines an orthomorphism of the group $C_3 \times C_3$ illustrated in Figure 6.1. We find that $P(x) - x = x^3 + (a - 1)x = x^3 + a^7x$ so:

$$\begin{array}{rcccccccccc} x & = & 0 & 1 & a & a^2 & a^3 & a^4 & a^5 & a^6 & a^7 \\ P(x) & = & 0 & a^2 & a^4 & a & a^7 & a^6 & 1 & a^5 & a^3 \\ P(x)-x & = & 0 & a & a^6 & a^4 & a^3 & a^5 & a^2 & 1 & a^7 \end{array}$$

For the purpose of using these orthomorphisms of the additive structure of GF$[q]$ to construct neofields, we need first to write the additive group in multiplicative form. Thus, for example, the group exhibited in Figure 6.1 has to be re-written in the form $\langle c : c^3 = e\rangle \times \langle d : d^3 = e\rangle$. We use the mappings $0 \longrightarrow e$, $1 \longrightarrow c$, $a \longrightarrow d$. Then, $a^4 = -1 = 1 + 1 = c^2$, $a^5 = -a = a + a \longrightarrow d^2$, $a^2 = 1 + a \longrightarrow cd$, $a^3 = 1 + (-a) \longrightarrow cd^2$, $a^6 = -1 - a = a^4 + a^5 \longrightarrow c^2d^2$, $a^7 = -1 + a = a^4 + a \longrightarrow c^2d$. We may then use the orthomorphism to construct a neofield of order 10 with multiplication group $C_3 \times C_3$.

7 Authentication, identification and non-repudiation

In addition to providing confidentiality, cryptology is often required to do other jobs. (That is the difference between cryptography and cryptology.) We shall mention three of these: namely, (i) Authentication; (ii) Identification; and (iii) Non-repudiation.

By *authentication* of a message, we mean that it is made possible for the receiver of a message to verify that the message has not been modified in transit, so that it is not possible for an interceptor to substitute a false message for a legitimate one. By *identification* of a message, we mean that it is made possible for the receiver of a message to ascertain its origin, so that it is not possible for an intruder to measquerade as someone else. By *non-repudiation* we mean that a sender should not be able later to deny falsely that he had sent a message.

In an earlier paper, the present authors suggested a new authentication scheme based on quasigroups (latin squares), see [D5] and page 313 of [D4]. In [D1], an evaluation of the scheme was carried out and it was considered to be safe except when implemented in the most unsophisticated way (an implementation included by the authors mainly for expository purposes and one which they do not recommend). In a recent review (Zbl Vol. 858, #94014), some further comments on implementation have been made.

The scheme can be made more secure by introducing various refinements. First we outline the procedure originally proposed but we incorporate some improvements.

Let $a_1 a_2 \ldots a_n$ be a message over a q-ary alphabet which is required to be authenticated by means of a tag of s additional q-ary digits $b_1\ b_2\ \ldots\ b_s$. Let $n = st$. We separate the message into s mutually disjoint ordered subsets S_i, $i = 1, 2, \ldots, s$ of t digits b_i. For the calculation, we use a quasigroup $(Q, *)$ of order q. If the ith ordered subset of message digits is $S_i = \{a_{i1}, a_{i2}, \ldots, a_{it}\}$, then $b_i = [\{(a_{i1} * a_{i2}) * \ldots\} * a_{it}]$. In general, it is best to choose $s = \lfloor \sqrt{n} \rfloor$ but this is not essential as we have explained in [D5].

For the separation of the message digits into disjoint subsets, we use a $v \times v$ latin square L whose entries are the digits $1, 2, \ldots, v$, where $v \geq \lceil \sqrt{n} \rceil$. The cells of L are numbered from 1 to v^2 $(\geq n)$ and the elements for the block S_i are determined by the cells of L in which the digit i occurs.

Our main new proposals are first to include a time stamp and second to replace the "primitive" tag $b_1, b_2, \ldots, b_s$ by another tag of the same length s obtained as follows. With the aid of a cyclic neofield $(Q, \oplus, .)$, we replace each b_i by a^{b_i}, where $\langle a \rangle$ is the multiplication group of the neofield. We then compute the "sum" $a^{b_1} \oplus a^{b_2} \oplus \ldots \oplus \ldots a^{b_s}$ in s ways, the order of the summations being determined by s pre-set ways of introducing parentheses. Let us denote these s different sums (different because $\oplus$ is a non-associative operation) by $c_1, c_2, \ldots, c_s$. They form the improved authentication tag for the message $a_1 a_2 \ldots a_n$ (improved because changing a single digit a_i of the original message will change all, or almost all, of the authentication tag digits c_i). They can be easily computed by an authorized receiver but present a very difficult task to a would-be imposter. (As the expert reader will realize, it is nearly always more difficult to attack a hash function based on a non-associative system than one based on an associative system.)

Because of the rapid advance of so-called "information technology" and, in particular, the rapidly growing practice of effecting commercial transactions electronically, it has become increasingly important not only to authenticate messages but also to sign them. (That is, provide them with the personal signature of the sender in such a way that their originator can be subsequently verified.) The usual way in which this is done is by the sender enciphering the authentication tag in a way which is personal to himself (i.e. using his private key) and which can be verified as such by the recipient (using the public key of the sender). In this way, *identification* is provided. (The enciphered authentication tag is called the *digital signature* of the sender.) At the present time, the usual scheme used for implementation is RSA but the security of this scheme is increasingly in doubt. A suggestion of the present authors is to use a ciphering scheme based on CI-quasigroups as an alternative.

Note In the RSA system, the public and private keys commute: that is, a message or authentication tag enciphered using a person's public key can be deciphered using that person's private key and, conversely, a message or authentication tag enciphered using a person's private key can be deciphered using that person's public key. If encipherment by means of a CI-quasigroup is used, this is no longer the case unless the inverse cycles are of length two. However, this fact presents no real problem.

Suppose that k_1, k_2, k_3 are successive elements of an inverse cycle of a CI-quasigroup $(Q, \circ)$ which is to be used for enciphering. User U_i is assigned k_2 as his public key and has k_1 as private key for authentication tag signing and k_3 as private key for message deciphering. If he wishes to sign an authentication tag A of a message which he is sending to user U_j, he computes $k_1 \circ A$. User U_j can check that this tag originated from U_i by computing $(k_1 \circ A) \circ k_2 = A$ using U_i's public key k_2. If U_j wishes to send a message M to U_i, he enciphers it as $k_2 \circ M$ using U_i's public key k_2. U_i can then decipher the message by computing $(k_2 \circ M) \circ k_3 = M$ using his private message decipherment key k_3. Thus, every user is assigned one public and two private keys.

The possibility that the sender may subsequently deny that he has sent a particular message remains. For example, the sender might sign his agreement to a particular financial transaction which he subsequently regrets because it will lead to financial loss. It is therefore very desirable that there should be a means of ensuring *non-repudiation*.

The realization that non-repudiation is of critical importance has been recognized only fairly recently and has led to the concept of a key escrow system. Such a system is now in operation in the USA and, according to information acquired by the present authors, similar systems will shortly be set up in Great Britain and Hungary among others.

A key escrow system works in the following way. A number of centres called "key escrow agents" are established by the Government. Each sender of enciphered messages is required to "deposit" his private enciphering key (the one with which, among other things, he enciphers the authentication tags of the messages which he sends) with one of the key escrow agents. In practice, because the possibility of corrupt action at all levels must be allowed for, it is essential that the enciphering key is deposited in parts with several different escrow agents using a secrete sharing scheme. (Such an arrangement is already implemented in the scheme used in the USA.) Only the Government agency assigned the task of operating the key escrow scheme (called the *escrow law enforcement agency*) has the means to reconstruct the split key and this agency is only authorized to do so in the event of suspected criminality. (A detailed account of the authorized procedures for the release of encryption key components in the USA scheme is in [H3], pages 243–246.) Thus, in the event that forging of signatures or repudiatión of messages is claimed in a court of law, the private key of the claimed sender can be reconstructed and used as evidence for the resolution of the dispute.

Since the senders of encrypted messages may be suspicious of this key escrow system, especially in the early days of its introduction, they can if they wish incorporate their own safeguard. (This is the idea of B. Pfitzmann [P2].) Each sender may adjoin to his or her message an additional "document number" (called an *invisible signature* by Pfitzmann) encrypted with a second personal key which is not deposited with the escrow agents. Only the sender himself has the means to decipher correctly this document number and so he has the means to provide a court of law proof independent of the key escrow agents that he was or was not the originator of the disputed message or messages. (A signing procedure which incorporates this additional safeguard is said by Pfitzmann to have the *fail-stop property*.)

It should be clear to the readers of his survey that the method of producing authentication tags described at the beginning of this section also provides a very effective way of producing an invisible signature.

Note In a country in which a key escrow system is in operation, a public key crypto-system which meets the requirements of the key escrow system has been called a *fair public key cryptosystem* by S. Micali, see [H3], pp. 149–160.

Finally, we draw attention to the application of non-associative systems to the production of dynamic passwords and to digital fingerprinting.

We suppose that a user U wishes to identify himself to a recipient R of some kind (for example, a computer network centre, a key distributing centre or a person) in a way which prevents impersonation. We suppose that U first sends his personal identification number (PIN) to R. R sends back a randomly generated latin square (a generating device for this purpose already exists) and U produces an authentication tag for this latin square, for example by an easily-designed modification of the scheme proposed earlier in this section. Also, with the aid of his computer terminal, his chip card, or otherwise, U enciphers this authentication tag using his private key and then sends it back to R. R has access to U's public key and so is able to decipher the authentication tag and check that it matches the authentication tag for the latin square which R originally sent. If the match is exact, he is sure that U is not being impersonated by someone else who has stolen his PIN. This is an example of a *dynamic password* procedure. (The necessity of implementing such a scheme for bank credit and debit cards especially is becoming every day more apparent because of the widespread theft of cards and fraudulent use of PINs.)

Lastly, we mention one other present-day application of an authentication tag: namely, the application to authenticating a banknote in a way which cannot be copied by a counterfeiter. During the manufacturing process of a banknote, a random pattern is created on or within it; for example, by inserting light-sensitive particles within its surface. Subsequently, the numbers of these particles within the squares of a superimposed grid may be counted and hence a codeword (authentication tag) unique to the particular banknote created. The latter is then encrypted using the issuing Bank's private key and the encrypted version is printed on the banknote and called its *digital fingerprint*. Later, the public key of the issuing Bank may be used to decrypt the authentication tag and so to check that it is appropriate to the particle pattern. The authenticity of the banknote is thus verified. In fact, several variants of this scheme are already in operation. In particular, the fact that one version of the scheme has been implemented by the German Central Bank is probably quite well-known. (See, for example, [B5].) For other present and future applications of digital fingerprinting, see [S9].

8 Construction of neofields whose addition loop is a CI-loop.

First we consider the special case of cyclic neofields: that is, neofields whose multiplicative structure is a cyclic group. These are the neofields whose structure is closest to that of a finite field.

In his book [H4], D.F. Hsu has given a detailed account of cyclic neofields whose additive loop is a CI-loop. He has shown that these are of four kinds which he has designated XIP-neofields of types (a)(i)(ii)(iii) and (b) and which we shall look at in more detail below. However, these particular neofields have the disadvantage (for some applications) that the inverse cycles of their additive loops are of shortest possible length, as we now show. (But see Example 5.1 for a situation in which this property is advantageous.)

THEOREM 8.1 *Let $(N,\oplus)$ be a CI-loop which is the additive group of a cyclic neofield $(N,\oplus,.)$. Then its inverse cycles, excluding that of the identity element, all have length 1 if N has even order or all have length 2 if N has odd order.*

Proof. We have $(a\oplus b)\oplus a' = b$ for all $a,b \in N$, where a' is the right crossed inverse of a : that is, $a \oplus a' = 0$. If the neofield is one constructed from an orthomorphism of its cyclic multiplicative group (in which case it is of even order) then $1\oplus 1 = 0$ and so, by the left distributive law, $a\oplus a = 0$. Thus $a' = a$ and all inverse cycles are of length 1. If the neofield is one constructed from a near orthomorphism of its multiplicative group, then $1+\eta = 0$ and so $a + a\eta = 0$, whence $a' = a\eta$. Now, η is the product of all the elements of the group $(N \setminus \{0\},.)$ (see Section 3) and so, if this group is abelian with a unique element of order 2 (in particular, cyclic of even order), η is the unique element of order 2 in $(N \setminus \{0\},.)$. Hence, $\eta^2 = 1$ and the inverse cycle of the element a has length 2 because $a' = a\eta$, $a'' = a'\eta = a\eta^2 = a$. □

Note In every abelian group, the product η of all the elements is either equal to the identity element 1 or else to the unique element of order 2 if the group has such a unique element of order 2 (see [D3], page 34) so the additive group of every neofield or left neofield whose multiplicative group is abelian has inverse cycles of lengths 1 or 2. Moreover, it is shown in [K5] that, in every two-sided neofield, η has multiplicative order 2 (or 1) and so to obtain an addition loop which is a CI-loop and has inverse cycles of length greater than two, we must construct a left neofield which is not a two-sided neofield and whose multiplication is a non-abelian group. Let us call such a left neofield a CI(L)-neofield (a "crossed inverse long-inverse-cycle left neofield").

THEOREM 8.2 *Let $(G,.)$ be a finite group. Then the following are necessary and sufficient conditions for $(G,.)$ to be the multiplication group of a CI(L)-neofield:* (i) *G is non-abelian;* (ii) *G possesses a near orthomorphism $g \longrightarrow \phi(g)$ with ex-domain element η of order h greater than 2;* (iii) $\phi(\{\phi(g)\}^{-1}\eta) = [\theta(g)]^{-1}$ *for all elements $g \neq \eta$ in G, where θ is the near complete mapping associated with ϕ.*

Proof. The first two statements follow immediately from the preceding discussion. For the third, we observe that we require that $(a \oplus b) \oplus a\eta = b$ for all $a, b \in G$. Equivalently, we require that $[a(1 \oplus a^{-1}b)] \oplus a\eta = b$ or that $[a\varphi(a^{-1}b)] \oplus a\eta = b$. Using the left distributive law a second time, we get $\varphi(a^{-1}b) \oplus \eta = a^{-1}b$ for all $a, b \in G$. Thus, it is necessary and sufficient that $\varphi(g) \oplus \eta = g$ for all $g \in G$. From Theorem 3.3, $\varphi(0) = 1$ and $\varphi(\eta) = 0$ so this relation holds automatically when $g = 0$ or η. When $g \neq 0$ or η, we have $\varphi(g) = \phi(g) = g\theta(g)$, where ϕ is a near orthomorphism of $(G,.)$ and θ is the corresponding near complete mapping. So $\phi(g)[1 \oplus [\phi(g)]^{-1}\eta] = g$ or $\theta(g)\phi([\phi(g)]^{-1}\eta) = 1$ is required. This is equivalent to statement (iii) of the theorem. □

As an example, suppose that $(G,.)$ is the non-abelian group of order pq, where p, q are two distinct primes with $q > p > 2$ (and necessarily p divides $q - 1$). Then $(G,.)$ has near orthomorphisms because, in particular, it has sequencings. The exdomain element η of such a near orthomorphism is the product of all the elements of G in some order and it cannot be the identity element of G so it must be an element of order p or order q. It remains to investigate whether requirement (iii) of the theorem can be met.

We return to the construction of XIP-neofields: in particular to ones of odd order so that the inverse cycles of the additive CI-loop have length two. The following constructions are due to D.F. Hsu [H4] and, so far as is convenient and possible, we adopt Hsu's notation. (In particular, for convenience, we use $(+)$ instead of $(\oplus)$ for the binary operation of the addition loop except in the two main theorems.) Much of Hsu's notation is non-standard and because, in addition, his first language is not English, many of his arguments are quite difficult to understand. Note also that a substantial part of the argument needed to treat the case when the order of the XIP-neofield is odd (which is the one of most importance in the present paper) is left to the reader to insert. Furthermore, the analysis of cases which precedes Hsu's Theorem I.52 contains an error which is perpetuated in the theorem and throughout the subsequent discussion.

We begin by noting that the cyclic multiplicative group $\langle a\rangle$ of an XIP-neofield N_v of odd order v has even order $v-1$ and that the product of all the elements of this group is its unique element $\eta = a^\ell$ of order two, where $\ell = (v-1)/2$. Since $1+\eta = 0$, it will be convenient to write $\eta = -1 = a^\ell$. Also, we remind ourselves that the structure of a neofield is completely determined by its multiplicative group (cyclic in the present case) and by its presentation function $\varphi : w \longrightarrow 1+w$ so our investigation consists of examining the properties of the latter in detail.

LEMMA 8.3 *In an XIP-neofield N_v of odd order v based on the cyclic group $\langle a : a^{v-1} = 1\rangle$, any of the statements* (i) $1+a^k = a^{\ell+n} = -a^n$, (ii) $1+a^{n-k} = a^{\ell-k} = -a^{-k}$, (iii) $1+a^{-n} = a^{\ell+k-n} = -a^{k-n}$ *implies the other two. (Here, $\ell = (v-1)/2$ and $a^\ell = \eta = -1$ as stated above.)*

Proof. (i)⇒(ii): $1+a^k = -a^n \Rightarrow -a^k+(1+a^k) = -a^k-a^n \Rightarrow 1 = -a^k-a^n \Rightarrow -a^{-k} = 1+a^{n-k} \Rightarrow 1+a^{n-k} = a^{\ell-k}$.

(ii)⇒(iii): $1+a^{n-k} = -a^{-k} \Rightarrow -a^{n-k}+(1+a^{n-k}) = -a^{n-k}-a^{-k} \Rightarrow 1 = -a^{n-k}-a^{-k} \Rightarrow -a^{k-n} = 1+a^{-n} \Rightarrow 1+a^{-n} = a^{\ell+k-n}$.

(iii)⇒(i): $1+a^{-n} = -a^{k-n} \Rightarrow -a^{-n}+(1+a^{-n}) = -a^{-n}-a^{k-n} \Rightarrow 1 = -a^{-n}-a^{k-n} \Rightarrow -a^n = 1+a^k \Rightarrow 1+a^k = a^{\ell+n}$. □

DEFINITION 8.1 In an XIP-neofield N_v of odd order v in which $1+a^{k_i} = a^{\ell+n_i}$, let us denote the set $\{k_i, n_i, n_i-k_i, -k_i, -n_i, k_i-n_i\}$ of residues modulo $(v-1)$ by $S(k_i,n_i)$ or, more briefly, by S_i.

Thus, from Lemma 8.3, S_i contains each of the not-necessarily-distinct pairs k_i, n_i which stand in the relationship $1+a^{k_i} = a^{\ell+n_i}$. The next lemma gives necessary and sufficient conditions for these ordered pairs to be distinct.

LEMMA 8.4 *In an XIP-neofield of odd order v, let* $1+a^k = a^{\ell+n} = -a^n$. *Then* $1+0=1$ *and* $1+\eta=0$. *For all other pairs k,n we clearly have* $k \not\equiv \ell$ *and* $n \not\equiv \ell$ mod $(v-1)$. *Also,* $k \not\equiv \ell+n$ mod $(v-1)$. *If, in addition,* $k \not\equiv 0$ mod $(v-1)$, $n \not\equiv 0$ mod $(v-1)$ *and* $k \not\equiv \pm n$ mod $(v-1)$ *then* $|S(k,n)| = 6$.

Proof.The first statement follows from Theorem 3.3. In the set $S(k,n)$ we have directly that $k \not\equiv \pm n$ (given) and $k \not\equiv -k$, $k \not\equiv k-n$ mod $(v-1)$ since $1 \not\equiv -1$ and $n \not\equiv 0$. If $k \equiv n-k$ then $1+a^k = 1+a^{n-k}$ and so, from the previous lemma, $-a^n = -a^{-k}$, which contradicts $k \not\equiv -n$ mod $(v-1)$. Thus, k is distinct from the remaining five elements of $S(k,n)$. Also, we have directly than $n \not\equiv n-k$, $n \not\equiv -k$, $n \not\equiv -n$. If $n \equiv k-n$, then $a^n = a^{k-n}$ and so, from the previous lemma, $1 + a^k = 1 + a^{-n}$ which contradicts $k \not\equiv -n \bmod (v-1)$. Thus, n is distinct from the remaining elements of $S(k,n)$. The remainder of the proof is similar. □

We shall need to consider what happens when $k \equiv 0$ and/or $n \equiv 0$ and/or $k \equiv \pm n \bmod (v-1)$. Before doing so, we look further at the possibilities which arise when $|S(k,n)| = 6$.

LEMMA 8.5 *Let N_v be an XIP-neofield of odd order v in which $1+a^k = a^{\ell+n}$, and $1+a^f = a^{\ell+h}$. Then, $|S(k,n)| = |S(f,h)| = 6$ implies that $S(k,n) \cap S(f,h)|$ is 0, 2 or 6.*

Proof. We have $S(k,n) = \{k, n, n-k, -k, -n, k-n\}$ and $S(f,h) = \{f, h, h-f, -f, -h, f-h\}$. Suppose that $u, v, w \in S(k,n) \cap S(f,h)$. If no two of u, v, w are negatives of one another we can suppose that $\{u,v,w\} = \{k, n, \pm(n-k)\}$ or $\{-k, -n, \pm(k-n)\}$. But the negative of each element of $S(k,n)$ or $S(f,h)$ is also in that set, so we find that $S(k,n) = S(f,h) = \{k, n, n-k, -k, -n, k-n\}$. If two of u, v, w are negatives one of the other, we have $\{u,v,w\} = \{u,-u,w\}$ say. Again using the fact that the negative of each element of $S(k,n)$ or $S(f,h)$ is in that set, we have $\{u, -u, w, -w\} \in S(k,n) \cap S(f,h)$. Then $S(k,n) = \{u, -u, w, -w, z, -z\}$ say, where $z = u-w$ or $w-u$ and $S(f,h) = \{u, -u, w, -w, y, -y\}$, where $y = z$ or $-z$. Therefore, as in the previous case, $S(k,n) = S(f,h)$. Thus, $|S(k,n) \cap S(f,h)| \geq 3$ implies that $|S(k,n) \cap S(f,h)| = 6$. Since the negative of each element of $S(k,n)$ or $S(f,h)$ is in that set, $|S(k,n) \cap S(f,h)| = 1$ is impossible when $|S(k,n)| = |S(f,h)| = 6$ so $|S(k,n) \cap S(f,h)| = 0$, 2 or 6. □

Let us consider in more detail the case when $|S(k_1,n_1)| = |S(k_2,n_2)| = 6$ and $|S(k_1,n_1) \cap S(k_2,n_2)| = 0$ or 2.

Let H denote the set of sextuples S_i of cardinality six and suppose that u members of H are totally disjoint from the remainder. Call this subset of sextuples H_u. Thus, no two sextuples of H_u intersect and no sextuple of H_u intersects any sextuple of $H \setminus H_u$. We note that no residue can occur in more than two sextuples of $H \setminus H_u$ because, if $k \in S_i$, then either $1 + a^k = a^{\ell+n}$ or else $1 + a^f = a^{\ell+k}$. In the first case, k and n belong to S_i and, in the second case, f and k belong to S_i. By Lemma 8.3, any sextuple which contains k and n also contains $n-k, -k, -n, k-n$: any sextuple which contains f and k also contains $k-f, -f, -k, f-k$. So $k \in \{k, n, n-k, -k, -n, k-n\}$ and $k \in \{f, k, k-f, -f, -k, f-k\}$. k occurs in only one sextuple (of cardinal 6) if and only if $f = n$ or $f = k-n$. In that case, the sextuple in which k occurs is in H_u and $1 + a^n = a^{\ell+k}$, $1 + a^{k-n} = a^{\ell-n}$, $1 + a^{-k} = a^{\ell+n-k}$ in the first case, $1 + a^{k-n} = a^{\ell+k}$, $1 + a^n = a^{\ell+n-k}$, $1 + a^{-k} = a^{\ell-n}$ in the second. Let us write

$$\begin{aligned} T_1(k,n) &= \{(k, \ell+n), (n-k, \ell-k), (-n, \ell+k-n), (n, \ell+k), \\ &\qquad (-k, \ell+n-k), (k-n, \ell-n)\}, \\ T_2(k,n) &= \{(k, \ell+n), (n-k, \ell-k), (-n, \ell+k-n), (n, \ell+n-k), \\ &\qquad (-k, \ell-n), (k-n, \ell+k)\}, \end{aligned}$$

Then, we have just shown in effect that, corresponding to a sextuple $S(k,n)$ of cardinal six which occurs in H_u, the six ordered pairs of residues modulo $(v-1)$ of either $T_1(k,n)$ or else $T_2(k,n)$ occur as pairs (x,y), where $1+a^x=a^y$ in the presentation function of the corresponding neofield.

Consider next the case of a sextuple $S(k,n)=\{k,n,n-k,-k,-n,k-n\}$ which is in $H\setminus H_u$.

Let $S_\alpha(k,n)=\{k,n-k,-n\}$ and $S_\beta(k,n)=\{n,-k,k-n\}$. We call these subsets of $S(k,n)$ the *subset of α-elements* and the *subset of β-elements* respectively.

Since $S(k,n)\in H\setminus H_u$ implies that $S(k,n)$ is not disjoint from the remaining sextuples of H, we see that each of the following sextuples must also belong to $H\setminus H_u$ because each α-element of $S(k,n)$ must occur as a β-element in some other sextuple of $H\setminus H_u$:

$$\begin{aligned}
&S(f,k)=\{f,k,k-f,-f,-k,f-k\}\,;\\
&S(g,n-k)=\{g,n-k,n-k-g,-g,k-n,g+k-n\};\quad\text{and}\\
&S(h,-n)=\{h,-n,-n-h,-h,n,h+n\}\,.
\end{aligned}$$

Thus, corresponding to a sextuple $S(k,n)$ of cardinal six which occurs in $H\setminus H_u$, only the three ordered pairs of residues modulo $(v-1)$ of the set

$$T_3(k,n)=\{(k,\ell+n),(n-k,\ell-k),(-n,\ell+k-n)\}$$

occur as pairs (x,y), where $1+a^x=a^y$ in the presentation function of the corresponding neofield.

Next, we need to consider the effect on $S(k,n)$ and on the three sets $T_1(k,n)$, $T_2(k,n)$ and $T_3(k,n)$ of ordered pairs of residues modulo $(v-1)$ when one or more of the conditions $k\not\equiv 0$, $n\not\equiv 0$ and $k\not\equiv\pm n$ modulo $(v-1)$ of Lemma 8.4 is relaxed.

If $k\equiv 0$, and $n\not\equiv 0 \bmod (v-1)$, then $S(0,n)=\{0,n,-n\}$ so $|S(0,n)|=3$ since $-n\equiv n$ would imply $2n\equiv 0 \bmod (v-1)$, whence $n\equiv(v-1)/2\equiv\ell$ contrary to Lemma 8.4. If $n\equiv 0$ and $k\not\equiv 0$, then $S(k,n)=\{k,0,-k\}$ and, if $k\equiv n\not\equiv 0$, then $S(k,k)=\{k,0,-k\}$. In either case, the cardinal of the set S is 3. We defer the case $k\equiv -n$ (which we call case II) until later as it requires more careful analysis. First, we look at the sets of ordered pairs $T_1(k,n), T_2(k,n)$ and $T_3(k,n)$ for the above cases.

Case Ia, $k\equiv 0 \bmod (v-1)$.
We have

$$\begin{aligned}
&T_1(0,n)=\{(0,\ell+n),(n,\ell),(-n,\ell-n)\}\,,\\
&T_2(0,n)=\{(0,\ell+n),(n,\ell),(-n,\ell-n),(n,\ell+n),(0,\ell-n),(-n,\ell)\}\,,\\
&T_3(0,n)=\{(0,\ell+n),(n,\ell),(-n,\ell-n)\}\,.
\end{aligned}$$

It $n\not\equiv 0 \bmod (v-1)$, then $\ell\not\equiv\ell-n \bmod (v-1)$, and so the three ordered pairs of $T_1(0,n)$ and $T_3(0,n)$ are distinct. Also, since $-n\equiv n \bmod (v-1)$

would imply $n \equiv \ell$ contrary to Lemma 8.4, the six ordered pairs of $T_2(0,n)$ are distinct.

If $n \equiv 0 \bmod (v-1)$, then $T_1(0,0) = T_2(0,0) = T_3(0,0) = \{(0,\ell)\}$.

Case Ib, $n \equiv 0 \bmod (v-1)$.

We have

$$\begin{aligned}
T_1(k,0) &= \{(k,\ell),(-k,\ell-k),(0,\ell+k)\}\,,\\
T_2(k,0) &= \{(k,\ell),(-k,\ell-k),(0,\ell+k),(0,\ell-k),(-k,\ell),(k,\ell+k)\}\,,\\
T_3(k,0) &= \{(k,\ell),(-k,\ell-k),(0,\ell+k)\}\,.
\end{aligned}$$

If $k \not\equiv 0 \bmod (v-1)$, the three ordered pairs of $T_1(k,0)$ and $T_3(k,0)$ are distinct. Also, since $-k \equiv k \bmod (v-1)$ would imply $k \equiv \ell$ contrary to Lemma 8.4, the six ordered pairs of $T_2(k,0)$ are distinct. The case $k \equiv 0 \bmod (v-1)$ has already been covered in Case Ia.

Case Ic, $k \equiv n \bmod (v-1)$.

We have

$$\begin{aligned}
T_1(k,k) &= \{(k,\ell+k),(0,\ell-k),(-k,\ell)\}\,,\\
T_2(k,k) &= \{(k,\ell+k),(0,\ell-k),(-k,\ell),(k,\ell),(-k,\ell-k),(0,\ell+k)\}\,,\\
T_3(k,k) &= \{(k,\ell+k),(0,\ell-k),(-k,\ell)\}\,.
\end{aligned}$$

If $k \not\equiv 0 \bmod (v-1)$, the three ordered pairs of $T_1(k,k)$ and $T_3(k,k)$ are distinct. Also, since $-k \equiv k \bmod (v-1)$ would imply $k \equiv \ell$ contrary to Lemma 8.4, the six ordered pairs of $T_2(k,k)$ are distinct.

If $k \equiv 0 \bmod (v-1)$, we have $T_1(0,0) = T_2(0,0) = T_3(0,0) = \{(0,\ell)\}$ as before.

Case II, $k \equiv -n \bmod (v-1)$.

We are assuming that $1 + a^k = a^{\ell+n}$ so we may use Lemma 8.3 to obtain $a^{\ell+n} = 1 + a^k = 1 + a^{-n} = a^{\ell+k-n} = a^{\ell-2n}$, whence $3n \equiv 0 \bmod (v-1)$.

If $\gcd(3, v-1) = 1$, we have $n \equiv 0 \bmod (v-1)$ and so $k \equiv -n \equiv 0 \bmod (v-1)$. Thus, $|S(0,0)| = 0$ and $T_1(0,0) = T_2(0,0) = T_3(0,0) = \{(0,\ell)\}$ in this case.

If $\gcd(3, v-1) \neq 1$, then 3 divides $v-1$ and so $n \equiv (v-1)/3$ or $n \equiv 2(v-1)/3$, whence $k \equiv -n \equiv 2(v-1)/3$ or $(v-1)/3$ respectively.

We find that $S(k,-k) = \{(v-1)/3, 2(v-1)/3\}$ in both cases, that $T_i(v-1)/3, 2(v-1)/3) = T_i(2(v-1)/3, (v-1)/3) = \{((v-1)/3, (v-1)/6), (2(v-1)/3, 5(v-1)/6)\}, i = 1,2$, and that

$$\begin{aligned}
T_3((v-1)/3, 2(v-1)/3) &= \{((v-1)/3, (v-1)/6\}\,,\\
T_3(2(v-1)/3, (v-1)/3) &= \{(2(v-1)/3, 5(v-1)/6)\}\,.
\end{aligned}$$

To summarize:

If, in an XIP-neofield N_v of odd order v, $1 + a^k = a^{\ell+n}$, then the ordered pairs of $T_1(k,n), T_2(k,n)$ and $T_3(k,n)$ are all distinct provided that $k \not\equiv 0, n \not\equiv 0$ and $k \not\equiv \pm n \bmod (v-1)$.

If $k \equiv 0$ or $n \equiv 0$ or $k \equiv n$, then the six pairs of $T_1(k,n)$ reduce to three.

If $k \equiv n \equiv 0$, then T_1, T_2, T_3 all reduce to a single pair.

If $k \equiv -n$ and $k \not\equiv 0$, $n \not\equiv 0$, then $\gcd(3, v-1) \neq 1$ and we have $\{k,n\} = \{(v-1)/3, 2(v-1)/3\}$.
Then, each of T_1, T_2 reduces to $\{((v-1)/3, (v-1)/6), (2(v-1)/3, 5(v-1)/6)\}$ while

$$T_3((v-1)/3, 2(v-1)/3) = \{((v-1)/3, (v-1)/6)\} \quad \text{and}$$
$$T_3(2(v-1)/3, (v-1)/3) = \{(2(v-1)/3, 5(v-1)/6\} .$$

LEMMA 8.6 *Let N_v be an XIP-neofield of odd order v and let*

$$T_3(k,n) = \{(k, \ell+n), (n-k, \ell-k), (-n, \ell+k-n)\}$$

where $1 + a^k = a^{\ell+n} = -a^n$.

If $v \equiv 3 \bmod 6$, the sets $T_3(k,n)$ are all of cardinal three with one exception: namely, the set $T_3(0,0) = \{(0,\ell)\}$ occurs and so the triple $T_3(0,h) = \{(0, \ell + h), (h, \ell), (-h, \ell - h)\}$ with $h \not\equiv 0 \bmod (v-1)$ does not occur.

If $v \equiv 5 \bmod 6$, the sets $T_3(k,n)$ all have cardinal three and so the triple $T_3(0,h)$ with $h \not\equiv 0 \bmod (v-1)$ does occur.

If $v \equiv 1 \bmod 6$, the sets $T_3(k,n)$ all have cardinal three with the exceptions that both of the singletons $T_3((v-1)/3, 2(v-1)/3) = \{((v-1)/3, (v-1)/6)\}$ and $T_3(2(v-1)/3, (v-1)/3) = \{(2(v-1)/3, 5(v-1)/6)\}$ occur. Moreover, the triple $T_3(0,h)$ with $h \not\equiv 0 \bmod (v-1)$ does occur.

Proof. We count the pairs (k,n) of exponents such that $1 + a^k = a^{\ell+n} = -a^n$ by counting the exponents $\ell + n$ of the elements $a^{\ell+n}$. Since $1 + 0 = 1$ and $1 + a^\ell = 0$, neither of the elements 1 or 0 occurs as an element $a^{\ell+n}$ and we always have $k \not\equiv \ell$. . By Lemma 8.3, when the pair (k,n) occurs so also do the other pairs of $T_3(k,n)$. Also, by what we proved above, if $|T_3(k,n)| < 3$, then either 3 divides $v-1$ and $\{k,n\} = \{(v-1)/3, 2(v-1)/3\}$ or $k \equiv n \equiv 0$. These two possibilities are mutually exclusive. If $k \equiv n \equiv 0$, then $T_3(0,0) = \{(0,\ell)\}$.

Since neither 1 nor 0 occurs as an element $a^{\ell+n}$, we have $\Sigma|T_3(k,n)| = v-2$.

Case $v \equiv 3 \pmod 6$: $\Sigma|T_3(k,n)| = 6u + 1$ for some integer u so, since at most one of the $T_3(k,n)$ is a singleton when 3 does not divide $v-1$, $T_3(0,0) = \{(0,\ell)\}$ must occur and $T_3(0,h)$ with $h \not\equiv 0 \bmod (v-1)$ does not occur.

Case $v \equiv 5 \pmod 6$: $\Sigma|T_3(k,n)| = 6u + 3 = 3(2u+1)$ for some integer u. Since 3 does not divide $v-1$, at most one of the $T_3(k,n)$ is a singleton but the sum is a multiple of three so no singleton can occur. The sets T_3 all have cardinal 3 and so a triple $T_3(0,h)$ with $h \not\equiv 0 \bmod (v-1)$ must occur.

Case $v \equiv 1 \pmod 6$: $\Sigma|T_3(k,n)| = 6u + 5 = 3(2u+1) + 2$ for some integer u. Since 3 divides $v-1$, both of the singletons $T_3((v-1)/3, 2(v-1)/3) =$

$\{((v-1)/3,(v-1)/6)\}$ and $T_3(2(v-1)/3,(v-1)/3) = \{(2(v-1)/3, 5(v-1)/6)\}$ must occur and the singleton $T_3(0,0)$ cannot occur. Consequently, a triple $T_3(0,h)$ with $h \not\equiv 0 \bmod (v-1)$ must occur. This completes the proof. □

DEFINITION 8.2 An ordered pair k, n of residues modulo $(v-1)$, v odd, such that $k \not\equiv \ell$, $n \not\equiv \ell$ and $k \not\equiv \ell + n \bmod (v-1)$ is an *XIP-admissible pair* of residues provided that one of the following five sets of conditions is satisfied:
(i) $k \not\equiv 0$, $n \not\equiv 0$, $k \not\equiv \pm n \bmod (v-1)$; or (ii) $k \equiv 0$, $n \not\equiv 0 \bmod (v-1)$; or (iii) $k \not\equiv 0$, $n \equiv 0 \bmod (v-1)$; or (iv) $k \equiv n \bmod (v-1)$; or (v) $\{k,n\} = \{(v-1)/3, 2(v-1)/3\} \bmod (v-1)$.

Let $S_i = S(k_i,n_i) = \{k_i, n_i, n_i - k_i, -k_i, -n_i, k_i - n_i\}$, $i = 1,2,\ldots,h$. We say that the collection $H = \{S_1, S_2, \ldots, S_h\}$ of sextuples form an *XIP-admissible decomposition* of the set R of residues modulo $(v-1)$ distinct from $\ell = (v-1)/2$ provided that each pair k_i, n_i is XIP-admissible and that one of the following holds:

either (a) $S_1, S_2, \ldots, S_h$ are disjoint sets and form a partition of R;

or (b) $\{S_1, S_2, \ldots, S_u\}$ is a sub-collection of sextuples which are disjoint from each other and from the sextuples of

$$H \setminus H_u = \{S_{u+1}, S_{u+2}, \ldots, S_{h'} : |S_i| = 6\} \cup \{S_{h'+1}, S_{h'+2}, \ldots, S_h : |S_i| < 6\}$$

and each element of $R \setminus \{S_1 \cup S_2 \cup \ldots \cup S_u \cup S_{h'+1} \cup S_{h'+2} \cup \ldots \cup S_h\}$ appears in exactly two sextuples of the subcollection $\{S_{u+1}, S_{u+2}, \ldots, S_{h'}\}$ and is an α-element of one of these sextuples and a β-element of the other.

Suppose now that the collection $H = \{S_1, S_2, \ldots, S_h\}$ of sextuples $S_i = S(k_i,n_i)$ form an XIP-admissible decomposition of the set R of residues modulo $(v-1)$ distinct from ℓ of type (a): that is, $\{S(k_i,n_i) : i = 1,2,\ldots,h\}$ is a partition of R. This can happen in any of three ways:

(i) For each $i, S(k_i,n_i) \equiv S(n_i,k_i) = \{n_i, k_i, k_i - n_i, -n_i, -k_i, n_i - k_i\}$. In this case, all of the pairs of the set $T_1(k_i,n_i)$ occur as pairs of indices in the presentation function $\varphi : a^k \longrightarrow a^{\ell+n} = 1 + a^k$ of the XIP-neofield.

(ii) For each $i, S(k_i,n_i) \equiv S(k_i - n_i, k_i) = \{k_i - n_i, k_i, n_i, n_i - k_i, -k_i, -n_i\}$. In this case, all of the pairs of the set $T_2(k_i,n_i)$ occur as pairs of indices in the presentation function φ.

(iii) For some values of i, $S(k_i,n_i) \equiv S(n_i,k_i)$ and, for the remaining values of i, $S(k_i,n_i) \equiv S(k_i - n_i, k_i)$.

Alternatively, suppose that the collection H of sextuples $S(k_i,n_i)$ form an XIP-admissible decomposition of type (b): that is, for some or all pairs i,j $(1 \le i,\ j \le h)$ $|S(k_i,n_i) \cap S(k_j,n_j)| = 2$. Let H_u denote the sub-collection of the $S(k_i,n_i)$ which are totally disjoint as in the discussion above. For each of the sextuples of H_u either (i), (ii) or (iii) above applies and so the ordered pairs of T_1 or T_2 occur as corresponding pairs of indices in the presentation function. But, for each $S(k_i,n_i) \in H \setminus H_u$ and of cardinal six, only the ordered pairs of the set T_3 occur as corresponding pairs of indices in the presentation function because k_i occurs as second member of an ordered pair (that is, as a β-element) in a different sextuple from that in which it occurs as a first member (that is, as an α-element).

THEOREM 8.7 *Let $G = \langle a : a^{v-1} = 1\rangle$ be the cyclic group of even order $v-1$ and let $\ell = (v-1)/2$. (We shall write $a^\ell = -1$.) Let 0 be an element not in G. Define a binary operation $(\oplus)$ on the set $N_v = G \cup \{0\}$ by the statements $1\oplus 0 = 1$, $1 \oplus a^\ell = 0$, $1\oplus a^k = a^{\ell+n}$, where k, n are the ordered pairs of residues distinct from ℓ modulo $(v-1)$ that occur in an XIP-admissible decomposition. Also, $x\oplus y = x(1\oplus x^{-1}y)$ for $x \neq 0$ and $0\oplus y = y$. Let $0.x = 0 = x.0$ for all $x \in N_v$. The $(N_v, \oplus, .)$ is an XIP-neofield of odd order v.*

Proof. It is easy to see from the above discussion that the mapping $\varphi : a^k \longrightarrow a^{\ell+n} = 1 + a^k$ is a one-to-one mapping of $G\setminus\{a^\ell\}$ onto $G\setminus\{1\}$. It follows that the elements $1\oplus 0 = 1$, $1\oplus a^\ell = 0$, $1\oplus a^k$ for $k = 0, 1, \dots, \ell-1, \ell+1, \dots v-1$ are all distinct: that is, the elements of the second row of the addition table of $(N_v, \oplus)$ are all distinct. The left distributivity of multiplication over addition follows easily from the definition of $x \oplus y$ (see [H5] or [K5]) and so the elements of each other row of the addition table of $(N_v, \oplus)$ also are distinct.

Next, we show that the left crossed inverse property holds in $(N_v, \oplus)$. We have

$$-1\oplus(a^{-k}\oplus 1) = a^\ell\oplus[a^{-k}(1\oplus a^k)] = a^\ell\oplus[a^{-k}a^{\ell+n}] = a^\ell(1\oplus a^{n-k}) = a^\ell a^{\ell-k} = a^{-k}.$$

Here, we have used the fact that, if the ordered pair (k, n) occurs in an XIP-admissible decomposition, so does the ordered pair $(n-k, -k)$. Thence, using the left distributive law, $-a^g \oplus (a^f \oplus a^g) = a^g[-1\oplus(a^{f-g}\oplus 1)] = a^g a^{f-g} = a^f$. That is, the left crossed inverse property holds for each pair of non-zero elements.

It follows that $a^f \oplus 1 = a^g \oplus 1 \Leftrightarrow -1\oplus(a^f\oplus 1) = -1 \oplus (a^g \oplus 1) \Leftrightarrow a^f = a^g$. Hence, the elements $0\oplus 1$, $a^\ell \oplus 1$, $a^k\oplus 1$ for $k = 0, 1, \dots, \ell-1, \ell+1, \dots, v-1$ are all distinct: that is, the elements of the second column of the addition table of $N_v, \oplus)$ are all distinct. Using the left distributive law, we easily deduce that the elements of each column of the addition table of $(N_v, \oplus)$ are all distinct. Thus, $(N_v, \oplus)$ is a loop. The rest of the proof can safely be left to the reader. □

Note that the fact that the right crossed inverse property holds in $(N_v, \oplus)$ follows from Lemma 3.1. Note also that we have proved in effect that, when we have an XIP-admissible decomposition, the mapping $\varphi : a^k \longrightarrow a^{\ell+n}$ is a near orthomorphism of the cyclic group $G = \langle a : a^{v-1} = 1\rangle$. It is, in fact, what we earlier called the presentation function of the neofield. See Definition 3.5 and compare our Theorem 3.3.

DEFINITION 8.3 The XIP-neofields constructed by the method of Theorem 8.7 are said to be of type (a)(i), (a)(ii), a(iii) or (b) according to the type of the corresponding XIP-decomposition of the residues modulo $(v-1)$.

THEOREM 8.8 *Every XIP-neofield $(N_v, \oplus, .)$ of odd order v which is of type (a)(i) has both the left and right inverse properties (as well as the crossed-inverse property) and so it is commutative.*

Proof. In such an XIP-neofield, all of the ordered pairs of residues occur in sets of the type $T_1(k_i, n_i) = \{(k_i, \ell + n_i), (n_i - k_i, \ell - k_i), (-n_i, \ell + k_i - n_i), (n_i, \ell + k_i), (-k_i, \ell + n_i - k_i), (k_i - n_i, \ell - n_i)\}$ $i = 1, 2, \ldots,$ and, including the at-most-two such sets which are degenerate (see Lemma 8.6), in no others. Thus, if $1 \oplus a^k = a^{\ell+n}$, we also have $1 \oplus a^n = a^{\ell+k}$ and $1 \oplus a^{k-n} = a^{\ell-n}$. It follows that $-1 \oplus (1 \oplus a^k) = a^\ell \oplus a^{\ell+n} = a^\ell(1 \oplus a^n) = a^\ell a^{\ell+k} = a^k$, and $(1 \oplus a^k) \oplus (-a^k) = a^{\ell+n} \oplus a^{\ell+k} = a^{\ell+n}(1 \oplus a^{k-n}) = a^{\ell+n}a^{\ell-n} = a^{2\ell} = 1$. Using the distributive laws, we easily deduce the desired result. The fact that such a cyclic neofield is commutative for addition follows from Lemma 3.4.

It is clear from Theorem 8.8 that XIP-neofields of odd order v and of type (a)(i) are of no use for our cryptological applications.

XIP-neofields of odd order v and of type (a)(ii) also have a special property and they exist only for orders $v \equiv 3 \bmod 6$ and excluding $v \equiv 15$ or $21 \bmod 24$ (see below).

DEFINITION 8.4 An XIP-neofield $(N_v, \oplus, .)$ is called *special* if $(x \oplus y)(y \oplus x) = xy$ for all non-zero $xy \in N_v$.

Hsu has shown that XIP-neofields which are special in the sense of this definition are co-extensive with those of type (a)(ii). We give an outline of the proof at the end of this section.

First, we give some illustrative examples.

EXAMPLE 8.1 For $v = 9$, $\ell = 4$ and $v \equiv 3 \bmod 6$ so, by Lemma 8.6, the sets $T_3(k, n)$ all have cardinal 3 except for the singleton $T_3(0, 0) = \{(0, 4)\}$. An XIP-admissible partition of $\mathbb{Z}_8 \setminus \{4\}$ of type (a) is given by the disjoint sextuples

$$S(1,6) = \{1,\ 6,\ 5,\ 7,\ 2,\ 3\} \quad \text{and} \quad S(0,0) = \{0\}.$$

Thence, $T_2(1,6) = \{(1,2), (5,3), (2,7), (6,1), (7,6), (3,5)\}$ and $T_2(0,0) = \{(0,4)\}$.

We get a proper XIP-neofield of type (a)(ii) with presentation function

$$\begin{array}{ccccccccccc} x & = & 0 & 1 & a & a^2 & a^3 & a^4 & a^5 & a^6 & a^7 \\ 1 + x & = & 1 & a^4 & a^2 & a^7 & a^5 & 0 & a^3 & a & a^6 \end{array}$$

EXAMPLE 8.2 For $v = 17$, $\ell = 8$ and $v \equiv 5 \bmod 6$ so, by Lemma 8.6, the sets $T_3(k, n)$ all have cardinal 3 and a triple $T_3(0, h)$ with $h \neq 0$ occurs. An XIP-admissible partition of $\mathbb{Z}_{16} \setminus \{8\}$ of type (a) is given by the disjoint sextuples

$$S(2,7) = \{2,\ 7,\ 5,\ 14,\ 9,\ 11\}, \quad S(3,4) = \{3,\ 4,\ 1,\ 13,\ 12,\ 15\},$$

$$\text{and} \quad S(0,6) = \{0,\ 6,\ 6,\ 0,\ 10,\ 10\}.$$

These give rise to three different XIP-neofields of type (a)(iii) as follows:

(I) $T_2(2,7) = \{(2,15),(5,6),(9,3),(7,13),(14,1),(11,10)\}$,
$T_2(3,4) = \{(3,12),(1,5),(12,7),(4,9),(13,4),(15,11)\}$,
$T_1(0,6) = \{(0,14),(6,8),(10,2)\}$.

x	=	0	1	a	a^2	a^3	a^4	a^5	a^6	a^7	a^8	a^9	a^{10}	a^{11}
$1+x$	=	1	a^{14}	a^5	a^{15}	a^{12}	a^9	a^6	a^8	a^{13}	0	a^3	a^2	a^{10}
x	=	a^{12}	a^{13}	a^{14}	a^{15}									
$x+1$	=	a^7	a^4	a	a^{11}									

Note In [H4], from which the above examples are taken (see pages 67 and 56), it is incorrectly stated on page 57 that this neofield is of type (a)(ii). Later, it is proved that odd order neofields of type (a)(ii) exist only when $v \equiv 3 \bmod 6$, see above and below.

(II) $T_1(2,7) = \{(2,15),(5,6),(9,3),(7,10),(14,13),(11,1)\}$,
$T_2(3,4) = \{(3,12),(1,5),(12,7),(4,9),(13,4),(15,11)\}$,
$T_1(0,6) = \{(0,14),(6,8),(10,2)\}$.

x	=	0	1	a	a^2	a^3	a^4	a^5	a^6	a^7	a^8	a^9	a^{10}	a^{11}
$1+x$	=	1	a^{14}	a^5	a^{15}	a^{12}	a^9	a^6	a^8	a^{10}	0	a^3	a^2	a
x	=	a^{12}	a^{13}	a^{14}	a^{15}									
$x+1$	=	a^7	a^4	a^{13}	a^{11}									

(III) $T_2(2,7) = \{(2,15),(5,6),(9,3),(7,13),(14,1),(11,10)\}$,
$T_1(3,4) = \{(3,12),(1,5),(12,7),(4,11),(13,9),(15,4)\}$,
$T_1(0,6) = \{(0,14),(6,8),(10,2)\}$.

x	=	0	1	a	a^2	a^3	a^4	a^5	a^6	a^7	a^8	a^9	a^{10}	a^{11}
$1+x$	=	1	a^{14}	a^5	a^{15}	a^{12}	a^{11}	a^6	a^8	a^{13}	0	a^3	a^2	a^{10}
x	=	a^{12}	a^{13}	a^{14}	a^{15}									
$x+1$	=	a^7	a^9	a	a^4									

Note If we replace $T_2(2,7)$ by $T_1(2,7)$ in this last example, we shall get a commutative inverse property cyclic neofield by Theorem 8.8. Likewise, since $T_1(0,0) = T_2(0,0)$, if we replace $T_2(1,6)$ in Example 8.1 by $T_1(1,6) = \{(1,2),(5,3),(2,7),(6,5),(7,1),(3,6)\}$ we shall again get a commutative inverse property neofield which, in that case, is the finite field $GF[3^2]$.

EXAMPLE 8.3 For $v = 13$, $\ell = 6$ and $v \equiv 1 \bmod 6$ so, by Lemma 8.6, the sets $T_3(k,n)$ must include both of the singletons $T_3(4,8)$ and $T_3(8,4)$ and also a triple $T_3(0,h)$ with $h \equiv 0 \bmod 12$. An XIP-admissible partition of $\mathbb{Z}_{12} \setminus \{6\}$ of type (a) is given by the disjoint sextuples

$$S(1,3) = \{1,3,2,11,9,10\}, \quad S(0,5) = \{0,5,5,0,7,7\},$$

$$\text{and } S(4,8) = \{4,8,4,8,4,8\}\,.$$

These give rise to an XIP-neofield of type (a)(iii) as follows:

$T_2(1,3) = \{(1,9),(2,5),(9,4),(3,8),(11,3),(11,7)\}$,
$T_1(0,5) = T_3(0,5) = \{(0,11),(5,6),(7,1)\}$,
$T_3(4,8) = \{(4,2)\}$,
$T_3(8,4) = \{(8,10)\}$.

$$\begin{array}{lcccccccccccccc}
x & = & 0 & 1 & a & a^2 & a^3 & a^4 & a^5 & a^6 & a^7 & a^8 & a^9 & a^{10} & a^{11} \\
1+x & = & 1 & a^{11} & a^9 & a^5 & a^8 & a^2 & a^6 & 0 & a & a^{10} & a^4 & a^7 & a^3
\end{array}$$

Note The same XIP-admissible partition of $\mathbb{Z}_{12} \setminus \{6\}$ gives rise to the finite field $GF[13]$ with 7 as primitive root as follows:

$T_1(1,3) = \{(1,9),(2,5),(9,4),(3,7),(11,8),(10,3)\}$,
$T_1(0,5) = T_3(0,5) = \{(0,11),(5,6),(7,1)\}$,
$T_1(4,8) = \{(4,2),(8,10)\}$.

$$\begin{array}{lcccccccccccccc}
x & = & 0 & 1 & 7 & 7^2 & 7^3 & 7^4 & 7^5 & 7^6 & 7^7 & 7^8 & 7^9 & 7^{10} & 7^{11} \\
 & = & 0 & 1 & 7 & 10 & 5 & 9 & 11 & 12 & 6 & 3 & 8 & 4 & 2 \\
1+x & = & 1 & 7^{11} & 7^9 & 7^5 & 7^7 & 7^2 & 7^6 & 0 & 7 & 7^{10} & 7^4 & 7^3 & 7^8
\end{array}$$

Hsu has shown that XIP-admissible partitions of type (a) do not exist if $v \equiv 15$ or $21 \bmod 24$. However, partitions of type (b) exist when $v = 15$ or 21.

EXAMPLE 8.4 For $v = 15$, $\ell = 7$ and $v \equiv 3 \bmod 6$ so, by Lemma 8.6, the sets $T_3(k,n)$ all have cardinal 3 except for the singleton $T_3(0,0) = \{(0,7)\}$. An XIP-admissible partition of $\mathbb{Z}_{14} \setminus \{7\}$ of type (b) is given by the sextuples

$S(1,4) = \{1,4,3,13,10,11\}$ $\quad S(2,6) = \{2,6,4,12,8,10\}$
$S(6,1) = \{6,1,9,8,13,5\}$ $\quad S(5,2) = \{5,2,11,9,12,3\}$
$S(0,0) = \{0\}$.

These give rise to an XIP-neofield of type (b) as follows:

$T_3(1,4) = \{(1,11),(3,6),(10,4)\}$ $\quad T_3(2,6) = \{(2,13),(4,5),(8,3)\}$
$T_3(6,1) = \{(6,8),(9,1),(13,12)\}$ $\quad T_3(5,2) = \{(5,9),(11,2),(12,10)\}$
$T_3(0,0) = \{(0,7)\}$.

$$\begin{array}{lcccccccccccc}
x & = & 0 & 1 & a & a^2 & a^3 & a^4 & a^5 & a^6 & a^7 & a^8 & a^9 \\
1+x & = & 1 & a^7 & a^{11} & a^{13} & a^6 & a^5 & a^9 & a^8 & 0 & a^3 & a \\
x & = & a^{10} & a^{11} & a^{12} & a^{13} & & & & & & & \\
x+1 & = & a^4 & a^2 & a^{10} & a^{12} & & & & & & &
\end{array}$$

Example 8.4 is an example of a general construction for an XIP-admissible partition of $\mathbb{Z}_{6m+2} \setminus \{3m+1\}$ of type (b) when $v = 6m+3$, $m \geq 2$. There are

$2m$ sextuples $S(k,n) = \{k, n, n-k, -k, -n, k-n\}$ which are as follows:

1	$m+2$	$m+1$	$6m+1$	$5m$	$5m+1$
2	$m+4$	$m+2$	$6m$	$5m-2$	$5m$
3	$m+6$	$m+3$	$6m-1$	$5m-4$	$5m-1$
•	•	•	•	•	•
•	•	•	•	•	•
$m-1$	$3m-2$	$2m-1$	$5m+3$	$3m+4$	$4m+3$
m	$3m$	$2m$	$5m+2$	$3m+2$	$4m+2$
$3m$	1	$3m+3$	$3m+2$	$6m+1$	$3m-1$
$3m-1$	2	$3m+5$	$3m+3$	$6m$	$3m-3$
$3m-2$	3	$3m+7$	$3m+4$	$6m-1$	$3m-5$
•	•	•	•	•	•
•	•	•	•	•	•
$2m+2$	$m-1$	$5m-1$	$4m$	$5m+3$	$m+3$
$2m+1$	m	$5m+1$	$4m+1$	$5m+2$	$m+1$

We note that each residue occurs just once as an α-element $k, n-k$, or $-n$ and just once as a β-element $n, -k$, or $k-n$.

For further general constructions of XIP-neofields of the various types, see [H4].

We end this section with the promised outline of the structure of XIP-neofields of type (a)(ii). We shall need two lemmata.

LEMMA 8.9 *In a special XIP-neofield $(N_v, +, .)$ of odd order v, any of the statements* (i) $1 + a^k = a^{\ell+n}$, (ii) $1 + a^{n-k} = a^{\ell-k}$, (iii) $1 + a^{-n} = a^{\ell+k-n}$, (iv) $1 + a^{-k} = a^{\ell-n}$ (v) $1 + a^{k-n} = a^{\ell+k}$, (vi) $1 + a^n = a^{\ell+n-k}$ *implies the other five.*

Proof. It was shown in Lemma 8.3 that (i) ⇒ (ii) ⇒ (iii) ⇒ (i) and that same lemma shows also that (iv) ⇒ (v) ⇒ (vi) ⇒ (iv). To complete the proof, it is only necessary to show that (i) and (iv) imply each other.

(i) ⇒ (iv): From the property $(x+y)(y+x) = xy$, we get $(1+a^k)(a^k+1) = 1.a^k$ and so, using (i), $a^{\ell+n}(a^k+1) = a^k$. Multiplying by $a^{\ell-n-k}$ and using the left distributive law and the fact that $a^{2\ell} = 1$, we get $1 + a^{-k} = a^{\ell-n}$ which is (iv).

(iv) ⇒ (i): We repeat the previous argument with k, n replaced by $-k, -n$. □

Let k, n be an XIP-admissible pair of residues in a special XIP-neofield N_v of odd order v. Then, by the preceding lemma, $1 + a^{k-n} = a^{\ell+k}$, $1 + a^n = a^{\ell+n-k}$, and $1 + a^{-k} = a^{\ell-n}$ and so, as our earlier discussion showed, k and n occur in only one sextuple $S(k,n) \equiv S(k-n,k) = \{k-n, k, n, n-k, -k, -n\}$ which is totally disjoint from the remainder. This sextuple has cardinal six except when $k \equiv 0$, $n \equiv 0$ or $k \equiv \pm n$ modulo $(v-1)$. We show now that each of these conditions occurs only when $k \equiv n \equiv 0$.

LEMMA 8.10 *In a special XIP-neofield $(N_v, +, .)$ of odd order v any one of the conditions $k \equiv 0$, $n \equiv 0$ or $k \equiv \pm n$ modulo $(v-1)$ occurs only when $k \equiv n \equiv 0$.*

Proof. It follows directly from Lemma 8.9 that the conditions $k \equiv 0$ or $n \equiv 0$ modulo $(v-1)$ imply each other in a special XIP-neofield of odd order. (If $k \equiv 0$, then relations (i) and (vi) give $1+1 = a^{\ell+n} = 1 + a^n$ so $n \equiv 0 \equiv k$. If $n \equiv 0$, then relations (i) and (v) give $a^\ell = 1 + a^k = a^{\ell+k}$ so $k \equiv 0 \equiv n$.) If $k \equiv n$ modulo $(v-1)$ occurs then, by relations (i) and (vi) of Lemma 8.9, $a^{\ell+n} = 1 + a^k = a^\ell$ so $k \equiv n \equiv 0$ as before. If $k \equiv -n$ modulo $(v-1)$ occurs then, by relations (i) and (ii) of Lemma 8.9, we get $1 + a^k = 1 + a^{-2k}$ whence $3k \equiv 0 \bmod (v-1)$. If $\gcd(3, v-1) = 1$, then $k \equiv 0$ and $n \equiv 0$ as before but, if $\gcd(3, v-1) \neq 1$, $\{k, n\} = \{(v-1)/3, 2(v-1)/3\}$.

By counting exponents $n + \ell$ of elements $a^{n+\ell}$ in manner similar to that used for the proof of Lemma 8.6, Hsu has shown that the latter case leads to a contradiction. Hence, each of the conditions $k \equiv 0$, $n \equiv 0$ and $k \equiv \pm n$ modulo $(v-1)$ occurs only when $k \equiv n \equiv 0$ as claimed. □

It follows from Lemma 8.10 and from the remarks which precede it that, in a special XIP-neofield of odd order, each sextuple in the decomposition of the residues $\mathbb{Z}_{v-1} \setminus \{\ell\}$ is such that $S(k,n) \equiv S(k-n, k)$ except for $S(0,0) = \{0\}$ and is totally disjoint from the remainder. Thus, all of the pairs of non-zero indices in the presentation function φ of the neofield occur as pairs in sets of type $T_2(k,n)$. That is, the XIP-neofield is of type (a)(ii).

Conversely, every partition of the non-zero residues modulo $(v-1)$ which is of type (a)(ii) defines an XIP-neofield in which $1+a^k = a^{\ell+n} \Rightarrow 1+a^{-k} = a^{\ell-n}$: that is one in which $1+a^k = a^{\ell+n} \Rightarrow a^k+1 = a^{\ell+k-n}$ and so $(1+a^k)(a^k+1) = a^{\ell+n}a^{\ell+k-n} = a^k$. It follows that $(a^r+a^s)(a^s+a^r) = a^{2r}[(1+a^{s-r})(a^{s-r}+1)] = a^{2r}a^{s-r} = a^r a^s$ and so $(x+y)(y+x) = xy$ for all non-zero elements of the neofield. Hence:

THEOREM 8.11 *The XIP-neofields of odd order v which are defined by partitions of the non-zero residues modulo $(v-1)$ of type* (a)(ii) *are precisely the special XIP-neofields of odd order.*

In any XIP-neofield, there exists a pair (k,n) of residues for which $k \equiv 0$ and one, possibly the same one, for which $n \equiv 0$. It follows from Lemma 8.10 that the conditions $k \equiv 0$ or $n \equiv 0$ modulo $(v-1)$ imply each other in an odd order XIP-neofield of type (a)(ii). Also, when $k \equiv n \equiv 0$, $1+1 = a^\ell = -1$. Thus, 3 divides the order of the addition loop of the neofield and so $v \equiv 3 \bmod 6$. We state this as a theorem:

THEOREM 8.12 *XIP-neofields of odd order v which are defined by partitions of the non-zero residues modulo $(v-1)$ of type* (a)(ii) *exist only for orders $v \equiv 3$ mod 6.*

Finally, we prove:

THEOREM 8.13 *XIP-admissible partitions of the residues modulo* $(v-1)$ *of type* (a) *do not exist if* $v \equiv 15$ *or 21* mod *24.*

Proof. Since $v \equiv 3 \bmod 6$, the singleton $T_3(0,0) = \{(0,\ell)\}$ must occur among the sets $T_3(k_i,n_i)$ by Lemma 8.6. Thus, all of the sets $S(k_i,n_i)$ into which the residues $\mathbb{Z}_{v-1} \setminus \{\ell\}$ are partitioned have cardinal 6 except for the set $S(0,0) = \{0\}$.

Let $v = 24x + 6y + 3$, where $y = 2$ or 3. Then $\mathbb{Z}_{v-1} \setminus \{0,\ell\}$ has cardinal $24x + 6y$ and so there are $4x + y$ sets $S_i = S(k_i,n_i)$ of cardinal 6. Now,

$$\mathbb{Z}_{v-1} \setminus \{0,\ell\} = \{1,2,3,\ldots,24x+6y+1\} \setminus \{12x+3y+1\}$$

since $\ell = (v-1)/2 = 12x + 3y + 1$.

When $y = 2$, $12x + 3y + 1$ is odd so then there are $12x + 3y$ odd residues and $12x + 3y$ even residues in the set $\mathbb{Z}_{v-1} \setminus \{0,\ell\}$.

When $y = 3$, $12x + 3y + 1$ is even so then there are $12x + 3y + 1$ odd residues and $12x + 3y - 1$ even residues in the set $\mathbb{Z}_{v-1} \setminus \{0,\ell\}$.

We now count the number of even residues in the set $\mathbb{Z}_{v-1} \setminus \{0,\ell\}$ in an alternative way. Consider $S(k,n) = \{k, n, n-k, -k, -n, k-n\}$. When k and n are both even, all of the members of $S(k,n)$ are even. When k is even and n is odd, only the residues k and $-k$ are even since arithmetic is modulo $v - 1 = 24x + 6y + 2$ which is even. When k is odd and n is even, only the residues n and $-n$ are even. When both k and n are odd, only the residues $n - k$ and $k - n$ are even. Suppose now that $\mathbb{Z}_{v-1} \setminus \{0,\ell\}$ contains r sets $S(k_i,n_i)$ with k_i, n_i both even and $4x + y - r$ sets $S(k_i,n_i)$ with at most one of k_i, n_i even. Then, the number of even residues in the set $\mathbb{Z}_{v-1} \setminus \{0,\ell\}$ is $6r + 2(4x + y - r)$ in total. This latter number must be equal to $12x + 3y$ when $y = 2$ and to $12x + 3y - 1$ when $y = 3$. Hence, $8x + 2y + 4r = 12x + 3y$ when $y = 2$ and $8x + 2y + 4r = 12x + 3y - 1$ when $y = 3$. That is, $4r = 4x + 2$ in both cases. But this is impossible because 4 does not divide 2. Consequently, a type (a) partition of the residues cannot exist. □

Note In [H4], Hsu only states the above non-existence theorem for XIP-neofields of type (a)(ii) (which he calls *SIP-neofields*, but later he assumes the more general statement given above.

Acknowledgements The first author would like to thank Y. Desmedt for introducing him to the concept of digital fingerprinting and for drawing his attention to the paper [S9] of G.F. Simmons. He also wishes to thank R.H.-Schulz for drawing his attention to the fact that the method of digital fingerprinting German bank notes is described in his book [S5] and in the book [B5] of A. Beutelspracher. The second author wishes to thank S. Blackburn for allowing him to include Theorem 4.5 in this survey.

The authors would like to thank S.W. Golomb for kindly making a private translation of [B3] from Russian to English. Also, they are grateful to C. Koscienly for his helpfulness and willingness to communicate his results and, in particular, the first author wishes to thank him for agreeing to carry out some relevant computations on his behalf.

Additional Note It has recently come to the attention of the authors that J. Szép in Chapter 1 of [S11] has employed a completely different non-associative algebraic system for coding and cryptographic purposes. Namely, he makes use of the so-called ρ-product of multisets which in general is not an associative operation.

References

[A1] A.A. ALBERT, *Quasigroups* I, II., Trans. Amer. Math Soc., **54** (1943), 507–579 and **55** (1944), 401–419.

[A2] R. ARTZY , *On loops with a special property*, Proc. Amer. Math. Soc., 6 (1955), 443–453.

[A3] R. ARTZY, *Crossed inverse and related loops*, Trans. Amer. Math. Soc., **91** (1959), 490–492.

[B1] H.J. BEKER and F. PIPER, *Cipher Systems: the Protection of Communications*, Northwood, London, 1982.

[B2] V.D. BELOUSOV, *Systems of quasigroups with generalized identities*, (Russian), Usp. Mat. Nauk, **20** (1965), No.1 (121), 75–176. Translated as Russian Math. Surveys, **20** (1965), 73–143.

[B3] V.D. BELOUSOV and B.V. TSURKIN, *Crossed inverse quasigroups (CI-quasigroups)*, (Russian), Izv. Vyssh. Uchebn. Zaved. Math., (1969) No.3 (82), 21–27. Translated as Soviet Math. Izv. VUZ.

[B4] S. BLACKBURN, Private communication to A.D. Keedwell, 12 June, 1998.

[B5] A. BEUTELSPRACHER, *Cryptology*, Math. Assoc. of America, 1994.

[C1] P.J. CAMERON, *Fisher and Bose, Hamming and Golay*, Talk given at the One-day Combinatorics Colloquium, Reading, England, 20 May, 1998.

[C2] J.H. CONWAY, *A tabulation of some information concerning finite fields*, In: Computers in Mathematical Research, Eds. R.F. Churchhouse, J.C. Herz, North Holland, Amsterdam, 1968, 37–50.

[C3] R.A. CROFT and S.P. HARRIS, *Public-key cryptography and re-usable shared secrets*, In: Cryptography and Coding, Eds. H.J. Beker and F. Piper, Clarendon Press, Oxford, 1989, 189–201.

[D1] ED DAWSON, DIANA DONOVAN, ALAN OFFER, *Quasigroups, isotopisms and authentication schemes*, Austral. J. Combin., **13** (1996), 75–88.

[D2] J. DÉNES, *On a problem of A. Kotzig*, Annals of Discrete Mathematics, **18** (1983), 283–290.

[D3] J. DÉNES and A.D. KEEDWELL, *Latin Squares and their Applications*, Akadémiai Kiadó, Budapest; Academic Press, New York; English Universities Press, London, 1974.

[D4] J. DÉNES and A.D. KEEDWELL (eds. and part authors), *Latin Squares: New Developments in the Theory and Applications*, Annals of Discrete Mathematics, Vol. 46, North Holland, Amsterdam, 1990.

[D5] J. DÉNES and A.D. KEEDWELL, *A new authentication scheme based on latin squares*, Discrete Math., **106/107** (1992), 157–161.

[D6] J. DÉNES, G.L. MULLEN, S.J. SUCHOWER, *Another generalized Golomb-Posner code*, IEEE Trans. Information Theory, IT-**36** (1990), 408–411.

[E1] A. ECKER and G. POCH, *Check character systems*, Computing **37** (1986), 277–301.

[E2] T. ELGAMAL, *A public key cryptosystem and a signature scheme based on discrete logarithms*, IEEE Trans. Information Theory IT-**31** (1985), 469–472.

[F1] D.J. FINNEY, *An introduction to the theory of experimental design*, Univ. of Chicago Press, Chicago and London, 1960.

[F2] R.A. FISHER, *The theory of confounding in factorial experiments in relation to the theory of groups*, Annals of Eugenics **11** (1942), 341–353.

[F3] R.A. FISHER, *A system of confounding for factors with more than two alternatives, giving completely orthogonal cubes and higher powers*, Annals of Eugenics, **12** (1945), 283–290.

[F4] W.F. FRIEDMAN and C.J. MENDELSOHN, *Notes on codewords*, Amer. Math. Monthly **39** (1932), 394–409.

[G1] M.J.E. GOLAY, *Notes on digital coding*, Proc. IRE **37** (1949), 657.

[G2] S.W. GOLOMB and E.C. POSNER, *Rook domains, latin squares, affine planes and error distributing codes* , IEEE Trans. Information Theory, IT-**10** (1964), 196–208.

[G3] R.K. GUY, Private communication to A.D. Keedwell, July, 1997.

[H1] R.W. HAMMING, *Error detecting and correcting codes*, Bell System Tech. J. **29** (1950), 147–160.

[H2] R. HILL, *A First Course in Coding Theory*, Clarendon Press, Oxford, 1986.

[H3] L.J. HOFFMANN, *Building in Big Brother: the Cryptographic Policy Debate*, Springer, New York, 1995.

[H4] D.F. HSU, *Cyclic neofields and combinatorial designs*, Lecture Notes in Mathematics, Vol. 824, Springer, Berlin, 1980.

[H5] D.F. HSU and A.D. KEEDWELL, *Generalized complete mappings, neofields, sequenceable groups and block designs*, I, II., Pacific Journal of Mathematics, **111** (1984), 317-332 and **117** (1985), 291–311.

[H6] K. HUBER, *Some comments on Zech's logarithms*, IEEE Trans. Information Theory, IT-**36** (1990), 946–950.

[H7] K. HUBER, *Solving equations in finite fields and some results concerning the structure of* GF$[p^m]$, IEEE Trans. Information Theory, IT-**38** (1992), 1154–1162.

[J1] C.G.J. JACOBI, *Über die Kreistheilungen und ihre Anwendung auf die Zahlentheorie*, Crelle Journal für die reine und angew. Math., **30** (1846), 166–182. Also published in Monatsbericht der Akademie der Wissenschaften zu Berlin von 16 October 1837; Bd 6, s254–274, Gesammelte Werke 1–7 Bd, Berlin, Reiner, 1881–91.

[J2] E.C. JOHNSON and T. STORER, *Combinatorial structures in loops; II Commutative inverse property cyclic neofields of prime power order*, Pacific J. Math., **52** (1974), 115–127.

[K1] D. KAHN, *The codebreakers: the story of secret writing*, Wiedenfield and Nicholson, London, 1967.

[K2] B.B. KARKLINÜSH and V.B. KARKLIN, *Inverse loops* (Russian), In: Nets and quasigroups, Mat. Issl., **39** (1976), 82–86.

[K3] A.D. KEEDWELL, *On orthogonal latin squares and a class of neofields*, Rend. Mat. e Appl. (Roma) (5) **25** (1966), 519–561.

[K4] A.D. KEEDWELL, *On property* D *neofields*, Rend. Mat. e Appl. (Roma) (5) **26** (1967), 383–402.

[K5] A.D. KEEDWELL, *The existence of pathological left neofields*, Ars Combinatoria, **B16** (1983), 161–170.

[K6] A.D. KEEDWELL, *Critical sets for latin squares, graphs and block designs; a survey*, Congressus Numerantium **113** (1996), 231–245.

[K7] A.D. KEEDWELL, *Crossed-inverse quasigroups with long inverse cycles and applications to cryptography*, Austral. J. Combin., **20** (1999), 241–250.

[K8] A.D. KEEDWELL, *A characterization of the Jacobi logarithms of a finite field*, Discrete Math., **231** (2001), 295–302.

[K9] C. KOŚCIELNY, *Spurious Galois fields*, Appl. Math. and Comp. Sci., **5** (1995), 169–188.

[K10] C. KOŚCIELNY, *A method of constructing quasigroup-based stream-ciphers*, Appl. Math. and Comp. Sci., **6** (1996), 109–121.

[L1] B.A. LAMACCHIA and A.M. ODLYZKO, *Computation of discrete logarithms in prime fields*, Designs, Codes and Cryptography, **1** (1991), 47–62.

[L2] C.F. LAYWINE and G.L. MULLEN, *Discrete Mathematics using Latin Squares*, Wiley, New York, 1998.

[L3] R. LIDL and H. NIEDERREITER, *Finite fields*, Addison-Wesley Publ. Co., Reading, Massachusetts, 1983.

[M1] F.J. MACWILLIAMS and N.J.A. SLOANE, *The Theory of Error-Correcting Codes*, North Holland, Amsterdam, 1977.

[M2] L. MITTENTHAL, *Block substitutions using orthomorphic mappings*, Advances in Applied Mathematics, **16** (1995), 59–71.

[M3] L. MITTENTHAL, *A source of cryptographically strong permutations for use in block ciphers*, Proc. IEEE Internat. Sympos. on Information Theory 1993, IEEE, New York, 17-22.

[O1] A.M. ODLYZKO, *Discrete logarithms in finite fields and their cryptographic significance*, In: Lecture Notes in Computer Science No. 209; Advances in Cryptology, Proc. Eurocrypt 84, Eds. T. Beth, N. Cot, I. Ingemarsson, Springer, Berlin, 1985, 224–314.

[O2] J.M. OSBORN, *Loops with the weak inverse property*, Pacific J. Math., **10** (1960), 295–304.

[P1] L.J. PAIGE, *Neofields*, Duke Math. J., **16** (1949), 39–60.

[P2] B. PFITZMANN, *Digital Signature Schemes: general framework and fail-stop signatures*, Springer, Berlin, 1996.

[R1] J.B. ROSSER and R.J. WALKER, *On the transformation group for diabolic magic squares of order four*, Bull. Amer. Math. Soc., **44** (1938), 416–420.

[R2] J.B. ROSSER and R.J. WALKER, *The algebraic theory of diabolic magic squares*, Duke Math. J., **5** (1939), 705–728.

[R3] R.A. RUEPPEL, *Analysis and design of strem ciphers*, Springer, Berlin, 1986.

[S1] R. SCHAUFFLER, *Eine Anwendung zyklischer Permutationen und ihre Theorie*, (Ph. D. Theis, Marburg University, 1948). English translation exists. Original manuscript: Scheibe und Schieber, Manuskr. Ausw. Amt, Berlin, 1941.

[S2] R. SCHAUFFLER, *Über die Bildung von Codewörter*, Arch. Elektr. Übertragung **10** (1956), 303–314.

[S3] C.P. SCHNORR, *Efficient identification and signatures for smart cards*, In: Lecture Notes in Computer Science No. 435; Advances in Cryptology, Proc. Crypto' 89", Ed. G. Brassard, Springer, Berlin, 1990, 239–351.

[S4] E. SCHÖNHARDT, *Über latinische Quadrate und Unionen*, J. Reine Angew. Math., **163** (1930), 183–229.

[S5] R.H.-SCHULZ, *Kodierungtheorie: eine Einführung*, Vieweg Verlag, Braunschweig, Wiesbaden, 1991.

[S6] R.H.-SCHULZ, *A note on check character systems using latin squares*, Discrete Math. **97** (1991) , 371–375.

[S7] R.H.-SCHULZ, *Check character systems over groups and orthogonal latin squares*, Applicable Algebra in Engineering, Communication and Computing **7** (1996), 126–132.

[S8] G.J. SIMMONS (ed.), *Contemporary cryptology*, IEEE Press, New York, 1991.

[S9] G.J. SIMMONS, *Identification of data, devices, documents and individuals*, In: Proc. 25th Annual IEEE Carnahan Conf. on Security Technology, 1991, IEEE, New York, 197–218.

[S10] D.R. STINSON, *Cryptology : Theory and Practice*, CRC Press, Boca Raton, London and Tokyo, 1995.

[S11] J. SZÉP, *Vector Products and Applications*, Akadémiai Kiadó, Budapest, 1998.