Quasigroups, Isotopisms and Authentication Schemes

Ed Dawson*, Diane Donovan** and Alan Offer**

*Information Security Research Centre
Faculty of Information Technology
Queensland University of Technology
GPO Box 2434, Brisbane, Qld 4001
Australia

**Centre for Combinatorics
Department of Mathematics
The University of Queensland
Brisbane, Qld 4072
Australia

Abstract

In 1992 Dénes and Keedwell proposed an authentication scheme in which a message is divided into blocks of length t and a set of signature characters is obtained by taking the product of the elements of each block. An analysis of the security of Dénes and Keedwell's scheme will be presented in this paper. It will be shown that the method used to divide the message into the blocks impacts on the security of the scheme. Also it will be shown that under certain circumstances the t–ary product is not unique, and so there are classes of binary operations all of which produce the same signature or authentication tag.

1 Introduction

In 1992 Dénes and Keedwell [2] used the theory of quasigroups to develop a new technique for authenticating a digital message. Let Q be a set of objects and define a binary operation, $*$, on the set Q such that given any two elements $a, b \in Q$ the equations $a * x = b$ and $y * a = b$ each have exactly one solution. Then Q together with the binary operation $*$ define a quasigroup, denoted by $(Q, *)$. A quasigroup may be thought of as a latin square bordered by a headline and a sideline. For more information on quasigroups see [1]. Essentially, Dénes and Keedwell took the digits of a message and used the binary operation of a quasigroup to compute the product of the digits. This product formed the signature or authentication tag and was appended to the message. The signed message was sent and the receiver used the binary operation of the same quasigroup to verify that the authentication tag

Australasian Journal of Combinatorics 13(1996), pp.75-88

corresponded to the message. So the authentication process can be classified as a cryptographic checksum.

An analysis of the security of this method of authentication will be presented in this paper.

In Section 2 it will be shown that if the product is obtained by simply multiplying consecutive digits of a message then it is possible for an eavesdropper to forge a signed message and under certain circumstances recover the entire quasigroup and impersonate the sender. Therefore one should use the alternative method suggested by Dénes and Keedwell to selecting the blocks. It will be mentioned that this method is secure against the attack presented in this paper.

During the investigation of this scheme it became apparent that the structure of the quasigroup also impacted on the security of the scheme. Computer simulation of an attack on the scheme verified that it was possible to identify several isotopic quasigroups all of which produce the same signature for messages of a given length. Two quasigroups $(Q, *)$ and $(P, \oplus)$ are said to be *isotopic* if there exists an ordered triple (α, β, γ) of one–to–one mappings α, β, γ of the set Q onto the set P such that

$$\alpha(x) \oplus \beta(y) = \gamma(x * y), \quad \text{for all } x, y \in Q.$$

The ordered triple (α, β, γ) is said to be an *isotopism*. If the one–to–one mappings α, β, γ map the set Q onto itself and if

$$\alpha(x) * \beta(y) = \gamma(x * y) \quad \text{for all } x, y \in Q,$$

then the ordered triple (α, β, γ) is said to be an *autotopism*. For more details see [1].

In Section 3 the structure of isotopic quasigroups will be investigated. A class of quasigroups on a set Q will be identified and it will be shown that, for given values of t, the product of t elements using the binary operation of any one of these quasigroups returns the same value. Finally, the impact of these general results on the authentication scheme proposed by Dénes and Keedwell will be discussed.

2 Possible attacks on the authentication scheme

The method of authentication proposed by Dénes and Keedwell is as follows.

Let $\mathcal{M}$ be the set of all possible messages on m symbols over an alphabet $Q = \{1, \ldots, q\}$. The sender X begins by choosing a quasigroup $(Q, *)$. When the sender wishes to authenticate a message $M = a_1\, a_2\, \ldots\, a_m$ he begins by dividing the message into blocks. Assume for now that there are s blocks each of length t, that is, $m = st$. Let

$$a_{i1}\, a_{i2}\, \ldots\, a_{it}$$

be one such block and denote it by B_i. A signature character b_i is obtained by calculating the product

$$b_i = (..((a_{i1} * a_{i2}) * a_{i3}) * \ldots) * a_{it}.$$

This process is repeated for each block of the message. The characters $b_1, b_2, \ldots, b_s$ form the signature or authentication tag. This authentication tag is concatenated to the message and

$$a_1\, a_2\, \ldots\, a_m\, b_1\, b_2\, \ldots\, b_s$$

is transmitted as a signed message to the receiver Y. The receiver Y also holds a copy of the quasigroup $(Q, *)$ and uses it to authenticate the message. When Y receives a message $a_1\, a_2\, \ldots\, a_m\, b_1\, b_2\, \ldots\, b_s$, the authentication tag is verified as being authentic if, for each $i = 1, \ldots, s$,

$$b_i = (..((a_{i1} * a_{i2}) * a_{i3}) * \ldots) * a_{it}.$$

If m is not a multiple of the block length t, then Dénes and Keedwell modified the scheme as follows. Let $m = t(s-1) + r$. Then one may take $s-1$ blocks of length t and the last block of length r or alternatively $t-r$ blocks of length $t-1$ and $s-t+r$ blocks of length t.

Dénes and Keedwell give two methods for generating the blocks. These are outlined below.

Method 1.

The block B_k contains the t consecutive symbols

$$a_{kt+1}, a_{kt+2}, \ldots, a_{(k+1)t},$$

for $k = 0, \ldots, s-1$ of the message M.

Method 2.

Let L be the latin square corresponding to the quasigroup $(Q, *)$ and assume for $k = 1, \ldots, q$, entry k occurs in the cells $(i_{k1}, j_{k1}), \ldots, (i_{kq}, j_{kq})$ of L.

Further, assume that the message M is of length q^2. Then one selects q blocks $B_1, \ldots, B_q$ as follows. For $k = 1, \ldots, q$, the $(i_{kr}-1)q + j_{kr}$-th, $(1 \leq r \leq q)$, characters of the message M are placed in block B_k.

Dénes and Keedwell only described this method for $m = q^2$ and $t = q$. However, it is possible to vary these parameters. If the block size t is less than q, the first t occurrences of the entry k are used to select the symbols of block B_k and if t is greater than q, then one works modulo q. If the message is of length less than qt, then one of the easiest techniques for handling this situation is to pad the message out by adding dummy symbols. This technique will be discussed in more detail later in the paper.

Dénes and Keedwell briefly discussed the security of their scheme and pointed out that each of the possible symbols of the alphabet is equally likely to occur as an authentication character. Dénes and Keedwell also pointed out that the longer the signature (that is, the smaller the size of each block), the more certain one is of the authentication, but one must balance the size of the blocks against the cost of a longer signed message. However, there are other considerations. The following analysis shows that the method used to select the blocks affects the security of the

scheme. It will be demonstrated that under certain circumstances it is possible for an outsider to forge signed messages and in some cases impersonate the sender.

The attack presented here will be based on the assumption that an eavesdropper can intercept a large number of signed messages. It will be assumed that the size of the alphabet Q and size of the quasigroup are known to the eavesdropper, and, for now, it will be assumed that they are the same. It will also be assumed that the block size is constant and is known. Using this information it is easy to take a signed message and use the division algorithm to calculate the number of blocks. Once this is obtained it is possible to identify those symbols which are message characters and those which are authentication characters. The actual method of attack will depend on the procedure used to select the blocks. Therefore Methods 1 and 2 will be analysed separately.

Method 1.

Assume that the sender uses Method 1 to select the blocks and that two blocks $a_1\, a_2 \ldots a_u\, a_{u+1} \ldots a_t$ and $c_1\, c_2 \ldots c_u\, a_{u+1} \ldots a_t$ have been intercepted. Furthermore, suppose that both of these blocks possess the same authentication character. Certainly, an eavesdropper can deduce that

$$(..((a_1 * a_2) * a_3) * \ldots) * a_u = (..((c_1 * c_2) * c_3) * \ldots) * c_u.$$

Now, whenever the product $(..((a_1 * a_2) * a_3) * \ldots) * a_u$ occurs in a message, it may be replaced by the product $(..((c_1 * c_2) * c_3) * \ldots) * c_u$, and vice versa. Therefore, it is certainly possible for an eavesdropper to forge messages.

Furthermore, if an eavesdropper intercepts two blocks which coincide in the last $t-2$ places and in the authentication character, then significant information about the quasigroup has been obtained. Take the blocks and authentication character given below.

$$(\ldots((a_1 * a_2) * a_3) * \ldots) * a_t = b$$
$$(\ldots((c_1 * c_2) * a_3) * \ldots) * a_t = b$$

From these blocks it may be deduced that

$$a_1 * a_2 = c_1 * c_2,$$

or, more importantly, that the entries in the cells (a_1, a_2) and (c_1, c_2) of the multiplication table for the quasigroup $(Q, *)$ are the same. At this point the exact value of this entry is not known, only that the cells contain the same entry. For now this entry is identified with a new symbol, say α, from a set A and this information is stored in the corresponding cells of a *pair table*. The pair table is a $q \times q$ table bordered by Q, and an entry $\alpha \in A$ is placed in the cells (a_1, a_2) and (c_1, c_2) of the pair table if $a_1 * a_2 = c_1 * c_2$. If an eavesdropper can intercept enough information, then he may use equivalent pairs together with his knowledge that the table forms a quasigroup to recover all entries of the pair table. Note that the pair table gives a quasigroup $(A, \oplus)$ which is isotopic to $(Q, *)$.

If the eavesdropper can identify the isotopism, then he may recover the quasigroup $(Q, *)$. To do this the eavesdropper returns to the intercepted messages and identifies those blocks which coincide in the last $t-3$ places and authentication character. He now has sets of equivalent triples. The triples d_1, d_2, d_3 and e_1, e_2, e_3 are said to be equivalent if it can be deduced that

$$(d_1 * d_2) * d_3 = (e_1 * e_2) * e_3.$$

This information can also be recorded in a triple table. A *triple table* has q columns and as many rows as there are distinct entries in the pair table. The set Q borders the triple table with a headline, and the entries of the pair table border the triple table with a sideline. A new symbol, say β, from an arbitrary set B is taken and placed in the cells (α_d, d_3) and (α_e, e_3) of the triple table, if α_d and α_e are the entries in the cells (d_1, d_2) and (e_1, e_2), respectively, of the pair table.

Now by considering both the pair table and the triple table the isotopism can be identified.

In view of this, the following is an attack which, given enough information, will reveal the entire key and allow the eavesdropper to impersonate the sender.

ATTACK

Step 1. Group the blocks into classes according to their authentication characters. From now on, disregard the authentication characters. At this stage there are blocks of size t in at most q classes. Blocks in the same class have the same authentication character.

Step 2. Within each of these classes, group the blocks according to their k-th ($k = t$ initially) message characters. From now on, disregard this k-th character. There are now reduced blocks of size $k-1$ in (initially, at most q^2) classes. The reduced blocks in the same class have the same product.

Step 3. At this point there may be a reduced block common to two of the classes. This indicates that the blocks of these two classes all have the same product. Consequently, these classes are merged into a single class. This process is repeated until there are no reduced blocks occurring more than once.

Step 4. Repeat Steps 2 and 3 for $k = t-1, t-2, \ldots, 4$. Note that at this point there are reduced blocks of size 3 sorted into classes and that any two blocks in the same class have the same product. Retain this information for later use. Then repeat Steps 2 and 3 again for $k = 3$. At this point there are reduced blocks of size 2 grouped such that any two blocks in the same class have the same product.

Step 5. Use the information obtained in Step 4 to construct a pair table and a triple table.

Step 6. The fact that the key is a quasigroup on q symbols can now be used to complete the pair and triple tables.

Step 7. Now, with both tables complete, select one of the elements of A. Try, one at a time, assigning the characters of the alphabet Q to this symbol. For each assignment,

compare the pair and triple tables to determine the correspondence between the elements of the sets A and B. Then determine the correspondence between the sets A and B and the characters of the alphabet Q. It is at this stage that contradictory statements may lead to the ruling out of certain assignments. For each assignment not giving rise to a contradiction a single quasigroup is produced.

Step 8. In the event that a unique quasigroup has not been produced in Step 7, then the intercepted blocks and corresponding authentication tags can be used to check which quasigroup gives the correct authentication characters for these blocks. At this point it is possible that several quasigroups have been obtained by this procedure, and that these all produce the same authentication characters for the given block size irrespective of the block chosen. (This point is expanded on in Section 3.)

This attack is illustrated with the following small example.

Example 2.1 Assume that the quasigroup used in the signing transformation is of order 5 and that this is the size of the alphabet, Q. Also assume that the block size is four.

An eavesdropper intercepts the message

3	3	3	1	1	4	4	5	5	5	4	5	5	3	3	4
1	5	2	2	4	5	3	1	2	3	4	5	2	4	2	2
1	2	3	4	4	1	1	2	5	2	1	2				

and the corresponding authentication tag

$$4 \quad 3 \quad 3 \quad 2 \quad 5 \quad 4 \quad 3 \quad 5 \quad 2 \quad 4 \quad 4.$$

Using Method 1, eleven blocks with their corresponding authentication characters can be identified. These are

$$\begin{array}{lll} ((3*3)*3)*1=4 & ((1*4)*4)*5=3 & ((5*5)*4)*5=3 \\ ((5*3)*3)*4=2 & ((1*5)*2)*2=5 & ((4*5)*3)*1=4 \\ ((2*3)*4)*5=3 & ((2*4)*2)*2=5 & ((1*2)*3)*4=2 \\ ((4*1)*1)*2=4 & ((5*2)*1)*2=4. & \end{array}$$

From the above equations, it can be seen that

$$\begin{array}{llll} 3*3=4*5, & 1*5=2*4, & 1*2=5*3, \\ 4*1=5*2, & 1*4=2*3=5*5, & \end{array}$$

and the pair table

$*$	1	2	3	4	5
1		D		B	C
2			B	C	
3			A		
4	E				A
5		E	D		B

is produced. This completes to the pair table given below.

*	1	2	3	4	5
1	A	D	E	B	C
2	D	A	B	C	E
3	B	C	A	E	D
4	E	B	C	D	A
5	C	E	D	A	B

Assume that another transmission is intercepted with enough information to equate the triples

$(3*3)*2 = (5*1)*3$ $(1*4)*1 = (4*3)*2$ $(2*2)*5 = (3*5)*4$
$(1*4)*5 = (4*1)*3$ $(4*5)*4 = (3*2)*5 = (2*1)*3.$

This information can be used to recover the triple table

*	1	2	3	4	5
A	d	a	b	e	c
B	b	e	c	a	d
C	c	b	a	d	e
D	a	d	e	c	b
E	e	c	d	b	a

which has the structure of the pair table but with rows permuted. If the information from the pair and triple tables is combined, then the quasigroup used to compute the authentication characters can be recovered. This is done by assigning a particular value to A and then checking the feasibility of this assignment. For instance, suppose one takes $A = 5$. Then by comparing the corresponding rows of the pair and triple tables, it may be deduced that $d = C$, $a = E$, $b = D$, $e = A$ and $c = B$. Now trying to determine B, produces

$$B * 1 = b = D = 2 * 1 \Rightarrow B = 2,$$

and

$$B * 5 = d = C = 1 * 5 \Rightarrow B = 1.$$

Thus there is a contradiction and so $A \neq 5$.

Continuing in this manner, it is found that $A = 1$ is the only possibility and the quasigroup

*	1	2	3	4	5
1	1	2	3	4	5
2	2	1	4	5	3
3	4	5	1	3	2
4	3	4	5	2	1
5	5	3	2	1	4

is thus recovered.

In general, the recovery of $(Q, *)$ is dependent on equating pairs and this is dependent on the amount of information an eavesdropper can intercept. Using computer simulation techniques, on a SPARC 10 model 30, which first generated B random blocks and their signature characters, it was possible to recover the quasigroup under the following circumstances.

TABLE 2.1
RECOVERY OF THE QUASIGROUP

Order of Q	Block size	Number of Blocks	CPU time
10	6	1600	less than 2 sec
	7	5000	less than 15 sec
	8	14000	less than 4 min
	9	40000	less than 45 min
	10	130000	less than 13 hr
15	4	1000	less than 1 sec
	5	2000	less than 2 sec
	6	6500	less than 25 sec
	7	22000	less than 8 min
	8	78000	less than 2.5 hr
20	4	1200	less than 2 sec
	5	4400	less than 10 sec
	6	17000	less than 3 min
	7	65000	less than 1.5 hr
	8	280000	less than 36 hr

For fixed order of Q, it can be seen that increasing the block size will increase the number of blocks usually required to recover the quasigroup. The following lemma gives an upper bound on this increase.

Lemma 2.1 *If one can recover the quasigroup given B blocks of size t, then one may recover the quasigroup given qB blocks of size $t+1$.*

Proof. This proof uses the methods described in the attack above. Suppose that B blocks of size t can recover the quasigroup and that qB blocks of size $t+1$ have been intercepted. After carrying out Step 1 of the attack, take the largest class and disregard all other information. Now, if the attack proceeds as described, the execution of Steps 2 and 3 has the same effect as starting again with Step 1 and treating the class of blocks of size $t+1$ as blocks of size t. This follows from the fact that in these steps the appropriate characters are used only for grouping purposes and their actual values are not significant. Treating the information in this manner, there are at least B blocks of size t and under the above assumption these may be used to reconstruct the quasigroup.

Remark. Lemma 2.1 gives an upper bound for the number of blocks needed to recover a quasigroup of order q when the block size is increased from t to $t+1$. However, the empirical evidence given in Table 2.1 suggests that this bound can be improved by a factor of $\sqrt{q}$.

The results indicate that once the block size or the alphabet size increases these techniques will not be enough to recover the entire quasigroup. However, blocks will still coincide in a certain number of positions and under these circumstances an eavesdropper will still be able to forge messages.

In addition, the following points should be noted.

- Dénes and Keedwell also suggested that the order of the quasigroup may be taken to be larger than the size of the alphabet from which the message symbols are chosen. This is certainly feasible and would make it harder to recover the entire quasigroup. However, it would still be possible to forge authentication tags under these circumstances.

- Thus far it has been assumed that the size of the message is divisible by the block size. If this is not the case, then Method 1 would yield a final block of length less than t. It would be unwise to simply take these elements to constitute a block. It is conceivable to have a block of length 2 which would immediately give an eavesdropper the exact value of one of the entries in the quasigroup. In this case the last block should be padded out with some dummy symbols. One way to do this is to take the quasigroup to be of order greater than the size of the alphabet, $\mathcal{A}$, and let $z \in Q \setminus \mathcal{A}$. Then if one has a block

$$a_1\, a_2 \ldots a_k,$$

for some k, then the authentication tag may be calculated by computing the product

$$(\ldots(((\ldots(a_1 * a_2) * \ldots) * a_k) * z) * \ldots) * z = b$$

where $t-k$ occurrences of the symbol z have been joined to the block.

Method 2.

If the latin square is used first to identify all symbols which belong to the same blocks, then the security of the scheme is greatly enhanced. The method of attack suggested above relies on the fact that an eavesdropper can readily identify a block and its corresponding authentication character. From here an eavesdropper can equate blocks and begin to forge signed messages. If one uses the second method to select the blocks, then this information is not available to an eavesdropper. However, it is still theoretically possible to gain information about the quasigroup and hence forge messages.

To present a theoretical attack on this method the following result is proved. Assume that the message is of length q^2 and the block size is taken to be q.

Lemma 2.2 *Let $(Q,*)$ be a quasigroup and let $M_a = a_1\ a_2\ \ldots\ a_{q^2}\ b_{a1}\ldots b_{aq}$ and $M_c = c_1\ c_2\ \ldots\ c_{q^2}\ b_{c1}\ldots b_{cq}$, where $a_i, c_i, b_j \in Q$, be signed messages. Assume that*

the authentication tags have been calculated according to Method 2. If M_a and M_c are such that they coincide in $q^2 - 2$ or $q^2 - 3$ message symbols and at least $q - 1$ authentication characters, then the message symbols which differ must belong to the same block.

Proof. Since $(Q, *)$ is a quasigroup for each $x, y \in Q$ there exists a unique $z \in Q$ such that $x * z = y$. It now follows that if two blocks of length q coincide in $q - 1$ message symbols and the corresponding authentication character, then they must in fact be in the same block. The result now follows.

Corollary 2.1 *If M_a and M_c are such that they differ in at most 3 message symbols and only one authentication character b_i, then the entries in the table of the quasigroup $(Q, *)$ corresponding to these message characters must be i.*

The proof of this corollary follows directly from the description of Method 2.

The attack presented below assumes that a large number of messages have been intercepted. Also it is not necessary to assume that the message size is q^2 or the block size is q. In these cases one selects the blocks using the techniques mentioned earlier. However, for ease of exposition it will be assumed that the message size is q^2 and the block size is q.

ATTACK

Step 1.

Intercept two messages which coincide in $q^2 - 3$ or more message symbols and all but one authentication character. Denote a pair of differing message symbols by a_u and c_u, and denote the differing authentication character by b_{ai} and b_{ci}.

Step 2.

Calculate v and w such that $u = vq + w$. Take an q by q array and label the headline and sideline $1, \ldots, q$. Then place i in cell (v, w) of this array.

Step 3.

Check to see if the array can be completed uniquely to a quasigroup. If so stop as the key has been recovered, otherwise repeat Steps 1 and 2 until the partial array does complete uniquely. This array is the key.

The probability of recovering a message which corresponds to a given message in $q^2 - 3$ or more places is less than

$$\binom{q^2}{3} \frac{1}{q^{q^2-3}} = \frac{q^2(q^2-1)(q^2-2)}{6q^{q^2-3}}.$$

Therefore, one can see that the probability of recovering the entire quasigroup or even forging a message is very small. Hence this method seems to offer a secure method of authentication.

3 Quasigroups and autotopisms

As mentioned earlier for certain quasigroups $(Q, *)$ it is possible to find a quasigroup $(Q, \oplus)$ such that for some t

$$(..((x_1 * x_2) * x_3) * \ldots) * x_t = (..((x_1 \oplus x_2) \oplus x_3) \oplus \ldots) \oplus x_t$$

for all $x_i \in Q$, $1 \leq i \leq t$. That is it is possible to find a class of quasigroups all of which will produce the same authentication characters for a given block size. It is the concurrence of authentication tags for several different quasigroups which is the subject of this section. The theory behind these ideas is now discussed.

In what follows $\imath$ denotes the identity permutation.

Theorem 3.1 *Let $(Q, *)$ be a quasigroup for which there exists an autotopism $(\sigma, \imath, \sigma^k)$, where $k \geq 1$. Denote the order of σ by d. If $d \,|\, (k^{T-1} + k^{T-2} + \cdots + k + 1)$, for some $T > 1$, then there exist at least $d-1$ quasigroups of the form $(Q, \oplus)$ distinct from $(Q, *)$ such that for any $t \equiv 1 (\mathrm{mod}\ T)$ and for any $x_{i1}, \ldots, x_{it} \in Q$*

$$(..((x_{i1} * x_{i2}) * x_{i3}) * \ldots) * x_{it} = (..((x_{i1} \oplus x_{i2}) \oplus x_{i3}) \oplus \ldots) \oplus x_{it}.$$

Proof.

Assume there exists a quasigroup $(Q, *)$ for which $(\sigma, \imath, \sigma^k)$ is an autotopism. Then by definition $\sigma(x) * y = \sigma^k(x * y)$ for all $x, y \in Q$. Notice that if $\sigma^m(x) * y = \sigma^{mk}(x * y)$, then $\sigma^{m+1}(x) * y = \sigma^k(\sigma^m(x) * y) = \sigma^k(\sigma^{mk}(x * y)) = \sigma^{(m+1)k}(x * y)$. So by induction, $\sigma^m(x) * y = \sigma^{mk}(x * y)$, for all $m \geq 1$.

Define a binary operation $\oplus$ as follows, for all $x, y \in Q$, $\quad x \oplus y = \sigma(x * y)$. Then $(Q, \oplus)$ is an isotope of $(Q, *)$.

Consider the equation

$$(..(x_1 \oplus x_2) \oplus \ldots) \oplus x_t = \sigma^{k^{t-2}+\ldots+k+1}[(..(x_1 * x_2) * \ldots) * x_t], \qquad (1)$$

where $x_1, \ldots, x_t \in Q$. By definition Equation (1) holds for $t = 2$. Assume that Equation (1) is true when $t = r$ and consider $r = r + 1$. Then

$$\begin{aligned}
((..(x_1 \oplus x_2) \oplus \ldots) \oplus x_r) \oplus x_{r+1} &= \sigma[((..(x_1 \oplus x_2) \oplus \ldots) \oplus x_r) * x_{r+1}] \\
&= \sigma[\sigma^{k^{r-2}+\ldots+k+1}[(..(x_1 * x_2) * \ldots) * x_r] * x_{r+1}] \\
&= \sigma[\sigma^{(k^{r-2}+\ldots+k+1)k}[((..(x_1 * x_2) * \ldots) * x_r) * x_{r+1}]] \\
&= \sigma^{k^{r-1}+\ldots+k+1}[((..(x_1 * x_2) * \ldots) * x_r) * x_{r+1}].
\end{aligned}$$

So by induction, Equation (1) is true for all $t \geq 2$.

If $t \equiv 1 (\mathrm{mod}\ T)$, then the exponent in Equation (1) can be simplified as follows:

$$\begin{aligned}
k^{t-2} + \ldots + k + 1 &= k^{rT-1} + \cdots + k + 1, \quad \text{for some } r \geq 1 \\
&= (k^{(r-1)T} + \cdots + k^T + 1)(k^{T-1} + \cdots + k + 1).
\end{aligned}$$

By assumption, $d \,|\, (k^{T-1} + \cdots + k + 1)$, so $d \,|\, (k^{t-2} + \cdots + k + 1)$. Therefore, one may deduce that

$$(..(x_1 \oplus x_2) \oplus \ldots) \oplus x_t = (..(x_1 * x_2) * \ldots) * x_t.$$

Now let $\tau = \sigma^m$, for some m. Then for all $x, y \in Q$

$$\tau(x) * y = \sigma^m(x) * y = \sigma^{mk}(x * y) = \tau^k(x * y),$$

and so $(\tau, \imath, \tau^k)$ is also an autotopism on $(Q, *)$. Now define $(Q, \oplus_m)$ by

$$x \oplus_m y = \tau(x * y),$$

and let m range over the values $1, \ldots, d-1$. Then it is easy to see that there exists $d-1$ quasigroups $(Q, \oplus_m)$ distinct from $(Q, *)$ such that

$$(..(x_1 \oplus_m x_2) \oplus_m \ldots) \oplus_m x_t = (..(x_1 * x_2) * \ldots) * x_t,$$

for all $x, y \in Q$ and any $t \equiv 1 (\mathrm{mod}\ T)$.

□

One can explore this theorem by taking the following example. Let $(Q, *)$ be the quasigroup given below. Let σ be the permutation (1324). Take the autotopism $(\sigma, \imath, \sigma)$, where $k = 1$ and choose $T = 4$. Let $(Q, \oplus)$ be the quasigroup (also listed below) such that $x \oplus y = \sigma(x * y)$ for all $x, y \in Q$.

$*$	1	2	3	4
1	1	2	3	4
2	2	1	4	3
3	3	4	2	1
4	4	3	1	2

$\oplus$	1	2	3	4
1	3	4	2	1
2	4	3	1	2
3	2	1	4	3
4	1	2	3	4

Using these quasigroups it can be seen, for example, that the product of the five elements listed below are equal.

$$(((4 * 3) * 2) * 3) * 4 \quad = \quad 2 \quad = \quad (((4 \oplus 3) \oplus 2) \oplus 3) \oplus 4$$

If $(Q, *)$ is a group, then it is easy to find a σ which satisfies the conditions of Theorem 3.1. In fact if $(Q, *)$ is a loop with a left associative element g of order d, then one simplies takes $\sigma(x) = g * x$, $k = 1$ and $T = d$.

In addition it can be shown that if one takes a quasigroup $(Q, *)$ satisfies the given properties then so does any quasigroup which is a direct product of $(Q, *)$ with any other quasigroup.

These examples lead to a discussion of the structure of the permutation σ and the quasigroup $(Q, *)$.

Lemma 3.3 *Let $(Q, *)$ be a quasigroup for which there exists an autotopism $(\sigma, \imath, \sigma^k)$ where $k \geq 1$ and σ is a permutation of order d for some d. Then σ can be expressed as the composition of disjoint cycles of order d.*

Proof.

Consider σ as the composition of disjoint cycles. Take two disjoint cycles σ_A and σ_B of σ. Define $A = \{x \in Q | \sigma_A(x) \neq x\}$ and $B = \{x \in Q | \sigma_B(x) \neq x\}$.

Let $x \in A$ and $y \in B$, and choose w to be the element of Q such that $x * w = y$. Then for any $x' \in A$, $x' = \sigma^m(x)$, for some m. So $x' * w = \sigma^m(x) * w = \sigma^{mk}(x * w) = \sigma^{mk}(y) \in B$. Thus $Aw \subseteq B$, so $|A| = |Aw| \leq |B|$. Similarly, $|B| \leq |A|$. Hence $|A| = |B|$. □

It is immediate that if d is the order of the permutation σ, then $d \mid q$, where $q = |Q|$.

If the square matrix A is a latin square, then a *latin subsquare of order n* of A is an $n \times n$ square submatrix of A which is itself a latin square.

Lemma 3.4 *Let $(Q, *)$ be a quasigroup for which there exists an autotopism $(\sigma, \imath, \sigma^k)$ where $k \geq 1$ and σ is a permutation of order d. Then the latin square corresponding to the multiplication table of $(Q, *)$ can be partitioned into latin subsquares of order d.*

Proof. From Lemma 3.3 it can be shown that $\sigma = \sigma_1\sigma_2 \ldots \sigma_s$ where the order of σ_i is d, for $1 \leq i \leq s$. Define $\Sigma_i = \{x \mid \sigma_i(x) \neq x\}$ so $|\Sigma_i| = d$ and the Σ_i partition Q.

Also define $Y_{ij} = \{y \mid x * y \in \Sigma_j \text{ for some } x \in \Sigma_i\}$ and $\Sigma_i Y_{ij} = \{x * y \mid x \in \Sigma_i, y \in Y_{ij}\}$. Then clearly $\Sigma_j \subseteq \Sigma_i Y_{ij}$.

Suppose $z \in \Sigma_i Y_{ij}$. Then $z = x * y$ for some $x \in \Sigma_i$ and $y \in Y_{ij}$. Now, by definition of the Y_{ij}, there is an $x' \in \Sigma_i$ such that $x' * y \in \Sigma_j$. Also, for some m, $x = \sigma^m(x')$. Thus

$$z = x * y = \sigma^m(x') * y = \sigma^{mk}(x' * y) \in \Sigma_j.$$

Hence $\Sigma_i Y_{ij} \subseteq \Sigma_j$, and it follows that $\Sigma_i Y_{ij} = \Sigma_j$.

Furthermore, since for any fixed $x \in \Sigma_i$ there are d distinct values of y such that $x * y \in \Sigma_j$, we must have $|Y_{ij}| \geq d$. Thus $d \leq |Y_{ij}| \leq |\Sigma_i Y_{ij}| = |\Sigma_j| = d$ and hence $|Y_{ij}| = d$. □

In the next theorem it will be shown that for a given set Q it is always possible to construct a quasigroup $(Q, *)$ which has the desired property.

Theorem 3.2 *For any q, k, T and d such that $k \geq 1$, $T > 1$, $d \mid q$ and $d \mid (k^{T-1} + \cdots + k + 1)$, there exists a quasigroup $(Q, *)$ of order q for which there is an autotopism $(\sigma, \imath, \sigma^k)$ satisfying the conditions of Theorem 3.1 with the given k and T.*

Proof.

The proof is by construction.

Let $Q = \{0, \ldots, q-1\}$, and let σ be a permutation on Q which consists of s disjoint cycles σ_k of order d, for $k = 1, \ldots, s$. For $k = 1, \ldots, s$, let $\Sigma_k = \{x \mid \sigma_k(x) \neq x\}$.

Select subsets Y_{ij} of Q of size d in such a way that the sets in any particular row or column of the array

$$\begin{array}{cccc} Y_{11} & Y_{12} & \cdots & Y_{1s} \\ Y_{21} & Y_{22} & \cdots & Y_{2s} \\ \vdots & \vdots & \ddots & \vdots \\ Y_{s1} & Y_{s2} & \cdots & Y_{ss}, \end{array}$$

form a partition of Q. The rows of this array are used to construct s rows of the quasigroup table of $(Q, *)$. For $i = 1, \ldots, s$, choose $x_i \in \Sigma_i$ and then, for each $j = 1, \ldots, s$ and for each $y \in Y_{ij}$, define $x_i * y$ such that $\{x_i * y \mid y \in Y_{ij}\} = \Sigma_j$. The s rows $x_1, \ldots, x_s$ have thus been constructed. Using the information in these s rows and the fact that $(\sigma, \iota, \sigma^k)$ is to be an autotopism of $(Q, *)$, the remaining rows of the quasigroup can be determined.

Consider determining $x' * y$. Certainly, $x' \in \Sigma_i$ for some i and so $x' = \sigma_i^m(x_i)$ for some known value of m depending on the cycle decomposition of σ. Now to determine $x' * y$ one proceeds as follows $x' * y = \sigma_i^m(x_i) * y = \sigma^{mk}(x_i * y) = \sigma^{mk}(z)$. □

Using the theory developed in this section, one can show that for an arbitrary block of given size it is possible to identify a class of quasigroups any one of which may be used to construct a unique signature character. Consequently this class of quasigroups forms a set of equivalent keys, and this reduces the security of the key.

4 Conclusion

If one considers the original authentication technique suggested by Dénes and Keedwell and the analysis presented in this paper one can make the following conclusions.

When the message is divided into blocks, Method 1 should not be used as it is certainly possible for an eavesdropper to obtain information which will allow him to forge messages and given enough information recover the entire quasigroup. If Method 2 is used then the scheme appears to be secure from the types of attacks presented in this paper. However, one should choose the parameters used in the scheme with care as certain sets of parameters can lead to equivalent classes of quasigroups all of which produce the same authentication tags.

The authors also wish to mention that they have been told that Dénes and Keedwell have made some changes to the scheme. However, the scheme has a patent pending so it has not been possible to obtain these modifications and analyse them.

Acknowledgement This project was supported by a Queensland University of Technology Meritorious Projects Grants Scheme and an Australian Telecommunications and Electronics Research Board Grant. The second author completed this work while being supported by a Queensland University of Technology's Postdoctoral Fellowship scheme.

References

[1] J. Dénes and A.D. Keedwell, Latin Squares and Their Applications, The English Universities Press Ltd, London, 1974.

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

(Received 20/9/94; revised 17/7/95)