М. М. Глухов, О применениях квазигрупп в криптографии,
ПДМ, 2008, номер 2, 28–32

https://www.mathnet.ru/pdm29

МАТЕМАТИЧЕСКИЕ МЕТОДЫ КРИПТОГРАФИИ

УДК 519.7

О ПРИМЕНЕНИЯХ КВАЗИГРУПП В КРИПТОГРАФИИ

М.М. Глухов

Академия криптографии РФ, г. Москва

E-mail: glukhovmm@rambler.ru

Приводится краткий обзор опубликованных результатов по рассматриваемому вопросу, в том числе по применению квазигрупп для построения схем аутентификации, шифрования и однонаправленных функций.

Ключевые слова: *квазигруппа*, *латинский квадрат*, *код аутентификации*, *шифр*, *однонаправленная функция.*

1. Схемы аутентификации

Первые известные нам работы с явным указанием на применение квазигрупп, или латинских квадратов, в криптографии относятся к построению кодов аутентификации, или А-кодов (см. [1, 2 – 7, 13, 14, 24 – 25, 27]). Во всех этих работах обсуждается и модифицируется схема, предложенная в работе [3]. Опишем основную конструкцию этой схемы по работе [7]. В ней в качестве сообщений рассматриваются слова длины, кратной m, в q-ичном алфавите Q, а в качестве подписи к сообщению s длины mt – слово $a_1 \ldots a_m$ длины m в том же алфавите, образованное следующим образом. Слово s разбивается по некоторому правилу на t слов $s^{(1)}, \ldots, s^{(t)}$ длины m, и по слову $s^{(i)}$ вырабатывается буква a_i с помощью квазигруппы $(Q, *)$, которая является ключом. А именно, если $s^{(i)} = s_1 \ldots s_m$, то буква a_i находится по формуле

$$a_i = (\ldots((s_1 * s_2) * s_3) * \ldots) * s_m.$$

Пользуясь лишь определением квазигруппы, легко показать, что произведение $(\ldots((s_1 * s_2) * s_3) * \ldots) * s_m$ принимает в качестве значений каждый элемент из Q одно и то же число раз. Отсюда следует, что при равномерном распределении вероятностей на множестве сообщений построенный А-код имеет минимальную вероятность успешной имитации, равную $1/q^m$. Особо рассматривается практически наиболее интересный, двоичный, случай, когда $q = 2^k$. Приводится естественная модификация схемы в случае, когда длина сообщений не кратна m. Исследуется также вариант, в котором алфавит подписи имеет большую мощность по сравнению с алфавитом сообщений.

В [4] анализируется возможность восстановления сообщения или ключевой квазигруппы в указанной схеме по ряду сообщений с определенными совпадениями букв в сообщениях и подписях. Рассматриваются два метода. В первом из них слова $s^{(1)}, \ldots, s^{(t)}$ являются отрезками слова-сообщения s, во втором – предполагается, что сообщение имеет длину q^2, t полагается равным q, а слова $s^{(1)}, \ldots, s^{(t)}$ образуются с использованием сообщения s и квазигруппы $(Q, *)$. Указываются условия, при которых в первом случае возможно восстановление открытого текста и даже ключевой квазигруппы. Схема второго типа является более стойкой к рассмотренной атаке.

В работе [4] рассматривается также вопрос об эквивалентности ключей, который сводится к рассмотрению определенных автотопий квазигруппы $(Q, *)$.

В [1] описанная выше схема аутентификации претерпевает дальнейшее усложнение с точки зрения образования слов $s^{(1)}, \ldots, s^{(t)}$. В ней рассматривается лишь случай, когда порядок q алфавита есть степень двойки, $t = q^2$, сообщение s имеет длину q^2 и представляется в виде квадратной матрицы M порядка q. По ключевой квазигруппе $(Q, *)$ строится система из $q/2$ попарно ортогональных квазигрупп, изотопных квазигруппе $(Q, *)$. С использованием матрицы M и таблиц Кэли имеющихся $(q/2)+1$ квазигрупп и строится последовательность слов $s^{(1)}, \ldots, s^{(t)}$. Авторы высказывают гипотезу, что построенная ими схема в некотором смысле является оптимальной.

2. Шифры

Более общий подход к использованию квазигрупп для шифрования был предложен в работах [14, 19]. В [14] вводится так называемое квзигрупповое преобразование множества Q^+ всех конечных наборов букв конечного алфавита Q (Quasigroup String Processing). Оно определяется следующим образом. Сначала по заданной квазигруппе $(Q, *)$ и любому ее элементу (лидеру) a определяется преобразование $E_a^{(1)}$ множества Q^+:

$$E_a^{(1)}(x_1, \ldots, x_k) = (y_1, \ldots, y_k), \tag{1}$$

где $y_1 = a * x_1$, $y_{i+1} = y_i * x_{i+1}$, $i = 1, \ldots, k–1$. Затем берется композиция n таких преобразований, соответствующих квазигруппам $(Q, *_i)$ и выбранным лидерам a_i, $i = 1, \ldots, n$. Итоговое преобразование обозначается в виде $E^{(n)}_{a_n,\ldots,a_1}$. Преобразование $E_a^{(1)}$ обратимо, и обратное к нему преобразование $D_a^{(1)}$ определяется следующим образом:

$$D_a^{(1)}(x_1, \ldots, x_k) = (y_1, \ldots, y_k),$$

где $y_1 = a \setminus x_1$, $y_{i+1} = x_i \setminus x_{i+1}$, $i = 1, \ldots, k–1$. Отсюда легко находится обратное преобразование и для $E^{(n)}_{a_n,\ldots,a_1}$. Оно обозначается в виде $D^{(n)}_{a_1,\ldots,a_n}$. Предлагается использовать преобразование $E^{(n)}_{a_n,\ldots,a_1}$ для шифрования информации. При этом в качестве ключей предлагается использовать операции $*_i$.

В работах [14, 19] изучаются свойства соответственно преобразований $E^{(n)}_{a_n,\ldots,a_1}$ и $D^{(n)}_{a_n,\ldots,a_1}$ и делается вывод о том, что указанные преобразования обладают некоторыми нужными для криптографии качествами. В частности, при любых фиксированных $(Q, *_i)$, a_i, c_i, $i = 1, \ldots, n$, уравнение

$$E^{(n)}_{a_n,\ldots,a_1}(x_1, \ldots, x_k) = (c_1, \ldots, c_k) \tag{2}$$

имеет единственное решение относительно неизвестных $x_1, \ldots, x_k$; по соотношению (2) при известных $a_1, \ldots, a_k, x_1, \ldots, x_k, c_1, \ldots, c_k$ для нахождения ключей $(*_i)$ необходимо произвести столько проб, сколько существует наборов из $n–1$ квазигрупповых операций; выходные последовательности обладают хорошими статистическими свойствами, а именно: при любом заданном вероятностном распределении букв во входных последовательностях предельные распределения s-грамм в выходных последовательностях длины k являются равномерными при $k \to \infty$ и $s \le n$.

В ряде работ квазигрупповые преобразования слов используются для построения поточных шифров, криптографическая стойкость которых основана на сложности решения таких задач, как факторизация целых чисел или дискретное логарифмирование в конечных полях. Рассмотрим один из таких шифров, предлагаемый и анализируемый в работе [16]. Он получается путем комбинирования шифра типа Эль-Гамаля и поточного квазигруппового шифра. Приведем его подробное описание.

Шифр типа Эль-Гамаля хорошо известен. В качестве поточного квазигруппового шифра берется шифр в алфавите $Q = \mathbf{Z}_p^*$ с функциями шифрования $E^{(n)}_{a_n,\ldots,a_1}$ и расшифрования $D^{(n)}_{a_1,\ldots,a_n}$ из [14, 19], которые обозначаются здесь в виде E_α и E_α^{-1} при $\alpha = (a_1, \ldots, a_n)$. Предполагается, что они определены для случая, когда все квазигруппы $(Q, *_i)$ совпадают с одной и той же квазигруппой $(Q, *)$.

В [16] указывается также и способ получения квазигрупповой операции $*$ на Q. Она определяется следующим образом. Для произвольного $K \in \{1, \ldots, p–2\}$ задается отображение f_K: $Q \to Q$ по формуле

$$f_K(j) = (1/(1 + (K + j)(\mathrm{mod}\ p–1)))(\mathrm{mod}\ p)$$

и полагается

$$i * j = i \cdot f_K(j)(\mathrm{mod}\ p).$$

Нетрудно проверить, что отображение f_K является подстановкой, а группоид $(Q, *)$ – квазигруппой с левой обратной операцией

$$i \setminus j = ((i \cdot j^{-1}(\mathrm{mod}\ p)) – 1 – K)(\mathrm{mod}\ p–1)$$

при условии, что вместо 0 берется $p–1$.

Предлагаемый алгоритм имеет две части. В нем установление связи, выработка и передача ключей осуществляется с помощью шифра Эль-Гамаля, а шифрование исходного открытого сообщения и его расшифрование – с помощью квазигруппового шифра. В итоге получается существенный выигрыш в скорости по сравнению с известными асимметричными шифрами.

Проблема стойкости для первой части шифра решается точно так же, как для шифра Эль-Гамаля. Поэтому автор анализирует стойкость лишь второй части шифра, а именно: рассматривается задача нахождения числа K, определяющего квазигруппу $(Q, *)$, и лидеров $a_i \in Q$, $i = 1, \ldots, k$, по открытому тексту и соответствующему ему шифртексту. Показано, что эта задача сводится к решению системы полиномиальных уравнений над полем $\mathbf{Z}_p$ при большом простом числе p. Вид такой системы зависит от числа k используемых лидеров. При $k = 1$ и $k = 2$ получаются соответственно системы уравнений 2-й и 3-й степеней, и они могут быть эффективно решены. При $k > 2$ получаются системы уравнений более высоких степеней. В общем случае эта задача является NP-трудной. В рассматриваемом случае возникающие системы уравнений имеют определенную специфику, и задача их решения остается открытой.

Отметим еще, что в рассматриваемой работе для получения квазигрупповой операции, или, что то же самое, латинского квадрата, на $\mathbf{Z}_p^*$ указывается на способ, предложенный в [22].

В работе [22] предлагается использовать квазигруппы для построения преобразований типа «Все или ничего» («All-Or-Nothing Transformation», сокращенно AONT). Такие преобразования введены в 1997 г. Р. Райвестом с целью повышения стойкости блочных шифров с постоянной длиной блоков к методам, использующим свойства открытого текста.

Преобразование T последовательности сообщений (блоков) $m = (m_1, \ldots, m_s)$ в последовательность $m' = (m_1', \ldots, m_t')$, $t \geq s$, является *преобразованием типа AONT*, если T обратимо, T и T^{-1} эффективно вычислимы (т.е. вычислимы за полиномиальное время) и невозможно получение какой-либо информации о любом блоке m_i, если неизвестен хотя бы один блок m_j'.

В качестве AONT Райвест предложил так называемое *пакетное преобразование*, которое может быть описано следующим образом.

Дана входная последовательность сообщений $m = (m_1, \ldots, m_s)$, в которой m_i – отрезок из b бит, $i = 1, \ldots, s$.

1. Выбираем случайно ключ K для пакетного преобразования в блочном шифре.
2. Вычисляем последовательность $m' = (m_1', \ldots, m_{s+1}')$ по правилу

$$m_i' = m_i \oplus E_K(i),\ i = 1, \ldots, s;\ m_{s+1}' = K \oplus h_1 \oplus \ldots \oplus h_s,\ h_i = E_{K'}(m_i' \oplus i),\ i = 1, \ldots, s,$$

где K' – фиксированный открытый ключ, а E_K – функция зашифрования рассматриваемого блочного шифра при реальном ключе K.

Легко видеть, что пакетное преобразование обратимо, т.е. по m' однозначно находятся K и m. При этом если хотя бы один из блоков m_i' неизвестен, то невозможно вычислить K, а потому и любой блок m_i.

В отличие от сообщения m последовательность m' называют *псевдосообщением*. Предполагается, что далее псевдосообщение шифруется обычным образом. Таким образом, пакетное преобразование является предварительным преобразованием открытого сообщения. Оно не уменьшает криптографическую стойкость основного шифра и в то же время не позволяет найти исходное открытое сообщение при любом неполном дешифровании псевдосообщения. В последующие годы преобразования такого типа и их использование в криптографии рассматривались и обсуждались многими авторами (см., например, [2, 22, 26, 27]).

Следует иметь в виду, что методы шифрования с использованием AONT имеют и недостатки, а именно: AONT размножают ошибки и отрицательно влияют на скорость шифрования. По сути дела в схеме Райвеста пакетное преобразование требует не меньше времени, чем последующее шифрование псевдосообщения. Для борьбы с первым недостатком предлагается использовать корректирующие коды и хорошие каналы связи. Для уменьшения второго недостатка в работе [22] предлагается использовать новый способ построения псевдосообщения, основанный на комбинировании AONT и квазигруппового шифрования. С этой целью авторы предлагают следующий способ быстрого получения квазигрупп (латинских квадратов) порядка $n = p-1$, где p – простое число. В работе рассматривается случай $n = 256$, $p = 257$, и квазигруппа строится на множестве $Q = \{1, \ldots, 256\}$.

Сначала выбирается случайная перестановка $(a_{11}, \ldots, a_{1n})$ чисел из Q, которая принимается за первую строку латинского квадрата и таблицы Кэли нужной квазигруппы, затем строятся остальные строки по правилу

$$a_{ij} = i \cdot a_{1j} (\mathrm{mod}\, p),\ i = 2, \ldots, n;\ j = 1, \ldots, n.$$

Очевидно, что в итоге получится латинский квадрат и таблица Кэли квазигруппы $(Q, *)$.

Далее по сообщению $u = (u_1 \ldots u_k)$, где u_i – байты, являющиеся двоичными записями чисел из Q с условием, что 256 представляется байтом нулей, строится псевдосообщение $v = (v_1 \ldots v_k)$ следующим образом. Случайно выбирается произвольный элемент $a_1 \in Q$, называемый лидером, и полагается

$$v_1 = a_1 * u_1,\ v_{i+1} = v_i * u_{i+1},\ i = 2, \ldots, k.$$

После этого полученное псевдосообщение расширяется путем добавления перед ним лидера a_1 и первой строки квазигруппы. Далее расширенное псевдосообщение шифруется обычным образом.

Из построения расширенного псевдосообщения видно, что по нему однозначно восстанавливается исходное открытое сообщение. При этом используется левая обратная операция для операции $*$. Кроме того, видно также, что описанное предварительное преобразование открытого текста является преобразованием типа «Все или ничего».

3. Однонаправленные функции

Вернемся к вопросу об использовании квзигрупповых преобразований. В работе [29] предлагается использовать квазигрупповые преобразования для построения однонаправленных функций и подстановок. С этой целью автор выбирает квазигруппу $(Q, *)$ и определяет два преобразования

$$R_i : Q^N \to Q^N,\ i = 1, 2,$$

с использованием введенного ранее преобразования $e_a = E_a$ (см. (1)). А именно, для набора $A = (a_0, \ldots, a_{N-1})$ определяются:

$$R_1(A) = e_{a_{N-1}}(\ldots(e_{a_1}(e_{a_0}(A)))\ldots),$$

$$R_2(A) = e_{a_{N-1}}(...(e_{a_1}(e_{a_0}(R_1(A))))...) .$$

Автор доказывает, что если исходная квазигруппа не коммутативна и не ассоциативна, то для нахождения прообраза в преобразованиях R_1, R_2 при использовании лишь таблицы Кэли квазигруппы Q понадобится соответственно $O(q^{[N/2]})$ и $O(q^N)$ квазигрупповых операций. Исходя из этого, автор считает введенные функции серьезными кандидатами в однонаправленные функции. Преобразование R_2 используются также для построения других, более сложных, кандидатов в однонаправленные функции.

В работе [9] предлагается и исследуется вариант построения сжимающих хэш-функций итеративного типа с использованием в боксах так называемых мультиподстановок на множестве E^2, где

$$E = F_2^m = \{e_0, e_1, \ldots, e_t\},\ t = 2^k-1,$$

F_2 – поле из двух элементов. Предлагаемые функции, обозначаемые автором в виде $g_{k,s}$, являются равновероятными отображениями 2^t-й степени множества E в его 2^{t-1}-ю степень.

Функция $g_{k,s}$ определяется с использованием $2^{k-1}(s + 1)$ боксов $B_{i,j}$, $i = 0, 1, \ldots, 2^{k-1}-1$, $j = 0, 1, \ldots, s$, объединенных определенным образом в сеть, состоящую из s +1 ярусов по 2^{k-1} боксов в каждом ярусе. В ярус с номером j входят боксы $B_{i,j}$ со значениями

$$i = i_0 + 2i_1 + \ldots + 2^{k-1}i_{k-1} \text{ при } i_{\mathrm{j}} = 0.$$

Боксы $B_{i,0}$ – входные, боксы $B_{i,s}$ – выходные. Каждый бокс осуществляет подстановку на множестве E^2.

Множество E разбивается на два подмножества H и M, где $H = \{e_i\colon i_0 = 0\}$ – множество хэш-входов, $M = \{e_i\colon i_0 = 1\}$ – множество входов-сообщений. На вход бокса $B_{i,j}$ подаются элементы $e_i \in H$ и $e_{i(j)} \in M$, отличающиеся лишь цифрами j-х разрядов. Предполагается, что на выходе блока $B_{i,j}$ получается также пара из $H \times M$, компоненты которой поступают соответственно на блоки $B_{i,j+1}$ и $B_{i(j),j+1}$. В итоге все входы-сообщения (а также и все хэш-входы) будут сниматься на каждом ярусе с разных блоков.

Далее, путем итерации преобразования $g_{k,s}$ авторы определяют искомую хэш-функцию $h_{k,s}$ следующим образом. Сообщение M в битах дополняется некоторым образом до числа бит, кратного $m2^{k-1}$, и представляется в виде $M = M_1M_2 \ldots M_n$, где M_i – набор длины $m2^{k-1}$. Теперь фиксируется начальное значение хэш-входа H_0 и вычисляются

$$H_i = g_{k,s}(H_{i-1}, M_i),\ i = 1, \ldots, n,$$

и в качестве значения хэш-функции $h_{k,s}$ (M) берется H_n.

В [8] исследуются свойства построенных таким образом хэш-функций в случае, когда в качестве боксов $B_{i,j}$ используются так называемые мультиподстановки множества E^2.

Под *мультиподстановкой* авторы понимают биективное отображение $B\colon E^2 \to E^2$, при котором $B(a, b) = (B_1(a, b), B_2(a, b))$ и функции B_1, B_2 являются подстановочными по каждому переменному. Это равносильно тому, что функции $B_1(a, b)$, $B_2(a, b)$ задают ортогональные квазигруппы на множестве E. В этом случае авторы указывают алгоритмы решения уравнения

$$h(H, M) = H'$$

относительно M при известных H, H' и нахождения коллизий. Находят верхние оценки сложности и выражают надежду, что эти оценки близки к нижним.

Для построения пар ортогональных квазигрупп авторы рекомендуют использовать ортоморфизмы групп. В частности, доказана теорема о том, что отображение $L_c\colon E^2 \to E^2$, при котором

$$L_c(a, b) = (a \oplus b, a \oplus bc \oplus R^n(b)),$$

где R – сдвиг вектора на 1 бит вправо, является мультиподстановкой тогда и только тогда, когда для любого $i \in \{1, \ldots, m\}$ среди векторов $R^{mt}(c)$, $t = 1, 2, \ldots, m$, найдутся векторы с различными i-ми координатами.

ЛИТЕРАТУРА

1. *Bakhtiari S*, *Safavi-Naini R.*, *Pieprzyk J.* A message Authentication Code based on Latin Squaresc // Proc. Australasian on Information Security and Privacy. 1997. P. 194 – 203.
2. *Canda V.*, *van Trung T.* A New Mode of Using All-Or-Nothing Transforms // Codes and Cryptography. 2001. P. 1 – 6.
3. *Carter S*, *Wegman M.N.* Universal Class of Hash Function // J. Computer and System Sciences. 1979. V. 18. No. 2. P. 143 – 154.
4. *Dawson E.*, *Donovan D*, *Offer A.* Quasigrops, isotopism and authentication schemes // The Australasian journal of combinatorics. 1996. V. 13. P. 75 – 88.
5. *Denes J.*, *Keedwell A.D.* Latin Squares. New Developments in the Theory and Applications. Amsterdam: Nord-Holland Publishing Co., 1981.
6. *Denes J.*, *Petroczki P.* A digital encrypting communication systems // Hungarian Patent. 1990. No. 201437A.
7. *Denes J.*, *Keedwell A.D.* A new Authentication Scheme based in Latin Squares // Discrete Mathematics. 1992. V. 106/107. P. 157 – 162.
8. *Vandenay S.* On the Need for Multipermutations: Cryptoanalysis of MD4 and SAFER // Proc. Fast Software Encryption. 1994. P. 286 – 297.

9. *Schnorr C.P.*, *Vandenay S.* Black box cryptoanalysis of hash networks based on multipermutations // Lecture Notes in Computer Science. 1995. V. 950. P. 47 – 57.
10. *Koscielny C. A* metod of constructing quasigroup-based stream-ciphers // Appl. Math. and Comp. Sci. 1996. V. 6. P. 109 – 121.
11. *Krawczyk H.* LFSR-based and Authentication // 1994, EUROCRYPT-94. P. 129 – 139.
12. *Krawczyk H.* New Hash Function for Message Authentication // 1995, EUROCRYPT-95. P. 301 – 310
13. *Markovski S.*, *Gligoroski D.*, *Andova S*. Using quasigroups for one-one secure encoding //Proc. VIII Conf. Logic and Comp. Sci. “LIRA 97”, Novi Sad, 1997. P. 157 – 162.
14. *Markovski S.*, *Gligoroski D.*, *Bakeva V.* Quasigroup String Processing: Part 1 // Proc. of Maked. Academ. of Sci. and Arts for Math. And Tech. Sci. XX. 1 – 2. 1999. P. 13 – 28.
15. *Denes J. and Owens P.J.* Some new latin power sets not based on groups // J. Combin. Theory, ser A. 1999. V. 85. P. 69 – 82.
16. *Gligoroski D.* Stream cipher based on quasigroup string transformation in $\mathbf{Z}_p^*$ // Universitet “St. Cyril and Methodious”, Faculty of Natural Sciences, Institute of Informatics, P.O. Box 162, Scopje, Republic of Macedonia. ArXiv:cs.CR/0403043 v2 22Apr 2004. gligoroski@yahoo.com
17. *Gligoroski D.*, *Markovski S.*, *Bakeva V*. Quasigroup and Hash Functions // Discr. Math. And Appl. Proc. of the 6th ICDMA, Bansko. 2001. P. 43 – 50.
18. *Gligoroski D.*, *Markovski S.*, *Bakeva V.* On infinite Class of strongly Collision Resistant Hash Functions “EDON-F” with Variable Length of Output // Proc. 1st International Conference on Mathematics and Informatics for Industry. Thessaloniki, Greece, 2003.
19. *Markovski S.*, *Kusacatov V.* Quasigroup String Processing: Part 2 // Proc. of Maked. Academ. of Sci. and Arts for Math. and Tech. Sci. XXI, 1 – 2. 2000. P. 15 – 32.
20. *Markovski S.*, *Gligoroski D.*, *Stojcevska B*. Secure two-way on-line communication by using quasigroup enciphering with almost public key // Novi Sad J. Mathematics. 2000. P. 30.
21. *Markovski S.* Quasigroup String Processing and Application in Cryptography // Invited talk. Proc. 1st International Conference on Mathematics and Informatics for Industry. Thessaloniki, Greece, 2003.
22. *Marnas S.I.*, *Angelis L.*, *Bleris G.L*. All-Or-Nothing Transform using quasigroups // Proc. 1st Balkan Conference in Informatics. 2003. P. 183 – 191.
23. *Rogaway P*. Bucket Hashing and its Application to Fast Message // 1995, CRYPTO-95. P. 30 – 42.
24. *Shoup V.* On Fast and Provably Sequre Message Authentication based on Universal Hashing // 1996, CRYPTO-96. P. 313 – 338.
25. *Stinson D.R.* Universal Hashing and Authentication Codes. Design // Codes and Cryptography. 1994. V. 4. P. 369 – 380.
26. *Stinson D.R.* Something about All-Or-Nothing (Transform). Design // Codes and Cryptography. 2001. P. 133 – 138.
27. *Taylor R.* Near optimal Unconditionally Sequre Authentication // 1994, EUROCRYPT-94. P. 245 – 255.
28. *Wegman M.N.*, *Carter S.* New Hash Functions and their Use in Authentication and Set Equality // J. Computer and System Sciences. 1981. V. 22. P. 265 – 279.
29. *Gligoroski D.* Candidate One-Way Functions and One-Way Permutations Based on Quasigroup String Transformations // 2005, gligoroski@yahoo.com