HCG Test Tools with GCD totient Graphics

User Manual

V1.02E_20130711

1. To start

This User Manual has made for using 'HCG Test Tools' smoothly, and has a purpose for generalizing the Hyper Curve Group for Cryptography and Mathematics. 'HCG Test Tools with GCD totient Graphics' is a software, available for the cryptosystem design, the signature design, and the primary tests without difficulties of a mathematical complex, and can easily make an original design with the determination of curve parameters, modulus p, and the group characteristics of HCG.

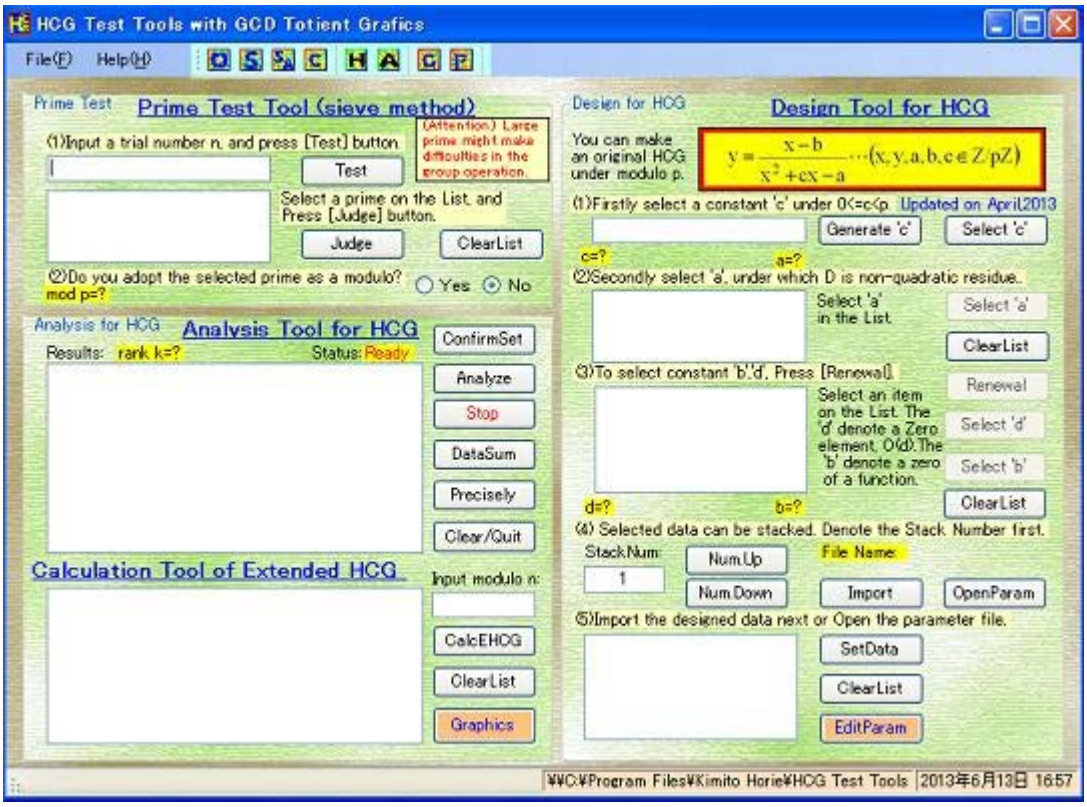
This software is also convenient for the tool of Mathematics, spatially for testing conformities of the theory of HCG. Your download of this software is available on the download WEB-site in free; this means you need not pay any fees to use this software.

http://www.din.or.jp~horie

Please remind this software is made only for an academic use, not for a professional designer use. So, the bits numbers of a modulus p, keys, so on, can not select bigger as you would expect.

2. Summary of 'HCG Test Tools with GCD totient Graphics'

This software consists of the few tools for the HCG , and each tool is very useful in a stand alone. And this is a second version manual of the 'HCG Test Tools, having strong graphical tools for the GCD totient and HCG characteristics.



(1) Prime Test Tool (Upper Left)

'Prime Test Tool' is normally used for determining a modulus p, as a prime. The modulus X(composition) is not treated here. This tool can test the trial number n, whether n is a prime or a composition for using a so-called sieve method.

[Usage] Input a trial number n, and press the button [TEST]. The result will be displayed on the List as a Prime Factor Decomposition of an Integer.

For example, if n=541, then represented as

[n=541^1

541 is a prime.].

This tool also has a function of determining a selected prime whether it is a Sophie-Germann prime, or not.

[Usage] Click the line (Ex.[541 is a prime.) in that List, and press the button [Judge]. Such action result the expression in the List, like [p=541 is Germann prime.

q=271 is also prime!]

If you want to adopt the selected trial number as a modulus, press the radio button [Yes].

Then the adoption is confirmed, like as [Modulus p=541 is adopted.](Yellow).

[Attention] If you select a large number as a modulus, the group operation on HCG will dissipate enormous time to complete it, that means you will be at fault. Please select a modulus p<65536(16bits), for your convenience.

(2) Design Tool for HCG (Right)

'Design Tool for HCG' can design the curve parameters of HCG with the modulus p. You can make the curve parameters (a, b, c) on the integer function

$$y = \frac{x-b}{x^2+cx-a} \cdots (x, y, a, b, c \in Z/pZ)$$

under this tool.

Firstly these parameters must satisfy the condition using Jacobi's symbol

$$\left(\frac{D}{p}\right) = -1$$

, where D is a discriminant of an order 2, and have a relation with the parameters, as $D = c^2 + 4a$.

Secondary, a group condition must be satisfied as

$$\left(\frac{x^2 + cx - a}{p}\right) = -1$$

for the parameters, a and c, and also the parameters b, d must be determined in terms of x.

The group under these conditions named 'a quadratic-hyperbolic curve group', which is consisted of the element P(x)s on the modulus p and the group operation [+]. The whole group definition with modulus n is expressed as

$$G_n = \left\{ P(x) \mid \left(\frac{x^2 + cx - a}{p_i}\right) = -1 \text{ for } \forall i, \text{on } Z/nZ, n = \prod_i p_i^{ei}, [+] \right\}$$

,for which has been studied in recent years and be resulted in.

Above conditions are adopted to limit Gn for making a quadratic-hyperbolic curve group to use this software. A quadratic-hyperbolic curve group is now known as a kind of 'Logarithmic Group'.

① Firstly, we select the parameter c, which has an optional in its selection. You can select the parameter c within a range of 0<c<p at leisure.

[Usage] Input trial number c, then press the button [Select 'c'].

That action will result in like [parameter c=* is adopted](Yellow) on the List, and also display few candidates of a parameter a on the next List under the discriminant

D.

② Next, we select the parameter a from the candidates, expressed on the List, as a result of the operation ①

[Usage] Click the one of candidates of a parameter a on the List, and press the button [Select 'a'].

Then, that List show you a message, like [parameter a=* is adopted](Yellow). If you want to select another candidates, then press the button [Select 'a'] again. So, the new candidates appear in place of the first candidates on the List.

③Next, we select the parameter b and d from the candidates, expressed on the List. The parameter b and d are the integer point of the HCG, and must satisfy the condition

$$\left(\frac{x^2+cx-a}{p}\right)=-1$$

in terms of x.

We must select the parameter b and d as a different point on the above condition. And also we can select the valuable x from that List, to determine the base point P(x).

[Usage] Click the one of candidates of a parameter 'b' or 'd' as displayed on the List, and press the button [Select 'b'] or [Select 'd'].The result show you on the List, like

[parameter b=* is selected](yellow) or [parameter d=* is selected](Yellow).

④Determined Parameters can be conserved in a temporally memory for future operations. Max set of that conservation is 20' s.

[Usage] Firstly select the data number and press the button [Import], then the set of the parameters on that data number is conserved on the temporal memory. Before that operation, be sure to confirm the contents just expressed on the Lists. If you want to change the memory place conserved, Please press the button [NumUP] or [NumDown].

Another way of transportation on the memory is opening the data file, like 'DataHCG_01.hcp', which will recover ascend parameters on this software, and express its file name on the front panel.

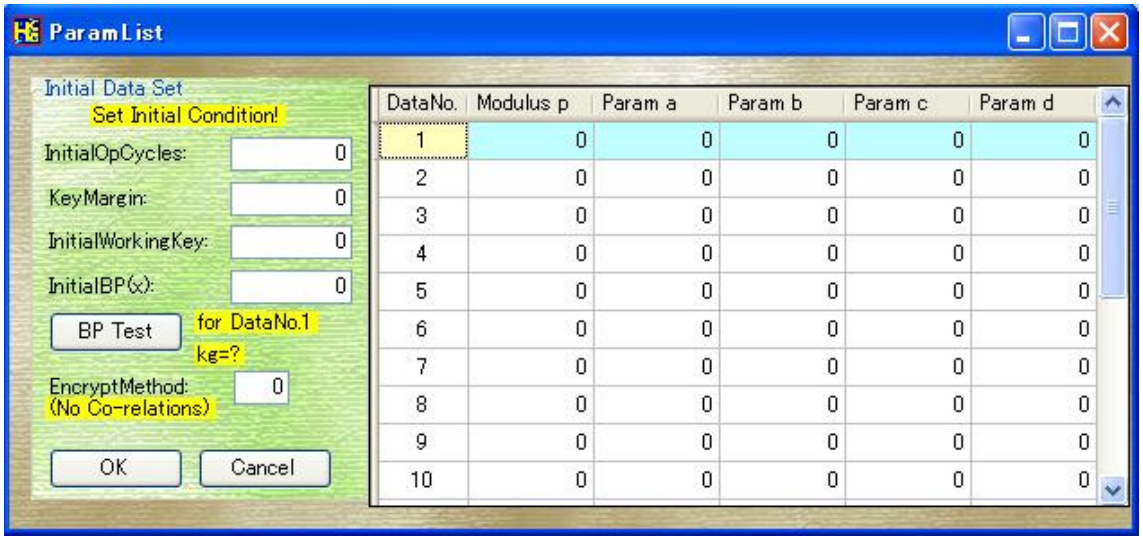
⑤Determine the set of HCG parameters, which is used on the group operations.

[Usage] Firstly select the data number and express the set of HCG parameters on the

List and Press the button [SetData] to use this set. This set is used on the group operations by the next tool for a HCG analytics.

⑥ This software contain its editor to edit directly the parameters, which you want to change its values appropriately according to the rules of HCG.

Please press the brown button [EditParam], then the next graphics with an Excel-base will appear.



This edit tool has 9 context-menu which appears by clicking mouse right button.

[ClearRowData] will clear that all row data to be 0.

[ResoreRowData] will recover the row data, which were exist before cleaning.

[DeleteSelectedRow] will delete the selected row data, and the rest of the data later will follow just after that row.

[CopySelectedRow] will copy the selected row data to the inner memory.

[PasteSelectedRow] will paste the data to the selected row from the inner memory.

[InsertNewRow] will add a new row at the position of the selected row. Then all row data will shift one to the bottom from that row, and last low will disappear.

[RecreateAllData] will create an appropriate set of parameters, on which the group condition are satisfied according to its Modulus p on the List. So, you must select a modulus p at first.

⑦ Other parameters, like ' InitialOpCycles' ,' KeyMargin' , 'InitialWorkingKey' ,' InotialBP' and 'EncryptionMethod' are related to the encryption applications with HCG, and have no relation to the HCG design itself.

(2)Analytic Tool for HCG(Left Middle)

'Analytic Tool for HCG' is supplied for confirming the structure of HCG with the

set of parameters just made on the Design Tool for HCG

① Firstly reconfirm your selection of the modulus p and parameters which will be used on the Analytic Tool for HCG. This operation is prepared for your convenience.

[Usage] Press the button [Confirm], then a modulus p and parameters which will be used on the Analytic Tool for HCG are expressed on the List. If the modulus p or parameters does not coincide with that you expected, please press the button [SetData] again to prepare another set of parameters after changing the data number.

②Finally we execute the analyzing of that HCG. This might have enormous time to complete, if you choose a large number as the modulus p. Do'nt miss it!

[Usage] Press the button [Analyze], then the result will be expressed on the List within an appropriate time. For example, like

「Q(2); kg=1;
Q(3); kg=271;
Q(6); kg=271;---」

, that result will be appeared. In this List, Q(x) is a sub-group of HCG in which you select the base point P(x), and kg is a rank of its sub-group. On these group operations with the adaptation of a possible base point, the all result are expressed serially on the List. This means the total number of the possible base point P(x) is equal to its rank of HCG. Be attention to remember, the element of Q(x) like mP(x) may not be a candidate of the base point in place of P(x) in this sub-group Q(x).

③This stage is to put the resultant data in order.

[Usage] Press the button [DataSum], so the data in the List are estimated and listed again. This function is very convenient, and you need not to count it. For example, the List show you like,

[The numbers of the sub-group of a rank kg=271 is 270.
The numbers of the sub-group of a rank kg=1 is 1.].

In the world of HCG, the rank k does not depend on
its curve parameters directly, and is constant k=(p+1)/2.
And the numbers of the sub-group Q(x) with kg is exactly G(kg).
You can confirm these truths on your calculations.

④ Adding this, we can also confirm the data of the sub-group Q(x) precisely

[Usage] Firstly select the one line of the sub-group Q(x) on the List, then press

the button [Precisely]. This operation results the precise data of the whole sub-group Q(x) with a rank of kg on the List. For example, the List show you like,

「The numbers of the sub-group of a rank kg=271 is 270.

Q(3);

Q(6);

Q(14);

---」

⑤ Furthermore, we can also confirm a one of the sub-group Q(x) precisely

[Usage] Firstly select the one line of the sub-group Q(x) on the List, then press the button [Precisely] again. This operation results the precise data of a one of the sub-group Q(x) with a rank of kg on the List. For example, the List show you like,

「The sub-group Q(6) consists of

1P=(6,434)

2P=(300,127)

3P=(508,227)

4P=(68,55)

5P=(14,411)---」

In this case, 1P means the base point P(x) itself, and the rank means itself as kgP=O. This List show you the whole results of kg times group operation, and each data is equivalent to the elements of a HCG, that is mP(x) on each, and the value of x is a point of the selected quadratic-hyperbolic curve.

⑥During the group operations, if you want to confirm its process on time, then you make it by [Stop](Red) button, which is next to the button [Analyze].

[Usage] Pushing the button [Stop] during the group operations, then the calculations are stopped, and the button name is changed to [Resume]. Furthermore, the process' s percentage at that moment is expressed on the Status, upper part of the List. So you can confirm the processes how going on. This is also useful for confirming the process is proceeding and not to be frozen. And if you want to resume the group operations again, please push the button [Resume]. Then the button changes its name to [Stop] and suspended task works again. If you wan to quit the operations or to clear the List, then press [Clear/Quit] button as you like.

(3) Calculation Tools of Extended HCG (Left Down)

On an Extended HCG, we know that the numbers of the sub-group Q(x) with a rank kg under a modulus X is G(kg), which is called 'the extended Euler' s function' (or I named it as '**GCD totient**'). But the extended Euler' s function is a new integer

function discovered in 2005, not so clear in precise, yet only few theories were proved till now. We must establish a calculation method for a future tool of Integer Theory. The extended Euler's function G(n) (= '**GCD totient**') is presented as

$$G(X)=\sum_{d|kq}\mu(d)\prod_{i}^{m}GCD\left(k_i,\left(\frac{X}{d}\right)\right)$$ or simply $$G(X)=\sum_{d|kq}\mu(d)\prod_{i}^{m}\left(k_i,\left(\frac{X}{d}\right)\right)$$

, with $X=p_1^{e1}p_2^{e2}\cdots p_m^{em}$ and $k_i=p^{ei\text{-}1}\left(\frac{p_i+1}{2}\right)$ And $\mu(d)$ is Mebius function.

GCD Totient $G(k_g)$ on mod X:

$$G(k_g)=\sum_{d|kg}\mu(d)\prod_{i}^{m}\left(k_i,\frac{k_g}{d}\right)$$

$$X=p_1^{e1}\cdots p_m^{em},p_i^{ei}\rightarrow k_i,$$

$$k_g\,|\,k_q,k_q=LCM[k_1,,,k_m];$$

This tool gives you many information about the EHCG on checking, for example, the expression of the EHCG with the form of a sum as the order of the dividend of kg in compared with the Euler's function ϕ, EHCG theory calculations, presentations of the GCD set, and the modulus n, which give us a same value or its multiples.

[Usage] Firstly input a modulus n, and press the button [CalcEHCG], then the List show you the whole calculation results, with the numbers of the sub-group Q(x) with a rank kg ,which is equal to G(kg). For example, this List is expressed as below:

[1]Basics EHCG modulus: n=34=2^1*17^1; $\omega(n)=2$;

GruopRank: k=9=1*9;

Max rank of sub-groups: kq=9;

[2]SubGroups The number of Q(x) with kg is total G(kg). G(X):= GCD totient.

$\phi(9)=6$; G(9)=6; Ratio=1; G(9):=+9*1-3*1;

$\phi(3)=2$; G(3)=2; Ratio=1; G(3):=+3*1-1*1;

$\phi(1)=1$; G(1)=1; Ratio=1; G(1):=+1*1;

[3]Theories kq=$\Sigma\,\phi(d)$=9; k=ΣG(d)=9=1*kq;

$\Sigma(-1)^{(kq/d)}\cdot G(d):=-6-2-1=-9$(kq:odd);

[4]Presentation of the GCD Set

Dim1: h(1)=1; h(2)=9;

Dim2: h(12)=1;

[5]GCD totientG(x) with modulus N

$\phi(34)=16$

G(34) mod(): No modulus_N found!

G(34) mod(): No modulus_N found!

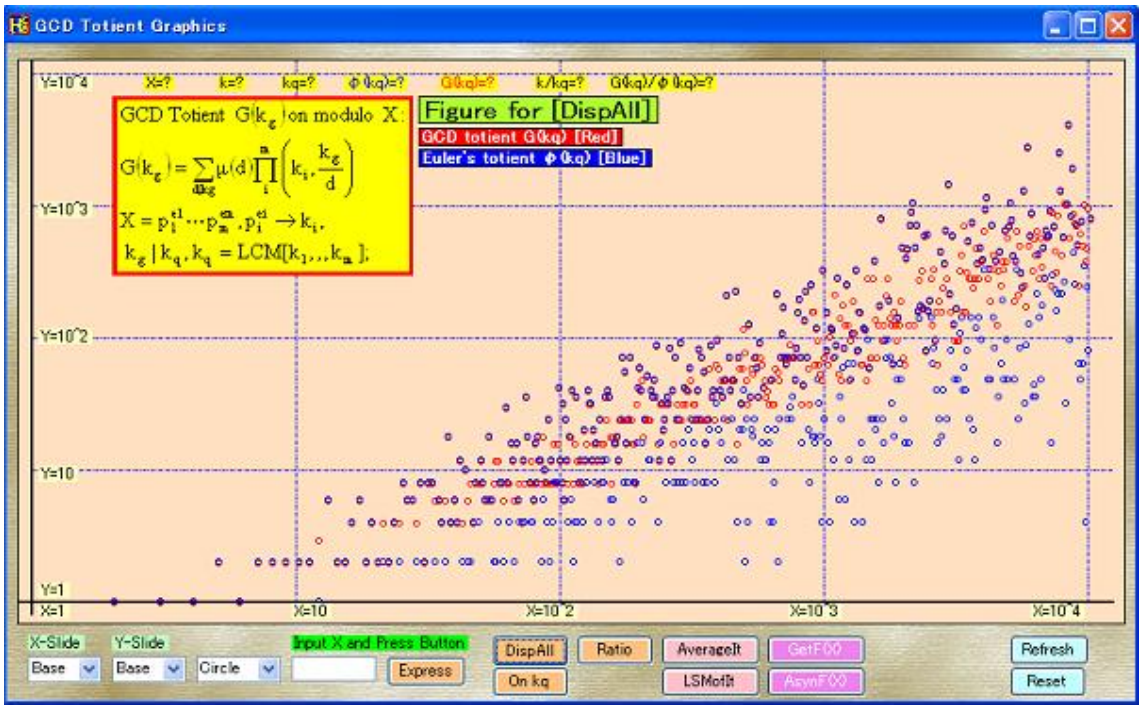
In this List, you can find the EHCG function to be expressed as the sum of integer factors, like 「G(9):=+9*1-3*1;」 as ordered with the dividend of kg. And also find the theory of EHCG, 「Σ(-1)^(kq/d)G(d|kq)」 is calculated and confirmed to be divided by the kq in any case. The GCD Set shows the structure of the k as the geometrical figure of the ki's in terms of the prime number product of each ki, which is the sub-group's total elements number(=order), and generated from the prime pi.

EHCG function is the multi-value integer one, and has several different 'modulus' for a one value. So using a new original method of finding a modulus n, this list express the modulus n's with the same value found by this method, only in the case of successfully having found it.

(4) Graphics Tool for the Extended HCG (Left Down)

This version of 'HCG Test Tools' has a strong graphical tool for the GCD characteristics, spatially for GCD totient. The brown button [Graphics] give you the graphical tool for the Extended HCG by pressing it. That Graphics is expressed as follows:

Yellow frame with a red line shows GCD totient definitions in brief. And the title of the graph is expressed on upper region. Other parameters expressed on the top are EHCG characteristics, which has a unique value depends on the X-axis.



[Usage]

①If you press the button [DispAll], then the calculated pictures appeared with the

red tiny circles of the extended Euler's function G(kq), though the blue tiny circles are the Euler's function ϕ(kq), on the common logarithmic axis of X and Y.
In this case, kq=LCM(k) is a max value of the rank of the sub-group Q(x).
② You can make an axis slide view of the graphics appropriate times by directly changing the values of 'X-Slide', or 'Y-Slide'. And the expressions are also modified by using 'Cross' or 'Line'.
③ If you click [On kq] button, X-coordinate is changed from the n-based to the kq-based.
④ On this Graphics, if you click on any place along with X-axis, then X-value of this place is displayed with EHCG characteristics on the top. Those are X-value, k-value, kq-value, ϕ(kq)-value, G(kq)-value, ratio k/kq and ratio G(kq)/ ϕ(kq). If you select X-value input on the text box, and push [Express] button, then the same shape markers with different color appears on the graphs, simultaneously the top EHCG characteristics change its values.
[Ratio] button displays the ratio G(kq)/ ϕ(kq) as red tiny circles, and k/kq as blue tiny circles, though theoretically these are equal or bigger than 1.
Other buttons are the tools of an assistant:
[AvarageIt] button displays the average curve of the data.
[LSMofIt] button displays the least square mean curves of the data.
[GetF(X)] button displays the linier which pass though two points that are made from clicking a mouse on the common logarithmic axis.
⑤ [Ratio] button displays the ratio of the k/kq and the ratio G(kq)/ ϕ(kq) with the kq value. Using rough hypothesis and the geometric mean, we know

$$\overline{\left(\frac{k}{k_q}\right)} \to \frac{\log(n)}{\log\log(n)} = \omega(n) : (n \to \infty)$$

when n going infinite.
[AsyncF(X)] button is for asymptotic functions of the EHCG characteristics, that are calculated counting on GCD theories with some hypothesis. This is only available for the Ratio for the time being.
⑥ We also give a convenient function, on which a mouse click on the graphics can give the values of kq, G(kq), and ϕ(kq) with a modulus X.
⑦[Reset] button makes this tool be initialized.
⑧[Close] button makes this tool be terminated.

(5)System Menu

This tool can conserve parameters of HCG, and etc. made by itself as a file.

①[File]>[Open] menu

[Open] menu has a function to open the file and read parameters of HCG, and etc. Such parameter file has an extension [.hcp] on default. This file consists of a text file basically. you can make it originally by yourself. Try to open [data_Hcg_01.hcp] file, the parameters of HCG, and etc. can restore again on its data numbers.

②[File]>[Save] menu

[Save] menu has a function to save the file with the parameters of HCG, and etc. If the same name of the file exists on the System, the new data will overwrite its contents after confirmation of paying attentions.

③[File]>[Save As] menu

[Save As] menu has a function to save the file with the parameters of HCG, and etc. with a new file name. If the same name of the file exists on the System, the new data will overwrite its contents after confirmation of paying attentions.

④[File]>[Close] menu

[Close] menu makes this file be terminated.

⑤[Help]>[How to use] menu

[How to use] menu will guide you to operate this tool to read and refer this manual.

⑥[Help]>[About] menu

[About] menu discloses the version of this manual and will link you to my private WEB site, the Room of HCG, made by myself.

(6)System Context Menu

This tool has another function to use a context menu by clicking right on a mouse.

①[Copy] context menu

[Copy] context menu copies the selected items to the Clip Board. So you can take it, when you want to use it externally.

②[Paste] context menu

[Paste] context menu paste the contained text on the Clip Board to the designated List. So you can take it, when you want to add something from the external.

③[Select All] context menu

[Select All] context menu can select all lines on the designated List. It is very convenient, when the List data is enormous.

This English Manual was made on 14 Jun, 2013.
Version: V1.02E_20130614 and revised later.
End.