1.1 Special functions

The following functions are constant expressions and defined inside the compiler:

Name	Description
$unit(***z***)	a value $(1+s)_N^{-1}$ calculated from ***z*** which can be used to increment and decrement ***z***
$X(***z***)	construct value given X representation of ***z*** (default is TS)
$peekrnd()	give the current random value without advancing it
$random()	give the current random value and advance it
$B2()	B_2
$beta()	β
$fkf()	$(\varphi k)_N^{-1} \varphi \bmod N\varphi$
$enc(*m*)	Encrypt value *m*

1.2 Usage

CEAL accepts the command line options shown in the table below.

Name	Description
-	input/output using stdin/stdout
-o file	specify output file ('stdout' for console output)
-p pragma	pragma string; overrides cryptoleq.pgm and input
-s	show compiler parameters and exit
-t nnn	show Tree at different stages (0 to 8), e.g. 0237
-r seed	random seed: either number or word 'time'
-E	preprocess only, no parse or evaluate; make output after Tokenizer's job
-x	execute; default for .sce files
-e	translate only; default for .sct files
-a	translate and execute; default for .sca files
-I	add include path, see also 1.3
-b ascii	set space separator; default ' ' for io=ts, '\n' for io=x
-c n f	run crypter; n=(xenc|xdec|tsenc|tsdec) f=(file|@num)
-d file	collect statistics, slower; file is input and output

'-c' crypter is a helper function to encrypt and decrypt numbers from the command line or stored in files. The prefix 'ts' or 'x' specifies the format of the values.
Example: `$ ceal -p "PQ=7.11 r=17 k=5" -c tsdec @1.71`
Outputs: `16`.

'-d' options initiates collection of statistics. File is both input (may exist or not) and output; input is optional – if it does not exists, it will be created. The format of the file is the following:

```
IP watch list { _G_start _omul_start _seq_start _smul_start }

IP pass counters
================
_G_start[2656604]   = 612
_omul_start[1704679]= 0
_seq_start[4938295] = 6
_smul_start[3664180]= 6

Instruction stat
================
Input/Output   = 8
Open           = 108342
Secure         = 55691
Mixed          = 35929
---------------
Total          = 199970
```

IP watch list is a list of labels (if alphanumeric) or addresses (if numeric) which are being passed by IP. From the example above (PIR 204) we can see that G function was called 612 times; open multiplication has never been executed; secure equal operation and secure multiplication was executed 6 times each (6 entries in the Database). Square brackets show X-value addresses of the corresponding labels. The addresses have to be specified explicitly in the *IP watch list* if emulation is run separately without compilation. The next section in the example shows the instruction count.

1.3 Include

Include directive has the format: *.include func "file"*. Function *func* is optional and can be one of "asis" (default) or "datax". The later convers values from X representation.

A file is searched first in the current directory. If it is not found, then the list of include directories (specified by command line option '-I' and pragma option 'incdir') is used in the order as directories added to the list. If file is not found in any directory, error is issued. When the file is found, the search ends.

A special directive is *.pragma once*, which instructs the include algorithm to include the current file only once in the program. For example, if A includes B and C, and B includes C, and file C has "pragma once" directive, then file C will be included only the first time.

1.4 Pragma

Pragma is a set of environment variables for Compiler and Processor objects. It can be specified in three places:

1. 'cryptoleq.pgm' file
2. Pragma directive in the program
3. Command line option

Each pragma specification is overridden in the above order – so a variable set in the command line overrides the one set in the program or pragma file. Pragma parameters are defined in format *name=value*.

List of pragma parameters

Name	Description
N	Value N
P	First prime of N
Q	Second prime of N
u	Minimal beta value the program requires. This does not affect the program except that the check may fail if N is selected so beta is not big enough.
k	k value
r	Seed for the random engine
entry	Entry address, default is 0
beta	beta parameter
PQ	Same as P and Q but in format X.Y
io	One of (ascii|a|ts|x). Format for input/output
sctype	One of (ts|x). Format of cryptoleq code
id	Informational parameter – name
ver	Informational parameter – version
incdir	Same as the command line option –I