The crypto* package

Mark Wooding

16 September 2001

Contents

1 User guide

1.1 Algorithm typesetting

A lot of provable-security papers need to be able to typeset algorithms describing adversaries, schemes, oracle behaviour, etc. There is a (relatively) standard format for doing this which we support.

`program` The program environment provides handy notation for describing algorithms formally. It gives a tabbing environment, so that things can be laid out nicely, and allows fragments of algorithms to be laid out in columns or rows, with separating rules.

`\next` Within the program environment, the `\next` command stops typesetting the current column, typesets a vertical separator rule, and starts a new column. Adjacent columns are spaced out evenly across the page, with equal space around the rules rules and at the current margins. This means that the rules don't line up, but it still seems to provide a pleasing effect.

`\newline` The `\newline` macro begins a new row of algorithm typesetting. A page break is possible at a `\newline`.

`\kw` A number of standard keywords are available, as shown in table 1. The typsetting of these is done by the `\kw` command, which usually sets its argument in text bold face, but can be redefined. The standard definition uses `\xspace` so that you don't need to remember to say `\␣` after a keyword command.

`\ind` Within a program environment, the `\ind` command shunts the indent level 1 em to the right.

`\gets` `\getsr` `\inr` Assignment can be represented using the standard command `\gets`, which typesets a left-pointing arrow '←'. Random sampling – the selection of a random

*The crypto package is currently at version 1.0, dated 16 September 2001.

Command	Keyword
\RETURN	**return**
\IF	**if**
\THEN	**then**
\ELSE	**else**
\REPEAT	**repeat**
\WHILE	**while**
\UNTIL	**until**
\FOREVER	**forever**
\DO	**do**
\FOR	**for**
\FOREACH	**for each**
\FROM	**from**
\IN	**in**
\TO	**to**
\ABORT	**abort**
\PARSE	**parse**
\NEW	**new**
\AS	**as**

Table 1: Keywords available for algorithm typesetting

element from a set or probability distribution – can be represented using the new command `\getsr`, which typesets an arrow with a little 'R' above it '$\xleftarrow{R}$'. Random membership – showing that something is a random variable with some distribution – can be represented using the `\inr` command, which just typesets an $\in$ sign with a subscript 'R': '$\in_R$'.

Should one wish, one can use a different character than 'R' to denote randomness. Some authors use '$', for example. I know of one (cheapskate?) author who has used '$\not\in$'. Redefining the `\random` command lets you do this. For example, you can say `\newcommand{\random}{\$}` should you so wish.

`\id` Long identifiers can be typeset using the `\id` command. giving the identifier name as an argument. The `\id` command is only valid in maths mode. As currently set up, `\id` sets its argument in *text* italics; this seems to look better in documents which use a PostScript body face and Computer Modern for maths.

`\Xid` It's handy to be able to glue a bit of (possibly fancy) maths typesetting to an identifier, e.g., to construct H'*-list*, or $\mathcal{E}$*-CTR*^{F}. This is done using `\Xid{`⟨*maths*⟩`}{`⟨*text*⟩`}`. The two bits are joined by a text hyphen '-'.

`\cookie` Sometimes textual names are used for special 'symbols', which have meaning to algorithms, e.g., the symbols find and guess in the standard indistinguishability game. These can be typeset using the `\cookie` command.

1.2 Other stuff

`\Thing` In the quantifiable-security world, there are standard symbols for advantage,

success probability, insecurity, etc. The generic 'style hook' for these is `\Thing{`⟨*name*⟩`}{`⟨*notion*⟩`}{scheme}`, which typesets $\mathbf{name}^{\mathrm{notion}}_{scheme}$. It helps a lot if you have the amstext package loaded.

`\Succ` `\Adv` `\InSec` `\Expt` `\Game` `\G`

Some standard '`things`' are provided: `\Succ{`⟨*notion*⟩`}{`⟨*scheme*⟩`}`, `\Adv{`⟨*notion*⟩`}{`⟨*scheme*⟩`}`, `\InSec{`⟨*notion*⟩`}`, `\Expt{`⟨*notion*⟩`}{`⟨*scheme*⟩`}`, and `\Game{`⟨*notion*⟩`}{`⟨*scheme*⟩`}`.

In proofs which proceed by varying the rules of the game played by the adversary and bounding the probability of it noticing at each step, game names are usually typeset as $\mathbf{G}_n$ for small numbers n. The command `\G{`⟨n⟩`}` command does this typesetting. There's an optional argument, which is a symbol to write instead of 'G'.

`\Func` `\Perm`

When dealing with finite PRFs and PRPs, we need to talk about the set of *all* functions (or permutations) over particular sets, usually n-vectors of bits. The macros `\Func{`⟨l⟩`}{`⟨L⟩`}` and `\Perm{`⟨L⟩`}` typeset $\mathcal{F}^{l,L}$ and $\mathcal{P}^{L}$ respectively, and are intended to denote the sets of all functions $F\colon \{0,1\}^l \to \{0,1\}^L$ and all permutations $\Pi\colon \{0,1\}^L \to \{0,1\}^L$ respectively.

`\PKCS`

Finally, the `\PKCS` macro typesets 'PKCS#n', allowing you to name RSA Security Inc.'s Public Key Cryptography Standards in a relatively nice way.

2 Implementation

We need David Carlisle's handy xspace package and the AMS `\text` command.

```
⟨*package⟩
\RequirePackage{amstext}
\RequirePackage{xspace}
```

2.1 Algorithm typsetting

`\cookie` `\kw` `\id`

First, some style issues. Note the `\xspace` at the end of `\kw`.

```
\def\cookie#1{\text{\normalfont\sffamily\/#1\/}}
\def\kw#1{\text{\normalfont\bfseries\/#1\/}\xspace}
\def\id#1{\text{\normalfont\itshape\/#1\/}}
```

`\getsr` `\inr`

The symbols for random selection and membership are fairly easy. The 'R' over $\xleftarrow{R}$ is actually in scriptscript style, because that seems to look nicer.

```
\providecommand\random{R}
\def\inr{\mathrel{\in_{\random}}}
\def\getsr{\mathrel{\mathop{\gets}\limits^{\scriptscriptstyle\random}}}
```

`\Xid`

The compound identifiers set by `\Xid` are easy.

```
\def\Xid#1#2{\id{$#1$-#2}}
```

Now for the various keywords. These are trivial, but useful.

```
\def\RETURN{\kw{return}}
\def\IF{\kw{if}}
\def\THEN{\kw{then}}
\def\ELSE{\kw{else}}
\def\REPEAT{\kw{repeat}}
\def\WHILE{\kw{while}}
```

```
\def\UNTIL{\kw{until}}
\def\FOREVER{\kw{forever}}
\def\DO{\kw{do}}
\def\FOR{\kw{for}}
\def\FOREACH{\kw{for\,each}}
\def\FROM{\kw{from}}
\def\IN{\kw{in}}
\def\TO{\kw{to}}
\def\ABORT{\kw{abort}}
\def\PARSE{\kw{parse}}
\def\AS{\kw{as}}
\def\NEW{\ifmmode\mathop{\kw{new}}\else\kw{new}\fi}
\def\SEND{\kw{send}}
\def\OUTPUT{\kw{output}}
\def\STOP{\kw{stop}}
```

program
\next
\newline
\ind

Now for the program environment and its associated twiddling. This is actually a little fiddly.

At the beginning, if we're in vertical mode – i.e., there was a paragraph break before the start of the environment – then remember this, because it affects the typesetting at the end. Set up `\next` and `\newline` in terms of the underlying machinery, and start a row of algorithm.

```
\def\program{%
  \normalfont%
  \@tempswatrue\ifvmode\@tempswafalse\fi%
  \def\next{\program@end\vrule\program@begin}%
  \def\newline{\program@endline\medskip\program@startline}%
  \def\ind{\quad\=\+\kill}%
  \ifdim\topsep<\parskip\topsep\parskip\fi%
  \ifdim\@topsepadd<\z@\@topsepadd\z@\fi%
  \begingroup\trivlist%
  \advance\@topsep-\parskip\advance\@topsepadd-\parskip\item%
  \program@startline%
}
```

Ending the environment is easy-ish. We stop the current row and leave a gap, matching the one that `\poem@startline` adds automatically. If we were initially in horizontal mode, then don't indent the next paragraph, and ignore spaces after the `\end{program}` command.

```
\def\endprogram{%
  \program@endline\endtrivlist\endgroup%
  \if@tempswa\@endparenv\fi\@ignoretrue%
}
```

Now for the guts of all of this. First of all, we turn to the typesetting of a column, which is just hfil glue, a minipage with zero width and a tabbing environment. The first tab is already set 1 em in from the margin. We use minipage to set up the list parameters correctly and manage the initial and final spacing. The zero width is OK because tabbing sets a list of hboxes rather than using outer horizontal mode, so the `\hsize` is irrelevant.

```
\def\program@begin{%
  \begingroup%
  \hfil%
```

```
  \minipage[t]\z@%
    \topsep\z@%
    \itemsep\z@%
    \parskip\z@\parsep\z@%
    \partopsep\z@%
    \tabbing%
```

This is rather messy. The `\item` from the trivlist messes up the spacing. We remove the box, and fix `\prevdepth` to ensure that there's no glue at the top.

```
      \quad\=dummy\\%
      \@stopfield%
      \begingroup%
        \setbox\z@\lastbox\unskip\unskip\unskip\setbox\z@\lastbox\unskip%
      \endgroup%
      \prevdepth-\@m\p@%
      \@startfield\strut\ignorespaces%
}
```

Ending a program has no discernable subtlety.

```
\def\program@end{%
    \endtabbing%
  \endminipage%
  \hfil%
  \endgroup%
}
```

Finally, the row setting is fairly easy. We have to ensure that we obey the prevailing list parameters.

```
\def\program@startline{%
  \moveright\@totalleftmargin%
  \hb@xt@\linewidth\bgroup%
    \program@begin%
}
\def\program@endline{%
    \program@end%
  \egroup%
}
```

2.2 Other stuff

`\Thing` Typesetting `\Thing` is easy. This acts as a style hook for the rest of these things.

```
\def\Thing#1#2#3{\text{\normalfont\bfseries#1}^{\text{\normalfont#2}}_{#3}}
```

`\Succ` `\Adv` `\InSec` `\Expt` `\Game` And now here they are.

```
\def\Succ{\Thing{Succ}}
\def\Adv{\Thing{Adv}}
\def\InSec#1{\Thing{InSec}{#1}{}}
\def\Expt{\Thing{Expt}}
\def\Game{\Thing{Game}}
```

`\G` The name of a game is typeset simply as

```
\newcommand\G[2][G]{\mathbf{#1}_{#2}}
```

\Func The finite sets of functions and permutations are just a style choice. We choose
\Perm to buck the standard trends and use caligraphic letters.

```
\def\Func#1#2{\mathcal{F}^{#1,#2}}
\def\Perm#1{\mathcal{P}^{#1}}
```

\PKCS Finally, I find that PKCS #n looks best typeset like this:

```
\def\PKCS#1{PKCS\,\##1}
```

That's all there is. Byebye.

⟨/package⟩

Mark Wooding, 16 September 2001

Appendix

A The GNU General Public License

The following is the text of the GNU General Public License, under the terms of which this software is distributed.

GNU GENERAL PUBLIC LICENSE
Version 2, June 1991

51 Franklin Street, Fifth Floor, Boston, MA 02110-1301, USA

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software—to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

Terms and Conditions For Copying, Distribution and Modification

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

   Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

   You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such

modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

(a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

(b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

(c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

(a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

(b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of

Sections 1 and 2 above on a medium customarily used for software interchange; or,

(c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as

a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

   Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

No Warranty

11. Because the program is licensed free of charge, there is no warranty for the program, to the extent permitted by applicable

LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

Appendix: How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

> one line to give the program's name and a brief idea of what it does.
> Copyright (C) yyyy name of author
>
> This program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 2 of the License, or (at your option) any later version.
>
> This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.
>
> You should have received a copy of the GNU General Public License along with this program; if not, write to the Free Software Foundation, Inc., 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301, USA.

Also add information on how to contact you by electronic and paper mail.

If the program is interactive, make it output a short notice like this when it starts in an interactive mode:

> Gnomovision version 69, Copyright (C) yyyy name of author
> Gnomovision comes with ABSOLUTELY NO WARRANTY; for details type 'show w'.
> This is free software, and you are welcome to redistribute it under certain conditions; type 'show c' for details.

The hypothetical commands `show w` and `show c` should show the appropriate parts of the General Public License. Of course, the commands you use may be called something other than `show w` and `show c`; they could even be mouse-clicks or menu items—whatever suits your program.

You should also get your employer (if you work as a programmer) or your school, if any, to sign a "copyright disclaimer" for the program, if necessary. Here is a sample; alter the names:

> Yoyodyne, Inc., hereby disclaims all copyright interest in the program 'Gnomovision' (which makes passes at compilers) written by James Hacker.
>
> signature of Ty Coon, 1 April 1989
> Ty Coon, President of Vice

This General Public License does not permit incorporating your program into proprietary programs. If your program is a subroutine library, you may consider it more useful to permit linking proprietary applications with the library. If this is what you want to do, use the GNU Library General Public License instead of this License.

Index

Numbers written in italic refer to the page where the corresponding entry is described; numbers underlined refer to the code line of the definition; numbers in roman refer to the code lines where the entry is used.