

! "#\$%&\$&%' (") * + , ' - . / ' 0 1 + ' 2 . 3 4 '
5 6 6 1 + 7 * & \$ 7 \$ " # ' 8 & , ' 3 9 8 : : " & % " #

!"



!"##' \$%&'%' (

!"#\$%&'" (") * + , - . & / 0 # (! 1

!"#\$% "'& \$ () *) # \$ + , & - # . / &) 0

1 2 3 * & 4 5 \$ 6 * , 7 * 8 9 / # : ' " & ' 2 /) *) # : # 7 ;

")) 6 5 < < = = : 9 / # : ' " & ' 2 /) *) # : # 7 ; < > 6 * , 7 *

31; 6*7\$&% a b

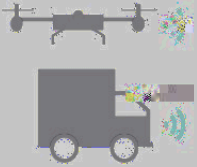
d cad

a

698#"#4

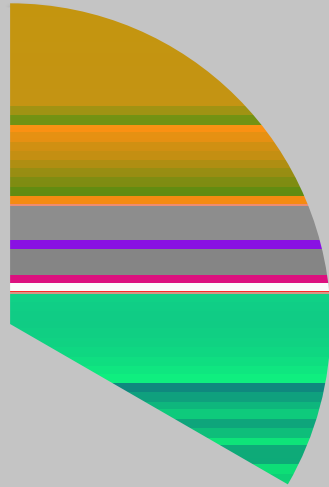


13#.?&, ?\$@' 36;)&, ?\$@' ,)&, ; ; 3



A*)*\$B' -#3#,)\$*, 7\$@' ,).' 4





-. / " 0 % 1 2 " * * + # 3 + 4 %

! " # \$ % " & ' " () * + \$ + , * - % " - + , * \$. + / 0 ') % 1 \$ 2 " ' \$ % 3 + . + \$
+ 4 + ' 5) , 5 \$ 6 & & 7) / 6 %) " , . \$ " , \$ / " 4 & 0 % , 5 \$ / " , % , 0 0 4 \$ #) % 3 \$
! 8 9 \$. 1 . % + 4 . . :

52.++%+7+*,%/8%9+:; .<=\$%9;))/.=4%

B* , \$87\$)* , +>)05&'83

Q" ; +>)05&'83

! "#+>)05&'83

A>1%?7+.7<+@



NIST Special Publication 800

NIST SP 800-122

Lowell Wofford
Rickey Gregg
Gary Key
Antwan Clark

Catherine Hinton
Andrew Prout
Albert Reuther
Ryan Adams

John W. Carr
Kunushadham H. Madhoo
Jeffrey D. Williams
Salim A. Elmaghrabi

This publication is available free of charge from:

NATIONAL INSTITUTE OF
STANDARDS AND TECHNOLOGY

NIST



>.+,+#="=</#%?7+.7<+@



?7+.7<+@%/8%#2+%| KD>|1A%>./L+: =

. 3456&#*7897: ;<, *&9=* <1>9?7, *&" #\$\$@4A7; 7B&

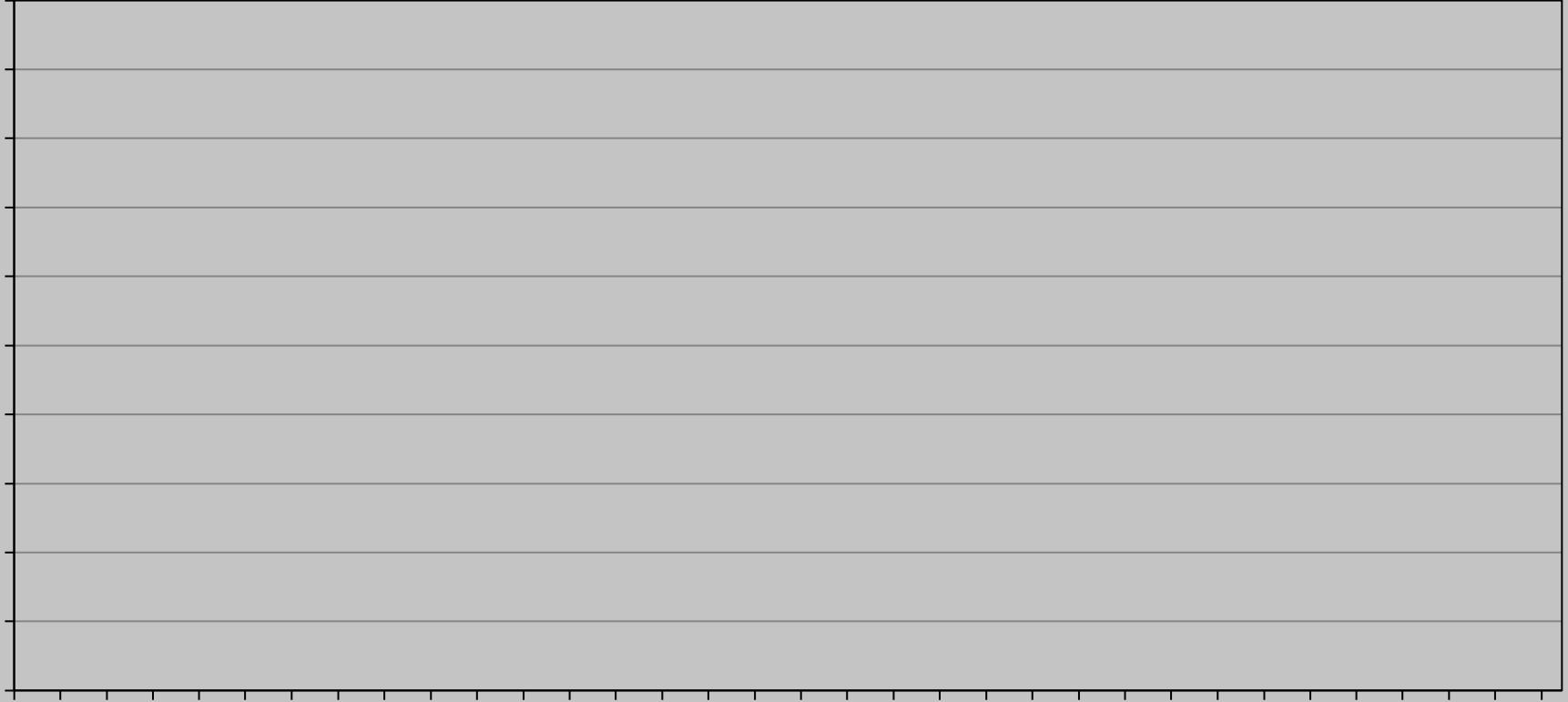
.)?==97+&897&: ?C+4=C*%&<+*7, 9<<* , +>

.)?==97+&897&: ?C+4=C*%&C; +897: >

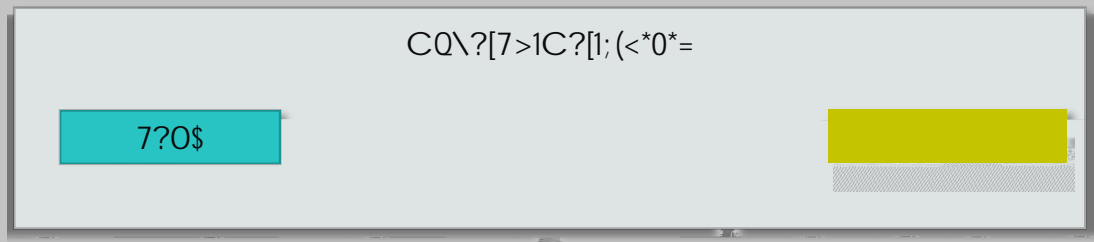
.)?==97+>&+6*%&; +* >+&" #1D-E&+; <F; 7F

. (FF4+49<; C&9=+4: 4G*F&H*7>49<>&897&F488*7* <+&>B>+*: >|* <H479<: * <+>J

! " # \$ % & ' () *



! >I%! KD>I1AGFO.<7+#%1 /#7+.3+0%9/8=@".+%9=":0%8/.%
A>1P%DIP%-<3%N"="P%"#0%N"="%9:<+#: +



19: ; %* (<&) => ?@ (%* >) > AA (A%*) & :) > = 9?: % / & B (A\$

/ (\$\$>: (%*>\$9?: %?C (<>@(
D / * " E

* 50F
DG * # H% J (? F1 / K / H% # O L H% G * # M M E

1NO)9B%77% / * "% M% P
D / * "% M% * 50F% M% J (? / * + # 9A Q E

+4' 3), %&* " & @ 2# (%) 2# 6) 8 (2? 2A?%)! " @ @ > # 4 (274" #) = > # 74 @ %

10#, -. (9:

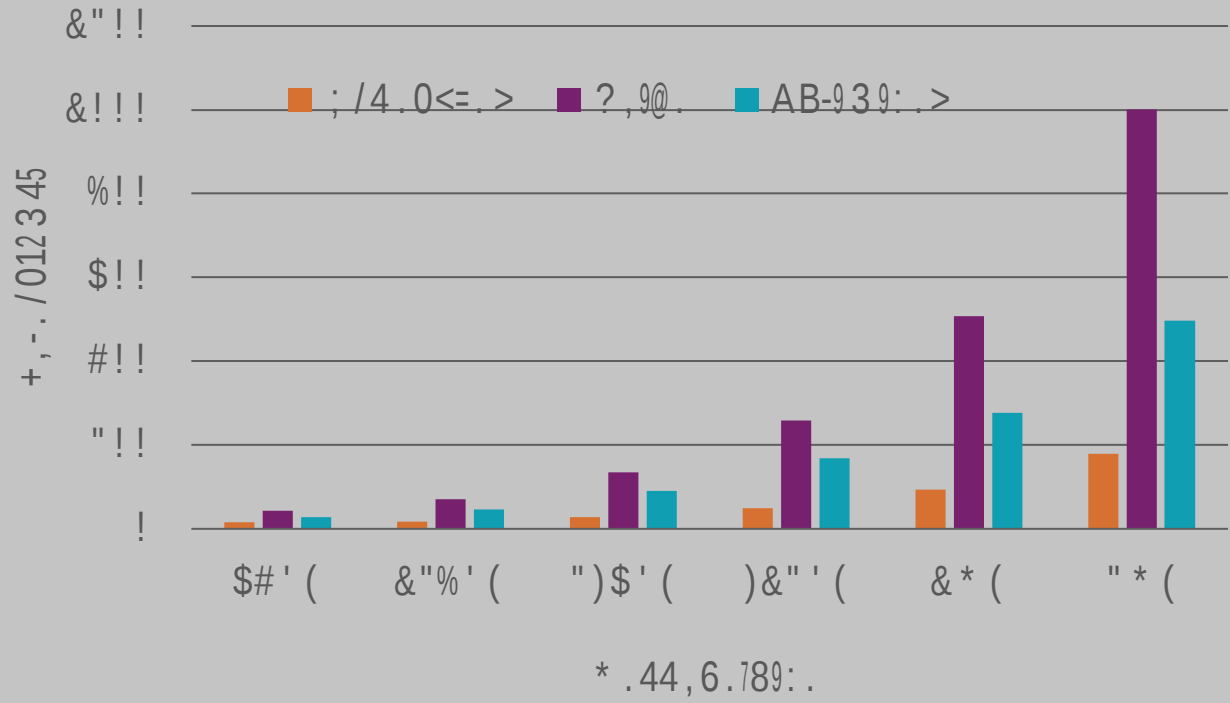
3) "" - * 4150\$) 617 -. # 8" (9: 1; 0 < - * 0" - * =

> ? 7 @ A), 8 * (" = 1 B C 0 = 1 D 2 E F

>.+,+#="=</#%?7+.7<+@

- ./", '01\$2/, +\$3""4\$56)*&0+)/07""/, 8\$9:68*&0+8/07""/, 8;*/ <=\$7, 2+>\$&\$%?@\$)! AB\$#>&, '
 - 0 P, \$&, 7; /).0\$/6', /' .\$/ L\$)"&/\$=' .Q/"" 6
-)*&0&C0+\$8/07""/, 8\$/D\$8+*7>+\$/ < < 7, "*"&'"/, \$<"220+3&>+\$C&8+2\$/ , '\$4+?\$)E\$
 - F G H I A J K L \$0"C>&>1
- M0+: "C0+\$) 7NN/>'\$D/>\$ < 70'"N0+\$/ >1N' /#>&N4"*\$0"C>&>" +8\$&, 2\$, , * >1N'"/, \$8*4+ < +8(\$
 - * /, D"#7>&C0+\$N+>\$78+>\$>+07+8'
-) 7NN/>'8\$))PQRP)\$+, * >1N'"/, \$N>/' / * /0
-) 7NN/>'8\$8+*7>+2\$N/", '6'/6N/", '\$*/ < < 7, "*"&'"/, \$/N+>&'"/, 8\$9C0/*S", #&&, 2\$, /, 6
 - C0/*S", #= D/>\$", '+>6

X R4' 9Q&, ?\$6' &,)2)' 2
 6' &,)\$/#, 7<.#9-
 X S\$, ' 7#/F\$T\$66,



* .44, 6.789:.

X



