Session 7

Algorithm Submitter
Rebuttals and Discussion

Outline of Session

- Submitter Comments
  - Jim Massey
  - Klaus Huber
- Issues (Miles)
- Audience Issues

Submitter Comments

Jim Massey Safer+

Klaus Huber, Magenta

Others

Issues (Miles)

Intellectual Property (IP)

- IP goal: AES will be available on a royalty-free basis worldwide.
- Concern: Submitters may claim that their IP is infringed by the practice of another candidate algorithm.

5

IP, continued

- NIST posed the following question to the 15 submitters (for an informal, non-binding response):

Are you willing to waive any IP rights you may have on any party who makes, uses, or sells implementations of the selected AES algorithm(s) (no matter which algorithm is selected) ?

6

Summary of Responses

Unqualified Yes:	**CAST-256, Crypton, DEAL, Frog, LOKI97, Rijndael, Serpent, and Twofish**	
Other responses:	**DFC, E2, MARS, HPC, RC6, and Safer+,**	**(Details follow)**
No response:	**Magenta**	

7

Details of "Other Responses"

DFC:

...Since the CNRS has been investing on this technique (my salary at least), I guess it would not like to see its technique adopted as a free standard without any form of recognition (e.g., having another candidate adopting its technology without any mention to CNRS and after having DFC not "promoted" at all). ...

CNRS do not need to make profit though. … My intuition is that it is possible to deal with the CNRS on reasonable basis if required. I regret I cannot say more on behalf of CNRS.

8

Details of "Other Responses"

E2:

If NIST publicly recognizes the contribution of NTT's intellectual property rights to the selected AES algorithm, we may agree to grant a license under the patent applications identified in Section 2.D.2 of the NTT AES submission to NIST.

Note that this comment is informal.

9

Details of "Other Responses"

MARS:

If the selected algorithm is one (or more) of the currently published 15 submissions and all submitters grant patent rights under terms at least as broad as those granted by IBM herein, IBM agrees to grant a license to practice the selected algorithm to any interested party under the patent application identified in Section 2.D.2 of the IBM AES submission to NIST.

10

Details of "Other Responses"

HPC:

Yes, provided the selected algorithm is one (or more) of the 15 submissions or a minor variation of a submission, or some combination of submissions or parts of submissions. And of course this waiver only applies [with respect to] the AES cipher, and not to any other activities of an AES maker/ user/ seller.

I will assert no patent or other intellectual property claims for my submission, the Hasty Pudding Cipher, regardless of whether it is selected.

I cannot speak officially for the University of Arizona [with respect to] the other ciphers.

11

Details of "Other Responses"

RC6

RSA will not require licensing or royalty payments for the manufacture, use, or sale of products utilizing the algorithm selected as the AES, which conform with the AES, on the basis of any patents that RSA may hold that could be deemed to cover the selected algorithm. However, RSA may require appropriate notices acknowledging RSA's ownership of such patents.

12

Details of "Other Responses"

Safer+ :

Cylink agrees to waive all claims for infringement under its intellectual property rights to any of the current AES candidate algorithms or minor modifications thereof against any party for making, using or selling implementations of AES.

I believe that this is what AES needs and is fully consistent with Cylink's business practices.

13

Audience Issues?

14