A SHORT REPORT ON THE RSA CHIP

Ronald L. Rivest

MIT Laboratory for Computer Science
Cambridge, Mass. 02139

The nMOS "RSA chip" described in our article [1] was initially fabricated by Hewlett-Packard. Testing revealed that while the control portion of the chip worked correctly, the arithmetic section suffered from transient errors and was usually too unreliable to complete a full encryption. We tested a number of chips and found the same problem, enough to convonce us that the cause was probably a design error and not a fabrication problem.

We have recently refabricated the chip, through the kind auspices of Xerox, with an improved power distribution network. While we had good reasons to believe this would help, it was disappointing to find out that this modification was insufficient to prevent the transient errors.

We are hopeful that we can identify and correct the bug in the near future.

The reader may be interested to know that a CMOS RSA chip of a rather different architecture is likely to be available soon as a commercial product; interested parties may contact the author for further information.

References

[1] Rivest, R. L., "A Description of a Single-Chip Implementation of the RSA Cipher," *LAMBDA Magazine* **1**, 3(Fourth Quarter 1980), 14-18.