WaveMeter Chip Provides Digital Money

Specialized Encryption Chip Acts as Utility Meter for Information

by Michael Slater

It isn't often that an entirely new type of microprocessor peripheral chip emerges, but the WaveMeter chip from startup Wave Systems is just that. The WaveMeter chip is an information meter, collecting money from the user on a per-item basis as information is accessed. Wave expects unlocking programs and data from CD-ROMs to be the largest initial application, but the meter and its associated on-line data center can be adapted (with third-party software) for a variety of other uses, including software license management, software rental, and data broadcasting.

The goal of Wave Systems (whose founder and CEO is Peter Sprague, chairman of National Semiconductor) is nothing less than to have its chip on the motherboard of every PC. The chips themselves will be made and sold by semiconductor partners; Wave Systems expects to make its money by providing the information network that controls the flow of money to the chips, taking its cut along the way.

WaveMeter Chip Meters Out Information

At the heart of the WaveMeter, as shown in Figure 1, is a DES (Data Encryption Standard) decryption engine. This engine is the main element in the chip's "security core," which also stores the secret keys. These keys, along with a 64-bit unique chip identifier, are loaded when the chip is initialized.

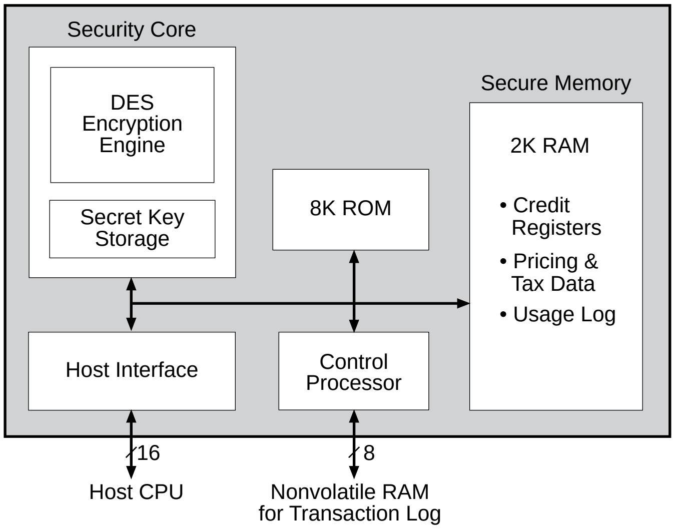

Figure 1. The WaveMeter chip includes an encryption engine, a control processor, and secure memory.

The chip has a custom microcontroller with 8K of ROM and 2K of RAM that controls the overall operation. The on-chip RAM stores credit balances, pricing information, and a usage log. More detailed usage information is stored in an off-chip nonvolatile memory. The initial systems will use battery-backed SRAM for the on-chip and off-chip memory. The chip also includes a secure timer to support software rental.

The WaveMeter chip interfaces to the host processor as an intelligent peripheral, via a 16-bit data bus. The maximum decryption rate is 100 Mbps (with a 25-MHz clock), or 12.5 Mbytes/s. The host system must provide the user-interface software and a modem for communication with the WaveNet network.

The WaveMeter chip is currently implemented in a gate array and consists of about 45,000 gates. A standard-cell version is planned to reduce the cost.

Wave will supply application developers with Windows 3.1 device drivers and software libraries for interfacing to the WaveMeter.

Buying with Digital Money

Figure 2 shows the flow of money and information in the Wave system. Information providers using the Wave scheme will generate CD-ROMs in which all the data is encrypted except for "clear" headers for each file. The user can search these headers, which include abstracts of the files' contents, to find the desired material. The chip then "sells" the user the desired items.

The system uses three-key DES encryption with 56-bit keys. Three keys make the system much more secure than single-key DES. The consumer can use the WaveMeter only for decryption (the device encrypts only its communications with the WaveNet data center), so Wave says that it has received permission to export it. (Export of most encryption products is banned by the U.S. government.)

Because the information on the CD-ROM is encrypted, information providers can fill it up with vast amounts of valuable information, yet give the disk away for free (or nearly so). Users then have instant access to whatever data they want from the disk, and have to pay only for the bits they select.

Essential to the usefulness of the WaveMeters is the specialized WaveNet on-line service that Wave will operate. All communications with WaveNet will be handled automatically by the application software; the user won't have any direct interface to this service.

For high-value purchases, the user's computer can

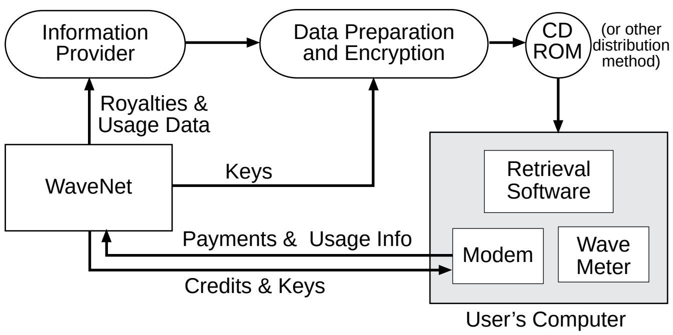

Figure 2. WaveNet delivers credit and decryption keys to WaveMeters (via modem), collects usage information, and pays royalties to information providers.

call WaveNet to make a specific purchase. WaveNet will charge the customer's credit card (or bill by other means) and then send to the meter the special key that is required for that particular WaveMeter to decrypt the desired information.

To provide more flexibility and support smaller purchases having a lower transaction cost, the WaveMeter chip includes "credit registers" that set the current value of the device. Credit is typically obtained by providing a credit card number (or otherwise establishing credit); the system then calls the WaveNet processing center and obtains credit. Once this is done, the user's money has been transferred to the WaveMeter; with this approach, the meter must be "filled" with money before any purchases can be made. Its advantages are that information can be purchased instantly—there is no need to make a phone call for each purchase—and communication costs are reduced. It also makes it possible to purchase information even from a portable system that is not currently within reach of a phone line.

As the user buys information from CD-ROMs (or other media) that support the Wave scheme, the costs are deducted from the credit balances stored in the chip. If the credit runs out, the user must buy more. The backup battery is critical; if the battery-backed RAM dies, so does your money. Eventually, the company plans to switch to EEPROM memory, which would eliminate this potentially serious problem.

The WaveMeter also stores tags that record each transaction. The next time WaveNet is accessed to gain more credit, the tags from the meter, which identify which vendors' information was purchased, are read into the WaveNet accounting system. Wave Systems then distributes the money to the information suppliers—after taking its cut, of course. All the essential information for paying royalties is stored in the on-chip memory, which is immune from tampering; the external memory stores more detailed usage information and is not essential to the payment process.

Because the credit registers are on the same chip as the encryption logic, the hardware provides a virtually impenetrable barrier to tampering with the till. Of course, this is also the ultimate attraction for hackers. Wave is confident that its encryption scheme is secure and plans to offer a substantial cash prize to anyone who can break it.

Price & Availability

An early version of the WaveMeter has been built by National Semiconductor, which has licensed Wave's technology. The version described in this article will be built by another as-yet unnamed semiconductor vendor, with which Wave is in the final stages of negotiation.

Samples of a gate-array version should be available this summer, with production in the fall, priced at about $22 in volume. Wave expects a future standard-cell version to bring the cost down to $13–$15. Packaging will be an 80-pin PQFP or 84-pin PLCC.

Wave Systems can be reached at 800.WAVE.NET, or 212.755.3282; fax 212.755.3436.

Getting to Critical Mass

As attractive as the Wave scheme is for information providers, it can work only if a WaveMeter is installed in the user's PC. Wave Systems and its partners plan to provide WaveMeters on PC/AT cards and PCMCIA cards as well as versions for SCSI, but the real future lies in getting the chip on the motherboard.

Normally, this would be an impossible task; the PC business is so cost-sensitive that putting an optional $20 chip on a motherboard just isn't going to happen. It also requires that the system have a modem, which would not otherwise be needed for CD-ROM access. Wave Systems has a bold scheme that could help overcome this hurdle: it will share the royalties with the PC maker. This still requires the PC maker to invest in the chip and hope for a future royalty stream, which might not be practical for many companies. Hewlett-Packard is the first major PC maker to agree to try the chip in a multimedia system.

Wave's big challenge is to convince a critical mass of information suppliers to use the system, making it more attractive for system vendors to include the chip on their motherboards. So far, Wave is working with IBM to use WaveMeter with IBM's CD Showcase (a collection of encrypted software on CD-ROM), with Novell on software license management, and with Personal Library Software on a search interface. The *Financial Times* (of London) also plans to distribute information using the Wave system.

The WaveMeter system has yet to be proven in the field, but it promises to offer information providers a new tool that could reshape the way information is sold—and to add another chip to the PC motherboard. ♦