An Ultra Small Individual Recognition Security Chip

The manufacture and distribution of goods requires good quality and inventory control. The RFID-enabled μ-chip's small size and low cost make it suitable for attachment to paper media and small products, aiding counterfeit prevention and product tracking in market environments.

Kazuo Takaragi
Mitsuo Usami
Ryo Imura
Rei Itsuki
Tsuneo Satoh
Hitachi

There is an ever increasing demand for improved electronic system solutions to support such fields as manufacturing, product distribution and sales, finance, transportation, and customer service. In manufacturing, electronic system solutions strictly control individual product quality. As for product distribution and sales, to maintain satisfied customers, the system must precisely track the location of individual deliveries, and provide high-quality products to the market. This helps detect counterfeit or copycat products entering the market, protecting the reputation and, hence, the profitability of reputable brand products. In finance, electronic systems help prevent forgery of such documents as paper money, credit cards, and gift certificates—an increasing threat as markets globalize and authentication of goods becomes more complicated. Product transportation requires advanced systems to control traffic information and logistics—information about how a company moves its raw materials and finished products—for individual areas. The demand for security in the customer service sector is also increasing. As Internet use grows, businesses and their customers require the safe exchange of business information and purchasing of goods over a computer network.

To meet these business and consumer needs, radio frequency identification (RFID) IC chips help control information and product distribution. Since the late 1980s, researchers in many fields have considered and experimented with RFID use in industry. Examples of applications include transportation management of storage containers, payment using smart cards, and even cattle breeding. Since the RFID chips used for these purposes were relatively large in terms of die size and expensive, they were appropriate for only large objects—such as cargo containers and oversize boxes—and for high-value products. However, it was difficult and inefficient to apply this type of large, RFID chip to products that were low cost, relatively small and disposable, packaged, or made from soft material such as paper. For these products, bar codes were more cost-effective and easier to handle. However, the bar code has several drawbacks—it is easily copied, has low security, and requires a large, relatively expensive reader that is difficult to miniaturize because it includes optical components.

Under this market background, we devel-

0272-1732/01/$10.00 © 2001 IEEE

oped a thin, micro-size RFID µ-chip. The µ-chip is attachable to thin, soft media, such as paper, preventing product counterfeiting. Using semiconductor technology instead of the bar code's print technology, the µ-chip provides micro-size data storage and acts as an automatic identification device. Because of its small, thin size, the µ-chip is suitable for low-cost and small products. Furthermore, because the µ-chip can attach to paper, wide-range digital tracking of individual materials outside of a computer database is possible.

Individual recognition technology

Technological innovation and availability is progressing with business and consumer use of digital information systems, such as the Internet. However, such systems don't necessarily include information about physical materials, such as shipping origination and destination locations. Because this information is not readily available, solving problems such as lost shipments requires a huge expenditure of time and money. These costs would be eliminated or reduced if businesses could immediately store this material information into a memory device when manufacturing or business processes create the data. In most cases, current processes do not allow such immediate storage, and reconstructing the information later is often complicated.

Material communication

Imagine if the commodities used in daily life, such as documents and their storage location or medicine and prescriptions could communicate with each other. For example, when a worker misplaces a document, the document tray might find its location. Or if a document has remained untouched for a long time, it might signal the creator to check it. If a patient was dizzy and about to take medication to alleviate this symptom, the medicine might warn him not to take it because the prescription and historical record stored in the RFID chip indicate that he has already taken the maximum dosage for a given time period.

Linking objects to distributed proxies

Imagine that an identifier is attached to every commodity in the world. Sensors, if located properly, could then recognize the identifier and provide information such as the commodity's location, handling time, and some environmental data. The system could also provide more detailed information by accumulating a lot of simple information, rearranging it, and reasoning about it in a certain context, for example, automatically checking product production volume versus the quantity ordered. This system would also be suitable for use with nonartificial objects, that is, human beings and other living creatures.

Each real object would have counterpart software in a computer. The software would receive information about the real objects through RF sensors. Then the software would execute data processing as if the real objects were intelligent. For example, if the real object were a product in transit, the software could verify that it was en route to the correct destination. Such software works on behalf of the real object and is called the *proxy* or *virtual object.* Furthermore, these virtual objects could exchange information with each other through the Internet, and perform intellectual processing. After this processing in the virtual world, the software would send feedback information from the virtual world to the real one. From this, we could build a type of data processing that realizes a new pattern of object interaction. In essence real objects can effectively pass information between each other through the interaction of their virtual objects.

Aims of ubiquitous computing

Researchers in the ubiquitous computing field have already explored the vision of making a real object smart by letting it communicate with a counterpart virtual object. For example, in the Smart Library experiment implemented by the Swiss Federal Institute of Technology, Zurich, and the German National Research Center for Information Technology, researchers used RFID-enabled IC chips to automatically sense people and books in a library-like environment.[1] In this experiment, a person's virtual object records what books that person is interested in. Conversely, the book's virtual object records the status of the book, such as whether it is out on loan and where it is currently located. When the person enters the library, the virtual objects exchange information to create and send desirable book information to a display device near the person. Here, a signal from the real-world object's IC chip triggers the upward information flow from the real-world object to the virtual one. Then the virtual objects process information in an intellectual manner—in this case, deciding whether the book relates to the person's previously recorded interests. The downward information flow from the virtual world to the real one creates a physical action, that is, showing information on a display device. Making these types of chips and sensors low in cost, small in size, and high in performance will make it easy to apply the chip to daily materials and increase their use and popularity.[2] In the future, we might even be able to make dust in the air smart.[3]

The μ-chip

Hitachi's μ-chip aids upward communication from real-world objects to virtual ones. The RFID μ-chip, shown in Figure 1, is 0.06-mm thick and 0.4-mm long on each side. By applying suitable packaging techniques, manufacturers can embed the chips in micro-objects. The 2.45-GHz band frequency for radio communication, similar to that used by Bluetooth technology, enables use of a small sensor device.

The current μ-chip itself does not have much intelligence. Its only function is returning the 128-bit identification data upon receiving the radio wave from an external sensor. This data is the same length as IPv6 addresses. In designing the μ-chip, we pursued a simple way of making material as identifiable as possible.

Securing pervasive material handling

The μ-chip's characteristics give it an advantage over other approaches to identifying and tracking products.

The μ-chip versus the bar code. The μ-chip is similar to the bar code in that both give identification numbers to objects. One major difference is that the μ-chip can be attached to small objects that the bar code cannot because of the bar code's larger size. Therefore, the μ-chip enables handling of objects efficiently in a wider range of applications than the bar code. Furthermore, copying μ-chips is much more difficult than copying bar codes. Thus, μ-chips can handle objects more securely than bar codes, preventing the forgery of security papers and providing counterfeit protection for branded products.

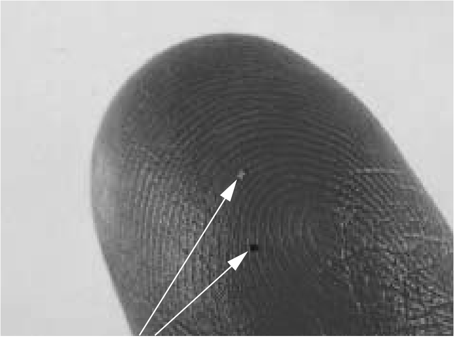

Figure 1. Two prototype μ-chips. Their die sizes are both 0.4×0.4 mm.

Unrewritable 128-bit identification code. The μ-chip retains 128-bit ID information in ROM, which is written only once at manufacturing time. It cannot be modified after shipment.

The data includes system-administrator-created system data. It also includes application data and a message authentication code (MAC)[4] created by a service provider. The service provider calculates MAC using cryptographic check function f with the input data comprised of the system data, application data, and secret key K.

$$\text{MAC} = fK\text{(system data, application data)} \quad (1)$$

The service provider's computer securely retains secret key K. When a sensor sends the 128-bit ID information to a computer, it checks to see if the original MAC matches the calculated one from Equation 1. If the system data and/or application data is altered during the data transmission or through other events, the computer easily detects the alteration because the calculated MAC would be incorrect.

Forgery prevention. Figure 2 shows the basic structure of chip operations. For example, a gift certificate (a type of security paper) and/or an expensive well-known brand product need forgery protection. At a location where these items are handled, for example,

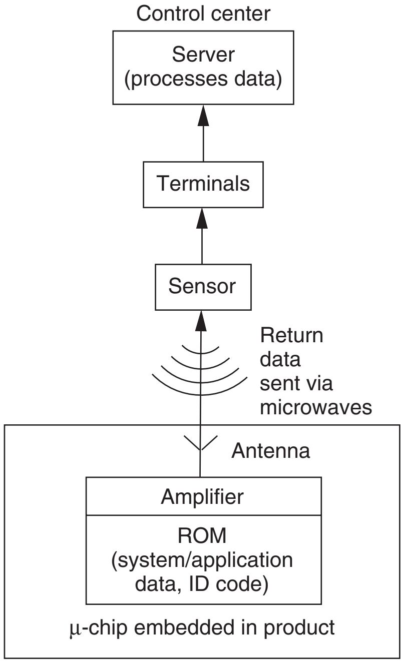
Control center
Server (processes data)
Terminals
Sensor
Return data sent via microwaves
Antenna
Amplifier
ROM (system/application data, ID code)
μ-chip embedded in product

Figure 2. Basic structure of μ-chip operations.

a wholesaler's distribution warehouse, a person visually examines the products to initially verify their authenticity. With visual examination alone, however, it is difficult to detect skillful counterfeits. One countermeasure is to embed a μ-chip into security papers or brand name products and verify authenticity with a sensor reading. In this case, a sensor reads the 128-bit ID information; with the antenna, the μ-chip is readable by the sensor within a 30-cm range, instead of proximate range for reading a μ-chip that does not have an antenna. In both cases, the security audit mechanism implemented in a server checks for any abnormality by analyzing network-transmitted records. The system signals an alarm when it detects an alleged counterfeit chip, identification numbers transmitted at the same time from different locations, or any other predefined abnormality.

Toward higher security and privacy

The μ-chip and encryption don't offer foolproof security. The previous examples do not cover all security risks. For example, the more personal the information stored, the higher the risk of privacy invasion from internal abuse, such as medical records or banking details, which require other types of security measures. Also, many experts and professionals anticipate that as ubiquitous computing advances, more difficult security and privacy problems will arise.[2] This could affect systems using the μ-chip.

Security evaluation standard ISO 15408 (*Evaluation Criteria for IT Security*) will provide a framework for constructing secure systems.[5] Among the conventional functional requirements—such as those for security audits, cryptographic support, and so on—the standard also covers privacy. To follow the standard, some applications must provide functionality that supports privacy. The standard stipulates subcategories of privacy functionality: anonymity, pseudonymity, unlinkability, and unobservability. To use this privacy functionality, those implementing security systems must define a protection profile for a specific user community. The profile should specify, for example, which subcategories of privacy functionality a system should use and to what extent it should implement for a given security level.

The μ-chip characteristics of having little intelligence and being difficult to duplicate will aid system construction under such security frameworks. For example, because it has no rewrite capability, the μ-chip itself cannot convey information about someone wearing a μ-chip unless the individual's identification was written onto the μ-chip when it shipped. In other words, the μ-chip can only send the information burnt into its ROM at the factory. Therefore, the μ-chip realizes a pseudonymity function similar to that of cash, that is, it offers a kind of anonymous payment.

Manufacturing the μ-chip

Research in various fields is promoting effective technologies for linking objects and network information. The μ-chip is an example of semiconductor technology making great contributions to information technology.

The μ-chip has both analog and digital circuits that operate without a battery. Figure 3 (next page) shows the μ-chip's basic internal structure. We realized the 2.45-GHz microwave carrier for receiving signals with a front-end circuit of 0.18-micron complementary metal oxide silicon (CMOS) semiconductor technology. Moreover, we designed the high-density chip layout with no parasitic effects; circuit malfunctions due to interference among transistors will not occur. Furthermore, our design uses a built-in 100-pf capacitor formed by the gate oxide of the MOS transistor as a power supply, eliminating the need for batteries.

Economy and reliability

When attached to media such as paper and linked to network information, the μ-chip has various implementation capabilities such as bank note counterfeit protection and document verification. Therefore, the μ-chip must be economical and reliable to meet different systems' needs.

Microminiaturization is necessary for an inexpensive and dependable IC chip. Since the production cost of the semiconductor wafer depends on the semiconductor process applied, increasing the number of chips obtained from a semiconductor wafer lowers per-chip cost. The percentage of good IC chips obtained from a wafer is called yield (Y), and it can be calculated by using the following formula:

$$Y = \exp(-D \times A) \qquad (2)$$

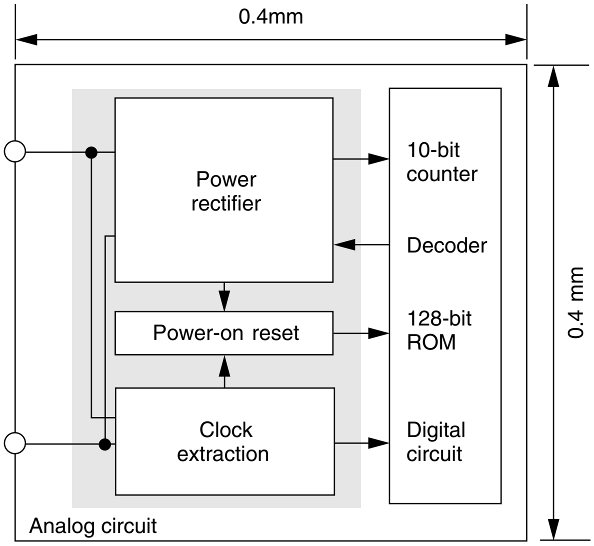

Figure 3. The μ-chip circuit block diagram.

In Equation 2, D stands for the number of defects per semiconductor wafer, and A stands for the chip dimensions. Even if semiconductor defects are relatively high, manufacturers can exponentially improve yield by reducing chip size. This formula promises future economical manufacturing of ultra small chips, such as the μ-chip.

For an IC chip to be usable on soft media such as paper, it must resist stress and remain undamaged during use. To measure this property, we used a mechanical strength test on the μ-chip. As Figure 4 shows, mechanical strength is higher when chip size is less than 0.5 mm × 0.5 mm. Thus, the microminiaturization of chips lets us develop an economical and reliable radio-recognition device.

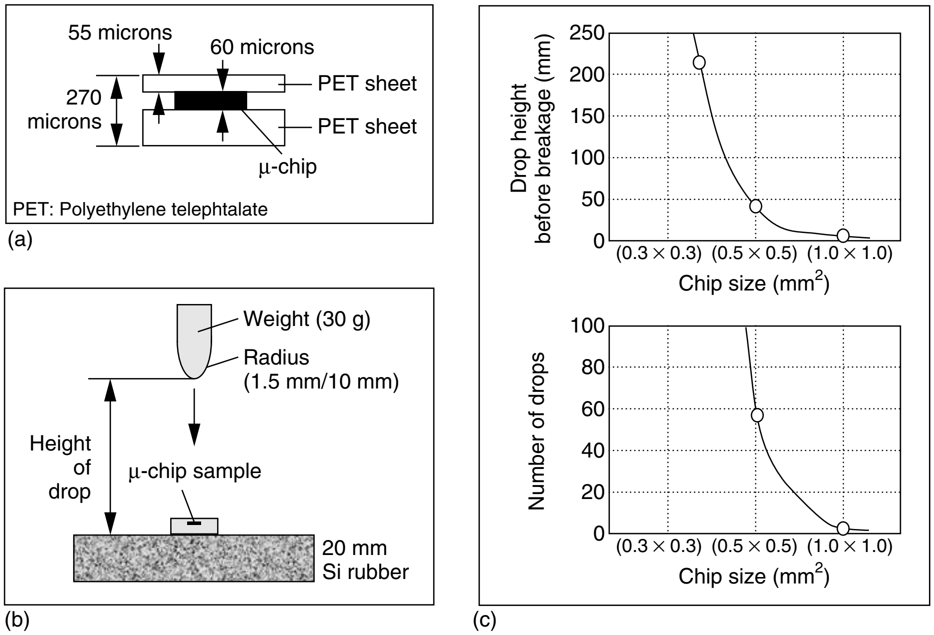

Figure 4. Mechanical strength of the μ-chip: Sample structure (cross section) (a), test condition (b), and test results (c).

Usability

Suppose a gift certificate manufacturing company embeds μ-chips in every gift certificate that it issues. The company would also record each μ-chip's ID information and the gift certificate data embedded in the chip—its face value and whether it's considered distributed or undistributed, and used or unused. A database at a gift certificate control center would have access to this information.

This control center database would include ID information about gift certificates stored in the distribution process. When a shop receives a gift certificate from a customer, a sensor reads the ID information from the embedded µ-chip and then retrieves data related to the ID information from the database at the control center. In this way, a store can confirm whether the customer's gift certificate is genuine or not. For example, suppose a criminal removed the µ-chip from a ¥1,000 gift certificate and incorporated it in the counterfeit gift certificate with a face value of ¥5,000. The store could easily discover the forgery by comparing the value printed on the gift certificate with the amount in the µ-chip information. It is also possible to prevent the double use of gift certificates, after sending data about which gift certificates were already used for a purchase to the control center. This system also helps retail stores cash in the gift certificate with the issuing company after a customer redeems the certificate at a store.

Another example of a µ-chip application is product counterfeit prevention and automatic substance identification. When manufacturers attach µ-chips to their goods, it aids distribution management intended to preventing forgery of brand name goods.

Some retailers say that they would rather not put a tag or seal using a bar code on their goods because these markers have a negative impact on the appearance of the product. Because of its small size, the µ-chip, therefore, has the advantage of being unnoticeable. Furthermore, it is difficult for a malicious person to find where it is attached on a product. Manufacturers can input data from attached µ-chips into the database at a control center. Such information includes the product's ID information, name, and picture. The manufacturer might also input data relevant to the distributor who delivers the goods and the retailer who receives them. Such distribution information helps control whether goods are properly delivered to the correct location. At the same time, it is also possible to construct a database for customer relationship management and counterfeit detection in a secondhand market by storing purchaser data on the ID information database.

The µ-chip offers a highly versatile and cost-effective solution for product authentication and verification applications. For low-value items, the bar code still has an advantage over the µ-chip in terms of unit cost, although the cost of bar code readers is generally higher due to its optical components. Bar code readers also have an inherent limitation in their scalability, whereas we could eventually reduce the µ-chip reader to a single chip solution, offering great benefits in terms of size and cost. An attached bar codes is also clearly visible, which may be an advantage in certain applications. However in applications such as bank note security and security tagging, the µ-chip's near invisibility offers unique benefits. In comparison to conventional RFID ICs, the µ-chip has a clear cost and size advantage. Although, the µ-chip's fixed memory configuration obviously implies limits in terms of supporting high-security protocols. Accordingly, companies will most likely use µ-chips in such fields where bar codes and IC cards aren't practical, such as for controlling small objects and paper media on which individual identification is difficult to apply.

There are several challenges with the uses we described. One is the construction of an identification control system that can serve as the base for information management. To securely use such a small RFID tag like the µ-chip, suppliers must strictly control personal, substance, and distribution channel information. Furthermore, manufacturers and distributors must use the µ-chip in combination with other measures to recover damage caused by counterfeiting—detection of the counterfeit item is only part of the solution for a business perspective.

In addition, the wide use of µ-chips will require developing a comprehensive system solution including readers, software, and other peripheral devices that meet the needs of a wide range of applications. MICRO

References

1. M.-L. Moschagth, J. Hohner, and R. Reine-

ma, "SmartLibrary—An Infrastructure for Ubiquitous Technologies and Applications," *Proc. Distributed Computing Systems Workshops 21st Int'l Conf.* (ICDCS Workshops), IEEE CS Press, Los Alamitos, Calif., 2001, pp.208-213.

2. F. Mattern, "Omnipresence of Computers—Privacy in a World of Smart Objects," *Congress Security—Enabler or Burden? The Feasibility of Internet-Security Congress*, Berlin, May 2001; http://www.inf.ethz.ch/vs/publ/selected_talks.html)
3. B. Warneke et al., "Smart Dust—Computing with a Cubic Millimeter Computer," *Computer*, vol. 34, no. 1, Jan. 2001, pp. 44-51.
4. *ISO/IEC 9797-1, Information Technology—Security Techniques—Message Authentication Codes (MACs)— Part 1; Mechanisms Using a Block Cipher*, Int'l Organization for Standardization (ISO), Geneva, 1999.
5. *ISO/IEC 15408 Information Technology—Evaluation Criteria for IT Security*, Int'l Organization for Standardization (ISO), Geneva, 1999.

Kazuo Takaragi is a senior manager at the Hitachi Systems Development Laboratory, Yokohama, Japan. His research interests include cryptography and information security techniques. Takaragi received an MS in control engineering from the Tokyo Institute of Technology and PhD in reliability engineering from Tokyo University. He is a member of the IEEE; the Information Processing Society of Japan; the Institute of Electronics, Information, and Communication Engineers; and the Institute of Electrical Engineers of Japan.

Mitsuo Usami is assistant to the general manager in the Hitachi Multimedia Systems Research Department. His research interests include application devices using thinned silicon chips, magnetic-card-like ultrathin IC cards, and bipolar high-speed logic LSIs for large-scale mainframe computers. Usami received a BS in electronics engineering from the Tokyo Institute of Technology.

Ryo Imura is chief executive officer of Mu-solutions, an in-house venture company at Hitachi. His research interests include information and secure ID systems. Imura received a PhD in material science from the University of Nagoya. He is a member of the Academic Society of Applied Physics and Applied Magnetics in Japan.

Rei Itsuki is a senior business coordinator of Mu-solutions, Hitachi. His research interests include knowledge engineering and business-to-business e-marketplace systems. Itsuki received a PhD in information system engineering from Osaka University. He is a member of the Information Processing Society of Japan and the Institute of Electrical Engineers of Japan.

Tsuneo Satoh is director of the IC Card Business Unit at Hitachi. His research interests include microprocessors with nonvolatile memory. Satoh received an M.Eng. in electronics from Tokyo Metropolitan University.

Direct questions and comments about this article to Kazuo Takaragi, Security Systems Research Dept., Hitachi Systems Development Laboratory, 292 Yoshida-cho, Totsuka-ku, Yokohama-shi, Kanagawa-ken, 244-0817 Japan; takara@sdl.hitachi.co.jp.

For further information on this or any other computing topic, visit our Digital Library at http://computer.org/publications/dlib.