Penny Tag Technologies for Removable Data Storage

Low-cost authentication and identification methods for removable data storage cartridges are the focus of ongoing research. Unlike other security methods, these "penny tag" technologies must be automated for use in a removable data storage drive.

Fred Thomas
Iomega

Manufacturers commonly use tags or markers to authenticate and identify commercial products. Some typical applications for authenticating a product's source include visual holograms on software packaging, fluorescent spectrally encoded fibers in a garment's brand label, and hidden microscopic brand marking of aerospace parts.

Applications that identify products, either individually or within a class, are most ubiquitous in retail and warehouse logistics. Retailers, manufacturers, and distributors spend more than $10 billion per year to purchase bar codes and their associated systems for use in tracking countless billions of dollars in merchandise. These low-cost structured ink markings allow for quick and reliable product identification within a virtually unlimited inventory system. Radio frequency (RF) coil tags are another product identification technology used to reduce retail theft. In this case, sensors can detect the tags if they were not deactivated when the merchandise was purchased.

Authentication and identification technologies have also found applications in removable data storage. For example, cartridge identification systems can protect a drive from damage that inserting a foreign object might cause. They can also help manage forward and backward media format compatibility; let drives identify media types for reduced spin-up and data-access time; and create unique, unalterable, and authenticatable media serial number implementations for digital rights management (DRM) and enterprise security. One beneficial implementation of the technology is its use to authenticate parts and prevent counterfeiting in various industries.

The primary difference between retail and removable data storage applications is cost constraints. The applications for retail settings require human intervention or instrumentation costing hundreds, if not thousands, of dollars. However, the authentication and identification of removable data storage cartridges must be automated at a very low cost.

The Massachusetts Institute of Technology Media Lab has dubbed these low-cost authentication and identification technologies *penny tags*. MIT's ongoing program to explore and develop penny tag applications and technology has evolved into the Auto-ID Center (www.autoidcenter.org), which focuses on establishing a low-cost RF ID tag standard.

FIELD-PROVEN TAG TECHNOLOGIES

The varying requirements of specific systems have driven the progression of Iomega's penny-tag technologies, described in the "Evolution of Iomega Removable Storage Products" sidebar. These technologies have different features, depending on the requirements of a particular storage system.

Media unique serialization

High-capacity magnetic removable data storage typically involves a factory servo write process and a factory media verification process. These manufacturing processes can write a unique serial num-

Published by the IEEE Computer Society

Evolution of Iomega Removable Storage Products

The evolution of building cartridge identification and authentication into a removable data storage drive at Iomega illustrates the varied requirements of this technology.

Initially, when Iomega's researchers created the Zip 100 (super floppy), they felt that the drive needed a means other than the cartridge's physical size to discriminate between a functional Zip disk and a foreign object. This was mainly because the 3.5-inch floppy fit into the Zip drive media opening. A floppy could, upon insertion, cause the drive to launch its read-write heads onto the foreign object and destroy the drive. Hence, the retroreflective tag (retrotag) was introduced and is used on the Zip 100, Jaz 1 Gbyte, and Jaz 2 Gbyte products.

The evolution of the Zip 250 and Pocket Zip (Clikl! 40 Mbyte) produced two new sets of requirements. The Zip 250 drive reduced data track size and differing data and servo frequencies from the original Zip 100. Economics and the desire to have Zip 100 media compatible with the new 250 drove the decision to make it the same size and shape as the Zip 100 cartridge. However, inserting a Zip 250 cartridge into a Zip 100 drive would potentially destroy the drive. A technology that would cause the Zip 250 cartridge to be ejected automatically upon insertion into a Zip 100 drive was ultimately necessary. This new tag system also needed to allow for Zip 100 insertion into a Zip 250 drive and appropriate detection and access to the previous generation cartridge.

Iomega needed to retain its foreign-object protection functionality and, if possible, the ability to identify multiple types of the new tag. This capability would be advantageous for future cartridge backward and forward compatibility management scenarios.

The Pocket Zip 40-Mbyte drive's small size and the reduced working distances between the cartridge and any identification system in the drive made the Zip 100 retrotag discrimination physics unworkable. This product also needed to support the licensed distribution of music content directly from recording houses to consumers' handheld play devices. This made authentication of the media's source part of the new technology requirements.

These requirements in aggregate drove the development of two parallel path tag technologies: the latent-irradiance-tag and the holographic-tag (X-LSD). The ability of both technologies to support identification of multiple authenticatable tag types opens the path for implementing various specialty media types such as cleaning disks, computer access authentication disks, drive-calibration disks, and restricted drive firmware upgrade paths.

The need for a technology that would offer an unalterable media serial number source for robust DRM implementations also fueled the development of the laser-marking technology or disk indelible utility mark (DIUM) for the Pocket Zip. Most recently, work on robust DRM and enterprise security implementations has focused on means for including source-protected cryptographic keys within the removable data storage cartridge. To this end, the Peerless cartridge includes a smart card-directed secure memory with cryptographic authentication IC in its design. This seems to be a good direction for removable media, which has a native electrical interface with the drive platform.

ber to the media in an area that is not rewriteable by drives in the field, such as in areas for grey codes and flagged sectors.

Iomega has applied these unique serial numbers to all its removable magnetic media products dating back to the Bernoulli boxes of the 1980s.

Retroreflective tags

A retroreflective tag (retrotag) produces a structured or patterned reflection of light from the removable data storage cartridge that disk drives can uniquely discriminate from other types of reflections. The "Patents for Removable Data Storage Tag Technologies" sidebar provides additional information about patents on this and other related technologies. The Iomega retrotag used on Zip and Jaz cartridges has an array of corner cubes molded into a clear, optical plastic tag. This tag is similar to a roadside retroreflective safety marker.

Patents for Removable Data Storage Tag Technologies

The patents issued for retroreflective tags (retrotags) and other identification and authentication technologies for removable data storage include the following:

- F. Thomas, *Retroreflective Marker for Data Storage Cartridge*, US patent 5,638,228, Patent and Trademark Office, Washington, D.C., 1997.
- F. Thomas, *Thin Retroreflective Marker for Data Storage Cartridge*, US patent 5,986,838, Patent and Trademark Office, Washington, D.C., 1999.
- F. Thomas and G. Dixon, *Latent Illuminance Discrimination Marker System for Authenticating Articles*, US patent 6,264,107 B1, Patent and Trademark Office, Washington, D.C., 2001.
- F. Thomas, *Readable Indelible Mark on Storage Media*, US patent 6,324,026 B1, Patent and Trademark Office, Washington, D.C., 2001.

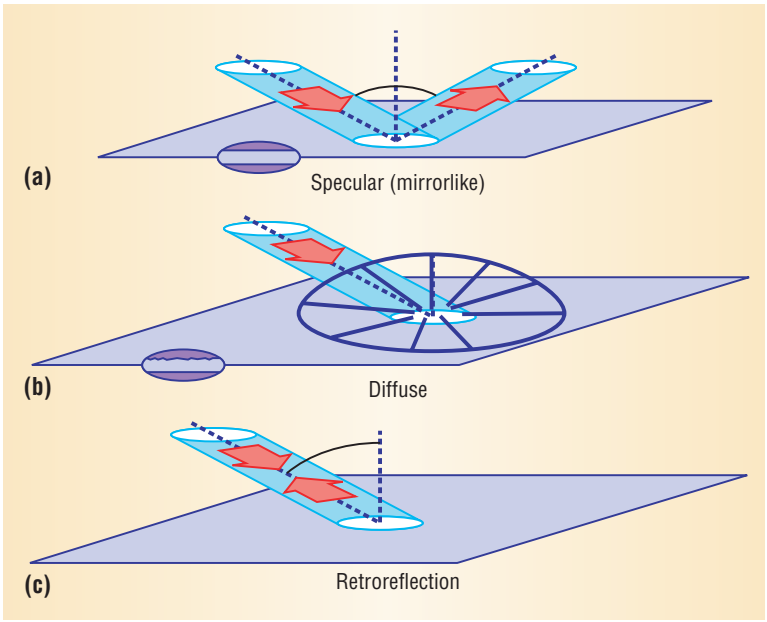

Figure 1. Principal types of reflection contrasted: (a) specular (mirrorlike), (b) diffuse, and (c) retroflection.

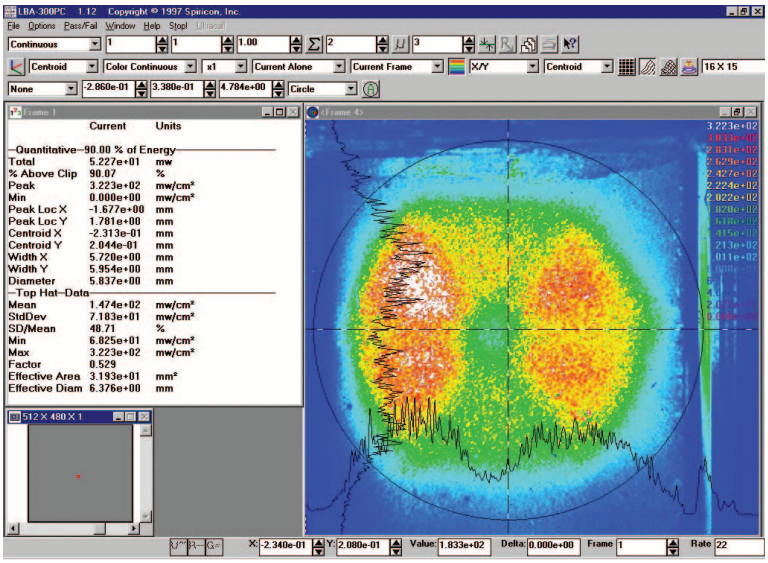

Figure 2. Reflective irradiance pattern of Zip 100 retrotag. The reflected irradiance in the structure is brightest in the hexagon's lobes where the photosensitive detector is placed.

Figure 1 illustrates retroreflection in contrast with the two other principal types of reflection from objects that might be inserted into a drive: specular and diffuse. Retroreflection is principally light reflected back at the source of the illuminating radiation. This property clearly defines the reflection's location, and its magnitude at that location is large relative to what equivalently sized diffuse or specular reflectors would provide.

Another retrotag characteristic is that the illumination and detection system's location relative to the tag is flexible. In Iomega drive implementations, a proximate LED and phototransistor/photodiode pair are positioned on the drive printed circuit board (PCB) below the retrotag location on the cartridge when the cartridge is fully in the drive.

As long as a significant portion of the LED irradiance is hitting the tag and the emitter/detector pair is within approximately a 40-degree cone of the tag's centroid, the system works well as a reflection-type discriminator. This latitude in locating the detection system provides flexibility in designing future compatible drive platforms. It also allows a generous tolerance of the retrotag's alignment to the detection system during manufacture.

The images in Figure 2 illustrate a bug's eye view of the reflection from a Zip retrotag from the location where the LED is illuminating the tag in the drive. A laser beam profiling software program and a frame-grabber system based on a charge-coupled device were used to generate these images.

The superposition of the array of 12 corner cubes found on the tag creates the reflection's hexagonal structure. The hexagonal reflection's size at the short working distances used in drive implementations is principally twice the diagonal size of the corner cubes.

To take advantage of this bright structured reflection, the detection device (phototransistor or photodiode) must be proximal to the LED, which is located at the hexagonal reflection's center. Therefore, the corner cubes' size must be physically matched to the separation distance on the PCB between the emitter and detector the system uses. In Figure 2, this distance is approximately 2.5 mm.

Figure 2 shows that the reflections from a retrotag are essentially localized to a small hexagonal area. Based on this reflective localization, we can create an even more effective discrimination system by adding a second photodetector positioned slightly outside this reflective lobe and using the difference between the signal inside the lobe and outside the lobe as the retrotag discrimination signal.

In fact, for the most difficult possible reflective sources that this system is intended to discriminate—specular reflectors such as metal foil or a polished shutter on a 3.5-inch floppy disk—this system enhancement improves performance significantly.

Figure 3a shows a contour plot for probability of discrimination of a specular reflector from a retrotag for the original single-detector system, and Figure 3b shows a contour plot for the differential dual-detector system. A Monte Carlo analysis system model generated these plots, which include empirical data on the reflective variability of the two different types of reflective markers among 20 other system variables with their distributions modeled.

The white sloping bands in Figures 3a and 3b

denote the region of 100-percent specular reflective foreign-object discrimination as a function of the system's photodetector gain (y) and the retrotag detection threshold voltage (x). These figures demonstrate that adding a $0.20 phototransistor to the design can broaden the 100-percent discrimination band by more than 60-fold.

Holographic tags

The large geometric size (2.5 mm) of the corner cubes used for reflection with the retrotag creates a structured irradiance pattern around the illuminating source LED. Holographic-tag technology does principally the same thing but with significantly more flexibility in the geometry of the structured, reflected light pattern. This follow-on invention uses the combination of a tiny retroreflective array material (150 microns across corner cubes) with a refractive holographic light shaping diffuser (LSD) material. Laminating these plastic film materials together creates a reflector, which in turn creates an assortment of structured light patterns upon reflection.

Figure 4 shows the reflected irradiance pattern that an X Light Shaping Diffuser (X-LSD), a holographic tag used on data storage cartridges, generates. The point at which the axes cross is the illuminating LED's location. To use the X-LSD for tag identification, three phototransistors are placed on the drive PCB on three axes separated by 45 degrees around the LED. The tag-cartridge identification is based on reflective illumination of the phototransistors. In this case, in which the tag has three photodetectors, the system can detect eight separate states.

Latent-irradiance tags

Latent-irradiant materials—more commonly described as fluorescent and phosphorescent—glow after being irradiated with light. The characteristic that distinguishes between fluorescent and phosphorescent materials is that the time period of light re-emission is longer than 10^{-8} seconds for phosphorescent materials and shorter for fluorescent materials.

The output spectra of different latent-irradiance materials have a distinguishing amplitude profile when illuminated with light having color within their absorption bands. *Stokes* materials irradiate at wavelengths longer than the stimulating irradiance, and *anti-Stokes* materials irradiate at shorter wavelengths.

Researchers have historically used the differentiation in spectral profiles of various latent-irradiance materials for authentication. For example, the fluorescent fibers in a $100 bill glow red when they

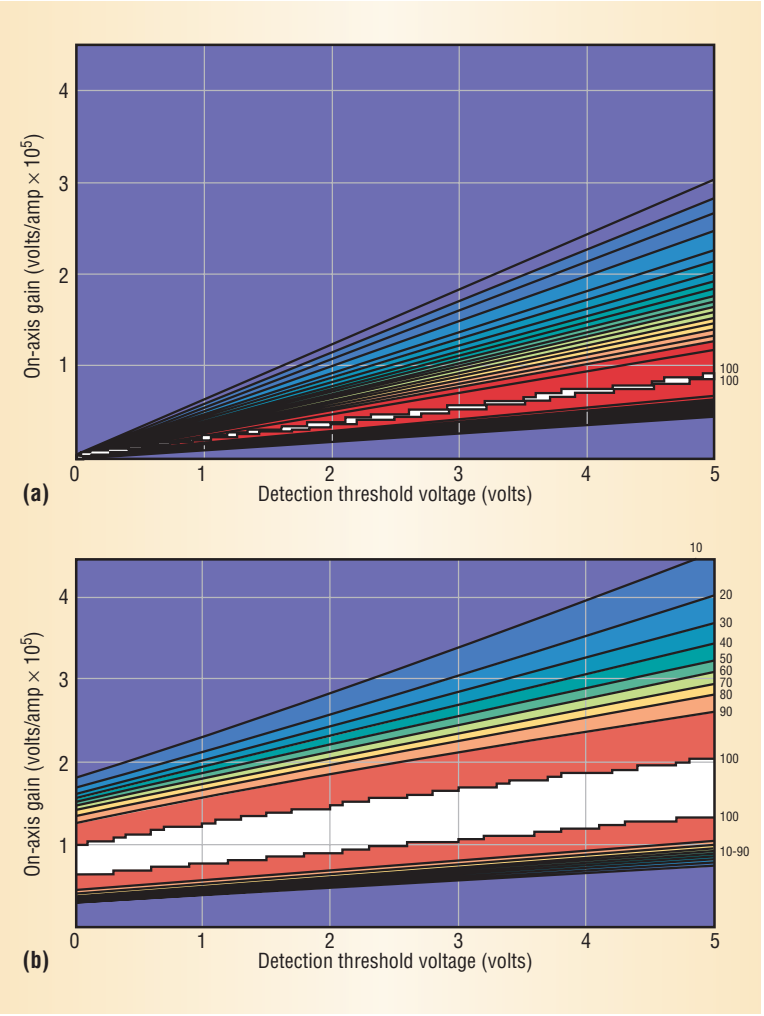

Figure 3. (a) Single-detector cartridge discrimination performance (retrotag versus specular reflector). (b) Dual-detector cartridge discrimination performance (retrotag versus specular reflector).

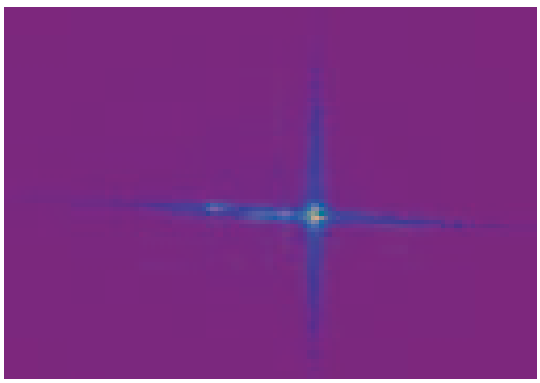

Figure 4. Reflected irradiance pattern for X-LSD holographic cartridge tag. The point at which the axes cross is the illuminating LED's location.

are irradiated with a UV source. A respected British scientist working in this area once told me that MI5 secret agents (made famous by the fictional agent 007, James Bond) wore phosphorescent authentication rings during World War II. In these cases,

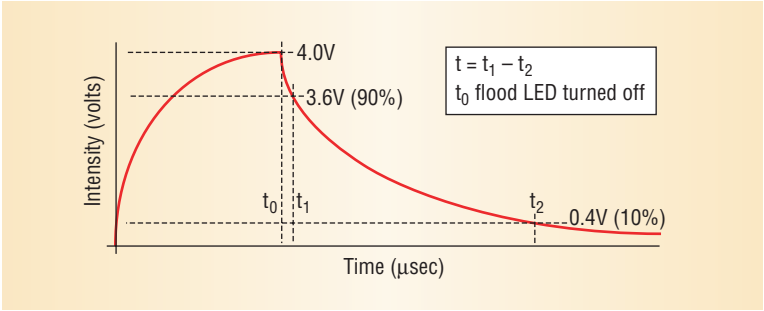

Figure 5. Typical temporal signal profile of a latent-irradiance material. The detection circuitry for this signal can implement automatic gain control (AGC) techniques. These implementations provide a significant level of system measurement robustness with varying signal amplitude.

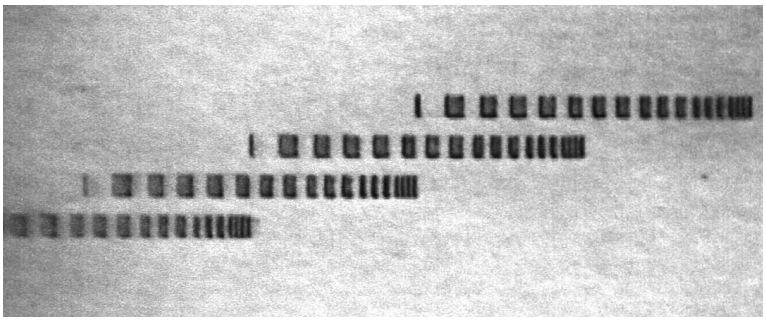

Figure 6. A disk indelible utility mark on Pocket Zip flexible media. DIUM creates an unalterable media serial number that a drive's magnetic head can read but not replicate.

authentication requires using either simple visual ID of a color or an elaborate and expensive photospectral analysis instrument.

In Iomega's patented technology for reducing the cost of a drive-automatable ID and authentication system, a single photodetector acquires a combination of spectral and temporal information from a latent-irradiance tag. After illuminating the tag with an LED within the tag's absorption band, a photodectector with a low-cost, dye-based polymer filter can monitor both the decay time and the temporal profile of the latent irradiance that the tag emits.

Blending combinations or matrices of different phosphor components can create multiple decay profiles, much like combining discrete frequencies in a Fourier series can describe any arbitrary piecewise temporal function. Figure 5 illustrates the typical exponential temporal decay profile of a single constituent phosphor component used to create such a matrixed latent-irradiance material. This temporal information is extracted from the data storage drive's microprocessor to identify and authenticate different tags types.

Security phosphors are a class of latent irradiance materials typically used for authentication on currency and other financial instruments. Developers can engineer these latent-irradiance materials so that they present a significant reverse-engineering hurdle to those trying to replicate their spectral and temporal response.

Generally, a phosphor matrix's response is fabrication-process dependent, so that constituent analysis only partially discloses information. In addition, numerous masking and obfuscating methods can further thwart reverse-engineering efforts, making this a robust means of authentication. A potential future application that leverages this security feature is to use a drive's read-write laser as the excitation source for DRM protection of content on optical data storage media.

Laser-marked media

The disk indelible utility mark (DIUM) is a laser-marking system that ablates a microscopic bar code into the media's magnetic recording layer. In one sense, this is a high-tech cattle brand for media. Figure 6 shows a magnified image of a DIUM on a piece of flexible magnetic data storage media. Four copies of the same code, which is several data tracks wide, are ablated for redundancy at the disk's inner diameter.

This technology creates an unalterable media serial number that a drive's magnetic head can read, but the drive cannot replicate it with a magnetic write operation. Because the mark, or code, is ablated into the media, overwriting it with a magnetic tone does not erase it. In practice, the drive firmware implementation of a DIUM-read constitutes an AC overwrite of the mark to ensure that the encode data is ablated and genuine.

The amortized costs of this technology for a removable data storage cartridge can be as low as one cent per disk. Analogous implementations for optical phase change media are also possible.

Solid-state secure memory devices

The Iomega Peerless cartridge has a built-in secure memory device that contains 192 bytes of memory.[1] Selectable portions of this memory are fusible at the factory, providing absolute in-the-field inalterability of those locations. Access to this memory requires the drive's firmware to engage in a cryptographic challenge-and-response protocol that unlocks the device's secret key.

The secure memory device was developed for financial transaction security in smart card applications such as cash-resident debit cards. Peerless drives leverage the SMD's unalterable feature to provide a trusted source for the DRM media serial number. All Peerless drives support commands for query and return of this unique cartridge-resident media serial number.

Table 1. Relative cartridge penny tag costs.

Technology	Tag cost ($)	Detection cost ($)	Authentication means	ID states
Written media serial no.	0.00	0.00	Low	∞
Retrotag	0.03	0.75	IP	1 bit
Holographic tag (X-LSD)	0.10	1.00	IP, CI, RE	3+ bits
Latent-irradiance tag	0.07	1.00	IP, CI, SRE	4+ bits
Laser mark (DIUM)	0.01	0.00	IP, CI	∞
Smart-card IC (SMD)	0.40	0.20 to 2.00	Encrypt	∞

Abbreviations: IP: intellectual property; CI: capital investment; RE: reverse engineering; SRE: significant reverse engineering; Encrypt: encryption and other protected secret methods.

Any removable data storage drive that incorporates an SMD also can leverage this digital and physical information safe by storing an assortment of security information in it. These codes enable many interesting data security applications including robust DRM support. This SMD-embedded information would include a series of cryptographic keys and sequences as well as the cartridge's unique media serial number.

SMD-embedded codes offer an asymmetric,[2] or public-private encryption, technology that implements a *secure-pipe* delivery of the media serial number to host PC DRM applications. In a secure pipe, the media serial number is provided to the DRM software application on the drive-attached host PC in an encrypted string so that it is resilient to attacks from software shims and emulators. Content providers in the music, video, and publishing industries can use this technology to robustly tie their content to an individual removable data storage cartridge.

A cartridge-supported application of this technology stores a subset of public-key hashes on the SMD to facilitate cryptographic drive authentication of software and hardware querying devices. To support enterprise-centric data-security solutions, a second portion of the secure memory device can store encryption keys. This implementation specifically addresses concerns about employees who are intent on removing proprietary digital content. It maintains the flexibility and transportability of data within the enterprise that removable data storage cartridge technology inherently provides.

Although SMD offers significant flexibility and utility, the system architecture requires direct electrical connectivity to the removable data storage cartridge with the drive.

RELATIVE IMPLEMENTATION COSTS

Depending on the cost, technical, and market requirements of a particular removable data storage system, one system might prove more compelling than another. For these systems, it is not enough to have a low-cost tag technology; the drive-based automated detection system must be low cost as well.

Table 1 summarizes the approximate costs for implementing these penny tag systems on a removable data storage cartridge as well as in the mating drive. The detection cost listed for latent-irradiance tags assumes that a drive microprocessor is available with access to a multiplexed analog-to-digital converter. The fourth column in the table is annotated with six abbreviations that summarize the principal obstacles of tag forgery and, hence, compromise of the tag system's authentication attributes. The last column places an order of magnitude estimate on the number of identifiable different states that the tag technology and detection system can support. The infinity symbol means at least tens if not hundreds of bits.

Iomega has developed a cadre of low-cost penny tag technologies with associated low-cost automated detection systems for removable data storage cartridge identification and authentication. In particular, the latent-irradiance technique remains under most active development at Iomega.

Patents issued to Iomega on the temporal signal discrimination techniques for latent-irradiance signals make licensing this technology to third parties for other applications a possible future direction for this work. Potential applications include authentication or identification of items such as optical data storage media, aerospace or nuclear facility fasteners, factory authorized auto parts, critical construction components, and financial and business instruments such as checks and credits cards.

Field-operable detection devices for applications without leverageable in situ electronics, such as a disk drive, can be manufactured in low volumes at

costs comparable to a volt-ohm meter ($20-$100). With high volume production, such devices could reasonably cost less than $10. The actual cost would depend on the desired level of sophistication.

The higher cost of detection presently precludes using powerless RF tags in removable data storage cartridges, except in automated cartridge repository management for enterprise and government applications where information security and accountability are at a premium.

Using security technologies always invokes the issue of raising the bar relative to attack and compromise. Implementing a variety of such means in tandem further raises that bar. A good example is the implementation of more than 30 authentication features for higher denominations of US currency.

Many believe that tag technologies provide innovative physical identification and authentication methods that have a high associated overall security-to-cost quotient. The current use of these technologies in more than 350 million data storage cartridges confirms their field worthiness. ■

Acknowledgments

I thank my Iomega colleagues who read the draft of this article and made several useful comments and contributions, especially Dave Griffith, Dave Hall, Todd Shelton, and Tom Wilke. Iomega presently has patents issued or pending on all the removable data storage cartridge penny tag approaches described in this article.

References

1. F. Thomas, "Peerless DRM & Enterprise Security-Enabled Removable Data Storage Cartridges (A Discussion of Security Issues and Architectures for Removable Data Storage)," *Proc. RSA E-Security Conf. 2002*, RSA Security, 2002, www.rsaconference.net/RSApresentations/pdfs/newthu1015_thomas.pdf.
2. B. Schneier, *Applied Cryptography*, 2nd ed., John Wiley & Sons, 1996, pp. 21-46.

Fred Thomas *is chief technologist in the Advanced R&D Group at Iomega Corporation. He received an MS in mechanical engineering from Bucknell University. He holds 30 US patents. Thomas's research interests include developing technologies that make magnetic recording in removable cartridge implementations more robust, novel optical data storage techniques, low-cost sensors, and digital information security technologies and their implementation. He is a member of SPIE and ASME. Contact him at thomasf@iomega.com.*