

# SecureRF Creates New Encryption Method

The data security startup says its Algebraic Eraser is faster, requires less processing power and could be used on EPC Gen 2 Class 1 tags for protecting data transmissions.

By Mary Catherine O'Connor

Nov. 9, 2005—[SecureRF](#), a data security startup in Westport, Conn., has announced what it calls a breakthrough data security application, which can be used to protect data transmitted by passive or active RFID tags. The company plans to sell its product to RFID users in the pharmaceutical and defense industries, as well as any other users that would benefit from securing the data exchanged between RFID tags and readers, or other wireless devices. SecureRF claims its methodology, dubbed the Algebraic Eraser, is faster, requires less computing power and consumes less energy than existing methods of encrypting data transmitted by an RFID tag or reader (interrogator).

According to Louis Parks, president and CEO of SecureRF, these factors make the Algebraic Eraser encryption method well-suited for transactions requiring fast data exchange with low energy consumption and low processing power, such as RFID reads—especially for passive tags, which are powered by the interrogator. Parks says the encryption protocol can be built into chips used in EPC Class 1 Gen 2 tags, and that SecureRF is working with a major RFID tag manufacturer to launch a field trial of the Algebraic Eraser in the coming weeks. The protocol must be built into a tag's integrated circuitry and also run on the interrogator that reads it.

End users of RFID have not shown a specific, widespread demand for the ability to encrypt data used on EPC Gen 2 Class 1 tags. Parks believes this to be due, in part, to the fact that the tags, not yet widely used, are just now entering the market. SecureRF predicts demand will grow once Gen 2 tags become ubiquitous, and as specific users needing highly secure identification mechanisms for their products—such as in the pharmaceutical industry—see the benefits of the SecureRF encryption methods.

Parks says a Gen 2 chip could run the Algebraic Eraser encryption protocol because it requires less processing power—i.e., fewer logic gates on the chip—than conventional encryption methods, such as those developed by [RSA Laboratories](#) and [Certicom](#).

Ari Juels, manager of applied research at RSA Laboratories in Bedford, Mass., notes, however, that the EPC Class 1 Gen 2 standard does not include a specification for encrypting the data transmitted between tag and reader. Moreover, he says, the Gen 2 chip is designed to be so small that it seems unlikely it could handle any secure cryptography. Encryption is, in fact, envisaged for the data transmission between Class 2 EPC tags and readers. Rather than encrypting the data being transferred between EPC Class 2 tags and readers, the tags could store encrypted data, as Gen 1 and Gen 2 Class 1 tags can.

While the data encoded to any passive tag can be encrypted, that won't prevent it from being cloned. A counterfeiter could copy a tag's encrypted data to create a clone and introduce that tag's twin into a supply chain. Plus, if a party just wanted to track a tag without decrypting its data, it can still do so as long as the tag does not require the reader to authenticate itself. In order to prevent cloning or tracking, a chip needs the

built-in ability to encrypt the transmission of that data dynamically, so that the encryption changes each time it's read.

Incorporating data encryption into the chips used in passive RFID tags is not new. [Texas Instruments](#) (TI) chips use an algorithm that encrypts transmissions by the tags used in [Mobil Speedpass](#) payment fobs. And the tags used in RFID-enabled payment cards and Near Field Communication (NFC) devices, such as cell phones and PDAs, also encrypt data transmissions. But these chips have significantly more processing power than those found in passive tags used for supply chain applications, such as EPC Gen 2 Class 1 tags.

Additionally, security flaws have been identified in encryption used by the Speedpass tag (see [Attack on a Cryptographic RFID Device](#)), and researchers at the [University of Cambridge](#) and other universities say they've succeeded in breaking the encryption used to secure data transmission between an ISO 14443A RFID smart card and an interrogator.

Algebraic Eraser encrypts data, then erases the part an attacker would use to try to break the encryption. Parks says one way to visualize this is to think of a tangle of fishing line. While it is being tangled, you can see where the lines cross each other, but once those intersections are no longer visible, it is very difficult to untangle the line.

According to SecureRF, partially erasing the data reduces the amount of information generated during the encryption process, and also increases the speed at which it is encrypted. Parks claims the Algebraic Eraser is 1,000 times faster than an RSA's application for equivalent security.

Conventional encryption generates significantly more data than Algebraic Eraser, says Parks, which grows exponentially as users dial up the level of encryption desired by using longer keys. Generally, he explains, the more data you need to encrypt or decrypt, the more processing power and time your system requires.

Juels notes that on paper, what SecureRF is proposing sounds highly implausible. However, he knows the mathematicians involved in the development of the Algebraic Eraser are well known and respected. Whether it will work, he says, won't be known until the protocol is built into tags and tested.

"One of the fundamental laws of cryptography is that a system is not to be trusted without peer review and focused scrutiny," he says. "This is particularly important with RFID tags that use cryptography, because they're very hard to patch. If there is a flaw in a browser, or Microsoft finds a flaw in its operating system, it deploys a patch over the Internet. You can't do that when you have a billion little hardware devices floating around and you find a flaw [in the encryption]. I would hope that Secure RF will publish its algorithms and provide time for their review."

Parks says SecureRF is working with a number of cryptographers to perform a peer review and search for weaknesses in the Algebraic Eraser. The algorithm it uses is patent-pending. "SecureRF is a little over a year old, but its roots go back over a decade. The mathematician-cryptographers who are responsible for this breakthrough have been working in the cryptography field for more than a decade and have invented the genesis of this new security platform," says Parks.

SecureRF is planning initially to market the Algebraic Eraser to RFID and smart card applications. However, Parks says the product is well-suited for any applications requiring fast and secure data encryption, such as WiMax (802.16), an emerging standard for high-bandwidth wireless networks. It could also be used, he says, to secure data sent via satellite communications and cell phones.