



News Release

SecureRF's Security Solution for RFID Recognized by the American Mathematical Society

First RFID tag to feature security and temperature sensor to debut March 2007

WESTPORT, CT, March 12, 2007 – SecureRF Corporation, a leading provider of secure radio frequency identification (RFID) solutions, is pleased to announce the publication of their method for strongly securing RFID tags in a book by the American Mathematical Society (AMS). The AMS has published SecureRF's peer-reviewed technical paper, which describes the company's breakthrough Algebraic Eraser™ – the world's first linear-based security protocol. SecureRF uses the Algebraic Eraser in conjunction with industry standard security protocols on their line of secure RFID tags to actively authenticate and protect reader-tag communications.

The publication of the paper, entitled "Key Agreement, The Algebraic Eraser and Lightweight Cryptography," provides important validation of the methods used by SecureRF. The paper is published as the first chapter in "Algebraic Methods in Cryptography," Vol. 418 of the AMS' peer-reviewed *Contemporary Mathematics* series. This series is a collection of high quality, refereed proceedings written by recognized experts in their fields in order to maintain high scientific standards.

"The Algebraic Eraser has enabled us to become the first company to put active security protocols on EPCglobal Gen 2 tags, something many in the industry have said could not be done," said Louis Parks, co-founder and CEO of SecureRF. "The submission of our methods to world-leading organizations like the AMS is part of our ongoing development and peer review process, and the current response supports the validity of the Algebraic Eraser as a solid solution for securing small devices like RFID tags."

The paper was authored by world-class mathematicians and cryptographers Drs. Anshel, Anshel and Goldfeld, who developed the Algebraic Eraser algorithm, and Dr. Lemieux who worked to test and validate their design.

Dr. Michael Anshel, co-founder and director of SecureRF, is a co-author of four related patents, an advisor to the National Institute of Standards and Technology (NIST) Advanced Technology Program, and professor in Computer Science at the City College of New York.

Dr. Dorian Goldfeld, co-founder and director of SecureRF, is a Sloan fellow and a Cole Prize winner in number theory, has been a recipient of National Science Foundation grants every year since 1976 and is a professor of mathematics at Columbia University.

Dr. Iris Anshel, co-founder and chief technology officer of SecureRF, has published extensive research in the field and has experience in the commercialization of security technology as a co-founder of Arithmetica.

Traditional cryptographic functions used by virtually all commercial vendors today have one thing in common—they all run in quadratic time. That is, they require the multiplication and division of large numbers to deliver secure results. These methods require computational levels that grow exponentially as the cryptographic key size increases, requiring system resources that often outstrip the processing limits found on RFID tags or embedded computing platforms. In contrast, SecureRF's Algebraic Eraser is the world's first cryptographic algorithm to have computational requirements that increase in direct proportion ("linearly") to the key size, thus running many orders of magnitude faster and more efficiently than traditional systems. This allows SecureRF to deliver security where no other methods can today.

The Algebraic Eraser can be used directly on passive, semi passive/active, and active RFID tags along with other small, resource-constrained computing platforms. A full range of asymmetric (public key) and symmetric (private key) protocols are available for authentication and data protection applications.

SecureRF's LIME Tag™ with Onboard Security™, the company's first [secure RFID tag](#), arrives in March 2007. This EPCglobal Gen 2 compliant RFID tag will also feature a temperature sensor function for item-level cold chain management.

About SecureRF

SecureRF Corporation provides secure radio frequency identification (RFID) solutions for high value asset tracking, monitoring and anti-counterfeiting applications in the pharmaceutical, defense and homeland security sectors. The company's technology, based on a breakthrough in cryptography that is lightweight yet highly secure, provides authentication and data protection security for passive, semi-active and active RFID tags that meet both EPCglobal and ISO standards. SecureRF solutions provide additional features for [cold chain management](#) and can also be licensed as a software toolkit, a core, or a chip, addressing a wide range of applications and environments. SecureRF is a member of EPCglobal and AIM Global. More information about SecureRF can be found on its Web site at www.SecureRF.com.

About American Mathematical Society

Founded in 1888 to further mathematical research and scholarship, the American Mathematical Society fulfills its mission through programs and services that promote mathematical research and its uses, strengthen mathematical education, and foster awareness and appreciation of mathematics and its connections to other disciplines and to everyday life. "Algebraic Methods in Cryptography," Vol. 418 of the AMS' peer-reviewed *Contemporary Mathematics* series can be purchased at the AMS Bookstore at <http://www.ams.org/bookstore?fn=20&arg1=conmseries&item=CONM-418>.