



News Release

SecureRF Granted U.S. Patent for Secure Communications Method Targeting Sensors and Wireless Platforms

Cryptographic Solution Suitable for Embedded or Low Resource Computing Devices

NEW HAVEN, CT, June 16, 2010 –SecureRF Corporation today announced that the United States Patent and Trademark Office has granted the company U.S. Patent 7,649,999 for the world’s first cryptography method to run in linear time. The patented algorithm provides a key agreement protocol and a method for generating a secret key to facilitate secure communications. The algorithm is computationally hard to reverse, while rapidly computable, enabling it to run on devices with very low computing resources. These methods can be used to secure users, sensors, networks, or machine-to-machine systems, like the Smart Grid, where stronger authentication and security will be critical to public implementation.

“This patent broadly covers the foundation of our methods, known as the Algebraic Eraser™,” said Louis Parks, SecureRF’s CEO. “Cryptographic protocols based on the Algebraic Eraser are thousands of times smaller and faster than any currently available security methods and we can provide both asymmetric and symmetric solutions.”

Sensors, radio frequency identification (RFID) tags, and other embedded, resource-constrained or performance-sensitive devices do not protect users from unauthorized reading, copying, or tracking due to the lack of adequate security. The security methods protected under this patent address this issue and are also applicable to high value asset tracking, contactless payment systems, wireless sensor networks, Smart Grid microcontrollers, and Defense and Homeland Security border security systems.

The American Mathematical Society published details on how the Algebraic Eraser’s key agreement protocol for public key cryptography is suitable for low resource devices, such as RFID tags, in their peer-reviewed book [Algebraic Methods in Cryptography](#). The paper can be found in the section titled *Key agreement, the Algebraic Eraser™ and Lightweight Cryptography*. SecureRF also recently published a white paper titled *An Introduction to Cryptographic Security Methods and Their Role in Securing Low Resource Computing Devices: An Overview of Public-key Cryptosystems based on RSA, Diffie-Hellman and the Next Generation of Public-key Cryptographic Security for Low-Resource Computing Devices - the Algebraic Eraser™*. Both papers are available on SecureRF’s web site (<http://www.securerf.com/white.shtml>).

The inventors of this method are SecureRF co-founders Dr. Michael Anshel, Dr. Dorian Goldfeld and Dr. Iris Anshel.

Contact: Joanne Kelleher, SecureRF Corporation, 203-227-3151 ext 1302, JKelleher@SecureRF.com

Dr. Michael Anshel is a security thought-leader and world-class mathematician with expertise in the field of cryptography. Dr. Anshel has authored and co-authored numerous papers in the area of public-key cryptography, is the co-inventor of four patents in the area of cryptography, zeta-one-way functions, and braid group and has received numerous fellowships and honors. He is a professor in the Department of Computer Science at The City College of New York.

Dr. Goldfeld is a world-class mathematician who has published over 50 papers and lectured internationally on a wide range of cryptographic topics and methods including applications of elliptic curves, quadratic fields, zeta functions, public-key cryptography, and group theoretic approaches to public-key cryptography. In 2009 he was inducted as a Fellow of the prestigious American Academy of Arts & Sciences. He is the co-inventor of three additional patents in the areas of multistream encryption systems, high-speed cryptography, and cryptographically secure algebraic key establishment protocols based on monoids. He has been a professor in the Faculty of Mathematics at Columbia since 1985.

Dr. Iris Anshel, SecureRF's Chief Scientist, is an accomplished mathematician and cryptographer. In addition to extensive research and publications, Dr. Anshel has experience in the commercialization of security technology. As a co-founder of Arithmetica, she was responsible for documenting methods for commercial deployment of new cryptography protocols including the AAG Braid Group Cryptosystem and supported sales and business development activity.

About the Patent

The company's patent, titled "Method and apparatus for establishing a key agreement protocol," can be viewed at <http://patft.uspto.gov/> by searching for patent number 7,649,999.

About SecureRF

SecureRF Corporation provides security solutions for embedded systems and radio frequency identification (RFID) technology used in high value asset tracking, monitoring and anti-counterfeiting applications in the pharmaceutical, food, defense, homeland security and other sectors. The company's technology, based on a breakthrough in cryptography that is very computationally efficient yet highly secure, provides strong authentication and data protection. SecureRF's LIME Tag™ is a secure, battery-assisted, passive RFID tag, which is EPCglobal Gen 2 compliant, with optional sensors that provide cold chain management functionality. SecureM2M™, a security software development kit (SDK), provides strong authentication and data protection solutions for low-resource platforms such as microcontrollers and integrated circuits. More information about SecureRF can be found on its Web site at www.SecureRF.com. SecureRF's insights into RFID Security can be found on its blog at www.SecureRF.com/RFID-Security-blog/.

###

SecureRF, LIME Tag, SecureM2M and Algebraic Eraser are trademarks of SecureRF Corporation.