

# Authentication and Security

New encryption techniques promise to make the use of RFID applications more secure, increasing the public's trust in the technology.

By Behnam Jamali

April 23, 2007—As RFID becomes more ubiquitous in every sector of industry, commerce and services, it will have a huge impact on the way that business owners run their companies. But companies will not be able to reap RFID's myriad benefits if the technology meets widespread resistance from the public due to its lack of security and privacy.

Today, RFID systems are not as secure as they need to be, because any reader can access any tag's data without the user's knowledge. The newest tags, those that comply with the EPC Class 1 Generation 2 standard, are likely to predominate in supply chains. But these tags will respond to any reader that interrogates them. The concern is, how do you keep an unauthorized person from interrogating the tags?

To build trust in RFID applications, we need to ensure that tags can be read only by authentic readers. Authentication is required at each of several interfaces within an RFID system: tag to reader, reader to tag, and reader to back-end database. In addition, we need to secure the data stored on the RFID tags.

Encryption techniques can be used to achieve these goals. But the existing (computationally intensive) encryption techniques are not suitable for RFID systems. Any proposed system must provide mutual authentication for both tags and readers, offering a means to secure the information stored on the tags while minimizing the tags' complexity and cost.

At the [Auto-ID Lab at the University of Adelaide](#), we are working to address this problem by developing novel encryption mechanisms based on the concept of lightweight cryptography. The aim of this research is to build security and reliability into an RFID system, and increase trust between users and providers.

Lightweight cryptography encompasses encryption algorithms, modes of encryption and key-management schemes that require reduced levels of circuit area and power usage and can be deployed without substantial network infrastructures. That is especially important for an RFID system with extremely constrained parameters, such as size, complexity, price, memory, communications bandwidth, device lifetime and power consumption.

Our goal is to strengthen RFID security by implementing lightweight cryptography that is secure, fast and efficient. This will provide government and industry with ideas and concepts they can use to secure RFID systems as they start to leverage the potential offered by the EPCglobal Network within the supply chain.

**RELATED\_ARTICLES** This research is in its preliminary stage and will be completed within the next two years. After completion, it will be submitted to the EPCglobal Software Action Group for approval. Our novel encryption systems will be available to the public through Auto-ID Lab white papers and seminars.

RFID is only in its infancy, and legislation and regulations related to its use in authentication systems are immature. While authentication may not be an important issue in today's basic RFID systems, over time, security requirements will expand. We'll be able to meet such expansion easily by increasing the strength of the encryption engine.

*Behnam Jamali is associate director of the Adelaide Auto-ID Lab in Australia.*

Copyright ©2005 RFID Journal, Inc. All Rights Reserved