SECURITY IN LOW RESOURCE ENVIRONMENTS

SECURERF WHITE PAPER

The "discovery" of a decades old technology is now promoted by many as the "Next Big Thing". This discovery, Radio Frequency Identification (RFID), covers a broad range of systems and methods including tags, readers, software and related services. Regardless of the form that this automatic identification technology takes, it promises to change the way we collect information and monitor everything from hospital patients and livestock to library books. Even as we debate how ubiquitous this technology will become, an estimated 50 million Americans are already using RFID technologies daily in the form of car keys, payment systems, and toll devices.

The U.S. government is a leading adopter of RFID technology. Their use of RFID goes back over 60 years to World War II where it was used in Identification Friend or Foe systems and the Cold War sparked extensive developments in the signal intelligence sector. Homeland Security's current concerns and mission is made to order for RFID applications and we can see this demonstrated in the significant effort to implement electronic passports equipped with embedded RFID tags. The FDA is also looking to RFID to secure the pharmaceutical supply chain and eliminate the estimated $32 Billion in annual losses currently attributed to counterfeit drugs.

The ability to improve processes, track items effortlessly, and provide near real-time information on assets would seem to make RFID a "…can't-miss, high-return technology…" according to Rothfeder (August, 2004). However, growing concerns over the privacy and security of all this readily-available data may stand in the way of RFID's "hockey stick" adoption charts. These apprehensions are based on well reported issues.

"New 'contactless' payment systems present new opportunities for fraudulent activity that are far less obvious…" according to Chasney (August, 2005). Hancke, at the University of Cambridge, has demonstrated 'borrowing' data from a smart card using the current RFID payment system standard without the victim ever knowing. Grunwald and Wolf released RFDump at the 2004 BlackHat conference in Las Vegas (eWeek 2004). This open-source tool allows anyone to read RFID tags based on ISO 15963 and 14443 standards. The same standards used in some smart-card financial platforms. And in an exercise that made it to the pages of the New York Times, a group of students at John Hopkins University successfully captured and used "secure" RFID data to start cars and purchase gasoline (NY Times, March 2005).

To address these concerns the cryptographic community has proposed several approaches to deal with security but the low-resource single-chip platforms used for most RFID tags has presented a significant challenge. Some proposed approaches have included Blocker Tags, Minimalist Cryptography and even Elliptic Curve Cryptography employing special Very Large Scale Integration (VLSI) circuitry. As innovative as many of these approaches are, issues and weaknesses in each approach have prevented any real adoption. If RFID is to attain its predicted title as the "disruptive technology" of this century then strong security functions are clearly needed to support the privacy requirements of today's user.

WHY CURRENT PUBLIC KEY PROTOCOLS CANNOT ADDRESS SECURITY ISSUES IN LOW RESOURCE ENVIRONMENTS

The earliest cryptosystems in practical use are, in modern parlance, termed symmetric. In a symmetric cryptosystem there is only one secret key which is used for both encryption and decryption. For example, in Julius Caesar's cipher, we encrypt an English word by offsetting the alphabet by n letters. Here n is the secret key. If n = 3, then A is replaced by D, B by E, C by F etc., so after encryption, the word HELLO becomes KHOOR. Anyone possessing the secret key n = 3 can decrypt by shifting back three letters. In a symmetric cryptosystem, the method used of encrypting and decrypting is the same, hence the term symmetric. Any individual in possession of the secret key can encrypt and decrypt messages at will. There are many known deficiencies in symmetric encryption, particularly in a local network, but because this method is computationally efficient it is used in many commercial applications like 802.11 WiFi networks. Perhaps the biggest problem to arise is that if the secret key is shared by a large number of users there is a great danger that it can get into the hands of an intruder, thereby compromising all confidential information. One solution to this problem is to routinely change and redistribute keys. But how do you transport the secret key from the sender to the recipient securely and in a tamperproof fashion? This leads to another significant problem - the generation, transmission, and storage of secret keys, which is called key management.

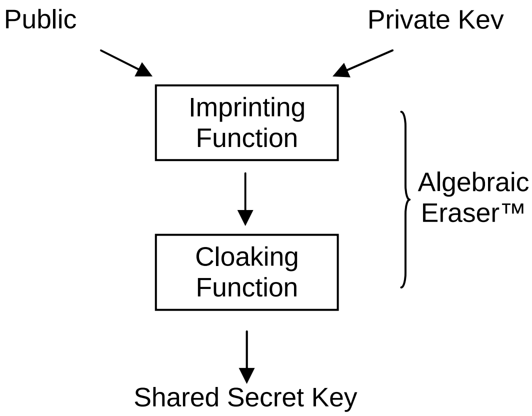
The most important solution to the key management problem was obtained by Whitfield Diffie and Martin Hellman in 1976 ([Diffie – Hellman, 1976]) who introduced public key cryptography. In a public key protocol there is a public key (known to everybody) and a protocol (known to everybody). There is also a private key which is in the sole possession of the intended recipient. Anyone can send an encrypted message by just using the public key and the public protocol, but the message can only be decrypted by someone who is in possession of the private key. It is not necessary to know the private key in order to encrypt a message! In practice, the public key protocol is used to securely distribute keys, thereby, solving the key management problem.

There are several current public key cryptosystems in wide commercial use including RSA, Diffie-Hellman, and Elliptic Curve Cryptography (ECC). Each of these systems has as its foundation the mathematical field of number theory. The security of these systems is based on the hardness of factoring, the discrete log problem in finite fields, and the discrete log problem in elliptic curves, respectively.

The above public key protocols cannot, and *never will* address the security issue in low resource environments due to their computational foundations. Each of these protocols run in quadratic time and each are inherently slow because they require the multiplication and division of very large numbers. ECC does run faster than RSA but still requires long and time consuming computations on geometric objects (elliptic curves). These methods simply cannot fit on a small RFID tag (e.g. EPCglobal Class 1 Generation 2 tag) without compromising security. An RSA or Diffie-Hellman key transfer (1024 bits) requires about 1000 repeated squarings and divisions of a 1024 bit number. Just one such squaring and division could take several seconds on a low resource chip. Clearly, 1000 such operations cannot be performed in feasible time on a processor with very few gates and low memory storage capability. The ECC cryptosystem can reduce the running time of an RSA computation by as much as 3 to 10 times, but it is still not possible to fit such a system on a low cost processor. If RFID systems are going to provide the needed authentication, data protection, and repudiation at the tag-reader level then a new methodology will clearly be needed.

THE ALGEBRAIC ERASER™: A BREAKTHROUGH SOLUTION FOR THE FUTURE

In order to work within the space and time constraints of a low resource environment the SecureRF team has developed the ground breaking concept of the Algebraic Eraser$^{\text{TM}}$ *(AE).* The *AE* is the engine within the SecureRF security solutions that supports a wide range of crypto functions including authentication, data protection, and repudiation. An asymmetric cryptosystem using the AE protocol would function as follows: a public key first leaves an imprint on a private key, and then the result of this process is put through a cloaking function. The security of the system lies in the fact that this process is not feasibly reversible, i.e., the required data which would allow for the system to be reversed (and hence broken) has been effectively erased by the AE process itself.



Traditional asymmetric cryptosystems have had their mathematical foundations either in classical number theory, finite fields, or elliptic curve theory. A relatively new branch of modern mathematics is infinite group theory which is the study of a group of infinitely many reversible operations such as the braiding of strings. A significant feature of the Algebraic Eraser™ is that it is based on the dynamic synergy between two distinct mathematical theories:

- *infinite group theory*
- *number theory.*

By bringing two fields together in this revolutionary manner, the security of the cryptosystem is enhanced by having a broader foundation. The complimentary nature of these combined theories eliminates corresponding weaknesses in each field resulting in fewer attack points. Infinite group theory brings a new security foundation that is akin to the fact that an ordinary fishing line can get entangled in a few seconds while it may take hours to untangle.

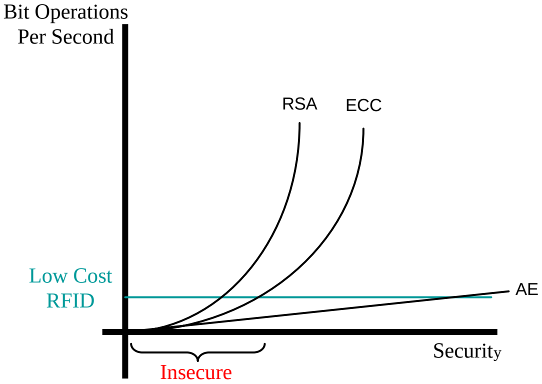
The SecureRF cryptosystem in its most basic form allows for a transmitter and receiver in a low resource environment to have a communication/exchange over a public channel after which the transmitter and receiver are both in possession of a shared secret key that can be used for further cryptographic applications. An adversary eavesdropping on the open public channel will be unable to determine the shared secret key due to the cloaking properties of the AE.

The AE can be used for authentication and encryption as follows. Assume we have a local network with many users. Each user will be in possession of a public key (known to everybody and published in a directory) and a private key known only to the user. A message can be sent to a particular user by encrypting the message with the public key of the user. Only the particular user can decrypt the message, because only he (or she) has possession of the required private key. The same process can be used for authentication.

The AE is the world's first protocol to run in linear time in the key length and use very little memory because it is erasing information as the algorithm proceeds. This is opposed to traditional asymmetric cryptosystems which run in quadratic time and require a lot of storage in order to perform multiplication and division of very large numbers. In practice, this means the running time of the AE protocol is thousands of times faster than traditional asymmetric cryptosystems, and it can perform authentication and encryption in real time on extremely small low cost processors such as inexpensive RFID tags.

The *AE* protocol can be performed in approximately 500,000 elementary bit operations to create a shared secret key of 512 bits with a running time which is several thousand times faster than the running time for the creation of an equally secure RSA or Diffie-Hellman key. The running time is also several hundred times faster than the protocol for the creation of an ECC key. The only attack known on this system, at present, is a brute force attack which is analogous to trying every combination on a combination lock. Such a brute force attack requires years of computer time. The extraordinary gain in computational expense makes the SecureRF cryptosystem ideal for low resource computing environments.

The following chart gives comparisons of the running times (in bit operations per second) between RSA, ECC, and *AE* in terms of security level. The blue line represents the very slow running time capability of low cost RFID chips. Note that both RSA and ECC can only work on low cost RFID in an insecure mode – if at all. The *AE* protocol, on the other hand, runs in linear time and can operate securely on a low cost RFID chip.



STRATEGIC ADVANTAGES

The incredible speed and efficiency of the Algebraic Eraser™ makes it a breakthrough innovation in cryptography. Some of its important strategic advantages and avenues of applications are:

- *Algorithms run in linear time with respect to key length and employ highly nonlinear operations in a non-commutative infinite algebraic structure making for extremely high security.*

- *Disposable keys which can be created as needed.*

- *Real time authentication in extremely low resource environments.*

- *SecureRF encryption technologies employ novel algebraic methods so there is no need for heroic efforts on the part of VLSI designers to achieve performance bounds at prohibitive costs.*

- *SecureRF technology can be used to produce highly efficient and low cost PRNG's (pseudo-random number generators), hash functions, and stream ciphers.*

- *The first linear time public key cryptosystem that can fit on a processor of 8K ROM, 256 bytes of RAM and 256 bytes of non-volatile memory, which can be clocked over a wide range and has a 1MHz "sweet-spot" in the power consumption vs. computational throughput tradeoff.*

As the promise of RFID grows exponentially so does the demand for good security methods that can support the significant privacy concerns this technology raises. Many of the initial adopters; the Department of Defense, the FDA, the financial sector, and Homeland Security all have obvious needs for security in their implementations. As consumers come to understand the power and capability of RFID we can now see their demands to address privacy issues further promoting the need for good security. Until now, the industry has unsuccessfully turned to 20 year old commercial protocols to address these security needs and we have seen that they simply can not operate in the low-resource world of RFID. SecureRF, and the Algebraic Eraser™, offers the first real cryptographically strong solutions that can uniquely deliver the safety and security demanded by the government and commercial implementations now underway.

.

REFERENCES

[Chasney 2005] J. Chasney, *Are Contactless Payment Cards Tickets to Wholesale Fraud?*, CIO Insight (August 18, 2005) Available at www.cioinsight.com/print_article2/0,1217,a=158341,00.asp

[Diffie – Hellman, 1976] W. Diffie, M.E. Hellman, *New directions in cryptography*, IEEE Trans. Inform. Theory, IT-22, 6, (1976), pages 644-654.

[Garfinkel-Juels-Pappu 2005] S.L. Garfinkel, A. Juels and R. Pappu, *RFID Privacy and Security: An Overview of Problems and Proposed Solutions*, IEEE SEcurity and Privacy, Volume 3 Number 3 (May/June 2005), pages 34-43.

[Hachman 2004] M. Hachman, *RFID Hack Could Allow Retail Fraud*, eWeek (July 29, 2004). Available at www.eweek.com/print_article2/0,2533,a=132404,00.asp

[Hancke 2005] G. Hancke, *A Practical Relay Attack on ISO 14443 Proximity Cards*, University of Cambridge Manuscript (February 2005). Available at www.cl.cam.ac.uk/gh275/relay.pdf

[Rothfeder 2004] J. Rothfeder, *What's Wrong with RFID?* , CIO Insight (August 1, 2004) Available at www.cioinsight.com/print_article/0,1406,a=133044,00.asp

[Sarma 2005] S. Sarma, *A History of EPC*, in RFID *Applications, Security and Privacy,* edited by S. Garfinkel and B. Rosenberg, Addison Wesely (2005), Chapter 3, pages 37-55.

[Schwartz 2005] J. Schwartz, *Graduate Cryptographers Unlock Code of 'Thiefproof' Car Key*, New York Times (January 29, 2005). Available from nytimes.com at www.nytimes.com/2005/01/29/national/29key.html?adxnnl=1&adxnnlx=1107268998