Design Challenges for Security and Privacy in RFID

Lawrence Leinweber, Christos Papachristou, Francis G. Wolff, Francis L. Merat

Department of Electrical Engineering and Computer Science

Case Western Reserve University

Introduction

The Problem: A shopper using RFID and Barack Obama have a security problem. Obama's problem was solved when his BlackBerry was replaced with a more secure device. Now, even if his communications are intercepted, they cannot be decoded because of encryption technology. The President's need for security is apparent. A customer using RFID has a similar problem. The tag she carries will send information that can be used to track her movements. Secure communication technology can protect her as it protects the President. But the National Security Agency can spend more money to protect the President's BlackBerry than we can spend on a shopper. Providing world class wireless security on a consumer's budget is the subject of this research.

RFID technology is sufficiently mature that its economic potential is clear. RFID is still a fertile research field, offering many opportunities for study in computer engineering. We have several research thrusts in RFID security:

1. A new cryptography-based protocol for privacy in RFID systems
2. Efficient architectures for elliptic curve cryptography processors for RFID
3. A methodology for designing power management circuits in small, passively powered systems.

Background: RFID systems consist of tags and readers. Tags are small devices attached to objects in the field. Readers are larger systems connected to the data processing infrastructure. The basic operation is one in which the reader wirelessly queries the tag for identification and other information about the object. Typically, there are thousands or millions of tags for every reader, so the cost and complexity of the tags characterize the system. Tags range in complexity from EAS at the low end to smart cards at the high end. EAS devices are used to discourage theft. An EAS tag is a tuned circuit that can be detected by a reader at the exit of a shop. After authorization, the tag is programmed to detune the circuit, encoding one-bit of information. A smart card is a credit card or loyalty card with embedded electronics which may include an eight-bit microprocessor. A card can identify its owner, carry volatile information such as an account balance and provide encryption to protect the owner from unauthorized readers.

Our Research: Building an RFID tag to transmit identification is relatively straightforward; however, this has implications for privacy. RFID provides the benefit of an economical remote sensing capability for data processing systems. This benefit can be abused. As semiconductor fabrication costs decrease, more computing power can be put on tags without increasing costs. The higher end functionality of smart cards can be incorporated into RFID tags to prevent them from providing information to unauthorized readers. To get this security capability, tags require a ***secure protocol***. We found that a public-key cryptographic system was necessary. In the RFID environment of limited resources and limited throughput requirements, an elliptic curve ***cryptographic processor*** is ideally suited; nevertheless, cryptography requires a great deal of energy. A passive RFID tag receives power from its antenna. We developed a ***power management*** methodology to ensure that power is efficiently delivered from the antenna is to the digital circuitry.

Q: What does a Woman's RFID fuel tag have in common with Barack Obama's BlackBerry?

A: Both use Wireless Communications

Both have a security problem

We are working on Solutions

Conclusions

The Solution: RFID tags provide a unique capability because they can be read without a line of sight. But this benefit is a double-edged sword. Steps must be taken to prevent unauthorized reading. By use the computing capabilities of tags, we have made progress on three fronts.

Our ***secure protocol*** defines an efficient method for storing, communicating and processing encrypted messages. For RFID product identification tags, individuals maintain their privacy. Using this protocol, tags do not identify themselves to rogue readers. The protocol is efficient implementing read and change-owner operations in a minimum number of encryption operations, message words and tag registers.

Our ***cryptographic processor*** designs reduce the cost of manufacturing by reducing circuit area. The designs also improve tag range by reducing processing time and power. These improvements were found by applying many techniques including an analysis of data flows for the elliptic curve cryptography formulas and by modifying the formulas. Our *R5* processor design uses fewer registers than any in the literature. Our *R6* design minimizes the number of Galois field multiply operations. Among processors that minimize multiplies, the *R6* uses the fewest registers.

Finally, our ***power management*** techniques ensure that energy from the antenna is used flexibly and efficiently by the power-hungry processor. We recommend logic that operates super- and subthreshold, so tags are still responsive when power is limited. Self-timed logic automatically adapts clock speed to changing power availability. Finally, using an adaptive voltage multiplier, antenna impedance can matched to the digital circuitry across the full range of available power.

Our research and the work of many others in the area of computer engineering is improving wireless security so that users can live more conveniently and work more efficiently whether they are buying gas or leading the free world.

Learn More: The following books and papers give more detailed information on the topics presented here.

S. Garfinkel & B. Rosenberg (Eds.), *RFID Applications, Security, and Privacy*, Addison-Wesley, 2005.

K. Finkenzeller, *RFID Handbook: Fundamentals and Applications in Contactless Smart Cards and Identification*, 2nd Ed., John Wiley & Sons Ltd., 2003.

L. Leinweber, F.G. Wolff, C. Papachristou and F.L. Merat, "A Minimal Protocol with Public Key Cryptography for Identification and Privacy in RFID Tags," *IEEE Int. Symp. on Signals, Circuits and Systems*, 2009.

A.P. Fournaris and O. Koufopavlou, "Hardware Design Issues in Elliptic Curve Cryptography," *Wireless Security and Cryptography, Specifications and Implementations*, N. Sklavos and X. Zhang (Eds.), CRC Press, 2007.

A. Raychowdhury, B.C. Paul, S. Bhunia and K. Roy, "Computing with Subthreshold Leakage: Device/ Circuit/ Architecture Co-Design for Ultralow-Power Subthreshold Operation," *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*, Vol. 13, 2005.

L. Leinweber, "Improved Cryptographic Processor Designs for Security in RFID and Other Ubiquitous Systems," Ph.D. dissertation, Case Western Reserve University, 2009.

Solution #1: Secure Protocol

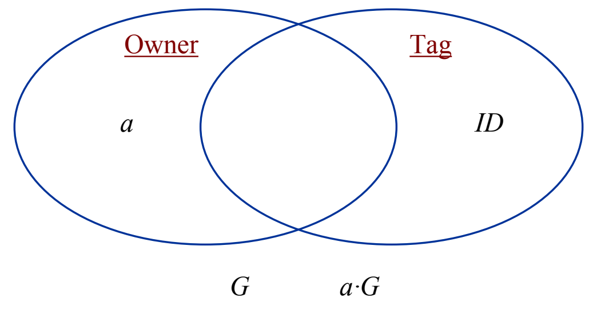

Fig. 1: Before Read Operation

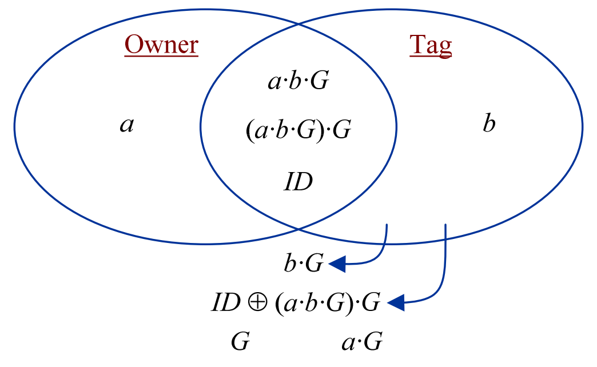

Fig. 2: After Read Operation

Read Operation: The tag generates a nonce, b, performs three encrypts $b{\cdot}G$, $b{\cdot}(a{\cdot}G)$ and $(b{\cdot}a{\cdot}G){\cdot}G$, using owner public key, $a{\cdot}G$, and sends two words, $b{\cdot}G$ and $\mathrm{ID}\oplus(b{\cdot}a{\cdot}G){\cdot}G$. The owner encrypts $a{\cdot}(b{\cdot}G)$ and $(a{\cdot}b{\cdot}G){\cdot}G$ using private key, a, and recovers the ID:

$$\mathrm{ID} = \mathrm{ID}\oplus(b{\cdot}a{\cdot}G){\cdot}G\oplus(a{\cdot}b{\cdot}G){\cdot}G$$

An intruder can't get $a{\cdot}b{\cdot}G$ or $(a{\cdot}b{\cdot}G){\cdot}G$ and therefore the ID remains secure.

The Need: Many designs have been proposed that make tags simple by moving as much computational effort as possible to the data processing infrastructure. But this approach requires a database system in which the records of every tag are available during every read operation.

We have considered the requirements of a protocol for identification and privacy in a system of small devices, especially RFID tags, with minimized tag storage, communication and encryption, while back-end database support for each tag is not required.

The Protocol: We propose a protocol in which identification is provided while privacy is maintained. The protocol requires a minimal amount of public key cryptography on the tags so that no per-tag back-end database records are required. The protocol is appropriate for RFID tags and other small, ubiquitous systems where the cost of individual devices is small and volume is high.

The proposed protocol requires the smallest number of encrypted (word) messages, encryption operations and word registers on the tag to provide identification and maintain privacy.

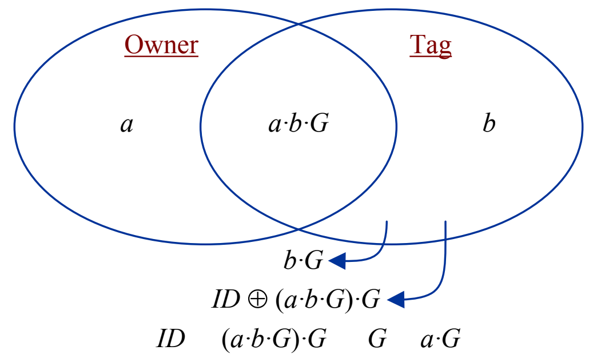

Fig. 3: Before Change-Owner Operation

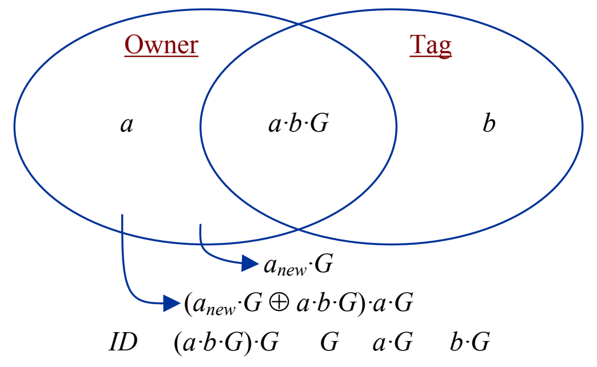

Fig. 4: After Change-Owner Operation

Change-Owner Operation: After a read operation, the owner can combine $a{\cdot}b{\cdot}G$ and new owner public key, $a_{new}{\cdot}G$, and encrypt with $a{\cdot}G$ to form the signature:

$$(a_{new}{\cdot}G \oplus a{\cdot}b{\cdot}G){\cdot}a{\cdot}G$$

The owner sends this and $a_{new}{\cdot}G$. The tag repeats these steps, verifying the signature, and updates the owner. An intruder can't get $a{\cdot}b{\cdot}G$ even if ID is known so the operation is secure.

Solution #2: Cryptographic Processor

***R6* Processor:** This data flow diagram of a straightforward implementation of the Lopez-Dahab formulas indicates that no more than five registers and six Galois field multiplies are required. The six register version of the processor, *R6*, requires one for the multiplier product and five for elliptic curve values, in six multiply operations per key bit.

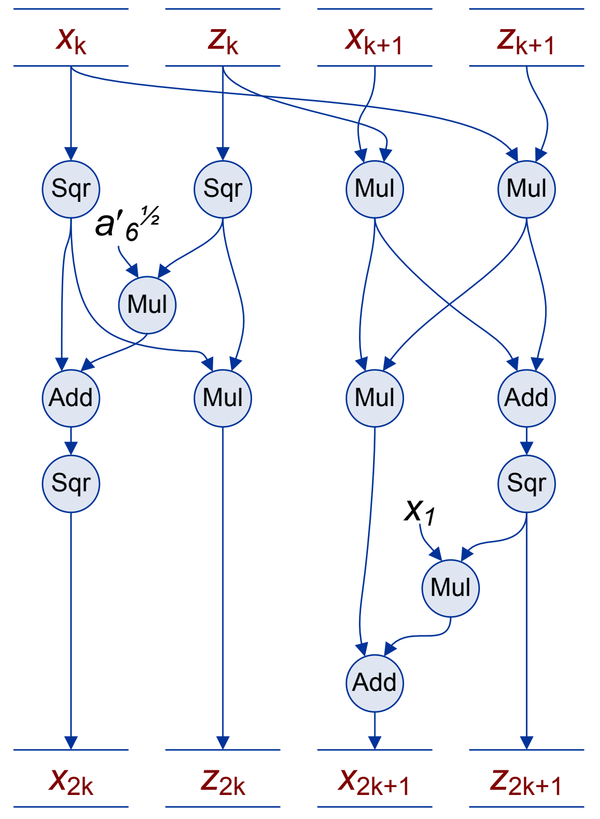

Fig. 5: *R6* Processor Data Flow

Improved Processor Designs: The contribution of this work is the integration of elements of elliptic curve processors. The resulting designs show a 12%-20% area and a 31%-45% time improvement over those in the literature.

These processors perform elliptic curve point multiplication and produce an affine abscissa for a small number of circuit elements and clock cycles. The processors do not sacrifice security for performance. The key has minimal influence on datapaths and no influence on the order of instruction execution.

The proposed designs include a new bus organization to minimize datapaths and specialized logic for key and inversion control. The proposed designs uses few registers including those for the Galois field ALU. One design requires a total of six full width registers and an alternative design requires five registers, plus a small number of flip-flops to support control logic. Register initialization is controlled by microcode avoiding special hardware.

The designs mesh Lopez-Dahab addition and doubling, Montgomery ladder multiplication and Itoh-Tsujii inversion in efficient architectures.

***R5* Processor:** This data flow diagram for the modified version of the Lopez-Dahab formulas requires five registers but the fifth register is also the multiplier product. This version requires seven Galois field multiply operations. The five register version of the processor, *R5*, requires five registers and seven Galois field multiply operations per key bit.

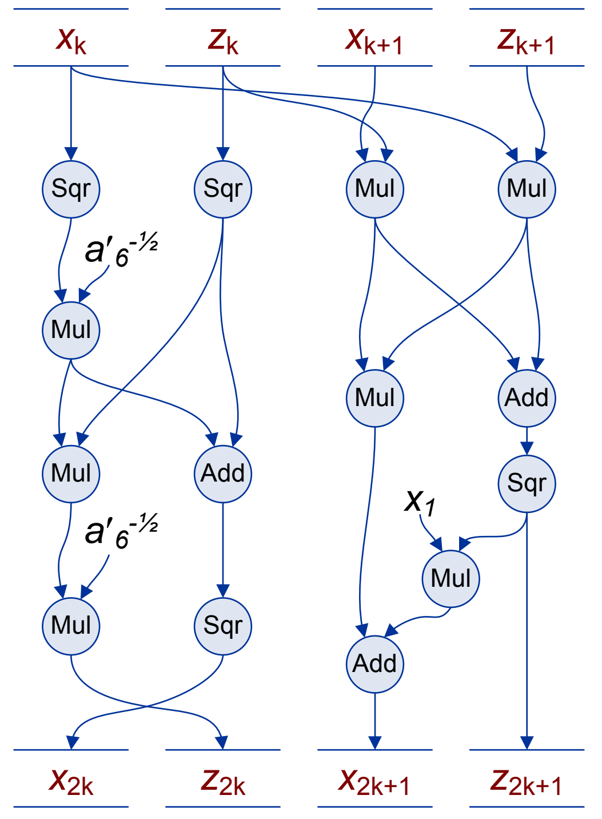

Fig. 6: *R5* Processor Data Flow

Solution #3: Power Management

Power for Cryptography: To make the best use of the fluctuating power available from the antenna, the digital circuitry can be designed to use power flexibly. The logic can be run at lower voltages, below even the threshold voltage. But as power decreases, delay increases. Clock speed can track with voltage by using self-timed logic, with a ring oscillator of the same technology.

In order to marry self-timed subthreshold logic with a power-supplying antenna, an impedance matching network is required; however, the impedance of the logic is not fixed because of the varying supply voltage and clock rate. Supply voltage affects average switching current of CMOS logic in a non-trivial way, affecting impedance. Also, because the circuit is self-timed, the ratio of time spent in dynamic to static operation is independent of the supply voltage. This was studied to the subthreshold regime.

Two circuits were studied in simulation. One circuit was a chain of four inverters. The other circuit studied was a small *R6* elliptic curve processor. The results for the inverter chain are shown in the figure. Processor results were similar. For this technology node, v_{th} is 0.45 V for NMOS and 0.60 V for PMOS.

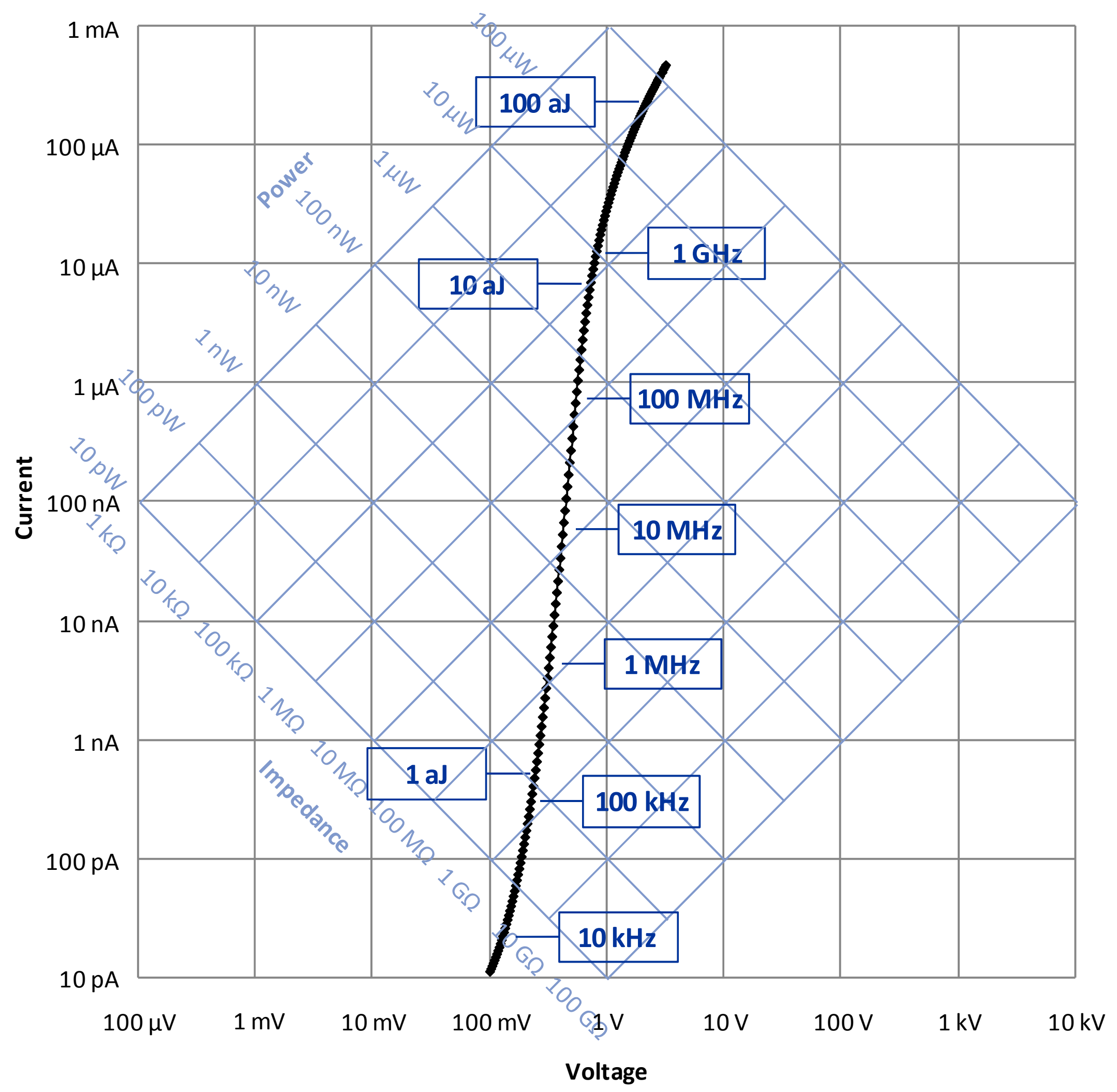

Fig. 7: Current vs. Voltage for a Chain of Four Inverters at Maximum Frequency