ISSN:2320-0790

An International Journal of Advanced Computer Technology

INTENSIFYING THE SECURITY IN RFID SYSTEMS

Jose Reena K#1, Prof. P.Anjugam *2

#1 Research scholar, K.M.G College of arts and science, Gudiyatham, 635803 TamilNadu, India
*2 Assistant Professor, K.M.G College of arts and science, Gudiyatham, 635803 TamilNadu, India

Abstract: Although promising, RFID is not without its challenges, which arise from both technological and usage point of View. A common concern with RFID is data security. Data Security is a key area in RFID usage; with a limited number of public key cryptosystems on passive RFID platforms, the proposed algorithm makes use of Montgomery multiplication primitives to reduce the amount of computation required on the power constrained tag therefore making the proposition viable. Public key cryptography is being suggested for next generation RFID systems to reduce the number of possible attack vectors native to this type of technology.
By estimating the area, power and time constraints of the RFID platform, it was determined that the area constraint was the critical variable in determining the maximum implementable security variable. Although the application of this algorithm has been targeted for passive HF RFID platforms, the algorithm could be used in other low power, sized constrained applications.

1. INTRODUCTION

RFIDs are currently being used, but are not limited to, inventory control mechanisms and identification. As these devices become more ubiquitous, concern is rising regarding the security of the information that is broadcast through the wireless medium.

This thesis attempts to identify a means of securing the technology using an asymmetric public key encryption, which can be used to perform authentication routines and secure the communications medium. The US government has implemented the RFID tags in their new passport cards for travel between the US, Canada, and Mexico, with many other countries following their stead.

The common concern amongst these implementations is the likelihood of private information being transmitted over the air which could possibly be intercepted by an unintended recipient actively reading the tags without appropriate permission. In the commercial case, information regarding inventory levels could lead to a competitive edge from individual, on the embedded RFID chip. A breach in security, or capability to read this information from a distance without proper encryption techniques, could lead to an increase in personal identity theft and an invasion of privacy.

2. PROPOSED WORK

The objective of this thesis is to determine the feasibility of implementing an RSA cryptographic system using a passive RFID tag system. It has been stated that an RSA algorithm implemented on a passive RFID tag would be difficult to implement with current technology.
The main reason that this technology is thought to be infeasible in the form factor presented is due to the size of a general RSA cryptographic implementation. It is stated, that there is only room for 4,383 gates on a passive UHF RFID, and that an RSA implementation would take 34,000 gates.
From the information that is gleaned from the research performed in the prior paper it indicates that it is not possible to perform RSA cryptography on an RFID tag. This conclusion does not take into account varying the distance of the tag nor does it analyze possible algorithmic variations that could lead to an implementation which would reduce the gate requirements for an RSA cryptosystem on an RFID tag. The suggested research will attempt to vary some of these variables to ascertain the possibility of implementing an RSA cryptosystem on an RFID tag. There are many methods of implementing an RSA cryptosystem that are described in literature primarily focused on the FPGA medium. Using this information, a considered effort is used to assess the suitability of various algorithms for the RFID application. Proper examination of the algorithms will be undertaken to

identify the most probable candidate for application to the RFID platform.

This will be done through the consideration of power, timing constraints, and the size of implementation. Through this examination a proper algorithm will be identified to meet the requirements of implementing an RSA based encryption on the RFID tag platform.

3. ALGORITHM

To be in line with the recommendations, a new RFID RSA security algorithm is proposed to reduce the overall burden of computation on the RFID tag and distribute the cryptographic computation. The proposal is to transmit a partial result of the Montgomery exponentiation result over the air instead of a transformed cryptographic response. A further description of the protocol for performing this and how it fits into the already established public key cryptosystem protocols is examined below.

The proposed algorithm will make use of the core Montgomery multiplication components and will redistribute the transformation from Montgomery residue format back to normal modulo n format at the reader. It was suggested that to perform the Montgomery multiplication there was pre-transformation that was required, namely the multiplication of the message by r and the subsequent reduction modulo n of each multiplied factor. Instead of performing this, the proposed algorithm will take the public key integer pair and message natively without transformation and perform the Montgomery multiplication technique in absentia of the transformation. This has the effect of creating a deficit in the computed number. Each time a Montgomery multiplication is performed the value is reduced by a factor of r. When compounded by the exponentiation algorithm, the value computed is equivalent to

$$c = m^e r^{-(k*(e-1))} \bmod n$$

The advantage of what is being suggested is that there is no conversion of the inputs or the outputs on the RFID tag, which frees up either clock cycles, area or a combination of both (depending on specific implementation). Instead this conversion is placed on the reading device where it there is more power and computational resources available. This is of significant benefit for the specific RFID implementation and other area, power, and time constrained implementations.

This puts additional computational power at the reader end. The pre-computation that is required at the reader needs to be computed only once for each public key pair. The computation that is required at the reader is shown below.

$$x = r^{(k*(e-1))} \bmod n$$

Examining the problem from a security aspect, it is important to note that the fidelity of the RSA algorithm is not lost. Transmitting the partial result does not affect the overall security of the system as can be shown analytically in the following example:

$$c' = m^e r^{-(k*(e-1))} \bmod n$$

$$c = (m^e \bmod n) \cdot (r^{-k*(e-1)} \bmod n) \cdot (r^{k*(e-1)} \bmod n)$$

Since the result that is transmitted is a multiplicative factor of the value of r, and r is composed of public key information, whatever is obtainable through as a result of the RSA algorithm is what is available to the adversary through the proposed algorithm. No additional information is revealed than what is revealed by the public key parameters themselves.

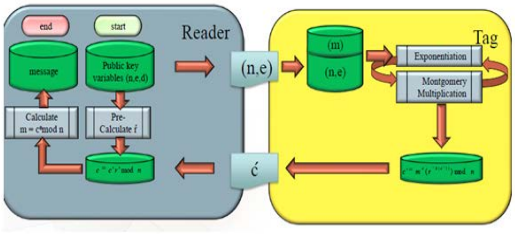

Fig 1.Proposed Algorithm

4. CONSIDERATIONS

Instead it is being suggested that the result be kept in Montgomery space and converted once received by the reader. This proposal addresses three main concerns.

First, the overall size of implementation is drastically reduced. Second, the number of clock cycles that are required is reduced, decreasing the power requirements of the tag. Third, security is maintained through the transaction which is one of the main goals of the work.

Reducing the overall system size is an important means of ensuring the smallest form factor for the implementation. The suggested implementation is far smaller than other comparable algorithms due to the lack of conversion step modules. With that in mind, this method is in fact performing this calculation at another location where it can be performed at a higher rate than on the RFID hardware. The distributed nature of the solution lends itself to optimizations that would not otherwise be obtainable.

The hardware usually dedicated to this is relocated to the reader which can better handle additional hardware and timing delays. This enables the tag to

free up some hardware space for other applications in the future and distribute some of the computational requirements to other parts of the system. The hardware savings consist of a divider circuit to find the residue, the additional memory required for the storage of temporary values, and a regular multiplier circuit required for the computation of the final result.

The final result at the reader will require the multiplication of the result of the Montgomery multiplication and the residue of the operation. The result of the multiplication will need to be reduced modulo n once more to arrive at the final encrypted result. These additional components are not required if the result is transmitted as a Montgomery multiplication result.

With regard to timing, no additional clock cycles dedicated to the conversion of the result from Montgomery space to normal space on the tag is required. This has a significant benefit since the exponentiation computation requires a significant number of clock cycles to complete as shown in prior works. The additional benefit of the reader performing the computation post tag interaction is that once the result is recorded by the reader it can then compute the result at a later time (assuming the message contains solely the tag id).

The benefit is apparent when there is a requirement to read numerous tags at an increased speed, and the time allotment is not sufficient for the tag to produce the final translated cryptographic result. By removing the requirement for additional computation the tag is now able to respond in a reduced period of time. It is also reasonable to assume that the reader will have additional computational power to finish the computation in a period of time that far out paces a tag's capabilities.

5. CONCLUSION

A variety of examinations have been done to determine an efficient means of performing a fast modular exponentiation algorithm. The concentration of work has focused on the speed of the algorithm and whether it there is a possibility of increasing the throughput of the algorithms.

An examination of the current state of the art with respect to RFID security was performed. Current technology and technical implementations for securing RFID tags was covered. The limitations of the current security protocols were examined and the future requirements of RFID tags explored.

An examination into security and its requirements was undertaken. A discussion about what makes an algorithm secure was performed. Current symmetric and asymmetric algorithms were discussed and compared. The RSA algorithm was explored and shown to be secure under OAEP as long as the modulus size (security parameter) is twice as large as the message that is to be encrypted.

Timing analysis was dictated by the standards that are currently in place. It was found that the maximum time between a write cycle and a read cycle would be 10.9 ms. This was then taken as the time in which the algorithm must be able to compute the result of the encryption. This study examined the methods being implemented and determined whether it would be feasible to implement an RSA cryptosystem onto an RFID tag.

Through examination it was determined that a novel method of performing encryption could be achieved by leveraging the capabilities of the RFID tag and reader. Using this new method of performing the RSA encryption, the results indicate that on 0.35μm CMOS technology it would be feasible to perform RSA cryptography on an RFID tag when used in conjunction with the reader.

From the results it can be shown that the limiting factor to the implementation RSA cryptosystem on an RFID tag is the power required to drive logic circuit. This can be seen by the limitation on the area of the RFID chip presented in Figure 5.1, which indicates a 129 bit modulus as the limit for implementation. This limitation is closely followed by the time constraint which shows 152 bits modulus as a maximum. Although, the overall power delivered to the tag indicates that a modulus of 256 bit can be computed, the division of power at a given clock frequency (6.78 MHz nominally) and the number of transistors required to be powered at a given time almost halves the number of bits which can be used in the RSA cryptosystem from more than 256 to 129 bits.

By distributing the encryption, it is possible to fit a RSA cryptosystem onto a passive RFID chip with a marginal security parameter of 128 bits, sufficient for a 64 bit message on 0.35um transistor technology.

6. FUTURE WORK

The work was commissioned as a feasibility study in the realm of performing RSA cryptographic computations on an RFID. The result of which was a

clear indication that under certain constraints this is indeed feasible.

Future work in along the lines of this work would be the implementation of this architecture on an ASIC design. Layout and power management have very interesting problems associated with them in which this project would have to surmount. This would be the natural progression to the work that was done in this thesis.

Analysis could be performed to evaluate the use of 0.18 μm CMOS technology using the same parameters. As this technology gains traction amount manufacturers, significant benefits can be realized for area restricted applications. The power required for a 0.18 μm CMOS implementation would likely be half of that required for a 0.35 μm implementation. The implementation area would reduce by a quarter due to the dimensions of the new transistors. This would mean that additional power and space is available for a given RSA cryptosystem based implementation significantly increasing the security parameter that could be successfully implemented.

Additional work would be to find even more efficient algorithms to perform RSA encryption on an inductive power harvesting platform. The work that was performed here would be a great spring board into this topic and further investigations into performance enhancement methods for a low power application.

7. REFERENCES

[1] L. Tobias, M. Schneider, and C. Ruland, "Analysis of Power Constraints for Cryptographic Algorithms in Mid-Cost RFID Tags," Lecture Notes in Computer Science, vol. 3928, pp. 278-288, 2006.

[2] S. Moon, "Design of a Scalable RSA Cryptoprocessor Embedded with an Efficient MAC Unit," in International Conference on Future Generation Communication and Networking, 2008, pp. 74-77.

[3] S. Wu, Y. Zhu, and Q. Pu, "Resource Efficient Hardware Design for RSA," in Proceedings of the First Interational Multi-Symposiums on Computer and Computational Sciences, 2006.

[4] S. Goldwasser and S. Macali, "Probabilistic Encryption," Journal of Computer and System Sciences, vol. 28, no. 2, pp. 270-299, Apr. 1984.

[5] M. Bolic, "Radio Frequency Identification Technology," University of Ottawa Course Notes, Sep. 2009.

[6] N. C. Wu, M. A. Nystrom, T. R. Lin, and H. C. Yu, "Challenges to global RFID adoption," Technovation, vol. 26, no. 12, pp. 1317-1323, Dec. 2006.

[7] D. Dobkin and T. Wandinger, "A Radio-Oriented Introduction to Radio Frequency Identification," High Frequency Electronics, pp. 46-51, 2005.

[8] J. Landt, "The History of RFID," IEEE Potentials, vol. 24, no. 4, pp. 8-11, Dec. 2005.

[9] International Standards Organization, "Radiofrequency identification of animals -- Advanced transponders -- Part 1: Air interface," International Standards Organization Standard 14223-1:2003, 2003.

[10] International Standards Organization, "Radiofrequency identification of animals -- Advanced transponders -- Part 2: Code and command structure," International Standards Organization Standard 14223-2:2010, 2010.

[11] International Standards Organization, "Identification cards -- Contactless integrated circuit cards -- Proximity cards -- Part 1: Physical characteristics," International Standards Organization Standard 14443-1:2000, 2000.