Analysis of Elliptic Curve Cryptography (ECC) for Energy Efficiency in Wireless Sensor Networks

Zain Ul Abideen Tariq, Shahzad Shahid Peracha, Khurram Aziz
NUST School of Electrical Engineering and Computer Sciences (SEECS), Pakistan
zain@almuash.com, shahzadperacha@hotmail.com, khurram@ieee.org

Abstract

Rapid growth of wireless sensor networks (WSN) in recent times has resulted in greater security requirements. One of the primary concerns in wireless sensor networks is energy efficiency and security mechanisms are no different. Currently, security in wireless sensor networks is often implemented by symmetric key cryptography due to its low-power implementation. Public Key Cryptography (PKC), on the other hand, is advantageous as it requires less overhead information during transmission of packets that ultimately lessens overall size of the protocol. In addition, Public Key Cryptography provides better data confidentiality and authentication in wireless sensor networks. In this study, we focus on Public Key Cryptography for greater efficiency in key distribution, low protocol overhead and efficient hardware implementation on the sensor nodes. Considering the constraints of energy efficient wireless sensor networks, we analyze and compare some well known Public Key algorithms, their implementation in wireless sensor networks, and how these algorithms can benefit the fundamental security services. We also evaluate energy consumption parameters for encryption as well as data transmission and suggest energy efficient encryption mechanisms.

Introduction

Wireless sensor networks are composed of sensors that acquire information, such as temperature, sound, vibration, pressure, motion or pollutants from physical or environmental conditions, at different locations [1]. Some of the nodes in wireless sensor networks act as base stations and others act as sensor nodes. The sensor node that connects the network to a monitoring device or a central server for data aggregation, processing and analysis is called gateway node.

A WSN sensor node consists of four main components:

1. Sensing unit that consists of an analog-to-digital converter and Sensor,
2. Processing unit that consists of a microprocessor and storage memory,
3. Transceiver unit such as an RF Antenna
4. Power unit

Certain additional application dependent modules can also be added such as a location finding system, mobilizer and a power generator.

Wireless sensor networks require a strong security mechanism for data authentication and confidentiality as they are composed of a number of tiny disposable and low power nodes that are left unattended for several hours, days or even months in extreme environments [2-3]. It is usually assumed that Public Key Cryptography is not an efficient solution to wireless sensor networks as security mechanisms on the nodes are strictly resource constrained and therefore symmetric key cryptography is used. We analyze different security algorithms of Public Key Cryptography and observe that Public Key Cryptography has a simplified implementation of many security services and reduces transmission power due to less protocol overhead. The sensor node does not contain global secretes of the network; hence its capture does not compromise security of the entire network. A custom-designed co-processor is considered as an option, to be embedded in the node that will handle all computational tasks and will overcome the difficulty in implementing the Public Key Cryptography [4]

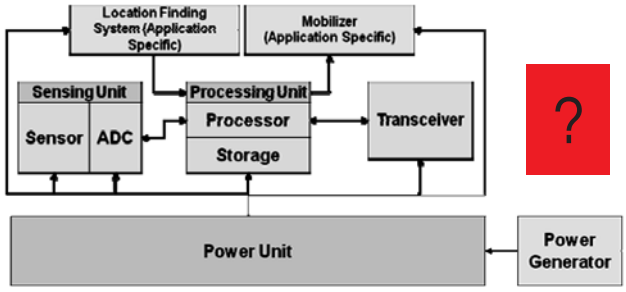

Fig. 1. Internal architecture of a sensor node [2]

We discuss certain security services for which Public Key Cryptography can be advantageous. Further we discuss different mechanisms of Public Key Cryptography for encryption and transmission of data and calculate the power consumed during the entire process. We then analyze our calculated results. And provide a guideline in how to achieve energy efficient security mechanisms in wireless sensor networks.

PKC Security Services

This section briefly describes the security services that could benefit from Public Key Cryptography in wireless sensor networks.

Wireless sensor networks consist of tiny disposable and low power devices known as sensor nodes. These

Corresponding Author: Zain Ul Abideen Tariq NUST Publishing, © (2009), ISSN: 2070-9900

sensor nodes contain sensing module for sensing the data from the environment. Sensor nodes communicate with a base station with the help of a communication module. The base station collects data from all the sensor nodes and forwards it to the outside world. Sensor nodes also transmit information to the neighbors. The base station is considered to have sufficient power for all computation and communications with the nodes and outside world. It acts as a root and the sensor nodes act as a routing tree to the base station.

Encryption

The large size of ciphertext after encryption of a message makes Public Key Cryptography quite expensive as compared to symmetric key cryptography. However Public Key Cryptography can be used for data encryption in cases where message expansion does not consume more computational and energy resources. Sensor nodes send data to the base station while encrypting with the public key of base station. In this way we can still ensure energy efficiency while using Public Key Cryptography for data encryption.

Authentication

Achieving data authentication efficiently in wireless sensor networks is one of our primary concerns. The base station broadcasts a set of commands to all sensor nodes at once. In order to be sure that the data sent is authentic each sensor node will have to verify that the message is actually sent by the original base station and not by any intruder. Public Key Cryptography can be ideally implemented in such cases. In order to read messages sent by the base station, all sensor nodes must have the public key of the base station embedded in them. This mechanism brings efficiency as previously used schemes required lots of overhead information in order to achieve data authentication or were using very complicated symmetric key algorithms.

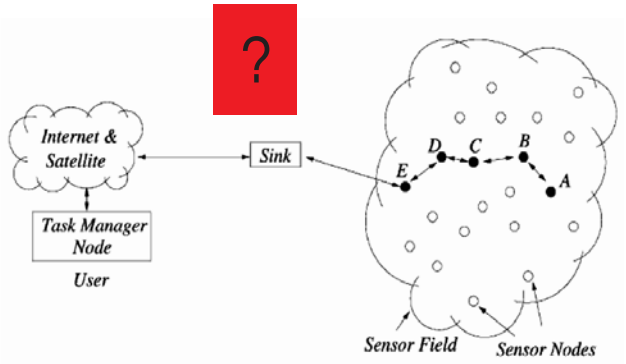

Fig. 2. Sensor nodes Scattered in a sensor filed [2]

Key Distribution Mechanism

Key agreement and key distribution are other implementations of Public Key Cryptography. Key distribution is a protocol where one party securely transmits a key to another party, whereas key agreement refers to a protocol where two parties jointly establish a key [6]. Each sensor node usually knows the public keys of its neighbors. There are two ways with the help of which Private Key can be distributed or assigned. It can be distributed during the routing setup phase or it can be acquired from the base station. Whenever one node decides to communicate with the neighboring node it just encrypts the data with the public key of the neighbor and sends it to the desired node. Then that node decrypts the data while using its private key. In this entire process base station is not involved, that ultimately saves transmission power hence we achieve the energy efficiency. If a node needs to be replaced, the base station sends a broadcast message to all nodes in the network announcing the removal of the node and revocation of its public key. All nodes in response to the broadcast message from the base station revoke the public key of the removed node.

Addition of a Sensor Node

As wireless sensor networks reside in extreme situations, many of the sensor nodes could be damaged or any new sensor node needs to be deployed. In both addition and replacement of a node, a node needs to be added in the security scheme of wireless sensor network. This can also be achieved by Public Key Cryptography. All sensor nodes have their public and private keys and the public key of the base station. Base station can send the private key of the new node and get the public key of the newly added node by the outside communication link. The base station can hence trust the newly added node and do further correspondence. The node announces its arrival by sending a signed message to the base station.

Execution

Security services for authentication, data encryption, key distribution and addition of new sensor nodes can easily be achieved by the use of several different Public Key Cryptography. In this paper our primary focus is on three widely known schemes in practice:

1. Rabin's Scheme,
2. Ntru variants
   a. *NtruEncrypt* for confidentiality
   b. *NtruSign* for authentication

3. Elliptic Curve Cryptosystem (ECC) variants [8]
   a. *ECMV* for confidentiality
   b. *ECDSA* for authentication

We carry out an analysis of the three schemes and try to evaluate energy consumption for encryption and data transmission. The architecture for encryption function is reported in [6].

The three above mentioned encryption schemes are inherently different in the way their core functionality works. We take the parameter sets with which we asses their ultra low power implementation and achieve approximately the same security level. In this way we identify the most energy efficient scheme for the wireless sensor networks.

Cipher text size differs to a large extent based on the encryption scheme [6]. Hence, we analyze the

consumption of energy during encryption and transmission of cipher text for various encryption schemes. For Rabin's Scheme we select a modulus of 512 bits that provides a security level of around 60 bits. For NtruEncrypt we select the system parameters as $(N, p, q) = (167, 3, 128)$, offering a security level of around 57 bits. ECC architecture performs arithmetic in a prime field of 100 bits in size, which provides a security level between 56 and 60 bits. [6].

Rabin's Scheme

Rabin's Scheme is very similar to RSA in functionality as well as in security as both schemes address the factorization problem of a large number. The comparison of encryption and decryption of Rabin's Scheme can be done with RSA both having similar parameter constraints. Due to its dissimilar computational ability in nodes and base station of a wireless sensor network Rabin's Scheme is an interesting choice. The encryption function of Rabin's Scheme is [6]

$E_{n,b}(x) \equiv x(x + b) \pmod{n}$ where
$0 <= E_{n,b}(x) < n$,
$0 <= x < n, 0 <= b < n$.
If we set $b = 0$ this function becomes a simple squaring operation $E_n(x) = x^2 \pmod{n} = y$

We observe that Rabin's Scheme needs just squaring for encryption process which means that we achieve decryption by only taking the square root of y. The decryption function is $D_n(x) \equiv (\sqrt{y}) \bmod n$ and yields four results.

The decryption of our implementation for Rabin's scheme is achieved in another way in which we build a squarer as a bit-serial multiplier, operating on the entire width of the 512-bit multiplicand and on a single bit of the multiplier at a time [6]. This is an advantageous approach in which the unit is easily converted to perform the exponentiations needed for decryption function.

Ntru Variants

Ntru uses NtruEncrypt for data encryption and NtruSign for digital Signature. NtruEncrypt asserts to provide the security equivalent to other recognized schemes in a highly efficient manner for fixed applications such as RFID tags and Smart Cards.

The measurable NtruEncrypt (data encryption) architecture provides data to which we apply NtruSign (digital signature) and estimate its performance. It is measurable with regards to the number of arithmetic units working in parallel, allowing a trade-off between area and performance [6].

Elliptic Curve Variants

Elliptic Curve Cryptography (ECC) has many variants for data encryption, key agreement and digital signature e.g ECDH, ECDSA, ECMV, etc. The basic building block of Elliptic Curve Cryptography is scalar point multiplication which results in most expensive computation operation. However the message size in Elliptic Curve Cryptography is lesser as compare to the other two schemes discussed, which makes Elliptic Curve Cryptography an energy efficient scheme when it comes to data transmission to a large domain.

Elliptic Curve Cryptography uses ECDSA for Digital Signature (Data Verification) and ECMV as a encryption and key transport protocol. The results obtained from Elliptic Curve Cryptography are used to estimate the convolution computation and performance.

ECC works in finite field termed as Galois Field (GF). Galois Field works in prime characteristic or binary extension fields e.g. GF(p) or GF(2) which is quite efficient arithmetic that results in low power hardware implementation of Elliptic Curve Cryptography.

Analysis

We analyze three PKC schemes i.e. Rabin's scheme, two variants of Ntru and ECC each for both confidentiality and authentication. We now analyze the further step of looking at how energy consumption varies for each of the three algorithms with the different ranges of the transmission power of the transmitters on wireless sensor nodes. Gaubatz et. al. [6] present the experimental results for the three said schemes that include only the energy consumption during the processes of encryption and decryption. It can be observed that the messages size expansion as a result of encryption and decryption varies to different degrees for each of the three schemes. They leave the issue of energy consumption for transmission at that point. We intend to present the factual estimates to help in design issues and see which algorithm works best for which design criteria of the wireless sensor networks.

Analysis Parameters

The parameters that determine and affect our analysis are data rate D, of the transmitted data, the size M_c of ciphertext to be transmitted and transmission power P_t, of the transmitter on the sensor node.

The transmission power P_t further depends on the range of the adjacent nodes. It varies for different applications and environments. The data as being given in Table 1, shows power and energy consumption for each of the three schemes provided the ciphertext expansion factors and time to encrypt the messages. The expansion factor of Ntru comes out to be the highest i.e. almost 5 times the message size and that of ECC variant ECMV or ECDSA is the lowest i.e. 2 times for ECMV and 1 time for ECDSA.

Analysis & Comparison

The transmission energy required to transmit the ciphertext bits is less for ECC and more for Ntru and Rabin's scheme as shown in Table 1. Data rate of the transmission is taken as 250 Kbps. In all cases, the trend for transmission energy for all three algorithms remains relatively same as shown in Figure 3. The comparison for the energy consumption for the three schemes with the two variants of Elliptic Curve Cryptography is shown in Figure 4. We calculate the energy consumption during transmission using following formula.

Transmission Energy = $E_t = M_c P_t D^{-1}$

Table 1. Comparison of PKC Algorithms with their energy consumption values

Encryption (Confidentiality)		**Rabin**	**NtruEncrypt**	**ECMV (ECC)**
- Message Payload [1] - Ciphertext (packets of 30 bytes) M_c [1]		< 512 bits 512 bits (3)	< 265 bits 1169 bits (5)	< 200 400 bits (2)
Encryption	Time per Message [1]	2.88 ms	0.87 ms	817.7 ms
	Avg. Power [1]	148.18 μW	118.7 μW	394.4 μW
	Energy per Message [1]	426.76 nJ	102.79 nJ	322.5 μJ
Time to Transmit for **D = 250 kbps**		2.50 ms	4.67 ms	1.86 ms
Energy to Transmit for Tx Power P_t = **26 dBm** (398.11 mW)		1.11 mJ	1.85 mJ	742.07 μJ
Total Energy Consumption		1.11 mJ	1.85 mJ	1.06 mJ
Digital Signature (Authentication)		**Rabin**	**NtruSign**	**ECDSA (ECC)**
- Signature length (packets of 30 bytes) Mc [1]		512 bits (3)	1169 bits (5)	200 bits (1)
Sign	Time per Message [1]	1.089 s	3.464 ms	410.45 ms
	Avg. Power [1]	191.5 μW	158.3 μW	394.4 μW
	Energy per Message [1]	208.64 μJ	548.35 nJ	161.88 μJ
Time to Transmit for **D = 250 kbps**		2.50 ms	4.67 ms	8.99 ms
Energy to Transmit for Tx Power P_t = **26 dBm** (398.11 mW)		1.11mJ	1.85mJ	371.04 μJ
Total Energy Consumption		1.11 mJ	1.85 mJ	532.91 μJ

Red box = thick line

where,

M_c = Encrypted Message Size
P_t = Transmission Power
D = Data Rate
The total energy consumed for both encryption and transmission becomes

Total Energy Consumed $= E_{tot} = E_t + E_e$
$= M_c P_t D^{-1} + P_e t_e$
where,

E_{tot} = Total Energy Consumed
E_t = Transmission Energy
E_e = Encryption Energy
P_e = Avg. Encryption Power
t_e = Encryption Time

When we take the total energy consumption in account we observe that Elliptic Curve Cryptography (ECC) variant ECMV becomes energy efficient for transmission powers greater than approx 13 dBm (19.95 mW) for data rate of 25 kbps. Taking the data rate at 250 Kbps we get different results i.e. Ntru scheme remains better than ECC until 20 dBm (100 mW) after which its total energy consumption goes higher than both ECC and Rabin's scheme, while Rabin's scheme remains better than ECC till 25 dBm (316.23 mW) after which ECC becomes the energy efficient choice. Therefore we note that for lower data rates ECC remains energy efficient for transmission power greater than 13 dBm (19.95 mW) while at higher data rates it remains efficient only for higher power values as shown in Figure 5 and 7. Similarly at 100 Kbps data rate the energy efficiency threshold for ECC comes to 21 dBm (125 mW). Therefore ECC works better for lower data rates and higher transmission power scenarios while for higher data rates and low transmission power scenarios Ntru and even Rabin's scheme works better. The graphs shown in Figure 5, 6 and 7 present the comparisons. The calculations above only apply in the case we take expansion factor for ECC as 2 i.e. ECMV encryption. In case we take ECC variant ECDSA the situation resolves further in favour of ECC. Taking the data rate of 250 Kbps we get the reduced point of energy efficiency for ECC variant ECDSA at 22 dBm (158.5 mW) as compared to 25 dBm (316.23 mW) for ECC variant ECMV. Similar results come for lower data rates e.g. 25 Kbps we get 15 dBm (31.6 mW) as energy efficiency point for ECC variant ECMV (message expansion factor 2) and 13 dBm (19.95 mW) for ECC variant ECDSA (message expansion factor 1).

This also gives us another perspective into the range of the adjacent nodes in wireless sensor networks. Greater the range, greater would be the transmission power used. It means that wider sensor networks would consequently use higher power transmissions and thus the choice of Public Key Cryptographic algorithms would fall in favour of ECC as seen in passive RFID tags having transmission power up to 30 dBm as given in [7] that easily crosses the energy efficiency point for ECC variants. While for short range

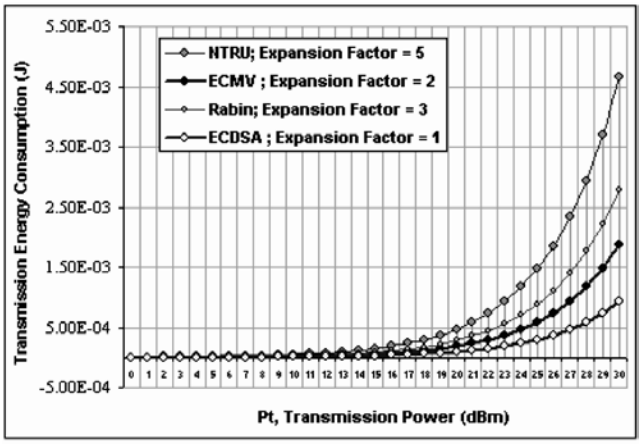

Fig. 3. Comparison for transmission energy for Public Key Cryptographic algorithms Ntru, Rabin's scheme and ECC variants ECMV and ECDSA at Data Rate D = 250 Kbps

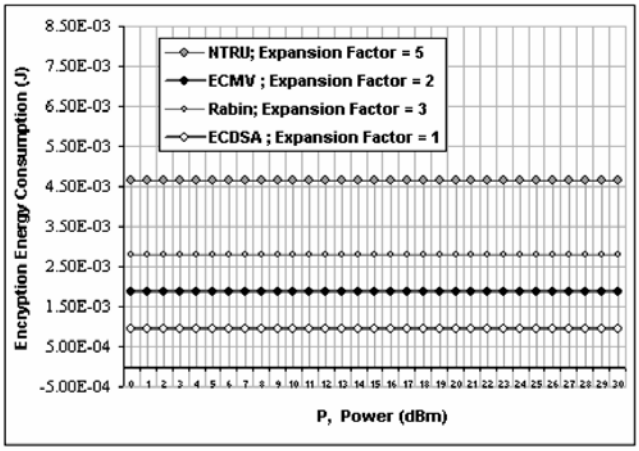

Fig. 4. Comparison for encryption energy for Public Key Cryptographic algorithms Ntru, Rabin's scheme and ECC variants ECMV and ECDSA.

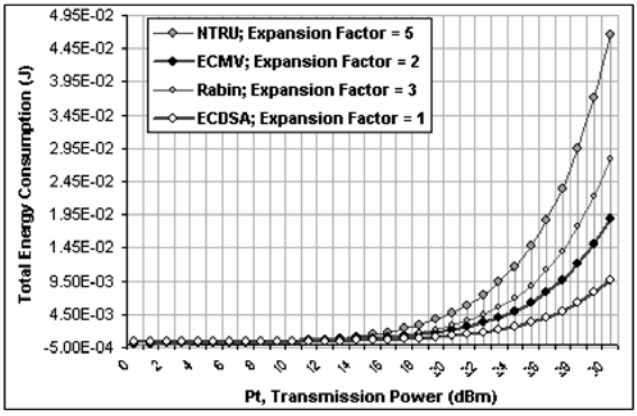

Fig. 5. Comparison for total energy (transmission and encryption/decryption) for Public Key Cryptographic algorithms Ntru, Rabin's scheme and ECC variants ECMV and ECDSA at Data Rate D = 25 Kbps

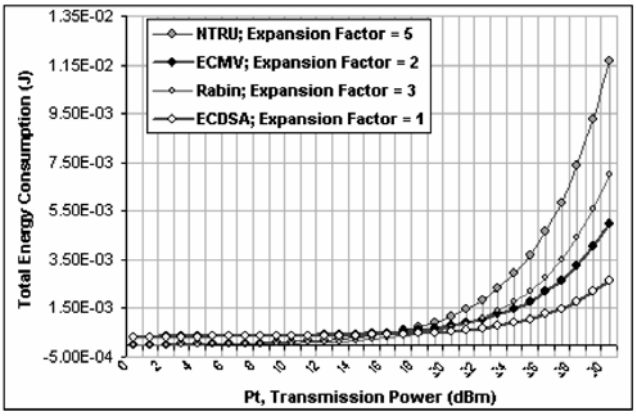

Fig. 6. Comparison for total energy (transmission and encryption/decryption) for Public Key Cryptographic Algorithms Ntru, Rabin's scheme and ECC variants ECMV and ECDSA at Data Rate D = 100 Kbps

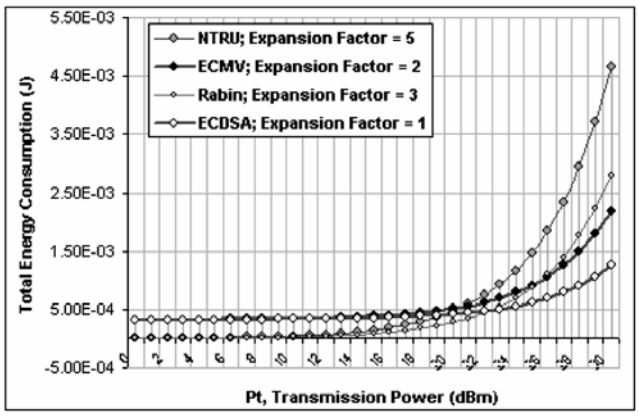

Fig. 7. Comparison for total energy (transmission and encryption/decryption) for Public Key Cryptographic Algorithms Ntru, Rabin's scheme and ECC variants ECMV and ECDSA at Data Rate D = 250 Kbps

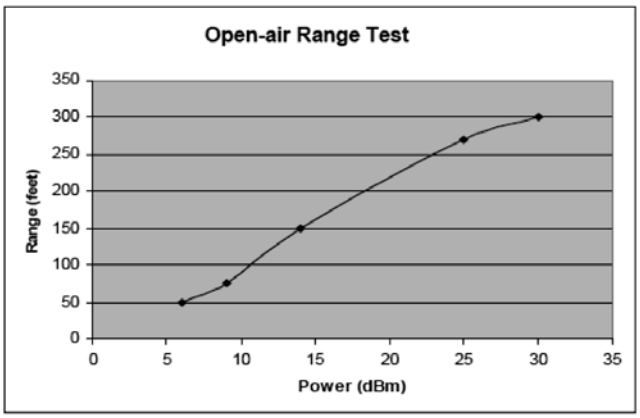

Fig. 8. Measured range in unobstructed outdoor environment as a function of output power of the reader [4]

applications for wireless sensor networks, the transmission power would be lower and thus the choice would fall in favour of Ntru or Rabin's scheme. Figure 8 taken from page 5 of [7] shows a graph comparing the power requirements at different ranges between passive RFID tags and RFID reader based on tests in open air. It shows that at 30 dBm the range is 300 ft i.e. around 100 meters as shown in Figure 8. But as can be seen, the typical applications of wireless sensor networks in vast areas would require higher lower data rates, greater ranges and higher transmission power thus pushing the designer's choice in favour of ECC variants. Taking the two variants of ECC i.e. ECMV and ECDSA, into account, we know that ECMV is used for confidentiality service and ECDSA gives authentication service. It is obvious that ECMV encryption and ECDSA authentication are mainly used at the beginning of a new session to share secret symmetric session key. ECDSA is also used when the new node enters the network. As observed, ECDSA has expansion factor of 1 as compared to 2 in ECMV; therefore ECDSA has better energy efficiency that is used frequently at the beginning of a new session, as compared to ECMV that is used for session key sharing before every new session.

Conclusion

We presented the comparison of three Public Key Cryptographic schemes used for authentication and confidentiality and concluded that Elliptic Curve variants ECMV and ECDSA are better choices for most of the wireless sensor networks applications due to low message expansion, especially in RFIDs, which require lower data rates and comparatively higher transmission power due to greater range and thus have less total energy consumption as compared to Ntru and Rabin's scheme. We presented the range of transmission powers where ECC would deliver favorable results as compared to other schemes.

REFERENCES

1. Kay Romer and Friedemann Mattern, "The design space of wireless sensor networks". *IEEE Wireless Communications Magazine,* vol. 11, no. 6, 2004, pp. 54-61
2. Perrig, R. Szewczyk, J. D. Tygar, V. Wen, and D. E. Culler. "SPINS: security protocols for sensor networks", *Wireless Networks*, vol. 8, no. 5, 2002, pp. 521–534
3. G. Gaubatz, J.-P. Kaps, and B. Sunar, "Public Key Cryptography in sensor networks—revisited" in *1st European Workshop on Security in Ad-Hoc and Sensor Networks (ESAS 2004)*, Heidelberg, Germany, August 6, 2004.
4. A. J. Menezes, P. C. van Oorschot, and S. Vanstone. *Handbook of Applied Cryptography*. CRC Press Inc., 1997.
5. F. Akyildiz , W. Su , Y. Sankarasubramaniam , E. Cayirci, "Wireless sensor networks: a survey" in *Computer Networks: The International Journal of Computer and Telecommunications Networking,* vol. 38 no. 4, March 2002, pp.393-422.
6. Gunnar Gaubatz, Jens-Peter Kaps, Erdinc Ozturk, and Berk Sunar. "State of the art in ultra-low power Public Key Cryptography for wireless sensor networks", in *3rd IEEE International Conference on Pervasive Computing and Communications Workshops,* , March 2005, pp. 146-150.
7. Intelleflex White paper "Passive battery assisted passive and active tags: a technical comparison". WP-.09054 © 2005 Intelleflex Corporation.
8. E. O¨ ztu¨rk, B. Sunar, and E. Savas¸. Low-power elliptic curve cryptography using scaled modular arithmetic. In *CHES 2004*, volume 3156 of *LNCS*, pages 92–106. Springer, 2004.