An ICMetrics based Lightweight Security Architecture using Lattice Signcryption

Ruhma Tahir, Klaus McDonald-Maier
School of Computer Science and Electronic Engineering
University of Essex
Colchester, United Kingdom
rtahir@essex.ac.uk, kdm@essex.ac.uk

***Abstract*—The advent of embedded systems has completely transformed the information landscape. With the explosive growth in the use of interactive real-time technologies, this internet landscape aims to support an even broader range of application domains. The large amount of data that is exchanged by these applications has made them an attractive target for attacks. Thus it is important to employ security mechanisms to protect these systems from attackers. A major challenge facing researchers is the resource constrained nature of these systems, which renders most of the traditional security mechanisms almost useless. In this paper we propose a lightweight ICmetrics based security architecture using lattices. The features of the proposed architecture fulfill both the requirements of security as well as energy efficiency. The proposed architecture provides authentication, confidentiality, non-repudiation and integrity of data. Using the identity information derived from ICmetrics of the device, we further construct a signcryption scheme based on lattices that makes use of certificateless PKC to achieve the security requirements of the design. This scheme is targeted on resource constrained environments, and can be used widely in applications that require sufficient levels of security with limited resources.**

Keywords-ICMetrics; Lattice based Cryptography; signcryption; digital signature; confidentiality; integrity; authentication; non-repudiation.

I. INTRODUCTION

Embedded computing systems play a major part in various aspects of life, ranging from their use in single user applications to large scale processes [1]. Examples of their use in large scale processes could be sensor nodes aggregating sensed data and transmitting it to a centralized server or simply their use in handheld devices for a range of single user applications. With the widespread deployment of high speed/bandwidth wireless networks even more applications are being ported to embedded systems. However embedded systems have limitations in terms of power, memory and execution time [1].

The data exchanged in embedded system applications is prone to attacks from unauthorized parties resulting in threat of vast amounts of data loss by organizations/ individuals. Thus, it is important to employ security mechanisms in order to protect the data. The resource constrained nature of embedded system networks affects the choice of cryptographic mechanisms employed for application security [2]. Traditional cryptographic mechanisms which provide security are not well suited for these systems. So the major challenge in embedded systems is using security approaches in accordance with their resource constraints, thereby providing authentication, confidentiality, integrity and non-repudiation in a resource efficient manner. The proposed security architecture has the following features that address the security issues in embedded system environments in a resource efficient manner:

1) To safeguard against issues related to key compromise, the proposed architecture generates the keys based on ICmetrics (Integrated Circuit Metrics) [17]. ICMetrics generates keys based on the hardware/ software characteristics and specification of the device which provides an effective means to address the issues related to the secrecy of key. Our scheme intends to bind a cryptographic key with the device's ICmetrics information.

2) For the purpose of identification of the device, we propose the use of Certificateless Public Key Cryptography (CL-PKC) rather than Certificate based Public Key Cryptography (CB-PKC). CB-PKC expends significant resources in managing certificates for identification purposes whereas CL-PKC does not need certificates for their operation. In our scheme a public/private key pair is formed by combining the ICMetrics generated key and a partial key generated by the Key Generating Centre (KGC).

3) Our proposed architecture makes use of cryptographic primitives based on lattices for providing security in a resource efficient manner. Firstly lattice-based cryptographic constructions hold a great promise for post-quantum cryptography and are therefore secure against post quantum attacks [3-4]. Secondly since the operations making up lattice structures are very efficient and simple, they prove to be very appropriate for providing security in resource constrained environments.

4) For guaranteeing authentication, confidentiality, integrity and non-repudiation of data in our scheme we propose the use of lattice based cryptographic primitives coupled with signcryption. Signcryption provides confidentiality and digital signatures in a single logical step, so rather than having to execute two operations separately when using simple encryption our scheme will perform this in a single logical thereby saving resources [8].

The remainder of this paper is organized as follows; in section 2 we discuss the design goals of the proposed lightweight security architecture. Section 3 introduces the security primitives on which the design of our proposed architecture rests. Section 4 discusses the ICmetrics technology and its features elaborating on how ICMetrics could be a viable solution for the proposed design. Section 5 explains how CL-PKC is more appropriate for resource constrained environments such as embedded systems. Section 6 explains the concept of signcryption and how it can help reduce the cost of carrying out operations separately required by digital signature and encryption. Section 7 discusses the concept of lattice based cryptography and the mathematical problems that lie at the heart of its design. The design of our proposed lightweight security architecture is presented in Section 8, with details of its working and the analysis of its cost-effectiveness for security in resource constrained environments. The conclusion and future work for our paper is presented in section 9.

II. DESIGN GOALS

Designing security protocols for embedded systems is a very challenging task due to their resource constrained nature such as limited amount of energy, low processing capability, limited storage space and low bandwidth. When designing a secure communication protocol between two parties, the need is to set a tradeoff between the level of security required and the amount of resources available. The following section enlists design goals of our proposed lightweight architecture:

Message **authentication** using minimal amount of resources is the first and the foremost goal of the proposed design. This enables the receiving party to verify that the data has not been sent by an illegitimate party.

Data **confidentiality** using minimal resources is another goal of our design so that private information is kept secret from unauthorized parties.

Data **integrity** safeguards the network from illegitimate manipulation of data, and ensures the receiver that the data is exactly what was sent by the sender. The proposed design aims to provide data integrity using minimal resources.

Non-repudiation is another goal of our design that ensures that an entity on the network cannot refuse to own a piece of information transmitted onto the network.

III. SECURITY PRIMITIVES

The design of the proposed lightweight security architecture rests on the following security primitives.

A. Public Key Cryptography

Public Key Cryptography (PKC) schemes are based on public/private key pairs for their operation [13]. As shown in fig 1 the sender and receiver each hold a private/ public key pair PR_S/PU_S and PR_R/PU_R respectively. The public keys of both parties are published publically to all participants in the network and the private keys are held privately by the owner of the key themselves. In PKC the sending entity encrypts the data using the public key (PU_R) of the destined entity so that the recipient can decrypt the received data with the associated private key pair (PR_R) to reveal the original message contents. Similarly if the receiver in turn wants to send a message back to the sender he/she would encrypt the message with the sender's public key and the sender on receiving the message would decrypt the contents with his/her private key. PKC overcomes the issues related to secret key sharing between communicating entities, since it is based on a public/private key pair setting and does not require sharing of secret keys over the communication channel.

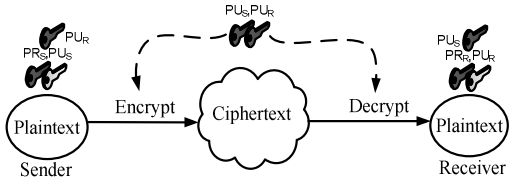

Figure 1. Public key cryptography

B. Hash Functions

A hash function is a cryptographic primitive that guarantees data integrity by performing operation on a variable sized input block to generate a fixed size hash value specific to the data block [13]. Hash functions are used to provide data integrity, so they are designed in such a way that any change in the input data will bring about a change in the generated hash value for that data block. A hash function can detect any sort of data manipulation; whether it's intentional and performed by an attacker, or is unintentional and is caused by the transmission channel.

Hash functions have a major role in digital signature generation, due to their ability to detect data manipulation and length advantages of generated hash value for performing further operations.

C. Digital Signature

Digital Signatures are PKC schemes that are used to provide authentication, integrity and non-repudiation of data. Digital Signatures to some extent are similar to handwritten signatures, with the added feature of providing data integrity [13]. Digital signatures provide a proof of message authenticity to the recipient and that the message has not been altered in transit. They also provide non-repudiation in that the sender cannot deny at any point in time that the message was not sent by him/her. Digital signatures are normally used in applications where it is important to detect illegitimate operations taking place such as forgery, counterfeiting or tampering of data. Fig. 2 and 3 show the digital signature process, comprising of digital signature generation and digital signature verification, detailing how digital signatures provide authentication, integrity and non-repudiation of data.

The digital signature generation process is shown in Fig. 2 whereby the sending party generates a hash value for the input message and signs the generated hash value using his/her private key (PR_S) to generate a signed message hash. Both the signed hash and the original message are further encrypted with the receiver's public key and sent to the destined party.

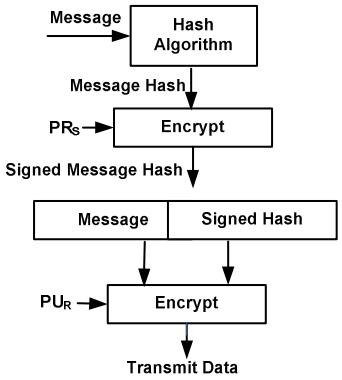

Figure 2. Digital signature generation

In the digital signature verification process as shown in Fig. 3, the receiving party decrypts the received data with the receiver's private key (PR_R) to reveal the original message and the signed message hash. Then the receiver further decrypts the signed message hash with the sender's public key (PU_S) to authenticate the sender and that the claimed sender sent this message and he/she won't be able to deny having signed that message. And finally the receiver also computes a message hash on the received message to compare both the calculated message hash and the received message hash. If the results of both hash values after comparison are same, that proves that the message has not been altered in transit.

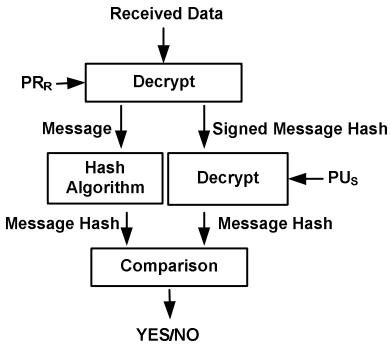

Figure 3. Digital signature verification

IV. ICMETRICS

Traditionally cryptographic algorithms have always relied on the use of stored keys for functioning of the network. However the use of stored keys to enable secure communication is threatened by the fact that, if the key used to encrypt the data is compromised, it will result in loss of data that is encrypted using the compromised key.

ICmetrics (Integrated Circuit metrics) makes use of system level characteristics to provide identification to the system [12]. It generates keys based on the hardware/ software characteristics and specification of the node. ICmetrics compute the required metrics on those hardware and software characteristics that are difficult for the attacker to deduce [17]. These metrics/ features are not static but infact vary in a pre-determined fashion. For example, the address and value from the data transactions of a processor; its program address; and metrics for the effectiveness of the program and data caches derived from performance counters, etc [18].

After each key generation stage the produced encryption key is temporary and exists only locally, and the reproduction of the key once again takes place from measurable characteristics of the integrated circuit [14]. ICmetrics generates encryption key from measurable properties of a given hardware device, similar to the way biometrics extracts human features.

V. CERTIFICATELESS PUBLIC KEY CRYPTOGRAPHY

Certificateless Public Key Cryptography (CL-PKC) bridges between the Certificate based PKC (CB-PKC) [13] schemes and ID based PKC (ID-PKC) schemes. In order to guarantee the authenticity of the public key associated with an entity, CL-PKC schemes do not make use of certificates like traditional CB-PKC schemes do; and nor do CL-PKC schemes generate identification based on a user identifier as the public key and the private key completely generated by a trusted third party. Infact, in CL-PKC schemes the key generation process is split between the Key Generating Centre (KGC) and the user; thereby a part of the key being generated by the KGC and a part of the key generated by the user. As a result of this CL-PKC schemes solve the certificate management and revocation problems inherent in CB-PKC schemes and the key escrow problem in the ID-PKC schemes.

VI. SIGNCRYPTION

Signcryption is a public key primitive proposed by Yuliang Zheng in 1997 that performs both the functions of digital signature and encryption in a single logical step [6]. Signcryption is a substitute to typical signature-then-encryption schemes but with the added advantage that it provides the functionality of both digital signature and confidentiality with less computational complexity and lower communication cost [8]. For this reason signcryption is well suitable for resource constrained devices that require security with little resources [14-15].

Fig. 4 shows the process of signcryption performed by the sending party. The required input parameters are generated according to the specific key generation algorithm that in turn generates a public/ private key pair for the sender. The private key of the sender (PR_S) and the public

key of the receiver (PU_R) are used for generating the signcryption ciphertext for the message 'M'.

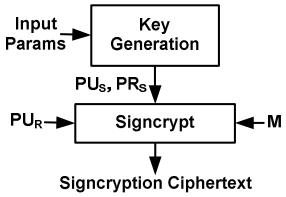

Figure 4. Process of signcryption

The process of unsigncryption that is carried out in accepting a legitimate message or rejecting an illegitimate message is shown in Fig. 5. The public key of the sender and the private key of the receiver alongwith the ciphertext 'C' are both used to unsigncrypt the ciphertext and give an accept/ reject decision [16].

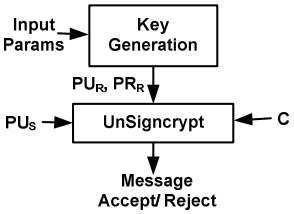

Figure 5. Process of unsigncryption

VII. LATTICE BASED CRYPTOGRAPHY

Lattice based cryptography (LBC) is asymmetric cryptography based on lattices [11]. A lattice is a set of points in n dimensional space with periodic structure. The main reason for interest in lattice based cryptographic schemes is due to the fact that they are secure against post quantum attacks [4]. Secondly another major factor that is motivating their usage in cryptographic constructions is their property of having worst case hardness and their simple constructions since most operations are based on modular addition [5].

Lattices can be used in the construction of various encryption schemes, digital signature schemes and hash generation schemes to provide authenticity, confidentiality, integrity and non-repudiation [7]. The security of lattice based security constructions is based on either one of the two mathematical problems namely Shortest Vector Problem (SVP) or Closest Vector Problem (CVP) [9]. SVP states if only the basis of the lattice in known, it is difficult to find the shortest vector in the lattice unless the attacker has some extra piece of information. The closest vector problem states that if the basis of a lattice and a vector not in the lattice are known, finding the lattice vector with the least distance to the given vector is a hard problem. All lattice based cryptosystems are based on either one of the stated lattice problems [10].

VIII. BUILDING BLOCKS OF THE PROPOSED SCHEME

In our design, we aim to improve the security and performance properties without significantly increasing the device's energy consumption. We construct an ICmetrics based certificateless signcryption scheme using lattices which performs message authentication, confidentiality, integrity and non-repudiation of each message. Due to the resource restrictions imposed on embedded systems, our major objective in designing a new security model is to minimize cost-effect of communication overhead and computation overhead while maintaining required levels of security.

A. ICmetrics based certificateless PKC

Key generation based on ICmetric values of the device is the first phase of our lightweight architecture for both the sender aswell as the receiver as shown in Fig. 6 and Fig. 7. The basis number generated by ICMetrics and the partial private key generated by the KGC are both used in the generation of public/ private key pair (PU_S, PR_S) for usage in lattice based signcryption. The combination of key from the KGC and the secret basis number provides a solution to key escrow problem inherent in case of ID-PKC.

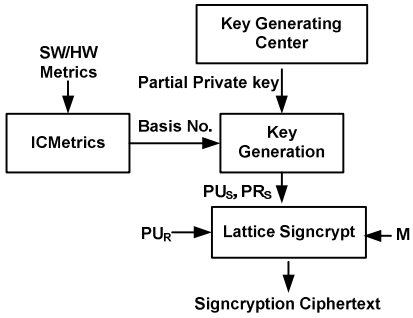

Figure 6. Proposed architectural diagram for sending side

Traditional ways of key generation/ maintenance are unable to provide non-repudiation because keys can be lost, captured; or when they are shared with other devices, there is no-way to know who the actual device was. Therefore, ICmetrics based keys are proposed in our design which provide the following advantages:

- ICMetric keys provide non-repudiation since they cannot be lost or forgotten and are permanently associated with a particular device based on its hardware/software characteristics.
- ICMetric keys are very difficult to forge since they cannot be guessed easily.

The use of CL-PKC in our design also provides performance advantages. Firstly it solves key escrow inherent in IB-PKC since in our scheme the public/private key pair is generated by partial key from KGC and a partial key based on basis number. Secondly it also solves the

problem of high computational cost for generation and revocation of digital certificates inherent in CB-PKC.
As a result, authentication based on ICMetrics coupled with CL-PKC is more reliable, secure and resource efficient than traditional schemes for providing authentication and non-repudiation of data.

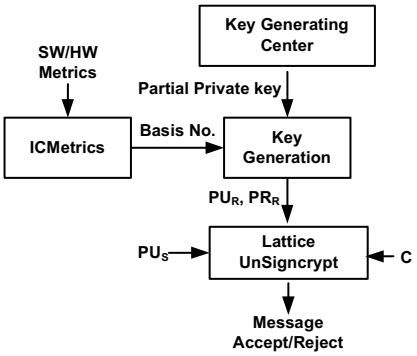

Figure 7. Proposed architectural diagram for receiving side

B. Lattice based Signcryption

The second phase of our architecture at both the sender/ receiver aims to provide authentication, confidentiality, integrity and non-repudiation all in one logical step using signcryption based on lattices. Fig. 6 shows the process of lattice based signcryption that is performed by the sending party. The generated public/ private key pair from the first phase is used for the process of generating the signcryption ciphertext. The private key of the sender (PR_S) and the public key of the receiver (PU_R) are both used for generating the lattice based signcryption ciphertext for the message 'M'.

Subsequently on the receiving side the process of lattice based unsigncyrption is carried out. The generated public/ private key pair at the receiving end is used in accepting a legitimate message or rejecting an illegitimate message. The public key of the sender and the private key of the receiver alongwith the ciphertext 'C' are both used to unsigncrypt using the lattice unsigncrypt and then finally give an accept/ reject decision.

Lattice based cryptographic constructions are particularly selected for our design, firstly due to the simplicity of lattice operations while having worst case hardness and secondly due to their resistance against post quantum attacks. The proposed design provides confidentiality as well as integrity for the communicated information and ensures authenticity and non-repudiation of the participants. Confidentiality and digital signature generation is achieved by lattice based signcryption. This prevents any illegitimate disclosure of information; and all in a single logical step as opposed to a separate process for encryption and digital signature generation in traditional security settings. So this phase provides double performance advantages from both lattices as well as signcryption thereby providing authentication, confidentiality, integrity and non-repudiation.

IX. CONCLUSION

An ICmetrics based security architecture using certificateless lattice signcryption scheme is introduced in this paper. The proposed scheme effectively combines the functionalities of ICMetric keys coupled with CL-PKC for providing authentication and non-repudiation; and lattice based cryptography coupled with signcryption for providing authentication, confidentiality, integrity and non-repudiation in a resource efficient manner. By employing our security architecture we are able to prevent most of the depicted threats while considering the constraints that embedded systems demands. The design decisions of our lightweight architecture have a number of important consequences and make it particularly suitable for resource constrained environments, which require elimination of computationally expensive and resource intensive operations while providing the required security.

Our future plan is to evaluate the scheme proposed here through experiments and analysis, thus benchmarking the results against existing schemes that provide security in resource constrained environments. We are confident that our proposed architecture will be an efficient and viable solution for providing comprehensive security in embedded systems.

ACKNOWLEDGEMENT

The authors gratefully acknowledge the support of the UK Engineering and Physical Sciences Research Council under grant EP/K004638/1.

REFERENCES

[1] L. Khelladi, Y. Challal, A. Bouabdallah, N. Badache, "On Security Issues in Embedded Systems: Challenges and Solutions", International Journal of Information and Computer Security 2008, Vol. 2, No.2, pp. 140-174.

[2] I. Ryu, "Issues and Challenges in Developing Embedded Software for Information Appliances and Telecommunication Terminals", Proceedings of the ACM SIGPLAN 1999, LCTES'99, Vol. 34, Issue7, July 1999, pp. 104-120.

[3] M. Ajtai, "Generating hard instances of lattice problems", Proceedings of the 28th annual ACM symposium on Theory of computing, 1996, pp. 99–108.

[4] M. Ajtai, "Generating hard instances of the short basis problem", Automata, Languages and Programming, 1999, pp. 706–706.

[5] D. Micciancio, O. Regev, "Lattice-based Cryptography", Encyclopedia of Cryptography and Security, 2005

[6] C. K. Li, G. Yang, D. S. Wong, X. Deng, S. S. M. Chow, "An Efficient Signcryption Scheme with Key Privacy", Journal of Computer Security-The 2007 European PKI Workshop: Theory and Practice (EuroPKI'07), Vol 18, Issue 3, Aug 2012,Spain, pp451-473

[7] W. Diffie, M. Hellman. "New Directions in Cryptography", IEEE Transactions on Information Theory, 22(6), 1976.

[8] Y. Zheng, “Digital Signcryption or How to Achieve Cost(Signature & Encryption) << Cost(Signature) + Cost(Encryption)”, Proceedings of the 17th Annual International Cryptology Conference on Advances in Cryptology, London, UK, pp. 165-179.

[9] I. Dinur, G. Kindler, R. Raz, and S. Safra. “Approximating CVP to within almost polynomial factors is NP-hard” Combinatorica, 2003, Vol. 23, No. 2, pp. 205–243.

[10] O. Goldreich, D. Micciancio, S. Safra, and J.P. Seifert. “Approximating shortest lattice vectors is not harder than approximating closest lattice vectors”. Information Processing Letters, 1999, Vol. 71, No. 2, pp. 55–61

[11] J. Hoffstein, N. Howgrave-Graham, J. Pipher, and W. Whyte. “Practical Lattice-Based Cryptography: NTRUEncrypt and NTRUSign”. The LLL Algorithm, pages 349–390, 2010.

[12] E. Papoutsis, W. G. J. Howells, A. B. T. Hopkins, and K. D. McDonald-Maier, “Integrating Multi-Modal Circuit Features within an Efficient Encryption System”, Third International Symposium on Information Assurance and Security, IEEE Computer Society Washington, DC, USA, 2007, pp. 83-88.

[13] Myers, M., R. Ankney, A. Malpani, S. Galperin and C. Adams, 1999. “X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP”, RFC 2560, June 1999.

[14] Li F, Shirase M., Takagi T, “Certificateless Hybrid Signcryption”, The 5th Information Security Practice and Experience Conference (ISPEC 2009), LNCS 5451, Springer-Verlag, 2009, pp. 112-123.

[15] F. Wang, Y. Hu, and C. Wang, “Post-Quantum Secure Hybrid Signcryption from Lattice Assumption”, Applied Mathematics & Information Sciences Journal, Vol 6, No.1, pp.23-28.

[16] Bao, F. and R.H. Deng, 1998. A signcryption scheme with signature directly verifiable by public key. In Proceedings of Advances in Cryptology - PKC'98, LNCS 1431, Springer-Verlag, Berlin, 1998, pp.55-59.

[17] E. Papoutsis, W. G. J. Howells, A. B. T. Hopkins, and K. D. McDonald-Maier, "Ensuring Secure Healthcare Communications via ICmetric based Encryption on unseen Devices", Symposium on Bio-inspired, Learning and Intelligent Systems for Security, Edinburgh, 20-21 Aug. 2009, pp. 113-117.

[18] E. Papoutsis, W. G. J. Howells, A. B. T. Hopkins, and K. D. McDonald-Maier, "Integrating Feature Values for Key Generation in an ICmetric System," in IEEE NASA/ESA Conference on Adaptive Hardware and Systems (AHS-2009) San Francisco, California, 2009, pp. 82-88.