REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE
MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE SCIENTIFIQUE

**UNIVERSITE MOHAMED BOUDIAF - M'SILA**
**FACULTE DES MATHEMATIQUES ET DE L'INFORMATIQUE**

**DEPARTEMENT D'INFORMATIQUE**



**MEMOIRE de fin d'étude**

**Présenté pour l'obtention du diplôme de MASTER**

**Domaine** : Mathématiques et Informatique

**Filière** : Informatique

**Spécialité** : Réseaux

**Par** : Ghehioueche Amar Abdelmalek

**SUJET**

# Implémentation des primitives cryptographiques dans les réseaux de capteurs sans fil

**Soutenu publiquement le : 31/ 05 /2016 devant le jury composé de :**

| | | |
|---|---|---|
| Gasmia Salah | Université de M'sila | Président |
| Chikouche Noureddine | Université de M'sila | Rapporteur |
| Mezrag Fares | Université de M'sila | Co-Rapporteur |
| Tahri Zouhir | Université de M'sila | Examinateur |

**Promotion : 2015 /2016**

# Table des matières

## Chapitre 2 - CRYPTOGRAPHIE SYMETRIQUE



## Chapitre 3 - CRYPTOGRAPHIE ASYMETRIQUE

# INTRODUCTION GENERALE

La convergence des technologies de communication sans-fil et la micro-électronique a permis la création d'une combinaison entre les systèmes distribués et les systèmes embarqués ayant engendre les Réseaux de Capteurs Sans-fil (RCSF) ou en anglais Wireless Sensor Networks (WSN). Les RCSF sont formés par des petits outils électroniques, autonomes, contenant des capteurs. Ces réseaux sont capables de contrôler un endroit ou un événement important, de produire des informations nécessaires par l'ensemble des mesures détectées par divers capteurs et de les communiquées ensuite à travers les ondes radio à l'utilisateur.

Les RCSF sont appliqué dans différentes d'applications, telles que : militaires, médicales, environnementales domotiques, etc. Ces applications ont souvent besoin d'un niveau de sécurité important. Parmi les caractéristiques importantes de capteurs dans ce type de réseau, on cite la limitation de l'énergie, l'espace de mémoire et la puissance de calcul. Dans l'état de l'art de la cryptographie, on peut trouver plusieurs primitives cryptographiques développés. Les principales catégories de ces primitives sont : cryptosystèmes à clé privée, cryptosystèmes à clé public, signatures numériques et les fonctions de hachage. Pour cela, il faut choisir bien les primitives cryptographiques qui convient avec les caractéristiques des capteurs dans les RCSF.

Dans ce mémoire, on présente un état de l'art des principales primitives cryptographiques, et particulièrement les cryptosystèmes à clé public et cryptosystèmes à clé privée. Notre objectif est de pouvoir implémenter des différentes primitives étudies dans un capteur pour évaluer ses performance en terme de consommation de l'énergie, occupation de l'espace de mémoire, et temps d'exécution. Nos résultats expérimentaux sont basés sur l'utilisation de deux types des simulateurs : TOSSIM [43] et Avrora [42].

## Organisation du mémoire

Ce mémoire est organisé de la manière suivante :

**Chapitre 1 :**

Présentation des caractéristiques liées aux réseaux de capteurs sans fil, leurs domaines d'applications et leur contrainte. Ainsi l'architecteur de communication (pile protocolaire).

**Chapitre 2 :**

Dans ce chapitre nous commençons par citer une définition de la cryptographie et quelque conception principale. Ensuite nous présentons deux algorithmes de chiffrement symétrique (à clé privée).

**Chapitre 3 :**

Dans ce chapitre nous présentons des algorithmes cryptographiques asymétriques (à clé public), ainsi que la signature numérique.

**Chapitre 4 :**

Ce chapitre effectue une étude de simulation en utilisant l'environnement TinyOS et les simulateurs TOSSIM et Avrora. Ensuit on fait l'implémentation des différentes primitives étudiés avec l'évaluation des performances de ces primitives.

Nous finalisons ce mémoire par une conclusion et des perspectives, où nous présentons nos remarques concluantes et nos suggestions pour une recherche future.

# CONCLUSION GENERALE

Depuis quelques années, les avancées technologiques en termes de miniaturisation des machines et des supports de communication y afférant ont rendu envisageable le déploiement et l'exploitation de milliers de capteurs. D'ailleurs, les réseaux de capteurs ont été identifiés comme l'une des technologies clefs de l'avenir et ce en raison de l'incroyable potentiel applicatif qu'elle renferme. Cependant, en raison de la jeunesse de cette technologie, le domaine de réseaux de capteurs soulève d'importantes problématiques de recherche en termes de la sécurisation de ces réseaux.

Dans ce mémoire, nous avons présenté les caractéristiques essentielles des réseaux de capteurs sans fil, ainsi que les besoins et les défis de la sécurité dans ces derniers. Ensuite, Nous avons présenté des primitives cryptographiques de type symétrique, asymétrique, et signature numérique.

On a développé l'algorithme de chiffrement du cryptosystèmes McEliece en NesC et on a utilisé des bibliothèques cryptographiques (TinyECC, TinyPKC, etc.) pour implémenter les autres cryptosystèmes. On a implémenté les différents cryptosystèmes étudiés dans le système embarqué des réseaux de capteurs sans fil, le TinyOS. Basant sur cette implémentation et avec l'utilisation de deux simulateurs TOSSIM et Avrora, on a fait une étude comparative entre ces primitives en termes de (1) l'occupation de la mémoire ROM Flash et la mémoire RAM, (2) consommation de l'énergie de nœud de capteur, et (3) le temps de traitement.

Notre travail réalisé est une étape initiative pour proposer une nouvelle approche de sécurisation des protocoles de communication dans les RCSF en utilisant les primitives cryptographiques à bas coût, celui-ci une perspective de notre travail.

# BIBLIOGRAPHIE


[1] W. Diffie, E. Hellman, New Directions in Cryptography, IEEE Trans- actions on Information Theory, 1976, pp. 644–654.

[2] A. PACHA, N. HADJ-SAID, La Cryptographie et ses principaux systèmes de références, Université des Sciences et de la Technologie d' Or an, Vol 12 n°01, Année 2002.

[3] R. Dumont, Cryptographie et Sécurité informatique, Université de Liége, [En ligne] http://www.montefiore.ulg.ac.be/~dumont/ , consulté le : 05/01/2016.

[4] A. Biryukov, O. Dunkelman, N. Keller, D. Khovratovich and A. Shamir, Key Recovery Attacks of Practical Complexity on AES Variants With Up To 10 Rounds, Cryptology ePrint Archive, Report 2009/374, 2009.

[5] Y. Tian, G. Chen, J. Li, On the Design of Trivium, Shanghai Jiaotong University, China.

[6] I. Mallouli, Implémentation d'une bibliothèque de fonctions cryptographiques optimisées pour les réseaux de capteurs sans fil, Ingénieur, L'Ecole Nationale d'Ingénieurs de Sfax, 2011.

[7] C. De Cannière, B. Preneel, Trivium Specifications, Katholieke Universiteit Leuven Belgium, 2002.

[8] S. Ballet, A. Bonecaze, Courbes Elliptiques Application à la Cryptographie, Ecole Polytech de Marseille,http://alexis.bonnecaze.perso.luminy.univ-amu.fr/CryptoAvancee.pdf, consulté le : 25/2/2016

[9] H. Michael, Courbes elliptiques et cryptographie, Marusia Rebolledo, 2006, http://math.univ-bpclermont.fr/~rebolledo/page-fichiers/projetMichael.pdf, consulté le : 25/2/2016

[10] Z. KHERBACHE, A. LARIBI, Étude de la Qualité de Service (QoS) dans les réseaux WIFI, Master, Université Tlemcen, 2011.

[11] C. De Cannière, B. Preneel, "Trivium – A Stream Cipher Construction Inspired by Block Cipher Design Principles", Katholieke Universiteit Leuven Belgium, 2002.

[12] D. SOW, Courbes elliptiques, Cryptographie à clés publiques et Protocoles d'échange de clés, Doctorale, Dakar, 2013.

[13] C. Grenier, Techniques de cryptanalyse de RSA, 2009.

[14] Signature numérique, [En linge] http://pvbookmarks.readthedocs.io/en/latest/devel/security/signature_numerique. Consulté le : 15/4/2016

[15] D. Johnson, A. Menezes, and S. Vanstone. The elliptic curve digital signature algorithm (ECDSA). International Journal of Information Security, 1, pp. 36–63, 2001.

[16] 1978. Robert J. McEliece. "A public-key cryptosystem based on algebraic coding theory." Jet Propulsion Laboratory DSN Progress Report 42–44,114–116.

[17] P.-L. Cayrel, Construction et optimisation de cryptosystèmes basés sur les codes correcteurs d'erreurs, Doctorat, Université de Limoges, 2008.

[18] T. Peyrin, Analyse de fonctions de hachage cryptographiques, Doctorat, Paris, 2008.

[19] Y.SHOU, Cryptographie sur les courbes elliptiques et tolérance aux pannes dans les réseaux de capteurs, Doctorat, l'Université de Franche-Comté, 2014

[20] MD4 Message-Digest Algorithm, [En ligne] http://www.ietf.org/rfc/rfc1320.txt consulté le : 06/02/2016

[21] MD5 message-digest Algorithm. [En ligne] http://www.ietf.org/rfc/rfc1321.txt consulté le : 06/02/2016

[22] National Institute of Standards and Technology. FIPS 180-1: Secure Hash Standard, April 1995. [En ligne] http://csrc.nist.gov/groups/ST/hash/index.html consulté le : 07/02/2016

[23] National Institute of Standards and Technology. FIPS 180-2: Secure Hash Standard, August 2002. [En ligne] http://csrc.nist.gov/groups/ST/hash/index.html consulté le : 07/02/2016

[42] ZigBee Specification. Zigbee standards organization. Document 053474r17, Jan 17 (2008).

[25] C. Yacine, « Réseaux de Capteurs Sans Fils », support-SIT60, Vol. 103, pp. 14-17, 2008.

[26] D. Gay, P. Levis, R. von Behren, M. Welsh, E. Brewer, and D. Culler, "The nesC language: A holistic approach to networked embedded systems," in SIGPLAN Conference on Programming Language Design and Implementation (PLDI'03), 2003

[27] F. MEZRAG, Sécurité du Routage Hiérarchique Basé sur les Clusters dans les Réseaux de Capteurs sans Fil, Magister, Université Amar Telidji - Laghouat, 2015.

[28] S.Bouguer, étude et simulation comparative entre les réseaux de capteurs sans fils traditionnels et les réseaux de capteurs véhiculaires, Ingénieur, Université Tlemcen, 2012.

[29] N. Bounegta, N. Aici, Approche Décentralisé pour la sécurité d'un Réseau de Capteurs Sans Fil (RCSF), Ingénieur, Université de Bechar, 2010

[30] Adams and T. Jon. An introduction to IEEE STD 802.15. 4. in Aerospace Conference, pp. 8. IEEE (2006).

[31] T. Watteyne, Proposition et validation formelle d'un protocole MAC temps réel pour réseaux de capteurs linéaires sans fils, Laboratoire CITI 2004/2005.

[32] Y. Younes, Minimisation d'énergie dans un réseau de capteurs, magister, université mouloud Mammeri de Tizi-Ouzou ,2012

[33] I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, E. Cayirci. "Wireless sensor networks: a survey". Computer Networks 38, Elsevier Science, pp. 393–422, 2002.

[34] S. Maarouf, S. Ouadah, Implémentation et évaluation des schémas de routage sur une plateforme réelle de réseaux de capteurs sans fil, Master, Université Tlemcen, 2014.

[35] M.Messai, Sécurité dans les Réseaux de Capteurs Sans-Fil, Magistère, Université Abderrahmane Mira de Bejaia, 2008.

[36] Crow, P. Brian, Widjaja, Indra, Kim, LG, Sakai, and T. Prescott. IEEE 802.11 wireless local area networks. Communications Magazine, IEEE 35(9), pp.116–126 (1997).

[37] IEEE 802.11, [En linge] http://www.ieee802.org/11/, Consulté le: 15/04/2016

[38] Eklund, Carl, Marks, B. Roger, Stanwood, L. Kenneth, Wang, and Stanley. IEEE standard 802.16: A technical overview of the WirelessMAN/sup TM/air interface for broadband wireless access. Communications Magazine, IEEE 40(6), 98–107 (2002).

[39] IEEE 802.16, [En linge] http://www.ieee802.org/16/, Consulté le : 15/04/2016

[40] SIG Bluetooth. Inc., specification of the Bluetooth system: Core, (2001).

[41] M.HADJILA, protocoles de routage économes en énergie pour les réseaux de capteurs sans fil, Doctorat, Université De Tlemcen, 2014.

[42] Ben L. Titzer, al, "Avrora: Scalable Sensor Network Simulation with Precise" Timing, 2005

[43] Simulateur TOSSIM, [En linge] http://tinyos.stanford.edu/tinyos-wiki/index.php/TOSSIM consulté le : 06/05/2016.

[44] Tinyos Documentation Wiki [En linge], http://tinyos.stanford.edu/tinyos-wiki/index.php/TinyOS_Documentation_Wiki. Consulté le : 29/04/2016

[45] CyaSSL [En linge], http://www.yassl.com/yaSSL/Products-cyassl.html consulté le:10/05/2016

[46] Tiny ecc page officielle [En linge], http://discovery.csc.ncsu.edu/software/TinyECC/. consulté le : 11/05/2016.

[47] Trivium site officielle [En linge], http://www.ecrypt.eu.org/stream/triviumpf.html consulté le : 12/05/2016

[48] I.MANSOUR, Contribution à la sécurité des communications des réseaux de capteurs sans fil, Doctorat, Université BLAISE PASCAL, 2013.

## ملخص

شبكة الاستشعار اللاسلكية تتزايد أهميتها وهذا نظرا لتواجدها في العديد من المجالات منها: العسكري والطبي ...إلخ، تلك التطبيقات تتطلب مستوى عالي من الأمن نظرا لحساسية هذه المجالات. في عملنا هذا نقدم مجموعة من خوارزميات التشفير المهمة. هدفنا الرئيسي هو استعمال وتطبيق هذه الخوارزميات في جهاز الاستشعار لتقييم أدائها بشأن استهلاك الطاقة، والتخزين في الذاكرة ووقت التنفيذ. نتائجنا تعتمد على استخدام نوعين مختلفين من أجهزة المحاكاة TOSSIM وAVRORA.



**الكلمات المفتاحية:** شبكة الاستشعار اللاسلكية،خوارزميات التشفير،TOSSIM، AVRORA.



## Résumé

Les réseaux de capteurs sans fil (RCSF) sont de plus en plus importants du fait qu'ils sont présents dans de nombreuses applications telles que : militaires, médicales…etc. Ces applications ont souvent besoin d'un niveau de sécurité important. Dans ce mémoire, on présente un état de l'art des principales primitives cryptographiques. Notre objectif est de pouvoir implémenter des différentes primitives étudies dans un capteur pour évaluer ses performance en terme de consommation de l'énergie, occupation de l'espace de mémoire, et le temps d'exécution. Nos résultats expérimentaux sont basés sur l'utilisation de deux types des simulateurs : TOSSIM et Avrora.



**Mots-clés** : RCSF, primitives cryptographique, capteur, TOSSIM, Avrora.



## Abstract

The wireless sensor networks (WSN) are growing more important that they exist in many applications such as: military, medical…etc. These applications require a high security level. In our work, we represent state of the art about cryptographic primitives. Our main objective is to implement different studied primitives in a sensor to evaluate its performance concerning the energy consumption, the occupied storage and the execution time. Our results based on using two different types of simulators: TOSSIM and Avrora.



**Keywords:** WSN, cryptographic primitives, TOSSIM, Avrora.