

Universidad de
Santiago de Chile, USACH



Departamento de Ingeniería
Industrial

UNIVERSITY OF
NEWCASTLE UPON TYNE



School of Electrical, Electronic
and Computer Engineering
University of Newcastle upon Tyne
Merz Court
NE1 7RU
Head of School
Professor O R Hinton

Secure data compression with coding and sphere packing

I. Soto, H. Rodriguez, C. Valencia and R. Carrasco

PBCT/CONICYT ACT11/04 – Chile

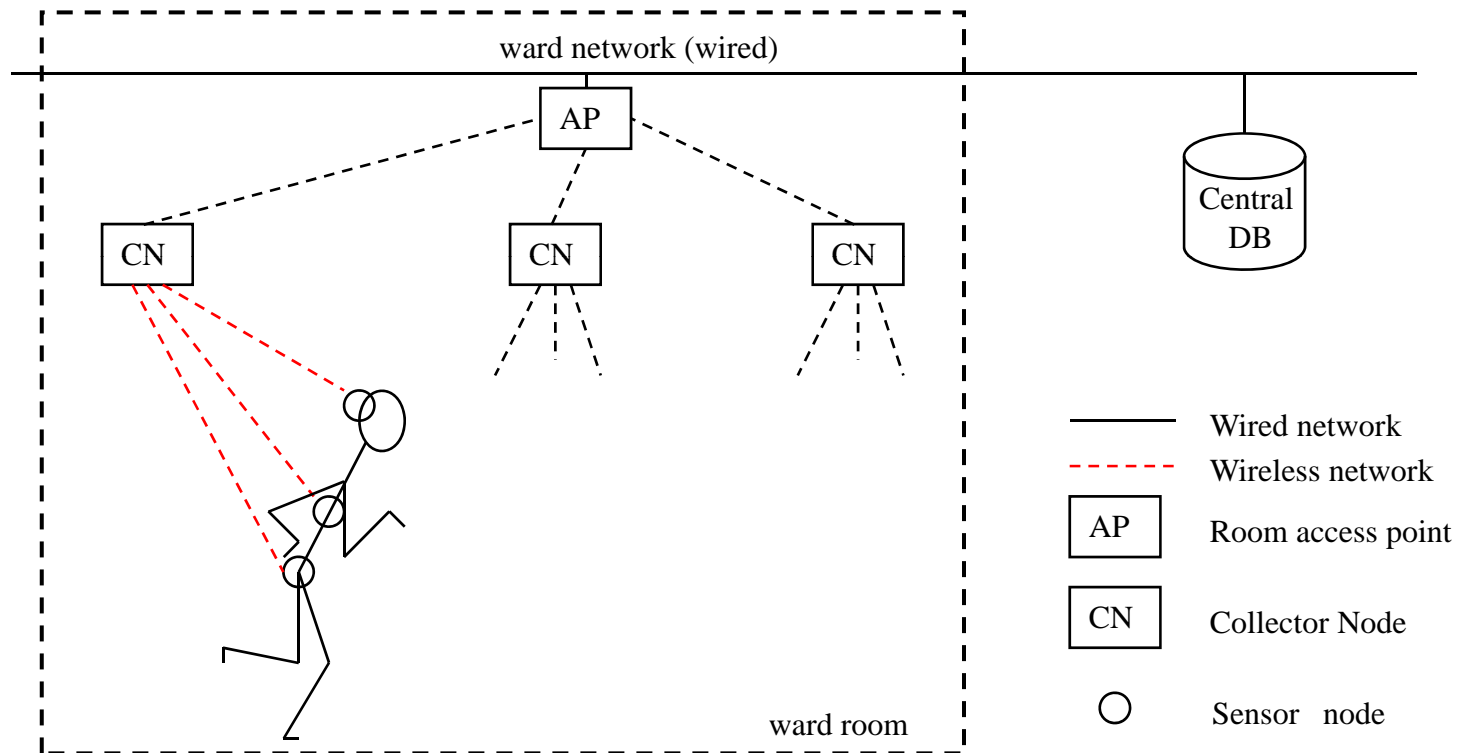
Index

1. Objective
2. A Wireless Sensor Network Model
3. Channel Models
4. Elliptic Curve
5. Lattice
6. LDPC Coding
7. Encryption and Encoding
8. Decoding and Decryption
9. Results
10. Conclusions

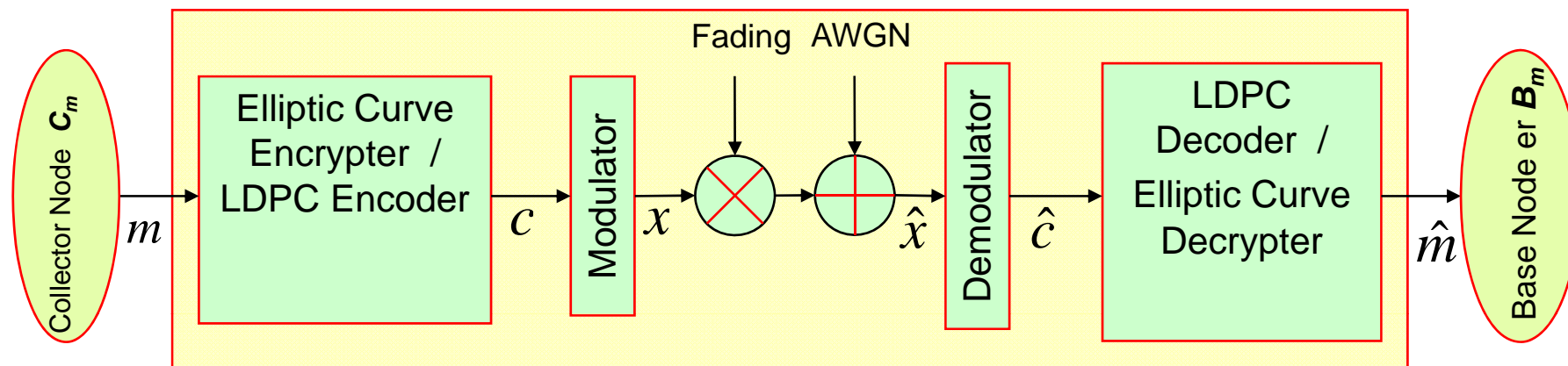
Objective

Propose a public key encryption scheme for wireless sensor networks, based on algebraic curves concatenated with sphere packing and a Low Density Parity Check code.

A WSN Model



Channel Model



m : Binary message sequence transmitted by the sender

c : Codeword

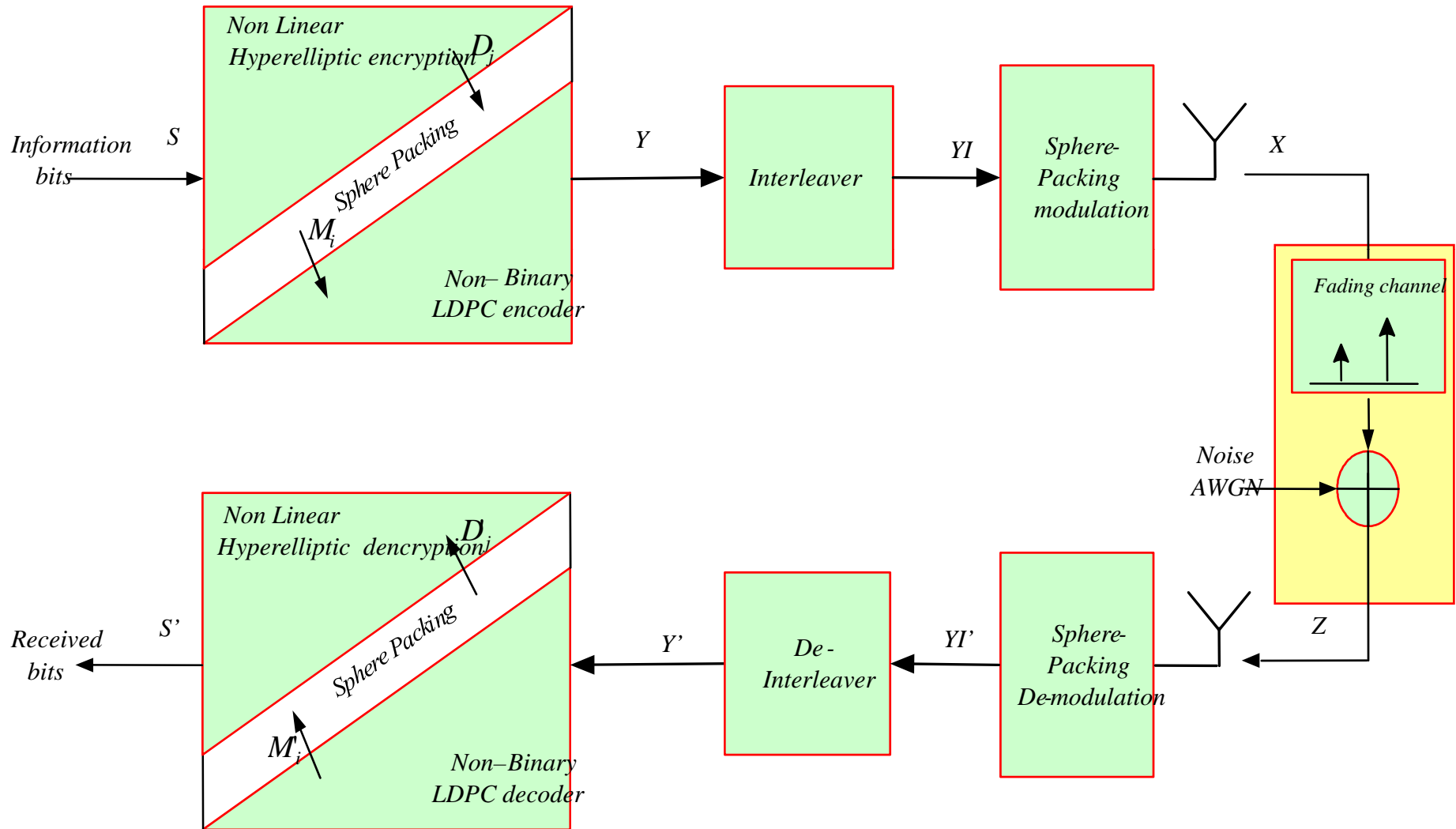
x : Modulated signal

\hat{x} : Modulated signal contaminated with noise

\hat{c} : Estimated codeword

\hat{m} : Estimated binary message sequence.

Channel Model



Rician Fading Channel

When the received signal is composed of multiple reflected rays and a component Line-of-sight, the enveloping of the received signal have a pdf given by:

$$p(r_0) = \begin{cases} \frac{r_0}{\sigma^2} \exp\left[-\frac{(r_0^2 + A^2)}{2\sigma^2}\right] I_0\left(\frac{r_0 A}{\sigma^2}\right) & \text{for } r_0 \geq 0, A \geq 0 \\ 0 & \text{in other case} \end{cases}$$

Rayleigh Fading Channel

When spectral components are reduced to zero, it has a pdf given by:

$$p(r_0) = \begin{cases} \frac{r_0}{\sigma^2} \exp\left[-\frac{r_0^2}{2\sigma^2}\right] & \text{for } r_0 \geq 0 \\ 0 & \text{in other case} \end{cases}$$

Elliptic Curve

In the a finite field F_{2^n} is defined as the set of points that satisfies the equation:

$$E(F_{2^n}): y^2 + xy = x^3 + ax^2 + b$$

where and in $a, b \in F_{2^n}$ and $b \neq 0$ in F_{2^n}

n-dimensional lattice

$$\Lambda_n = \left\{ (x_0, x_1, \dots, x_n) \in \mathbb{Z}^{n+1} : x_0 + \dots + x_n = 0 \right\}$$

LDPC

LDPC codes are a class of linear block codes characterized to have its parity-check matrix dispersed. A few 1's in comparison to the amount of 0's

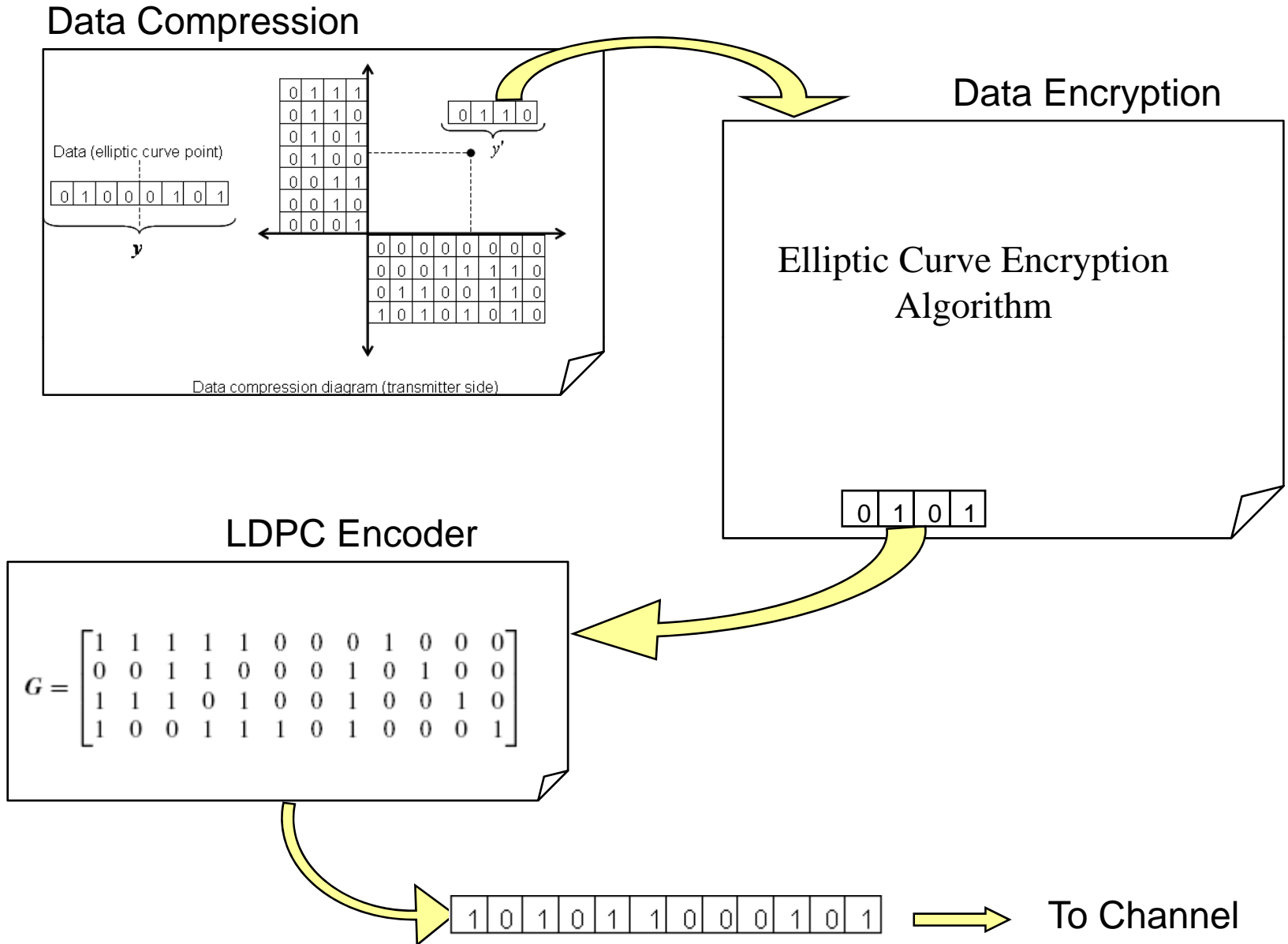
There are two kinds of LDPC codes: regular and irregular

C(12,4)

$$G = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 \end{bmatrix}$$

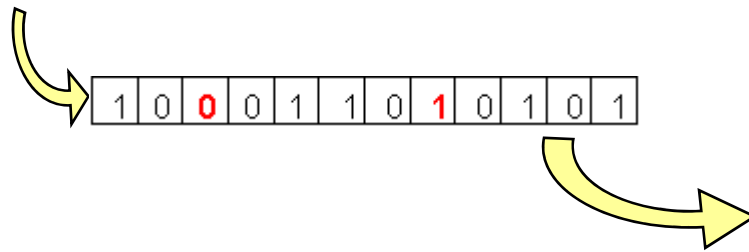
$$H = \begin{bmatrix} 0 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}$$

Encryption and Encoding

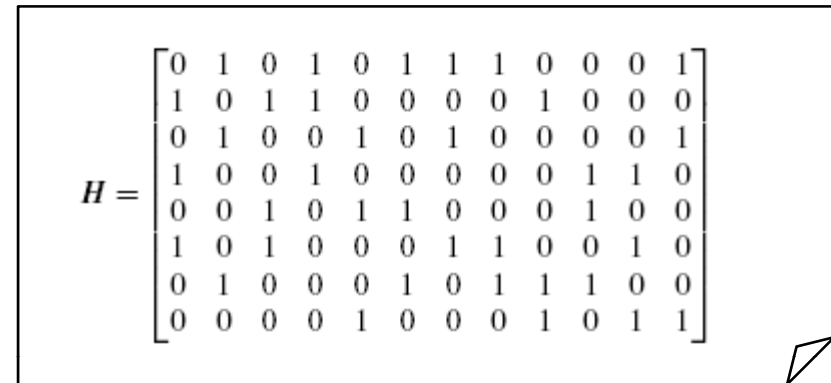


Decoding and Decryption

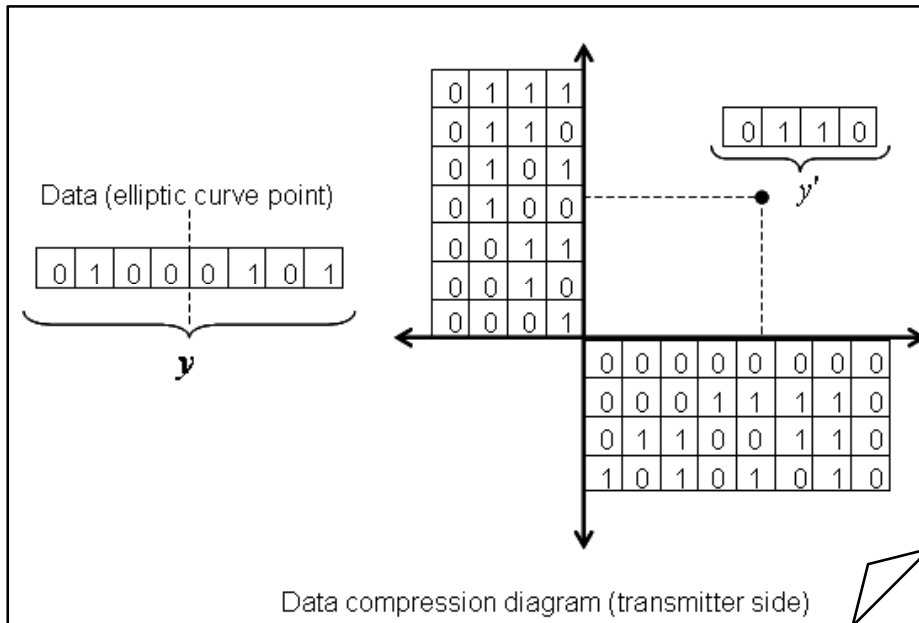
From Channel



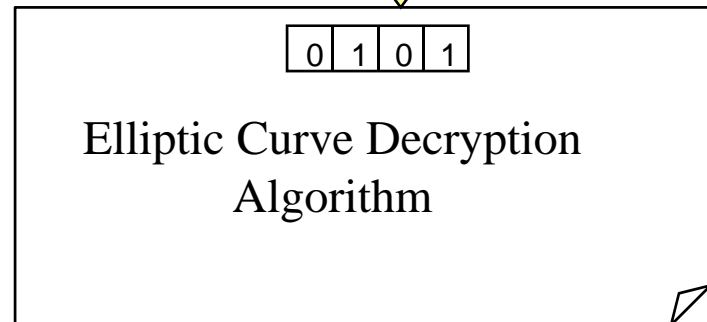
LDPC Decoder (*Iterative Process*)



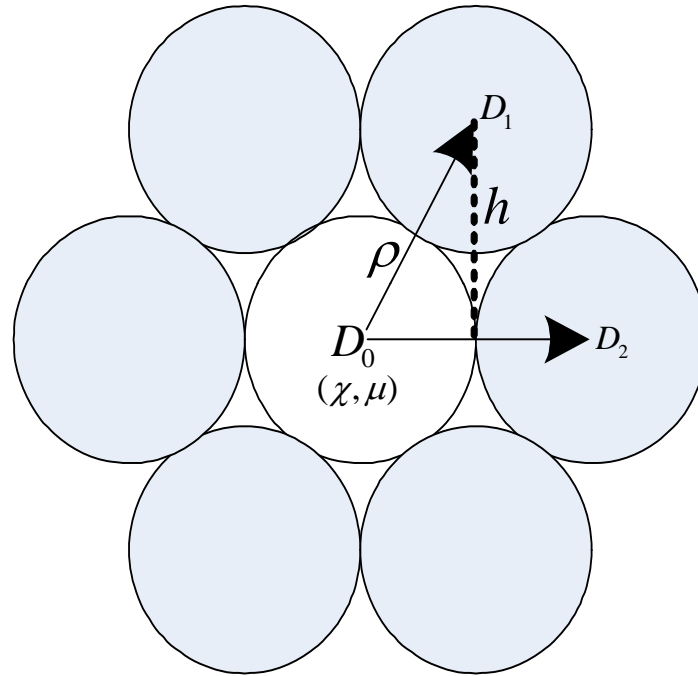
Inverse Mapping



Data Decryption

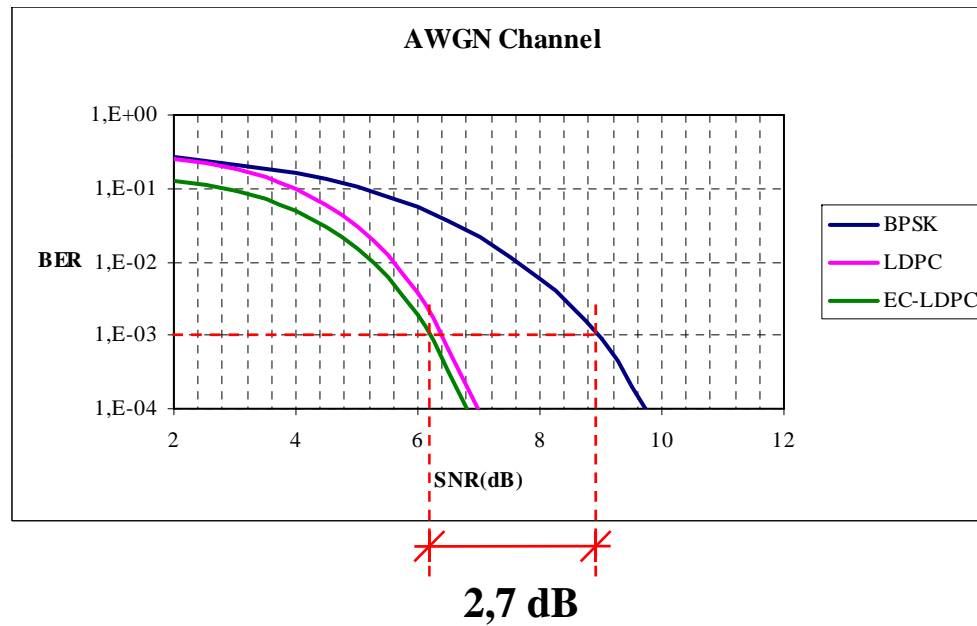


Sphere packing

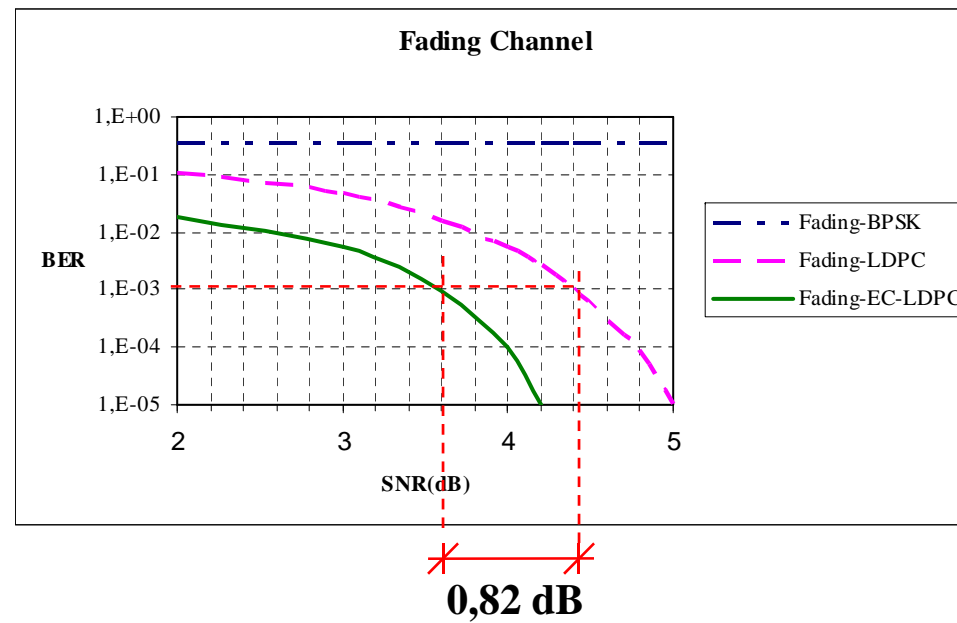


$$M_{\chi, \mu} = \begin{bmatrix} \rho + \chi & \mu \\ \rho / 2 & h + \mu \end{bmatrix}$$

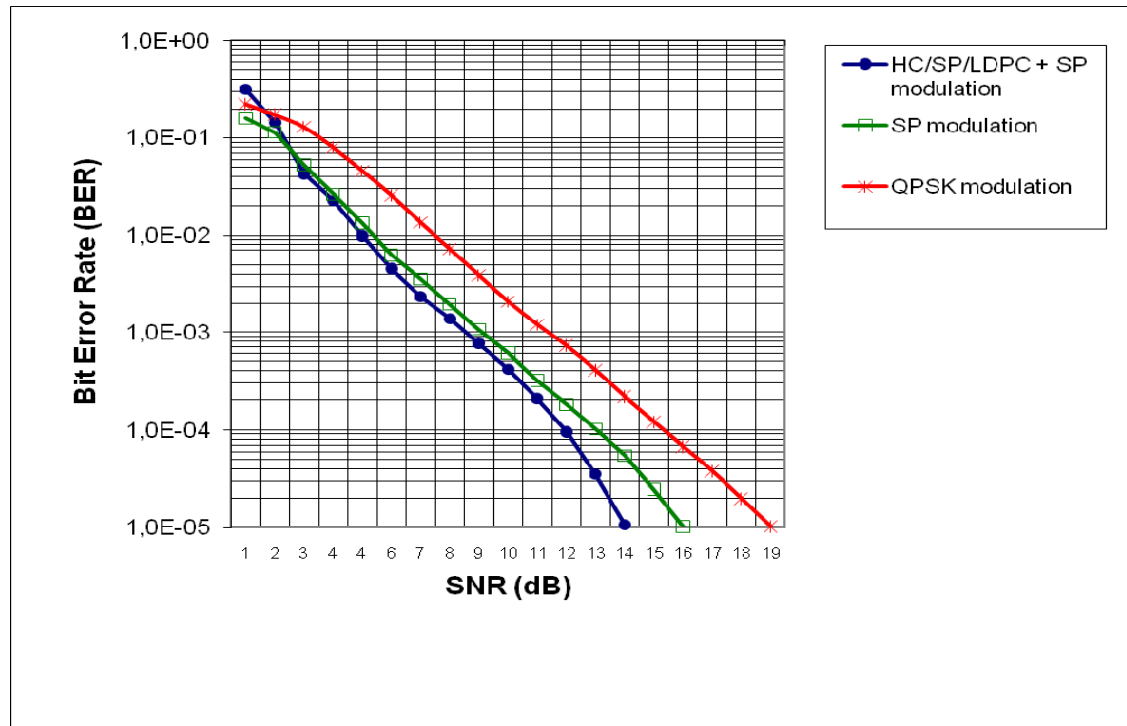
Results



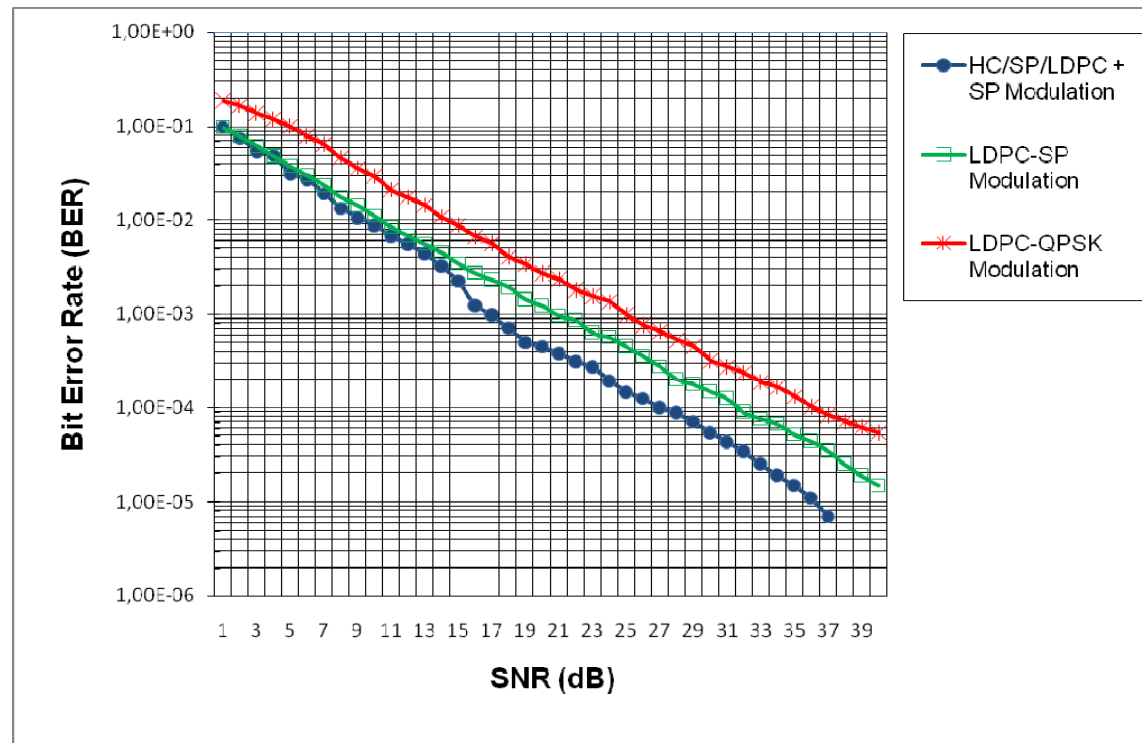
Results



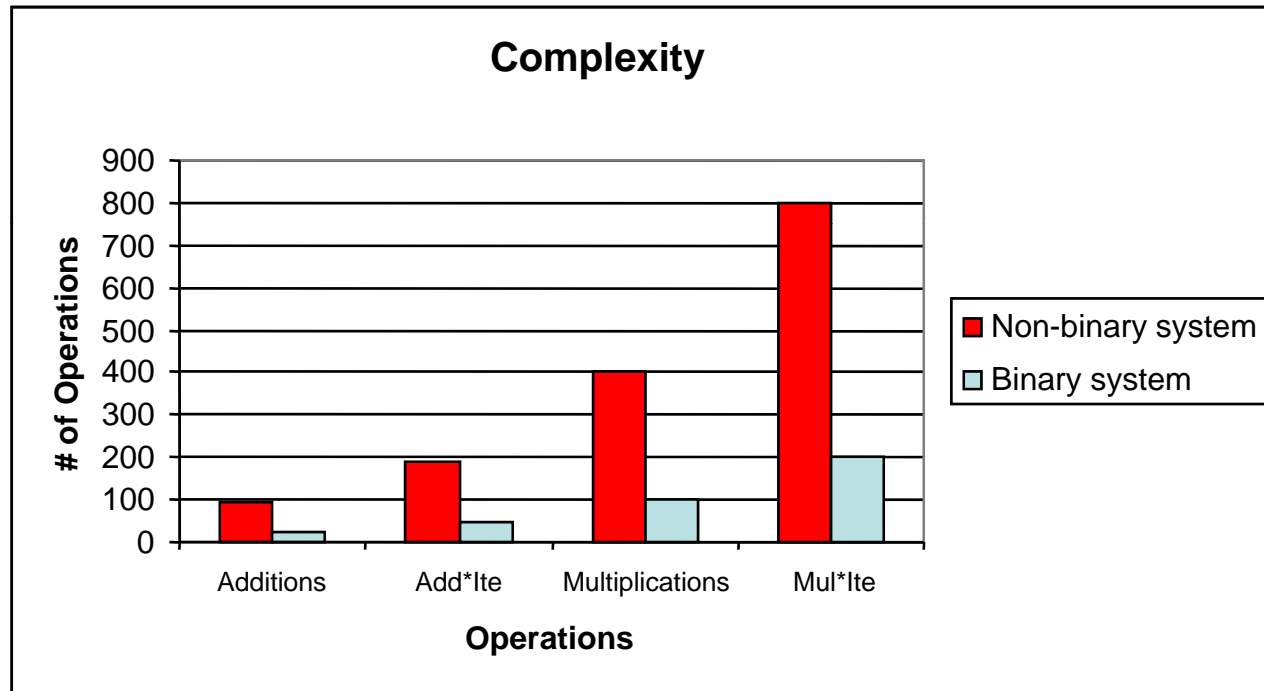
Results



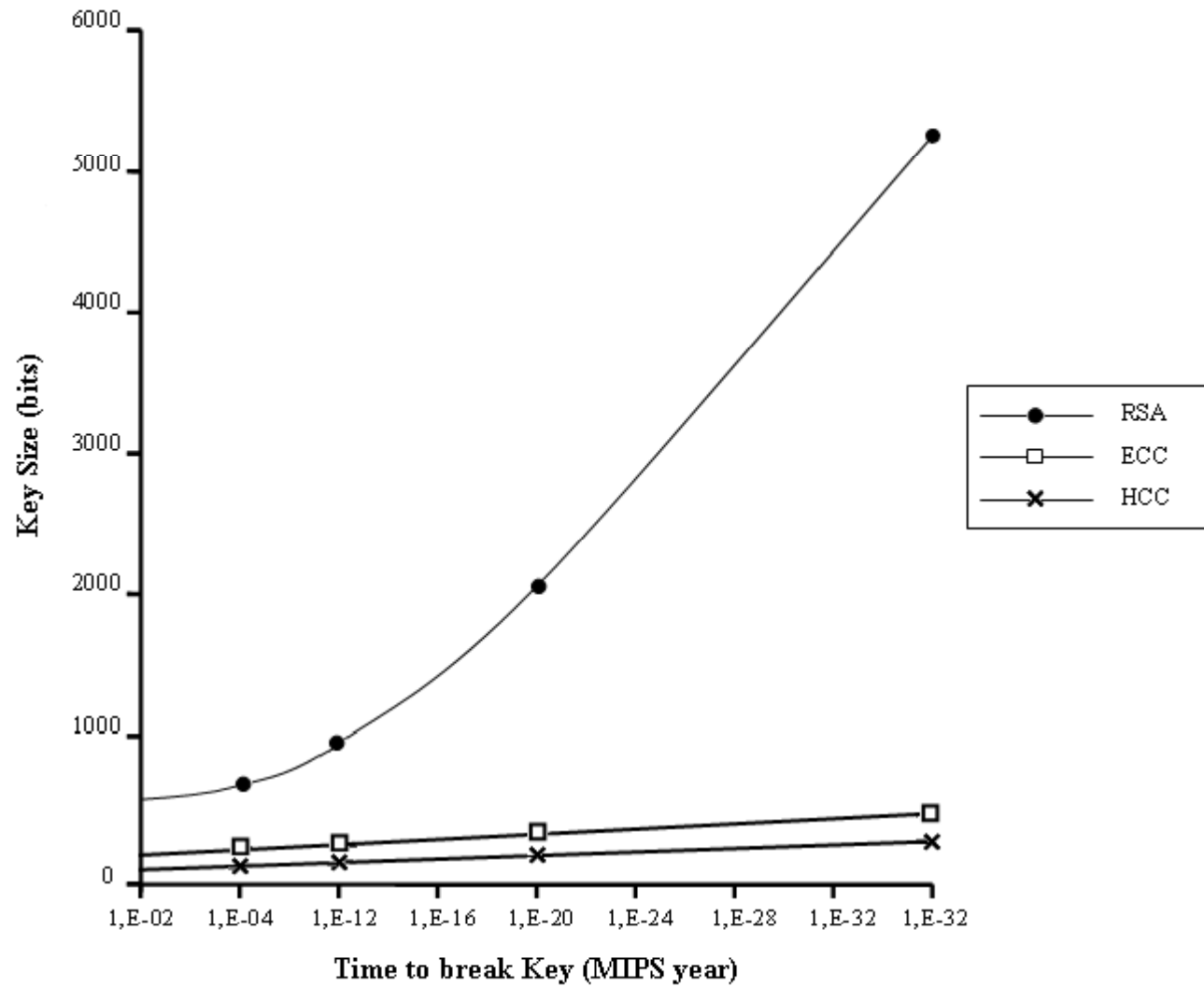
Results



Results



Security Level



Conclusions

1. A new public key encryption scheme for wireless sensor networks has been presented, which combined codes and encryption.
2. The use of encryption and encoding to the channel level allows the save of energy in each node of the WSN, according to the curve and code in use an improvement of 2.7 dB for Gaussian and 0.82 dB for Rayleigh can be achieved in each pair of nodes.
3. The concatenation of a hyper-elliptic curve with sphere packing and a non-binary LDPC code generates gains over three channels, an AWGN channel, a one tap fading channel, and a two taps fading channel, which means more information is transmitted in a shorter time and in a sure way.
4. It is important to mention that future communication systems, such as quantum processors, will probably incorporate non-binary finite fields in their elements. Given that, the proposed system is suitable for that demand, although the complexity is greater than that of previous systems.

Universidad de
Santiago de Chile, USACH



Departamento de Ingeniería
Industrial

UNIVERSITY OF
NEWCASTLE UPON TYNE



School of Electrical, Electronic
and Computer Engineering
University of Newcastle upon Tyne
Merz Court
NE1 7RU
Head of School
Professor O R Hinton

Secure data compression with coding and sphere packing

I. Soto, H. Rodriguez, C. Valencia and R. Carrasco

PBCT/CONICYT ACT11/04 – Chile