Lightweight Stream Cipher Scheme for Resource-Constrained IoT Devices

WIMOB 2019 – October 21st – 23rd, 2019
Casa Convalescència, Barcelona, Spain

Authors: Hassan Noura, Raphaël Couturier, CongDuc Pham and Ali Chehab

Presented on October 22nd, 2019 by Prof. Congduc Pham

Prof. Congduc Pham
http://www.univ-pau.fr/~cpham
Université de Pau, France

IoT – from idea to reality

Deploying IoT in Africa

[technology does not automatically or inevitably improve people's lives; creative solutions must be contextually grounded and designed in response to on-the-ground needs]

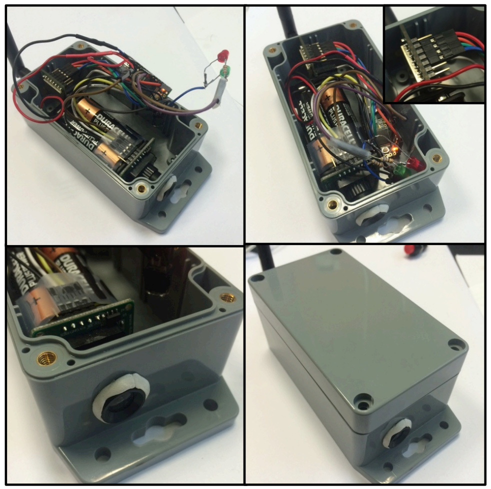
From Bill & Melinda Gates foundation, Global Grand Challenges

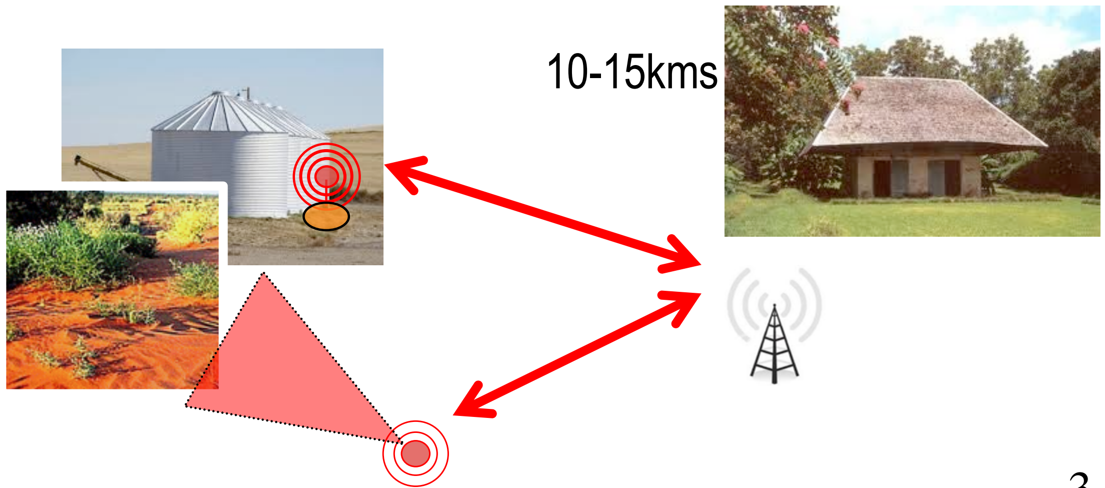
Needs, constraints, cost, design approach, control mechanism

Challenge: Bridging the digital divide

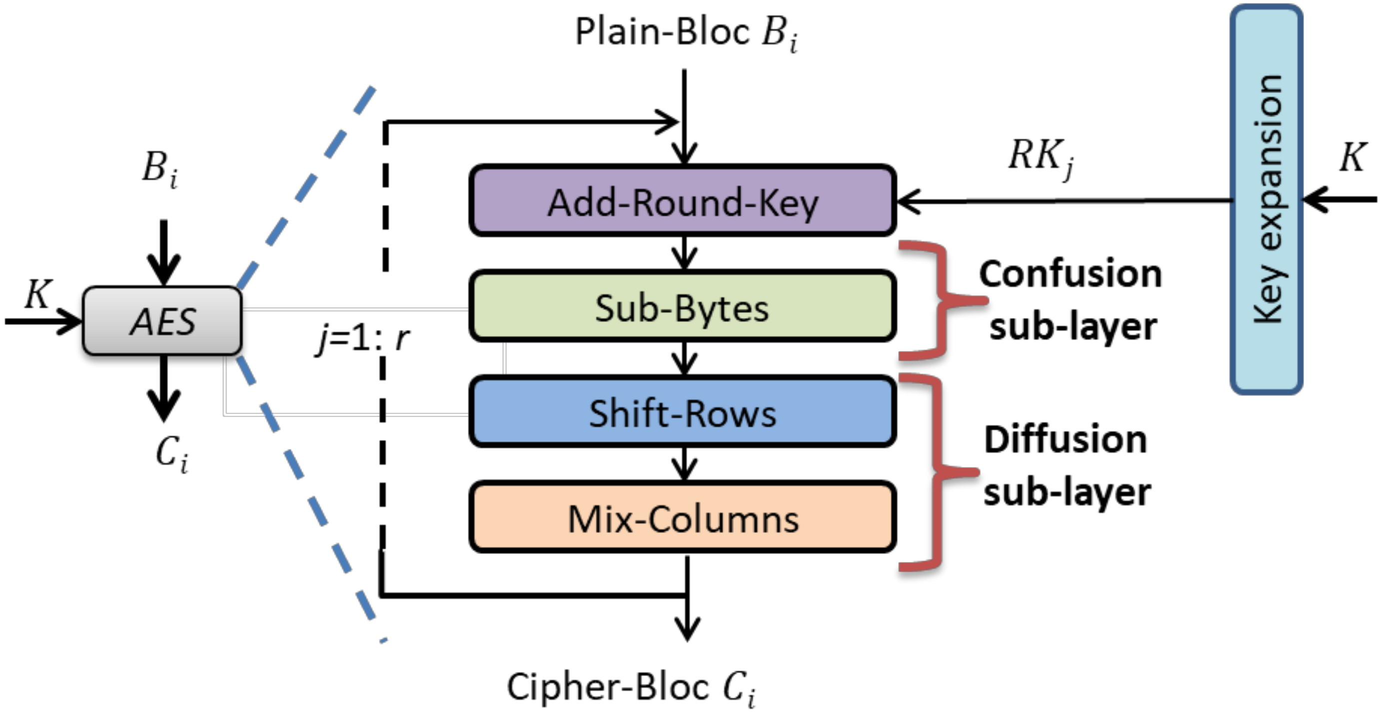
IoT security

- Introducing security/encryption can dramatically impact the IoT system performance
  - Higher computation
  - Additional delays
  - Higher energy consumption, thus decreasing lifetime
- Innovative IoT systems can have larger amount of data to send
  - Image IoT devices





Symmetric cryptographic algorithms



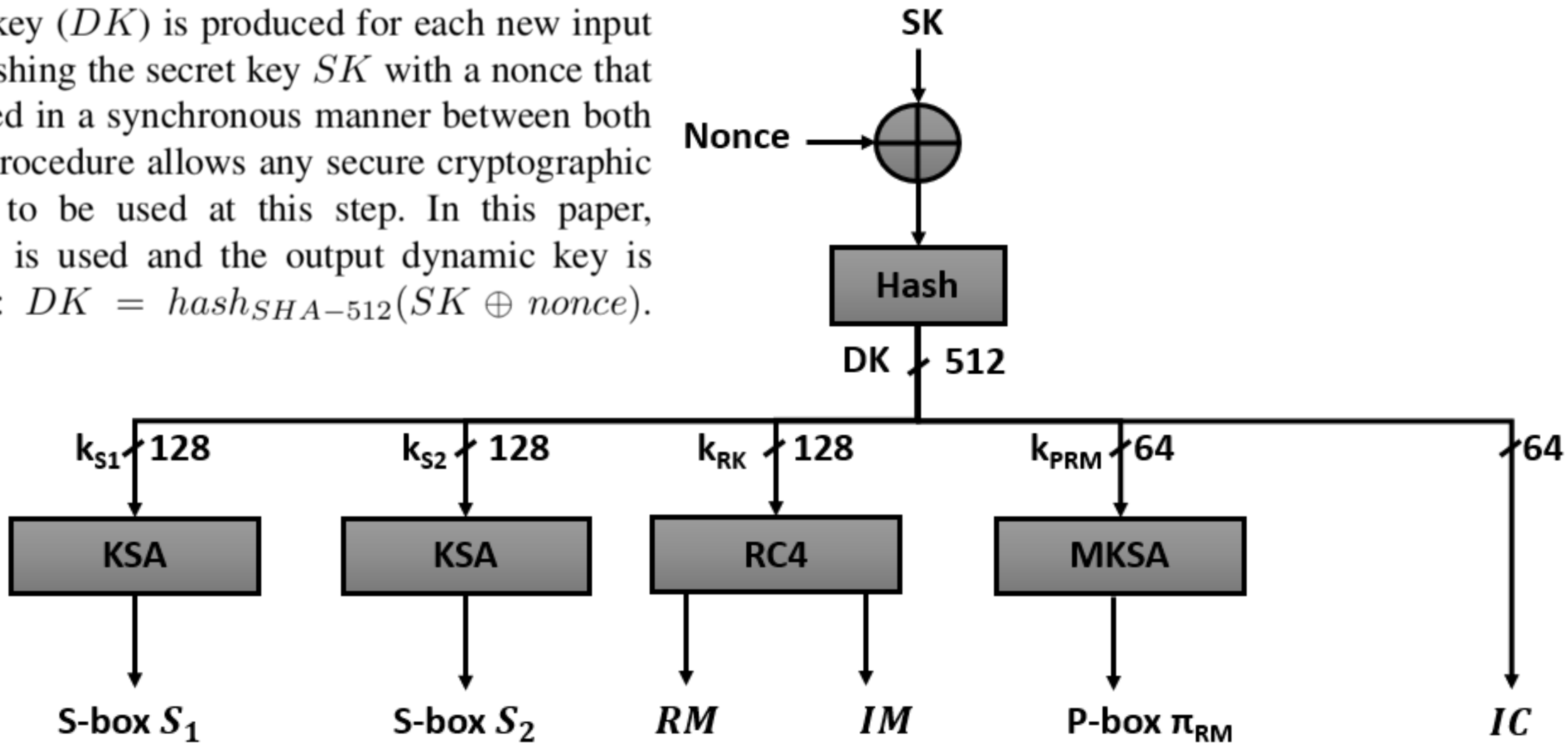
|K|	r
128	10
196	12
256	14

Requires a large number of rounds and operations such as AES (Advanced Encryption Standard) because round functions are usually static

Proposed approach

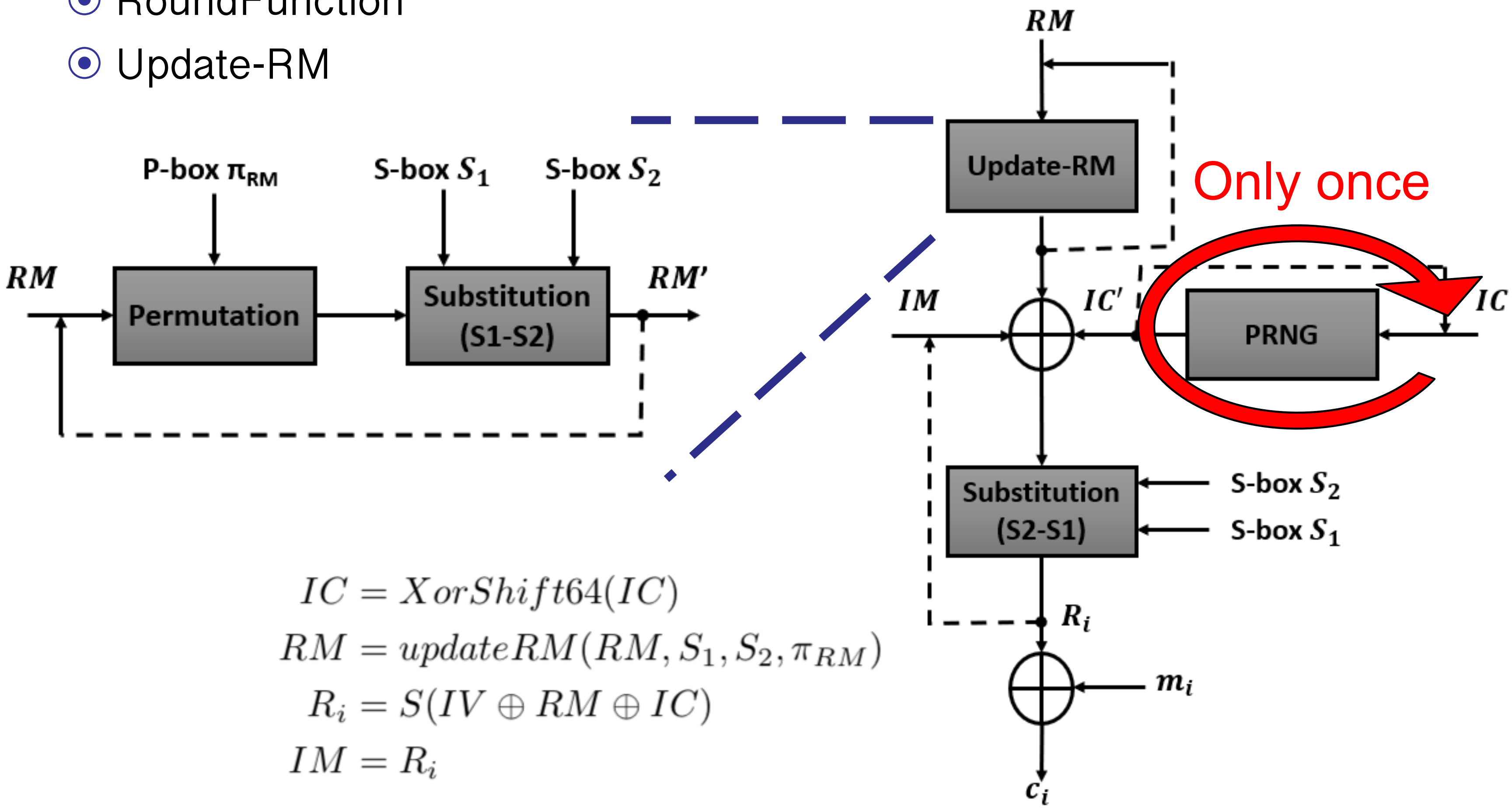
- Lightweight Stream Cipher: dynamic key derivation function

A dynamic key (DK) is produced for each new input message by hashing the secret key SK with a nonce that can be produced in a synchronous manner between both entities. This procedure allows any secure cryptographic hash function to be used at this step. In this paper, SHA-512 [11] is used and the output dynamic key is 64 bytes long: $DK = hash_{SHA-512}(SK \oplus nonce)$.



Cipher scheme

- LSC's Cipher scheme is divided into two sub-functions
  - RoundFunction
  - Update-RM



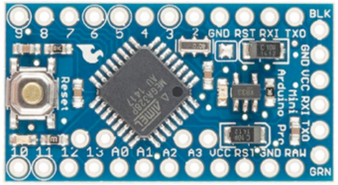
$$IC = XorShift64(IC)$$
$$RM = updateRM(RM, S_1, S_2, \pi_{RM})$$
$$R_i = S(IV \oplus RM \oplus IC)$$
$$IM = R_i$$

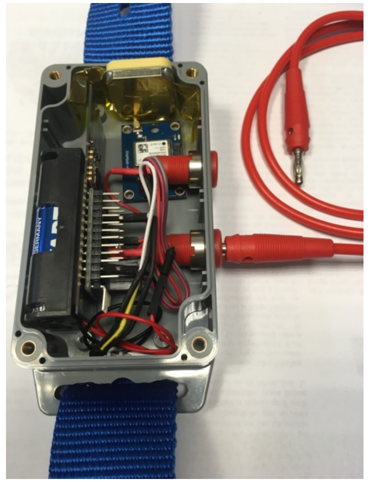
LSC's main advantages

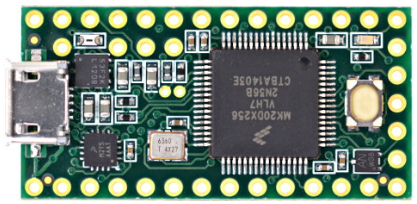
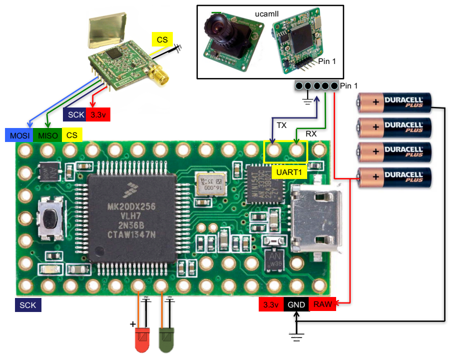
- LSC is based on the dynamic key dependence approach and therefore can use only one iteration which requires less computation and resources
- LSC also avoids chaining and diffusion operations to further reduce the computational complexity
- LSC updates the cryptographic primitives after each encrypted/decrypted block to provide a higher security level
- Minimum effect of error propagation as LSC encrypts 1 block at a time instead of 2 blocks
- Overall, it can result in simpler implementation

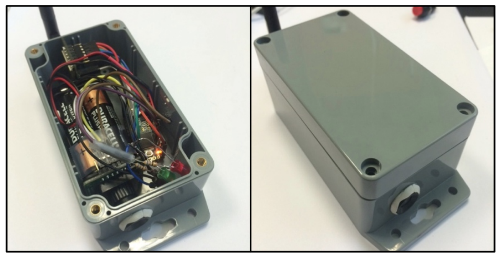
Analysis

- Security analysis
  - Randomness analysis
  - Key sensitivity
  - Message sensitivity
- Performance analysis
  - Using low-end microcontroller: 8-bit ATmega328P, 2K RAM, 8MHz
  - Using high-end micro-controller: 32-bit Cortex-M4, 96K RAM, 48MHz
- Comparison between
  - AES (multi-round)
  - Speck (multi-round, light)
  - LSC (single-round, light)







56° lens

76° lens

116° lens

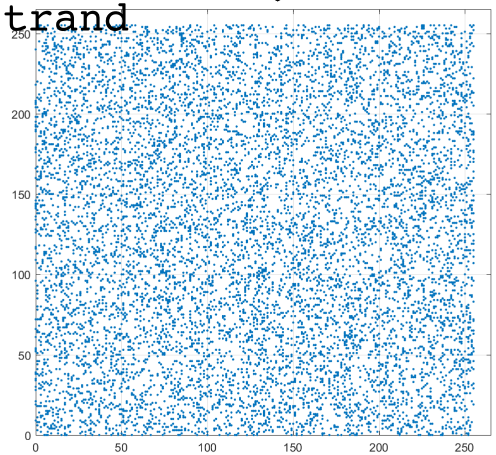
Randomness analysis

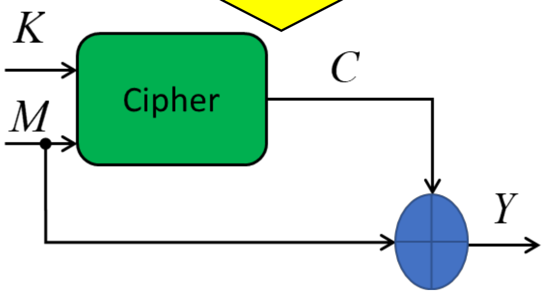
The encrypted message should reach a high level of randomness

Two different tests can be applied to quantify the randomness level, which are :

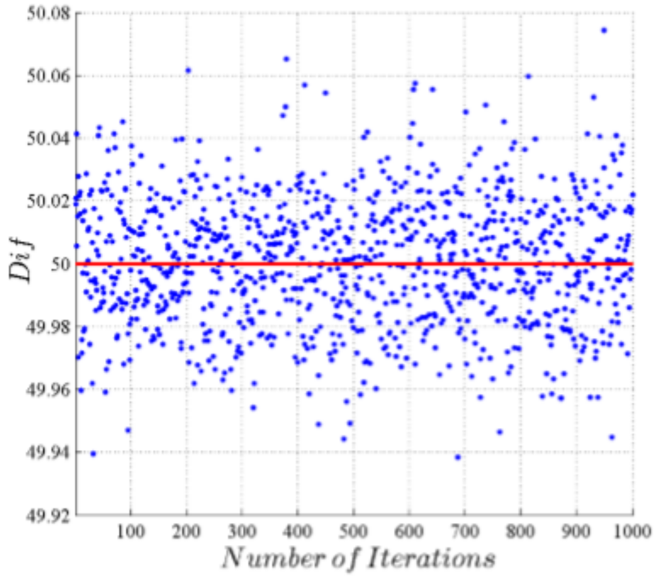
the correlation between adjacent elements	the difference between the original and encrypted

TestU01
practrand





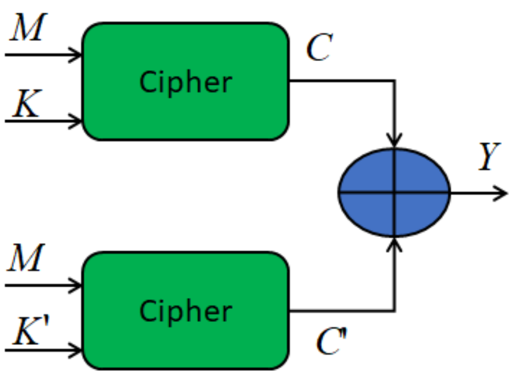
$$\frac{\text{Counts of bit occurrences in Y}}{\text{Length of Y in bit level}} \times 100$$



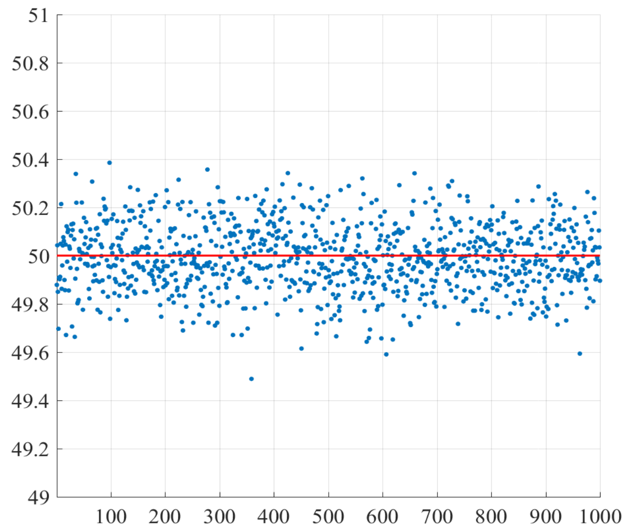
cipher scheme reaches the independence if and only if it satisfies *Diff* ≈50%

Key sensitivity

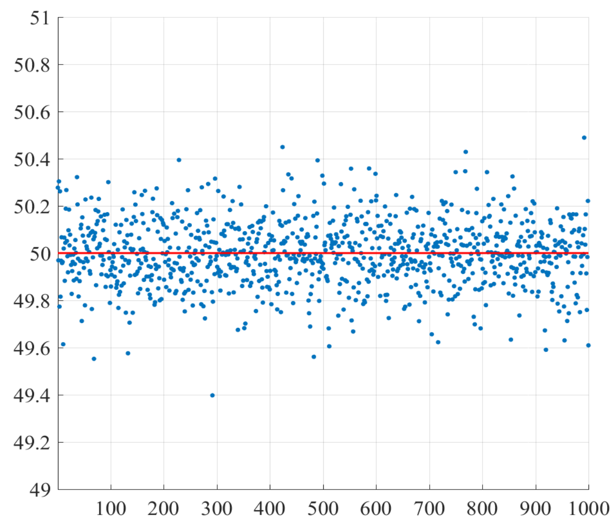
- Difference in percentages between the encrypted messages, if one bit differs in the secret key (i.e. our dynamic key)
- The desired value is 50% difference at the bit level.



$$KS = \frac{\text{Counts of bit occurrences in } Y}{\text{Length of } Y \text{ in bit level}} \times 100\%$$



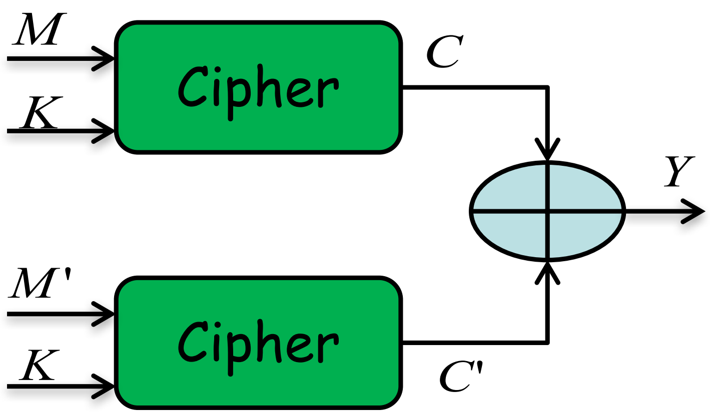
Key



Nonce

Prof. Congduc Pham
http://www.univ-pau.fr/~cpham

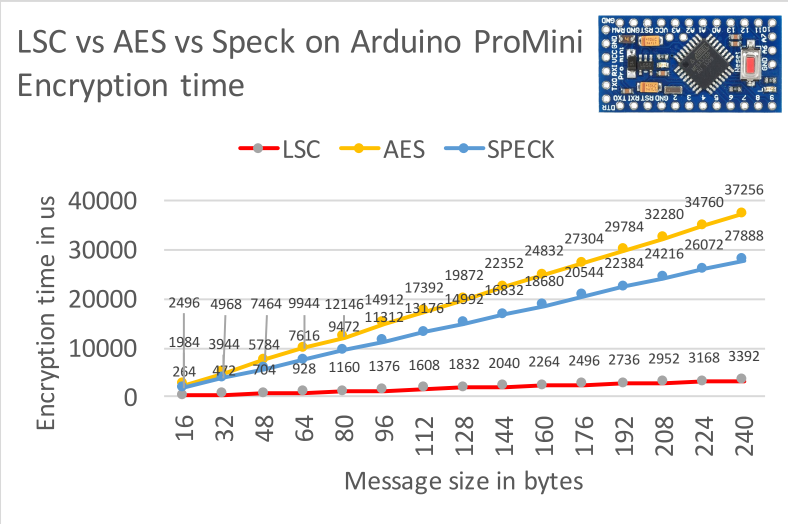
Message sensitivity

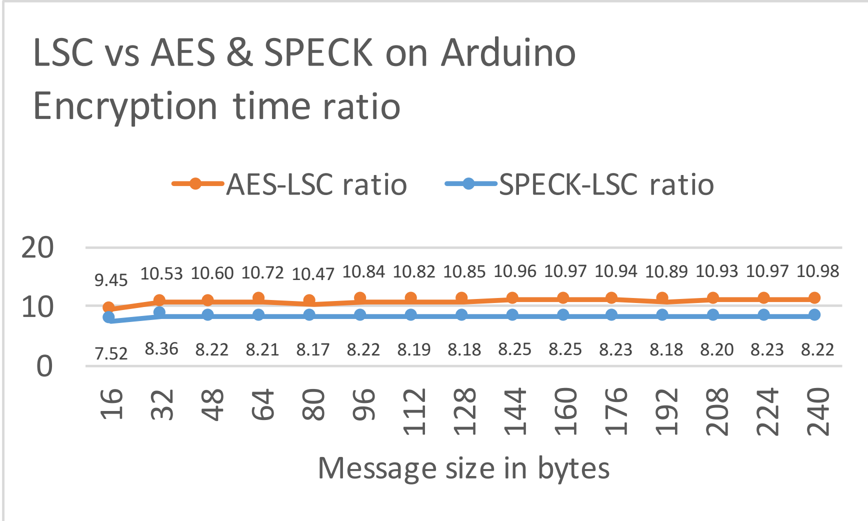


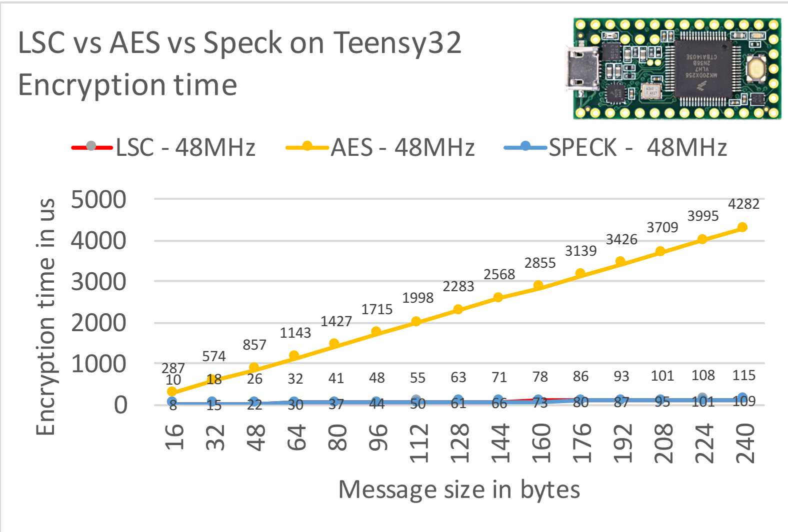
$$PS = \frac{\text{Counts of bit occurrences in } Y}{\text{Length of } Y \text{ in bit level}} \times 100\%$$

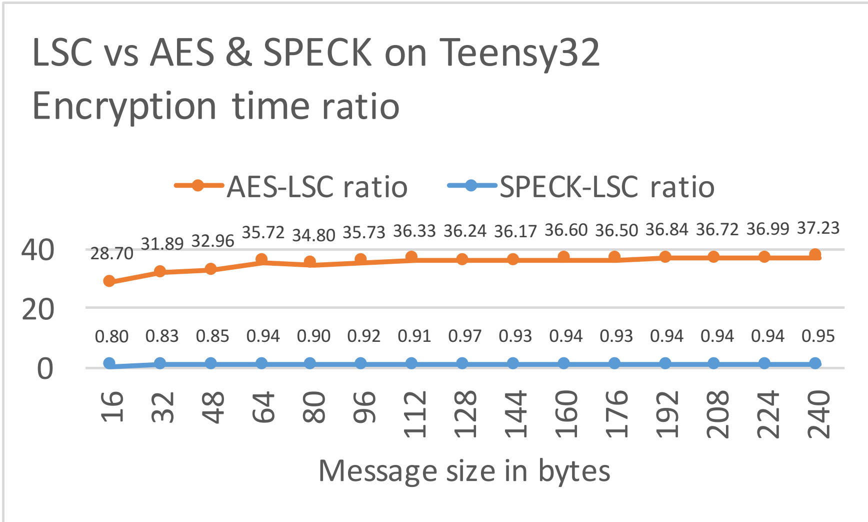
- LSC uses a dynamic key approach which changes cipher primitives for each input message
- Identical messages will then be encrypted under different dynamic keys and consequently different encrypted messages will be obtained (difference close to 50%)

Performance









Conclusions

- an efficient lightweight stream cipher scheme (LSC) was proposed for tiny IoT devices
- existing standard ciphers are not adapted for these devices since a higher number of round iterations is required to reach the desired security level (because of static round function)
- LSC is based on the dynamic key dependence approach to reach a good balance between security level and device's performance
- statistical tests and experimentations on real IoT hardware show that LSC is a promising candidate for resource-constrained IoT
- outperforming traditional AES in terms of encryption/decryption time as well as the more recent Speck algorithm on low-end microcontrollers

Prof. Congduc Pham
http://www.univ-pau.fr/~cpham