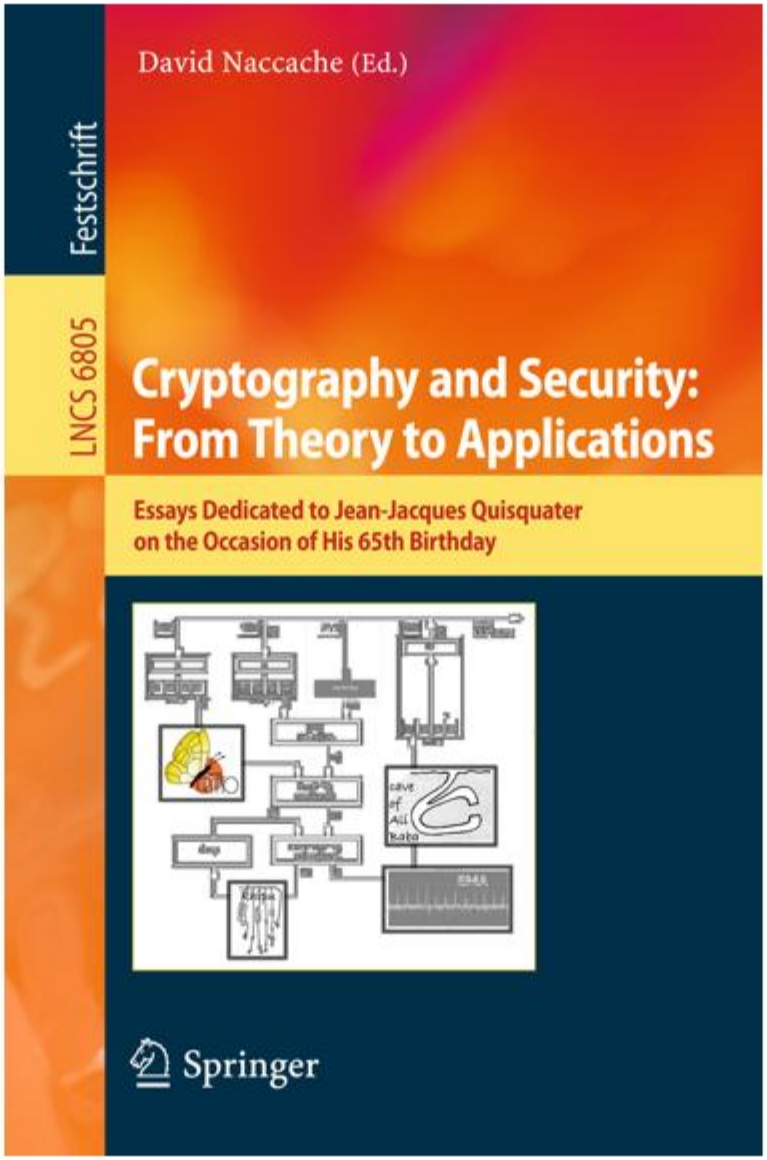
Complete Cover deCryption: the Challenge of LNCS 6805

Jean-Jacques Quisquater
UCL Crypto Group
Louvain-la-Neuve
jjq@uclouvain.be

Rump session EUROCRYPT '12
Cambridge, UK

twitter : @_jjq


Festschrift
LNCS 6805
David Naccache (Ed.)
Cryptography and Security:
From Theory to Applications
Essays Dedicated to Jean-Jacques Quisquater
on the Occasion of His 65th Birthday
Springer

1

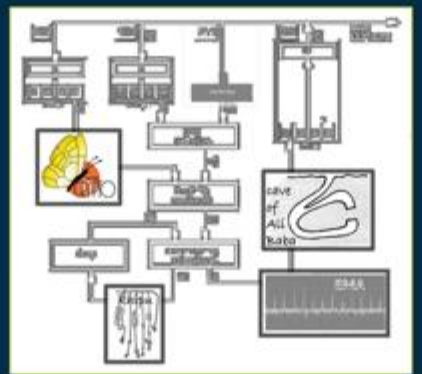
David Naccache (Ed.)

Festschrift

LNCS 6805

Cryptography and Security: From Theory to Applications

Essays Dedicated to Jean-Jacques Quisquater on the Occasion of His 65th Birthday



Springer

1. David Naccache (Ed.)

- He did the job finding and editing
- 1 + 32 papers
- With 84 authors (12 in the room)

2

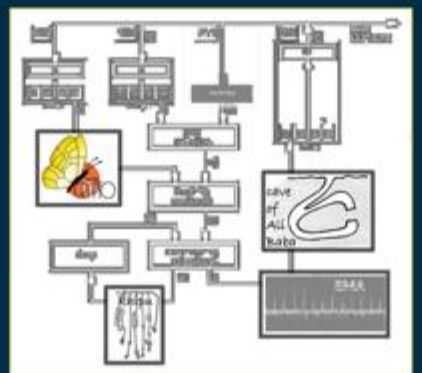
Naccache (Ed.)

Festschrift

LNCS 6805

Cryptography and Security: From Theory to Applications

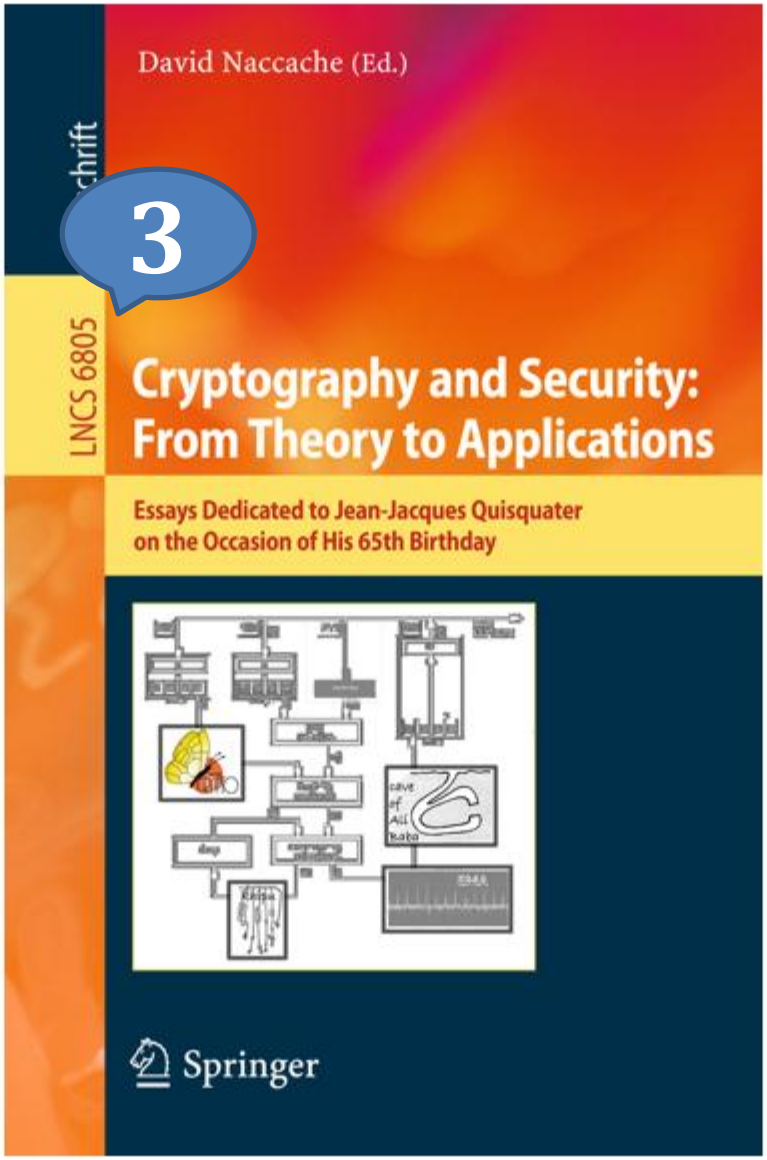
Essays Dedicated to Jean-Jacques Quisquater on the Occasion of His 65th Birthday



Springer

2. LNCS Festschrifts

- Festschrifts honor individual researchers and their scientific work, or they honor institutions or fields.
- Historical and even personal aspects may show up.
- They present internationally relevant technical contributions with a reasonable topical focus.
- Designed with a fresh orange and blue cover.


David Naccache (Ed.)
chrift
3
LNCS 6805
Cryptography and Security:
From Theory to Applications
Essays Dedicated to Jean-Jacques Quisquater
on the Occasion of His 65th Birthday
Springer

3. LNCS 6805

- This number is also the number of a processor family (Motorola) used for the first smart cards I was working

3. LNCS 6805

Motorola - 6805

6805 Family

Homepage: none ?
Family description: ...

Designer:	Motorola	Architecture:	8-bit
Initial release:	?	Frequencies:	?
Datasheet:	?	Technology:	?

Motorola - MC6805R2L1

General Specifications:

Manufacture:	Motorola	Family:	6805
Chip type:	MCU	Introduced:	?
Speed:	?	Architecture:	8-bit
Application:	?		

Architecture Specifications:

CPU arch:	?	ISA:	?
Microarch:	?		
Processor core:	?	# of cores:	1
Designer:	Motorola	FPU:	NA
Ext data bus:	8	Address bus:	8
Instruction Set:	?		
Features:	?		

Technology:

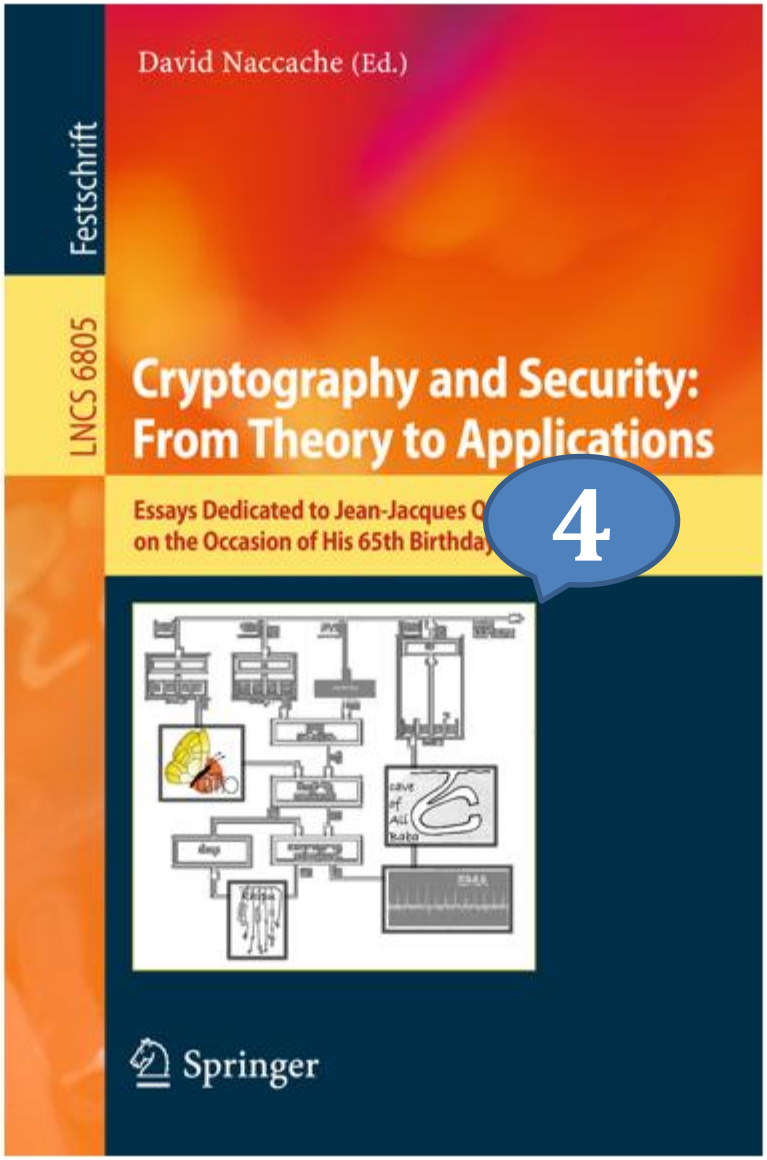
Technology:	HMOS	Process:	?
Transistors:	?	Die size:	?
Vcc:	?	Voltage I/O:	?

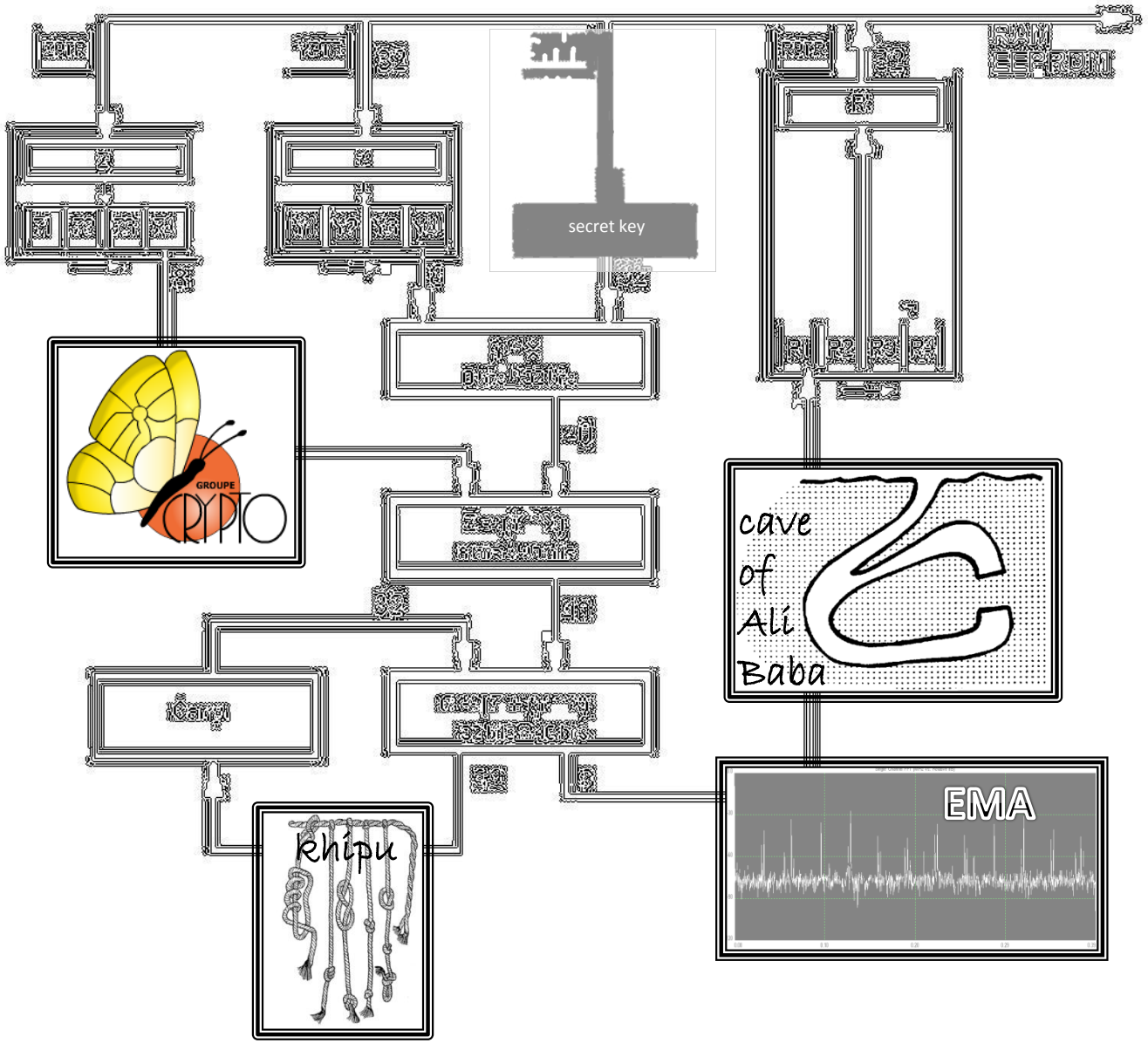
- This number is also the number of a processor family (Motorola) used for the first smart cards I was working

6800 or 6805

- David reserved long time ago 2 numbers from LNCS: 6800 and 6805
- I did the choice
- Waiting 8051(the main family of processors I was working) was too long …

My only contribution on June 3, 2011




secret key
GROUPE
CRYPTO
cave
of
Ali
Baba
EMA
khipu

COprocessor
for
RSA
In a
Rush

CORSAIR: A Smart Card for Public Key Cryptosystems

Dominique de Waleffe & Jean-Jacques Quisquater

Philips Research Laboratory
Avenue Albert Einstein, 4
B-1348 Louvain-la-Neuve, Belgium
E-mail: {ddw, jjq}@prlb.philips.be

Abstract. *Algorithms best suited for flexible smart card applications are based on public key cryptosystems — RSA, zero-knowledge protocols ... Their practical implementation (execution in ≈1 second) entails a computing power beyond the reach of classical smart cards, since large integers (512 bits) have to be manipulated in complex ways (exponentiation). CORSAIR achieves up to 40 (8 bit) MIPS with a clock speed of 6 Mhz. This allows to compute* X^E mod M*, with 512 bit operands, in less than 1.5 second (0.4 sec for a signature). The new smart card is in the final design stage; the first test chips should be available by the end of 1990.*

Keywords: smart card, public key algorithms, RSA, digital signature, zero-knowledge protocols.

1 Introduction

A large number of security problems can be solved by correct use of cryptographic methods. However, all methods found to date are more or less computationally intensive.

- DES works by applying a complex multiround algorithm on medium size numbers.
- Diffie-Hellman key exchange protocol is based on modular exponentiation of large integers.
- RSA is based on the same exponentiation and needs large exponents.
- Zero-knowledge protocols like those of Fiat-Shamir [9] or Guillou-Quisquater [10] use large number exponentiation but the exponents are not as large as in RSA.
- Many identity-based systems also rely on modular exponentiation of large numbers.

Public key techniques are the most promising for the future as they provide more flexible solutions and impose less burden both on users and security management. Most practical techniques rely on large integer arithmetic.

A.J. Menezes and S.A. Vanstone (Eds.): Advances in Cryptology - CRYPTO '90, LNCS 537, pp. 502-513, 1991.

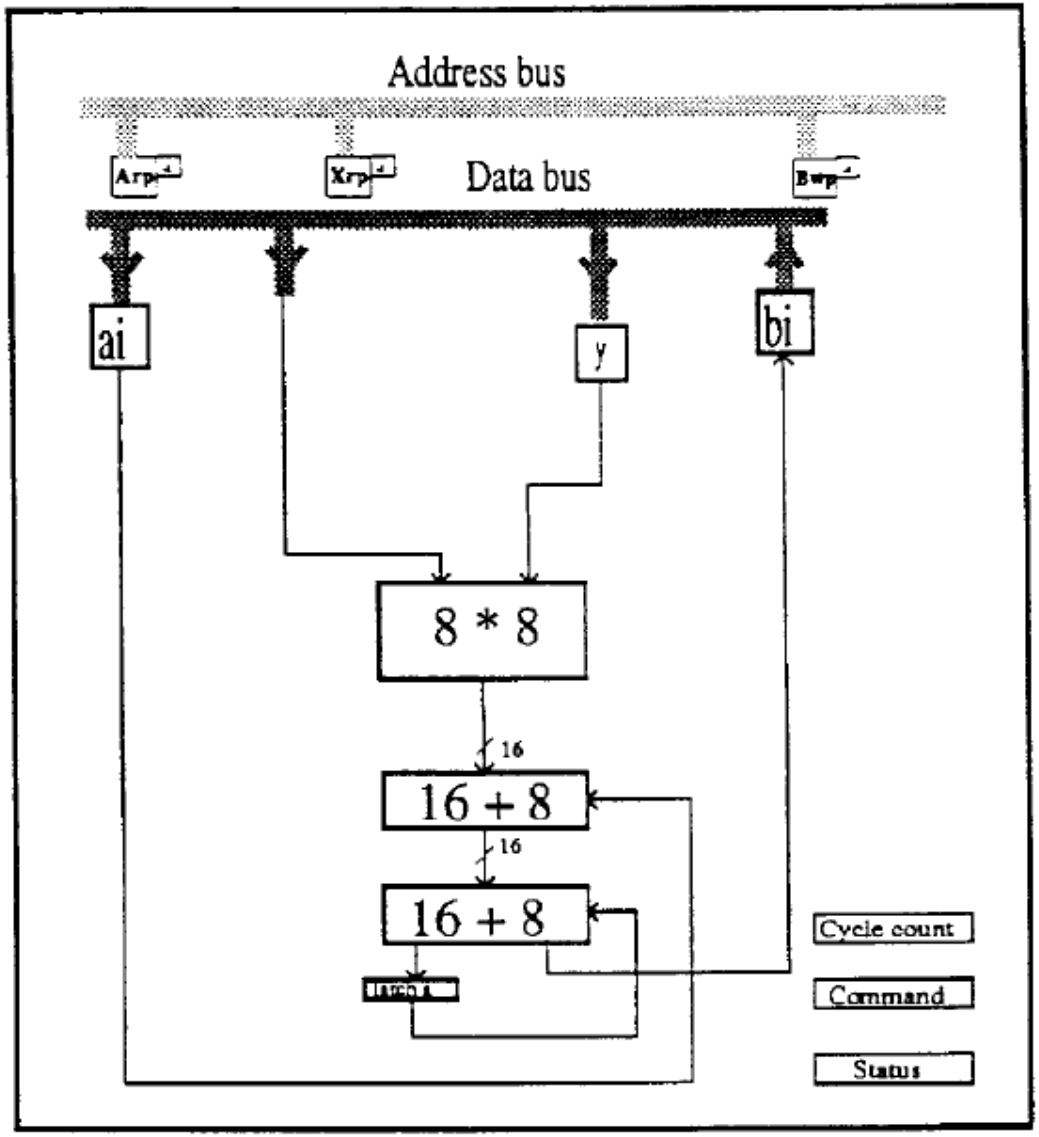


Figure 2: Simple cell

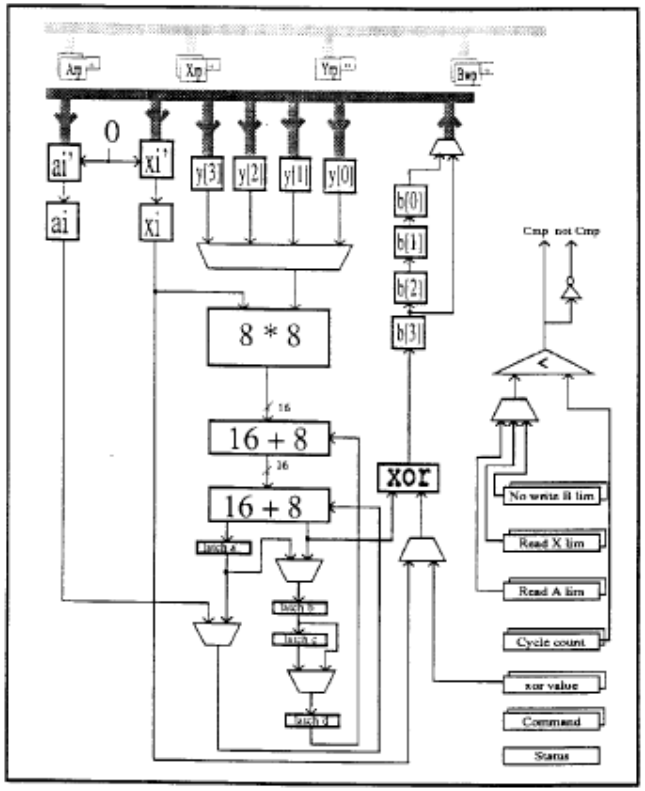
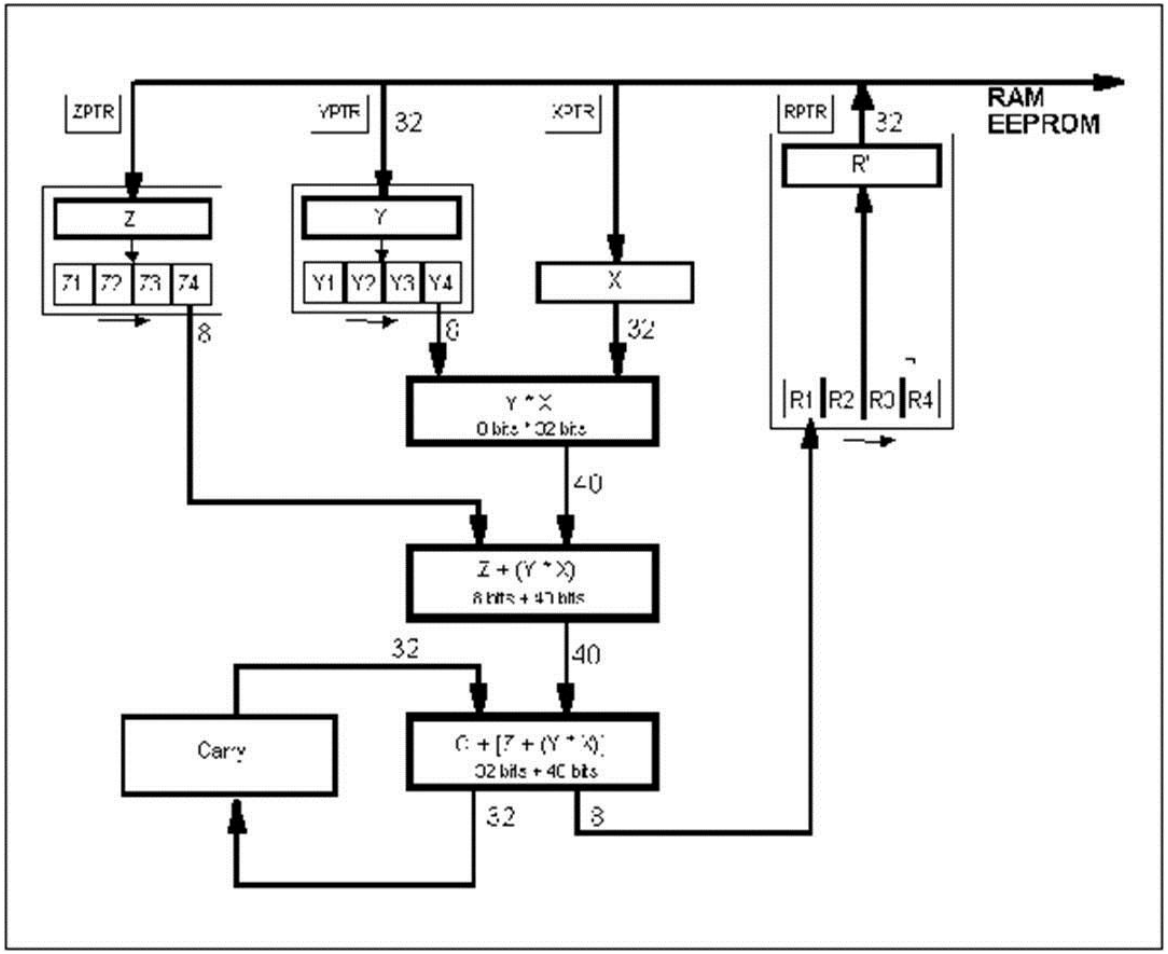
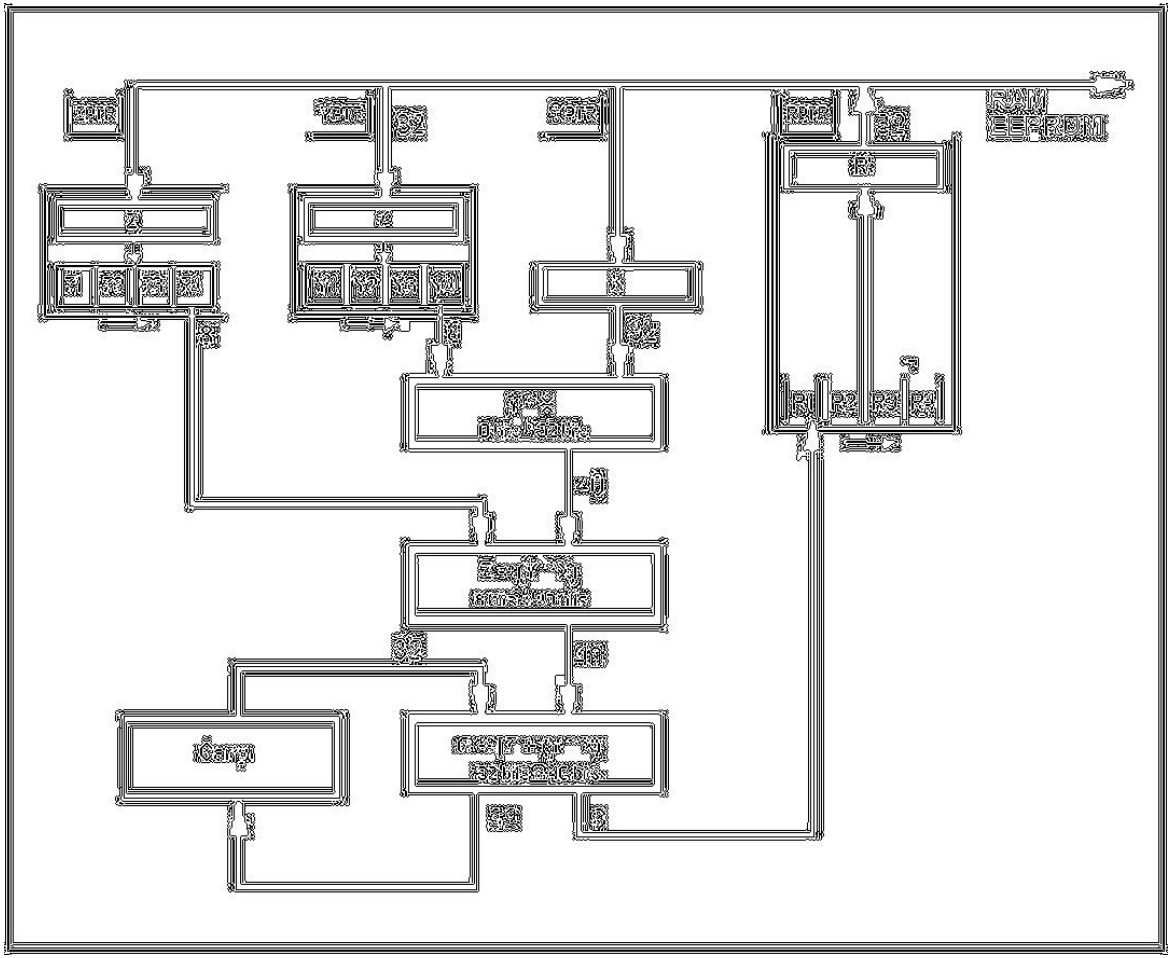


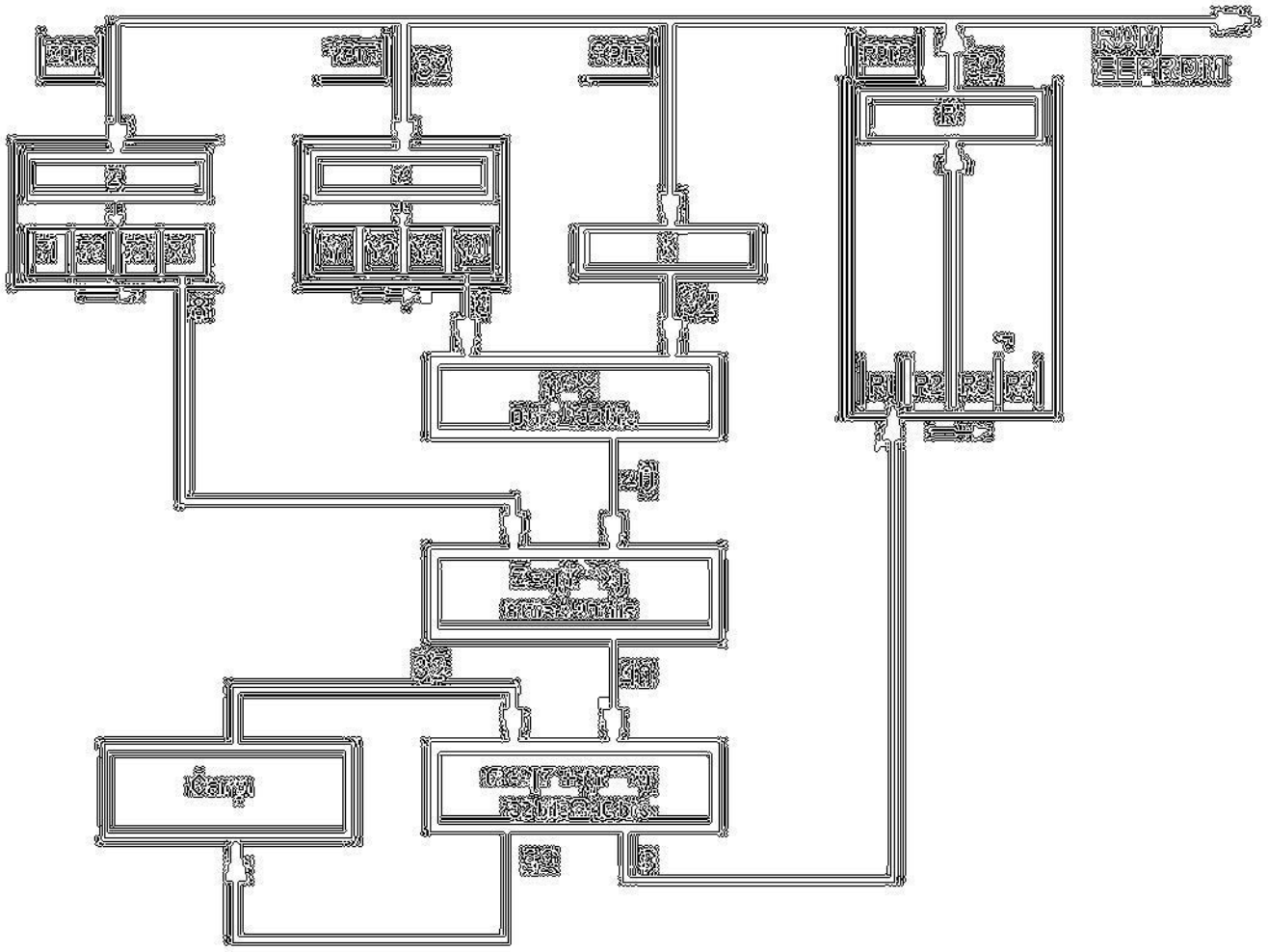
Figure 5: Final architecture

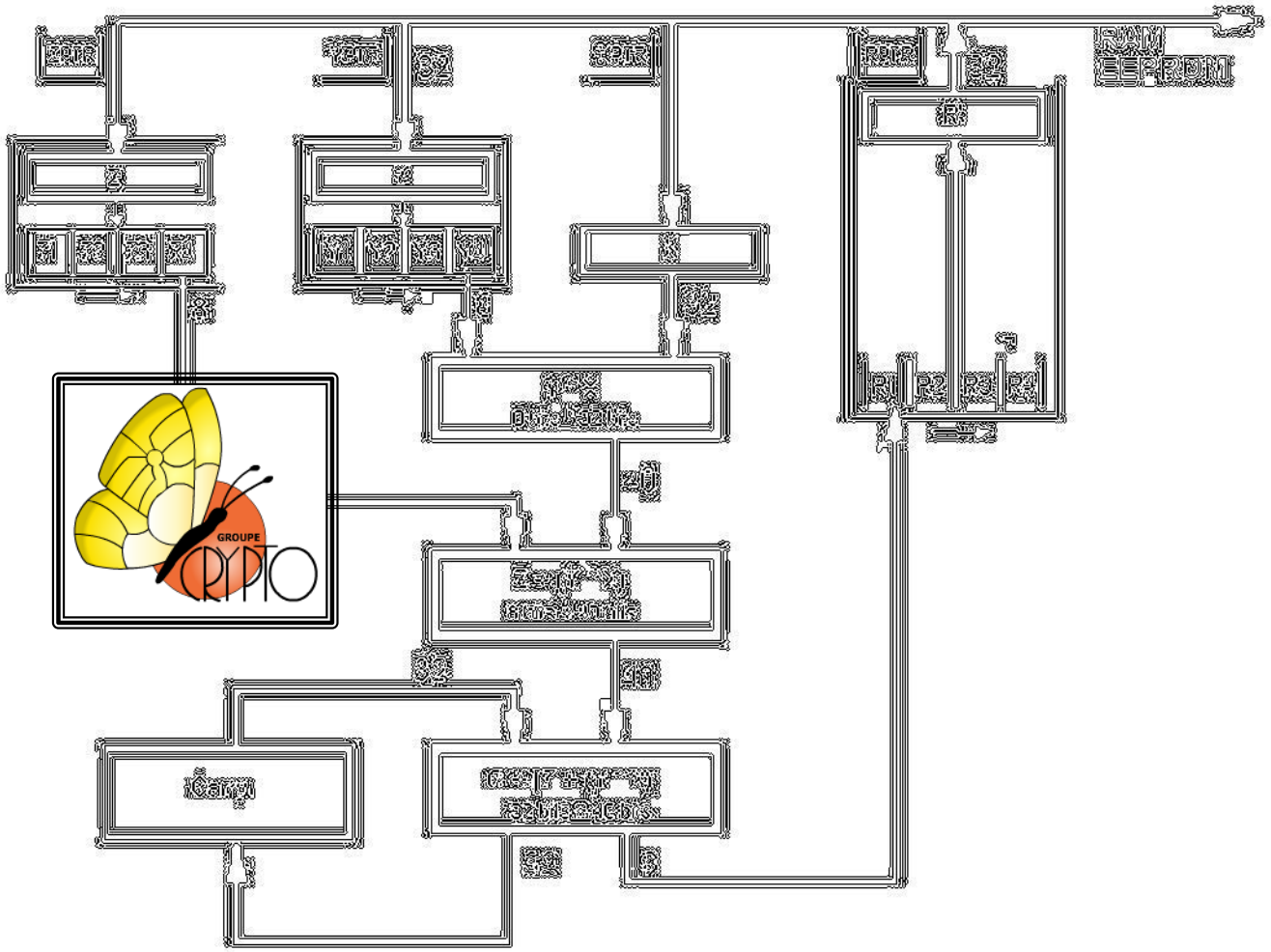
Next step: FAME from NXP-Philips

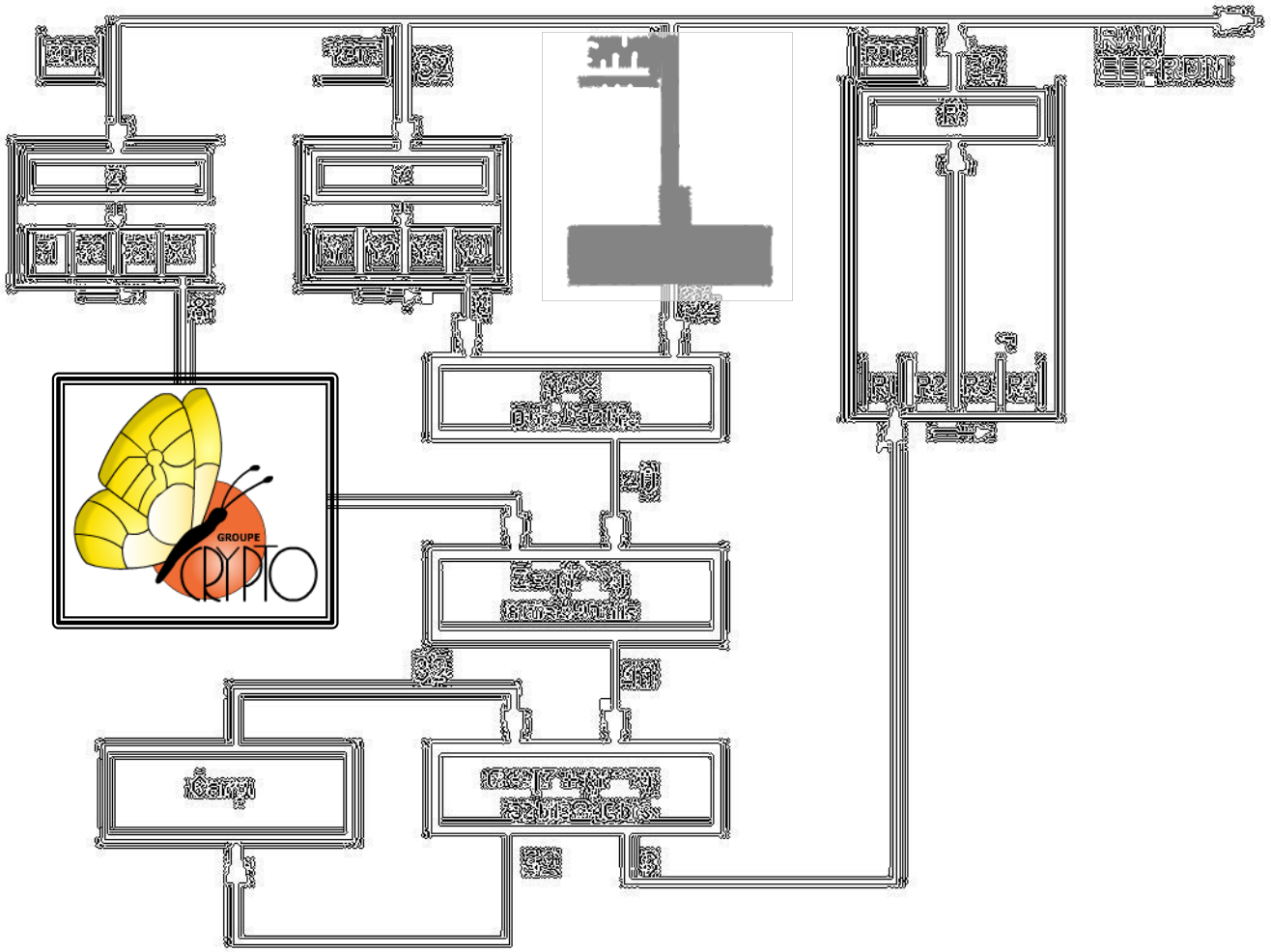


Using photoshop (fuzzy) and adding

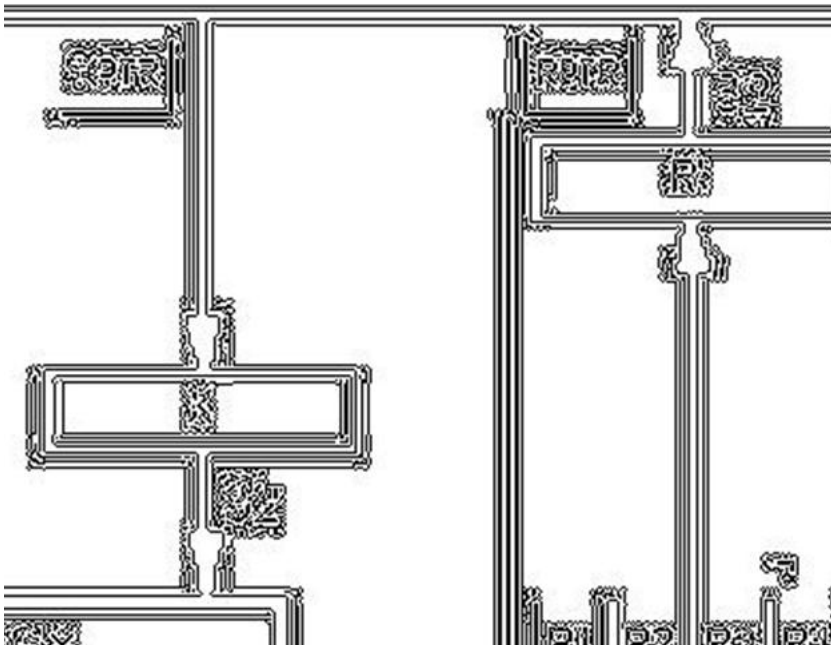




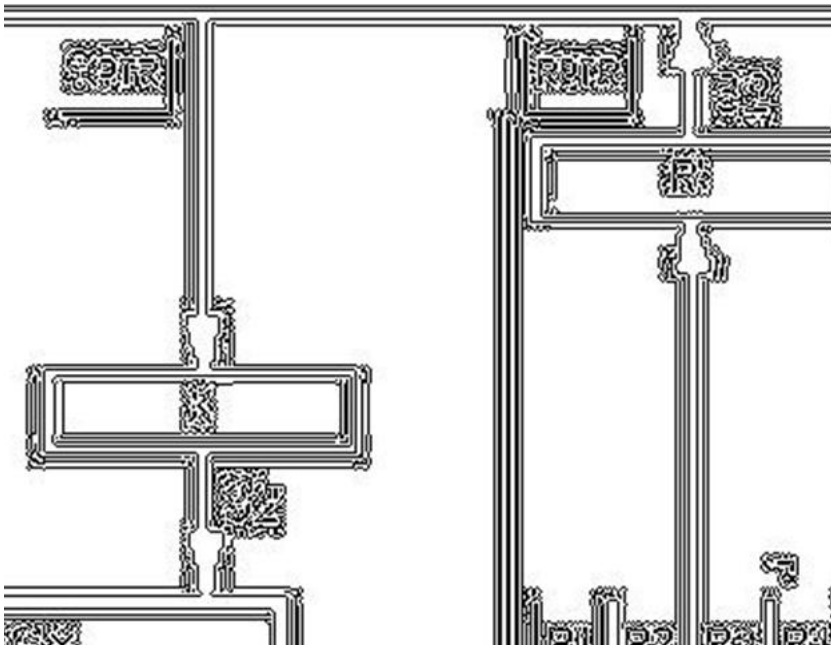

GROUPE
CRYPTO


GROUPE
CRYPTO

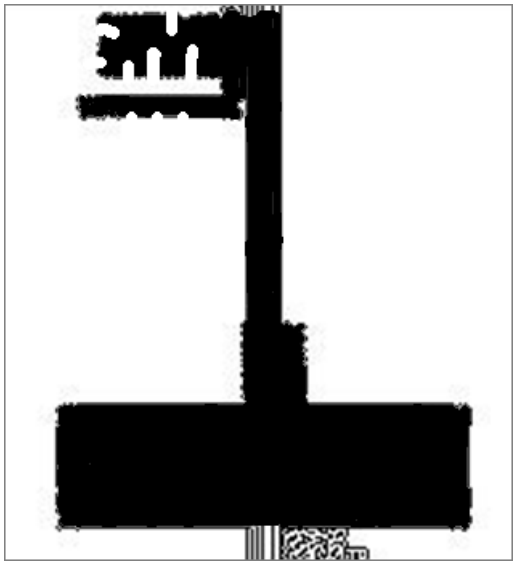
Secret key

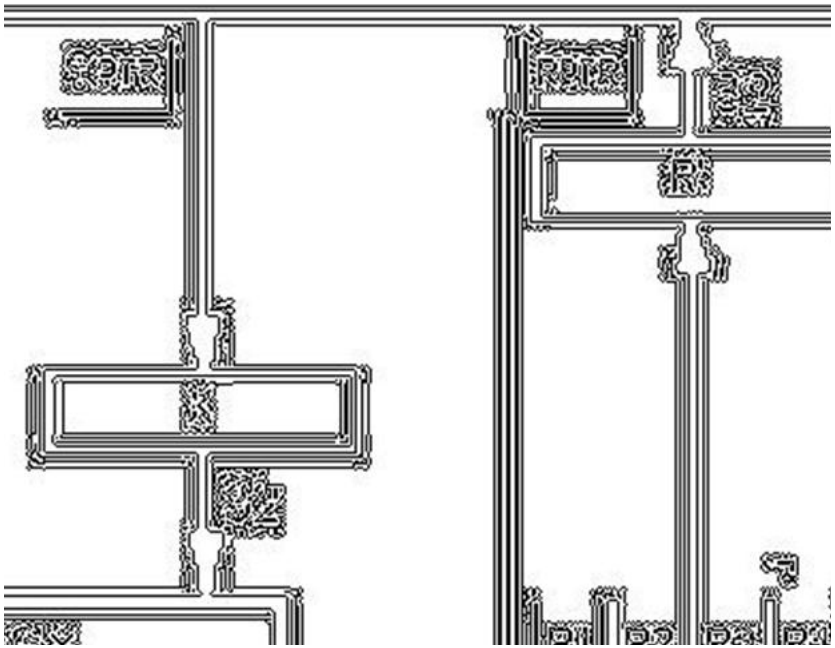


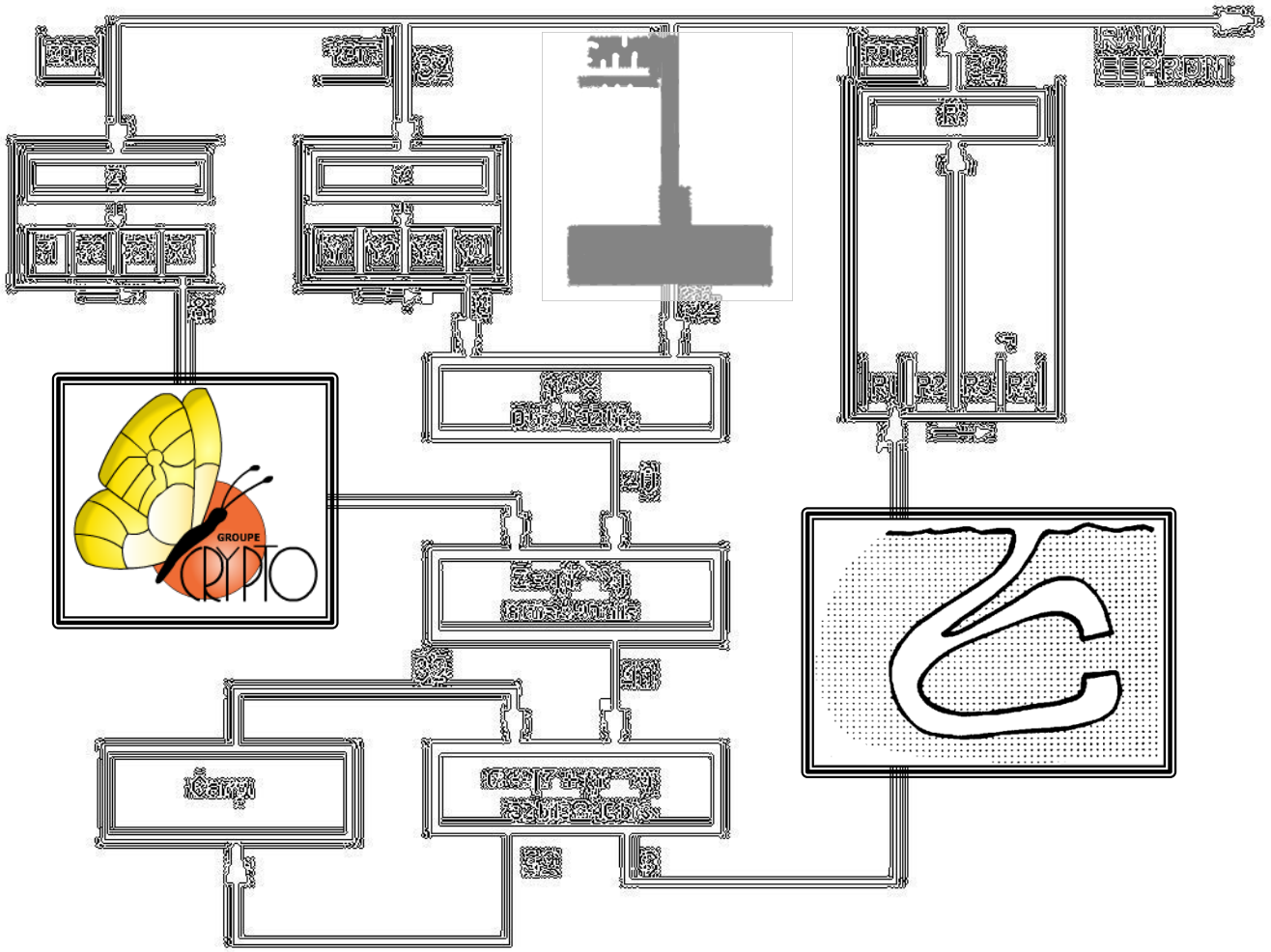
Secret key



Secret key






GROUPE
CRYPTO

How to Explain Zero-Knowledge Protocols to Your Children

QUISQUATER Jean-Jacques[1], *Myriam, Muriel, Michaël*
GUILLOU Louis[2], *Marie Annick, Gaïd, Anna, Gwenolé, Soazig*
in collaboration with *Tom BERSON*[3] for the English version

[1] Philips Research Laboratory, Avenue Van Becelaere, 2, B–1170 Brussels, Belgium.
[2] CCETT/EPT, BP 59, F–35512 Cesson Sévigné, France.
[3] Anagram Laboratories, P.O. Box 791, Palo Alto CA 94301, USA.

The Strange Cave of Ali Baba

◇ Know, oh my children, that very long ago, in the Eastern city of Baghdad, there lived an old man named Ali Baba. Every day Ali Baba would go to the bazaar to buy or sell things. This is a story which is partly about Ali Baba, and partly also about a cave, a strange cave whose secret and wonder exist to this day. But I get ahead of myself ...

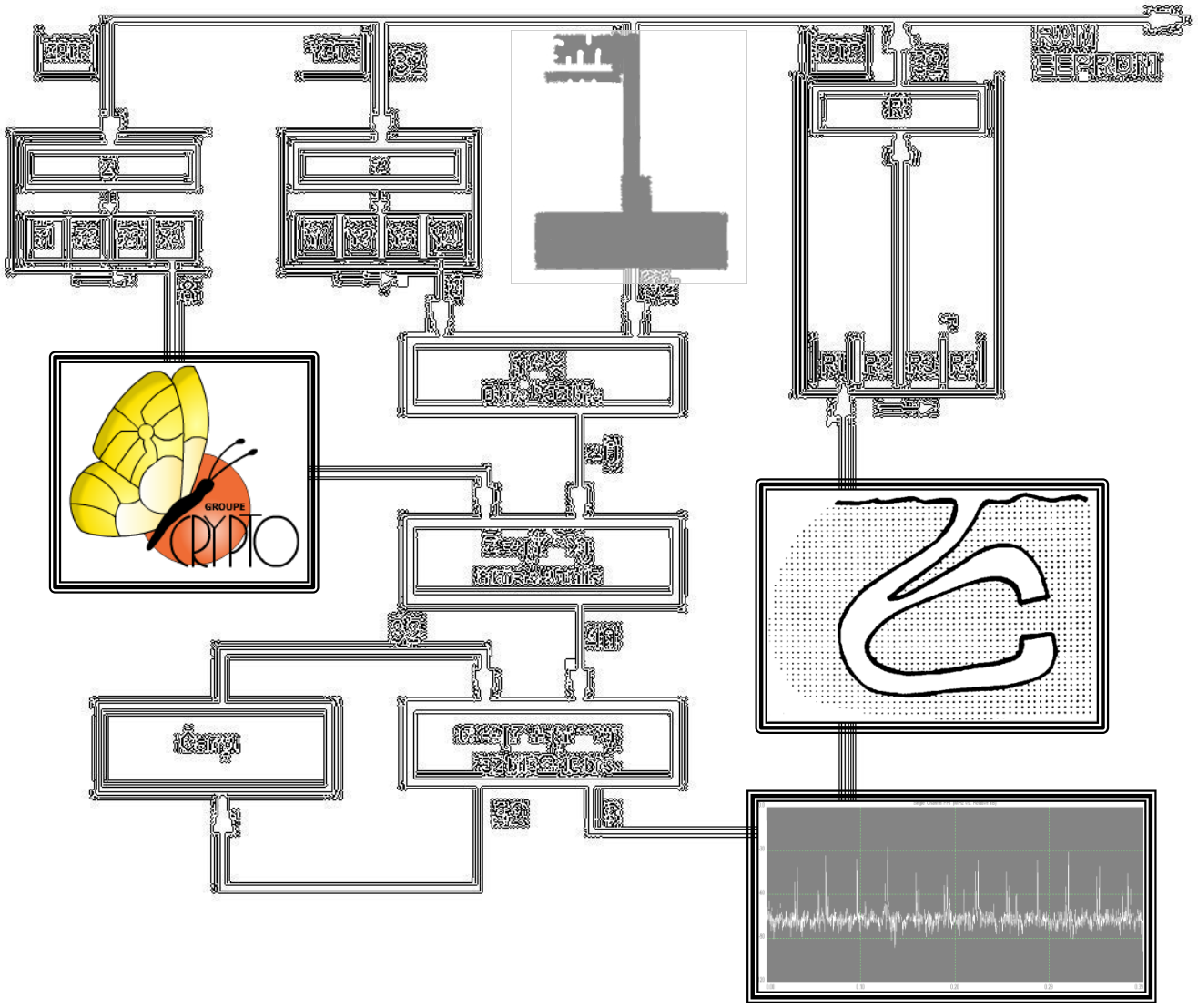
One day in the Baghdad bazaar a thief grabbed a purse from Ali Baba who right away started to run after him. The thief fled into a cave whose entryway forked into two dark winding passages: one to the left and the other to the right (The Entry of the Cave).

Ali Baba did not see which passage the thief ran into. Ali Baba had to choose which way to go, and he decided to go to the left. The left-hand passage ended in a dead end. Ali Baba searched all the way from the fork to the dead end, but he did not find the thief. Ali Baba said to himself that the thief was perhaps in the other passage. So he searched the right-hand passage, which also came to a dead end. But again he did not find the thief. "This cave is pretty strange," said Ali Baba to himself, "Where has my thief gone?"

The following day another thief grabbed Ali Baba's basket and fled, as the first thief had fled, into the strange cave. Ali Baba pursued him, and again did not see which way the thief went. This time Ali Baba decided to search to the right. He went all the way to the end of the right-hand passage, but he did not find the thief. He said to himself that, like the first thief, the second thief had also been lucky in taking the passage Ali Baba did not choose to search. This had undoubtedly let the thief leave again and to blend quietly into the crowded bazaar.

The days went by, and every day brought its thief. Ali Baba always ran after the thief, but he never caught any of them. On the fortieth day a fortieth thief grabbed Ali Baba's turban and fled, as thirty-nine thieves had done before him, into the strange cave. Ali Baba yet again did not see which way the thief went. This time Ali Baba decided to search the left-hand passage, but again he did not find the thief at the end of the passage. Ali Baba was very puzzled.

He could have said to himself, as he had done before, that the fortieth thief had been as lucky as each of the other thirty-nine thieves. But this explanation was so


GROUPE
CRYPTO

- J.-J. Quisquater et D. Samyde:
- *« a new tool for non intrusive analysis of smart cards based on electro-magnetic emissions, the SEMA and DEMA methods* »
- Presented at the rump session of EUROCRYPT ’2000, Bruges, Belgium.

Eurocrypt 2000

Bruges (Brugge), Belgium, May 14-18, 2000

Eurocrypt 2000 Rump Session

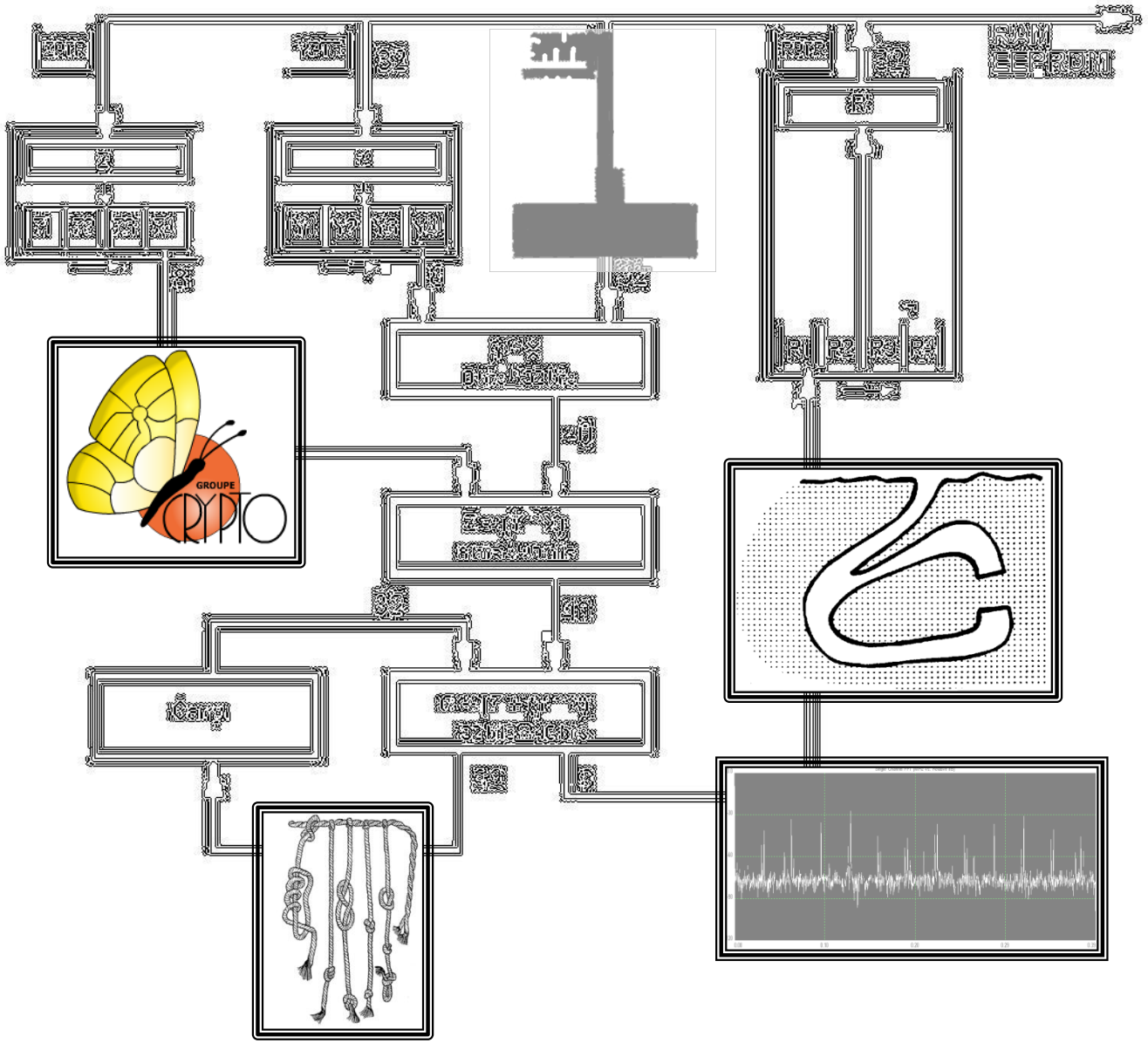
The occasional drink and poster session (part one)

Efficient Protocols from Homomorphic Threshold Cryptography	*Ivan Damgård*, Ronald Cramer, Jesper Buus Nielsen, Mads Jurik
Elliptic Curve Systems Too Risky? Or TRoublesome?	*Arjen K. Lenstra*
The Schoof-Elkies-Atkin algorithm in characteristic 2 - The Previous world record	*Frederik Vercauteren*
A New Record in point counting on elliptic curves	*Pierrick Gaudry*
A new tool for non-intrusive analysis of smart cards based on electro-magnetic emissions. The SEMA and DEMA methods	*Jean-Jacques Quisquater, David Samyde*
On the Soundness of Girault's Scheme	*Fabrice Boudot*
The NESSIE Call for Cryptographic Algorithms	*Eli Biham*
FPGA Implementation of Modular Exponentiation Using Montgomery Method	*Elena Trichina*
One-round secure computation and secure Autonomous Mobile Agents	Christian Cachin, Jan Camenisch, Joe Kilian, *Joy Müller*

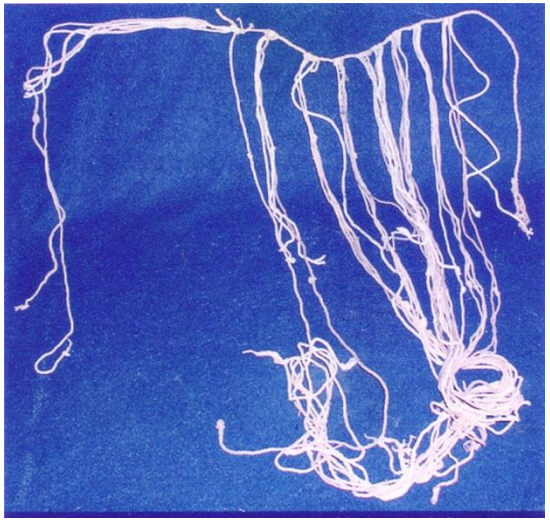
The occasional drink and poster session (part two)

Braid Group Cryptosystem, the Arithmetic Key Agreement Protocol	*Jim Hughes*
Update on UMAC Fast Message Authentication	*Phil Rogaway*
Small generic hardcore subsets for the discrete logarithm: short secret DL-keys	*Clauss P. Schnorr*
A popular protocol whose security decreases as key size increases	*David Naccache*
Necessary and Sufficient Assumptions for Non-Interactive Zero-Knowledge Proofs of Knowledge for all NP relations	Alfredo De Santis, *Giovanni Di Crescenzo*, Giuseppe Persiano
A proven secure tracing algorithm for the optimal KD traitor tracing Scheme	Kaoru Kurosawa, Mike Burmester, *Yvo Desmedt*
Efficient Algorithms for Differential Probability modulo 2^n and Related Problems	*Helger Lipmaa*, Shiho Moriai

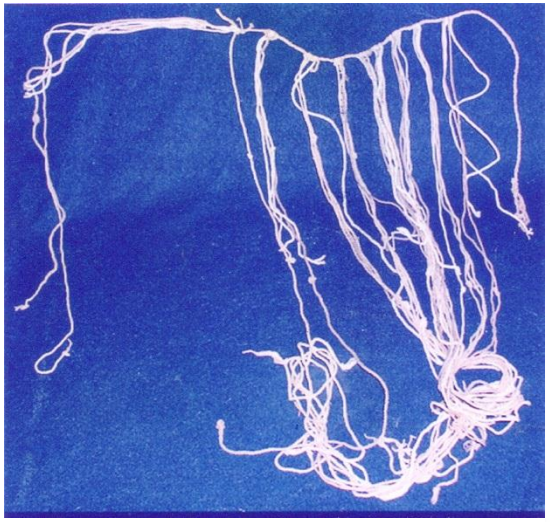
Eurocrypt 2000 Poster Session


GROUPE
CRYPTO

Inca khipus



Inca khipus



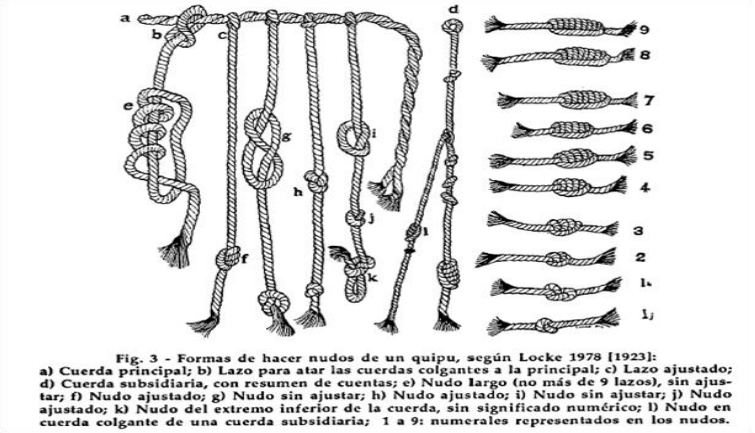
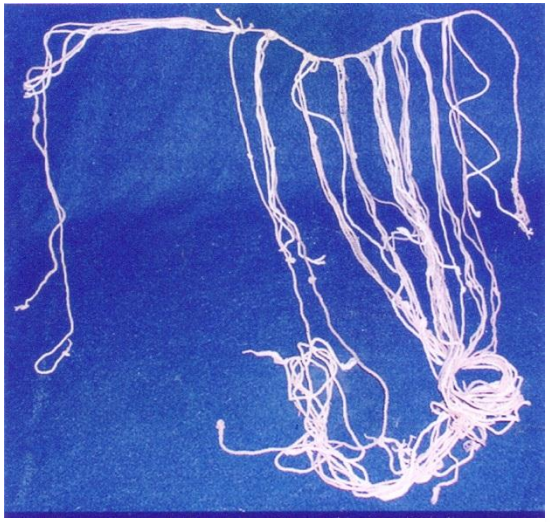


Fig. 3 - Formas de hacer nudos de un quipu, según Locke 1978 [1923]:
a) Cuerda principal; b) Lazo para atar las cuerdas colgantes a la principal; c) Lazo ajustado; d) Cuerda subsidiaria, con resumen de cuentas; e) Nudo largo (no más de 9 lazos), sin ajustar; f) Nudo ajustado; g) Nudo sin ajustar; h) Nudo ajustado; i) Nudo sin ajustar; j) Nudo ajustado; k) Nudo del extremo inferior de la cuerda, sin significado numérico; l) Nudo en cuerda colgante de una cuerda subsidiaria; 1 a 9: numerales representados en los nudos.

Inca khipus



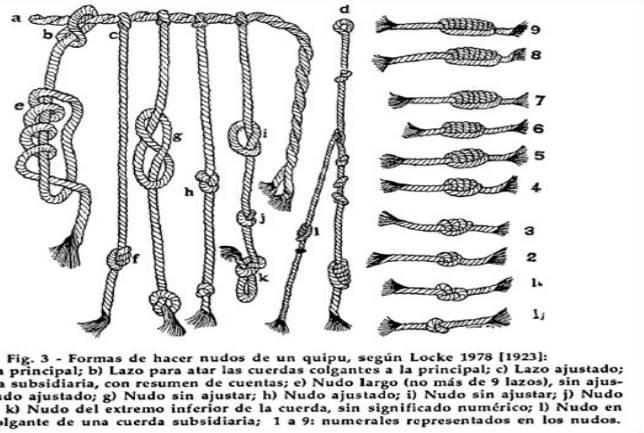
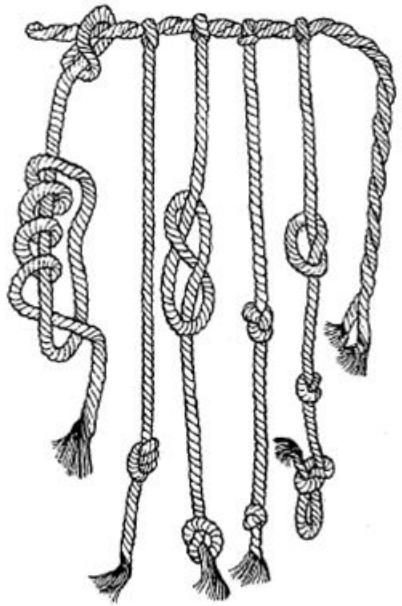
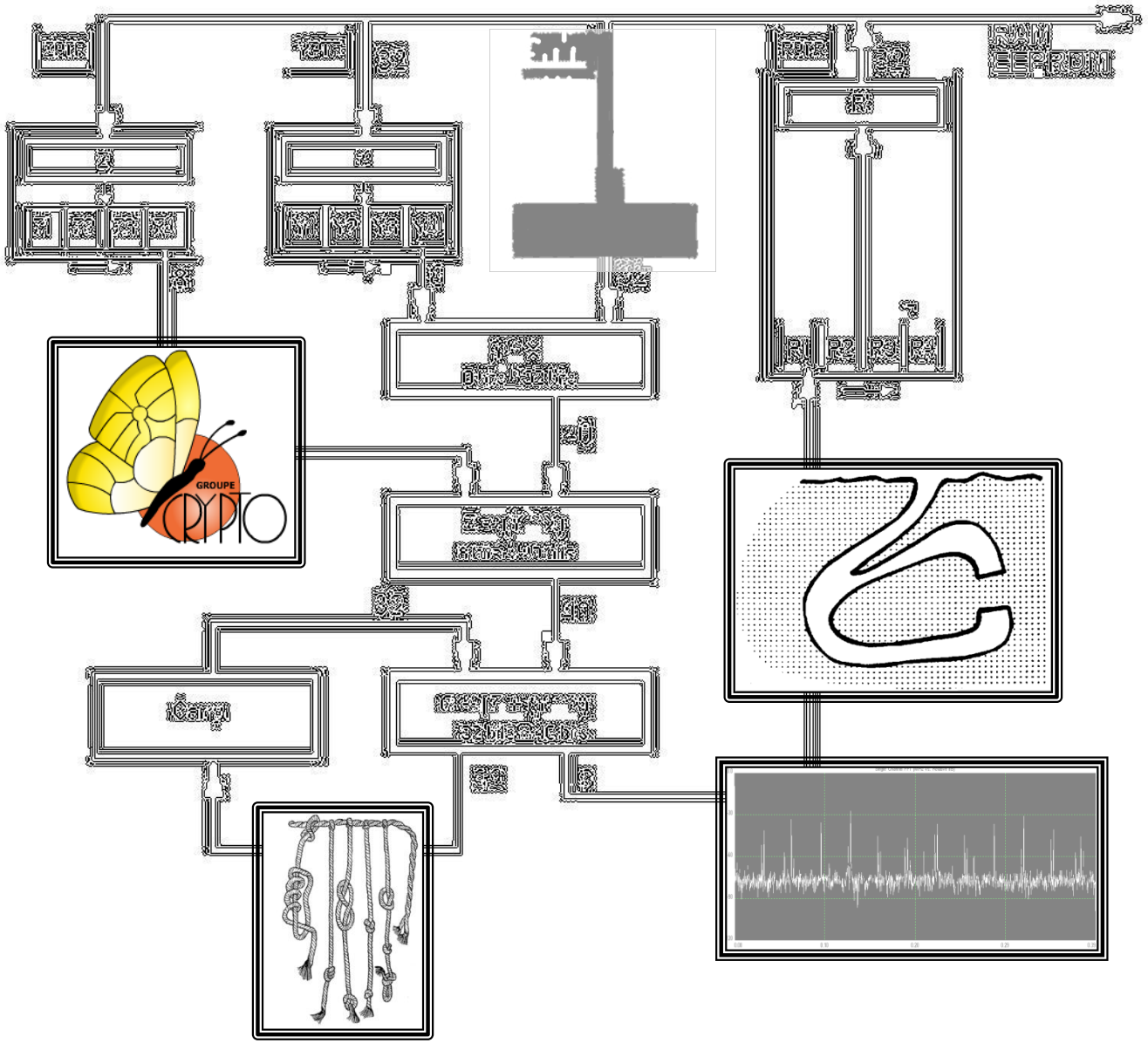
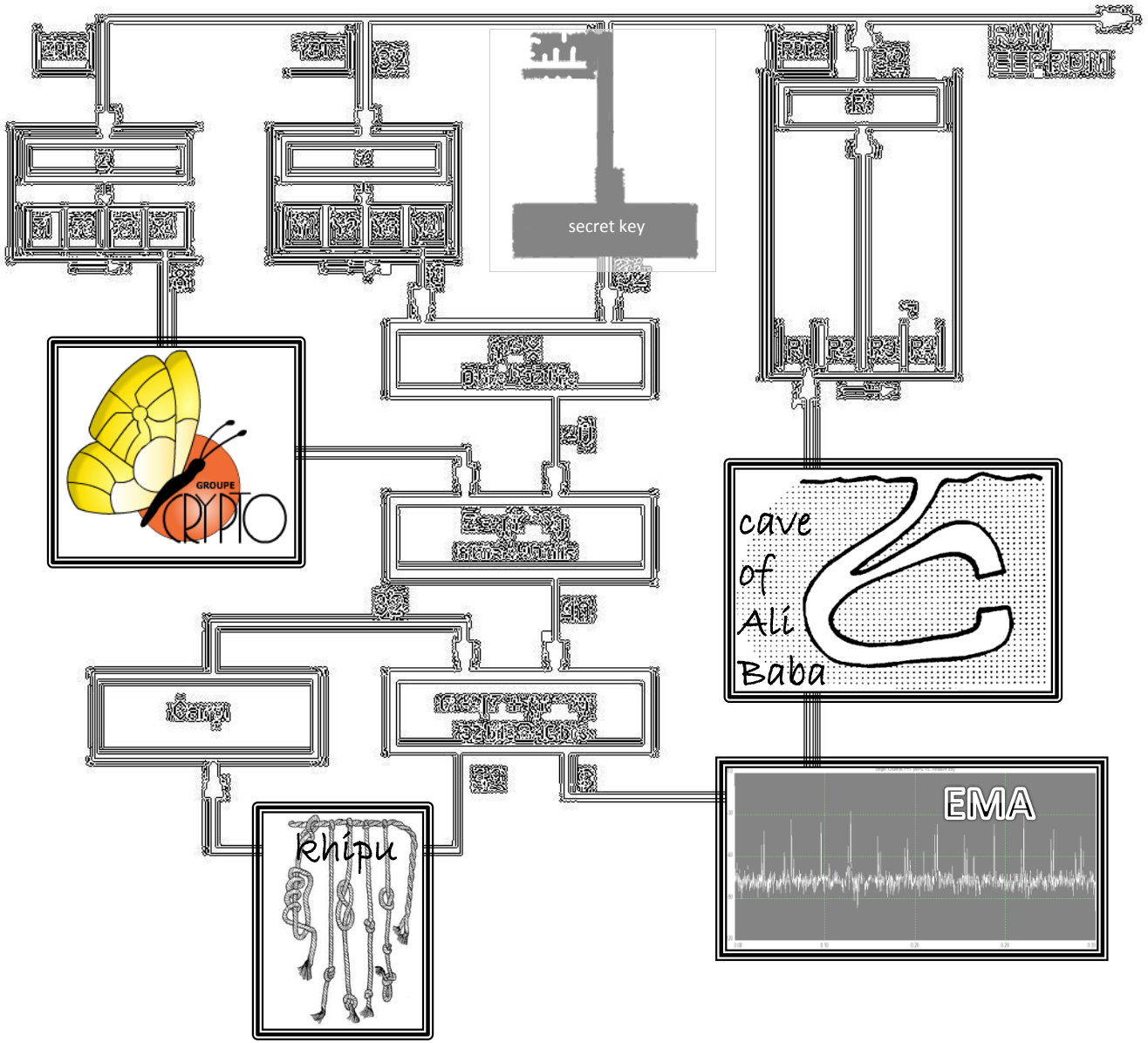


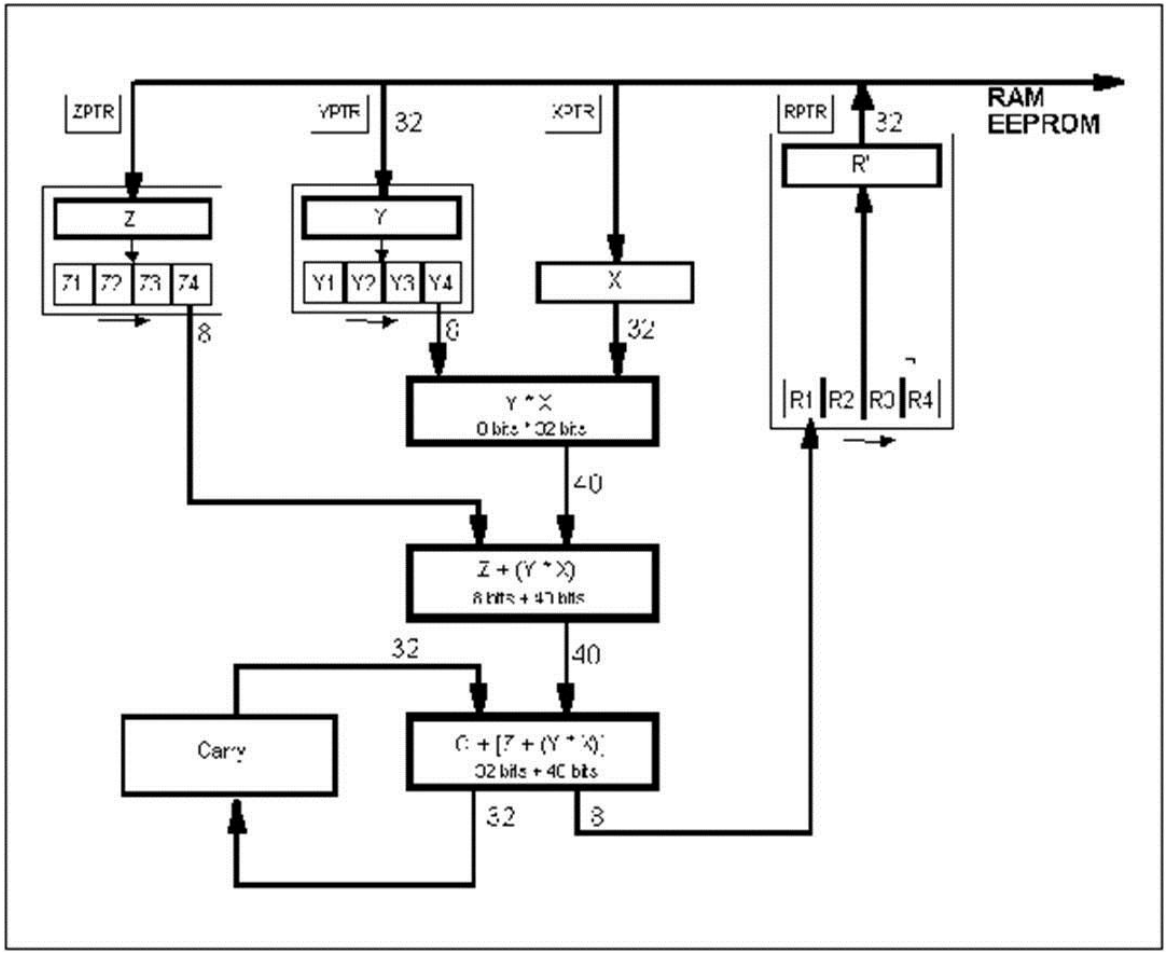
Fig. 3 - Formas de hacer nudos de un quipu, según Locke 1978 [1923]: a) Cuerda principal; b) Lazo para atar las cuerdas colgantes a la principal; c) Lazo ajustado; d) Cuerda subsidiaria, con resumen de cuentas; e) Nudo largo (no más de 9 lazos), sin ajustar; f) Nudo ajustado; g) Nudo sin ajustar; h) Nudo ajustado; i) Nudo sin ajustar; j) Nudo ajustado; k) Nudo del extremo inferior de la cuerda, sin significado numérico; l) Nudo en cuerda colgante de una cuerda subsidiaria; 1 a 9: numerales representados en los nudos.

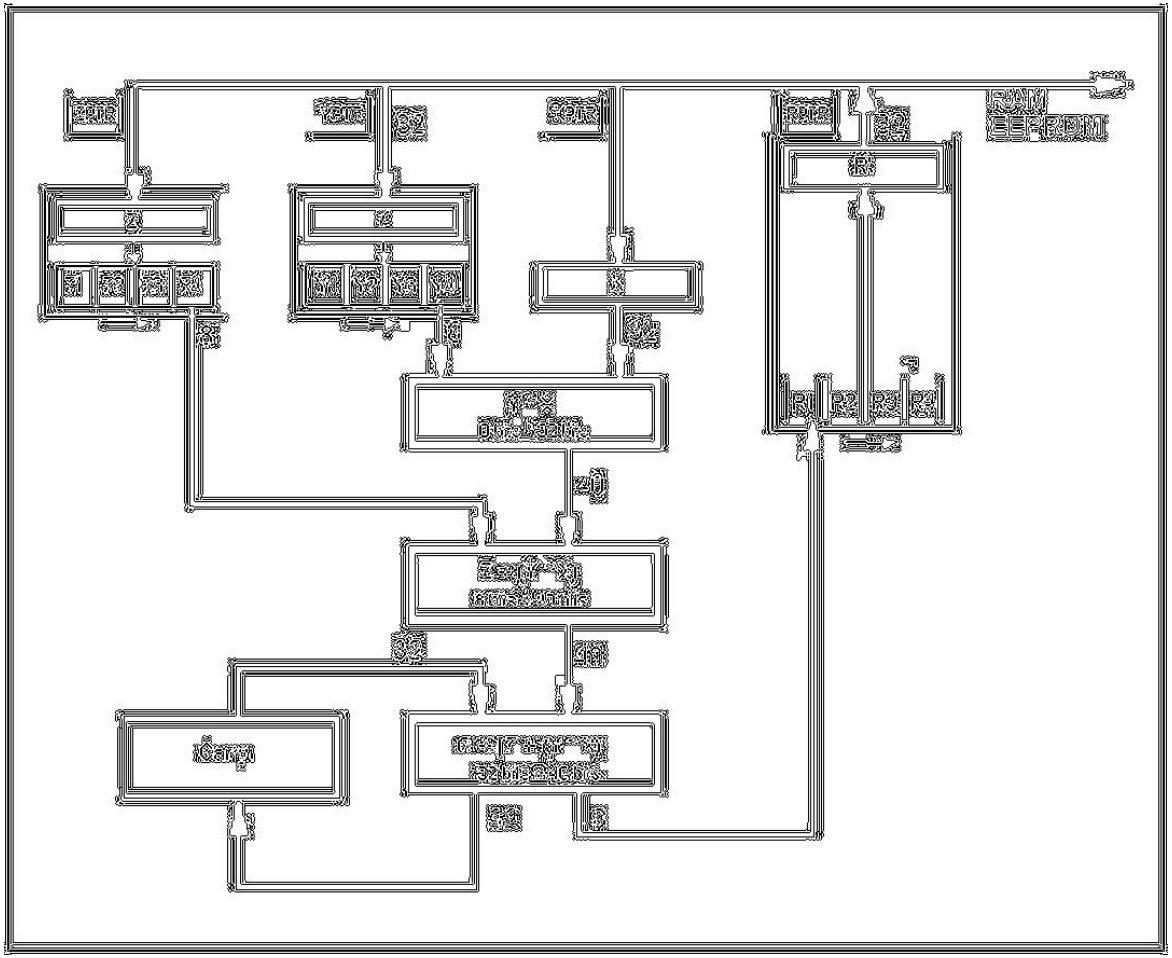


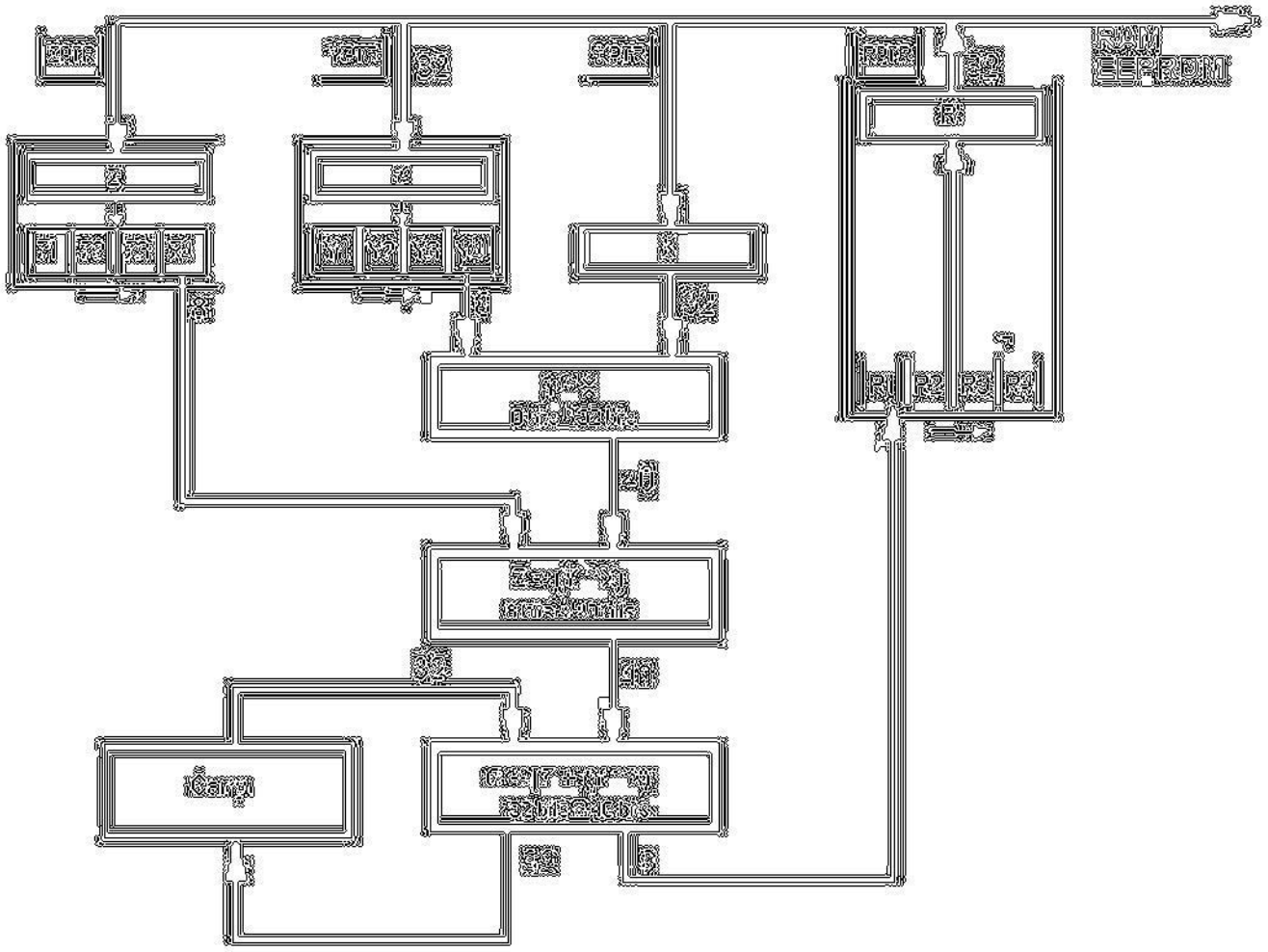

GROUPE
CRYPTO

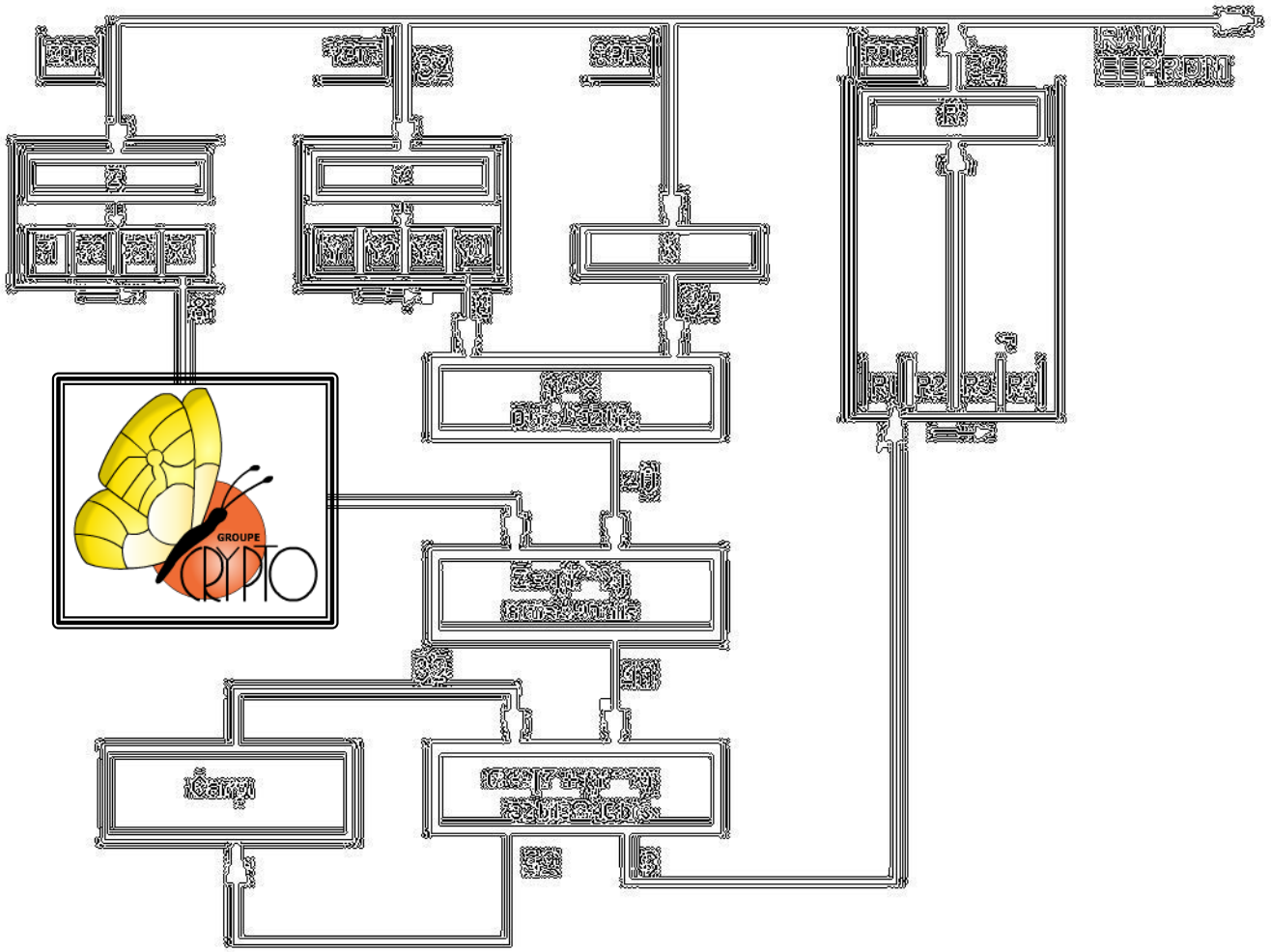

secret key
GROUPE
CRYPTO
cave
of
Ali
Baba
EMA
khipu

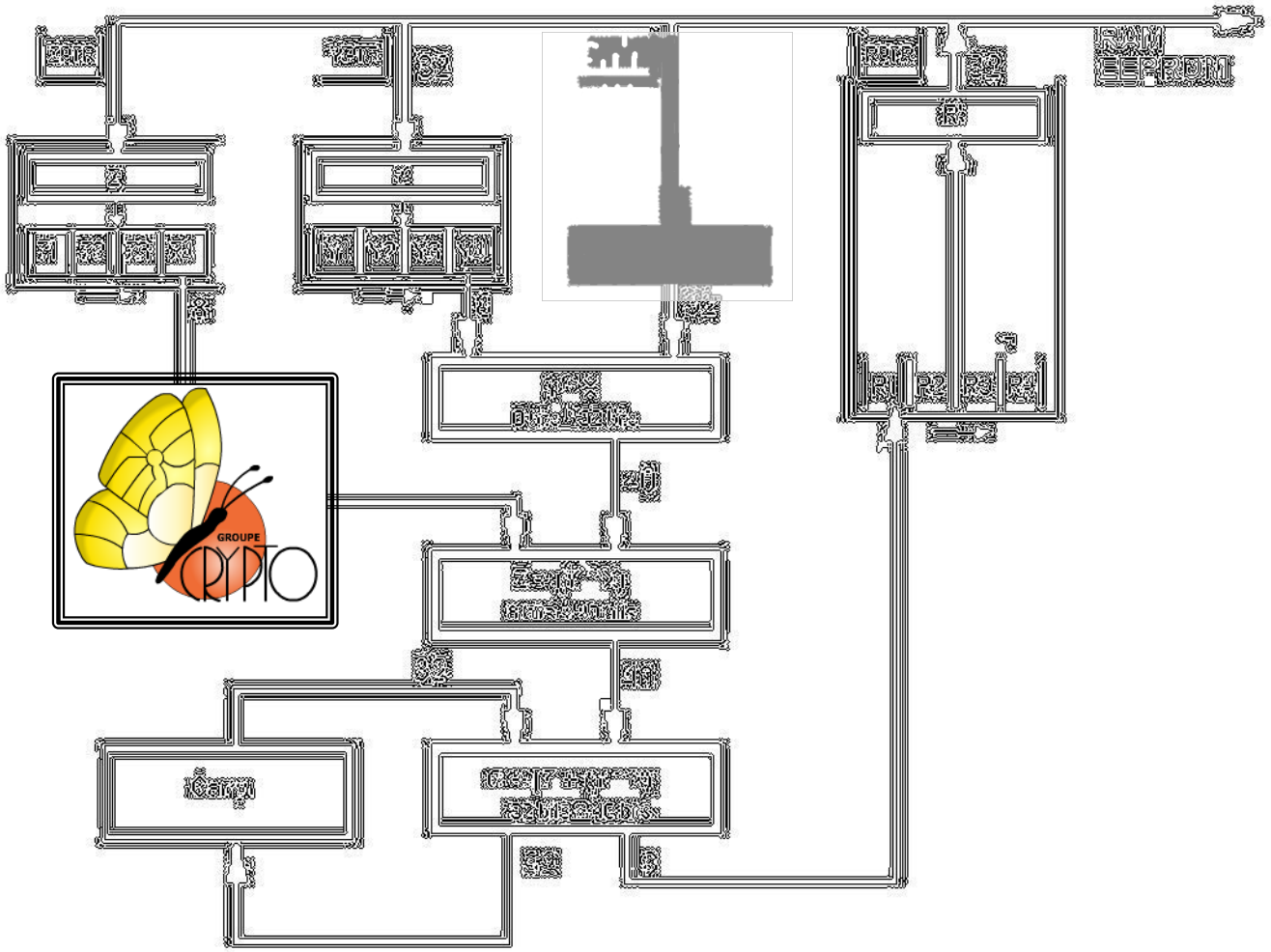
Again!

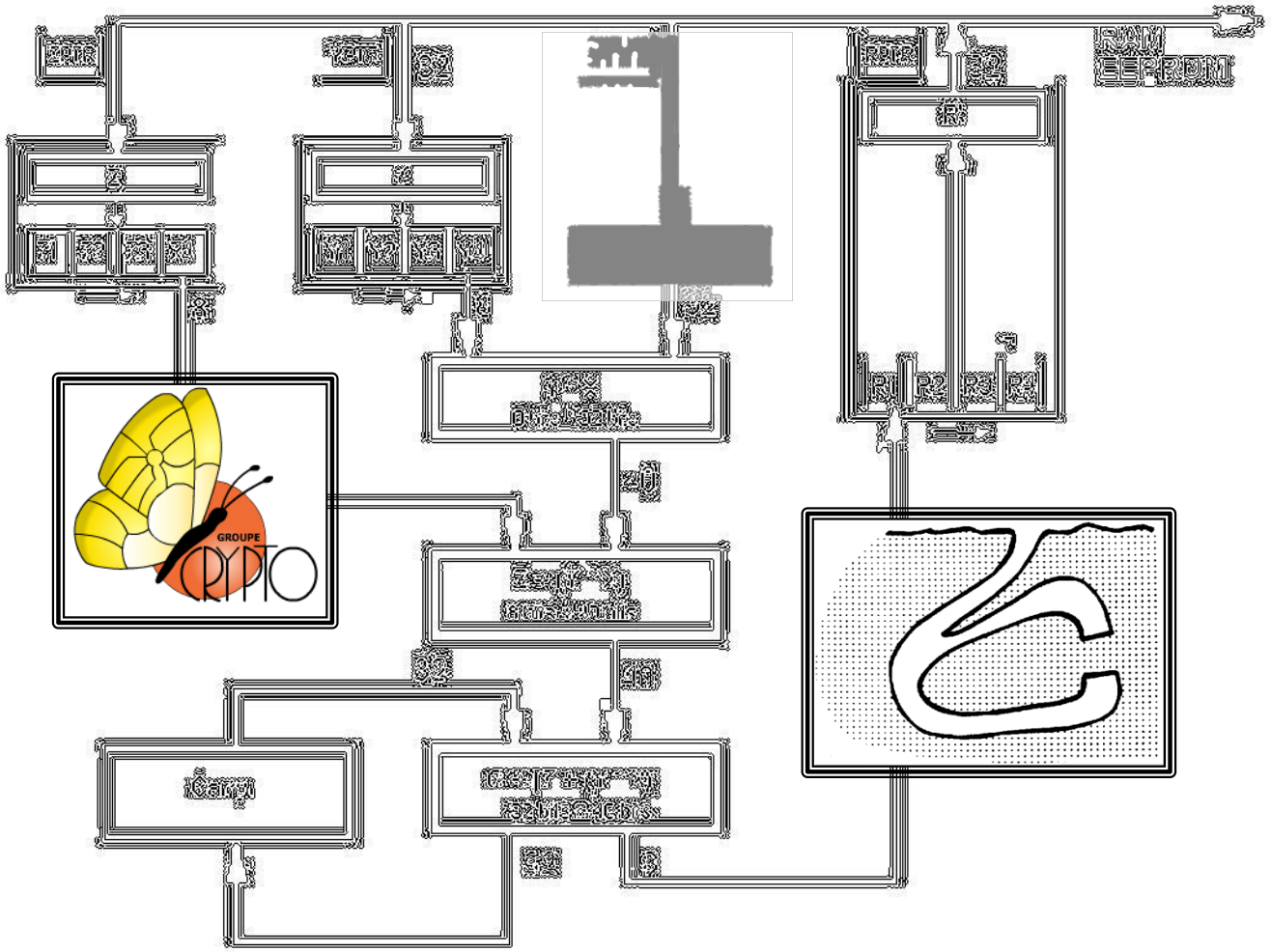

ZPTR
YPTR
32
XPTR
RPTR
32
RAM
EEPROM
Z
Y
R'
Z1
Z2
Z3
Z4
Y1
Y2
Y3
Y4
X
R1
R2
R3
R4
8
8
32
Y * X
8 bits * 32 bits
40
Z + (Y * X)
8 bits + 40 bits
32
40
Carry
C + [Z + (Y * X)]
32 bits + 40 bits
32
8

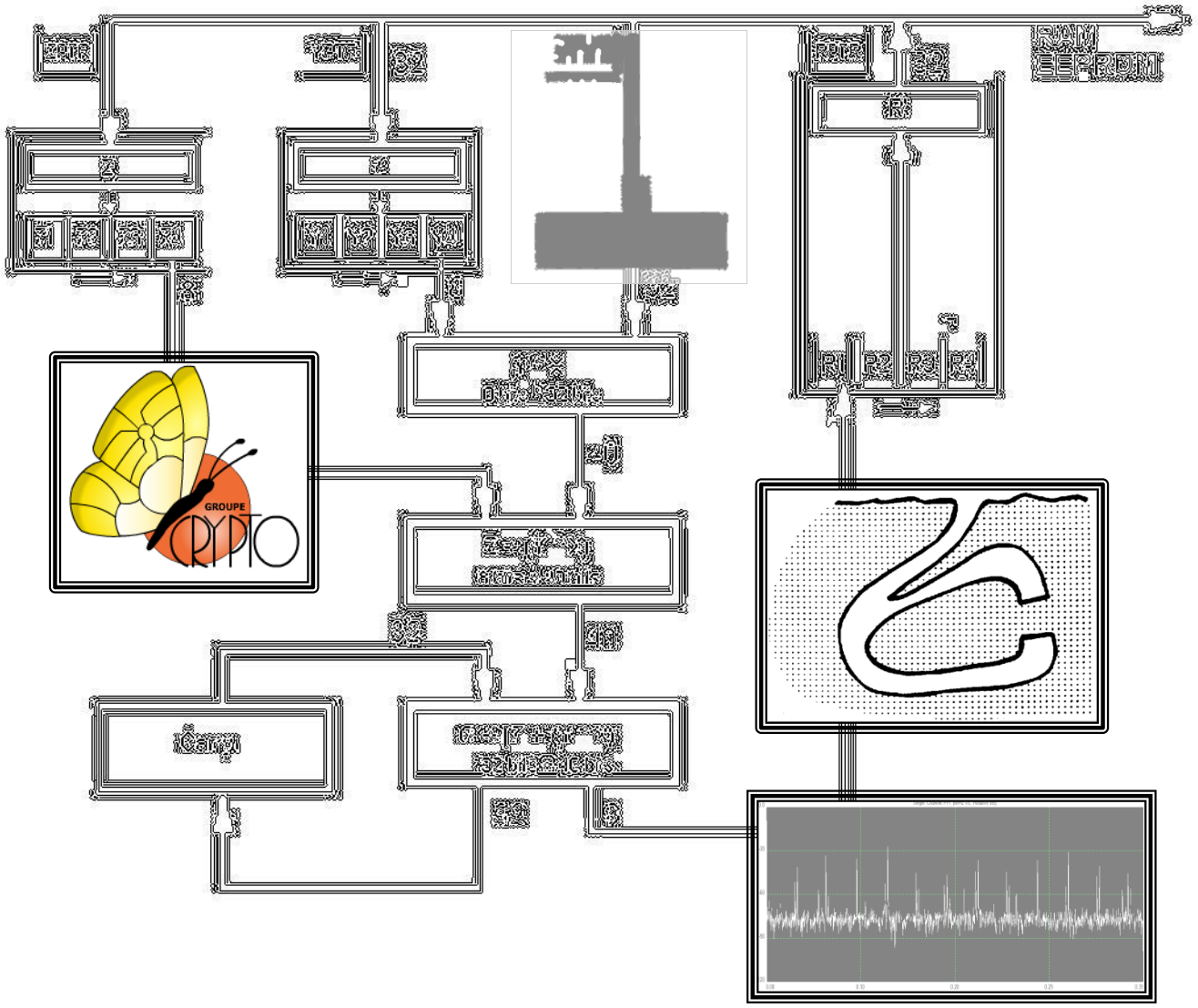


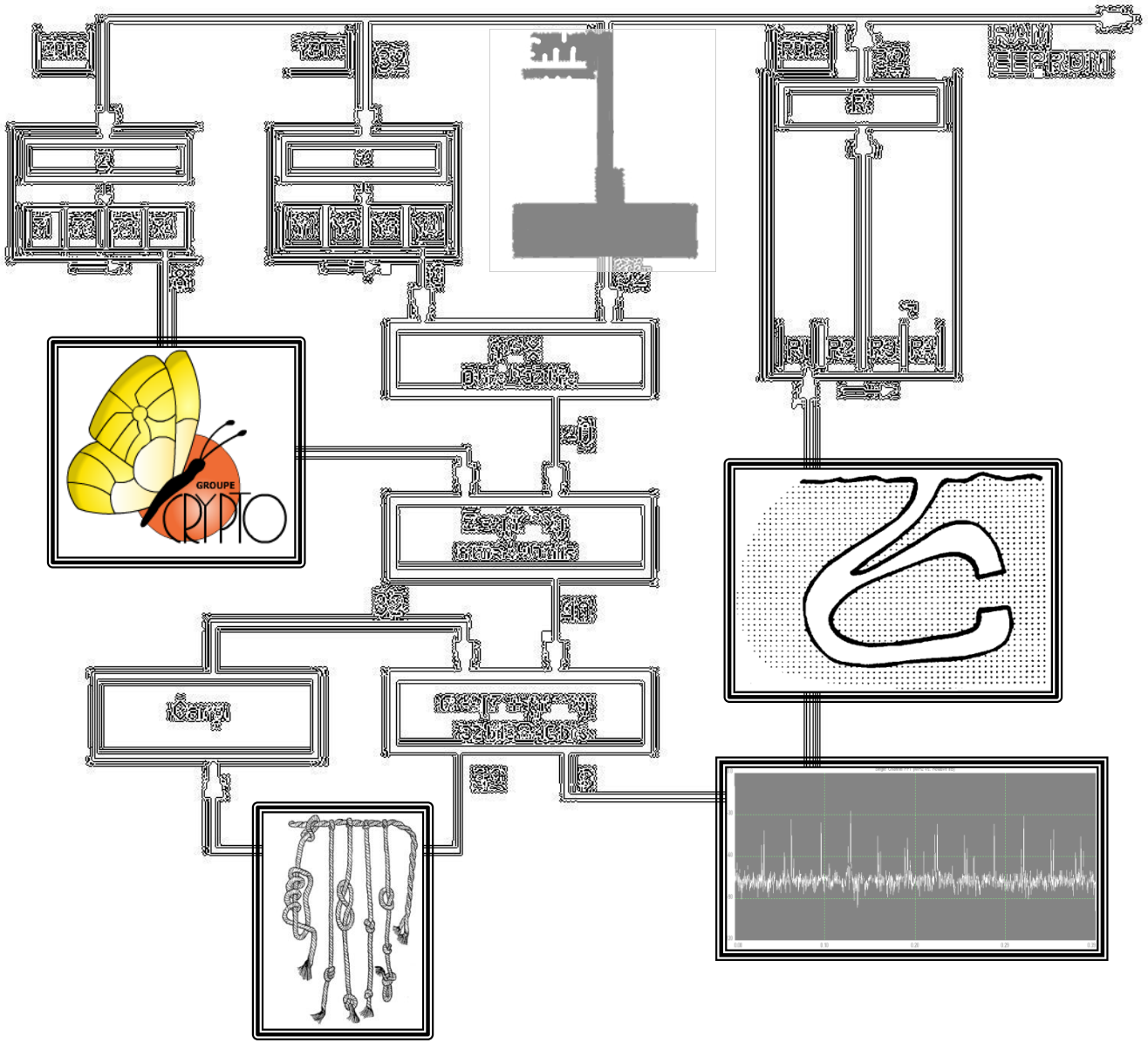


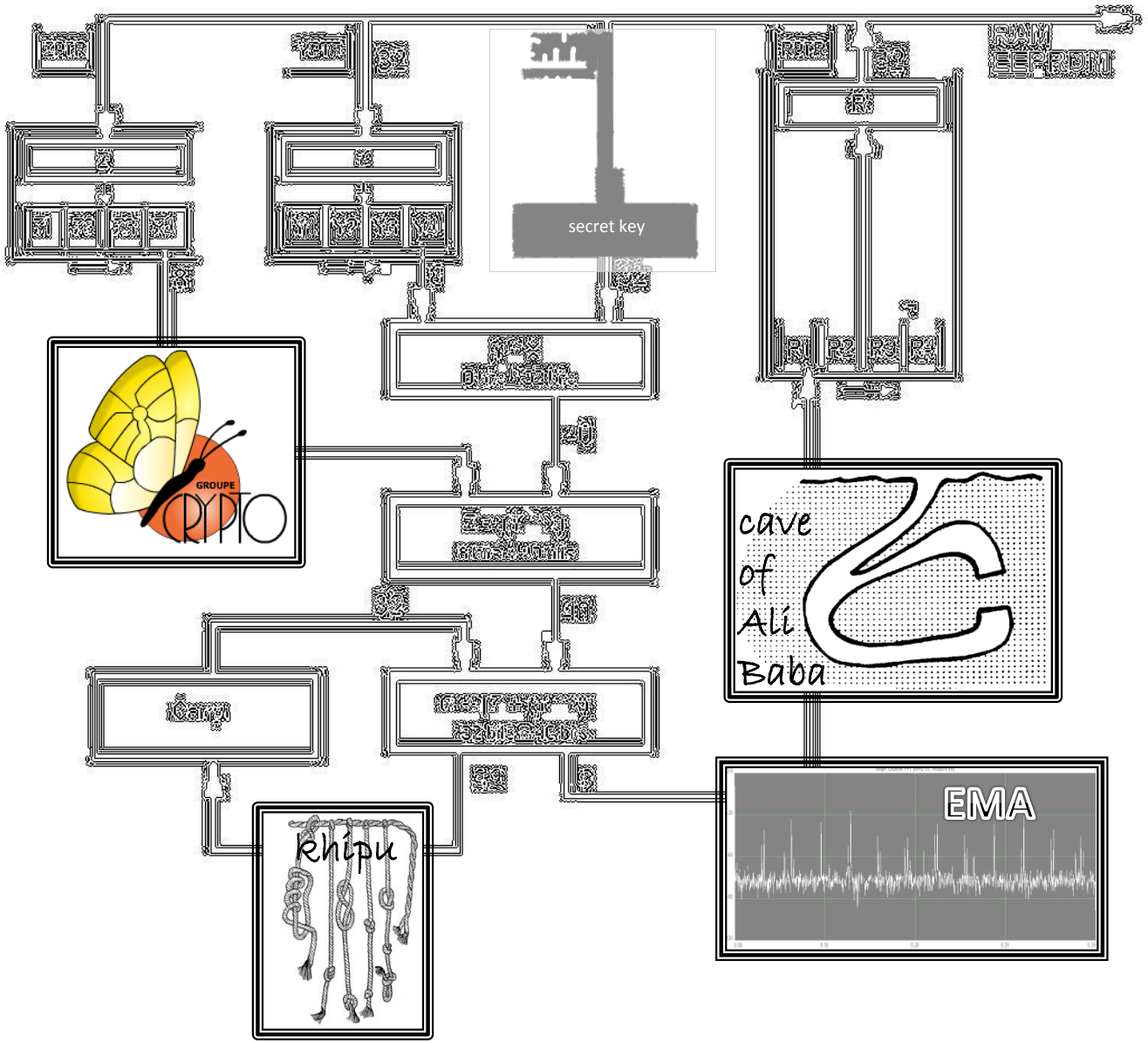

GROUPE
CRYPTO


GROUPE
CRYPTO

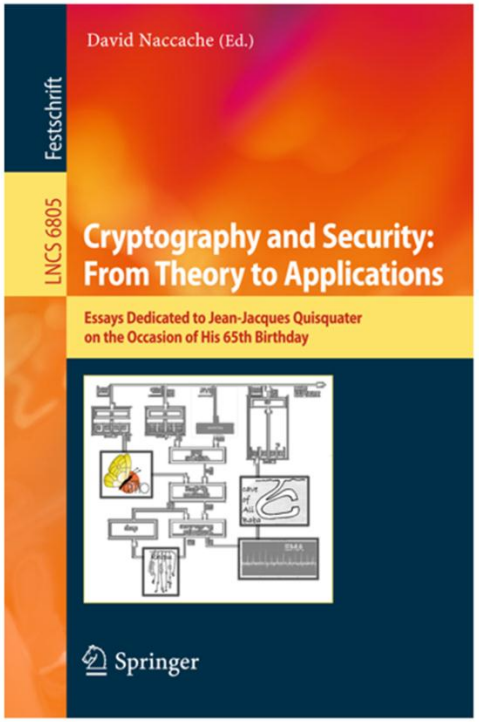

GROUPE
CRYPTO


GROUPE
CRYPTO

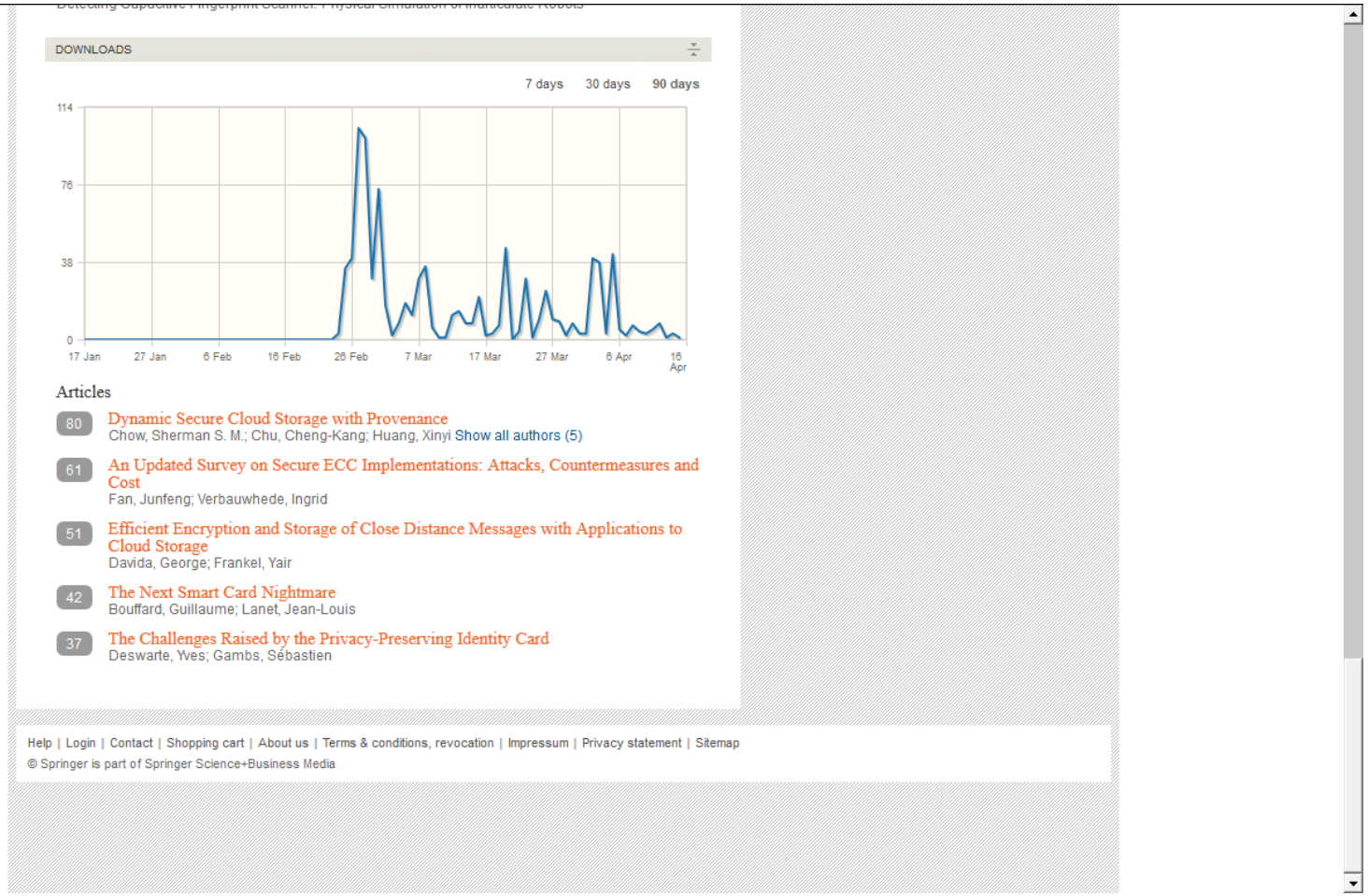

GROUPE
CRYPTO


secret key
GROUPE
CRYPTO
cave
of
Ali
Baba
EMA
khipu

Thanks, David!



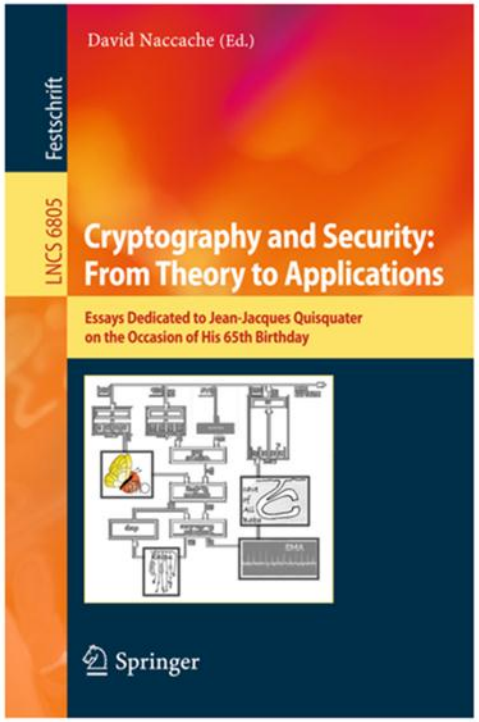
A success!


DOWNLOADS
7 days
30 days
90 days
114
76
38
0
17 Jan
27 Jan
6 Feb
16 Feb
26 Feb
7 Mar
17 Mar
27 Mar
6 Apr
16 Apr
Articles
80 Dynamic Secure Cloud Storage with Provenance
Chow, Sherman S. M.; Chu, Cheng-Kang; Huang, Xinyi Show all authors (5)
61 An Updated Survey on Secure ECC Implementations: Attacks, Countermeasures and Cost
Fan, Junfeng; Verbauwhede, Ingrid
51 Efficient Encryption and Storage of Close Distance Messages with Applications to Cloud Storage
Davida, George; Frankel, Yair
42 The Next Smart Card Nightmare
Bouffard, Guillaume; Lanet, Jean-Louis
37 The Challenges Raised by the Privacy-Preserving Identity Card
Deswarte, Yves; Gambs, Sébastien
Help | Login | Contact | Shopping cart | About us | Terms & conditions, revocation | Impressum | Privacy statement | Sitemap
© Springer is part of Springer Science+Business Media

Now the challenge!

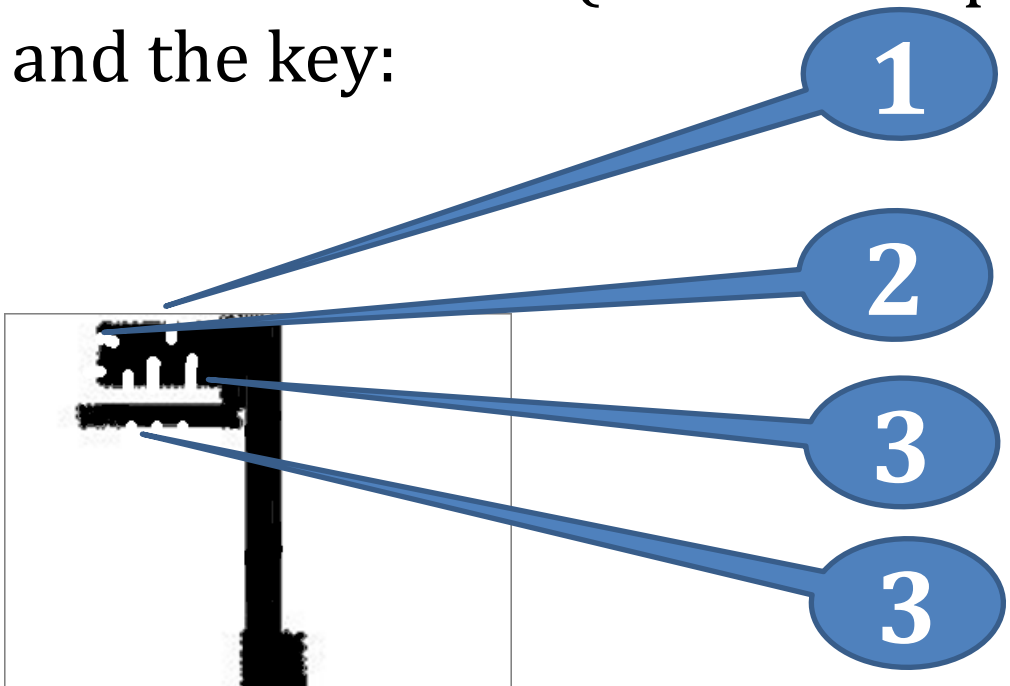
- What is the integer value of the secret key?
- 4 digits: some hint was already given
- Give me a piece of paper with the value and your name: the prize will be given to the first correct answer or the closest one (my definition)

Now the prize!



After the rump session
News from the challenge

- The winner is Mark Manulis (University of Surrey)
- My hope was that somebody remarks an anomaly on the first slide … ☺
- The secret key is: 1233
  - See the first slide (with a fake page number) and the key:



Next game

- At CRYPTO 2012?