HAL
archives-ouvertes.fr

Symmetric Cryptanalysis: the Foundation of Trust

María Naya-Plasencia

▶ To cite this version:

María Naya-Plasencia. Symmetric Cryptanalysis: the Foundation of Trust. Lorentz Center Highlights, Mar 2018, Leiden, Netherlands. hal-01954612

HAL Id: hal-01954612
https://hal.inria.fr/hal-01954612

Submitted on 19 Dec 2018

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Symmetric Cryptanalysis: The Foundation of Trust

María Naya-Plasencia
Inria, France

ERC project QUASYModo

informatics mathematics

European Research Council
Established by the European Commission

Lorentz Center- 20 Mars 2018

Outline

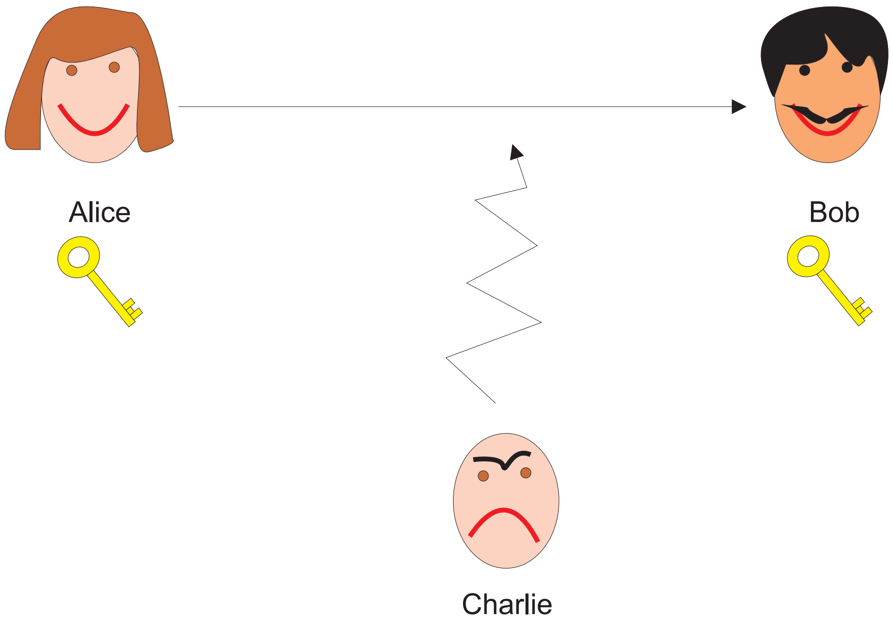
- Symmetric Cryptography
- Symmetric Cryptanalysis: Foundation of Trust
- Quantum Symmetric Cryptanalysis

Symmetric Cryptography

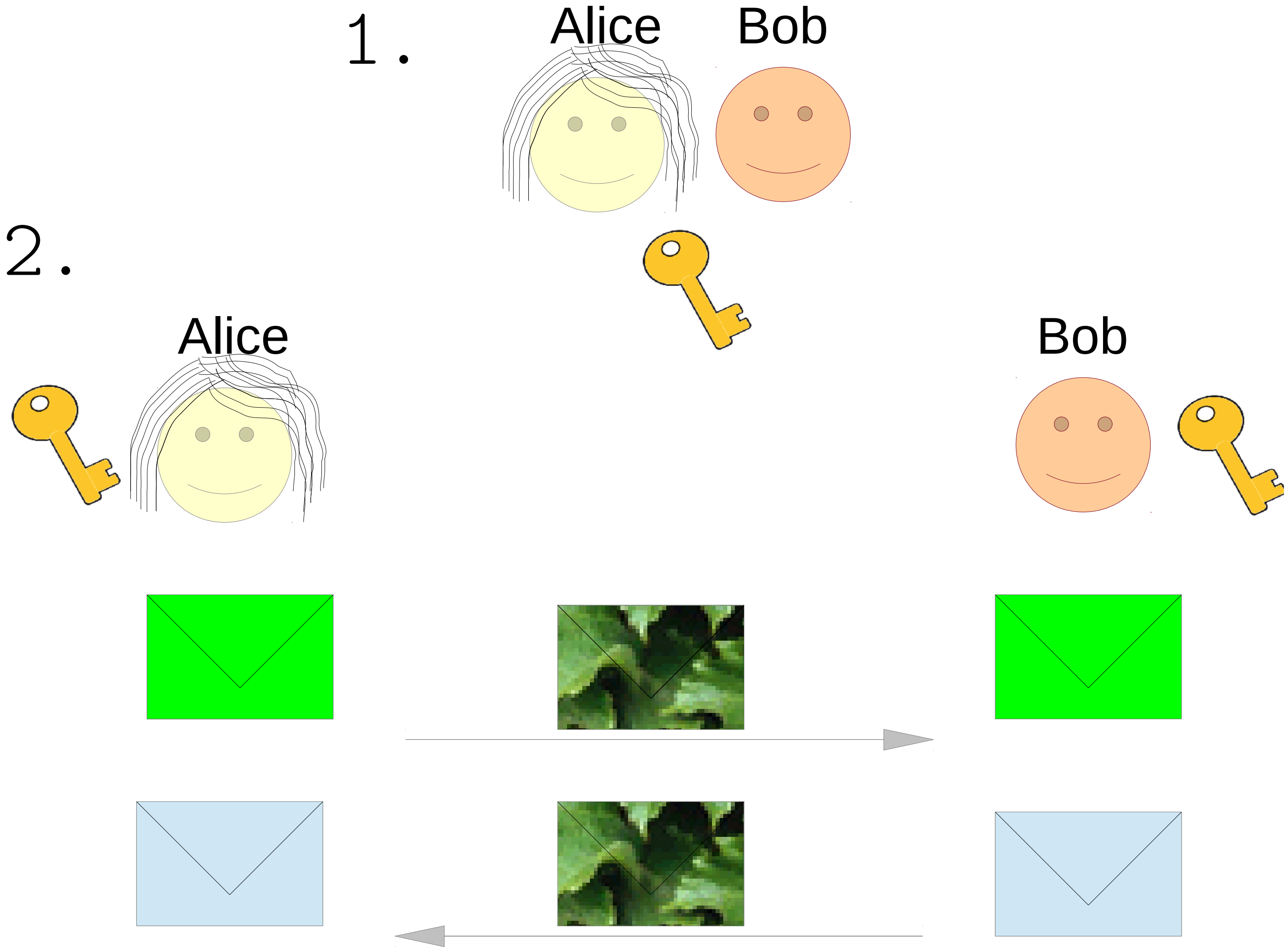
Cryptography

- Cryptography : hiding/protecting information, usually with the help of a key.

Symmetric cryptography and Asymmetric cryptography

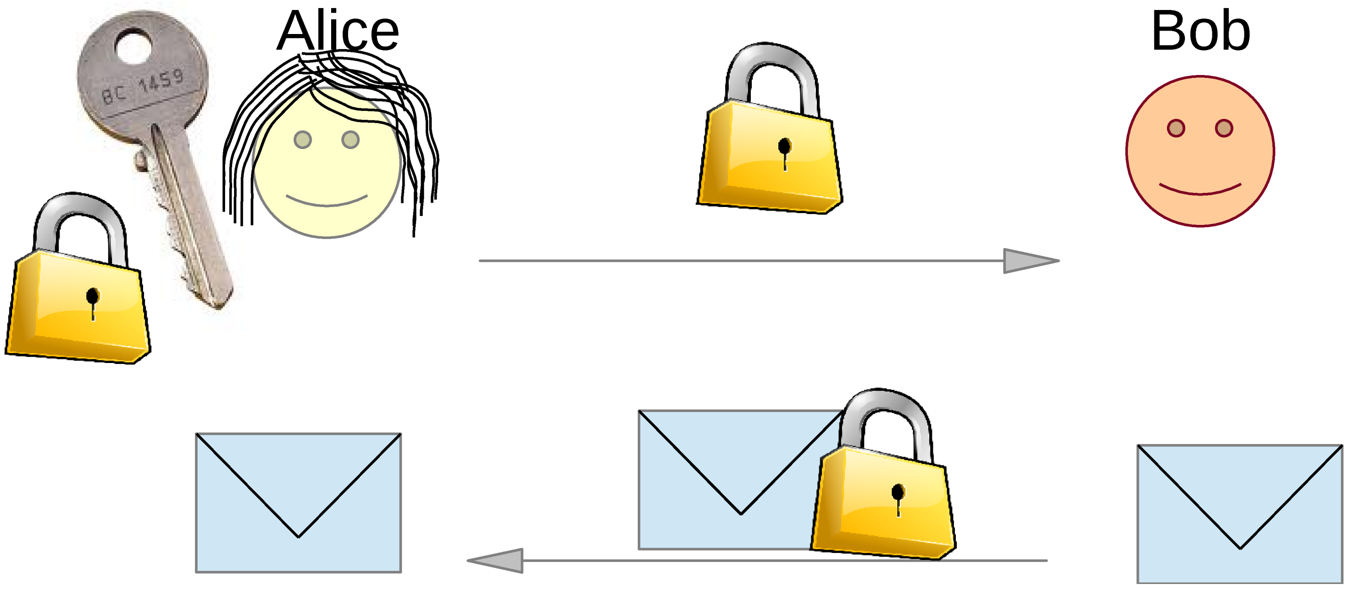


Symmetric Cryptography



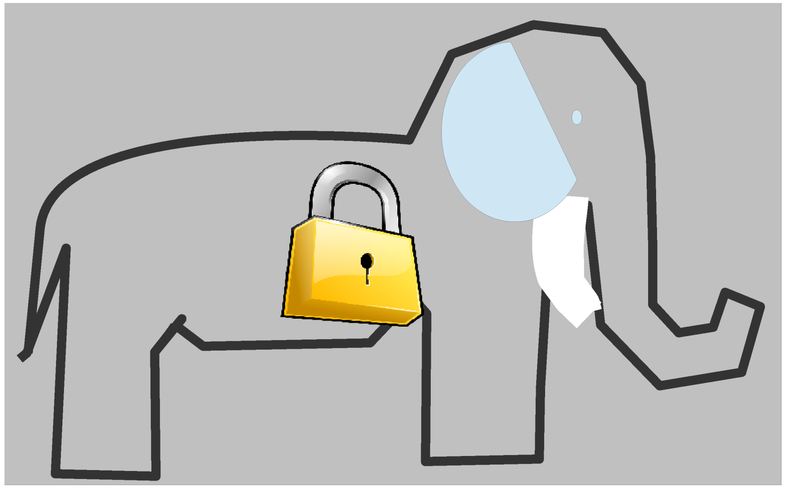
Asymmetric Cryptography

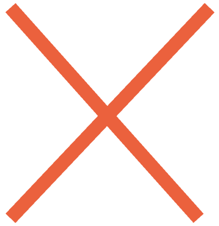
Without needing a previous meeting:

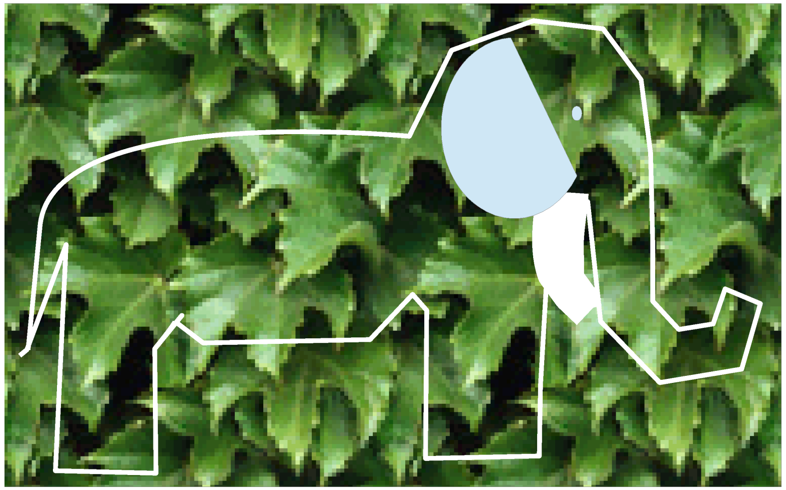


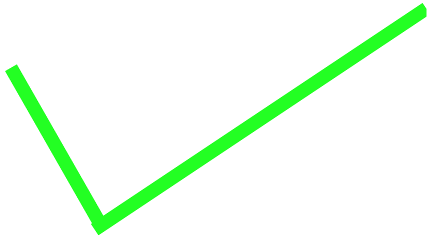
Asymmetric vs Symmetric Cryptography

Efficiency:









Asymmetric vs Symmetric Cryptography

Asymmetric:

- Advantage: No need of key exchange.
- Disadvantage: In "real life", "slow" and "big".

Symmetric:

- Disadvantage: Need of key exchange.
- Advantage: Performant, adapted to constrained environments.

$\Rightarrow$ Use asymmetric for key exchange, and next use symmetric!!.

Classical Cryptography

Enable secure communications even in the presence of malicious adversaries.

Asymmetric (e.g. RSA) *(no key exchange/computationally costly)*

Security based on well-known hard mathematical problems (e.g. factorization).

Symmetric (e.g. AES) *(key exchange needed/efficient)*

Ideal security defined by generic attacks ($2^{|K|}$).

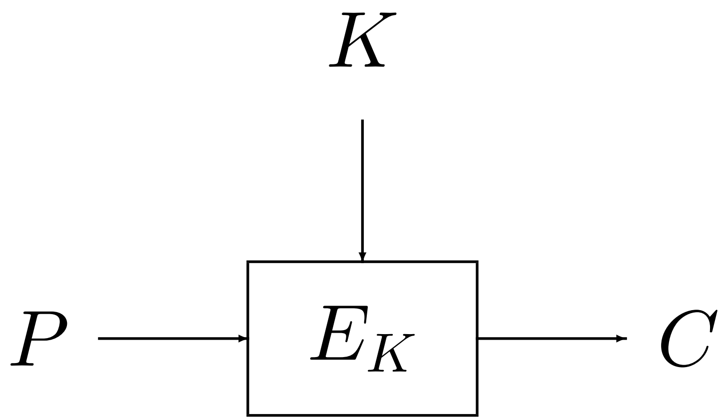
Need of continuous security evaluation (cryptanalysis).

⇒ Hybrid systems! (e.g. in SSH)

Symmetric primitives

- Block ciphers, (stream ciphers, hash functions..)

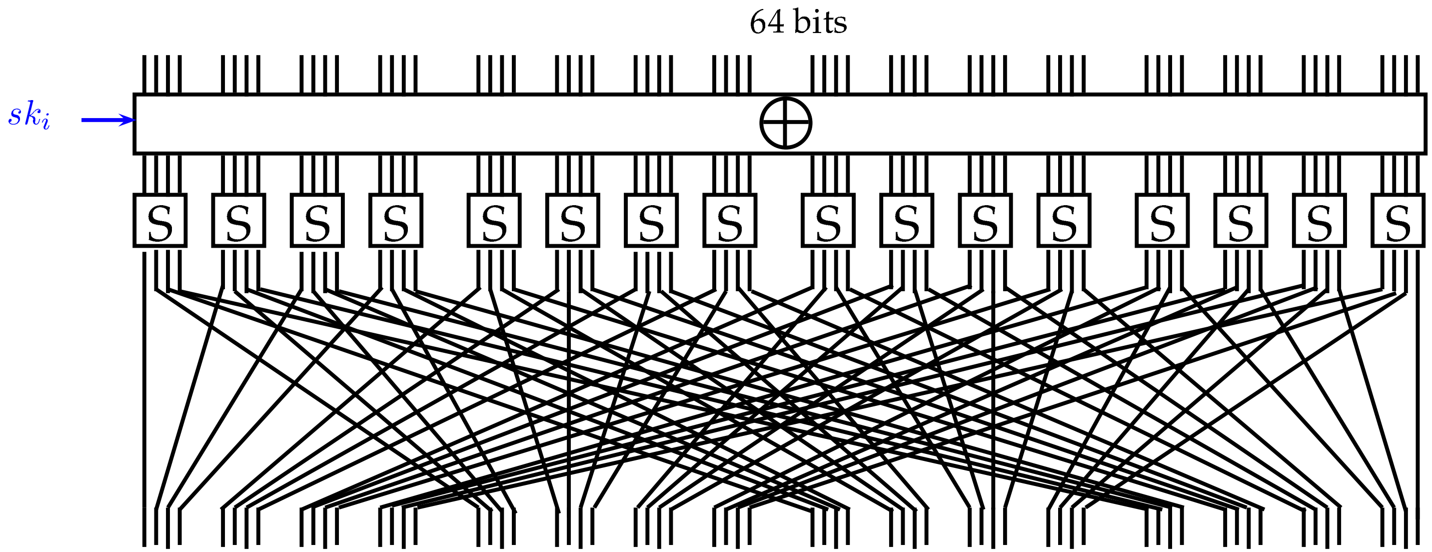
Message decomposed into blocks, each transformed by the same function E_K.



E_K is composed of a round transform repeated through several similar rounds.

Example: PRESENT [BKLPPRSV'07]

Block $n = 64$ bits, key 80 or 128 bits.



31 rounds + 1 key addition.

Generic Attacks on Ciphers

- Security provided by an ideal block cipher defined by the best generic attack:
  exhaustive search for the key in $2^{|K|}$.

- Recovering the key from a secure cipher must be infeasible:

  $\Rightarrow$ typical key sizes $|K| = 128$ to 256 bits.

Cryptanalysis: Foundation of Confidence

Any attack better than the generic one
is considered a "break".

- Proofs on symmetric primitives need to make unrealistic assumptions.
- We are often left with an empirical measure of the security: cryptanalysis.

Current scenario

- Competitions (AES, SHA-3, eSTREAM, CAESAR).
- New needs: lightweight, FHE-friendly, easy-masking.
  $\Rightarrow$ Many good proposals/candidates.

- How to choose?

- How to be ahead of possible weaknesses?

- How to keep on trusting the chosen ones?

Cryptanalysis: Foundation of Confidence

When can we consider a primitive as secure?

- A primitive is secure as far as no attack on it is known.
- The more we analyze a primitive without finding any weaknesses, the more reliable it is.

Design new attacks + improvement of existing ones:

- essential to keep on trusting the primitives,
- or to stop using the insecure ones!

On weakened versions

If no attack is found on a given cipher, what can we say about its robustness, security margin?

The security of a cipher is not a 1-bit information:

- Round-reduced attacks.
- Analysis of components.

$\Rightarrow$ determine and adapt the security margin.

On high complexities

When considering large keys, sometimes attacks breaking the ciphers might have a very high complexity far from practical *e.g.*. 2^{120} for a key of 128 bits.

Still dangerous because:

- Weak properties not expected by the designers.
- Experience shows us that attacks only get better.
- Other existing ciphers without the "ugly" properties.

- ▶ When determining the security margin: find the highest number of rounds reached.

Post-Quantum
Symmetric Cryptography

Post-Quantum Cryptography

Adversaries have access to **quantum computers.**

Asymmetric (e.g. RSA):

Shor's algorithm: Factorization in polynomial time

$\Rightarrow$ current systems not secure!

Solutions: lattice-based, code-based cryptography...

Symmetric (e.g. AES):

Grover's algorithm: Exhaustive search from $2^{|K|}$ to $2^{|K|/2}$.

Double the key length for equivalent ideal security.

We don't know much about cryptanalysis of current ciphers when having quantum computing available.

Post-Quantum Cryptography

Problem for present existing long-term secrets.
$\Rightarrow$ start using quantum-safe primitives NOW.

Important tasks:

- Conceive the cryptanalysis algorithms for evaluating the security of symmetric primitives in the P-Q world.
- Use them to evaluate and design symmetric primitives for the P-Q world.

Quantum Symmetric Cryptanalysis

Some recent results on Q-symmetric crytanalysis:

3-R Feistel [Kuwakado-Morii10], Even-Mansour [Kuwakado-Morii12], Mitm [Kaplan14], Related-Key [Roetteler-Steinwandt15], Diff-lin [Kaplan-Leurent-Leverrier-NP16], Simon's[Kaplan-Leurent-Leverrier-NP16], FX [Leander-May17], parallel multi-preim. [Banegas-Bernstein17], Multicollision [Hosoyamada-Sasaki-Xagawa17],
AEZ [Bonnetain17].

Final Conclusion

Symmetric (Quantum) Cryptanalysis

Better safe than sorry:

Lots of things to do !