What Innovative Solutions for Encryption?

Eric Filiol
Axe Confiance Numérique & Sécurité
Laboratoire de cryptologie et de virologie opérationnelles
filiol@esiea.fr

Introduction

- Encryption becomes an even more critical issue than in the past
  - Control stakes by nation states for their security
  - Issue for the protection of individual freedom and privacy
  - Stakes in protecting business
- What will be the evolution of control on cryptology by nation states?

Introduction

- When facing these challenges, cryptology must evolve to meet new challenges, new uses and new threats
- These issues depend on the perspective taken and the security posture
  - Attacker's view (*e.g.* Protection of his malware in memory)
  - Defender (*e.g.* Encrypted content filtering)
  - We need to adopt a broad view
- Scientific and technical evolutions
- Legal and societal evolutions

Aim of this Masterclass

- Evoking the main possible innovations in cryptology, particularly encryption
  - Without (too much) math!
  - Without claiming to be exhaustive
- Think on the growing impact of the use of cryptology in our societies
- Based on scientific and technological watch, R & D conducted in my laboratory, the analysis of specific cases (defense and justice)
- The encryption feature will be considered primarily

Agenda

- Introduction ✓
- Definitions, concepts and limitations
- Scientific and technical evolutions
  - Homomorphic encryption, authenticated encryption schemes, COMSEC vs TRANSEC, mathematical poly/metamorphism for encryption, mathematical backdoors, the quantum era…
- Legal and societal evolutions
- Conclusion

Agenda

- Introduction
- Definitions, concepts and limitations
- Scientific and technical evolutions
  - Homomorphic encryption, authenticated encryption schemes, COMSEC vs TRANSEC, mathematical poly/metamorphism for encryption, mathematical backdoors, the quantum era…
- Legal and societal evolutions
- Conclusion

Definitions & concepts

- Symmetric cryptography
  - Alice and Bob share the **same secret** key K
  - Lies on the Information theory (Shannon's 3rd theorem)
  - Very high encryption speed (processing of huge information quantities)
  - Encryption key management issues
- Essentially dedicated to encipher data for confidentiality purposes
- Message M, key K and cryptogram C
  - C = E(K, M) and M = E(K, C) = E(K, E(K, M))

Definitions & concepts

- Asymmetric cryptography
  - Alice and Bob each have a key pair (public, private); they share only their respective public part
  - Lies on the complexity theory
  - Implementation issues and alleged/practical proof of security only supposée (do computationally problems really exist?)
  - Very slow (processing of small amounts of information)
- Mainly dedicated to authentication, integrity and digital signature functionalities

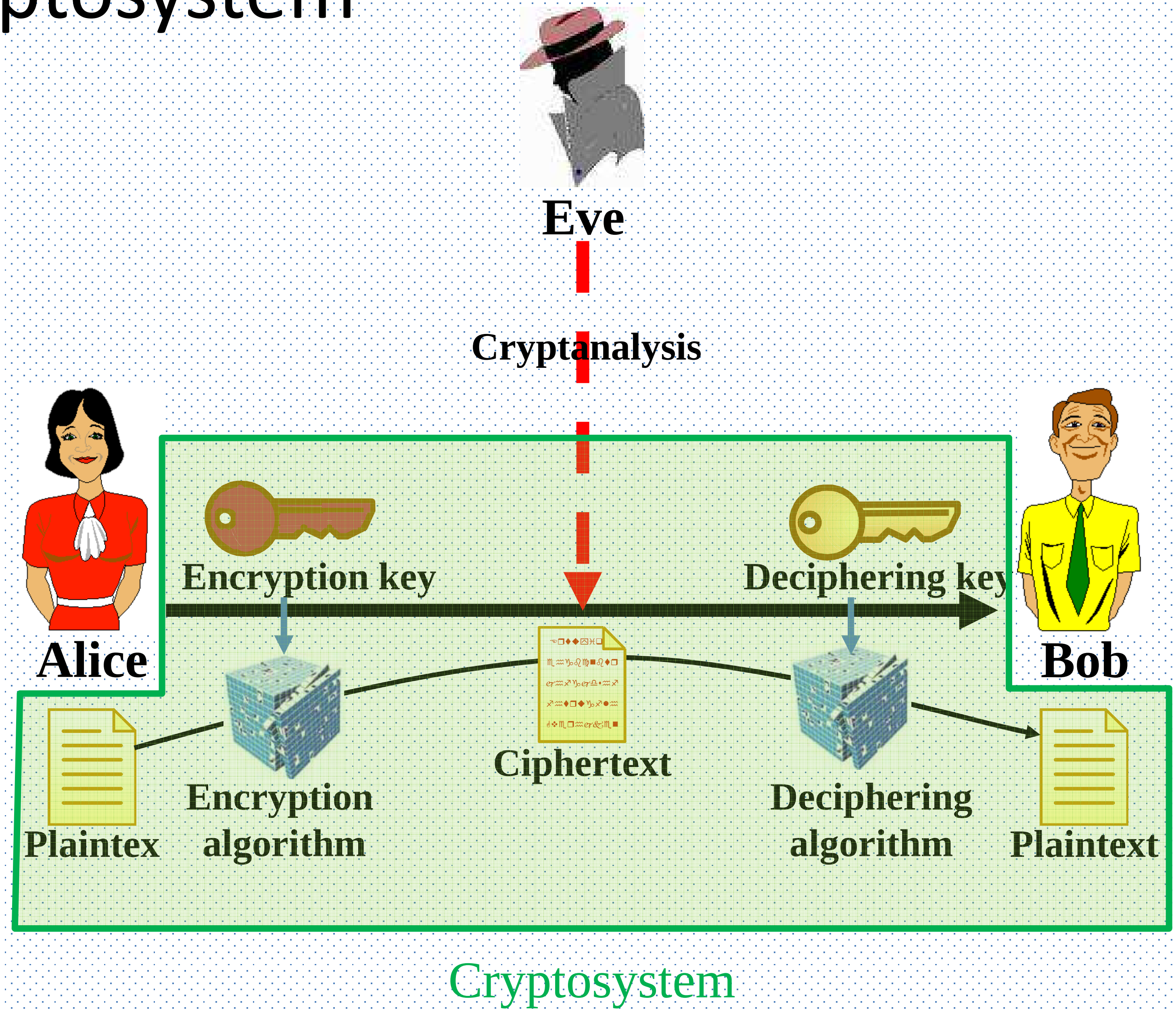
Symmetric vs asymmetric

	Symmetric	Asymmetric
Existence	For centuries	Less than 50 years
Security	Secure in theory and practically	Lie on a supposed security (untractable problems are supposed to exist [non proved])
Encryption speed	Very fast	slow
Keys	Secret key	(“public” key, private key)
Key management	Prior key exchange	PKI, trust sphere

Definitions & concepts

- Hybrid cryptolography
  - Optimal combination (regarding performances and use) of symmetric and asymmetric cryptography
  - The global security is equal to that of the weakest component
  - A message/session (symmetric) key is encrypted with asymmetric encryption and sent along with the encrypted text
- PGP, GnuPG, ACID Cryptofiler…

Cryptosystem



Why Encryption Must Evolve?

- The main current limitations actually require these evolutions
  - Encryption is easy to detect (COMSEC vs TRANSEC)
  - Implementation security
  - Limited scope: some calculations or operations can be done on plaintext data only (electronic vote, DB search, CPU/memory processing ...)
  - Trust issues regarding mathematical algorithms
  - Deterministic nature of encryption algorithms
  - …

Agenda

- Introduction
- Definitions, concepts and limitations
- Scientific and technical evolutions
  - Homomorphic encryption, authenticated encryption schemes, COMSEC vs TRANSEC, mathematical poly/metamorphism for encryption, mathematical backdoors, the quantum era…
- Legal and societal evolutions
- Conclusion

The Issue

- In many situations, data must remain in plaintext to be processed
  - Data in memory (voting scheme, auctions, binary code ...)
  - Data in "public" spaces (DB, cloud)
- *“Can we do arbitrary computations on data while it remains encrypted, without ever decrypting it?”* (Rivest, Adleman, Dertouzos, 1978).
- Yes! With homomorphic encryption
- « Fully homomorphic encryption is a bit like enabling a layperson to perform flawless neurosurgery while blindfolded, and without later remembering the episode » (C. Lickel, Vice président d’IBM *Software Research*)
- Considered as the cryptography graal

Principles

- Having an encryption system to achieve basic operations directly on encrypted data
- These basic operations enable to describe any computable functions with logical (Boolean) circuits (AND and OR functions)
- Two types :
  - Partially homomorphic systems
  - Fully homomorphic systems

Partially Homomorphic Encryption (PHE)

- They enable to achieve only a subset of desirable operations
- RSA with $E(x) = x^e \bmod m$
  - $E(x_1).E(x_2) = E(x_1x_2) \bmod m$ (multiplication only)
- Pailler's system
  - $E(x_1)E(x_2) = E(x_1 + x_2)$ (addition only)
- A large number of systems proposed since (Micali & Goldwasser, 1984)

PHE: Electronic Vote

- Candidates C_1 & C_2, voters V_1, …, V_n

	C_1	C_2
V_1	$V_{1,1} = E(1, pk_A)$	$V_{1,2} = E(0, pk_A)$
V_2	$V_{2,1} = E(0, pk_A)$	$V_{2,2} = E(1, pk_A)$
…		
V_n	$V_{n,1} = E(0, pk_A)$	$V_{n,2} = E(1, pk_A)$
Totals	$\prod_{i=1}^{n} v_{i,1} = E(Score_{C1,}\ pk_A)$	$\prod_{i=1}^{n} v_{i,2} = E(Score_{C2,}\ pk_A)$

- Authority A deciphers with sk_A
- http://heliosvoting.org/

Fully Homomorphic Encryption (FHE)

- Having an encryption system allowing data processing algorithms to pass through the encryption layer
  - A cloud customer wants to perform some calculations on his data
  - It is sufficient that require the supplier to perform these calculations on encrypted data
  - The provider sends the results (encrypted), the client decrypts and obtains the result (plaintext)
- Example (source Futjitsu)

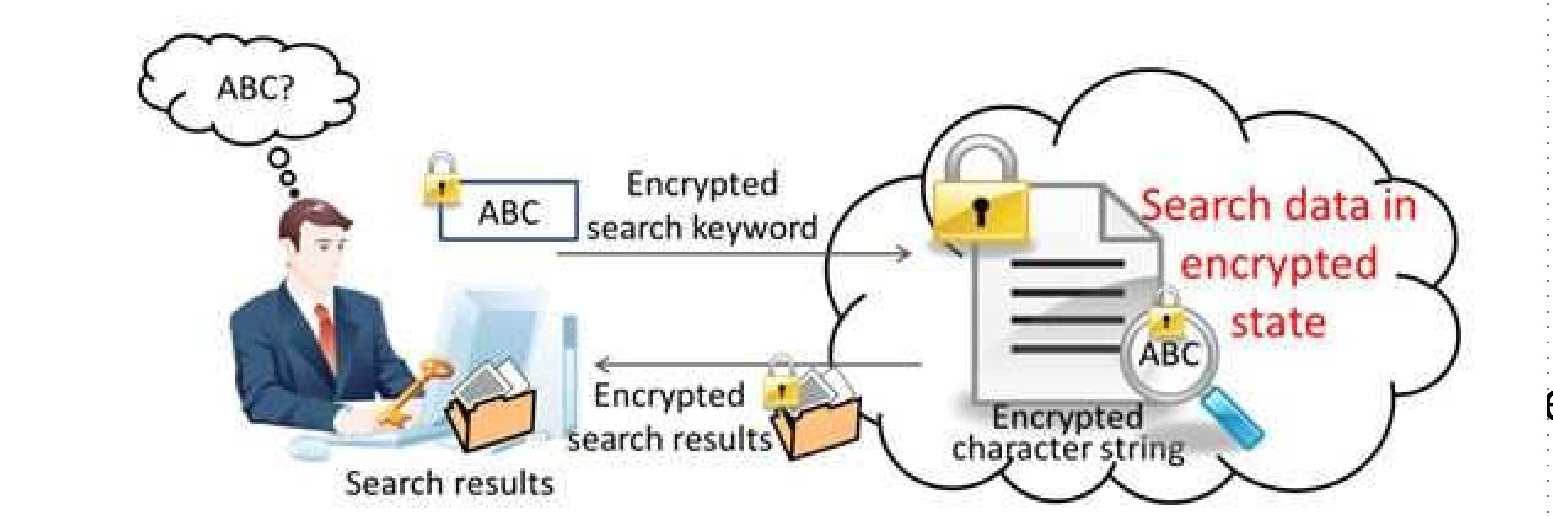
Fully Homomorphic Encryption (FHE)

- Having an encryption system allowing data

on

on

ese



  - The provider sends the results (encrypted), the client decrypts and obtains the result (plaintext)

- Example (source Futjitsu)

Fully Homomorphic Encryption (FHE)

- Great progress with the work of G. Gentry (2009 thesis) and successive developments (2010 - 2015)
- Based on Euclidian networks/lattices or NTRU-based systems as well as complex statistical techniques (bootstrapping)
- DARPA funding (more than 30 millions €)
- Encryption of both the data and the calculations on the data

FHE Principes

- Key generation : *GenCle*(k) = (pk, sk, evk)
- Encryption : c = E(m, pk)
- Decryption : m = D(c, sk)
- Homomorphic evaluation: c_f = Eval(f, c_1,…, c_n, evk)
  - f is described by an arithmetic Boolan circuit

FHE - Limitations

- Still very slow systems with huge size of keys
  - AES evaluation (Gentry, Halevi & Smart, 2015)
    - 2 sec/bloc & 3Gb of RAM
- Security analysis of these scheme to be done
- But very promising advance with many possible applications
  - The principle is acquired, it just remains to be improved
- Potential problems for the validity of the (encrypted) "digital evidence" in court

FHE – Further Reading & Pointers

- http://blogs.teamb.com/craigstuntz/2010/04/08/38577/
- http://blogs.teamb.com/craigstuntz/2010/03/18/38566/
- Open Source libraries
  - HELib https://github.com/shaih/HElib (Halevi & Shoup)
  - FHEW https://github.com/lducas/FHEW (Ducas & Micciancio, 2014)
- Reference papers
  - C. Gentry thesis (2009) http://crypto.stanford.edu/craig/
  - http://eprint.iacr.org/2014/873
  - http://eprint.iacr.org/2014/816
  - http://eprint.iacr.org/2014/106
  - http://eprint.iacr.org/2012/099 (revised January 2015)

Agenda

- Introduction
- Definitions, concepts and limitations
- Scientific and technical evolutions
  – Homomorphic encryption, authenticated encryption schemes, COMSEC vs TRANSEC, mathematical poly/metamorphism for encryption, mathematical backdoors, the quantum era…
- Legal and societal evolutions
- Conclusion

The Issue

- In a number of protocols, the combination of encryption mode with authentication mode is subject to many security vulnerabilities
  - Refer to http://competitions.cr.yp.to/disasters.html
- How to ensure confidentiality AND authentication simultaneously with one single system?
  - Authenticated Encryption system (AE or AED)
- International challenge launched in 2013 (CAESAR)

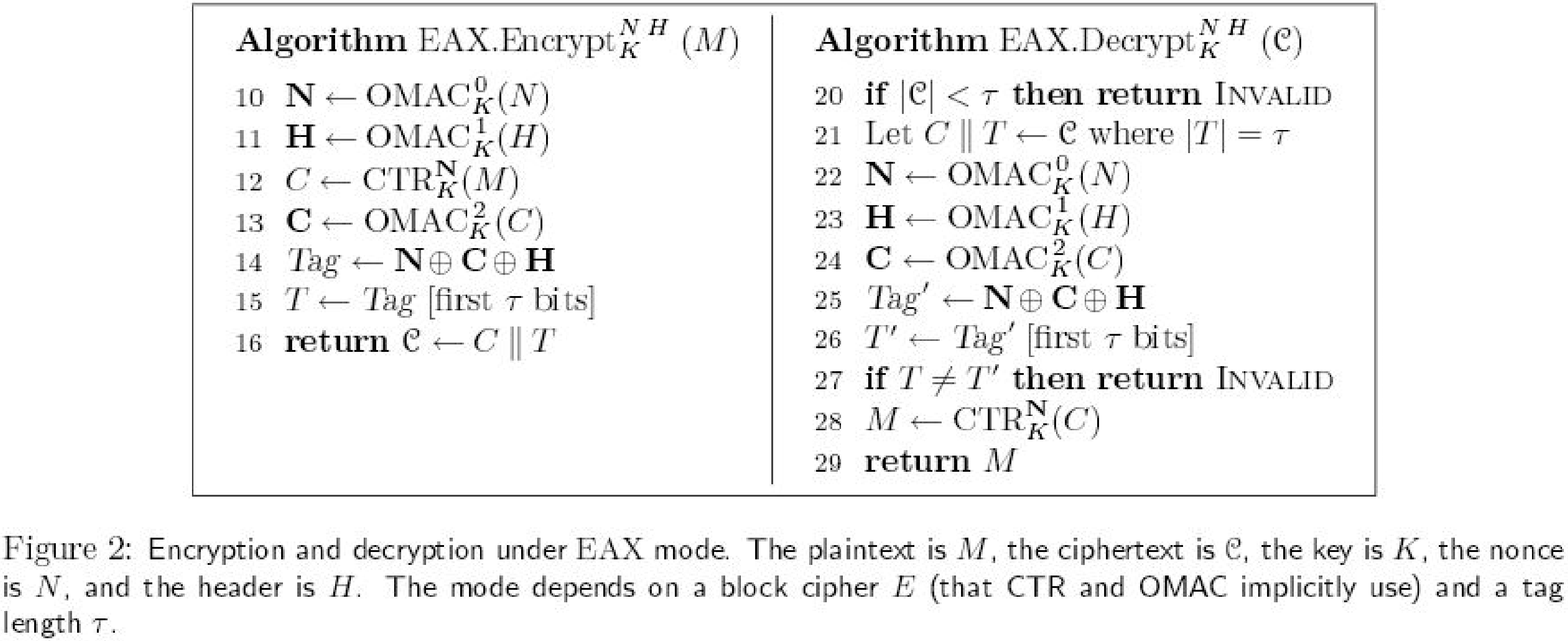
AE - Principles

- Consists in optimally combining an encryption system with a MAC primitive (*Message Authentication Code*)
  - – EtM (Encryption then MAC) ISO/IEC 19772:2009
  - – M&E (MAC and Encryption)
  - – MtE (MAC then Encryption) SSL/TLS
- Message have the form

<H header> <M payload> <T Tag>

AE – EAX Scheme

- Protocol due to Bellare & Namprempre (2000)



```
Algorithm EAX.Encrypt$_K^{N\,H}(M)$
    $\mathbf{N} \leftarrow \mathrm{OMAC}_K^0(N)$
    $\mathbf{H} \leftarrow \mathrm{OMAC}_K^1(H)$
    $C \leftarrow \mathrm{CTR}_K^{\mathbf{N}}(M)$
    $\mathbf{C} \leftarrow \mathrm{OMAC}_K^2(C)$
    $Tag \leftarrow \mathbf{N} \oplus \mathbf{C} \oplus \mathbf{H}$
    $T \leftarrow Tag$ [first $\tau$ bits]
    return $\mathcal{C} \leftarrow C \,\|\, T$
```

```
Algorithm EAX.Decrypt$_K^{N\,H}(\mathcal{C})$
    if $|\mathcal{C}| < \tau$ then return INVALID
    Let $C \,\|\, T \leftarrow \mathcal{C}$ where $|T| = \tau$
    $\mathbf{N} \leftarrow \mathrm{OMAC}_K^0(N)$
    $\mathbf{H} \leftarrow \mathrm{OMAC}_K^1(H)$
    $\mathbf{C} \leftarrow \mathrm{OMAC}_K^2(C)$
    $Tag' \leftarrow \mathbf{N} \oplus \mathbf{C} \oplus \mathbf{H}$
    $T' \leftarrow Tag'$ [first $\tau$ bits]
    if $T \neq T'$ then return INVALID
    $M \leftarrow \mathrm{CTR}_K^{\mathbf{N}}(C)$
    return $M$
```

Figure 2: Encryption and decryption under EAX mode. The plaintext is M, the ciphertext is $\mathcal{C}$, the key is K, the nonce is N, and the header is H. The mode depends on a block cipher E (that CTR and OMAC implicitly use) and a tag length τ.

AE – Further Reading & Pointers

- J. Bernstein “*Failures of Secret-key Cryptography*”, http://cr.yp.to/talks/2013.03.12/slides.pdf
- CAESAR http://competitions.cr.yp.to/caesar.html
- DIAC 2014: Directions in Authenticated Ciphers http://2014.diac.cr.yp.to/
- RFC 7366 (extension EtM pour TLS et DTLS)
- Bellare et Namprempre 2000 http://cseweb.ucsd.edu/~mihir/papers/oem.html

Agenda

- Introduction
- Definitions, concepts and limitations
- Scientific and technical evolutions
  - Homomorphic encryption, authenticated encryption schemes, COMSEC vs TRANSEC, mathematical poly/metamorphism for encryption, mathematical backdoors, the quantum era…
- Legal and societal evolutions
- Conclusion

The Issue

- Communicating through an encrypted traffic consists to send/receive noise
  - Maximal entropy profile
  - Very easy to detect and to filter
- Only the communication is protected (COMSEC) not the channel (TRANSEC)
- How to securely exchange while concealing the existence of a communication?
  - Problem of political opponents or journalists ...

Solutions

- Steganography
  - Hiding a secret (encrypted) information into an innocent-looking content (image, sound…)
  - Problem: hiding rate very (too much) low for an operational use on message beyond a few hundreds of bits
- Lower naturally the entropy of the ciphertext while keeping the COMSEC security untouched
- Other?

Solutions

- Steganography

n

n

ls

- xt

- Other?

Example: PERSEUS Technology

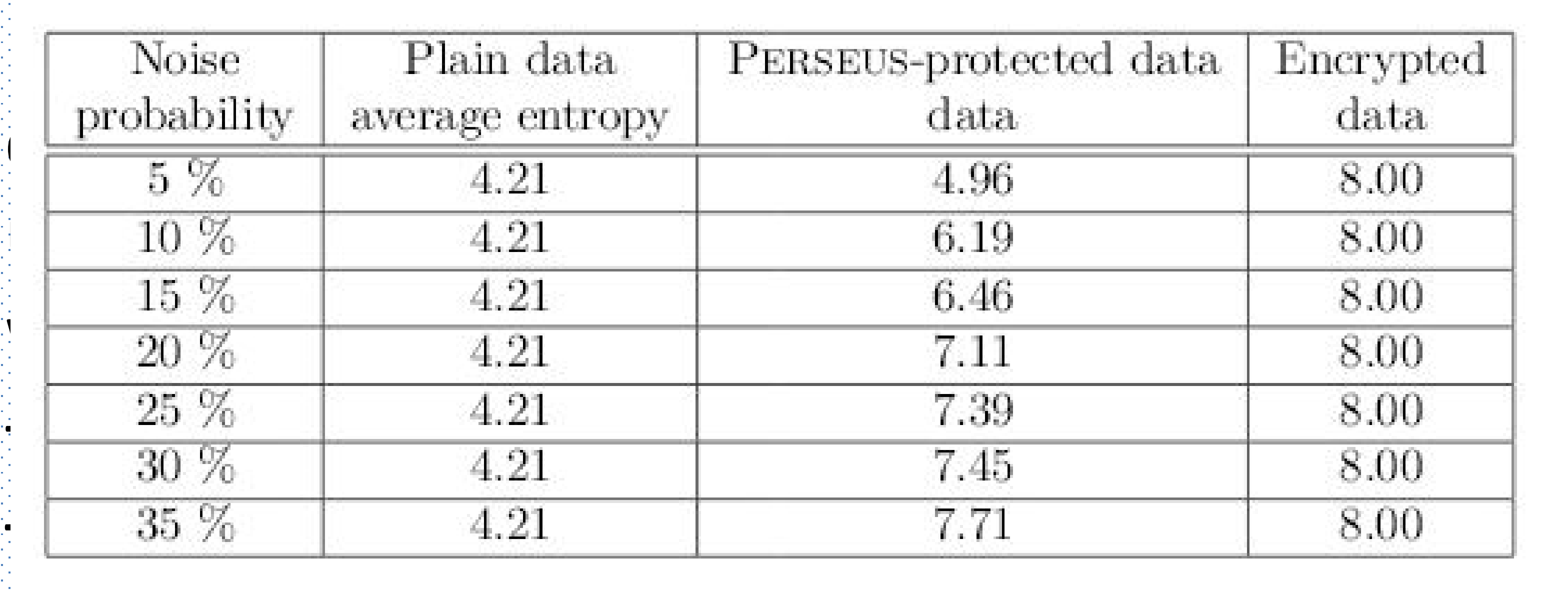
- Inspired by coding theory, since an encoded message has a lower entropy than an encrypted text
- Application of a secret random convolutional code C on the message M
  - Partly used by the Czech army during the 90s
  - M’ = $\mathrm{Conv}_C(M)$
  - Add a random deterministic noise: sequence $\sigma(K)$
    - C = M’ $\oplus$ $\sigma(K)$
- C and $\sigma(K)$ depend on a secret key K

PERSEUS Technology (ctd)

- The security relies on the fact that reconstructing an unknown encoder in a noisy context (beyond a very few % of noise) is an untractable problem
- Without the secret encoder, it is not possible to decode M
- The entropy is easily tunable according the needs
- SMS Perseus et VoIP

PERSEUS Technology (ctd)

- The security relies on the fact that sy
  (an



Noise probability	Plain data average entropy	PERSEUS-protected data data	Encrypted data
5 %	4.21	4.96	8.00
10 %	4.21	6.19	8.00
15 %	4.21	6.46	8.00
20 %	4.21	7.11	8.00
25 %	4.21	7.39	8.00
30 %	4.21	7.45	8.00
35 %	4.21	7.71	8.00

- le
- ne
  needs
- SMS Perseus et VoIP

PERS (ctd)

- at sy an

Noise probability	ave	ata	Encrypted data
5 %			8.00
10 %			8.00
15 %			8.00
20 %			8.00
25 %			8.00
30 %			8.00
35 %			8.00

- le

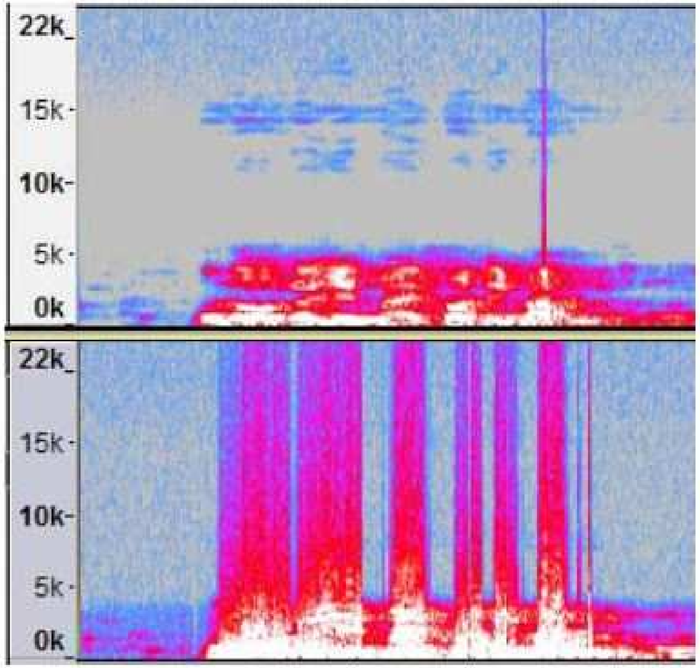


Fig. 2. Spectrogram and distortion of the RTP speaker (top) and listener (bottom).

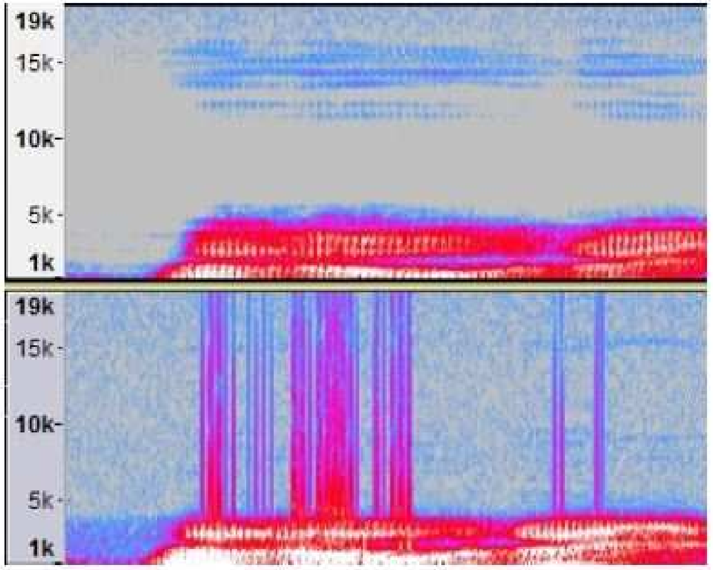
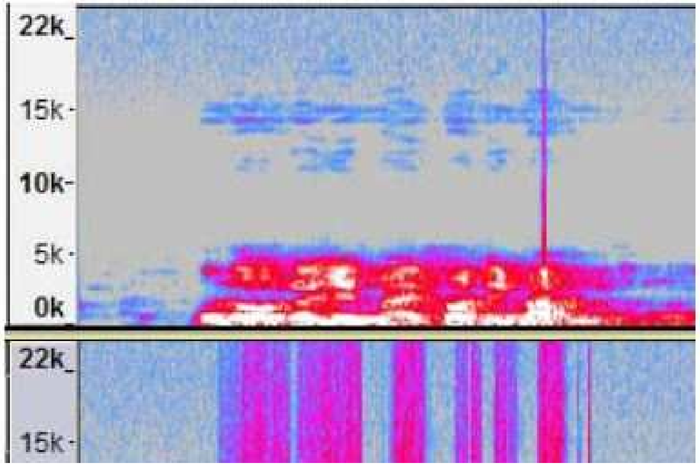


Fig. 3. Spectrogram and distortion of the PERSEUS speaker (top) and listener (bottom)

- The entrop according the needs
- SMS Perseu

PERS (ctd)



- at sy an

Noise probability	avc	ata	Encrypted data

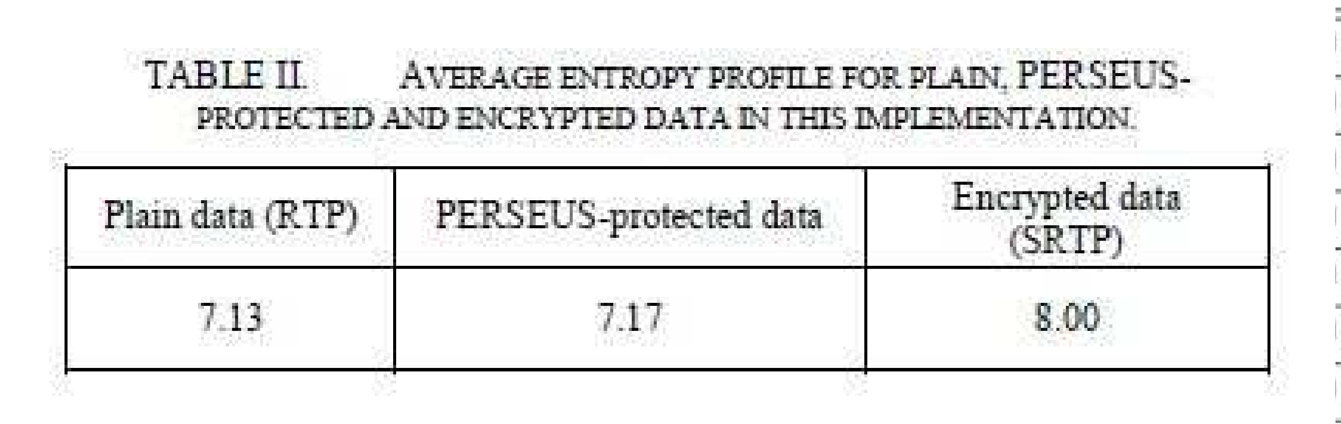


TABLE II. AVERAGE ENTROPY PROFILE FOR PLAIN, PERSEUS-PROTECTED AND ENCRYPTED DATA IN THIS IMPLEMENTATION.

Plain data (RTP)	PERSEUS-protected data	Encrypted data (SRTP)
7.13	7.17	8.00

- le

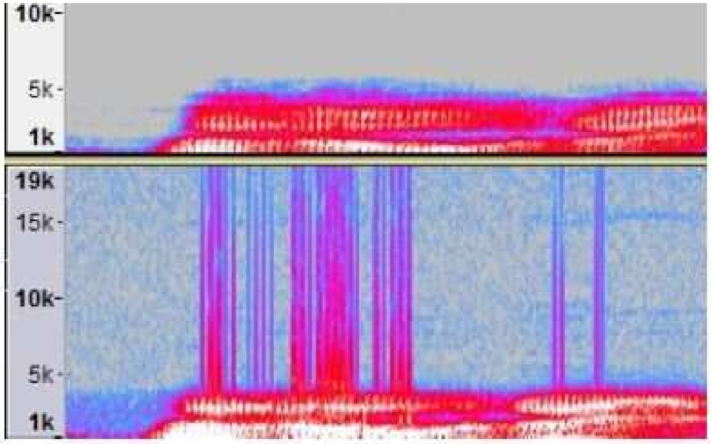


Fig. 3. Spectrogram and distortion of the PERSEUS speaker (top) and listener (bottom)

- The entrop according the needs
- SMS Perseu

Further Reading

- Eric Filiol *Reconstruction Techniques in Cryptology and in Coding Theory.* Ph D Thesis 2001
- Johann Barbier. *Analysis of communication channels in a non cooperative context.* Ph D Thesis 2007
- Bhume Bhumiratana, Saran Chiwtanasuntorn and Eric Filiol. "*Perseus on VoIP Protocols - Development and Implementation of VoIP Platforms*". IEEE - ECTI-CON, Thailand, May 14-17th, 2014
- E. Filiol. *PERSEUS Technology: New Trends in Information and Communication Security http://arxiv.org/abs/1101.0057 (presented at iAWACS 2010)*

Agenda

- Introduction
- Definitions, concepts and limitations
- Scientific and technical evolutions
  - Homomorphic encryption, authenticated encryption schemes, COMSEC vs TRANSEC, mathematical poly/metamorphism for encryption, mathematical backdoors, the quantum era…
- Legal and societal evolutions
- Conclusion

The Issue

- Existing encryption systems are deterministic algorithms
  - The {statistical, mathematical} analysis of the algorithm is then possible since the algorithm is fixed
  - No variability/uncertainty to opposer to the cryptanalyst
- How to oppose uncertainty regarding the algorithm while maintaining a high level of cryptographic security?

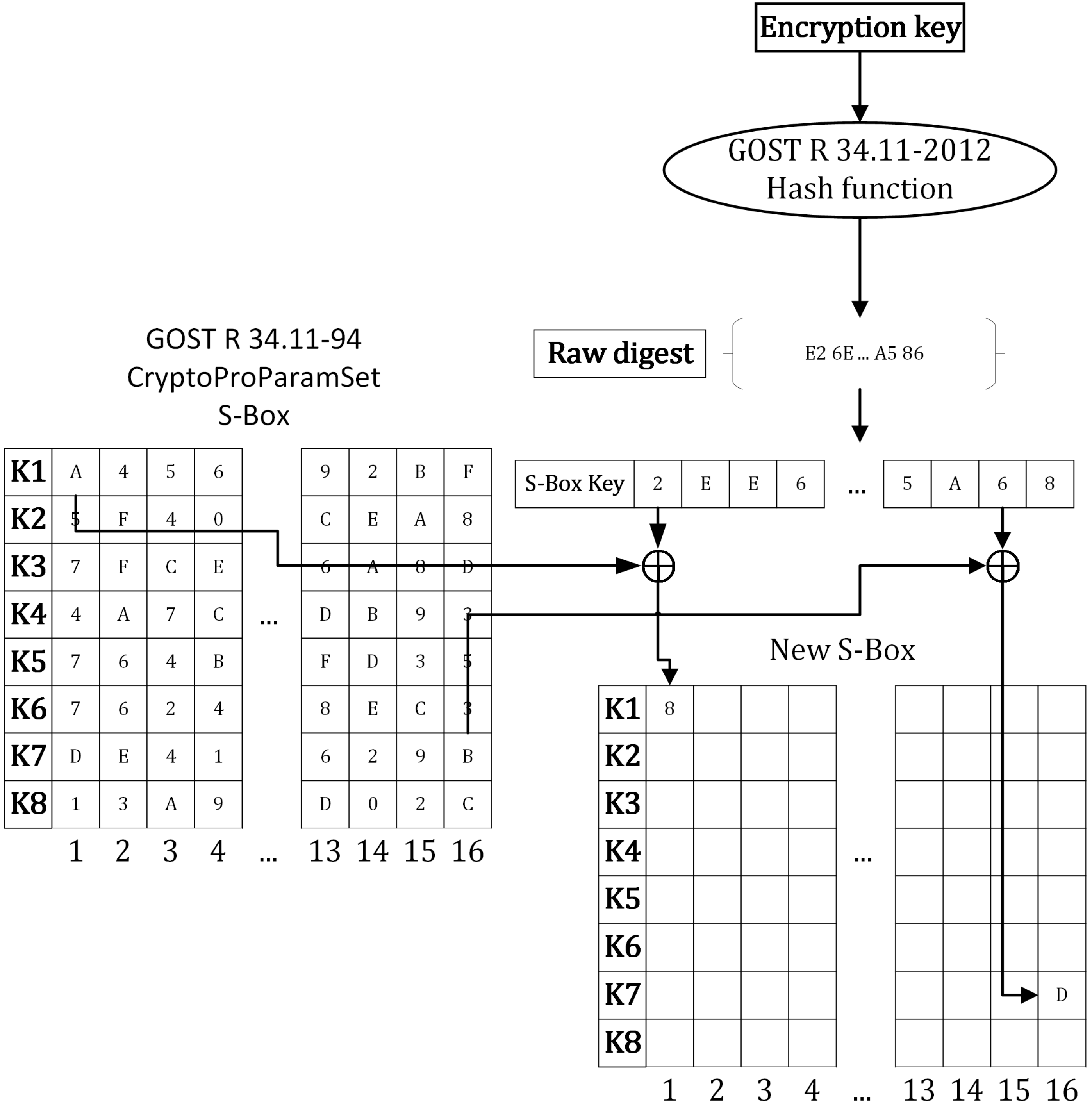
Cryptographic Polymorphism & metamorphism

- Inspired by mutation code techniques used in malware
  - Mathematical polymorphism: the mutation algorithm is deterministic, the mathematical description of the encryption is not
  - Mathematical metamorphism: both the mutation algorithm and the mathematical description of the encryption are constantly mutating
- MetaCrypt project (started in 2012) – Ph D student wanted

Example

- GostCrypt (https://www.gostcrypt.org)
  - 1st mutation level: the user's secret key modifies the Sbox in the algorithm
  - 2nd mutation level: an additional key (message key) change every 512 byte of data (XTS mode, data unit ID)
  - No existing known cryptanalysis can work

- Go
  - fies
  - age ode,



GOST R 34.11-94 CryptoProParamSet S-Box

	1	2	3	4	...	13	14	15	16
K1	A	4	5	6		9	2	B	F
K2	5	F	4	0		C	E	A	8
K3	7	F	C	E		6	A	8	D
K4	4	A	7	C	...	D	B	9	3
K5	7	6	4	B		F	D	3	5
K6	7	6	2	4		8	E	C	3
K7	D	E	4	1		6	2	9	B
K8	1	3	A	9		D	0	2	C

S-Box Key	2	E	E	6	...	5	A	6	8

New S-Box

	1	2	3	4	...	13	14	15	16
K1	8								
K2									
K3									
K4					...				
K5									
K6									
K7									D
K8									

Agenda

- Introduction
- Definitions, concepts and limitations
- Scientific and technical evolutions
  - Homomorphic encryption, authenticated encryption schemes, COMSEC vs TRANSEC, mathematical poly/metamorphism for encryption, mathematical backdoors, the quantum era…
- Legal and societal evolutions
- Conclusion

The Issue

- Is is possible to design an undetectable **mathematical** backdoor?
- A few works in the area
  - Rijmen & Preenel, 1997
  - C. Harpes, 1997
  - K. G. Paterson, 1999
  - NSA research (G. Simmons, non public)
- Know (weak) example: DUAL_EC_DRBG de RSA confirmed by E. Snowden

Issues

- Who knows the backdoor is able to break the system easily (or at least in operational conditions)
- Exhibiting the backdoor is computationally untractable (combinatorial explosion)
- Being able to prove that it is practically possible to design a mathematical backdoor is a critical issue
  - Critical issue especially if we use non national system or cryptographic standards imposed by another country
- Of course the system must remain totally public
- NB: a backdoor may be a « natural » weakness which has been identified but never disclosed!

Cryptographic Scheme Transformation

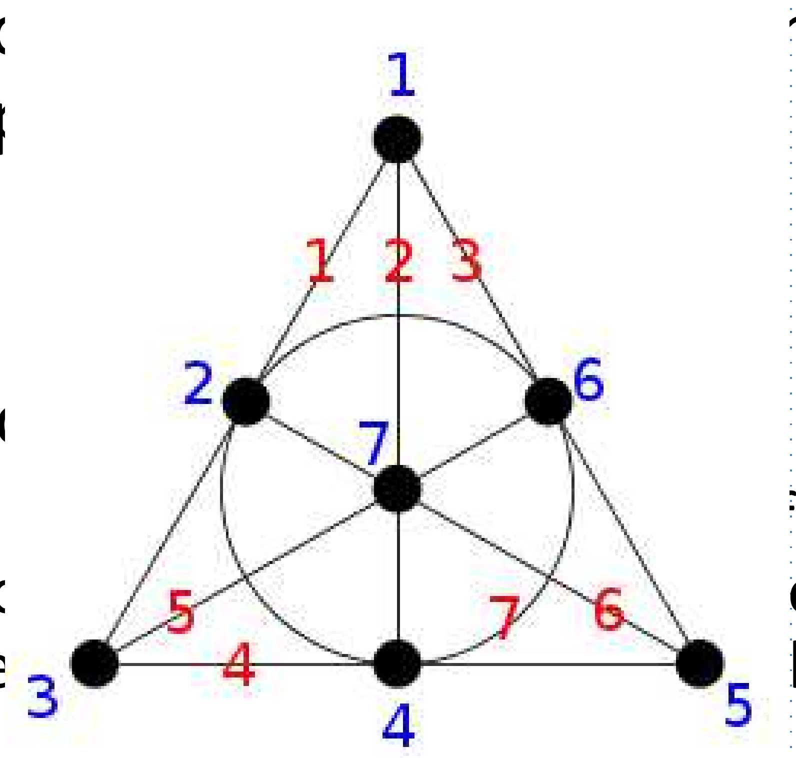
- We start from a (secret) algebra in which we design an algorithm E_T embedding a mathematical backdoor mathématique
- Design a one-way transformation S from A to the Boolean algebra $\mathcal{L}(\mathbb{B}^n,\mathbb{B})$
  - Computing $E = S(E_T)$ (scheme transformation) is computationally easy
  - Retrieving E_T from E is computationally untractable unless knowing some secret transformation S’ such that $S' \circ S \approx$ identity with probability $p \neq 0.5$.
  - E exhibit all desirable, strong cryptographic properties
  - The backdoor can be exploited only in A
- Other approaches are possible

Combinatorial Approach

- Use of combinatorial designs having strong invariance properties
  - Example : 2-(7, 3, 1) symmetric design
- Ph D thesis started in 2013
- Results (about to be submitted)
  - Formal description of S-Box families having combinatorial backdoor while being perfectly resistant to differential and linear cryptanalysis (and their variants)
  - Submission of backdoored SPN by mid-July

Combinatorial Approach

- Use of co aving strong invariance p
  - Example :
- Ph D thesis
- Results (ab
  - Formal amilies having combinat erfectly resistant to differe lysis (and their variants)
  - Submission of backdoored SPN by mid-July



Further Reading

- V. Rijmen & B. Preneel, A Familiy of Trapdoor Systems, http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.54.9031
- K. G. Paterson http://www.hpl.hp.com/techreports/1999/HPL-1999-12R1.pdf
- Harpes & Massey (1997), Partitionning cryptanalysis, FSE 1997
- Colbourn & Dinitz, Handbook of Combinatorial Design, CRC Press.

Agenda

- Introduction
- Definitions, concepts and limitations
- Scientific and technical evolutions
  - Homomorphic encryption, authenticated encryption schemes, COMSEC vs TRANSEC, mathematical poly/metamorphism for encryption, mathematical backdoors, the quantum era…
- Legal and societal evolutions
- Conclusion

Quantum Cryptography

- Relies on quantum physics properties to protect information
- Until recently, it was in fact just quantum distribution of keys
  - Transmission of a one-time pad sequence (Vernam)
  - BB84 protocol (polarized photons)
  - Ekert91 protocol (entangled photons)
  - Jouguet et al. protocol (CNRS 2012)

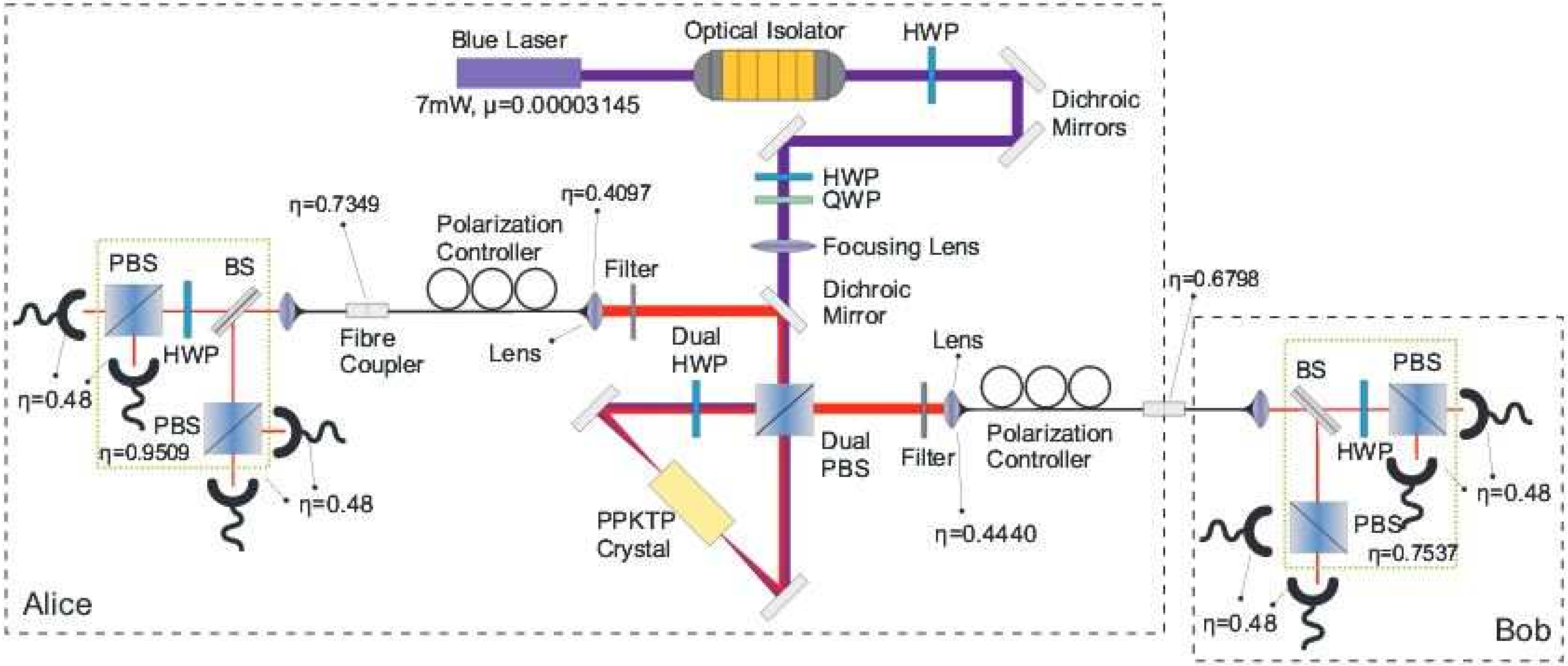
Quantum Key Distribution

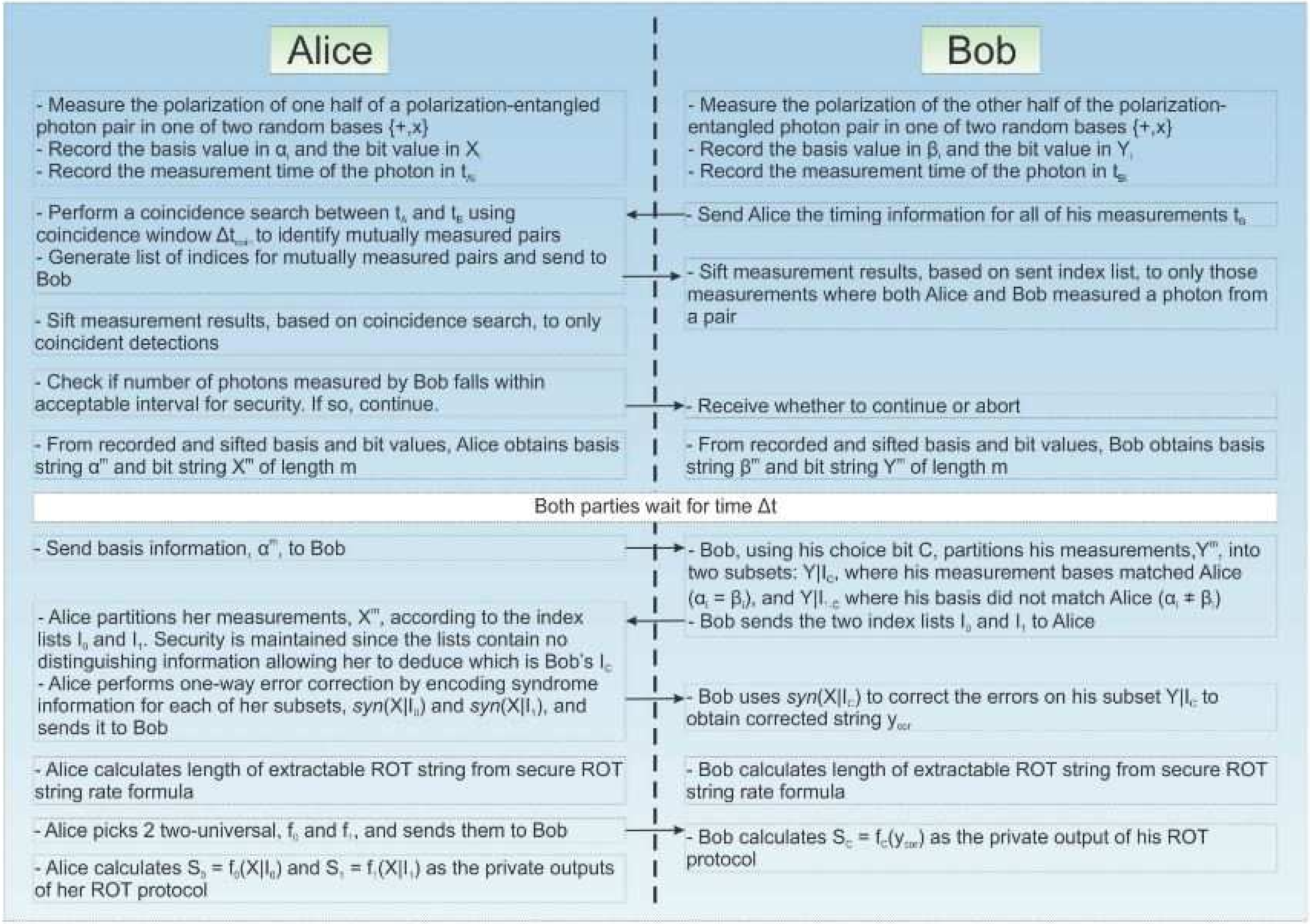
- Record obtained by CNRS Jouguet et al.
  - Over 80 km and a transmission rate of a few hundreds of bits/s
- Very slow techniques
- Still technical problems
  - Dark current, efficient photon counting
  - Implementation security is still an open problem (J. Skaar, 2010 ; Jain et al, 2015)

Quantum Encryption

- Realised for the first time by Erven et al. in 2014 (Nature, March 2014)
- « Encryption » of 1336 bits in 3 sec.
- Complex technique based on entangled photons and oblivious transfert protocols.

Quantum Encryption





Alice

- Measure the polarization of one half of a polarization-entangled photon pair in one of two random bases {+,x}
- Record the basis value in α_i and the bit value in X_i
- Record the measurement time of the photon in t_A

- Perform a coincidence search between t_A and t_B using coincidence window Δt_{cw} to identify mutually measured pairs
- Generate list of indices for mutually measured pairs and send to Bob

- Sift measurement results, based on coincidence search, to only coincident detections

- Check if number of photons measured by Bob falls within acceptable interval for security. If so, continue.

- From recorded and sifted basis and bit values, Alice obtains basis string α^m and bit string X^m of length m

Bob

- Measure the polarization of the other half of the polarization-entangled photon pair in one of two random bases {+,x}
- Record the basis value in β_i and the bit value in Y_i
- Record the measurement time of the photon in t_B

- Send Alice the timing information for all of his measurements t_B

- Sift measurement results, based on sent index list, to only those measurements where both Alice and Bob measured a photon from a pair

- Receive whether to continue or abort

- From recorded and sifted basis and bit values, Bob obtains basis string β^m and bit string Y^m of length m

Both parties wait for time Δt

Alice

- Send basis information, α^m, to Bob

- Alice partitions her measurements, X^m, according to the index lists I_0 and I_1. Security is maintained since the lists contain no distinguishing information allowing her to deduce which is Bob's I_c
- Alice performs one-way error correction by encoding syndrome information for each of her subsets, *syn*($X|I_0$) and *syn*($X|I_1$), and sends it to Bob

- Alice calculates length of extractable ROT string from secure ROT string rate formula

- Alice picks 2 two-universal, f_0 and f_1, and sends them to Bob

- Alice calculates $S_0 = f_0(X|I_0)$ and $S_1 = f_1(X|I_1)$ as the private outputs of her ROT protocol

Bob

- Bob, using his choice bit C, partitions his measurements, Y^m, into two subsets: $Y|I_c$, where his measurement bases matched Alice ($\alpha_i = \beta_i$), and $Y|I_{1-c}$ where his basis did not match Alice ($\alpha_i \neq \beta_i$)
- Bob sends the two index lists I_0 and I_1 to Alice

- Bob uses *syn*($X|I_c$) to correct the errors on his subset $Y|I_c$ to obtain corrected string y_{cor}

- Bob calculates length of extractable ROT string from secure ROT string rate formula

- Bob calculates $S_c = f_c(y_{cor})$ as the private output of his ROT protocol

FIG. 1. Flow chart of the 1-2 ROT protocol.

- Measure the polarizatio
photon pair in one of two
- Record the basis value
- Record the measureme

- Perform a coincidence s
coincidence window Δt_{c}
- Generate list of indices
Bob

- Sift measurement result
coincident detections

- Check if number of phot
acceptable interval for se

- From recorded and sifte
string α'' and bit string X'''

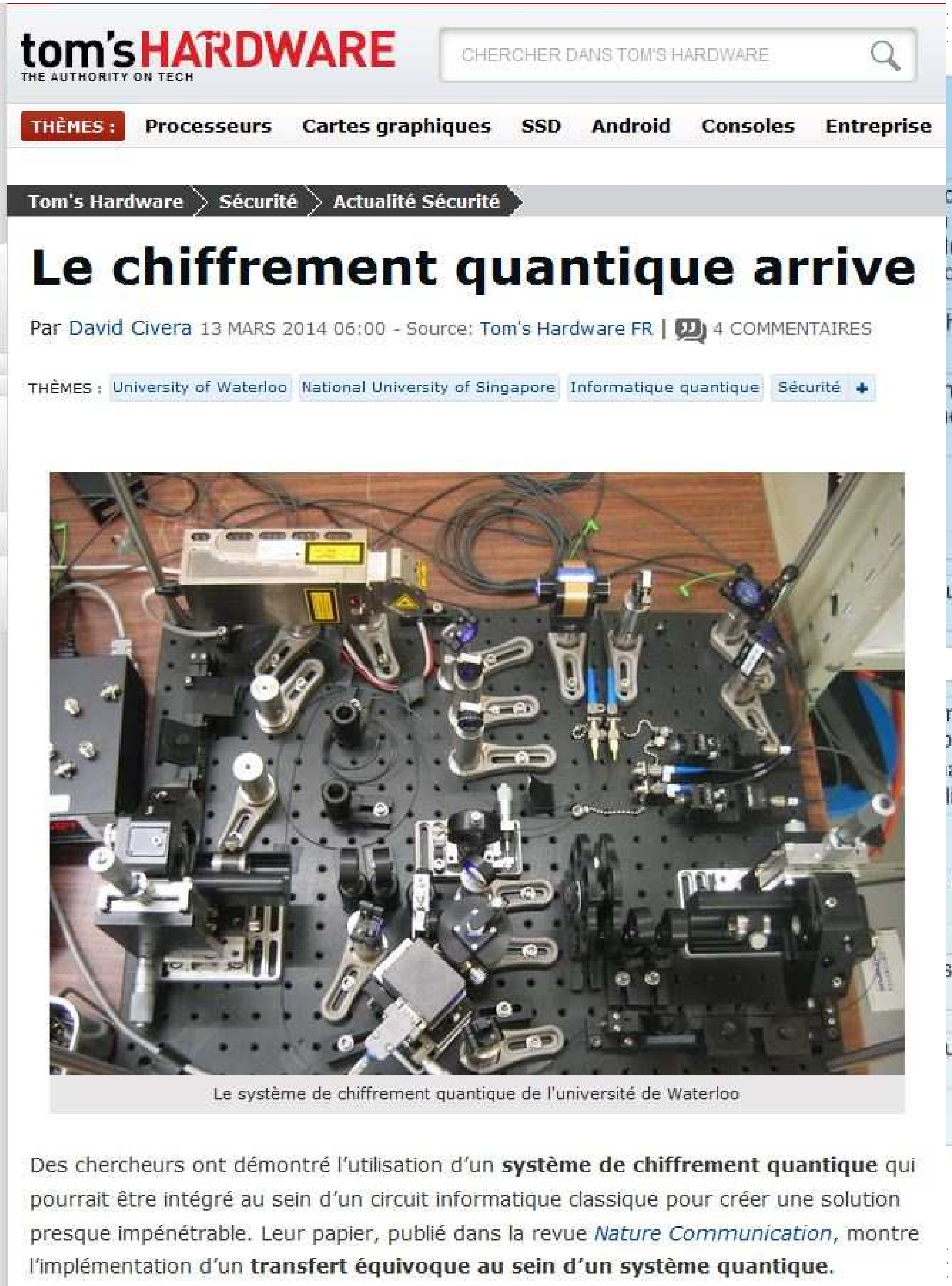
- Send basis information,

- Alice partitions her mea
lists I_0 and I_1. Security is r
distinguishing informatior
- Alice performs one-way
information for each of he
sends it to Bob

- Alice calculates length c
string rate formula

- Alice picks 2 two-univers

- Alice calculates $S_0 = f_0(X$
of her ROT protocol



tom's HARDWARE
THE AUTHORITY ON TECH
CHERCHER DANS TOM'S HARDWARE
THÈMES : Processeurs Cartes graphiques SSD Android Consoles Entreprise
Tom's Hardware › Sécurité › Actualité Sécurité

Le chiffrement quantique arrive

Par David Civera 13 MARS 2014 06:00 - Source: Tom's Hardware FR | 4 COMMENTAIRES

THÈMES : University of Waterloo National University of Singapore Informatique quantique Sécurité +

Le système de chiffrement quantique de l'université de Waterloo

Des chercheurs ont démontré l'utilisation d'un **système de chiffrement quantique** qui pourrait être intégré au sein d'un circuit informatique classique pour créer une solution presque impénétrable. Leur papier, publié dans la revue *Nature Communication*, montre l'implémentation d'un **transfert équivoque au sein d'un système quantique.**

of the polarization-
bases {+,x}
lue in Y_i
on in t_B

his measurements t_B

ndex list, to only those
easured a photon from

ues, Bob obtains basis

neasurements,Y''', into
bases matched Alice
atch Alice ($\alpha_i \neq \beta_i$)
lice

his subset $Y|I_C$ to

string from secure ROT

utput of his ROT

Quantic Era – Further Reading & Pointers

- Jouguet et al. http://arxiv.org/abs/1210.6216
- Quantic Key distribution hacking techniques http://www.vad1.com/lab/publications.html
- Erven et al., 2014 http://xxx.tau.ac.il/abs/1308.5098v1
- R. ERRA *Cryptographie Quantique & Cryptographie Post-Quantique – Mythes, Réalités & Futur*, NDH 2012 https://nuitduhack.com/slides/ndh2k12/Robert%20La%20Nuit%20Du%20Hack%202012.pdf

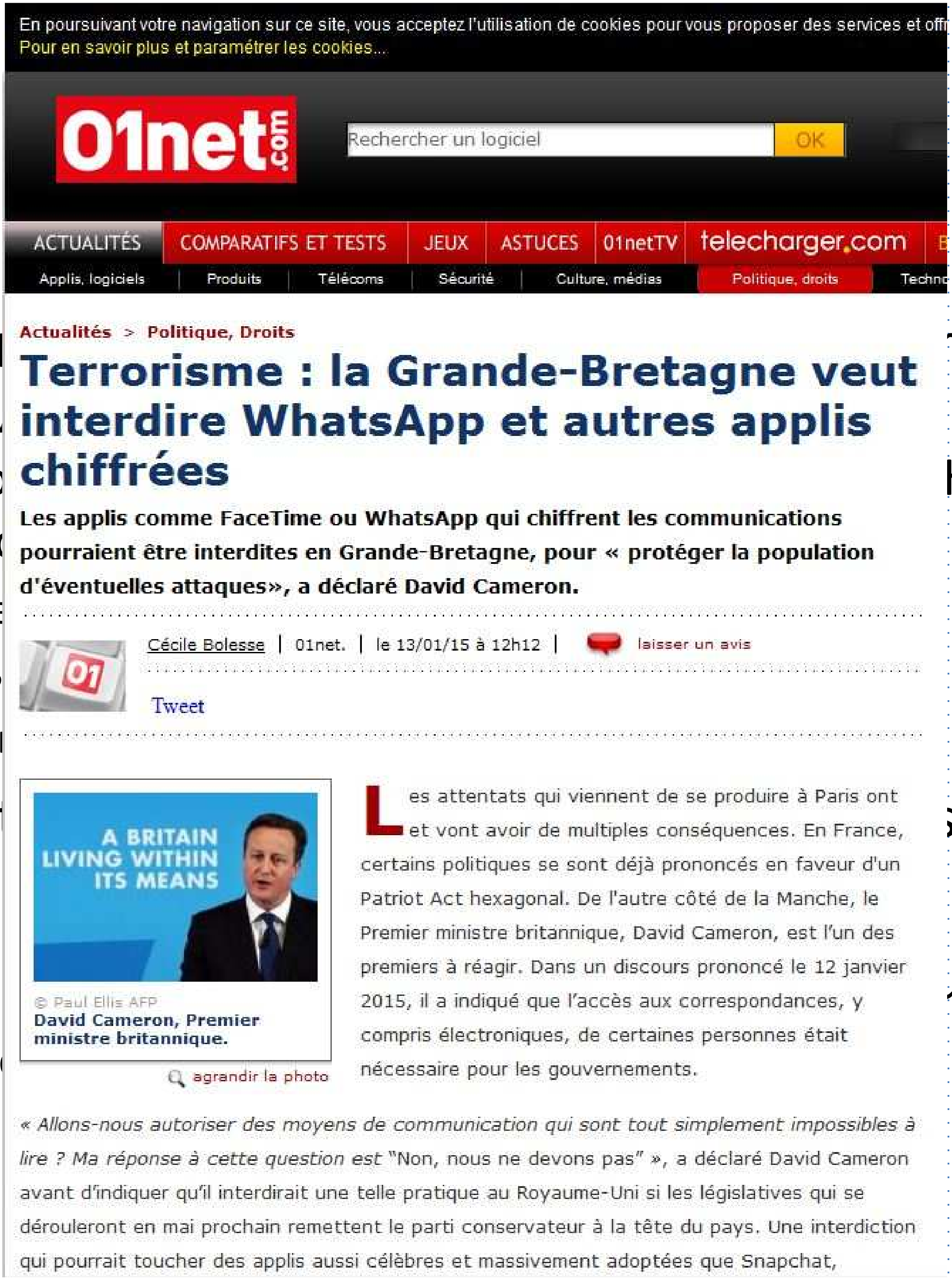
Agenda

- Introduction
- Definitions, concepts and limitations
- Scientific and technical evolutions
  - Homomorphic encryption, authenticated encryption schemes, COMSEC vs TRANSEC, mathematical poly/metamorphism for encryption, mathematical backdoors, the quantic era…
- Legal and societal evolutions
- Conclusion

The Context

- Use of Encryption becomes totally free in 2004 (after Patriot Act!)
- Since a few weeks, political posturing and alarming signs around of a possible coming back for encryption control or the prohibition of certain applications
  - Unexplained disappearance of TrueCrypt
  - Note ANSSI No DAT-NT-19/ANSSI/SDE/NP du 01/10/2014
  - D. Cameron speech (January 2015)
- Accepting the principle will inevitably lead to discuss the modalities
- Let us first apply existing regulations and procedures
  - Let us strengthen the role of judges before all

- Use of Encry iot Act!)
- Since a few around of a possible co hibition of certain applic
  - Unexplaine
  - Note ANSS
  - D. Cameron
- Accepting scuss the modalities
- Let us first ures
  - Let us str



Actualités > Politique, Droits

Terrorisme : la Grande-Bretagne veut interdire WhatsApp et autres applis chiffrées

Les applis comme FaceTime ou WhatsApp qui chiffrent les communications pourraient être interdites en Grande-Bretagne, pour « protéger la population d'éventuelles attaques», a déclaré David Cameron.

Cécile Bolesse | 01net. | le 13/01/15 à 12h12 | laisser un avis

Tweet

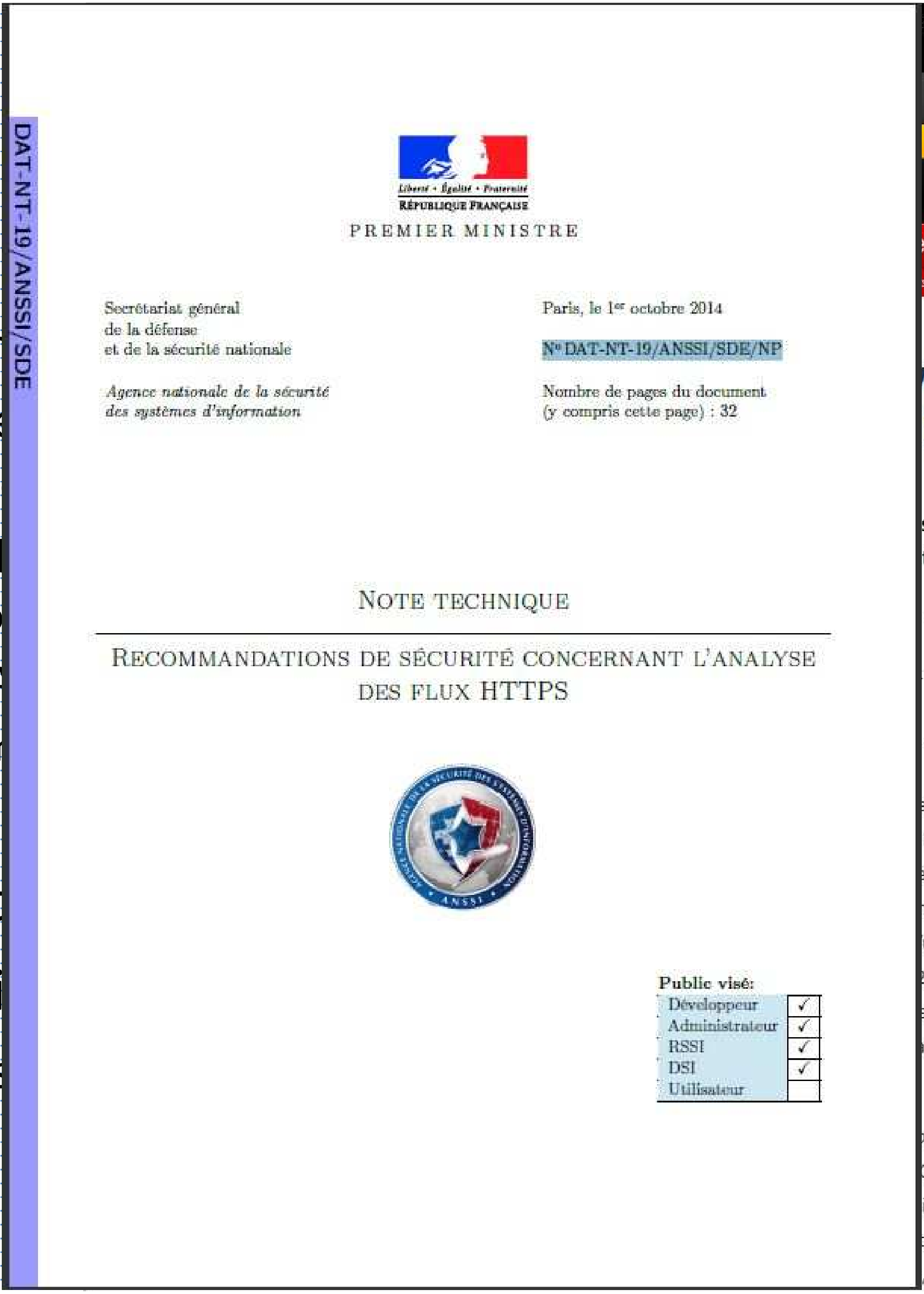
© Paul Ellis AFP
David Cameron, Premier ministre britannique.

agrandir la photo

Les attentats qui viennent de se produire à Paris ont et vont avoir de multiples conséquences. En France, certains politiques se sont déjà prononcés en faveur d'un Patriot Act hexagonal. De l'autre côté de la Manche, le Premier ministre britannique, David Cameron, est l'un des premiers à réagir. Dans un discours prononcé le 12 janvier 2015, il a indiqué que l'accès aux correspondances, y compris électroniques, de certaines personnes était nécessaire pour les gouvernements.

« Allons-nous autoriser des moyens de communication qui sont tout simplement impossibles à lire ? Ma réponse à cette question est "Non, nous ne devons pas" », a déclaré David Cameron avant d'indiquer qu'il interdirait une telle pratique au Royaume-Uni si les législatives qui se dérouleront en mai prochain remettent le parti conservateur à la tête du pays. Une interdiction qui pourrait toucher des applis aussi célèbres et massivement adoptées que Snapchat,

- Use of Er iot Act!)
- Since a fe around of a possibl hibition of certain a
  - Unexp
  - Note A
  - D. Can
- Accepti scuss the modalit
- Let us fi ures
  - Let us



DAT-NT-19/ANSSI/SDE

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE

Secrétariat général
de la défense
et de la sécurité nationale

*Agence nationale de la sécurité
des systèmes d'information*

Paris, le 1er octobre 2014

N° DAT-NT-19/ANSSI/SDE/NP

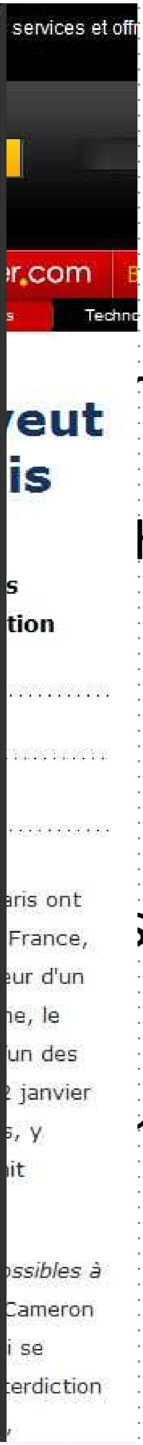
Nombre de pages du document
(y compris cette page) : 32

NOTE TECHNIQUE

RECOMMANDATIONS DE SÉCURITÉ CONCERNANT L'ANALYSE DES FLUX HTTPS

Public visé:

Développeur	✓
Administrateur	✓
RSSI	✓
DSI	✓
Utilisateur	



services et offr

r.com

Techno

eut
is

s
tion

aris ont
France,
eur d'un
ne, le
un des
janvier
s, y
it

ssibles à
Cameron
i se
erdiction

What Are the Risks

- A study of the AFUU (French Association of Users of Unix and Open Systems) conducted in 1998 indicated that 86% of the first 1,500 French companies "*claimed to have suffered due to the lack of use of encryption means*“
- Encryption is the only guarantee for the protection of privacy and our life
  - Our existence as human being is directly determined by our private life and our free will
  - What impact on European citizens would have a come back of control over free encryption?
- What is the real part of the use of encryption by criminals and offenders?

Agenda

- Introduction
- Définitions, concepts et limitations
- Evolutions scientifiques et techniques
  - Chiffrement homomorphe, schémas de chiffrement authentifié, COMSEC vs TRANSEC, algorithmes poly/métamorphes, trappes mathématiques, l'ère quantique…
- Evolutions légales et sociétales
- Conclusion

Conclusion

- Many possible evolutions giving a huge field of industrial opportunities and scientific developments as well as in terms of use
- Implementation and environments (OS) have an extreme impact over the real security
- What about the willingness of states to control it all again strongly?
- Cryptographic freedom is fundamental
- The XXIst century will be spi~~rit~~ual or will not be.

cryptographic

“Those who would give up essential Liberty, to purchase a little temporary Safety, deserve neither Liberty nor Safety.”

Benjamin Franklin (November 11th, 1755)

Thanks for listening

QUESTIONS & ANSWERS