THE CONTROL OF TECHNOLOGY BY NATION STATE: PAST, PRESENT AND FUTURE II

The (unofficial) case of Cryptology and Information Security

Eric FILIOL – ESIEA (C + V)O Lab – filiol@esiea.fr

http://sites.google.com/site/ericfiliol/

конференция
РусКрипто

INTRODUCTION

- Question:

Just imagine that if unconditionally secure systems (computer, information security…) would be possible (theoretically AND practically), would it be desirable to export them?

- The answer is no due to
  - National Security Issues (Intelligence, Defense, Police, Justice…)
  - Strategic dominance, information assurance…
  - Economic warfare & dominance (since 1989)

INTRODUCTION

- Before WWII
  - No export control. No control over technology.
- After WWII
  - Strong export control (Cold war, rise of terrorism…)
- These controls have always been in place since WWII
- Since 9/11, export controls are strengthened
- In this context, what to think of issues like DES, AES, so-called « crypto freedom », trapdoors, CoCom, Wassenar agreement, Echelon, bitlocker, Carnivore, DCS10000, NarusInsight, Prism…?
- An unsustainable control over Nation States by a handful of States and multinational companies has taken over from the necessary control and protection of each State at the national level (the country, citizens…) by their own!
  - Problem of sovereignty (classical and technological).
  - Security of national companies and interests.

PREREQUISITE

- Without loss of generality, the case of cryptography will be taken as the recurrent theme.
  - The oldest case historically.
  - The most critical case: who controls cryptography controls everything.
- As for all IT/Security technologies, the control over cryptography goes through its implementation and the way it is brought into play:
  - Hardware.
  - Software (for example playing with computer cache).
  - Regulations and standards (e.g. ISO/IEC)
  - Commercial power and dominance.

WHAT IS OPERATIONAL CRYPTANALYSIS?

- From an intelligence/operational point of view, **really** breaking an encryption system means
  - Accessing the plaintext in a time shorter than the life of the information (regarding its operational value)
  - Practically speaking: a matter of hours (recall supercomputing time is horribly expensive)
  - With a reduced amount of encrypted data (a few Kb to a few Mb)
  - Must be played a large number of times (a clever enemy changes the key very often)
- These operational constraints mean that academic attacks have just…. an academic interest!
- Mathematical research time versus exploitation time

AIM OF THE TALK

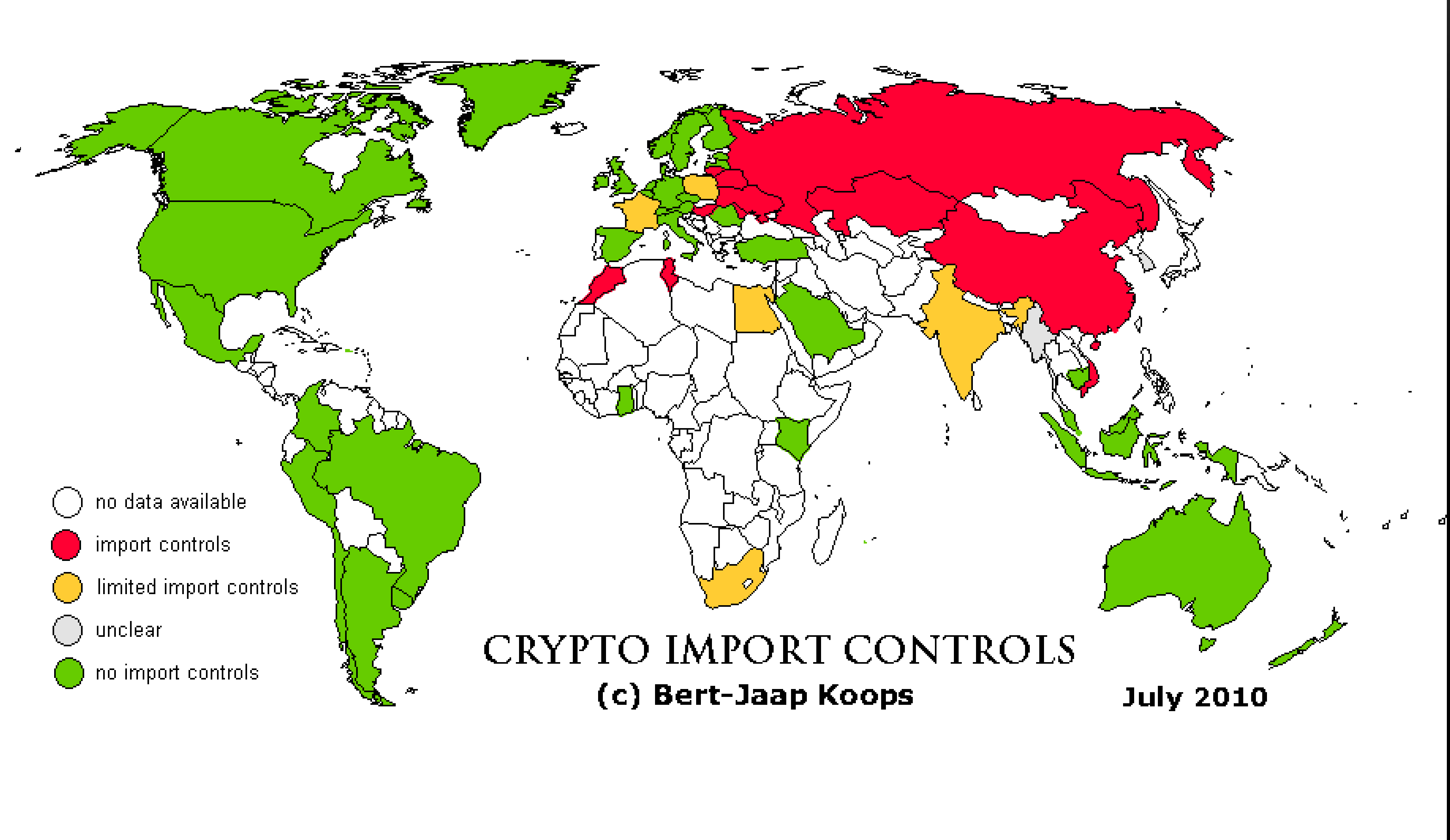
- To present one of the unofficial versions of technology history
  - Part II (refer to my paper Journal of Information Warfare 2013 for part I).
- To provide a different reading of cryptology history based on my operational experience
- To explain a few of the issues of « modern cryptology »
- Illustrate the issue with the ГОСТ encryption algorithm.

HISTORY & LEGAL

FIVE PHASES OF CONTROL

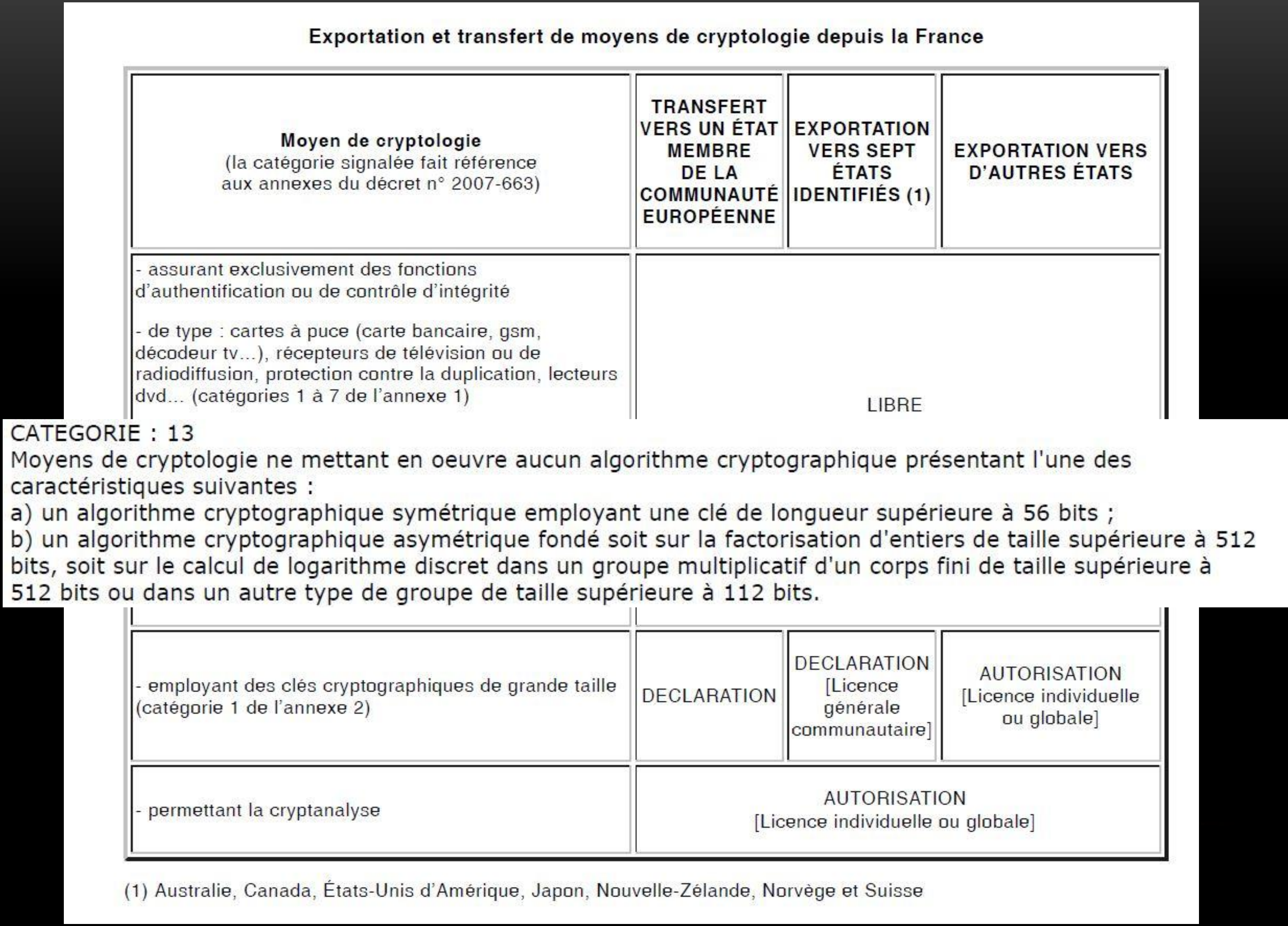
- Prehistory: from 1945 to 1975 (CoCom)
- The Mutation phase: from 1975 to 2001 (Wassenaar, controlling academics…)
- The Globalization Phase: from 2001 to 2012 (Patriot Act, WTO, ISO…)
- The legal Phase: from 2010 to now (patents, licenses, standards, PRISM, PIPA, ACTA…)
- The cultural assimilation phase: now and next. Target the youth with consumerism (TV, marketing, US products…). Make sure that the next generation will think/love US.
- For more details see my talk at HIP 2013, Paris or my paper (Journal in Information Warfare, 2013).

CRYPTOLOGY CONTROL



THE WASSENAAR AGREEMENT

- http://www.wassenaar.org/
- 42 members
- Cryptology is listed in part 5b
- First level of control:
  - « Good/fair » countries vs other countries (the rest of the world)
- If you analyze the regulations, exporting encryption algorithms with key size greater than 56 bits is subject to export control!
- The world diffusion of the AES (key size ≥ 128 bits) is hence a clear violation of the Wassenaar agreement…unless some sort of control has been organized/enforced.



Exportation et transfert de moyens de cryptologie depuis la France

Moyen de cryptologie (la catégorie signalée fait référence aux annexes du décret n° 2007-663)	**TRANSFERT VERS UN ÉTAT MEMBRE DE LA COMMUNAUTÉ EUROPÉENNE**	**EXPORTATION VERS SEPT ÉTATS IDENTIFIÉS (1)**	**EXPORTATION VERS D'AUTRES ÉTATS**
- assurant exclusivement des fonctions d'authentification ou de contrôle d'intégrité - de type : cartes à puce (carte bancaire, gsm, décodeur tv...), récepteurs de télévision ou de radiodiffusion, protection contre la duplication, lecteurs dvd... (catégories 1 à 7 de l'annexe 1)	LIBRE		
- employant des clés cryptographiques de grande taille (catégorie 1 de l'annexe 2)	DECLARATION	DECLARATION [Licence générale communautaire]	AUTORISATION [Licence individuelle ou globale]
- permettant la cryptanalyse	AUTORISATION [Licence individuelle ou globale]		

(1) Australie, Canada, États-Unis d'Amérique, Japon, Nouvelle-Zélande, Norvège et Suisse

CATEGORIE : 13

Moyens de cryptologie ne mettant en oeuvre aucun algorithme cryptographique présentant l'une des caractéristiques suivantes :

a) un algorithme cryptographique symétrique employant une clé de longueur supérieure à 56 bits ;

b) un algorithme cryptographique asymétrique fondé soit sur la factorisation d'entiers de taille supérieure à 512 bits, soit sur le calcul de logarithme discret dans un groupe multiplicatif d'un corps fini de taille supérieure à 512 bits ou dans un autre type de groupe de taille supérieure à 112 bits.

SECOND LEVEL OF CONTROL

- USA vs the rest of the world
- « *The power of a country lies in its ability to impose standards* »

Bernard Carayon (French MP)

- US Cryptographic standards everywhere despite the wind of cryptographic freedom in Europe!
- During the AES contest, block cipher technology was the only standard authorized.
- The issue for the USA is hence to control norms and standards (e.g ISO)

THIRD LEVEL OF CONTROL

- Use the academic world as a scientific backing
- Academic world has been used as smoke screen and scientific hostage
  - Complexity/combinatorial issues make any real, operational advances in cryptanalysis impossible
  - What is academically broken is far from being broken operationnally
  - Scientific orthodoxy promoted
- Cryptographic algorithms are chosen by the pair {State, Industry} in reality
- About 20 % of cryptology research results only are published (famous example, differential cryptanalysis)

IS THE ACADEMIC COMMUNITY INDEPENDENT?

- Unfortunately, the academic community is under some sort of control as well (part of the game)
- Program committees control
  - Fashion topics « suggested » by higher levels (e.g. Block ciphers, then Hash functions)
  - Clever exploitation of the « publish or perish » effect
- Control by money
  - Research funds (NSF, NSA, FP7…)
  - Academic positions

CRYPTOGRAPHY INDUSTRY AFTER WWII

- Producing countries of crypto:
  - UK (Racal), D (Siemens), S (Ericsson), CH (Gretag, Crypto AG), FR (Sagem, Thales, Matra), SF (Nokia), Hungary…
  - Guess which is missing?
- In Switzerland, Crypto AG/Gretag hold more than 90 % of the world market (since 1945)
  - Almost all countries/organizations (120 in 1995) were buying cryptomachines for {gvt, mil, diplomatic, economic} needs except a very few.
- 1995 The Hans Buehler case changed the cryptologic face of the world.

The Hans Buehler Case

- Crypto AG's top marketing representative arrested in Teheran in 1992.
- Leaks in the Press (Berlin Club bombing, Chapur Bakhtiar assassination in Paris) by Gov. officials that gave hints to Iranian government that cryptography was probably trapdoored.
- 9 months in Iranian jails
- Reveals the scandal: NSA, BND and others have infiltrated Crypto AG. Gretag and others to put trapdoors in export versions of crypto machines systematically
- The USA were able to read openly most of the world encrypted traffic during nearly 50 years
- Consequences: confidence in cryptography industry is severely weakened
- Need for more « transparency »
  - Next step prepared from the end of the 60s
  - The academic community will be used to play the role of moral/scientific caution
- **Interesting point**: from the early 90s a significant number of trapdoored algorithms were block ciphers!

An illustrative case analyzed in the light of my past experience

THE ГОСТ CIPHER CASE

BLOCK CIPHER HISTORY

- Mid 60s the concept of Feistel network is born (IBM & NSA)
- 1971 – Lucifer at IBM
- 1973 – Official birth of block ciphers (Feistel’s paper in Scientific American)
- 1976 – Data Encryption Standard
- End of 60s (declassified 1994) – Russian ГОСТ
- 1998 - 2001 – AES Contest under the control/supervision of NIST/NSA
- 2001 – AES has become the unchallenged world standard for encryption.
- Unless being naïve and according to Wassenaar agreement, this algorithm is bound to be “under control” by the USA.
- This control is possible only if no other algorithm is challenging it.
- Here comes the ГОСТ case!

ГОСТ'S OPERATIONAL SECURITY

- Practically and operationally unchallenged since 1994.
- Up to now, no academic attack really questions ГОСТ's operational security.

Method	# of plaintexts	Time complexity
Differential cryptanalysis on related keys	2^{35}	2^{224}
Slide attack with weak keys	2^{64}	2^{64}
Reflection- MitM attack	2^{32}	2^{225}
Algebraic attack	2^{64}	2^{178} (memory 2^{70})

(Babenko, Ishchukova & Maro, 2013)

- From an operational point of view ГОСТ cipher
  - remains the most secure public block cipher
  - has better algebraic complexity than the AES.

THE ГОСТ ISSUE (2)

- Only a very few Western products dare using ГОСТ preferably to AES
  - Most of the time they switch to AES under different sorts of pressure.
- Strong feeling that AES hegemony might be a problem. **There is a strong need for a AES alternative.**
- The ISO affair
  - ГОСТ has been submitted to ISO/IEC 18033 standardization in 2010 to become a worldwide encryption standard (thus a challenger to AES)
  - Isobe's paper (2011) did not succeed in creating doubts about ГОСТ security. Decision has been made to make ISO/IEC criteria more explicit.
  - Following Courtois' paper (2012), January 27th 2012, the addendum on ГОСТ 28147-89 was deleted from ISO/IEC 18033-3.
  - This clever succession of events perfectly illustrates how things are manages to control technology

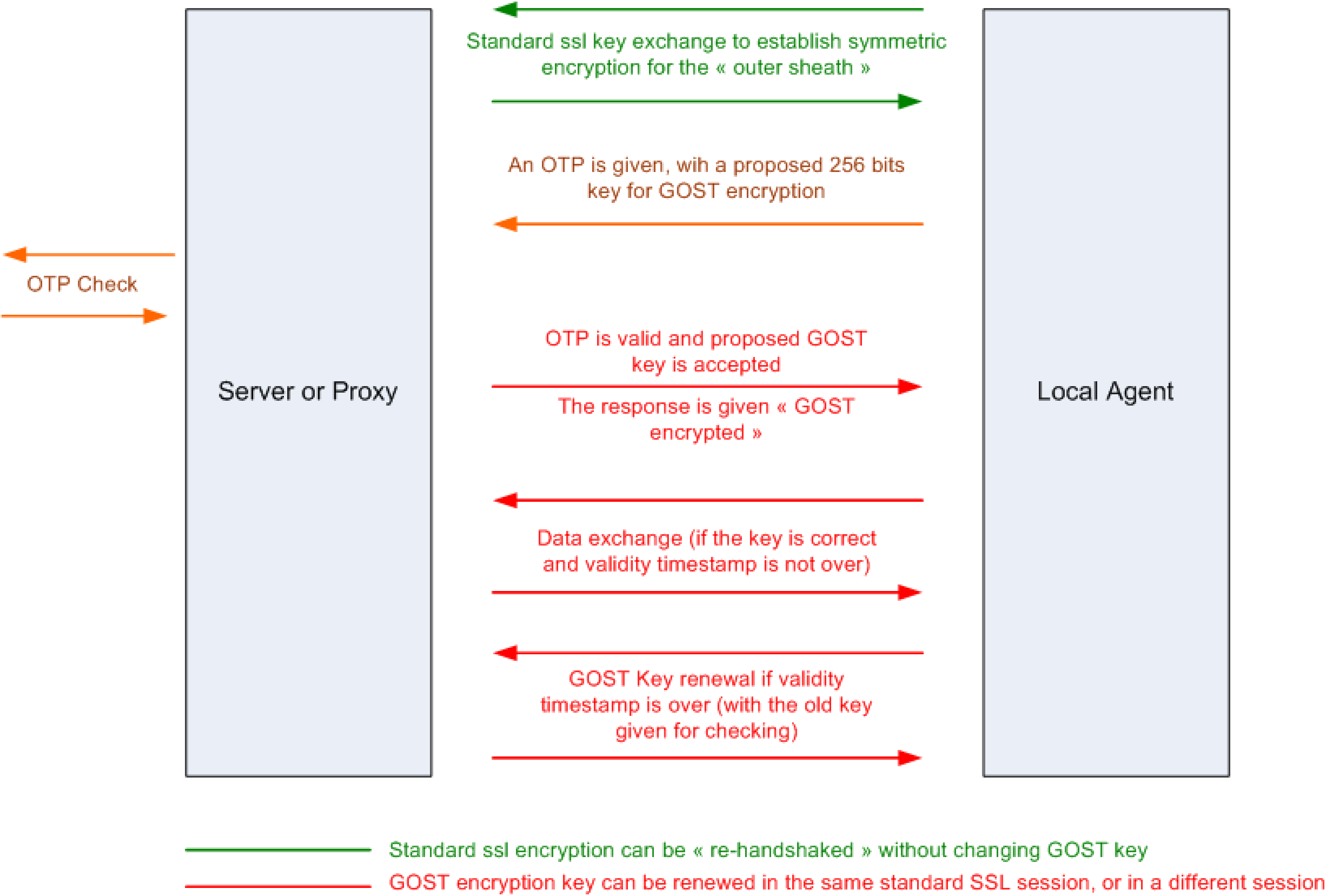
DOUBLE STANDARDS POLICY

"We have one criticism of AES: we don't quite trust the security… What concerns us the most about AES is its simple algebraic structure… No other block cipher we know of has such a simple algebraic representation. We have no idea whether this leads to an attack or not, but not knowing is reason enough to be skeptical about the use of AES."

(B. Schneier & N. Fergusson, *Practical Cryptography*, 2003, pp56–57)

- When considering (academic) recent attacks on AES, it is obvious that ГОСТ is far from being weaker than AES.
- AES is however still a (unchallenged) ISO/IEC 18033 standard.
- For operational and practical security ГОСТ offers a very high security level and brings more confidence than the AES
  - AES has been selected and validated by NIST/NSA for the world.
  - ГОСТ has been created for former USSR's own security.

PROJECTS USING ГОСТ (1)



Server or Proxy

Local Agent

OTP Check

Standard ssl key exchange to establish symmetric encryption for the « outer sheath »

An OTP is given, wih a proposed 256 bits key for GOST encryption

OTP is valid and proposed GOST key is accepted

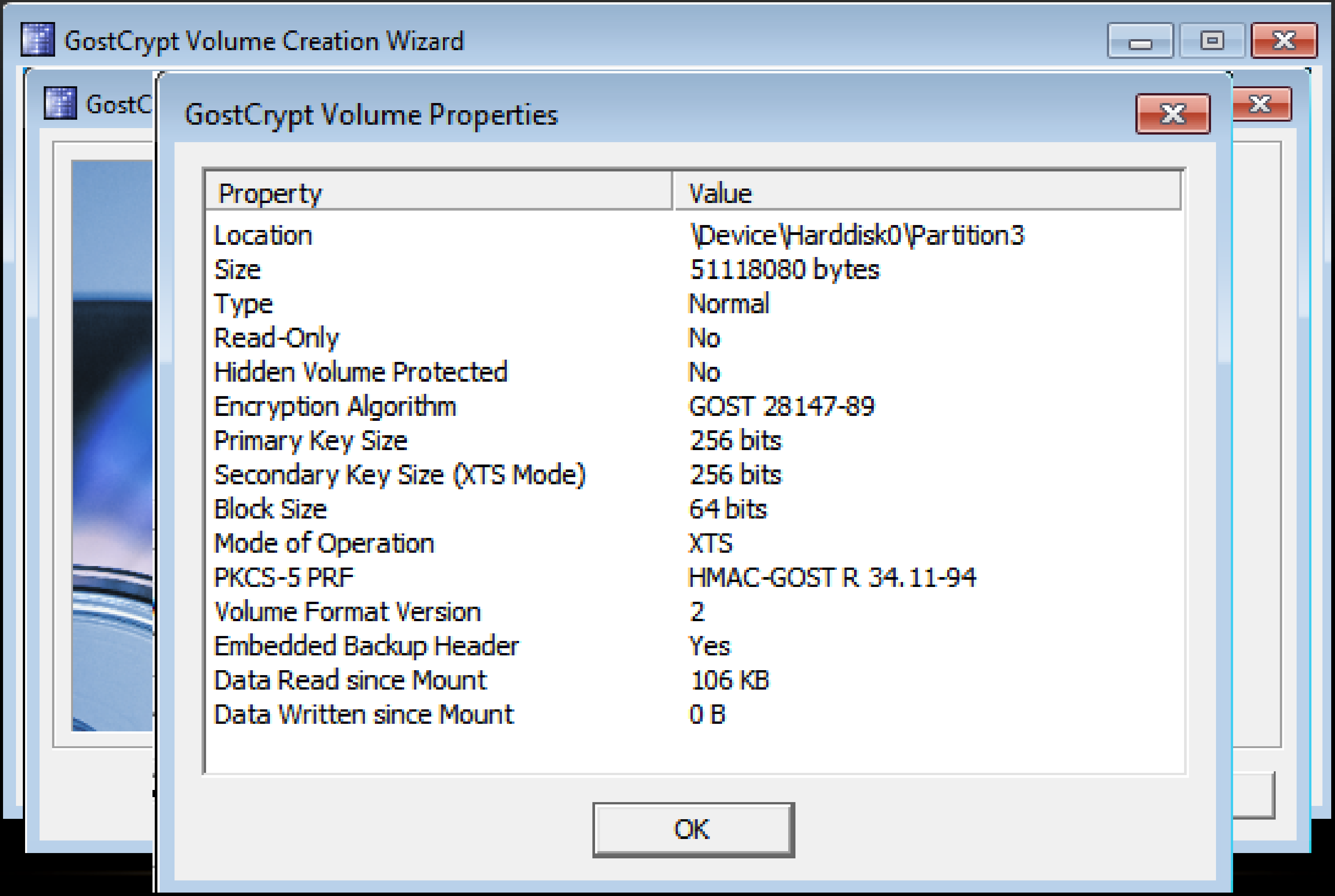
The response is given « GOST encrypted »

Data exchange (if the key is correct and validity timestamp is not over)

GOST Key renewal if validity timestamp is over (with the old key given for checking)

Standard ssl encryption can be « re-handshaked » without changing GOST key

GOST encryption key can be renewed in the same standard SSL session, or in a different session



GostCrypt Volume Properties

Property	Value
Location	\Device\Harddisk0\Partition3
Size	51118080 bytes
Type	Normal
Read-Only	No
Hidden Volume Protected	No
Encryption Algorithm	GOST 28147-89
Primary Key Size	256 bits
Secondary Key Size (XTS Mode)	256 bits
Block Size	64 bits
Mode of Operation	XTS
PKCS-5 PRF	HMAC-GOST R 34.11-94
Volume Format Version	2
Embedded Backup Header	Yes
Data Read since Mount	106 KB
Data Written since Mount	0 B

A Few Hints

HOW TO HIDE TRAPDOOR

THE BACKDOOR ISSUE

- Hiding trapdoor is possible as long as the attacker (the designer of the trapdoor) has a technological/scientific/legal advantage
- Different level of backdoors (see my talk at HIP 2013)
  - If you can access the computer physically, forensics techniques will exploit implementation backdoors (controlling hidden features of the OS and of the cache management for example)
  - Hardware backdoors may leak information outside.
  - Mathematical backdoors (the worst case): to manage offline encryption (e.g. satellite communications).
- Do not neglect the importance of standards/norms (stream ciphers versus block cipher encryption)

DESIGN TRANSFORMATION

- Consider a (secret) “starting” algebra A in which you design your algorithm with trapdoor E_T
- Use a one-way transformation S from A to the Boolean algebra L(B^n,B)
  - Computing E = S(E_T) is computationally easy.
  - Computing E_T from E is computationally intractable unless you know some secret S’ such that S’○ S = Identity.
  - E exhibits all desirable cryptographic properties
  - The trapdoor can be detected/used only in A
- Many other approaches possible.
- DeBlock Project about to be launched in 2014 (funding pending) in my lab!
  - Combinatorial trapdoor framework for block ciphers.

CONCLUSION

CONCLUSION

- IT/Security technologies (design, products…) **should remain a strategic, national issue!**
  - Do not lose your national scientific capability
  - Keep away from scientific orthodoxy and « scientific standards »
  - Every country must have a strong, independent academic community working with the State and the Industry (national issue and strategy)
  - In this respect, Russian Federation approach should be a model for European countries.
- International/academic standards are neither a fatality nor a doom!
- Remain pessimistic about the world scientific community independence and ability. Academic most of the time are just writing papers!

Thanks you for listening - Спасибо за внимание

QUESTIONS & ANSWERS - ВОПРОСЫ И ОТВЕТЫ