Ежегодная международная научно-практическая конференция
«РусКрипто'2019»

Thoughts about the Future and Trends of Cryptology

Eric FILIOL,
ESIEA, Operational Cryptology and Virology Lab

esiea
ECOLE D'INGENIEURS
DU MONDE NUMERIQUE

Thanks

- I would like wholeheartedly to thank Professor Alex Zhukov, Yuri Malinin and all Ruskrypto organizers for the very great honor to speak at RuskKrypto.
- Beyond my great attachment to Russia and to the Russian culture, I am convinced that your country is a major country in the general field of science and more particularly in the field of cryptology:
  - on the mathematical level,
  - but also on the operational and strategic level (GOST Standards for instances)
- It is an excellent news to see GOST Standards entering the TLS Cipher Suite.

Introduction

- It is with a certain humility that I wish to share a few thoughts on possible evolutions in cryptology to be desired or anticipated
- It is nothing more than my own vision
- ``*Les prévisions sont difficiles surtout quand elles concernent l'avenir*'' (Прогнозировать сложно, особенно когда речь идет о будущем.) (Jacques Chirac)
- Based on my experience and thoughts hence may be prone to subjectivity.

Trend 1.- Backdoors Conception and Detection

- Backdoors are and will be more than ever a critical issue
  - Bannier \& Filiol (2017): first real-life block cipher but what about existing ciphers?
- Research trends
  - Characterization and classification of backdoors **[theory]**
  - Conception of backdoors for stream, block ciphers, hash functions **[theory, practical]**
  - Detection of backdoors (existing crypto systems) **[theory, practical]**
  - Prevention of backdoors [theory, practical]. New designs to deal with with potential existing backdoors (inspired from WBC field [e.g. 256-3 block cipher]; meta block-ciphers)
- **Backdoors and presence/absence of structures are absolutely not equivalent!**

Trend 2 - Weak keys/strong Keys Encryption System

- Many algorithms are provided by one single (leading) country [e.g. USA to NATO countries; RIM/Blackberry?]
  - Cryptographic keys are provided by the leading nation only.
  - How to manage countries that would be tempted to use their own cryptographic keys?
- The solution is weak keys/strong keys technology. Let us consider a k-bit secret key system and $E_K(.)$ the encryption algorithm.
  - Keys K provided by the leading country are ``strong''. It means that $E_K(.)$ are cryptographically strong instances that cannot be broken by cryptanalysis. They form a class of 2^{k-r} keys
  - Keys K' not provided by the leading countries are ``weak''. $E_{K'}(.)$ are weak enough instances in order to enable cryptanalysis with respect to K'. They form a class of 2^r keys
  - Parameter r is critical and its value is determined by the operational context

Trend 3 - Combinatorial Approach

- Cryptology has nearly exclusively considered statistical and/or algebraic approaches
  - In cryptography, we just consider a superficial/global view. Design are base on the combination of small cryptographic primitives to build larger ones.
  - In cryptanalysis, we are doomed to face too huge amounts of plaintext and ciphertext, computing resources to have **practical** attacks
- It is essential to have a more qualitative view to understand the internal ``configurations'' in an encryption system.
  - Combinatorial designs appears to be the right objects to consider.
  - Example: instead of considering ``linear partitioning'', it seems natural to generalize to combinatorial partitioning (subsets of combinatorial design blocks, parallel classes of RBIBD...) and consider combinatorial invariants (with a probability significantly high enough).

Trend 4 - Cryptography in the Wild

- Many strong algorithms can be easily broken or backdoored at its environment level:
  - Software environment (Operating system, critical third party software)
  - Hardware environment. Probably the most critical part: whoever controls the hardware controls everything above.
- The most critical risk in industrial cryptography is to lose control over the whole environment
- Key evolutions:
  - RISC-V technology revolution: enable processor production which is open, free, without microcode or similar obscure layer/parts.
  - Independent, open and free UEFI-like technology: from hardware (TPM-like chip like Chinese Hengzhi) to basic OS (https://github.com/tianocore/edk2)

Conclusion

- The key fundamental concept in (cryptographic) security is more than ever SOVEREIGNTY!
  - Countries that are not able to have their own trusted **industry** will be technologically weak and live in an evergrowing insecurity
  - In the telecommunications domain, it is precisely all the debate around Huwai/5G (present) but also CISCO/Microsoft/Intel.
- Cryptology research
  - Nearly nothing conceptually new since the origin of the so-called ``modern cryptology''.
  - Researchers just use the same recipes with nearly the same ingredients.
- Strong need to think differently and to explore new mathematical approaches

Thank you for your attention

Контактная информация

Электронная почта:

filiol@esiea.fr

efiliol@netc.fr

Телефон:

+33 243 594 609

Сайт:

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