Ежегодная международная научно-практическая конференция
«РусКрипто'2019»

Thoughts about the Future and Trends of Cryptology
О будущем и о тенденциях криптографии

Eric FILIOL,
ESIEA, Operational Cryptology and Virology Lab

esiea
ECOLE D'INGENIEURS
DU MONDE NUMERIQUE

Благодарности

- От всего сердца благодарю А.Е. Жукова, Ю.В. Малинина и весь оргкомитет РусКрипто за большую честь – возможность выступить на РусКрипто.
- Я сильно привязан к России и российской культуре, но не только и не столько поэтому я убежден, что ваша страна является одним из лидеров как в целом в научной сфере, так и в области криптографии:
  - в части математических вопросов,
  - а также в части стратегии развития и конкретных шагов в области криптографии (применение стандартов ГОСТ в различных областях).
- Внесение ГОСТ в перечень криптонаборов протокола TLS – великолепная новость.

Введение

- Хотел бы поделиться несколькими соображениями о возможных путях развития криптографии – как желаемыми, так и ожидаемыми.
- Это не более, чем мое личное видение.
- ``*Les prévisions sont difficiles surtout quand elles concernent l'avenir*'' (Прогнозировать сложно, особенно когда речь идет о будущем.) (Жак Ширак)
- Основываюсь на моем опыте и соображениях – доклад может быть подвержен субъективности.

Тенденция 1: изучение и обнаружение закладок

- Закладки есть и будут исключительно важной проблемой для рассмотрения.
  - Bannier & Filiol (2017): первый практически применимый блочный шифр [с закладкой] – но что насчет существующих реально применяемых шифров?
- Тенденции исследований
  - Характеризация и классификация закладок **[теория]**
  - Изучение, как могут быть устроены закладки для поточных и блочных шифров, хэш-функций **[теория, практика]**
  - Обнаружение закладок (в существующих криптосистемах) **[теория, практика]**
  - Предотвращение закладок **[теория, практика]**. Новые методы предотвращения угроз со стороны потенциально существующих закладок (идеи из white-box-криптографии [напр., блочный шифр 256-3]; блочные «меташифры»).
- **Закладки и наличие/отсутствие [скрытых] структур – совсем не то же самое!**

Тенденция 2: слабые и сильные ключи в системах шифрования

- Ряд алгоритмов – от одной (ведущей) страны [напр., от США в страны НАТО; RIM/Blackberry?]
  - Ключи предоставляются только от этой ведущей страны.
  - Что делать со странами, у которых возникает соблазн использовать свои ключи?
- Решение: технология разделения на слабые и сильные ключи. Рассмотрим криптосистему с ключом длины k бит и алгоритмом зашифрования $E_K(.)$.
  - Ключи K, поставляемые от ведущей страны, – «сильные». Это значит, что $E_K(.)$ – криптографически стойкие объекты. Формируют класс из 2^{k-r} ключей.
  - Ключи K', поставляемые не от ведущей страны, – «слабые». $E_{K'}(.)$ – в достаточной мере нестойкие объекты, к ним могут быть успешно применены методы криптоанализа с целью нахождения K'. Формируют класс из 2^r ключей.
  - Параметр r критически важен, его значение определяется исходя из практических задач.

Тенденция 3: комбинаторный подход

- Криптография в основном опирается на статистические и/или алгебраические подходы.
  - В синтезе криптоалгоритмов – более общий взгляд на проблемы. Построение примитивов более высокого уровня на основе нескольких низкоуровневых.
  - В криптоанализе имеем дело с большим числом открытых и шифрованных текстов, вычислительных ресурсов с целью строить **практические** методы атак.
- Принципиально иметь более качественный взгляд, понимать внутренние «конфигурации» систем шифрования.
  - Рассмотрение комбинаторных структур, возникающих в примитивах.
  - Пример: вместо рассмотрения разложений на смежные классы по линейным подпространствам представляется естественным обобщение до разложения по другим подмножествам (подмножества, возникающие при комбинаторном анализе элементов конструкции криптопримитива, RBIBD (сбалансированные неполные блок-схемы...)) и рассматривать «комбинаторные инварианты» (с достаточно высокими вероятностями).

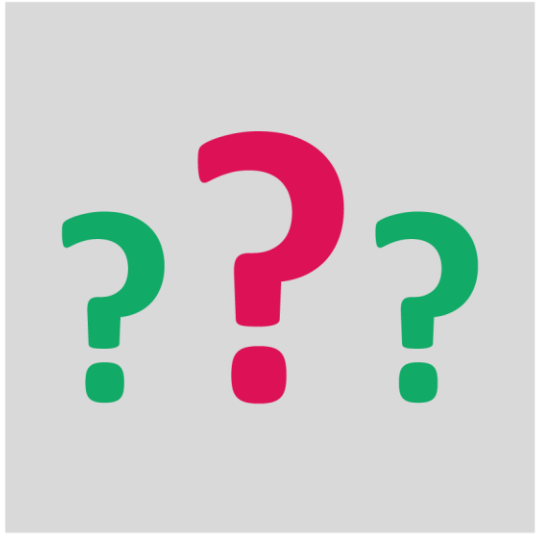
Тенденция 4: криптография в реальном мире

- Многие стойкие алгоритмы могут быть легко взломаны или подвластны уязвимости из-за закладок на уровне окружения, в котором они работают:
  - Программное окружение (операционные системы, системное ПО).
  - Аппаратное окружение. Вероятно, наиболее важная часть: кто контролирует аппаратную часть, контролирует и всё над ней.
- Наиболее критический риск в промышленной криптографии – потеря контроля над всем окружением.
- Развитие технологий:
  - RISC-V как технологическая революция: производство процессоров с открытой архитектурой, без микрокода или скрытых уровней/компонент.
  - Независимая, открытая и свободно распространяемая технология наподобие UEFI: от аппаратной части (чип с функционалом TPM, наподобие китайского Hengzhi) до базовой ОС (https://github.com/tianocore/edk2).

Заключение

- Ключевой фундаментальный принцип в (криптографической) защите информации, больше, чем когда-либо – СУВЕРЕННОСТЬ!
  - Страны, которые не могут развивать свою **доверенную промышленность**, будут технологически слабыми и всё более беззащитными.
  - В области телекоммуникаций в настоящее время именно по указанным причинам развивается дискуссия вокруг Huawei/5G; CISCO/Microsoft/Intel.
- Криптографические исследования
  - Принципиально ничего нового с момента появления т.н. «modern cryptology».
  - Исследователи используют те же рецепты примерно с теми же ингредиентами.
- Явная потребность мыслить иначе и развивать новые математические подходы.

Спасибо за внимание!



Контактная информация

Электронная почта:

filiol@esiea.fr

efiliol@netc.fr

Телефон:

+33 243 594 609

Сайт:

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