Криптографические алгоритмы Китая: развитие и применение

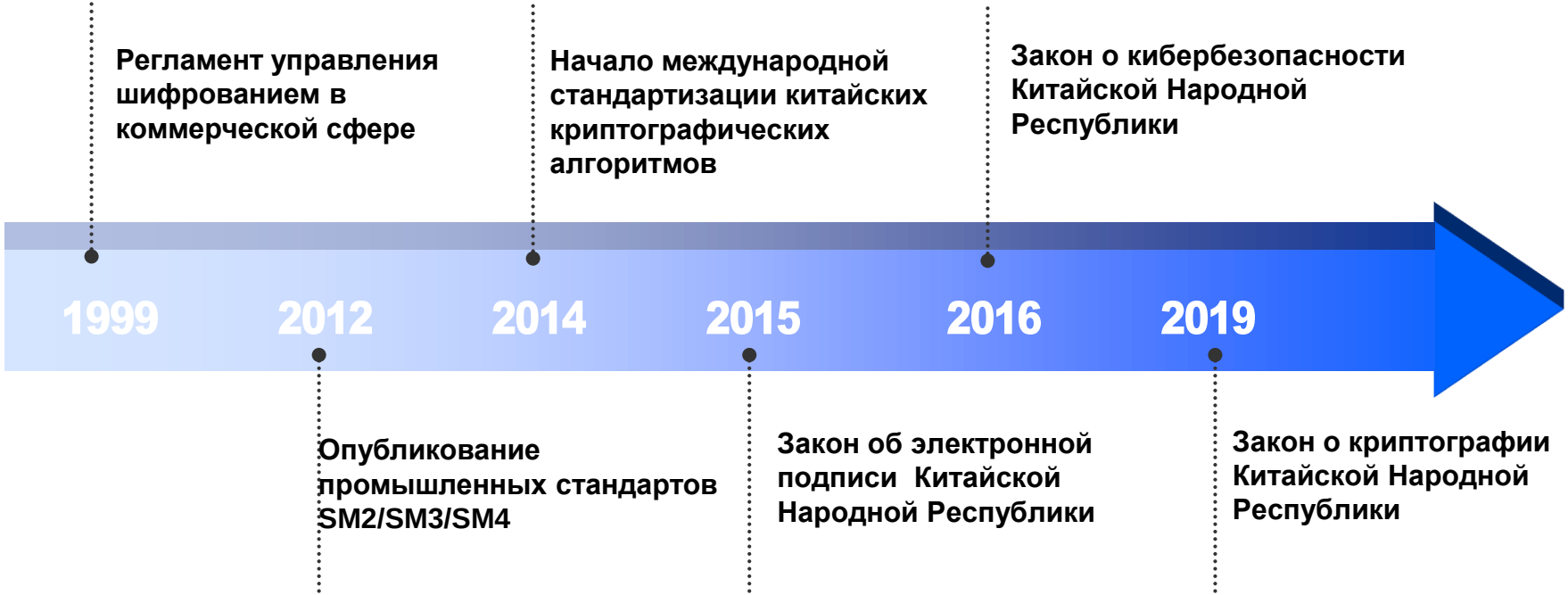
Ченхай ХУАНГ
China IWNCOMM Co., Ltd.

Примечание: Данный документ был подготовлен для российской конференции RusCrypto в марте 2020 года. Он служит основой для обсуждения и не представляет собой какого-либо обязательного ограничения для автора или предоставителя этого документа. При дальнейшем исследовании материалы данного документа могут измениться по форме и содержанию.

Содержание

1. Развитие и статус китайских криптографических алгоритмов

Развитие политики управления криптографическими алгоритмами



Китайские криптографические алгоритмы

- **SM2 - Криптографические алгоритмы с открытым ключом на основе эллиптических кривых**
  - включают Алгоритм цифровой подписи, Протокол обмена ключами, Алгоритм шифрования с открытым ключом
- **SM3 - Криптографический алгоритм хеширования** (256 бит)
- **SM4 – Алгоритм блочного шифрования** (128 бит)
- **SM9 - Криптографические алгоритмы на основе идентификации**
  - включают Алгоритм цифровой подписи, Протокол обмена ключами, Механизм инкапсуляции ключей и Алгоритм шифрования с открытым ключом
- **Zuc – Алгоритм Steam-шифрования**
  - включает Алгоритм конфиденциальности и Алгоритм целостности, одобренные консорциумом

Организация по стандартизации криптографических алгоритмов в Китае

- **SAC: Администрация по стандартизации в КНР**
- **SAC/TC 260: Национальный технический комитет по стандартизации в области информационной безопасности**
  - Разрабатывает стандарты для технологий в области информационной безопасности, включая криптографию и безопасность, аутентификацию и авторизацию, безопасность связи, безопасность больших данных и пр.
- **Технический комитет по криптографической стандартизации**
  - Разрабатывает промышленные стандарты, имеющие отношение к криптографии, включая криптографические алгоритмы, криптографические приложения, протоколы безопасности и т.д.
- **SAC/TC 180: Национальный технический комитет по финансовой стандартизации**
- **Взаимодействие**: с Техническим комитетом по стандартизации криптографических приложений (SAC/TC 28、SAC/TC 124, и пр.)

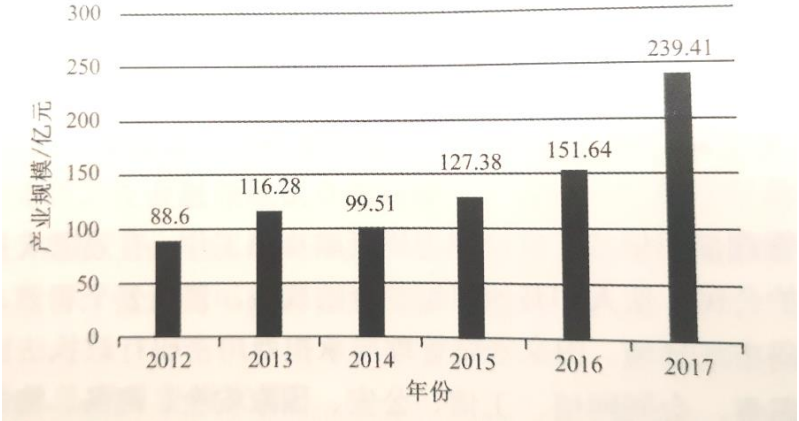
Стандартизация китайских криптографических алгоритмов

Криптографический алгоритм	Промышленные стандарты	Национальные стандарты	Стандарты Международной организации по стандартизации (ISO)	Другие
SM2	GM/T 0003-2012	GB/T 32918-2017	ISO/IEC 14888-3:2018 (SM2-DSA)	/
SM3	GM/T 0004-2012	GB/T 32905-2016	ISO/IEC 10118-3:2018	/
SM4	GM/T 0002-2012	GB/T 32907-2016	ISO/IEC FDIS 18033-3	/
SM9	GM/T 0044-2016	Стадия одобрения	ISO/IEC 14888-3:2018 (SM9-DSA)、 ISO/IEC 11770-3/Amd.2 (SM9-KA，CDAM)、 ISO/IEC 18033-5/Amd.1 (SM9-IBE，CDAM)	/
Zuc	GM/T 10004-2012	/	ISO/IEC 18033-4/Amd.1 (DAMD)	3GPPTM EEA3/EIA3

2. Применение и вклад китайских криптографических алгоритмов

Промышленное развитие китайского коммерческого шифрования

- **Промышленный масштаб:** В 2017 промышленный масштаб составлял 23,94 миллиарда (в китайских юанях) и позже рос на 57,9% ежегодно. В 2020 году ожидаемый масштаб – свыше 40 миллиардов (в китайских юанях).
- **Объемы продаж:** 1,32 миллиарда (комплектов продукции) в 2017 году
- **Количество корпораций:** 1700+



Стандартизация и индустриализация китайских криптографических протоколов безопасности (WAPI - в качестве примера)

- **WAPI: Инфраструктура аутентификации и конфиденциальности беспроводной локальной сети**
  - Опубликовано в качестве национального стандарта Китая **GB 15629.11** в мае 2003 года.
  - Базовая технология WAPI была опубликована в качестве международного стандарта **ISO/IEC 9798-3:1998/Amd.1:2010** (JTC 1/SC 27)
  - Использование блокового шифрования **SM4**

Стандартизация и индустриализация китайских криптографических протоколов безопасности (WAPI - в качестве примера)

- Сделать международную промышленность, использующую беспроводную локальную сеть WLAN, более безопасной
  - Wi-Fi: KRACK, Dragonblood и другие уязвимости были обнаружены для WPA2 и WPA3 в 2017 году
  - WAPI: бреши в безопасности обнаружены не были

Получение и передача Msg3 в стандарте IEEE 802.11

12.7.6.4

The Authenticator sends Message 3 to the Supplicant.

On reception of Message 3, the Supplicant silently discards the message if the Key Replay Counter field value has already been used or if the ANonce value in Message 3 differs from the ANonce value in Message 1. The Supplicant also

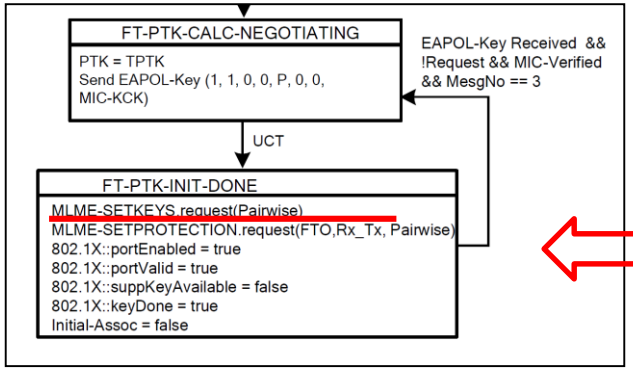
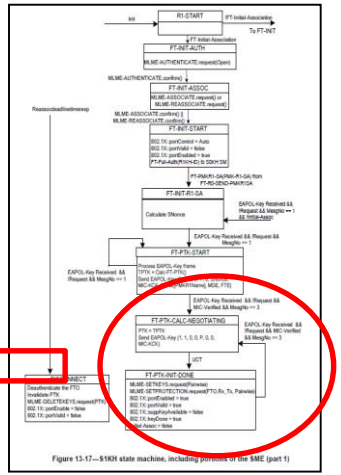


Fig.13-17

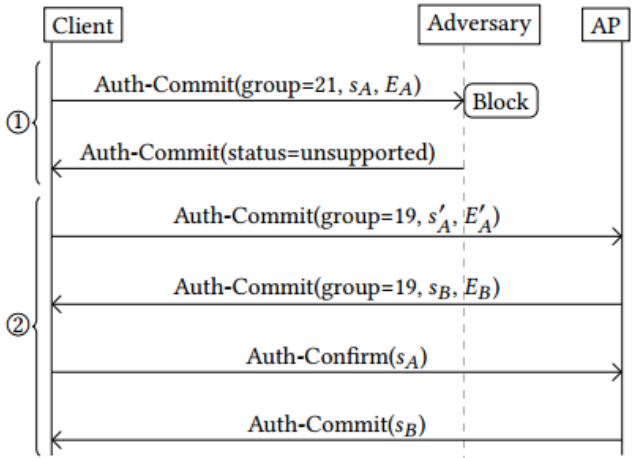


https://papers.mathyvanhoef.com/ccs2017.pdf
https://www.krackattacks.com/

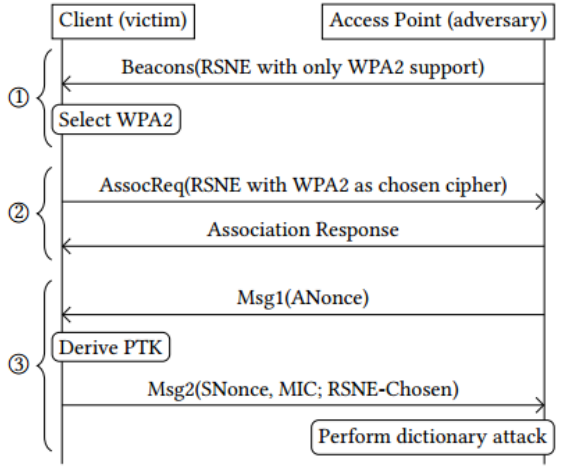
Стандартизация и индустриализация китайских криптографических протоколов безопасности (WAPI - в качестве примера)

https://wpa3.mathyvanhoef.com/#new

Движение протокола WPA3 в стандарте IEEE 802.11:



Злоумышленники заставляют обе стороны выбирать более слабые параметры безопасности, вставляя конкретные сообщения в процессе взаимодействия



Злоумышленник запускает словарную атаку после ата через демодернизацию

Стандартизация и индустриализация китайских криптографических протоколов безопасности (WAPI - в качестве примера)

Вклад в международное регулирование криптографических алгоритмов

Регулирующие нормы и практика: криптографические алгоритмы

- Когда криптографические алгоритмы прописаны в стандарте:
  - Случай № 1: Предложение по стандарту указывает AES в качестве единственного варианта для шифра. Это означает, что принятие других криптоалгоритмов не соответствует стандарту.
  - Случай № 2: В случае национальной адаптации с модификациями международного стандарта, если использование его национальных шифров предусмотрено как предмет местного регулирования, могут возникать внешние возражения против содержания, которые отличаются от международного стандарта по причине «установления технических барьеров для торговли».

F. Там, где международные стандарты существуют или их соблюдение является неизбежным, агентство по стандартизации должно использовать их или их соответствующие части в качестве основы для тех стандартов, которые оно разрабатывает, за исключением тех случаев, когда такие международные стандарты или их соответствующие части будут неэффективными или несоответствующими, например, из-за недостаточного уровня защиты или фундаментальных климатических или географических факторов или фундаментальных технологических проблем.

Вклад в международное регулирование криптографических алгоритмов

Регулирующие нормы и практика: криптографические алгоритмы

- Как достичь баланса? Объективность, обоснованность, честность
- Практика: Утверждение или описание в тесте международных стандартов (например, в ISO/IEC 29157:2015, опубликованном в JTC 1/SC 6):

“Криптографические алгоритмы, которые должны применяться к механизму информационной безопасности, могут быть подвергнуты национальному и региональному регулированию. В данном международном стандарте криптографические алгоритмы подкреплены примерами, что должно соответствовать национальному законодательству и нормам и может быть выбрано в соответствии с конкретными требованиями в различных странах и регионах”.

Вклад в международное регулирование криптографических алгоритмов

Регулирующие нормы и практика: криптографические алгоритмы

- **Регулирующие нормы Международной организации по стандартизации (ISO) в отношении криптографических алгоритмов, задействованных в международных стандартах**
  - Резолюция ISO/TMB (Совета технического управления) № 8/2012:

РЕЗОЛЮЦИЯ СОВЕТА ТЕХНИЧЕСКОГО УПРАВЛЕНИЯ № 8/2012 Заявления, направленные на ограничение цели использования конечного продукта
Дополнительно согласовывает, что заявления (требования), имеющие отношение к контрактным обязательствам или постановлениям правительства, также не допускаются,
Требует, чтобы любые такие заявления удалялись в ходе разработки конечного продукта (т.е. до закрытия диагностической информационной системы) и чтобы любые такие заявления в существующих конечных продуктах удалялись при пересмотре конечного продукта.

  - Резолюция Совета технического управления № 70/2018 (г. Сан-Паулу, Бразилия, 14-15 июня 2018 г.) дает дальнейшие уточнения для Резолюции № 8/2012:

РЕЗОЛЮЦИЯ СОВЕТА ТЕХНИЧЕСКОГО УПРАВЛЕНИЯ № 70/2018
Принята на 72-м заседании Совета технического управления в города Сан-Паулу (Бразилия), 14-15 июня 2018 года
Юридические обязывающие заявления в конечных продуктах Международной организации по стандартизации
Совет технического управления,
Принимая к сведению вопросы интерпретации Резолюции Совета технического управления № 8/2012 относительно фразы «Дополнительно согласовывает, что заявления (требования), имеющие отношение к контрактным обязательствам или постановлениям правительства, также не допускаются»;
Также принимая во внимание, что
• формулировка, имеющая отношение к соответствию контрактным обязательствам, юридическим требованиям и правительственным постановлениям, применяется во многих стандартах ISO; и
• конечные продукты ISO могут использоваться для дополнения таких требований и служат в качестве полезных инструментов для всех соответствующих участников процесса (включая государственные структуры и промышленность);
Также принимая к сведению ответы, полученные из Таблицы динамических методов (DMT) по данному вопросу;
Проясняет, что для всех конечных продуктов ISO :
a) Заявления, которые включают явное требование или рекомендацию по соответствию какому-либо конкретному закону, постановлению или контракту (например, нормативной ссылке на такие требования) или его части, не допускаются;
b) Заявления, имеющие отношение к юридическим и регулирующим требованиям , разрешены, если они не нарушают пункт a);
c) Фактологические примеры содержания конкретных законов или постановлений разрешаются в информационных целях; и
d) Никаких исключений для пункта a) не предусмотрено;

Криптография: участие в различных сферах работы Международной организации по стандартизации/Международной электротехнической комиссии (ISO/IEC)

- Объединенный технический комитет (JTC) № 1 ISO/IEC и криптографическая технология: общий интерфейс безопасности, встроенные средства защиты информации

Основан в 1987 году
Секретариат: ANSI (Американский национальный институт стандартов)

22 подкомитета (SC)

SC 6

1964, KATS (Ю. Корея)

JTC 1/SC 6

Телекоммуникации и обмен информацией между системами

SC 27

1990, DIN (Германия)

JTC 1/SC 27

Информационная безопасность, кибербезопасность и защита конфиденциальности

SC 31

1996, ANSI (США)

JTC 1/SC 31

Методы автоматической идентификации и сбора данных

… …

Криптография: участие в различных сферах работы ISO/IEC

- **Управление ключами защиты**
  - **ISO/IEC 11770** Управление ключами защиты
- **Криптографический алгоритм**
  - **ISO/IEC 18033** Алгоритм шифрования
  - **ISO/IEC 9796** Схемы цифровой подписи, обеспечивающие восстановление сообщений
  - **ISO/IEC 14888** Механизмы цифровой подписи с приложением
  - **ISO/IEC 20008** Алгоритм анонимной цифровой подписи
  - **ISO/IEC 29192** Легковесная криптография
  - **ISO/IEC 10118** Алгоритмы хеширования
- **Протокол криптографической безопасности**
  - **ISO/IEC 9798** Аутентификация объекта
  - **ISO/IEC 20009** Анонимная аутентификация объекта
  - **ISO/IEC 9797** Код аутентификации сообщения
- **Криптографический протокол сетевой безопасности**
  - **ISO/IEC 29167** Безопасность радиочастотной идентификации
  - **ISO/IEC 13157** Безопасность стандарта ближней радиосвязи NFC
  - **ISO/IEC 7816** Безопасность карты с интегральной схемой (IC Card)

Вклад Китая в стандарты ISO/IEC, имеющие отношение к криптографии (в рамках работы Объединенного технического комитета № 1)

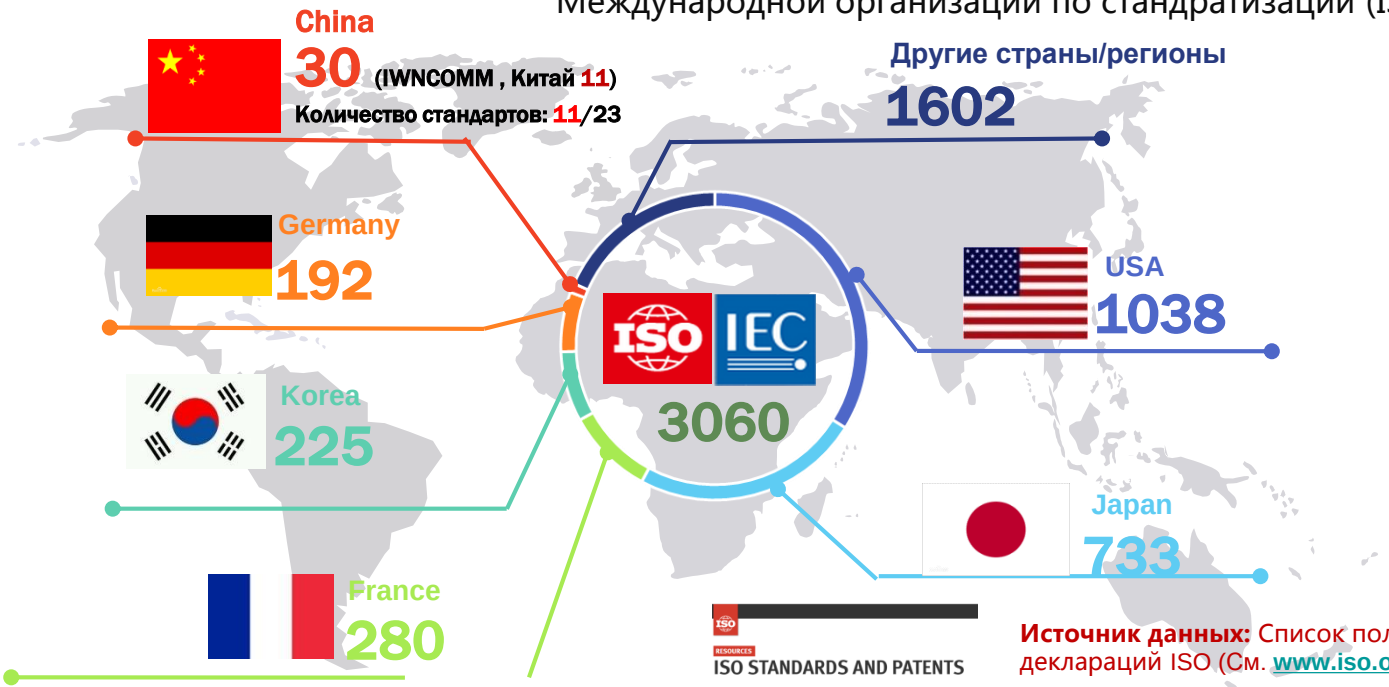
- SC (подкомитет) 27
  1. ISO/IEC 9798-3 Аутентификация объекта (TePA-EA)
  2. ISO/IEC 20009-2 Аутентификация анонимного объекта (TAEA)
  3. ISO/IEC 14888-3 Цифровая подпись (SM2 DSA, SM9 DSA)
  4. ISO/IEC 10118-3 Хэш-функция (SM3)
  5. ISO/IEC 18033-3 Алгоритм шифрования (SM4)
  6. ISO/IEC 11770-3/Amd.2 (SM9-KA, CDAM)
  7. ISO/IEC 18033-5/Amd.1 (SM9-IBE, CDAM)
  8. ISO/IEC 18033-4/Amd.1 (DAMD)
- SC (подкомитет) 31
  1. ISO/IEC TS 29167-15 RFID КриптоПакет (TRAIS-X)
  2. ISO/IEC 29167-16 RFID КриптоПакет (TRAIS-P)
- SC (подкомитет) 6
  1. ISO/IEC 13157-4 Безопасность стандарта ближней радиосвязи NFC (NEAU-A)
  2. ISO/IEC 13157-5 Безопасность стандарта ближней радиосвязи (NEAU-S)
  3. ISO/IEC 22425 Методы тестирования стандарта NFC (NEAU-TEST)
  4. ISO/IEC 15149-4 Безопасность сети магнитного поля (MSAI)
  5. ISO/IEC 29157 Безопасность беспроводных сетей ближнего действия и беспроводных сетей с низкой скоростью (PLAS)
  6. ISO/IEC 29180 Безопасность сенсорных сетей (TSSI)
  7. ISO/IEC 17821 Беспроводная ячеистая сеть (AKEP)

  .....

Вклад Китая в стандарты ISO/IEC, имеющие отношение к криптографии

(Обновлено до февраля 2020 г.)

- Вклад Китая в развитие криптографических технологий с точки зрения патентных деклараций в Международной организации по стандратизации (ISO).



ISO STANDARDS AND PATENTS

Источник данных: Список полученных патентных деклараций ISO (См. www.iso.org/patents)

Итог: 3060 патентных деклараций по IS

3. Перспективные направления развития и планы на будущее

Достижения в исследовании криптографических алгоритмов в Китае

- **Национальный конкурс по дизайну криптографических алгоритмов**
  - **Начался 11 июня 2018 г. и окончился 31 декабря 2019 г.**
  - Результаты выбора включают две категории: **криптографические алгоритмы с открытым ключом и криптографические алгоритмы блочного шифрования.**
  - **Криптография с открытым ключом (14 предметов)**：

    Aigis-sig、LAC.PKE、 Aigis-enc、LAC.KEX、SIAKE、SCloud、AKCN、OKCN、Fatseal、木兰、AKCN-E8、TALE、PKP-DSS、Piglet-1
  - **Блочные шифры (10 предметов)**：

    uBlock、Ballet、FESH、ANT、TANGRAM、Raindrop、NBC、FBC、SMBA、SPRING
- Эти 24 алгоритма являются показательными достижениями Китая в области криптографических алгоритмов нового поколения

Прогресс в области постквантовых криптографических алгоритмов и вклад Китая

Постквантовая криптография (PQC)：метод, основанный на квантовой механике, который использует основные характеристики квантовой физики для защиты информации.

Прогресс в области постквантовых криптографических алгоритмов и вклад Китая

ISO/IEC, Объединенный технический комитет (JTC) № 1/Подкомитет (SC) 27/ Рабочая группа (WG) 2 SD8, изучает алгоритмы PQC для подготовки к возможной стандарти-зации. Редактор – из NIST (Национального института стандартов и технологии). Китайские эксперты работают в качесвте редакторов для одного из разделов.

RFC 8391
XMSS:
Расширенная схема получения подписи Merkle, опубликованная в 2018 году.

Набор алгоритмов PQC был инициирован в 2016 году и ожидается к получению в 2021 году, а проект стандарта будет готов в 2023 году.
Китайский алгоритм LAC был выбран для второго раунда.

В 2015 году были инициированы флагманский проект PQCRYPTO по глобальному алгоритму PQC и проект SAFCRYPT по применению алгоритма PQC.

Китайская ассоциация криптографических исследований запустила национальный конкурс по созданию дизайна криптографических алгоритмов с более 60 предложениями и 24 финалистами, включая постквантовые криптографические алгоритмы.

Некоторые глобальные усилия по криптографии

- **Сеть/Связь:**
  - 5G (включая алгоритм ZUC)
  - Интернет вещей (Легковесный алгоритм)
  - Интернет транспортных средств (Легковесный алгоритм)
- **Квантовые вычисления:**
  - PQC, QKD (Распределение квантовых ключей)
- **Большие данные/Искусственный интеллект:**
  - Гомоморфное шифрование, безопасное многосторонне вычисление
- **Блокчейн:** цифровая подпись
- **Защита конфиденциальности:** технология анонимности

Благодарю за внимание

Ченхай ХУАНГ

Электронная почта: zhenhai.huang@iwncomm.com


专注通信网络与信息系统安全技术
ISO/IEC JTC1 SC6/CHINA
BWIPS
无线网络安全技术国家工程实验室
创立于2004年
西电捷通
TePA
4,000,000,000
WAPI
TISec
RAIS
WSAI
TCA
TAAA
PCT TOP500
Beijing 2008
Chinese Cryptographic Algorithms: Development and Applications
Zhenhai HUANG
China IWNCOMM Co., Ltd.