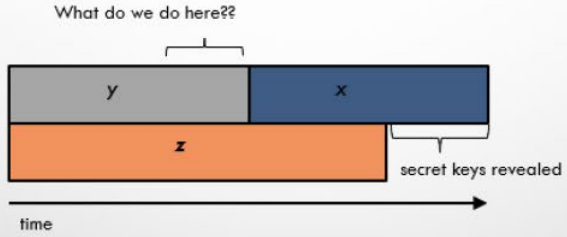
RECSI 2022

CCN-PyTec. Retos y Desafíos de la Evaluación Criptológica.

centro criptológico nacional

Índice

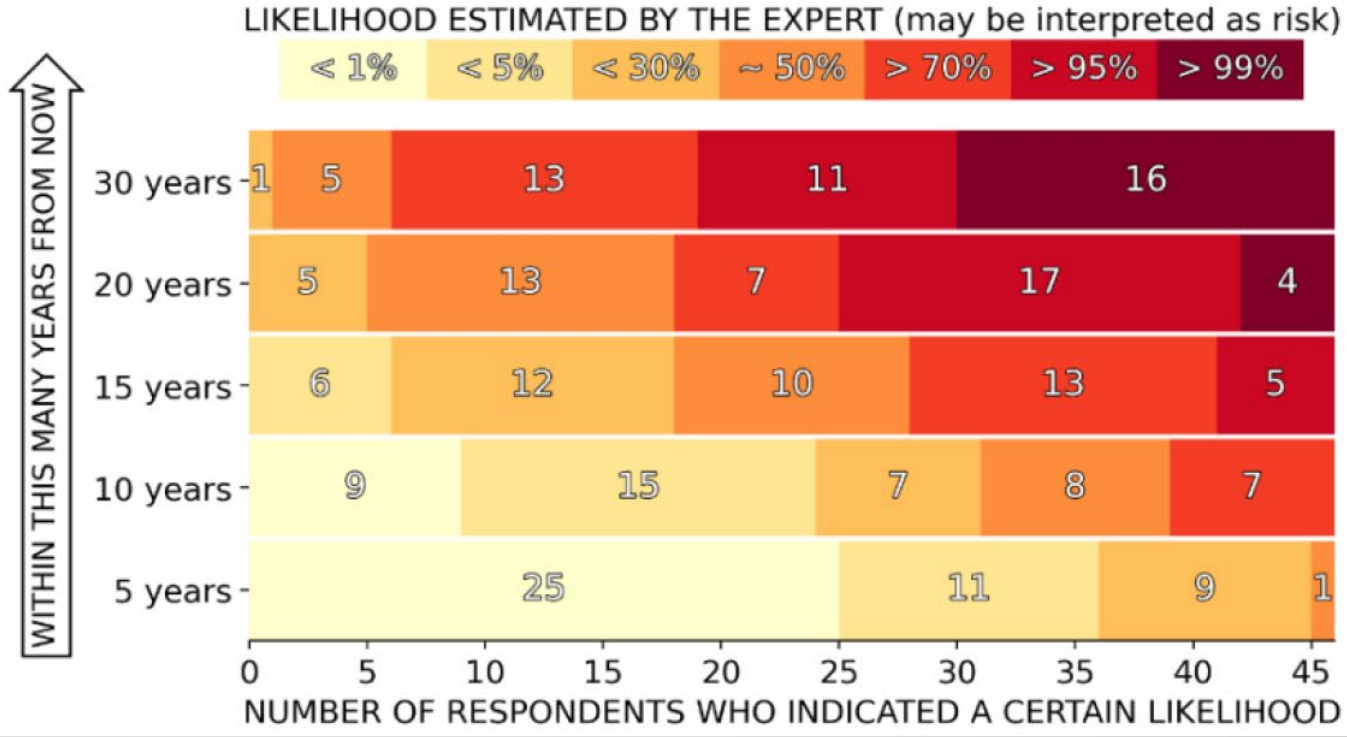
Theorem (Mosca): If $x + y > z$, then problem ("*Harvest now, decrypt later*")



x – how long data needs to be safe
y – time for standardization and adoption
z – time until quantum computers

EXPERTS' ESTIMATES OF THE LIKELIHOOD OF A QUANTUM COMPUTER ABLE TO BREAK RSA-2048 IN 24 HOURS

The experts were asked to indicate their estimate for the likelihood of a quantum computer that is cryptographically relevant—in the specific sense of being able to break RSA-2048 quickly—for various time frames, from a short term of 5 years all the way to 30 years.



Source: M. Mosca, M. Piani, Quantum Threat Timeline Report, 2021
https://globalriskinstitute.org/publications/2021-quantum-threat-timeline-report//

1. El gran reto

Modernizar toda la criptografía utilizada en la Administración en 10 años.

- *Amenaza de la computación cuántica*
- *Criptografía obsoleta*

Cada Organización es responsable de:

- *Analizar qué información es vulnerable*
- *Priorizar su necesidad*
- *Ser impulsora del cambio*

2. La elección de los mecanismos criptográficos (I)

- *CRIPTOGRAFÍA OBSOLETA*
  - *Algoritmos y Mecanismos Obsoletos*
    - *DES, MD5, SHA-1, Triple-DES,*
    - *Claves cortas de RSA y (EC)DH*
    - *PKCS#1v1.5, TLS 1.0, …*

  - ***Dificultad para sustituir algoritmos obsoletos***
    - *2008 -> Criptoanálisis de SHA-1*
    - *2012 -> Primeros cálculos que demostraban que era un problema abordable*
    - *2017 -> primera colisión*
    - *2020 -> colisiones a 45k USD*
    - ***2020/08 Microsoft ya no da soporte a firmas con SHA-1***

      ¡Realmente se deja de utilizar SHA-1 en la práctica!

2. La elección de los mecanismos criptográficos (II)

DISPONIBILIDAD DE ALGORITMOS POST CUÁNTICOS

- *2017 comenzó el Proceso de estandarización de algoritmos Post Cuánticos (NIST PQC)*
- *2022/07 Fin de Ronda 3:*
  - *KEM (1):*
    - ***CRYSTALS-Kyber***
  - *Signatures (3)*
    - ***CRYSTALS-Dilithium, Falcon, SPHINCS+***
- *Ronda 4:*
  - *KEM (4):*
    - *ClassicMcEliece, BIKE, HQC, SIKE*
  - *Signatures (0):*
    - *Se piden nuevos candidatos preferiblemente no basados en retículos*

- *Comienza un período de actualización de los estándares de protocolos de autenticación y acuerdo de claves para usar los nuevos algoritmos.*

2. La elección de los mecanismos criptográficos (III)

- ***Guía de Mecanismos Autorizados por el CCN:***
  - *CCN, CSIC-ITEFI (Luis Hernández Encinas)*
  - *Alineado con normas internacionales SOG-IS Crypto, NIST, ISO,…*
- *Objetivo:*
  - *Eliminar algoritmos obsoletos*
  - *Incluir resistencia post-cuántica*
  - *Establecer pautas para alguno de los **protocolos más comunes***
    - *TLS, IPSEC, OpenSSH,…*

- *Necesidad de una **lista acotada** de algoritmos aceptados:*
  - *Hay muchos buenos algoritmos además del AES (Serpent, Camellia,…)*
  - *La realidad:*
    - *Después de tantos años, sigue siendo difícil implementar AES de manera eficiente y segura frente a ataques de canal lateral. (Emanaciones, Timing attacks,...)*
    - *La implementación de Contramedidas es esencial*

2. La elección de los mecanismos criptográficos (IV)

- *Lista acotada, pero…*
  ¿Que hacemos con algoritmos CHACHA20+POLY1305 , BLAKE2s, EdDSA?
  - *Estándares de facto en la industria no tiene sentido no aceptarlos dentro del ENS*

- *Para incluirlos en la lista:*
  - *Implementación de referencia (RFCxxxx, ISO-xxxx, NIST-SPxxxx)*
  - *Batería de vectores de test en librería de referencia*
    - *KATs*
    - *Baterías completas que cubran casos límite*
  - ***Análisis de seguridad criptográfico***

3. Analizando la seguridad (I)

1.- Algoritmos criptográficos que no estandarizados, pero son estándares de facto de la industria.

*Necesidad de **garantías de seguridad***

2.- La criptografía tipo A para información clasificada

¿Qué es la criptografía tipo A?

¿Donde se usa y por qué?

¿Cómo es? ¿En que se basa?

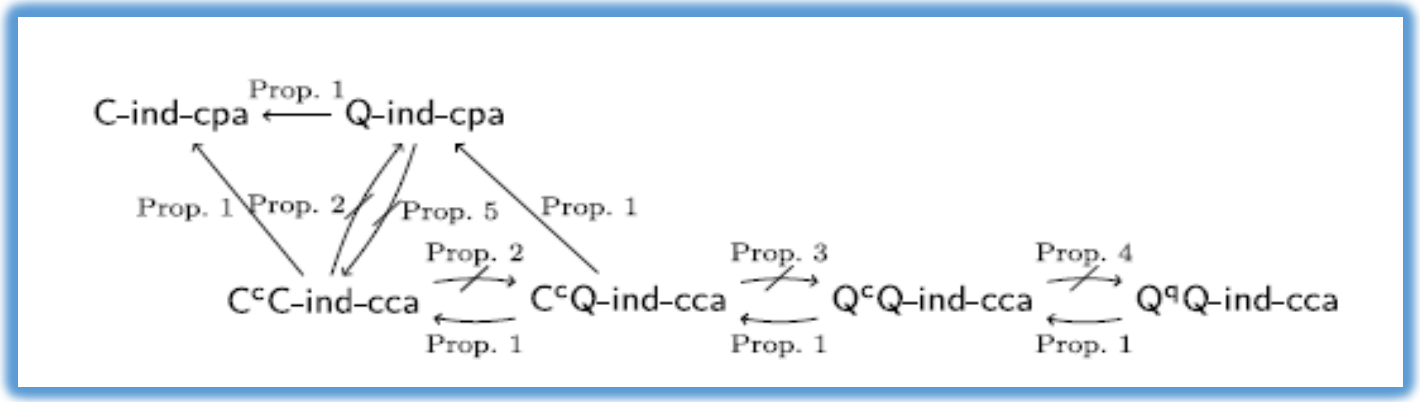
Mejorar la capacidad nacional para analizar la seguridad de este tipo de algoritmos.

Es fundamental seguir con interés los concursos públicos internacionales para la definición de algoritmos (i.e. los del NIST para PQC o para LightWeigthCrypto) no solo por conocer el ganador. También es interesante conocer las técnicas y ataques desarrollados para criptoanalizar a los distintos candidatos.

3. Analizando la seguridad (II)

Mejorar la capacidad nacional para analizar la seguridad de algoritmos y esquemas criptográficos

Nociones de seguridad exigibles a los esquemas criptográficos: ***IND-CCA, IND-CPA***
Reducciones de seguridad en el ROM y en el QROM (Quantum-Random-Oracle Model)



Estudio de algoritmos PQC:

- ***Fortaleza del problema M-LWE:***
  - ***Primal lattice attacks***
  - ***Dual lattice attacks***

Algoritmos simétricos

- ***Correlation attacks, Differential attacks, Biclique attacks***

Solidez ante Ataques de Canal Lateral

- *Diseño de contramedidas y valoración del esfuerzo necesario para superarlas*

4. La formalidad de los protocolos (I)

Un protocolo debe cumplir todas o parte de las siguientes propiedades de seguridad:

Protecciones Anti-replay
Integridad de los mensajes
Perfect Forward Secrecy
Post Compromise Secrecy
Post Quantum resistance

Del concurso de NIST y de los estudios propios hemos obtenido un conjunto de primitivas criptográficas.
Todos los protocolos y estándares de intercambio de claves, firma digital, etc. ***tienen que ser actualizados****.*
IKEv2, TLS1.3, ECIES (HPKE), PAKE, PKI,…

Necesidad de Verificación Formal:
Detectar vulnerabilidades y debilidades en una etapa temprana

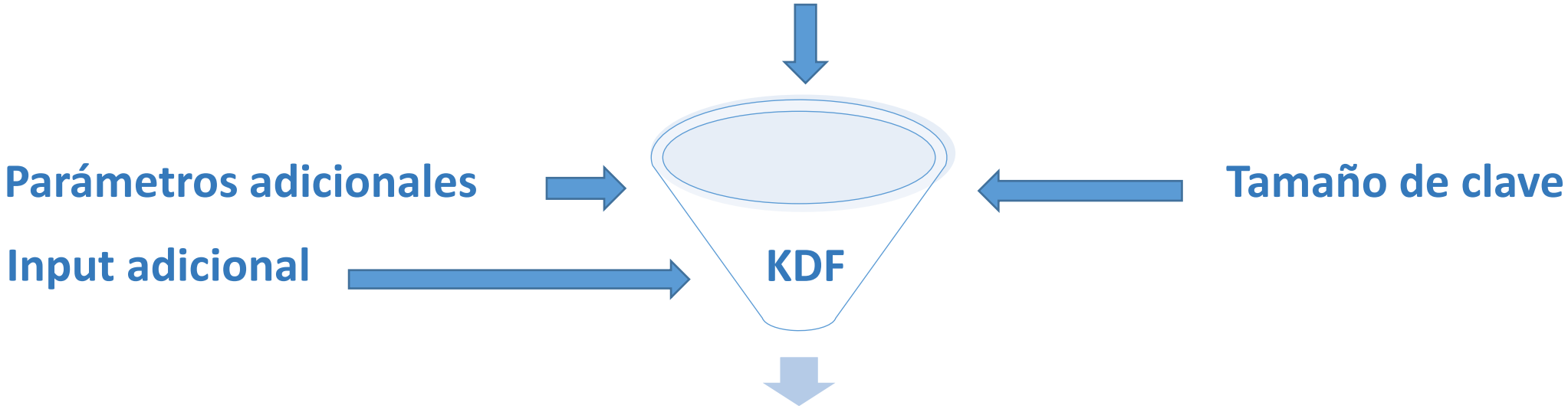
La tendencia actual es a verificar formalmente los protocolos con herramientas de análisis simbólico:
Tamarin, ProVerif, VerifPal*,...*

4. La formalidad de los protocolos (II)

MEDIDAS DE TRANSICIÓN - SISTEMAS HÍBRIDOS

Claves de al menos 2 de las siguientes:

- Intercambio de claves “clásico”
- Intercambio de claves post-cuántico
- Claves precompartidas



4. La formalidad de los protocolos (III)

QKD

- *Nuevos protocolos basados tecnologías cuánticas*
  - *Fuentes de fotones entrelazados (E91)*
  - *Polarizados (BB84, B92)*
- *Teóricamente son protocolos muy interesantes.*
- *Las implementaciones prácticas tienen sus hándicaps*
  - *La cantidad de bits a transmitir se reducen con la distancia*
  - *Necesidad de canal autenticado clásico*
  - *Disponibilidad de fuentes de fotones únicos*

¿cómo evaluar la seguridad de este tipo de sistemas (no-estandarizados)?
ITU-T esta desarrollando normativa
BSI definiendo perfiles de protección Common Criteria

IMPORTANTE => Migrar a PQC tiene prioridad frente al uso de QKD

5. Un problema de ruido (I)

Los generadores de secuencia aleatoria son una parte fundamental de cualquier sistema criptográfico.

Es relativamente fácil demostrar que tiene buenas propiedades estadísticas, pero muy difícil garantizar el origen de la entropía

AIS-20/31 y NIST 800-90 son las base que utilizamos para evaluar generadores de ruido

Ambas normas definen distintas categorías para los RNG en función del nivel de seguridad a alcanzar

Es posible encontrar semejanzas entre ambas normas, con ligeras diferencias

La diferencia más importante entre ambos estándares:
AIS 20/31 requiere un modelo estocástico de la fuente de entropía

5. Un problema de ruido (II)

Modelo estocástico *de la fuente física de entropía*

Exigido por AIS20/30. NIST lo comenzará a exigir en un futuro cercano.

¿Cómo validamos que los modelos estocásticos son buenos?

+ Argumentación de propiedades físicas basado en publicaciones reconocidas

+ Verificar la conformidad del modelo con la distribución medida es condición necesaria pero no suficiente

+ Aportar evidencias de que el modelo estocástico se ajusta la fuente de ruido físico implementada

6. Conclusión

EL OBJETIVO DE LA CHARLA ES TRANSMITIR LOS GRANDES PROBLEMAS PRÁCTICOS QUE SURGEN DE ESTA MODERNIZACIÓN CRIPTOLÓGICA.

DESDE EL CCN ESTAMOS CONVENCIDOS DE QUE ES NECESARIO EL APOYO DEL MUNDO ACADÉMICO PARA DAR SOLUCIONES A MUCHOS DE ESTOS PROBLEMAS.

Muchas

Gracias

E-mails

ccn@cni.es

criptosec.ccn@cni.es

organismo.certificacion@cni.es

Páginas web:

www.ccn.cni.es

www.ccn-cert.cni.es

oc.ccn.cni.es