Developing security targets for novel cryptography

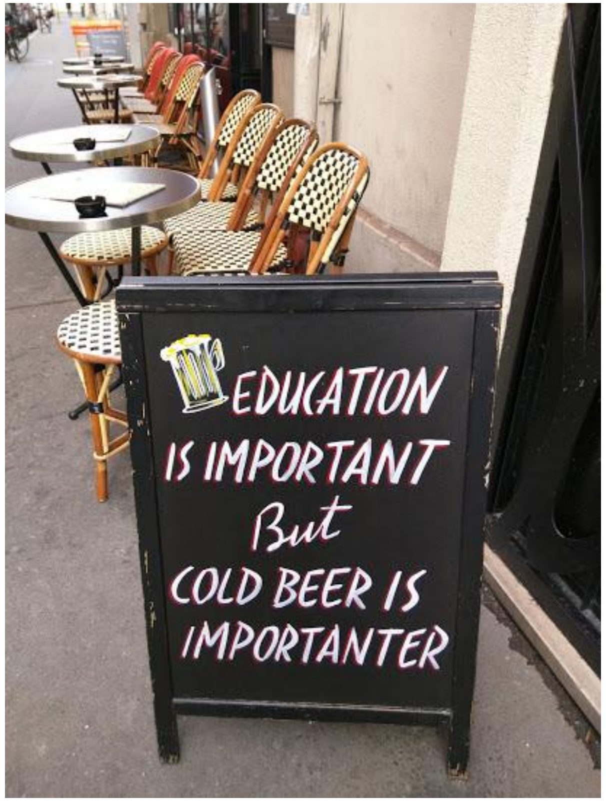
a.k.a. Certifying “new” cryptographic constructions

Vashek Matyas ✉ ***matyas@fi.muni.cz***
Centre for Research on Cryptography and Security, Masaryk University, Czechia
& currently hosted by Cybernetica, CHESS project

CROCS
Centre for Research on
Cryptography and Security

Sincere apologies & acknowledgements

- Many hearsays and very narrowly-viewed observations
  - – Even sarcastic comments ☹
- Very speculative at many points
- Certainly mistakes – I’m guilty of those!



- Big thanks to ChatGPT & sec-certs

Certification of IT products – pros

- **Quality assurance**: Product meets certain industry standards (e.g., security, compatibility, performance).
- **Interoperability**: Guaranteed compatibility with other certified systems.
- **Market trust**: Viewed as more reliable and safer by customers and partners.
- **Compliance**: Meeting legal or regulatory requirements.
- **Competitive edge**: Differentiation from competitors in the market.

Certification of IT products – cons

- **Cost**: Testing fees, labs, paperwork, consultant costs.
- **Time-consuming**: Often extensive testing and review periods.
- **Maintenance overhead**: Re-certification when products or standards change.
- **Limited innovation**: Some products may have to sacrifice experimental features or design flexibility.
- **Fragmentation**: Different markets/regions with different certifications, creating complexity (e.g., CE in Europe vs. FCC in the US).

ChatGPT dialogue I

`Few real-world examples of famous product certifications in IT`

1. Wi-Fi CERTIFIED™ (Wi-Fi Alliance)
2. FCC certification (US Federal Communications Commission)
3. **Common Criteria certification (ISO standard for IT security)**
4. UL (Underwriters Laboratories) certification
5. **PCI DSS compliance certification (for payment systems)**

ChatGPT dialogue II

Examples of worst failures in the IT industry despite certifications

1. Intel Pentium FDIV Bug (1994)
2. Samsung Galaxy Note 7 Battery Explosions (2016)
3. **Heartbleed Bug in OpenSSL (2014)**
4. **Healthcare.gov Launch (2013)**
5. Therac-25 Radiation Machine (1985-87)

ChatGPT dialogue III: Big problems with crypto?

Big problems despite cryptographic certifications.

1. Heartbleed (OpenSSL, 2014).
2. ROCA vulnerability (Infineon chips, 2017).
3. Dual_EC_DRBG (NSA backdoor allegation, 2006–2013).

New crypto algorit – 70's

- Have a call
- Run the competition a osed circles
- Tweak some paramet ecosystem
- Tweak other paramet

- 80's & 90's: keep on making sure that no (better) algorithm replaces that one where you spent some effort…

Recall the AES (call) evaluation criteria

Initial:

- security – effort for practical cryptanalysis,
- cost – in terms of computational efficiency,
- algorithm & implementation characteristics.

Final:

- general security,
- ease of software & hardware implementation,
- implementation attacks,
- flexibility (in en/decryption, keying, other factors).

Recall the AES (call) results…

- Non-US algorithm selected.
- Algorithm with “adequate” (and not “high”) level of security.
- Algorithm with performance advantages across SW & HW platforms of various kinds.

ChatGPT dialogues IV

- `How & where are crypto & security certifications evolving?`

- Post-quantum cryptography.
- Formal verification.
- Cloud security & cryptography
- More focus on real-world attacks.
- Compliance-driven certification.
- Open-source trend.

Relevant EU regulations

- GDPR
- Cybersecurity Act (Regulation (EU) 2019/881)
  - Certification schemes voluntary – but can be made mandatory by EU or national law for certain products/services.
- NIS2 Directive (2022/2555)
- Digital Operational Resilience Act (DORA – 2022/2554)
- Cyber Resilience Act (CRA)

FIPS 140-3 – cryptographic modules

- First draft appeared 2005, the standard came out nearly 15 years later.
- Aligns more closely with the ISO/IEC 19790 standard.
- When considering v2, it comes with
  - More robust physical security, side-channel resistance, and entropy testing.
  - Requirements re. modern threats (supply chain, embedded devices, etc.)
  - Room for v2 validity till September 2026 for some use cases.

Common Criteria 101

- Compromise on interests of users, manufacturers, evaluators.
- *Target of evaluation* (TOE) – what is (to be) evaluated.
- *Protection profile (PP)* (smartcards, biometrics, etc.)
  - Catalogued as a self-standing evaluation document.
- *Security target* (ST) – theoretical concept/aim.

- **Evaluation of TOE – is the reality corresponding to theory (ST)?**

Case 1: Homomorphic encryption

- Homomorphic encryption is not yet included in the FIPS-approved algorithm suites. (Or any gov’t-level suites, AFAIK.)
  - ISO/IEC 18033 (Part 6 – Homomorphic encryption – 2 algorithms only).
- High computational overhead and lack of hardware acceleration.
  - DARPA DPRIVE program – investing in HE-specific hardware acceleration.
- Pilots…
- Security proofs and implementations are still evolving (e.g., noise growth, ciphertext expansion).

Case 1: Homomorphic encryption cont’d

- “The TOE is a homomorphic encryption engine for database queries.”
- “The ZeroReveal Server (the TOE) and ZeroReveal Client are evaluated as software applications only and the homomorphic encryption techniques used for the ZeroReveal Client and ZeroReveal Server operations are outside the scope this evaluation.”
  - “The TOE is the ZeroReveal Compute Fabric Server software that includes the following libraries:… SEAL Homomorphic Encryption Library v3.7.2.0.”
  - “Excluded Functionality:…The homomorphic encryption process, including the algorithms, uses and the security strength of the resultant ciphertext.”
- Protection Profile for Application Software

Case 2: Multiparty computing in crypto key operations

- STs with threshold crypto schemes, e.g., decentralised signing.
- ST can implement MPC internally to secure keys but still claim conformance to existing crypto PPs.

- Slowdown factors:
  - Diverse protocols and implementations.
  - Missing standards.

Case 3: Multiparty computing in bigger data* operations

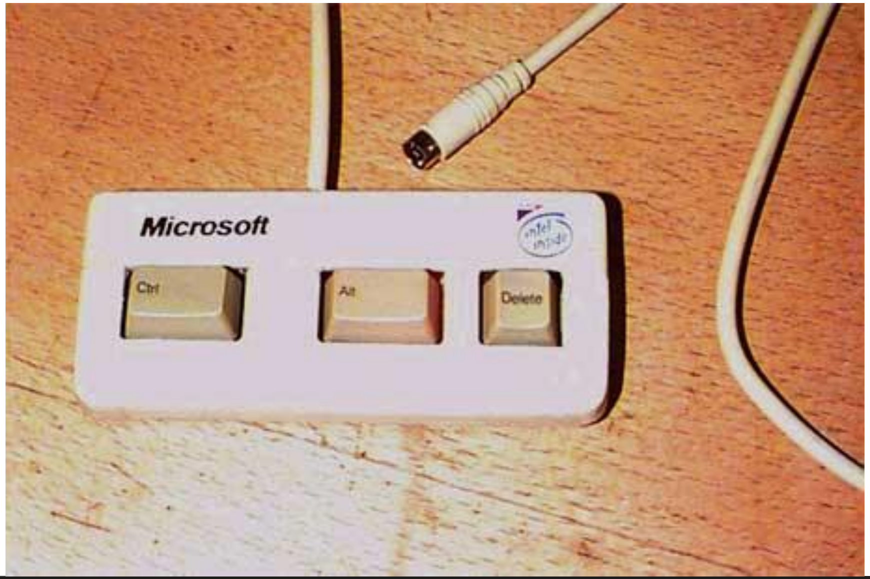
- Typically, privacy-preserving data analysis…
- Threat models are trickier than for the crypto key threats.

- Slowdown factors:
  - Diverse protocols and implementations.
  - Missing standards.
  - Performance overhead – slow uptake.

* *Bigger than standard crypto keys.*

Key takeaways by ChatGPT (after our long dialogues ☺)

1. Certified crypto is better than random crypto — but certification alone ≠ secure system.
2. Always combine certified crypto plus real code audits, formal proofs if possible, and assume future attacks will happen.



Additional key takeaways

1. Certified crypto is better than random crypto — but certification alone ≠ secure system.
2. Always combine certified crypto plus real code audits, formal proofs if possible, and assume future attacks will happen.
3. Understand (and re-assert) why you certify => what exactly you certify.
4. Map the ecosystem well (or even better ☺).
5. Avoid mistakes – but don’t fear them!

CHESS

Cyber-security Excellence Hub in
Estonia and South Moravia

Thank you for your attention!

sec-certs