Conclusion

Stefan Dziembowski

www.crypto.edu.pl/Dziembowski

University of Warsaw

23.01.19

version 1.0

Main take-home messages

1. Cryptography is a **mature** (yet still quickly deveopling) **field**.
2. Seurity of all popular constructions is **well-defined**.
3. Popular schemes have been **analyzed for a long time** by lots of smart people.
4. Do **not** invent your own crypto.
5. If you have your own idea for a new crypto promitive "do your homework" by **checking if it hasn't been invented before**.

Where is crypto research published

Crypto conferences (most of them organized by the **International Association for Cryptologic Research**, ww.iacr.org):

1. CRYPTO, Eurocrypt,
2. Asiacrypt, Theory of Cryptography Conference (TCC), Public-Key Cryptography (PKC), Fast Software Encryption (FSE), Cryptographic Hardware and Embedded Systems (CHES),...

Security conferences: IEEE Symposium on Security and Privacy (IEEE S&P), ACM Conference on Computer and Communications Security (ACM CCS), Usenix Security, Network and Distributed System Security (NDSS),...

Journals are less important.

Non-reviewed internet repository: eprint.iacr.org.