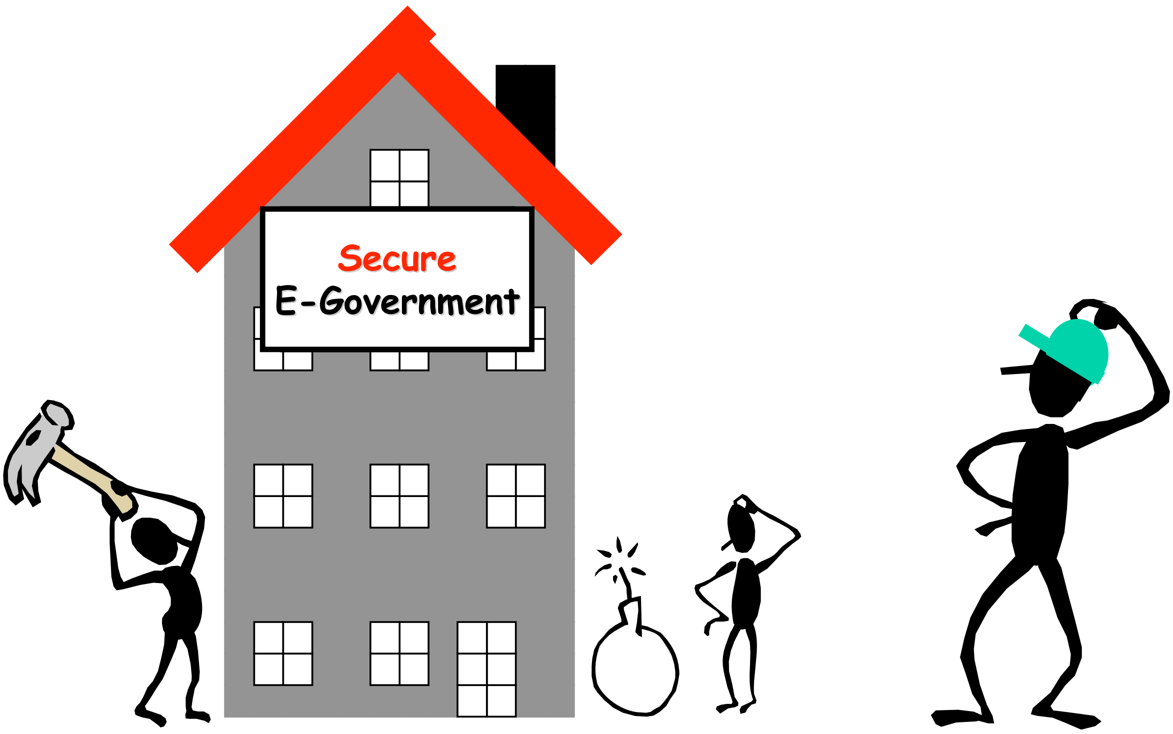
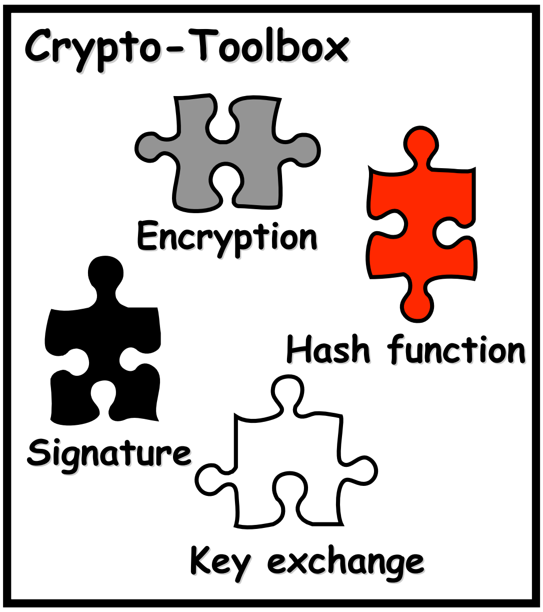
Scalable Verification of Systems with Cryptography

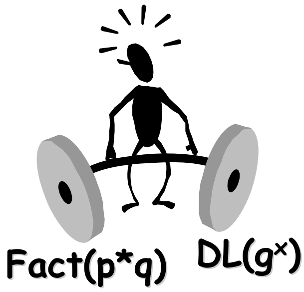
Birgit Pfitzmann (IBM Research, Zurich)
Joint work mainly with Michael Backes (Univ. Saarbrücken) and Michael Waidner (IBM Research & SWG)

Building Secure Systems



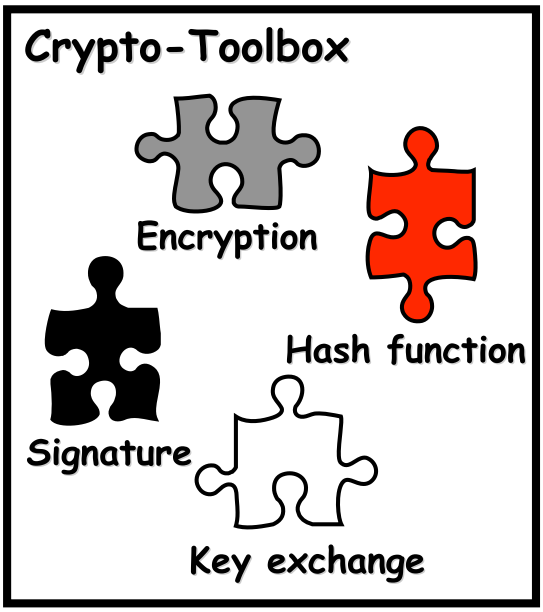
Cryptography: The Details



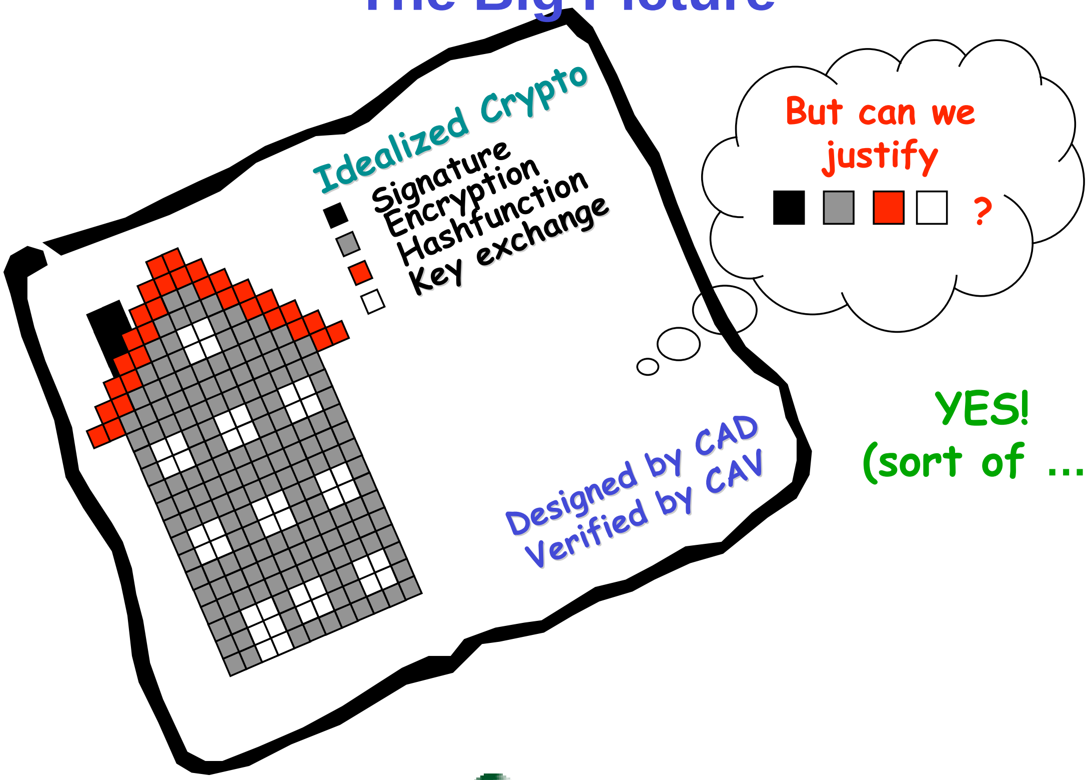


IBM Research

Cryptography: The Details



Prior Automated Crypto Protocol Proofs: The Big Picture



YES!
(sort of ...)

E.g.: Secure Channels like SSL

(with mutual authentication)

- If you use them in a larger system, what would you assume about them, or how would you model them?
- E.g., as "ideal secure channel"

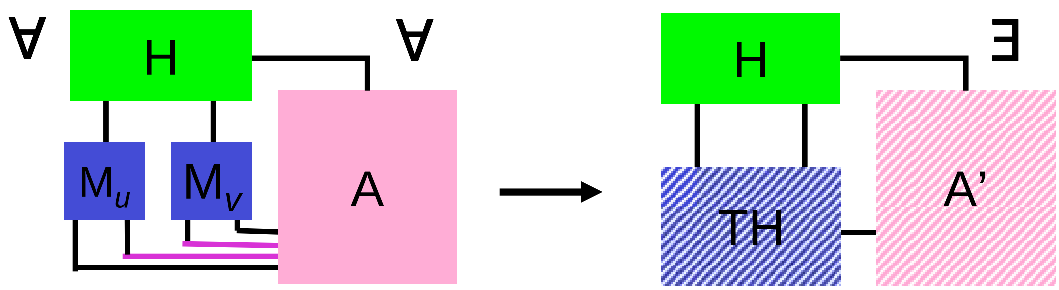
- E.g., as a primitive in π-calculus etc.

Secure Channels, ctd.

- **How correct is this compared with actual SSL?**
- **Not bad, but not quite correct:**
  - **Computational assumptions and error probabilities from crypto** } **Always very similar ⇒ make part of semantics ("fulfillment" relation)**
  - **Message length and traffic pattern leak** } **Special ⇒ extend specification**
  - **No availability** } **Rather general ⇒ can just be in asynchronous model**

Reactive Simulatability (RSIM)

Here "General RSIM" variant

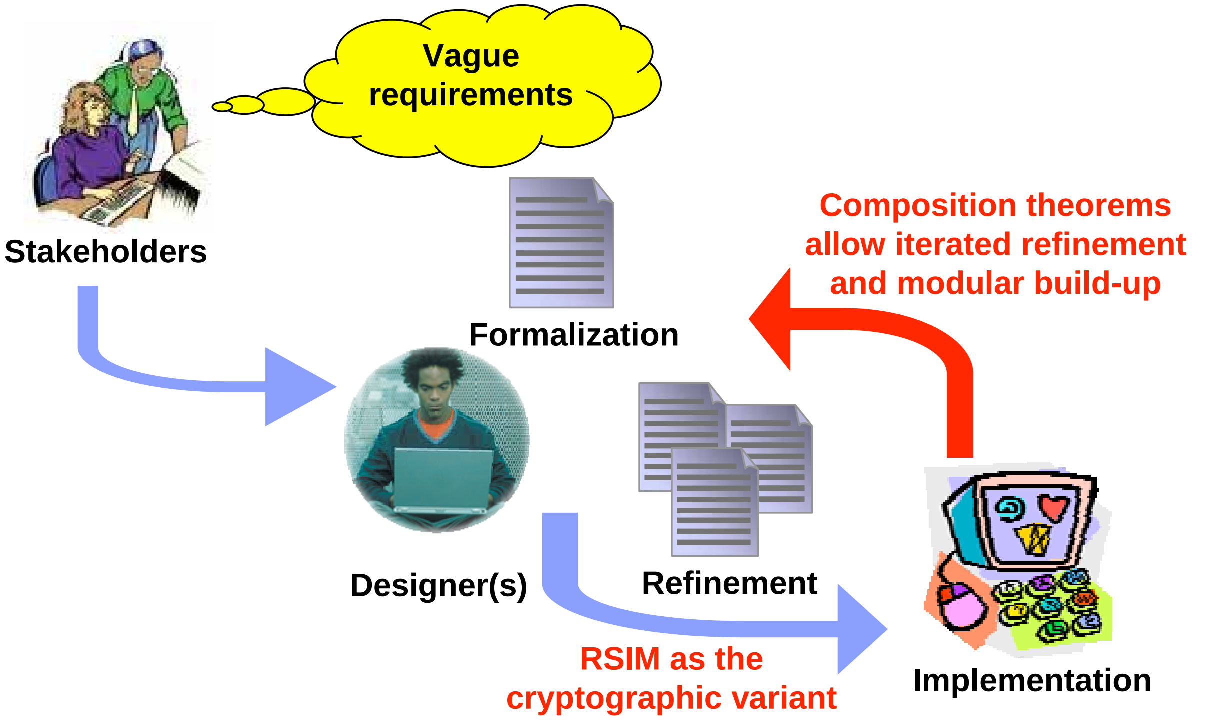


Real system **Ideal system**

$$\text{view}_{real}(H) \approx \text{view}_{ideal}(H)$$

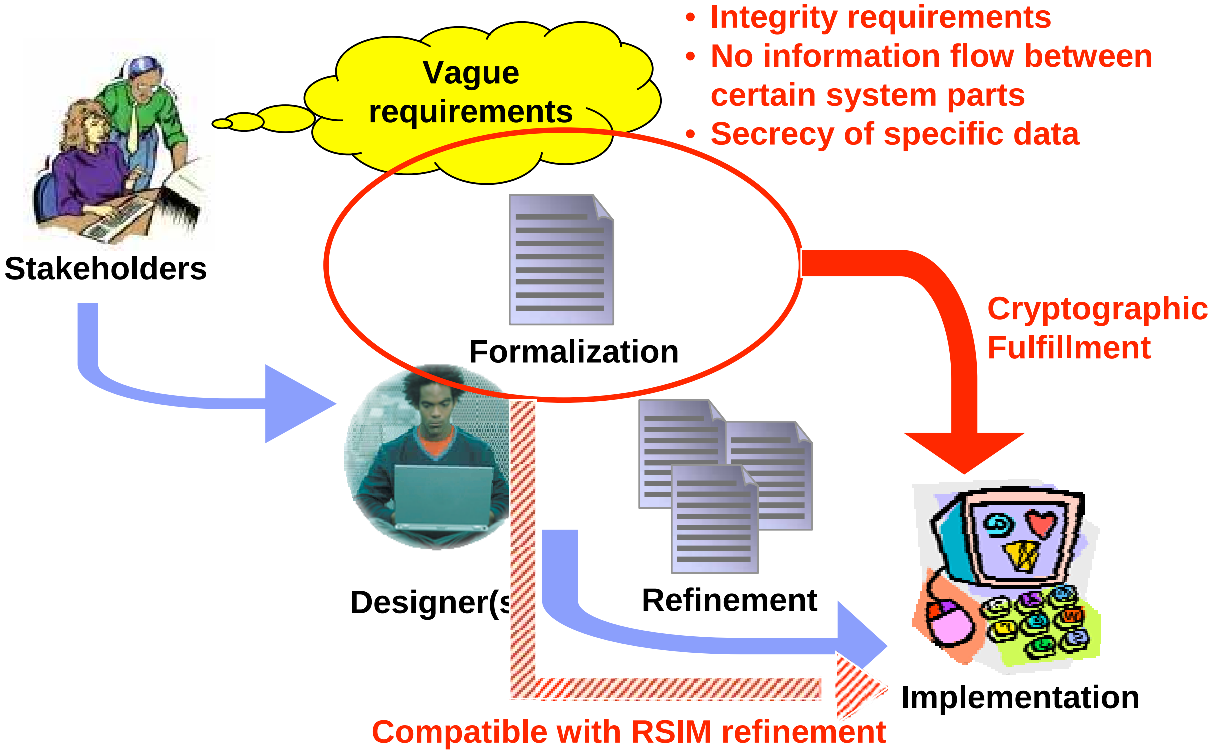
Indistinguishability of random variables

RSIM in Overall Design Process



Treating Properties Cryptographically

- Integrity requirements
- No information flow between certain system parts
- Secrecy of specific data



Recent Work

- Extended prior results for “Dolev-Yao models” – specific term-algebra abstractions widely used in verification community
- Impossibility results for certain Dolev-Yao model variants
- BPW-Dolev-Yao model in Isabelle/HOL (with Ch. Sprenger and D. Basin)
- Attempt to apply to real-world Web Services