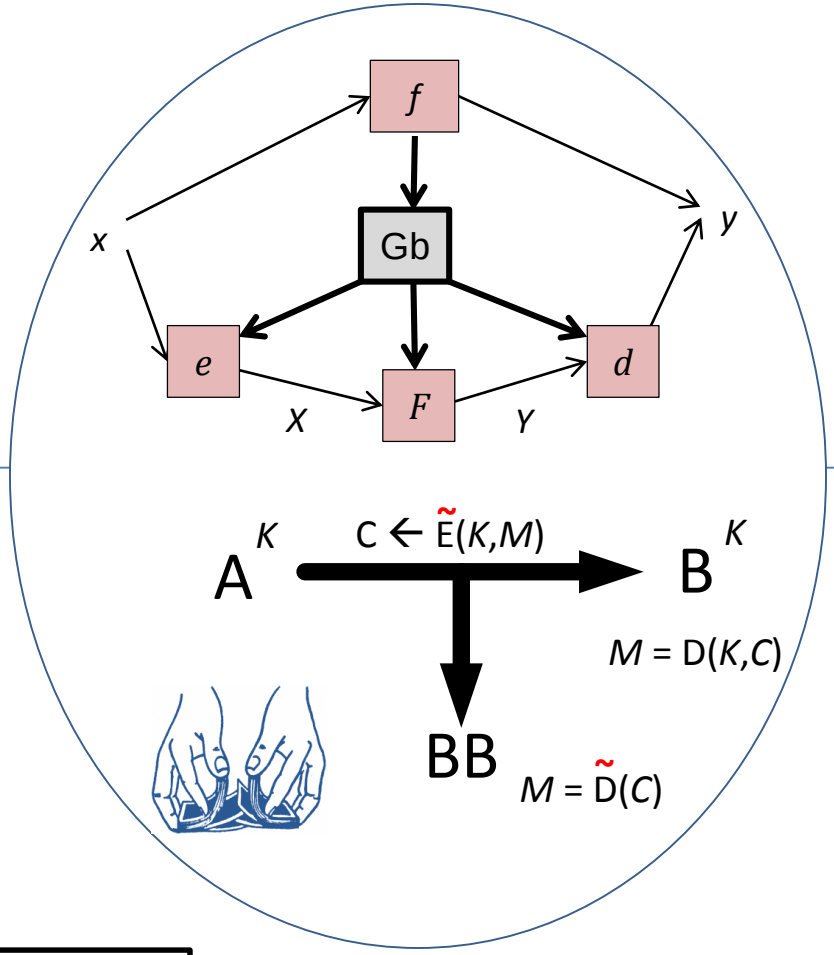
Deconstructing Encryption

Challenge:

- Numerous “kinds” of encryption can be devised. Can “exotic” encryption be made useful to cryptographic practice?

Solution:

- Use **practice-oriented provable security** to invent / deconstruct new kinds of encryption.
- Formalize **circuit garbling** and make faster techniques for it
- Find new techniques for **FPE** (format-preserving encryption)
- Formalize **algorithm-substitution attacks** to address mass-surveillance threat
- Introduce **UCE** (universal computational extractors) as an alternative to the random-oracle model (ROM)



Scientific Impact:

- Garbled circuits transformed from a technique to first-class security notion
- First workable alternative to the ROM
- New notions and schemes for robust and online authenticated encryption

Broader Impact:

- Expansion of the scope of utilized cryptography
- Increased sensitivity to the technical and social power implicit in cryptographic techniques

TWC: Medium: Collaborative: Deconstructing Encryption
#1228828 Phillip Rogaway – UC Davis
#1228890 Mihir Bellare – UC San Diego