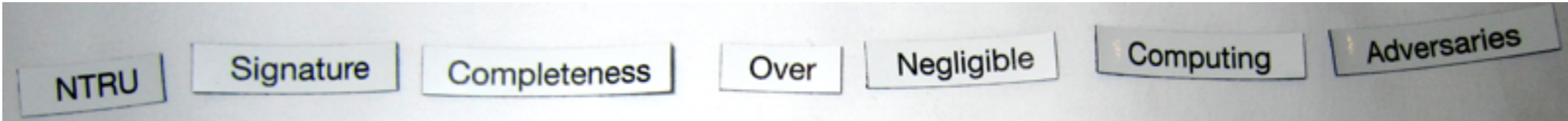# Event Announcement: FridgeCrypt 2013
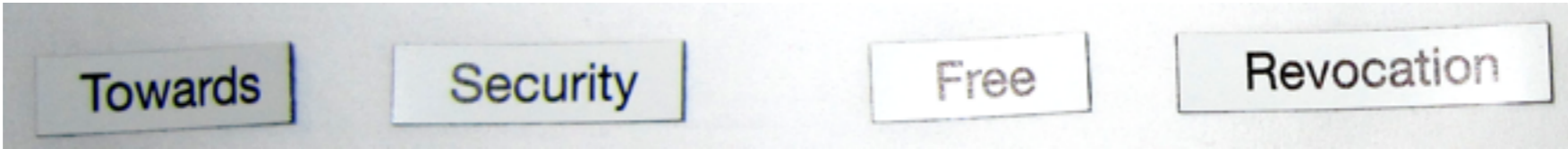
Jon Callas, Tamzen Cannoy, and Nicko van Someren
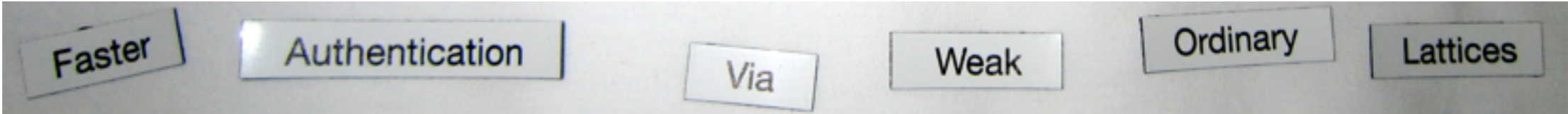
1

# CFP for FridgeCrypt

- Topics have all been selected

- Call for papers to match the titles

# Public Key Cryptography

- NTRU  Signature  Completeness  Over  Negligible  Computing  Adversaries

- Towards  Security  Free  Revocation

- Faster  Authentication  Via  Weak  Ordinary  Lattices

3

# Buzzword-Compliant Cryptography

- Quantum  Algorithms  From  Almost  Fully  Homomorphic  Hash  Functions

- Non  Adaptive  Side  Channel  Threshold  Indifferentiability

- Statistical  Polynomial  Storage  Based  Interactive  Applications

4

# Invited Talk

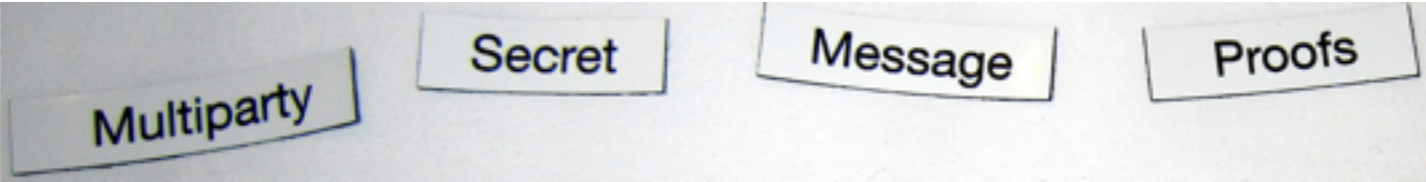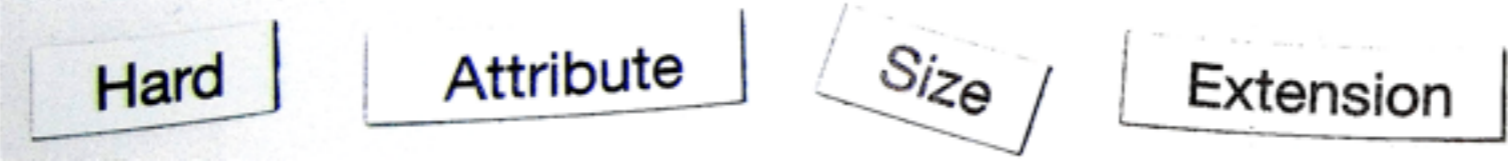- Come up with an appropriate talk, and we'll invite you!
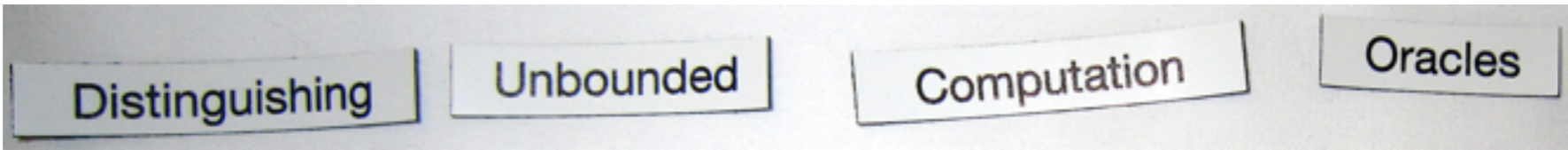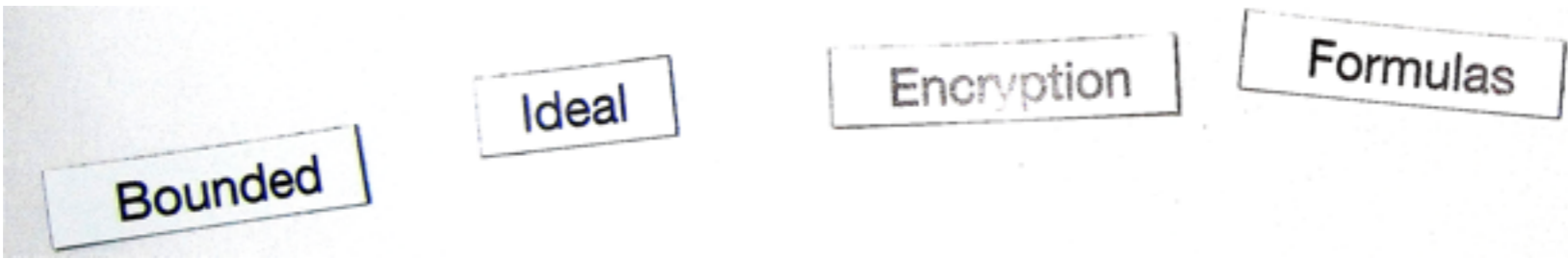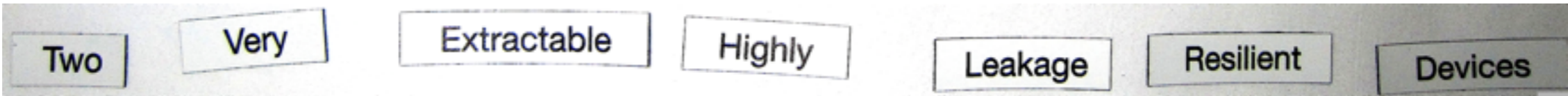
5

# Social Aspects of Cryptography

# Hardware

- Beyond | Limitations | With | Compact | Nanoscale | Issues

- Improved | Formal | Knapsacks | Without | Output | Noise | Amplification

- Probability | Limits | And | Pseudo | Power | Leaking | Cryptosystems

7

# Spam and Email Security

- Multiparty Secret Message Proofs
- Hard Attribute Size Extension
- Careful Study Of The Optimum Model Curves

8

# Boundaries

- Distinguishing  Unbounded  Computation  Oracles

- Ideal  Encryption  Formulas  Bounded

- Two  Very  Extractable  Highly  Leakage  Resilient  Devices

9

# Cryptanalysis Implementations

- Linear DDH Attacks On AES

- An Independent Framework Implementing Random Cryptanalysis

- A Public HIBE Detection Implementation In Scheme

# Other Details

- Talks will be selected, then location and dates