On the Leakage of Zero-Knowledge

Jon Callas, Tamzen Cannoy, Nicko van Someren

Leakage is a Hot Topic

Leakage is a Hot Topic

Leakage-Resilient
Pseudorandom Functions
and Side-Channel Attacks
on Feistel Networks

Leakage is a Hot Topic

Leakage-Resilient
Pseudorandom Functions
and Side-Channel Attacks
on Feistel Networks

Gulf oil leaks exceeds
BP's 'worst case
scenario'

Leakage is a Hot Topic

Leakage-Resilient Pseudorandom Functions and Side-Channel Attacks on Feistel Networks

Continual Leakage in the Only-Computation Leakage Model

Gulf oil leaks exceeds BP's 'worst case scenario'

Leakage is a Hot Topic

Leakage-Resilient Pseudorandom Functions and Side-Channel Attacks on Feistel Networks

Continual Leakage in the Only-Computation Leakage Model

Gulf oil leaks exceeds BP's 'worst case scenario'

WikiLeaks set to release 15000 documents on Afghan war

Our Previous Work

- “The Oblivious Transfer of Zero-Knowledge” [CC&vS, Crypto 2004]
- Protocol to let Alice prove Bob doesn’t know Jack

Colluding with the Dishonest Majority

- What if Bob and Jack have been conspiring against Alice?
- Bob *does* know Jack, he’s actually Jack’s brother.
  - They have been hiding this for years.
  - Now they want to securely leak this knowledge

First Attempt

- Use a Dissociative Probablistically-Checkable Proof model
- Fails for two reasons:

1. Method would reveal a dirty secret of Jack's that he wants to keep from Alice
2. PCP is illegal in the US because of its dissociative properties

Next Attempt

- Bob and Jack convince Alice to play a game of Mental Solitaire with the Queen of Hearts under Continuous Side-Channels

Jack’s Game

- Jack proves to Alice that the Queen of Hearts is her real mother without telling her who her real father is
- The Queen of Hearts proves to Alice that Jack knows Bob, and Bob knows Jack because Bob is Jack’s brother

Zero-Knowledge Leaks

- Unfortunately, the Queen's proof that proves Bob knows Jack is not truly ZK because it leaks Jack's dirty secret

Semantically Insecure Protocols

- The leak occurs at the conclusion of the proof.
- Instead of finishing with QED, she reveals…

…Bob’s your Uncle!