I. Background: DNS Cache Poisoning Attack

- **Attack Scenario**: 
  1. Attacker sends DNS queries to the resolver with spoofed IP addresses.
  2. Responder returns IP addresses to the resolver, which are then cached.
  3. Attacker sends UDP probes with spoofed IP addresses to the resolver.

- **Impact**: Traffic hijacking, phishing & scams, fake certificate issuance, etc.

II. Challenges

- **UDP Probes**: UDPS with guessed dst port #
  - **UDP Verification**: UDP destined to a known closed port (e.g., port 1)

- **ICMP Transmission**: Reduce counter by 1
  - Empty counter = no ICMP transmission

III. Side Channel

- **Revolution**
  - No open port
  - Attacker NS
  - Victim Resolver NS
  - Global Counter = 50

- **UDP Probes**: 50 UDP probes
  - 50 closed ports
  - Global Counter = 50

- **ICMPs**: 49 ICMPs
  - UDP Verification: UDP destined to a known closed port (e.g., port 1)

- **UDP Probes**: UDPS with guessed dst port #

- **UDP Verification**: UDP destined to a known closed port (e.g., port 1)

IV. Evaluation

- **Real World Attacks**
  - **Revolution**
    - Victim Resolver: Tsinghua
    - Commercial
    - # of backend servers: 2, 4
    - # of NS: 2, 1
    - Jitter: 3ms, 2ms
    - Delay: 20ms, 30ms
    - Loss: 0.2%, 0.6%
    - Success Time: 15 mins, 2.45 mins
    - Success Rate: 5/5, 1/1

- **Resurrection**
  - Victim Resolver: Controlled
  - # of backend servers: 1
  - # of NS: 2
  - Jitter: 3ms
  - Delay: 40ms
  - Loss: 0.2%
  - Success Time: 6.83 mins
  - Success Rate: 20/20