Fault Attacks on Seed Pointers and Their Effects on Post-Quantum Algorithms

Hariprasad K V[1, 2], Prasanna Ravi[4,5], Shivam Bhasin[2,3]

[1] School of Physical and Mathematical Sciences, Nanyang Technological University, Singapore
[2] Temasek Laboratories, Nanyang Technological University, Singapore
[3] National integrated Centre For Evaluation, Nanyang Technological University, Singapore.
[4] College of Computing and Data Science, Nanyang Technological University, Singapore.
[5] PQStation, Singapore.

Motivation

Modern post-quantum cryptographic designs, rely on a short, initial random seed. This seed is typically hashed to generate almost all the randomness needed for critical operations like key generation, data encapsulation, or digital signing. **This turns the random seed into a single point of failure.** Therefore it is critical to assess the random seed's susceptibility to fault-injection attacks and to devise robust countermeasures.

Pointer Redirection Fault

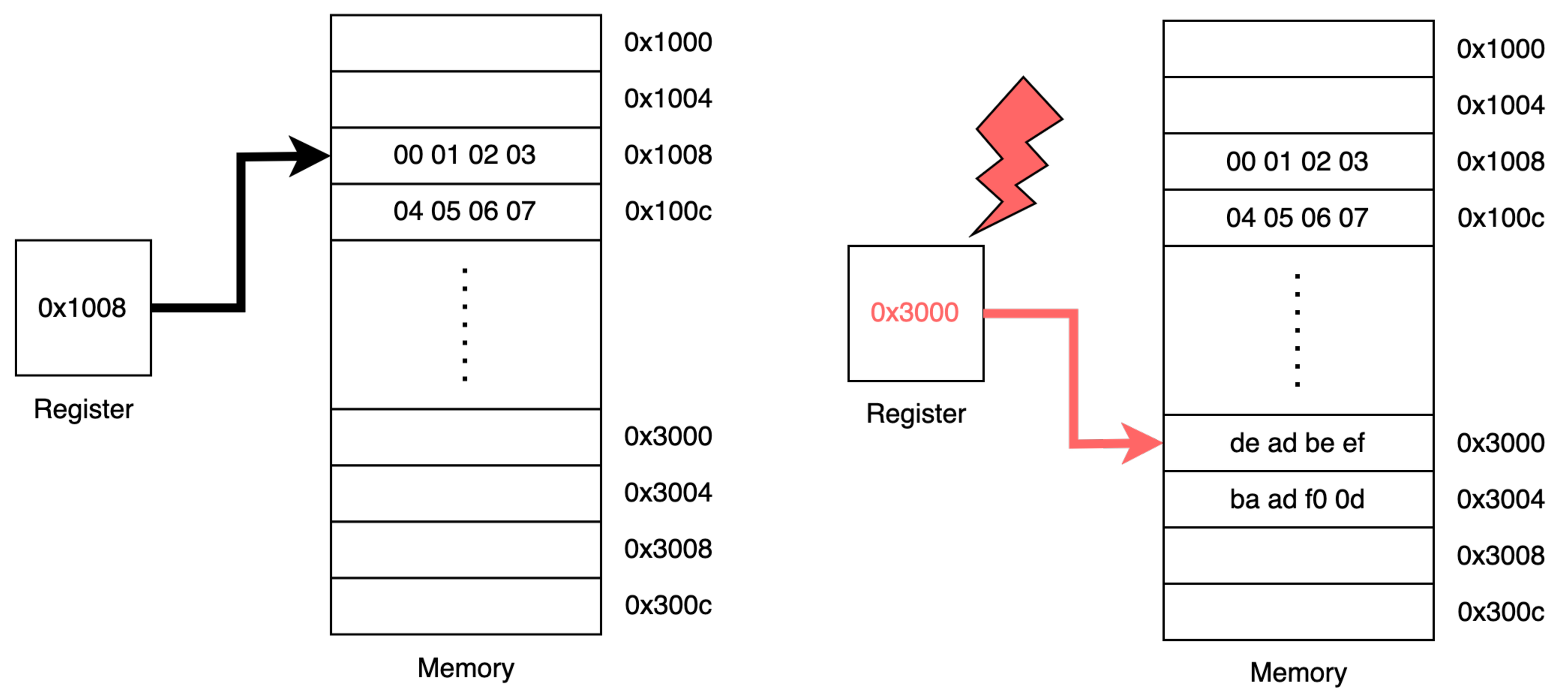

Fig. 1: **Pointer Redirection Fault**

The attack target is a single pointer register which modifies the content during the initialization, causing all later accesses to reference a different address while the program logic remains untouched.

Fault Models

1. **FM-1: Instruction-skip on Addition**
   Model: $out \leftarrow inp + c \;\Rightarrow\; out^{\star} \leftarrow inp.$
   Effect: Pointer initialized with base address instead of the offset.
2. **FM-2: Redirect to zero-filled memory**
   Model: $out^{\star} \leftarrow addr_Z$, ($addr_Z \Rightarrow$ predictable bytes like `0x00` / `0xFF`)
   Effect: Data becomes low-entropy/known. Further algotihm becomes deterministic.
3. **FM-3: Redirect to constant memory**
   Model: $out^{\star} \leftarrow addr_C$, ($addr_C \Rightarrow$ Constant Data)
   Effect: Removes randomness of an algorithm across iterations.

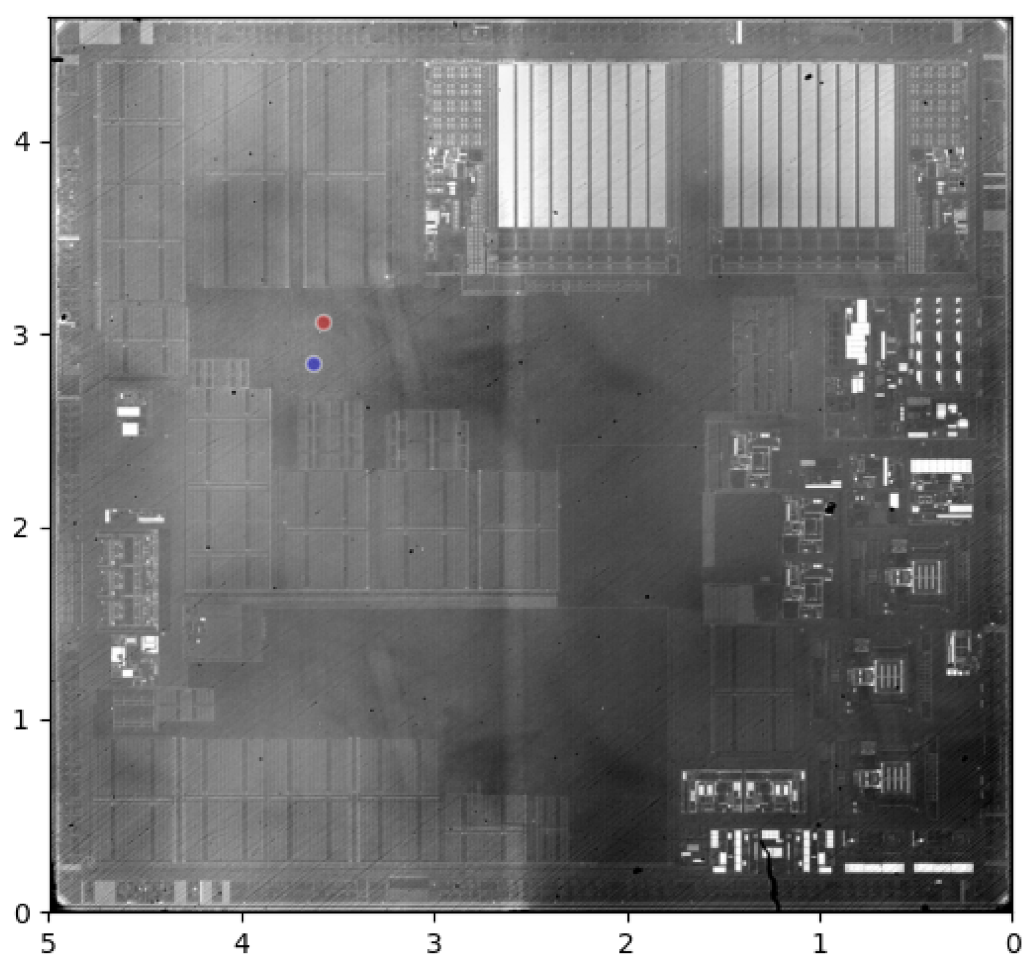

Fig. 2: **Locations of reliable Laser Fault Injection on STM32H7 Microcontroller**

Experiment Setup

Main Attack vector is Laser Fault Injection. The setup includes:

1. **Laser:** Alphanov dual spot laser fault injection setup. 980 nm laser is used for experiments.
2. **DUT**: STM32H753ZIT Microcontroller with ARM Cortex-M7.
3. Oscilloscope, Relay and software for Setup synchronization.

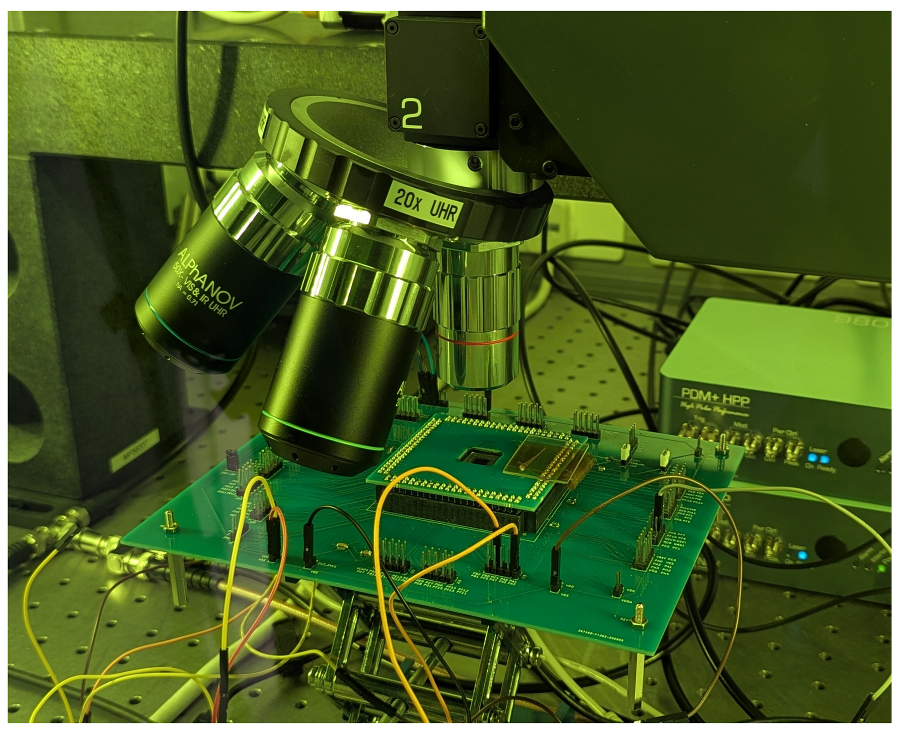

Fig. 3: **Experiment Setup**

Attacks on ML-KEM

The mentioned fault models were applied on PQM4 implementations of ML-KEM and ML-DSA

ML-KEM:

1. **FM-1**: Skips the add instruction on `noiseseed` initialization, `noiseseed = buf + KYBER_SYMBYTES`
2. **FM-2**: Redirect `coins` at memcpy to zero-filled region, leading to a predictable secret key. Message recovery is is also possible using a MITM attack.
3. **FM-3**: Redirect `noiseseed` to constant data. Key Recovery using differential attack.

```
void indcpa_keypair(unsigned char *pk,
                    unsigned char *sk,
                    const unsigned char *coins){

    unsigned char buf[2 * KYBER_SYMBYTES];
    unsigned char *publicseed = buf;
    unsigned char *noiseseed = buf + KYBER_SYMBYTES;    FM1, FM3

    memcpy(buf, coins, KYBER_SYMBYTES);                 FM2
    buf[KYBER_SYMBYTES] = KYBER_K;
    hash_g(buf, buf, KYBER_SYMBYTES + 1);
    // ...
    // Remainder of function
}
```

Fig. 4: **ML-KEM PKE key generation seed initialization**

Attack	Pulse width (ns)	Power (%)	Offset (ns)	Repeat. (%)
FM-1	25	45	769	93.2
FM-2	25	55	991	100
FM-3	22.5	50	718	100

Tab. 1: **Laser parameters and success rate for each attack**

Future Works

1. Extend the attack to signature schemes like ML-DSA, and code based KEMs.
2. Design low-cost countermeasures like seed sanity check, seed blacklist.
3. Explore other potential targets affected by the pointer redirection.

Learn more about this work