Number theory and side-channel attacks from normalized running time distributions

PI: Stephen D. Miller, Department of Mathematics, Rutgers University

http://www.math.rutgers.edu/~sdmiller

The underlying mathematics of many cryptosystems is often:

- Number theory (e.g., RSA, Elliptic Curves, Isogenies....)
- Lattices (e.g., NTRU, post-quantum crypto)

Question how much of the *identity* of an algorithm is leaked by side-channel information

- Can we tell if weak key generation is being used to cut corners?
- Can we detect a man-in-the-middle attack from timing information

Motivation: ROCA (**R**eturn **o**f **C**oppersmith **A**ttack) attack on Infineon smart cards/TPMs

- uses lattice methods to attack weak RSA keys
- Infineon's closed-source RSALib contained a fast prime generator which samples a small subset of primes (low entropy).

Problem: How to detect such weaknesses without the source code?

Potential impact: design statistical tests using side-channel information to detect substandard key generators.

- more generally, want to detect if an algorithm is behaving differently than advertised
- Potential applications to threat detection

Running time alone is not enough: may not know implementation or hardware speeds

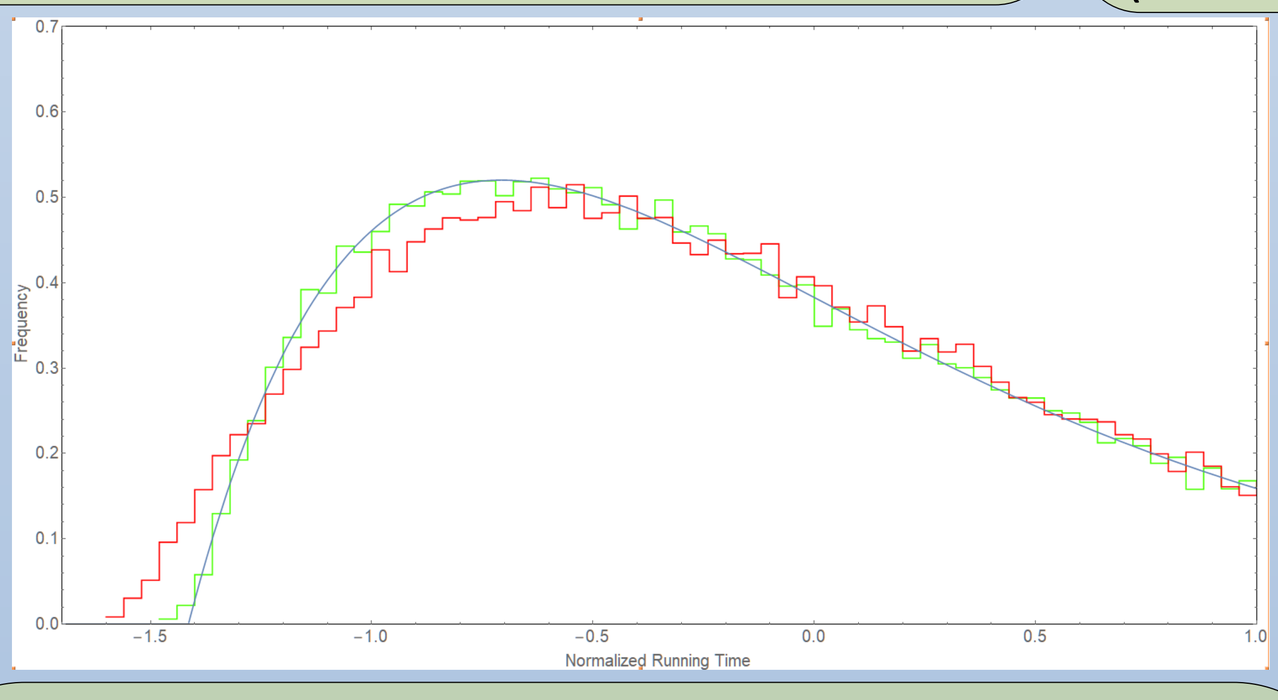
Methodology (Deift-Miller-Trogdon):

Instead of raw times, look at its fluctuations.

Notion of *"time-signature":* the histogram of running times, normalized to have *mean 0 and standard deviation 1.*

Successful experiment:

Time signatures can distinguish 512-bit RSA keys made from uniformly-distributed primes (green) vs. a simulation of Infineon's weaker keys (red) (black curve = theoretical approximation).



Potential impacts: What else can time-signatures be used to detect?

Should be applicable to some threat detection situations

- Distinguish between slow equipment and interference by an adversary
- Example: Diffie-Hellman has a different time-signature when there is a man-in-the-middle
- Would like to detect intrusions from this essential *shape* of side-channel data.

Broader impacts

Infineon's bug had major effect: 750,000 digital ID cards were recalled in Estonia.

Time-signatures are a potential tool to identify bad algorithms (without knowing them).

Many implementations of RSA exist. It is important to be able to tell them apart from the keys (if possible), in case a weakness is discovered in one.

Hope to identify sources of weak keys.

SaTC Award CNS-1815562