

PINPAS: Simulating side channel attacks on smartcards

Jerry den Hartog

Technische Universiteit Eindhoven

Content

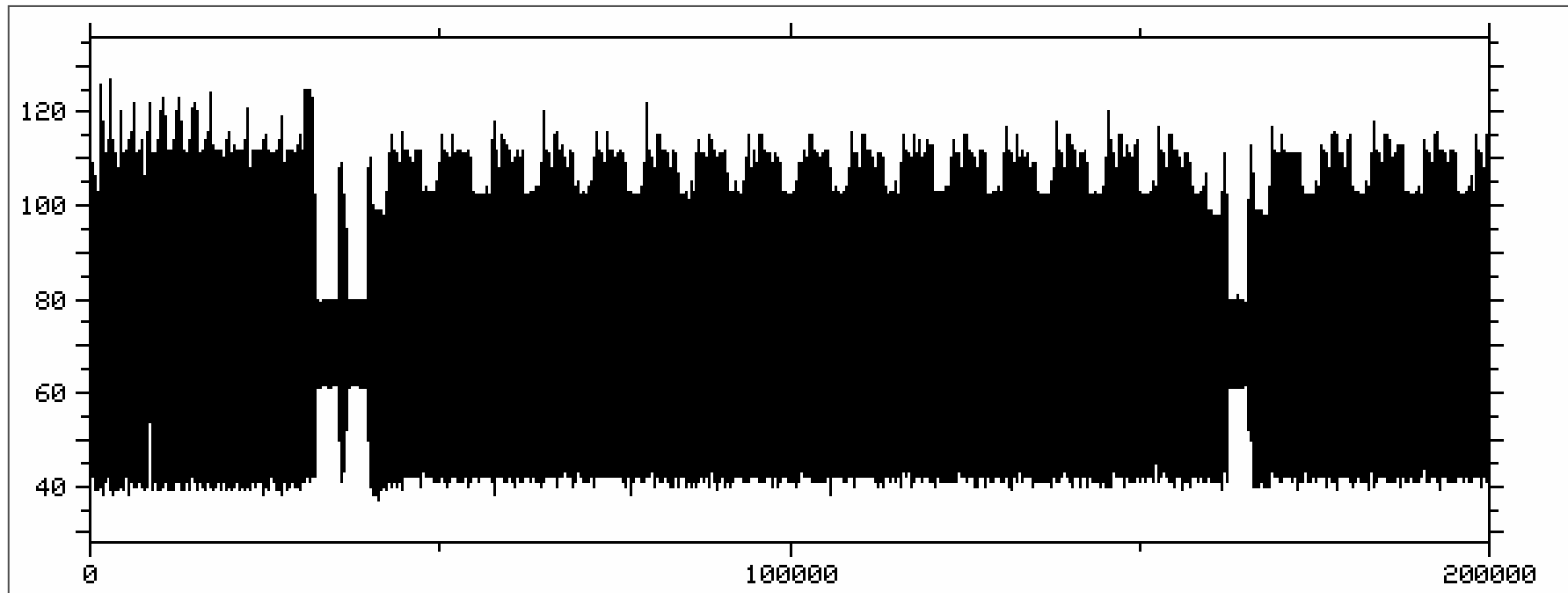
- Introduction
- Power Analysis
- DPA
- PINPAS tool
- Demonstration
- Conclusions

Introduction: The PINPAS Project

- Program INferred Power Analysis in Software
- Partners:
 - TNO-TPD (Jan Verschuren, Jaap de Vos)
 - TU/e (Jerry den Hartog, Erik de Vink)
- Detect DPA possibilities in an early stage.
- Use of simulation:
 - No card needed.
 - Quickly test algorithms and countermeasures.

Power Analysis (1)

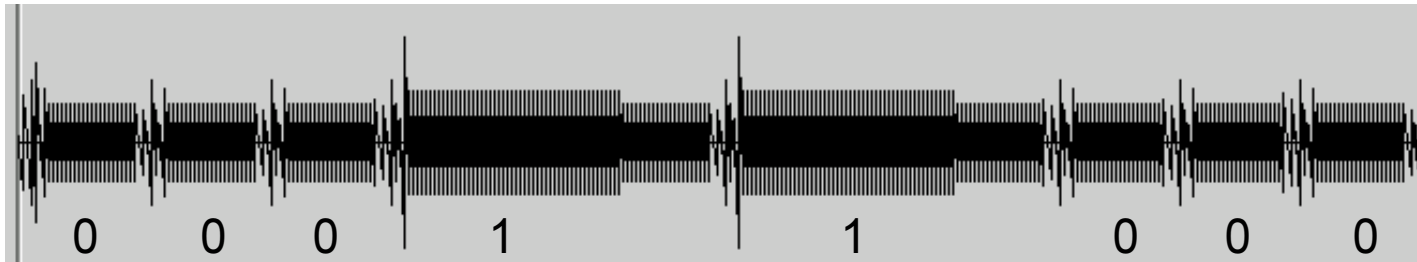
Measure Power Consumption (*power trace*):



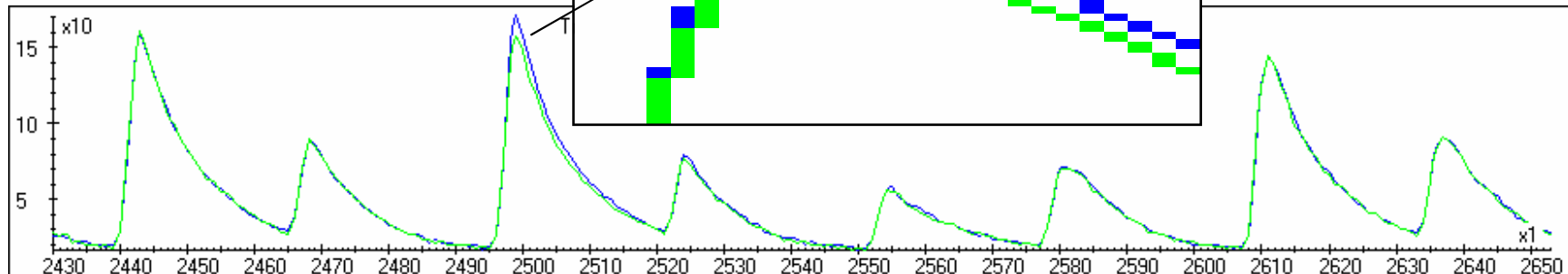
Power Consumption in DES.

Power Analysis (2)

- Simple power analysis
 - Timing

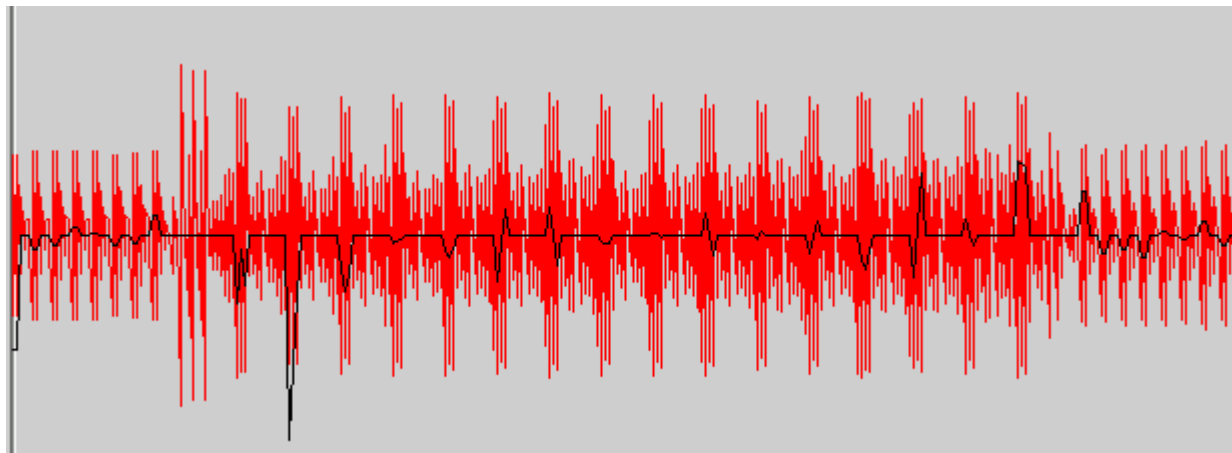


- Power consumption of simulated data: 1 uses more power than 0



Differential Power Analysis (DPA)

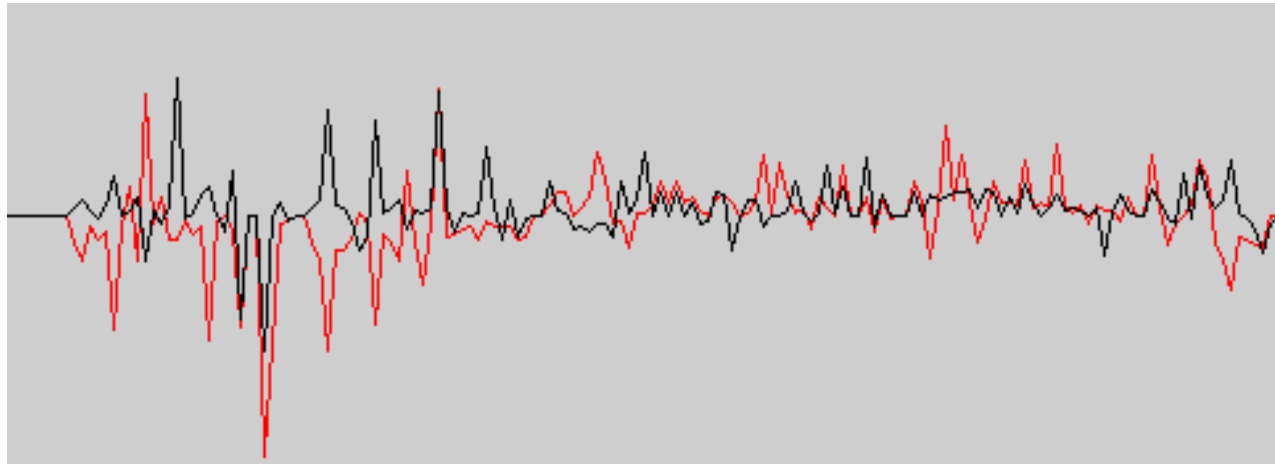
- Generate lots of traces
- Predict value & use to split traces
- Compare average power consumption (*difference trace*)
- Difference if value predicted correctly



Recognizing second input byte in start of AES

Extracting keys with DPA

- Find intermediate value which depends on **part** of the key
- **Guess** a value of this part of the key
- Calculate value using guess
- Correct guess will show a difference
- Incorrect guess will not



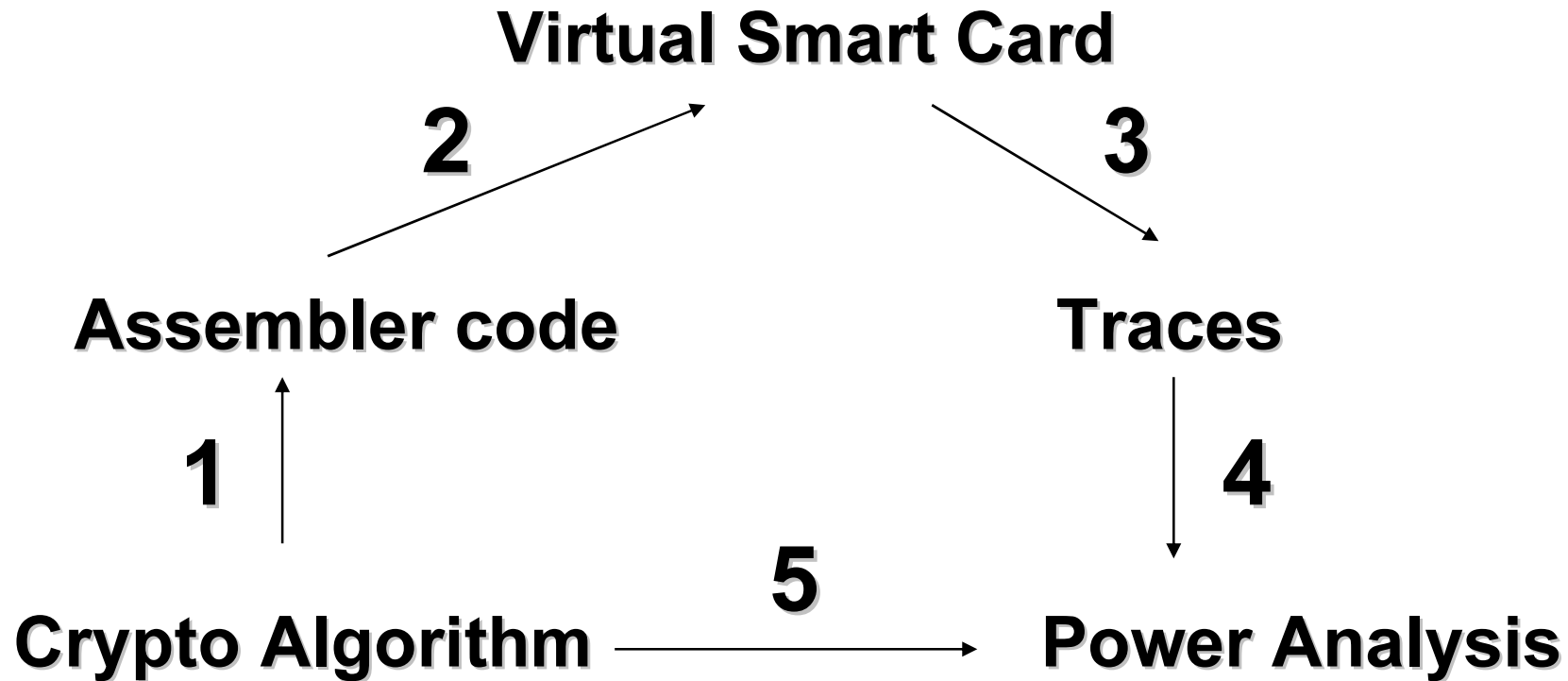
Example: AES (Rijndael)

- Symmetric cipher 128 bits key (i.e. 16 bytes)
- First round starts with:

```
void AddRoundKey()  
{  
    for( i = 0; i < 16; i++ )  
    {  
        inputdata[ i ] = inputdata[ i ] ^ key[ i ];  
    }  
}
```

- Intermediate value: $\text{input}[i] \wedge \text{key-guess}$.
(Need to check 256 possibilities.)

PINPAS Tool



- Simulation of program on smart card
- Simulated power traces
- DPA based on algorithm

PINPAS TOOL: Flexibility

- Choice in program
 - Different algorithms
 - Different implementations (software defenses)
- Choice in simulator
 - Work with different cards
 - Alter or extend existing simulation (hardware defenses, coprocessor)
- Choice in leakage profile
 - Simulate different side channels

Demonstration.

Conclusions

- Power analysis poses threat to security smart card.
- PINPAS Tool: Simulation to test in early development stages
 - Can test hardware and software defenses.
- Can extend to other side channel attacks.
- Tests done with e.g. DES, AES, RSA.