# 1. Acquisition Platform

## 1.1 Oscilloscope

1) Oscilloscope type
   - RIGOL DS6000 Series Digital Oscilloscope
2) Oscilloscope features
   - Bandwidth 1 GHz, 600MHz
   - Sample rate up to 5 GSa/s
   - Standard 140 Mpts deep memory
   - Capture rate up to 180,000 waveforms per second
   - Waveform recording up to 180,000 frames
   - Build-in 1GB flash memory

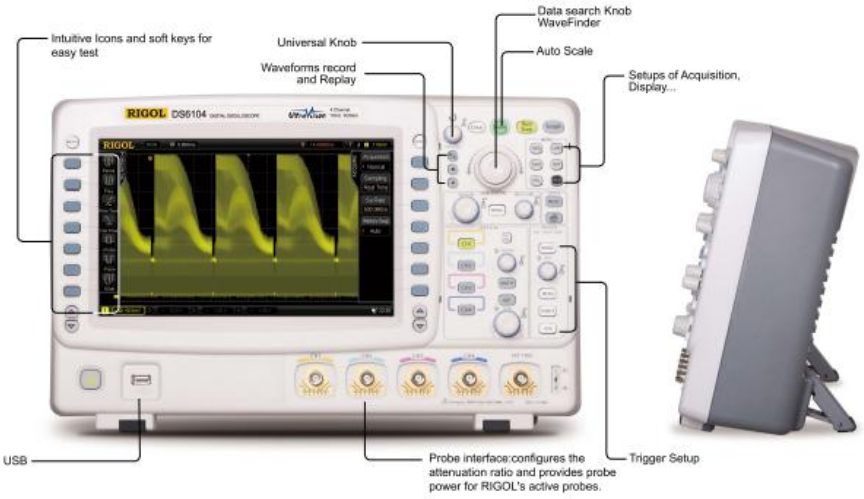


Fig.1.1. RIGOL DS6000 Series Digital Oscilloscope

3) Complete connectivity
   - External trigger((Front Panel)
   - Trigger output and calibration signal output
   - 10MHz In/Out: 10MHz reference clock In/Out
   - VGA: Connect to an external monitor or projector
   - LAN: For remote control(LXI-C compliant)
   - USB: 2 USB HOST ports and 1 USB DEVICE port, provide PC, Flash drive , and printer connectivity
   - Supports the optional USB-GPIB adapter


Fig.1.2. Connectivity of RIGOL DS6000

## 1.2 Probes

The probes supported by DS6000 series are shown in Table.1.1.

Table.1.1. The probes supported by DS6000 series

| Model Number | Attenuation Ratio | Bandwidth | Input R | Max.Input voltage | Recommended applications |
|---|---|---|---|---|---|
| RP2200 | 1:1 or 10:1 | 1X: DC~7 MHz | 1X: 1MΩ ±2% | 1X: CAT II 150 V AC | Small signal test (1X) |
| | | 10X:DC~150 MHz | 10X: 10 MΩ±2% | 10X: CAT II 300V AC | General purpose test |
| RP3300 | 1:1 or 10:1 | 1X: DC~8 MHz | 1X: 1 MΩ ±2% | 1X: CAT II 150 V AC | Small signal test (1X) |
| | | 10X:DC~350 MHz | 10X: 10 MΩ±2% | 10X: CAT II 300V AC | General purpose test |
| RP3500 | 10:1 | DC~500 MHz | 10 MΩ±2% | CAT II 300VAC | General purpose test |
| RP5600 | 10:1 | DC~600 MHz | 10 MΩ±2% | CAT II 300VAC | General purpose test |
| RP6150 | 10:1 | DC~1.5 GHz | 500 Ω±10 Ω | CAT I 10VAC | High frequency single ended small signal test |
| RP1300H | 100:1 | DC~300 MHz | 100 MΩ | CAT I 2000V (DC+AC), CAT II 1500 V (DC+AC) | High voltage test |
| RP1050H | 1000:1 | DC~50 MHz | 10 MΩ±0.5% | DC: 0~15KV DC<br>AC: pulse <=30 KVp-p<br>AC: sine wave <=10 KVrms | High voltage test |
| RP7150 | 10:1 | DC~1.5 GHz | Differential mode: 50 kΩ±1%<br>Single ended mode: 37 kΩ±1% | 30V Peak, CAT I | Differential /Single ended high frequency signal test |

The probe we use in the experiment is RP5600 600MHz Passive Probe, as Fig.1.3.

Fig.1.3. RP5600 600MHz Passive Probe

The specific information about the oscilloscope and probe can be found at [11].

# 2. Post Processing Methods

## 2.1 First Processing Method

The method was proposed in [1], the paper illustrated the temporal misalignment side channel signals as Fig.2. 1.

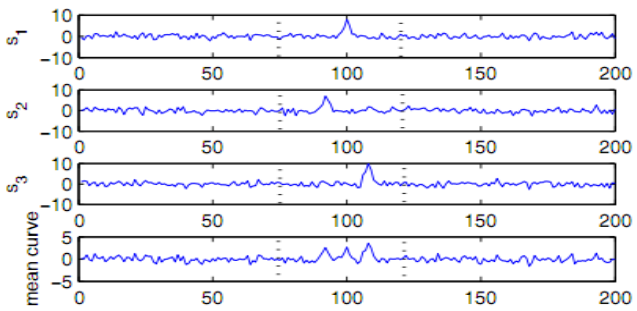


Fig.2. 1. Misaligned signals

The processing method firstly divides the power traces into many segments with same length and we should compute the energy of each segment. The samples of each segment will be replaced by its energy as illustrated in Fig. 2.2.

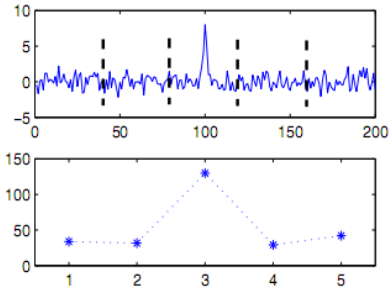

Fig. 2.2. Original and energy signals

The algorithm is summarized as follow

S = original signal, m = length(S), L= length of segments, EBS = EnergyBasedSignals(S)
For I from I to m/L
    beginSegment = ((i-1)*L+1,endSegment = i*L,
    segment(i) = S(beginSegment : endSegment),
    EBS = <segment.segment>
End
Return ESB

The paper did not mentions clearly how to divide the power trace and how to compute the energy of each segment, which could be consider as the most important part of the method. In fact, the length of each segment is related to the sampling frequency of the Oscilloscope and the operating frequency of the chip. Once we can divide the power trace into the segments correctly, the method is effective to enhance Side Channel Analysis. Our experiments are shown below.

In order to compare the effect after processing, We applied MIA[2] on subkey of the first round with both the original traces and the processing traces.

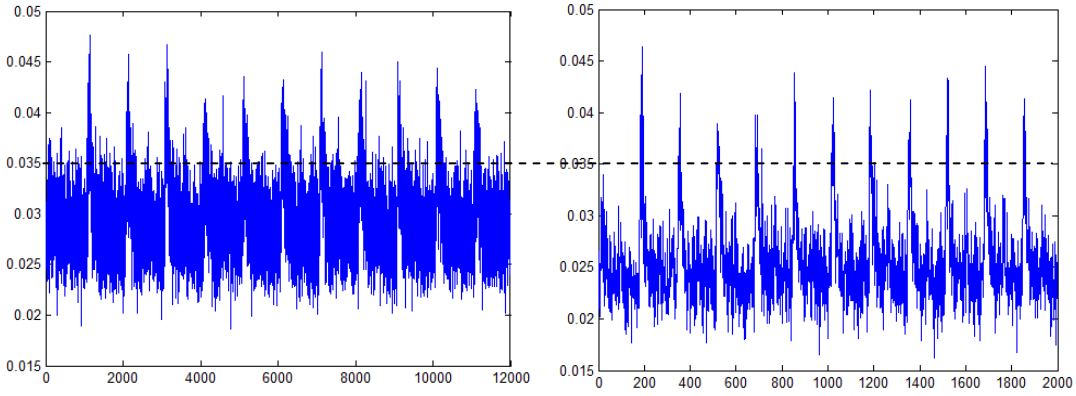


Fig. 2.3. MIA attack with 5000 traces(left: the original traces; right: the post-processing traces)

From the Fig. 2.3, we can see that the processing method can reduce the noise of the power trace. But the spike on the position we attack( the output of the s-box on first round) are almost the same. In addition, it is too difficult to divide the power traces into segment accurately. In this case, we do not choose this method to complete elastic alignment.

## 2.2 Second Processing Method

This method was proposed by Jasper G.J. van Woudenberg in 2011[3], he used the FastDTW[4] to achieve elastic alignment.

The method firstly obtains the warp path of the reference trace and the trace without alignment. The example of warp path is shown in Fig. 2.4.

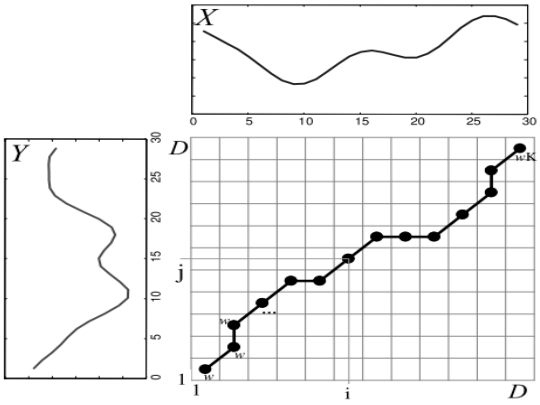


Fig. 2. 4. Example warp path for trace X and Y

We define a warp path F for trace X and Y:

$$F = (c(1), c(2), \dots, c(K)) \tag{1}$$

$c(k) = (x(k), y(k))$ indexes in X and Y respectively.

In order to find out the minimum cost warp path, we should firstly calculates the distances between all samples of X and Y, as follow.

$$d(i,j) = |X[i] - Y[j]| \tag{2}$$

To simplify the algorithm, we drop the subscript $k$ and define the following equations.

$$g(1,1) = 2d(1,1) \tag{3}$$

$$g(i,j) = \min\{g(i,j-1) + d(i,j), g(i-1,j) + d(i,j), g(i-1,j-1) + 2d(i,j)\} \tag{4}$$

To avoid boundary problems, we define $d(i,0) = d(0,j) = \infty$. After we get the g(i,j), we can find out the minimum warp path. A example is given below.

Trace X and Y:

| | | | | | |
|---|---|---|---|---|---|
| X | 1 | 1 | 2 | 3 | 4 |
| Y | 1 | 2 | 3 | 4 | 4 |

Calculating d(i,j) and g(i,j):

$d(i,j)$

| | | | | | |
|---|---|---|---|---|---|
| | 3 | 3 | 2 | 1 | 0 |
| | 3 | 3 | 2 | 1 | 0 |
| $i \uparrow$ | 2 | 2 | 1 | 0 | 1 |
| | 1 | 1 | 0 | 1 | 2 |
| | 0 | 0 | 1 | 2 | 3 |
| | | | | | $j \rightarrow$ |

$g(i,j)$

| | | | | | |
|---|---|---|---|---|---|
| | 9 | 9 | 5 | 2 | 0 |
| | 6 | 6 | 3 | 1 | 0 |
| $i \uparrow$ | 3 | 3 | 1 | 0 | 1 |
| | 1 | 1 | 0 | 1 | 3 |
| | 0 | 0 | 1 | 3 | 6 |
| | | | | | $j \rightarrow$ |

Computing the minimum warp path:

F=((1,1),(2,1),(3,2),(4,3)(5,4), (5,5));

If we use DTW algorithm, the complexity will be high to achieve elastic alignment(O(N*N)). In this case, we can divide the power trace into several segments if we choose DTW algorithm. And to achieve elastic alignment for each segment with DTW.

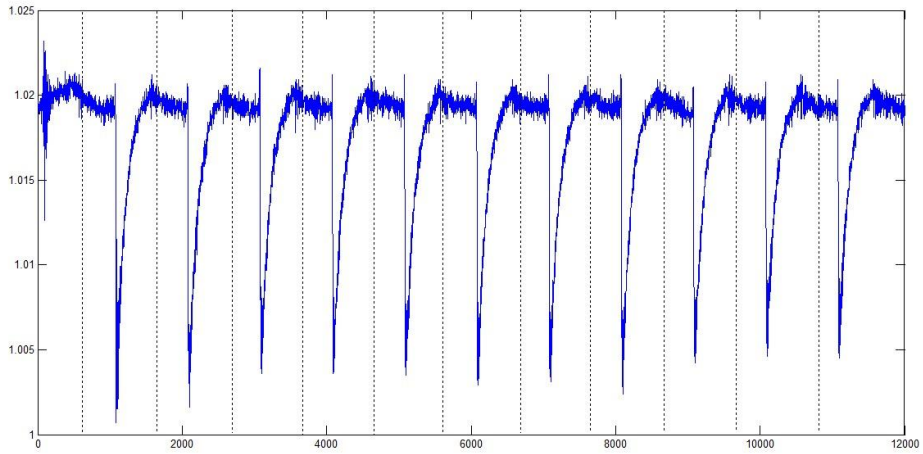


Fig. 2.5. Segments of the power trace

As for the FastDTW algorithm, the complexity can be reduced to O(N). The Algorithm is given below.

---

**Input**: X – a TimeSeries of length |X|

Y – a TimeSeries of length |Y|

radius – distance to search outside of the projected warp path from the previous resolution when refining the warp path.

**Output:** 1) A min. distance warp path between X and Y

2) The warped path distance between X and Y

1| // The min size of the coarsest resolution.

2| Integer minTSsize = radius+2;

---

```
 3|
 4| IF (|X| ≤ minTSsize OR |Y| ≤ minTSsize)
 5| {
 6|     // Base Case: for a very small time series run
 7|     // the full DTW algorithm.
 8|     RETURN DTW(X, Y);
 9| }
10| ELSE
11| {
12|     // Recursive Case: Project the warp path from
13|     // a coarser resolution onto the current
14|     // current resolution.    Run DTW only along
15|     // the projected path (and also 'radius' cells
16|     // from the    projected path).
17|     TimeSeries shrunkX = X.reduceByHalf();
18|     TimeSeries shrunkY = Y.reduceByHalf();
19|     WarpPath lowResPath =    FastDTW(shrunkX,shrunkY, radius);
20|     SearchWindow window =    ExpandedResWindow(lowResPath, X, Y, radius);
21|     RETURN DTW(X, Y, window)
22| }
```

Due to the FastDTW may increase the length of the power traces, we use the asymmetric projections for trace X and Y, as follow.

$$X'[i] = X[i] \tag{5}$$

$$Y'[j] = \frac{1}{|\{k|x(k)=j\}|}\sum_{x(k)=j} Y[y(k)] \tag{6}$$

where the minimal length warping path is denoted as c(k) = (x(k), y(k)).

We use FastDTW algorithm to processing the power trace and apply the SCA attack on the power traces to verify the effectiveness. In the FastDTW, we set the radius as 30. The result is given below.

We use a reference trace and utilize FastDTW algorithm to achieve elastic alignment. The comparison between the original trace and post processing trace is shown as Fig. 2.6.

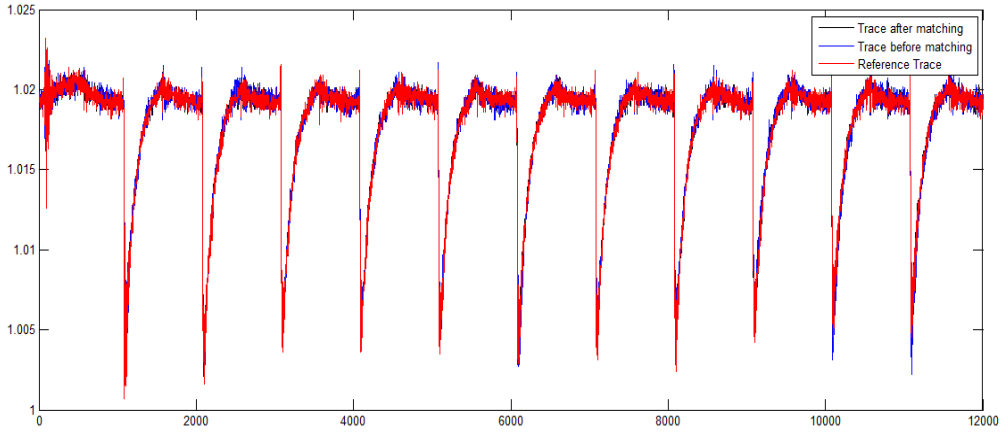


Fig. 2.6. The Trace before matching and after matching

We can see that post processing trace matches the reference trace well. In order to detect the effectiveness clearly, we zoom in the samples between index 1080 and 1100, as Fig. 2.7.

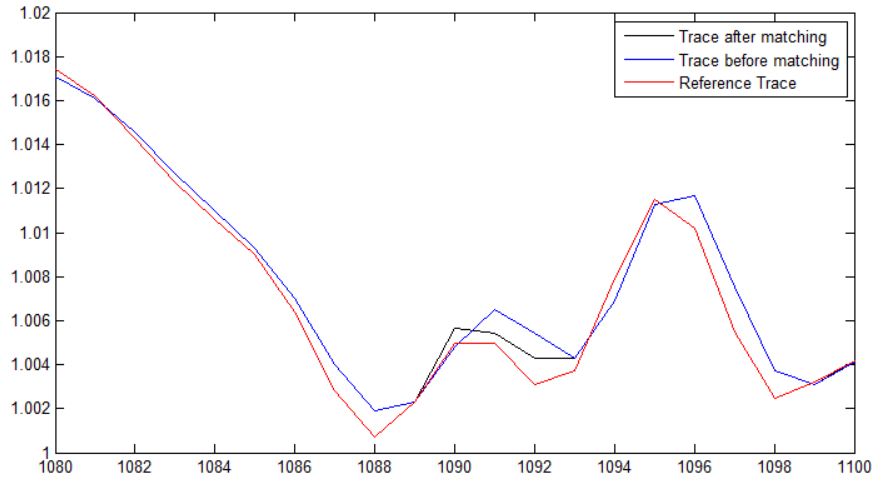


Fig. 2.7. The comparison after zooming in

From Fig. 2.7, the black line is almost the same as the red one and the elastic alignment will make great sense to achieve the SCA analysis. Still, we apply classic DPA[10] with the post processing traces and the result is given below.

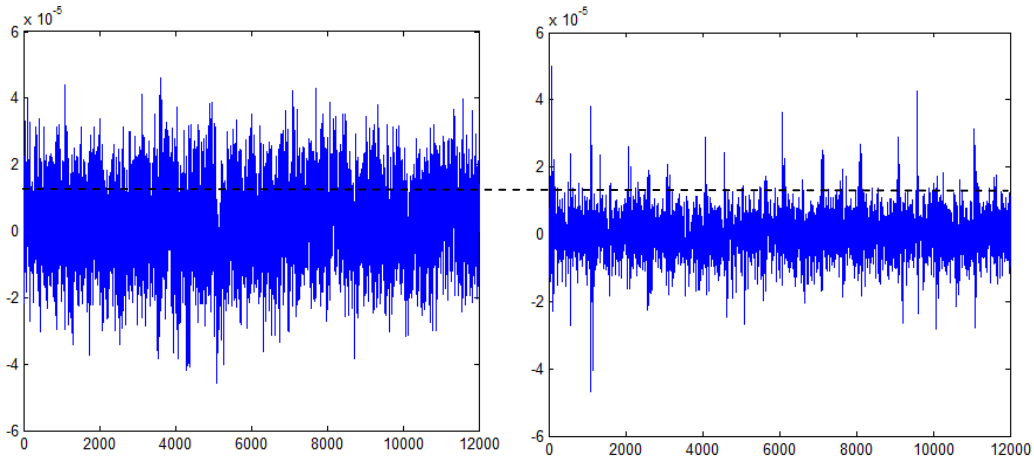


Fig. 2.8. DPA attack with 4000 traces(left: the original traces; right: the post-processing traces)

From Fig 2.8, it is obvious that the elastic alignment is effective and we choose this method to post-process the power traces which will be saved in wave.txt.

## Reference

[1] Le Thanh-Ha, J. Clediere, C. Serviere, and J. Lacoume, “Efficient Solution for Misalignment of Signal in Side Channel Analysis,” in Conference on Acoustics, Speech and Signal Processing ICASSP 2007, Honolulu, HI, 2007, pp. II-257-II-260 vol. 2.

[2] Gierlichs, B., Batina, L., Tuyls, P., Preneel, B.: Mutual Information Analysis. In: Oswald, E., Rohatgi, P. (eds.) CHES 2008. LNCS, vol. 5154, pp. 426–442. Springer, Heidelberg (2008)

[3] van Woudenberg, J.G.J., Witteman, M.F., Bakker, B.: Improving Differential Power Analysis by Elastic Alignment, http://www.riscure.com/fileadmin/images/Docs/elastic_paper.pdf

[4] Salvador, S., Chan, P.: FastDTW: Toward Accurate Dynamic Time Warping in Linear Time and Space. In: Proc. KDD Workshop on Mining Temporal and Sequential Data (2004), Java

implementation,
[5] Tunstall, M., Benoit, O.: Efficient Use of Random Delays in Embedded Software. In: Sauveron, D., Markantonakis, K., Bilas, A., Quisquater, J.-J. (eds.) WISTP 2007. LNCS, vol. 4462, pp. 27–38. Springer, Heidelberg (2007)
[6] Nagashima, S., Homma, N., Imai, Y., Aoki, T., Satoh, A.: DPA Using PhaseBased Waveform Matching against Random-Delay Countermeasure. In: ISCAS, May 27-20, pp. 1807–1810. IEEE Computer Society, Los Alamitos (2007), doi:10.1109/ISCAS.2007.378024
[7] Coron, J.-S., Kizhvatov, I.: Analysis and improvement of the random delay countermeasure of CHES 2009. In: Mangard, S., Standaert, F.-X. (eds.) CHES 2010.LNCS, vol. 6225, pp. 95–109. Springer, Heidelberg (2010)
[8] Homma, N., Nagashima, S., Imai, Y., Aoki, T., Satoh, A.: High-resolution sidechannel attack using phase-based waveform matching. In: Goubin, L., Matsui, M. (eds.) CHES 2006. LNCS, vol. 4249, pp. 187–200. Springer, Heidelberg (2006)
[9] Homma, N., Nagashima, S., Sugawara, T., Aoki, T., Satoh, A.: A High-Resolution Phase-Based Waveform Matching and Its Application to Side-Channel Attacks. IEICE Transactions 91-A(1), 193–202 (2008)
[10] P. Kocher, J. Jaffe, B. Jun: Differential Power Analysis. In proceedings of CRYPTO 1999, LNCS 1666, pp. 388-397, Springer-Verlag, 1999.
[11] http://www.rigolna.com/products/digital-oscilloscopes/ds6000/