Efficient acquisition technique of side-channel information using event-model simulation

COSADE workshop
March 7th-8th, 2013
Télécom ParisTech

Toshiya Asai and Masaya Yoshikawa
Department of Information Engineering
Meijo University

Table of Contents

Table of Contents

Motivation (1/2)

1. Evaluation of tamper resistance in LSI design stage
2. Technical issues
   - ①Efficiency of power simulation
   - ②Efficiency of attack simulation
3. Improvements in this study

   Improves efficiency of power simulation by the event-model simulation (proposed method)

Motivation (2/2)

Effieciency of power waveform simulation

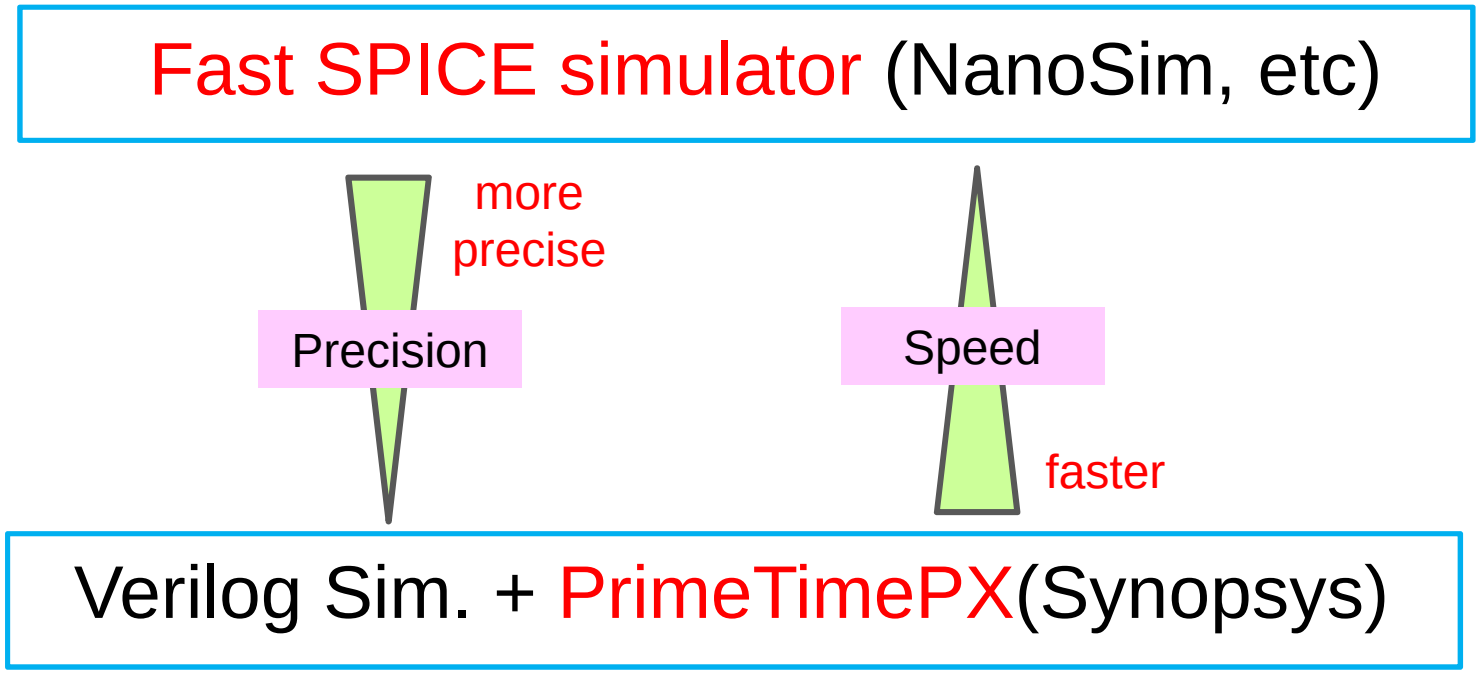
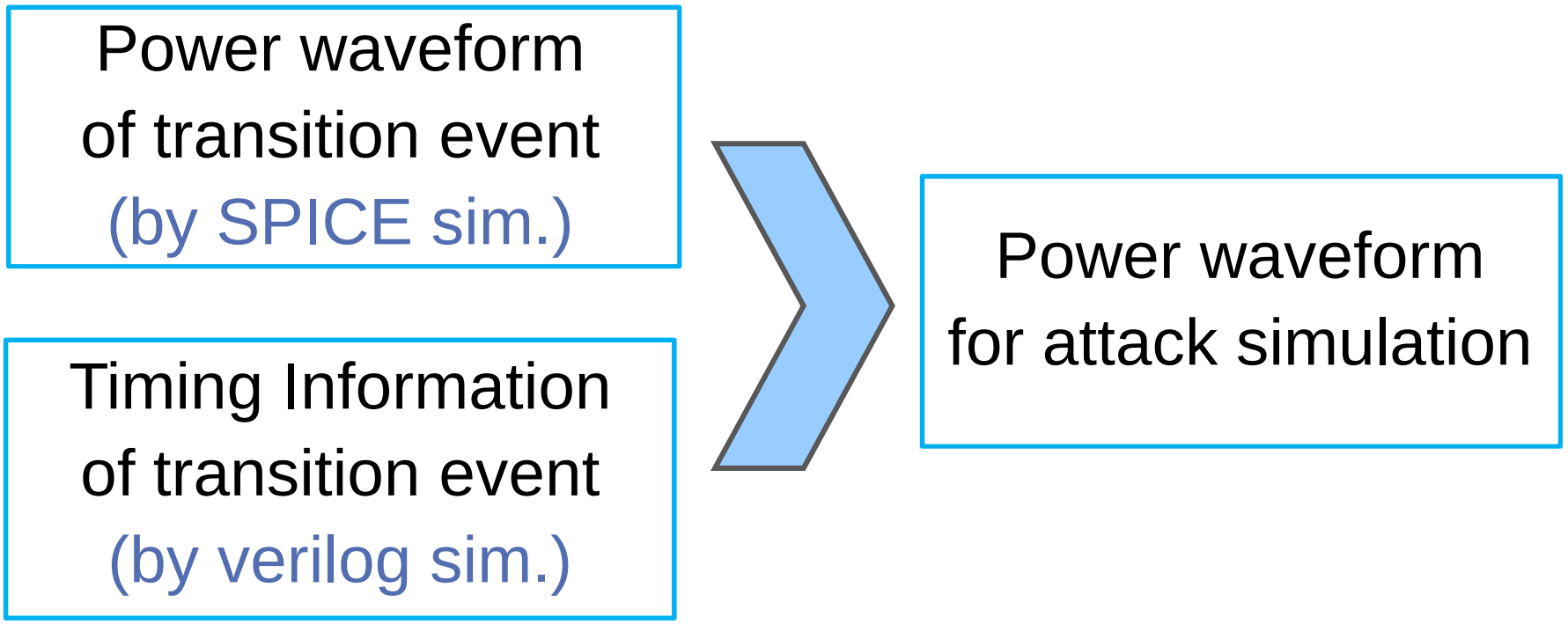


Table of Contents

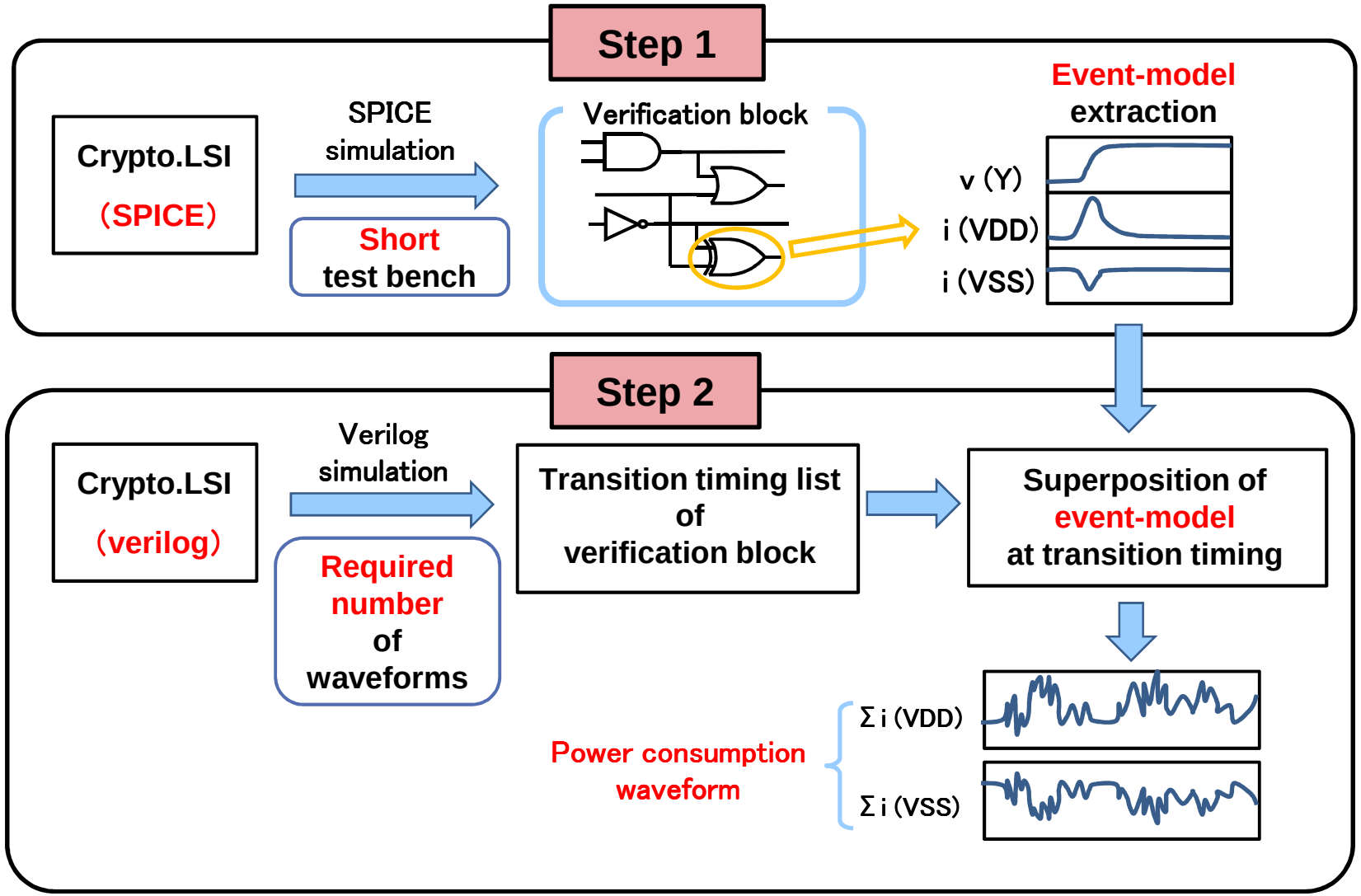
Proposed method (1/5)

Concept of event-model simulation



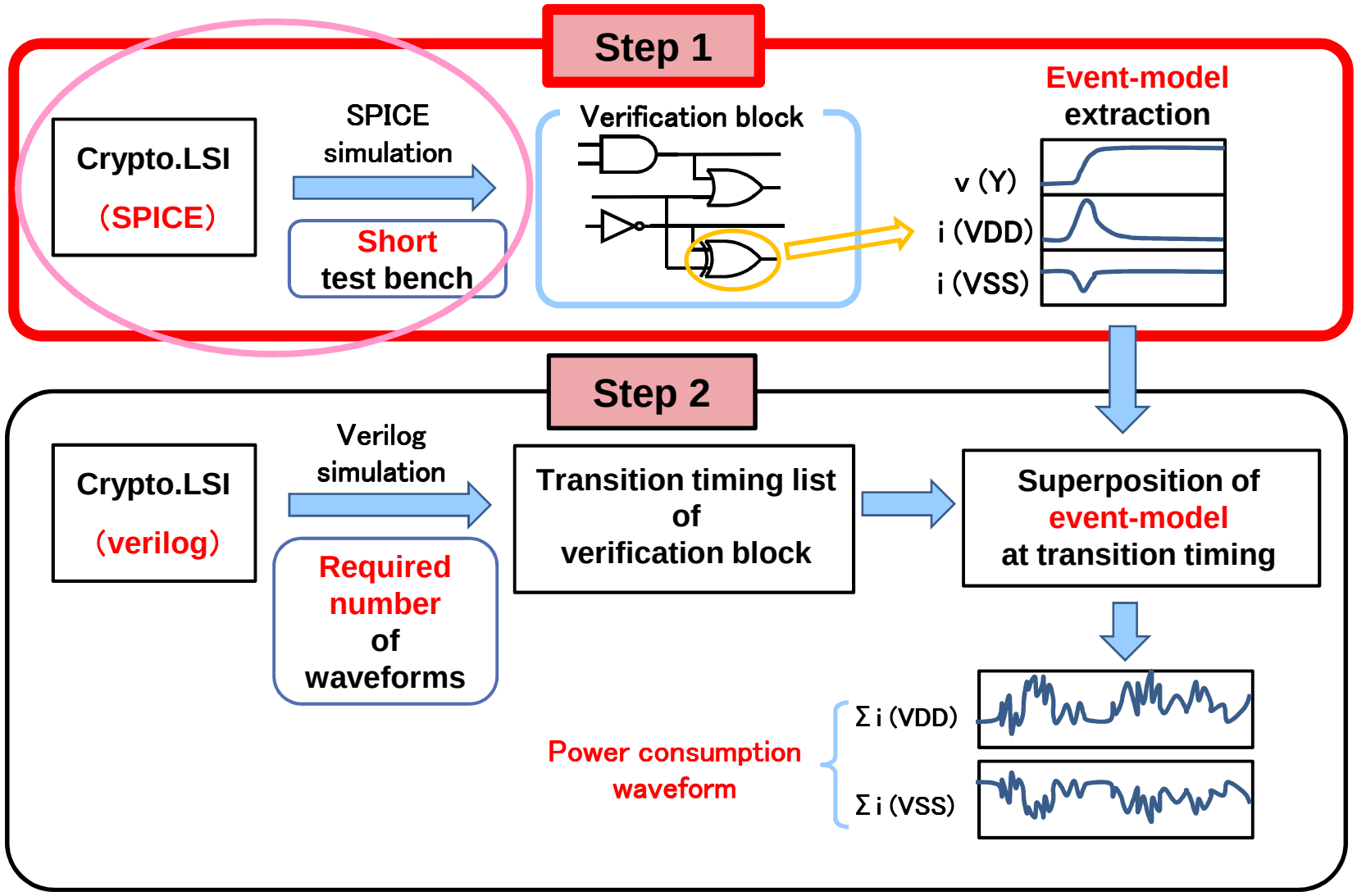
Proposed method (2/5)

Procedure of event-model simulation



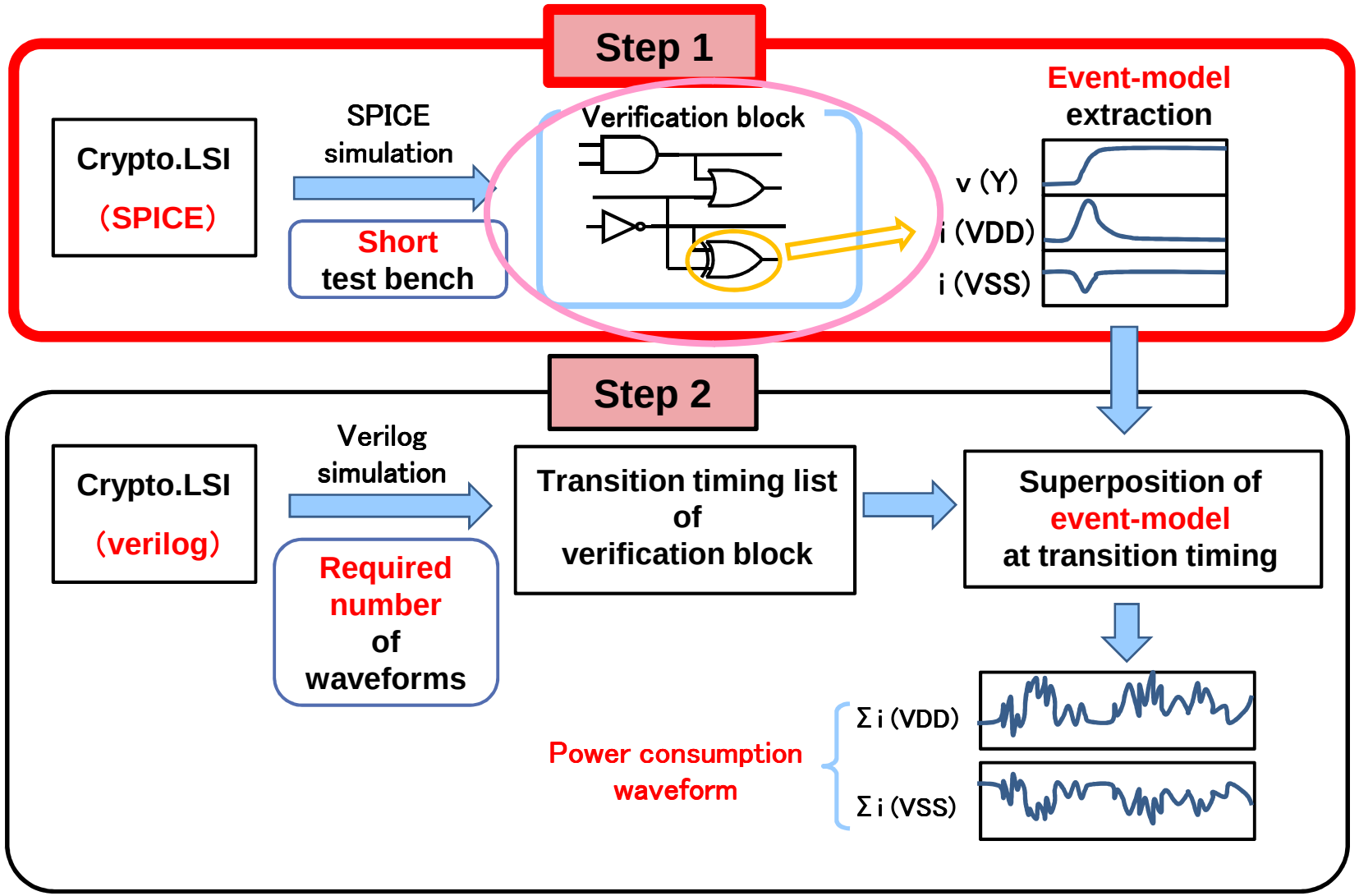
Proposed method (2/5)

Procedure of event-model simulation



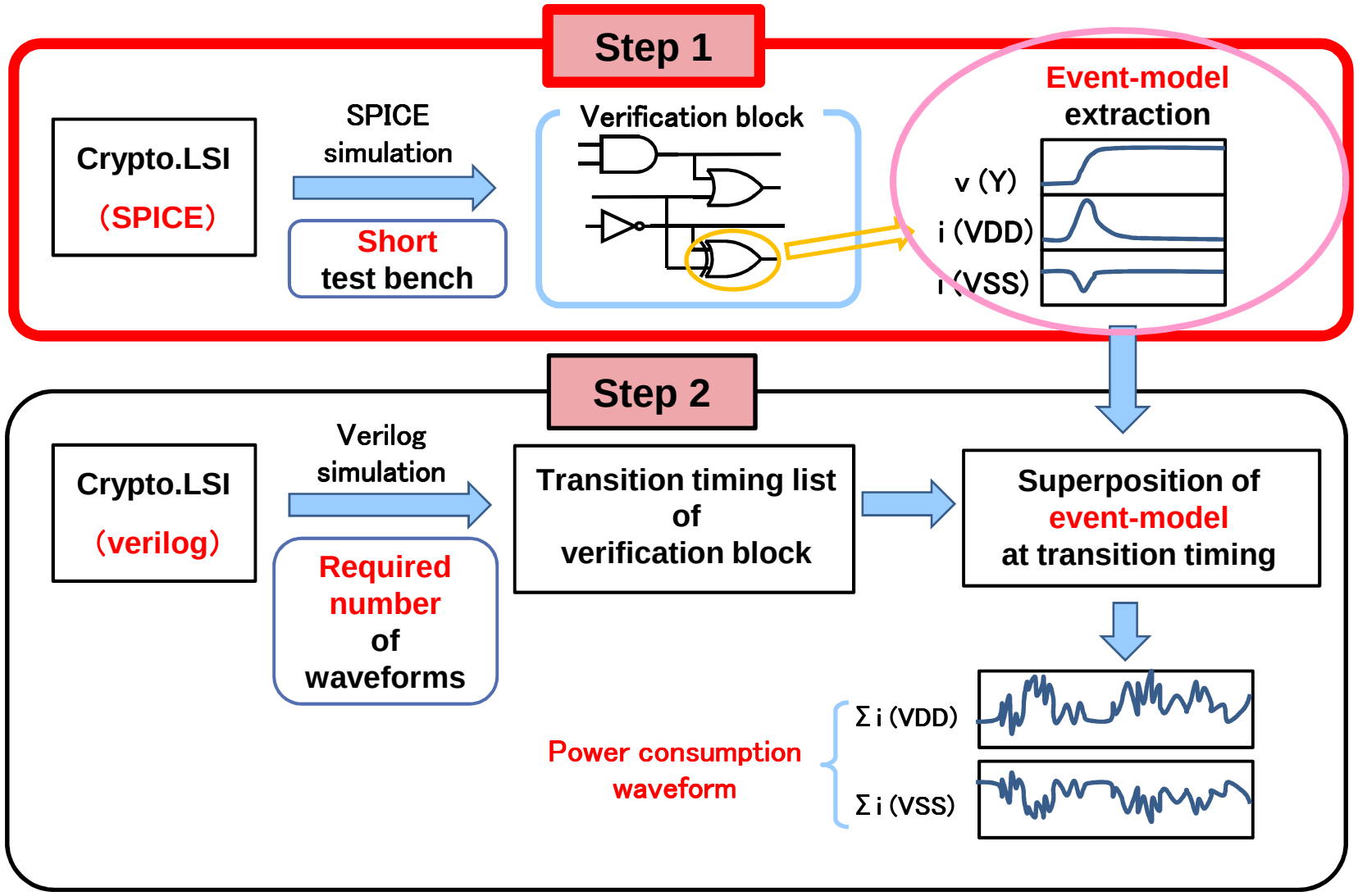
Proposed method (2/5)

Procedure of event-model simulation



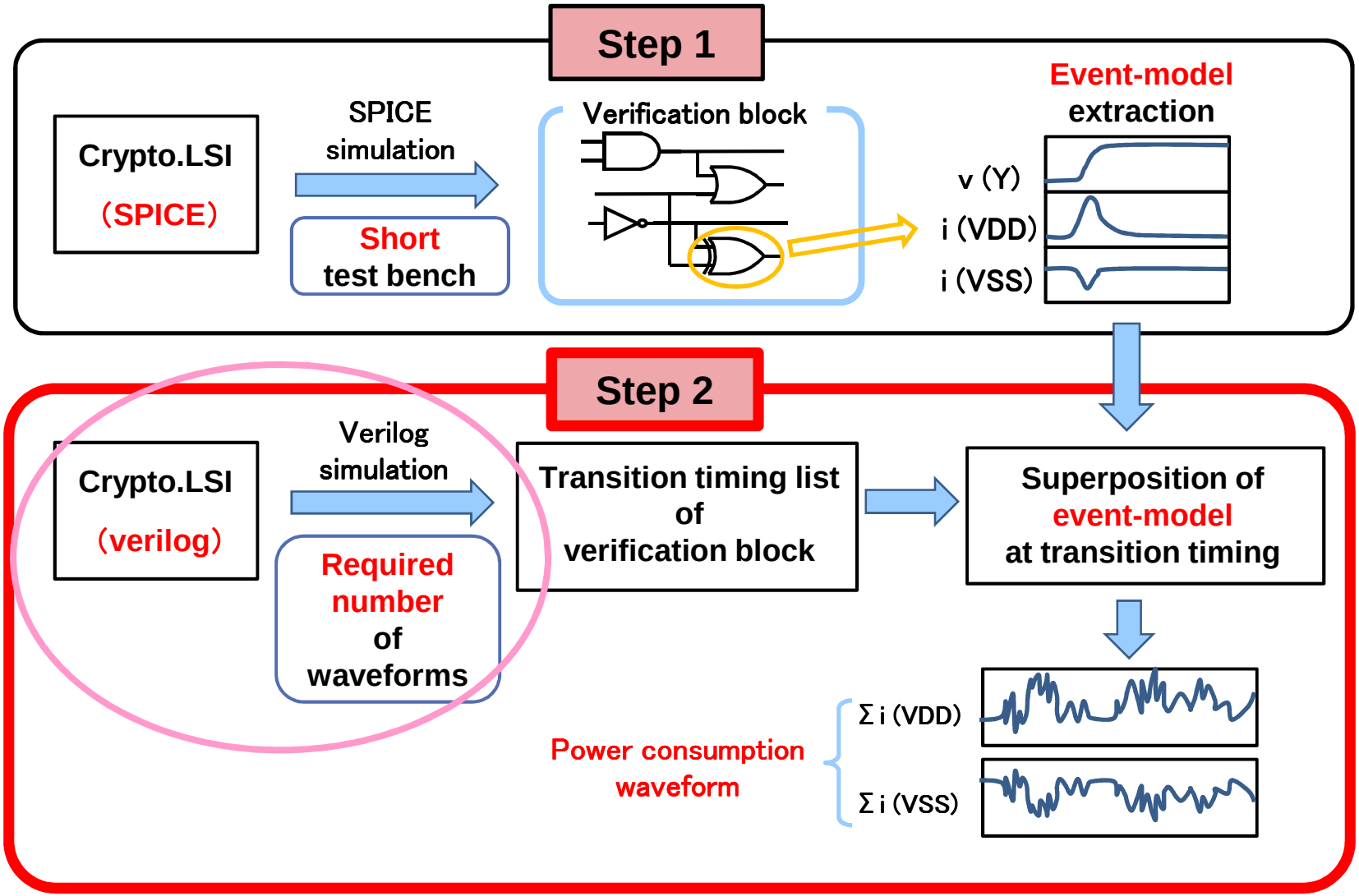
Proposed method (2/5)

Procedure of event-model simulation



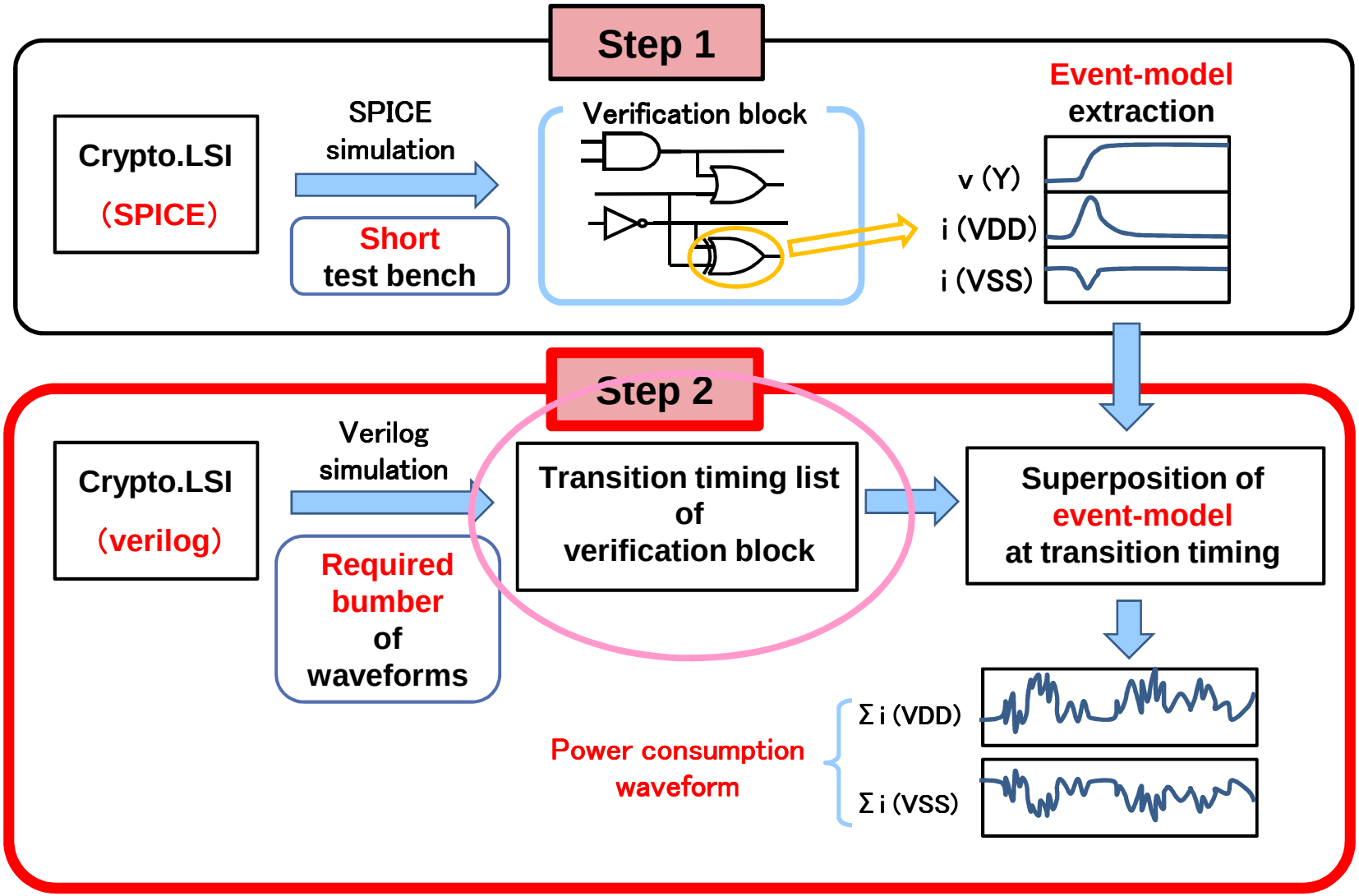
Proposed method (2/5)

Procedure of event-model simulation



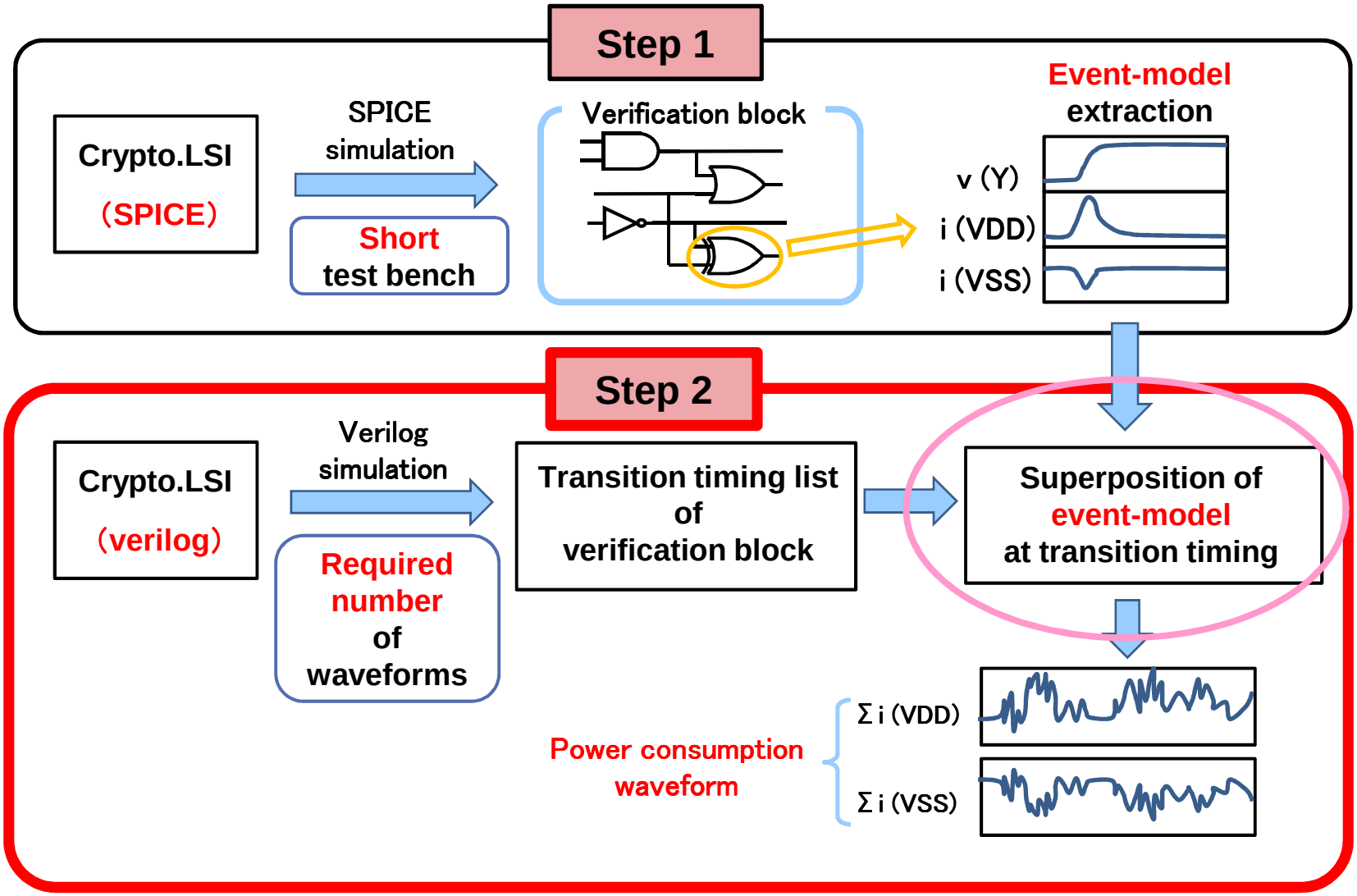
Proposed method (2/5)

Procedure of event-model simulation



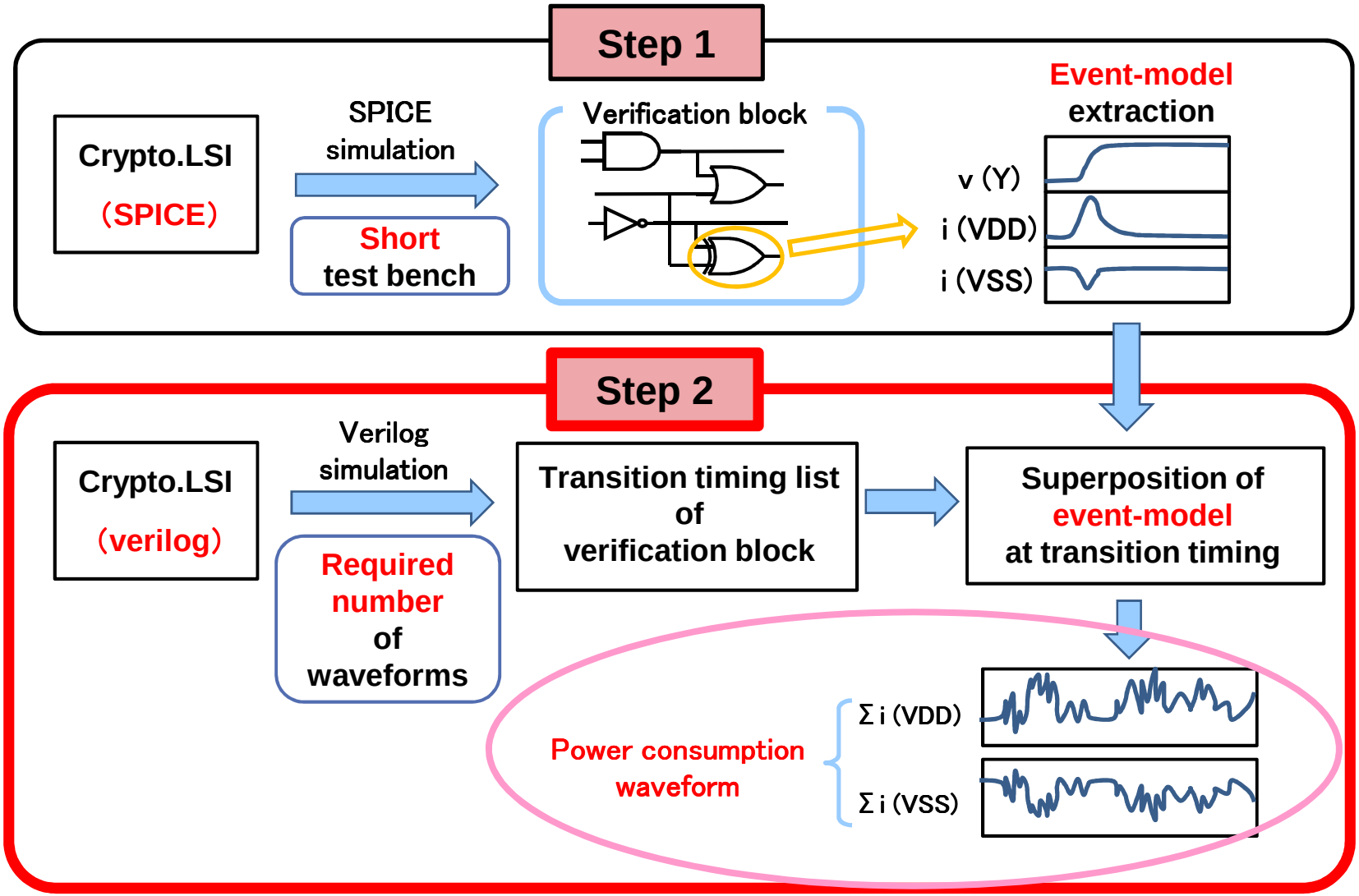
Proposed method (2/5)

Procedure of event-model simulation



Proposed method (2/5)

Procedure of event-model simulation



Proposed method (3/5)

Step 1

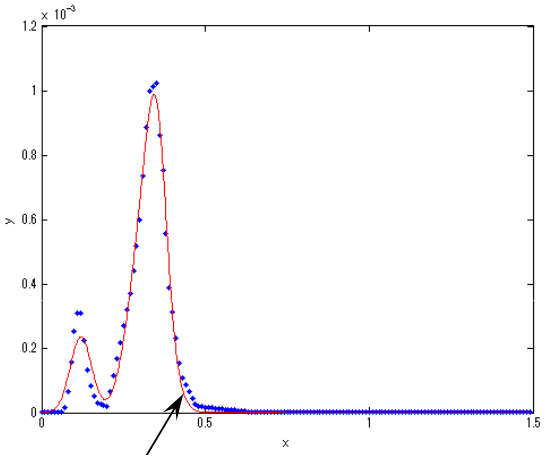
Crypto. LSI

SPICE netlist
・Post layout netlist
・Parasitic extraction data

SPICE simulation

Short test bench
(AES: 2～3 encryption)

Extracted current waveform of each cell



Curve fitting

Proposed method (3/5)

Step 1

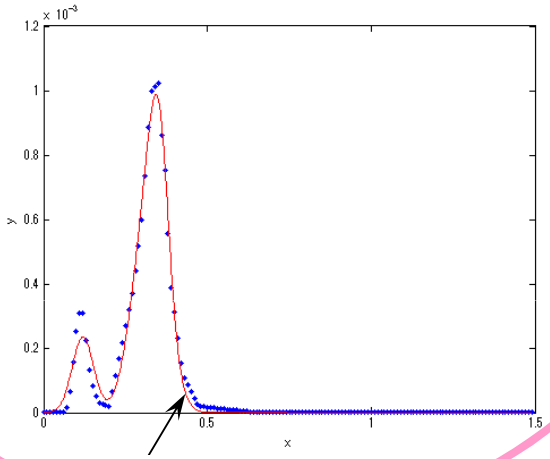
Crypto. LSI

SPICE netlist
・Post layout netlist
・Parasitic extraction data

SPICE simulation

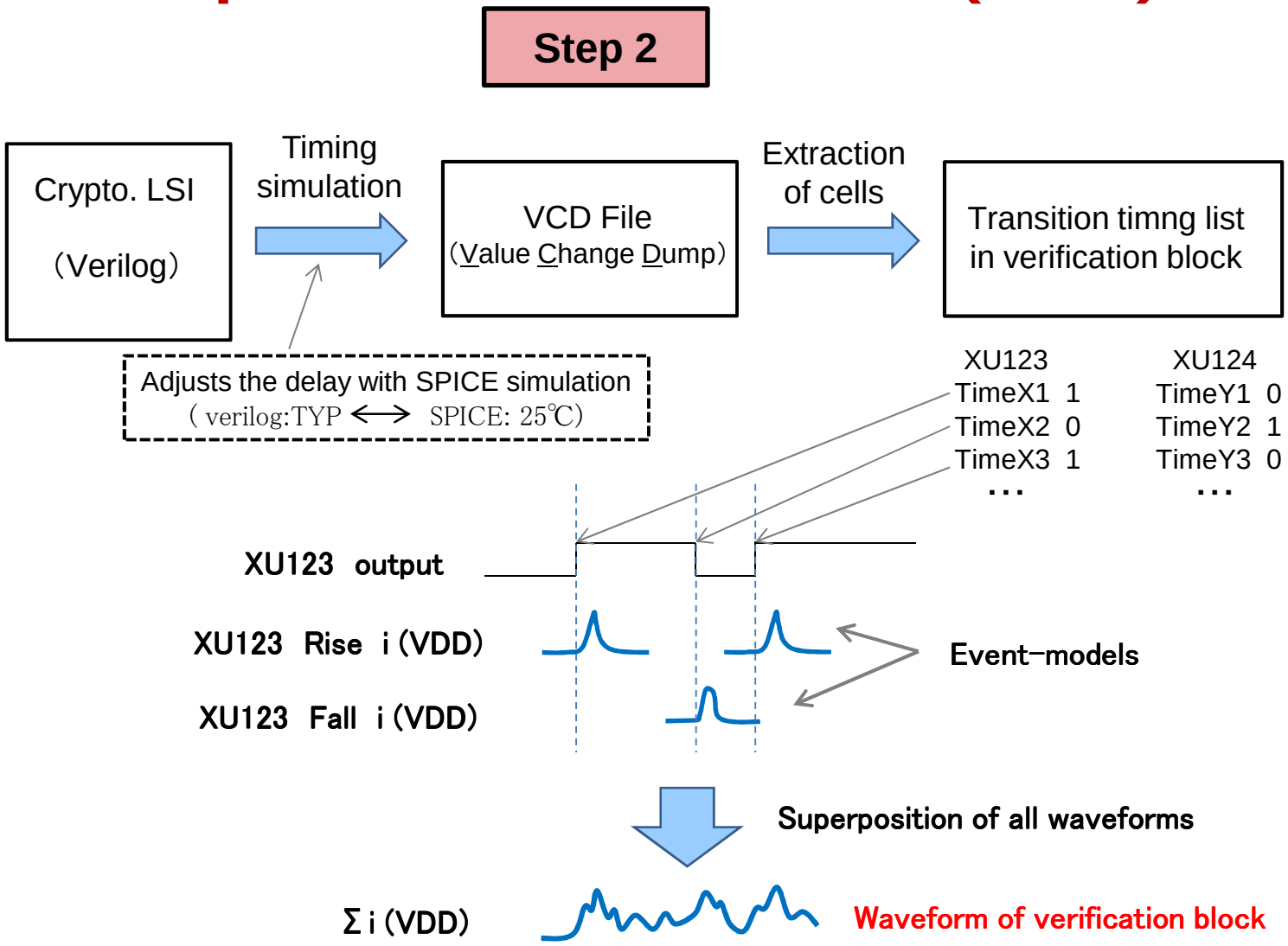
Short test bench
（AES: 2～3 encryption）

Extracted current waveform of each cell

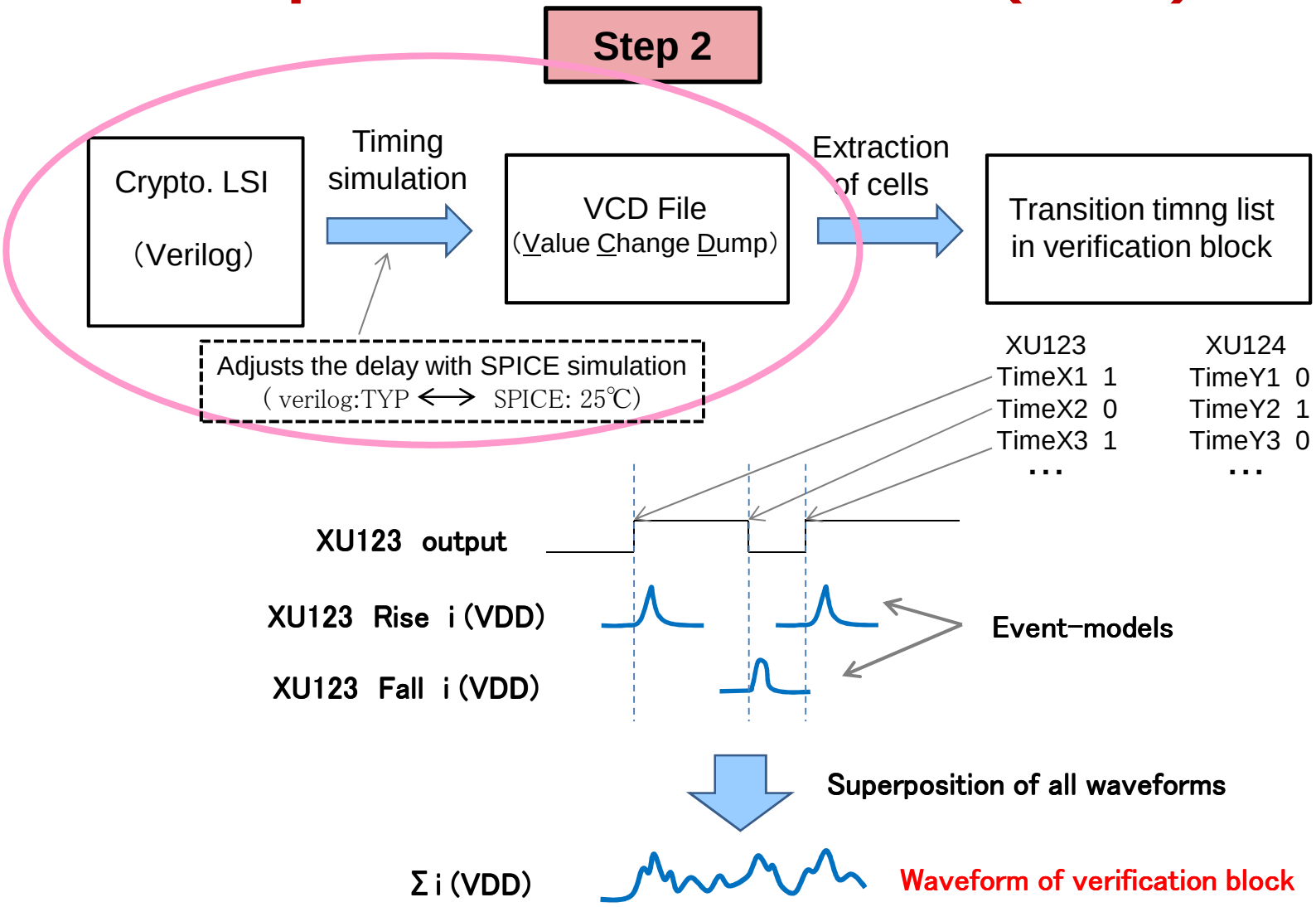


Curve fitting

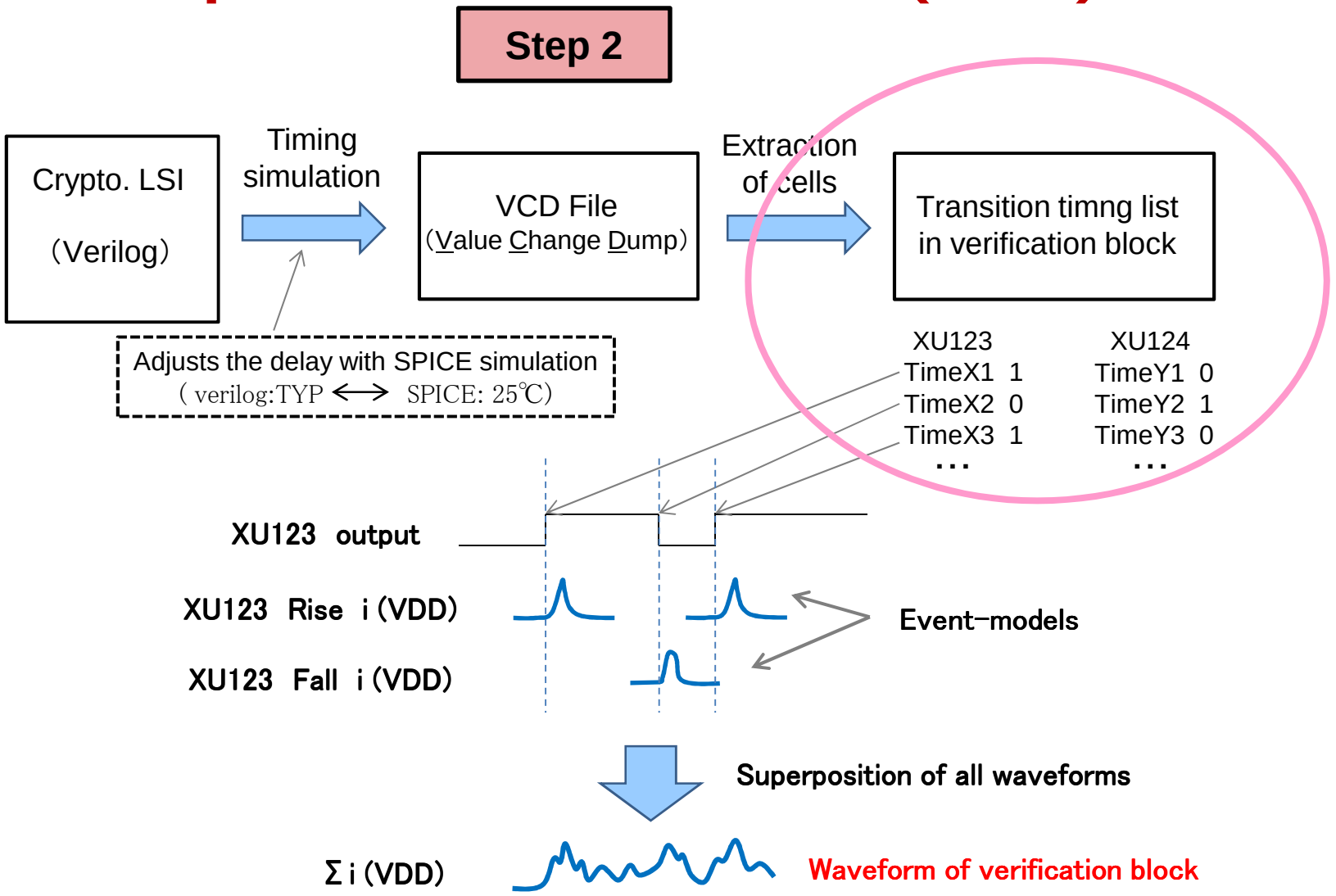
Proposed method (4/5)



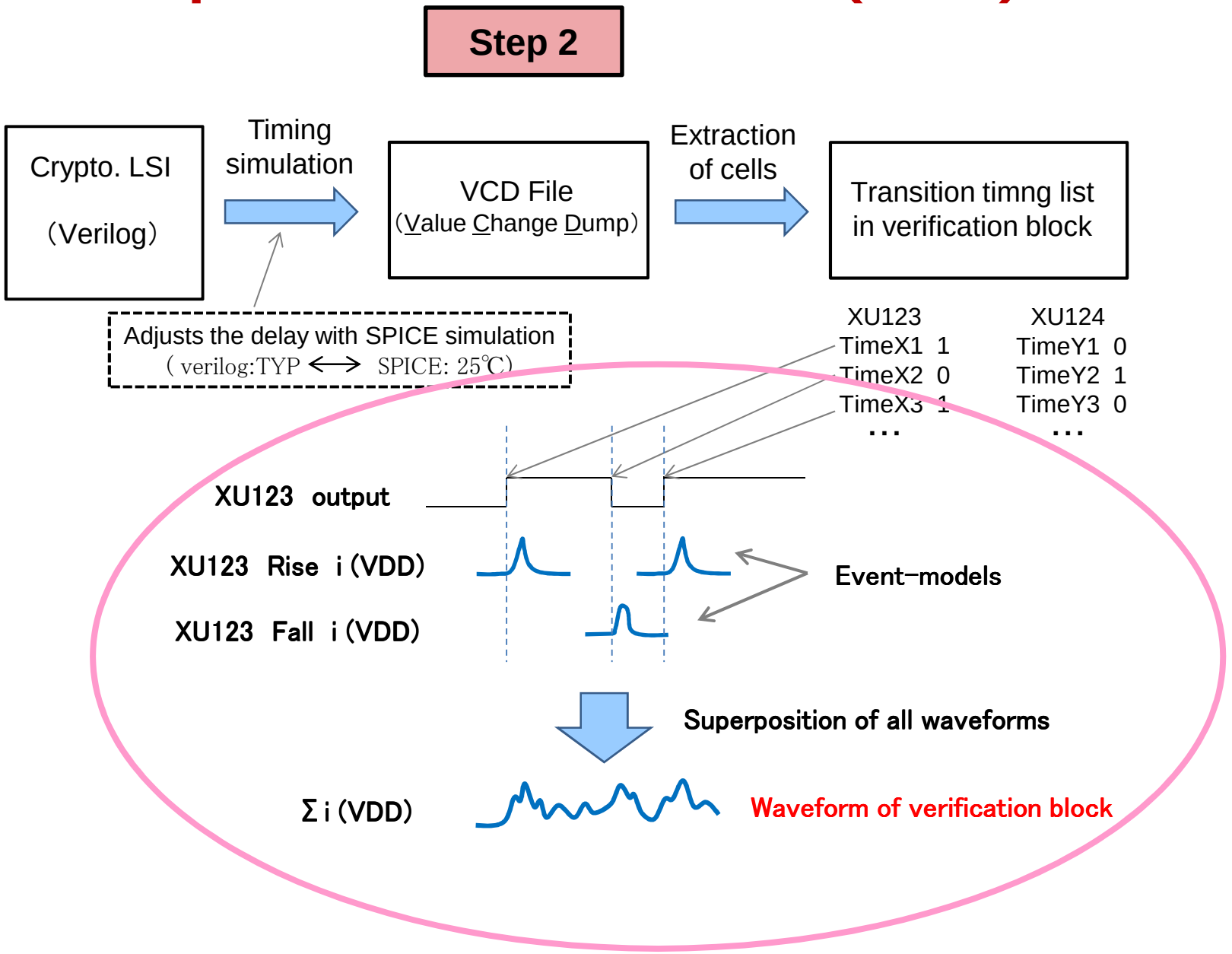
Proposed method (4/5)



Proposed method (4/5)



Proposed method (4/5)



Proposed method (5/5)

Partial generation of required waveforms

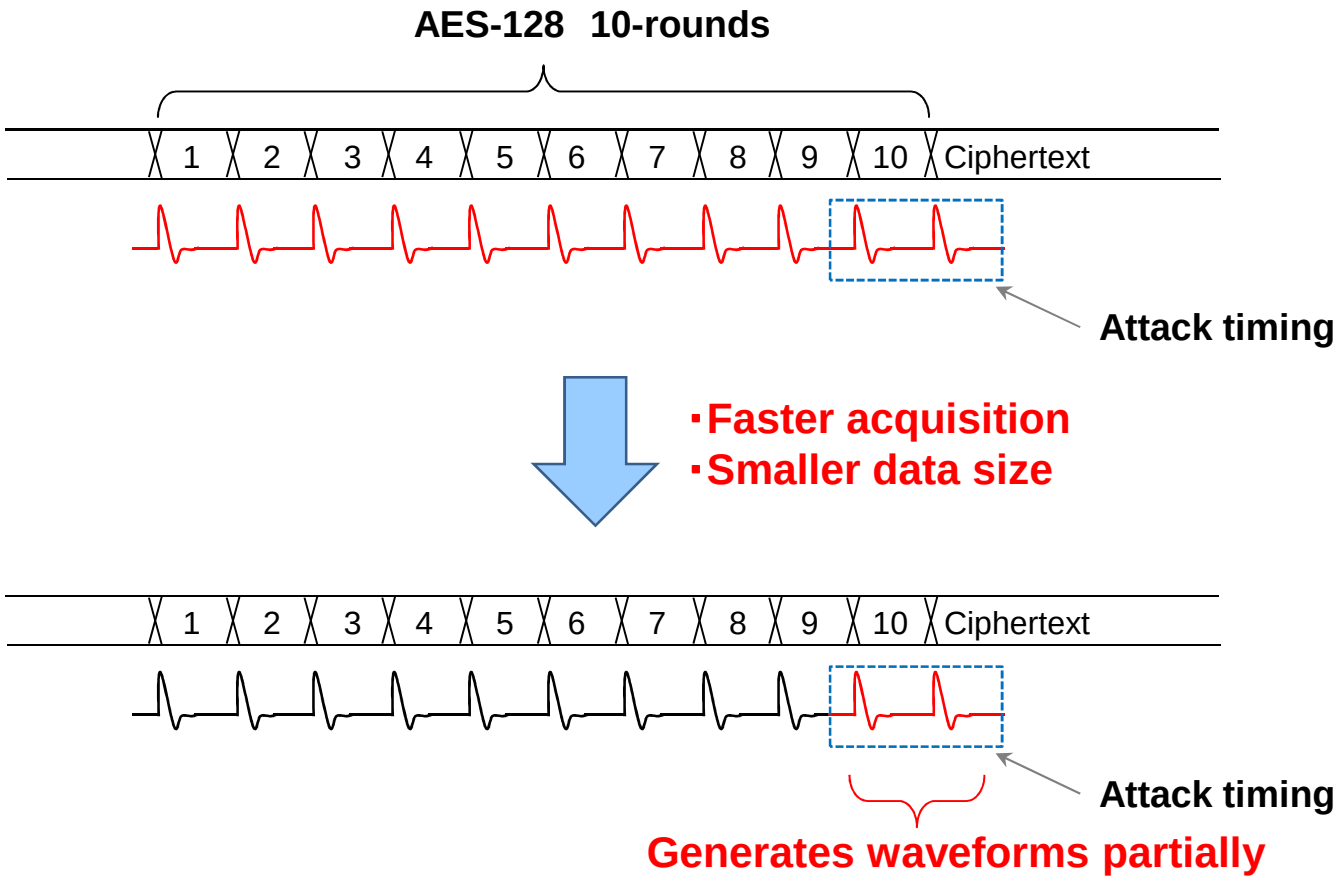
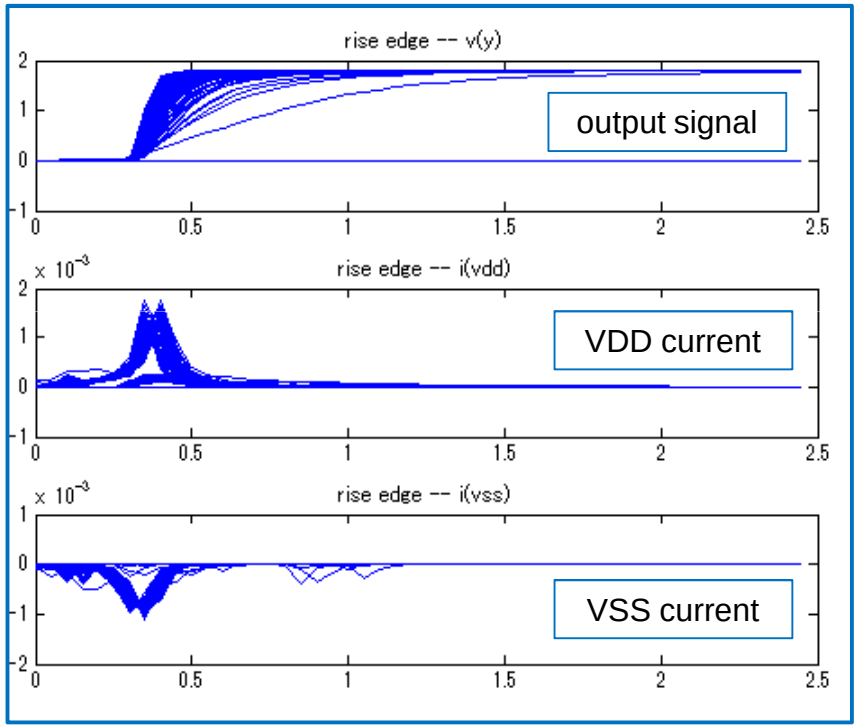


Table of Contents

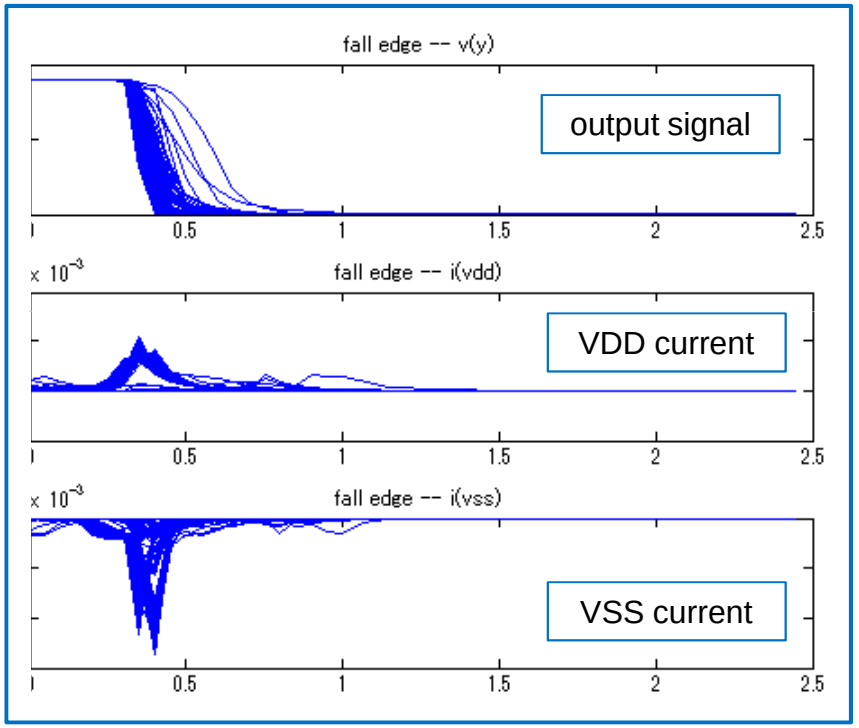
Expermental results(1/4)

Step 1 : modeling

Rise edge



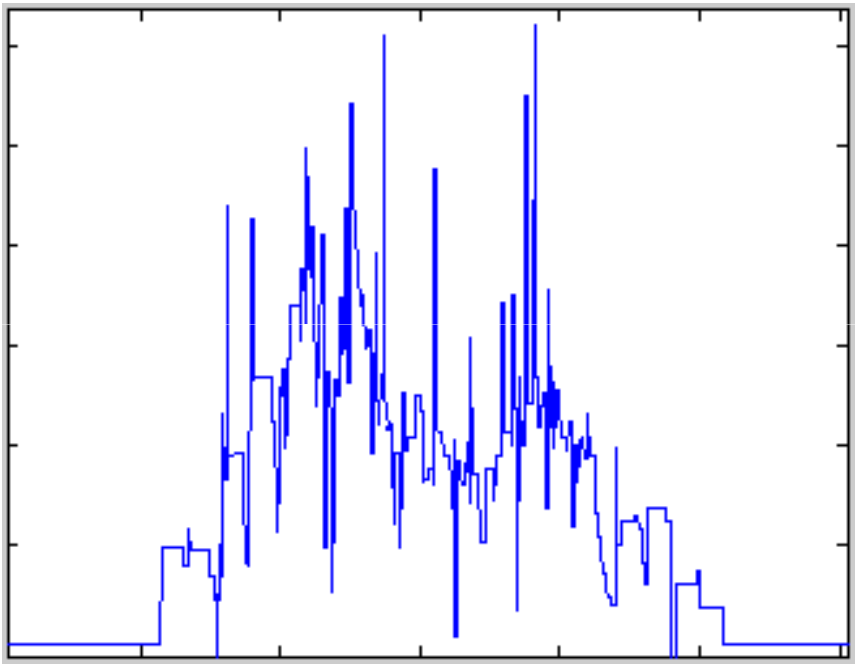
Fall edge



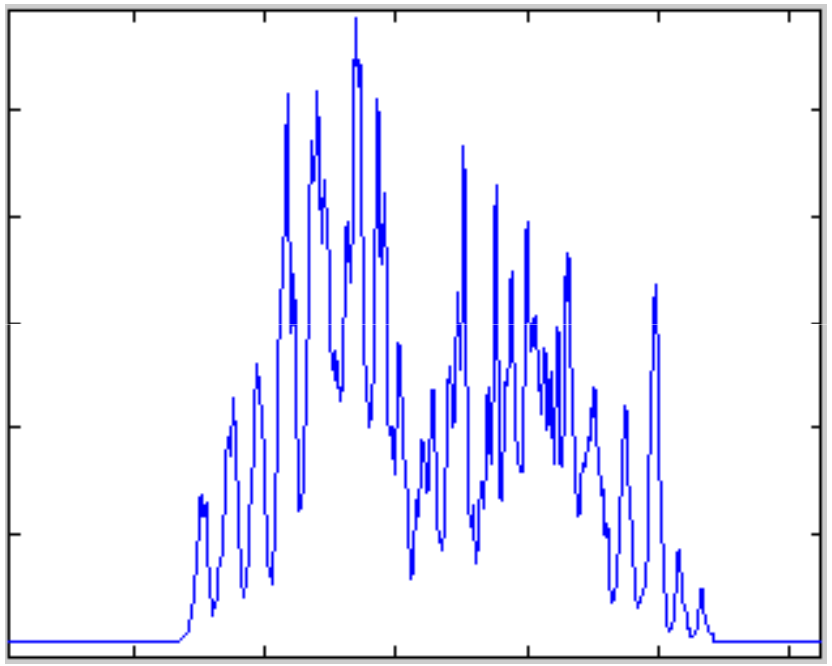
- **0.18μm CMOS technology LSI**
- **AES SubBytes : composite field**
- **Plots waveforms of all cells in SubBytes**

Expermental results(2/4)

Step 2 : waveform generation



Conventional
（PrimeTime PX）



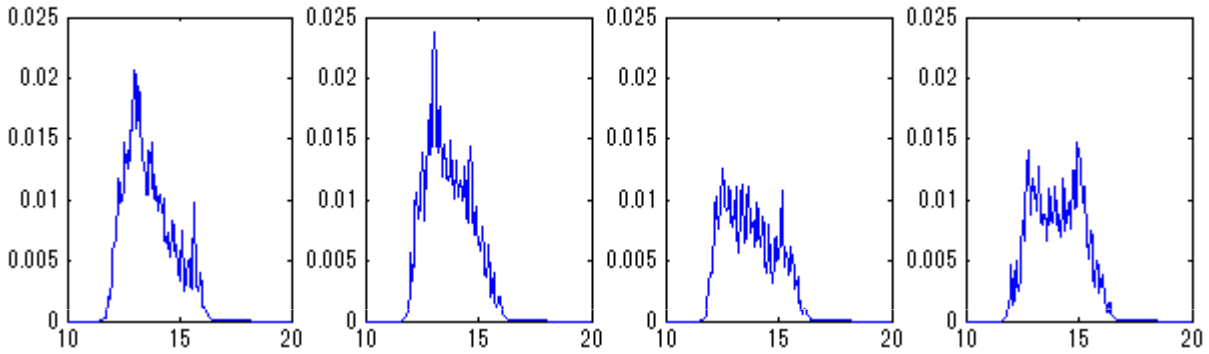
Proposed
（Event-model simulation）

・AES Round 10
・SubBytes ：composite field

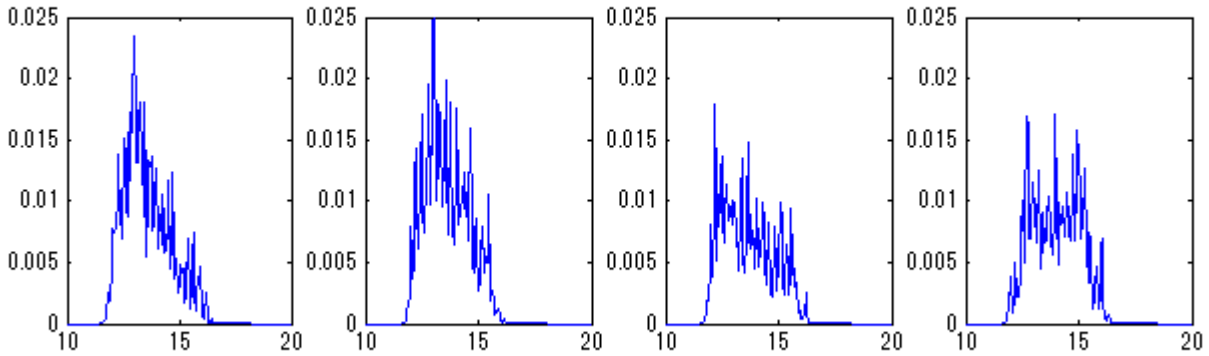
Expermental results(3/4)

Partial waveform generation (AES round-10)

i (VDD)



i (VSS)

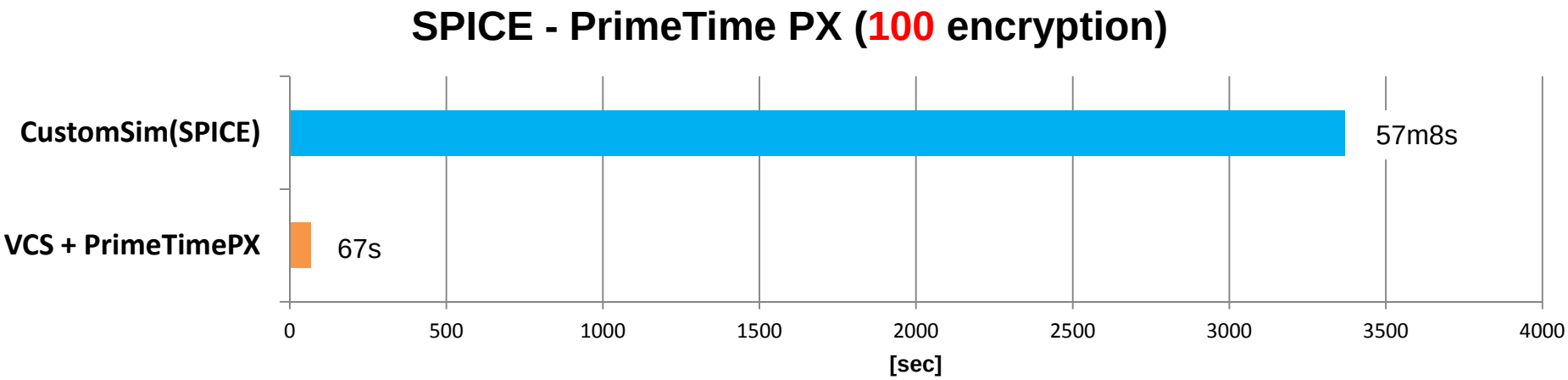


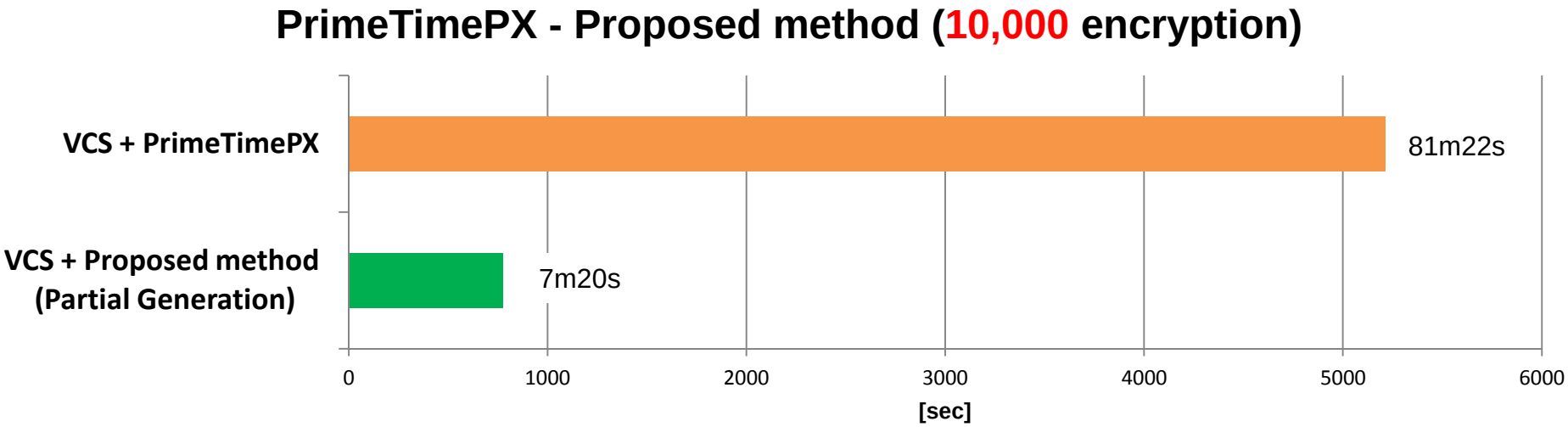
Encryption 1'st 2'nd 3'rd 4'th

Expermental results(4/4)

Comparison of processing time

- AES SubBytes：composite field
- Processing for one SubBytes block
- Machine：Xeon W3565 3.2GHz / 8GB

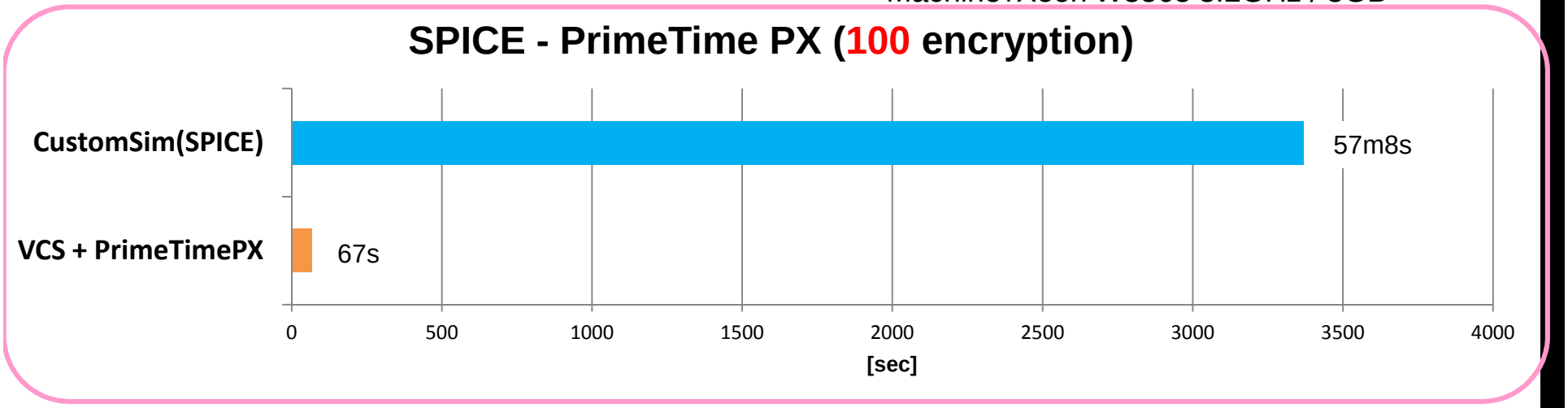


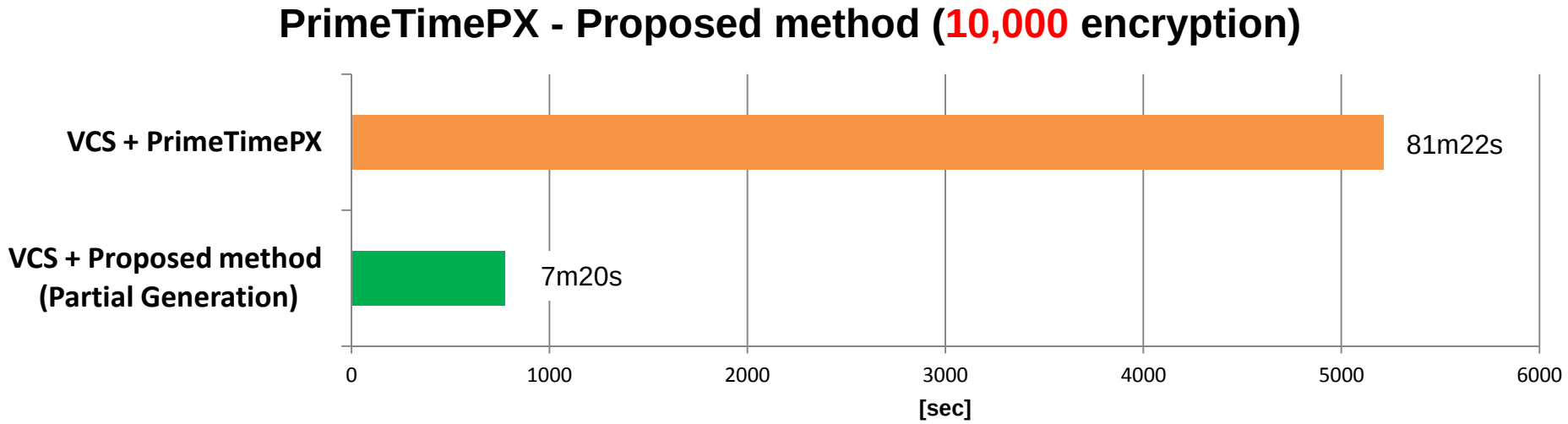


Expermental results(4/4)

Comparison of processing time

- AES SubBytes：composite field
- Processing for one SubBytes block
- Machine：Xeon W3565 3.2GHz / 8GB

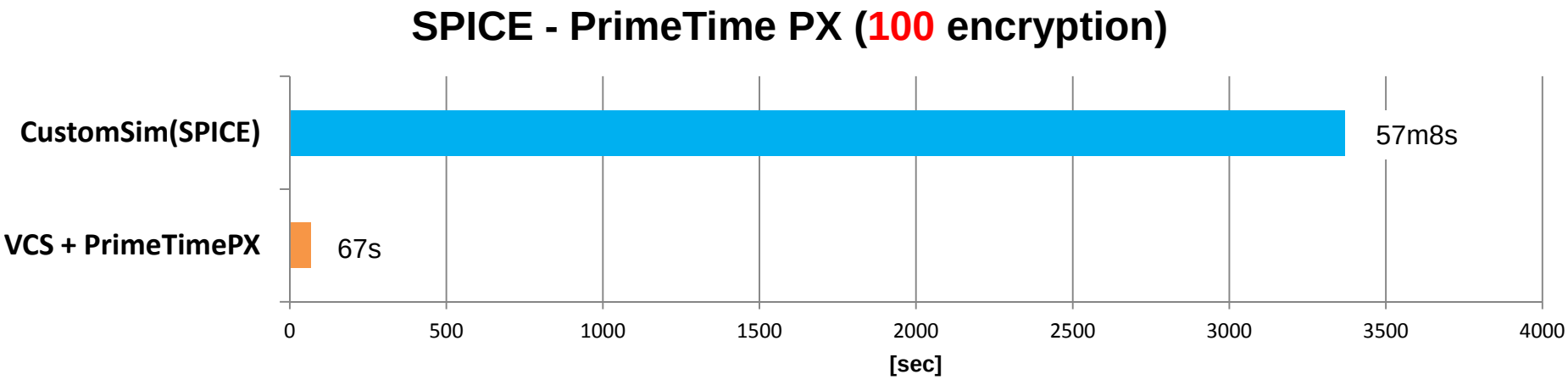




Expermental results(4/4)

Comparison of processing time

- AES SubBytes：composite field
- Processing for one SubBytes block
- Machine：Xeon W3565 3.2GHz / 8GB



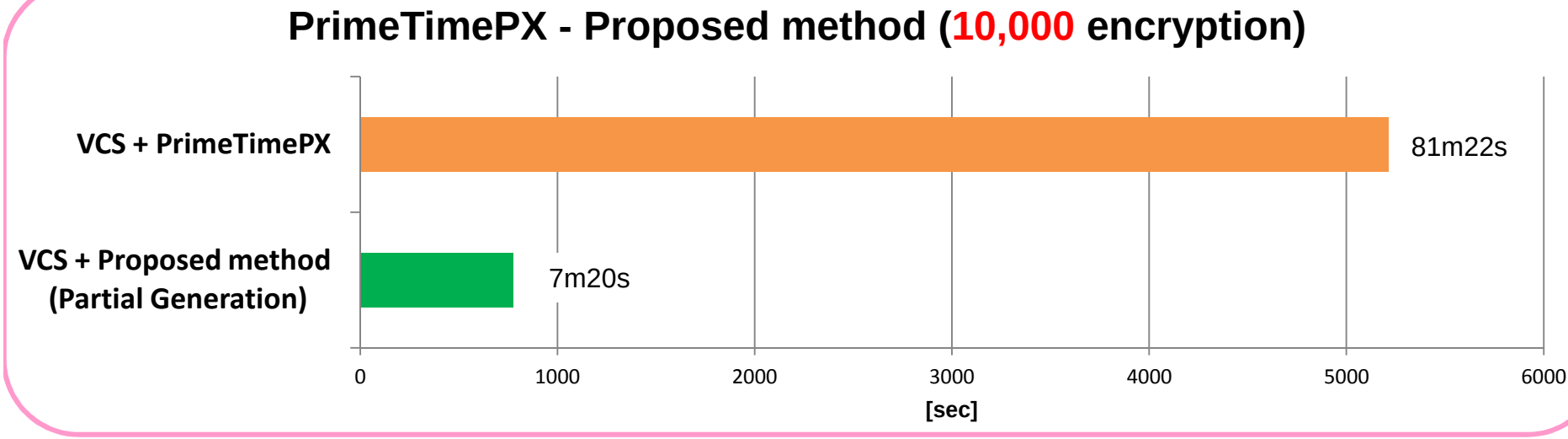


Table of Contents

Summary and future plans

■ Summary

Proposed method — event-model simulation

- Utilizes tools of EDA vendors
- Takes balance between precision and speed
- Confirmed availability with prototype LSI

■ Future plans

- Improves efficiency
- Applies to electro-magnetic analysis

Thank you for your attention

Expermental results

Comparison of processing time

- AES SubBytes : composite field
- Processing for one SubBytes block
- Machine : Xeon W3565 3.2GHz / 8GB