SEGRIDS

Frank Schuhmacher

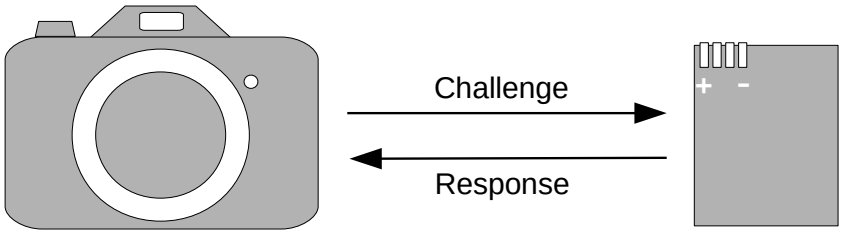
Canonical DPA attack on HMAC-SHA1/SHA2

Outline

- HMAC-SHA256
- New attack strategy
- Attack demonstration on the Bq27Z561 battery IC
- Alternative approach to accessory authentication

HMAC-SHA256

Authentication use case: battery counterfeit prevention



HMAC-SHA256

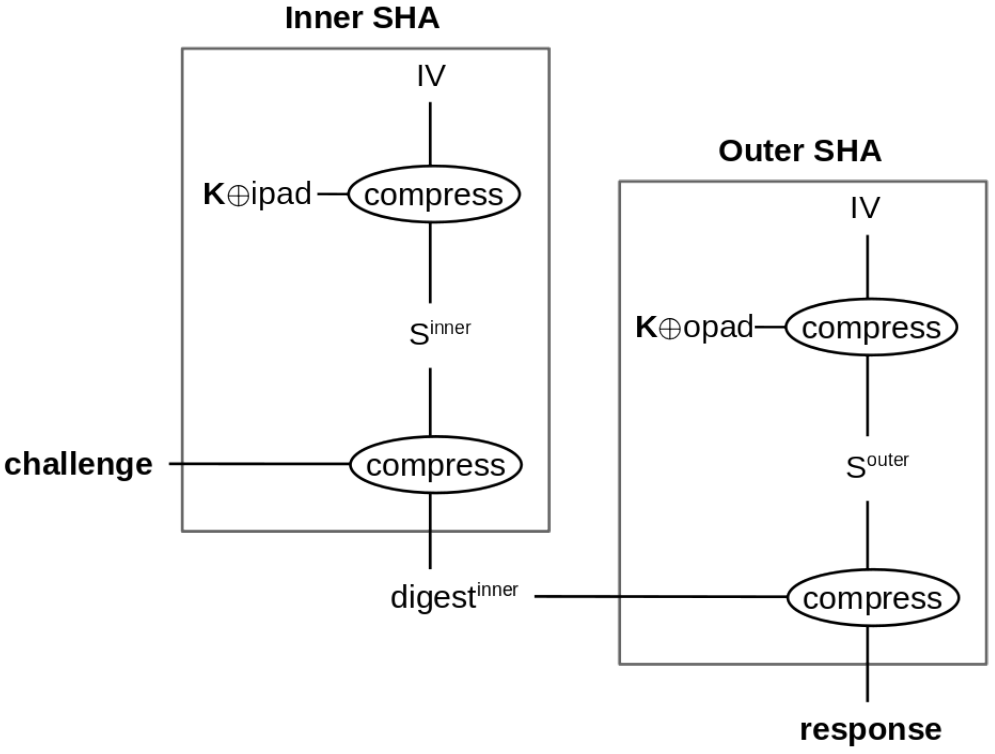
Authentication use case: battery counterfeit prevention

HMAC-SHA256

The HMAC secrets

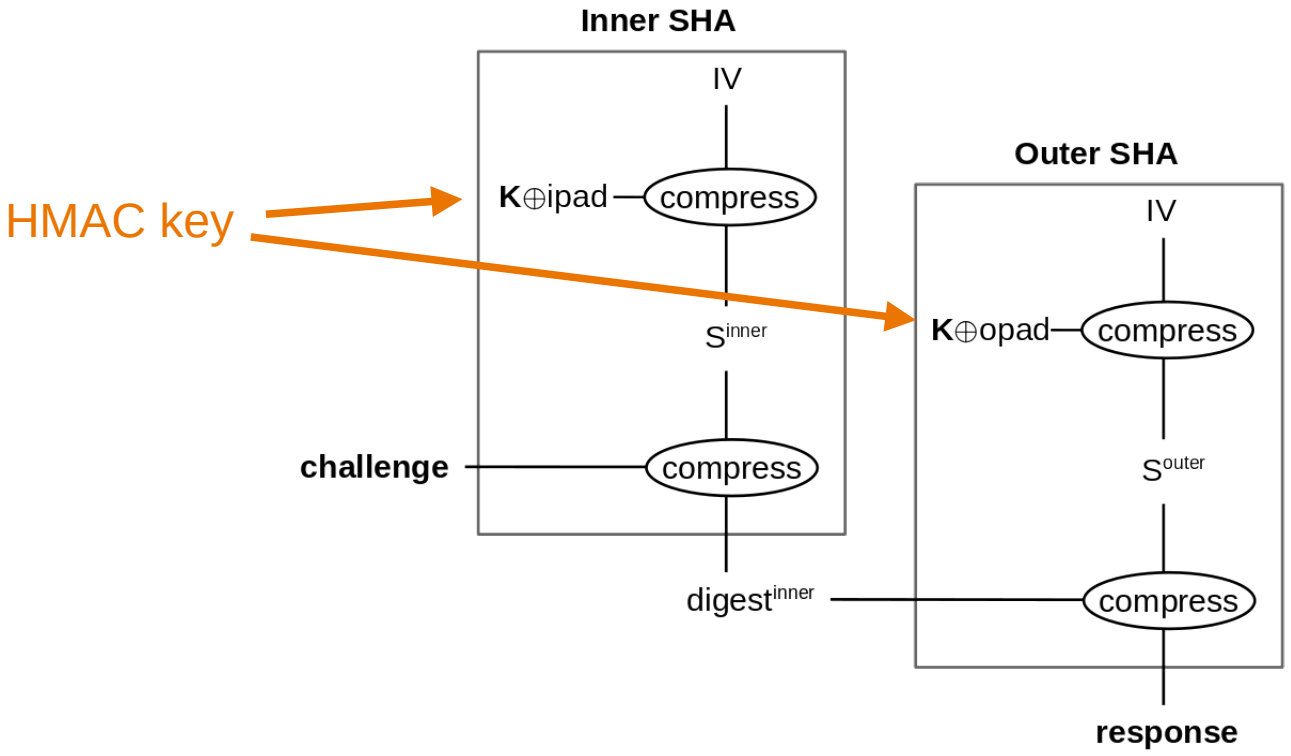
HMAC-SHA256

The HMAC secrets



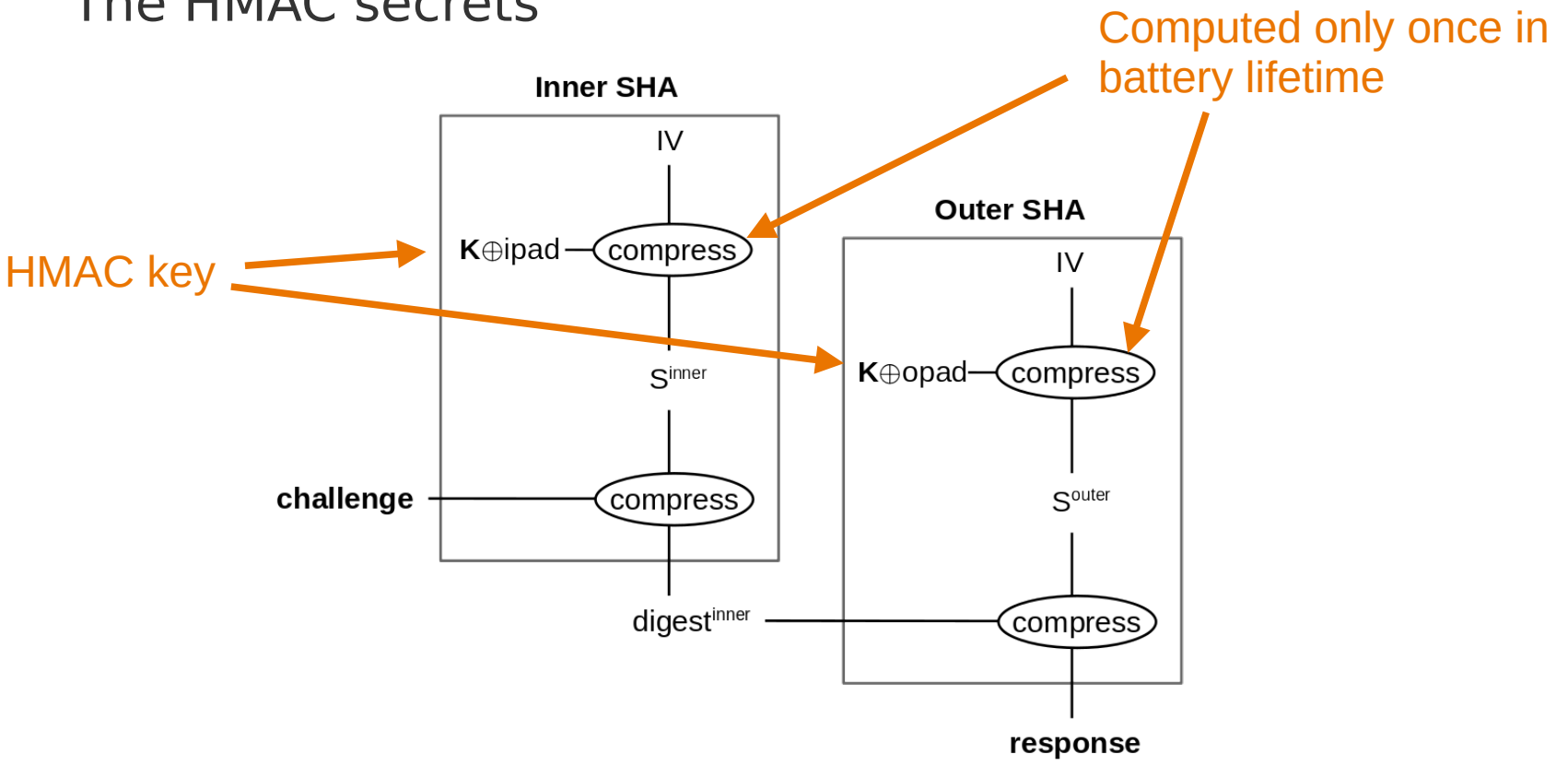
HMAC-SHA256

The HMAC secrets



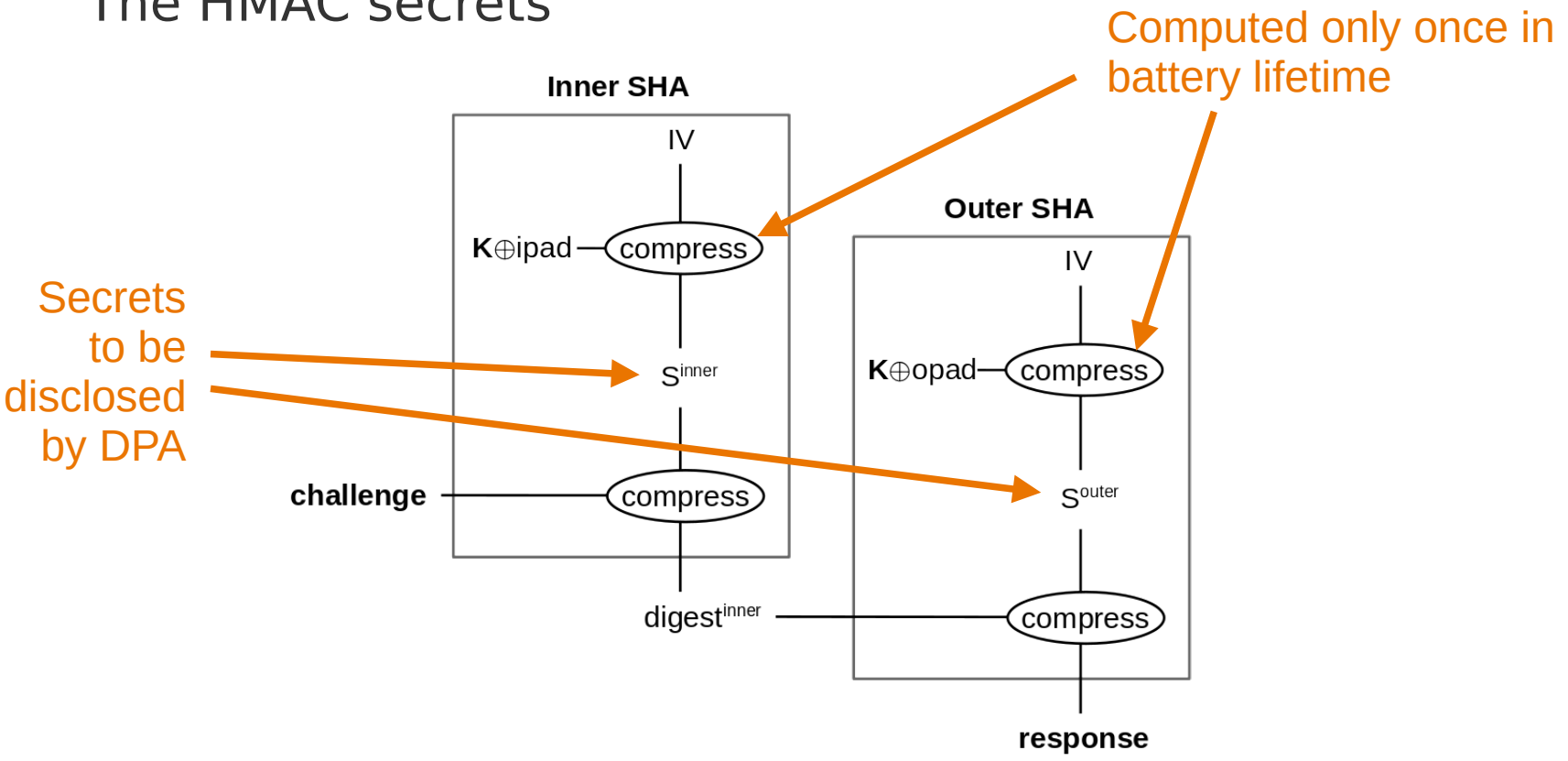
HMAC-SHA256

The HMAC secrets



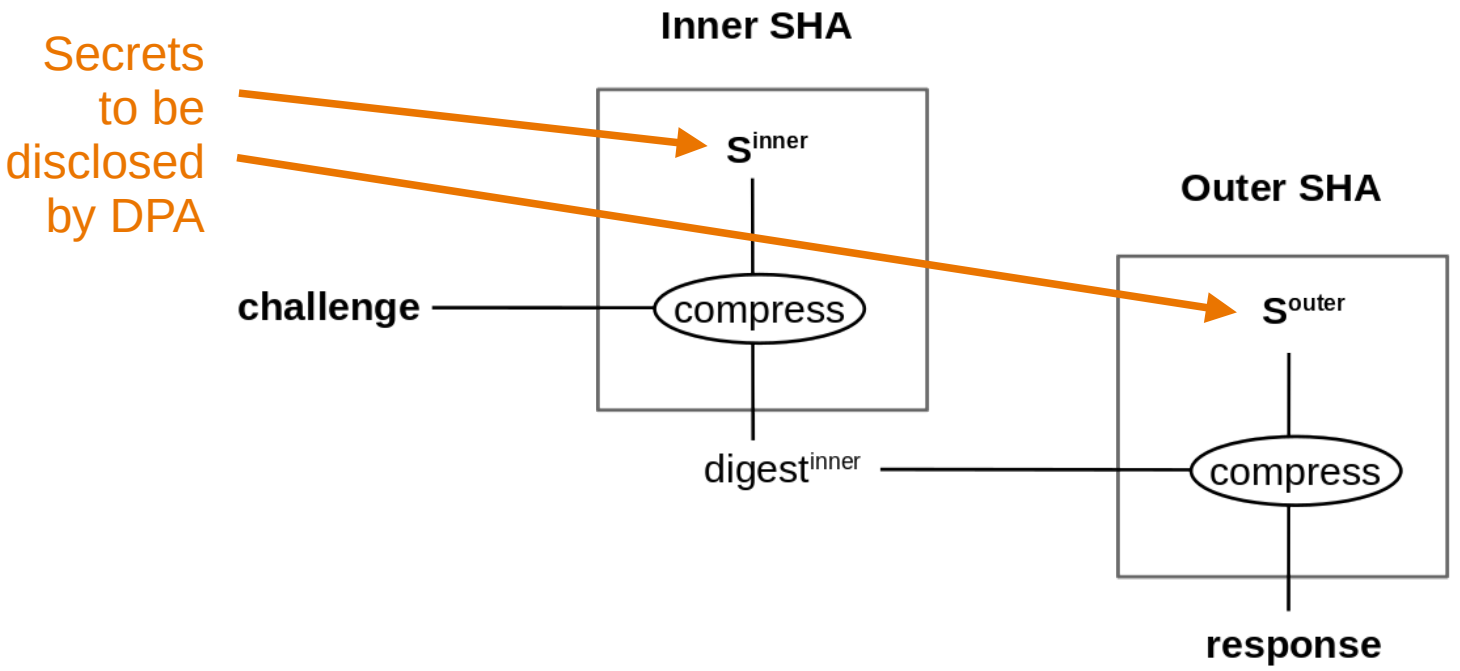
HMAC-SHA256

The HMAC secrets



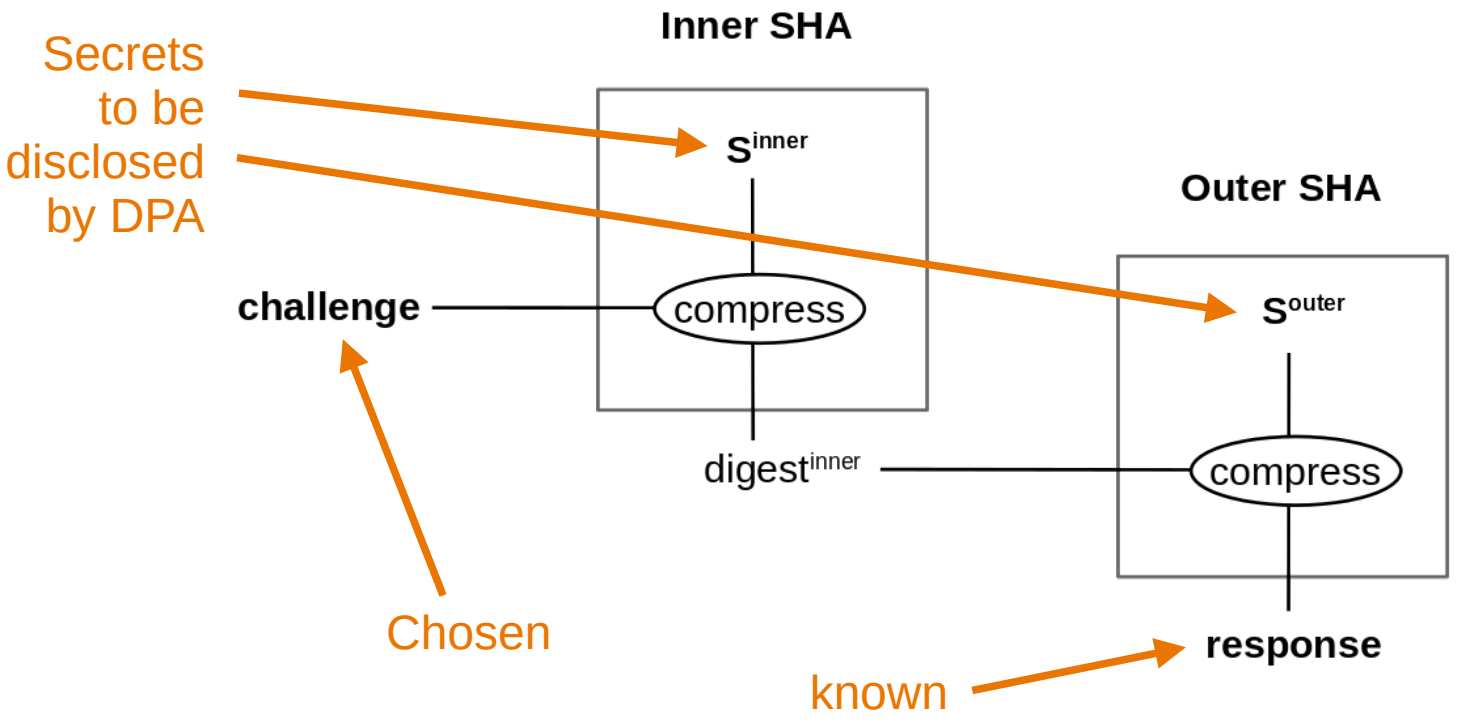
HMAC-SHA256

The HMAC secrets



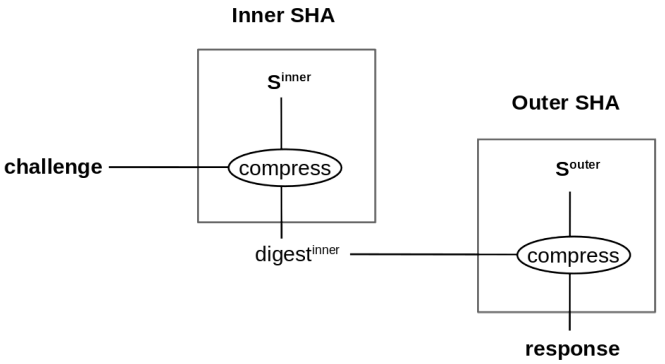
HMAC-SHA256

The HMAC secrets



HMAC-SHA256

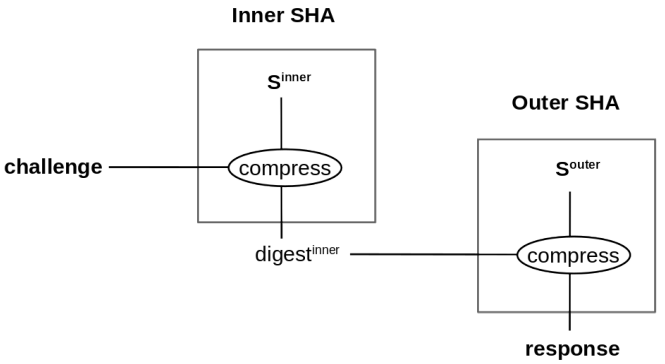
The compress function



HMAC-SHA256

The compress function

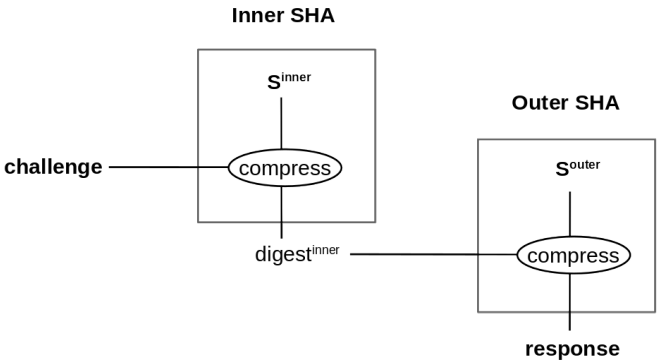
1. Extend **challenge** to 64 words.



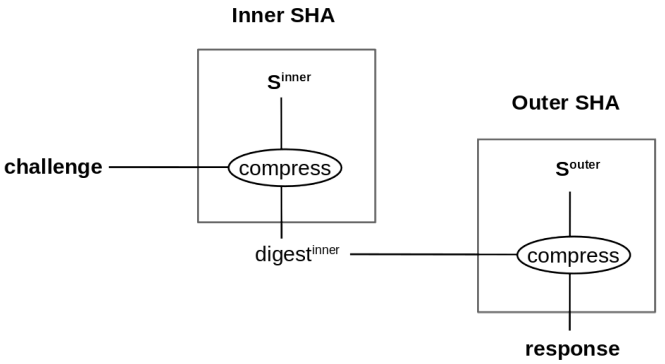
HMAC-SHA256

The compress function

1. Extend **challenge** to 64 words.
2. (a,b,c,d,e,f,g,h) := $\mathbf{S^{inner}}$

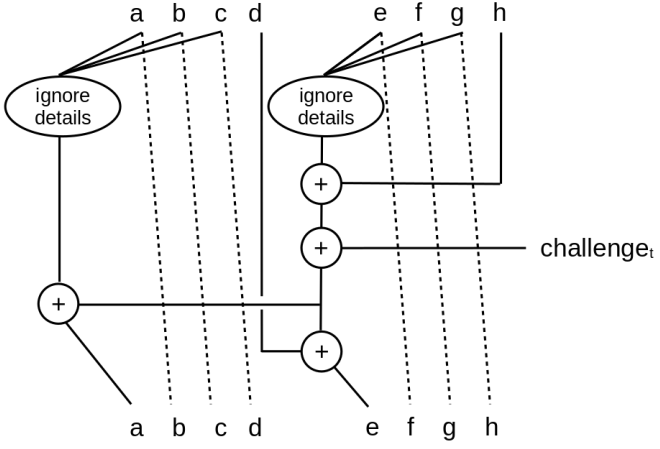


HMAC-SHA256

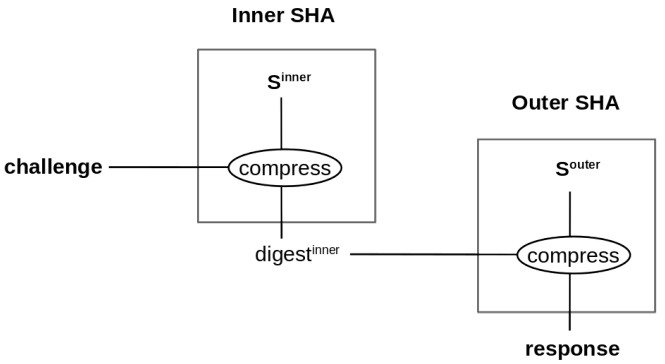


The compress function

1. Extend **challenge** to 64 words.
2. (a,b,c,d,e,f,g,h) := $\mathbf{S^{inner}}$
3. Do 64 times:

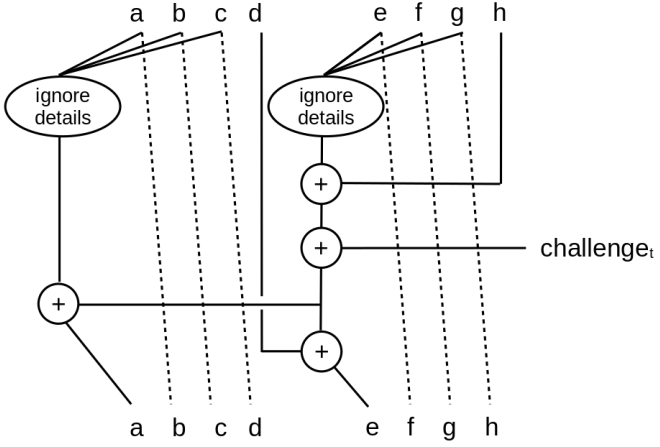


HMAC-SHA256



The compress function

1. Extend **challenge** to 64 words.
2. (a,b,c,d,e,f,g,h) := $\mathbf{S^{inner}}$
3. Do 64 times:

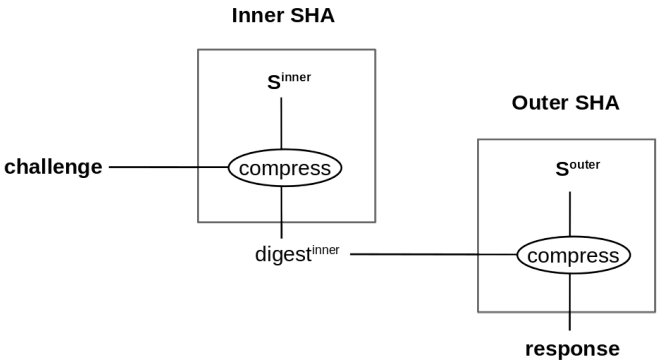


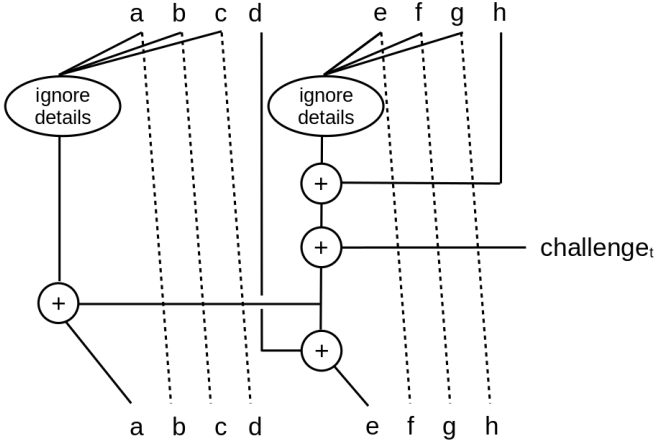
4. $digest^{inner}$:= (a,b,c,d,e,f,g,h) + $\mathbf{S^{inner}}$

HMAC-SHA256

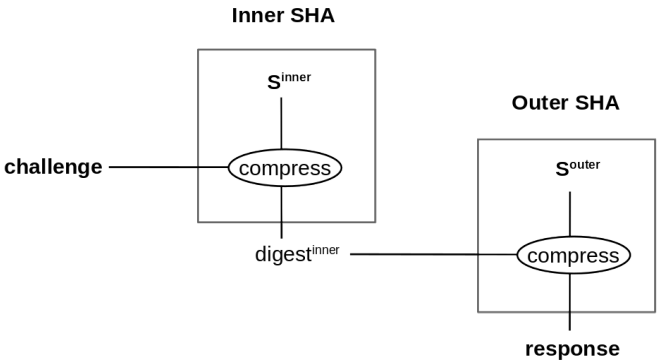
Persistent versus ephemeral variables:

- a and e are persistent
  - $d_{t+3} = c_{t+2} = b_{t+1} = a_t$
  - $h_{t+3} = g_{t+2} = f_{t+1} = e_t$



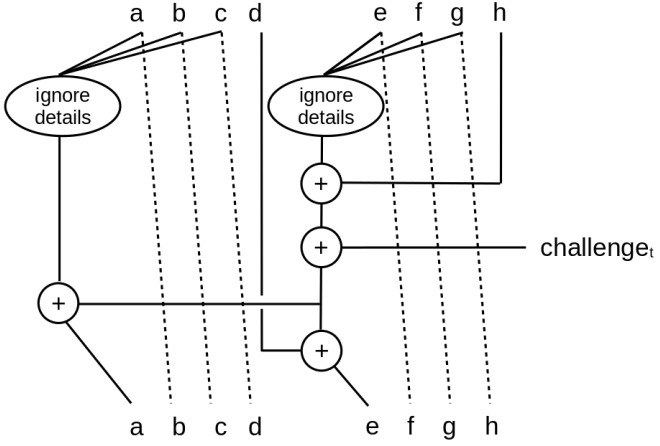


HMAC-SHA256

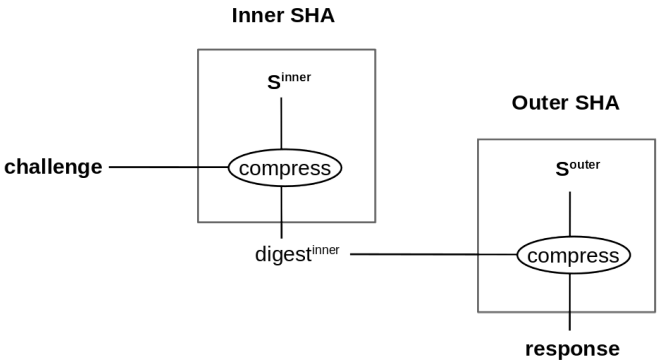


Persistent versus ephemeral variables:

- a and e are persistent
  - $d_{t+3} = c_{t+2} = b_{t+1} = a_t$
  - $h_{t+3} = g_{t+2} = f_{t+1} = e_t$
- Intermediates of „ignore details“ are ephemeral

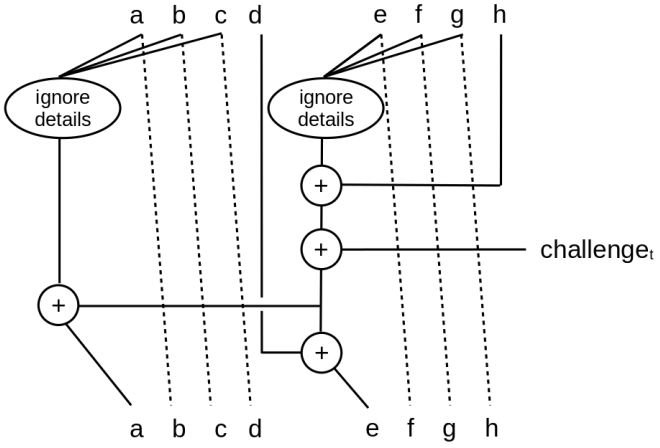


HMAC-SHA256

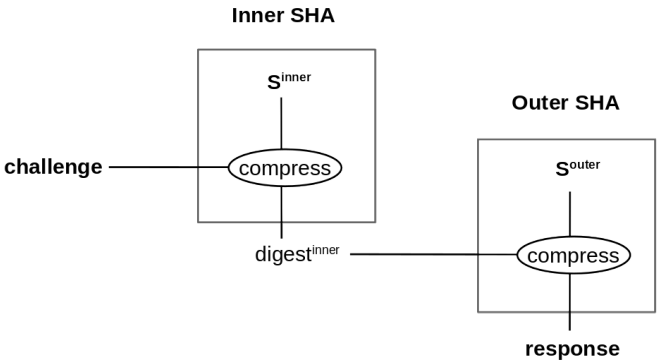


Persistent versus ephemeral variables:

- a and e are persistent
  - $d_{t+3} = c_{t+2} = b_{t+1} = a_t$
  - $h_{t+3} = g_{t+2} = f_{t+1} = e_t$
- Intermediates of „ignore details“ are ephemeral
- Hamming distance is ephemeral

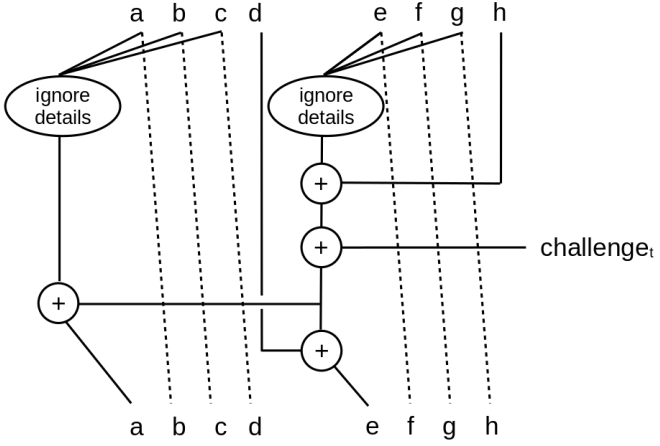


HMAC-SHA256



Persistent versus ephemeral variables:

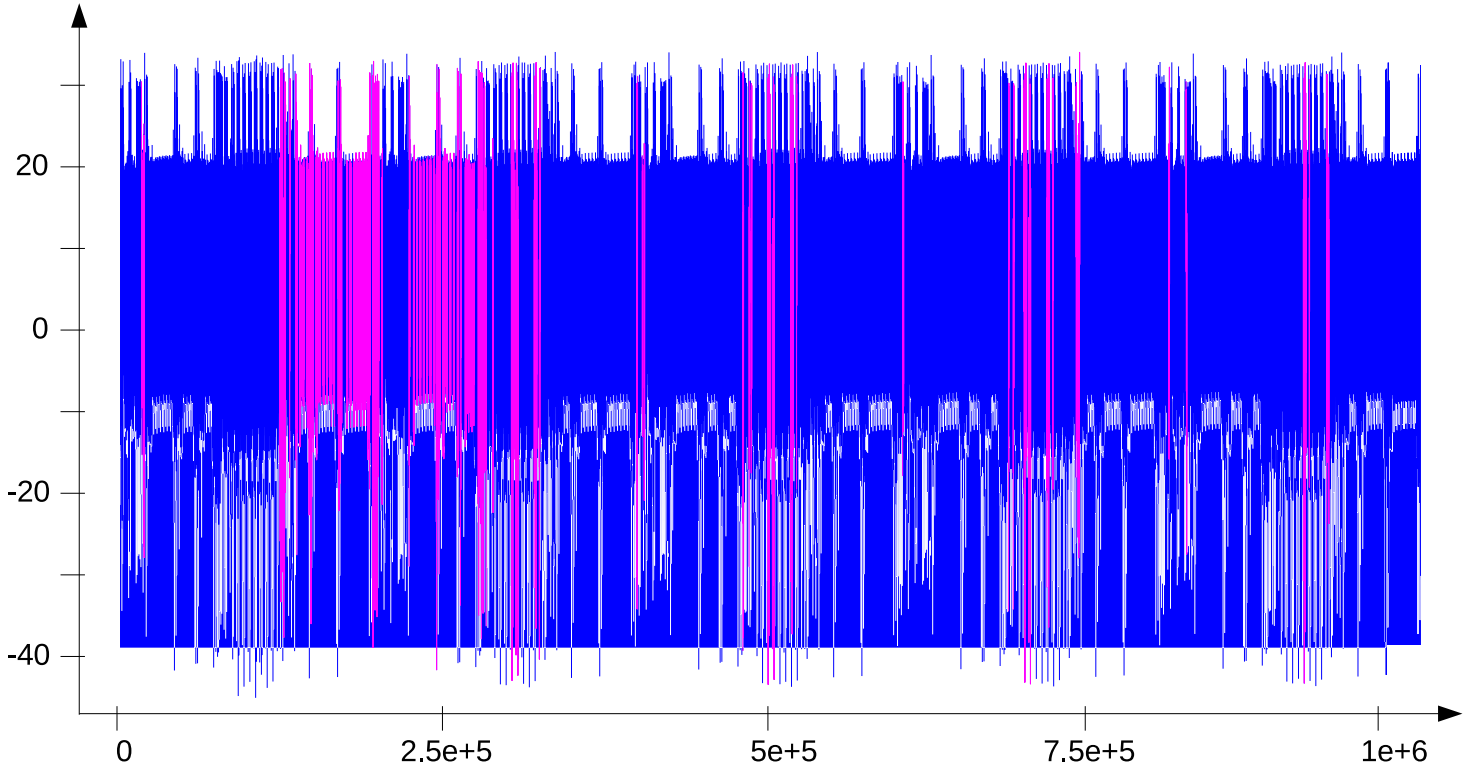
- a and e are persistent
  - $d_{t+3} = c_{t+2} = b_{t+1} = a_t$
  - $h_{t+3} = g_{t+2} = f_{t+1} = e_t$
- Intermediates of „ignore details“ are ephemeral
- Hamming distance is ephemeral



NEW: DPA only targeting persistent variables

HMAC-SHA256

Example: Leakage of a_4 and e_4 in rounds 3...7



Outline

- HMAC-SHA256
- New attack strategy ←
- Attack demonstration on the Bq27Z561 battery IC
- Alternative approach to accessory authentication

New attack strategy

Leakage model:

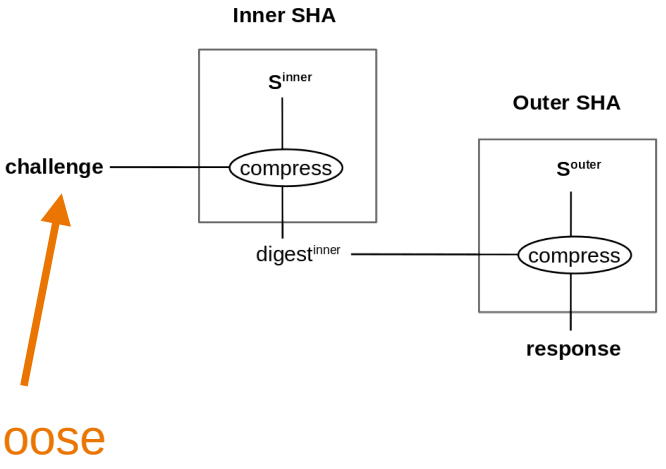
HW leakage of a_t,e_t for t=1,2,3,4, 60,61,62,63

Combine

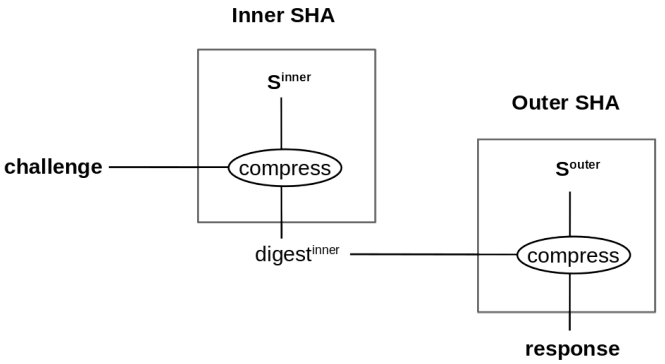
- Known attack on $\mathbf{S^{inner}}$
- New attack on $\mathbf{S^{outer}}$

New attack strategy

Known attack on $\mathbf{S^{inner}} = (a_0,\ldots,h_0)$



New attack strategy

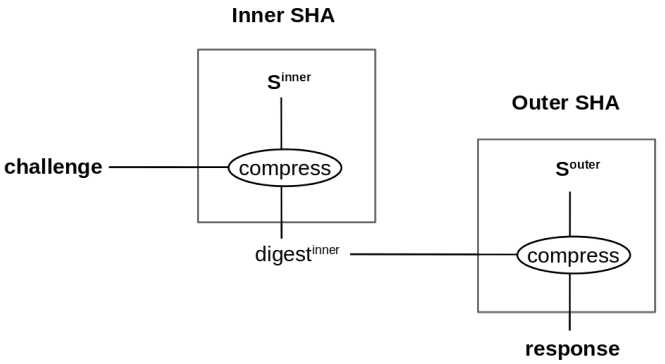


Known attack on $\mathbf{S^{inner}} = (a_0,\ldots,h_0)$

- Targets:

$a_t(0) := a_t(\text{challenge}=(0,0,\ldots))$
$e_t(0) := e_t(\text{challenge}=(0,0,\ldots))$

New attack strategy



Known attack on $\mathbf{S^{inner}} = (a_0,\ldots,h_0)$

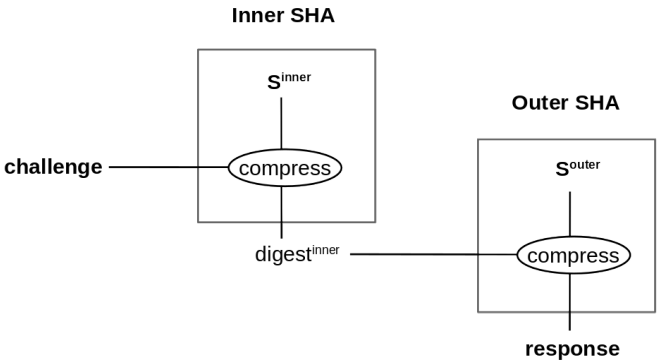
- Targets:

  $a_t(0) := a_t(\text{challenge}=(0,0,\ldots))$
  $e_t(0) := e_t(\text{challenge}=(0,0,\ldots))$

- 4 DPAs

1. DPA on $a_1(0)$ and $e_1(0)$ with challenge=(random, …)
2. DPA on $a_2(0)$ and $e_2(0)$ with challenge=(0, random,…)
3. DPA on $a_3(0)$ and $e_3(0)$ with challenge=(0,0, random,…)
4. DPA on $a_4(0)$ and $e_4(0)$ with challenge=(0,0,0, random,…)

New attack strategy



Known attack on $\mathbf{S^{inner}} = (a_0,\ldots,h_0)$

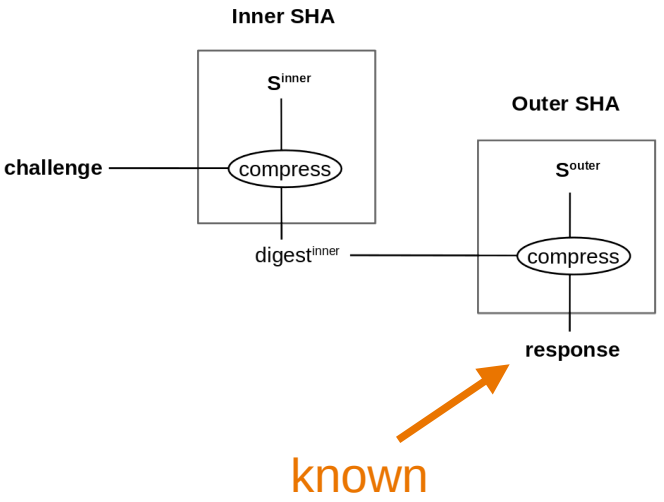
- Targets:

  $a_t(0) := a_t(\text{challenge}=(0,0,\ldots))$
  $e_t(0) := e_t(\text{challenge}=(0,0,\ldots))$

- 4 DPAs
  1. DPA on $a_1(0)$ and $e_1(0)$ with challenge=(random, …)
  2. DPA on $a_2(0)$ and $e_2(0)$ with challenge=(0, random,…)
  3. DPA on $a_3(0)$ and $e_3(0)$ with challenge=(0,0, random,…)
  4. DPA on $a_4(0)$ and $e_4(0)$ with challenge=(0,0,0, random,…)
- Compute back $\mathbf{S^{inner}}$ from $a_1(0),e_1(0),\ldots,a_4(0),e_4(0)$

New attack strategy

New attack on $\mathbf{S^{outer}}$

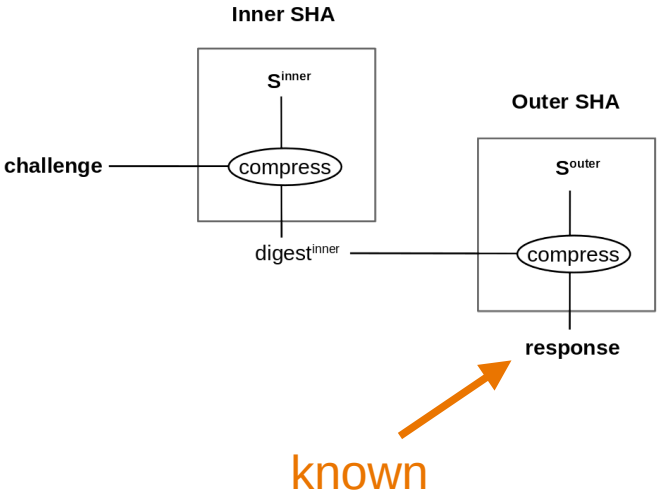


New attack strategy

New attack on $\mathbf{S^{outer}}$

- Final addition:

$$\mathbf{response} = \mathbf{S^{outer}} + (a_{64},\ldots,h_{64})$$



New attack strategy

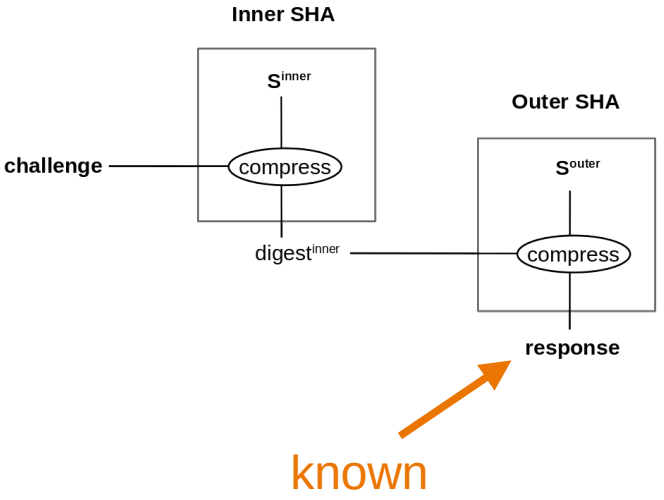
New attack on $\mathbf{S^{outer}}$

- Final addition:

  $\mathbf{response} = \mathbf{S^{outer}} + (a_{64},\ldots,h_{64})$

- DPA attack on:

  $(a_{64},\ldots,h_{64}) = \mathbf{response} - \mathbf{S^{outer}}$



New attack strategy

New attack on $\mathbf{S^{outer}}$

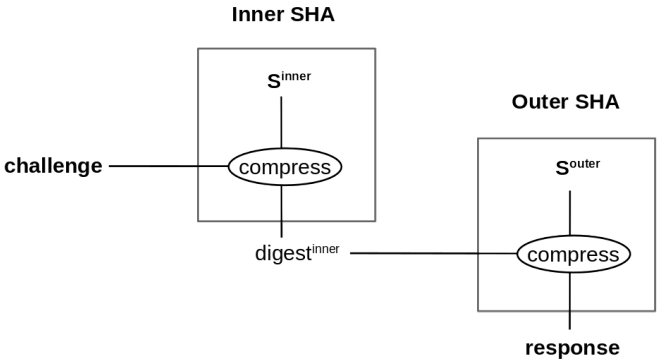
- Final addition:

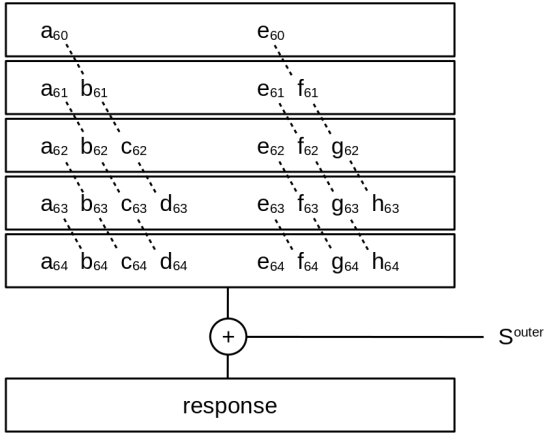
  $$\mathbf{response} = \mathbf{S^{outer}} + (a_{64},\ldots,h_{64})$$

- DPA attack on:

  $$(a_{64},\ldots,h_{64}) = \mathbf{response} - \mathbf{S^{outer}}$$

Leaking in rounds
t=61,…,63





New attack strategy

New attack on $\mathbf{S^{outer}}$

- Final addition:

  $$\mathbf{response} = \mathbf{S^{outer}} + (a_{64},\ldots,h_{64})$$

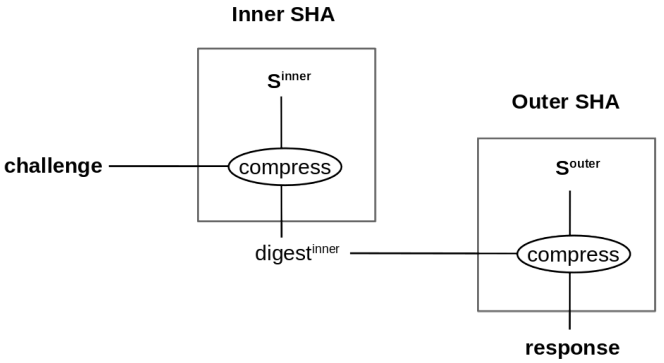
- DPA attack on:

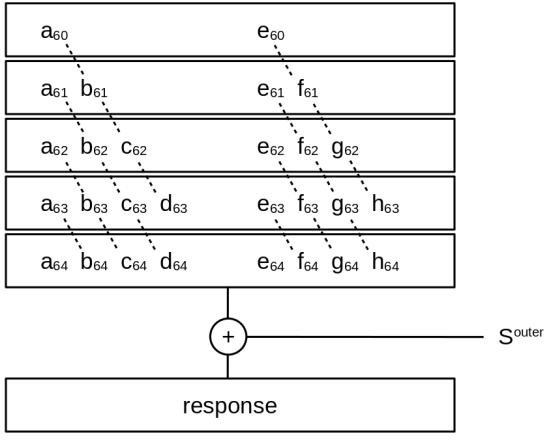
  $$(a_{64},\ldots,h_{64}) = \mathbf{response} - \mathbf{S^{outer}}$$

Leaking in rounds t=61,…,63

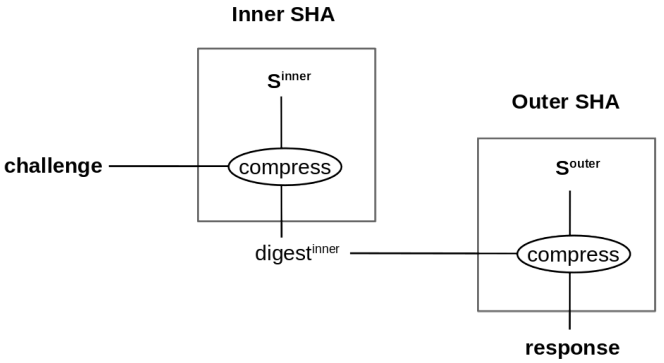
Known & random

Secret & constant





New attack strategy



New attack on $\mathbf{S^{outer}}$

- Final addition:

  $\mathbf{response} = \mathbf{S^{outer}} + (a_{64},\ldots,h_{64})$

- DPA attack on:

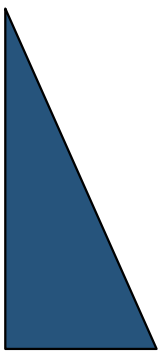
  $(a_{64},\ldots,h_{64}) = \mathbf{response} - \mathbf{S^{outer}}$

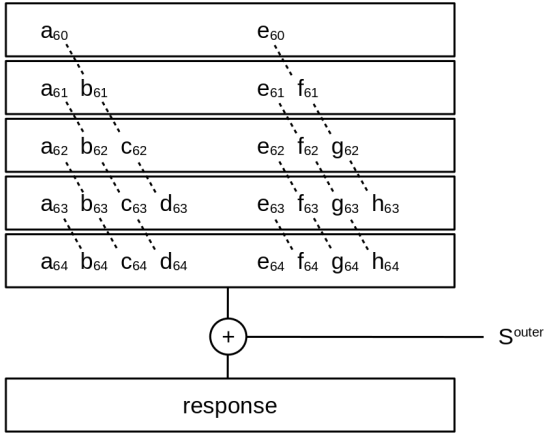
  a_{64} leakage => $\mathbf{S^{outer}}[0]$

  a_{63} leakage => $\mathbf{S^{outer}}[1]$

  a_{62} leakage => $\mathbf{S^{outer}}[2]$

  a_{61} leakage => $\mathbf{S^{outer}}[3]$

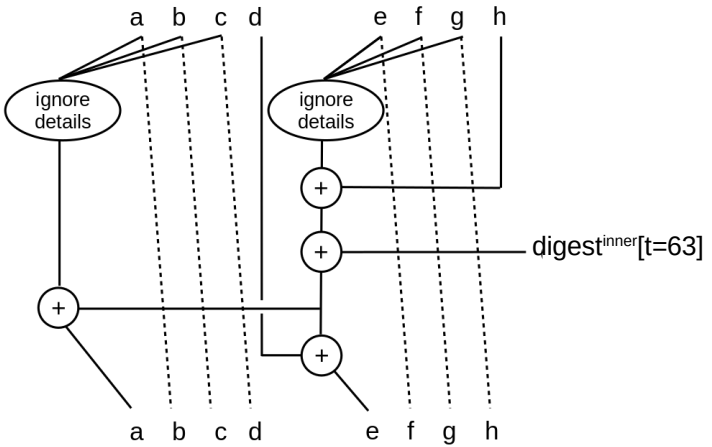


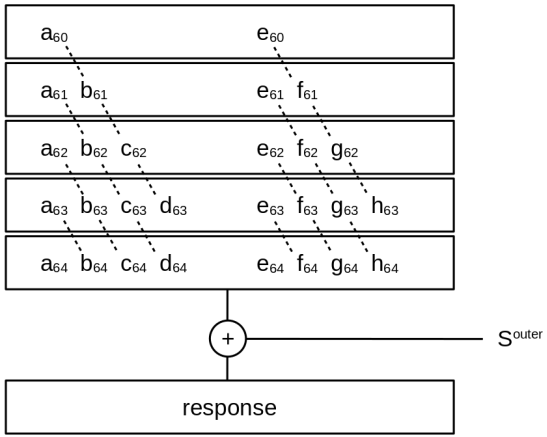


New attack strategy

New attack on $\mathbf{S^{outer}}$

- Optimize disclosure of $\mathbf{S^{outer}}[0,4]$:

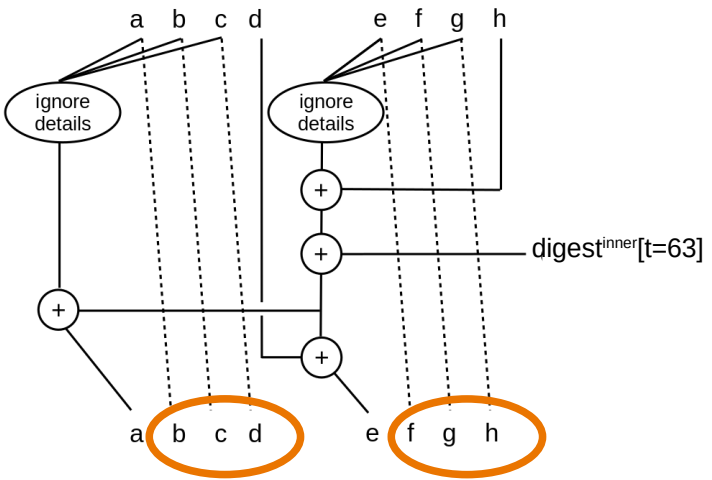


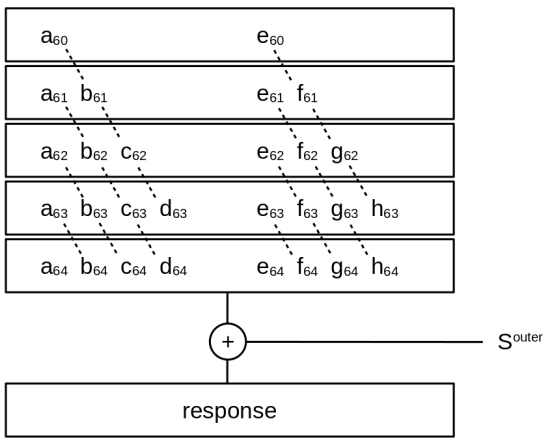


New attack strategy

New attack on $\mathbf{S^{outer}}$

- Optimize disclosure of $\mathbf{S^{outer}}[0,4]$





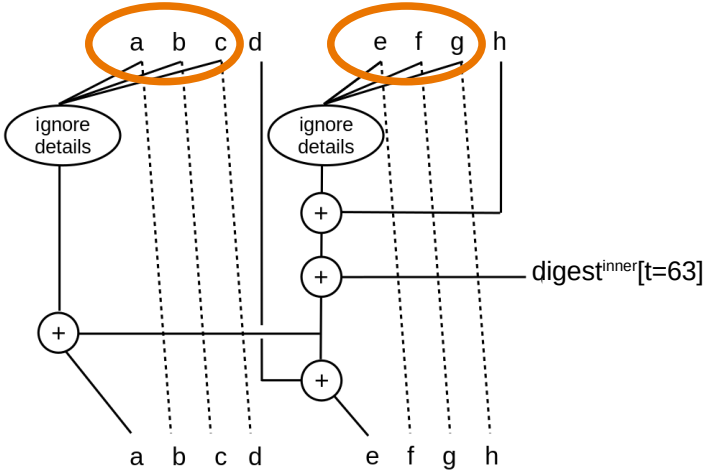
Known from response - S^{outer}

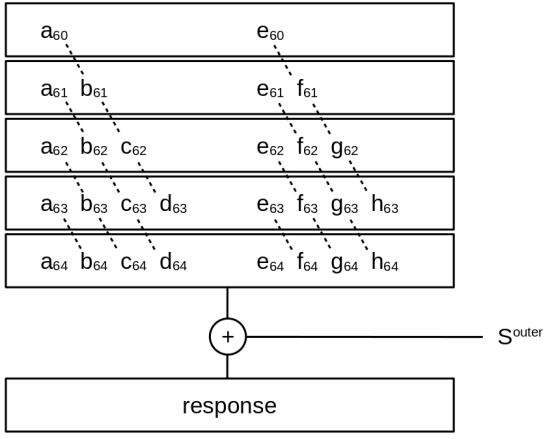
New attack strategy

New attack on $\mathbf{S^{outer}}$

- Optimize disclosure of $\mathbf{S^{outer}}[0,4]$

Known from response - S^{outer}



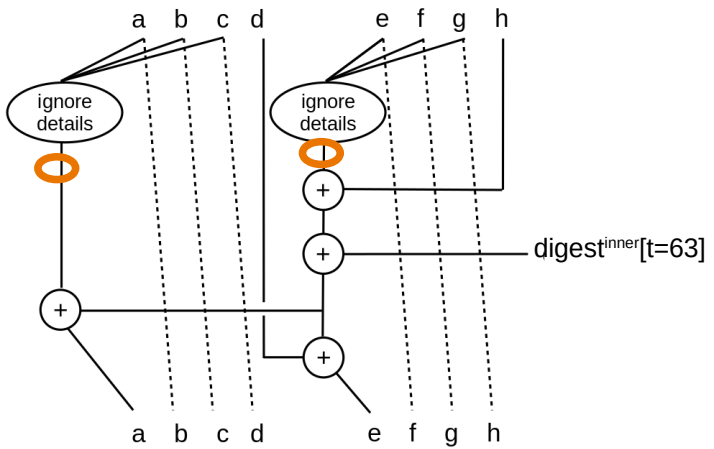


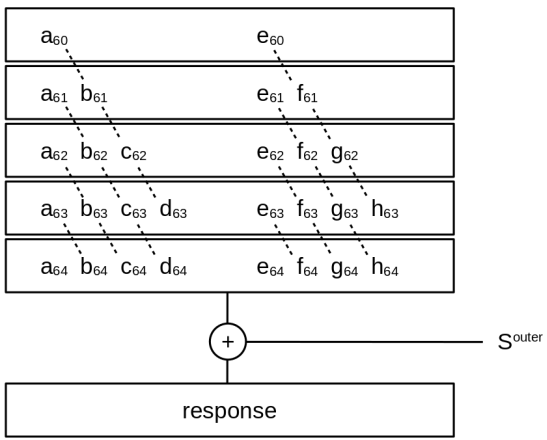
New attack strategy

New attack on $\mathbf{S^{outer}}$

- Optimize disclosure of $\mathbf{S^{outer}}[0,4]$

Known from response - S^{outer}



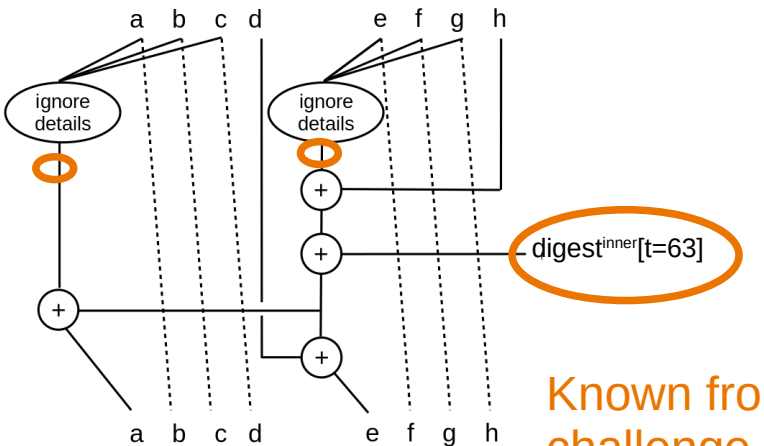


New attack strategy

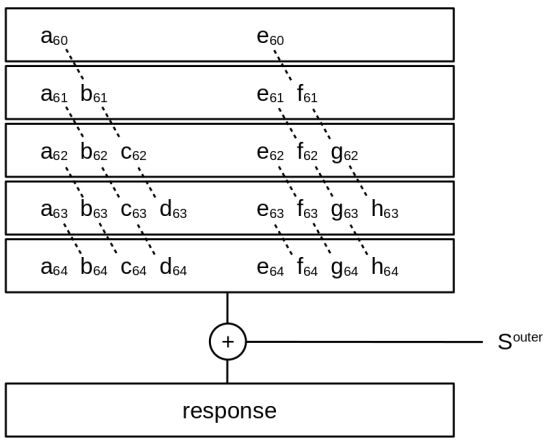
New attack on **S^{outer}**

- Optimize disclosure of **S^{outer}**[0,4]

Known from response - S^{outer}



Known from challenge and S^{inner}

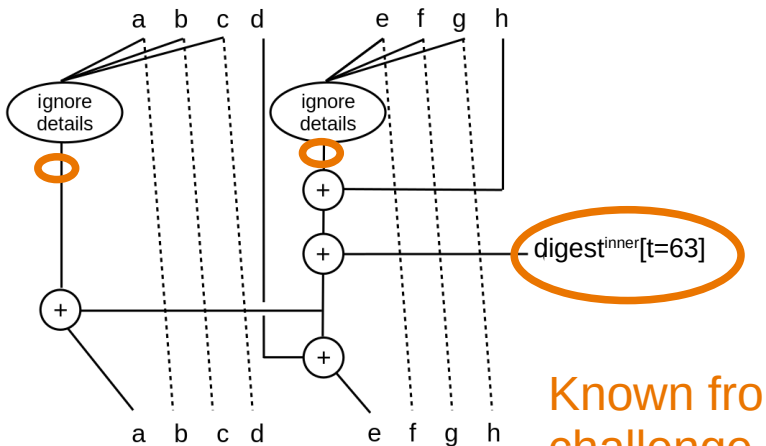


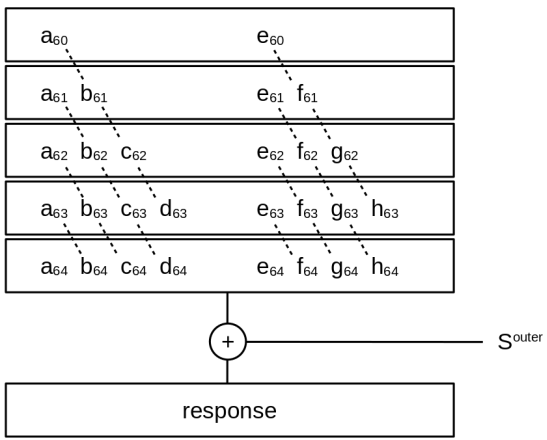
New attack strategy

New attack on **S^{outer}**

- Optimize disclosure of **S^{outer}**[0,4]

Known from response - S^{outer}





Known from challenge and S^{inner}

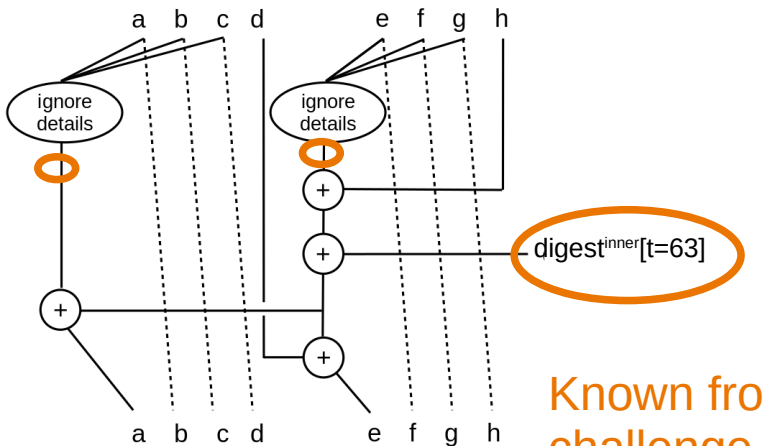
=> a_{64} = known data + h_{63}

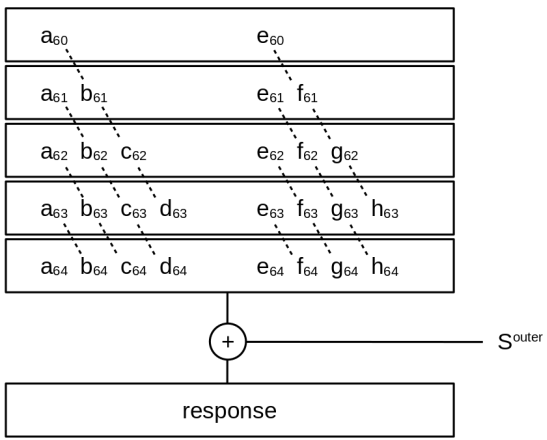
New attack strategy

New attack on **S^{outer}**

- Optimize disclosure of **S^{outer}**[0,4]

Known from response - S^{outer}





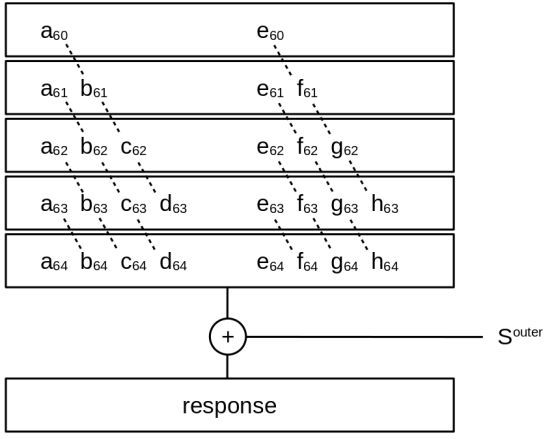
Known from challenge and S^{inner}

=> a_{64} = known data + e_{60}

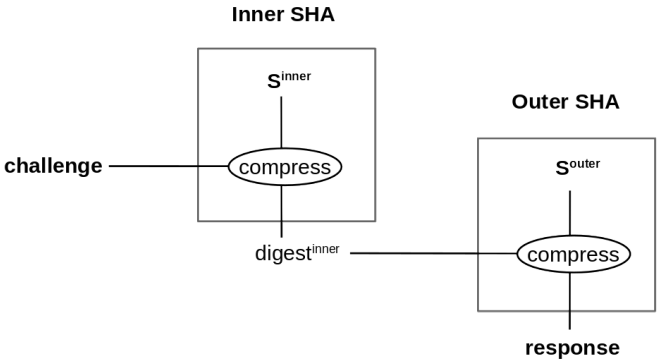
New attack strategy

New attack on $\mathbf{S^{outer}}$

- Optimize disclosure of $\mathbf{S^{outer}}[0,4]$:
  - e_{60} leakage => $\mathbf{S^{outer}}[0]$
  - a_{63} leakage => $\mathbf{S^{outer}}[1]$
  - a_{62} leakage => $\mathbf{S^{outer}}[2]$
  - a_{61} leakage => $\mathbf{S^{outer}}[3]$



New attack strategy



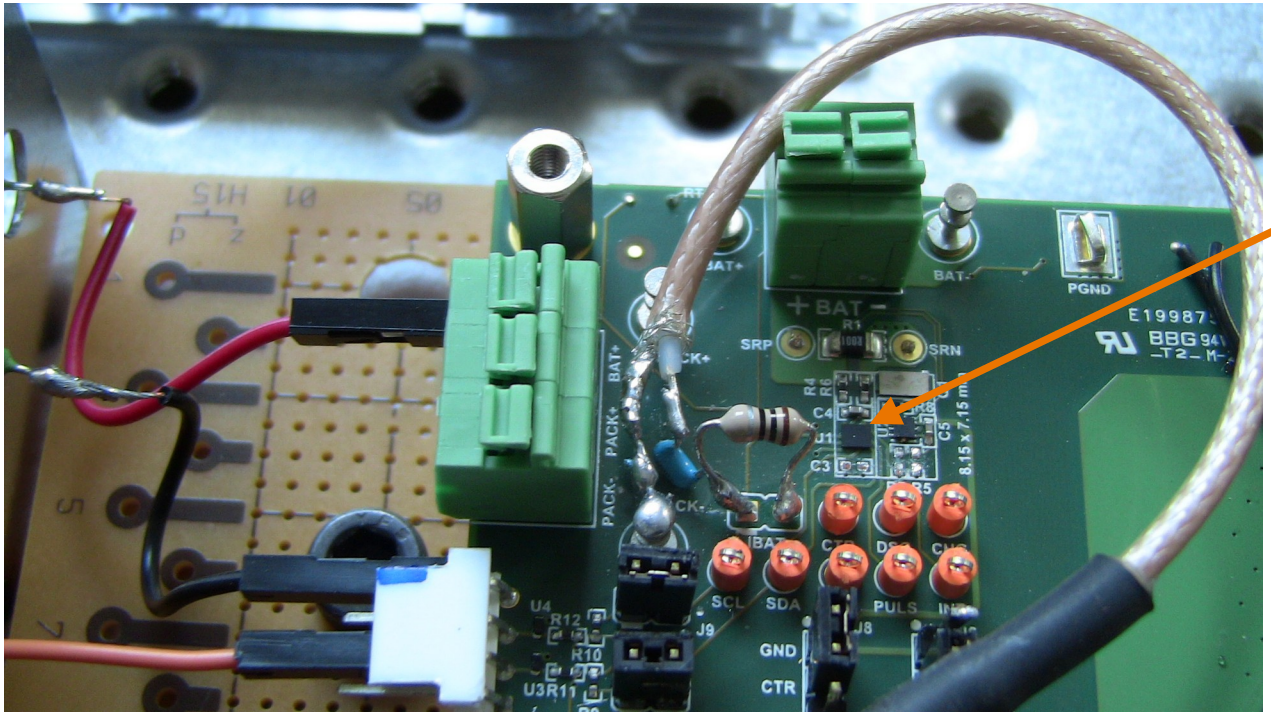
Summary:

- New attack on HMAC only targeting persistent variables a and e.
- Applicable similar to SHA1 and SHA512
- Not applicable to SHA384 due to truncated response

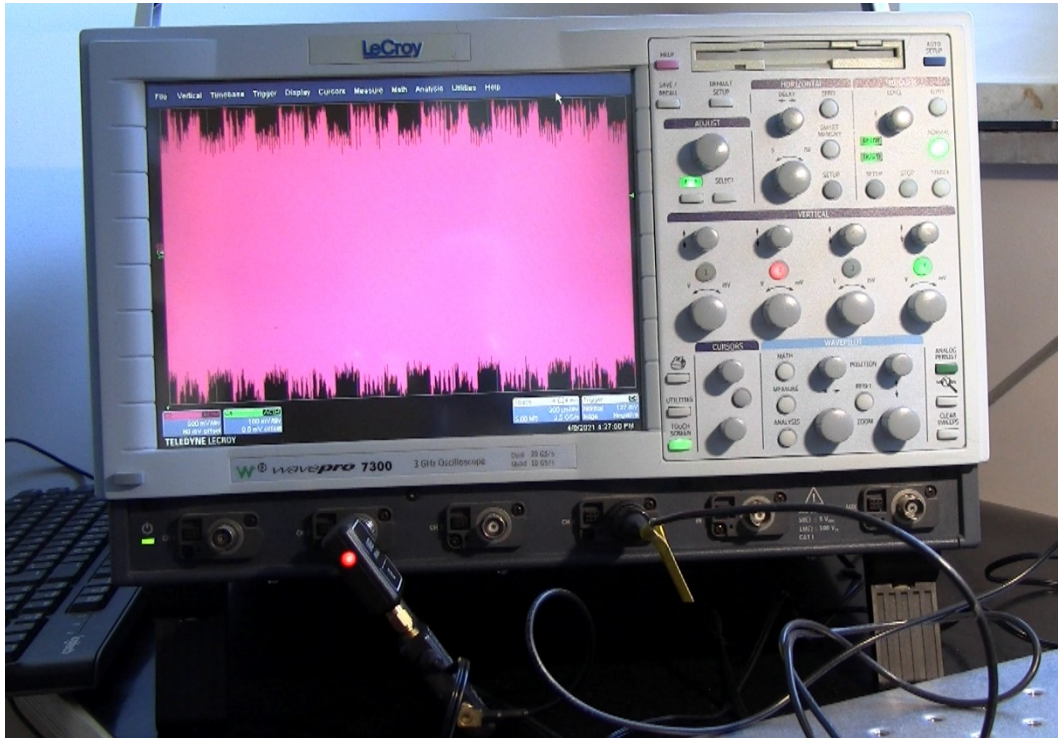
Outline

- HMAC-SHA256
- New attack strategy
- Attack demonstration on the Bq27Z561 battery IC ←
- Alternative approach to accessory authentication

Attack demonstration



Attack demonstration



Alternative approach

Hardware intrinsic accessory authentication

- Cheaper than certified security controllers
- Our solution is based on MCU intrinsic timing properties
- SIMPL = SIMulation Possible but Laborious is sufficient for the use case

The End

Thank you for your attention!

Contact:

Frank.Schuhmacher@segrids.com
www.segrids.com