- Remote attestation (last class)
- Selected storage
- Flicker

- The key should only be stored in a certain application.
- The identity of the movie application is the Harsh in TCM.
- The key is secure and temporary.
- When the application reboot again, the system will send ‘SS’ to TPM to unseal, then the TPM will compare $h_s$ with $h_s = H(\text{System})$. If it matches, TCM will send the $k$ to the system.

When the system is rebooted, the attacker may replace $E(DB)$ by the old $E(k, DB)$. The TPM will be a $ctr$, every time it seals, it will send the $ctr$ ($SS_T = E(P_{tt}, h_T || ctr || S_T)$).

To unseal it, the $ctr$ should be the same.
Flicker:

The only thing of the trust hardware is TPM

Flicker depends on SKINIT (construct the Flicker)

SKINIT: allow system reboot, transfer it into trusted code.

\[
\text{SKINIT} (p, n) \quad \text{Disables interrupt}
\]

\[
h = H(p[0], \ldots, p[n-1]) \quad \text{Disables DMA access to P}
\]

\[
jmp p \quad \text{Disables debugging}
\]

\[
\text{Recuts cpu}
\]

How PAL will be organized?

To enter PAL:

1. Copy inputs to PAL

1.5 to output area

2. Save return state to saved information
   - Registers
   - Page table pointers
   - Other basic state
3. SKINIT(PAL, n)
   h = H(PAL, n)

next fill the output into the hash

To exit a PAL:

1. Write output to output area

   When do SKINIT, it will not do EXTEND

2. EXTEND (output area)
   EXTEND (p, n)
   h = H(h || p[0], ... , p[n-1])

3. EXTEND (0000...0): the end of the execution of PAL
   means I am done

4. Restore OS state from saved information