TimeTravel: Real-time Timing Drift Attack on System Time Using Acoustic Waves

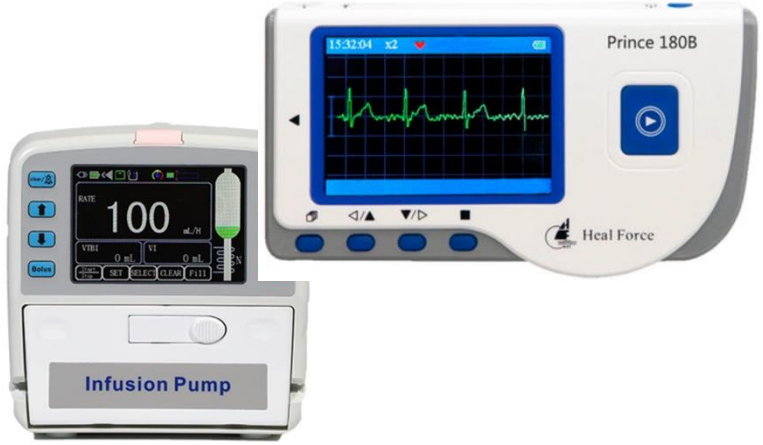
Jianshuo Liu, Hong Li, Haining Wang, Mengjie Sun, Hui Wen, Jinfa Wang, Limin Sun

Institute of Information Engineering, Chinese Academy of Sciences
Department of Electrical and Computer Engineering, Virginia Tech

中国科学院信息工程研究所
INSTITUTE OF INFORMATION ENGINEERING,CAS

VIRGINIA TECH

Timestamps Are Widely Used in Embeeded Devices



IoT hub

Schedules timed tasks for paired devices

PLC controller

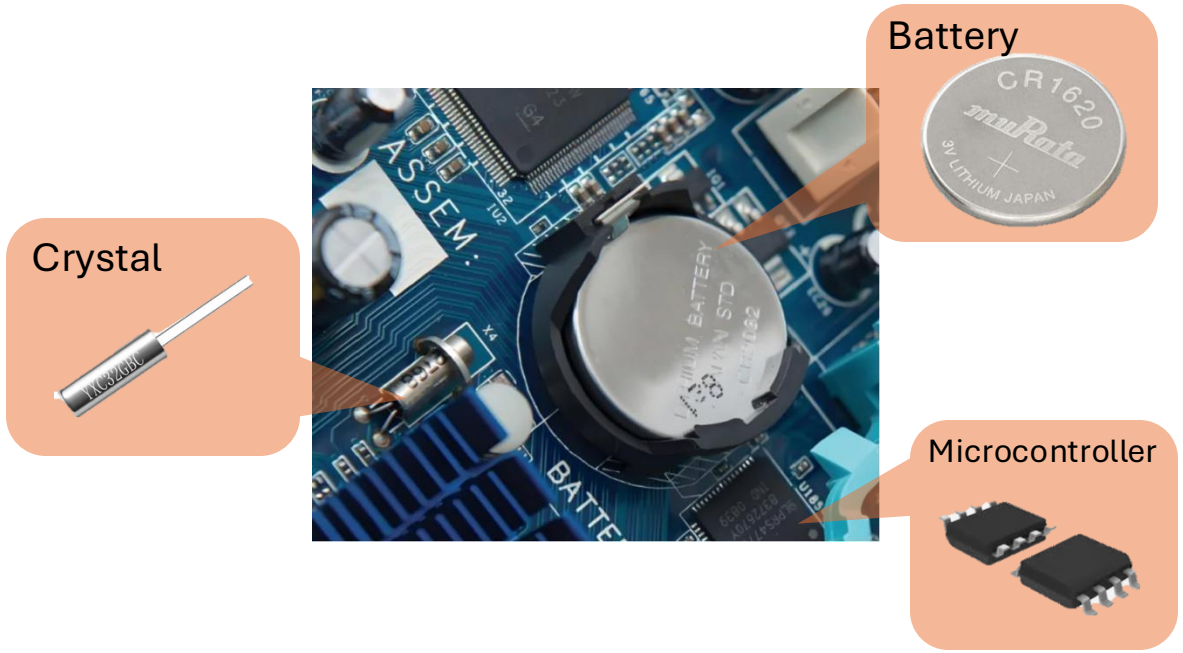
Records events and executes scheduled tasks

Medical devices

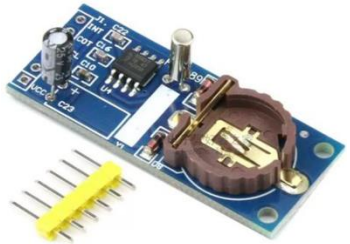
Uses timestamps to record patient vital signs accurately

Timestamps can be generated by Real-time Clock(RTC) Circuit

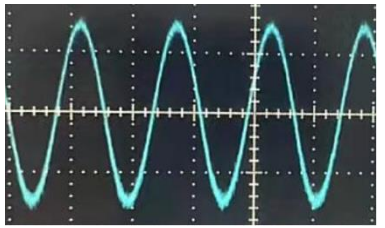
RTC Working Principle



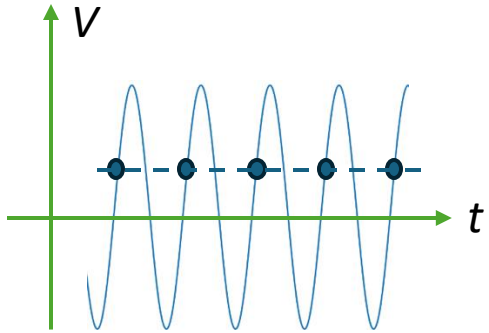
RTC Circuit



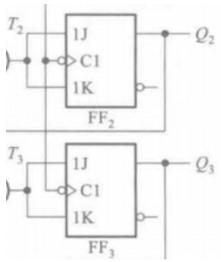
RTC Crystal Generates Oscillation Signal



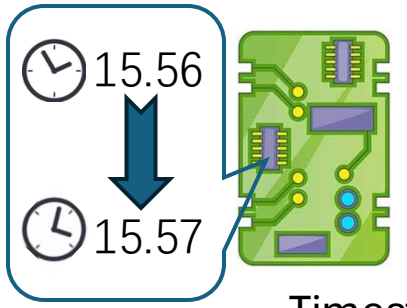
Waveform



Filter+ Edge triggering



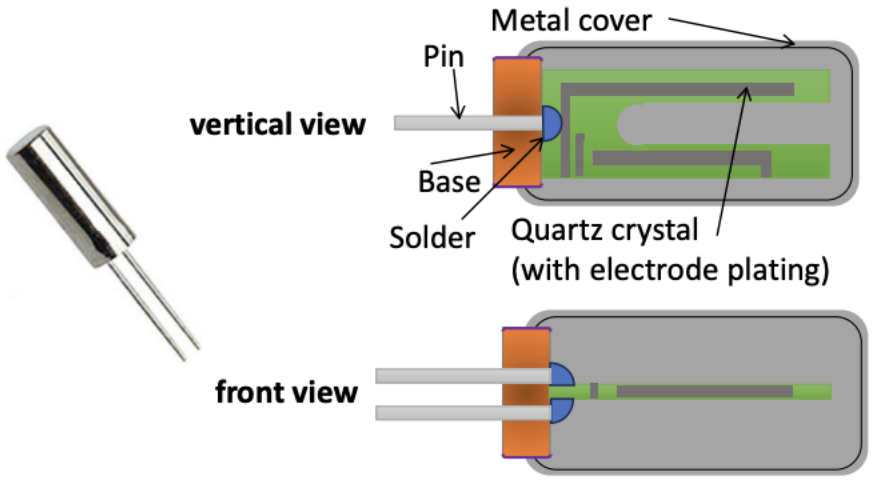
MCU digit counter increments by one



Timestamps increase

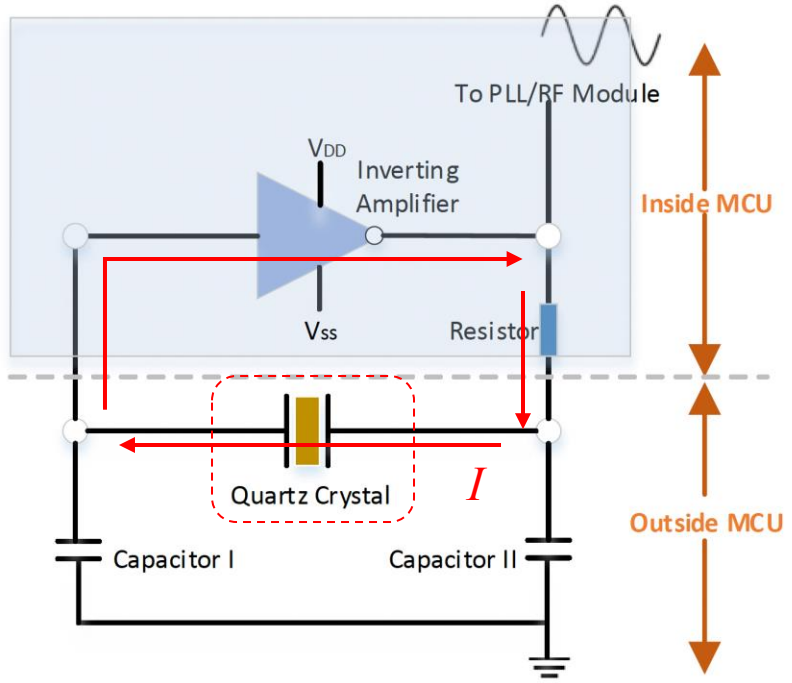
RTC Timing Principle

Quartz Crystal

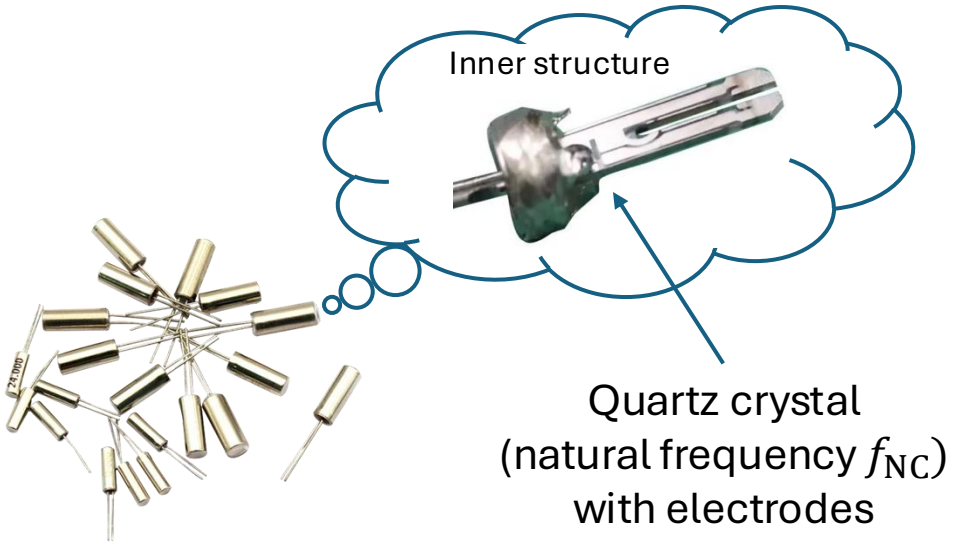


Equivalent

To Inductance

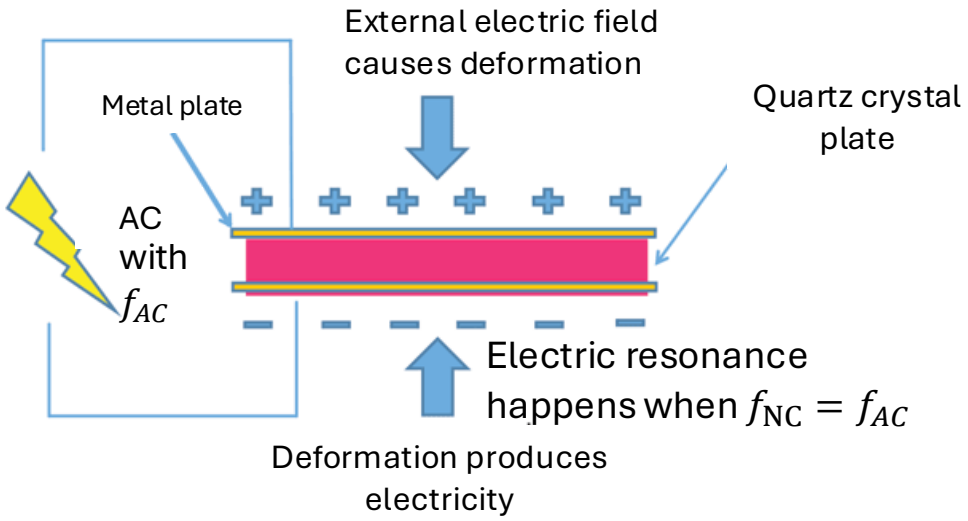


Piezoelectric and Resonance Effect



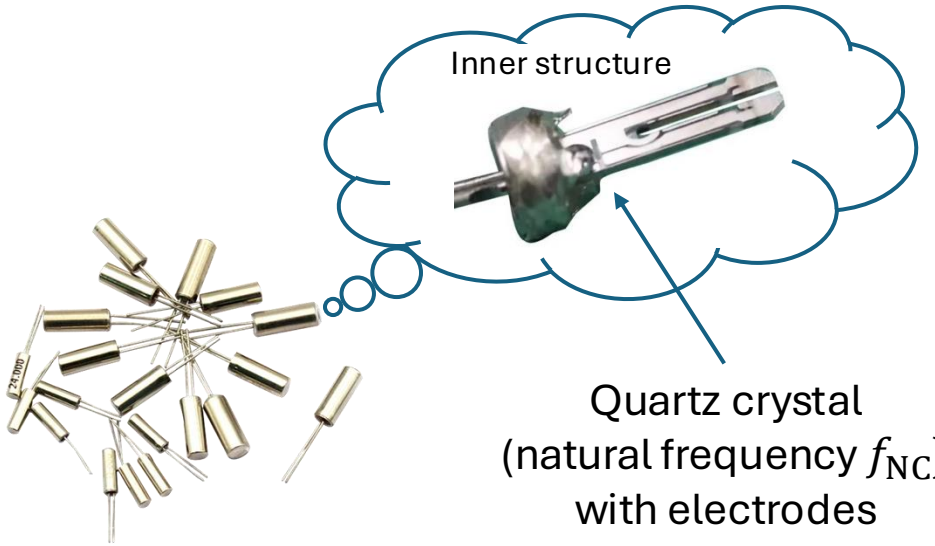
Exhibits

Piezoelectric effect



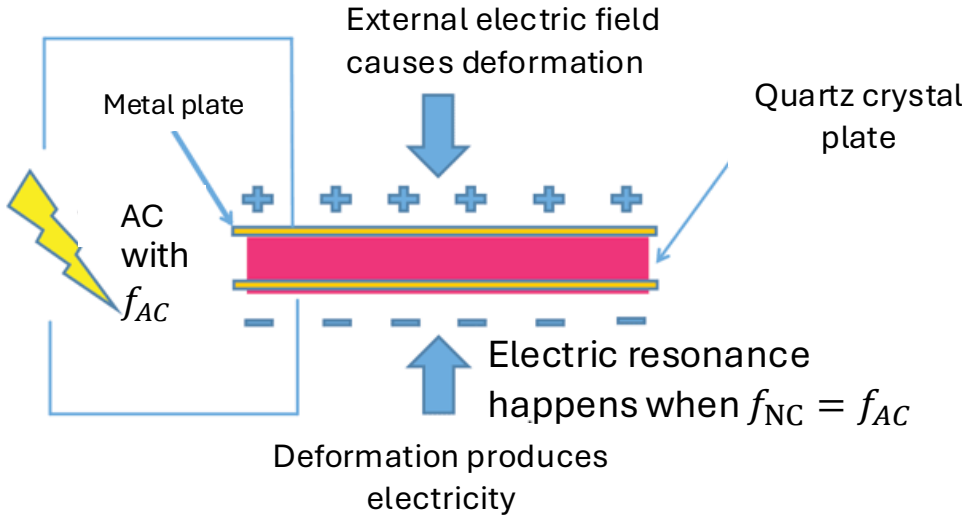
A crystal may experience jitter when subjected to resonant excitation!

Motivation



Exhibits

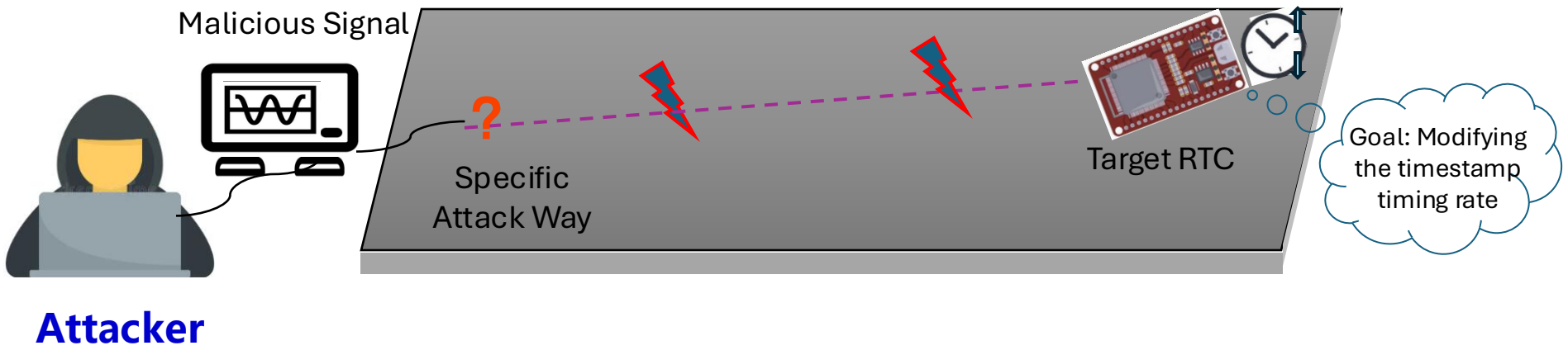
Piezoelectric effect



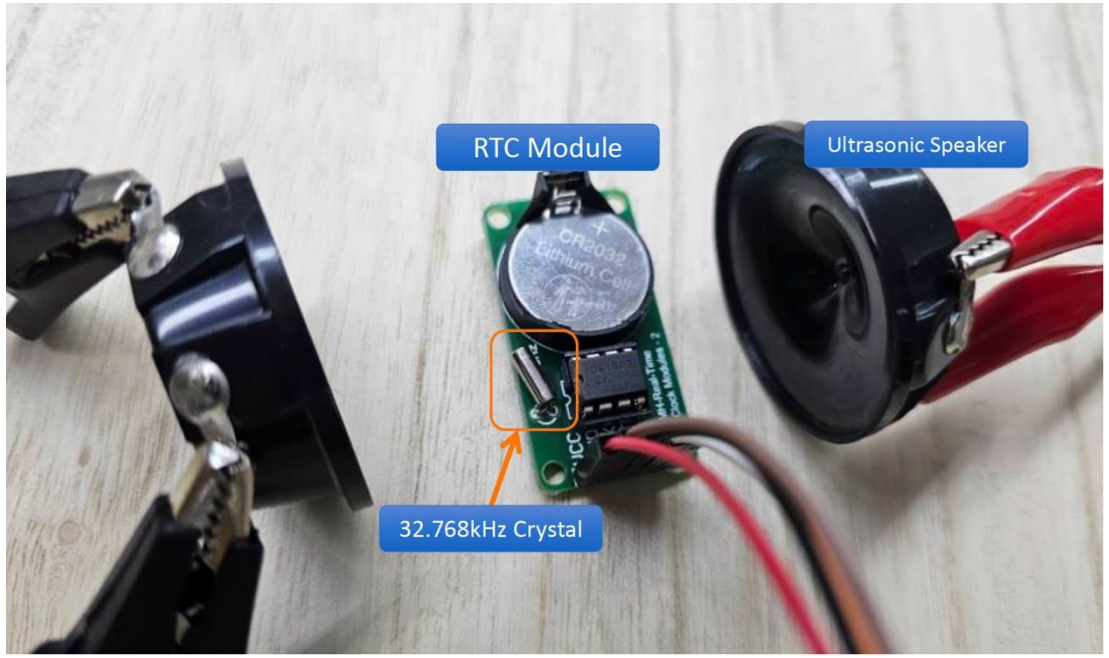
Is it possible to manipulate the RTC timing via a crystal?

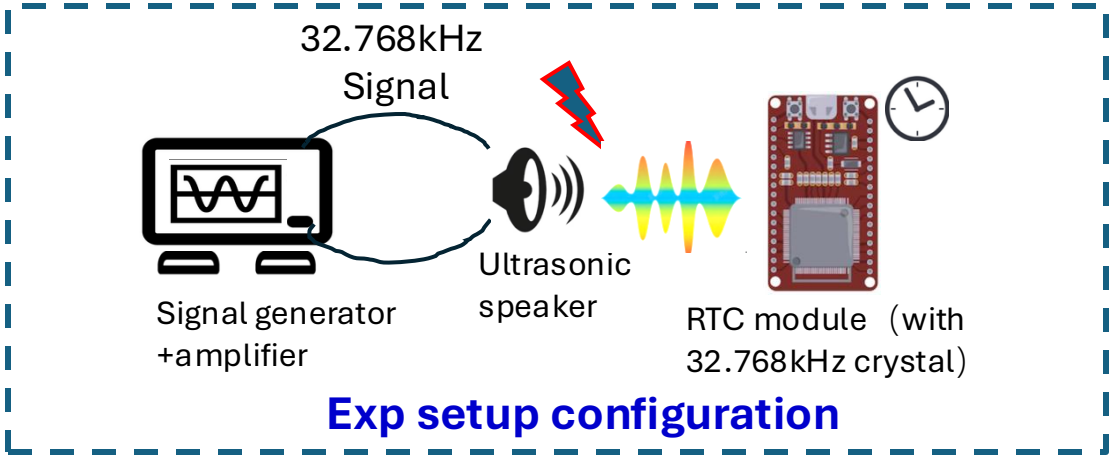
Threat Model

- Close-proximity, non-invasive attack
- Attackers can secretly set up attack equipment in the target environment in advance
- Attackers pretest an identical device in advance but can only infer component status during the attack via EM leakage

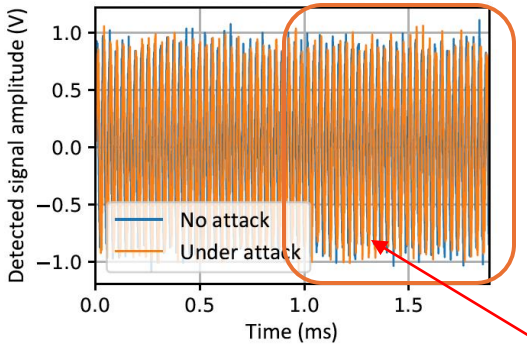


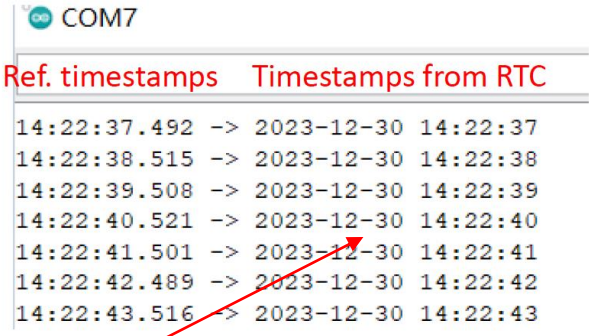
Attack Strategy Exploration





Exp setup configuration



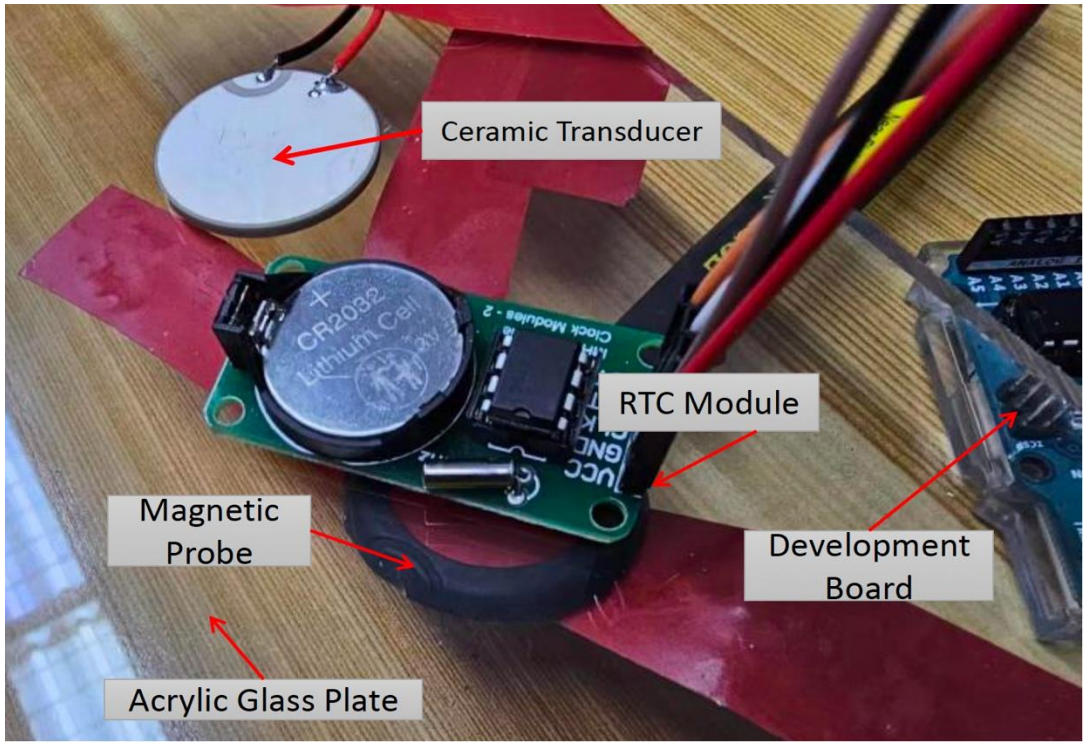


Testing results

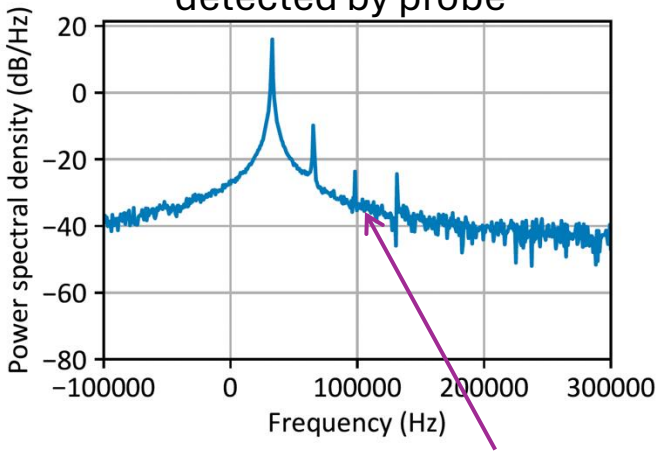
The large air–solid acoustic-impedance mismatch makes it difficult for sound to penetrate the shell and excite resonance

What if vibration is directly applied to the surface where the module is attached?

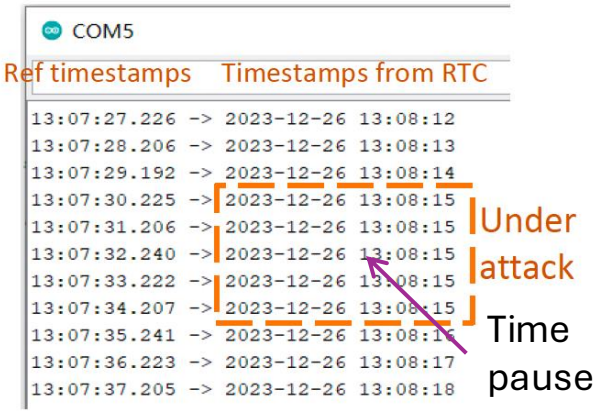
Attack Strategy Exploration

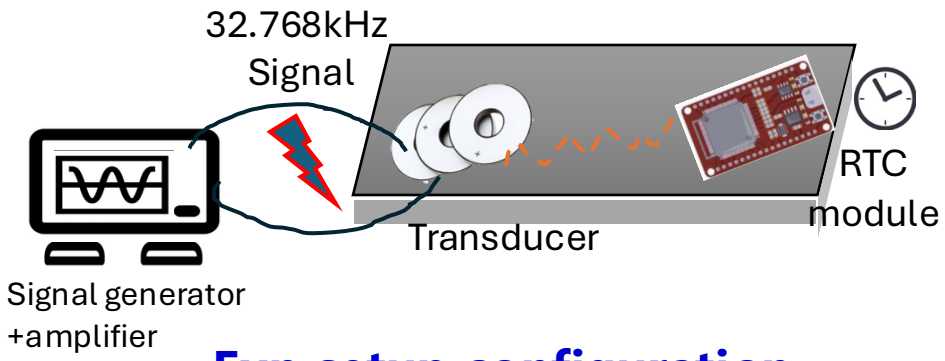


Oscillation signals detected by probe



Burrs caused by phase jitter

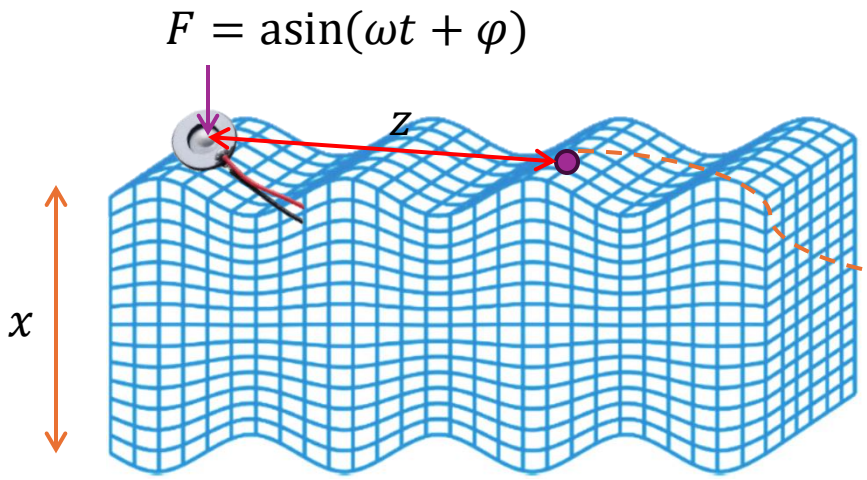




Exp setup configuration

Solid vibration waves circumvent acoustic impedance mismatches, transferring energy to the crystal oscillator to cause resonance

Lamb Wave



$$u_x(t) = [\alpha A \cos(\alpha x) - ik_a B \cos(\beta x)] \cdot V \cdot e^{i(\omega(t-t_T)+\varphi-k_a z)}$$

The frequency, amplitude and phase pattern of the longitudinal displacement of particles on the solid surface are fixed and follow a sinusoidal pattern

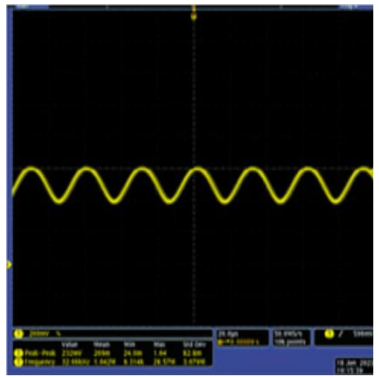
Attack Strategy Exploration

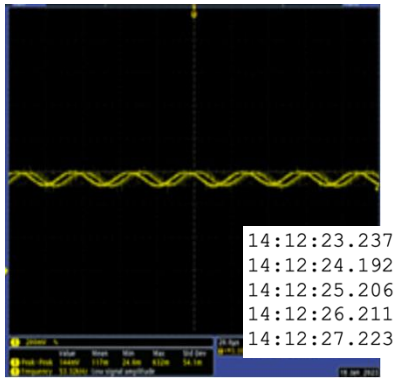
Apply 32.768kHz vibration with different initial phases Φ' to the crystal oscillator

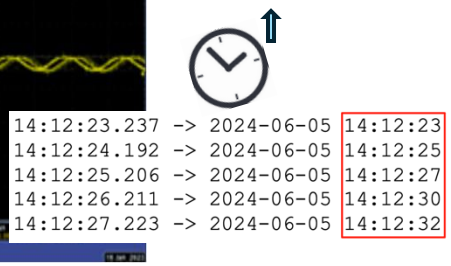
*Send continuous vibration for 0.01ms when observed phase $\varphi = \frac{\pi}{2}$

Setting..

$\Phi' = \frac{\pi}{6}$



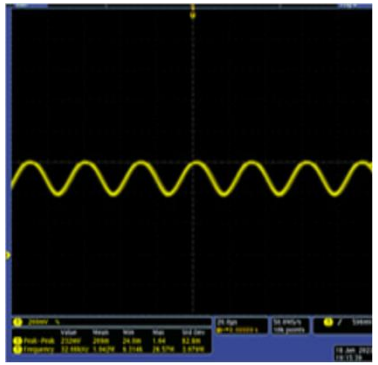


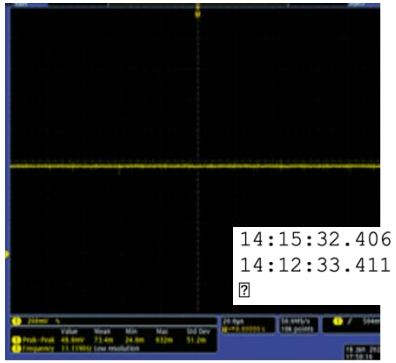


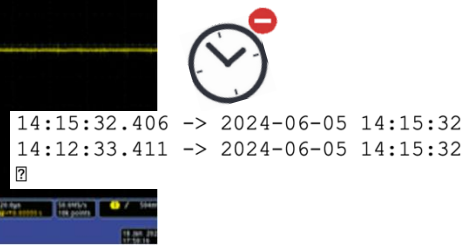
Normal

Jitter/Amplitude changed

$\Phi' = \frac{3\pi}{2}$







Normal

Nearly stop vibration

Interference between signals with different phases alters the timing rate.

Methodology

1.Building Timing Response Dataset

Medium	Wave Speed($10^3 m/s$)		Density
	Longitudinal	Transverse	(g/cm^3)
Aluminum	6.26	3.08	2.7
Stainless steel	6.10	3.30	7.85
Quartz glass	5.57	3.52	2.2
Acrylic glass	2.70	1.30	1.18
Hard rubber plastic	2.30	0.94	1.22
Oak wood	3.31	1.55	0.85
Polyethylene	2.14	0.72	0.94
	c_L	c_T	

1. Look up medium properties c_L, c_T

$$u_x(t) = [\alpha A\cos(\alpha x) - ik_a B\cos(\beta x)]\cdot V\cdot e^{i(\omega(t-t_T)+\varphi-k_a z)}$$

where $\alpha = \sqrt{(\frac{\omega^2}{c_L})^2 - k_a^2}, \beta = \sqrt{(\frac{\omega^2}{c_T})^2 - k_a^2}$

2. Calculate Wavenumber k_a from guided wave equations

$$\frac{\tan(\sqrt{\frac{\omega^2}{c_L^2}-k_a^2}d)}{\tan(\sqrt{\frac{\omega^2}{c_T^2}-k_a^2}d)} = -\frac{4\sqrt{(\frac{\omega^2}{c_T^2}-k_a^2)(\frac{\omega^2}{c_L^2}-k_a^2)k_a^2}}{(\frac{\omega^2}{c_L^2}-2k_a^2)^2}$$

Thickness of the medium

$$u_x(t) = [\alpha A\cos(\alpha x) - ik_a B\cos(\beta x)]\cdot V\cdot e^{i(\omega(t-t_T)+\varphi-k_a z)}$$

? (on k_a)

3. Calculate the phase Φ' and amplitude λ of the vibration wave at the crystal.

$$\lambda = \sqrt{[\alpha A p\cos(\alpha x)]^2 + [k_a B p\cos(\beta x)]^2}$$

$$\Phi' = -\omega t_T + \varphi - k_a z + \arctan(\frac{\alpha A\cos(\alpha x)}{k_a B\cos(\beta x)}),$$

Horizontal distance between transducer and RTC crystal

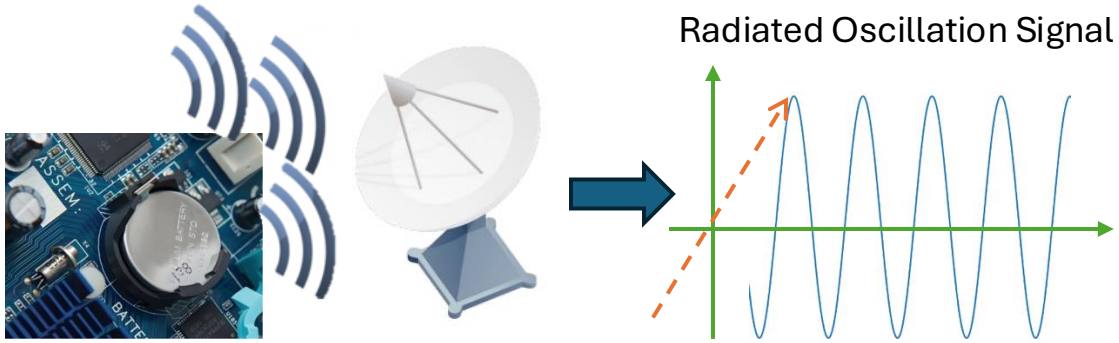
$$\xi = \mathrm{Re}\{u_x(t)\} = \lambda\sin(\omega t + \Phi)$$

Test & Collect: $\{\Phi', \varphi, \Delta\}$

Phase jitter variation after a single attack

Methodology

2&3. EMI Sync and Send The Attack Sequence

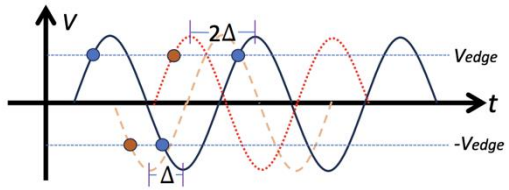


Set Φ',look up $\{\Phi', \varphi, \Delta\}$

Set up intended timing drift T

Calc: k bursts, dur. t_1, gap t_2; phase-triggered

Launch attack when phase φ detected

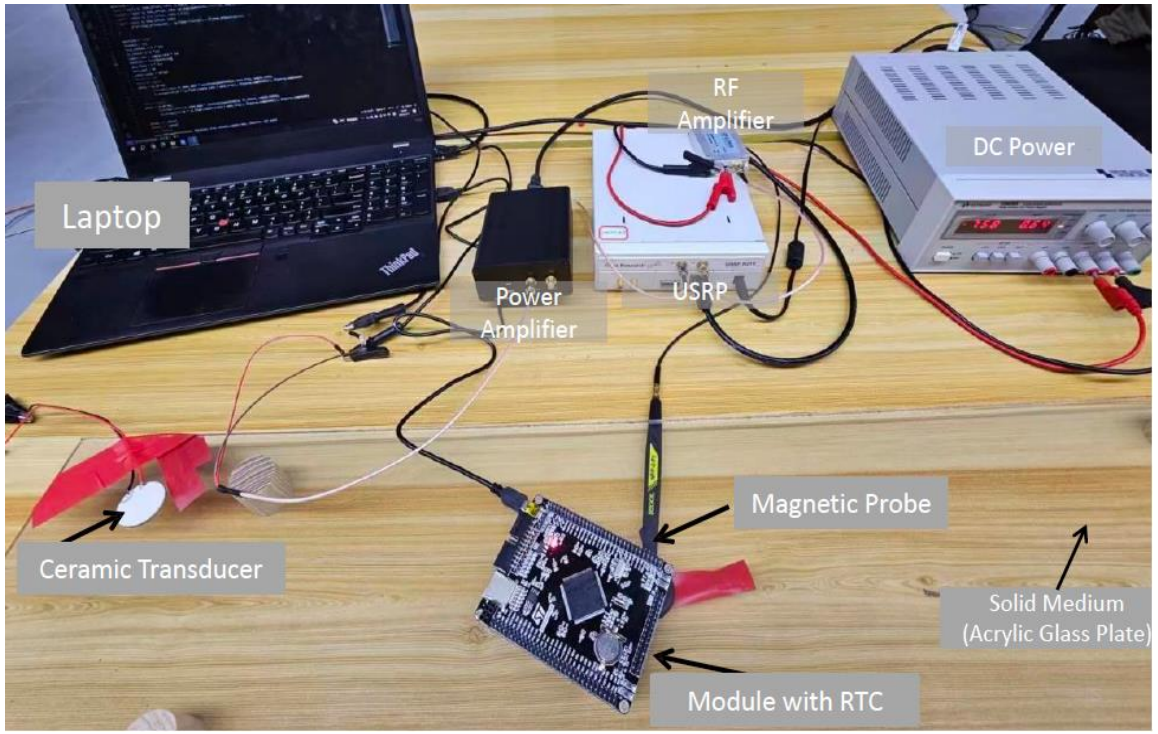


Filter+ Edge triggering

Introduce Phase Jitters -> Timing change

Experimental Evaluation

Physical Setup



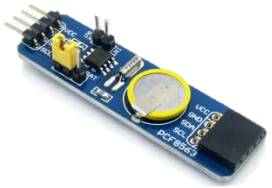
4 RTC modules+ 5 Dev boards + 2 Commercial devices

Tested Boards/Devices

RTC module


DS1302

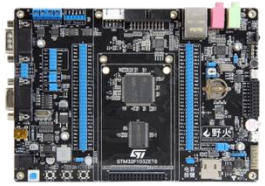

DS1307


PCF8563T


DS3231


F103ZET6


C6SLX16


F103ZGT6

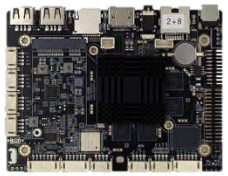
Dev board equipping RTC


KDB Intranet POS

HM-7132

Commercial devices


F407ZGT6


DC-A566

Overall Performance

Select different attack initial phases φ_2, to drift forward/backward for different amount of time

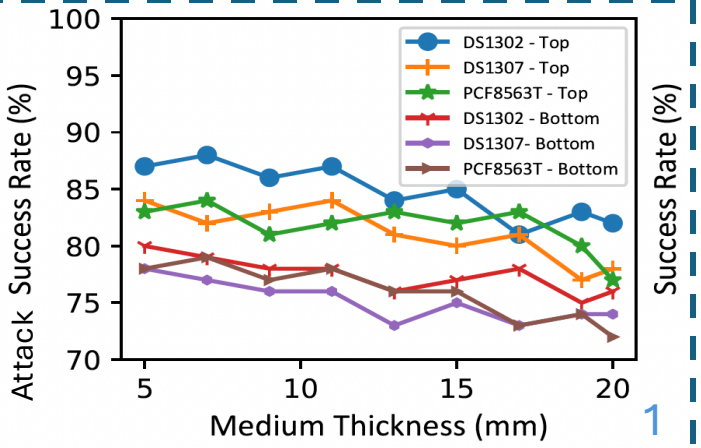
#	Module	Pw.↑	Pw.↓	↓5s	↓25s	↓5.5s	↓20.05s	↑25s	↑45s	↑20.5s	↑40.05s
1	DS1302	68.2V	75V	89%/ 2.519[1]	87%/ 2.519	—	—	88%/ 1.009	90%/ 1.979	—	—
2	DS1307	67.1V	76V	88%/ 2.515	90%/ 2.515	—	—	88%/ 1.005	85%/ 1.975	—	—
3	PCF8563T	66.9V	73V	89%/ 2.521	85%/ 2.521	—	—	91%/ 1.011	86%/ 1.981	—	—
4	DS3231	64.6V	75V	91%/ 2.527	89%/ 2.527	—	—	88%/ 1.017	87%/ 1.987	—	—
5	STM STM32-F103ZET6	71.8V	79V	**93%**/ 2.535	89%/ 2.535	87%/ 2.535	86%/ 2.535	87%/ 1.025	86%/ 1.995	85%/ 0.844	87%/ 1.922
6	Alientek XC6-C6SLX16	71.1V	95V	84%/ 2.518	85%/ 2.518	85%/ 2.518	86%/ 2.518	84%/ 2.79	85%/ 2.395	84%/ 0.827	82%/ 1.905
7	Alientek STM32-F103ZGT6	72.3V	94V	85%/ 2.519	**83%**/ 2.519	86%/ 2.519	84%/ 2.519	84%/ 2.791	84%/ 2.399	**81%**/ 0.828	**78%**/ 1.906
8	Alientek STM32-F407ZGT6	71.9V	86V	89%/ 2.536	88%/ 2.536	90%/ 2.536	85%/ 2.536	85%/ 2.809	87%/ 2.413	86%/ 0.845	81%/ 1.923
9	DINGCHANG DC-A566	73.2V	88V	89%/ 2.921	91%/ 2.921	**92%**/ 2.921	89%/ 2.921	**83%**/ 2.801	85%/ 2.396	89%/ 0.83	**90%**/ 1.908

* The initial phase of the excitation signal applied by attackers to the transducer, expressed in radian (rad); Pw.↑ and Pw.↓ refer to the minimum power transmitted to transducer, to cause the desired forward and backward timing drift, respectively.

TimeTravel executed the attack 100 times with different RTC modules/parameters, with a success rate of no less than 78%

Factors

1.Medium Thickness



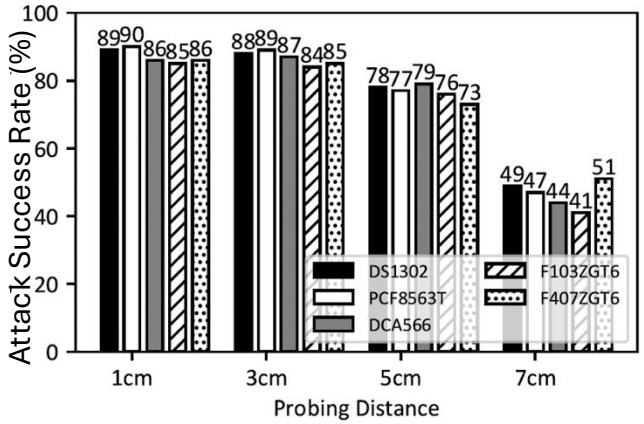
1

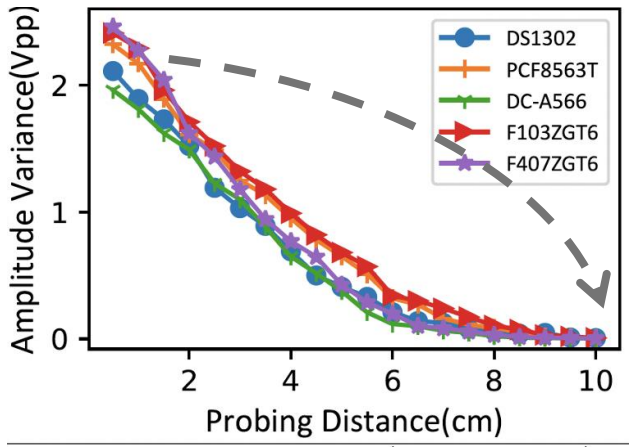
1. The thicker the solid medium, the more difficult the attack.

2. Attack success rate>70% when the probe is within 5 cm of the crystal.

3. Nearby obstacles have little impact on the attack success rate.

2.Magnetic Sensing Distance





2

3. Environment Configuration with Obstacles

Attack Success Rate (%)

Module	Setting 1	Setting 2	Baseline*
DS1302	89%	90%	89%
DS3231	85%	87%	86%
STM32F10-3ZGT6	82%	83%	83%
STM32F40-7ZGT6	87%	85%	87%

Setting 1

Setting 2

*Baseline: No obstacle

3

Please check the paper!

Factors

4. Impact of Medium Materials

Material	↓25s	Phase	↑45s	Phase
RTC Module: DS1302				
Acrylic Glass	75V	2.519	68.2V	1.979
Hard Rubber	86V	2.018	79.1V	1.471
Oak Wood	80V	1.972	75.3V	1.426
Quartz Glass	69V	2.299	66.1V	1.753
Development Board: XC6C6SLX16				
Acrylic Glass	95V	2.518	75.1V	2.395
Hard Rubber	104.2V	2.132	85V	1.613
Oak Wood	99V	2.213	81.6V	1.728
Quartz Glass	87.5V	2.302	71V	1.897
Development Board: STM32-F407ZGT6				
Acrylic Glass	86V	2.536	71.9V	2.413
Hard Rubber	94.9V	1.947	81.2V	1.563
Oak Wood	90V	2.119	77V	1.718
Quartz Glass	79.8V	2.387	68.5V	2.012

4

4. Hard rubber materials generally require more energy to successfully execute an attack.

5. Probing is generally effective within 5cm distance (>50% succ. Rate)

5.EM-Side Channel Quality

Probing Distance	Accuracy	Recall	F1 Score
Solid Material: Acrylic Glass			
1cm	99.43%	99.24%	99.33%
2cm	99.41%	99.22%	99.31%
3cm	99.38%	99.16%	99.27%
4cm	93.29%	91.48%	92.38%
5cm	82.43%	77.38%	79.83%
6cm	54.69%	50.25%	52.38%
7cm	38.74%	33.62%	36%
Solid Material: Polyethylene			
1cm	99.37%	99.26%	99.31%
2cm	99.31%	99.24%	99.27%
3cm	99.3%	99.21%	99.25%
4cm	92.76%	90.74%	91.74%
5cm	79.66%	72.8%	76.08%
6cm	49.97%	47.82%	48.87%
7cm	31.08%	26.65%	28.7%
Solid Material: Hard Rubber Plastic			
1cm	99.46%	99.4%	99.43%
2cm	99.41%	99.38%	99.39%
3cm	99.22%	98.92%	99.07%
4cm	93.02%	91.47%	92.24%
5cm	82.43%	80.06%	81.23%
6cm	56.12%	52.98%	54.5%
7cm	33.96%	29.93%	31.82%

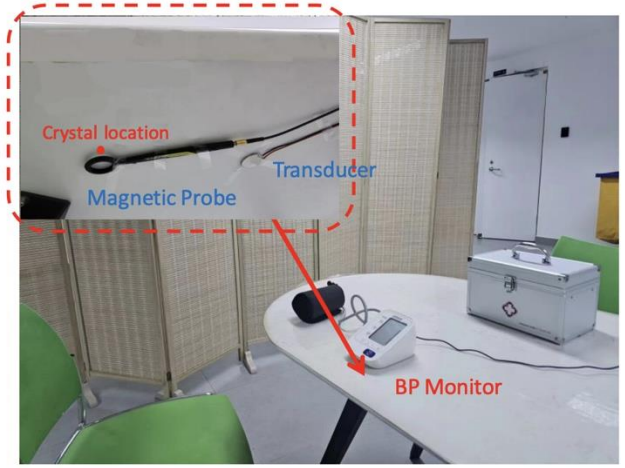
Layer	Operation	Kernel Size
1	Input	100000×1
2	Conv1D	16×64
3	MaxPool	4
4	Conv1D	8×128
5	MaxPool	4
6	Conv1D	8×256
7	MaxPool	4
8	Flatten	-
9	FC1	1024
10	Dropout	0.2
11	Output+Softmax	16*

Classify 6 BP Monitors via EM-side channel

5

Factors

4.Real-world Attack Example

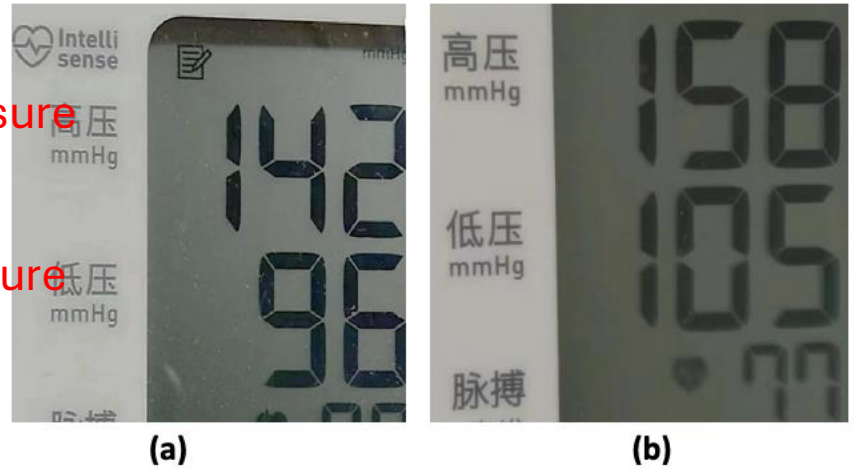


Normal Condition

BP Monitor Outputs Wrong Readings Under Different Attack Configurations

H Pressure

L Pressure



(a) (b)

(c) (d)

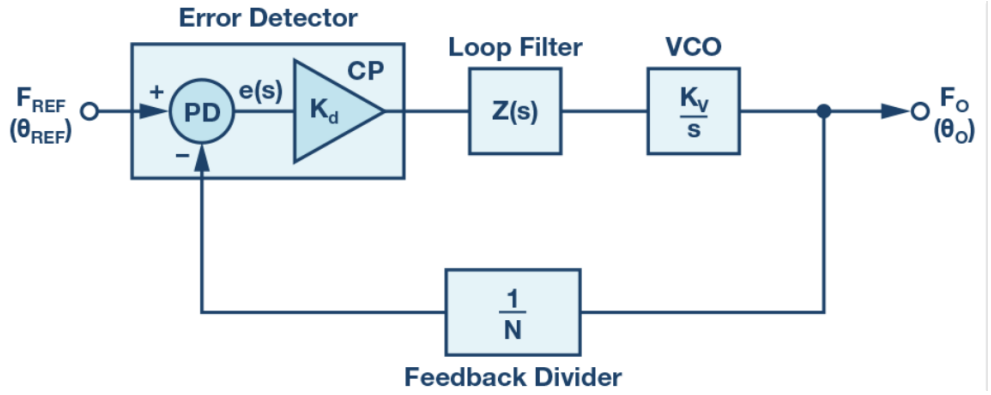
Under Attack

Countermeasures

- Replacing Oscillating Source.

$f = 32.768kHz$

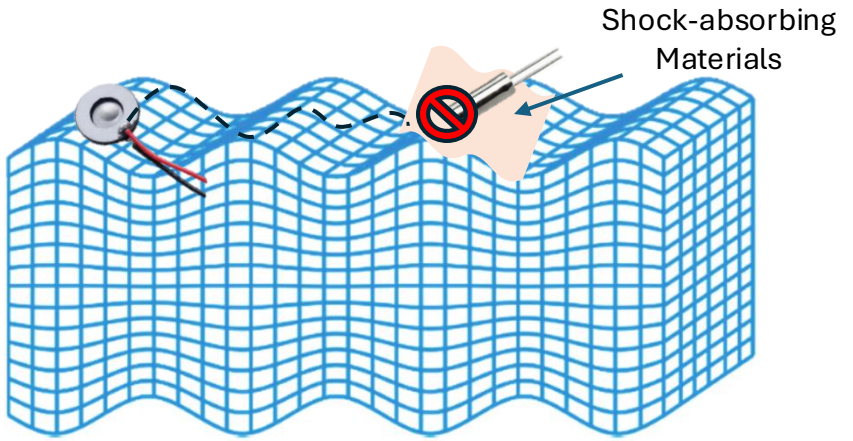
$f' = 25MHz$



PLL divider

- Applying Shock-absorbing Materials.

Suppress vibration energy transmission



Takeaways

- Using guided waves to stimulate crystal resonance can affect the RTC timing accuracy.
- By injecting signals with varying phases and amplitudes, the RTC timing speed can be manipulated.
- The tests on time drift granularity, medium thickness, obstacles, and signal detection range prove the effectiveness of TimeTravel.

Resource:
https://en.wikipedia.org/wiki/Real-time_clock
https://en.wikipedia.org/wiki/Crystal_oscillator

Thanks for listening!