
BURIED CAPACITIVE SENSORS FOR TAMPER PROTECTION

1. Relevant Devices

C8051F70x, C8051F71x, C8051F8xx, and C8051F99x.

2. Supporting Documentation

- AN367: Understanding Capacitive Sensing Signal to Noise Ratios and Setting Reliable Thresholds
- AN447: Printed Circuit Design Notes for Capacitive Sensing with the CS0 Module
- AN529: Capacitive Sensing Through Long Wires

3. Introduction

An individual's financial matters are increasingly electronic in nature and decreasingly interpersonal. As financial institutions replace human interaction with electronic interfaces such as ATMs, the need to make electronic circuits tamper-proof becomes critical. A typical numeric keypad for financial transactions may contain up to hundred or more tamper prevention and detection features. Tamper detection circuits raise alarms and disable functionality, while tamper prevention features are designed to prevent intrusions and breaches.

This application note addresses the elimination of copper pads on the accessible top surface of printed circuit boards (PCBs). Burying traces to internal layers of a PCB prohibits electrical contacts from snooping on copper elements within the PC board.

4. Applications

A typical button plunger application is depicted in Figure 1. Figure 1's top drawing is a side view of a single electrical switch. The plunger is either conductive or has a conductive material on the surface that interacts with two copper elements on the PCB. Figure 1's bottom drawing is a top view of the round plunger hovering over two semicircle copper pads. The copper pads are monitored by an MCU that identifies when the circuit is completed.

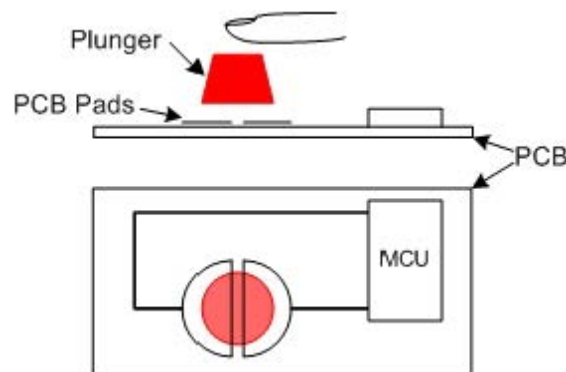


Figure 1. Conductive Plunger Switch

There is typically a gasket dome over the top of the plunger that contains the key label and provides some protection from the elements. If one were to attempt to snoop this system, it would not be all that difficult to attach conductive wires to the two semi-circle pads to monitor when they are shorted. Detecting that pads have shorted can enable someone to capture a sequence of keys signifying personal data such as a bank account PIN.

One solution to this problem is to bury the copper semi-circle pads and their connections within the inner layers of the printed circuit material. This disables the ability to solder wires directly to the conductive surface of the printed circuit. This scenario assumes that the MCU is mounted on the backside of the PCB and inaccessible. Figure 2 depicts this configuration. Note that no conductive layers should appear in the PCB between the semi-circle elements and the MCU.

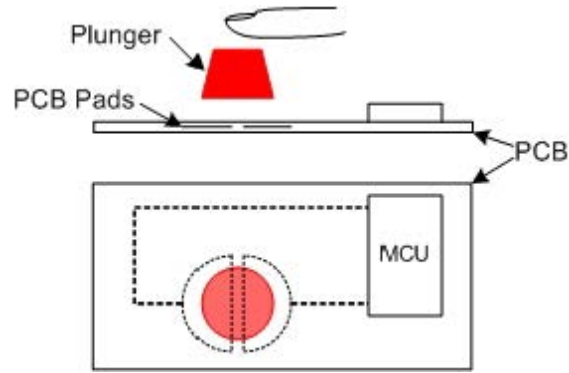


Figure 2. Conductive Plunger Switch

While this approach eliminates the soldered form of snooping, it also eliminates the direct conductive contact of the plunger to the semi-circles, which prevents the key press from being detected. One method of sensing a key press in a system with buried semi-circle sensors is to measure the change in capacitance as the plunger approaches. The magnitude of this capacitive change is a function of how deeply the traces are buried, the traces' size, the material dielectrics, and the plunger's size and conductivity. This change, which can be relatively slight, requires the high level of sensitivity achieved with the capacitance-to-digital converter (CDC) in Silicon Labs' MCU families. The suggested implementation is to connect one of the semi-circles to ground and to measure the capacitance of the two plate + dielectric system.

Considerable material disclosed in this article is the subject of patents applied for. Consult appropriate party for details.

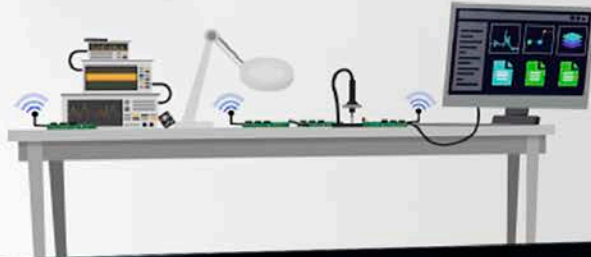
DOCUMENT CHANGE LIST

Revision 0.1 to Revision 0.2

- Removed “QuickSense”

Silicon Labs

Simplicity Studio™4



Simplicity Studio

One-click access to MCU and wireless tools, documentation, software, source code libraries & more. Available for Windows, Mac and Linux!



IoT Portfolio
www.silabs.com/IoT



SW/HW
www.silabs.com/simplicity



Quality
www.silabs.com/quality



Support and Community
community.silabs.com

Disclaimer

Silicon Labs intends to provide customers with the latest, accurate, and in-depth documentation of all peripherals and modules available for system and software implementers using or intending to use the Silicon Labs products. Characterization data, available modules and peripherals, memory sizes and memory addresses refer to each specific device, and "Typical" parameters provided can and do vary in different applications. Application examples described herein are for illustrative purposes only. Silicon Labs reserves the right to make changes without further notice and limitation to product information, specifications, and descriptions herein, and does not give warranties as to the accuracy or completeness of the included information. Silicon Labs shall have no liability for the consequences of use of the information supplied herein. This document does not imply or express copyright licenses granted hereunder to design or fabricate any integrated circuits. The products are not designed or authorized to be used within any Life Support System without the specific written consent of Silicon Labs. A "Life Support System" is any product or system intended to support or sustain life and/or health, which, if it fails, can be reasonably expected to result in significant personal injury or death. Silicon Labs products are not designed or authorized for military applications. Silicon Labs products shall under no circumstances be used in weapons of mass destruction including (but not limited to) nuclear, biological or chemical weapons, or missiles capable of delivering such weapons.

Trademark Information

Silicon Laboratories Inc.®, Silicon Laboratories®, Silicon Labs®, SiLabs® and the Silicon Labs logo®, Bluegiga®, Bluegiga Logo®, Clockbuilder®, CMEMS®, DSPLL®, EFM®, EFM32®, EFR®, Ember®, Energy Micro, Energy Micro logo and combinations thereof, "the world's most energy friendly microcontrollers", Ember®, EZLink®, EZRadio®, EZRadioPRO®, Gecko®, ISOModem®, Precision32®, ProSLIC®, Simplicity Studio®, SiPHY®, Telegesis, the Telegesis Logo®, USBXpress® and others are trademarks or registered trademarks of Silicon Labs. ARM, CORTEX, Cortex-M3 and THUMB are trademarks or registered trademarks of ARM Holdings. Keil is a registered trademark of ARM Limited. All other products or brand names mentioned herein are trademarks of their respective holders.



SILICON LABS

Silicon Laboratories Inc.
400 West Cesar Chavez
Austin, TX 78701
USA

<http://www.silabs.com>