

Hi Marc,

Apologies for the delay. I've assumed your interest is both in the product and the technical details and that you would probably want to pull it apart, so have included a few bits and information to save you some trouble. Also a rather out of date video introducing some prototype product and demonstrating manual authorizations which is the easiest way to learn how to use.

#### What's in the pack

1. 2 x Gen1.5 keys.
2. 1 x cam lock, virgin; meaning one must acquire master key to open. See "quick-start" below.
3. 1 x functional plug, virgin. Easy demonstration of freely rotating tailpiece unless clutch is engaged by an authorized key.
4. 1 x "classic" Gen1 actuator illustrating function, non-production materials but easy to see and re-assemble – just pop the tailpiece off the back. Note if re-inserting the PCB the small arrow should line up with the mark on the plastic housing. Also the bobbin legs must line up with holes in the clutch mechanism.
5. 1 x Gen1.5 actuator slid into a blank housing, less easy to assemble as each clutch leg is separate – die-cast for extra strength. Use housing as an assembly jig. To remove actuator from housing just slip a knife blade between the black plastic and metal about ¼-way from back of plug to pry it out the back.

#### Quick-start (See also video)

1. Insert key #1 into virgin cam lock, all 3 LEDs flash red twice indicating it is virgin. Turn key and cam tailpiece won't rotate.
2. Hold a key blade facing away with decal side up, touch wedge-shaped pads left, right, left, right about 0.5 second spacing. Key beeps and left "ISSUE" green LED starts flashing.
3. Place thumb over pads and hold to "lock" ISSUE function, LED starts flashing red.
4. Still holding, insert key into virgin lock. Key beeps twice and green LED flashes twice.
5. Remove key, release thumb, key stops flashing. This is now the lock's "master key".
6. Re-insert key, first and third LED flash very briefly with beep. Turn key and cam rotates.
7. Insert key #2 into cam, all 3 LEDs flash once indicating key is not authorized and lock is no longer virgin.
8. To authorize 2<sup>nd</sup> key, repeat steps 2-5. Then insert key #2. All 3 LEDs flash green. Re-insert key 2 and cam will turn.
9. To return lock to virgin state, repeat steps 2-3. Then touch right pad to light up 3<sup>rd</sup> "WIPE" LED before placing thumb over pads. Hold down thumb to lock function and insert. Lock is returned to virgin state and neither key can open.

#### User documentation (Product folder)

Something a little more comprehensive on the key function and the full product suite:

- Gen1.5 key quick-start, some explanation of what the various key functions are.
- Understanding the blinking lights and beeping sounds on the Yebo Gen1.5 key.
- System capabilities, an overview of the entire system.

#### Technical Documentation (Technical folder)

Since your main field of expertise is security I've included a few extracts from technical documentation you may find interesting. The full scope is vast but if there's anything of particular interest let me know.

1. YT-YLP\_SG0-IDD-1.5 - Yebo Tech Cryptographic Protocol SG0 Specification - extract: a brief description of the CHAP protocol used to authenticate operations.
2. YT-YLP-IDD-1.8 - Yebo Lock Protocol Interface Definition - operations: a protocol view of the kinds of operations that can be performed on devices (both locks and keys). An "authorization" is required to perform one or more operations.
3. YT-YLP-IDD-1.8 - Yebo Lock Protocol Interface Definition - proxies. The trick we use to stamp out new unique authorizations for every key on e.g. a central management system.
4. Plug Gen1.5 electronics schematic rev 1.1: The electronics schematic for the plug, ultimately to control the "actuator" coil inside the plug's clutch mechanism.
5. YT-PLUG1.5-MDDD-1.0 - Yebo Plug Gen1.5 Mechanical Detailed Design - extract. A description of the original Gen1 plug clutch mechanism. Rather dated and a few details have been revised but still the best description available.
6. YT-PLUG\_SHOCK-QTR-1.0 - Yebo Plug - Shock and vibration response - extract. The most obvious method of attacking a delicate mechanism is to shake it a lot, this is an extract from shock and vibration tests and analysis.
7. YT-PLUG\_ATTACK-QTR-1.2 - Yebo Plug - Attacks resistances - extract. Table of contents of the current master attack document listing all the various methods we've tried to subvert the clutch mechanism. One or two resulted in changes to manufacturing processes. Perhaps you can think of a few more.

Generally companies like to hold such information close to the chest but you can't fix a vulnerability you don't know anything about, so I would greatly appreciate any observations you might make.

#### Other stuff

1. There is a management system at [secure.yebotech.com](https://secure.yebotech.com). You need a Yebo sync station or alternatively an Android NFC-enabled cell phone which is able to talk to a key using YeboSync app. Let me know if you wish to try this.

Something worth noting: the product was originally designed to be cheap for access control application in e.g. store cabinets, and we have no pretence that it is super high security or very good quality: store assistants don't care and nobody mounts a sophisticated attack on a cabinet door they can just kick in. But increasingly we're getting demand to guard homes and businesses and facilities which significantly raises the burden of responsibility. And currently things are evolving swiftly: just this month 3 new locksets are entering tooling and these samples are already dated compared to what's coming off the line now. So if we've overlooked anything important now is the time to find out, which really makes this delay doubly unfortunate.

Best regards,  
David Harley.