



**ARC FORENSICS** INC.  
"CERTIFIED"  
FORENSIC LOCKSMITHS ~ PHOTOGRAPHERS  
VEHICLE THEFT & FIRE ~ TRANSPONDER DIAGNOSTICS  
Honesty ~ Professionalism ~ Integrity  
P.O. BOX 239 WESTFIELD, IN 46074-0239  
Phone (317) 669-7581 ~ Fax (317) 669-7582 ~ Cell (317) 710-7971 ~ mail@ARCForensics.com



## Ford Busted! Or, Not?

By Herbert T. Miller Sr., CFL

***With the Ford Encrypted Transponder Key Technology Broken by John Hopkins Research, Is Theft An Easier Option?, we think not.***

### Introduction

Broadcasting the potential theft of millions of Ford vehicles; this weekend's media reporting of recent transponder research at John Hopkins is **creating unwarranted concerns of uncontrolled theft and fraud.**

At the heart of the issue is the recent cracking by the researchers of the algorithm used in the encryption protection of the Texas Instrument **chip used in a single type of Ford key.**

In typical media fashion, however, the degree of theft risk this "breakthrough research" presents is **exaggerated and overstated.**

Here are some facts:

1. Currently, based on the information provided by the media, relative to automotive applications, the "crack" affected a single chip currently used only on the **Ford Focus** and **Escape**, and the Ford produced **Mazda Tribute.**
2. This breakthrough simply means that keys that could not previously be cloned are **now cloneable**; but **only under laboratory conditions.**
3. This breakthrough **affects the key only**, and **does not affect** the ability to bypass or defeat **the immobilizer system installed in the vehicle** when a working and programmed key is not present or available.
4. The research was performed by researchers whose leader is heavily involved and knowledgeable of encryption technology. Despite their credentials, it still took this group and a handful of computers three months of full-time work to crack the chip; the research was also heavily financed.

## Discussion

The recent code breaking of the Texas Instrument based Ford transponder key is neither new nor unexpected. Private companies with interests in the production and duplication of the transponder based keys and cloning equipment have always recognized that the protection schemes of encrypted transponder keys are breakable. In fact, probably due more to international restrictions regarding encrypted data than by technical limitations, the chip(s) used in these transponder keys use 40-bit instead of the more robust 128-bit encryption. As the “breaking” process is nothing more than a trial run of every single possible code, the 40-bit encryption scheme is obviously less secure.

From a commercial standpoint, the sole reason for not pursuing this technology is simple economics – the time, legal hurdles and resources required to break the codes of the various transponder keys is not only costly, but subject to copyright, patent and other protections. As such, the investment needed to create commercially available products cannot be justified.

So, what does this **supposed breakthrough mean** to the face of auto security?, **not much if anything at all** in the opinion of this expert. Simply put, once all the hype is boiled out of this issue, it means that the keys using this particular Texas Instrument chip can be cloned. That’s it.

And as a **cloneable key**, using this technology **to steal a car still requires access to cloning equipment and keys capable of working with the encrypted chip, plus an already programmed and working key**. In typical media fashion, however, the **ability to use this technology for theft is overstated**.

In reviewing the information on this breakthrough it should be remembered that the John Hopkins research performed the break and cloning under **ideal conditions**. The subject chips or keys were exposed and stable, **not the conditions of an actual attempted theft**.

In reality, the limitations of cloning severely limit its effectiveness as a method of theft:

1. The extremely **short transmission range of the chip** (4 to 20 mm) **makes “code grabbing” extremely difficult** without having **the key in hand**. Coming into close enough proximity of a transponder chip for the time needed to grab the code is highly unlikely. Plus, **barriers** such as the material of a pocket or a purse, other metallic objects like keys, and even one’s hand **can limit the ability to grab a code**.
2. Compounding the difficulty is the fact that in many chips, **direction** also **affects the ability to properly grab or steal a transponder code**. When a standard GM PK3 transponder key (a cloneable key) is placed into a common and well known transponder reader, the unit correctly detects a Megamos chip. Inserted upside down, however, it detects a Phillips brand chip.

When an otherwise uncloneable encrypted Cadillac Catera key is placed upside down in a commercial cloning device, the key can be read, copied and a cloned key created. Ford's **newest key**, using the Texas Instrument Encrypted "Wedge" chip, **only operates when properly positioned in the ignition lock's keyway.**

3. As more than 70 percent of today's vehicles come equipped with transponder based immobilizers, the likelihood of an individual having more than one transponder key on his/her person is extremely high. If more than one transponder is on the key chain or within close proximity to one another, grabbing or stealing causes both keys to simultaneously transmit their code, disrupting or corrupting the code received by a code grabbing device.
4. Once a key is cloned, the vehicle must be located. This can only occur in targeted thefts; which involve not only access to a working programmed key, but also enough surveillance to determine the vehicle owner's address or location of the vehicle.
5. Finally, from a commercial perspective, due to the legal and economic barriers mentioned earlier, the production of and **accessibility to commercially available equipment and keys capable of working with the encrypted chips is not likely to occur anytime soon**; severely limiting the potential for using this technology for theft.

### **Conclusion:**

It seems the media has struck the chord of the alarmist public. The research considered a breakthrough is simply a working demonstration on the limits of some levels of encryption technology. But, the technology used to break the encryption on the Ford key is not new and not, generally speaking, complicated. However, it does demand time and money.

While 128-bit is preferred, the global market under which this technology is used imposes legal limits that restrict manufacturers to the less secure but still extremely effective 40-bit encryption.

Aside from the time and development costs, using this technology to actually steal a vehicle requires the time and expense involved in targeting and surveillance. In fact, the only credible scenario for a theft of this type involves car owners having their key cloned at a car dealership, hardware store, and/or locksmith; where both a working key and vehicle location or owner address are surrendered. Still, as stated earlier, the necessary equipment is not currently commercially available, and probably won't be for some time.

For a car thief to use cloning as the method of theft, it is necessary to have direct access to a working and programmed key, the technology and tools to clone the key, time to clone the key, and foreknowledge of the vehicle's location. In all likelihood, these opportunities may only present themselves through direct contact with the vehicle owner.

Needless to say, considering the personal exposure and the degree of planning required for this theft technique, the cloning “breakthrough” of the John Hopkins research team really isn’t the crime industry’s auto-theft method of choice.

As it regards to fraud, insurance companies are bound to see a surge in stolen vehicle claims that involve the use of a cloned key. Remember that, as presented by the media, the automotive transponder chip in question affected the Ford Focus and Escape, and the Ford produced Mazda Tribute only. And, while the same code breaking process can be applied to most all other auto manufacturer’s keys that employ the challenge-response encrypted technologies, it still involves an investment in time and money.

Finally, we need to ask, Does the John Hopkins demonstration reduce the security of the Ford (or any) encrypted transponder technology and increase the likelihood of theft? That depends on perspective. Relative to “security by obscurity,” the research has now made public what has been known privately for years. In this vein, **security of these transponder systems has not been reduced.**

Relative to an increase in actual and legitimate theft? Not likely, this method requires targeting and surveillance to be affective, and there are too many cost and time effective alternatives to this method. Still, time will tell.

Relative to detecting give-ups? Highly unlikely, the **equipment to clone encrypted keys is not commercially available** and development is beyond the means of most individuals, small gangs, and small companies. All in all, the media hype behind the research is intriguing, but void of real world application.

*Author Herb Miller is a Certified Forensic Locksmith with an extensive background in vehicle key and lock systems, immobilizer technology and aftermarket alarm technology.*