Introducing

KeyQLIQ

A unique, proprietary solution

For protecting your car and home

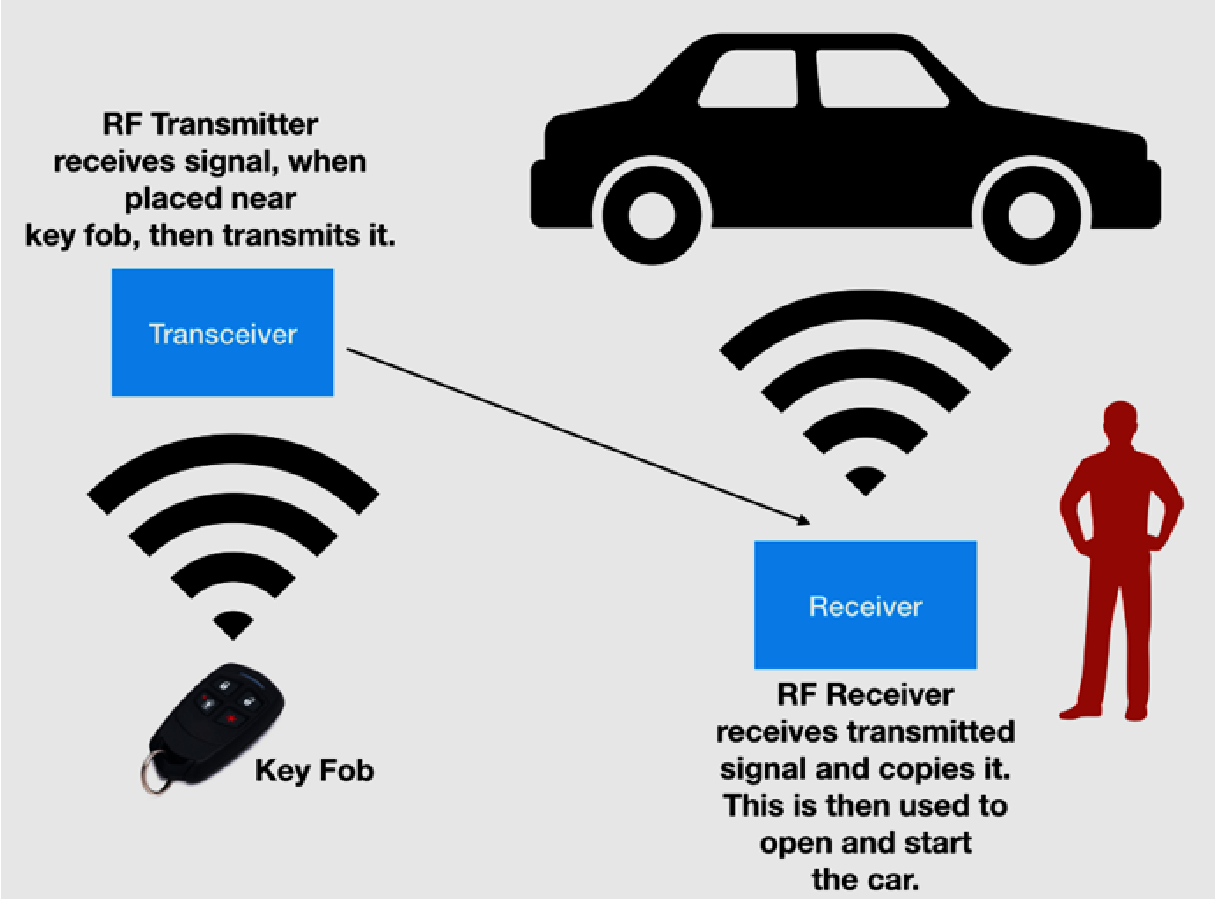
By intercepting the key signal…

Car thieves now intercepting key fob signals for remote-control heists

…a thief can unlock or enter without any alarms going off.

KeyQLIQ can stop their access…

Keyless entry systems use a “handshake” signal that sends a signal from the key fob to the car’s lock control unit ….



RF Transmitter receives signal, when placed near key fob, then transmits it.

RF Receiver receives transmitted signal and copies it. This is then used to open and start the car.

The encryption is usually programmed by the manufacturer

KeyQLIQ SECURITY SYSTEMS, pronounced (Key-Click), utilizes our advanced State of the Art Encryption technology

- Encryption is the process of protecting personal information in such a way that will only allow an authorized party to access and receive transmission codes
- Car key fobs, garage door openers, etc. are "encrypted" and designed to be specific to the car or door.
- KeyQLIQ enhances the process of encryption by producing a higher level of security

It's all about the math!

Our "EA" Encryption Algorithm

- At KEYQLIQ, our solution has a built-in an "advanced" encryption technology to safeguard critical assets.
- Encryption Algorithms exist in several forms but the two used the most for mobile devices are Symmetric and Asymmetric.
- From the beginning, in 2000, the Software was developed on *Sun Solaris* servers using a *Linux OS* and written in Java applets to facilitate growth, not limit it.
- Our apps have been scaled from Day One to keep up with evolving technology
- We use **State of the Art** Algorithms, 2048-bit SSL Certificates, that will stay ahead of the *Game* for the foreseeable future (e.g., IOS 12 currently uses 286 AES; Android uses Enterprise Features)
- Symmetric algorithms used for encryption are still thought to be safe (with sufficient key length – e.g. AES-256 or larger); however, current asymmetric algorithms will be rendered.

Check Out the Numbers …
The Math Behind Estimations to Break a 2048-bit Certificate

- In order to "break" an RSA key-based certificate, one must factor very large numbers that make up the RSA modulus.

- A certificate is considered "cracked" when the computer utilized reaches the average probability of time to factor the RSA modulus (*absolute value*) associated with the key in the

- In December 2009, Lenstra et al announced the factorization of a 768-bit RSA modulus. This is a 232-digit number, and was at the time (and potentially still is) the record for factoring the largest general integer.

- The most efficient method known to factor large integers, and the method used in the factorization record listed above, is via the *number field sieve (NFS)*

- It is estimated that factoring a 1024-bit RSA modulus would be about 1,000 times harder than their record effort with the 768-bit modulus, or in other words, on the same hardware, with the same conditions, it would take about 1,000 times as long.

- Our base standard is to use 2048-bit keys in secure SSL certificates - it would require factoring a 617-digit number.

- RSA Labs claim that 2048-bit keys are 2^32 (2 to the power of 32) times harder to break using NFS, than 1024-bit keys. 2^32 = 4,294,967,296 or almost 4.3 billion,

- Therefore, **breaking a 2048-bit SSL certificate** would take about 4.3 billion times longer (using the same standard desktop processing) than doing it for a 1024-bit key

What about NOW…

ENTER …. Quantum Computing

Circa 2019… To summarize, Quantum Computers exist, and access to them via the cloud is affordable. University and industry-developed education is increasing, and government funding (1) was approved to further research and focus on needed workforce development.

(2) If usable quantum computing were accessible, the field of cryptography would dramatically change, encryption codes **could be broken quickly** and perhaps crushing Blockchain technology and other similar technologies (3).

References:

(1) **Congress New Bill** (2) **The quantum computing tipping point is now**

(3) **The Future is Now**

IBM says move your Data now

In order that the system works, the KeyQLIQ algorithm must be installed both on the onboard computer in the car and on the key fob. On a new car the algorithm will be installed by the manufacturer.

On an aftermarket car the dealer will access the data port on the onboard computer under the dashboard of the car and install the onboard computer software. Once the algorithm is installed on the onboard computer you can reprogram the key fob by inserting it in the ignition switch and following the instructions below for your model of car. After Market is defined as the market for replacement parts, accessories, and equipment for the care or enhancement of the original product, especially an automobile, after the sale to the consumer.

The cost to get a car key programmed

The cost to get your car programmed

How it Works: The Computer Inside Your Car

Links to How to Reprogram Key Fob

Toyota

Porsche

Nissan

Ford

GM

Mercedes

Hyundai

KIA

Preserving the Safety, Efficacy and Legacy of Our Apps...

…This IS our number one Priority

Contact

Stephen R. Winters, Managing Director

404 – 276 – 1700

Eric L. Ruud, SVP of Business Development

678 – 462 – 1777