The Model 686 AWGs for QKD and Quantum Applications

APPLICATION NOTE

Introduction

In our digital age, sensitive information, from financial transactions to classified government data, flows through networks at an unprecedented rate. However, conventional encryption methods, relying on mathematical algorithms, face an existential threat from quantum computers.
Quantum computers, when they become powerful enough, could easily crack these encryption codes. Hence, the urgency to develop quantum-resistant encryption methods, and QKD stands at the forefront of this endeavor.

The laws of quantum mechanincs not only are used to protect our communications and data, but also to understand the world around us at an unprecedented level of detail. Light, temperature, pressure, heat, but also things that are imperceptible to more traditional sensors can be measured by
quantum sensors.
The quantum sensors depend on constants of nature, their reliability never degrades, so they are self-calibrating, and their measurements don't drift off over time like traditional sensors do.

High performance AWGs like the model 686 Arbitrary Waveform Generators are becoming extremely popular in designing and developing these emerging breakthrough technologies.

Key Issues:
• Generate pulses for Quantum Sensors and QKD applications.

Solutions:
• Model 686 Arbitrary Waveform Generator.

Results:
• Accelerate testing, reliability, characterization of quantum sensors, optics & photonics systems.

• Reduce the time to generate pulses and control signals for electro-optic modulators and quantum systems.

QKD: Quantum Key Distribution

Quantum key distribution (QKD) is a secure communication method for exchanging encryption keys only known between shared parties.
It uses properties found in quantum physics to exchange cryptographic keys in such a way that is provable and guarantees security. QKD enables two parties to produce and share a key that is used to encrypt and decrypt messages. Specifically, QKD is the method of **distributing** the key between parties.

Key distribution on a conventional scale relies on public key cyphers that use complicated mathematical calculations requiring a prohibitive amount of processing power to break. The viability of public key ciphers, however, faces several issues, such as the constant implementation of new strategies used to attack these systems, weak random number generators and general advances in computing power. In addition, quantum computing will render most of today's public key encryption strategies **unsafe**.

QKD is different from conventional key distribution because it uses a quantum system that relies on basic and fundamental laws of nature to protect the data, rather than relying on mathematics.

QKD works by transmitting many light particles, or photons, over fiber optic cables between parties. Each photon has a random quantum state, and collectively, the photons sent make up a stream of ones and zeros. This stream of ones and zeros are called qubits and they are the equivalent of bits in a binary system. When a photon reaches its receiving end, it travels through a beam splitter, which forces the photon to randomly take one path or another into a photon collector.

The receiver then responds to the original sender with data regarding the sequence of the photons sent and the sender then compares that with the emitter, which would have sent each photon.

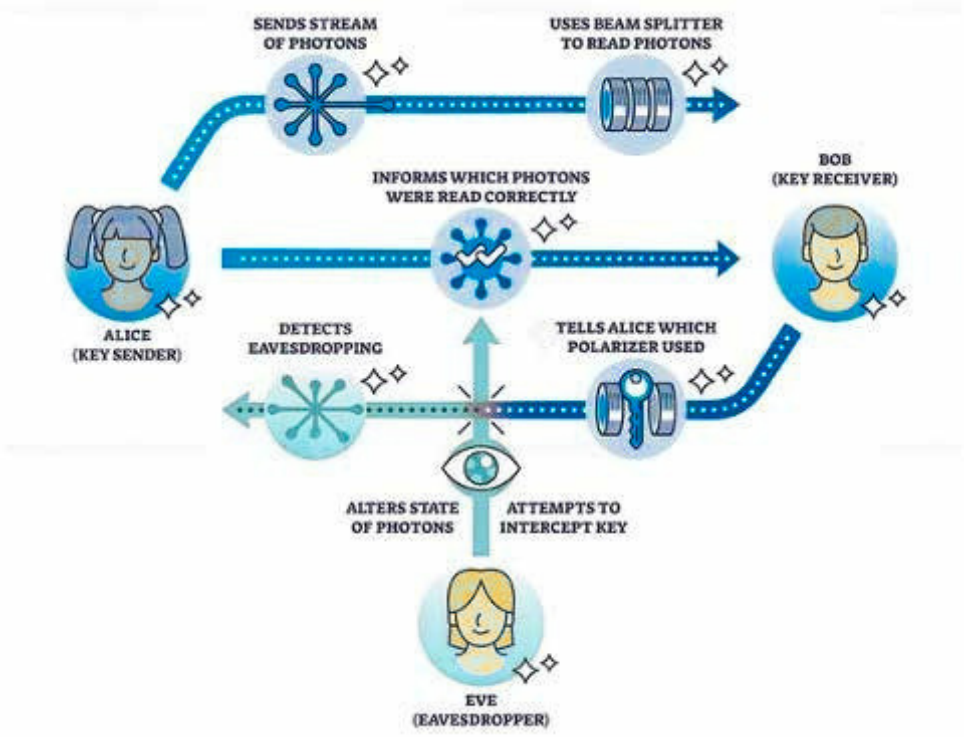

Figure 1: Alice, Bob and Eve

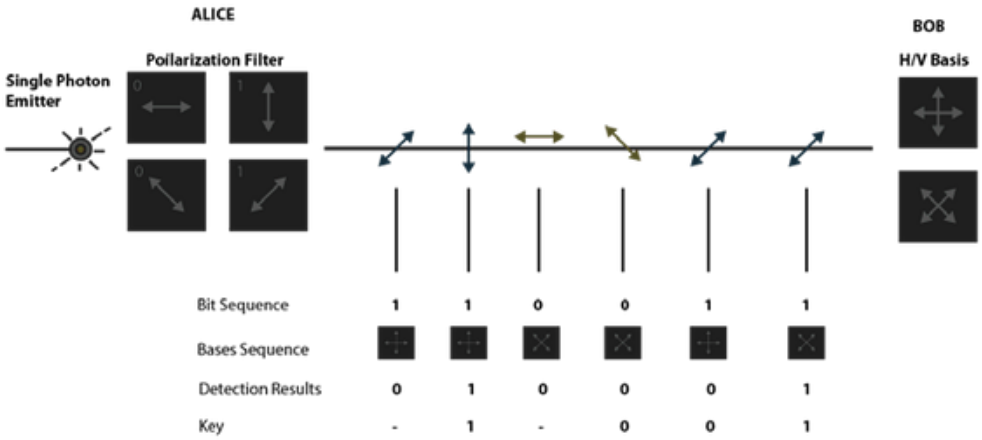

Figure 2: Alice and Bob transmitting photons

Photons in the wrong beam collector are discarded; what's left is a specific sequence of bits. This bit sequence can then be used as a key to encrypt data; any errors and data leakage are removed during a phase of error correction and other post-processing steps.

To do this, Alice sends photons, the smallest part of light, to Bob. Since photons are not only particles but also waves, they oscillate. They can oscillate in different directions; when they oscillate in only one direction, they are called polarized.
With polarizing filters, we can filter photons, then, for example, only the photons that oscillate up and down can pass through; these are then called vertically polarized. With the help of quantum mechanics it is possible to send single photons: Alice sends polarized photons to Bob and if Bob holds his filter the same way as the photons polarized by Alice, the light passes through.
If, on the other hand, he holds his filter crosswise to the direction of polarization, no photon passes through and each photon can be measured only once. What does it happen if Bob turns his filter just a little bit to Alice's polarization direction, diagonally? Sometimes a photon can pass through the filter and sometimes not; if both polarize diagonally in the same direction, the photons all pass through again. If, on the other hand, they polarize in different diagonal directions, the photons no longer pass through Bob's filter.

Quantum key exchange (QKD)

Alice makes notes of the polarization with which she sent the photons off and Bob makes a note of how he held his filter and whether light was received or not. Now the two can talk publicly about how Alice polarized her photons and how Bob held his filter. Everyone can hear this. Whenever one person used the filter diagonally and the other vertically or transversely, that part gets deleted; from the remaining ones they build their key.

If an attacker (man-in-the-middle) called Eve tries to read along a photon with a polarization filter, she has to send a new photon to Bob afterwards. Eve does not know if she has held the filter correctly: if she doesn't see any light, she could have held her filter crosswise to Alice's filter or just slightly differently, but the photon didn't get through. If she does see light, it could still be because the photon came through with the filter slightly rotated, so she may still have held the filter incorrectly.
Eve doesn't know if holding the filter diagonally was correct or not.

Photons cannot be copied and only be measured once, so Eve has to guess quite oftenwhat she sends on to Bob.

Alice and Bob only talk later about how they used their filtersand which parts they can use for their key.

Eve, however, has to decide beforehand whether she was correct with diagonal or non-diagonal, but without the public conversation, she has to guess how to proceed, and thus often makes mistakes. Bob makes as many mistakes as Eve, but his are simply deleted, before Alice and Bob build their key, they compare individual digits.

They don't use them for the key afterwards, but if they don't match they know that someone has been listening, so the quantum encryption is used to agree on a key. Since the method is based on the randomness of quantum mechanics, whether photons can pass through slightly twisted filters or not, it is considered unbreakable.

Figure 3: Quantum encryption

Types of QKD

There are many different types of QKD, but two main categories are prepare-and-measure protocols and entanglement-based protocols.

Prepare-and-measure protocols focus on measuring unknown quantum states. They can be used to detect eavesdropping, as well as how much data was potentially intercepted.

Entanglement-based protocols focus on quantum states in which two objects are linked together, forming a combined quantum state. The concept of entanglement means that measurement of one object thereby affects the other. If an eavesdropper accesses a previously trusted node and changes something, the other involved parties will know.

By implementing quantum entanglement or quantum superpositions, just the process of trying to observe the photons changes the system, making an intrusion detectable.

It is difficult to implement an ideal infrastructure for QKD. It is perfectly secure in theory, but in practice, imperfections in tools such as single photon detectors create security vulnerabilities. It is important to keep security analysis in mind.

Modern fiber optic cables are typically limited in how far they can carry a photon. The range is often upward of 100 km. Some groups and organizations have managed to increase this range for the implementation of QKD. The University of Geneva and Corning Inc. worked together, for example, to construct a system capable of carrying a photon 307 km under ideal conditions.

Another challenge of QKD is it relies on having a classically authenticated channel of communications established. This means that one of the participating users already exchanged a symmetric key in the first place, creating a sufficient level of security. A system can already be made sufficiently secure without QKD through using another advanced encryption standard. As the use of quantum computers becomes more frequent, however, the possibility that an attacker could use quantum computing to crack into current encryption methods rises, making QKD more relevant.

QKD attack methods

Eventhough QKD is secure in theory, imperfect implementations of QKD have the potential to compromise security. Techniques for breaching QKD systems have been discovered in real-life applications. For example, even though the BB84 protocol should be secure, there is currently no way to perfectly implement it.

The phase remapping attack was devised to create a backdoor for eavesdroppers. The attack takes advantage of the fact that one party member must allow signals to enter and exit their device. This process takes advantage of methods used widely in many commercial QKD systems.

Another attack method is the photon number splitting attack. In an ideal setting, one user should be able to send one photon at a time to the other user. However, most of the time, additional similar photons are sent. These photons could be intercepted without either party knowing. To combat this type of attack, an improvement to the BB84 protocol was implemented, called decoy state QKD, which uses a set of decoy signals mixed in with the intended BB84 signal while enabling both parties to detect if an eavesdropper is listening.

QKD implementation methods

There are two different approaches to implement QKD: one focuses on discrete variable (DV-QKD) and relies on single photons with encoded random data. The other one plays on the wave nature of light with information encoded in the quadrature of its electromagnetic fields, it is continuous variable (CV-QKD). Coherent homodyne or heterodyne detection is used to continuously retrieve the quadrature value of the signal to read the key into it.

In the market there are different modulation solutions for the transmitter side of the communication (Alice) and also for the receiver side (Bob) optical hybrid demodulators can be used. One of the most technologically advanced intensity modulator is the Exail NIR-MX800: the intrinsec and unparalleled benefits of LiNbO3 modulation offers high bandwidth, high contrast and ease of use.

Figure 4: Electro-optic modulator

The **model 686** Arbitrary Waveform Generators allow controlling directly those kind of Electro-Optic Modulator and to generate very short optical pulses. The unique features of generating pulse with 50 ps rise/fall time, 100 ps pulse width and 5Vpp amplitude offers the solution of driving the EOM without using an external amplifier.

Figure 5: Berkeley Nucleonics AWG- 686

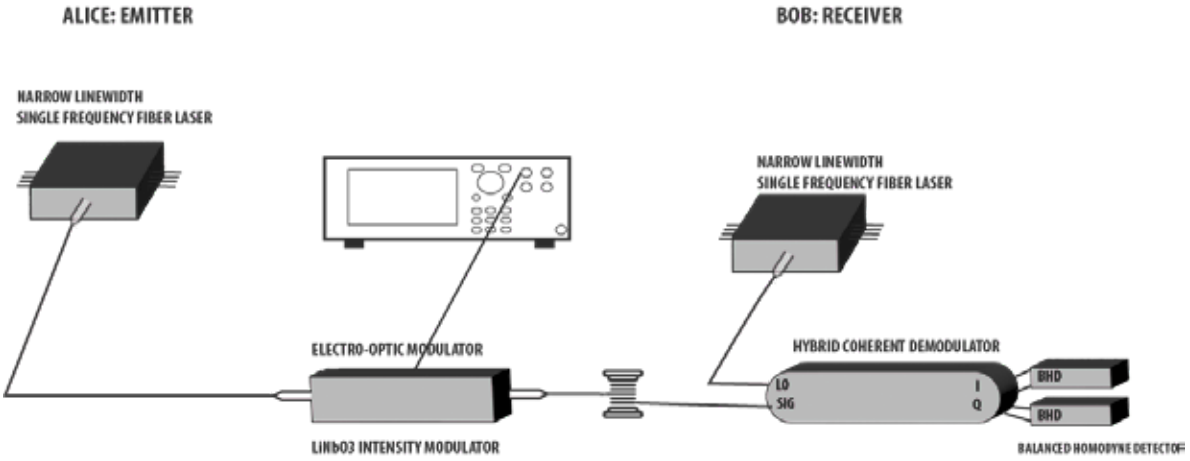

Figure 6: Short optical pulses generation with the 686

The diagram above represents a typical connection of the Arbitrary Waveform Generator 686 with a first modulation block used to generate short optical pulses. For example using Exail's NIR-MX800 and the Berkeley Nucleonics model 686, very short optical pulses width from 100 ps can be achieved at 850 nm, 1310 nm and 1550 nm respectively. It is important to note that in the connection diagram between the model 686 and the Intensity Modulator are not used external amplifier, since the model 686 is able to generate very narrow pulses of 100 ps width at full amplitude 5Vpp like in the pictures below.

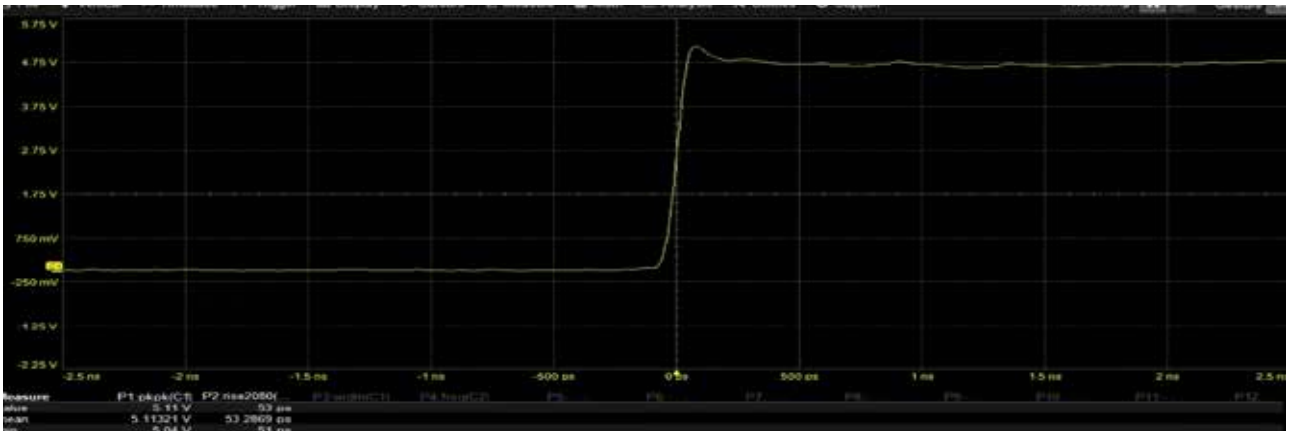

Figure 7: 50 ps Rise time @ 5Vpp

Figure 8: 100 ps pulse width @ 5Vpp

Quantum Sensors

Quantum sensors allow us to understand the world around us at an unprecedented level of detail: their advanced sensor technology vastly improves the accuracy of how we measure, navigate, study, explore, see, and interact with the world around us by sensing changes in motion, and electric and magnetic fields. The analyzed data is collected at the atomic level and collecting these "delicate" data at the atomic level often means extracting information from individual atoms instead of from the huge collections of atoms, as happens in classical physics.

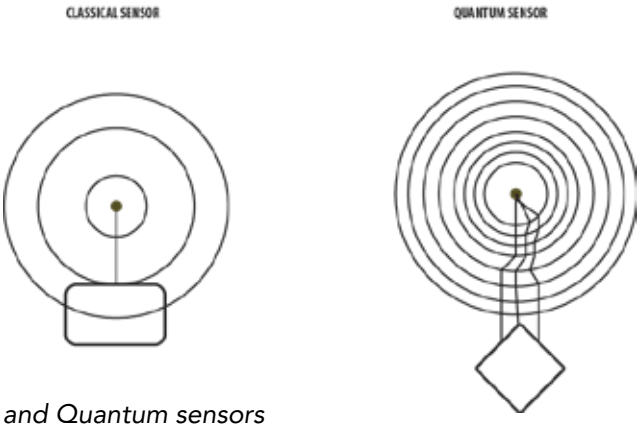

Figure 9: Classical and Quantum sensors

This allows quantum sensors to make our technological devices exponentially more accurate, more thorough, more efficient, and more productive. Devices that use quantum sensing are also not subject to the same physical constraints as conventional sensors, allowing for exceptional reliability with less vulnerability to the signal jamming and other electromagnetic interference that is increasingly common with today's light- and sound-based data sensors.

Because quantum sensing measures activity in the physical world using atomic properties, they can help in everyday's life for:

- faster, more accurate, more reliable geolocation than is possible with today's satellite-dependent global positioning system (GPS) devices, with far fewer limitations.
- Providing doctors with more detailed and accurate medical diagnostic images at lower cost and with fewer potential side effects for patients.
- Better, safer autonomous navigation of vehicles on the ground, in the air, and at sea – even in high traffic areas and around unexpected obstacles.
- More accurate and less vulnerable guidance systems in space, under water, and in the increasing number of zones overwhelmed by radio-frequency (RF) signals

- Reliable detection, imaging, and mapping of underground environments from transit tunnels, sewers, and water pipes to ancient ruins, mines, and subterranean habitats.
  Deeper, more active sensing of gravitational changes and tectonic shifts that can forewarn or trigger avalanches, earthquakes, volcanic eruptions, tsunamis, or climate change activities.

Magnetic Resonance Imaging

MRI quantum sensors have been around for decades. For example, MRI machines use quantum sensors and have been around since the 1970s. Inside one of these machines the very atoms in your body are turned into individual quantum sensors.
MRIs use magnetic fields to manipulate a quantum property called spin within your body's atoms, and the response of those spins to the magnetic fields can be measured and transformed into an image.

Figure 10: MRI machine

Nitrogen Vacancy Centers (NV) Magnetometer

Atomic clocks are another kind of quantum sensor and have been around since the 1950s. They keep time in GPS satellites and even define the official SI Atomic Clockunit of a second, but things have changed since then.
Modern innovations are making new quantum sensors and applications possible: one of these newer technologies makes use of nitrogen vacancy centers, or NV centers, which can be found or fabricated within diamonds.
Pure diamond consists of a perfect lattice of carbon atoms. If two of those adjacent carbons are removed and one is replaced with a nitrogen atom, then the nitrogen together with the hole or vacant spot function as an incredibly sensitive magnetometer.

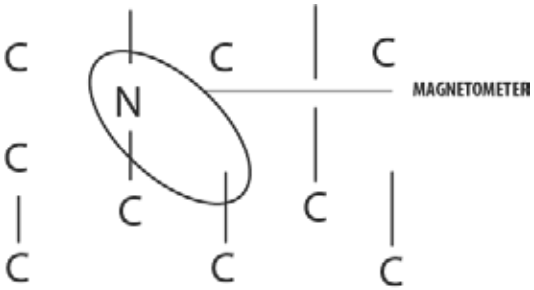

Figure 11: Magnetometer

That magnetometer uses electron spin to detect tiny changes in magnetic fields. In fact, NV centers are sensitive enough to detect changes that are 50 million times smaller than the strength of Earth's magnetic field. And even more impressive is that they can accurately detect those tiny changes despite the presence of the Earth's magnetic field in the background.

A diamond is a collection of carbon atoms, each bonded to four other carbons to form an orderly crystalline array. But sometimes there's a glitch in the matrix: a stray atom of another element finds its way in or a carbon atom is missing, leaving an empty space. These defects cause a diamond to sparkle in different hues, and are called colour centres.

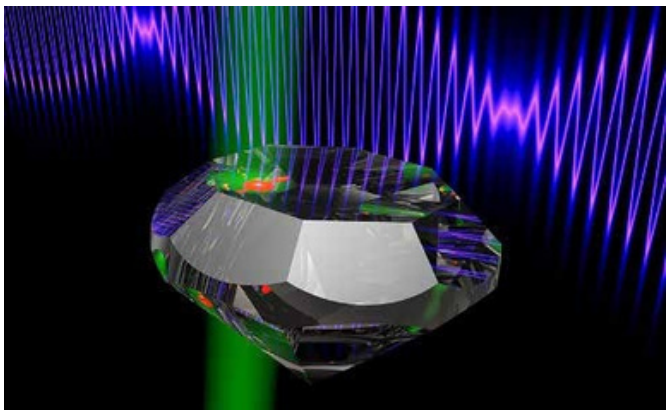

Figure 12: Nitrogen-vacancy centre in diamond

One particularly interesting defect occurs when a carbon in the crystal is replaced by a nitrogen atom, and the adjacent carbon is missing. This defect is known as a **nitrogen-vacancy (NV) centre** and has its own quantum spin, which can be thought of as a rotating magnet. Diamonds are mostly made of spin-neutral carbon-12 atoms, so the NV centre's spin is unaffected by that of its immediate neighbours. And because the diamond matrix is so stiff, the atoms don't jostle enough at room temperature to nudge the spin into a different state.

The spin can be altered, however, by electromagnetic radiation or a magnetic field — a property that enables diamonds with NV centres to be used as sensors. The NV centre is also photoluminescent: when lit with green light it will emit a red glow. Because the spin state of the NV centre determines how strongly the diamond fluoresces, scientists can use changes in brightness to monitor changes in the centre's spin state due to microwaves or a magnetic field. By examining which frequencies cause changes in the light, researchers can even use the diamond to measure the strength of a magnetic field. This technique is called optically detected magnetic resonance.

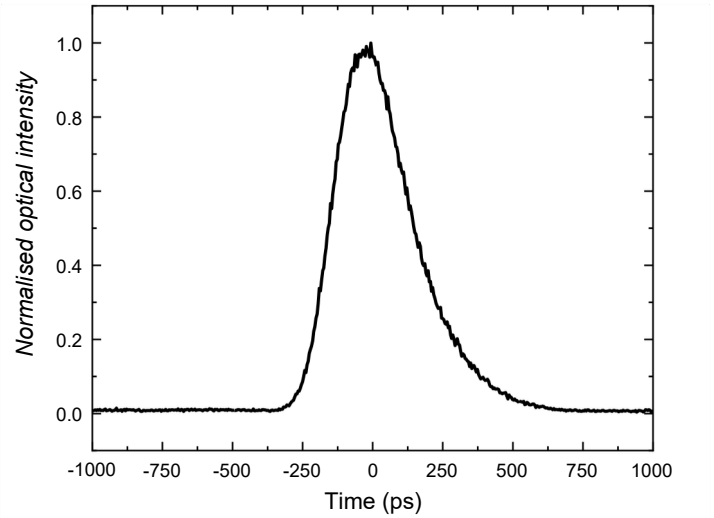

Figure 13: Gaussian pulse

The digital output channels of the model 686, allow to control acousto-optical amplitude modulators or they are used to generate trigger pulses for timing of experimental sequences. In the future, it will be necessary the real time control of the measurement protocols depending on the outcome of a certain readout within the sequence.

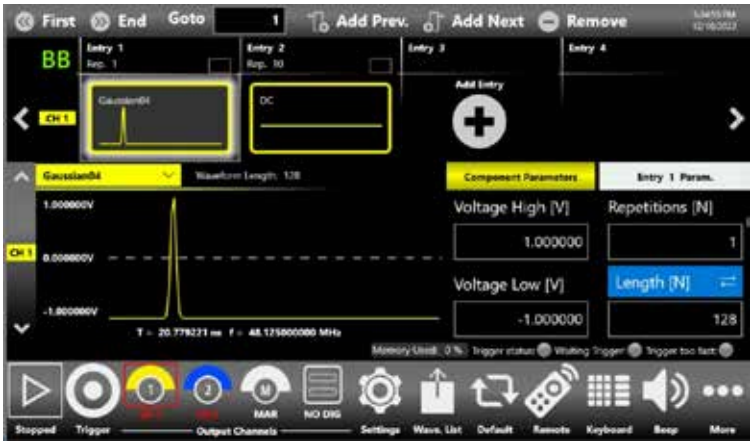

Figure 14: True-Arb UI

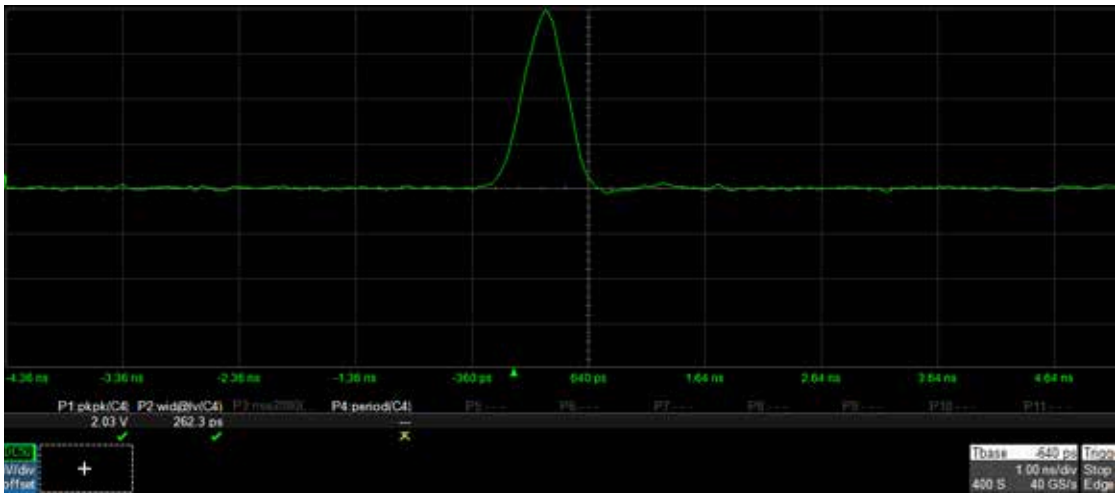

Figure 15: Narrow Gaussian pulse with model -686

BNC
Berkeley Nucleonics Corp.

Call us:

(800) 234- 7858

(415) 453- 9955

Email:

info@berkeleynucleonics.com

Linkedin:

www.linkedin.com/company/
berkeley-nucleonics-corporation

Youtube:

www.youtube.com/xBNC2Media

About Us

Berkeley Nucleonics Corporation (BNC) is a leading manufacture of precision electronic instrumentation for test and measurement, radiation detection, nuclear research and RF/microwave. From signal generators to spectrum analyzers, we offer the widest range of signal generation and analysis tools from a single manufacturer. Our application engineers are always available to discuss your specific needs. BNC happily offers product demonstrations if you're interested in testing out a unit on site to make sure that it is right for you.

Our corporate headquarters are in San Rafael, California, with additional manufacturing facilities and sales offices located throughout the United States.

Berkeley Nucleonics offers several short courses on RF, T&M and Nuclear technology to allow students and technical staff entering the field to quickly develop a basic understanding of the principles involved. Courses may be completed online and supplemented with downloadable materials. Completion certificates are issued and onsite training is also available.