Noisecom

25 Eastmans Road
Parsippany, NJ 07054 USA

Encryption Solutions with Noise Sources

As data travels over a communications network, its safety and security must be assured while in transit. Without protection, unauthorized parties can gain access to confidential information. Encryption is a process that safeguards sensitive data along a communications pathway, ensuring it is received by only the intended recipient. This process involves encrypting data before transmission, so it appears unintelligible to would-be interceptors, while the authorized recipient safely decrypts the data upon arrival.

Encryption systems typically use an algorithmically generated, pseudo-random sequence to encode and decode data. The pseudo-random key masks data from network eavesdroppers as well as enables the receiver to decipher the contents. Interception is possible without possessing the specific key; however, this feat demands vast computational resources. While keys are sufficient for various encryption use-cases, they are not produced by genuinely random processes and theoretically repeat. Furthermore, complicated encryption algorithms can increase system inefficiency and resource investments.

Instruments that generate noise waveforms eliminate the need for pseudo-random keys, providing a method that utilizes a truly random signal to strengthen viability against interception. By using a Zener diode in a reverse biased circuit, noise sources can generate random white noise with a constant power spectral density and a Gaussian distribution, referred to as additive white Gaussian noise (AWGN) waveforms. The resulting AWGN-camouflaged transmission will be seen as inconsequential background noise while traveling to its authorized destination. In addition to producing a completely random signal, noise sources also provide a simpler, more efficient process of signal generation when compared to systems that rely upon complex algorithms for data encryption.

For more than 30 years, Noisecom has been designing noise generation devices and instruments for Carrier-to-Noise, signal jamming and impairment, multipath fading, satellite test, and calibration across a wide variety of industries. Noisecom has a depth of experience unmatched in the industry and works closely with technical end users to find the right project for the application with both off-the-shelf and customized solutions. This experience and close relationship with customers and markets has led to the development of amplified and calibrated coaxial AWGN modules that can supply truly random, easily generated noise waveforms to fortify the design of today’s encryption systems.

Customization

Each encryption setup is different, and the set of technical challenges varies in every device or system. This diverse range of unique encryption system requirements is why Noisecom products, including amplified and calibrated coaxial AWGN modules, are highly customizable to meet the unique needs of challenging applications. Noise sources can be customized for high power, high crest factor, and flexibility in frequency range and output characteristics, among other project-specific requirements. Whether it is an encryption system drawing inspiration from RF signal polarization or noise radar technology, Noisecom has a broad range of capabilities and solutions for every budget.

RF Signal Polarization

Encryption systems built around the concept of RF signal polarization can use noise waveforms to securely send and decrypt information. Transmissions consist of oppositely polarized RF signals, such as on the horizontal and vertical planes, with one polarization containing a noise waveform and the other comprising of the same noise waveform plus the sensitive data. Disguised during transit, receive antennas designed to capture both polarizations combine the two captured signals out of phase to cancel out the noise and reveal the data.

Noise encryption based on RF signal polarization can only integrate a single physical noise generating device, which is typically implemented on the transmit side of the encryption circuit. This leaves the receiver to employ specific decryption techniques to extract the data from the noise signal. Due to a noise source's random nature and lack of coherency, two noise signals generated from different devices (even of the same make and model) will not have matching timing and voltage characteristics, rendering them ineffective for encryption and decryption.

Noise encryption systems that utilize RF signal polarization techniques require higher power noise sources due to the inherent losses suffered when transmitting a signal through a guiding structure (i.e., an antenna) and into the air to travel over free space. The Noisecom NC1000 Series Amplified Noise Modules produce AWGN as high as +13 dBm and have bandwidths up to 18 GHz in a compact, low-cost form factor. The high-power modules produce the power levels necessary to overcome a transmission's free-space losses after leaving the dual-polarized antenna. Beyond the standard configuration in the product range, various customizations are available to meet specific encryption system requirements (Figure 1).

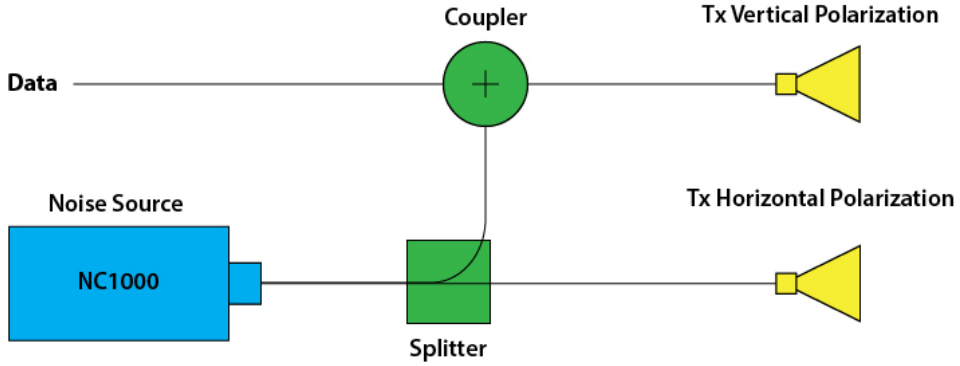

Figure 1: An encryption system's horizontal (noise from the NC1000 Series) and vertical (noise plus data) polarizations.

Noise Radar Technology

The notions behind noise radar technology can serve as a foundation for noise-based encryption systems. Reducing the probability of signal interception and exploitation, noise radar combines a transmit signal with a noise waveform, typically generated from a high-frequency noise source. The signal, posing as negligible background noise, reflects off an intended target (e.g., an aircraft) and is recaptured by the radar antenna. Analyzing the reflected signal and uncovering its changes from the initial transmission can

determine various pieces of desired information about the object of interest, (e.g., distance, angle, and velocity). While noise radar reduces the signal's visibility from adversaries, it also limits mutual interference from other radar signals when operating in crowded environments. Similarly, only a single physical noise source, typically on the transmit side, can be embedded into encryption systems using noise radar techniques due to a noise source's truly random and noncoherent characteristics.

Noisecom noise sources, such as the NC3000 Series Calibrated Coaxial AWGN Modules and NC1000 Series Amplified Noise Modules, provide optimal noise signals for encryption systems utilizing noise radar techniques. The preferred component depends on system-specific requirements and the stage at which the noise signal will be added. The NC1000 Series, for instance, would be best suited for later-stage integration within an encryption system after amplification occurs (Figure 2). The ability of the NC1000 Series to produce AWGN up to +13 dBm is again able to overcome any inherent signal losses after transmission. If a noise source is used that is too low in power, the noise signal will get lost within the background noise that is intrinsic in the environment.

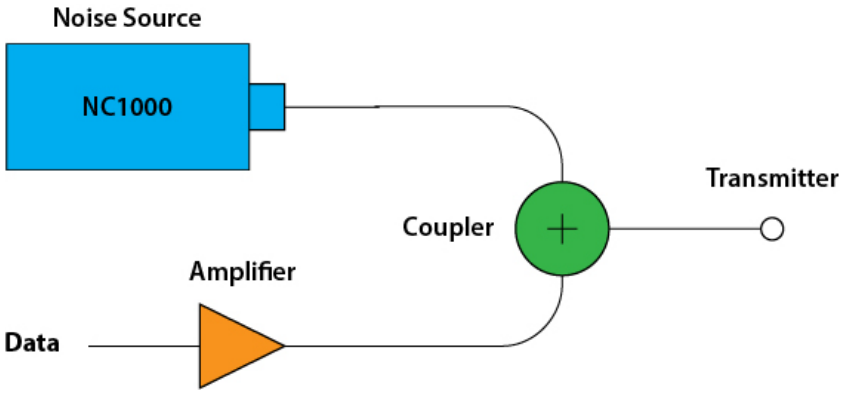

Figure 2: The high-power NC1000 Series can integrate later in a noise radar-based encryption system.

The NC3000 Series, on the other hand, would prove most useful at an earlier stage in an encryption system, such as where the data is being manipulated before subsequent amplification (Figure 3). Ideal for applications requiring broad bandwidth and fast switching time, the NC3000 Series include high noise output modules between 26 and 35 dB ± 1 dB Excess Noise Ratio (ENR).

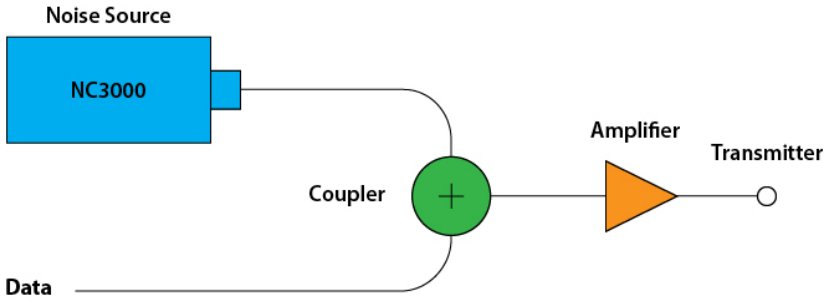

Figure 3: Integration of the NC3000 Series earlier in the encryption process, before amplification stages.

The safety of data is paramount, and noise sources offer an effective way to enhance today's advanced encryption systems. To learn more, visit noisecom.com.