Application of the Frequency Based Coding to Smart Gun Technology

Award Number 2002-IJ-CX-K006

Final Report: draft
Technology Next, Inc.

Application of the Frequency Based Coding to Smart Gun Technology

EXECUTIVE SUMMARY

This effort was funded by the US Department of Justice, Office of Justice Programs, National Institute of Justice (NIJ). NIJ's purpose in funding this effort was to explore an innovative approach to the solution of "a handgun that operates in a normal manner for authorized law enforcement users, but disables itself when in the possession of an unauthorized user."

The goal of this project was to examine and develop a technical design of a smart gun system based on Company's proprietary technology "Frequency Based Coding" (FBC) that would meet or exceed the requirements set in two Sandia National Laboratories reports on smart gun technologies (SAND-96-1131, "Smart Gun Technology Final Report", and updated SAND2001-3499, "Smart Gun Technology Update").

This report presents an electronic design that adapts the proprietary FBC technology so it can be used as an add-on part of a smart gun system which is addressed in details in the technical section of this report.

SYSTEM OVERVIEW

Terminology

The proposed technology belongs to the class of radio frequency identification (RFID) systems. In the report terminology associated with smart gun technologies and RFID is used interchangeably. A valid operator who is recognized by the system is an "authorized user", and the process of recognition is named "authorization". The unique identifier of an authorized user is called "key". The circuitry and software that evaluates the key and compares it to the list of authorized users is determined as "discriminator". In RFID terms "key" is synonymous with the transmitter and "discriminator" is associated with the receiver. The mechanical part of the system is "latch" that "unlocks" the firearm to allow it to be fired by an authorized user. The functional subsystem named "use-control" consists of the key, discriminator, and the latch. Finally, the process of adding the user to the list of authorized users is referred as "enrollment".

SYSTEM DESIGN

FBC Technology

While there is no perfect solution for the smart gun technology, RFID is presently viewed as the best candidate. In this class Frequency Based Coding (FBC) developed by Technology Next has a number of significant advantages over the existing RFID technologies that can enhance the reliability of a smart gun system. The characteristics that make FBC technology unique are the robustness of its specific signal which makes radio signals interference impossible.

The goal of this effort was to design three modules: two components of the use-control subsystem, namely the transmitter module and the receiver module, as well as the enrollment/code re-setting module. Designing latch was not part of this effort.

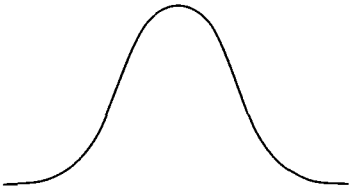
The transmitter module – the key – consists of a chip embedded in a ring that the authorized user wears on his firing hand. The other chip – the receiver module – is embedded in the firearm. The discriminator is a part of the receiver module. Unless the ring is within a few inches of the pistols grip, the gun cannot be made to fire. The transmitter can be placed in different ways but we have chosen to embed it in the ring which minimizes transmission distance and thus power consumption.

ID Signal

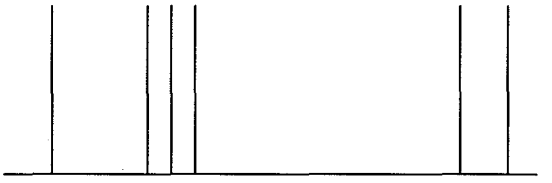
By definition, any ID signal should transmit the same information permanently. The signal transmission theory states that the information transmission rate for such signal is a very small value. This feature gives us an opportunity to make the signal undetectable, immune to jamming and radio interference.

Frequency Based Coding (FBC) is an RFID technology with novel signal structure, which is based on the mentioned above characteristics of the ID signal. Any ID information can be transformed into binary code. FBC system uses this binary code for the ID signal transmission. FBC signal consists of a number of carriers at different frequencies instead of one single carrier.

The transmitter broadcasts these carriers that have extremely narrow bandwidth. The basic FBC coding principle is that the existence or absence of a carrier is a binary "1" or binary "0" respectively. The spectrum of the transmitted signal would be modified as it is schematically shown:



Conventional Spectrum



FBC Spectrum

This narrow bandwidth signal has no modulation and due to that FBC signal is optimized for hiding it within noise.

This coding method provides sufficient number of options to prepare codes for all the guns on the Earth with small number of transmitted carriers. By using the coding principle – existence/absence of carrier means 1/0 in binary coding – we get the total number of possible options:

$$N! / (N-K)! / K!$$

Where:

N is the number of possible carriers
K is the number of transmitted carriers

For N = 64 & K = 32 the quantity of options is $1.8*10^{18}$

Frequency Selection

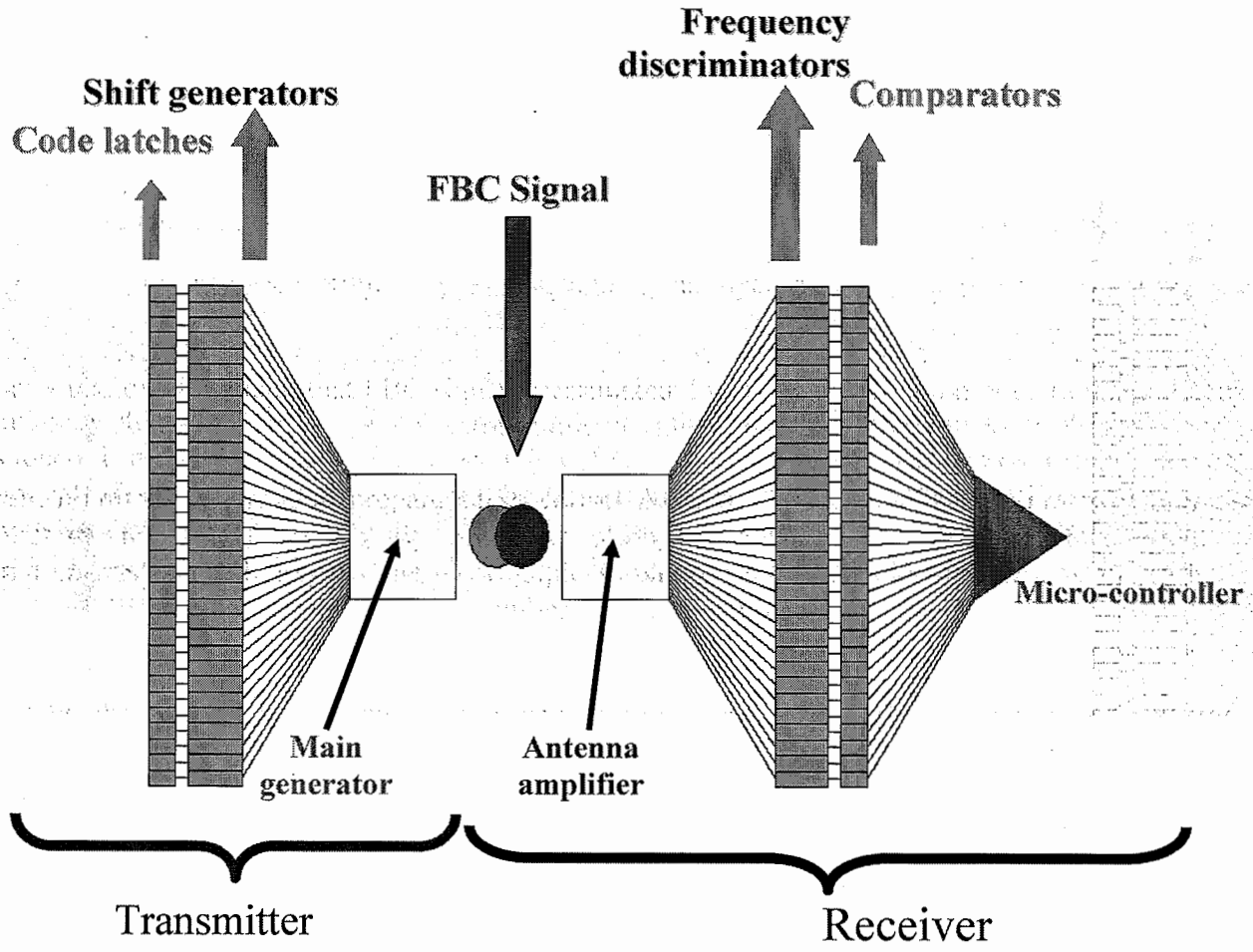
Any electronic transmitting device placed next to human skin has an issue with frequency stability. To overcome this problem coding based on frequencies' difference was included in the design. With this feature FBC system has no limitations on the stability of the main frequency.

Based on the FCC frequency allocation table the main frequency was chosen in the range 150-450 MHz. Due to low transmitting power, FBC system has no limitations regarding the FCC compliance under 47CFR15.109.

As to the shift frequencies they were chosen in the range of 2-9 MHz. The shift frequencies' stability had to be better than 0.05%. The latter requirement created additional difficulties for the design of shift generators because of the IC design limitations.

ELECTRONIC SCHEMATICS DESIGN

The whole system can be presented as follows:



The system consists of three parts: transmitter chip, receiver chip with signal analyzing module, and a special module for users' enrollment and code re-setting. For the system to satisfy the updated requirements a number of technical problems had to be resolved in the process of designing the FBC system:

- Increase transmitter battery lifetime
- Integrate protection from take-away
- Integrate protection from reverse engineering
- Incorporate protection from radio frequencies interference, eavesdropping, and jamming
- Establish users hierarchy
- Add new feature of re-setting the codes on the transmitter/receiver pair

Transmitter Battery Lifetime

Our system is designed to work in the permanent transmission mode as it is the most reliable method of signal exchange. According to the existing requirements battery lifetime should be more than 12 months. In our design 10000 hours of uninterrupted transmitter work were projected.

Transmitter weight/volume limitations are so stringent that it is possible to embed in the ring the batteries with maximum charge capacity 0.2 A-h. Computer simulation of the system showed that transmitter power consumption is less than 0.02 mA, which is enough for the battery lifetime of more than 10000 hours.

System Protection

The frequency based coding provides a possibility to develop a design for the ID system based on codes stored in the system. Both the transmitter and the receiver keep code while batteries are on. Switching off power necessitates codes re-setting.

The developed transmitter design includes secondary control system (toggle switch) that switches off power if the ring is taken away. The receiver has similar secondary control system (toggle switch) that switches off power if any attempt to open a gun is made. By switching off power these secondary control systems erase all the codes stored in the system. The actual design of the FBC ID system based on codes stored in the system makes reverse engineering useless.

Protection from Radio Frequencies Interference, Eavesdropping, and Jamming

The FBC principle of coding provides the opportunity to avoid the eavesdropping problem entirely. The carriers forming the signal could be placed at any frequency bandwidth, which prevents signal analysis. High frequencies difference and high main frequency prevents signal recording and its transmission backward.

FBC implementation prevents jamming of the system due to the extremely narrow bandwidth of each carrier. Any jamming attempt would require extremely high power of

electromagnetic waves. Radio frequencies interference is impossible for the exact same reason.

Hierarchy of Users

For initial design number of carriers was fixed to:

$$N = 64$$

These carriers were divided into the following three groups:

Top code: 8 carriers: 255 combinations
Team code: 50 carriers: $1.2 * 10^{15}$ combinations
Member code: 6 carriers: 64 combinations

Each group has separate means of code registration to prevent unauthorized privilege elevation.

Group Designation

Top group

Their codes enable designated superior officers to use any guns of the associated teams.

Team group

Their codes permit team members to use firearms assigned to their team. These codes should be re-set periodically for each team by law enforcement agency.

Member codes

These codes allow tracing the use of a given firearm to a specific team member and will have no effect on their own actions with the guns.

Re-setting the gun requires special authorization. The re-setting device contains authentication infrastructure to enable this restriction.

Codes Re-setting

The FBC ID system can prevent possible collaboration between criminals and some law enforcement officers by periodical code changes by law enforcement agencies and, consequently, by re-setting codes using special cards and without any disclosure to the team members.

Both the transmitter and the receiver have two working modes: normal and code recording. For re-setting the codes on the transmitter and the receiver the third module was designed. Special signal activated by the third module switches the working modes of the transmitter and the receiver. This special logic signal is a time sequence frequency-hopping signal that prevents non-authorized users from reading this signal from the hardware.

The transmitter has additional pin jack for special signal, which is a sum of proper shift generator signals and special logic signal initializing the code recording.

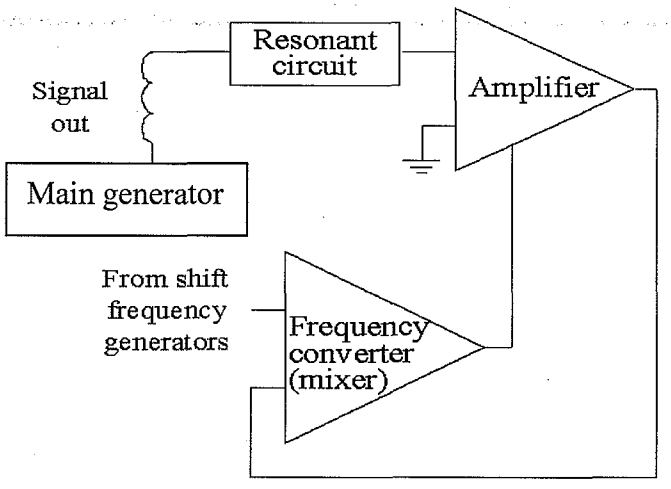
The receiver has additional pin jack for a special logic signal only. While the special logic signal is applied to the receiver, the transmitter must be placed near the receiver to provide the code from transmitter to the receiver. By this procedure we excluded any mistakes in the re-setting the codes into the pair transmitter-receiver.

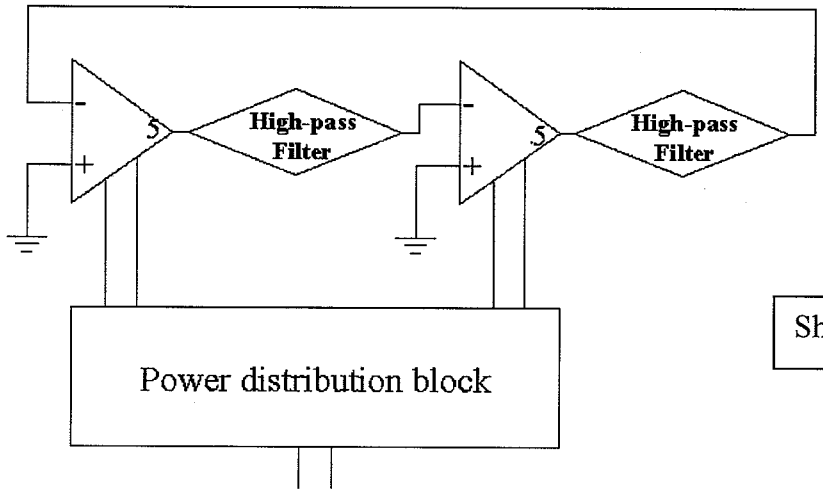
SCHEMATICS DESIGN

The system consists of two main modules: the transmitter and the receiver. Both modules have two working modes: signal exchange and recording. The equipment for the re-setting codes for these two modules was designed as an additional module.

Transmitter and Receiver

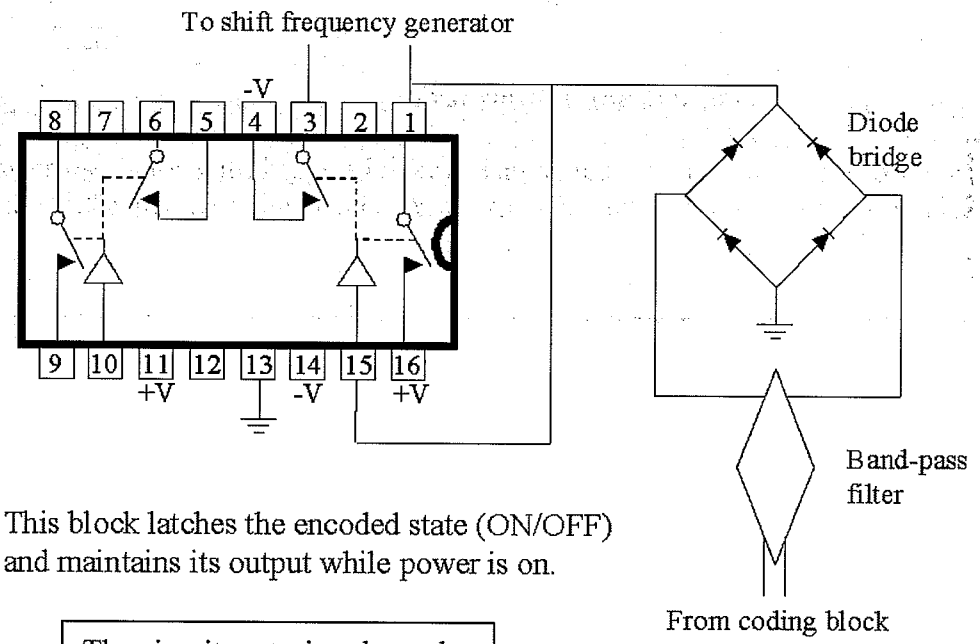
The transmitter was designed as a low power oscillator with high efficiency. The signal from this oscillator was mixed with precise shift generators signals. The resulting signal was a mix of shifted and unchanged signals.





Shift frequency generator

The circuitry that stores the codes was designed using the Maxim' analog circuitry switches with the power consumption 1 nW each.



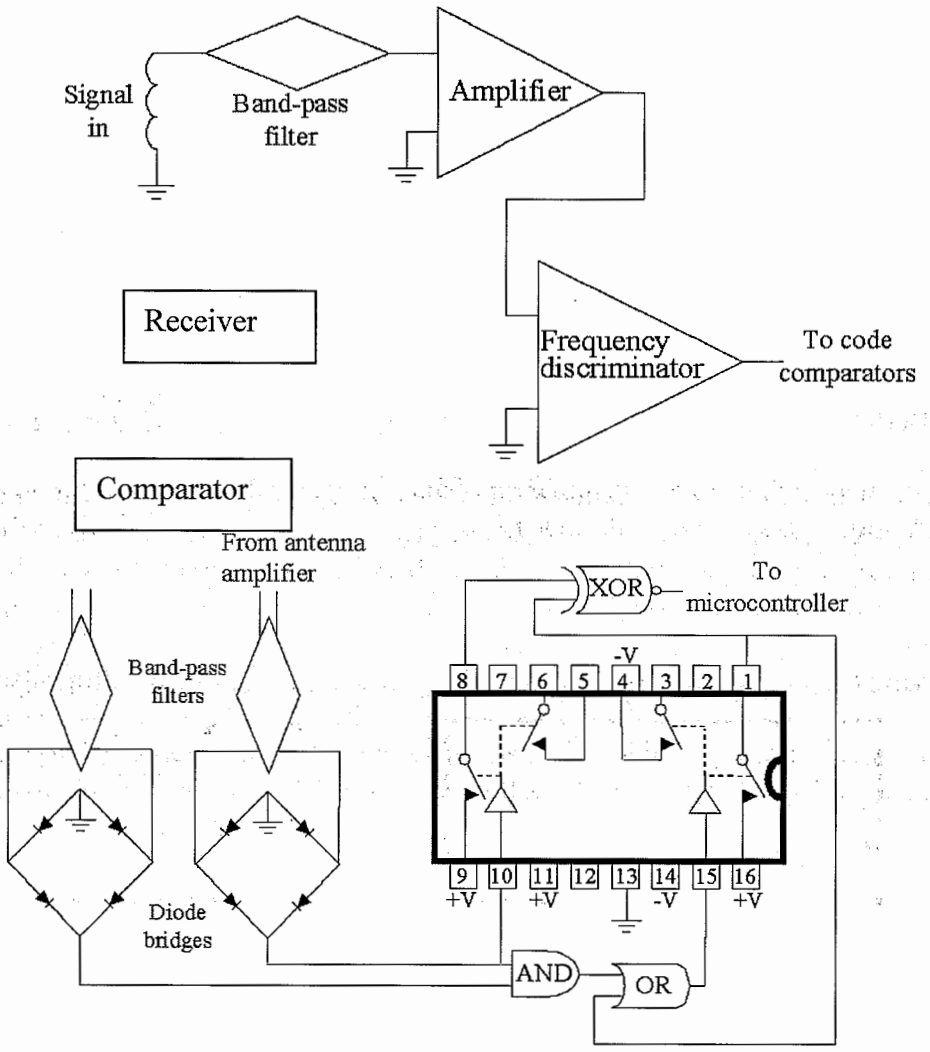
This block latches the encoded state (ON/OFF) and maintains its output while power is on.

The circuitry storing the codes

The receiver was designed as a resonance antenna amplifier with multi-channel discriminators for each carrier. The circuitry that stores the codes was designed in the same way as it was done for the transmitter. This circuitry sends the signal to the latch.

Two independent groups of discriminators were designed to provide independent signal analysis for "top group" and for "team group" of users. We did not do any design for the

"member codes" recording. This part of schematics depends on the requirements from the law enforcement community regarding the number of rounds fired that should be recorded.



It is worth noting that we encountered serious problems with PSpice models for components while designing the FBC smart gun system. The existing PSpice models are not accurate enough for low voltage range of power supply. The absence of the precise PSpice models for components in the required parameters range forced us to carry out more accurate measurements. The main results of these measurements were new data on the power consumption of the components. These PSpice model calibrations were not anticipated and thus were not stipulated in the initial working plan. These calibrations delayed the completion of the project.

Summary

The goal of this effort was to adapt a new signal transmission technology, Frequency Based Coding (FBC) developed by Technology Next to smart gun system. The characteristics that make this novel FBC technology unique are the robustness of its specific signal that has the potential to enhance the reliability of a smart gun system.

To prove this premise Technology Next designed three modules: the transmitter module and the receiver module, as well as the enrollment/code re-setting module. Computer simulation of these modules proved the effectiveness of this technological approach to creating smart gun system. Stability and reliability of the electronic schematics were confirmed. In addition, electronic schematics developed during this effort include all the initially suggested smart gun system features.

At present Technology Next is looking for additional funds to assemble the system.