NATIONAL SECURITY AGENCY
TECHNOLOGY TRANSFER PROGRAM

Office of Research & Technology Applications

NSA PATENT PORTFOLIO

CREATING PARTNERSHIPS

IGNITING INNOVATION

NSA Patent Portfolio

V 4.0

National Security Agency
Technology Transfer Program
Office of Research & Technology Applications
NSA Research Directorate
9800 Savage Road, Suite 6843
Ft. Meade, MD 20755-6843

tech_transfer@nsa.gov
866-680-4539
www.nsa.gov/techtransfer

S cientific breakthroughs and technical advances can be accelerated through successful partnerships between the public and private sectors. Shared knowledge inspires and challenges this country's brightest minds to create products that shape our future.

This is the goal of the National Security Agency (NSA) Technology Transfer Program's (TTP) patent licensing activities—to create dynamic, effective partnerships between the Agency and industry that deliver advanced capabilities into the marketplace. Since 2010, the White House has focused on initiatives to increase the impact of federally-funded research, boosting economic growth through commercialization efforts. A healthy and growing economy yields a more secure and stable nation. It is our priority to use NSA's research to support technology development that will advance Agency mission, create jobs, grow our economy, and add dimension, depth, and strength to our national security.

Patent license agreements with NSA create opportunities for businesses to gain product differentiation and a competitive edge. Our greatest satisfaction comes from helping businesses discover new applications for Agency technologies. Whether your business is a large corporation, a medium-sized business, or an entrepreneurial start-up, the NSA TTP stands ready to be your committed partner. We hope you will work with us to ignite innovation at your company!

Sincerely,

Linda L. Burger

Linda Burger
Director, NSA Office of Research & Technology Applications (ORTA)
Technology Transfer Program

Awards

Excellence in Tech Transfer, Federal Laboratory Consortium 2017, 2015, 2012

🏆 **American Inhouse Design Awards**, Graphic Design USA (2017)
🏆 **Maryland's 2016 Top 100 Women**, Daily Record (Linda Burger 2016)
🏆 **Top 18 Women in Technology**, State of Maryland (Linda Burger 2016)

Table of Contents

INTERNET OF THINGS (IOT)   41

MOBILITY   49

References   67

> *"A game changer... that is how I describe the effect of licensing NSA technology on my business.* The next generation of our data encryption app will have NSA's patented technology as the foundation. Once released commercially, this app will be cryptographically stronger and more efficient than existing authenticated encryption solutions in the marketplace."

Sudesh Kumar, Founder and CEO
Kapalya, Inc.

> *"Licensing NSA's port protector technology has allowed us to expand our market share and add new product lines.* As a small business, we benefited from a partnership scaled to address our needs as we grew."

Jim Bolain, Founder and CEO
PadJack, Inc.

Our Mission

The National Security Agency (NSA) Technology Transfer Program (TTP) mission is to:

- Establish partnerships to translate NSA discoveries into commercial products and practical applications that strengthen national security and help grow the economy, and
- Accelerate the exchange of expertise and capabilities between NSA and industry, academia, and other government agencies to advance NSA mission, technology, and innovation.

Our mission fulfills federal technology transfer legislation, White House Cross-Agency Priority (CAP) goals, and NSA mission objectives.[1]

[1] *Legislation, policy, and guiding principles can be found in the References section of this catalog.*

Leveraging NSA Technology

Patent License Agreements (PLAs)

A PLA is an agreement that allows businesses to license patented NSA technology for commercial purposes. These agreements can be exclusive or non-exclusive, and the terms of each PLA are negotiated individually. Once a PLA is in place, NSA's TTP continues to be a partner for business, connecting companies to valuable resources throughout the innovation ecosystem.

GOVERNMENT FUNDS   **FEDERAL LABS, R&D**   **COMMERCIAL MARKETPLACE**

Benefits

- Create new products or enhance your current products
- Launch a company around one of our technologies
- Achieve market advantage by accessing innovative technology
- Save time and money by leveraging federal research and development (R&D) resources

1. Discover
Browse our patent portfolio

Discover NSA technologies in this patent portfolio, which provides a listing of NSA technologies available for licensing.

2. Imagine
Grow your company with our technologies

Does one of our patents interest you? Imagine fueling your business's growth with NSA technology.

3. Connect
Reach out to NSA's TTP

Contact us and get help moving your ideas to innovation! 866-680-4539 or tech_transfer@nsa.gov

4. Engage
Talk with our inventors

Get first-hand access to the intellect behind NSA's inventions.

5. Pitch
Provide your plan for our technology

How will you use our technology? Tell us your business plan and outline your technical, business, marketing, and economic strategy.

6. Negotiate
Let's make a deal

Now that your business plan has been accepted, it's time to negotiate and sign a patent license agreement.

7. Acquire
Put NSA technology to work for you

Bring your idea to life by moving NSA technology from the lab to the commercial marketplace.

8. Create
New products, new business, new jobs

Do your part to strengthen the economy by creating new products, businesses, and jobs.

NSA Technologies Available for Licensing

NSA's patent portfolio contains solutions that span four primary technology categories: Big Data, Cyber, Internet of Things (IoT), and Mobility. Not sure where to start? You can also take a look at our index of keywords in the back of this catalog. Full patent text can be found on the United States Patent and Trademark Office website (www.uspto.gov).

There are always new technologies being created at NSA. Contact us to learn more!

The NSA TTP is always happy to provide more details on any of our patents or answer any questions about working with us. Feel free to contact us at tech_transfer@nsa.gov or 866-680-4539.

Big Data

Big data is a term for data sets that are so large or complex that they become difficult to work with using traditional data processing applications. Managing data at such a large scale brings its own set of challenges; exceptional technologies are needed to efficiently complete tasks such as capturing, storing, visualizing, and analyzing data. NSA has taken the lead in confronting complications in dealing with big data, exploring and developing solutions for processing, managing, and/or analyzing large amounts of data. The innovations in this section span multiple industries including acoustics, mathematics, communications, and information processing.

Cyber

Cyber relates to information technology, computer hardware, computer software, computer networks, or the internet. Oftentimes, cyber describes the digital version of something that has a non-digital counterpart. For example, cyberspace is the non-physical terrain created by computer systems.

Navigating the safest and fastest path through cyberspace involves many moving pieces. The ever-evolving cyber field presents opportunities for dynamic solutions for information processing, networking, and physical, hardware, and access security. Through novel research and design, NSA is able to offer innovations that enable improved authentication, protect an array of data ports, and provide other cyber security measures.

Internet of Things (IoT)

IoT describes networks of objects that transmit data. These objects may be connected to the internet, internal networks, or peer-to-peer paths. IoT uses data-gathering sensors and cloud computing to make objects "smart." As the demand for internet-enabled devices continues to grow, NSA similarly continues to expand its development of IoT technologies. The innovations in this section provide time and cost-saving efficiencies, ensure accuracy of results, and improve or replace complicated or expensive solutions for technologies in the microelectronics and optic arenas.

Mobility

Mobility can be generally defined as a technology or methodology that enables the free and efficient movement of data, things, people, or services. NSA has long applied its intelligence and expertise to the mobility field by finding new ways to ensure that information is transported both safely and securely. The technologies in this section have numerous applications in several fields including signals processing, physical security, and communications.

Big Data

Big data is a term for data sets that are so large or complex that they become difficult to work with using traditional data processing applications. Managing data at such a large scale brings its own set of challenges; exceptional technologies are needed to efficiently complete tasks such as capturing, storing, visualizing, and analyzing data. NSA has taken the lead in confronting complications in dealing with big data, exploring and developing solutions for processing, managing, and/or analyzing large amounts of data. The innovations in this section span multiple industries including acoustics, mathematics, communications, and information processing.

Single-Image Super Resolution of Low Resolution Images

Method of Neighbor Embedding for OCR Enhancement
US PATENT # 8,938,118 | EXPIRES MAY 5, 2033

This technology improves the readability of optical character recognition (OCR) output for low resolution (LR) scanned documents. Super resolution (SR) images are typically generated using multiple LR images. This invention, however, is a single-image super resolution (SISR) method that drastically reduces the character error rate (CER) found when high resolution image estimates obtained with this technology are input to OCR engines, compared with CER found with the original LR images. Moreover, this technology significantly lowers CER found with competing SISR methods, with speed comparable to fast SISR interpolation methods.

POTENTIAL APPLICATIONS:

- Document archival and retrieval
- Automated tools for information management and maintenance
- Document image collection

SAGA: Measuring Similarity between Data Sets

Device for and Method of Measuring Similarity between Sets
**US PATENT # 8,799,339 | EXPIRES OCTOBER 19, 2032**

This invention measures similarities between sets of data. The data could be natural-language documents or articles, product descriptions, queries, computer code, metadata, or measurements from any real-world objects or processes. The technology is able to determine similarities between data sets without needing to know how they interact. Omitting duplicate pieces of data allows the technology to provide more accurate results. Additionally, this technology can provide patterns over time of the data entered. This invention takes a holistic view of the data to make recommendations that are more accurate than commonly used methods.

Critical for managing and sorting through immense quantities of data, this capability can enhance big data analytics in multiple fields including online shopping, social media, genetics, and law enforcement.

POTENTIAL APPLICATIONS:

- A recommendation system that is more accurate and doesn't require ratings
- Analyze usage patterns in websites or applications
- Social network analysis
- Focused advertising
- Identify correlations in medical documents, articles, or reports
- Genetic analysis
- Forensic accounting
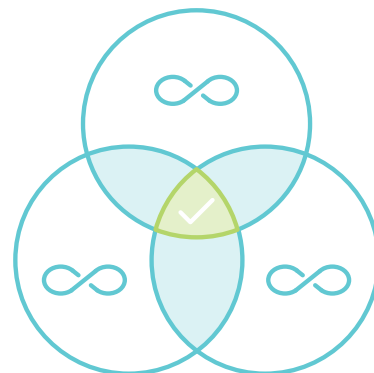
Linear Interpolative Coding

Device for and Method of Linear Interpolative Coding
US PATENT # 8,539,307 | EXPIRES APRIL 14, 2032

Data transmission is no stranger to packet loss, but what can you do when the missing information is vital? This technology can test the continuity of data packets and predict—based on what came before and after the loss—what information is missing or garbled. The tool could be used for debugging, data analysis, or error detection for all types of transmissions including sound samples and facsimiles.

POTENTIAL APPLICATIONS:

- Data acquisition and forwarding systems
- Debugging and/or analysis (e.g., debugging errors in a handshake)
- Telecom equipment that interfaces with different timing and communication systems
- Analog to digital conversion (e.g., digitizing audio, scanning documents)
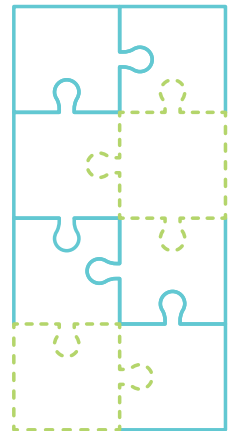
Real-Time Simultaneous Identification of Multiple Voices

Biomimetic Voice Identifier
US PATENT # 8,442,825 | EXPIRES JANUARY 18, 2032

Infinite Impulse Response Resonator Digital Filter
US PATENT # 8,396,912 | EXPIRES NOVEMBER 15, 2031

The technology provides multiple speaker identification by identifying voices (or other sounds) in a manner that uniquely mimics the essence of the ear-to-brain interconnection through extensive human voice identification learning and recognition training. The object is real-time or faster voice identification needing only relatively simple computing resources. Specifically, this invention looks for prosody matches (spectral patterns over time periods) that were trained into a software Artificial Neural Network (ANN)—based model. Although intended to be used together, the Infinite Impulse Response (IIR) filter patent can be singularly applied to other uses as well.

REAL-TIME VOICE IDENTIFICATION

POTENTIAL APPLICATIONS:

- Voice recognition for home automation
- Sound detection for security systems
- Assistive technology
- Audio forensics
- Biomimetic voice systems

Digital Transmission Decoder

Device for and Method of Identifying Minimum Candidate Codewords for List Decoder
US PATENT # 8,397,146 | EXPIRES OCTOBER 19, 2033

BIG DATA

This technology streamlines the decoding of digital transmissions by identifying which parts are the actual message and should be decoded first. The system also identifies the minimum number of messages that must be decoded to achieve desired results.

Encoded messages typically contain redundant data to counteract communications noise that can introduce errors, but the presence of extra information makes decoding more difficult. This technology overcomes the problem by treating redundant data as code words that identify the message portion.

POTENTIAL APPLICATIONS:

- Telecommunications
- Knowledge management
- Big data analytics

ScribeZone®: A Multimedia Instructional Design System
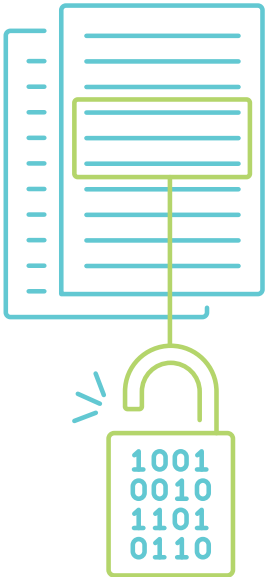
Device for and Method of Language Processing
US PATENT # 8,380,485 | EXPIRES AUGUST 11, 2031

BIG DATA

ScribeZone® is an educational technology that facilitates development and delivery of interactive multimedia courseware for the classroom. ScribeZone® enables instructors to synchronize multimedia files with their corresponding written texts and then divide the media into manageable learning blocks to appropriately focus and challenge their learners. Instructors can customize and frame courseware with hints, glossaries, and links to outside resources. ScribeZone® presents the multimedia courseware and its sophisticated media playback system in one window, making course materials easy to develop, access, navigate, and complete.

POTENTIAL APPLICATIONS:

- K-12 and higher education
- Foreign language and English as a Second Language (ESL) courseware development
- Government, military, and law enforcement applications
- Medical and legal transcription and translation
- Media and broadcasting

Collision-Free Hashing for Near-Match Inputs

Device for and Method of Collision-Free Hashing for Near-Match Inputs
US PATENT # 8,363,825 | EXPIRES FEBRUARY 26, 2031

Method of Collision-Free Hashing for Near-Match Inputs
US PATENT # 8,355,501 | EXPIRES FEBRUARY 3, 2032

BIG DATA

This technology is a hash function that does not produce collisions for inputs that are near matches of each other, enabling faster hashing and data retrieval. In this instance, a near match is one where the number of bit locations that differ is small and, therefore, could more easily be found than if the inputs were not near matches. This technology reduces the time spent searching for collision-causing inputs.

POTENTIAL APPLICATIONS:

- Big data analytics
- Data processing
- Encryption algorithms

HASH FUNCTION

NO COLLISIONS
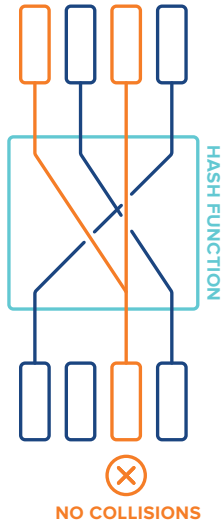
Assessing Language Translation and Interpretation

Method of Assessing Language Translation and Interpretation
US PATENT # 8,185,373 | EXPIRES JANUARY 17, 2031

BIG DATA

This patented method establishes a standard for translation metrics, offering analysis and feedback for grading and improving translation activities. When translating from a source language to a target language, word-for-word substitutions are not always adequate due to nuance, cultural variation, and native meaning. This technology provides user-definable ratings of accuracy, interpretation of intended message, and formatting, enabling effective language translation and interpretation of the source material. By not focusing on specific word choice, the technology is also able to more accurately assess the quality and accuracy translations and interpretations, taking concerns such as sentiment and content into account.

POTENTIAL APPLICATIONS:

- Language training and evaluation
- Language curricula/materials development and assessment
- Linguistics
- Speech signal processing

TRANSLATION METRICS

IMPROVED TRANSLATION

FEEDBACK

Identifying Connected Data in a Relational Database

Method of Identifying Connected Data in Relational Database
US PATENT # 8,001,137 | EXPIRES FEBRUARY 2, 2030

BIG DATA

This technology leverages Structured Query Language (SQL) in relational databases to discover connected data. Because the data does not need to be transformed, the algorithm is able to operate in the database's natural information storage format. This also enables efficient discovery of connected data and easy identification of common labels. This approach is limited only by the processing capacity of the database and delivers results faster and more accurately than other methods.
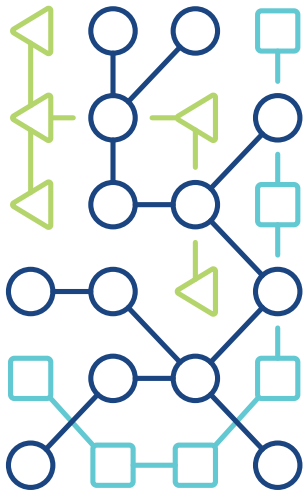
POTENTIAL APPLICATIONS:

- Genetics
- Epidemiology
- Social media
- Retail
- Telecommunications

Measuring Voice Signal Enhancement

Method of Measuring Degree of Enhancement to Voice Signal
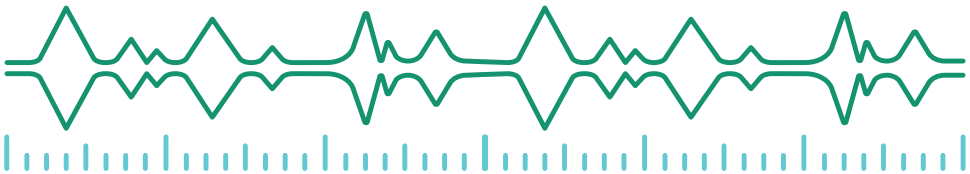**US PATENT # 7,818,168 | EXPIRES AUGUST 18, 2029**

**BIG DATA
MOBILITY**

This technology measures the degree of enhancement made to a voice signal, reducing the need for human arbitrations and other various listening tests. Statistically, voice signals are "non-stationary," changing over time. The more a signal becomes corrupted, however, the more stationary its distribution of values becomes. In this technology, the degree of reduction in the signal's distribution indicates the degree of enhancement made to the signal. This invention quantifies the voice enhancement by comparing how stationary the distribution of values are between original and enhanced signals.

POTENTIAL APPLICATIONS:

- Law enforcement
- Audio forensics
- Medical analysis

Automatic Topic Identification

Method of Identifying Topic of Text Using Nouns
US PATENT # 7,805,291 | EXPIRES NOVEMBER 17, 2028

BIG DATA

This technology enables automatic identification of topics in machine-readable text in any language and from any source, including voice transcripts and material scanned for optical character recognition (OCR). This method of topic identification in a machine-readable text overcomes the limitations of earlier approaches based on keyword searches, which tend to degrade in performance when dealing with variations in keyword spelling without any significant change in meaning.

POTENTIAL APPLICATIONS:

- Search engine enhancement
- Search tools for mobile devices
- Document storage and retrieval
- Automated tools for information management and maintenance

TOPIC

ALADDIN: Database Searching and Identifying Text

Method of Database Searching
US PATENT # 7,797,152 | EXPIRES FEBRUARY 10, 2028
Natural Language Database Searching Using Morphological Query Term Expansion
US PATENT # 7,761,286 | EXPIRES MARCH 7, 2029
Method of Identifying and Highlighting Text
US PATENT # 7,539,611 | EXPIRES MARCH 1, 2027

BIG DATA

This technology is a combination of three inventions: two natural language database search methods and a method of identifying and highlighting text. The Tagger searches for transliterated terms (such as names) within large data sets using lexical, contextual, and morphological information. The Matcher is then applied to determine which candidate terms are known within the database and are therefore of likely increased interest to the reader. This knowledge-based system's ability to work without relying on any one query language grants non-expert users access to an extensive collection of linguistic information and expertise. A typical application for this technology is name searching since names have unique linguistic and cultural complications and extracting names from data sources can be difficult.

POTENTIAL APPLICATIONS:

- Genealogy
- Financial/banking industry
- Medical record retrieval
- Fraud detection systems
- Background checks

LARGE DATA SETS   TRANSLITERATED TERMS   TERMS KNOWN WITHIN DATABASE

Realistic Testing and Comparison of Voice Signals

Method of Comparing Voice Signals That Reduces False Alarms
US PATENT # 7,650,281 | EXPIRES OCTOBER 1, 2028

**BIG DATA
MOBILITY**

This technology tests the robustness of a given voice-matching algorithm by providing the algorithm with variants of a digital file. The testing done against the original voice sample could include time-reversal, segmented re-arrangement, or a mixture of both time-reversal and segmented re-arrangement. This approach produces a larger corpus from fewer files, allowing for realistic testing under controlled conditions. It also reduces the Equal Error Rate (EER) i.e., the rates of false acceptance and false rejection, increasing performance in voice comparison methods.

POTENTIAL APPLICATIONS:

- Voice matching systems
- Authentication systems
- Biometric systems

✓ **ORIGINAL**

✓ **TIME-REVERSAL**

✓ **SEGMENTED RE-ARRANGEMENT**

Identifying Digital Audio Signal Format

Method of Identifying Digital Audio Signal Format
US PATENT # 7,620,469 | EXPIRES JULY 30, 2028

BIG DATA

This technology identifies the format of a digital audio signal, including signals that are either self-defining or headerless. Some audio signal file formats include header information indicating the digital encoding scheme, while other file formats—referred to as headerless—do not indicate the encoding scheme. This technology automatically identifies file format, an improvement over other methods, and reduces or eliminates the need for human listening.

POTENTIAL APPLICATIONS:

- Audio forensics
- Archiving and cataloguing audio libraries
- Media systems

Automated Detection of Duplicate Audio and Voice Recordings

Method of Identifying Duplicate Voice Recording
US PATENT # 7,571,093 | EXPIRES APRIL 18, 2028

BIG DATA

This technology detects duplicate audio and voice recordings in a sample collection without relying on transcription or phonetic comparison for detection. This method is able to determine that two recordings of different lengths may be duplicates and two recordings of the same length may not be duplicates. This invention is independent of the recording's language and content.

POTENTIAL APPLICATIONS:

- Voicemail systems
- Digital libraries
- Caller ID systems
- Conference calling systems
- Auto-dialer detection systems

Modeling Single-Class Data from Multi-Class Data

Method of Modeling Single Data Class from Multi-Class Data
US PATENT # 7,454,337 | EXPIRES APRIL 16, 2026

BIG DATA

This extensible technology isolates data (text, image, and voice) representing a target class from heterogeneous data representing multiple data categories of the same type. The method may be applied to identify speech from a speaker of interest in an audio stream containing speech from several other speakers, and extends naturally to language and gender identification and more generally to image and text applications. By automatically selecting data representing a particular class from multi-class data, nonessential artifacts may be removed from models trained on multi-class data, thereby enhancing detection and identification capabilities. The complexity of statistical models is also reduced, eliminating the need for costly memory swapping.

POTENTIAL APPLICATIONS:

- Speech applications such as speaker recognition, gender identification, or language recognition
- Improved classification accuracy in pattern recognition scenarios
- Biometric data discrimination

Recognizing Sounds of Speech of Any Language

Method of Combining Corpora to Achieve Consistency in Phonetic Labeling
US PATENT # 7,430,503 | EXPIRES OCTOBER 27, 2026

Method of Recognizing Phones in Speech of Any Language
US PATENT # 7,406,408 | EXPIRES DECEMBER 6, 2026

BIG DATA

This technology processes spoken sounds, independent of the language used, and translates them into text. Using a unique, universal alphabet comprised of phonetic sounds from approximately 15 languages, this technology enables the ability to train speech recognition systems to recognize sounds from different languages.

Speech processing applications rely on their corpora for translation—that is, their internal database of text that aids in translation. Multi-lingual speech processing applications typically require corpora from each language to be merged into one large corpora. This is problematic, as the applications can sometimes produce inaccurate or unintelligible results. This technology's built-in corpora, or database of writings, allows speech processing applications to identify sounds from multiple languages without the need for manual checking or outside databases.

POTENTIAL APPLICATIONS:

• Language training and evaluation of artificial intelligence

• Foreign language and English as a Second Language (ESL) courseware development

• Medical and legal transcription and translation

• Media and broadcasting

• Government, military, and law enforcement applications
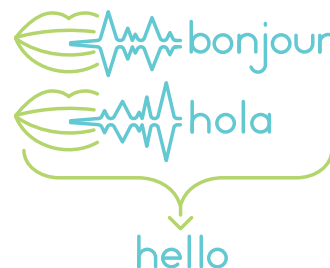
Morphological Text Processing

Method of Text Processing
US PATENT # 7,409,334 | EXPIRES MAY 12, 2026

BIG DATA

This technology draws on lexical morphology (a branch of linguistics) to improve processing of machine-readable text. This method of morphological text processing provides all inflected forms, or any subset thereof, of an input word or group of words of a highly tone-varying language. By cross-referencing the textual unit with a rules database and a lexicon database, the system derives the word's dictionary form to obtain all inflected endings (suffixes) for that word. The output is a subset of the inflected forms and information associated with the dictionary form and suffixes.

POTENTIAL APPLICATIONS:

• Language identification and analysis systems

• Automated systems for language translation

• Word searches in large databases

TEXTUAL UNIT

LEXICON DATABASE　　**RULES DATABASE**

DICTIONARY FORM

ALL SUFFIXES
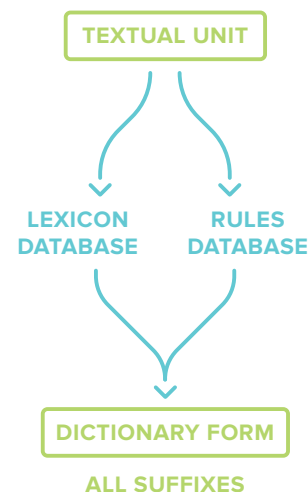
Automatic Voice Activity Detection in a Signal

Device for and Method of Detecting Voice Activity
US PATENT # 7,127,392 | EXPIRES JULY 9, 2025

Voice Activity Detector
US PATENT # 6,556,967 | EXPIRES MARCH 12, 2019

BIG DATA

This technology eliminates the need to manually search audio files for speech content by automatically locating speech intervals that contain other signals such as music, noise, or empty space. It reports the start and stop times of these intervals relative to the beginning of the file, ignoring non-speech portions of the file. By classifying signal segments as speech or non-speech, this technology improves the performance of speaker recognition systems by reducing the amount of bandwidth and traffic to be analyzed.

POTENTIAL APPLICATIONS:

• Automated transcription services

• VoIP and mobile telephony

• Audio conferencing

• Speaker recognition processing

• Noise suppression systems

• Frequency scanning equipment

Automated Separation of Handwritten and Machine-Printed Images

Method of Distinguishing Handwritten and Machine-Printed Images
US PATENT # 7,072,514 | EXPIRES MARCH 11, 2023

BIG DATA

This language-agnostic technology automatically characterizes documents as handwritten, machine-printed, or unknown, enabling quick scoring and storing of images. The technology can be useful in maximizing the accuracy of optical character recognition (OCR) applications, resulting in the capability to more accurately search and sort large document collections.

POTENTIAL APPLICATIONS:

• Document image collection

• Document indexing

• Records management

Solving a Problem in Pattern Recognition

Method of Geometric Linear Discriminant Analysis Pattern Recognition
US PATENT # 7,010,167 | EXPIRES SEPTEMBER 21, 2024

BIG DATA

This technology works against a core problem known as feature selection, which is seen in almost every pattern recognition problem. The Geometric Linear Discriminant Analysis Pattern Recognition System diminishes the complexity of pattern recognition systems by reducing the dimension of the observation space. System performance is driven by accurate modeling. The ability to build good models is driven by the number of model parameters and the amount of data available to obtain reasonable estimates of those model parameters. This technology's design enables better modeling and better performing pattern recognition systems. This technology can also provide a method for ranking and selecting features that are important to the classification of objects and recognition of patterns.

POTENTIAL APPLICATIONS:

- Speech recognition
- Machine readable optical labels
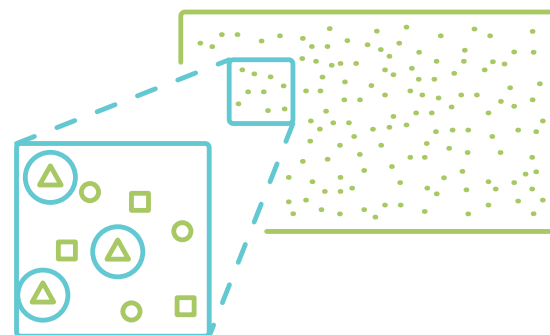
Summarizing Text by Sentence Extraction

Method of Summarizing Text by Sentence Extraction
US PATENT # 6,990,634 | EXPIRES FEBRUARY 26, 2023

BIG DATA

This technology uses a simplified, internal algorithm to extract only those sentences from text that convey the essential meaning, providing a concise summary of the full text. The number of sentences is limited to provide a summary of the text with only enough information for a user to determine whether or not to read the text in its entirety. This technology produces a concise summary independent of any additional input or evaluation upon which other mechanisms rely such as seed lists, common expression information, analysis of number and patterns of stop words, or identification of component words.

POTENTIAL APPLICATIONS:

- Condensed text for mobile applications
- Search engine query results
- Database entry summarization
- Abstract development

KODA: Text Summarization

Method of Summarizing Text Using Just the Text
US PATENT # 6,904,564 | EXPIRES DECEMBER 7, 2023

BIG DATA

KODA is able to quickly process large amounts of textual data sets, extract key phrases or sentences, and reduce each document to a few representative passages. The depth of detail is user-definable. The results provide users the ability to make rapid, accurate decisions about whether the document is relevant to their needs. This technology can be applied to any search-like application that returns a large number of potential document matches.

POTENTIAL APPLICATIONS:

- Accurate summaries of search results listed
- Efficient, accurate summaries of document lists such as transcripts or articles

Cyber

Cyber relates to information technology, computer hardware, computer software, computer networks, or the internet. Oftentimes, cyber describes the digital version of something that has a non-digital counterpart. For example, cyberspace is the non-physical terrain created by computer systems.

Navigating the safest and fastest path through cyberspace involves many moving pieces. The ever-evolving cyber field presents opportunities for dynamic solutions for information processing, networking, and physical, hardware, and access security. Through novel research and design, NSA is able to offer innovations that enable improved authentication, protect an array of data ports, and provide other cyber security measures.

Data Port Protection

Port Connector Securement Device
US PATENT # 9,559,462 | EXPIRES JUNE 1, 2035

USB Port Protector
US PATENT # 8,449,309 | EXPIRES FEBRUARY 16, 2032

Single-Use USB Port Protector
US PATENT # 8,414,314 | EXPIRES DECEMBER 14, 2031

*Port Protector Assembly for D-Sub Connectors*
US PATENT # D662,894 | EXPIRES FEBRUARY 24, 2024

This technology suite consists of patented devices (reusable and single-use) that provide methods for blocking access to data ports, as well as tamper evidence when bypassed. Increasingly, computer data ports are becoming a preferred method to covertly extract data or introduce malicious software into a computer system. As a result, the need to secure data ports from unauthorized access is becoming a priority for security personnel and system administrators. These port protectors are an inexpensive solution to address a significant security vulnerability and can be easily installed to provide an additional layer of security over software-based systems.

With port protectors in place, users can deny, deter, and detect unauthorized access to On-Board Diagnostic (OBD) ports in vehicles, HDMI ports, Universal Serial Bus (USB) ports, and D-sub (DB9, DB15, DB25, DB26, and DVI) ports, as well as the removal of USB cables, improving cyber defense and maintaining system integrity.

POTENTIAL APPLICATIONS:
- Data center security
- Mobile device tamper evidence when traveling
- Workstation, router, or network hub tamper evidence and deterrence
- Tamper evidence and deterrence on vehicle ports while vehicle is out of sight
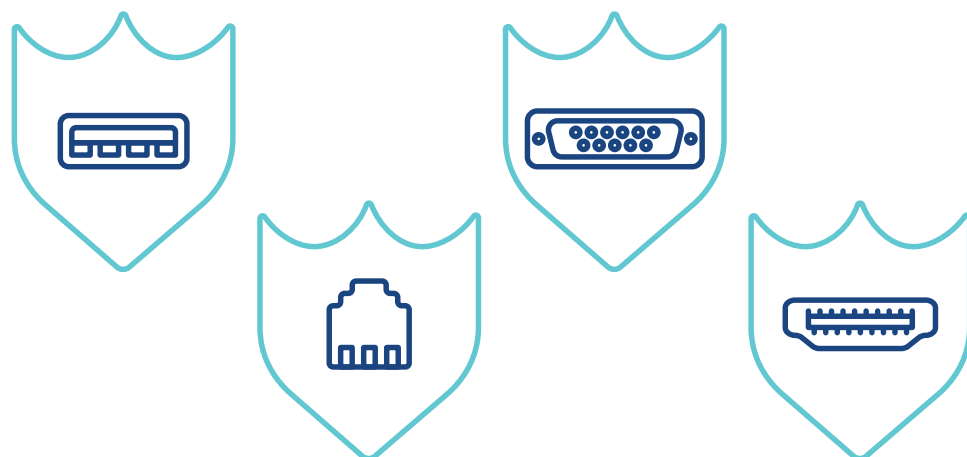
Digital Camera Fingerprinting

Building a Digital Camera Fingerprint from Cropped or Corrupted Images
US PATENT # 9,525,866 | EXPIRES APRIL 18, 2036

Given a collection of digital images, this technology performs digital camera fingerprinting without needing access to the source camera. Every camera sensor is unique and leaves a noise pattern in images that can be extracted and analyzed. By calculating the noise residual of a digital image, this technology generates a fingerprint for the camera, and then determines whether an image is associated to that fingerprint or not. This method can perform fingerprinting from cropped or corrupted images—a unique feature compared to similar fingerprinting methods. Using a smarter sequence of computations, it also provides better identification than existing methods and reduces the number of calculations needed to complete the task.

POTENTIAL APPLICATIONS:
- Digital forensics
- Image analysis
- Identity verification
- Law enforcement
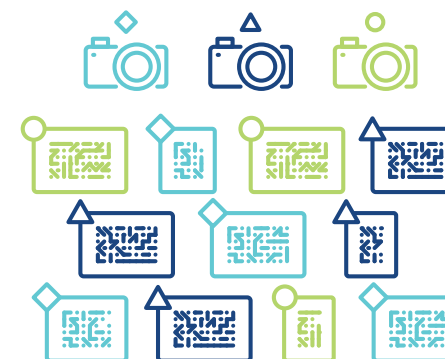
Computer Intrusion Anticipation, Detection, and Remediation

Device for and Method of Computer Intrusion Anticipation, Detection, and Remediation
**US PATENT # 8,898,784 | EXPIRES MAY 29, 2033**

This invention enhances electronic network security in the same way that radar improved weather forecasting improves safety, by providing advanced information to experts who can then determine what, if any, protective action must be taken.

This technology anticipates network intrusion attempts, detects actual attempts, and detects both existing and new malware. Improving on existing technology, the system remedies intrusions by changing network topology, or the way in which constituent parts are interrelated or arranged, countering computer traffic associated with the various phases of intrusion and countering the source of the adversarial computer traffic.

POTENTIAL APPLICATIONS:
- Intrusion prevention systems (IPS)
- Identity theft protection
- Malware defense
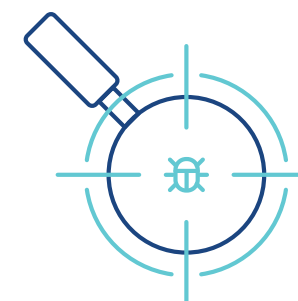
Rapid Biometric Authentication

Method of Controlling a Transaction
US PATENT # 8,886,952 | EXPIRES SEPTEMBER 9, 2033

This technology provides additional security to a computer transaction by projecting a summary of transaction details onto a user's face, then capturing the user's spoken or gestured acceptance. The distortions created by projection onto the user's face combined with facial recognition make it harder to forge a fraudulent transaction record for unauthorized use. With the number of electronic transactions growing every day, traditional security methods such as passwords or PIN-based controls may become more prone to hacking attacks and other vulnerabilities. This capability can enhance the security of transactional activity in practically any field, including banking, e-commerce, and access control.

POTENTIAL APPLICATIONS:

- E-commerce
- Identity authentication
- Financial/banking transactions
- Access control
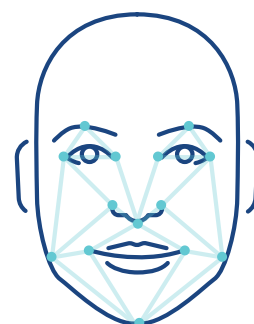
CYBER

State-Change Detector

Device for and Method of Determining Changes to GUI
US PATENT # 8,826,158 | EXPIRES FEBRUARY 1, 2033

This invention provides a way of determining "state changes" to a graphical user interface (GUI)—or, identifying what has changed on a user's screen—without having a user profile for each program. This method is more structured than previous technology as it does not require the use of a configuration file or data from an application's previous operation. Unlike existing systems that provide "snapshot coverage," this invention provides a comprehensive coverage of changes, or real-time monitoring. The technology could be used to enhance security access to computers, computer networks, or other transactional activities.

POTENTIAL APPLICATIONS:

- Enhanced computer security applications
- Change control tracking, version state history application or widget
- Braille processing, screen readers, or other assistive technology
- Parental-control software applications

CYBER

ON   OFF
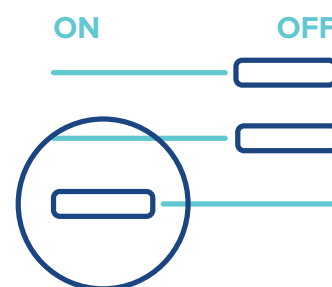
Image-Projection Plus Facial Recognition User Authentication

Method of Image-Based User Authentication
US PATENT # 8,655,027 | EXPIRES OCTOBER 4, 2032

This technology enables greater security for access control systems. It combines facial recognition technology with projection, rotation, and an image grid to the type of user authentication system that verifies identity by selecting a particular image, which is then matched to a previous choice. To log in, the user selects an image from the grid that determines the pre-selected image to be projected onto the face with rotation. If the facial features and pattern images match the user's profile, the user is authenticated. The combination of the user's facial geometry, the correct image manipulation, and the distortion of the image in the process of projection is evaluated to authenticate the user. The system is more user friendly than obtrusive "look here" technologies such as iris scans.

POTENTIAL APPLICATIONS:

- Physical access control
- Network user authentication
- Identity verification for any age group
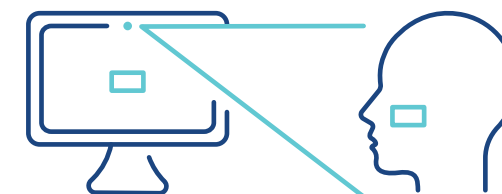
CYBER

Tracking Activity of Removable Electronic Components

Device for and Method of Detecting SIM Card Removal and Reinsertion
US PATENT # 8,478,340 | EXPIRES JANUARY 12, 2032

This technology detects the removal and reinsertion or enable and disable of a Subscriber Identity Module (SIM) card, memory card, flash drive, hard drive, computer peripheral, or any component attached to an electronic device. Using time recording capabilities, the system can correlate the action, such as removal of an electronic component, with other events associated with the device, activating alerts of unauthorized activity.

This invention takes detection to a new level by not just detecting an unauthorized device but detecting adversarial changes, activation, and interactions with legitimate devices.

POTENTIAL APPLICATIONS:

- Antitheft, anti-hacking, and antivirus monitoring
- Mobile Management System (MDM) security
- Alerts for diagnostic equipment attachment or detachment (e.g., aviation diagnostics)
- Cell phone usage tracking, including parental controls and alerts
- Home or office security systems

CYBER MOBILITY

PULSE: MESH Network Routing

Device for and Method of Network Routing
**US PATENT # 8,443,105 | EXPIRES JANUARY 31, 2032**

CYBER
IOT

This technology characterizes the physical layer capabilities of a network device in one simple measure to dynamically decide the best path based on the performance level of the next-hop neighbor. Traditional wireless ad hoc routing algorithms route traffic based on whether a path exists and disregard the physical layer limitations of wireless communication. With PULSE, however, routing decisions are distributed to individual nodes on a next-hop basis, eliminating the need to determine the full path through the network. This method increases throughput by directing traffic to less congested, more capable paths and drastically reduces the overhead in both routing messages and the required information tracked by each node to direct packets.

POTENTIAL APPLICATIONS:

- Distributed sensor networks used in upcoming IoT (e.g., electric meters passing usage data back to company)
- Range and throughput extension of wireless peer to peer networks (e.g., disaster relief operations)
- Military MESH networks
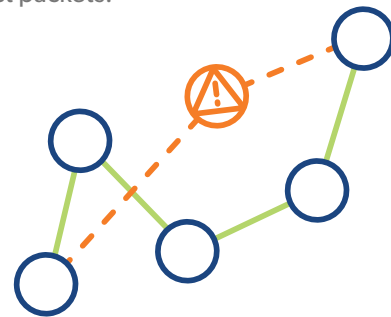
Measuring Software Integrity with LKIM

Method and System for Program Execution Integrity Measurement
US PATENT # 8,326,579 | EXPIRES MARCH 4, 2031

Methods and System for Program Execution Integrity Measurement
US PATENT # 7,904,278 | EXPIRES JANUARY 4, 2029

CYBER

This technology, the Linux Kernel Integrity Measurer (LKIM), verifies that running system software has not been modified and is authorized to run on the system. Unlike other system integrity technologies like antivirus programs, LKIM does not require a database of known malware signatures and is capable of detecting modifications resulting from previously unknown attacks. While LKIM was initially designed for Linux, there are variations that extend to other operating systems (including Microsoft Windows and the Xen Hypervisor). Proper use of this technology increases confidence that running systems, even those that might be known to be vulnerable to malicious attacks, have not actually been compromised, making the system more trustworthy for its intended purpose.

POTENTIAL APPLICATIONS:

- Measurement and attestation
- System monitoring
- Configuration control
- Protecting access to network resources
- Projecting trust across the network
- Computer forensics

Dynamic Network Traffic Rerouting

Device for and Method of Making Element Appear in Shortest Network Path by Minimal Decrements and Increments
US PATENT # 8,233,397 | EXPIRES FEBRUARY 28, 2031

CYBER

This technology calculates a new shortest path in a network, allowing administrators to take advantage of underused links more effectively and reduce the network congestion experienced by users. In telecommunication networks, it is often desirable to change link weights to produce path changes in a certain desired fashion. As new services are added, certain sections of the network may become congested due to changes in the capacity of individual links. This technology enables administrators to reroute traffic efficiently in case a high-capacity link suddenly becomes available.

POTENTIAL APPLICATIONS:

- Internet service providers
- Telecommunications carriers
- Vehicles (driverless cars)
- Geolocation / positioning system
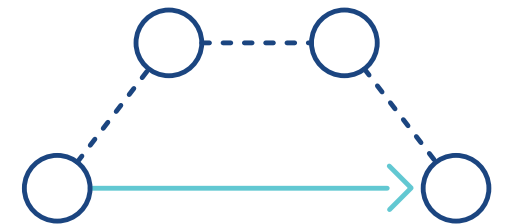
Select High-Level Privileges for Computer Users

Method of Providing a Computer User with High-Level Privileges
US PATENT # 7,945,947 | EXPIRES MARCH 15, 2030

CYBER

This technology eliminates a common workflow problem caused by users not having administrative access to their computers. Users are often locked out of certain configurations or set-up functions, which can delay critical work until a network administrator either grants the user access or does the work themselves. Even administrators are locked out of certain parts of the system. Some versions of the Windows operating system lack the built-in interactive utility to launch a command shell that has the high-privileges of LocalSystem. This utility establishes a realm for so-called "power users" within specific environments while still logged in with regular credentials.

POTENTIAL APPLICATIONS:

- Advanced vulnerability or system analysis
- Emergency or backup administrative access
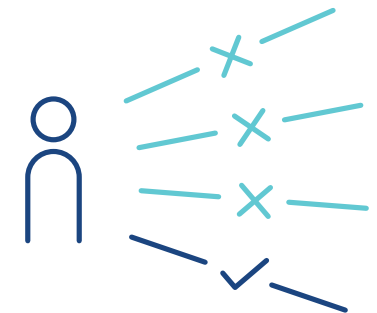
Objectively Assessing System Security

Method of Assessing Security of an Information Access System
US PATENT # 7,895,659 | EXPIRES OCTOBER 8, 2029

CYBER

Popular security assessments of information access systems typically rely on such subjective labels as low, medium, or high, ignoring specific protection tradeoffs between intrusion and Denial-of-Service (DoS) attacks. This technology objectively estimates the total vulnerabilities of an information access system that is protected by multiple verification mechanisms. The final estimation of system vulnerability is derived from the combination of the error tradeoffs for each specific verification.

POTENTIAL APPLICATIONS:

- Technology/cyber security auditing firms
- Security verification system providers
- Creation of a comprehensive verification product portfolio

TOTAL VULNERABILITY

FINAL ESTIMATION

Accelerated Batch Digital Signature Verification

Method of Identifying Invalid Digital Signatures Involving Batch Verification
US PATENT # 7,890,763 | EXPIRES DECEMBER 15, 2029

CYBER

This technology provides three methods of identifying invalid digital signatures in a group of signatures that have failed a batch verification test. The first two methods offer significant increase in speeds for processing batches of pairing-based digital signatures. The third method improves the efficiency of previous "divide-and-conquer" methods and has applications to both pairing-based and non-pairing-based digital signatures. High-speed bulk processing of digital signatures commonly starts with group processing until a failure occurs, at which point the process slows until bad signatures are segregated from the remainder of the batch. These new methods speed up the step of segregating the bad signatures that caused the batch to fail, allowing faster processing of large batches.

POTENTIAL APPLICATIONS:

- Digitally signed banking transactions
- Electronic voting system verification
- Wireless network routing authentication
- Ad hoc and peer-to-peer network authentication
- Sensor/radio frequency identification (RFID) access authentication
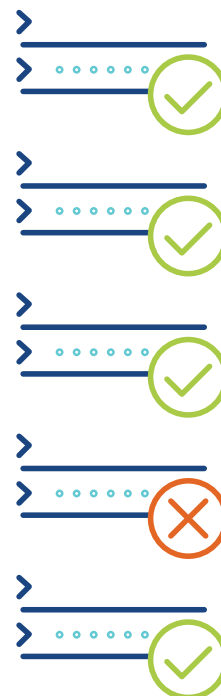
Reliably Communicating Via Computer Network

Method of Reliably Communicating Via Computer Network
US PATENT # 7,743,122 | EXPIRES OCTOBER 30, 2028

CYBER

This invention increases the reliability of network communications by adaptively constraining the routing of communications within a network. By identifying and communicating between the hub and leaf nodes and between hub nodes, the technology is able to re-designate leaf nodes as hub nodes and vice versa when needed, freeing up network resources and strengthening network communications. This technology significantly improves network communications on systems that commonly experience interruptions in data delivery due to the lack of availability or bandwidth.

RE-DESIGNATE NODES

INCREASE RELIABILITY
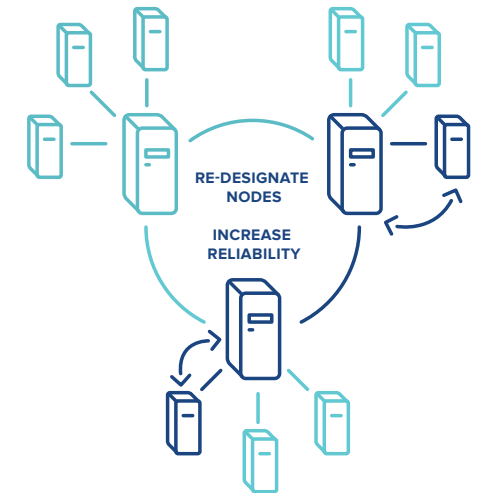
POTENTIAL APPLICATIONS:

- Multi-computer data transfer
- Network administration and communication

Establishing Suitable Master Nodes in Computer Networks

Method of Establishing and Updating Master Node in Computer Network
US PATENT # 7,738,504 | EXPIRES FEBRUARY 26, 2029

CYBER

In cluster type networks, a master node typically controls decision making and tasks non-master nodes. A master node may malfunction or a node may be added to a network that is more suited to be the master node than the designated master node.

This technology establishes and updates a master node in a computer network by scoring each node based on physical attributes, rather than subjective information entered into metadata fields. The scoring methods do not require a global administrator to monitor it, allowing administrators to focus on higher priority tasking.

POTENTIAL APPLICATIONS:

- Network management
- Telecommunications

Computer Stack Protection

Method of Protecting a Computer Stack
US PATENT # 7,581,089 | EXPIRES JANUARY 23, 2028

This technology protects against malware that attempts to gain control by corrupting return addresses kept on a computers stack. This is commonly known as return oriented programming (ROP). ROP is one of the most vicious techniques malware authors use and easily encompasses 50% of malware today. This invention's approach modifies the hardware of a computer's central processing unit (CPU) using a second stack to validate return addresses stored on the existing stack. The system's hardware-based approach works transparently with unmodified binary applications and does not degrade processing efficiency.

POTENTIAL APPLICATIONS:

- E-commerce security
- Protection of network-enabled objects

ROP ATTACKS ENCOMPASS 50% OF MALWARE TODAY

Cryptographic Key Exchange Using Efficient Elliptic Curve

Method of Generating Cryptographic Key Using Elliptic Curve and Expansion in Joint Sparse Form and Using Same
**US PATENT # 7,505,585 | EXPIRES MARCH 17, 2026**

Method of Elliptic Curve Digital Signature Using Expansion in Joint Sparse Form
US PATENT # 7,024,559 | EXPIRES OCTOBER 15, 2024

Cryptographic Key Exchange Method Using Efficient Elliptic Curve
US PATENT # 6,993,136 | EXPIRES DECEMBER 28, 2023

This technology is a combination of three patented methods for generating a cryptographic key between two users. The patents include the groundbreaking methods of identifying a digital signature using an efficient elliptic curve but also builds on previous technologies by adding a binary expansion in joint sparse form and a method of generating and verifying a cryptographic digital signature using coefficient splitting. Further innovation includes a method of generating a cryptographic key using coefficient splitting on two different classes of elliptic curves. This can be implemented in both a non-authenticated key exchange method and an authenticated key exchange method, minimizing the number of elliptic curve operations.

POTENTIAL APPLICATIONS:

- Safeguarding confidential information
- Secure digital banking transactions
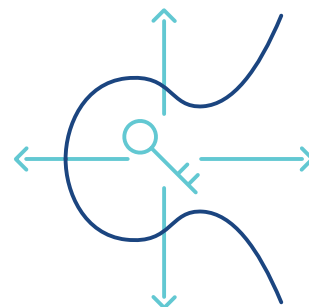
Dual Counter Mode

Method of Packet Encryption that Allows for Pipelining
US PATENT # 7,406,595 | EXPIRES OCTOBER 26, 2026

Dual Counter Mode is a codebook encryption mode that combines features of several previous modes to get the advantages of each while eliminating their flaws. The use of two keystreams enables the encryption mode to be pipelined in hardware, unlike other modes that only allow pipelining on decryption. Pipelining is a more efficient method of encryption that allows packets to be decrypted as soon as they are received, preventing packets from bottlenecking and slowing down network performance.

POTENTIAL APPLICATIONS:

- High-speed data transmissions
- Encrypted Asynchronous Transfer Mode (ATM) or other packet-based networks
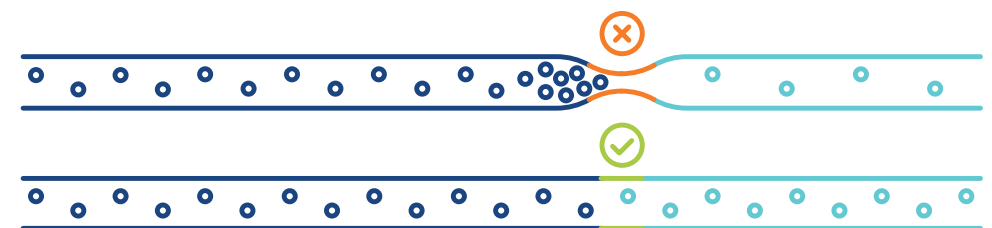
Random Number Generation

Device for and Method of Generating Pseudo-Random Sequence Uniformly Distributed over Any Range
US PATENT # 7,379,955 | EXPIRES APRIL 27, 2026

This technology enables pseudo-random number generation distributed uniformly over any arbitrary user-definable range, including a range that is not a power of 2 or a prime number. Analog components are complex and difficult to implement, and multiple clock cycles significantly decrease the performance of the generator. This technology provides increased performance over similar approaches by operating without analog components and producing a random number sequence with each new clock cycle.

POTENTIAL APPLICATIONS:

- Stochastic neural networks
- Gambling industry
- Interactive gaming
- Identification generation
- Authentication methods
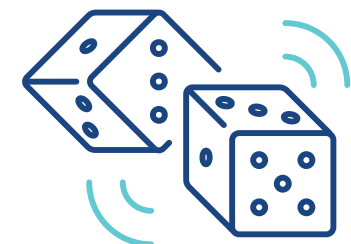
Proof of Unsatisfiability Solution

Method and System for Non-Linear State-Based Satisfiability
US PATENT # 7,380,224 | EXPIRES APRIL 14, 2026

Method and System for Non-Linear State-Based Satisfiability
US PATENT # 6,912,700 | EXPIRES MARCH 16, 2023

This invention solves a system of generalized non-linear Boolean equations and enables users to prove either that a solution exists ("Satisfiability") or does not exist ("Unsatisfiability"). This method does not require the translation of the system of equations into Conjunctive Normal Form (CNF) or to solve for all inputs such as Binary Decision Diagrams (BDDs).

POTENTIAL APPLICATIONS:

• Evaluation of software systems

• Design and testing of integrated circuits or other complex devices or systems

• Solving non-linear systems of Boolean equations

• Implementation of satisfiability algorithms in computer programs
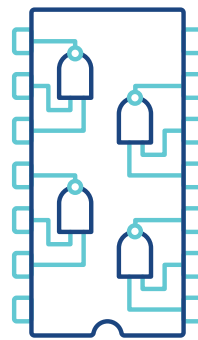
Secure, Efficient Firewall for Connectionless Network Packets

Firewall for Processing a Connectionless Network Packet
**US PATENT # 7,073,196 | EXPIRES APRIL 7, 2019**

Firewall Security Apparatus for High-Speed Circuit Switched Networks
US PATENT # 6,141,755 | EXPIRES APRIL 13, 2018

This invention provides a secure and efficient firewall for connectionless network data packets, such as Internet Protocol (IP) data packets, while enabling high-speed data transfer over a connection-oriented system such as an Asynchronous Transfer Mode (ATM) or Transmission Control Protocol (TCP) network.

Connectionless communications involve transmission of each packet based on routing information within the packet itself, rather than according to pre-established rules as in a connection-based network. The invention minimizes processing time by making an access determination only on the first occurrence of a new connectionless data flow. The results of this initial evaluation—to approve or reject access—are then applied to subsequently received packets associated with that flow. Comparison time is spent only on packets that have a flow tag never encountered before. The more effective processing improves firewall performance and reduces operating costs.

POTENTIAL APPLICATIONS:

• Network management

• Firewall security
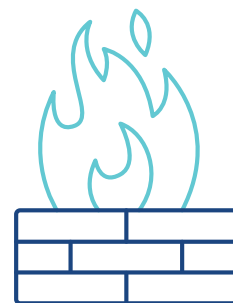
• Secure data transfer

Cryptographic Key Agreement

Method of Elliptic Curve Cryptographic Key Agreement Using Coefficient Splitting
US PATENT # 7,062,044 | EXPIRES JANUARY 21, 2025

This technology efficiently generates cryptographic keys between users that have not previously shared secret keys with each other using an elliptic curve. The design allows encrypted messages to be sent along unencrypted channels and decrypted by the intended recipient upon receipt. This technology does not require extra computing time as well as can be implemented in a non-authenticated key exchange method and in an authenticated key exchange method.

POTENTIAL APPLICATIONS:

• Online financial transactions

• Secure web browsing and messaging

• Identity verification

Cryptographic Identification and Digital Signature Using Elliptic Curve

Method of Elliptic Curve Digital Signature Using Coefficient Splitting
**US PATENT # 7,062,043 | EXPIRES JANUARY 21, 2025**

Method of Elliptic Curve Digital Signature Using Expansion in Joint Sparse Form
US PATENT # 7,024,559 | EXPIRES OCTOBER 15, 2024

Cryptographic Identification and Digital Signature Method Using Efficient Elliptic Curve
US PATENT # 6,898,284 | EXPIRES DECEMBER 12, 2023

This group of patented technologies highlight enhanced uses of Elliptic Curve Cryptography (ECC) for cryptographic identification, cryptographic key generation and exchange, and digital signatures. This approach is more efficient than existing approaches due to reduced amount of resource requirements for each operation as well as a reduced number of required operations.

POTENTIAL APPLICATIONS:

• Secure web browsing

• Identity verification
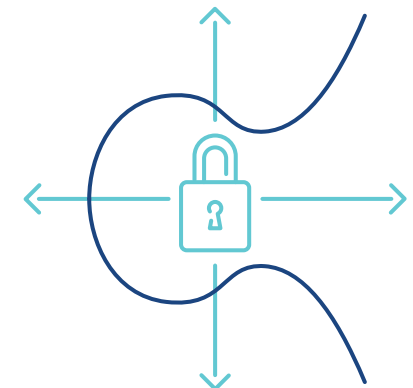
## Enhanced Forward Scattered Electron Imaging (FSEI)

Sample-Stand for Scanning Electron Microscope
US PATENT # 7,005,652 | EXPIRES SEPTEMBER 17, 2023

Sample-Stage for Scanning Electron Microscope
US PATENT # 6,777,678 | EXPIRES OCTOBER 4, 2024

This technology brings Transmission Electron Microscope (TEM) quality to the less expensive Scanning Electron Microscope (SEM) by providing information about the sample that is both surface sensitive and high resolution. This new technology enables improved high-resolution imaging on a general category of samples and eliminates the need for additional hardware at a tremendous cost savings.

POTENTIAL APPLICATIONS:

• Biomedical applications

• Nanotechnology devices

• Microelectronics
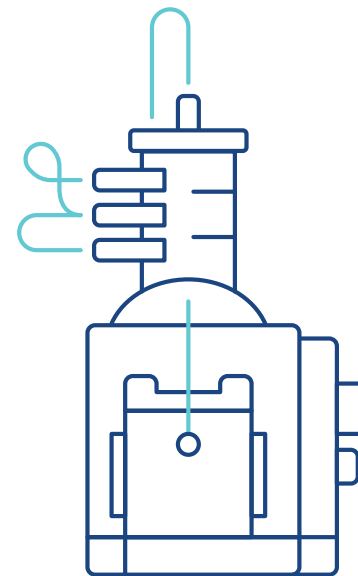
**HIGH RESOLUTION
LOW COST**

Efficient Acknowledgement of Data Packets

Method of Acknowledging Receipt of Data Packets
US PATENT # 6,957,374 | EXPIRES APRIL 22, 2023

This invention is an efficient method of reassembling, acknowledging, and transmitting data packets by accounting for the received packets in groups rather than individually. The groups may be comprised of received data packets or gaps in the received data packets. Both groupings provide a more efficient way of processing data packets.

POTENTIAL APPLICATIONS:

• Network management

• Wide area network (WAN) data transport

• Quality of Service (QoS) applications

INCREASED EFFICIENCY

NetTop®: Secure Computing Using Virtual Machines

Device for and Method of Secure Computing Using Virtual Machines
US PATENT # 6,922,774 | EXPIRES SEPTEMBER 28, 2023

NetTop® significantly reduces risks and recurring information technology (IT) investment by allowing a user secure simultaneous access to multiple networks or environments independent of the operating system or user applications on one machine. Public and private executives and IT managers are acutely aware of the risks in allowing their users access to proprietary, sensitive, or otherwise classified information, and access to the internet from the same device. With this technology, users can seamlessly "window" across multiple environments or networks accessing the same information and applications. Each network or environment and its data is securely isolated from the other without the need for multiple workstations at the end user's location.

POTENTIAL APPLICATIONS:

• Financial/banking industry

• Government use

• Network administration

Self-Authenticating Cryptography

Self-Authenticating Cryptographic Apparatus
US PATENT # 6,912,284 | EXPIRES JUNE 28, 2027

This encryption/decryption system incorporates a linear sequence generator and provides encryption and authentication in a single process. The system enables self-authentication capability without the need for a parity check code. The result is an improved autokey cipher using infinite error extension while also possessing a high degree of cryptographic security.

POTENTIAL APPLICATIONS:

• Telecommunications

• Secure communication

• Encryption and authentication

• Error detection

**ENCRYPTION
& DECRYPTION**

One-Way, Secure Hashing

Device for and Method of One-Way Cryptographic Hashing
US PATENT # 6,829,355 | EXPIRES JUNE 5, 2022

This technology is a one-way cryptographic hash algorithm, Secure Hash Algorithm-2 (SHA-2), that provides a level of security commensurate with the standards of National Institute of Standards and Technology's (NIST) Advanced Encryption Standard (AES). Hash algorithms are used frequently to transform digital messages into shorter, digestible messages for security applications such as digital signatures or message authentication. This patented technology enables security commensurate with NIST's AES standard while also conforming to NIST's elliptic curve-based digital signature algorithms.

POTENTIAL APPLICATIONS:

- Digital signatures
- Random number generation
- Computer-to-computer communication (e.g., secure http)
- Password protection
- Message authentication codes

MESSAGE

↓

ONE WAY HASH ALGORITHM

⬇

PASSWORD 🔒
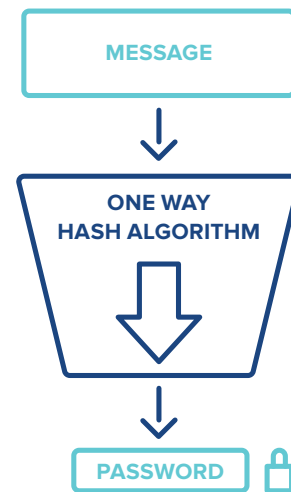
Randomizer Quality Test

Method of Testing a Randomizer
US PATENT # 6,798,883 | EXPIRES JANUARY 24, 2024

This technology tests the sufficiency of the output from a random number generator (or randomizer) by taking samples of the data from within the randomizer, going beyond traditional randomness tests that use the output from the randomizer. More than just a "pass/fail" tester, which can produce false positives, this technology shows designers how to improve or fix the design of the randomizer in order to present sufficiently random results.

POTENTIAL APPLICATIONS:

- Encryption testing, authentication, session keys, public keys
- Secure, private web browsing
- Network/access security
- Generating identification numbers
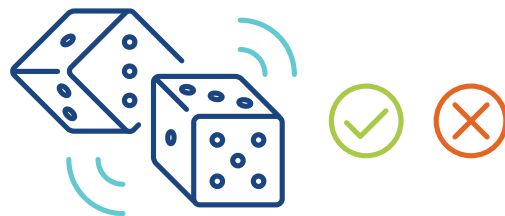
Efficient, Compatible Key Escrow (Enabling Third-Party Access to Cryptographic Keys)

Method of Passing a Cryptographic Key that Allows Third Party Access to the Key
US PATENT # 6,724,893 | EXPIRES JULY 16, 2021

This invention is a method of key escrow or passing a "secret" cryptographic key between users so an authorized third party (e.g., law enforcement) can access the key. This technology allows users to exchange keys in a secure, bandwidth-efficient manner.

With this method, a key recovery access field is embedded into the key pass method. The access field allows an authorized third party escrow agent to securely recover the key should that become necessary. Alternate methods add steps that would allow the second user to determine if the first user is complying with escrow aspects of the method. This method could be applied in any communication system (e.g., email, text messaging, voice) needing encryption to provide confidentiality between arbitrary members, to protect access to cryptographic keys during session establishment over non-secure channels, and to enable secure recovery of those keys at a later date should that be necessary.

POTENTIAL APPLICATIONS:

- Secure corporate communication
- Encrypted data recovery
- Corporate employee monitoring
- Parental controls

THIRD PARTY
AUTHORIZED ACCESS

Cryptography Using Modified Fractional Fourier Transform Kernel

Cryptographic Method Using Modified Fractional Fourier Transform Kernel
US PATENT # 6,718,038 | EXPIRES JUNE 24, 2023

This technology is a cryptographic method, using at least one component of a modified fractional Fourier transform (FrFT) kernel, that enables an encrypted message header to act as an electronic signature. This method encrypts digital signals by the sequential action of a modified FrFT kernel. The encryptor key is a set of positive numbers controlling the phase, angle, exponent, FrFT kernel, and wavelet family. Decryption is achieved by reversing the operations.

POTENTIAL APPLICATIONS:

- Data processing and analysis
- Secure digital communications

Hacker-Resistant Firewall

Firewall for Processing Connection-Oriented and Connectionless Datagrams Over a Connection-Oriented Network
**US PATENT # 6,615,358 | EXPIRES APRIL 7, 2019**

CYBER

This technology provides an efficient and hacker-resistant firewall for receiving Internet Protocol (IP) data packets, Asynchronous Transmission Mode (ATM) signaling, and ATM data.

Although a goal of a connectionless network such as an IP network is to ensure a data stream will reach its destination, there is a performance penalty (e.g., transmission time, latency, etc.) associated with the additional information added to each packet. To address these challenges, this technology enables efficient and secure processing using rules that can be based solely on one type of network (e.g., connection-oriented or connectionless) as well as on one type of network in relationship to other types of networks.

This method yields a more efficient, more secure firewall than networks that combine IP and connection-oriented ATM by transmitting IP packets over an ATM transmission channel (commonly referred to as IP over ATM).

POTENTIAL APPLICATIONS:

• Network management

• Firewall security

• Secure data transfer
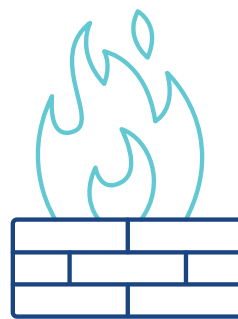
Multi-Dimensional Anomaly Detection and Deviation Identification

Method of Multi-Dimensionally Accentuating a Deviation in Information and Identifying its Cause
US PATENT # 6,470,297 | EXPIRES MARCH 7, 2021

CYBER

This technology can multi-dimensionally detect any anomalies in a transmitted message's information and identify the cause of the deviation. The technique provides an organized and manageable representation of communications activity to the user that is comprehensive and easy to understand. The message's information can be described with a variety of functions including entropy-based, temperature-based, or energy-based, either separately or in any combination of functions.

POTENTIAL APPLICATIONS:

• Network security

• External and internal intrusion detection

ENERGY BASED

ENTROPY BASED

TEMPERATURE BASED

## Filter System for Information Network Traffic

Filter System for Information Network Traffic
US PATENT # 6,385,205 | EXPIRES FEBRUARY 8, 2020

CYBER

This technology is an improved hardware-only filter system for controlling data packet traffic. Hardware-only and hardware and software combination devices are designed to optimize the performance of the network by evaluating packets and either determining a specific destination or providing a filter to only pass designated packets. This filter addresses the challenge of improving network performance by increasing the speed at which evaluating and directing the packets takes place.

POTENTIAL APPLICATIONS:

• Network administration

• Network security
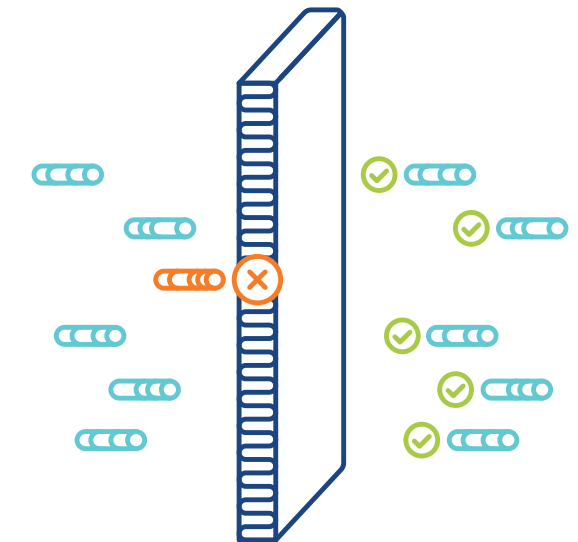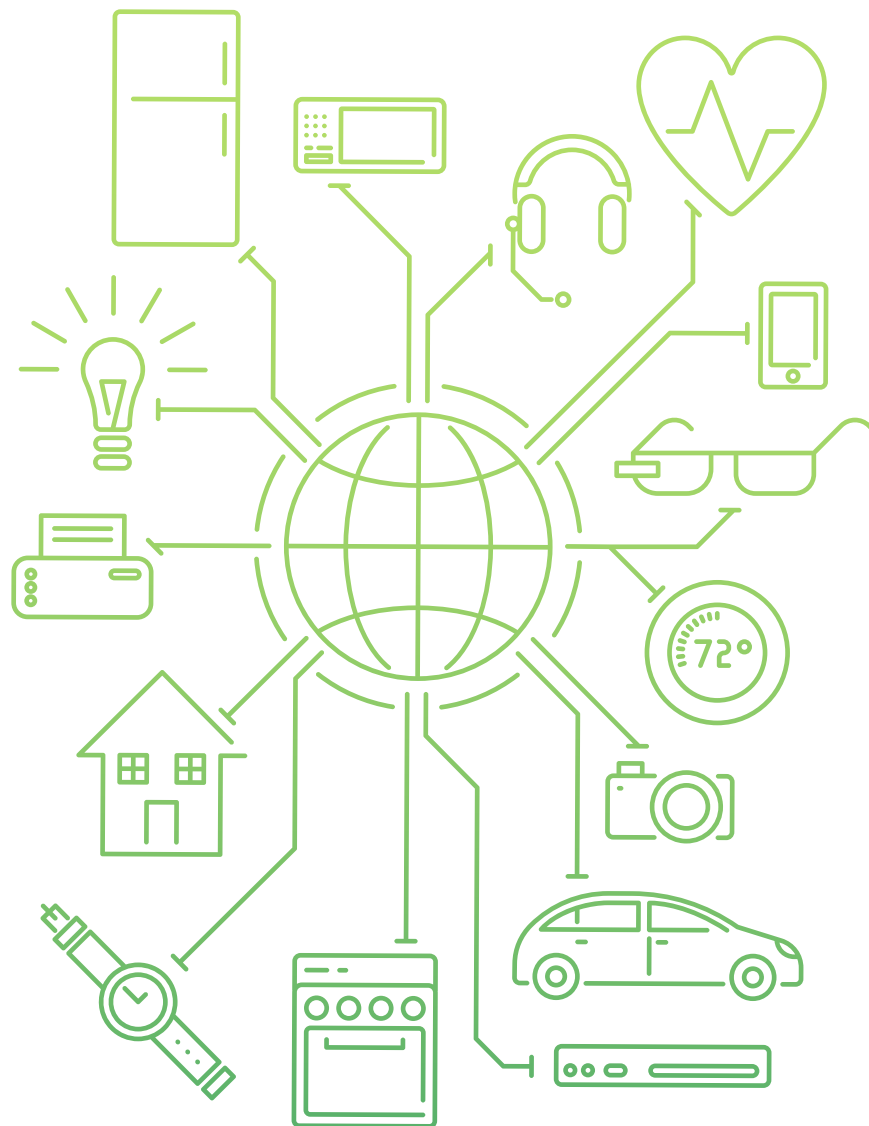
Internet of Things (IoT)

IoT describes networks of objects that transmit data. These objects may be connected to the internet, internal networks, or peer-to-peer paths. IoT uses data gathering sensors and cloud computing to make objects "smart." As the demand for internet-enabled devices continues to grow, NSA similarly continues to expand its development of IoT technologies. The innovations in this section provide time and cost-saving efficiencies, ensure accuracy of results, and improve/replace complicated or expensive solutions for technologies in the microelectronics and optic arenas.

PULSE: MESH Network Routing

Device for and Method of Network Routing
US PATENT # 8,443,105 | EXPIRES JANUARY 31, 2032

This technology characterizes the physical layer capabilities of a network device in one simple measure to dynamically decide the best path based on the performance level of the next-hop neighbor. Traditional wireless ad hoc routing algorithms route traffic based on whether a path exists and disregard the physical layer limitations of wireless communication. With PULSE, however, routing decisions are distributed to individual nodes on a next-hop basis, eliminating the need to determine the full path through the network. This method increases throughput by directing traffic to less congested, more capable paths and drastically reduces the overhead in both routing messages and the required information tracked by each node to direct packets.

IOT CYBER

POTENTIAL APPLICATIONS:

- Distributed sensor networks used in upcoming IoT (e.g., electric meters passing usage data back to company)
- Range and throughput extension of wireless peer to peer networks (e.g., disaster relief operations)
- Military MESH networks

Flexible Circuit

Method of Fabricating a Flexible Organic Integrated Circuit
US PATENT # 7,452,746 | EXPIRES JULY 1, 2027

Method of Thinning Semiconductor Other Publications Wafer of Smaller Diameter than Thinning Equipment Was Designed for
US PATENT # 6,017,822 | EXPIRES SEPTEMBER 16, 2018

IOT

This invention is a method of fabricating flexible organic integrated circuits (ICs) such as flexible substrates used for large area displays, identification tags, electronic paper, etc. This technology enables assembly of ICs requiring high temperature processes, which in turn enables higher system performance at lower power consumption rates.

POTENTIAL APPLICATIONS:

- Wearable and conformal electronics
- Flexible ICs with irregular shapes
- Large-area displays
- Identification tags
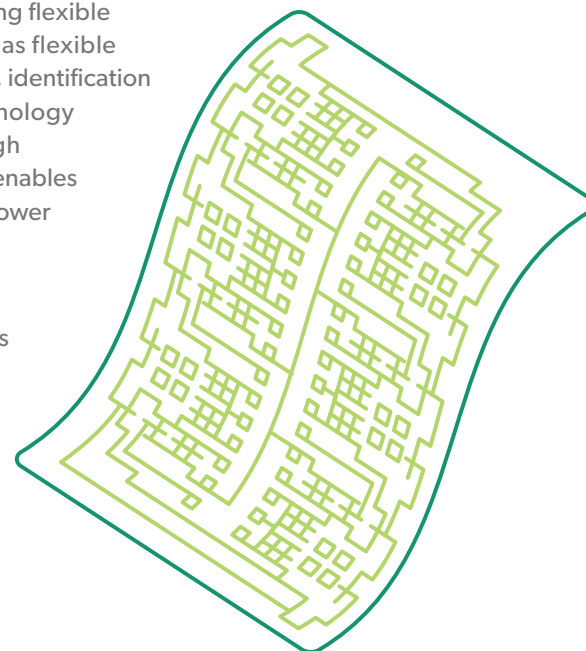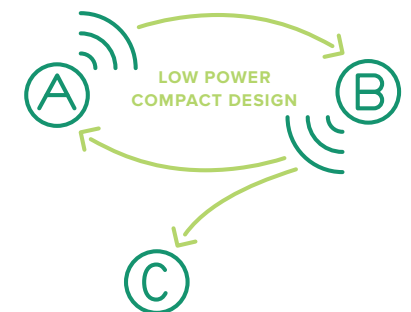
Wideband Retroreflector

Wideband Retroreflector
US PATENT # 7,383,026 | EXPIRES JANUARY 26, 2027

This wideband retroreflector provides signal retransmission with low power in a compact design. This invention can significantly improve communications and remote-sensing applications including air traffic control, ground-to-satellite communications, and high-rate data transfer from radio-frequency identification (RFID) sensors. The system can also improve communications within or between structures by enhancing signals in areas with weak wireless reception.

IOT MOBILITY

The invention consists of an antenna, a circulator, and a mixer, and eliminates the need for a local oscillator and local transmitter. This compact design makes the system easy to deploy and maintain in remote locations. There are minimal power requirements because the power comes from an illuminating transmitter and antenna. This technology also handles high bandwidths more effectively than current systems.

POTENTIAL APPLICATIONS:

- Remote or dangerous area data collection
- Vehicle-to-vehicle, or vehicle to stationary object communication and vice versa (e.g., updates to/from or between manual or self-driving vehicles)
- Unmanned aerial vehicle swarms
- Gamification

LOW POWER COMPACT DESIGN

Fabricating and Integrating Decoupling Capacitors

Method of Fabricating and Integrating High Quality Decoupling Capacitors
US PATENT # 7,297,613 | EXPIRES JULY 28, 2026

IOT

This technology is a method of fabrication and integration for high-quality decoupling capacitors with high capacitance values, low parasitic losses, and long-term reliability. This method produces very high yields, enables other passive elements to be placed very close to the processor (or other associated integrated circuit (IC)), and provides improved signal integrity between components on ICs.

POTENTIAL APPLICATIONS:

- High performance processor systems
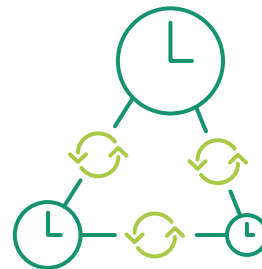- Mobile or miniature electronics

CICADA: Synchronizing Time without a Broadcast Signal

Method of Synchronization without Broadcasting Synchronization Signal
US PATENT # 7,227,858 | EXPIRES NOVEMBER 25, 2025

This technology synchronizes time using environmental triggers to ensure that nodes (e.g., computer or telecommunication) are working in sync. After the desired environmental conditions are set, the node remains in a sleeping state until those conditions are met. Synchronization can occur without using radio signals, Wi-Fi, or cellular networks, which reduces susceptibility to loss of service and detectability. Without the need for battery power, the technology is able to conserve energy between intervals of time, making it suitable for potential use in extreme environmental situations.

POTENTIAL APPLICATIONS:

- Sensors
  - Triggering recording equipment for studies or documentaries
  - Military and emergency operations
- Synchronizing resource constrained embedded systems

IOT MOBILITY

Clearer Imaging for Integrated Circuits

Method of Surface Preparation and Imaging for Integrated Circuits
US PATENT # 7,183,123 | EXPIRES JUNE 4, 2025

Method of Surface Preparation and Imaging for Integrated Circuits
US PATENT # 7,019,530 | EXPIRES DECEMBER 20, 2024

IOT

These semiconductor analysis techniques allow clear imaging of the components in an integrated circuit (IC) to be obtained from the top and backside perspectives without adding, altering, or removing elements to the IC.

These techniques enable clear imaging without staining or removing the upper layers of metal on the chip. This allows enhanced viewing of the interconnects, which reside at the lowest level of the chip, and analysis by multiple conventional imaging techniques.

IC analysis imaging techniques are used during failure analysis. Interconnects are a frequent source of failure in an integrated circuit; clear inspection greatly reduces the number of defective parts.

POTENTIAL APPLICATIONS:

- Reverse engineering integrated circuits
- Chemical laboratory analysis
- Failure analysis, quality control
- Counterfeit IC detection
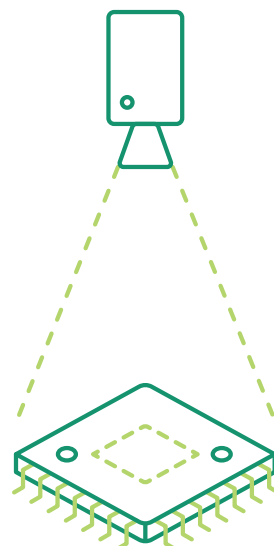
Low-Loss Fiber Chip Alignment

Photonic Integrated Circuit and Method of Fabricating Same
US PATENT # 7,128,476 | EXPIRES APRIL 13, 2025

IOT

This invention is a method of aligning optical fiber to a photonic integrated chip that results in lower back reflections.

Fiber optic technology is used in a variety of computer and communications applications due to its high data transmission rates compared to traditional copper wire. Since computers and communications devices still operate using electrical signals, optical signals received must be translated to electrical signals, and vice versa, for communication to take place over optical fibers. For effective signal conversion, optical fibers must be precisely aligned with appropriate devices for translation. This easily scalable and inexpensive method results in lower insertion losses, easier alignment, and a more rugged package.

POTENTIAL APPLICATIONS:

- Telecommunications
- Computer networking
- Medical tools, such as magnetic resonance imaging (MRI) machines

SCALABLE INEXPENSIVE
— **EASIER** —
ALIGNMENT

Optical Clock Recovery Device Using Non-Linear Optical Waveguides

Optical Clock Recovery Device Using Non-Linear Optical Waveguides
US PATENT # 6,701,049 | EXPIRES MAY 13, 2023

IOT

This technology provides an all-optical timing extraction device using the non-linear characteristics of optical waveguides for counter-propagating pulses. This invention can resolve timing delays between pulses on the order of a few picoseconds, keeping the signal intact.

POTENTIAL APPLICATIONS:

- Optical communications systems

Acousto-Optic Bandpass Filters

Tension-Tuned Acousto-Optic Bandpass Filter
US PATENT # 6,647,159 | EXPIRES MAY 27, 2022

Chirped Fiber Acousto-Optic Bandpass Filter
US PATENT # 6,580,841 | EXPIRES NOVEMBER 8, 2021

Acousto-Optic Bandpass Filter
US PATENT # 6,556,729 | EXPIRES AUGUST 11, 2021

This group of patented acousto-optic bandpass filters provide three varying methods of enabling one or more wavelength bands to be selected for further transmission. Signal switching is an important function in telecommunications. With the move to fiber optic cable transmissions, the demand for lower costs and higher switching speeds steadily increased, resulting in an increased need for optical switching. These technologies perform the function of bandpass filters at a lower cost, with lower power consumption, lower optical insertion loss, more versatility, and greater reliability than other bandpass filter technologies.

POTENTIAL APPLICATIONS:

- High performance fiber optic systems requiring switching, equalization, and tuning
- Telecommunications networks
- Integrated circuit component devices

HIGH SPEED
– & –
LOW COST

Timer Circuit Utilizing Thermal Effect

Timer Circuit Utilizing Thermal Effect
US PATENT # 6,498,770 | EXPIRES AUGUST 1, 2021

This technology is a timer circuit that utilizes the thermal runaway effect. The timer circuit includes a switch, resistor, transistor, and protective device. While the use of similar circuits may be necessary for situations requiring high precision, many of them contain additional components, such as clocks, which make the timer circuit more complicated, larger, and more susceptible to failure.

In this technology, the cycle of current flow is designed to activate a protective device, which acts as a time indicator and disconnects the power to protect the transistor from damage. The result is a process that is less complicated and more reliable than other existing methods. Its typical limits are from 0.1 seconds to 5 seconds of delay, set by the operating parameters.

POTENTIAL APPLICATIONS:

- Thermal trigger and timer for home automation
- Timer circuit for door locks for home, office, or vehicles
- Integrated circuit for a startup delay or watchdog timer

INCREASE IN
REACTION RATE

EXOTHERMIC
REACTION

HEAT

HEAT
ESCAPE
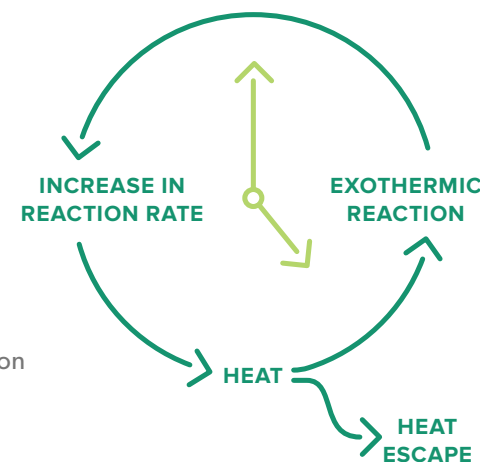
Recovering a Gate-Level Netlist from a Transistor-Level Netlist

Method of Recovering a Gate-Level Netlist from a Transistor-Level
US PATENT # 6,190,433 | EXPIRES NOVEMBER 10, 2018

This technology provides high-level abstraction to describe integrated circuits (IC), where layout information for the gates contained in the IC is not known. Various tools have been created to quickly analyze an IC based on a textual description of transistor connections (or a transistor-level netlist) and layout of the IC. In many instances, however, the layout of the IC is not available, resulting in missing or unknown gate-level netlist information. This technology enables recovery of different circuit implementations of a particular gate function using a single functional description of the gate function in question.

POTENTIAL APPLICATIONS:

- Integrated circuit design
- Integrated circuit analysis
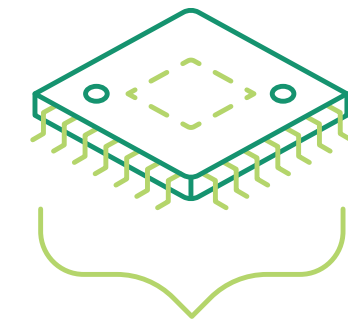
DESCRIPTION
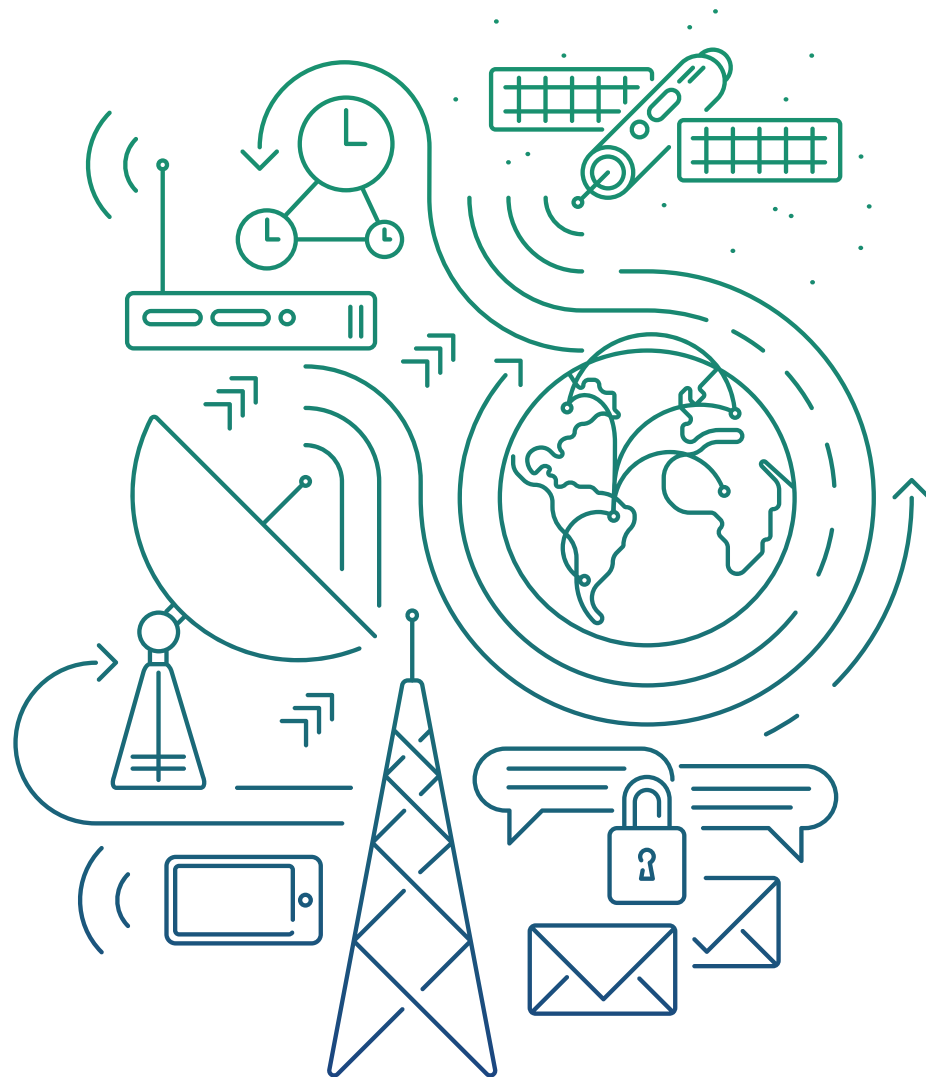
Mobility

Mobility can be generally defined as a technology or methodology that enables the free and efficient movement of data, things, people, or services. NSA has long applied its intelligence and expertise to the mobility field by finding new ways to ensure that information is transported both safely and securely. The technologies in this section have numerous applications in several fields including signals processing, physical security, and communications.

Improving a Maritime Communications System

AIS Demodulator for Unknown Carrier Phase and Baud Alignment
US PATENT # 8,665,997 | EXPIRES OCTOBER 28, 2032

MOBILITY

This technology improves functionality of the Automatic Identification System (AIS), a maritime communications system used for ship tracking, collision avoidance, search and rescue, and port security. Unlike existing technology, the system can demodulate communications signals even when transmission characteristics are largely unknown or interference is present. The demodulator can function on a signal that transmits data at a known baud rate but which has an unknown carrier frequency, an unknown carrier phase, and an unknown "preamble" (the pause in transmission just before a signal reaches a receiver), reducing the risk of at-sea collisions.

POTENTIAL APPLICATIONS:
- Ship or drone tracking and collision avoidance
- Water-based search and rescue
- Port security
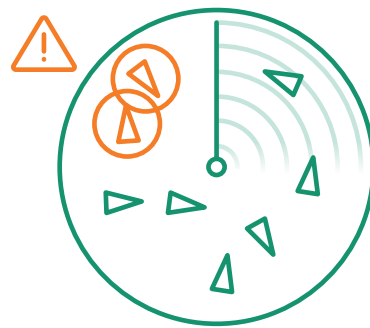
Tracking Activity of Removable Electronic Components

Device for and Method of Detecting SIM Card Removal and Reinsertion
US PATENT # 8,478,340 | EXPIRES JANUARY 12, 2032

MOBILITY
CYBER

This technology detects the removal and reinsertion or enable and disable of a Subscriber Identity Module (SIM) card, memory card, flash drive, hard drive, computer peripheral, or any component attached to an electronic device. Using time recording capabilities, the system can correlate the action, such as removal of an electronic component, with other events associated with the device, activating alerts of unauthorized activity.

This invention takes detection to a new level by not just detecting an unauthorized device but detecting adversarial changes, activation, and interactions with legitimate devices.

POTENTIAL APPLICATIONS:
- Antitheft, anti-hacking, and antivirus monitoring
- Mobile Management System (MDM) security
- Alerts for diagnostic equipment attachment or detachment (e.g., aviation diagnostics)
- Cell phone usage tracking, including parental controls and alerts
- Home or office security systems

Real-Time Simultaneous Identification of Multiple Voices

Biomimetic Voice Identifier
US PATENT # 8,442,825 | EXPIRES JANUARY 18, 2032

Infinite Impulse Response Resonator Digital Filter
US PATENT # 8,396,912 | EXPIRES NOVEMBER 15, 2031

MOBILITY
BIG DATA

The technology provides multiple speaker identification by identifying voices (or other sounds) in a manner that uniquely mimics the essence of the ear-to-brain interconnection through extensive human voice identification learning and recognition training. The object is real-time or faster voice identification needing only relatively simple computing resources. Specifically, this invention looks for prosody matches (spectral patterns over time periods) that were trained into a software Artificial Neural Network (ANN)—based model. Although intended to be used together, the Infinite Impulse Response (IIR) filter patent can be singularly applied to other uses as well.

REAL-TIME VOICE IDENTIFICATION

POTENTIAL APPLICATIONS:
- Voice recognition for home automation
- Sound detection for security systems
- Assistive technology
- Audio forensics
- Biomimetic voice systems

Coherent Demodulation of GMSK-AIS Signals

Coherent Demodulation of AIS-GMSK Signals in Co-Channel
US PATENT # 8,275,077 | EXPIRES MARCH 26, 2031

MOBILITY

Originally implemented for the US Navy, the Automatic Identification System (AIS) system transmits a burst Gaussian Minimum Shift Keyed (GMSK) signal designed to alert ships of other nearby ships. This technology is an improved method of demodulating GMSK AIS signals that does not require user-specific training codes and does not utilize an equalizer.

In this technology, the GMSK signal is basebanded, which enhances favorable signal qualities and decorrelates interfering signals. The error rate is also significantly reduced by using and applying poly-bit matched filters and a Viterbi decoding algorithm.

The technology also does not require preamble codes.

POTENTIAL APPLICATIONS:
- Demodulation of GMSK signals with co-channel interference
- Improved AIS signal processing

## Determining a Coherence Measurement for a Digital Signal

Device for Determining a Coherence Measurement for a Digital Signal That Does Not Require Spectral Estimation
US PATENT # 8,200,731 | EXPIRES APRIL 13, 2031

This technology estimates digital signal coherence in support of processing systems that generate frequency estimates as inputs to large-scale decision operations. Coherence is a measurement of spectral sharpness, by comparison to a pure sinusoid whose coherence is 100%.

Using methods alternative to involved frequency analysis, this method is able to exploit different signal features and does not require thresholds to obtain coherence figures-of-merit. This invention uses efficient algorithms resulting in real time output and the graphical output has easy-to-analyze results. The graphical user interface (GUI) is intuitive and can function on any tablet, laptop, or desktop platform using Windows® operating systems.

POTENTIAL APPLICATIONS:

- Signal processing
- Radar/sonar detection
- Materials fault discovery
- Medical scanning
- Structural integrity testing
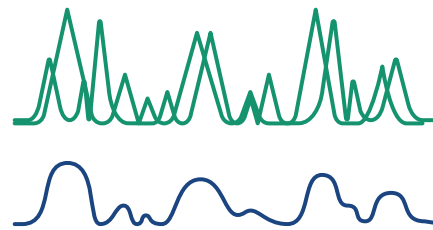
Reusable Tamper-Evident Bag Closure

Reusable Tamper Indicating Bag Closure
US PATENT # 8,196,442 | EXPIRES AUGUST 21, 2031

This bag closure has multiple tamper-indication features so that a user can easily verify if the package has been tampered with or compromised. Multiple bag closure options also allow the bag to be used in several different ways in order to meet specific transport needs. This tamper-evident bag closure is defined by a lid with multiple hasps and a base with knobs that attach to the bag.

This technology can be used to maintain a chain of custody to provide the user with the assurance that the content being protected has not been compromised.

POTENTIAL APPLICATIONS:

- Transporting sensitive documents from medical facilities, government offices, courts, and banks
- Transporting portable computing devices
- Maintaining integrity of legal evidence

Reusable Tamper-Indicating Tube

Reusable Tamper Indicating Transport Tube
US PATENT # 8,177,089 | EXPIRES AUGUST 17, 2030

This reusable tamper-indicating tube can be used to securely transport large drawings and other documentation without damaging or distorting them.

The tamper-evident tube comprises an outer tube with cap, an inner tube with cap, an inner tube locking mechanism, and an outer tube locking mechanism that is affixed to the peripheral surface of the outer cap. This device provides a high level of security and is tamper evident.

POTENTIAL APPLICATIONS:

- Transporting sensitive architectural and mechanical drawings
- Proprietary couriers
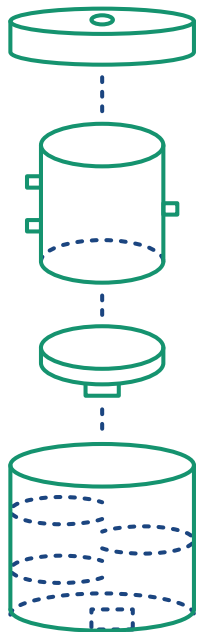
Transmitter Geolocation

Method of Locating a Transmitter
US PATENT # 8,068,850 | EXPIRES SEPTEMBER 29, 2030

This technology geolocates uncooperative transmitters at a centralized control station via TDOA (Time Difference of Arrival) without requiring complex equipment at each receiving station and therefore greatly reduces the cost of operations. Geolocation is performed by subtracting the communications link time delay from the time of arrival for each received signal. Alternately, it can be performed by calculating the communications link TDOA for each pair of receiving stations and subtracting the result from the TDOA calculated from the received signal.

POTENTIAL APPLICATIONS:

- Mobile geolocation services
- Military and law enforcement
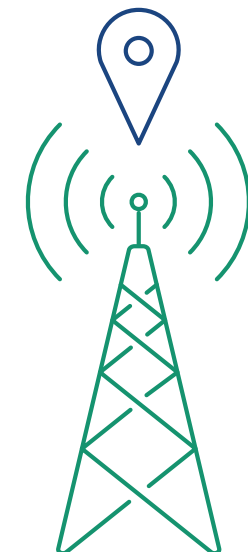
MOBILITY

## Reusable Tamper-Evident Cargo Seal

Tamper Evident Cargo Seal
US PATENT # 8,052,180 | EXPIRES NOVEMBER 20, 2030

MOBILITY

This technology is designed to protect cargo shipments from tampering, theft, counterfeiting, and introduction of hazardous or other unwanted material. A hasp closure secures access to containers like bulk cargo containers or storage building doors, and a reusable, serialized tamper-indicating seal provides easy visual tamper indication.

POTENTIAL APPLICATIONS:

• Industrial security

• International shipments

• Awareness of unauthorized entry to a secured area such as a room, cargo area, or luggage compartment
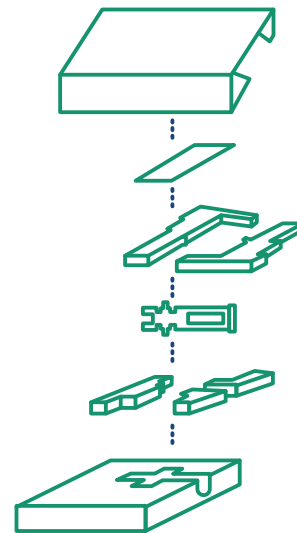
Wideband Signal Geolocation

Device for and Method of Geolocation
US PATENT # 7,893,875 | EXPIRES SEPTEMBER 12, 2029

MOBILITY

This patented device processes large-length, wideband signals, even at very low signal-to-noise ratio (SNR), to geolocate an electromagnetic transmitter. The method also extends methods for real-valued signals to handle complex-valued signals, which simplifies geolocation modeling of electromagnetic signals (e.g., when base-banding is required).

Two receivers, whose locations and velocities are known, receive a real-valued transmitted signal. The signals are digitized, converted to complex-valued, and the method computes the difference in radial velocities of the receivers relative to the transmitter. The difference in radial velocities and the difference in arrival times of the signal at the receivers are used to geolocate the transmitter with precision exceeding standard cross ambiguity function (CAF)—based methods.

POTENTIAL APPLICATIONS:

• Electromagnetic transmitter geolocation

• Search and recovery applications

• Geolocation of mobile phones

• Wildlife tracking
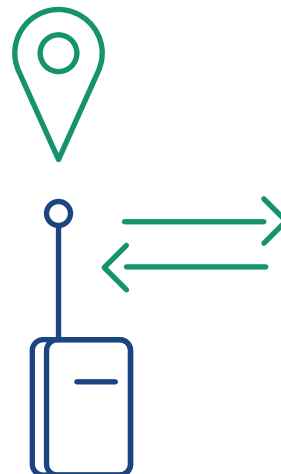
Measuring Voice Signal Enhancement

Method of Measuring Degree of Enhancement to Voice Signal
US PATENT # 7,818,168 | EXPIRES AUGUST 18, 2029

MOBILITY
BIG DATA

This technology measures the degree of enhancement made to a voice signal, reducing the need for human arbitrations and other various listening tests. Statistically, voice signals are "non-stationary," changing over time. The more a signal becomes corrupted, however, the more stationary its distribution of values becomes. In this technology, the degree of reduction in the signal's distribution indicates the degree of enhancement made to the signal. This invention quantifies the voice enhancement by comparing how stationary the distribution of values are between original and enhanced signals.

POTENTIAL APPLICATIONS:

• Law enforcement

• Audio forensics

• Medical analysis

Determining Range and Velocity of an Object

Method of Signal Processing for Determining Range and Velocity of an Object
US PATENT # 7,755,536 | EXPIRES MAY 14, 2029

Method of Signal Processing
US PATENT # 7,545,325 | EXPIRES JULY 28, 2027

MOBILITY

This technology combines two patented methods to finding range and velocity of a transmitter in a radar system using a time scale factor. The first technology (7,545,325) determines the position and velocity of a transmitter over a wide range of bandwidths, wherein the position and velocity are determined using a scalar relationship dependent on the radial velocity of the transmitter with respect to the receiver. The second technology (7,755,536) models the Doppler process as a time shift and change of scale of the original signal. Unlike other methods, this combined process resamples the signal at a rational multiple of the original sample rate, enabling efficient implementation of the scale correlation function.

POTENTIAL APPLICATIONS:

• Geolocation

• Radar processing application

• Fixed transceiver tracking applications
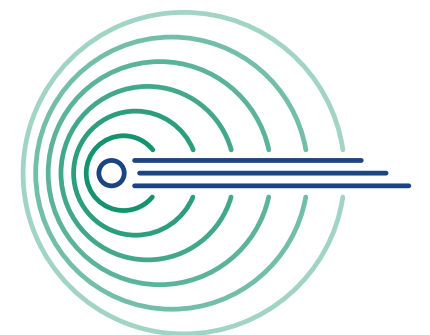
Rapid Encoding and Decoding of Signals with Binary BCH Codes

Method of Encoding Signals with Binary Codes
US PATENT # 7,734,991 | EXPIRES APRIL 9, 2029

Method of Decoding Signals Having Binary BCH Codes
US PATENT # 7,694,207 | EXPIRES FEBRUARY 4, 2029

These inventions embody methods of rapidly encoding and decoding block codes in communications signals for the purpose of error detection and correction. By taking advantage of the fast binary syndrome calculations to identify error-free blocks at initiation, the decoding technology reduces the overall time in software error correction of long binary Bose Chaudhuri Hocquenghem (BCH) codes by as much as 40% over other known methods. The encoding technology uses the decoding method's first step results to derive check values. The method applies to any binary cyclic codes, including cyclic redundancy checks (CRCs), and requires no branch processing as it is data independent.

POTENTIAL APPLICATIONS:

- Applications conforming to interoperability standards (such as FNBDT/SCIP)
- Networks using multiple communication protocols such as ISDN, PTSN, and IP

REDUCES
— ERROR —
CORRECTION TIME
BY
40%

Estimating Digital Signal Frequency

Method of Estimating Digital Signal Frequency
US PATENT # 7,715,996 | EXPIRES JUNE 25, 2028

This technology uses a simple differentiation operation to estimate frequency compared to other processes. This technique is free of localization constraints and can resolve time and frequency equally well. This technology improves upon existing technology by having all operations performed in the time domain and without any filtering.

POTENTIAL APPLICATIONS:

- Digital spectral estimations
- Radar, sonar, and telephony signal processing
- Complex modulation structures

120 Ghz
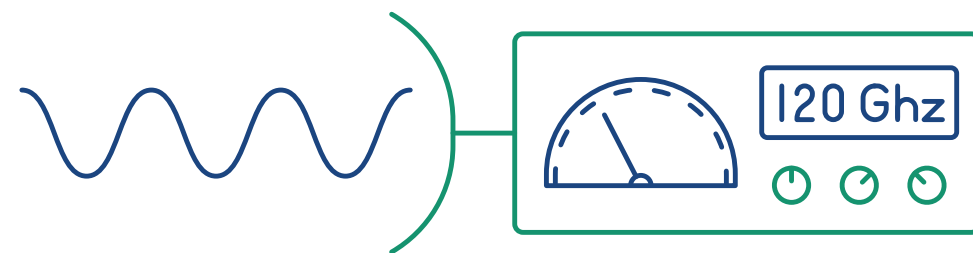
Code Generation that Minimizes Error Propagation

Method of Code Generation that Minimizes Error Propagation
US PATENT # 7,676,725 | EXPIRES JANUARY 9, 2029

When transmitting binary data, encoding schemes make the resulting waveform more immune to noise and interference. One class of transmission codes, block or line codes, are used to modulate binary symbols 0 and 1. There is a need to minimize error propagation in a line code, subject to information rate, one's density, and maximum run length. This technology generates a line code so that error propagation is minimized. Other alternatives create more work by increasing the output error rate; this method, however, works with existing error Correction Codes by presenting a lower number of errors.

POTENTIAL APPLICATIONS:

- Satellite communications
- Free space optical communications
- Fiber optics
- Integrated circuits
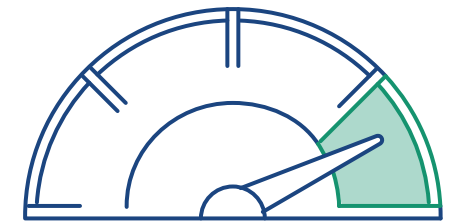
Removing Noise and Interference from a Signal

Method of Removing Noise and Interference from Signal
US PATENT # 7,676,046 | EXPIRES JANUARY 7, 2034

Method of Removing Noise and Interference from Signal Using Peak Picking
US PATENT # 7,492,814 | EXPIRES AUGUST 16, 2027

Method of Generating Time-Frequency Signal Representation Preserving Phase Information
US PATENT # 7,457,756 | EXPIRES FEBRUARY 16, 2027

This technology is a combination of three patents that remove noise and interference from speech signals. Unlike previous noise and interference removal methods, this technology is able to preserve phase information contained in a signal, which is critical for reconstructing the waveform after noise removal, and adequately identify and separate the signal and non-stationary interference components.

POTENTIAL APPLICATIONS:

- Mobile telecommunications
- Voice-over-IP applications
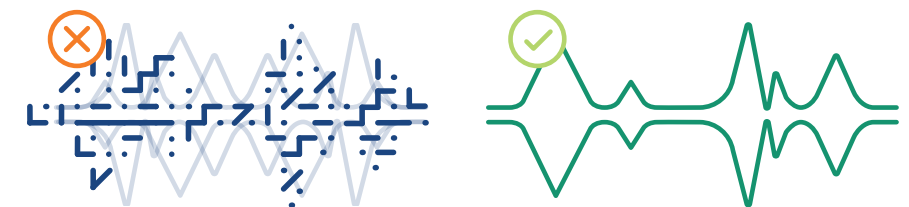
Realistic Testing and Comparison of Voice Signals

Method of Comparing Voice Signals That Reduces False Alarms
US PATENT # 7,650,281 | EXPIRES OCTOBER 1, 2028

MOBILITY
BIG DATA

This technology tests the robustness of a given voice-matching algorithm by providing the algorithm with variants of a digital file. The testing done against the original voice sample could include time-reversal, segmented re-arrangement, or a mixture of both time-reversal and segmented re-arrangement. This approach produces a larger corpus from fewer files, allowing for realistic testing under controlled conditions. It also reduces the Equal Error Rate (EER) i.e., the rates of false acceptance and false rejection, increasing performance in voice comparison methods.

POTENTIAL APPLICATIONS:
- Voice matching systems
- Authentication systems
- Biometric systems

ORIGINAL

TIME-REVERSAL

SEGMENTED
RE-ARRANGEMENT

Range Limited Antenna

MOBILITY

Range Limited Antenna
US PATENT # 7,642,986 | EXPIRES JULY 18, 2028
Range Limited Antenna
US PATENT # 7,292,202 | EXPIRES JANUARY 15, 2026

This technology is a Range Limited Antenna (RLA) containing two or more antenna elements arranged in sets. The technology features a radio frequency (RF) signal processing network connected to paired sets of antenna elements so the antenna is sensitive to signals within a Region of Interest (ROI) and insensitive to signals outside the ROI. Since the impinging signal sources in most RF environments are distributed over a very wide physical area, each signal must be analyzed and identified manually, though much of the spectrum is dynamic and cannot be easily classified. This technology solves this problem, allowing users to determine the approximate range of the signal source from the antenna array. The design supports an operating frequency range of 1MHz to 3GHz and allows adjustments to cut-off, radius-attenuation rate, frequency band, and sensitivity.

POTENTIAL APPLICATIONS:
- Small-radius radio operations (airport towers, special ops command vehicles)
- Warehousing a close-range radio-frequency identification (RFID) tracking
- Detecting, monitoring, and locating unlicensed emitters
- Broadcast systems that deal with cross-interference from competing signals
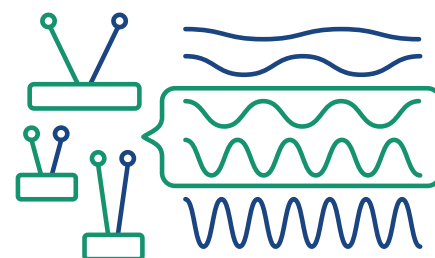
Estimating a High Frequency Carrier Signal

Method of Estimating a High Frequency Carrier Signal
US PATENT # 7,444,128 | EXPIRES JULY 22, 2027

MOBILITY

This technology estimates the carrier frequency of a mistuned high frequency (HF) single sideband signal from the structure of the underlying speech signal. Relying on the structure found in voiced speech signals, this technology processes the observed pitch harmonics to estimate the signal carrier frequency, which eliminates the need for manual tuning of the receiver and ensures that the signal is tuned correctly each time.

POTENTIAL APPLICATIONS:
- Ham (radio) operators
- Military use
- Linguistic analysis

NO
MANUAL
TUNING
NEEDED

Amplifying a Digital Signal

Method of Amplifying a Digital Signal and Device Therefor
US PATENT # 7,400,194 | EXPIRES OCTOBER 24, 2026

MOBILITY

This technology enables all-digital power amplification suited for small, battery-operated devices. Utilizing a sleep mode for the switching amplifier prolongs the battery life and increases efficiency in power usage. Reduced electromagnetic interference (EMI), which can degrade performance in surrounding elements, allows the amplifier to be employed without additional shielding. Both of these qualities make the system easier to conceal and reduce the cost of production.

POTENTIAL APPLICATIONS:
- MP3 players
- Hearing aids
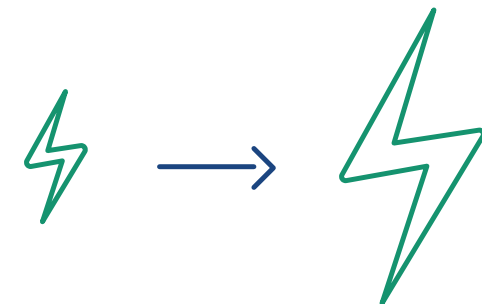
Wideband Retroreflector

Wideband Retroreflector
US PATENT # 7,383,026 | EXPIRES JANUARY 26, 2027

**MOBILITY
IOT**

This wideband retroreflector provides signal retransmission with low power in a compact design. This invention can significantly improve communications and remote-sensing applications including air traffic control, ground-to-satellite communications, and high-rate data transfer from radio-frequency identification (RFID) sensors. The system can also improve communications within or between structures by enhancing signals in areas with weak wireless reception.

The invention consists of an antenna, a circulator, and a mixer, and eliminates the need for a local oscillator and local transmitter. This compact design makes the system easy to deploy and maintain in remote locations. There are minimal power requirements because the power comes from an illuminating transmitter and antenna. This technology also handles high bandwidths more effectively than current systems.

POTENTIAL APPLICATIONS:

- Remote or dangerous area data collection
- Vehicle-to-vehicle, or vehicle to stationary object communication and vice versa (e.g., updates to/from or between manual or self-driving vehicles)
- Unmanned aerial vehicle swarms
- Gamification
- vehicle swarms
- Gamification

LOW POWER COMPACT DESIGN
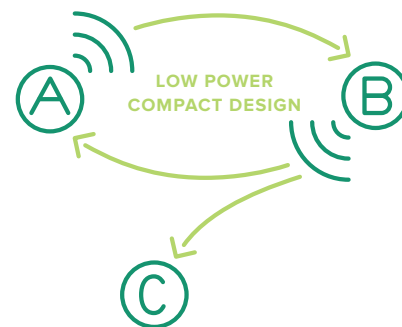
Reusable Tamper-Evident Bag

Reusable Tamper Evident Envelope
US PATENT # 7,350,689 | EXPIRES OCTOBER 17, 2026

MOBILITY

This invention provides the ability to initiate roundtrip courier services without including supplemental supplies or complex procedures. The technology provides couriers a tamper-indicating bag that can be reused while still maintaining a characteristic level of confidentiality and security.

The dual-seal characteristic of this container allows items to be outbound couriered, the primary seal inspected and certified by a recipient, and a return trip initiated using the container's secondary seal.

POTENTIAL APPLICATIONS:

- Courier services
- Industrial or medical packaging
- Sealed court/medical/banking documents
- Transporting proprietary or confidential documents
- Situations requiring return-receipt completion evidence and certification

Single Frequency Repeater

Single Frequency Repeater
US PATENT # 7,346,311 | EXPIRES AUGUST 23, 2026

MOBILITY

This technology is a single frequency repeater that retransmits a signal at the same frequency and at a higher power level. The repeater is also designed to avoid problems associated with feedback and concurrent oscillation. This technique requires less spectrum than retransmitting at a second frequency while still eliminating feedback.

The single plane design of this technology makes it adaptable to different locations, and its ability to adjust to different frequencies enable it to be useful to a large variety of communication devices.

POTENTIAL APPLICATIONS:

- SCADA range extension applications (e.g., power plants or refineries)
- Local Area Network (LAN) repeaters
- Cellular applications

REPEATER
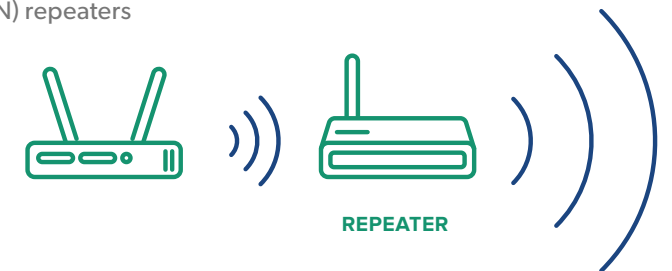
Impedance Matching RF Open Wire Transmission Lines

Device for Impedance Matching Radio Frequency Open Wire Transmission Lines
US PATENT # 7,283,015 | EXPIRES DECEMBER 13, 2025

MOBILITY

This technology is an innovative device for impedance matching along open wire lines. The invention is adjustable, easy to manufacture, and doesn't have issues such as sliding contact noise. The device is engineered with a balanced transmission line and a movable dielectric plate that, when moved, is able to increase or decrease impedance and linearly change the phase. As a result, this device matches impedance during transmission in a manner that significantly reduces noise.

POTENTIAL APPLICATIONS:

- Applications with a practical frequency range of 100 MHz to 5 GHz (i.e., cell phones, GPS, Wi-Fi, etc.)
- Antenna applications
- Any radio frequency transmission applications

MATCHES IMPEDANCE DURING TRANSMISSION

SIGNIFICANTLY — REDUCES — NOISE

CICADA: Synchronizing Time without a Broadcast Signal

Method of Synchronization without Broadcasting Synchronization Signal
US PATENT # 7,227,858 | EXPIRES NOVEMBER 25, 2025

This technology synchronizes time using environmental triggers to ensure that nodes (e.g., computer or telecommunication) are working in sync. After the desired environmental conditions are set, the node remains in a sleeping state until those conditions are met. Synchronization can occur without using radio signals, Wi-Fi, or cellular networks, which reduces susceptibility to loss of service and detectability. Without the need for battery power, the technology is able to conserve energy between intervals of time, making it suitable for potential use in extreme environmental situations.

POTENTIAL APPLICATIONS:

- Sensors
  – Triggering recording equipment for studies or documentaries
  – Military and emergency operations
- Synchronizing resource constrained embedded systems

Reusable Tamper-Indicating Label Fixture

Reusable Tamper Evident Security Device
US PATENT # 7,201,410 | EXPIRES AUGUST 14, 2025

This invention enables labels to be mounted on surfaces that normally do not work well with pressure-sensitive labels like concrete, unfinished wood, or slick surfaces. The reusable, tamper-indicating label fixture is a scalable unit designed to provide a disposable, smooth surface upon which to affix tamper-indicating labels. The fixture consists of two base units with disposable blank labels in each.

POTENTIAL APPLICATIONS:

- Inventory or evidence security for banks or law enforcement
- Medicine or food storage and transport
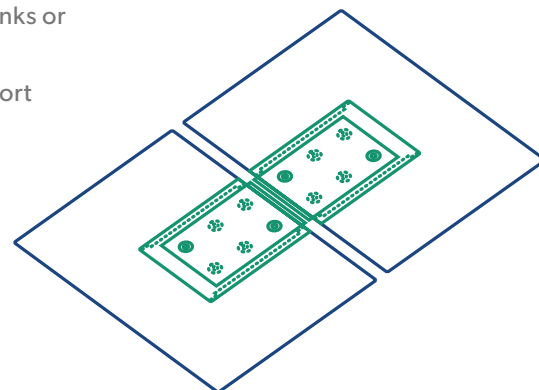
Shredder Residue Dispersion System

Shredder Residue Dispersion System
US PATENT # 6,820,830 | EXPIRES JULY 21, 2023

This shredder residue dispersion system directs shredded document residue into multiple residue receptacles in order to thwart reassembly. The system increases the security of a standard shredder by dispersing the shredded paper into multiple bins on a continuous basis, ensuring that no one document will be complete in any one residue bag.

POTENTIAL APPLICATIONS:

- Safeguarding propriety information
- Financial or banking industry
- Medical recordkeeping
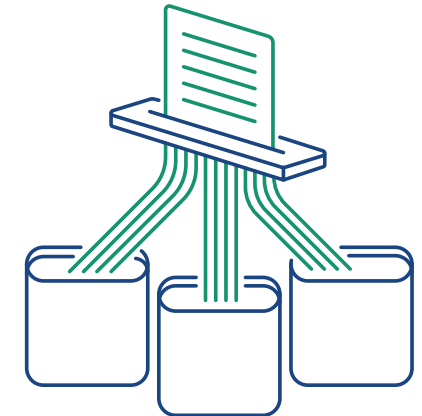
Multiple Pressure-Sensitive Adhesive Tamper-Evident Label

Tamper-Evident Label with Multiple Pressure-Sensitive Adhesives of Different Sensitivity
US PATENT # 6,670,008 | EXPIRES APRIL 9, 2022

This invention is a label that is coated with multiple adhesives, providing tamper-detection security to multiple vulnerable environmental situations. Coating labels with only one type of adhesive allows them to be removed without any evidence of tampering. This tamper-evident label is backed with a pattern of three different types of pressure-sensitive adhesives that offset three specific potential attempts—extreme high temperatures, extreme low temperatures, and the use of common solvents—to lift the label intact.

POTENTIAL APPLICATIONS:

- Industrial security
- Confidential information security
- Medicine or food storage and transport

SENSITIVE TO:

- HIGH TEMPS
- LOW TEMPS
- SOLVENTS
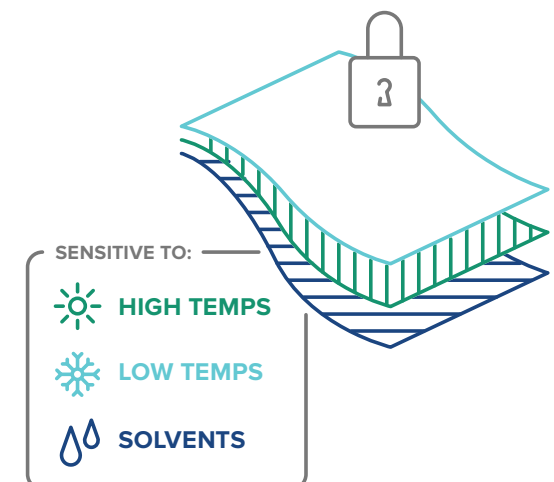
Estimating Signal Frequency

Method of Estimating Signal Frequency
US PATENT # 6,577,968 | EXPIRES JANUARY 24, 2022

MOBILITY

This technology estimates the frequency of a signal using multidimensional Fast Fourier Transform (FFT), where the signal is converted to a row vector and segmented. This solves the common problem of detecting weak tones in noise and estimating the frequency of the tone. This invention is both able to resolve multiple signals and resolve signals separated by less than the width of one transform cell.

POTENTIAL APPLICATIONS:
- Data communications
- Speech detection
- High-resolution spectral estimation
- Resolving signals in a search or threat warning application

Streamlined Synchronization

Method of Identifying Boundary of Markerless Codeword
US PATENT # 6,560,745 | EXPIRES NOVEMBER 15, 2021

MOBILITY

This technology provides a simplified method of error detection and correction when encoding and decoding synchronization between communication devices. All communication transmissions experience noise and errors, creating a need for error detection and correction. Information lost in chunks, or burst errors, can cause users to miss important data that is often difficult to recover. This technology enables blind synchronization to occur, removing the need to implement redundant transmissions, reducing the size of the transmission, and increasing the error detection and correction rates typically lost on burst errors.

POTENTIAL APPLICATIONS:
- Medical equipment
- Radio/satellite communications

EFFICIENT ERROR DETECTION & CORRECTION

COMMUNICATION DEVICE

COMMUNICATION DEVICE
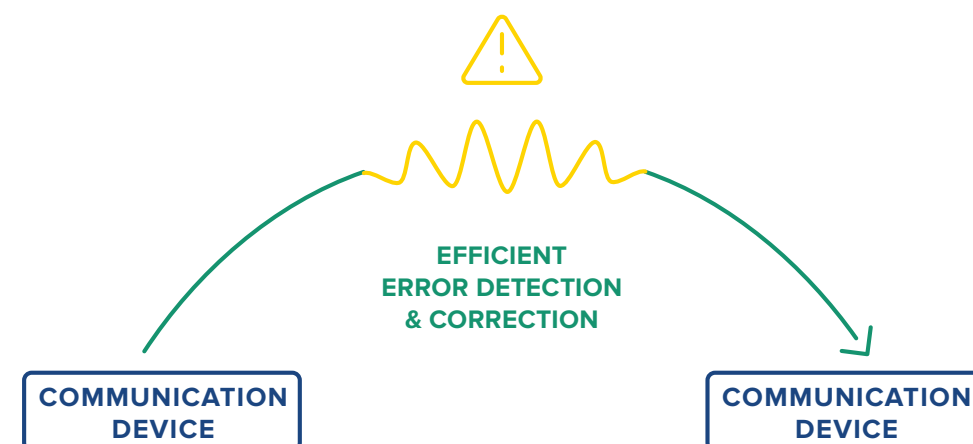
Feature Removal Using Wavelet and Fourier Transformation

Method of Feature Extraction Using Combination of Wavelet and Fourier Transformation
US PATENT # 6,385,543 | EXPIRES MAY 17, 2020

MOBILITY

This method removes user-definable frequencies from a signal. The technology measures high frequency signals in various cluttered environments at high sampling rates to perform front-end downsampling to only those frequency bands with signals of interest—such signals can be adaptively followed with a suitable tracker. Though originally implemented in MATLAB®, the technology can also be implemented on Field Programmable Gate Arrays (FPGA) and other modern Graphics Processing Unit (GPU) architectures. This method is a more efficient frequency removal process than prior methods and can be applied to signals containing a number of samples.

POTENTIAL APPLICATIONS:
- Internet of Things (IoT) sensors
- Cognitive radio applications
- Radar applications
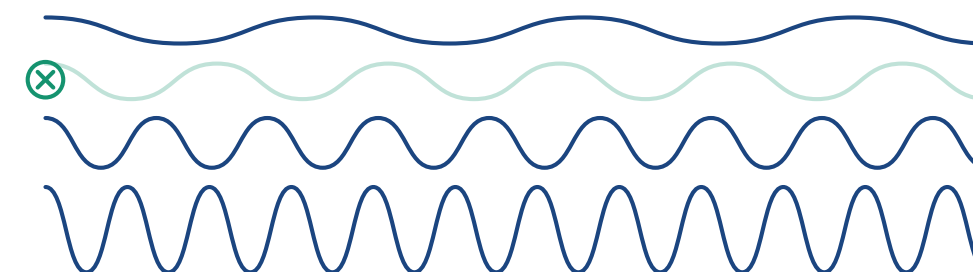
Data Signal Conversion

Device for Converting Multiple Signal Types to NRZ Format with Automatic Self-Test
US PATENT # 6,246,348 | EXPIRES FEBRUARY 23, 2020

MOBILITY

This device converts data signals in a Non-Return-To-Zero (NRZ) format into one of a variety of other user-selectable signal formats. Signals are transmitted in a wide range of formats, voltage levels, and speeds, which can result in signal format compatibility issues. The design of this technology eliminates the need and expense for additional procedures, equipment, and/or training typically needed to process varying signal formats.

POTENTIAL APPLICATIONS:
- Coded data generation or conversion

References

Legislation, Policy, and Guiding Principles

The NSA Office of Research and Technology Applications (ORTA) Technology Transfer Program (TTP) was established by a series of federal laws that promote technology transfer. These laws, as well as subsequent federal policies, White House directives, and Agency-wide goals, constitute the legal framework and guiding principles for the NSA ORTA. Successful transfer and commercialization of NSA technologies:

- Gives traction to the Federal Government's annual commitment to research and development, now totaling over $145 billion
- Accelerates NSA mission solutions
- Creates new companies, new jobs, and new revenue
- Strengthens the economy which in turn strengthens national security

Federal Technology Transfer Legislation and Executive Actions

The NSA ORTA TTP is built upon a federal legislation and policy framework that dates from 1980. This guiding framework enables the transfer of federal technology to the nonfederal sector to share the benefits of the national investment in research and development. Bidirectional sharing between federal laboratories and private industry includes technologies, personnel, facilities, methods, expertise, and technical information in general. Key technology transfer and Executive Actions include:

- Stevenson-Wydler Technology Innovation Act of 1980
- Bayh-Dole Act of 1980
- Federal Technology Transfer Act of 1986
- Executive Order 12591 of 1987
- Presidential Memo on Technology Transfer of 2011

White House Office of Science and Technology Policy

Cross Agency Priority (CAP) Goal: Lab to Market

The Lab to Market CAP Goal is to increase the economic impact of federally-funded research and development by accelerating and improving the transfer and commercialization of technologies from the federal laboratory to the marketplace. NSA ORTA is guided by this CAP goal and is a member of the National Science and Technology Council's Subcommittee that coordinates all federal technology transfer and commercialization efforts.

NSA Policy 10-9

This Agency policy establishes NSA ORTA and its authorities through the application of the federal technology transfer legislation and Executive Orders. It defines the roles and responsibilities for technology transfer activities at NSA.

NSA Innovation

NSA promotes innovative collaboration between its world-class technical workforce and external partners to more rapidly overcome mission challenges. Partnerships executed by NSA ORTA between Agency innovators and outside organizations fulfill this Agency-wide focus.

NSA Research Directorate Goals

NSA ORTA is located within the Agency's Research Directorate (RD). Technology transfer partnerships executed by ORTA help RD meet its mission goals to create solutions for customers and partners, maintain cryptologic excellence, and collaborate across boundaries.

Glossary

Cooperative Research and Development Agreement (CRADA)

An agreement between two parties, such as a federal lab and industry, academia, non-profits, and state and local governments, whereby each party's resources are leveraged in order to conduct research and development that benefit both. Through this collaboration, each party shares the benefits and risks in obtaining valuable technology transfer goals and objectives.

Design Patent

A form of legal protection granted to the ornamental design of a functional item.

Education Partnership Agreement (EPA)

An agreement between a federal lab and an educational institution or non-profit organization to transfer or enhance technology and provide technology assistance to the institution or organization.

Expiration of a Patent

The end of the enforceable term of a patent. At this time, anyone can practice the invention.

Federal Laboratory Consortium (FLC)

The FLC is the formally chartered, nationwide network of over 300 federal laboratories, agencies, and research centers that foster commercialization best practice strategies and opportunities for accelerating federal technologies from laboratories into the marketplace.

Intellectual Property (IP)

Refers to creations of the mind such as, inventions, literary and artistic artworks, designs, symbols, names, and images, used in commerce. Intellectual property is protected by law, for example, patents, copyrights, or trademarks.

Non-Disclosure Agreement (NDA)

An agreement in which the parties promise to protect the confidentiality of information that is disclosed during a relationship between parties.

Office of Research and Technology Applications (ORTA)

An office established at each federal lab to facilitate technology transfer.

Patent License Agreement (PLA)

An agreement between two parties in which one party licenses their intellectual property to the other party for its own use.

Patent Pending

A legal designation referring to a product or process once a patent application for the product or process has been filed with the USPTO but prior to the patent being issued.

Technology Transfer (T2)

Technology transfer at NSA is the legal process by which existing knowledge, intellectual property, or capabilities is exchanged between NSA and industry, academia, or other government agencies.

United States Patent and Trademark Office (USPTO)

An agency within the U.S. Department of Commerce that grants patents and registers trademarks. (www.uspto.gov)

Utility Patent

A patent issued for the invention of a new and useful process, machine, manufacture or composition of matter, or a new and useful improvement thereof.

Index by Keyword

R

S

T

U

V

W

Index by Patent Number

CREATING PARTNERSHIPS

IGNITING INNOVATION