Secure and Robust Tactical Communications Based on Code-Hopping CDMA (CH-CDMA)

Dipl.-Ing. Frank Hermanns
Dept. FKIE/KOM
Research Establishment for Applied Science (FGAN e.V.)
Neuenahrer Str. 20, D-53343 Wachtberg, Germany

email: hermanns@fgan.de

ABSTRACT

This paper proposes a secure and robust tactical spread spectrum transmission system based on Code-Hopping CDMA (CH-CDMA). It is both useful for terrestrial radio communication links as well as for satellite communication links. Very low detectability and highest robustness against jamming are the major design goals. Traditionally, long CDMA spreading codes are based on simple linear feedback shift registers (LFSR) like the Gold code family. Although arguments like low probability of intercept (LPI) and antijamming capabilities are regularly cited, they are not relevant for simple LFSR codes. A strong approach with the AES block cipher and code hopping schemes is presented. This way, the signal will become less vulnerable against coded jamming and eavesdropping. In the simulation, the secure AES-OFB spreading system shows no performance drawbacks in comparison to conventional Gold-code systems. Also code-collision jammers are demonstrated with AES-OFB and Gold-codes.

1.0 INTRODUCTION

Today, most effort is done in civil wireless communications to secure the transmission above the physical layer. Even "secure" CDMA systems communications are using vulnerable linear feedback shift register (LFSR) generators to create the spreading sequences. According to [2], the hidden 42-bit LFSR mask value of IS-95 mobile phone communications can be revealed in about 1 second of interception. The argument of CDMA-based "voice privacy" in IS-95 is weakened by this. Stronger sequences based on nonlinear combinations of LFSR elements require more effort in breaking, but this is not impossible in general. Once knowing the PRNG seed values, also jamming becomes much easier and all the antijamming gain of CDMA is lost when the jammer is using the coded signal. When talking about SS/CDMA based security, the basic assumption usually is (from [3], p.139):

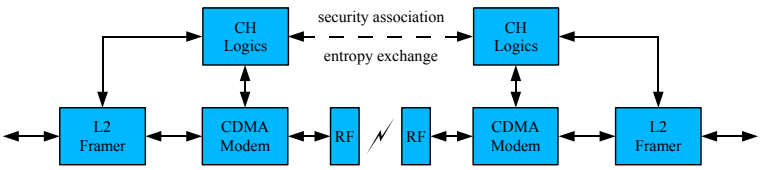


Figure 1: Architecture of a secure spread spectrum transmission system [1]

> The jammer has complete knowledge of the spread-spectrum system design except he does not have the key to the pseudorandom sequence generators.

This static key, however, can be acquired by cryptanalysis or by theft of communication devices. Nobody can really rely on this assumption. To exploit the power of CDMA for antijamming and low probability of intercept, flexible waveforms with dynamic spreading codes have to be developed. A general system architecture is shown in Fig. 1.

The main difference to traditional CDMA systems is the dynamics of secure pseudonoise spreading code generators by true random sources of entropy. That makes the actual spreading sequence unpredictable, but can still be synchronized by cryptographic means (asymmetric public key blocks). The spreading code can be realized in hardware by AES blocks in OFB mode. Simple variants with basic LFSR generators are possible

	Physical layer	Link layer	Network Layer	Transport Layer	Application Layer
Major advantages	Jamming and interception protection, prevents traffic analysis, additional line of defense	Protects the most vulnerable wireless part, prevents higher-layer traffic analysis	IPSec is the best solution for Internet security. End-to-end / host-to-host security	Widely used for securing TCP connections, no need to modify the unsecured IP-networks	Can satisfy applications requirement very well. User-specific keys for documents
Major disadvantages	Not real crypto, complexity, synchronization issues	Only one hop is secure, not end-to-end	IPSec works only for IP networks, not user-to-user, PEP/IPSec incompatibility	No security for UDP and multicast, applications have to be modified for TLS	No transparency, where applications need modification to fit security

Table 1: Security layers comparison for tactical wireless networks

to reuse existing CDMA hardware. By dynamically re-seeding the LFSR, attacks become much harder. Cross correlation and BER performance of long AES codes are comparable to optimized LFSR Gold codes.

Code-Hopping CDMA seems to be the only reasonable antijamming technology for civil communication systems. Interception and eavesdropping renders impossible for unpredictable spreading codes. At negative SNR, the signal disappears in noise and the attacker cannot even detect a signal. The advantages of CH-CDMA grow with the signal bandwidth. Best are modern Ultrawideband (UWB) transmission systems.

Military and civil security problems are not fundamentally different. Also in civil networks, Internet attacks are daily threats. Falun Gong in China is jamming national satellite TV signals quite often. In WLAN networks, single users can kick out others to get the full cell bandwidth. So, antijamming is a certain topic in civil wireless communications as well. It is useful to have this dual-use in mind, when designing new security solutions.

2.0 MULTI LAYER SECURITY FOR WIRELESS NETWORKS

Securing the physical transmission layer is not the only way of getting a secure and robust tactical communication link. It has to be seen in a context of the 7 layer OSI stack model. OSI itself defined security functions in serveral layers, but this is far from reality in current systems. The old standardization documents need to be updated to cope with recent technology developments.

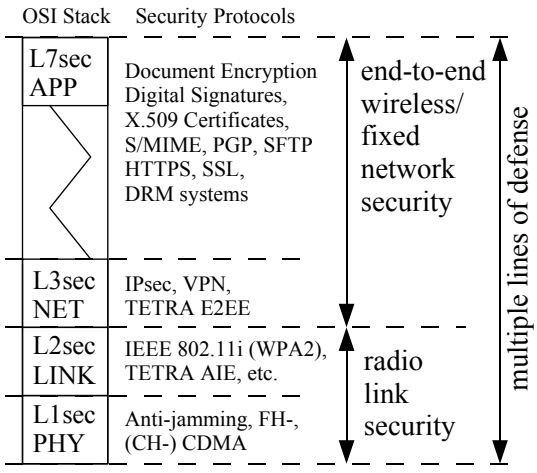


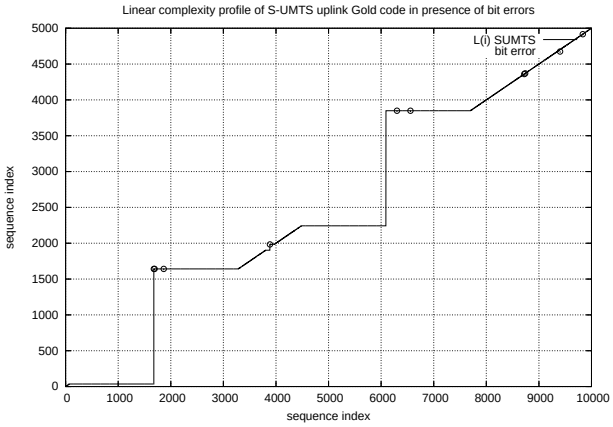
Figure 2: Wireless Security vs. OSI layers

Security architectures of networked systems like wireless TCP/IP or wireless more OSI-oriented networks (UMTS, GSM) are usually focused on layer 2,3 and 7 security protocols. Quite often, layer 3 security is omitted, because it would need network based PKI infrastructures for hosts. This is not available on the public internet. Only some virtual private networks or remote access solutions rely on IPsec. Furthermore, the PEP / IPsec incompatibility is a real challenge. A prominent satellite DSL provider did a traffic split because of this: routing less bandwidth applications like Email via IPsec and transmitting high bandwidth applications like WWW in plain text. The term "'transport layer security"' in the Internet is a bit misleading, because in the OSI context it is more an application layer protocol gateway.

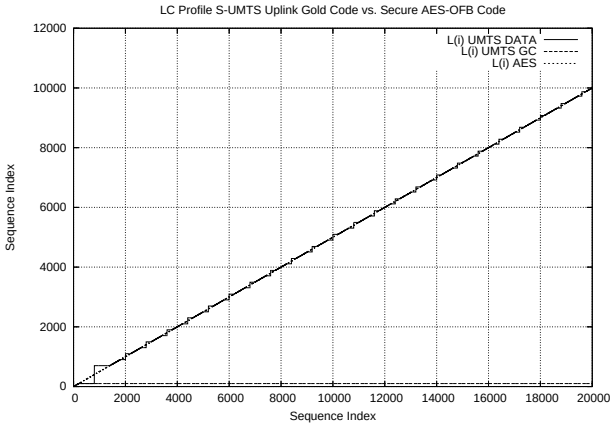
Table 1 gives an overview about the specific advantages and disadvantages of security in several OSI layers. There is a certain redundancy if more than one security protocols are used at the same transmission. But looking at the details, it is evident, that each solution has some specific advantages. Combining those features, a better overall security can be achieved. Even if two security technologies with the same features

are combined, this lowers the risk of dramatically, that implementation specific security flaws hit those technologies at the same time. History has been shown that faulty implementations are one of the main security risks. Combining security technologies at different OSI layers are more complementary. The confidentiality protection of layer 1 data helps to prevent traffic analysis on layer 2, as an example.

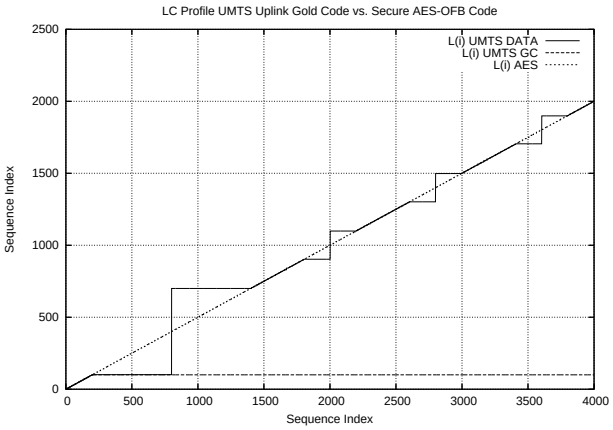
3.0 LFSR CODES AND THEIR PROBLEMS



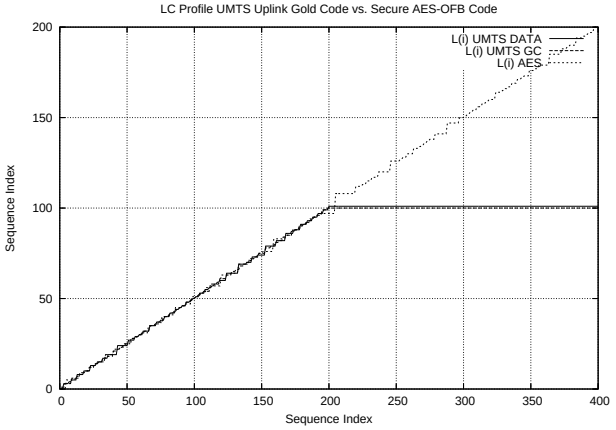
(a) Linear complexity profile, LFSR in presence of bit/chip errors



(b) LCP(i): S-UMTS Gold vs. AES-OFB with data modulation



(c) LCP(i): S-UMTS Gold vs. AES-OFB, zoom 1



(d) LCP(i): S-UMTS Gold vs. AES-OFB, zoom 2

Figure 4: Linear complexity profiles of distorted spreading sequences [1]

Many spread spectrum communication systems are based on linear feedback shift register codes (LFSR). Especially Gold codes (LFSR based on 2 m-sequences) are popular in code division multiplex systems (CDMA) due to their good correlation properties. However, their simple generator structure makes it easy to detect them as non-random, even in modulated and distorted form. Figure 3 shows the ideal linear complexity profile (LCP) of LFSR sequences compared to true random sequences. The LCP is the intermediate output of the Berlekamp-Massey algorithm (BMA) to determine the linear complexity of a sequence. True random sequences with unlimited complexity go approximately linear with the sequence index i. The ideal curve is

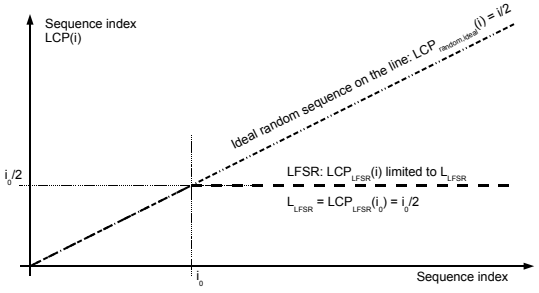


Figure 3: Linear complexity profile, ideal LFSR

$$LCP_{random,ideal}(i) = i/2$$

and the real measurement is only slightly fluctuating around this one. LFSR sequences with random initialization vectors and random weights look similar, but only until the sequence index i_0, twice the register length (weights plus initial state vector size).

This algorithm can be used to detect linear generators in spreaded signals. In presence of bit errors, the LCP deviates from the ideal form. But single bit errors are recognized as complexity steps in the LCP. In between the bit errors, the linear segments reveal the basic generators. This is demonstrated in figure 4(a) with the S-UMTS uplink code (Gold code of degree 18).

LFSR-spreaded signals with a factor greater than i_0 are easily visible in the LCP, as shown in the figures 4(c) and 4(d). However, on a large scale (Fig. 4(b)) they come close to the ideal linear LCP of random sequences. Note that the AES based code in comparison behaves like a true random code on all scales of the LCP curve.

When signals are spreaded by a factor smaller than i_0, a priori knowledge about the data structures must be used to eliminate the data modulation. A number of known header bits can be sufficient for this. An interesting approach is [2] by reducing the linear equations to determine the secret mask values of the American IS-95 cellular mobile telephone standard.

LFSR in combination with nonlinear elements create more complex sequences. The Berlekamp-Massey algorithm could not distinguish them from true random generators, the $LCP(i)$ goes approx. linear with i. Also AES based codes behave similar in $LCP(i)$. But still there is a difference. While for simple nonlinearized LFSR generators the code can be broken ([4]), for AES there is no way yet to break the sequence. There are theoretic approaches for cryptanalysis of AES ([5]), but no one up to now has reported that it works in practice. One example of broken codes is the GSM code, a clock-controlled LFSR. Sometimes it's not even necessary to break the code itself, if the communication protocol contains security flaws ([6]). Quite often, only one weak element of a complex security system can cause the security completely to fail. Protocols like UMTS [7] for example are quite complex with some questionable "compromises" of security vs. (GSM-) tradition. Additional strong physical layer security measures provide additional "fuses" against leaks on higher layers, next to its actual task.

4.0 AES BASED CODES AS A BASIS FOR FUTURE SOFTWARE DEFINE RADIO WAVEFORMS

4.1 The AES block cipher

In 1997, the American National Institute of Standards and Technology (NIST) initiated a process to select a symmetric-key encryption algorithm as a successor of the outdated and insecure Data Encryption Standard (DES) from 1976. Its name should be AES, for Advanced Encryption Standard. Main criteria were security (resistance against attacks) and performance of hardware and software implementations. In an open process within the cryptographic research community, the 15 candidate algorithms were discussed and analyzed. The winner algorithm was Rijndael by the two Belgium inventors Joan Daemen and Vincent Rijmen ([8, 9]). Its now officially registered as Federal Information Processing Standard FIPS PUB 197. Both DES and AES are certified in the US to protect sensitive (unclassified) Federal information.

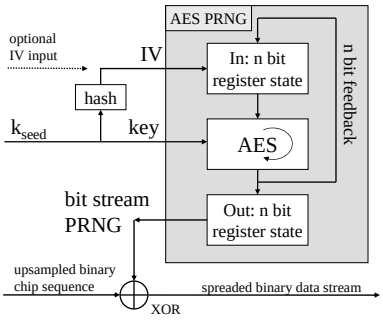


Figure 5: AES output feedback circuit [1]

4.2 AES-OFB circuit to generate spread spectrum sequences

As a block cipher, AES is usually implemented in cipher block chaining (CBC) or electronic code book (ECB) circuits ([10]). But to generate direct sequence DS-CDMA spreading codes, an output feedback circuit (OFB) should be employed for AES. Figure 5 shows a block diagram of this circuit.

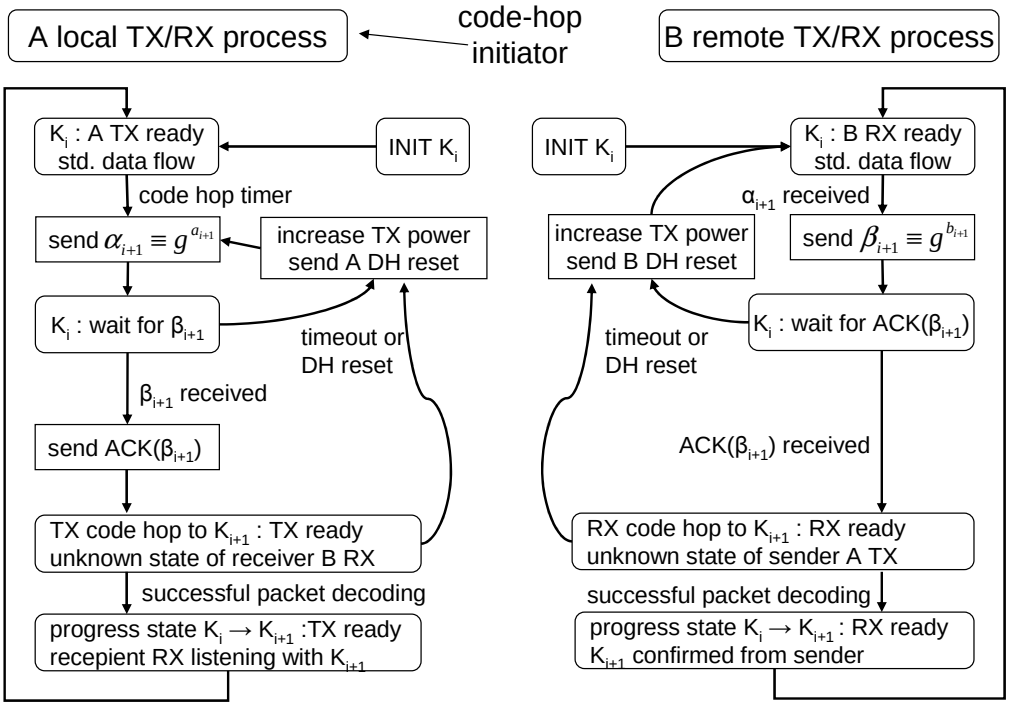


Figure 6: CH-CDMA state machine [13]

The circuit can be realized entirely in simple hardware elements. No arithmetic unit or CPU is necessary. The hardware performance is much better than with other algorithms of similar cryptographic strength. VHDL core designs are available from [11] for ASIC or FPGA usage. ASIC implementation results reach more than Gigabit/s. Applied to direct sequence CDMA this means a chip rate of $> 10^9$ chip/s. So, AES is even suitable for secure broadband applications.

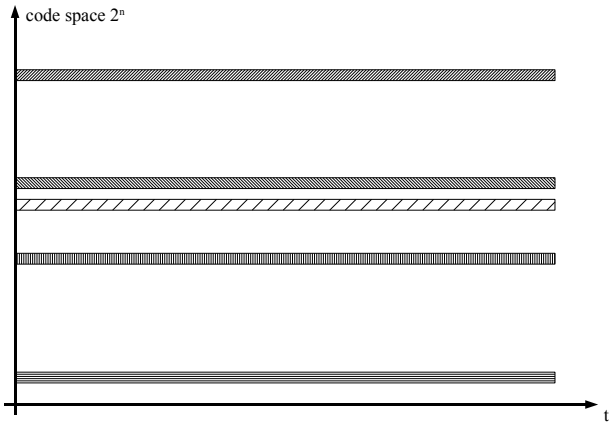
4.3 AES-OFB spreading code properties

Ideal long spreading codes have those properties of true random sequences. Fully orthogonal code vectors are only realistic in short spreading codes. As there is no ultimate way to measure randomness, a set of statistical randomness tests have been run to compare AES-OFB sequences with those of conventional Gold codes (UMTS spreading code generator), see [12]. Both AES-OFB and UMTS Gold codes fulfill all the thresholds of the randomness criteria. But AES is not better in all categories. The frequency test, serial test and runs test was better performed by the simple LFSR sequence. Probably the simplicity of the generator is even the reason for this. More important for spread spectrum are the correlation properties. And this test, the autocorrelation test and also the poker test was better with the AES-OFB code.

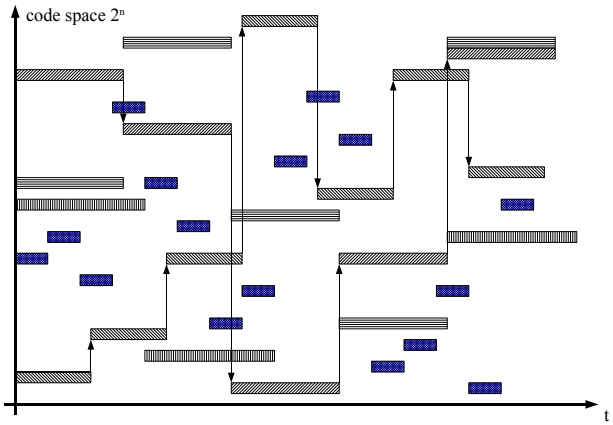
The cross correlation properties are not explicitly measured in the randomness test suite. But they are the dominant factor for the good results in the multi-user performance simulation, see chapter 6.1.1. The seed values are selected randomly for security reasons. But the cross correlation is nearly ideal when using very long spreading codes. The risk of randomly choosing identical codes for different users is negligible. There are $N = 2^{128}$ different spreading codes available for a 128 bit AES block cipher. The key management protocol can handle these very rare cases by just generating another seed value after a certain time-out interval.

Spreading Method	Multiplex Based On
Direct Sequence DS-CDMA	(near) code-orthogonality, CCF between 2 codes dissapears
Frequency Hopping FH-CDMA	distribution of Garbor containers in the time-frequency domain
Time-Hopping TH-CDMA	synchronized pulses, distributed in the time domain
Hybrid DS-FH-CDMA	mix of code- and frequency orthogonality, separated by time, frequency and code
Chirp-Modulation (Radar)	chirp transform
Chaos-Modulation (CSK, CPPM ..)	near-orthogonality of sequences from parametric chaotic systems

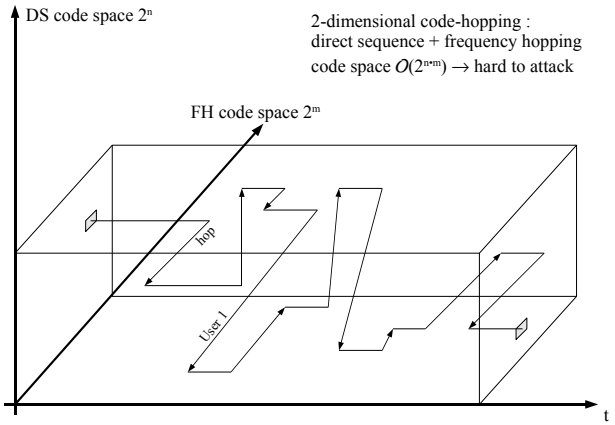
(a) Conventional static SS/CDMA systems



(b) Static SS/CDMA systems (DS/FH/TH-CDMA,CSK,CPPM...) employ pseudo-random sequences, but leave their seed values constant



(c) DS-CH-CDMA or FH-CH-CDMA code-hopping with dynamic seed values



(d) DS-FH-CH-CDMA, hybrid code-frequency-hopping

Figure 7: Static and dynamic SS/CDMA codes [1]

5.0 AES CODE HOPPING SYSTEMS

5.1 Dynamize pseudonoise generators

The idea of using AES for spread spectrum generators came up during the design of a secure code-hopping system (Fig. 5). Pseudonoise generators are more secure, if their seed values are dynamic. These PN sequences inherit a higher "randomness" if their seed vector is fed by a true physical random source (e.g. [14]). Stronger cipher algorithms do not increase the algorithmic information of the sequence (as defined by Gregory Chaitin), but in practice their entropy appears higher, as high as true random sequences.

Using the code-hopping approach for spread spectrum signal transmission needs transmitter and receiver to be synchronized. Also the AES-OFB pseudonoise sequences with random entropy sources for the seed (the initialization vector) need to be synchronized. That is only possible with public key cryptography. Diffie-Hellmann (strictly speaking, it is the Diffie-Hellmann-Merkle algorithm) would be one approach to form one common random key out of the two random sources of transmitter and receiver. So, the code-hopping logics in figure 5 is based on Diffie-Hellmann computations.

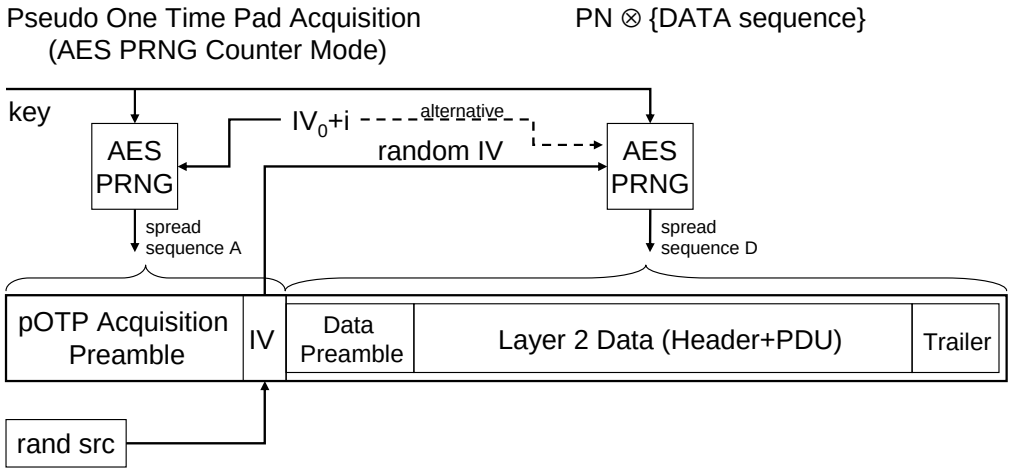


Figure 8: CH-CDMA burst structure [13]

5.2 CH-CDMA burst structure

Code-hopping CDMA (CH-CDMA) needs a special formatting of the data packets. In burst mode, figure 8 points out a possible packet structure. This is not implemented yet, but shows important elements for transmission security. The burst is split into one acquisition preamble and one data part. The data part itself consists of the layer 2 payload data (incl. forward error correction) with a preamble and a trailer sequence. Several measures have to be implemented to prevent repetition of chip sequences. Repetitions undermine the effort of hiding the signal and additionally allow jammers to perform code collision attacks.

Anti-repetition strategies are "pseudo" one time pad aquisition preambles, generated from AES counter mode circuits. If the IV can be additionally randomized, the data preamble and trailer would not repeat any more. In the economic reality, this ideal structure might be simplified in a compromise between complexity and security.

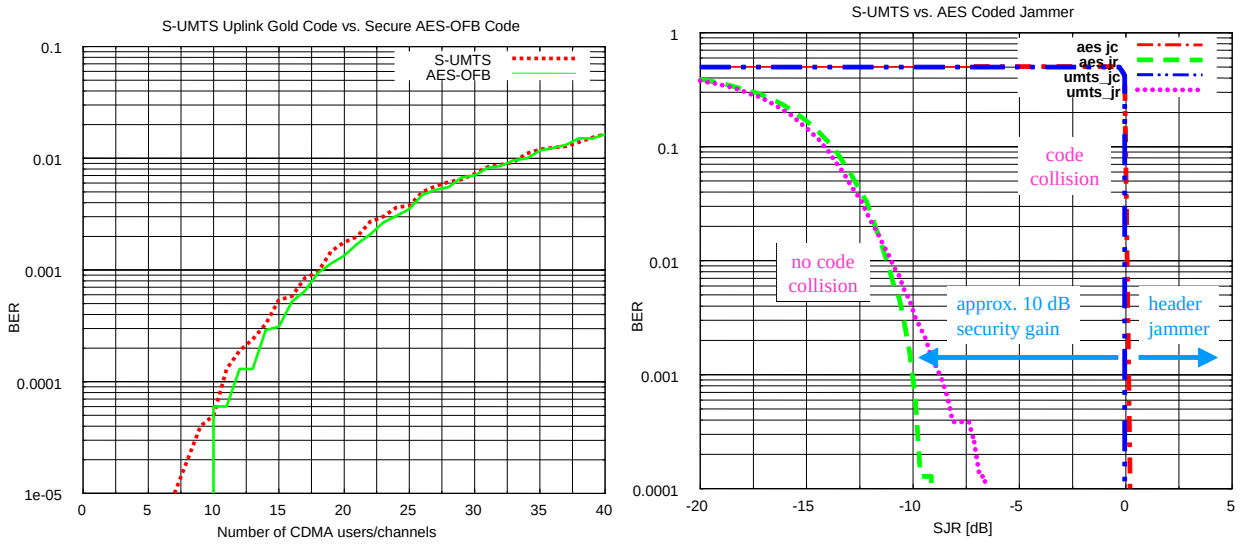
5.3 CH-CDMA state machine

To guarantee synchronization during re-keying, a complex CH-CDMA state machine (Fig. 6) has to prevent that transmitting and receiving process apply different spreading codes. The basic idea is the asymmetric key exchange of Diffie-Hellmann ([10]) with the (true) random parameters $a_{i+1}, b_{i+1} \in \boldsymbol{N}$ and the public values $\alpha_{i+1} \equiv g^{a_{i+1}} (mod\ p)$ and $\beta_{i+1} \equiv g^{b_{i+1}} (mod\ p)$. ($g \in \boldsymbol{N}$ and a public Prime $p \in \boldsymbol{N}$). Each of them can then compute $k_{i+1} \equiv \beta_{i+1}^{a_{i+1}} \equiv (g^{b_{i+1}})^{a_{i+1}} \equiv g^{b_{i+1}a_{i+1}} \equiv (g^{a_{i+1}})^{b_{i+1}} \equiv \alpha_{i+1}^{b_{i+1}} (mod\ p)$, used now as the AES-OFB PRNG common seed value. This is a standard operation.

After the exchange of α_{i+1} and β_{i+1}, transmitter and receiver reach a critical state when they have to decide about hopping the spreading code to a new AES-OFB seed. At this moment it is unclear if the partner is still using the old spreading code due to packet loss or the new one. A false decision here has the result that the receiving partner cannot decode or even detect the packet any more. So, this intermediate state with a new spreading code has to be provisional as long as the partners know that both are using the new code. Only then, the code-hop is considered as complete. If nothing happens after a certain time-out, the partners try to get into contact with the old code again. One measure could be to increase the transmit power, because synchronization loss can be caused by jammers or bad channel conditions.

6.0 SIMULATION

To demonstrate the feasibility of code-hopping systems with AES based spreading codes, a simulation system was created.



(a) Multi-user interference of AES-OFB and S-UMTS (uplink) codes

(b) S-UMTS vs. AES-OFB coded jammer scenario

Figure 9: Performance simulation results [1]

6.1 Simulation setup

First demonstrations were done with a simplified communication model. Transmitter and receiver were assumed to be chip-synchronous and the transmission channel was modeled as AWGN. The signal was modulated as direct sequence (DS-CDMA) QPSK. The receiver was a matched filter with a bit-length integrate & dump circuit. [12]

In this setup, the performance of AES based spreading codes was evaluated and jamming scenarios were demonstrated.

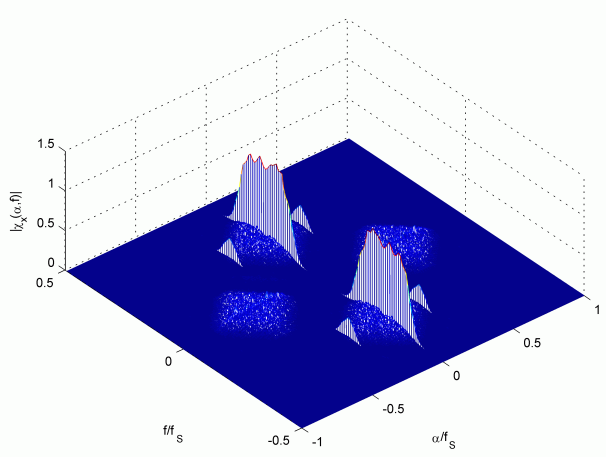
Several functional tests and jamming scenarios have been run. Due to limited computing power, the accuracy in the low BER regions is not very high. Sufficient bit error numbers would require large signal vectors after spreading and oversampling. The presented results already saturated the AMD64 machine with 3 GB RAM.

6.1.1 Multiuser performance

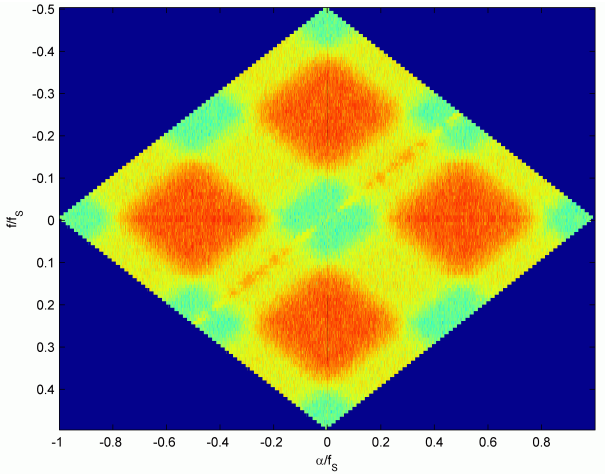
Figure 9(a) compares the multiuser performance of S-UMTS Gold codes and AES-OFB spreading codes. As expected, the AES-OFB code has no performance drawback against Gold codes. It is even slightly better, in conformance with the slightly better correlation test parameter in table **??**.

So, secure spreading codes can compete with optimized Gold codes. This is important for the economic frequency use. The resulting curve is slightly different at other test runs, because the code selection is random. The advantage of AES was seen in every run. In future study, as far as possible, analytical error bounds should be developed for the AES based code. The only remaining economic factor is the higher computing complexity of AES-OFB against simple LFSR.

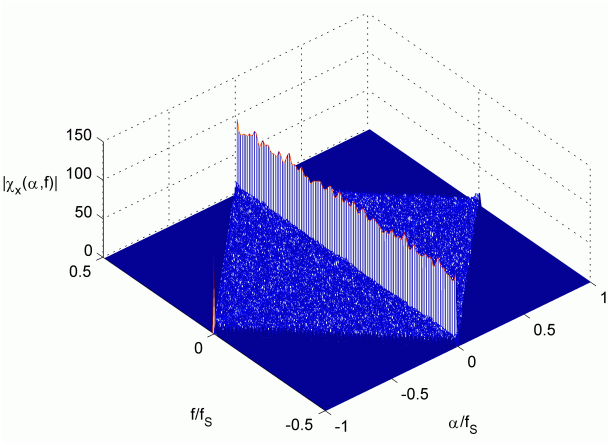
Competing approaches with chaotic signal generators [15–17] did not reach that performance. They were proposed for similar reasons, to be robust against jamming and secure because of chaos. In general, chaotic sequences are worse in their randomness and correlation parameters. In terms of security, their simple structure cannot compete with block ciphers like AES. But this has not been demonstrated yet. Although they are much simpler to implement (e.g. simple oscillators with nonlinear elements), they don't reach the performance of Gold codes or AES-OFB.



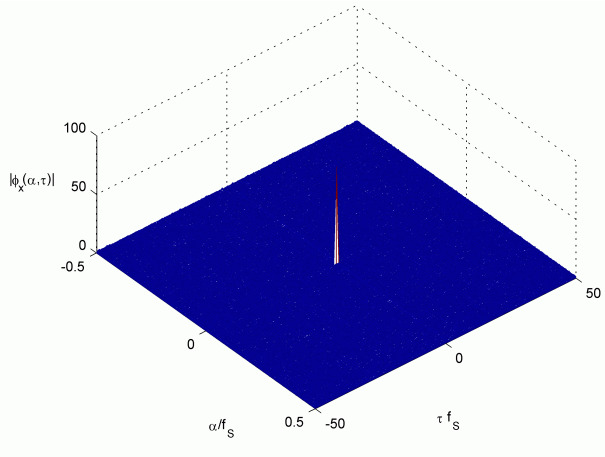
(a) $|\chi_x(\alpha, f)|$ spectral ACF at 20dB SNR, clear signal



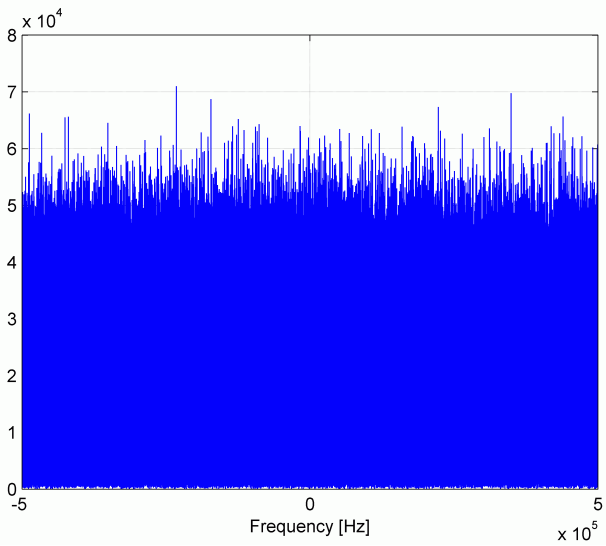
(b) $\log|\chi_x(\alpha, f)|$ spectral ACF at 20dB SNR, clear signal



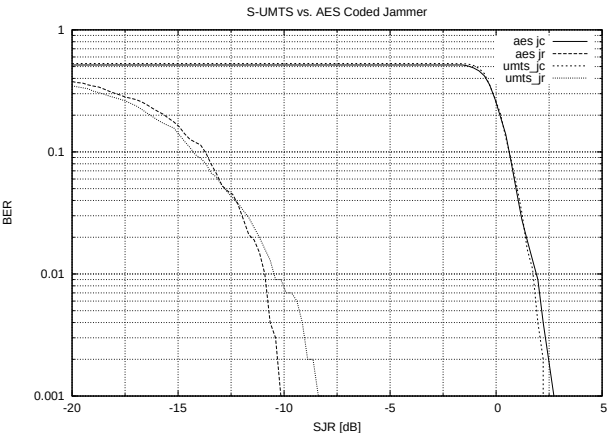
(c) $|\chi_x(\alpha, f)|$ spectral ACF at -20dB SNR



(d) $|\phi_x(\alpha, \tau)|$ cyclic ACF at -20dB SNR



(e) spectrum at -20 dB SNR, signal disappeared



(f) Coded Jammer Performance at -20 dB SNR

Figure 10: AES-OFB Spreaded Signal hidden at -20 dB below noise level

6.1.2 Antijamming performance

Main motivation of using AES-OFB was the higher security, better antijamming performance and lower probability of intercept (LPI). Figure 9(a) is the result of a jamming scenario of UMTS and AES-OFB codes, with and without code collision. Simulation parameters were $N = 2 * 488$ Bytes packet size, background noise of $SNR = 3dB$ and a huge spreading factor of $SF = 1000$. This is a scenario of a "high security-level" transmission system of Ultrawideband spreading (UWB). The security level of consumer devices may be downsized.

In case of LFSR it can be assumed that the jammer is able to discover the secret LFSR parameters (initial vector and secret mask). So, for UMTS codes the jammer can perform a code collision with the victim. The BER increases dramatically when the signal to jam ratio (SJR) falls below the 0 dB value.

With the AES-OFB spreading code, especially in combination with code-hopping, we assume that the jammer is unable to determine the user's spreading code and therefore cannot cause any code collisions. His jamming efficiency is not much better than simple broadband noise jamming. So, the protection level of AES-OFB codes is much higher than with LFSR codes.

In our simulation, the security gain (in SJR) is about 10 dB at the 10^{-3} BER level (sufficient for data transmission with FEC channel coding). So, the jammer would need about 10 dB more power to disturb AES-OFB transmissions, compared to the UMTS code.

The security gain can further increase if the possibility of header jammers are taken into account. This will be an extension in future. A header jammer is a sort of intelligent jammers that are able to detect and specifically jam headers of a packet transmission. A packet is considered as totally corrupt or lost when the header is corrupt. With this, the effective bit error rate dramatically increases. Assuming that this is only possible when the signal can be intercepted and not for AES-OFB, the security gain increases. Attacking special control functions of a protocol is quite common in higher layers. Also the physical layer might be affected, although it is not very common today.

6.2 Future developments

In the future development, the simulator should implement the signal acquisition and tracking algorithms to allow asynchronous transmission. Next, the code-hopping idea should be realized. The physical transmission layer cannot handle this any more. It needs a link layer (OSI layer 2) control protocol to run the CH-CDMA state machine. In real applications, those functions can be integrated with the other layer 2 functions (resource control, authentication etc.).

Future research should evaluate analytical properties of this approach. Simulations should demonstrate further system properties of CH-CDMA systems.

7.0 CH-CDMA BASED WAVEFORMS FOR FUTURE STANAG SOFTWARE DEFINED RADIO (SDR) STANDARDS

A Software defined radio (SDR) is a radio that substitutes many traditional hard-wired signal processing components by software implementations. The ideal concept is to place the A/D conversion directly at the antenna and to perform all RF and baseband processing in software. However, in practical receivers, there are still many reasons to realize RF components in analog hardware and to limit software to the baseband signal processing. The great advantages of SDR are the flexibility, expandability and reconfigurability.

First SDR approaches mainly imitated existing radio standards, analog and digital modulations. In the military domain, for national and multinational operations, it is important to allow interoperable communications between many incompatible radio standards. This even includes civil cellular radio networks like Tetrapol, Tetra and GSM. Ideally, it needs only one SDR hardware terminal to communicate with all those standards.

But SDR allows more than just imitating existing standards. The software concept enables fundamentally different methods such as code-hopping spread spectrum (CH-SS/CH-CDMA).

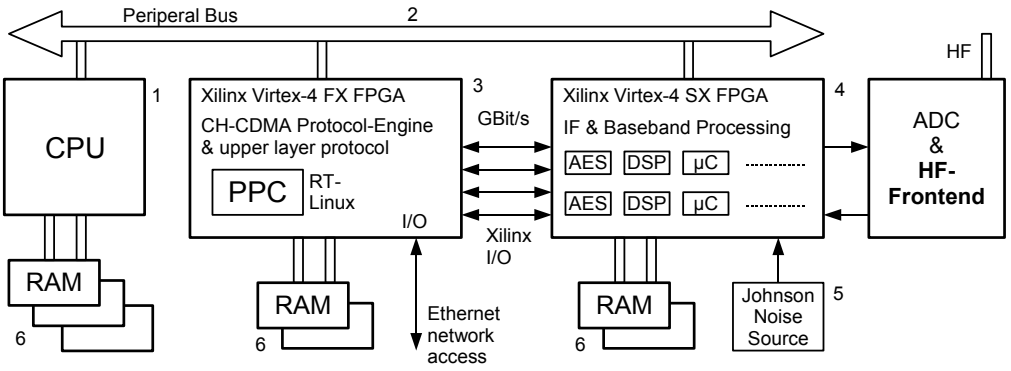


Figure 11: CH-CDMA SDR Terminal Prototype Design (for Phd thesis [1])

The CH-SS/CDMA concept was first proposed in [13] and is examined in a greater link security concept in [1]. Basis for a prototype design are two Virtex-4 FPGA with specializations in baseband processing (SX-Type) and protocol processing (FX-Type). The SX-Type profits from a large number of DSP blocks and logical fields. The FX-Type has an embedded PowerPC core, ideally suited for the complex protocol and cryptographic processing. A single Virtex-4 would not provide a sufficient gate count. On the other hand, an external CPU might not handle the time-critical state machines for the complex cryptographic synchronization. Nevertheless, a conventional CPU is forseen to host the general Modem/Terminal operating system and to provide higher-layer network functions, such as authentication, certificate processing, configuration, router and firewall functions. It could be a Linux variant without GUI. The PowerPC core could run a realtime OS such as RT-Linux, because the layer 2 processing is very time-critical.

Another advantage of a CH-CDMA based STANAG standard is that of multiplexing. Wireless NATO radios should handle national closed user groups as well as multinational closed user groups. CH-CDMA is a natural scheme to achieve those requirements simultaneously. Every traffic channel runs its own dynamic security code and can be synchronized within a closed group, without affecting the others. Of course, the simple one by one cryptographic synchronization scheme has to be extended to a group cryptographic exchange. Similar requirements are known from higher layer security protocols in Mobile AdHoc Networks (MANET).

7.1 Future STANAG LPI/LPD modes for covert tactical communications based on CH-CDMA

Low Probability of Intercept (LPI) and Low Probability of Detection (LPD) are very important concepts of spread spectrum. Signal detection is a classical field. Next to pure energy detection, also advanced methods such as spectral and cyclic autocorrelation are possible.

Figure 10 shows one example with a -20 dB SNR signal hidden in noise at a spreading factor of 1000. This is still suitable for low-rate high secure and robust links, as the coded jammer performance chart indicates (f). But the spectral and cyclic autocorrelation diagrams do not indicate any difference from random noise (c-d). For clear signals (a-b) or slightly noise signals, they can be used to extract modulation parameters. Fig. 10a has discrete lines at the QPSK chip symbol rate. In (d) there are no lines any more.

These are pure chip modulation properties. The situation is different if a constant LFSR spreading code could be extracted from the random sequence. Then, after the decorrelator stage, the original signal is visible again. Only Code-Hopping with strong sequences is able to fight this risk effectively.

7.2 Future STANAG combat modes for robust tactical communications based on CH-CDMA

The combat mode relies on a high spread spectrum "‘processing gain"’ (PG) to increase robustness against jamming signals. The PG factor is proportional to the minimum required power that the jammer has to invest

to archive the jamming effect. While the PG factor is very flexible in the SDR, the jammer transmission power may saturate very soon. The PG is relevant for all types of jamming waveforms like broadband noise, partial band noise, pulse, chirp or continuous wave. Robust communications in this sense is fighting with PG against jamming signal power.

However, this antijamming capability with the PG is completely lost, if the jammer can achieve code-collision attacks. This demands for previous signal analysis and pseudorandom seed determination. This is practically impossible with CH-CDMA and therefore, it is also the most jamming-robust waveform.

In military satellite systems, antenna nulling is used as another antijamming technique. With an interferometric circuit, the signal of a small narrow-beam antenna is subtracted from the signal of the usual wide-beam antenna. So, signals from a region around the jammer are simply blocked. With phased array SDMA antenna techniques, multiple regions can be blocked. However, jammers located in near distance cannot be blocked. Furthermore it is a problem of blocking several jammers at the same time. And at last, the cost of antenna nulling is is very high price, too high for civil mobile satellite communications.

8.0 CONCLUSION

The dynamic code hopping approach with AES based spreading codes offers best protection against eavesdropping and intentional jamming in CDMA spread spectrum communications. Systematic vulnerabilities in conventional secure spread spectrum systems will be fixed by this countermeasure. Performance drawbacks did not appear in the transmission simulation, but the PRNG generators and synchronization will have a higher complexity. It has been shown that AES based spreading codes are suitable for the code hopping approach. Their cryptographic strength is remarkable and the performance of AES hardware implementations is sufficient.

Simplified variations of this idealistic approach can also help to increase security of existing spread spectrum solutions like WLAN, UWB or (S-)UMTS. In satellite communications, vulnerable telemetry channels and military communication channels will find a high-end solution in this approach ([18]).

CH-CDMA / CH-SS can be a candidate for future military standards in the STANAG family. Although it might be oversized for peace-time communications, it does not degrade high-bandwidth performance. The SDR concept is still flexible, to switch between civil protocols, LPD/LPI and antijamming modes. CH-CDMA offers high-grade physical layer security for national as well as multinational closed user groups. Physical layer security is not the only mean of securing wireless links, but it is a valuable component and complement of a multi layer security concept.

REFERENCES

[1] Hermanns, F., “Code-Hopping CH-CDMA als Link-Security-Erweiterung von Kryptokommunikationsprotokollen in Funkübertragungssystemen,” Phd Work in Progress (unpublished).

[2] Zhang, M., Carroll, C., and Chan, A., “Analysis of IS-95 CDMA Voice Privacy,” *Seventh Annual Workshop on Selected Areas in Cryptography, Ontario/Canada*, Springer, Aug. 2000.

[3] Simon, M. K., Omura, J. K., Scholtz, R. A., and Levitt, B. K., *Spread Spectrum Communications Handbook*, McGraw-Hill, 1994.

[4] Löhlein, B., “Attacks based on Conditional Correlations against the Nonlinear Filter Generator,” Cryptology ePrint Archive, Report 2003/020, 2003.

[5] Murphy, S. and Robshaw, M. J. B., “Essential Algebraic Structure within the AES,” *Advances in Cryptology - CRYPTO 2002, 22nd Annual International CryptologyConference*, Vol. 2442, IACR, Springer, Aug. 2002.

[6] Barkan, E., Biham, E., and Keller, N., "Instant Ciphertext-Only Cryptanalysis of GSM Encrypted Communication," *CRYPTO 2003 - The 23rd Annual International Cryptology Conference*, IACR, Springer, Aug. 2003.

[7] Køien, G. M., "An introduction to access security in UMTS," *IEEE Wireless Communications*, Feb. 2004.

[8] Damen, J. and Rijmen, V., "American Encryption Standard AES / FIPS 197," .

[9] Damen, J. and Rijmen, V., *The Design of Rijndael – AES - The Advanced Encryption Standard*, Springer, 2002.

[10] Schneier, B., *Applied Cryptography*, Addison-Wesley, 1996.

[11] CAST Inc., "AES hardware designs in VHDL, Verilog RTL & EDIF, up to 4.64 Gbit/sAES-128 bandwidth," .

[12] Skoda, M., *Modelling and Simulation of a Secure Spread-Spectrum Transmission System*, Master's thesis, DLR Oberpfaffenhofen and Technical University Hamburg-Harburg, Oct. 2004.

[13] Hermanns, F., "Gesichertes Spread-Spectrum-Nachrichtenübertragungssystem," mar 2006, Patent Nr. DE102004013884.

[14] Jun, B. and Kocher, P., "The Intel® Random Number Generator," Cryptography Research Inc., April 1999.

[16] Abel, A. and Schwarz, W., "Chaos Communications - Principles, Schemes and System Analysis," *Proceedings of the IEEE*, Vol. 90, No. 5, May 2002, pp. 691–710.

[17] Rulkov, N. F., Sushchik, M. M., Tsimring, L. S., and Volkovskii, A., "Digital communication using chaotic-pulse-position modulation," *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications*, Vol. 48, No. 12, Dec. 2001, pp. 1436–1444.

[15] Larson, L. E., Tsimring, L. S., and Liu, J. M., *Digital Communications Using Chaos and Nonlinear Dynamics*, No. ISBN: 0387297871, Springer, Institute for Nonlinear Science, University of California, Los Angeles (UCLA), 3 2006.

[18] Heinz Schulte (Ed.), Frank Hermanns, et al., *Vom LAN zum Kommunikationsnetz - Systeme und Applikationen*, No. ISBN: 3-8245-3502-5, Interest-Verlag, Augsburg, 2006.