Towards a Cryptanalysis of Spectral-Phase Encoded Optical CDMA with Phase-Scrambling

Sharon Goldberg*, **Ronald C. Menendez**†, **Paul R. Prucnal***

* *Department of Electrical Engineering, Princeton University, Princeton, NJ, 08544*
† *Telcordia Technologies, Applied Research, One Telcordia Dr., Piscataway, NJ, 08854*
goldbe@princeton.edu

Abstract: We show how an eavesdropper with a small amount of knowledge about the traffic sent via a spectral-phase optical CDMA system with phase-scrambling can break the confidentially of certain systems within a few bit intervals.

OCIS codes: (060.4250) Networks; (060.4510) Optical communications

Optical CDMA (OCDMA) [1] is a particularly attractive alternative to traditional digital encryption because it has the potential to perform encryption at ultra-high data rates by initializing passive optical components ($e.g.$ phase masks, delay lines) according to a secret key that needs only occasional updates. To be a viable alternative to digital encryption, OCDMA systems should maintain data confidentiality even when these optical components are reconfigured ($i.e.$ the key is refreshed) at rates much slower than aggregate system data rates. We focus on spectral-phase-encoded OCDMA systems using phase-scrambling [2, 3], which have emerged as the leading proposal for providing data confidentiality at the physical layer. Typical OCDMA schemes require some orthogonality between codewords and are therefore restricted to use codes with low cardinality [4, 5]. These schemes are therefore vulnerable to brute force searches by an eavesdropper who cycles through all possible codewords in an effort to find one that results an ungarbled datastream. On the other hand, a spectral-phase scrambling scheme offers a keyspace that grows *exponentially* with the number of frequency bins used, so that brute-force searches can be made infeasible. We assume that the *secret key* used in the system is the setting of the phase-scrambler, and analyze this system using the assumptions of cryptanalysis [6]. In particular, we explore *known plaintexts attacks* in which an eavesdropper obtains the encryption of some set of known messages, and uses this information to learn the secret key. Our first contribution is to show circumstances in which confidentiality is determined by the parallelism ($i.e.$ the number of users) in the system, rather than by the number of frequency bins used for encoding. Our next contribution is to show that even when some systems are highly parallelized ($i.e.$ have a large number of users), an eavesdropper can still learn the key with high probability after only two bit intervals. Our results thus far suggest that to maintain confidentiality when the secret key is the phase-scrambler setting, components should be tuned at rates comparable to the system data rates.

System Overview: In spectral-phase-encoded OCDMA, pulse streams are encoded by adjusting the phase of their frequency components using all-optical pulse shaping techniques. For each optical pulse, the encoding process consists of dividing the pulse spectrum into W frequency bins, applying one of C possible discrete phase shifts at each frequency (as prescribed by the choice of codeword), and recombining the frequency bins to produce the coded pulse. Decoding is achieved in a similar manner, by applying inverse phase-shifts at each frequency bin [1]. We envision a scheme where a group of N time-synchronized OCDMA users ($i.e.$ transmitter-receiver pairs) simultaneously share a waveband of a single optical fiber (that may then be overlayed onto a WDM network, or shared by another group OCDMA of users). Each user's encoded pulse train is passively coupled onto the waveband, transmitted along the fiber, and then the superposed encoded pulse trains are passively split and individual pulse streams are recovered at each decoder. To prevent energy detection attacks on on/off keyed OCDMA [5], we consider 2-code keyed (2CK) systems where each user uses a 'bright' codeword to send a '1' bit, and a different 'dark' codeword to send a '0' bit. (Other constant-energy modulation formats such as phase-shift keying are also possible.) Spectral phase OCDMA systems use orthogonal code families to reduce multiple access interference [1], so that number of available codewords is typically limited to W, making the system vulnerable to brute force attacks. To eliminate this vulnerability, an additional scrambling (descrambling) encoder that can take on any of C^W possible spectral-phase settings, is placed immediately after the coupler (before the splitter) as in Fig. 1. We assume that the setting of the shared scrambler is the secret key that is used to prevent an eavesdropper from understanding the messages sent along the OCDMA waveband [2, 3]. Since there are now C^W (as opposed to just W) possible keys, when W is large (say $W \approx 70$) a simple brute force search through the keyspace is no longer feasible. Finally, to avoid attacks on a link carrying only a single user's encoded pulse stream [5, 7], links between each transmitter and the passive coupler are physically secured so that an eavesdropper can only tap the line between the scrambler and descrambler. We can expresses the field of the scrambled superposition of n encoded codestreams at the eavesdropper's tap as $\chi(t) = \sum_{j=1}^{N} \sum_{i=1}^{W} \cos(f_i t + \theta_{i,j}(t) + \phi_j(t) + k_i)$ where f_i is the the frequency of the i^{th} frequency bin, and $\theta_{i,j}(t)$ is the phase shift applied on the i^{th} frequency bin according to the particular codeword sent by user j during the bit interval containing time t, k_i is the phase setting of the i^{th} frequency bin in the scrambler (which we assume remains the same for the duration of the eavesdropper's attack), and ϕ_j is the *randomly time-varying* phase shift of user j's encoded pulse stream relative to all other other users' encoded pulse streams caused by variations in the lengths of the fibers between user j's transmitter and the passive coupler, and time-varying fluctuations in laser intensity or temperature.

Background - Encryption Schemes: An encryption scheme uses a secret key to encrypt a plaintext message to a ciphertext. When analyzing an encryption scheme, it is standard practice to apply Kerckhoffs' Principle [6], which states that that a cryptosystem should be secure even if everything about the system, except from the secret key, is *public knowledge*. We now enumerate some standard cryptanalytic attacks on encryption schemes, ranked in order of increasing difficulty for the eavesdropper: (a) *Ciphertext Only Attacks (COA):* The eavesdropper obtains a set of ciphertexts, and uses these to learn the secret key. (b) *Known Plaintext Attacks (KPA):* The eavesdropper *knows* some set of plaintexts and obtains the corresponding ciphertexts, and uses these to learn the secret key. (c) *Chosen Plaintext Attacks (CPA):* The eavesdropper has the capability to *choose* plaintexts to be encrypted and obtains the corresponding ciphertexts, and uses these to learn the secret key. (Note that once the eavesdropper learns the key, she has completely broken the system since she is able to decrypt all ciphertexts.) Since the COA-attack is the easiest attack for the eavesdropper to perform, a scheme that is secure against COA-attacks ($i.\,e.$ COA-secure) is less secure than a scheme that is KPA-secure. Thus, while COA-security is the weakest form of security, to date it is the only form of security considered in the literature on OCDMA [3, 4, 5, 7]. Note the *minimal* threshold for security of standard digital encryption schemes is the ability to withstand CPA-attacks ($e.g.$ [8] §3.2.1.) In this paper, we focus on KPA-attacks. The KPA-attack is a realistic threat, since data traffic is never completely random; it contains packet headers, 'hello' packets, or framing elements ($e.g.$ SONET framing) that are publicly known and may be used to launch a KPA-attack.

Security Parameters of System: Recall that N is the number of OCDMA users, W is the number of frequency bins used for OCDMA encoding, and C is the number of discrete phase shifts possible at each frequency bin. In this paper, we assume that for the system in Fig. 1, the set of 'bright' and 'dark' codewords assigned to each OCDMA user is *not* part of the secret key. (Note that schemes in which codewords assigned to each user are also kept secret are possible as well [2].) Therefore, by Kerckhoffs' principle, we assume that this information is known to the eavesdropper. Then, for each bit-interval, instead of defining the *plaintext* as the bits transmitted by each of the N users during that bit-interval, we define the plaintext as the set of *codewords* transmitted by each of the N users during that bit-interval. (For ease of exposition, assume that encoders and scramblers are restricted to use binary phase shifts of $0, \pi$.) We represent the plaintext as an $W \times N$ $\{0, \pi\}$-matrix Θ, where entry $\theta_{j,i}$ gives the phase shift applied to frequency bin i corresponding to the codeword send by user j. The *secret key* is the set of W phase shifts $k_i \in \{0, \pi\}$ applied by the scrambler at frequency bin i. The ciphertext is $\chi(t)$, the optical signal seen at the eavesdropper's tap. We assume that the eavesdropper detects the ciphertext $\chi(t)$ using optical beat detection [5, 9] by passing $\chi(t)$ through a demultiplexer to obtain $\chi_i(t)$ for $i = 1, ..., W$ (where $\chi_i(t)$ is $\chi(t)$ filtered at i^{th} frequency bin). By interfering each $\chi_i(t)$ with a local oscillator signal $\cos(f_i t)$ and then detecting $\chi_i(t) + \cos(f_i t)$ with a photodetector that operates a square law device with envelope detection, she obtains a *measurement* of the form $y_i(t) = \sum_{j=1}^{n} \cos(\theta_{i,j}(t) + \phi_j(t) + k_i)$. Thus, the eavesdropper has a total of W equations, (one equation for each of the W measurements y_i). In this paper we assume that the eavesdropper makes perfect *noise-free* measurements of the y_i's, and use this assumption to discover the vulnerabilities of the system. Our future work will discuss the effect of noise in the eavesdroppper's measurements.

Size of Brute Force Search Space in a KPA attack: If the eavesdropper in the COA setting attempts to learn *all* W elements of the key, then the strongest attack shown by [2, 3] on a system with $N > 1$ users is to have the eavesdropper do a brute force search through a space of size C^W . Thus, in the COA setting, when W is large (say $W > 70$) an exhaustive search to learn all W elements of the key becomes infeasible (since $2^{70} \approx 10^{20}$). However, consider now eavesdropper with *one known plaintext* Θ and corresponding beat detection measurement vector $\mathbf{y} = [y_1 \; .... \; y_N]$. Then the eavesdropper has a system of W equations with $W + N$ unknowns ($i.\,e.$ W unknown key elements $\mathrm{k} = [k_1 \; ... \; k_W]$, and N unknown inter-user phases $\phi = [\phi_1 \; ... \; \phi_N]$). She can use these equations to reduce the size of her search space. Since the eavesdropper knows the θ_{ij}, she may guesses N elements of the key and use N of her equations to obtain a guess $\widehat{\phi}$ for the N-vector of inter-user phases. She can then use $\widehat{\phi}$ to solve the other $W - N$ equations for the remaining $W - N$ key elements. Because the eavesdropper need only guesses only N elements of k, *in the KPA-setting, the size of the space in an exhaustive search for* all w *elements of the key is* C^N.[1] That is, confidentiality is determined by the the amount of parallelism in the system, (the number of parallel OCDMA users N), rather than by the number of frequency bins W used for in encoding. This can be significant reduction in the key search space, since systems are typically designed so that $N < W$ ($e.g.$ in 2CK with orthogonal codes $N \leq \frac{W}{2}$). As an example, in the KPA-setting, a system using a large number of frequency bins $W = 70$ but only a small number of users $N = 4$ has a key search space of size only $2^4 = 16$ rather than 2^{70}, as implied by [2, 3].

KPA Attack to Learn Key with 2 Known Plaintexts: Even when the system is highly parallelized so that N is large enough to prevent brute force attacks (say $N \approx 70$ users), we now present another KPA-attack that eavesdropper can use reduce the size of the key search space from C^N to an even smaller set of possibilities. Suppose the eavesdropper obtains *two known plaintexts* and corresponding measurements $(\Theta_1, \mathbf{y}_1), (\Theta_2, \mathbf{y}_2)$. Then the eavesdropper has $2W$ equations and $W + 2N$ unknowns, that can be solved for the W elements of the key (when $N \leq \frac{W}{2}$). *We show in [10] that the eavesdropper's key search space is reduced from* C^N *to the set of solutions to this system of* $2W$ *equations. Furthermore, if there is a unique solution to these* $2W$ *equations then the eavesdropper immediately learns the key.*

To quantify the size of the key search space after solving these $2W$ equations, we have done a detailed analysis in [10] of a N-user system using 2-code-keying with $W = 2N$ frequency bins and the standard $2N$-Hadamard codes, where key and codewords elements can take on binary phases ($C = 2$). We present in Fig. 2 the probability (over all possible combinations of known plaintexts Θ_1, Θ_2) of the existence of a unique solution to to the system of $2W$ equations (so that the eavesdropper learns the key immediately by solving these equations) . We can see, for example, that when $N = 8$ users, then over 95% of known plaintexts pairs result in a unique solution. Fig. 2 further shows that as N increases, the probability that an eavesdropper with arbitrary pair of known plaintexts will immediately learn the key (because of the existence of a unique solution) increases as well. Finally, to generalize to an arbitrary number of users N, we used linear algebra to prove that for any N, *at least* 75% of all possible known plaintexts pairs Θ_1, Θ_2 will result in a unique solution to the $2W$ equations. Taken together, our results indicate that an eavesdropper with an *arbitrary* pair of known plaintexts has a very high probability of learning the key.

Future Work: In future papers we will study how noise in measurements $\mathbf{y}_1, \mathbf{y}_2$ affects our KPA-attacks. Other interesting directions include analyzing systems using other modulation schemes (instead of 2-code keying), or OCDMA spreading codes (instead of the standard Hadamard codes), or when *both* the scrambler setting and the codewords assigned to users are kept secret and refreshed periodically ($e.g.$ codewords could be assigned from one of $W!$ instantiations of the Hadamard codes (see [2] §VII), where the instantiation chosen would be kept secret).

Conclusions: When analyzing the confidentiality provided by OCDMA systems, we have demonstrated the importance of formulating security analyses using standard cryptanalytic notions ($e.g.$ Kerckhoffs' Principle, KPA-attacks), particularly if these systems are to present a viable alternative to standard digital encryption schemes. Moreover, the existence of the attacks we describe here suggest that *spectral-phase encoded OCDMA systems that use* only *the phase scrambler setting as a secret key are unlikely to guarantee confidentiality, unless the key is refreshed at rates comparable to the system data rates*. Other variants of OCDMA ($e.g.$ when user codewords and scrambler settings are both secret) may or may not be secure. Determining the confidentiality of these variants is left for future work.

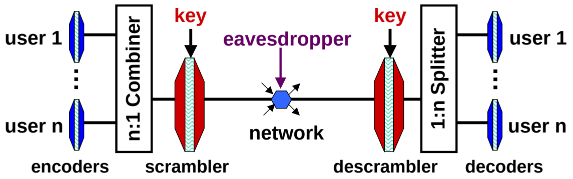

Fig 1. System overview

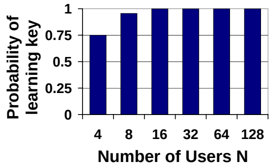

Fig 2. KPA Attack with 2 known plaintexts

Fig 2. shows relationship between number of users N and probability, over all possible known plaintexts pairs, of eavesdropper learning key (due to existence of unique solution to system of $2W$ equations). For $N \geq 16$ probabilities obtained from 10000 randomly sampled plaintext pairs.

Parts of this work were supported by the DARPA O-CDMA project under contracts MDA972-O3-C-0078 and MDA972-03-1-0006. Any opinions, findings and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of DARPA.

References

1. P.R. Prucnal, Ed. "Optical Code Division Multiple Access : Fundamentals and Applications", New York: Taylor and Francis, 2005.
2. R. Menendez et. al., "Network Applications of Code Translation for Spectrally Phase-Encoded OCDMA", *J. Lightwave Technol.*, Oct. 2005.
3. F. Xue et. al., "Security Issues on Spectral-Phase-Encoded Optical CDMA with Phase-masking Scheme", OFC 2006.
4. T. H. Shake, "Security Performance of Optical CDMA Against Eavesdropping", *J. Lightwave Technol.*, Feb. 2005.
5. T. H. Shake, "Confidentiality Performance of Spectral-Phase Encoded Optical CDMA", *J. Lightwave Technol.*, April 2005.
6. N. Ferguson and B. Schneier, *Practical Cryptography*, Indianapolis, IN: Wiley, 2003
7. J. Jiang et. al. "Experimental Investigation of Security Issues in OCDMA", OFC 2006.
8. J. Nechvatal et. al., "Report on the Development of the Advanced Encryption Standard (AES)" , NIST, Oct. 2000.
9. A. Agarwal et. al, "Ring-Resonator-Based Integrated Photonic Circuit for Phase Coherent Applications"*J. Lightwave Technol.*, Jan 2006.
10. S. Goldberg et. al. Princeton University Dept. of Computer Science, Technical Report, 2006.

[1] Note that noisy measurements $\tilde{\mathbf{y}}$ will result in noisy guesses for the $W - N$ key elements obtained by solving the W equations. However, an eavesdropper with multiple known $(\Theta, \tilde{\mathbf{y}})$ pairs can usually limit her search space to C^N taking a majority vote over the noisy guesses [10].