Dense Parity Check Based Secrecy Sharing in Wireless Communications

Sheng Xiao, Hossein Pishro-Nik, Weibo Gong
Department of Electrical and Computer Engineering
University of Massachusetts, Amherst
Amherst, Massachusetts 01375

Abstract—**It is generally believed harmful to have transmission errors in the wireless communications. The high decoding complexity of dense parity check codes is unfavorable. This paper proposes to apply these two ”negative” facts to enable the secrecy sharing with the information theoretical security. We claim that the secrecy sharing is always possible if the wiretap channel is not error-free, regardless of the main channel performance. Particularly, the proposed secrecy sharing protocol can provide provable and testable security using the existing wireless technologies.**

Index Terms—**wireless security, parity check code, wiretap channel model, information theoretical security**

I. Introduction

A. Motivation

A fundamental problem in the security research is: when only the public communication channel is available, how to share some secrecy between the legitimate users. The vast deployment of wireless applications brings more challenges to us. The broadcasting nature enables almost zero-cost eavesdropping. The mobility makes it difficult to pre-configure for the secret key cryptography. In practice, the public key cryptography (PKC) is used to establish a computationally secure channel for the initial secret key exchange, then other secret key based cryptography protocols could be functional. However, if the privacy is only guarded by the computational barrier, the adversary always can ”save” the cipher text and wait for the advancement of computing technology, the novel reverse algorithms or the reveal of protocol implementation flaws.

Hence, a secrecy sharing protocol which can provide the provable security would be highly desirable for the wireless communications. A general purpose, theoretically beautiful solution might be very difficult because it had been proved that given an unrestricted adversary full control of the communication channel, a robust secrecy sharing protocol is not possible [1].

By restricting the adversary’s storage capacity, Maurer proposed the bounded storage model (BSM) which provides provable unconditional security [2]. This model is very elegant but hard to implement mainly because the storage technology advancement makes it is infeasible to generate and transmit such a huge amount of random bits. By defining the channel with quantum effects and using single photon sources, the quantum key distribution (QKD) offers information theoretical security. It is not implemented in most wireless environments because of high cost on wireless quantum transceivers and the unrealistically short applicable range when channel noise presents.

The previous research motivates us to seek a method by restricting some easily testable aspects on the adversary, use off-the-shelf technologies, to achieve information theoretical security for the secrecy sharing. The modern wireless communication researches stimulate a counter-intuitive direction.

In most wireless communication occasions, SNR limitation and complex multipath effects cause the transmission errors very hard to reduce. In the channel coding area, researchers are dedicating to make the best use of the redundancy to recover transmission errors. In this paper, we follow the reverse direction. We can force the eavesdropper to have inevitable errors by restricting transmission power, choosing vulnerable modulations or even actively jamming. We have the testability by measuring the noise and interference. If the channel coding is only effective on error detection but not capable of recovering the error, then the legitimate users can keep those reliably received information to build the agreement. As long as the eavesdropper can not receive the exactly identical information as the legitimate users, he or she is guaranteed to suffer from the information loss regardless of the computing power or algorithm advantage. Therefore, it is possible to build the secrecy sharing protocol based on the error measurement and the detectable but non-correctable channel coding.

To release the worry that the eavesdropper might receive identically with the legitimate users, the electromagnetic wave propagation theory states that when the receivers are physically apart more than half of the carrier wave length, their errors would be considered as independent. There are experiment results on $2.4GHz$ networks that verifies the theory [3].

B. Related Works

This paper is an interdisciplinary research. It is motivated and built on many previous research milestones.

In the security research domain, Wyner proposed the wiretap channel as a simple, highly abstract yet effective model to illustrate the information theoretical security capacity when the eavesdropping exists [4].

As shown in fig. 1, the legitimate users Alice and Bob communicate through the main channel and the eavesdropper

1930-529X/07/$25.00 © 2007 IEEE
This full text paper was peer reviewed at the direction of IEEE Communications Society subject matter experts for publication in the IEEE GLOBECOM 2007 proceedings.

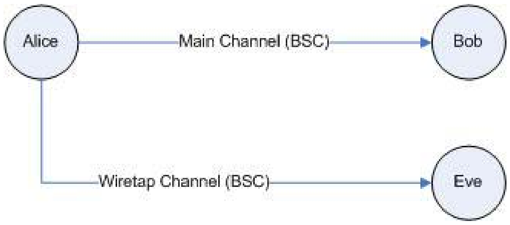

Fig. 1. the wiretap channel model

Eve listens via the wiretap channel. Both channels are discrete memoryless channels (DMC). This model can represent general wireless eavesdropping scenarios because most of the time, eavesdropper would be far away from the legitimate user (far more than half carrier wave length).

Wyner concludes the relationship between the upper bound of secrecy sharing rate and the channel capacities as

$$C_S = \begin{cases} C_M - C_W & C_M > C_W \\ 0 & C_M \leq C_W \end{cases} \tag{1}$$

C_S is the secrecy capacity. C_M and C_W are the main channel capacity and the wiretap channel capacity respectively.

This conclusion is discouraging because it implies that the secrecy sharing is only feasible when the wiretap channel is worse than the main channel which is difficult to guarantee in practice.

Maurer improved this model by introducing public discussions and repeating bits transmission [5]. In the physical layer, Barros and Rogdrigues proposes that the variation of physical layer errors could produce positive secrecy capacity [6]. Cooperating with them, Bloch and Mclaughlin proposes a physical layer approach in the quasi-static fading channels for secure key agreement[7].

In the channel coding research domain, unlike the prominent low density parity check (LDPC), dense parity check is not favorable because the error propagation prevents the possibility of iterative decoding and the maximum likelihood decoding is an NP-complete problem [8].

This paper is built on these important research results. We propose a protocol that could produce information theoretical security in the wireless communications. Not only the theoretical bound is concretely proved, but also the protocol could be easily implemented with the publicly available wireless technologies. We will focus on the binary symmetric channel (BSC) instead of general DMC in this paper for the calculation of the secrecy capacity.

II. The Secrecy Sharing Protocol

We use the traditional Alice, Bob and Eve scenario to describe the protocol. The concepts and techniques used in the protocol are formally defined immediately after the framework, then the secrecy capacity of this protocol is proved.

Protocol Framework

1) Alice and Bob agrees on the (n, R) equiprobable parity check codes and other parameters which will be used in the secrecy sharing process.
2) Alice generates a set of uniformly distributed binary sequences and encodes them as $\mathbf{t}_1, \mathbf{t}_2, \cdots$ to transmit.
3) Bob receives the transmitted codewords as $\mathbf{r}_1, \mathbf{r}_2, \cdots$
4) According to the expecting security threshold, Bob keeps m correctly received binary sequences $\mathbf{r}_{k(1)}, \mathbf{r}_{k(2)}, \cdots, \mathbf{r}_{k(m)}$ and broadcasts the index set $\{k(1), k(2), \cdots, k(m)\}$ repeatedly until Alice confirms completely correctly received it.
5) Alice uses privacy amplification techniques to distill a secrecy $\mathbf{s}_A$ from
$$\mathbf{t}_{k(1)}, \mathbf{t}_{k(2)}, \cdots, \mathbf{t}_{k(m)}$$
6) Bob uses privacy amplification techniques to distill a secrecy $\mathbf{s}_B$ from
$$\mathbf{r}_{k(1)}, \mathbf{r}_{k(2)}, \cdots, \mathbf{r}_{k(m)}$$

$\mathbf{s}_A$ and $\mathbf{s}_B$ are equal with very high probability and the information leak to the adversary is lower bounded.

This protocol framework is very similar to the quantum key distribution. They share the same three steps: transmission, data reconciliation and privacy amplification. We call our protocol *Poor's QKD*. The difference is that our protocol works on codewords while QKD works on qubits. Our protocols requires no expensive quantum instruments but uses the natural noise and interference.

It is noteworthy that the legitimate users do not need to face the decoding complexity problem of the equiprobable parity codes. They just use the privacy amplification techniques to compress the received strings.

A. Equiprobable Parity Check Codes

Among all dense parity check codes, the equiprobable parity check codes is of our interests. For the simplicity, we define the codes in the systematic form. The equivalent codes to the system form codes are equiprobable parity check codes too.

The systematic form of the generation matrix M_G for the (n, R) equiprobable parity check codes is

$$M_G = \left[\ I_{nR}\ M\ \right] \tag{2}$$

I_k represent the k by k identity matrix. The M inside M_G is an nR by $n(1-R)$ matrix. It is filled with statistically independent equiprobable binary bits (e.g. all of its bits are i.i.d. with equal probability of being 0 or 1). .

It is trivial to show that the corresponding parity check matrix would be

$$M_H = \left[\begin{array}{c} M \\ I_{n(1-R)} \end{array} \right] \tag{3}$$

The equiprobable parity check codes have two important properties: the lower bounded equivocation after transmission in BSC channel and the upper bounded false negative probability.

By defining

- $\mathbf{t}$ row vector for the transmitted codeword
- $\mathbf{r}$ row vector for the received binary sequence
- Ω the codeword set

- p_e the bit transition probability of the BSC channel

we have the following two theorems.

Theorem 1 (lower bounded equivocation): With two supplement functions[1]

$$h(x) = x \log x + (1-x)\log(1-x) \tag{4}$$

$$\phi_k(x) = \frac{1 + (1-2x)^k}{2} \tag{5}$$

the equivocation of $\mathbf{t}$ given $\mathbf{r}$ is lower bounded by

$$H(\mathbf{t}|\mathbf{r}) \geq nh(p_e) - n(1-R)h(\phi_{nR+1}(p_e)) \tag{6}$$

Proof:

$$\begin{aligned} H(\mathbf{t}|\mathbf{r}) &= H(\mathbf{t},\mathbf{r}) - H(\mathbf{r}) \\ &= H(\mathbf{t},\mathbf{t}\oplus\mathbf{r}) - H(\mathbf{r}) \\ &= nR + nh(p_e) - H(\mathbf{r}) \end{aligned} \tag{7}$$

We then divide $\mathbf{r}$ into two parts

$$\mathbf{r} = \begin{pmatrix} \mathbf{r}_s & \mathbf{r}_c \end{pmatrix} \tag{8}$$

$\mathbf{r}_s$ is the first nR bits and $\mathbf{r}_c$ is the rest $n(1-R)$ bits. Let $r_c^{(i)}$ represent the i^{th} bits of $\mathbf{r}_c$. We interpret $H(\mathbf{r})$ as

$$\begin{aligned} H(\mathbf{r}) \quad = H(\mathbf{r}_c, \mathbf{r}_s) \quad &= H(\mathbf{r}_c) + H(\mathbf{r}_c|\mathbf{r}_s) \\ &\leq nR + H(\mathbf{r}_c|\mathbf{r}_s) \\ &\leq nR + \sum_{i=1}^{n(1-R)} H(r_c^{(i)}|\mathbf{r}_s) \end{aligned} \tag{9}$$

The second $\leq$ is because the overlapping of parity check set can only reduce the uncertainty of $\mathbf{r}$.

Let $M^{(i)}$ represent the i^{th} column in the random matrix M as defined in equation (2) and (3). $k(i)$ is the number of 1s in $M^{(i)}$.

$$\begin{aligned} H(r_c^{(i)}|\mathbf{r}_s) &= E_{\mathbf{r}_s \in \{0,1\}^{nR}}[H(r_c^{(i)}|\mathbf{r}_s)] \\ &= E_{\mathbf{r}_s \in \{0,1\}^{nR}}[h(p(r_c^{(i)} = \mathbf{r}_s M^{(i)}|\mathbf{r}_s))] \\ &= h(\phi_{k(i)+1}(p_e)) \\ &\leq h(\phi_{nR+1}(p_e)) \end{aligned} \tag{10}$$

The third equality is because M is a equiprobable random binary matrix, $p(r_c^{(i)} = \mathbf{r}_s M^{(i)}|\mathbf{r}_s)$ is the probability of even number of bit errors occur in this parity check set and this probability is unchanged for any $\mathbf{r}_s \in \{0,1\}^{nR}$.

The last $\leq$ is because $h(\phi_k(p))$ is monotonically increasing with k and $k(i) \leq nR$.

Combining the equation (7), (9) and (10), we have

$$H(\mathbf{t}|\mathbf{r}) \geq nh(p_e) - n(1-R)h(\phi_{nR+1}(p_e)) \tag{11}$$

Theorem 1 is proved. ■

Equation (6) illustrates that when the code rate R is high, the uncertainty about transmitted codeword $\mathbf{t}$ given received binary sequence $\mathbf{r}$ is lower bounded above zero. This is the minimum loss of information when the eavesdropper receives an error prone codeword.

Theorem 2 (upper bounded false negative probability): For the (n, R) equiprobable parity check codes, regardless of the transmission error pattern, the false negative (undetected error) probability would be upper bounded as

$$p_{ud} = p_{\mathbf{r}\in\Omega}(\mathbf{t} \neq \mathbf{r}) \leq 2^{-n(1-R)} \tag{12}$$

Proof: Define the error vector

$$\mathbf{e} = \mathbf{t} \oplus \mathbf{r} = \begin{pmatrix} \mathbf{e}_s & \mathbf{e}_c \end{pmatrix} \tag{13}$$

$\mathbf{e}_s$ contains the first nR bits of $\mathbf{e}$ and $\mathbf{e}_c$ is the later part.

According to equation (3), the syndrome is

$$\mathbf{s} = \mathbf{e}M_H = \mathbf{e}_s M \oplus \mathbf{e}_c I_n(1-R) \tag{14}$$

When $\mathbf{s} = 0$, the received binary sequence is believed to be correct. Hence

$$\mathbf{e}_s M = \mathbf{e}_c \tag{15}$$

There are three possible error types:

1) $\mathbf{e}_s = 0$, $\mathbf{e}_c \neq 0$
2) $\mathbf{e}_s \neq 0$, $\mathbf{e}_c = 0$
3) $\mathbf{e}_s \neq 0$, $\mathbf{e}_c \neq 0$

Type 1) error will bring non-zero syndrome and always can be detected.

For type 2) and 3) errors, we rewrite equation (15) to an equation array.

$$\begin{cases} \mathbf{e}_s M^{(1)} & = e_c^{(1)} \\ & \vdots \\ \mathbf{e}_s M^{(i)} & = e_c^{(i)} \\ & \vdots \\ \mathbf{e}_s M^{(n(1-R))} & = e_c^{(n(1-R))} \end{cases} \tag{16}$$

M is an equiprobable random binary matrix. $M^{(i)}$ is a random binary string picked from $\{0,1\}^{nR}$. Therefore no matter what the values of $\mathbf{e}_s$ and $e_c^{(i)}$ are, $p(\mathbf{e}_s M^{(i)} = e_c^{(i)}) = \frac{1}{2}$. Because each equation in the array (16) is independent to the others, the probability of all equations in (16) are satisfied would be $2^{-n(1-R)}$. According the above analysis we have

$$p_{ud} = p(\mathbf{t} \neq \mathbf{r}|\mathbf{r} \in \Omega) \leq 2^{-n(1-R)} \tag{17}$$

Theorem 2 is proved. ■

B. Privacy Amplification

The privacy amplification is a matured topic in the cryptography research. There are many literatures explaining this technique in details such as [9], [10] and [11]. In general, it is shortening the message strings to defend potential information leaking.

To be more specific, When Eve's information about the original message X is limited by $n - r$ bits, Alice and Bob could publicly choose a compression function $g : \{0,1\}^n \rightarrow \{0,1\}^r$ such that Eve has arbitrarily little information about $g(X)$ with overwhelming probability.

[1] If not specified, all log functions in this paper are base-2.

1930-529X/07/$25.00 © 2007 IEEE

C. Provable Security

Take a closer look at equation (1), it could be rewritten as

$$\begin{aligned} C_S &= \max\{C_M - C_W, 0\} \\ &= \tfrac{1}{n}\max\{\max_{p(\mathbf{t})} I(\mathbf{t};\mathbf{r}_M) - \max_{p(\mathbf{t})} I(\mathbf{t};\mathbf{r}_W), 0\} \end{aligned} \tag{18}$$

It is a general result for the one-directional transmission for all possible distribution $p(\mathbf{t})$. However, in our protocol, the legitimate users could choose certain $p(\mathbf{t})$ and certain $\mathbf{t}$ in their favor. The eavesdropper is forced to work with their choices.

When $p(\mathbf{t})$ is given, the secrecy capacity of our protocol in BSC wiretap channel model is

$$C_S = \frac{1}{n}\max\{H(\mathbf{t}|\mathbf{r}_W) - H_{\mathbf{r}_M \in \Omega}(\mathbf{t}|\mathbf{r}_M), 0\} \tag{19}$$

$\mathbf{r}_M$ and $\mathbf{r}_W$ are the received binary sequence of Bob and Eve respectively.

Let $p_{e,E}$ represent the bit transition probability of the wiretap channel, p_{ud} represent the false negative probability of the codes and recalling equation (4) and (5). We have the following theorem on the secrecy capacity.

Theorem 3 (protocol secrecy capacity): Regardless of the performance of the main channel, the secrecy capacity is lower bounded by the coding parameters and the performance of the wiretap channel as

$$C_S \geq \max\{h(p_{e,E}) - (1-R)h(\phi_{nR+1}(p_{e,E})) - Rp_{ud}, 0\} \tag{20}$$

Proof: According to equation (6), we have

$$H(\mathbf{t}|\mathbf{r}_W) \geq nh(p_{e,E}) - n(1-R)h(\phi_{nR+1}(p_{e,E})) \tag{21}$$

Referring to equation (12), the equivocation of $\mathbf{t}$ by $\mathbf{r}$ given $\mathbf{r}_M \in \Omega$ would be

$$\begin{aligned} & H_{\mathbf{r}_M \in \Omega}(\mathbf{t}|\mathbf{r}_M) \\ &\quad = E_{\mathbf{r}_M \in \Omega}[-\log p(\mathbf{t}|\mathbf{r}_M)] \\ &\quad = p_{ud} E_{\mathbf{r}_M \in \Omega}[-\log p(\mathbf{t}|\mathbf{r}_M)|\mathbf{t} \neq \mathbf{r}_M)] \\ &\qquad + (1-p_{ud}) E_{\mathbf{r}_M \in \Omega}[-\log p(\mathbf{t}|\mathbf{r}_M)|\mathbf{t} = \mathbf{r}_M)] \\ &\quad \leq p_{ud} \cdot nR + (1-p_{ud}) \cdot 0 \\ &\quad = nRp_{ud} \end{aligned} \tag{22}$$

The $\leq$ is because the uncertainty about $\mathbf{t}$ would not exceed nR bits; when $\mathbf{r}_M \in \Omega$ and the false negative detection does not occur, the equivocation would be zero.

Substitute equation (21) and (22) into equation (19), we have equation (20).

Theorem 3 is proved. ∎

Equation (20) clearly shows that when R is approaching 1 and p_{ud} is small (n large), the secrecy capacity is guaranteed to be positive if the eavesdropper's bit error probability is not zero. The existence of positive secrecy capacity is irrelevant to the main channel's performance.

We illustrate the secrecy capacity lower bound on fig. 2. It almost increase linearly with n after being strictly positive.

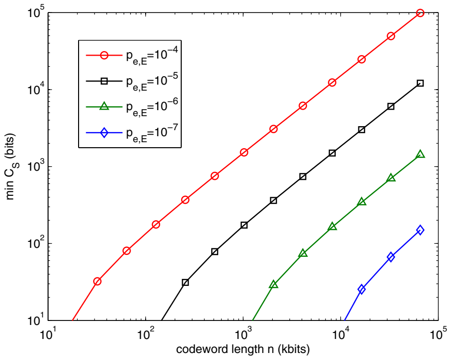

Fig. 2. C_S lower bound on various n and $p_{e,E}$ with 16 checksum bits

Even the eavesdropper also gains benefit from the error detection, the probability for the eavesdropper to correctly receive all legitimate user selected codewords is exponentially decreases with m. The probability of the eavesdropper has k out of m erroneous binary sequences are

$$p_k = \begin{pmatrix} m \\ k \end{pmatrix} (1-p_{e,E})^{n(m-k)}(1-(1-p_{e,E})^n)^k \tag{23}$$

The expectation number of the eavesdropper's erroneous codewords would be

$$\bar{k} = \sum_{k=0}^{m} kp_k = (1-(1-p_{e,E})^n)m \tag{24}$$

According to equation (24), one execution of the protocol can averagely share $(1-(1-p_{e,E})^n)mnC_S$ bits of secret information between Alice and Bob. However, if the main channel is bad, it takes many transmissions to accumulate m correctly received codewords.

Considering the discarded bits in both data reconciliation stage and privacy amplification stage, the secrecy capacity on the BSC-wiretap channel model would be

$$C_S^* = C_S(1-p_{e,B})^n(1-(1-p_{e,E})^n) \tag{25}$$

Here C_S is defined as in equation (19) and lower bounded by equation (20).

C_S^* in equation (25) is an average. Its instantaneous value is random due to the error randomness in wireless communications. However, the non-zero capacity of secrecy sharing is guaranteed whenever C_S is strictly positive.

D. Decoding Difficulty for the Eavesdropper

Not only the equivocation is lower bounded, but also the eavesdropper need to solve the NP-complete problem to make the redundancy useful in attempts of recovering errors from the received binary sequences.

It is extremely rare that the random parity check codes would coincidentally satisfy the iterative decoding criteria. The generation matrix would almost surely be complicated circled on the Tanner graph. The error propagation is inevitable.

It is well known that the coset weights problem for the linear block codes is NP-complete [12]. When non-zero syndrome appears, the maximum likelihood (ML) decoding can reduce to the coset weights problem. Therefore it is also NP-complete.

1930-529X/07/$25.00 © 2007 IEEE

TABLE I
TYPICAL PARAMETER SETS AND PERFORMANCES

measured bit error prob.	10^{-3}	10^{-4}	10^{-5}	10^{-6}
number of codewords to keep	32	32	32	32
checksum length (bits)	16	16	16	16
codeword length (kbits)	2	16	128	1024
Bob's bit error prob.	10^{-4}	10^{-4}	10^{-5}	10^{-6}
avg. secrecy shared (bits)	205.4	210.7	180.5	136.9
avg. total transmitted bits (Mbits)	0.48	2.57	14.83	91.3

Furthermore, there could be multiple indistinguishable solution candidates at the same Hamming weight when R is high.

This decoding complexity barrier provides us more confidence in executing the protocol because n usually would be large. The eavesdropper would need to fight against computational complexity barrier to recover its received erroneous binary sequences.

III. Practical Implementation Scenarios

Because the above proposed protocol is based on physical layer properties of the wireless communications, it is naturally capable of serving as an enhanced layer to almost all existing cryptographic systems. We can use the shared secrecy as the one time pad to protect the public key transmission, promoting the public key cryptographic system to be information theoretically secure. We can also directly use the shared secrecy as the secret key to encrypt data.

Table I shows parameter sets and performances on some typical bit error probabilities. Even for the home-use wireless LAN, the protocol would be fairly low cost.

One of the novel feature of the proposed protocol is the testability. The user need to measure the surrounding environment noise to determine the parameters. Because the signal decays proportional to at least the square of the distance to the source, this feature is essential to defend outside eavesdroppers, e.g. perimeter protection. The testability is the key to build up true confidence to the security concerns.

Another feature is that the better main channel can provide significant performance gain in the secrecy sharing. Since the legitimate users can decide the transmission scheme and utilize the active interference (jamming, antenna polarization, etc), they can always exploit these benefits to build up the privilege. Also, the racing on the receiver capability is easy to testify. It would be obviously suspicious when someone pointing a huge antenna towards the legitimate communication scenario.

This protocol requires only binary XOR and AND operations besides the common cryptographic requirement of a random number generator. It can be easily implemented in hardware and excel the computational security methods in both power consumption and speed aspects. Hence it would be suitable for resource limited situations such as the RFID security.

IV. Future Works

The equiprobable parity check codes might not be the best candidate for the detectable but non-correctable purpose. There might be codes that can more effectively utilize the error in the wiretap channel. The secrecy capacity bound is loose. There should be tighter bounds to replace the inequalities (10), (22) and (25).

We are proposing to prototype this protocol in both the mesh network using 802.11a/b/g wireless LAN and the access point based network with 802.11n and the beam-forming technology. These experiments would optimize this protocol and hopefully reveal new theoretical breakpoint.

We hope this paper can stimulate the research interests to pursue the low-cost and technology-ready solution for the provable security in wireless communications.

V. Conclusion

This paper presents an improvement to the secrecy capacity bound in the BSC-wiretap channel model with public channel feedback. The strictly positive secrecy capacity only relies on the wiretap channel performance but not the main channel. Based on the theoretical results, a secrecy sharing protocol is proposed to obtain the provable and testable security in the wireless communications. The security doesn't rely on the restriction of adversary's computing power or algorithm advantage, but the testable physical limitations. This protocol can be implemented in various applications to provide an extra layer of information theoretical security to the existing security models.

References

[1] U. M. Maurer and S. Wolf, "Secret key agreement over a non-authenticated channel - part i: Definitions and bounds," *IEEE Transactions on Information Theory*, vol. 49, pp. 822–831, 2003.

[2] C. Cachin and U. Maurer, "Unconditional security against memory-bounded adversaries," in *Advances in Cryptology - CRYPTO'97, Lecture Notes in Computer Science*, vol. 1294, 1997, pp. 292–306.

[3] L. C. Wood and W. S. Hodgkiss, "Indoor spatial correlation measurements at 2.4 ghz," in *Conference Record of the Thirty-Ninth Asilomar Conference on Signals, Systems and Computers*, 2005.

[4] A. D. Wyner, "The wire-tap channel," *Bell System Technical Journal*, vol. 54, pp. 1355–1387, 1975.

[5] U. M. Maurer, "Secret key agreement by public discussion from common information," *IEEE Trans. on Information Theory*, vol. 39, pp. 733–742, 1993.

[6] J. Barros and M. Rodrigues, "Secrecy capacity of wireless channels," in *ISIT'06 Proceedings*, 2006.

[7] M. Bloch, J. Barros, M. R. D. Rodrigues, and S. W. McLaughlin, "Wireless information-theoretic security - part i: Theoretical aspects," *IEEE Trans. on Information Theory*, 2006.

[8] R. G. Gallager, *Low-Density Parity-Check Codes*, M. Press, Ed. MIT Press, Cambridge, MA, 1963.

[9] C. H. Bennett, G. Brassard, C. Crkpeau, and U. M. Maurer, "Generalized privacy amplification," *IEEE Transaction on information theory*, vol. 41, pp. 1915–1923, 1995.

[10] U. M. Maurer and S. Wolf, "Secret key agreement over a non-authenticated channel - part iii: Privacy amplification," *IEEE Transactions on Information Theory*, vol. 49, pp. 839–851, 2003.

[11] R. Konig, U. Maurer, and R. Renner, "Privacy amplification secure against an adversary with selectable knowledge," in *ISIT'04 Proceedings*, 2004.

[12] E. Berlekamp, R. McEliece, and H. van Tilborg, "On the inherent intractability of certain coding problems," *IEEE Transactions on Information Theory*, vol. 24, pp. 384–386, 1978.

This full text paper was peer reviewed at the direction of IEEE Communications Society subject matter experts for publication in the IEEE GLOBECOM 2007 proceedings.