Journal of Information Processing Vol.23 No.5 554–561 (Sep. 2015)

[DOI: 10.2197/ipsjjip.23.554]

Invited Paper

A Model for Adversarial Wiretap Channels and its Applications

Reihaneh Safavi-Naini[1,a)] Pengwei Wang[1,b)]

Received: July 1, 2015, Accepted: July 31, 2015

Abstract: In the wiretap model of secure communication, Alice is connected to Bob and Eve by two noisy channels. Wyner's insight was that the difference in noise between the two channels can be used to provide perfect secrecy for communication between Alice and Bob, against the eavesdropper Eve. In Wyner's model, the adversary is passive. We consider a coding-theoretic model for wiretap channels with active adversaries who can choose their view of the communication channel and also add adversarial noise to the channel. We give an overview of the security definition and the known results for this model, and discuss its relation to two important cryptographic primitives: secure message transmission and robust secret sharing. In particular, we show that this model unifies the study of wiretap channels and secure message transmission in networks.

Keywords: wiretap channel, active adversary, secure message transmission, robust secret sharing

1. Introduction

In the most basic secure communication scenario, Alice wants to securely send a message m to Bob over a channel that is eavesdropped by Eve. Noise is inherent in all communication systems, and so Alice must also ensure that Bob correctly receives the message. Formal modelling and analysis of the problem of secure and reliable communication over an eavesdropped channel has two distinct solution approaches.

Shannon's approach. Shannon [1] proposed a two-step solution, wherein the first step Alice and Bob remove the noise from the channel and construct a reliable channel from Alice to Bob. To formalize this step, Shannon founded information theory, modelled a noisy channel, and defined the capacity of a channel as the highest rate of error-free transmission over the channel. Modelling a channel requires estimating the noise in the channel (i.e., finding channel transition probability) and using this estimate to employ an appropriate error-correcting code. In the second step, once a reliable channel between Alice and Bob is established, Alice and Bob can use a *shared secret key* to encrypt their communication. Using information-theoretic measures, Shannon defined perfect secrecy, and showed that perfect secrecy is possible using a one-time-pad (OTP) encryption system. In a OTP, a binary message is XORed with a random binary string of the same length as the message, hence effectively masking the message with pure noise. The binary string is the *cryptographic key*, which must be shared between the sender and the receiver.

Wyner's approach. In Ref. [2], Wyner proposed a radically different approach. He noted that noise is in fact a friend of the cryptographer, since it partially obstructs the view of the eavesdropper. In Wyner's original model and its generalization to *broadcast channels* [3], the sender is connected to the receiver over a noisy channel that is called the *main channel*, and to the eavesdropper over a second noisy channel called the *wiretap channel*. The secrecy capacity of a wiretap channel is an extension of Shannon's channel capacity for reliable communication, with the extra requirement that the rate of information leakage about the message to the adversary approaches zero as the message length goes to infinity.

To provide reliable communication between Alice and Bob, both of the above approaches require Alice to be able to estimate the noise in the main channel. Wyner's model however also requires estimating the noise in the eavesdropper's channel. Shannon's model does not require this estimate, but assumes a shared secret key between Alice and Bob, hence effectively requiring a solution to the key establishment problem.

Solving the key establishment problem (and hence Shannon's solution approach) without making any assumption about the adversary Eve is impossible. Wyner's approach can be seen as assuming that Eve's channel has a minimum level of noise. This is a *physical assumption* on the environment of the communication. A different type of assumption is limiting Eve's computational power.

1.1 Computational Cryptography

In computational cryptography, Eve is assumed to have polynomial-time computation. With this assumption, Diffie and Hellman [4] gave an elegant solution to the key establishment problem that allows Alice and Bob to share a secret key over a noise-free channel eavesdropped by an adversary. Here, eavesdropping provides a perfect view of the communication to the adversary, since the noise-free channel is accessible to the adversary

[1] University of Calgary, 2500 Northfield Ave. NW, Calgary Ab T3A 2M9, Canada
[a)] rei@ucalgary.ca
[b)] pengwwan@ucalgary.ca

also.

The security of the Diffie-Hellman key agreement protocol relies on the difficulty of the *Diffie-Hellman* (*DH*) *problem*. For a cyclic group with generator g, the computational DH problem requires that, given the knowledge of g^a and g^b, finding g^{ab} remain hard. A second hard problem that is the basis of the DH algorithm security is the *Discrete Logarithm* (*DL*) *problem*, which assumes that finding a from g^a is hard.

Shor [5] gave an efficient (polynomial time) quantum algorithm for the DL problem, and so effectively showed that DH key establishment becomes insecure if quantum computers exist. Advances in algorithms and computer technologies give strong motivations to the study of alternative approaches to providing security, including replacing computational assumptions with other reasonable non-computational assumptions.

1.2 Physical Assumptions

Wyner's model relies on a physical assumption about the noise in the eavesdropper's channel. The model has attracted considerable attention and provides a natural model for wireless communication in which the sender's transmission is intercepted by an eavesdropper who is within the reception distance of the sender. There is a large body of research [6], [7], [8], [9], [10], [11], [12], [13], [14], [15], [16], [17], [18] on the wiretap model, its extensions, and implementations. In the original Wyner's model, secrecy of communication is quantified by $\frac{1}{n}H(M|Z)$, where M is a uniformly distributed random variable associated with the message of length n, and Z is the random variable representing the adversary's view of the channel. Perfect secrecy of communication requires that the above *rate of equivocation* become arbitrarily small for large n. Reliability of communication requires that the average error rate (over all messages) is arbitrarily small for large n. The secrecy capacity of a channel is the highest rate of communication that achieves perfect secrecy and reliability as defined above.

The secrecy capacity of a *degraded* wiretap channel, where the wiretapper channel is a concatenation of the main channel and a second noisy channel, and the existence of codes that achieve secrecy capacity was given in Ref. [2], and its generalization to broadcast channel in Ref. [3]. The followup works have strengthened the definition of secrecy to inlcude the total information leakage, and not rate of leakage. The capacity results are not affected by this new measure.

1.2.1 Active Adversaries

Wyner and Ozarow [19] introduced the *wiretap II model*, in which the main channel is noiseless and the wiretap channel can be seen as an erasure channel, where the adversary can *choose* a subset of codeword components for eavesdropping. The subset is of size pN, where N is the length of the codeword sent over the channel and p is a constant,

In both Wyner's models, the adversary can eavesdrop on communication but does not tamper with it. In the original wiretap model, Eve's view is probabilistic, and in the wiretap II model, it is chosen by Eve. Active adversaries that modify the transmission over the main channel have been considered in recent years [11], [20], [21]. In these works, active adversaries are modelled by an *arbitrarily varying wiretap channel*, where the channels from the sender to the receiver and the adversary are specified by a set of transition probabilities $\mathsf{Pr}(y, z|x, s), x \in \mathcal{X}, y \in \mathcal{Y}, z \in \mathcal{Z}, s \in \mathcal{S}$ that depend on the *state of the channel*, represented by a random variable $\mathcal{S}$ that is unknown to Alice and Bob. Here, $\mathcal{X}$, $\mathcal{Y}$ and $\mathcal{Z}$ are Alice's input alphabet, and Bob's and Eve's output alphabet, respectively. The results in these works are existential and do not give explicit constructions.

In Ref. [22], an adversarial model for a wiretap channel with a jamming adversary is proposed in which the adversary can eavesdrop and corrupt the communication. The adversary's power is specified by a pair of constants (ρ_r, ρ_w) denoting the fraction of the codeword that is read and modified by the adversary, respectively. The goal of communication in Ref. [22] is reliability. This is later extended [23] to *Adversarial Wiretap Channels* (*AWTP*), which consider the same adversary model but requires both reliability and secrecy for the communication. In this paper, we give an overview of this model and the known results, its relation to two important cryptographic primitives, and outline directions for future research. We first show that AWTP channels, although motivated by active adversaries in point-to-point communication, are closely related to *Secure Message Transmission* (*SMT*), a cryptographic primitive for providing secrecy and reliability in networks that are partially controlled by a Byzantine adversary, and provide a natural coding-theoretic framework for the study of these protocols. We then show that for special parameter values, an AWTP code provides a *robust secret sharing* (*RSS*), a widely studied cryptographic primitive for distributed applications. These relationships allow constructions and bounds from one to be used in the other, enriching and expanding the study of these areas. We also review the known results when the same adversarial channel is considered, but the goal of communication is only reliability.

Organization: In Section 2, we introduce the model and give an overview of the main results. In Section 3, we outline our capacity-achieving construction. In Section 4, we present the relationship between SMT and AWTP channels. Section 5 is on the relationship between robust secret sharing schemes and the AWTP model. In Section 6, we introduce reliable communication (no secrecy) over the same adversarial channel and discuss the relation with list-decodable codes. Section 7 concludes the paper.

2. Adversarial Wiretap Channel

Let Σ denote a channel alphabet with a group structure, N denote the length of a codeword, and $\mathsf{SUPP}(x)$ be the set of indices where x_i is not zero. Let $[N] = \{1, \cdots, N\}$, $S_r = \{i_1, \cdots, i_{\rho_r N}\} \subseteq [N]$ and $S_w = \{j_1, \cdots, j_{\rho_w N}\} \subseteq [N]$.

Definition 1 A (ρ_r, ρ_w) adversarial wiretap channel (AWTP channel) is an adversarial channel that is partially controlled by an adversary. The adversary has two capabilities: 1) Eavesdropping (Reading): The adversary can select a subset S_r of codeword components where $|S_r| = \rho_r N$, for eavesdropping. 2) Jamming (Writing): The adversary can add errors to a subset S_w of the codeword components where $|S_w| = \rho_w N$.

The adversary is adaptive and selects the elements of S_r, S_w

and the added noise, one by one using all their information in each selection. The adversary of an AWTP channel is called *restricted* if they are limited to choosing the same set for reading and writing; i.e., $S = S_r = S_w$ and $|S| = \rho N$.

Adversarial wiretap codes (AWTP code) are used for secure and reliable communication over AWTP channels.

Definition 2 An Adversarial Wiretap Code (AWTP code) of length N over an alphabet Σ for a (ρ_r, ρ_w)-AWTP channel has two algorithms: a probabilistic encoding algorithm $\mathsf{AWTPenc} : \mathcal{M} \times \mathcal{R} \to C \subset \Sigma^N$, and a deterministic decoding algorithm $\Sigma^N \to \mathcal{M}$. The code guarantees secure and reliable communication over an AWTP channel, where security and reliability are defined as follows:

(1) *Secrecy:* Secrecy is defined as the indistinguishability of the adversary's view of the communication for any two messages $m_1, m_2 \in \mathcal{M}$, and is measured by the statistical distance between the views of the two messages:

$$\mathbf{SD}(\mathsf{View}(\mathsf{AWTPenc}(m_1), r_{\mathcal{A}}), \mathsf{View}(\mathsf{AWTPenc}(m_2), r_{\mathcal{A}})) \le \epsilon, \quad \forall m_1, m_2 \in \mathcal{M}.$$

(2) *Reliability:* The probability that the adversary outputs an incorrect message $m' \neq m$ is bounded by δ. That is, for any adversary chosen message distribution:

$$\Pr(M_S \neq M_{\mathcal{R}}) \le \delta.$$

A code provides *δ-strong reliability* if it only outputs the correct message or $\perp$, and the probability of the decoder outputting $\perp$ is bounded by δ.

The AWTP code is perfectly secure if $\epsilon = 0$.

The above definitions are the strongest notions of secrecy and reliability for wiretap channels. The secrecy definition is equivalent to semantic security, which is the strongest notion of security for encryption systems [17]. The reliability requirement is for any message and is equivalent to the worst case error.

A *family of AWTP codes* $\mathbb{C}$ is a family $\{C^N\}_{N\in\mathbb{N}}$ of AWTP codes indexed by N, where C^N has length N.

Definition 3 (i) The rate of an (ϵ, δ)-AWTP code over a (ρ_r, ρ_w)-AWTP channel is $R(C^N) = \frac{\log|\mathcal{M}|}{N \log \Sigma}$.
(ii) A rate $R(\mathbb{C})$ is achievable by a code family over a (ρ_r, ρ_w)-AWTP channel if for any small $\xi > 0$, there exists $N > N_0$ such that for all C^N with $N > N_0$, we have $\frac{1}{N}\log_\Sigma |\mathcal{M}| \ge R(\mathbb{C}) - \xi$, and the decoding error is $\delta < \xi$.
(iii) The secrecy capacity of a (ρ_r, ρ_w)-AWTP channel is denoted by C and is the highest achievable rate of AWTP code families for the channel.

2.1 Upper Bound on the Rate

Upper bounds on the rate of a code, a code family, and the secrecy capacity of AWTP channels have been derived in Ref. [24]. The upper bound on the code rate is derived by considering a special adversarial strategy and requiring the code to provide security and reliability against this strategy. This bound is then extended to code families and secrecy capacity.

Theorem 1 (i) The rate of an (ϵ, δ)-AWTP code for a (ρ_r, ρ_w)-AWTP channel is upper bounded by,

$$R(C^N) \le 1 - \rho_r - \rho_w + 2\epsilon\rho_r\left(1 + \log_{|\Sigma|}\frac{1}{\epsilon}\right) + 2\mathsf{H}(\delta). \tag{1}$$

(ii) The achievable rate of a code family is bounded by:

$$R(\mathbb{C}^\epsilon) \le 1 - \rho_r - \rho_w + 2\epsilon\rho_r\left(1 + \log_{|\Sigma|}\frac{1}{\epsilon}\right). \tag{2}$$

The secrecy capacity of a (ρ_r, ρ_w)-AWTP channel is upper bounded by,

$$\mathsf{C}^\epsilon \le 1 - \rho_r - \rho_w + 2\epsilon\rho_r\left(1 + \log_{|\Sigma|}\frac{1}{\epsilon}\right). \tag{3}$$

For the special case of $\epsilon = 0$, we have:

$$\mathsf{C}^0 \le 1 - \rho_r - \rho_w. \tag{4}$$

This last bound can be explained by noting that the components of a codeword that are either eavesdropped or corrupted cannot contribute to secure and reliable transmission of information. Since the capacity result must hold for *all* adversaries and so all possible choices of S_r and S_w, for an adversary that uses $S_r \cap S_w = \emptyset$ we will have the rate bounded by $1 - \rho_r - \rho_w$.

2.2 Restricted Channels

In restricted AWTP channels, the adversary's choice is limited to $S_r = S_w$ and the channel is specified by a single parameter $\rho = \rho_r = \rho_w$. The proof strategy of Theorem 1 can be used for this subset of AWTP channels to prove the following upper bound on the rate of AWTP codes and the secrecy capacity of AWTP channels.

Theorem 2 (i) The rate of an (ϵ, δ)-AWTP code for a restricted ρ-AWTP channel is bounded by:

$$R(C^N) \le 1 - 2\rho + 2\epsilon\rho\left(1 + \log_{|\Sigma|}\frac{1}{\epsilon}\right) + 2\mathsf{H}(\delta). \tag{5}$$

(ii) The achievable rate of a code family and the secrecy capacity of a restricted ρ-AWTP channel are upper bounded by:

$$R(\mathbb{C}^\epsilon) \le 1 - 2\rho + 2\epsilon\rho\left(1 + \log_{|\Sigma|}\frac{1}{\epsilon}\right), \tag{6}$$

and

$$\mathsf{C}^\epsilon \le 1 - 2\rho + 2\epsilon\rho\left(1 + \log_{|\Sigma|}\frac{1}{\epsilon}\right). \tag{7}$$

For the special case of $\epsilon = 0$ we have,

$$\mathsf{C}^0 \le 1 - 2\rho. \tag{8}$$

In Section 4, we will use the above bounds to derive new bounds on the transmission rate of secure message transmission protocols.

3. AWTP Code Construction

In Ref. [24], an efficient capacity-achieving $(0, \delta)$-AWTP code family $\mathbb{C} = \{C^N : N \in \mathbb{N}\}$ was constructed for (ρ_r, ρ_w)-AWTP channels with polynomial-time encoding and decoding. The construction uses three building blocks: (i) an Algebraic Manipulation Detection code, (ii) a Folded Reed-Solomon code, and

(iii) a Subspace Evasive Set. We give an outline of these building blocks, and the intuition behind the construction.

1) Algebraic Manipulation Detection Code (AMD code): An AMD code [25] is used to detect algebraic manipulation of a codeword when the adversary is oblivious to the codeword. A codeword is an element of Σ^N, where Σ has a group structure, and the adversarial tampering is by adding (component wise) a noise vector to the codeword. We use the AMD code given in Ref. [25] over an extension field. Let ϕ be a bijection between a vector $\mathbf{v}$ in $\mathbb{F}_q^N$ and an element of $\mathbb{F}_{q^N}$. The AMD code $(\mathbf{x}, \mathbf{r}, \mathbf{t})$ is generated as follows:

$$\mathbf{t} = f(\mathbf{x}, \mathbf{r}) = \phi^{-1}\left(\phi(\mathbf{r})^{d+2} + \sum_{i=1}^{d} \phi(\mathbf{x}_i)\phi(\mathbf{r})^i\right) \mod q^N.$$

For the AMD code above, the success probability of an adversary in tampering with a codeword $(\mathbf{x}, \mathbf{r}, \mathbf{t})$ and constructing a new codeword $(\mathbf{x}' = \mathbf{x} + \Delta\mathbf{x},\ \mathbf{r}' = \mathbf{r} + \Delta\mathbf{r},\ \mathbf{t}' = \mathbf{t} + \Delta\mathbf{t})$ that satisfies $\mathbf{t}' = f(\mathbf{x}', \mathbf{r}')$ is no more than $\frac{d+1}{q^N}$.

2) Folded Reed-Solomon Code (FRS code): An error-correcting code over $\Sigma = \mathbb{F}_q$ with length N is a subset of Σ^N. A (ρ, ℓ) list decodable code [26] can decode a corrupted codeword that has at most ρN errors, and output a list of codewords of size at most ℓ. Compared to uniquely decodable codes, list decodable codes can decode a larger fraction of errors. FRS codes [27] give an explicit construction of list decodable codes with an efficient encoding algorithm. A decoding algorithm for FRS codes is given in Ref. [28], where decoding is by finding a solution to a set of linear equations. The output of the decoder is a list of codewords, where the list size is exponential in N.

3) Subspace Evasive Set: Subspace evasive sets [28] have been used to reduce the decoding list size of list decodable codes. A subset evasive set is a subset of $\mathbb{F}_q^n$ with the property that it has small intersection with every k-dimensional affine subspace. Dvir et al. [29] gave an efficient construction of subspace evasive sets over large fields, and used it to reduce the list size of the FRS code to a constant.

The intuition behind our construction of AWTP codes is as follows. We use a list decodable code (FRS code) to correct the $\rho_w N$ errors in the corrupted received codeword. The decoder output is a list of codewords, and we need to identify the sent codeword in this list. For this, the message of the codeword is given a special structure using an AMD code. This allows Bob to use the decoding algorithm of the AMD code to check the message part of the codewords in the list, and identify the sent codeword. To guarantee perfect secrecy, the view of the adversary, given by the $\rho_r N$ read components of the codeword, must be independent of the sent message. This is achieved by appending a sufficient number $(\rho_r N)$ of random elements to the AMD codeword. To achieve efficient decoding, the AMD codeword with the appended randomness is encoded using the subspace evasive set in Ref. [29], and the resulting element of the subspace evasive set is used as the message of the FRS code.

Theorem 3 For any small $0 < \xi < 1$, there is a $(0, \delta)$-AWTP code C^N of length N for a (ρ_r, ρ_w)-AWTP channel. The rate of the code is $R(C^N) = 1 - \rho_r - \rho_w - \xi$, the alphabet size is $|\Sigma| = O(q^{1/\xi^2})$, and the decoding error is bounded by $\delta < \xi$. Both encoding and decoding computation of the AWTP code are polynomial time in N. The AWTP code family $\mathbb{C}$ achieves the secrecy capacity $R(\mathbb{C}) = 1 - \rho_r - \rho_w$.

4. AWTP Codes and Secure Message Transmission

An AWTP channel models an adversarial point-to-point wiretap channel. Interestingly, the codes that provide security for these channels can also be used to construct secure protocols for node-to-node communication in networks that are partially controlled by an adversary. In Secure Message Transmission (SMT) [30], Alice and Bob are connected through a set of N node-disjoint paths that are called *wires*. The adversary can adaptively choose a subset of wires to eavesdrop and arbitrarily modify. Although the original model considered adversaries who select distinct sets of wires for listening, corrupting, and blocking, the most widely studied SMT adversary is a (t, N)-threshold adversary who adaptively selects t out of N wires and has full control over them. A 1-round (ϵ, δ)-SMT protocol has a pair $(\mathsf{SMTenc}, \mathsf{SMTdec})$ of algorithms to encode and decode the message, and guarantees privacy loss is at most ϵ and probability of error is bounded by δ.

Definition 4 A (t, N)-threshold (ϵ, δ)-secure message transmission (SMT) protocol satisfies the following properties for any choice of t wires by the adversary:

- *Secrecy:* For any pair of messages $m_1, m_2 \in \mathcal{M}$,

$$\max_{m_1, m_2} \mathbf{SD}(\mathsf{View}_{\mathcal{A}}(\mathsf{SMTenc}(m_1), r_{\mathcal{A}}), \mathsf{View}_{\mathcal{A}}(\mathsf{SMTenc}(m_1), r_{\mathcal{A}})) \leq \epsilon_{SMT}.$$

- *Reliability:* The probability of the receiver outputting an incorrect message is bounded by,

$$\Pr(M_{\mathcal{S}} \neq M_{\mathcal{R}}) \leq \delta_{SMT},$$

where the message distribution is chosen by the adversary.

An SMT protocol is perfectly secure if $\epsilon = 0$, and perfectly reliable if $\delta = 0$. It has been shown that an (ϵ, δ)-SMT protocol can be constructed only if $N \geq 2t + 1$, and 1-round $(0, 0)$-SMT protocol requires $N \geq 3t + 1$.

An SMT protocol has one or more rounds, with each round consisting of a message from Alice to Bob or vice versa. The efficiency of SMT protocols is measured by the transmission rate of the protocol and the computational time of the encoder and the decoder. The transmission rate of an SMT protocol is defined by $\tau(SMT) = \frac{\text{Length of Transmission over all Wires}}{\text{Message Length}}$. For 1-round $(0, 0)$-SMT protocols the lower bound on the transmission rate is $\frac{N}{N-3t}$ [31], and for $(0, \delta)$-SMT, the bound is $\frac{N}{N-2t}$ [32]. An SMT protocol is called transmission *optimal* if its transmission rate asymptotically approaches the corresponding lower bound. The computational complexity of a protocol is the total computation of Alice and Bob. An SMT protocol is efficient if both Alice and Bob have polynomial time computation.

4.1 AWTP Codes and 1-round SMT

AWTP codes and 1-round SMT protocols are closely related.

However, one needs to consider subtle differences in their definitions. AWTP codes are defined over an alphabet Σ, and so all components of a codeword are elements of Σ. An SMT protocol, however, may use different alphabet sets for transmission over different wires. Without loss of generality for threshold SMT protocols, we will consider *symmetric SMT* protocols that use the same set of possible values for all wires [*1]. All known threshold SMT protocols are symmetric. The relation between 1-round SMT protocols and AWTP codes is given below.

Theorem 4 (Ref. [23]) There is a one to one correspondence between (ϵ, δ)-AWTP codes for a ρ-restricted AWTP channel and 1-round symmetric $(\epsilon_{SMT}, \delta_{SMT})$-SMT protocols against (t, N)-threshold adversaries, with $t = \rho N$, $\epsilon_{SMT} = \epsilon$, and $\delta_{SMT} = \delta$.

The one-to-one correspondence is by identifying each wire with a component of the codeword. A main observation is that when $S_r = S_w$, the additive error and arbitrary error are the same. That is, a codeword component c_i that is seen by the adversary ($i \in S_r$) can be changed to an arbitrary value $\hat{c}_i$ by choosing the noise value $a = \hat{c}_i - c_i$ to be added to the component. The security and reliability relations follow from the corresponding definitions in the two primitives. The transmission rate of a 1-round (ϵ, δ) symmetric SMT protocol can be bounded using the above relationship between SMT protocols and AWTP codes.

Theorem 5 For a 1-round (ϵ, δ) symmetric SMT protocol, the transmission rate is lower bounded by:

$$\tau(SMT) \geq \frac{N}{N - 2t + 2t\epsilon\left(1 + \log_{|\mathcal{V}|}(\frac{1}{\epsilon})\right) + 2H(\delta)}. \qquad (9)$$

For $\epsilon = 0$ and vanishing δ, the bound reduces to $\tau(SMT) \geq \frac{N}{N-2t}$. Bound (9) is the only known bound on the transmission rate of (ϵ, δ)-SMT protocols.

The construction of $(0, \delta)$-AWTP codes outlined in Section 3 gives the construction of an efficient 1-round $(0, \delta)$-SMT protocol for $t = \alpha N$ where $0 < \alpha < 1/2$ is a real-valued constant.

Theorem 6 A 1-round SMT for $t = \alpha N$ can be constructed from the $(0, \delta)$-AWTP code in Theorem 3. The protocol has efficient encoding and decoding and its transmission rate approaches the optimal rate for sufficiently large N.

5. AWTP and Robust Secret Sharing (RSS)

Secret sharing schemes were independently proposed by Shamir [33] and Blakely [34], and are a foundational primitive in secure distributed computation. In the original model of secret sharing, in the *share distribution phase* a trusted dealer distributes the *shares* of a *secret* among a group of players such that during the *reconstruction phases*, any *authorized subset* of players, also called *access sets*, can reconstruct the secret by pooling their shares together. This is the *correctness* property of the scheme. *Perfect security* requires that the players who do not form an access set learn no information about the secret. In (t, N)-*threshold secret sharing*, any subset of $t + 1$ players is an access set. We consider (t, N)-threshold secret sharing schemes.

In the original model of secret sharing schemes, the adversary is passive and the goal is to provide perfect secrecy against the leakage of the secret to an unauthorized set. A stronger form of the adversary is when the players that are controlled by the adversary present modified shares during the reconstruction phase. The most basic requirement in this case is that the set of all shares in the system can reconstruct the secret. In other words, there is sufficient information in the system to recover the secret. In robust secret sharing (RSS) [35], [36], [37], there is a dealer $\mathcal{D}$, N players $P_1, \cdots, P_N$, a reconstructor $\mathcal{R}$, and an adversary $\mathcal{A}$. An RSS scheme has two phases, each with an associated protocol, called *share distribution* and *reconstruction*, respectively. In the share distribution phase, the dealer $\mathcal{D}$ takes a secret s, computes the shares $s_1, \cdots, s_N$, and sends the i^{th} share s_i to the player P_i over a secure channel. In the reconstruction phase, the reconstructor $\mathcal{R}$ receives some values from each player P_i for $i = 1, \cdots, N$, and uses these values to reconstruct the secret. The adversary $\mathcal{A}$ can adaptively corrupt t out of N players. In the sharing phase, the adversary $\mathcal{A}$ learns $P_i's$ share s_i for all the corrupted players, but remains passive. During the reconstruction phase, the adversary can modify the information that the corrupted players send to $\mathcal{R}$. If the adversary is *non-rushing*, $\mathcal{A}$ decides on the information of corrupted players at the start of the reconstruction phase and before seeing the information of other players. Rushing adversaries, on the other hand, can observe the information that the non-corrupted players send to the reconstructor, and then decide on the information that the corrupted players provide. We only consider non-rushing adversaries.

Definition 5 In a (t, δ_{RSS})-robust threshold secret sharing scheme ((t, δ_{RSS})-RSS), for any distribution on $s \in \mathcal{S}$ and any subset of corrupted players, the following two requirements hold.

- Privacy: The adversary has no information about the secret s before the reconstruction phase starts.
- Reconstructability: Players send some information to the reconstructor $\mathcal{R}$ who uses the information to reconstruct the secret. The correct secret is output with probability at least $1 - \delta$.

The set of shares in Shamir (t, N)-secret sharing form a codeword of a Reed-Solomon code. It immediately follows that Shamir secret sharing is a RSS when $t < N/3$, and it is impossible to have robustness when $t > N/2$. The efficient construction of RSS schemes for the range $N/3 \leq t < N/2$ has been an interesting research question.

The efficiency of robust secret sharing schemes is measured by the *share redundancy* and the computational complexity. It is known [38] that for secret sharing with perfect secrecy, the share size is at least equal to the secret size. Share redundancy η is the extra information that a player must store to achieve robustness. That is, $\eta = \max_i(\log|\mathcal{S}_i|) - \log|\mathcal{S}|$. Here, $\mathcal{S}_i$ is the set of possible shares for player P_i. The computational complexity of robust secret sharing is the computational efficiency of share distribution and secret reconstruction.

5.1 AWTP Codes and RSS

In RSS, the share sizes may be different. For threshold RSS, without loss of generality we consider symmetric RSS protocols that use the same set of possible shares for all players. That is, in a symmetric RSS scheme $\mathcal{S}_j = \mathcal{S}$ is independent of j. All known

[*1] This class of protocols was also considered in Ref. [32] (page 12).

constructions of threshold RSS are symmetric.

A (t, N)-RSS has the requirement that any $t+1$ correct shares must reconstruct the secret. There is no corresponding requirement for AWTP protocols and so in general the two primitives are not the same. For $N = 2t+1$, however, the two primitives have identical security and reliability requirements.

Theorem 7 There is a one to one correspondence between a $(0, \delta)$-AWTP code C^N for restricted ρ-AWTP channels, and a (t, δ_{RSS})-symmetric RSS scheme where $t = \rho N$, $\rho = \frac{N-1}{2N}$ and $\delta = \delta_{RSS}$.

Note that in the above theorem, the correspondence between the AWTP code and the RSS is for a specific value of ρ, which is a function of N. One may use the upper bound on the rate of a $(0, \delta)$-AWTP code C^N for a restricted ρ-AWTP channel to obtain a lower bound on η in this case. However, this results in a trivial lower bound. This is not surprising because AWTP codes have less "structure" (allowing arbitrary $0 < \rho < 1$, $S_r \neq S_w$ and do not require $t+1$ shares to reconstruct the secret) and so the bound obtained from this less structured primitive may not give a good bound for the special case of $\rho = \frac{N-1}{2N}$, $S_r = S_w$, and the secret must be reconstructible from $t+1$ correct shares.

Construction. The construction of a $(0, \delta)$-AWTP code for (ρ_r, ρ_w)-AWTP channels in Section 3 can be used to construct a (t, δ)-RSS for $N = 2t+1$. By choosing $v = 6N+1$, $w = u = v^2$, and $R = \frac{1}{2N}$, we obtain a (t, δ)-RSS scheme for $N = 2t+1$ with decoding error $\delta \leq \frac{O(N^{N \log\log N})}{q^N}$. Since $u = O(N^2)$ and $q = O(N^{\log\log N})$, the redundancy of the RSS is:

$$\begin{aligned}\eta &= \log|\Sigma| - \log|\mathcal{M}| \\ &= u \log q - \frac{u}{2} \log q = O(N^2 \log N \log\log N).\end{aligned}$$

The RSS scheme has $\log \frac{1}{\delta} = O(N \log N \log\log N)$, which implies $\eta = N \log \frac{1}{\delta}$. This is not as good performance as the best known RSS schemes [37]. However, the scheme allows the corruption set of the adversary in the sharing and reconstruction phase to be different. That is the adversary can corrupt a subset S_r of players during the sharing phase to learn their shares, and choose a second subset S_w of players during the reconstruction phase and modify their submitted values by adding noise values to them. This is, the only known RSS with this property.

6. Reliable Communication

Reliable communication when the channel corruption is adversarial (and not probabilistic) dates back to Hamming [39], who proposed a channel that can introduce arbitrary error subject to the limit on the number of errors. In Hamming's model, the channel has access to the whole codeword. In our notation, $|S_r| = N$ and $|S_w| \leq pN$, where p is a constant showing the fraction of a codeword that is corrupted. Reliable communication over adversarial channels, where the adversary's capabilities are specified by a pair of parameters $(\rho_r, \rho_w), 0 \leq \rho_r, \rho_w \leq 1$ specifying the sizes of the adversary's read and write sets, have been considered in Ref. [22]. The adversarial channel was called *limited view* adversarial channels (LV adversary channel) and the codes that provide reliable communication were referred to as *limited view* adversary codes (LV-code). The adversary's capabilities in a (ρ_r, ρ_w)-LV channel are the same as their capabilities in a (ρ_r, ρ_w)-AWTP channel. The goal of an LV-code however is to only provide reliability for the communication.

Definition 6 (Refs. [22], [40]) Let Σ be an additive group. A Limited View Adversary Code (LV-code) for a (ρ_r, ρ_w)-LV adversarial channel is defined by a pair $(\mathsf{LVACenc}, \mathsf{LVACdec})$ of encoding and decoding algorithms with the following properties. The encoding algorithm $\mathsf{LVACenc} : \mathcal{M} \to C^N$ maps messages in $\mathcal{M}$ to codewords in $C^N \subset \Sigma^N$, and the decoding algorithm $\mathsf{LVACdec} : \Sigma^N \to \mathcal{M}$ outputs an element of $\mathcal{M}$ for any element of Σ^N. For any sent message m, the probability that the decoder outputs a message $m' \neq m$ is at most δ. That is for any $m \in \mathcal{M}$ and any adversary strategy, we have:

$$\mathsf{Pr}(\mathsf{LVACdec}(\mathsf{LVACenc}(m) + e) \neq m) \leq \delta,$$

where $e \in \Sigma^N$ and $|\mathsf{SUPP}(e)| \leq \rho_w N$.

The above definition of reliability is for *strong LV codes*. In *weak LV codes* the decoding error probability is the average over all messages:

$$\mathsf{Pr}(M_{\mathcal{S}} \neq M_{\mathcal{R}}) \leq \delta.$$

Upper bounds on the rate of LV-codes and LV-code families have been derived in Ref. [40].

Theorem 8 (i) The rate of an LV-code C^N over a (ρ_r, ρ_w)-LV adversary channel is bounded by:

$$R(C^N) \leq 1 - \rho_w + 2\mathsf{H}(\delta).$$

(ii) The achievable rate of a code family is bounded by:

$$R(C^N) \leq 1 - \rho_w,$$

and the capacity of LV adversarial channels is upper bounded by:

$$\mathsf{C} \leq 1 - \rho_w. \tag{10}$$

Construction. An efficient capacity-achieving LV adversary code family $\mathbb{C} = \{C^N : N \in \mathbb{N}\}$ for a (ρ_r, ρ_w)-LV adversary channel was given in Ref. [40]. The building blocks of the construction are: (i) a Message Authentication Code (MAC), (ii) a Folded Reed-Solomon Code, and (iii) an Adversarial Wiretap Code.

A *message authentication code* is a shared key cryptographic primitive that provides security against adversarial tampering of a message. Assume Alice and Bob share a secret key k. A MAC system consists of a pair of algorithms $(\mathsf{Tag}, \mathsf{Ver})$ with the following properties. For a message m, the Tag algorithm generates a tag $t = \mathsf{TAG}(k, m)$ that is appended to the message. The Ver algorithm takes a tagged message $\mathsf{Ver}(k, (m', t'))$ and outputs accept or reject for authentic and forged messages, respectively.

The outline of the construction is as follows. To encode a message block m, Alice chooses a random key r and constructs a tagged message (m, t), which is then encoded using a list decodable code. The key block r is encoded using an AWTP code. The i^{th} component of the LV code consists of the i^{th} component of the AWTP code concatenated with the i^{th} component of the list decodable code. The receiver decodes the received word of the list decidable code and generates a list of possible codewords. It then

decodes the received (corrupted) codeword of the AWTP code and finds the MAC key. The MAC verification algorithm is used to identify the sent codeword in the list.

Theorem 9 There is an LV code family $\mathbb{C} = \{C^N\}$ for a (ρ_r, ρ_w)-LV adversary channel with rate $R(\mathbb{C}) = 1-\rho_w$ if the reading and writing parameters of the channel satisfy $\rho_r+\rho_w < 1$. The encoding and decoding algorithms are polynomial time in N.

The above construction is capacity achieving. The restriction $\rho_r + \rho_w < 1$ follows from the requirement of AWTP codes that is used as a building block in the construction.

LV-codes are in one-to-one correspondence [40] with Reliable Message Transmission (RMT) protocols [41]. The RMT adversary is the same as the SMT adversary, however the goal of communicants is only reliability. The relationship between LV codes and 1-round RMT allows a unified study of these two apparently different problems and relates and enriches the results in the two areas.

7. Concluding Remarks

AWTP channels provide a coding-theoretic model for wiretap channels when an active adversary can choose their view of the communication and also add noise to the transmission. The model naturally extends the wiretap II model and gives a coding-theoretic model for active adversaries for the wiretap. This can be seen as the relation between Hamming's model and Shannon's model of noisy channels. We outlined an upper bound on the rate of a code and a code family, and the explicit construction of a code family that achieves the rate upper bound (and hence capacity) of the code family.

AWTP channels capture an important cryptographic primitive for networks (SMT) and are closely related to another cryptographic primitive known as robust secret sharing (RSS). In both cases, AWTP presents a more powerful adversary model by allowing the reading set S_r and writing set S_w to be different. The efficiency measures of SMT and RSS are transmission rate and share redundancy, respectively. The upper bound on the rate of AWTP codes gives a lower bound on the transmission rate of (ϵ, δ)-SMT, and this is the only known lower bound on the transmission rate of SMT when $\epsilon > 0$. The rate bound of AWTP codes does not give a useful result for RSS.

Interestingly, the known lower bound on the transmission rate of $(0, \delta)$-SMT gives an upper bound on the rate of restricted $(0, \delta)$-AWTP codes given by $R(C^N) \le 1 - 2\rho$, which also holds for *any* $(0, \delta)$-AWTP code, since the adversary in the latter is more powerful. This upper bound is tighter than the upper bound on rate that is obtained from bound (1) in Theorem 1, by letting $\epsilon = 0$ and requiring $S_r = S_w$.

SMT and RSS adversaries are special cases of AWTP channels when $S_r = S_w$, and so using a construction in one of the former two adversarial models does not necessarily give a secure construction for AWTP codes. A secure construction for AWTP channels, however, directly gives a corresponding construction for SMT, and when $N = 2t + 1$, for RSS. We showed that the capacity-achieving construction in Section 3 gives an asymptotically optimal 1-round SMT construction. The RSS construction obtained from this AWTP code, however, does not have the best known efficiency. In both SMT and RSS, security is against a stronger adversary.

Using the same adversarial model but requiring only reliability for the communication, results in LV codes. By limiting the adversary's view of the communication, these codes can achieve the *capacity of* $1-\rho_w$ *with unique decoding*. If the adversary can see the whole codeword, the same capacity is achievable only by list decodable codes, where the decoder outputs a list of possible codewords. Our capacity-achieving construction requires $\rho_r + \rho_w < 1$. It is an open question if this is a necessary condition for capacity achieving LV codes.

LV codes also raise an interesting open question on the relation between the list size and the parameters ρ_r and ρ_w the specify the limitation on the view and the corruption power of the adversary. For full view adversary ($\rho_r = 1$), the decoder can only decode to a list of possible codewords. For $\rho_r < 1$, unique decoding becomes possible (in our construction for $\rho_w < 1-\rho_r$). In between the two limits, the relationship remains unknown.

Capacity-achieving constructions of AWTP codes and LV codes are for large alphabets. Construction of capacity-achieving codes for small alphabets is an open question. Extensions of AWTP channels when communicants can interact over the channel, or have access to resources such as a public discussion channel, are interesting directions for future research. Finally limiting the view of the adversary in error detecting codes relaxes the definition of AMD codes when the adversary has access to part of the codeword.

Acknowledgments This work is supported in part by Alberta Innovates Technology Futures, in the Province of Alberta, Canada.

References

[1] Shannon, C.E.: A mathematical theory of communication, *Mobile Computing and Communications Review*, Vol.5, No.1, pp.3–55 (2001).
[2] Wyner, A.D.: The wire-tap channel, *Bell System Technical Journal*, Vol.54, pp.1355–1387 (Oct. 1975).
[3] Csiszár, I. and Körner, J.: Broadcast channels with confidential messages, *IEEE Trans. Information Theory*, Vol.24, pp.339–348 (May 1978).
[4] Diffie, W. and Hellman, M.E.: New directions in cryptography, *IEEE Trans. Information Theory*, Vol.22, No.6, pp.644–654 (1976).
[5] Shor, P.W.: Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer, *SIAM Journal on Computing*, Vol.26, No.5, pp.1484–1509 (1997).
[6] Leung-Yan-Cheong, S.K. and Hellman, M.E.: The Gaussian wire-tap channel, *IEEE Trans. Information Theory*, Vol.24, No.4, pp.451–456 (1978).
[7] Maurer, U.M.: Protocols for secret key agreement by public discussion based on common information, *Proc. Advances in Cryptology – CRYPTO '92, 12th Annual International Cryptology Conference*, Santa Barbara, California, USA, Brickell, E.F. (Ed.), *Lecture Notes in Computer Science*, Vol.740, pp.461–470, Springer (1992).
[8] Maurer, U.M. and Wolf, S.: Information-theoretic key agreement: From weak to strong secrecy for free, *Proc. Advances in Cryptology – EUROCRYPT 2000, International Conference on the Theory and Application of Cryptographic Techniques*, Bruges, Belgium, pp.351–368 (2000).
[9] Maurer, U.M. and Wolf, S.: Secret-key agreement over unauthenticated public channels I: Definitions and a completeness result, *IEEE Trans. Information Theory*, Vol.49, No.4, pp.822–831 (2003).
[10] Lai, L., Gamal, H.E. and Poor, H.V.: The wiretap channel with feedback: Encryption over the channel, *IEEE Trans. Information Theory*, Vol.54, No.11, pp.5059–5067 (2008).
[11] MolavianJazi, E., Bloch, M. and Laneman, J.N.: Arbitrary jamming can preclude secure communication, *47th Annual Allerton Conference*

on Communication, Control, and Computing, pp.1069–1075 (Sep. 2009).
[12] Mahdavifar H. and Vardy, A.: Achieving the secrecy capacity of wiretap channels using polar codes, *IEEE Trans. Information Theory*, Vol.57, pp.6428–6443 (Oct. 2011).
[13] Czap, L., Prabhakaran, V.M., Fragouli, C. and Diggavi, S.N.: Secret message capacity of erasure broadcast channels with feedback, *2011 IEEE Information Theory Workshop* (*ITW*), pp.65–69 (Oct. 2011).
[14] Cheraghchi, M., Didier, F. and Shokrollahi, A.: Invertible extractors and wiretap protocols, *IEEE Trans. Information Theory*, Vol.58, No.2, pp.1254–1274 (2012).
[15] Liang, Y., Poor, H.V. and Shamai (Shitz), S.: Information theoretic security, *Found. Trends Commun. Inf. Theory*, Vol.5, pp.355–580 (Apr. 2009).
[16] Liu, R. and Trappe, W.: *Securing wireless communications at the physical layer*, Vol.7, Springer (2010).
[17] Bellare, M., Tessaro, S. and Vardy, A.: Semantic security for the wiretap channel, *Proc. Advances in Cryptology – CRYPTO 2012 – 32nd Annual Cryptology Conference*, Santa Barbara, CA, USA, Safavi-Naini, R. and Canetti, R. (Eds.), *Lecture Notes in Computer Science*, Vol.7417, pp.294–311, Springer (2012).
[18] Bloch, M. and Barros, J.: *Physical-layer security: From information theory to security engineering*, Cambridge University Press (Nov. 2011).
[19] Ozarow, L.H. and Wyner, A.D.: Wire-tap channel II, *Advances in Cryptology: Proc. EUROCRYPT 84, A Workshop on the Theory and Application of Cryptographic Techniques*, Paris, France, pp.33–50 (1984).
[20] Boche, H. and Schaefer, R.F.: Capacity results and super-activation for wiretap channels with active wiretappers, *IEEE Trans. Information Forensics and Security*, Vol.8, No.9, pp.1482–1496 (2013).
[21] Igor Bjelaković, H.B. and Sommerfeld, J.: Capacity results for arbitrarily varying wiretap channels, *Information Theory, Combinatorics, and Search Theory*, pp.123–144, Springer (2013).
[22] Safavi-Naini, R. and Wang, P.: Codes for limited view adversarial channels, *Proc. 2013 IEEE International Symposium on Information Theory*, Istanbul, Turkey, pp.266–270, IEEE (2013).
[23] Wang, P. and Safavi-Naini, R.: A model for adversarial wiretap channel, *arXiv preprint arXiv:1312.6457* (2013).
[24] Wang, P. and Safavi-Naini, R.: An efficient code for adversarial wiretap channel, *Proc. 2014 IEEE Information Theory Workshop*, Hobart, Australia, pp.40–44, IEEE (2014).
[25] Cramer, R., Dodis, Y., Fehr, S., Padró, C. and Wichs, D.: Detection of algebraic manipulation with applications to robust secret sharing and fuzzy extractors, *Proc. Advances in Cryptology – EUROCRYPT 2008, 27th Annual International Conference on the Theory and Applications of Cryptographic Techniques*, Istanbul, Turkey, Smart, N.P. (Ed.), *Lecture Notes in Computer Science*, Vol.4965, pp.471–488, Springer (2008).
[26] Elias, P.: Error-correcting codes for list decoding, *IEEE Trans. Information Theory*, Vol.37, pp.5–12 (Jan. 1991).
[27] Guruswami, V. and Rudra, A.: Explicit capacity-achieving list-decodable codes, *Proc. 38th Annual ACM Symposium on Theory of Computing*, Seattle, WA, USA, Kleinberg, J.M. (Ed.), pp.1–10, ACM (2006).
[28] Guruswami, V.: Linear-algebraic list decoding of folded Reed-Solomon codes, *Proc. 26th Annual IEEE Conference on Computational Complexity, CCC 2011*, San Jose, California, pp.77–85, IEEE Computer Society (2011).
[29] Dvir, Z. and Lovett, S.: Subspace evasive sets, *Proc. 44th Annual ACM Symposium on Theory of Computing*, *STOC '12*, New York, NY, USA, pp.351–358, ACM (2012).
[30] Dolev, D., Dwork, C., Waarts, O. and Yung, M.: Perfectly secure message transmission, *J. ACM*, Vol.40, pp.17–47 (Jan. 1993).
[31] Fitzi, M., Franklin, M., Garay, J. and Vardhan, S.H.: Towards optimal and efficient perfectly secure message transmission, *Theory of Cryptography*, pp.311–322, Springer (2007).
[32] Patra, A., Choudhury, A., Rangan, C.P. and Srinathan, K.: Unconditionally reliable and secure message transmission in undirected synchronous networks: Possibility, feasibility and optimality, *IJACT*, Vol.2, No.2, pp.159–197 (2010).
[33] Shamir, A.: How to share a secret, *Comm. ACM*, Vol.22, No.11, pp.612–613 (1979).
[34] Blakley, G.R.: Safeguarding cryptographic keys, *Proc. National Computer Conference*, Vol.48, pp.313–317 (1979).
[35] Rabin, T. and Ben-Or, M.: Verifiable secret sharing and multiparty protocols with honest majority (extended abstract), *Proc. 21st Annual ACM Symposium on Theory of Computing*, Seattle, Washigton, USA, Johnson, D.S. (Ed.), pp.73–85, ACM (1989).
[36] Cramer, R., Damgård, I. and Fehr, S.: On the cost of reconstructing a secret, or VSS with optimal reconstruction phase, *Proc. Advances in Cryptology – CRYPTO 2001, 21st Annual International Cryptology Conference*, Santa Barbara, California, USA, Kilian, J. (Ed.), *Lecture Notes in Computer Science*, Vol.2139, pp.503–523, Springer (2001).
[37] Cevallos, A., Fehr, S., Ostrovsky, R. and Rabani, Y.: Unconditionally-secure robust secret sharing with compact shares, *Advances in Cryptology – EUROCRYPT 2012*, pp.195–208, Springer (2012).
[38] Stinson, D.: On the Connections Between Universal Hashing, Combinatorial Designs and Error-Correcting Codes, *Proc. Congressus Numerantium 114*, pp.7–27 (1996).
[39] Hamming, R.W.: Error detecting and error correcting codes, *Bell System Technical Journal*, Vol.29, No.2, pp.147–160 (1950).
[40] Wang, P. and Safavi-Naini, R.: Limited view adversary codes: Bounds, constructions and applications, *Information Theoretic Security*, pp.214–235, Springer (2015).
[41] Franklin, M.K. and Wright, R.N.: Secure communication in minimal connectivity models, *J. Cryptology*, Vol.13, No.1, pp.9–30 (2000).

Reihaneh Safavi-Naini is the AITF Strategic Chair in Information Security at the University of Calgary. Before joining University of Calgary in 2007, she was a Professor of Computer Science and the Director of Telecommunication and Information Technology Research Institute at the University of Wollongong, Australia. She has over 300 refereed publications in journals and conferences. She has served as program chair of a number of conferences including Crypto 2012, ACNS 2013, Financial Cryptography 2014, and ACM CCSW 2014. She has served as an Associate Editor of IEEE Transactions on Information Theory and ACM Transactions on Information and System Security (TISSEC), and is currently an Associate Editor of IEEE Transactions on Secure and Dependable Computing and IET Information Security. She has a Ph.D. in Electrical Engineering from University of Waterloo, Canada. Her current research interests are cryptography, Information theoretic security, provable security, communication security, data privacy and cloud security.

Pengwei Wang received Bachelor and Master of Science degrees in Mathematics from Shandong University in the People Republic of China, in 2005 and 2008, respectively. He received his Ph.D. degree in Computer Science from University of Calgary, Canada, in 2015. His main research interests are information theoretic security, cryptography, and network security.