Optimal Parameter Encoding Based on Worst Case Fisher Information Under a Secrecy Constraint

Çağrı Göken, *Student Member, IEEE*, and Sinan Gezici, *Senior Member, IEEE*

***Abstract*—In this letter, optimal deterministic encoding of a uniformly distributed scalar parameter is performed in the presence of an eavesdropper. The objective is to maximize the worst case Fisher information of the parameter at the intended receiver while keeping the mean-squared error (MSE) at the eavesdropper above a certain level. The eavesdropper is modeled to employ the linear minimum MSE estimator based on the encoded version of the parameter. First, the optimal encoding function is derived when there exist no secrecy constraints. Next, to obtain the solution of the problem in the presence of the secrecy constraint, the form of the encoding function that maximizes the MSE at the eavesdropper is explicitly derived for any given level of worst case Fisher information. Then, based on this result, a low-complexity algorithm is provided to calculate the optimal encoding function for the given secrecy constraint. Finally, numerical examples are presented.**

***Index Terms*—Fisher information, mean-squared error (MSE), optimization, parameter estimation, secrecy.**

I. Introduction

PHYSICAL layer secrecy has gained a renewed interest with the advances in wireless communication systems. The main objective of physical layer secrecy is to ensure secret communications between a transmitter and an intended receiver in the presence of an eavesdropper by exploiting physical channel characteristics. One common approach to quantify the amount of achieved secrecy is to use information theoretic metrics, such as the mutual information and secrecy rate, which have been investigated in a multitude of studies in the literature for various channels (e.g., fading, Gaussian broadcast or interference, wiretap, etc. [1]–[7]) and transmission scenarios (e.g., with user or jammer cooperation to facilitate security [8]–[10]). Alternatively, quality-of-service frameworks based on signal-to-noise-ratio [11]–[13] or estimation theoretic tools, such as mean-squared error (MSE) have recently been used to measure the security performance of communication systems. The latter framework is of particular interest to design low-complexity practical secure systems and has been adopted in various studies [14]–[18]. In [14], the secret communication problem is investigated for Gaussian interference channels in the presence of eavesdroppers. The problem is formulated to minimize the total minimum MSE (MMSE) at the intended receivers while keeping the MMSE at the eavesdroppers above a certain level, where joint artificial noise and linear precoding schemes are used to satisfy the secrecy constraints. The estimation theoretic secrecy is also employed in distributed inference networks, where the information coming to a fusion center from various sensor nodes can also be observed by eavesdroppers [15].

In estimation theoretic approaches, the Cramér–Rao bounds (CRBs) provide useful fundamental limits for assessing performance of estimators, hence they can be employed as a performance metric for the intended receiver to optimize [16], [19]. In this regard, the optimal parameter encoding for secret communication is investigated based on the expectation of conditional CRB (ECRB) in [16]. In particular, the optimal encoding function is obtained to minimize the ECRB at the intended receiver, while keeping the MSE at the eavesdropper above a certain threshold. Instead of the ECRB metric employed in [16], this letter focuses on the worst case CRB (equivalently, the worst case Fisher information) in order to develop a robust parameter encoding approach that guarantees a certain level of estimation accuracy at the intended receiver. The proposed problem requires different solution approaches than that in [16] due to the minimax nature of the worst case optimization.

In this letter, we investigate the transmission of a uniformly distributed scalar parameter to an intended receiver in the presence of an eavesdropper. To facilitate secret communications, we utilize an encoding function applied on the original parameter. The objective is to minimize the maximum CRB (equivalently, to maximize the minimum Fisher information) at the intended receiver while ensuring a certain MSE target at the eavesdropper. The eavesdropper is modeled to employ the linear MMSE (LMMSE) estimator based on the noisy observation of the encoded parameter without being aware of encoding. An optimization problem is formulated to obtain the optimal encoding function for a given target MSE level at the eavesdropper. First, the secrecy constraint is omitted and the optimization problem is solved under no constraints, which yields a closed-form analytical solution. Then, to solve the optimal encoding problem in the presence of the MSE constraint on the eavesdropper, the optimal encoding function that maximizes the MSE at the eavesdropper is derived analytically for any given level of minimum Fisher information at the intended receiver. Based on this analytical result, a low-complexity algorithm is proposed to obtain the solution of the proposed problem.

II. Problem Formulation

A scalar parameter $\theta \in \Lambda$ is to be transmitted to an intended receiver over a noisy channel, where the channel noise is represented by N_r and the instantaneous fading coefficient of the channel is denoted by constant h_r. In addition, there exists an eavesdropper that tries to estimate the parameter, θ [16].

Manuscript received July 25, 2017; revised September 4, 2017; accepted September 4, 2017. Date of publication September 7, 2017; date of current version September 22, 2017. The associate editor coordinating the review of this manuscript and approving it for publication was Prof. Yong Xiang. *(Corresponding author: Sinan Gezici.)*

The authors are with the Department of Electrical and Electronics Engineering, Bilkent University, Ankara 06800, Turkey (e-mail: cgoken@ee.bilkent.edu.tr; gezici@ee.bilkent.edu.tr).

Color versions of one or more of the figures in this letter are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/LSP.2017.2749517

The objective is to perform accurate estimation of the parameter at the intended receiver while keeping the estimation error at the eavesdropper above a certain level. Therefore, the parameter is encoded by a continuous (except at a finite number of points), real valued, and one-to-one function $f : \Lambda \rightarrow \Gamma$. Then, the received signal at the intended receiver is expressed as $Y = h_r f(\theta) + N_r$, where N_r is modeled as a zero-mean Gaussian random variable with a variance of σ_r^2 and is independent of θ. Also, it is assumed that θ has uniform distribution over Λ. On the other hand, the eavesdropper observes $Z = h_e f(\theta) + N_e$, where N_e is zero-mean Gaussian noise with a variance of σ_e^2, which is independent of θ, and h_e is the fading coefficient for the eavesdropper [2], [3]. The intended receiver tries to estimate parameter θ by using observation Y, whereas the eavesdropper employs observation Z for estimating θ (see Fig. 1 in [16] for the system model).

A robust approach is proposed in this letter for the optimal parameter encoding design and the worst case (maximum) CRB is used for quantifying the estimation accuracy at the intended receiver. Namely, the aim is to minimize the maximum CRB over the parameter set via an encoding function while keeping the MSE at the eavesdropper (which employs the LMMSE estimator) above a certain target value. Hence, the following problem formulation is proposed

$$f_{\text{opt}} = \arg\min_{f} \max_{\theta} \big(I(\theta)\big)^{-1} \text{ s.t. } E\big(\big|\hat{\beta}(Z) - \theta\big|^2\big) \geq \eta \quad (1)$$

where $\hat{\beta}(Z)$ is the LMMSE estimator employed at the eavesdropper, η is the MSE target for the eavesdropper, $(I(\theta))^{-1}$ represents the CRB, and $I(\theta)$ denotes the Fisher information, which is given by $I(\theta) = \int \left(\frac{\partial \log p_{Y|\theta}(y)}{\partial \theta}\right)^2 p_{Y|\theta}(y) dy$ with $p_{Y|\theta}(y)$ representing the conditional probability density function of Y for a given value of θ [19]. The problem in (1) can also be stated as

$$f_{\text{opt}} = \arg\max_{f} \min_{\theta} I(\theta) \text{ s.t. } E\big(\big|\hat{\beta}(Z) - \theta\big|^2\big) \geq \eta \quad (2)$$

which means that the aim is to maximize the minimum (worst case) Fisher information at the intended receiver. It is noted that the distribution of θ does not affect the objective function in (2) since the worst case parameter value is the main concern.

As motivated in [16], the parameter space and the intrinsic constraints on the encoding function f are specified as follows: 1) $\theta \in \Lambda = [a, b]$, 2) $f(\theta) \in [a, b]$, and 3) f is a continuous (except at a finite number of points) and one-to-one function.

III. Optimal Encoding Function

In this section, the solution of the proposed problem in (2) [equivalently, in (1)] is investigated in the absence and presence of the secrecy constraint. To that end, the Fisher information for parameter θ can be obtained as follows [16]:

$$I(\theta) = h_r^2 f'(\theta)^2 / \sigma_r^2 \quad (3)$$

where $f'(\theta)$ denotes the derivative of $f(\theta)$.

A. Optimization Without Secrecy Constraint

Consider the optimization problem in (2) without the secrecy constraint; i.e., in the absence of the eavesdropper. From (3), the problem in (2) can be expressed by removing the constant terms as

$$f_{\text{opt}}(\theta) = \arg\max_{f} \min_{\theta} f'(\theta)^2 \,. \quad (4)$$

The following proposition is related to the solutions of (4).

Proposition 1: The optimal continuous encoding functions in the absence of an eavesdropper are $f(\theta) = a + b - \theta$ and $f(\theta) = \theta$.

Proof: Let T denote an operator on $f(\theta)$ such that $T(f) = \min_\theta f'(\theta)^2$. It is given that f is one-to-one but not necessarily a monotone function over $[a, b]$ due to the possibility of discontinuous points. However, f has to be monotone over the interval between any two consecutive discontinuous points as it is one-to-one. Thus, for any one-to-one function f, there exists a monotone function f_m such that $T(f) = T(f_m)$, which can be generated by adjusting the signs of the derivatives without changing their absolute values. Hence, it can be assumed without loss of generality that f is a monotone function. Furthermore, it is noted that since f is not differentiable at discontinuous points and $T(f)$ is the pointwise minimum of $f'(\theta)^2$, the points at which the jumps occur cannot be the optimal points. Therefore, one can remove the jumps at the discontinuities to obtain a continuous version, denoted by f_c. Thus, for any one-to-one function f, there exists a continuous function f_c such that $T(f) = T(f_c)$; hence, it can also be assumed that f is a continuous function without any loss. First, consider the case of $f'(\theta) > 0$, $\forall \theta \in [a, b]$. Then, based on the properties of the encoding function f, $\int_a^b \frac{df}{d\theta} d\theta = f(b) - f(a) \leq b - a$. Let $g(\theta)$ be defined as $g(\theta) \triangleq f'(\theta)$. Then, the problem in (4) becomes $\max_g \min_\theta g(\theta)^2$ subject to $\int_a^b g(\theta) d\theta \leq b - a$ and $g(\theta) > 0$. Consider the function $g^*(\theta) = 1$, $\forall \theta \in [a, b]$, which satisfies both of the constraints. Next, suppose that there exists a function h with $\min_\theta h(\theta) > 1$. Then, $\int_a^b h(\theta) d\theta > b - a$, leading to a violation of the constraint. Hence, for any given function g, there is an upper bound specified as $\min_\theta g(\theta) \leq 1$. Since the constant function satisfies this upper bound, it is the maximizer over all possible functions. Since $g(\theta) = 1$ for $\theta \in [a, b]$, it is obtained that $f(\theta) = \theta$ is an optimal solution. For the case of $f'(\theta) < 0$, let $g(\theta) \triangleq -f'(\theta)$. Then, based on similar arguments, $g(\theta) = 1$ can be obtained, resulting in an optimal solution of $f(\theta) = a + b - \theta$.[1] ■

Proposition 1 reveals that if there exist no secrecy constraints, parameter encoding does not provide any benefits in terms of the worst case Fisher information as $f(\theta) = \theta$ is optimal.

B. Optimization With Secrecy Constraint

To obtain the optimal encoding function in the presence of the secrecy constraint, the problem in (2) can be rewritten, based on (3), as

$$f_{\text{opt}}(\theta) = \arg\max_{f} \min_{\theta} f'(\theta)^2 \text{ s.t. } E\big(\big|\hat{\beta}(Z) - \theta\big|^2\big) \geq \eta \quad (5)$$

where the additional constraints on the parameter domain and the encoding function are as stated at the end of Section II. Since the eavesdropper employs the LMMSE estimator, the MSE at the eavesdropper can be expressed as [16]

$$E\big(\big|\hat{\beta}(Z) - \theta\big|^2\big) = \frac{h^2 V(V - 2C)}{h^2 V + 1} + (E(X) - E(\theta))^2 + \text{Var}(\theta) \quad (6)$$

where $X = f(\theta)$, $V = \text{Var}(X)$, $C = \text{Cov}(X, \theta)$, and $h = h_e/\sigma_e$.[2] From (5), it is noted that the optimal encoding func-

[1] The solution set for (4) also contains the set of all one-to-one functions on $[a, b]$ with $f(\theta) \in [a, b]$ and with finitely many discontinuous points, where between any two consecutive discontinuities, $|f'(\theta)| = 1$. Hence, there exist infinitely many encoding functions that solve (4). The encoding functions in Proposition 1 correspond to the optimal continuous solutions.

[2] It is noted from (5) and (6) that the transmitter requires the knowledge of the channel quality parameter for the eavesdropper, h, which can be challenging

tion should satisfy the MMSE constraint by making the smallest slope in $[a,b]$ as large as possible. It is known that when the secrecy constraint is not effective (or, removed), the linear encoding function is optimal according to Proposition 1, and $|f'_{\rm opt}(\theta)|=1$. Therefore, for a given target level η in (5), one strategy to find the optimal encoding function is to search among eligible encoding functions that satisfy $\min_{\theta\in[a,b]}|f'(\theta)|=k$ and to check if any of them satisfies the target secrecy level, where k is set to 1 initially. If there exist no solutions for a given k, then k is decreased and the procedure is repeated, until a feasible function satisfying the secrecy constraint is found. Let $\mathcal{F}^k$ denote the family of one-to-one and continuous (except at a finite number of points) functions with the domain and codomain being given by $[a,b]$, and $\min_\theta|f'(\theta)|=k$. Then, a sufficient condition for optimality of $f\in\mathcal{F}^k$ is that it should satisfy the secrecy constraint and there should be no elements in $\mathcal{F}^m$ that satisfy the secrecy constraint for $m>k$. To determine whether the secrecy constraint can be satisfied for a given k, the highest MMSE at the eavesdropper has to be calculated for that specific value of k. Hence, the solution of the following optimization problem should be performed in the first step:

$$\hat{f}_{\rm opt}=\arg\max_{\hat{f}}\ E\big(\big|\hat{\beta}(Z)-\theta\big|^2\big)\ \text{s.t. } k\le\big|\hat{f}'(\theta)\big|,\forall\theta\in[a,b] \tag{7}$$

where $0\le k\le 1$ is a given parameter.

Remark 1: The domain of the parameter is taken to be $\Lambda=[a,b]$ in the general case. However, due to Proposition 2 in [16], it can be assumed that $\Lambda=[0,\gamma]$ and $\hat{f}(\theta):[0,\gamma]\to[0,\gamma]$, where $\gamma=b-a$, without loss of generality. Hence, in the rest of the manuscript, θ is assumed to be distributed uniformly in $[0,\gamma]$.

The following result characterizes the solution of (7).

Proposition 2: For a given k, the form of the solution of (7) is given by

$$\hat{f}_{\rm opt}(\theta)=\begin{cases}\gamma-\theta k, & \text{if } 0\le\theta\le\alpha\\ \gamma k-\theta k, & \text{if } \alpha<\theta\le\gamma\end{cases}. \tag{8}$$

Furthermore, if $2-\frac{h^2\gamma^2}{12}(2k-k^2)\ge(k+1)(h^2V_{\min}+1)(h^2V_{\max}+1)$, where h is the channel quality for the eavesdropper, $V_{\min}=\frac{k^2\gamma^2}{12}$ and $V_{\max}=\frac{k^2\gamma^2}{12}+\frac{(1-k)\gamma^2}{4}$, then, both $\alpha=0$ and $\alpha=\gamma$ are optimal α values. Otherwise, $\alpha=\gamma/2$ is optimal.

Proof: The first step in the proof is to specify the characteristics of the encoding function that maximizes the LMMSE. Note that $f(\theta)=X$ results in a random variable with $V=\mathrm{Var}(X)$, $C=\mathrm{Cov}(X,\theta)$ and $\mu=E(X)$, and the value of $E(|\hat{\beta}(Z)-\theta|^2)$ depends on these values. Hence, the LMMSE value is to be maximized over the possible values of V, C, and μ. It is noted that the slope constraint induces limitations on the possible values of μ, V, and C. Let S^k denote the feasible set of μ, V, and C values in the presence of the constraint $k\le|f'(\theta)|$. As parameter θ is distributed uniformly on the interval $[0,\gamma]$, $E(\theta)=\gamma/2$ and $\mathrm{Var}(\theta)=\gamma^2/12$. Then, the optimization problem in (7) can be expressed as $\max_{\mu,V,C}\ \frac{h^2V(V-2C)}{h^2V+1}+\big(\mu-\frac{\gamma}{2}\big)^2+\frac{\gamma^2}{12}$, $(\mu,V,C)\in S^k$. After some manipulation, the objective function in this optimization problem can be stated as $\lambda(V)E(|X-\theta|^2)+(1-\lambda(V))(\mu^2-\gamma\mu+\gamma^2/3)$, where $\lambda(V)\triangleq h^2V/(h^2V+1)$. Note that for a given μ, $E(|X-\theta|^2)$ can be maximized, which would yield an upper bound on the objective function. It can be found by inspection that when the slope constraint is taken into account, $E(|X-\theta|^2)$ is maximized for

$$\hat{X}^\alpha=\begin{cases}\gamma-\theta k, & \text{if } 0\le\theta\le\alpha\\ \gamma k-\theta k, & \text{if } \alpha<\theta\le\gamma\end{cases} \tag{9}$$

where $(1-k)\alpha=\mu-k\gamma/2$ and $k\gamma/2\le\mu\le\gamma-k\gamma/2$. Hence, the following the relationship is obtained

$$\begin{aligned}E\big(\big|\hat{\beta}(Z)-\theta\big|^2\big)&\le\lambda(V)\beta_1(\alpha,k)+(1-\lambda(V))\beta_2(\alpha,k)\\&=\lambda(V)(\beta_1(\alpha,k)-\beta_2(\alpha,k))+\beta_2(\alpha,k)\end{aligned} \tag{10}$$

with $\beta_1(\alpha,k)\triangleq(k^2-1)(\alpha^2-\gamma\alpha)+(k^2-k+1)\gamma^2/3$ and $\beta_2(\alpha,k)\triangleq(k-1)^2(\alpha^2-\gamma\alpha)+(3k^2/4-3k/2+1)\gamma^2/3$. Now, notice that for a fixed k, the following equality holds: $\beta_1(\alpha,k)-\beta_2(\alpha,k)=(\alpha^2-\gamma\alpha)(2k-2)+\left(\frac{k^2}{4}+\frac{k}{2}\right)\frac{\gamma^2}{3}$. Since $\beta_1(\alpha,k)$ is a concave function of α and $\beta_2(\alpha,k)$ is a convex function of α for $0\le k\le 1$, $\beta_1(\alpha,k)-\beta_2(\alpha,k)$ is a concave function of α; hence, it attains its minimum at $\alpha=0$ and $\alpha=\gamma$. Therefore, the following inequality is obtained: $\beta_1(\alpha,k)-\beta_2(\alpha,k)\ge(k^2/4+k/2)\gamma^2/3\ge 0$, which implies that for a given value of μ, the right-hand-side of (10) is an increasing function of $\lambda(V)$. Hence, a further upper bound can be obtained for (10) by using the same $\hat{X}^\alpha$ defined above since it maximizes the variance under the slope constraint. For this function, the variance is given by $V(\alpha,k)=(k-1)(\alpha^2-\alpha\gamma)+k^2\gamma^2/12$. It is noted that $\lambda(V(\alpha,k))$ and the resulting upper bound are functions of α for fixed k and h. Hence, the upper bound can be maximized over α as follows:

$$\begin{aligned}&E\big(\big|\hat{\beta}(Z)-\theta\big|^2\big)\\&\quad\le\lambda(V(\alpha,k))\beta_1(\alpha,k)+(1-\lambda(V(\alpha,k)))\beta_2(\alpha,k)\\&\quad=\lambda(V(\alpha,k))(\beta_1(\alpha,k)-\beta_2(\alpha,k))+\beta_2(\alpha,k)\\&\quad\triangleq g(\alpha,k)\le\max_{\alpha\in[0,\gamma]}g(\alpha,k).\end{aligned} \tag{11}$$

If $\hat{\alpha}=\arg\max_{\alpha\in[0,\gamma]}g(\alpha,k)$, then $E(|\hat{\beta}(Z)-\theta|^2)$ achieves this upper bound by employing $\hat{\alpha}$ at the encoding function. Therefore, the optimal encoding function is $\hat{X}^{\hat{\alpha}}$, where $\hat{\alpha}=\arg\max_{\alpha\in[0,\gamma]}g(\alpha,k)$.

To conclude the proof, $\hat{\alpha}$ should be characterized for given k and h. Overall, the optimization problem can be written as

$$\max_{\alpha\in[0,\gamma]}\frac{h^2V(\alpha,k)}{h^2V(\alpha,k)+1}(\beta_1(\alpha,k)-\beta_2(\alpha,k))+\beta_2(\alpha,k) \tag{12}$$

where $h,\gamma>0$ and $k\in[0,1]$. Instead of optimizing over α, the optimization can be performed over V based on a change of variables by noting that for $\alpha\in[0,\gamma]$, $V(\alpha,k)\in[V_{\min},V_{\max}]$, where $V_{\min}=k^2\gamma^2/12$ and $V_{\max}=k^2\gamma^2/12+(1-k)\gamma^2/4$. Then, (12) is rewritten as

$$\max_{V\in[V_{\min},V_{\max}]}z(V)=\frac{h^2(k+1)V^2+HV+F}{h^2V+1} \tag{13}$$

where $H=(h^2\gamma^2/12)(4-4k+3k^2-k^3)+k-1$ and $F=(\gamma^2/12)(4-6k+4k^2-k^3)$. Then, according to the Weierstrass theorem, the global maximum exists for (13), and the solution can be found by applying Fermat's rule. Namely, the optimal solution either satisfies $z'(V)=0$ or is at the boundary, i.e., $V=V_{\min}$ or $V=V_{\max}$. For $z'(V)=0$, $V^2+2V/h^2+d/h^4=0$, where $d=(H-Fh^2)/(k+1)$. Then, $\hat{V}=-h^{-2}+h^{-2}\sqrt{1-d}$ is a candidate solution. However, $\hat{V}$ should belong to $[V_{\min},V_{\max}]$.

to obtain accurately. Based on imperfect knowledge of h, the parameter encoding design can be performed, for example, by considering the minimum possible value of the MSE at the eavesdropper according to the uncertainty in the parameter (Remark 3 in [16]).

Algorithm 1: $f_{opt} = \text{ENCODER}(\eta)$.

```
% Δ is the decrement of slope at each iteration.
k ← 1
while k > 0 do
    Pick α = 0 or γ, if condition in Prop. 2 holds. Else, α = γ/2.
    X̂^α = f̂_opt(θ) as given in (8)
    MSE ← E(|β̂(X̂^α) − θ|^2)
    if MSE ≥ η then
        f_opt = X̂^α
        break
    else
        k ← k − Δ
    end
end
if k < 0 then
    Problem is infeasible
else
    return f_opt
end
```

To guarantee this condition, $h^2 V_{\max} \geq \sqrt{1-d} - 1 \geq h^2 V_{\min}$ should be satisfied. Therefore, $h^2 V_{\min} + 1 \leq \sqrt{1-d}$. If this holds, then $\text{sgn}(\lim_{V \to V_{\min}^+} z'(V) = \text{sgn}(V_{\min}^2 + 2h^{-2} V_{\min} + h^{-4} d) \leq 0$. In conclusion, it is possible that a candidate solution is inside the feasible interval $[V_{\min}, V_{\max}]$; however, there is only one such solution and V is decreasing at the beginning of the interval. Due to continuity, it is noted that if $\hat{V} \in (V_{\min}, V_{\max})$, then it is in fact the global minimum. Hence, it is concluded that the solution of (13) is either $V_{\min}$ or $V_{\max}$, excluding the possibility of the other case. Finally, the regions in which a certain end point is optimal are characterized. The condition of $z(V_{\min}) \geq z(V_{\max})$ occurs if h and k satisfy $2 - \frac{h^2\gamma^2}{12}(2k - k^2) \geq (k+1)(h^2 V_{\min} + 1)(h^2 V_{\max} + 1)$ and $z(V_{\min}) < z(V_{\max})$ holds otherwise. Note that if the optimal solution is $V_{\max}$, then $\hat{\alpha} = \gamma/2$. If the optimal solution is $V_{\min}$, both $\hat{\alpha} = 0$ and $\hat{\alpha} = \gamma$ are the optimal solutions. ■

As the form of the optimal encoding function that maximizes the LMMSE at the eavesdropper is derived for any value of the minimum slope constraint (k) via Proposition 2, the optimal encoding function based on the worst case Fisher information metric can be obtained by finding the maximum of such constraints. Hence, the problem reduces to the determination of the best (maximum) value of $k \in (0, 1]$ such that $\exists f \in \mathcal{F}^k$ in the form specified by (8) that satisfies the secrecy constraint. This approach can be implemented by using the procedure shown in Algorithm 1. It is noted that $E(|\hat{\beta}(\hat{X}^\alpha) - \theta|^2)$ in Algorithm 1 can be calculated explicitly via (6) and (8).

IV. Numerical Results and Conclusion

In this section, a numerical example is provided based on the theoretical results and the proposed algorithm in Section III. The channel parameters are selected as $h_r = \sigma_r = 1$ for the intended receiver and $h = 0.5$ and $h = 1.5$ for the eavesdropper. The parameter θ is assumed to be uniformly distributed in the interval of $[0, 2]$; i.e., $\gamma = 2$. The eavesdropper employs the LMMSE estimator by using the observations based on the encoded parameter $X = f(\theta)$. Also, Δ is set to 0.001 in the proposed algorithm for calculating the optimal encoding functions. In Fig. 1, the worst case Fisher information values achieved by the proposed algorithm are presented with respect to the target secrecy level for $h = 0.5$ and $h = 1.5$. For comparison purposes, the worst case Fisher information values corresponding to the ECRB based encoding algorithm in [16] are also provided in the same figure. (The proposed scheme provides higher worst case Fisher information than the ECRB based scheme since the latter aims to optimize the average CRB.) In Fig. 2, the optimal encoding functions based on the worst case Fisher information metric are provided for various η values for $h = 0.5$. As justified in Proposition 2, the optimal encoding function is either linear with a certain slope between 0 and 1, or piecewise linear with a single discontinuity at $\theta = \gamma/2$ depending on the target secrecy level η.

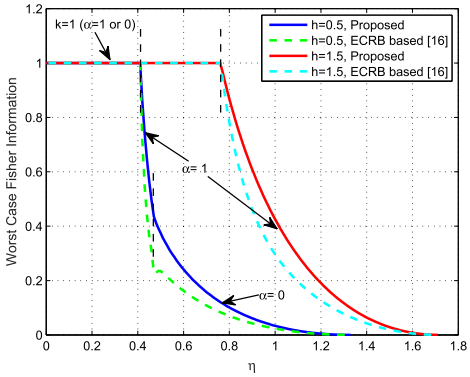

Fig. 1. Worst case Fisher information versus η.

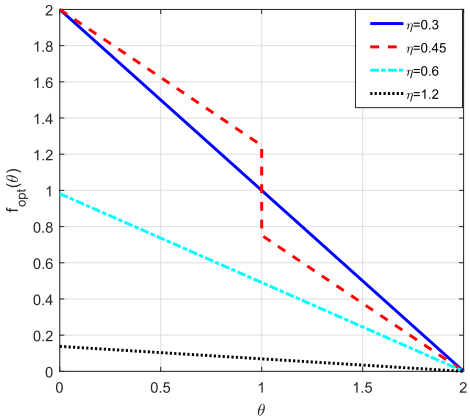

Fig. 2. $f_{\text{opt}}(\theta)$ versus θ for $h = 0.5$.

In Fig. 1, it is observed that as the target secrecy level increases, the worst case Fisher information achieved by the proposed algorithm decreases, as expected. In addition, it is possible to obtain higher worst case Fisher information values when $h = 1.5$ for the same MSE target compared to the case of $h = 0.5$ since the distortion due to the encoding is transmitted to the eavesdropper more effectively under better channel conditions. Note that when $h = 0.5$, the three different regions are observable in the performance figure. When $\eta \leq \eta_1 = 16/39 = 0.4101$, employing $k = 1$, that is, $f_{\text{opt}}(\theta) = \gamma - \theta$, is sufficient to attain the target secrecy levels. In general, η_1 can be found as $\eta_1 = 0.25\gamma^2 \left(h^2\gamma^2/(h^2\gamma^2 + 12) + 1/3\right)$. When $\eta_1 < \eta \leq \eta_2$ with $\eta_2 = 0.4708$, it is observed that the optimal α value becomes $\gamma/2$. It is noted that η_2 can be found by determining the point at which the inequality in Proposition 2 becomes an equality in general. Therefore, in this region, the optimal encoding function has a single discontinuity at $\theta = \gamma/2$. Finally, when $\eta_2 < \eta \leq 4/3$, the optimal α is 0; hence, the optimal encoding function is linear with no discontinuities. It is interesting to note that the worst case Fisher information decreases faster in the second region, and it decays to zero in the third region more slowly as compared to the second region. On the other hand, when $h = 1.5$, only two of such regions are observed in Fig. 1.

REFERENCES

[1] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, 1975.

[2] Y. Liang, H. V. Poor, and S. Shamai, "Secure communication over fading channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2470–2492, Jun. 2008.

[3] P. K. Gopala, L. Lai, and H. El Gamal, "On the secrecy capacity of fading channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 10, pp. 4687–4698, Oct. 2008.

[4] P. Xu, Z. Ding, X. Dai, and K. K. Leung, "A general framework of wiretap channel with helping interference and state information," *IEEE Trans. Inf. Forensics Security*, vol. 9, no. 2, pp. 182–195, Feb. 2014.

[5] H. Weingarten, Y. Steinberg, and S. S. Shamai, "The capacity region of the Gaussian multiple-input multiple-output broadcast channel," *IEEE Trans. Inf. Theory*, vol. 52, no. 9, pp. 3936–3964, Sep. 2006.

[6] O. O. Koyluoglu, H. El Gamal, L. Lai, and H. V. Poor, "Interference alignment for secrecy," *IEEE Trans. Inf. Theory*, vol. 57, no. 6, pp. 3323–3332, Jun. 2011.

[7] Y. Liang, A. Somekh-Baruch, H. V. Poor, S. Shamai, and S. Verdu, "Capacity of cognitive interference channels with and without secrecy," *IEEE Trans. Inf. Theory*, vol. 55, no. 2, pp. 604–619, Feb. 2009.

[8] L. Lai and H. El Gamal, "The relay-eavesdropper channel: Cooperation for secrecy," *IEEE Trans. Inf. Theory*, vol. 54, no. 9, pp. 4005–4019, Sep. 2008.

[9] Z. Chu, K. Cumanan, Z. Ding, M. Johnston, and S. Y. Le Goff, "Secrecy rate optimizations for a MIMO secrecy channel with a cooperative jammer," *IEEE Trans. Veh. Technol.* vol. 64, no. 5, pp. 1833–1847, May 2015.

[10] Z. Chu, K. Cumanan, Z. Ding, M. Johnston, and S. L. Goff, "Secrecy rate optimization for a MIMO secrecy channel based on Stackelberg game," in *Proc. 2014 22nd Eur. Signal Process. Conf.*, Lisbon, Portugal, 2014, pp. 126–130.

[11] H. Shen, Y. Deng, W. Xu, and C. Zhao, "Secrecy-oriented transmitter optimization for visible light communication systems," *IEEE Photon. J.*, vol. 8, no. 5, pp. 1–14, Oct. 2016.

[12] H. Shen, W. Xu, and C. Zhao, "QoS constrained optimization for multi-antenna AF relaying with multiple eavesdroppers," *IEEE Signal Process. Lett.*, vol. 22, no. 12, pp. 2224–2228, Dec. 2015.

[13] W. C. Liao, T. H. Chang, W. K. Ma, and C. Y. Chi, "QoS-based transmit beamforming in the presence of eavesdroppers: An optimized artificial-noise-aided approach," *IEEE Trans. Signal Process.*, vol. 59, no. 3, pp. 1202–1216, Mar. 2011.

[14] A. Ozcelikkale and T. M. Duman, "Cooperative precoding and artificial noise design for security over interference channels," *IEEE Signal Process. Lett.*, vol. 22, no. 12, pp. 2234–2238, Dec. 2015.

[15] B. Kailkhura, V. S. S. Nadendla, and P. K. Varshney, "Distributed inference in the presence of eavesdroppers: A survey," *IEEE Commun. Mag.*, vol. 53, no. 6, pp. 40–46, Jun. 2015.

[16] C. Goken and S. Gezici, "ECRB based optimal parameter encoding under secrecy constraints," *IEEE Trans. Signal Proc.*, under review. [Online]. Available: http://www.ee.bilkent.edu.tr/∼gezici/ECRB.pdf

[17] T. C. Aysal and K. E. Barner, "Sensor data cryptography in wireless sensor networks," *IEEE Trans. Info. Forensics Security*, vol. 3, no. 2, pp. 273–289, Jun. 2008.

[18] M. Pei, J. Wei, K. K. Wong, and X. Wang, "Masked beamforming for multiuser MIMO wiretap channels with imperfect CSI," *IEEE Trans. Wireless Commun.*, vol. 11, no. 2, pp. 544–549, Feb. 2012.

[19] H. V. Poor, *An Introduction to Signal Detection and Estimation.* New York, NY, USA: Springer, 1994.