Private Message Transmission Using Disjoint Paths

Hadi Ahmadi[*] and Reihaneh Safavi-Naini

Department of Computer Science, University of Calgary, Canada[**]
{hahmadi,rei}@ucalgary.ca

Abstract. We consider private message transmission (PMT) between two communicants, Alice and Bob, in the presence of an eavesdropper, Eve. Alice and Bob have no shared keys and Eve is computationally unbounded. There is a total of n communicating paths, but not all may be simultaneously accessible to the parties. We let t_a, t_b, and t_e denote the number of paths that are accessible to Alice, Bob and Eve respectively. We allow the parties to change their accessed paths at certain points in time during the PMT protocol. We study perfect (P)-PMT protocol families that guarantee absolute privacy and reliability of message transmission. For the sake of transmission rate improvement, we also investigate asymptotically-perfect (AP)-PMT protocol families that provide negligible error and leakage and behave the same as P-PMT families when message length tends to infinity.

We derive the necessary and sufficient conditions under which P-PMT and AP-PMT are possible and introduce explicit PMT schemes. Our results show AP-PMT protocols attain much higher information rates than P-PMT ones. Interestingly, AP-PMT may be possible even in poor conditions where $t_a = t_b = 1$ and $t_e = n - 1$. We study applications of our results to private communication over the real-life scenarios of multiple-frequency links and multiple-route networks. We show practical examples of such scenarios that can be abstracted by the multipath setting: Our results prove the possibility of keyless information-theoretic private message transmission at rates 17% and 20% for the two example scenarios, respectively. We discuss open question and future work.

1 Introduction

With the rapid growth of online communication, an increasing number of daily activities are moved to the online world and fall under prying eyes resulting in increasing loss of privacy. Personal data can be under surveillance by various entities. Hackers easily tap into WiFi connections to steal online communication data [9]. There are reported news on security agencies watching civilian communications through routers in the Internet [8]. Given massive computational resources accessible to the adversaries, naïve usage of traditional cryptographic

[*] The author has moved to Nulli Identity Solution Inc., Canada (hahmadi@nulli.com).

[**] This work is in part supported by Alberta Innovates Technology Futures.

I. Boureanu, P. Owesarski, and S. Vaudenay (Eds.): ACNS 2014, LNCS 8479, pp. 116–133, 2014.

systems for protecting communication in many cases creates a false sense of security rather than real protection [7]. Development of quantum algorithms such as Shor's algorithm [13] will also render all today's widely used crypto algorithms insecure. The widely known one-time-pad alternative with information-theoretic security requires prior sharing of long keys, which is impractical.

In this paper, we investigate using multiple paths of communication as an alternative resource for providing privacy against a computationally-unbounded eavesdropper. A path may have different realizations such as a network route, a frequency channel in wireless communication, or a fiber strand in fiber-optics. Using path redundancy for security has been considered in the context of secure message transmission (SMT) [5]. The focus of SMT research however has been security against Byzantine active adversaries, an objective which is impossible in many cases of interest where the majority of paths are corrupted. Note that studying active adversaries is not necessary for networks under surveillance.

1.1 Our Work: PMT in the Multipath Setting

We consider message transmission over the following abstract communication system with three parties: a message sender *Alice*, a message receiver *Bob*, and an eavesdropper *Eve.* Alice wants to send a message to Bob, without leaking information to computationally-unbounded Eve. There is no shared key between Alice and Bob. The system provides n disjoint paths, but not all paths can be accessed simultaneously: Alice, Bob, and Eve can have access to up to t_a, t_b, and t_e paths at a time, respectively. We assume time is divided into intervals of equal length λ, and the parties can change their accessed paths at the beginning of each time interval. The value of λ is determined by the technological limitations of the parties, esp. Eve, in switching between paths.

We refer to this problem as private message transmission (PMT) in the $(n, t_a, t_b, t_e, \lambda)$*-multipath setting.* We provide formal definitions of PMT protocols in this setting. Foremost, we are interested in necessary and sufficient connectivity conditions, under which PMT is possible. But we do not stop here. We study how to attain the so-called *secrecy capacity*, i.e., highest possible rate (message bits divided by communicated bits). The study of secrecy capacity and optimal constructions is essential due to bandwidth limitations and communication cost in most practical scenarios.

P-PMT and AP-PMT. The security of PMT protocols is measured by reliability (δ) and secrecy (ϵ) parameters. The former shows the probability of "incorrect" transmission and the latter represents information leakage. Ideally, a PMT protocol is expected to provide perfect security $\delta = \epsilon = 0$. Relaxing the security requirements to a desired extent may however let PMT at higher rates. We consider designing of two types of PMT protocol families, namely *perfect (P)-PMT* families with perfectly-secure protocols and *asymptotically-perfect (AP)-PMT* families that allow positive yet decreasing δ and ϵ, with respect to message length. The latter family is particularly interesting because it may provide security for a much wider connectivity range. We define *P-secrecy capacity* C_0 and

AP-secrecy capacity $C_{\sim 0}$ as the highest achievable rates by P-PMT and AP-PMT families. We start our investigation in full-access case (when $t_a = t_b = n$), and then extend the study to the general case.

PMT Results. Our precise results on P-PMT and AP-PMT protocols are rather complex (see Section 5). For the sake of a quick overview, we provide in Table 1 an approximation of these results for sufficiently large λ. Section 6 gives details about why assuming large λ is plausible.

Table 1. PMT conditions and capacities in the $(n, t_a, t_b, t_e, \lambda)$-multipath setting

		Full Access		**Partial Access**	
		One-way	Two-way	One-way	Two-way
Condition	**P-PMT**	$t_e < n$		$t_e < t_{ab}$	
	AP-PMT			$t_e < t_b$	$t_e < n$
Capacity	$\mathbf{C_0}$	$\approx 1 - \frac{t_e}{n}$		$\approx [1 - \frac{t_e}{t_{ab}}]_+$	
	$\mathbf{C_{\sim 0}}$			$\approx 1 - \frac{t_e}{n}$	$\approx 1 - \frac{t_e}{n}$

In the full-access case, P-PMT and AP-PMT behave the same in rate and connectivity condition. This result is not surprising: When $t_e = n$, Eve can collect all data communicated over the paths to retrieve the message. Conversely when $t_e < n$, message is divided into n shares and sent such that $n - t_e$ shares remain private, implying the secrecy rate of $1 - \frac{t_e}{n}$. We show that relaxing security to asymptotically-prefect does not change the results. Surprisingly however, in the case of partial-access, AP-PMT shows a huge advantage. P-PMT protocols cannot exceed rate $[1 - \frac{t_e}{t_{ab}}]_+$, with $t_{ab} = \min\{t_a, t_b\}$, whereas it is possible to get rates close to $1 - \frac{t_e}{n}$ through AP-PMT. To appreciate this advantage more, consider cases where Alice and Bob possess poor connectivity, but Eve has access to almost all paths (i.e., $t_a, t_b \ll t_e \approx n$): While P-PMT is clearly impossible, one may take the benefit of positive-rate AP-PMT protocols.

We introduce one-round and two-round AP-PMT schemes to prove our AP-secrecy rates. The schemes consist of two primitive blocks, namely a (low-rate) *key establishment block* followed by a (high-rate) *coordinated (keyed) PMT block*. The former allows the parties to share a secret key and the latter allows them to use the secret key for high rate message transmission.

Practical Consideration. To show the practical relevance of our results, we elaborate on two example scenarios of communication over multiple-frequency links and multiple-route networks and show private communication is achieved at rates 17% and 20%, respectively. *This provides a novel attempt to build optimal-rate communication with information-theoretic privacy in these scenarios.*

Secrecy Rates and Multipath Setting Parameters. Although it may not be clearly from Table 1, precise secrecy rates of P-PMT and AP-PMT (see Section 5) depend on all multipath setting parameters $(n, t_a, t_b, t_e, \lambda)$. Here are a few words on how the rates are affected generally by these parameters. First, all secrecy rates are functions of path ratios $\frac{t_a}{n}$, $\frac{t_b}{n}$, and $\frac{t_e}{n}$: As long as these three values are not changed increasing/decreasing the total number n of paths does not affect the derived rates. Next (and intuitively), the rates are improved by allowing Alice and Bob higher connectivity (increasing $\frac{t_a}{n}$ and $\frac{t_b}{n}$) and are decreased when Eve obtains higher connectivity ($\frac{t_e}{n}$ is increased). Finally, having longer time intervals (larger λ) results in better rates: The reason is larger λ implies that Alice and Bob can send more information before Eve switches her accessed paths.

1.2 Related Work and Discussion

Secure Message Transmission. In secure message transmission (SMT) [5], Alice and Bob are connected by n paths, out of which $t \leq n$ can be corrupted by the active adversary, Eve. The objective is to guarantee privacy and reliability of a transmitted message. Our study of PMT deviates in a few directions from SMT. Firstly, we focus on passive attacks and study capacity-achieving constructions. Note that a great portion of threats to online communication are passive and using immediate SMT results is an over-design with sub-optimal solutions.

Secondly, SMT assumes Alice and Bob can use all n paths. In dense networks or wide-band frequency channels however, there are more communication paths than parties can possibly afford access. We address this by allowing partial access for Alice and Bob. Last but not least, there is no concept of time interval in SMT, i.e., Alice and Bob can communicate arbitrarily many bits (in a round) without Eve switching her corrupted paths. In a real-life scenario however, Eve may switch paths if enough time is provided. We capture this by adding a time-interval length parameter λ to our abstract model. A SMT protocol that transmits more than λ bits in one round without accounting for Eve's movements is not necessarily functional in our new model. Note that the last two differences cause our study to be more general than SMT.

Frequency Hopping. Frequency-hopping spread spectrum (FHSS) is a communication technique which transmits data as a sequence of blocks sent over pseudorandom frequency channels. The technology has appeared in early WiFi and Bluetooth applications to enhance resistance against interference and narrow-band noise, and more recently, to countermeasure jamming-based denial of service (DoS) attacks [15]. FHSS originally requires share keys between the communicants. Strasser et al. [14] introduced keyless or uncoordinated frequency hopping (UFH) for jamming-resistant key establishment. Although UFH provides "jamming resistance" security without share keys, its security relies on higher-layer cryptography, which implies two drawbacks: (i) the need for a public-key infrastructure and (ii) only computational security guarantees. Looking at a different objective, our PMT results show the possibility of private communication over multiple-frequency channels. In contrast to UFH, the PMT guarantees (i) do not rely on higher-layer cryptography, and (ii) provide security against computationally-unlimited adversaries.

Notation. For real value x, we denoted $[x]_+ = \max\{0, x\}$. For two random variables $X \in \mathcal{X}$ and $Y \in \mathcal{Y}$, we denote their statical distance by $SD(X, Y) = 0.5 \sum_{x \in \mathcal{X}} |\Pr(X = x) - \Pr(Y = x)|$. Throughout, we use $(n, t_a, t_b, t_e, \lambda)$ as multipath setting parameters, and let $t_{ab} = \min(t_a, t_b)$ and $\Delta = 2^{\frac{\lambda}{2}-2} - 0.25)^{-1}$. We consider Δ to be negligible for our numerical analysis by assuming large λ.

2 Preliminaries: Ramp and Quasi-ramp Secret Sharing

A secret sharing scheme (SSS) distributes a secret S among a set of m players such that every "qualified" subsets can reconstruct S, while no information is leaked to an "unqualified" subset. The scheme is defined by a pair $(\mathbf{Share}, \mathbf{Rec})$ of functions: **Share** maps secret S to shares $\underline{X} = (X_1, X_2, \ldots, X_m)$ and **Rec** maps shares $\underline{X}' = (X'_1, \ldots, X'_m)$ to a secret reconstruction $\hat{S}$. A (k, m)-threshold SSS [12] distributes the secret via m shares such that any $\geq k$ shares are qualified and any $\leq k - 1$ shares are unqualified. A (k, r, m)-ramp SSS extends the above (to $r \neq 1$) such that any $\geq k$ shares are qualified and $\leq k - r$ shares are unqualified, and information leakage increases by the number of shares.

Polynomial-based ramp SSS. The simplest (k, r, m)-ramp SSS is Shamir's polynomial-based construction [12] denoted by $(\mathbf{Share}_{pol}, \mathbf{Rec}_{pol})$ and described below. Define integer $p \geq m + r$ and let $S = (S_0, \ldots, S_{r-1}) \in \mathbb{F}_p^r$ be the secret.

- $\mathbf{Share}_{pol}(S)$ chooses a random polynomial $f(x)$ of degree $\leq k-1$ over $\mathbb{F}_p[x]$, such that $f(0) = S_0, f(1) = S_1, \ldots, f(r-1) = S_{r-1}$; it returns m shares $X_1 = f(r), \ldots, X_m = f(r + m - 1)$.
- $\mathbf{Rec}_{pol}(\underline{X}')$ chooses the first k present shares: If this is not possible, returns $\perp$; otherwise obtains $f(x)$ through interpolation and returns $S = (f(0), f(1), \ldots, f(r-1))$.

Algebraic-geometric Quasi-ramp SSS. The polynomial-based ramp SSS requires $m + r \leq p$ since there is only p points on the polynomial. Algebraic-geometric constructions relax this requirement by using curves of high genus. Garcia and Stichtenoth [6, Theorem 3.1] show an explicit family of curves with arbitrary genus g and $(\sqrt{p}-1)g$ many points over $\mathbb{F}_p$ (when p is a square). Chen and Cramer [3] use these curves to construct an algebraic geometric (k, r, g, m)-quasi-ramp SSS for any $m < (\sqrt{p}-1)g$ shares. A Quasi-ramp SSS allows $\geq k+2g$ shares to be qualified and any $\leq k - 1$ shares to be unqualified.

(k, r, g, m)-quasi-ramp SSS $(\mathbf{Share}_{alg}, \mathbf{Rec}_{alg})$. Let $\mathcal{C}$ be a Garcia-Stichtenoth curve with genus g over $\mathbb{F}_p$, where p is a square and $(\sqrt{p}-1)g \geq m+r$. Define Q, $P_0, P_1, \ldots, P_{m+r-1}$ as any $m+r+1$ distinct rational points on $\mathcal{C}$, $D = (k+2g).(Q)$ as a rational divisor of $\mathcal{C}$, and $\mathcal{L}(D)$ as the Riemann-Roch space associated with D. Let $S \in \mathbb{F}_p^r$ be the secret.[1]

[1] Refer to [3] for the definitions of rational divisor and Riemann-Roch space.

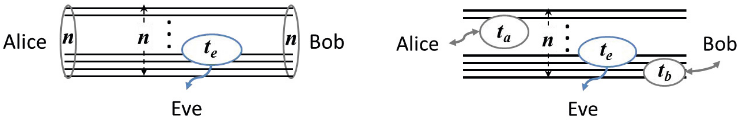
- $\mathbf{Share}_{alg}(S)$ chooses a random function $f(.) \in \mathcal{L}(D)$ such that $f(P_0) = S_0, f(P_1) = S_1, \ldots, f(P_{r-1}) = S_{r-1}$ and returns shares $X_1 = f(P_r), \ldots, X_m = f(P_{m+r-1})$ over $\mathbb{F}_p$.
- $\mathbf{Rec}_{alg}(X'_1, \ldots, X'_m)$ chooses the first $k + 2g$ present shares: If not possible, returns $\perp$); otherwise, obtains $f(.)$ through linear interpolation and returns $S = (f(0), f(1), \ldots, f(r-1))$.

The above SSS allows for more shares at the price of increasing the gap between the number of qualified and unqualified players. If field size p is large enough, one can generate $\sqrt{p} - 1$ additional shares by allowing only 2 players gap in SSS. We use this interesting property in our PMT constructions which let $p = 2^\lambda$, for time-interval length λ.

3 Problem Description

3.1 Multipath Setting Abstraction

A *multipath setting* refers to an abstract communication system which consists of n disjoint communication paths, out of which at most t_a, t_b, and t_e can be simultaneously accessed by Alice, Bob, and Eve, respectively. More precisely, time is divided into equal-length intervals each of which corresponds to λ bits of communication over at least one path. In the beginning of a time intervals, the parties choose their access paths and will hold on to their choice till the end of that interval, i.e., until λ bits are communicated over a path. This abstraction of time intervals in bits is obtained by multiplying the bit-transmission speed by path switching time. The value of λ depends on how fast the communicants and (more importantly) Eve can release old paths and capture new paths without possibly missing the live communication. This relates to the actual communication scenario, the communication capability of devices, and the transmission speed. We shed more light on this in Section 6: The practical scenarios considered there suggest typical values of $\lambda > 100$. To summarize, a multipath setting is defined by five public parameters $(n, t_a, t_b, t_e, \lambda)$ and we denote $t_{ab} = \min(t_a, t_b)$ throughout. When $t_{ab} = n$, we refer to the setting as the (n, t_e, λ)-full-access setting. Figure 1 illustrates full-access versus partial-access settings.



(a) Full-access: $t_a = t_b = n$. (b) Partial-access: $t_a, t_b \leq n$.

Fig. 1. Full-access vs. partial-access multipath settings

3.2 PMT protocol and Secrecy Capacity: Definition

To deliver message S from Alice to Bob, a PMT protocol makes them communicate sequences of data so that Bob can obtain an estimate $\hat{S}$. The protocol leaves Eve with some view $View_E(S)$ of the communication. The randomness in $View_E(.)$ comes from the PMT protocol and the adversary.

Definition 1 (PMT Protocol). *A protocol Π over a multipath setting is a (k, c, δ, ϵ)-PMT protocol if it transmits any k-bit message using c bits of communication such that*

$$\begin{aligned} \textit{Reliability}: \ \forall s \in \{0,1\}^k : \quad & \Pr(\hat{S} \neq s) \leq \delta, & (1) \\ \textit{Secrecy}: \quad \forall s_1, s_2 \in \{0,1\}^k : \quad & SD\left(View_E(s_1), View_E(s_2)\right) \leq \epsilon. & (2) \end{aligned}$$

Π is called perfect (P)-PMT if $\delta = \epsilon = 0$. The secrecy rate *of Π equals $R = \frac{k}{c}$.*

In practice, the message length may be unknown beforehand and one needs a family of PMT protocols for arbitrarily long messages. PMT families are desired to have a guaranteed rate for any message length. We refer to this guaranteed rate as the *secrecy rate* of the family.

Definition 2 ((δ, ϵ)-PMT and P-PMT Families). *A (δ, ϵ)-PMT family $\mathcal{F}$ for a multipath setting $\mathscr{S}$ is a sequence $(\Pi_i)_{i \in \mathbb{N}}$, where for each i, Π_i is a $(k_i, c_i, \delta, \epsilon)$-PMT protocol over $\mathscr{S}$ and $k_{i+1} > k_i$. The (δ, ϵ)-secrecy rate of $\mathcal{F}$ equals $R_{\mathcal{F}:\delta,\epsilon} = \inf\{\frac{k_i}{c_i} : i \in \mathbb{N}\}$.[2] When $\delta = \epsilon = 0$, $\mathcal{F}$ is called a perfect (P)-PMT family and the P-secrecy rate is denoted by $R_{\mathcal{F}:0}$.*

Designing P-PMT families is crucial for highly-sensitive data transmission. There are however scenarios which desire non-zero yet negligible δ and ϵ. We define asymptotically-perfect (AP)-PMT families with (δ, ϵ)-PMT protocols, such that the values δ and ϵ tend to zero for longer messages.

Definition 3 (AP-PMT Family). *An AP-PMT family $\mathcal{F}$ for a multipath setting $\mathscr{S}$ is a sequence $(\Pi_i)_{i \in \mathbb{N}}$ where for each i, Π_i is a $(k_i, c_i, \delta_i, \epsilon_i)$-PMT protocol over $\mathscr{S}$, and it holds $k_{i+1} > k_i$, $\delta_{i+1} \leq \delta_i$, $\epsilon_{i+1} \leq \epsilon_i$, and $\lim_{i \to \infty} \delta_i = \lim_{i \to \infty} \epsilon_i = 0$. The* AP-secrecy rate *of $\mathcal{F}$ is defined as $R_{\mathcal{F}:\sim 0} = \inf\{\frac{k_i}{c_i} : i \in \mathbb{N}\}$.*

We accordingly define the secrecy capacity of a multipath setting as the highest secrecy rate that can be guaranteed for all message lengths. We are particularly interested in two types of capacities.

Definition 4 (Secrecy Capacity). *The P- (resp. AP-) secrecy capacity C_0 (resp. $C_{\sim 0}$) of a setting $\mathscr{S}$ equals the largest P-secrecy (resp. AP-secrecy) rate achievable by all possible P- (resp. AP-) PMT families over $\mathscr{S}$.*

[2] The infimum exists as the sequence is bounded from below by zero.

3.3 Relation among P-secrecy and AP-secrecy Capacities

Definition 1 implies that any $(k, c, \delta_1, \epsilon_1)$-PMT protocol is also $(k, c, \delta_2, \epsilon_2)$-PMT for $\delta_2 \geq \delta_1$ and $\epsilon_2 \geq \epsilon_1$. Since families simply consist of protocols, any (δ_1, ϵ_1)-PMT family is also a (δ_2, ϵ_2)-PMT family. This shows $C_0 \leq C_{\sim 0}$. It is important to know whether the above can be replaced by a strict inequality: It is fairly reasonable to tolerate negligible deviation from perfect security to improve rate or to make PMT possible. Below, we study P-PMT and AP-PMT protocols starting from the full-access case (when $t_a = t_b = n$) and extend it to the general multipath setting. Our study leads us the following ultimate conclusion:

For a wide range of settings, it holds $C_{\sim 0} > C_0$.

4 PMT in the Full-access Scenario

In the (n, t_e, λ)-full-access setting (i.e., $t_a = t_b = n$) with infinite interval length $\lambda = \infty$, the PMT problem relates to the SMT work [5] (for passive adversary): The optimal solution, denoted by $\mathcal{F}_0^{pol}$, simply uses a polynomial-based (n, r, n)-ramp secret sharing scheme (SSS), $(\mathbf{Share}_{pol}, \mathbf{Rec}_{pol})$, where $r = n - t_e$. Let $S \in \mathbb{F}_{2^u}^r$ be the secret message, for some integer $u > \log(2n - t_e)$.

- Alice calculates shares $\underline{X} = (X_1, X_2, \ldots, X_n) = \mathbf{Share}_{pol}(S)$ and sends $X_i \in \mathbb{F}_{2^u}$ over path i.
- Having received X_i's, Bob obtains the message as $S = \mathbf{Rec}_{pol}(\underline{X})$.

The perfect reliability and secrecy follow trivially from the properties of (n, r, n)-ramp SSS: n shares are qualified and $n - r = t_e$ shares are unqualified.

Proposition 1. *The scheme $\mathcal{F}_0^{pol}$ gives a family of $(u.r, u.n, 0, 0)$-P-PMT protocols with rate $R_{\mathcal{F}_0^{pol}} = 1 - \frac{t_e}{n}$ over the (n, t_e, λ)-full-access setting with $\lambda = \infty$.*

4.1 P-PMT for Finite λ

When λ is finite, the scheme $\mathcal{F}_0^{pol}$ (without any modification) does not provide us with a P-PMT family since it cannot give P-PMT protocols for message lengths $u.r$ such that $u > \lambda$. There is of course an easy fix to this. One can stay with a constant field size 2^λ and instead repeat $\mathcal{F}_0^{pol}$ for sufficiently many times to send arbitrarily long messages; hence, a PMT family.

Proposition 2. *Repeating $\mathcal{F}_0^{pol}$ for arbitrary times results in a P-PMT family with rate $R_{\mathcal{F}_0^{pol}} = 1 - \frac{t_e}{n}$ in any (n, t_e, λ)-full-access setting with $2n - t_e \leq 2^\lambda$.*

The situation is unfortunate when $2n - t_e > 2^\lambda$: $\mathcal{F}_0^{pol}$ cannot provide any PMT protocol since the polynomial-based SSS cannot generate more points than the field size 2^λ. To resolve this, we propose a P-PMT scheme, $\mathcal{F}_0^{alg}$, that is similar to $\mathcal{F}_0^{Pol}$ but uses the algebraic-geometric SSS of Section 2 with arbitrarily many shares over $\mathbb{F}_{2^\lambda}$ and transmits message in q time-intervals. In precise, the scheme uses a $(qn-2g, r, g, qn)$-quasi-ramp SSS $(\mathbf{Share}_{alg}, \mathbf{Rec}_{alg})$ for the secret message $S = (S_1, \ldots, S_r) \in \mathbb{F}^r_{2^\lambda}$: To generate $qn + r \leq (\sqrt{2^\lambda} - 1)g$ points, we choose $g = \lceil \frac{q(2n-t_e)}{2^{\lambda/2}-1} \rceil$ and $r = q(n-t_e)-2g$. The reliability and secrecy properties of $\mathcal{F}_0^{alg}$ follow from the quasi-ramp SSS: $qn-2g+2g = qn$ shares are qualified and $qn - 2g - r = qt_e$ shares are unqualified. The rate equals $R_{\mathcal{F}_0^{alg}} = \frac{r\lambda}{qn\lambda} = 1 - \frac{t_e}{n}$, where (inequality (a) follows by choosing $q \geq \frac{2^{\lambda/2}-1}{t_e} - \Delta$)

$$\Delta = \frac{2\lceil \frac{2qn}{2^{\lambda/2}-1} - \frac{qt_e}{2^{\lambda/2}-1} \rceil}{qn} \overset{(a)}{\leq} \frac{4qn}{(2^{\lambda/2} - 1)qn} = (2^{\frac{\lambda}{2}-2} - 0.25)^{-1}. \qquad (3)$$

Proposition 3. *The scheme $\mathcal{F}_0^{alg}$ gives a P-PMT family over any (n, t_e, λ)-full-access setting. The P-secrecy rate of the family is $R_{\mathcal{F}_0^{alg}:0} = [1 - \frac{t_e}{n} - \Delta]_+$ where $\Delta \leq (2^{\frac{\lambda}{2}-2} - 0.25)^{-1}$.*

Implication to P-secrecy Capacity The existing work on SMT (cf. [11]) suggests the upper-bound $1 - \frac{t_e}{n}$ on achievable P-PMT secrecy rates. This combined with the above results leads us to the following approximation of the P-secrecy capacity for the full-access case:

$$[1 - \frac{t_e}{n} - \Delta]_+ \leq C_0^{\mathbf{FA}} \leq 1 - \frac{t_e}{n}. \qquad (4)$$

It remains an interesting theoretical question to close the gap between the two bounds. For practical scenarios ($\lambda > 100$), the gap Δ is reasonably small.

4.2 AP-PMT in the full-access Case

We are interested in finding whether PMT rates can be improved if reliability or secrecy requirements are relaxed to asymptotically perfect. We already have the trivial lower-bound $C_{\sim 0}^{\mathbf{FA}} \geq C_0^{\mathbf{FA}}$. To derive an upper-bound, we obtain a bound on (δ, ϵ)-secrecy rates and then study its behavior when δ and ϵ approach zero. The bound is obtained by relating to (δ, ϵ)*-secret-key rates for secret-key establishment protocols.* The proof is rather technical and is removed due to lack of space. We refer to the full version [2, Section 4.3] for the proof.

Theorem 1. *There is no (possibly multiple-round) (k, c, δ, ϵ)-PMT protocol in the (n, t_e, λ)-full-access setting with $\frac{k}{c} > \frac{1-t_e/n}{1-1.25\epsilon'-\epsilon' \log \epsilon'}$, where $\epsilon' = \epsilon + \delta$. This implies the AP-secrecy capacity of (using the lower-bound (4))*

$$[1 - \frac{t_e}{n} - \Delta]_+ \leq C_{\sim 0}^{\mathbf{FA}} \leq 1 - \frac{t_e}{n}. \qquad (5)$$

The bounds (4) and (5) show that P-secrecy and AP-secrecy capacities fall in the same range and will equal $1 - \frac{t_e}{t_{ab}}$ assuming $\Delta \to 0$: We can conclude *relaxing security requirements from perfect to asymptotically-perfect does NOT help improve the secrecy rate in the "full-access" case.*

5 PMT in the General Multipath Setting

Unlike full-access, relaxing security to asymptotically perfect benefits PMT in the general setting. We study P-PMT and AP-PMT rates separately.

5.1 P-PMT: Capacity and Construction

We derive lower and upper bounds on the P-secrecy capacity in the general (two-way) multipath communication setting that prove $C_0 \approx [1 - \frac{t_e}{t_{ab}}]_+$ and imply P-PMT impossibility when $t_e \geq t_{ab}$.

Lower-bound via one-round P-PMT. The lower-bound on C_0 is attained by using one-round PMT schemes, $\mathcal{F}_0^{pol}$ or $\mathcal{F}_0^{alg}$, over a fixed (hard-coded) set of t_{ab} paths. The constructions promise the rate $1 - \frac{t_e}{t_{ab}} - \Delta$ when $t_e \leq t_{ab}$ (see (4)).

Upper-bound on P-PMT achievable rates. Any (possibly multiple-round) P-PMT protocol in the multipath setting needs to provide "perfect" secrecy, even in the "worst" case when Eve always captures t_e of the $\leq t_{ab}$ communication paths between Alice and Bob. This suggests the maximum rate $1 - t_e/t_{ab}$ stated in the following Lemma. For the proof, we refer to the full version [2, Appendix D].

Lemma 1. *There is no (possibly multiple-round) $(k, c, 0, 0)$-PMT protocol over the $(n, t_a, t_b, t_e, \lambda)$-multipath setting with rate $R = \frac{k}{c} > [1 - \frac{t_e}{t_{ab}}]_+$.*

Theorem 2 concludes the results on P-secrecy capacity.

Theorem 2. *The P-secrecy capacity of any $(n, t_a, t_b, t_e, \lambda)$ multipath setting satisfies $[1 - \frac{t_e}{t_{ab}} - \Delta]_+ \leq C_0 \leq [1 - \frac{t_e}{t_{ab}}]_+$ and the lower-bound is achieved by an explicit one-round PMT protocol.*

5.2 AP-PMT: Capacity and Constructions

Achievable AP-secrecy rates in the general setting cannot be upper-bounded by some similar approach to the full-access case (as in Section 4.2). This leaves us with the trivial upper-bound

$$C_{\sim 0} \leq U_{\sim 0} \triangleq 1 - \frac{t_e}{n}. \tag{6}$$

At a first look, the upper-bound seems far from tight. It seems impossible to reach secrecy rates up to $1 - \frac{t_e}{n}$, regardless of connectivity parameters t_a and t_b. We prove however that for sufficiently large λ, there are AP-PMT families which can get close to this rate. For one-way multipath setting, the required connectivity condition is $t_b > t_e$; for two-way setting however, AP-PMT is always possible only if $t_e < n$ and $t_a, t_b > 0$.

AP-PMT Approach. We introduce three different AP-PMT schemes for different connectivity ranges. All schemes consist of two primitive blocks: (i) *low-rate key establishment block* and (ii) *high-rate coordinated PMT block*. The key-establishment block lets Alice and Bob share a long secret-key W in q_1 intervals. The coordinated PMT block allows Alice to send her message to Bob in q_2 intervals over the secret paths chosen based on W: Since Eve is unaware of W, the coordinated PMT rate equals (almost) $1 - \frac{t_e}{n}$. The overall rate however takes into account the overhead communication for block (i). Both blocks take use of the algebraic-geometric SSS of Section 2.

One-round AP-PMT for $t_e \leq t_{ab}$. We introduce a one-round AP-PMT scheme $\mathcal{F}_1$ with an AP-secrecy rate close to $1 - \frac{t_e}{n}$. The scheme has perfect reliability, but allows for negligible leakage. It composes a key-transport block and a coordinated PMT block as follows. Given the $(n, t_a, t_b, t_e, \lambda)$ multipath setting, define $w = \lceil \log \binom{n}{t_{ab}} \rceil$. For arbitrarily small $\psi > 0$, and sufficiently large $q_1 \in \mathbb{N}$ (to be determined), define [3]

$$g_1 = \lceil \frac{q_1(2t_{ab} - t_e)}{2^{\lambda/2} - 1} \rceil, \quad r_1 = q_1(t_{ab} - t_e) - 2g_1 \tag{7}$$

$$q_2 = \frac{r_1 \lambda}{w}, \; t'_{e,2} = (1+\psi)\frac{t_{ab} t_e}{n}, \; g_2 = \lceil \frac{q_2(2t_{ab} - t'_{e,2})}{2^{\lambda/2} - 1} \rceil, \; r_2 = q_2(t_{ab} - t'_{e,2}) - 2g_2. \tag{8}$$

Let $(\mathbf{Share}_{alg,1}, \mathbf{Rec}_{alg,1})$ be a $(q_1 t_{ab} - 2g_1, r_1, g_1, q_1 t_{ab})$-quasi-ramp SSS over $\mathbb{F}_{2^\lambda}$ used for key transport, and $(\mathbf{Share}_{alg,2}, \mathbf{Rec}_{alg,2})$ be a $(q_2 t_{ab} - 2g_2, r_2, g_2, q_2 t_{ab})$-quasi-ramp SSS over $\mathbb{F}_{2^\lambda}$ used for coordinated PMT. Let $\mathcal{T}_0$ be a set of fixed (public) t_{ab} paths and $S \in \mathbb{F}_{2^\lambda}^{r_2}$ be the message to be transmitted.

One-round $(0, \epsilon)$*-PMT scheme* $\mathcal{F}_1$*.*

(i) *Key transport (q_1 intervals).* Alice generates randomly $W = (W_1, \dots, W_{q_2}) \in \{0,1\}^{q_2 w}$. She obtains shares $\underline{X} = (X_{i,j})_{1 \leq i \leq q_1, 1 \leq j \leq t_{ab}} = \mathbf{Share}_{alg,1}(W)$ and sends $(X_{i,j})_{1 \leq j \leq t_{ab}}$ over the t_{ab} paths of $\mathcal{T}_0$ in interval $1 \leq i \leq q_1$. Having received shares, Bob reconstructs $W = \mathbf{Rec}_{alg,1}(\underline{X})$.

(ii) *Coordinated PMT (q_2 intervals).* Alice and Bob calculate path sets $\mathcal{T}_i$ of size t_{ab}, for $1 \leq i \leq q_2$, using key $W_i \in \{0,1\}^w$. Alice calculates message shares $\underline{Y} = (Y_{i,j})_{1 \leq i \leq q_2, 1 \leq j \leq t_{ab}} = \mathbf{Share}_{alg,2}(S)$ and sends the part $(Y_{i,j})_{1 \leq j \leq t_{ab}}$ over $\mathcal{T}_i$ in interval $q_1 + i$. Having received all shares, Bob reconstructs $S = \mathbf{Rec}_{alg,2}(\underline{Y})$.

Theorem 3. *For any small $\psi, \epsilon > 0$, the scheme $\mathcal{F}_1$ gives $(0,\epsilon)$-PMT and AP-PMT families over an $(n, t_a, t_b, t_e, \lambda)$ multipath setting with $t_e < t_{ab} \leq n$. The AP-secrecy rate of the scheme equals*

$$R_{\mathcal{F}_1:\sim 0} = \frac{1 - \frac{t_e}{n} - \Delta}{1 + \xi_1}, \quad \textit{where} \;\; \xi_1 = \frac{\log(\frac{en}{t_{ab}})}{\lambda(1 - \frac{t_e}{t_{ab}} - \Delta)} \quad \textit{and} \;\; \Delta = (2^{\frac{\lambda}{2}-2} - 0.25)^{-1}.$$

[3] Here, we assume that q_1 is chosen such that w divides $r_1 \lambda$.

Proof. See Appendix A.

Remark 1. It is crucial to use the algebraic-geometric (rather than polynomial) SSS. Expecting arbitrarily small $\epsilon > 0$ requires sufficiently many $(q_2 t_{ab})$ shares over field of constant size 2^λ.

The rate $R_{\mathcal{F}_1:\sim 0}$ shows rate improvement of AP-PMT compared to P-PMT. The rate is however lower than upper-bound (6) mainly due to the key-transport block communication overhead ξ_1.

One-round AP-PMT for $\boldsymbol{t_e \geq t_{ab}}$. The scheme $\mathcal{F}_1$ cannot achieve any positive secrecy rate when $t_e \geq t_{ab}$. We observe the following two restricting properties of $\mathcal{F}_1$: (i) it provides perfect reliability, and (ii) it is non-interactive. In this section, we focus on relaxing perfect reliability and introduce a PMT scheme $\mathcal{F}_2$ that only modifies the key-transport block in $\mathcal{F}_1$: It fixes a larger set $\mathcal{T}_0$ of $\max(t_a, t_b) \leq n' \leq n$ (instead of t_{ab}) paths and requires Alice and Bob to communicate over random subsets of $\mathcal{T}_0$. This sacrifices the reliability, but allows for pushing the multipath connectivity condition to $t_e < t_b$ instead of $t_e < t_{ab}$ (for scheme $\mathcal{F}_1$).

$\mathcal{F}_2$ uses same parameters (8) for coordinated PMT, but updates parameters for key transport: It uses the algebraic-geometric $(q_1 t'_{b,1} - 2g_1, r_1, g_1, q_1 t_a)$-quasi-ramp SSS $(\mathbf{Share}_{alg,1}, \mathbf{Rec}_{alg,1})$, where

$$\begin{aligned} t'_{b,1} &= (1-\psi)\tfrac{t_a t_b}{n'}, \quad t'_{e,1} = (1+\psi)\tfrac{t_a t_e}{n'}, \\ g_1 &= \lceil \tfrac{q_1(t_a + t'_b - t'_{e,2})}{2^{\lambda/2}-1} \rceil, \quad r_1 = q_1(t'_{b,1} - t'_{e,1}) - 2g_1. \end{aligned} \tag{9}$$

One-round (δ, ϵ)-PMT scheme $\mathcal{F}_2$.

(i) *Key transport (q_1 intervals).* Alice generates random $W = (W_1, \ldots, W_{q_2}) \in \{0,1\}^w$ and shares $\underline{X} = (X_{i,j})_{1 \leq i \leq q_1, 1 \leq j \leq t_a} = \mathbf{Share}_{alg,1}(W)$. In each round $1 \leq i \leq q_1$, she sends the part $(X_{i,j})_{1 \leq j \leq t_a}$ over t_a (random) paths from $\mathcal{T}_0$, and Bob listens over t_b (random) paths from $\mathcal{T}_0$. If Bob's observation $\underline{X}'$ includes less than $q_1 t'_{b,1}$ shares, he aborts and chooses $\hat{S} \in_R \mathbb{F}_{2^\lambda}^{r_2}$; otherwise, he reconstructs $W = \mathbf{Rec}_{alg,1}(\underline{X}')$.

(ii) *Coordinated PMT (q_2 intervals).* This is the same as $\mathcal{F}_1$.

Theorem 4. *For any small $\psi, \delta, \epsilon > 0$, the scheme $\mathcal{F}_2$ gives (δ, ϵ)-PMT and AP-PMT families over any $(n, t_a, t_b, t_e, \lambda)$ multipath setting with $t_e < t_b$. The AP-secrecy rate of this scheme reaches*

$$R_{\mathcal{F}_2:\sim 0} = \frac{1 - \frac{t_e}{n} - \varDelta}{1 + \xi_2}, \quad \textit{where}$$

$$\xi_2 = \frac{\log(\frac{en}{t_{ab}})}{\lambda\left(\frac{t_b - t_e}{n'} - \varDelta\right)}, \quad n' = \max(t_a, t_b), \quad \textit{and} \quad \varDelta = (2^{\frac{\lambda}{2}-2} - 0.25)^{-1}.$$

Proving Theorem 4 is similar to Theorems 3. We refer the reader to the full version [2, Appendix F] for the proof.

Remark 2. When $t_b = n$ Scheme $\mathcal{F}_2$ can be simplified to achieve a higher rate: Only Stage (i), key-transport, suffices to serve message transmission at rate $\frac{t_b - t_e}{t_b} - \Delta = 1 - \frac{t_e}{n} - \Delta$, for $n' = n$.

Impossibility of One-way PMT for $t_e \geq t_b$. It is impossible to obtain AP-PMT in one-round when $t_e \geq t_b$. The reason any protocol that lets Bob recover the message will let Eve too. For the proof, refer to [2, Appendix G]

Proposition 4. *When $t_e \geq t_b$, there is no one-round (k, c, δ, ϵ)-PMT protocol of rate $R = \frac{k}{c} > \frac{2\epsilon}{1-\delta-\alpha}$ to transmit $k \geq 3/\alpha$ bits of messages, implying the AP-secrecy capacity of $C_{\sim 0} = 0$.*

Implication to one-way AP-secrecy capacity. Putting things together, we reach the following on AP-secrecy capacity of one-way communication.

Corollary 1. *For any one-way $(n, t_a, t_b, t_e, \lambda)$-multipath setting, it holds that $\overrightarrow{L}_{\sim 0} \leq \overrightarrow{C}_{\sim 0} \leq \overrightarrow{U}_{\sim 0}$, where*

$$\overrightarrow{L}_{\sim 0} = \begin{cases} [\frac{1 - \frac{t_e}{n} - \Delta}{1 + \min(\xi_1, \xi_2)}]_+, & \mathit{if} \;\; t_e < t_{ab} \\ [\frac{1 - \frac{t_e}{n} - \Delta}{1 + \xi_2}]_+, & \mathit{if} \;\; t_{ab} \leq t_e < t_b \\ 0, & \mathit{if} \;\; t_e \geq t_b \end{cases}, \quad \overrightarrow{U}_{\sim 0} = \begin{cases} 1 - \frac{t_e}{n}, & \mathit{if} \;\; t_e < t_b \\ 0, & \mathit{if} \;\; t_e \geq t_b \end{cases} \tag{10}$$

AP-PMT: Always Positive Rates via Two-way Communication. We introduce a two-round AP-PMT scheme $\mathcal{F}_3$ that achieves positive rates even when $t_e \geq t_b$. The idea is using an *interactive key-agreement* block, instead of key transport. Bob sends random elements over random paths and Alice publicly responds (over a fixed path) which elements she has received. Having shared common elements, Alice and Bob apply privacy amplification to convert them into a secret-key. We use the algebraic-geometric SSS for privacy amplification.

Scheme $\mathcal{F}_3$ uses same parameters as $\mathcal{F}_1$ for coordinated PMT (8), but updates paraments for key agreement: It uses the $(q_1 t'_{a,1} - 2g_1, r_1, g_1, q_1 t'_{a,1})$-quasi-ramp SSS $(\mathbf{Share}_{alg,1}, \mathbf{Rec}_{alg,1})$, where

$$t'_{a,1} = (1 - \psi)\frac{t_a t_b}{n}, \quad t'_{e,1} = (1 + \psi)\frac{t'_{a,1} t_e}{n}, \tag{11}$$

$$g_1 = \lceil \frac{q_1(2t'_{a,1} - t'_{e,1})}{2^{\lambda/2} - 1} \rceil, \quad r_1 = q_1(t'_{a,1} - t'_{e,1}) - 2g_1. \tag{12}$$

Two-round (δ, ϵ)-PMT scheme $\mathcal{F}_3$.

(i) *Interactive key agreement (q_1 intervals).* Bob generates $\underline{X} = (X_{i,j})_{1 \leq i \leq q_1, 1 \leq j \leq t_b}$ randomly from $(\mathbb{F}_2^\lambda)^{q_1 t_b}$. In each interval $1 \leq i \leq q_1$, he sends $(X_{i,j})_{1 \leq j \leq t_b}$ over t_b random paths and Alice listens over t_a random paths. If Alice's observation includes $< q_1 t'_{a,1}$ elements from $\underline{X}$, she aborts and Bob outputs $\hat{S} \in_R \mathbb{F}_{2^\lambda}^{r_2}$; otherwise, let $X_A \subseteq \underline{X}$ be the first $q_1 t'_{a,1}$ elements observed by Alice over path sets $(\mathcal{P}_i)_{1 \leq i \leq q_1}$. Alice sends $(\mathcal{P}_i)_{1 \leq i \leq q_1}$ information over a fixed (public) path to Bob. Alice and Bob use X_A as shares to calculate $W = (W_1, \ldots, W_{q_2}) = \mathbf{Rec}_{alg,1}(X_A)$.

(ii) *Coordinated PMT (q_2 intervals).* This is the same as $\mathcal{F}_1$.

Theorem 5. *For any $\psi, \delta, \epsilon > 0$, the scheme $\mathcal{F}_3$ gives (δ, ϵ)-PMT and AP-PMT families over any $(n, t_a, t_b, t_e, \lambda)$ multipath setting with $t_a, t_b > 0$ and $t_e < n$. The AP-secrecy rate of $\mathcal{F}_3$ equals:*

$$R_{\mathcal{F}_3:\sim 0} = \frac{1 - \frac{t_e}{n} - \varDelta}{1 + \xi_3},$$

$$\textit{where} \quad \xi_3 = \frac{\left(\frac{n}{t_a} + \frac{\log(en^2/(t_a t_b))}{\lambda}\right) \log \frac{en}{t_{ab}}}{\lambda\left(1 - \frac{t_e}{n} - \varDelta\right)} \quad \textit{and} \quad \varDelta = (2^{\frac{\lambda}{2}-2} - 0.25)^{-1}.$$

The proof is similar to those for Theorems 3 and 4. We refer the reader to the full version [2, Appendix H].

Implication to two-way AP-secrecy capacity. The capacity is trivially upper-bounded by $1 - \frac{t_e}{n}$, unless when $t_a = 0$ or $t_b = 0$. Combining the lower bounds from $\mathcal{F}_1$, $\mathcal{F}_2$, and $\mathcal{F}_3$, we have:

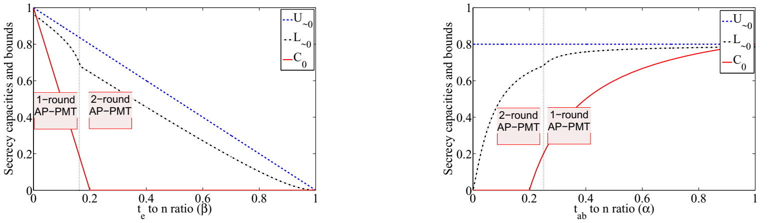
Corollary 2. *For any $(n, t_a, t_b, t_e, \lambda)$-multipath setting, it holds $L_{\sim 0} \leq C_{\sim 0} \leq U_{\sim 0}$, where*

$$L_{\sim 0} = \begin{cases} [\frac{1 - \frac{t_e}{n} - \varDelta}{1 + \min(\xi_1, \xi_2, \xi_3)}]_+, & \textit{if } t_e < t_{ab} \\ [\frac{1 - \frac{t_e}{n} - \varDelta}{1 + \min(\xi_2, \xi_3)}]_+, & \textit{if } 0 < t_{ab} \leq t_e < t_b \\ [\frac{1 - \frac{t_e}{n} - \varDelta}{1 + \xi_3}]_+, & \textit{if } 0 < t_b < t_e \ \wedge \ t_a > 0 \\ 0, & \textit{else} \end{cases}, U_{\sim 0} = \begin{cases} 1 - \frac{t_e}{n}, & \textit{if } t_a, t_b > 0 \\ 0, & \textit{else} \end{cases} \quad (13)$$

5.3 Comparison of P-secrecy and AP-secrecy Rates

We have proved that in partial-access multipath communication, Alice and Bob can achieve higher secrecy rates if they choose AP-PMT protocols over P-PMT ones. To give more sense about how much rate improvement is attained by AP-PMT protocols, we compare the P-secrecy and AP-secrecy capacities for typical multipath parameters that match practical scenarios. Figure 2(a) graphs the lower and upper bounds on $C_{\sim 0}$ as well as C_0 for different values of $\beta = \frac{t_e}{n}$, assuming $\lambda = 100$ and $t_a = t_b = 0.2n$. For this value of λ, we approximate $\varDelta \approx 0$ and thus $C_0 \approx 1 - \frac{t_e}{t_{ab}} = 1 - 5\beta$ (see Theorem 2). The capacity C_0 and the bounds $L_{\sim 0}$ and $U_{\sim 0}$ are shown by solid, dotted, and dashed lines, respectively. The graph clearly illustrates the benefit of using AP-PMT: While the lower-bound $L_{\sim 0}$ remains positive throughout, C_0 drops fast and equals 0 for $\beta \geq 0.2$. For $\beta \leq 0.15$, the lower bound $L_{\sim 0}$ is achieved by one-round AP-PMT and is quite close to the upper bound. Outside of this range, the lower-bound corresponds to our two-round scheme $\mathcal{F}_3$. This is not surprising since one-way AP-PMT is impossible when $\beta \geq 0.2$ (implying $t_e \geq t_b$).

Figure 2(b) graphs the same three quantities (C_0, $L_{\sim 0}$, and $U_{\sim 0}$) with respect to $\alpha = \frac{t_{ab}}{n}$, assuming $\lambda = 100$, $t_a = t_b$, and $t_e = 0.2n$. The gap between



(a) w.r.t. $\beta=\frac{t_e}{n}$ for $t_a=t_b=0.2n$ (b) w.r.t. $\alpha=\frac{t_{ab}}{n}$ for $t_a=t_b$ and $t_e=0.2n$

Fig. 2. Comparing the secrecy capacities and bounds

the bounds on $C_{\sim 0}$ bridges as we increase α. What causes more gap for small $\alpha < 0.25$ is small is the two-round AP-PMT communication overhead ξ_3. Finding a better approximation of the AP-secrecy capacity, especially in the low connectivity regime where $t_a, t_b < t_e$ is recommended as future work.

6 Practical Consideration

We discuss two practical applications of our PMT results in the multipath setting model, i.e., sending secret data over (i) multiple-frequency links and (ii) multiple-route networks. Both scenarios include a set of paths that connect communicants and can be tapped into by present eavesdroppers.

6.1 PMT Using Multiple-frequency Links

Multiple-frequency communication environments, such as wireless and fiber-optics, realize our multipath setting. Our PMT results show the possibility of secure communication, provided that the wiretapper does not have simultaneous access to all frequencies (i.e., $t_e < n$ in our setting). The challenge is to design a multiple-frequency system that enforces this property. Existing frequency-hopping solutions do not satisfy this requirement. Bluetooth for example transmits data at speed of 1Mbps over 79 adjacent 1-MHz frequency channels and by the current technology, one can easily capture all the 80-MHz frequency range and store hours of communication in a 1 Terabyte disk.

It is yet possible to design systems that serve our purpose as it is practically infeasible for a single transceiver (and ADC) to deal with wider than 100 MHz ranges [10]. All we need is to use a system whose frequency channels are far apart. Consider for instance a system design that uses $n = 70$ 20-MHz frequency-channels distributed evenly (with 80-MHz distances) over the 57–64 GHz (unlicensed Gigabit WiFi) frequency range. Data transmitted at 100 Mbps speed. Since there is only one frequency channel in each 100-MHz slot, the eavesdropper would require 70 transceiver blocks to access all 70 channels simultaneously. This is not practical in certain scenarios due to expense concern or space restriction (e.g., stealth attack on indoor communication).

Let us assume legitimate devices use only $t_a = t_b = 4$ transceivers, while the wiretapper's device can embed $t_e = 35$ such blocks. The wiretapper may switch between frequencies to learn more information. Fastest frequency synthesizers have switching time around 1μs [1]. Although one may allow longer switching time for legitimate parties, the 1μs time determines λ in our design. At the speed of 100 Mpbs, this gives $\lambda = \lfloor 10^{-6} \times 100 \times 2^{20} \rfloor = 104$ bits, implying a $(70, 4, 4, 35, 104)$-multipath setting for which the two-round AP-PMT scheme $\mathcal{F}_3$ sends private data at rate 17%. *This solution does not require pre-shared keys and provides information-theoretic security.*

6.2 PMT Using Multiple-route Networks

Multipath routing has been shown [16] to benefit reliable transmission over large networks such as mobile ad hoc networks (MANETs) and the Internet. We study whether the resource can be used to enhance privacy of communication when middle routers can be tapped into. We focus on MANETs. Studies have shown the average number of node-disjoint paths in a moderately-dense (around 500-node) MANET is over 10. Consider the following scenario: There are $n = 10$ paths between the source and destination nodes. The source can send over only $t_a = 2$ paths while the destination receives data through all $t_b = 10$ paths. The adversary's resources allow for compromising at most $t_e = 8$ paths at a time, and at least 1 millisecond is needed to redirect resources to tap into new nodes (and paths); this is quite plausible, noting the technical challenges of tapping into communicating devices. The source transmits data at the speed of 512 Kbps, implying $\lambda = \lfloor 10^{-3} \times 512 \times 2^{10} \rfloor = 524$. This leads to the $(10, 2, 8, 10, 524)$-multipath setting for which the simplified version of scheme $\mathcal{F}_2$ (Block (i) only – see Remark 2) guarantees private transmission at rate 20%.

7 Conclusion and Future Work

We have derived connectivity conditions for the possibility of P-PMT and AP-PMT in the multipath setting. We also derived lower and upper bounds on the secrecy capacities. Although in the full-access case, P-PMT and AP-PMT behave the same, in general, AP-PMT protocols attain strictly higher rates. The maximum rate for P-PMT is $[1 - \frac{t_e}{t_{ab}}]_+$, whereas AP-PMT protocols can achieves rates close to the upper-bound $1 - \frac{t_e}{n}$. The is yet a gap between the proved achievable rates and this upper-bound. *Bridging the gap is an interesting question which we leave for future work.*

Any practical communication system with path diversity can be a case to test the feasibility our PMT results. We considered the real-life scenarios of communication over multiple-frequency links and multiple-route networks. In both cases, we elaborated on how to derive multipath setting parameters and used our results to provide private communication at rates 17% and 20%, respectively. Showing the possibility of keyless communication with information-theoretic privacy is interesting. *A followup work can be the design of concrete protocols considering all practical and technical concerns that may have been missing in this work.*

References

1. Winradio ms-8323 multichannel telemetry receiver, `http://www.winradio.com/home/ms8323.htm`
2. Ahmadi, H., Safavi-Naini, R.: Multipath private communication: An information theoretic approach. CoRR, abs/1401.3659 (2014)
3. Chen, H., Cramer, R.: Algebraic geometric secret sharing schemes and secure multiparty computations over small fields. In: Dwork, C. (ed.) CRYPTO 2006. LNCS, vol. 4117, pp. 521–536. Springer, Heidelberg (2006)
4. Chernoff, H.: A measure of asymptotic efficiency for tests of a hypothesis based on the sum of observations. Annals of Mathematical Statistics 23(4), 493–507 (1952)
5. Dolev, D., Dwork, C., Waarts, O., Yung, M.: Perfectly secure message transmission. Journal of the ACM (JACM) 40(1), 17–47 (1993)
6. Garcia, A., Stichtenoth, H.: On the asymptotic behaviour of some towers of function fields over finite fields. Journal of Number Theory 61(2), 248–273 (1996)
7. Leyden, J.: Worried openssl uses nsa-tainted crypto? this bug has got your back (2013), `http://www.theregister.co.uk/2013/12/20/openssl_crypto_bug_beneficial_sorta/`
8. Lichtblau, E., Risen, J.: Spy agency mined vast data trove, officials report. New York Times (2005)
9. Linder, F.: Cisco ios attack and defense the state of the art. Presented at the 25th Chaos Communication Congress (2008)
10. Löhning, M., Fettweis, G.: The effects of aperture jitter and clock jitter in wideband adcs. Computer Standards & Interfaces 29(1), 11–18 (2007)
11. Patra, A., Choudhury, A., Pandu Rangan, C., Srinathan, K.: Unconditionally reliable and secure message transmission in undirected synchronous networks: Possibility, feasibility and optimality. International Journal of Applied Cryptography 2(2), 159–197 (2010)
12. Shamir, A.: How to share a secret. Communications of the ACM 22(11), 612–613 (1979)
13. Shor, P.W.: Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM Journal on Computing 26(5), 1484–1509 (1997)
14. Strasser, M., Capkun, S., Popper, C., Cagalj, M.: Jamming-resistant key establishment using uncoordinated frequency hopping. In: IEEE Symposium on Security and Privacy (SP), pp. 64–78 (2008)
15. Wood, A.D., Stankovic, J.A.: Denial of service in sensor networks. Computer 35(10), 54–62 (2002)
16. Ye, Z., Krishnamurthy, S.V., Tripathi, S.K.: A framework for reliable routing in mobile ad hoc networks. In: INFOCOM 2003. Twenty-Second Annual Joint Conference of the IEEE Computer and Communications. IEEE Societies, vol. 1, pp. 270–280. IEEE (2003)

A Proof of Theorem 3

Given $\psi, \epsilon > 0$, the PMT family from choices of q_1 such that

$$q_1 \geq \frac{2^{\lambda/2}-1}{t_e} \quad \text{and} \quad q_2 \geq \max\left(\frac{(2+\psi)n}{\psi^2 t_e} \ln\frac{1}{\epsilon}\ ,\ \frac{2^{\lambda/2}-1}{t'_{e,2}}\right).$$

Secrecy Rate. The two blocks communicate $c_1 = q_1 t_{ab}\lambda$ and $c_1 = q_1 t_{ab}\lambda$ bits, respectively. Recalling (7), $t_{ab} = \min(t_a, t_b)$, and $\varDelta = (2^{\frac{\lambda}{2}-2} - 0.25)^{-1}$, we calculate

$$R_{\mathcal{F}_1} = \frac{r_2\lambda}{(q_1+q_2)t_{ab}\lambda} = \frac{q_2\left(1 - \frac{t'_{e,2}}{t_{ab}} - \frac{2g_2}{q_2 t_{ab}}\right)}{q_2+q_1} = \frac{q_2\left(1 - \frac{t'_{e,2}}{t_{ab}} - \frac{2g_2}{q_2 t_{ab}}\right)}{q_2 + \frac{r_1}{t_{ab}-t_e-\frac{2g_1}{q_1}}}$$

$$= \frac{q_2\left(1 - \frac{t'_{e,2}}{t_{ab}} - \frac{2g_2}{q_2 t_{ab}}\right)}{q_2 + \frac{q_2 w}{\lambda t_{ab}\left(1-\frac{t_e}{t_{ab}}-\frac{2g_1}{q_1 t_{ab}}\right)}} \overset{(a)}{\geq} \frac{1 - \frac{t'_{e,2}}{t_{ab}} - \varDelta}{1 + \frac{\log\binom{n}{t_{ab}}}{\lambda t_{ab}\left(1-\frac{t_e}{t_{ab}}-\varDelta\right)}} \overset{(b)}{\geq} \frac{1 - \frac{t'_{e,2}}{t_{ab}} - \varDelta}{1 + \frac{\log(en/t_{ab})}{\lambda\left(1-\frac{t_e}{t_{ab}}-\varDelta\right)}}.$$

Inequality (a) follows by using a similar argument as in (3), noting the choices of g_1 and g_2 (7) as well as $q_1 \geq \frac{2^{\lambda/2}-1}{t_e}$ and $q_2 \geq \frac{2^{\lambda/2}-1}{t'_{e,2}}$. Inequality (b) holds due to Stirling's inequality $\binom{n}{t_{ab}} < (ne/t_{ab})^{t_{ab}}$. The fact that $\psi > 0$ can be arbitrarily small implies that $\lim_{\psi\to 0} \frac{t'_{e,2}}{t_{ab}} = \frac{t_e}{n}$; hence, the rate.

0**-reliability.** This is trivial: Both key-transport and coordinated-PMT use common paths.

ϵ**-secrecy.** Leakage occurs only if Eve observes more than $q_2 t'_{e,2}$ of the $q_2 t_{ab}$ secret paths during coordinated PMT (otherwise SSS guarantees no information leakage to Eve). Let $T'_i \leq \min(t_{ab}, t_e) = t_e$ be the number paths that Eve observes in interval $q_1 + i$. For every $s_1, s_2 \in \{0,1\}^k$, we have

$$SD(View_E(s_1), View_E(s_2)) \leq \Pr(\sum_{i=1}^{q_2} T'_i > q_2 t'_{e,2}) \times 1 = \Pr(\sum_{i=1}^{q_2} T'_i > q_2 t'_{e,2}).$$

We upper-bound the right hand side. T'_i's are independent with hyper-geometric distribution

$$\forall 0 \leq j \leq t_e: \quad \Pr(T'_i = j) = \frac{\binom{t_{ab}}{j}\binom{n-t_{ab}}{t_e-j}}{\binom{n}{t_e}},$$

with an expected value of $\frac{t_{ab}t_e}{n}$. We apply the Chernoff bound [4] to the sum of normalized variables $\frac{T'_i}{t_{ab}}$, with mean $\mu = t_e/n$, to obtain (the last inequality is due to the choice of q_2):

$$\Pr\left(\sum_{i=1}^{q_2} T'_i > q_2 t'_{e,2}\right) = \Pr\left(\sum_{i=1}^{q_2} \frac{T'_i}{t_{ab}} > (1+\psi)q_2\mu\right) < e^{-\frac{\psi^2}{2+\psi}q_2\mu} \leq e^{-\ln(1/\epsilon)} = \epsilon.$$