A General Construction for 1-Round δ -RMT and $(0, \delta)$ -SMT

Reihaneh Safavi-Naini, Mohammed Ashraful Alam Tuhin, and Pengwei Wang

Department of Computer Science, University of Calgary
{rei,maatuhin,pengwwan}@ucalgary.ca

Abstract. In Secure Message Transmission (SMT) problem, a sender $\mathcal{S}$ is connected to a receiver $\mathcal{R}$ through N node disjoint bidirectional paths in the network, t of which are controlled by an adversary with *unlimited computational power*. $\mathcal{S}$ wants to send a message m to $\mathcal{R}$ in a *reliable* and *private* way. It is proved that SMT is possible if and only if $N \geq 2t + 1$. In Reliable Message Transmission (RMT) problem, the network setting is the same and the goal is to provide reliability for communication, only. In this paper we focus on 1-round δ -RMT and $(0, \delta)$ -SMT where the chance of protocol failure (receiver cannot decode the sent message) is at most δ , and in the case of SMT, privacy is perfect.

We propose a new approach to the construction of 1-round δ -RMT and $(0, \delta)$ -SMT for all connectivities $N \geq 2t + 1$, using list decodable codes and message authentication codes. Our concrete constructions use folded Reed-Solomon codes and multireceiver message authentication codes. The protocols have optimal transmission rates and provide the highest reliability among all known comparable protocols. Important advantages of these constructions are, (i) they can be adapted to all connectivities, and (ii) have simple and direct security (privacy and reliability) proofs using properties of the underlying codes, and δ can be calculated from parameters of the underlying codes.

We discuss our results in relation to previous work in this area and propose directions for future research.

1 Introduction

In a Secure Message Transmission (SMT) system a sender is connected to a receiver through N wires, t of which are controlled by the adversary. Wires are abstractions of bidirectional node disjoint paths in a network. The adversary's control of a wire is by taking complete control of a node or a link on the path, allowing them to stop, inject or change arbitrarily, the messages that are sent on the path. The goal of the system is to provide *reliability* and *privacy* for the transmitted messages against an adversary with *unlimited computational power* without assuming any prior shared key between the sender and the receiver. In *Perfectly Secure Message Transmission* (PSMT) systems, the adversary will not learn anything about the message, and the receiver always correctly receives the sent message. SMT protocols can have one or more *rounds* and their communication efficiency for a given number of rounds is measured by the *transmission*

rate which is the total number of communicated bits per one message bit. Protocols with the lowest rate for a given number of rounds, are called *optimal*. The initial motivation for this model was to simulate secure links between nodes in a distributed setting (e.g., multi-party computation [1,2]), where there are no direct secure links between nodes but there are multiple paths that connects the two nodes. In recent years, however, the protocols, and in particular 1-round SMT protocols, have found other applications including key agreement and key strengthening in wireless sensor networks (e.g., [22]).

It has been shown [3] that 1-round PSMT is possible if and only if $N = 3t + 1$. To increase the number of corrupted wires that can be tolerated by the protocol without increasing the number of rounds, one may sacrifice some reliability. A 1-round $(0, \delta)$ -SMT protocol provides perfect privacy and bounds probability of error in receiving the message by δ . These protocols can be constructed for $N \geq 2t + 1$.

A related scenario, known as *Reliable Message Transmission (RMT)*, is when the only requirement is the reliability of communication assuming the same network and adversary model (N wires, t of which are controlled by the adversary) as the SMT problem. A trivial protocol for reliable transmission when $N \geq 2t + 1$ is by sending the message on all the wires and using majority voting at the receiver to recover the correct message. This will correctly recover the message as only $t \leq \frac{N-1}{2}$ wires are corrupted. However the transmission rate of this protocol is N , which grows linearly with N (similar to repetition codes) and so the goal of δ -RMT protocols is to achieve optimal transmission rate (which is *constant* for 1-round when $N = 2t + K$, where $K \geq 1$ is a constant).

In this paper we consider 1-round δ -RMT and 1-round $(0, \delta)$ -SMT protocols. **Towards a systematic construction of 1-round δ -RMT and $(0, \delta)$ -SMT.** All existing optimal 1-round $(0, \delta)$ -SMT protocols use complex combinations of secret sharing and authentication systems for message encoding, together with elaborate secret reconstruction and verification algorithms to construct a decoding algorithm for the SMT. A disadvantage of these complex and clever constructions is the difficulty of verifying their properties. It was shown [12] that the proofs of security of the 1-round $(0, \delta)$ -SMT protocol in [18] were not correct.

A limitation of these constructions in practice is that a protocol is designed for a specific type of connectivity (for example, $N = 2t + 1$, or $N = 2t + K$, $K > 1$, or $N = (2 + c)t$, $c > \frac{1}{t}$), and when used in a setting with different types of connectivity, the optimality of the protocol cannot be guaranteed. This means that for optimality guarantee, one may need to implement multiple protocols in cases that the connectivity is not known beforehand. Similar observations can be made for optimal 1-round δ -RMT with $N \geq 2t + 1$. The only construction with optimal rate is given in [16]. The construction uses a complex combination of secret sharing for encoding and an elaborate verification for the decoding.

In contrast to the above constructions, there is a simple and elegant construction of an optimal 1-round PSMT [7] for $N = 3t + 1$, that uses Reed-Solomon (RS) code. The encoding and decoding in this construction are encoding and decoding of RS-codes. The construction also works for higher connectivity of

the form, $N = 3t + K$, $K > 1$, and sends K messages instead of one. For this construction the receiver only has to implement the decoder of an RS-code which has many well-known implementations. For less connectivity, $2t + 1 \leq N \leq 3t$, 1-round PSMT is not possible. However, it is an open question if it is possible to have simple and modular constructions for δ -RMT and $(0, \delta)$ -SMT using known primitives such as RS-codes.

Our Contributions

A general construction of a 1-round δ -RMT. We give a general construction of a 1-round δ -RMT for $N \geq 2t + 1$ from two components: a list decodable code and a Message Authentication Code (MAC). In a (ρ, L) -list decodable code (LD code) of length n , the number of codewords within distance ρn of any received word is at most L .

The basic idea of the construction is as follows. An information block I_S is first appended with a tag generated by a symmetric key authentication mechanism, to form a message m_S , which is then encoded using the LD code, and each component is sent over a wire. LD code allows correction of up to t adversarial errors and so the decoder will obtain a list of L closest codewords to the received word. The key for the authentication mechanism will be generated by the sender and sent along the wires to the receiver and so parts that are sent over the corrupted wires, will be corrupted. The authentication information together with the key information will allow the receiver to use the corresponding verification mechanism to recognize the correct codeword in the decoded list. The authentication mechanism must ensure that despite partly corrupted keys, the receiver will output the correct codeword. We describe our approach and prove a general theorem that proves reliability of the construction, with a value of δ that can be calculated from the parameters of the underlying components.

We then give a concrete construction when $N = 2t + 1$ using a Folded RS-code and a new multireceiver MAC that we propose. The result is an optimal δ -RMT with the *smallest* δ (highest reliability) among all known optimal δ -RMT protocols.

The drawback of this construction is that the receiver algorithm in RMT is exponential. For higher connectivities of the form $N = (2+c)t$, $c > \frac{1}{t}$ however, we will have an optimal δ -RMT with efficient (polynomial) receiver algorithm. The main challenge in this construction is choosing the authentication mechanism and its parameters, as well as parameters of FRS-code to achieve the required performance. We give details of these selections for $N = 2t + 1$, and for higher connectivities we omit the details because of space. (We will provide details for SMT when $N = (2+c)t$, $c > \frac{1}{t}$, which gives a good idea of challenges of designing δ -RMT for these connectivities.)

Constructing 1-round $(0, \delta)$ -SMT from FRS-codes. Although it is possible to give a general construction of $(0, \delta)$ -SMT using an approach similar to δ -RMT, for clarity of results and because of space limitations we limit ourselves to concrete constructions. We first describe a construction for a 1-round $(0, \delta)$ -SMT for $N =$

$2t + 1$ using FRS-codes and a multireceiver MAC, and then extend the result to the case where $N = (2 + c)t$, $c > \frac{1}{t}$. For $N = 2t + K$, $K > 1$, a similar approach can be used resulting in an optimal 1-round $(0, \delta)$ -SMT.

The construction of 1-round PSMT for $N = 3t + 1$ [7] uses an RS-code to encode the message, and the receiver algorithm uses unique decoding algorithm of RS-codes. For connectivity $2t + 1 \leq N \leq 3t$, the minimum distance of the RS-code will be $t + 1 \leq d \leq 2t$, and so unique decoding for t adversarial errors is not possible.

We use *list decoding* to correct errors beyond unique error correcting radius of the code, and use an authentication mechanism to recognize the sent codeword. There are however two major challenges:

- (i) In SMT the sender and the receiver *do not share a secret key* and so the key for the authentication mechanism (based on MACs) must be delivered to the receiver over the wires, some of which are corrupted.
- (ii) For $N = 2t + 1$, and code dimension $k = t + 1$ which is dictated by the perfect privacy requirement, the code rate is $R = k/N = \frac{t+1}{2t+1}$ and so the percentage of errors that needs to be corrected is $\rho = \frac{t}{2t+1} = 1 - R$, which is the information theoretic *list decoding capacity* of the code. Codes that can achieve this capacity and have efficient decoders need special construction.

An important property of the resulting $(0, \delta)$ -SMT protocols is that *they have the lowest δ* and so the highest reliability among all known optimal 1-round $(0, \delta)$ -SMT protocols with comparable connectivity (for protocols that output correct messages, or **Fail**.) Our proposed constructions of multireceiver MACs provide optimal and near optimal (different by a factor of 2) forgery probabilities and are of independent interest.

Advantages of the Approach

A general construction for 1-round δ -RMT. LD codes and multireceiver MACs are both well-established primitives with numerous efficient constructions. The advantage of a general construction using these two primitives as building blocks, is that one can choose appropriate constructions for a given setting. Moreover, advances in LD codes and MACs can result in better construction for δ -RMT systems. The instantiation of the LD code with FRS-code is directly adaptable (with revised message structure and code parameters) to $(0, \delta)$ -SMT. This means that the main building block of the receiver will stay the same in both cases and development of more efficient decoding for FRS-codes will translate into more efficient receiver algorithms for SMT.

1-round $(0, \delta)$ -SMT and RS-codes. FRS-codes are in fact RS-codes with blocks of symbols interpreted as elements of a larger field. The construction of $(0, \delta)$ -SMT from FRS-codes provides an elegant and systematic construction for 1-round $(0, \delta)$ -SMT for all connectivities ($N \geq 2t + 1$) using RS-codes.

The decoding algorithm is the same for RMT and SMT and in all cases consists of a two step algorithm: list decoding of the FRS-code, and a message verification algorithm based on the MAC for every element of the list. The proof of privacy

is based on the properties of the FRS-codes and are intuitive. The proof of reliability (calculation of δ) is also intuitive with concrete values depending on the parameters of the FRS-codes and the MAC.

A unified approach to 1-round δ -RMT and $(0, \delta)$ -SMT. The above shows a unified approach for the construction of these two primitives, reliable communication without or with privacy, for all connectivities $N \geq 2t + 1$. This means that the sender and receiver can use a modular construction in which the module with the higher complexity, which is the list decoding module, is implemented once and its parameters are adjusted depending on the required properties (reliability only, or both reliability and privacy) and the choice of the MAC determined by the given N and t .

δ -RMTs are similar to error correcting codes with protection against adversarial errors with the difference that adversary's view is limited to the t corrupted wires. In error correcting codes with protection against adversarial channels, the adversary can see the whole codeword before choosing the error pattern. In δ -RMT the adversary only sees the positions that it corrupts.

Related Work

Srinathan et al. designed an efficient and optimal 1-round δ -RMT protocol [16]. This protocol uses a complex combination of secret sharing by the sender and elaborate verification of the received information by the receiver to determine the correct message block. There are two optimal and efficient 1-round $(0, \delta)$ -SMT protocols for $N = 2t + 1$ [13,21]. The protocol in [13] is based on the 1-round δ -RMT protocol of [16] and has similar complexity. Moreover, to achieve the optimal transmission rate for higher connectivity, this protocol can not be directly used as the encrypted message blocks are broadcasted. The protocol of [21] suffers from the same problem as that of [13].

On the other hand, for $N = (2 + c)t, c > \frac{1}{t}$, there are two optimal and efficient 1-round $(0, \delta)$ -SMT protocols [21,19]. The protocol of [19] uses two SMT protocols in two levels. The first SMT protocol for the lowest connectivity is used many times on different subsets of the wires. The second protocol which works for higher connectivity is applied to virtual wires obtained from the actual physical wires. The shortcoming of this protocol is that to achieve optimal rate, the sender needs to send a very large information block (of size at least N^3 field elements). The protocol in [21] also uses multiple secret sharings in a clever way which results in a lower δ than that of [13].

2 Background and Primitives

In SMT problem, there is an incomplete network, that connects a sender $\mathcal{S}$ to a receiver $\mathcal{R}$. The sender and the receiver are connected by N vertex-disjoint paths, also known as *wires* or channels. The network is undirected and communication on the wires is synchronous and bidirectional. Both $\mathcal{S}$ and $\mathcal{R}$ are honest. The goal is to enable $\mathcal{S}$ to send a message m , drawn from a message space $\mathcal{M}$ with a probability distribution $\Pr(m)$, to $\mathcal{R}$ such that $\mathcal{R}$ receives the message *correctly* and *privately*.

In a *message transmission protocol*, the sender $\mathcal{S}$ chooses m from a message space $\mathcal{M}$ with a probability distribution $\Pr(m)$, and uses a protocol with one or more rounds, to send the message to the receiver. In each protocol round, $\mathcal{S}$ or $\mathcal{R}$, constructs a protocol message that is sent over the wires to the other party. A protocol message is received by the recipient of the round, possibly in a corrupted form, before the next round starts. At the end of the protocol, the receiver outputs a message m' , or outputs a **Fail**.

We consider only 1-round protocols. The adversary $\mathcal{A}$ has unlimited computational power and can corrupt and control a subset of wires: the adversary can eavesdrop, block or modify the communication over the corrupted wires. $\mathcal{A}$ can corrupt at most t out of the N wires and the corrupted wires are unknown to $\mathcal{S}$ and $\mathcal{R}$.

Denote by $V_{\mathcal{A}}(M_{\mathcal{S}}, r_{\mathcal{A}})$ the random variable that denotes the view of the adversary $\mathcal{A}$ when attacking the protocol assuming the sender has chosen $M_{\mathcal{S}}$ and $r_{\mathcal{A}}$ is the random coins of the adversary. Let the statistical distance of two random variables X, Y defined over a set $\mathcal{U}$ be defined as, $\Delta(X, Y) = \frac{1}{2} \sum_{u \in \mathcal{U}} |\Pr[X = u] - \Pr[Y = u]|$.

Definition 1. A message transmission protocol between $\mathcal{S}$ and $\mathcal{R}$ is an (ε, δ) -Secure Message Transmission $((\varepsilon, \delta)$ -SMT) protocol if the following two conditions are satisfied:

- *Privacy:* For every two messages $m_0, m_1 \in \mathcal{M}$ and every $r \in \{0, 1\}^*$ used by the adversary,
 $\Delta(V_{\mathcal{A}}(m_0, r), V_{\mathcal{A}}(m_1, r)) \leq \varepsilon$, where the probability is over the randomness of $\mathcal{S}$ and $\mathcal{R}$.
- *Reliability:* $\mathcal{R}$ outputs the message m with probability $\geq 1 - \delta$, and **Fail** with probability $\leq \delta$. That is, the receiver never outputs an incorrect message and, $\Pr[\text{Receiver outputs Fail}] \leq \delta$.

This is the definition of reliability used by Kurosawa et. al. [12]. The original definition of reliability in [8] however assumes that the receiver always outputs a message m' and δ -reliability is, $\Pr[m' \neq m] \leq \delta$. Kurosawa et al. require that the receiver be sure that the received message is correct. When $\varepsilon = 0$, the protocol is said to achieve *perfect privacy*, and when $\delta = 0$, the protocol is said to achieve *perfect reliability*. A δ -Reliable Message Transmission (δ -RMT) protocol is a protocol between $\mathcal{S}$ and $\mathcal{R}$ in the same network setting, and only requiring the reliability of transmission.

It was shown [8] that $(0, \delta)$ -SMT is possible if and only if $N \geq 2t + 1$ and 1-round PSMT is possible if and only if $N \geq 3t + 1$ [3]. 1-round δ -RMT protocols exist if and only if $N \geq 2t + 1$ [8].

Communication efficiency of RMT and SMT protocols is in terms of the number of rounds, and transmission rate. The number of rounds of an SMT protocol is the number of interactions between $\mathcal{S}$ and $\mathcal{R}$. Transmission rate of RMT and SMT protocols is the ratio of the total communication to the length of the message: that is the communication cost of sending one bit.

Lower bounds on transmission rates of 1-round δ -RMT and 1-round $(0, \delta)$ -SMT protocols are $\Omega(\frac{N}{N-t})$ [14] and $\Omega(\frac{N}{N-2t})$ [13], respectively. Protocols whose transmission rate asymptotically match the associated lower bounds are called *optimal*. For 1-round δ -RMT with $N = 2t + 1$, the lower bound on the transmission rate is $\Omega(1)$. For 1-round $(0, \delta)$ -SMT protocols with $N = 2t + 1$ and $N = (2 + c)t, c > \frac{1}{t}$, optimal protocols must have transmission rates $O(N)$ and $O(1)$, respectively.

Computation efficiency of RMT and SMT protocol is the amount of computation performed by $\mathcal{S}$ and $\mathcal{R}$ throughout the protocol. A protocol that needs exponential (in N) computation for $\mathcal{S}$ and $\mathcal{R}$, is called *inefficient*. Efficient protocols need polynomial (in N) computation.

2.1 Folded Reed-Solomon Codes

A (k, n) linear error correcting code over $\mathbf{F}_q$ is a subspace of dimension k of the n dimensional vector space over $\mathbf{F}_q$. The *information rate* of a linear error correcting code is, $R = \frac{k}{n}$. A decoder takes a corrupted word and determines the most likely codeword that was sent. In unique decoding, the closest (Hamming distance) codeword to the received one is found. In list decoding, a list of codewords within a radius from the received word is found. For a constant ρ , let ρn denotes the number of errors that can be corrected by the decoder.

Definition 2. A code C with the encoding function $LD : \mathbf{F}_q^k \rightarrow \mathbf{F}_q^n$ is (ρ, L) -list decodable (LD) if the number of codewords within distance ρn of any received word is at most L . That is for every word $y \in \mathbf{F}_q^n$, there are at most L codewords at distance ρn (where ρ is the relative distance) or less from y .

The *list decoding capacity* $\rho_{cap}(R)$ of a code with rate R is the information theoretic limit of list decodability and is given by $\rho_{cap}(R) = 1 - R = 2\rho_U(R)$, where $\rho_U(R) = (1 - R)/2$, is the unique decoding radius of the code. It is shown [6] that for sufficiently large alphabet size $\rho_{cap}(R)$ can reach $1 - R - \epsilon$. So for any code rate, *list decoding can potentially correct twice as many errors as unique decoding* [10].

To achieve this potential however, one needs special constructions that guarantee that the list size is bounded by L . Efficient list decoding algorithms are polynomial time. *Folded Reed-Solomon codes (FRS-codes)*, proposed by Guruswami et al. [10], is a special type of RS-codes that corrects up to a fraction $\rho = 1 - R - \epsilon$ of errors, for any rate R and arbitrary $\epsilon > 0$ using a polynomial time list decoding algorithm. The list size, however for some parameter choices of the code, becomes exponential.

Description of Folded Reed-Solomon Codes. FRS encoding and decoding are defined using an RS-code of length n and dimension k over a finite field $\mathbf{F}_q$, using two parameters, u , the *folding parameter* and s , which determines the $(s + 1)$ -variate interpolation used in the decoding. Let u be an integer, called the *folding parameter*, such that n is divisible by u . n is chosen as the largest integer that is less than $q = |\mathbf{F}_q|$ and is divisible by u .

Let γ be a generator of $\mathbf{F}_q^*$, the multiplicative group of the field $\mathbf{F}_q$. A codeword $(f(1), f(\gamma), f(\gamma^2), \dots, f(\gamma^{n-1}))$ of $RS[n, k]$ is the evaluation of a polynomial $f(x)$, of degree at most $k - 1$ over $\mathbf{F}_q$, at the (ordered) points $1, \gamma, \gamma^2, \dots, \gamma^{n-1}$.

Definition 3. *The u -folded FRS-code is a code with block length $N = n/u$ over $\mathbf{F}_q^u$. The encoding of a message, represented by a polynomial $f(x)$ of degree at most $k - 1$ over $\mathbf{F}_q$, is obtained as u -tuples, $(f(\gamma^{ju}), f(\gamma^{ju+1}), \dots, f(\gamma^{ju+u-1}))$, for $0 \leq j < N$. In other words, a codeword of the u -folded RS-code is in one-to-one correspondence with codewords of the RS-code C , and is obtained by grouping consecutive u -tuples of components of C .*

$$\begin{bmatrix} f(1) & f(\gamma^u) & \dots & f(\gamma^{u(N-1)}) \\ f(\gamma) & f(\gamma^{u+1}) & \dots & f(\gamma^{u(N-1)+1}) \\ \vdots & \vdots & \ddots & \vdots \\ f(\gamma^{u-1}) & f(\gamma^{2u-1}) & \dots & f(\gamma^{uN-1}) \end{bmatrix}$$

Decoding u -folded RS-code uses $(s + 1)$ -variate interpolation followed by a list pruning step. In the full version of the paper [20], we give an outline of the original decoding algorithm.

Linear-algebraic list decoding. In [9] a variant decoding for FRS-code is given in which the interpolation uses polynomial $Q(X, Y_1, \dots, Y_s)$ where degree of Y_i is 1. This variant has a simpler exposition and allows a simpler way of choosing the code parameter, s and u . However it can correct less errors. By appropriate choice of s and u , the code can reach $1 - R - \epsilon$ radius and so asymptotically is optimal. Lemma 1 below, given in [9], gives the condition that needs to be satisfied by the two parameters and the number of errors to be corrected.

Lemma 1. *In linear-algebraic list decoding, for every integer u and s , the linear interpolation FRS decoding algorithm successfully list decodes to a radius $N - T$ as long as the agreement parameter T satisfies:*

$$T \geq N \left(\frac{1}{s+1} + \frac{s}{s+1} \frac{uR}{u-s+1} \right).$$

T is the number of correct positions. The algorithm outputs a list of size at most $|\mathbf{F}_q|^{s-1} = q^{s-1}$ codewords.

2.2 Multireceiver Message Authentication Codes

A one-time MAC in information-theoretic setting, is a shared key cryptographic primitive, defined by two functions: a MAC function that takes a message $m \in \mathcal{M}$ and the shared key $k_{MAC} \in \mathcal{K}$ and outputs a tag $MAC(m, k_{MAC})$, which is appended to the message, and a verification function, $V((m', x'), k_{MAC})$, which outputs 1 if (m', x') is a valid pair for the key k_{MAC} , and 0, otherwise. The following definition is for security of one-time MAC.

Definition 4. A one-time MAC, $MAC : q^{l_{msg}} \times q^{l_{key}} \rightarrow q^{l_{tag}}$ has forgery probability γ if the best success chance of a computationally unbounded adversary with access to a message and tag pair $(m, x), x = MAC(m, k_{MAC})$, to construct a different pair (m', x') where $m \neq m'$, and $V((m', x'), k_{MAC}) = 1$ is at most γ , where the probability is taken over all keys.

Multireceiver authentication codes [5] allow a sender to efficiently send a message to a group of N receivers such that each receiver can individually verify the message, using his individual shared key k_i with the sender. The sender is honest but upto t receivers can be corrupted and attempt to forge a message to be acceptable by an uncorrupted receiver. In a $(t + 1, N)$ -multireceiver message authentication system, there are N receivers and at most t receivers can be corrupted.

Definition 5. A one-time $(t + 1, N)$ -multireceiver authentication code (multi-receiver MAC) with N receivers and $k_{MAC} = (k_S, k_1, \dots, k_N)$, is γ -secure if the best success chance of any colluding set of receivers (size at most t) with access to a message and tag pair, $(m, x, x = MAC(m, k_S))$ in forging a different message, tag pair (m', x') , where $m \neq m'$, and $V_i((m', x'), k_i) = 1$, is at most γ , and the probability is over all unknown keys.

2.3 New Constructions for Multireceiver MAC

The basic construction of $(t + 1, N)$ -multireceiver MACs is for authenticating a single message. To authenticate a block of messages one can use a one-time multireceiver MAC multiple times, or for more efficiency, use separately designed multireceiver MAC for message blocks. In the following, we give two new constructions for $(t + 1, N)$ -multireceiver MACs for message blocks that are used in the RMT and SMT constructions of this work. Construction 1 is a generalization of [5] for $d > 1$ messages. Construction 2 is built over a brand new MAC.

Construction 1.

Let $m = (m_1, \dots, m_d)$, where $m_i \in \mathbf{F}_q^{s'}, i = 1, \dots, d$, be the message block.

- *Key distribution:* A Trusted Initializer does the following: (i) randomly generates $d + 1$ polynomials $P_1(z), P_2(z), \dots, P_{d+1}(z)$, each of degree at most t , over $\mathbf{F}_q^{s'}$; chooses N random distinct elements $z_1, z_2, \dots, z_N$, where $z_i \in \mathbf{F}_q^{s'}, i = 1, \dots, N$; makes $z_1, z_2, \dots, z_N$ public, assigns z_i to receiver i and privately sends $k_i = (P_1(z_i), P_2(z_i), \dots, P_{d+1}(z_i))$ to receiver i , for $1 \leq i \leq N$ and to the sender.
- *Constructing authenticated messages:* The sender computes the authentication tag as:

$$A(z) = P_1(z)m_1 + P_2(z)m_2 + \dots + P_d(z)m_d + P_{d+1}(z).$$

The authenticated messages consist of the message block and the tag polynomial, $((m_1, m_2, \dots, m_d), A(z))$.

- *Verification:* Receiver i accepts $(m_1, m_2, \dots, m_d, A(z))$ if and only if $A(z_i) = P_1(z_i)m_1 + P_2(z_i)m_2 + \dots + P_d(z_i)m_d + P_{d+1}(z_i) \pmod{q^{s'}}$.

The above construction is a $(t+1, N)$ -multireceiver MAC for authentication of a block of size d . The size of the tag is $t+1$ elements of $\mathbf{F}_{\mathbf{q}}^{s'}$ and so only depends on the collusion size (rather than the total number of receivers).

The following Theorem is proved in the full version of the paper [20].

Theorem 1. *For construction 1, the forgery probability is bounded as $\gamma \leq q^{-s'}$.*

Construction 2.

This multireceiver MAC is built on a new one-time MAC which has message block size $\binom{t+2}{2} - 1$ (each block element from $\mathbf{F}_{\mathbf{q}}^{s'}$) and has forgery probability bounded by $\frac{2}{q^{s'}}$.

- *Key distribution:* Same as Construction 1, with $d = t$.
- *Constructing authenticated messages:* For $m = (m_1, m_2, \dots, m_{\binom{t+2}{2}-1})$, the sender computes,

$$A(z) = m_1 P_1(z) + \dots + m_t P_t(z) + m_{t+1} P_1(z)^2 + \dots + m_{2t} P_t(z)^2 \\ + m_{2t+1} P_1(z) P_2(z) + \dots + m_{\binom{t+2}{2}-1} P_{t-1}(z) P_t(z) + P_{t+1}(z).$$

- *Verification:* Receiver i accepts $(m_1, m_2, \dots, m_{\binom{t+2}{2}-1}, A(z))$ if and only if

$$A(z_i) = m_1 P_1(z_i) + \dots + m_t P_t(z_i) + m_{t+1} P_1(z_i)^2 + \dots \\ + m_{\binom{t+2}{2}-1} P_{t-1}(z_i) P_t(z_i) + P_{t+1}(z_i).$$

Here $m_i \in \mathbf{F}_{\mathbf{q}}^{s'}$, and $P_1(z), P_2(z), \dots, P_{t+1}(z)$ are polynomials of degree at most t over $\mathbf{F}_{\mathbf{q}}^{s'}$. The MAC function is a linear sum (coefficients being the message block) of all products of at most two polynomials from the set, $\{P_1(z), P_2(z), \dots, P_t(z)\}$. Finally $P_{t+1}(z)$ is used to mask the result. The final MAC value is a polynomial over $\mathbf{F}_{\mathbf{q}}^{s'}$. The size of the message block (over $\mathbf{F}_{\mathbf{q}}^{s'}$) that is authenticated by the MAC, is $\binom{t+2}{2} - 1$.

Theorem 2. *For construction 2, the forgery probability is bounded as $\gamma \leq 2q^{-s'}$.*

The proof outline is provided in the full version of the paper [20].

3 Construction of 1-Round δ -RMT for $N \geq 2t + 1$

Construction 3: A general construction of 1-round δ -RMT. The protocol requires a (ρ, L) LD code of dimension k and length N over $\mathbf{F}_{\mathbf{q}}$, with $\rho = \frac{t}{N}$ and list size L , and a $(t+1, N)$ -multireceiver MAC with message space $\mathbf{F}_{\mathbf{q}}^{k'}$, $k' = k - l_{tag} < k$, and forgery probability ϵ . Here l_{tag} is the length of tag in terms of $\mathbf{F}_{\mathbf{q}}^{s'}$ elements.

- **Sender Algorithm:**

- 1) Securely generates keys $(k_S, k_1, \dots, k_N)$ for a multireceiver MAC and assigns the key k_i to the i^{th} wire, W_i .
- 2) Constructs the message block $m_S, m_S \in \mathbf{F}_{\mathbf{q}}^k$ to be sent to the receiver as,

$$m_S = (I_S, \text{MAC}(I_S, k_S)). \quad (1)$$

The sender constructs the codeword c_S of the LD code by encoding m_S as $c_S = LD(m_S)$. The sender sends the i^{th} component of the codeword c_S , and k_i through wire W_i . k_S is kept by the sender.

– **Receiver Algorithm:**

1) Parses the received (corrupted) N -vector; separates the key k_i from the i^{th} component (possibly corrupted) of the received word for $i = 1, \dots, N$; constructs the corrupted codeword and uses LD decoding algorithm to obtain a list (of size L) of codewords that are at distances at most $\rho = \frac{t}{N}$ from the received word. *The list will always include the correct codeword.*

2) To identify the sent codeword, the receiver (i) parses each codeword in the list into a message, tag pair $(\widehat{m}_i, \widehat{t}_i), i = 1, \dots, L$; (ii) for each message $\widehat{m}_i$, uses all keys $k_j, j = 1, \dots, N$, and checks the verification equations $V_j(\widehat{m}_i, k_j) = \widehat{t}_i$. The message is accepted if at least $t+1$ verification equations are passed; otherwise the codeword is rejected.

The decoding algorithm of the SMT succeeds if there is a unique codeword that is accepted by the verification algorithm above. Otherwise, the receiver outputs a Fail.

Theorem 3. *The above construction is a 1-round δ -RMT protocol for $N = 2t + 1$, with $\delta = 1 - (L - 1)\epsilon$ and transmission rate $\frac{N(1+|k_i|)}{k - l_{\text{tag}}}$.*

The proof is omitted due to lack of space.

3.1 An Optimal δ -RMT

In the following we give an instantiation of the general construction above using (i) an FRS-code for the LD code, and (ii) Construction 2 for multireceiver MAC. The multireceiver MAC allows authentication of a message block of size $\sim t^2$ field elements requiring $\sim t$ field element for encoding of m_S as, to be sent on each wire, resulting in optimal transmission rate.

Selecting Parameters of the FRS-code. Let $N = 2t + 1$ for the RMT. We consider a u -folded RS-code of length N with length $n = Nu$ for the underlying RS-code. Using the message format in (1) and using a block of size $\left(\binom{t+2}{2} - 1\right)$ of elements of $\mathbf{F}_q^{s'}$ for information block we will have the required dimension for the code as,

$$k = |m_S| = \left(\binom{t+2}{2} - 1\right)s' + ts' + s' = \frac{s'(t^2 + 5t + 2)}{2}. \quad (2)$$

For a code of length $N = 2t + 1$ and dimension k as (2), we must choose folding parameter u , number of decoding variable s , and the finite field sizes s' and q , to ensure that decoding succeeds for linear-algebraic decoding (outlined in Section 2.1) for radius $\rho = t/N$ (t errors in the FRS-code). That is, the inequality 3 below, is satisfied.

$$t + 1 \geq N\left(\frac{1}{s+1} + \frac{s}{s+1} \frac{uR}{u-s+1}\right). \quad (3)$$

Let $0 < \sigma < 1$ and set $s = \frac{N}{\sigma} - 1$. Furthermore, choose $s' = \left\lfloor \frac{2u(t+1-2\sigma)}{t^2+5t+2} \right\rfloor$, and $u > s^2 - 1$. the following shows that with these choices of parameters inequality (3) is satisfied. We have,

$$t+1 > t+1-\sigma = \sigma + (t+1-2\sigma) \stackrel{(a)}{=} \sigma + \frac{s'(t^2+5t+2)}{2u} \stackrel{(b)}{=} \sigma + \frac{k}{u} \quad (4)$$

where (a) is because of the choice of s' and (b) is because of the value of k in (2). Note that because $s \geq 1$, we have $\frac{1}{u} > \frac{s}{s+1} \frac{1}{u-s+1}$ and so, (4) gives the following:

$$t+1 > \sigma + \frac{k}{u} > \sigma + \frac{s}{s+1} \frac{k}{u-s+1} = N \left(\frac{1}{s+1} + \frac{s}{s+1} \frac{uR}{u-s+1} \right)$$

Finally we can choose q to be the smallest prime that is bigger than the codeword length $n = Nu$.

The Protocol. The construction uses (i) an FRS-code with parameters u and s obtained above and (ii) Construction 2 of the multireceiver MAC in Section 2.3. The final protocol is as follows.

– **Sender Algorithm:**

1. Uses the key generation algorithm of Construction 2 and obtains for wire $W_i, i = 1, \dots, N$, the associated key,

$$k_i = (P_1(z_i), P_2(z_i), \dots, P_{t+1}(z_i)).$$

The tag for the information part $I_S = (m_0, m_1, \dots, m_{\binom{t+2}{2}-1}), m_i \in \mathbf{F}_q^{s'}$:

$$\begin{aligned} A(z) = & m_1 P_1(z) + \dots + m_t P_t(z) + m_{t+1} P_1(z)^2 + \dots + m_{2t} P_t(z)^2 \\ & + m_{2t+1} P_1(z) P_2(z) + \dots + m_{\binom{t+2}{2}-1} P_{t-1}(z) P_t(z) + P_{t+1}(z). \end{aligned}$$

2. The message m_S is of the form (1), $m_S = (m_0, m_1, \dots, m_{\binom{t+2}{2}-1}, A(z))$. The dimension of the FRS-code is $(\binom{t+2}{2} - 1)s' + ts' + s'$ over $\mathbf{F}_q$, where $s' = \left\lfloor \frac{2u(t+1-2\sigma)}{t^2+5t+2} \right\rfloor$.

3. The sender encodes the message to a codeword c_S using the FRS encoding algorithm. Wire j , $1 \leq j \leq 2t+1$, transmits the j^{th} component of c_S and k_j .

– **Receiver Algorithm:** Uses the two step decoding of Construction 3 for FRS-code as the LD code, and Construction 2 as the multireceiver MAC. The algorithm outputs the correct message or **Fail**.

Theorem 4. *The above construction is a δ -RMT with $\delta = \frac{2(t+1)}{q^{s'}-s+1}$, which is equal to $\frac{N+1}{q^{s'}-s}$, when $N = 2t+1$. The transmission rate is constant.*

The proof is given in the full version of the paper [20].

Comparison with Related Work

For $N = 2t+1$, this protocol has $\delta = \frac{N+1}{q}$. The value of δ for the only other known optimal 1-round δ -RMT protocol [13], is $\frac{N^2(N-1)}{q}$ ($q \geq \frac{N^2(N-1)}{\delta}$). The field size required in our construction is Nu .

Table 1 compares our protocol with the protocol in [13]. For simplicity of comparison we have used $s' = s$, resulting in $\delta = \frac{t+1}{q}$. The comparison shows that for all connectivities the proposed protocol has a much higher reliability. The field size although asymptotically is larger (N^4 and N^3 , respectively) for concrete values (for example $N < 1000$, and $\delta < 10^{-3}$) could be smaller or comparable. Decoder efficiency for higher connectivities is the same. For $N = 2t + 1$, however, our protocol has exponential cost.

Table 1. Comparison of 1-round δ -RMT protocols for different connectivities which never outputs an incorrect message; here Comp. refers to computation complexity, Poly. refers to polynomial (in N), Exp. refers to exponential (in N), and $\mathbf{F}_q$ is the field

Author	Comp. $N = 2t + 1$	Comp. $N = (2 + c)t$	q	δ	Optimality
[13]	Poly.	Poly.	$\geq \approx \frac{N^3}{\delta}$	$\leq \approx \frac{N^3}{q}$	Yes
This Work	Exp.	Poly.	$\geq Nu$	$\leq \frac{2(t+1)}{q} \approx \frac{N+1}{q}$	Yes

4 1-Round $(0, \delta)$ -SMT

To use the approach of Construction 3 for $(0, \delta)$ -SMT, one needs to ensure that the view of the adversary does not leak any information about the information block I_S . Using FRS-code for LD code allows us to achieve this goal by choosing the dimension of the code to be at least $t + 1$. Code parameters need to be chosen such that decoding up to $\rho = \frac{t}{N}$ is achievable. For $N = 2t + 1$ given in Section 4.1, this requires the FRS-code to achieve the list decoding capacity. The construction for $N = (2 + c)t$, $c > \frac{1}{t}$, given in Section 4.2, uses Construction 2 for multireceiver MAC to allow easier calculation of code parameters while maintaining optimal asymptotic performance. Same approach can also be used for connectivity $N = 2t + K$, where $K > 1$ is a constant. Details are omitted because of space.

In all cases, decoding is the two step Receiver Algorithm of Construction 3.

4.1 A Construction for 1-Round $(0, \delta)$ -SMT for $N = 2t + 1$

The construction uses the approach of Construction 3, but with a different message structure to guarantee perfect privacy.

Message Structure. The message m_S consists of three parts: (i) information part $I_S = (m_0, m_1, \dots, m_{\sigma u-1})$, $m_i \in \mathbf{F}_q^{s'}$; (ii) ut random elements $(a_1, a_2, \dots, a_{ut})$, $a_i \in \mathbf{F}_q$ that are used to ensure privacy that the ut captured components do not reveal anything about I_S ; (iii) $MAC(X, k_S)$ where $X = (m_0, m_1, \dots, m_{\sigma u-1}, a_1, \dots, a_{s'd-\sigma u})$.

That is,

$$m_S = (m_0, m_1, \dots, m_{\sigma u-1}, a_1, a_2, \dots, a_{ut}, MAC(X, k_S)).$$

Here σ is a positive constant. To have optimal rate, the information block size must be a constant fraction of u . Using Construction 1, this size is $s'd$, where d is message length for the MAC. To find s' , the information block (I_S) and the first $s'd - \sigma u$ elements a_i are used to form d blocks of size s' , where $d = \lceil \frac{\sigma u}{s'} \rceil$. Each s' block is interpreted as an element of $\mathbf{F}_q^{s'}$ and MAC calculations are performed over $\mathbf{F}_q^{s'}$. The ut random elements appended to I_S will ensure perfect privacy. The MAC is only computed on X . The total length of m_S to be encoded by the FRS-code is $ut + \sigma u + s'(t + 1)$ where $\sigma < 1$ is a constant. The key k_i for wire i consists of $d + 1$ elements $P_1(z_i), P_2(z_i), \dots, P_{d+1}(z_i)$ over $\mathbf{F}_q^{s'}$. The multireceiver MAC value for X is:

$$MAC(X, k_S) = A(z) = P_1(z)x_1 + P_2(z)x_2 + \dots + P_d(z)x_d + P_{d+1}(z).$$

The codeword of the FRS-code that is constructed for m_S , will have N components, each an element of $\mathbf{F}_q^u$. The adversary's view will contain only t elements of $\mathbf{F}_q^u$ and will be independent from I_S .

Parameters of the FRS-code. The u -folded RS-code will have $N = 2t + 1, n = Nu$, and $k = ut + \sigma u + ts' + s'$. We must choose u, s , and the field size q , to ensure that decoding succeeds for linear-algebraic decoding (outlined in Section 2.1) up to radius $\rho = t/N$.

According to Lemma 1,

$$t + 1 \geq N \left(\frac{1}{s + 1} + \frac{s}{s + 1} \frac{uR}{u - s + 1} \right).$$

We set the parameter $s = (N/\sigma) - 1$, $u > s^2 - 1$, and $s' = \left\lfloor \frac{u(1-3\sigma)}{t+1} \right\rfloor$, where $0 < \sigma < \frac{1}{3}$ is a positive constant. By using these values of σ, u, s' , one can verify that the inequality is satisfied. Finally we can choose q to be the smallest prime that is bigger than the codeword length $n = Nu$.

Construction 4: $(0, \delta)$ -SMT Protocol for $N = 2t + 1$.

– **Sender Algorithm:**

1. Uses the key generation of Construction 1 and obtains for wire $W_i, i = 1, \dots, N$, the associated key,

$$k_i = (P_1(z_i), P_2(z_i), \dots, P_{d+1}(z_i)).$$

2. Constructs m_S : Forms $I_S = (m_0, m_1, \dots, m_{\sigma u - 1}), m_i \in \mathbf{F}_q^{s'}$ and calculates the tag,

$$A(z) = x_1 P_1(z) + x_2 P_2(z) + \dots + x_d P_d(z) + P_{d+1}(z),$$

for d and s' chosen as above. Here $X = (m_0, \dots, m_{\sigma u - 1}, a_1, \dots, a_{s'd - \sigma u})$. m_S is of the form (1) given by, $(m_0, m_1, \dots, m_{\sigma u - 1}, a_1, a_2, \dots, a_{ut}, A(z))$.

3. Constructs c_S and message transcript: The sender encodes the message to a codeword c_S using the FRS encoding algorithm. Wire $j, 1 \leq j \leq 2t + 1$, transmits the j^{th} component of c_S and k_j .

– **Receiver Algorithm:** Uses the decoding algorithm of Construction 3.

Theorem 5. *The SMT protocol described above is a $(0, \delta)$ -SMT for $N = 2t + 1$, with $\delta = \frac{t+1}{q^{s'-s+1}}$.*

The proof is omitted due to lack of space, but is given in the full version of the paper [20].

Transmission rate: The transmission rate is $\frac{uN+(s'd+s')N}{\sigma u} = \mathcal{O}(N)$ and it is optimal for 1-round $(0, \delta)$ -SMT for $N = 2t + 1$.

Computation complexity: The list size is at most q^{s-1} . Each element of the list must be verified and so the complexity of SMT decoding algorithm is $\mathcal{O}(q^N)$ (as $s = \mathcal{O}(N)$).

Comparison with Related Work. Table 2 compares the protocol with 1-round $(0, \delta)$ -SMT protocols that have the property that the output is either the correct message or **Fail**. For simplicity of comparison we have used $s' = s$, resulting in $\delta = \frac{t+1}{q} = \frac{N+1}{2q}$, when $N = 2t + 1$. The table shows that δ for this construction is the lowest. The minimum field size however is larger and decoding is computationally inefficient. In Section 4.2 we show that both these shortcomings can be removed for higher connectivities.

Table 2. Comparison of 1-round $(0, \delta)$ -SMT protocols for $N = 2t + 1$; here Comp. refers to computation complexity, Poly. refers to polynomial (in N), Exp. refers to exponential (in N) and $\mathbf{F}_q$ is the field. The protocols never output incorrect message. Here b is a constant and λ is the probability that the cheater wins in a secret sharing scheme with a cheater.

Author	Comp.	q	δ	Optimality
[12]	Exp.	$> N$	$\leq ((\binom{N}{t+1} - 1)\lambda \approx N^{(N+1)/2}\lambda)$	Yes
[17]	Poly.	$\geq \frac{2N^3}{\delta}$	$\leq \frac{N^3}{q}$	Yes
[4]	Poly.	$\geq bt(t+1) \approx N^2$	$\leq \frac{t(t+1)}{q} \approx \frac{N^2}{q}$	No
[21]	Poly.	$\geq bt(t+1) \approx N^2$	$\leq \frac{t(t+1)}{q} \approx \frac{N^2}{q}$	Yes
This Work	Exp.	$\geq Nu \approx N^4$	$\leq \frac{t+1}{q} \approx \frac{N+1}{2q}$	Yes

4.2 1-Round $(0, \delta)$ -SMT for $N = 2t + ct, c > 1/t$

Let $N = 2t + ct, c > \frac{1}{t}$. We use the same approach as Construction 4, using Construction 2 for multireceiver MAC and choose parameters of the FRS-code and multireceiver MAC such that the SMT construction has optimal rate and efficient computation. The message m_S has the format of (1) and can be written as $(m_0, m_1, \dots, m_{(\binom{t+2}{2}-1)}, a_1, a_2, \dots, a_{ut}, \text{MAC}(X, k_S))$, where $X = I_S = (m_0, m_1, \dots, m_{(\binom{t+2}{2}-1)})$ is the information block. The MAC function is over $\mathbf{F}_q^s$, where s is the parameter of FRS decoding (instead of $\mathbf{F}_q^{s'}$ for $N = 2t + 1$). The tag value is:

$$A(z) = m_1 P_1(z) + \cdots + m_t P_t(z) + m_{t+1} P_1(z)^2 + \cdots + m_{2t} P_t(z)^2 \\ + m_{2t+1} P_1(z) P_2(z) + \cdots + m_{\binom{t+2}{2}-1} P_{t-1}(z) P_t(z) + P_{t+1}(z),$$

where $m_i \in \mathbf{F}_{\mathbf{q}}^s$ and polynomials $P_1(z), P_2(z), \dots, P_{t+1}(z)$ are over $\mathbf{F}_{\mathbf{q}}^s$ and have degree t .

Parameters s, u , and q are chosen to allow the receiver to decode up to t errors. The number of correct wires $t + ct$ must satisfy,

$$t + ct \geq N \left(\frac{1}{s+1} + \frac{s}{s+1} \frac{uR}{u-s+1} \right).$$

For a constant c_0 , let $u = c_0 t$. We show that list decoding upto $\rho = \frac{t}{N}$ is possible for a constant value of $s = s_0$ when $t > 7c_0 + 2s_0 + 1$, and the value of c satisfies $c > \frac{s_0}{c_0} + \frac{1}{s_0}$. The details are in the full version of the paper [20]. Table 4.2 below gives example values for s_0 and c , and the size of the resulting list. The complete protocol is given below.

Table 3. Values of c and the list size for different values of s_0

s_0	list size	c
$s_0 = 1$	q^0	$c \approx \frac{1}{c_0} + 1$
$s_0 = 2$	q	$c \approx \frac{2}{c_0} + 1/2$
$s_0 = 3$	q^2	$c \approx \frac{3}{c_0} + 1/3$

SMT Protocol for $N = (2 + c)t, c > \frac{1}{t}$.

– **Sender Algorithm:**

1. Uses the key generation of Construction 2 and obtains for wire $W_i, i = 1, \dots, N$, the associated key,

$$k_i = (P_1(z_i), P_2(z_i), \dots, P_{t+1}(z_i)).$$

2. The message m_S is,

$$m_S = (m_0, m_1, \dots, m_{\binom{t+2}{2}-1}, a_1, a_2, \dots, a_{ut}, A(z)),$$

where the tag for the information block $I_S = (m_0, m_1, \dots, m_{\binom{t+2}{2}-1}), m_i \in \mathbf{F}_{\mathbf{q}}^{s_0}$ is,

$$A(z) = m_1 P_1(z) + \cdots + m_t P_t(z) + m_{t+1} P_1(z)^2 + \cdots + m_{2t} P_t(z)^2 \\ + m_{2t+1} P_1(z) P_2(z) + \cdots + m_{\binom{t+2}{2}-1} P_{t-1}(z) P_t(z) + P_{t+1}(z).$$

3. The FRS-code is over $\mathbf{F}_{\mathbf{q}}^u$ and has dimension $k = ut + (\binom{t+2}{2} - 1)s_0 + ts_0 + s_0$. The sender encodes the message to a codeword c_S using the FRS encoding algorithm. Wire $j, 1 \leq j \leq 2t + ct$, transmits the j^{th} component of c_S and k_j .

– **Receiver Algorithm:**

Uses the SMT decoding algorithm of Construction 3.

Theorem 6. *The protocol above is a 1-round $(0, \delta)$ -SMT for $N = (2+c)t, c > \frac{1}{t}$ with optimal transmission rate, and has efficient (polynomial time) decoding. The value of δ is given by $\frac{2(t+1)}{q}$ and is the smallest among all known protocols with the same connectivity.*

The proof outline is given in the full version of the paper [20].

Comparison with Related Work

There has been two other optimal (transmission rate) and efficient (computation) 1-round $(0, \delta)$ -SMT protocols for higher connectivity ($N = (2+c)t, c > \frac{1}{t}$) [19,21]. The protocol presented in Section 4.2 has the least δ . The comparison of these protocols is outlined in Table 4.

Table 4. Comparison of 1-round $(0, \delta)$ -SMT protocols for $N = (2+c)t, c > \frac{1}{t}$; here Comp. refers to computation complexity, Poly. refers to polynomial (in N), Exp. refers to exponential (in N) and $\mathbf{F}_q$ is the field. Here ν is a parameter used in wire-virtualization which refers to the number of *physical* wires in each *virtual* wire.

References	Comp.	δ	Optimality	Outputs Incorrect Message
[19]	Poly.	$\leq \frac{N^\nu t(t+1)}{q} \approx \frac{N^{\nu+2}}{q}$	Yes	Yes ¹
[21]	Poly.	$\leq \frac{t(t+1)}{q} \approx \frac{N^2}{q}$	Yes	No
This Work	Poly.	$\leq \frac{2(t+1)}{q} \approx \frac{N}{q}$	Yes	No

5 Concluding Remarks

We showed a novel general approach to the construction of 1-round δ -RMT and $(0, \delta)$ -SMT protocols using LD codes and MACs. The approach has a number of advantages, (i) it is general, unifies construction of 1-round δ -RMT and $(0, \delta)$ -SMT protocols, and is applicable to all connectivities including $N = 2t + K, K \geq 1$, where K is a constant, (ii) relies on well-studied mathematical objects (list decodable codes and MACs) and so allow a wide range of instantiations; this also allows direct translation of advances in those areas into better constructions for 1-round δ -RMT and $(0, \delta)$ -SMT, and finally (iii) resulting in proofs of security (privacy and reliability) to be intuitive and easily verifiable. Instantiation of this general approach, using FRS-codes and our proposed multireceiver MACs result in constructions that have optimal transmission rates and the smallest δ , when $N = 2t + 1$ and $N = (2+c)t, c > \frac{1}{t}$. For $N = 2t + 1$ the protocol is not computationally efficient for our instantiations. It is an interesting open problem if this general construction can be instantiated to achieve efficient and optimal construction for $N = 2t + 1$. Another interesting open question is whether δ can be further lowered while maintaining optimality. Another open problem is establishing lower bound on δ and constructing protocols that can achieve the

¹ The authors in [19] mention that their protocol can be modified to output only correct message block by using a different sub-protocol.

bound. We note that 1-round δ -RMT, can be seen as error correcting code in the traditional setting where channel corruption is adversarial and adversary has a limited view of the codeword (only t component).

References

1. Ben-Or, M., Goldwasser, S., Wigderson, A.: Completeness Theorems for Non-cryptographic Fault-tolerant Distributed Computation (extended abstract). In: Proc. of STOC, pp. 1–10 (1988)
2. Chaum, D., Crepeau, C., Damgard, I.: Multiparty Unconditionally Secure Protocols (Extended Abstract). In: Proc. of FOCS, pp. 11–19 (1988)
3. Dolev, D., Dwork, C., Waarts, O., Yung, M.: Perfectly Secure Message Transmission. *Journal of the ACM* 40(1), 17–47 (1993)
4. Desmedt, Y., Erotokritou, S., Safavi-Naini, R.: Simple and Communication Complexity Efficient Almost Secure and Perfectly Secure Message Transmission Schemes. In: Bernstein, D.J., Lange, T. (eds.) AFRICACRYPT 2010. LNCS, vol. 6055, pp. 166–183. Springer, Heidelberg (2010)
5. Desmedt, Y., Frankle, Y., Yung, M.: Multi-receiver/Multi-sender network security: efficient authenticated multicast/feedback. In: IEEE Infocom, pp. 2045–2054 (1992)
6. Elias, P.: List Decoding for Noisy Channels. Technical Report 335, MIT Research Lab of Electronics (1957)
7. Fitzi, M., Franklin, M., Garay, J., Vardhan, S.H.: Towards Optimal and Efficient Perfectly Secure Message Transmission. In: Vadhan, S.P. (ed.) TCC 2007. LNCS, vol. 4392, pp. 311–322. Springer, Heidelberg (2007)
8. Franklin, M.K., Wright, R.N.: Secure Communication in Minimal Connectivity Models. *Journal of Cryptology* 13(1), 9–30 (2000)
9. Guruswami, V.: Linear-algebraic List Decoding of Folded Reed-Solomon Codes. CoRR abs/1106.0436 (2011)
10. Guruswami, V., Rudra, A.: Explicit Codes Achieving List Decoding Capability: Error-Correction With Optimal Redundancy. *IEEE Transactions on Information Theory* 54(1) (2008)
11. Guruswami, V., Sudan, M.: Improved Decoding of Reed-Solomon and Algebraic-Geometric Codes. In: FOCS, pp. 28–39 (1998)
12. Kurosawa, K., Suzuki, K.: Almost Secure (1-Round, n -Channel) Message Transmission Scheme. In: Desmedt, Y. (ed.) ICITS 2007. LNCS, vol. 4883, pp. 99–112. Springer, Heidelberg (2009)
13. Patra, A., Choudhary, A., Srinathan, K., Rangan, C.: Unconditionally Reliable and Secure Message Transmission in Undirected Synchronous Networks: Possibility, Feasibility and Optimality. *IJACT* 2(2), 159–197 (2010)
14. Srinathan, K.: Secure Distributed Communication. PhD Thesis, IIT Madras (2006)
15. Sudan, M.: Decoding of Reed Solomon Codes beyond the Error-Correction Bound. *J. Complexity* 13(1), 180–193 (1997)
16. Srinathan, K., Patra, A., Choudhary, A., Rangan, C.P.: Probabilistic Perfectly Reliable and Secure Message Transmission – Possibility, Feasibility and Optimality. In: Srinathan, K., Rangan, C.P., Yung, M. (eds.) INDOCRYPT 2007. LNCS, vol. 4859, pp. 101–122. Springer, Heidelberg (2007)
17. Srinathann, K., Choudhary, A., Patra, A., Rangann, C.: Efficient Single Phase Unconditionally Secure Message Transmission with Optimum Communication Complexity. In: PODC, p. 457 (2008)

18. Srinathan, K., Narayanan, A., Pandu Rangan, C.: Optimal Perfectly Secure Message Transmission. In: Franklin, M. (ed.) CRYPTO 2004. LNCS, vol. 3152, pp. 545–561. Springer, Heidelberg (2004)
19. Safavi-Naini, R., Tuhin, M.A.A., Shi, H.: Optimal Message Transmission Protocols with Flexible Parameters. In: Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security (ASIACCS 2011), pp. 453–458 (2011)
20. Safavi-Naini, R., Tuhin, M.A.A., Wang, P.: A General Construction for 1-round δ -RMT and $(0, \delta)$ -SMT. Cryptology ePrint Archive (2012)
21. Tuhin, M.A.A., Safavi-Naini, R.: Optimal One Round Almost Perfectly Secure Message Transmission (Short Paper). In: Danezis, G. (ed.) FC 2011. LNCS, vol. 7035, pp. 173–181. Springer, Heidelberg (2012)
22. Wu, J., Stinson, D.R.: Three Improved Algorithms for Multi-path Key Establishment in Sensor Networks Using Protocols for Secure Message Transmission. In: IEEE Transactions on Dependable and Secure Computing, pp. 929–937 (2011)