Nearly Optimal Robust Secret Sharing

Mahdi Cheraghchi
Department of Computing, Imperial College London, UK

***Abstract*—We prove that a known approach to improve Shamir's celebrated secret sharing scheme; i.e., adding an information-theoretic authentication tag to the secret, can make it robust for n parties against any collusion of size δn, for any constant $\delta \in (0, 1/2)$. This result holds in the so-called "non-rushing" model in which the n shares are submitted simultaneously for reconstruction. We thus finally obtain a simple, fully explicit, and robust secret sharing scheme in this model that is essentially optimal in all parameters including the share size which is $k(1+o(1))+O(\kappa)$, where k is the secret length and κ is the security parameter. Like Shamir's scheme, in this modified scheme any set of more than δn honest parties can efficiently recover the secret.**

Using algebraic geometry codes instead of Reed-Solomon codes, the share length can be decreased to a constant (only depending on δ) while the number of shares n can grow independently. In this case, when n is large enough, the scheme satisfies the "threshold" requirement in an approximate sense; i.e., any set of $\delta n(1 + \rho)$ honest parties, for arbitrarily small $\rho > 0$, can efficiently reconstruct the secret.

I. Introduction

Secret sharing, introduced by the seminal works of Shamir [1] and Blackley [2], is the following problem (in its most basic formulation): Suppose we wish to encode and distribute a secret $s \in \mathbb{F}_2^k$ among n parties in such a way that i) the n parties can reconstruct the original secret s by revealing their respective shares; and, ii) for some integer parameter $t > 0$ (called the *privacy parameter*), any group of t parties cannot infer any information about the secret from their collection of shares. Shamir proposed a beautiful scheme that provides an optimal solution to the problem. The scheme regards the secret as an element of the finite field $\mathbb{F}_Q$, for some prime power $Q \geq n$, and then samples a uniformly random univariate polynomial of degree t over $\mathbb{F}_Q$ with the constant term set to be s. The secrecy follows by observing that in this scheme, the secret is encoded, after random padding, using a Reed-Solomon code which is MDS.

Due to its coding-theoretic nature, Shamir's scheme provides at least two additional benefits. First, any group of parties is able to recover s as long as the size of the group is larger than t. This so-called "threshold property" is due to the fact that the Reed-Solomon code is an MDS code. Second, any Reed-Solomon code of rate R is able to tolerate any fraction of errors up to $(1-R)/2$ and this can be achieved by an efficient decoder (such as the Berlekamp–Massey decoding algorithm, cf. [3, Chapter 6]). As a result, a straightforward calculation shows that Shamir's secret sharing scheme is *robust*, in the sense that it can tolerate any less than $1/3$ fraction of *dishonest* parties. That is, the correct secret s can be reconstructed even if any less than $1/3$ fraction of the parties reveal their shares incorrectly. In fact, this holds true even if the malicious parties are able to arbitrarily communicate with each other and choose the incorrect shares adversarially.

The full version of this paper appears in IACR ePrint Archive, Report 2015/951, September 2015. Available at: https://eprint.iacr.org/2015/951
Email: ⟨m.cheraghchi@imperial.ac.uk⟩

A. Previous work

The robust notion of secret sharing has been studied in the literature, and some of the key results in the area are summarized in Table I. It is known that robust secret sharing is impossible when the fraction of dishonest parties is at least $1/2$ [4]. It is also impossible to always reconstruct the secret correctly (i.e., with probability 1) when the fraction of dishonest parties may be $1/3$ or larger, in which case a small probability of error $\eta > 0$ is unavoidable. Therefore, Shamir's scheme provides optimal robustness for a scheme with zero probability of error.

When an honest majority exists, Rabin and Ben-Or [5] provide a scheme based on Shamir's combined with message authentication codes. The share length $q := \log Q$ in this scheme is, ignoring small terms, $k + \Omega(n \log(1/\eta))$, where $\eta > 0$ is the probability of incorrect reconstruction. In contrast, an appealing feature of Shamir's scheme is that the shares are *compact*; namely, the bit length of each share is equal to the bit length of the secret (under the natural assumption that $n \leq 2^k$). This turns out to be optimal for schemes with perfect privacy satisfying the threshold property [6]. Another scheme, due to Cramer et al. [7] (and based on [8] and also using Shamir's scheme) improves the share length to $\max\{k, O(n + \log(1/\eta))\}$. However, the reconstruction time for this scheme is in general exponential in n (more precisely, at least $\binom{n}{t}$), and the scheme is secure only against non-rushing[1] adversaries (cf. [9]). Cevallos et al. [9] propose a scheme similar to [5] that achieves more compact shares, namely of length $k + O(\log(1/\eta) + n(\log n + \log k))$. This scheme provides efficient share and reconstruction procedures. Jhanwar and Safavi-Naini [10] consider a model in which all parties (including the adversary) have access to public, shared, randomness. They construct information-theoretically optimal secret sharing schemes in this model by re-encoding Shamir's shares using the available public randomness. This construction achieves the same share length as Shamir's while providing privacy and robustness against any collusion of size less than $n/2$.

[1] In the non-rushing model, all shares are submitted simultaneously at the reconstruction stage.

Cramer et al. [11] introduce the notion of *algebraic manipulation detection (AMD) codes*, which is a natural variant of error-detection codes in situations where the adversary's perturbations on a codeword are chosen independently of the codeword. By using this primitive as a pre-code in Shamir's secret sharing scheme (or any secret sharing scheme with linear decoder), they are able to make the scheme robust against adversarial manipulations. The key difference in their model is the notion of robustness; i.e., the requirement is that if the adversary corrupts any of the shares, the reconstruction should *detect* the adversary and fail (rather than output the correct share) with high probability. More recently, Lewko and Pastro [12] defined a variation of robust secret sharing in which the robustness requirement is against *local* adversaries. That is, the error in each share corrupted by the adversary can only depend on the particular share being corrupted. They show that even in this restricted model, the minimum required share length is $k + \log(1/\eta) - O(1)$ (under the standard threshold assumption that any set of $t+1$ must reconstruct the secret with probability at least $1-\eta$). Furthermore, they construct efficient schemes in the local model that attains a nearly optimal share length of $k + O(\log(1/\eta))$.

In another recent work, Cramer et al. [13] combine AMD codes with universal hash functions and (folded) list decodable codes to construct a secret sharing scheme with potentially constant share length (more precisely, share length $\Theta(1 + \log(1/\eta)/n)$). Their construction is with respect to a randomly chosen hash function from a universal family and is thus a Monte-Carlo construction. That is, the code construction relies on the probabilistic method (and thus may not result in the desired secret sharing scheme with unfortunate choices of the randomness). However, the encoder and decoders are efficient once the randomness of the code construction is set to an appropriate choice. Moreover, this construction considers the "ramp model" in which it is not necessary to be able to reconstruct the secret from any $t + 1$ of the shares. This relaxation is in fact necessary for any secret sharing scheme with share length smaller than the secret length k.

Recently, Safavi-Naini and Wang [14] construct secret sharing schemes based on codes for the wiretap channel problem for the case $n = 2t + 1$. This construction is based on wiretap codes that are in turn based on list decodable Reed-Solomon codes, subspace-evasive sets and AMD codes, and attains a share length of $k + O(n^2(\log n)(\log\log n) + n\log(1/\eta))$.

B. Our contributions

In this work, we construct an essentially optimal robust secret sharing scheme against possibly adaptive[2], non-rushing adversaries. Somewhat surprisingly, our construction turns out to be strikingly similar to some of the known constructions mentioned in §I-A. More precisely, the construction first amends the secret with a tag using an AMD code. Then, it uses Shamir's scheme to encode the result into mn shares, for a carefully chosen integer parameter $m > 1$. Finally, the resulting shares are bundled into n groups of size m each which are distributed among the n parties. In other words, we use a variant of Shamir's scheme based on *folded Reed-Solomon codes* (instead of plain Reed-Solomon codes) combined with an AMD pre-code. This is very similar to what used in [11] to provide robustness in the sense of error-detection, as well as the coding-theoretic construction of Safavi-Naini and Wang [14] (the latter additionally uses subspace-evasive sets that we do not need). Combining Shamir's scheme with some type of information-theoretic pre-code (such as a message authentication code) can also be seen as the underlying idea of other existing constructions such as [7].

The techniques that we use are remarkably simple to describe as well. To prove robustness, we first use an efficient list decoding algorithm of folded Reed-Solomon codes [15] to show that the reconstruction procedure always outputs a short list containing an AMD encoding of the correct secret. Second, we use an elegant observation by Guruswami and Smith [16] that was used by them to construct "stochastic" error-correcting codes. The observation is that, for any list decodable code that is linear over some base field, the list of potential messages corresponding to the any given received word is the translation of the original message by elements of a set that only depends on the noise vector. In particular, the list of potential messages, shifted by the correct message, is only determined by the code and the error vector chosen by the adversary. For our application in secret sharing, privacy of Shamir's scheme implies that the perturbations of the adversary, and thus the set of error vectors in the message domain, must be independent of the original message and the internal randomness of the AMD code. As a result, the error detection guarantee of the AMD code ensures that, with high probability, all the incorrect potential messages are correctly identified by the reconstruction procedure so that only the correct secret remains in the end.

Our construction and underlying ideas share an overlap with the above-mentioned recent result of Cramer et al. [13] in which the authors construct a Monte-Carlo secret sharing scheme with small share length in the ramp model. The

Ref.	Share length	Efficient? (restrictions)
[1]	k	Yes ($t < n/3$)
[10]	k	No
[11]	$k + O(\log(1/\eta))$	Yes (only error detection)
[12]	$k + O(\log(1/\eta))$	Yes (only local adversaries)
[8]	$k + O(n + \log(1/\eta))$	No
[9]	$k + \tilde{O}(n + \log(1/\eta))$	Yes
[5]	$k + O(n\log(1/\eta))$	Yes
[14]	$k + \tilde{O}(n^2 + n\log(1/\eta))$	Yes
[13]	$O(1)$	Yes (Monte-Carlo)
This work	$k(1 + o(1)) + O(\log(1/\eta))$	Yes (Corollary 10)
This work	$O(1)$	Yes (Corollary 13)

TABLE I
SUMMARY OF RESULTS IN ROBUST SECRET SHARING SCHEME, AND THEIR KEY FEATURES AND LIMITATIONS. THE PARAMETER t IS THE PRIVACY PARAMETER, n IS THE NUMBER OF SHARES AND η IS THE ERROR PROBABILITY OF RECONSTRUCTION.

[2]Note that adaptivity refers to the adversary's strategy in observing shares.

construction in this work also uses a list decodable code and an AMD layer, in addition to a randomly chosen linear hashing layer. In particular, the secret along with the AMD tag is randomly "un-hashed" via a randomly chosen hash function (known in advance to all parties), and then the result is encoded using a list decodable code. This results in an insignificant increase in the share length. But more importantly, the result is a Monte-Carlo construction; i.e., the choice of the hash function is not explicitly defined but rather it is shown that "most" choices of the hash function are satisfactory. This result also focuses on shares of constant length which necessarily results in a ramp scheme. Our construction completely eliminates the hashing stage and also can be instantiated for a wide range of the parameters, including those obtained in [13]. Thus we obtain a fully explicit, and technically simple, construction of efficient secret sharing schemes with nearly optimal parameters in all aspects. Our main result is as follows:

Theorem 1: (Corollary 10, rephrased) Let $\delta < 1/2$ be any fixed constant. For any $\eta > 0$, there is an efficient, robust and perfectly private secret sharing scheme with n shares, secret length k, and share length $q \leq k(1 + o(1)) + O(\log(1/\eta))$ that is secure with privacy parameter $t = \delta n$, attaining a reconstruction error of at most η. ∎

Same as Shamir's scheme and [14], our result does not necessarily require the observations of the adversary to coincide or overlap with the set of manipulated shares. In fact, the number of adaptive observations by the adversary may in general be different from the number of incorrect shares.

Although a share length of at least k bits is necessary for any robust secret sharing scheme [6] (even against local, or oblivious, adversaries [12]), it is possible to obtain smaller shares at cost of slightly relaxing the threshold property. That is, instead of requiring the secret to be reconstructible (either with probability 1 or close to 1) from any set of more than t shares, we may require reconstructability from any set of more than $t + g$ shares, for a small "gap" parameter g. We adapt our secret sharing scheme to nonzero gap parameters and, moreover, show that when g is a small fraction of n, the alphabet size may be reduced to an absolute constant. This is achieved by using folded algebraic geometry codes instead of Reed-Solomon codes, and as a result, we prove the following:

Theorem 2: (Corollary 13, rephrased) For any constant $\rho > 0$, and any $\delta \leq 1/2 - \rho$, there is a constant $q = O_\rho(1)$ such that the following holds. There is a robust and perfectly private secret sharing scheme with n shares, secret length k, and share length $O(q)$, attaining a reconstruction error of $\eta = \exp(-\Omega(\rho n q))$, provided that $n \geq k/(\rho q)$. The scheme satisfies the threshold property in an approximate sense; namely, that the secret can be reconstructed (with probability 1) given any set of $t + \rho n$ shares. The scheme is efficient given polynomial (in n) amount of pre-processed information about the scheme. ∎

Previously, the best known construction achieving small share length was due to Cramer et al. [13] in which the share length is $\Theta(1+\log(1/\eta)/n)$ and thus grows with the security parameter (see Table I). Moreover, as mentioned above, this construction is not fully explicit and requires a randomly chosen hash function that is fixed once and for all and there is no clear efficient way of explicitly finding an appropriate hash function.

The efficiency of our scheme is dictated by the efficiency of the underlying list decoding algorithm for algebraic geometry codes. Naturally, any subsequent improvements in list decoding algorithms of folded algebraic geometry (and for that matter, folded Reed-Solomon) codes would automatically improve the performance of the above secret sharing schemes (information theoretically, one may hope to achieve $n = 2t + O(1)$ for threshold schemes using better codes). We remark that the natural idea of reducing share length by using algebraic geometry codes rather than Reed-Solomon codes in secret sharing schemes dates back to a result of Chen and Cramer [17] and has been extensively studied since (cf. [18]), especially in the context of arithmetic secure multiparty computation.

Remark 3: After the original draft of this work appeared online, Bishop et al. [19][3] used different (and quite involved) techniques to construct an efficient robust secret sharing scheme with close-to-optimal share length of $k + O(\log(1/\eta)(\log^4 n + \log^3 n \log k))$ for the case $n = 2t+1$ and where the set of t observed and corrupted shares are the same. It can be argued that our work is conceptually simpler, proving that a natural modification of Shamir's *original* scheme that had been proposed as early as 2008 [11] in fact achieves essentially optimal parameters. Thus a particular significance of our work is in showing that *existing* secret sharing systems that rely on Shamir's original scheme can be improved to nearly optimal ones with little change in the implementation (i.e., by simply tagging the original data with an optimal AMD code).

II. Robust secret sharing schemes and AMD codes

In this section, we describe the basic notions that are used in the paper, including the exact definition of robust secret sharing schemes that we use. More formal definitions appear in the full version of this work. The general notion of coding schemes is defined as follows.

Definition 4 (coding scheme): A pair of functions $(\mathsf{Enc}, \mathsf{Dec})$ where $\mathsf{Enc}\colon \mathbb{F}_2^k \times \mathbb{F}_2^\ell \to \mathbb{F}_{2^q}^n$, and $\mathsf{Dec}\colon (\mathbb{F}_{2^q} \cup \{\perp\})^n \to \mathbb{F}_2^k \cup \{\perp\}$ is called a coding scheme if for all $s \in \mathbb{F}_2^k$ and all $z \in \mathbb{F}_2^\ell$, we have $\mathsf{Dec}(\mathsf{Enc}(s, z)) = s$. The function Enc and Dec are respectively called the *encoder* and the *decoder*, and parameters k and q are respectively called the *message length* and the *symbol length*. We use the notation $\mathsf{Enc}(s)$ to denote the random variable $\mathsf{Enc}(s, Z)$ when Z is sampled uniformly at random from $\mathbb{F}_2^\ell$. The coding scheme is called *efficient* if $\mathsf{Enc}, \mathsf{Dec}$ can be computed in polynomial time in nq. The *rate* of the coding scheme is the quantity $k/(nq)$. ∎

Definition 5 (robust secret sharing scheme): A robust secret sharing scheme with secret length k, share length q, and number of shares n is a coding scheme $(\mathsf{Share}, \mathsf{Rec})$ with message

[3]This work also claims a flaw in the security proof of [10].

length k, symbol length q and block length n satisfying the following:

1) **Adaptive privacy:** For a parameter t (known as the *privacy parameter*), and for any "secret" $s \in \mathbb{F}_2^k$, an adversary who (possibly adaptively) observes any up to t of the shares gains no information about the secret s.
2) **Robustness:** For a parameter d (known as the *robustness parameter*), an adversary who arbitrarily corrupts up to any d of the shares (possibly after adaptively observing any t of the shares) cannot make Rec output an incorrect secret with probability more than η, where η is called the *robustness error* parameter. The scheme satisfies *perfect robustness* if $\eta = 0$.

The quantity $\log(1/\max\{\eta, \epsilon\})$ is called the *security parameter* of the scheme. We say the scheme satisfies the *threshold property* with gap g if the secret can be reconstructed from any set of $t + g + 1$ shares. If $g = 0$, we say that the scheme satisfies a *sharp threshold*. Otherwise, the scheme is called a *ramp scheme*. ■

Definition 6 (AMD (algebraic manipulation detection) code): [11] A binary coding scheme $(\mathsf{Enc}, \mathsf{Dec})$ with message length k and block length n is an *AMD code* with error η if for every message $s \in \mathbb{F}_2^k$ and every $\Delta \in \mathbb{F}_2^n$, we have $\Pr(\mathsf{Dec}(\mathsf{Enc}(s) + \Delta) \notin \{s, \perp\}) \leq \eta$, where the probability is taken over the internal randomness of Enc. ■

Theorem 7: [11] For every k and parameter $\eta > 0$, there is an efficient AMD code with message length k and encoder of the form $\mathsf{Enc}(s, z) = (s, z, f(s, z))$ for some $f : \mathbb{F}_2^k \times \mathbb{F}_2^q \to \mathbb{F}_2^q$ such that $q = O(\log(1/\eta))$.

III. The construction

The following is the main technical tool used by our constructions, in which we prove that a combination of AMD codes with linear list decodable codes can be used to construct robust secret sharing schemes.

Theorem 8: There is a constant $c_0 > 0$ such that the following holds for any integer $k > 0$ and parameter $\eta > 0$. For some $Q = 2^q$ and $m \mid q$, let $\mathcal{C} \subseteq \mathbb{F}_Q^n$ be an explicit $\mathbb{F}_{Q^{1/m}}$-linear code with rate R that is efficiently list decodable from any δ fraction of errors with list size bounded by L and has minimum distance $d > \delta n$. Moreover, suppose $\mathcal{C}$ has a subcode $\mathcal{C}' \subseteq \mathbb{F}_Q^n$ that, over $\mathbb{F}_{Q^{1/m}}$, is linear with dual distance at least $tm + 1$ and rate $R' \leq R - 1/n$ satisfying

$$(R - R')nq \geq k + c_0 \log(L/\eta). \tag{1}$$

Then, there is an efficient and perfectly private robust secret sharing scheme $(\mathsf{Share}, \mathsf{Rec})$ with secret length k and n shares, share length q, privacy parameter t, robustness δn, and robustness error η. Moreover, the scheme satisfies the threshold property with gap $g = n - t - d$.

Proof: Let $\eta' := \eta/L$. We first instantiate the AMD code of Theorem 7 for message length k and block length $n_0 = k + O(\log(1/\eta')) \leq k + c_0(\log(L/\eta))$, for some constant $c_0 > 0$. Let $(\mathsf{Enc}_0, \mathsf{Dec}_0)$ be the resulting AMD coding scheme.

We can write the code $\mathcal{C}$ as a direct sum $\mathcal{C} = \mathcal{C}' + \mathcal{C}''$ of complementary codes, where $\mathcal{C}'' \subseteq \mathbb{F}_Q^n$ is an $\mathbb{F}_{Q^{1/m}}$-linear sub-code of $\mathcal{C}$ of rate $R - R' > 0$. For the sake of clarity, in the sequel we use $\mathcal{C}_0, \mathcal{C}_0' \subseteq (\mathbb{F}_{Q^{1/m}})^{nm}$ to be the codes $\mathcal{C}, \mathcal{C}'$, respectively, when regarded as subspaces of $(\mathbb{F}_{Q^{1/m}})^{nm}$ (in other words, $\mathcal{C}_0, \mathcal{C}_0'$ are the "unfolded" representations of $\mathcal{C}, \mathcal{C}'$). Recall that $\mathcal{C}_0, \mathcal{C}_0'$ are linear codes over $\mathbb{F}_{Q^{1/m}}$.

Let $f : \mathbb{F}_2^{n_0} \to \mathcal{C}''$ be any efficient and $\mathbb{F}_2$-linear invertible function. Such a function exists since $\log_2 |\mathcal{C}''| = (R - R')nq \geq n_0$ by (1). Note that there is also an efficiently computable $\mathbb{F}_2$-linear projection $f' : \mathbb{F}_Q^n \to \mathbb{F}_2^{n_0}$ such that for any $w \in \mathcal{C}'$, and any $x \in \mathbb{F}_2^{n_0}$, we have $f'(w + f(x)) = x$. We define the secret sharing scheme $(\mathsf{Share}, \mathsf{Rec})$ as follows:

- Share: Given $s \in \mathbb{F}_2^k$, $\mathsf{Share}(s)$ first computes $S' := \mathsf{Enc}_0(s)$. Then, it samples a $Z \in \mathbb{F}_Q^n$ according to the uniform distribution on $\mathcal{C}'$ and outputs $Y := f(S') + Z$.
- Rec: Given $Y' \in \mathbb{F}_Q^n$, the procedure $\mathsf{Rec}(Y')$ first uses the list decoding algorithm of $\mathcal{C}$ to compute a list $M \subseteq \mathbb{F}_Q^n$ of size at most L consisting of all codewords of $\mathcal{C}$ that agree with Y' in at least $1-\delta$ fraction of the positions. Let $M' \subseteq \mathbb{F}_2^{n_0}$ be the set $M' := f'(M)$. If the set $\mathsf{Dec}_0(M') \setminus \{\perp\}$ contains only one element, the algorithm outputs the unique element. Otherwise, the algorithm returns $\perp$.

Due to space restrictions, we defer the formal analysis of our scheme to the full version of the paper. Intuitively, privacy holds in a similar way as the original Shamir's scheme, due to the dual distance property of the subcode of $\mathcal{C}$. The main novelty is the robustness analysis, which, as briefly sketched in §I-B, works in two steps. First, due to list decodability of $\mathcal{C}$, it is always possible to reconstruct a short list that must contain the correct secret, along with the correct AMD tag. The linearity property of $\mathcal{C}$ can be used in combination with the properties of AMD codes to show that, with sufficient probability, the correct secret is the only element of the list that is tagged correctly. ■

IV. Instantiations

A. Construction based on Reed-Solomon codes

In this section, we instantiate Theorem 8 using folded Reed-Solomon codes of [15]. The result is the following theorem whose proof appears in the full version of the work.

Theorem 9: For every integers $n > t \geq 1$, $g \geq 0$ and real parameters $\delta, \nu, \eta > 0$ such that $\rho := 1 - \delta - \frac{t+g+1}{n} > 0$, there is a $q_0 = O(\frac{\log^2(1/\rho)}{\nu\rho^2} \log n)$ such that for any integer $q \geq q_0$ the following holds. There is an efficient and perfectly private secret sharing scheme $(\mathsf{Share}, \mathsf{Rec})$ with n shares, share length q, privacy parameter t, threshold property with gap g, and secret length k satisfying $k \geq (1+g-\nu)q - O(\log(1/\eta))$. Moreover, the scheme achieves a robustness parameter of δn and robustness error η. ■

We remark that for any (not necessarily robust) secret sharing scheme with threshold property and gap g, it is known that the share length q must satisfy $q \geq k/(1 + g)$ (cf. [13]). Therefore, the share length achieved by Theorem 9 is essentially optimal. For the important special case of $\delta = t/n$ and $g = 0$ we derive the following corollary from Theorem 9:

Corollary 10: Let $\delta < 1/2$ be any fixed constant. For every integer $n > 1/(1-2\delta)$ and $\eta > 0$ and $\nu > 0$, there is an efficient and perfectly private secret sharing scheme $(\mathsf{Share}, \mathsf{Rec})$ with n shares, share length $q = O_\nu(\log n)$, and secret length $k \geq q(1-\nu) - O(\log(1/\eta))$. It attains a sharp threshold, privacy and robustness δn, and error η. ∎

B. Reducing the share length using algebraic geometry codes

Using algebraic geometry codes instead of Reed-Solomon codes in Theorem 8, it is possible to reduce the share length to a constant at cost of (necessarily) introducing a nonzero gap. Namely, by instantiating Theorem 8 with a family of folded algebraic geometry (AG) codes in [20], the following result is obtained (see the full version for the proof):

Theorem 11: There is a constant $c_0 > 0$ such that the following holds. For any constants $\rho, \delta > 0$, there is an integer $q = \Theta(\log(1/\rho)/\rho^2)$ and $n_0 = (1/\rho)^{O(1)}$ such that for all integers t, k and $n \geq n_0$ and real parameter $\eta > 0$ that satisfy

$$\frac{k}{qn} + \frac{t}{n} + \delta \leq 1 - \rho - c_0 \frac{\log(1/\eta)}{nq} \tag{2}$$

the following holds. There is an efficient and perfectly private secret sharing scheme $(\mathsf{Share}, \mathsf{Rec})$ with n shares, share length q, privacy parameter t and secret length k. Moreover, the scheme achieves a robustness parameter of δn and error η, and satisfies the threshold property with gap at most $n(1 - \frac{t}{n} - \delta)$. ∎

From this result, we obtain the following corollary (see the full version for the proof).

Corollary 12: For any constants $\delta, \gamma, \rho > 0$, there is a $q_0 = O(\log(1/\rho)/\rho^2)$ and $n_0 = O(1/\rho)$ such that for all integers $c \geq 1$, the following holds. Let $q := cq_0$. For any integers $k > 0$, $n \geq n_0$, and parameter $\eta > 0$ such that

$$\frac{k}{qn} + \gamma + \delta \leq 1 - \rho, \tag{3}$$

There is a perfectly private secret sharing scheme $(\mathsf{Share}, \mathsf{Rec})$ with n shares, secret length k, share length q, privacy parameter at least γn, and threshold property with gap at most $n(1 - \delta - \gamma)$. Moreover, the scheme achieves a robustness parameter of δn and error $\eta = \exp(-\Omega(\rho n q))$. ∎

Corollary 12, in turn, immediately implies the following result on robust secret sharing with privacy and robustness parameter δn for any $\delta < 1/2$.

Corollary 13: For any constant $\rho > 0$, and any $\delta \leq 1/2 - \rho$, There is a $q_0 = O(\log(1/\rho)/\rho^2)$ such that for any $q \geq q_0$ and integers $k > 0$ and $n \geq k/(\rho q)$, the following holds. There is a perfectly private secret sharing scheme $(\mathsf{Share}, \mathsf{Rec})$ with n shares, secret length k, and share length at most $2q$. The scheme attains privacy and robustness parameters equal to δn and error $\eta = \exp(-\Omega(\rho n q))$, and satisfies the threshold property with gap at most $2\rho n$. ∎

Compared with the result of Corollary 10 obtained from Reed-Solomon codes, we see that the share length q can be chosen to be a constant (depending on the difference $1/2 - \delta$), and at the same time the number of shares can be made arbitrarily large as well. However, for this to be possible when the designed share length is small, the number of shares n needs to be large enough[4] so that $n \geq k/(\rho q)$. In the full version of this paper we show that this is necessary for any robust secret sharing scheme with share length q that attains privacy and robustness parameters close to $n/2$. The proof constructs a reduction from the *wiretap channel problem* to robust secret sharing and applies the known information theoretic bounds on wiretap codes. It follows that for a general share length q, a robust secret sharing scheme satisfying (3) for arbitrarily small $\rho > 0$ is essentially optimal (even if the threshold property is not a concern).

REFERENCES

[1] A. Shamir, "How to share a secret," *Communications of the ACM*, vol. 22, no. 11, pp. 612–613, 1979.

[2] G. Blakley, "Safeguarding cryptographic keys," in *National Computer Conference*. Springer, 1979, vol. 48, pp. 313–317.

[3] R. Roth, *Introduction to Coding Theory*. Cambridge University Press, 2006.

[4] Y. Ishai, R. Ostrovsky, and H. Seyalioglu, "Identifying cheaters without an honest majority," in *TCC*, 2012, pp. 21–38.

[5] T. Rabin and M. Ben-Or, "Verifiable secret sharing and multiparty protocols with honest majority," in *Proc. of STOC*, 1989, pp. 73–85.

[6] D. Stinson, "An explication of secret sharing schemes," *Designs, Codes and Cryptography*, vol. 2, no. 4, pp. 357–390, 1992.

[7] R. Cramer, I. Damgård, and S. Fehr, "On the cost of reconstructing a secret, or VSS with optimal reconstruction phase," in *CRYPTO*. Springer, 2001, pp. 503–523.

[8] S. Cabello, C. Padró, and G. Sáez, "Secret sharing schemes with detection of cheaters for a general access structure," in *FCT*, 1999, pp. 185–194.

[9] A. Cevallos, S. Fehr, R. Ostrovsky, and Y. Rabani, "Unconditionally-secure robust secret sharing with compact shares," in *EUROCRYPT*, 2012, pp. 195–208.

[10] M. Jhanwar and R. Safavi-Naini, "Unconditionally-secure robust secret sharing with minimum share size," in *Financial Cryptography and Data Security*, 2013, pp. 96–110.

[11] R. Cramer, Y. Dodis, S. Fehr, C. Padró, and D. Wichs, "Detection of algebraic manipulation with applications to robust secret sharing and fuzzy extractors," in *EUROCRYPT*, 2008, pp. 471–488.

[12] A. Bishop Lewko and V. Pastro, "Robust secret sharing schemes against local adversaries," IACR ePrint 2014/909, 2014.

[13] R. Cramer, I. Damgård, N. Döttling, S. Fehr, and G. Spini, "Linear secret sharing schemes from error correcting codes and universal hash functions," in *EUROCRYPT*, 2015, pp. 313–336.

[14] R. Safavi-Naini and P. Wang, "A model for adversarial wiretap channels and its applications," *J. Inf. Processing*, vol. 23, pp. 554–561, 2015.

[15] V. Guruswami and A. Rudra, "Explicit codes achieving list decoding capacity: Error-correction with optimal redundancy," *IEEE Transactions on Information Theory*, vol. 54, no. 1, pp. 135–150, 2008.

[16] V. Guruswami and A. Smith, "Codes for computationally simple channels: Explicit constructions with optimal rate," in *Proc. of FOCS*, 2010, pp. 723–732.

[17] H. Chen and R. Cramer, "Algebraic geometric secret sharing schemes and secure multi-party computations over small fields," in *CRYPTO*, 2006, pp. 521–536.

[18] R. Cramer, I. Damgård, and J. Nielsen, *Secure Multiparty Computation and Secret Sharing*. Cambridge University Press, 2015.

[19] A. Bishop, V. Pastro, R. Rajaraman, and D. Wichs, "Essentially optimal robust secret sharing with maximal corruptions," *IACR ePrint Archive*, vol. 2015, p. 1032, 2015.

[20] V. Guruswami and C. Xing, "Optimal rate list decoding of folded algebraic-geometric codes over constant-sized alphabets," in *Proc. of SODA*, 2014, pp. 1858–1866.

[4] Note such a requirement is not a barrier for constructions such as Shamir's scheme and the result of Theorem 9, since we have $q \geq k$ in those schemes.