Asymptotically-Good Arithmetic Secret Sharing over $\mathbb{Z}/p^{\ell}\mathbb{Z}$ with Strong Multiplication and Its Applications to Efficient MPC

Ronald Cramer, Matthieu Rambaud, and Chaoping Xing

[1] CWI Amsterdam & Leiden University
[2] LTCI Telecom Paris, Institut Polytechnique de Paris
[3] Nanyang Technological University, Singapore

Abstract. This paper deals with (1) asymptotics of "strongly-multiplicative" arithmetic secret sharing over an arbitrary fixed ring $R_\ell := \mathbb{Z}/p^\ell\mathbb{Z}$ ($p > 0$ prime, $\ell > 0$ an integer) and supporting an unbounded number of players n, and with (2) its applications to communication complexity of arithmetic MPC over this ring.

For each integer $r > 0$, let $R_\ell(r)$ be the degree-r Galois-ring extension of R_ℓ, with maximal ideal p, residue field $(R_\ell(r))/p = \mathbb{F}_{p^r}$, and $|R_\ell(r)| = p^{\ell r}$.

Using the theory of AG-codes over finite fields and over rings, combined with nontrivial algebraic-geometric lifting techniques, we show that, for arbitrary fixed ring $R_\ell = \mathbb{Z}/p^\ell\mathbb{Z}$, there is a fixed integer $\hat{r} = \hat{r}(p) > 0$ and a (dense) family of $R_\ell(\hat{r})$-linear codes C of unbounded length such that:

- Denoting the reduction of C modulo p (an $\mathbb{F}_{p^{\hat{r}}}$-linear code) by $\overline{C}$, each of $\overline{C}$, $(\overline{C})^\perp$ (dual), $(\overline{C})^{*2}$ ("square under Schur-product") is asymptotically good.
- Each of C, $C^\perp$, C^{*2} is free over $R_\ell(\hat{r})$, with the same dimension as its reduction. Therefore, each has the same minimum distance as its reduction. Particularly, each is asymptotically good.
- All constructions are efficient.

This implies arithmetic secret sharing over the fixed ring $\mathbb{Z}/p^\ell\mathbb{Z}$ (rather, the constant-degree extension) with unbounded (dense) n, secret-space dimension $\Omega(n)$, share-space dimension $O(1)$, t-privacy $\Omega(n)$ with t-wise share-uniformity and $1/3 - t/n > 0$ a constant arbitrarily close to 0, and, *last-but-not-least*, "multiplicativity-locality" $n - t$. This extends Chen-Cramer (CRYPTO 2006), which only works over any (large enough) finite fields, significantly. Concrete parameters we show here are at least as large.

We also show a similar lifting result for asymptotically-good reverse multiplication-friendly embeddings (RFME) and we show how to get an asymptotically-good alternative for the functionality of "hyper-invertible matrices" (essential for efficient active-security MPC), as the latter are inherently asymptotically-bad.

Finally, we give two applications to general arithmetic MPC over $\mathbb{Z}/p^\ell\mathbb{Z}$ (in the BGW-model with active, perfect security) with communication complexity significantly better than the obvious approach based on combining MPC over $\mathbb{F}_p$ with added circuitry for emulation of the basic $\mathbb{Z}/p^\ell\mathbb{Z}$-operations over $\mathbb{F}_p$. Concretely, recent results by Cascudo-Cramer-Xing-Yuan on amortized complexity of MPC (CRYPTO 2018) are now achievable over these rings instead of finite fields, with the same asymptotic complexity and adversary rates.

1 Introduction

1.1 Statement of the problem and main results in multiparty computation

This paper deals with (1) asymptotics of "strongly-multiplicative" arithmetic secret sharing over an arbitrary fixed ring $R_\ell := \mathbb{Z}/p^\ell\mathbb{Z}$ ($p > 0$ prime, $\ell > 0$ an integer) and supporting an unbounded number of players n, and with (2) its applications to communication complexity of arithmetic (information-theoretic) MPC over this ring.

In arithmetic MPC defined over $\mathbb{Z}/p^\ell\mathbb{Z}$, the circuit that is to be evaluated is defined over this ring and protocols are provided for (ongoing) secure addition and secure multiplication over the ring. From a practical perspective, this model is motivated by the fact that secure computations involving e.g. many comparisons or bit-wise operations, such as secure benchmarking based on linear programming, are naturally expressed in terms of ring operations (with $p = 2$ being the most interesting case).

Arithmetic MPC typically being defined over finite field, an obvious approach to arithmetic MPC over $\mathbb{Z}/p^\ell\mathbb{Z}$ is to consider any standard arithmetic MPC over finite fields and to emulate securely the ring operations in terms of the finite field operations but this incurs substantial overhead. In a recent line of work on efficient MPC over $\mathbb{Z}/p^\ell\mathbb{Z}$ with n large and p small (which is especially relevant in the practically interesting case $p = 2$), significant advances have been made in order to avoid the overhead incurred by this emulation, by redesigning basic arithmetic MPC so as to work "more directly"over the ring in question. The first published paper [Cra+18] in this line introduces the SPD$\mathbb{Z}_{2^k}$ protocol, a full redesign of the well-known SPDZ-protocol [Dam+12], the benchmark for the case of cryptographic security with dishonest majority in Beaver's preprocessing model, that works directly over the rings in question and that is essentially as efficient as the most efficient SPDZ-incarnation. For more discussion about practical advantages, see [Cra+18] and its follow-up implementation paper [Dam+19], which also reports on applications to machine-learning that significantly outperform approaches from field-based MPC.

Now, in a series of companion papers (besides the present one, this includes [Anoa; Anob]), the various cases of secret-sharing-based, information-theoretic arithmetic MPC are studied in this light. Whereas in the case of [Cra+18] the nontrivial hurdles to be overcome relate to homomorphic MAC's over the rings in question instead of finite fields and several tricky technical issues concerning the preprocessing phase, the nontrivial challenges arising here concern the fact that, when p is small compared to n, it is not straightforward to design arithmetic secret sharing over the rings in question and the fact that efficient amortization techniques for MPC based on so-called hyper-invertible matrices, widely used in the case of active security, appear troublesome in the case of the rings in question —even more in the asymptotic regime, for which hyper-invertible matrices are inherently bad.

Let us start with the main issues surrounding arithmetic secret sharing. An arithmetic secret sharing scheme over a finite field K is typically a K-linear scheme where each share-space has dimension 1 over K and where the secret-space may have dimension 1 or greater. Furthermore, "coordinate-wise" (or Schur-) multiplication of two vectors in a space is considered. Whereas t-privacy is defined in the usual way, reconstruction is defined with respect to this multiplication. I.e., the scheme is said to be multiplicative if there is a K-linear map that, when applied to the coordinate-wise product of two arbitrary and full share-vectors, yields the coordinate-wise product of the two underlying secrets. The scheme is said to be strongly-multiplicative if, in addition to the t-privacy, the latter multiplicative condition holds even if an arbitrary selection of t players is removed from consideration (the linear map may depend on the selection). As for MPC, the multiplicative notion is typically relevant to the passive security case and to the active security case with statistical security (i.e., small error), whereas the strongly-multiplicative notion typically pertains to the case of perfect, active security (i.e., no error).

Whereas the multiplicative notion in combination with secret-space of dimension 1 has strong connections with the classical theory of self-dual (self-orthogonal) codes (and thus has many solutions in various parameter regimes), the strongly-multiplicative notion is more intricate and restrictive. In a non-asymptotic setting, efficient solutions can be based on polynomial evaluation codes such as Reed-Solomon (i.e., Shamir's scheme with $t < n/3$ and its variations) or related. The asymptotic case, where the field is fixed, n is unbounded and strong-multiplication must hold with t in $\Omega(n)$ (optionally, the dimension of the secret-space is $\Omega(n)$ as well), has achieved some level of notoriety: only solutions making heavy use of algebraic-geometry are known, starting with [CC06]. In fact, the basis of such solutions is formed by algebraic-geometric constructions of codes C such that each of C, $C^{\perp}$ (its dual) and C^2 (its square [4]) are asymptotically good, i.e., each dimension and minimum distance is linear in the length. Note that the scheme from [CC06] has been shown to have numerous applications in theoretical (two-party) cryptography, on account of the so-called MPC-in-the-Head paradigm introduced by [Ish+07]. For a full account of results, history and applications, please refer to [CDN15].

Now consider our ring case. For instance, for small p (say, the interesting case $p = 2$) and for large number of players n, the standard polynomial interpolation techniques underlying Shamir's scheme over finite fields fail. [5] In [Cra+03], it has been shown how one can, in principle, work around this problem with the aid of blackbox secret-sharing schemes defined over algebraic number fields. In [Anoa], which adresses the non-asymptotic regime, a much more direct approach based

[4] the linear code (with the same length as C) generated by all vectors y such that y is the coordinate-wise product of some vectors x, x' in C.

[5] It should be noted that, for very small n only, known combinatorial methods for (arithmetic) secret sharing are essentially insensitive to any choice of ring or field, but complexity grows exponentially in n and so this approach does not scale well. See, e.g., Sharemind [BLW08].

on Galois-rings is given that leads to (strongly-)multiplicative arithmetic secret sharing schemes over these rings supporting much more efficient (information-theoretic) arithmetic MPC over $\mathbb{Z}/p^\ell\mathbb{Z}$ compared to [Cra+03] (honest-majority with statistical security or $t < n/3$ corruption with perfect security).

Galois-rings are defined as follows. Let p be a positive prime number, let ℓ be a positive integer and let r be a positive integer and let $f(X) \in \mathbb{Z}/p^\ell\mathbb{Z}[X]$ be a monic polynomial of degree r such that its reduction modulo p is an irreducible polynomial in $\mathbb{F}_p[X]$. Then the degree-r Galois-ring extension of $\mathbb{Z}/p^\ell\mathbb{Z}$ is the ring $\left(\mathbb{Z}/p^\ell\mathbb{Z}[X]\right)/(f(X))$. [6] It is an extension ring of $\mathbb{Z}/p^\ell\mathbb{Z}$, free as a module over $\mathbb{Z}/p^\ell\mathbb{Z}$, with polynomial basis $1, \overline{X}, \ldots, \overline{X}^{r-1}$. In particular, this means that $\mathbb{Z}/p^\ell\mathbb{Z}$ is embedded in this extension ring in a natural, easy way, i.e., "in the first coordinate", so to speak. (This is important in the MPC applications). Moreover, it is local, i.e., it has a unique maximal ideal (p). The residue-field (i.e., the field obtained by modding out this extension ring by the maximal ideal) is precisely the finite field $\mathbb{F}_{p^r}$. [7]

As shown in [Anoa], this enables the construction of (strongly-)multiplicative arithmetic secret-sharing schemes defined over Galois-rings from polynomial interpolation over rings (in the non-asymptotic regime), and, after overcoming several technical hurdles in the corresponding protocols that are also caused by the fact that they should operate over a ring instead of a field (e.g., hyper-invertible matrices —which are inherently bad for the asymptotic regime— are shown to exist here, as well as error-correction), this leads to efficient arithmetic MPC over $\mathbb{Z}/p^\ell\mathbb{Z}$ as discussed above.

In [Anob], the question is raised as to what extent linear secret sharing over a finite field can be "lifted" by *elementary means* to linear secret sharing with similar parameters but defined e.g. over a Galois-ring whose residue field is the given finite field (in fact, a more general class of rings is considered but we do not detail this here). The answer is as follows. Define a good lift (of a code) as a code over the Galois-ring that is free and that, when reduced modulo the maximal ideal, collapses to the given code "below." . Then, such a good lift inherits dimension and (at least) the minimum distance from the code below, Moreover, "a good lift commutes with taking the dual": the dual of a good lift of a code is a good lift of the dual "below". Thus, dual dimension and (at least) dual distance are *also* inherited by a good lift.

Besides, dual distance of a good lift has the essential property, as in the case over fields, that projection on any coordinates whose number m equals the dual distance minus 1 is the m-fold cartesian product over the ring in question. (This enables control over secret-space dimension and privacy when used for secret sharing; basically, it works if the sum of these two parameters equals m.) Finally, a good lift can be obtained by taking a basis below, lifting it arbitrarily,

[6] Thus, it is a "truncation" of the Witt-ring, which is the direct limit taken over the Galois-rings.

[7] Note that, with r fixed, choosing different polynomials (subject to the same conditions as above) leads to rings that are isomorphic. So there is essentially one degree-r Galois-ring extension of $\mathbb{Z}/p^\ell\mathbb{Z}$.

and by letting the result generate a code over the ring. Moreover, there is a more refined but still elementary lifting technique for self-dual (self-orthogonal) codes (assuming the characteristic is greater than 2).

This essentially settles the case of asymptotically-good arithmetic secret sharing over Galois-rings *with multiplication*, by using ideas from [CDM00] in combination with classical results on codes and their duals. However, we show here in §2.3 that this does *not* work in general for strong-multiplication: a class of counter-examples is given where a good lift does not commute with taking the square. Therefore, not much can be said about the minimum distance or dimension of the square of the lift.

It is in this present paper that we settle the asymptotic, strong-multiplication case by devising a nontrivial algebraic-geometric "good lift" that, for a rather general class of AG-codes over a finite field is lifted to an AG-code over the desired ring such that the square of this dedicated lift is a good lift (in the sense above) of the square "below." Thus, we also control the minimum distance and dimension of the square of this dedicated lift, as opposed to the case of an arbitrarily chosen good lift.

By combining this with appropriate asymptotically-good towers of algebraic function fields over finite fields, we get the following result.

Main Theorem 1. Fix any prime number $p > 0$ and any integer $\ell > 0$. Write $R_\ell = \mathbb{Z}/p^\ell\mathbb{Z}$. For each integer $r > 0$, denote the degree-r Galois-ring extension of R_ℓ by $R_\ell(r)$. Then there is a fixed integer $\hat{r} = \hat{r}(p) > 0$ and a (dense) family of $R_\ell(\hat{r})$-linear codes C of unbounded length such that:

1. Denoting reduction of C modulo p (an $\mathbb{F}_{p^r}$-linear code) by $\overline{C}$, each of $\overline{C}$, $(\overline{C})^\perp$, $(\overline{C})^2$ is asymptotically good.
2. Each of C, $C^\perp$, C^2 is free over $R_\ell(\hat{r})$, with the same dimension as its reduction. Therefore, each has the same minimum distance as its reduction. Particularly, each is asymptotically good.
3. All constructions are efficient.

Corollary 2. *This implies arithmetic secret sharing over the fixed ring $\mathbb{Z}/p^\ell\mathbb{Z}$ (rather, the constant-degree extension) with unbounded (dense) n, secret-space dimension $\Omega(n)$, share-space dimension $O(1)$, t-privacy $\Omega(n)$ with t-wise share-uniformity and $1/3 - t/n > 0$ a constant arbitrarily close to 0, and,* last-but-not-least, *"multiplicativity-locality" $n - t$. Moreover, the scheme obtained by reduction modulo p may be assumed to be asymptotically good as well.* [8]

Moreover, being a good lift guarantees that we have linear reconstruction, so multiplicative locality is *efficient* here.

Let us overview the proof of Main Theorem 1. From standard lifting techniques in algebraic geometry —known since Grothendieck's 1959 "GFGA"— we

[8] This fact is quite useful in some practical protocol applications but it is not strictly necessary for general arithmetic MPC

have that smooth projective curves lift over Galois rings $R_\ell(r)$, along with their points and divisors. From this data and Walker's theory [Wal99], we can deduce algebraic geometric codes $C(D)$, over $R_\ell(r)$, as (isomorphic) evaluations of Riemann Roch spaces $L(D)$ which are good lifts of the evaluation codes over fields. The key property of these good lifts is that they behave well with respect to inclusions and squares:

$$C(D)^2 \textit{ included in } C(2D)\ , \tag{1}$$

contrary to the square of an arbitrary good lift, which may "spread out" too much. Here the code $C(2D)$ is proven to be a "good lift", that is to say it is free and of same dimension as the reduced code —which is an AG code over fields. Hence by elementary theory, $C(2D)$ has same minimum distance than the reduced code, which thus nicely lower bounds the distance of $C(D)^2$. [9] We then show that inclusion (1) is actually an equality, which proves that $C(D)^2$ is itself a good lift, whence the equality of minimum distances claimed in Theorem 1 (and also uniformity of secret sharing deduced from $C(D)^2$). First, equality is shown *over fields* by a theorem of Mumford which we extend to nonnecessary algebraically closed fields. Notice that it follows from straightforward arguments in the case where $\deg D \geq 4g$. Then equality is deduced over *rings* from the elementary theory.

Finally, *computing efficiently* multiplication-friendly lifts of algebraic geometry codes can be done by elementary ways. To start with, generating such codes over finite fields has become computable in subquadratic time thanks to [NW17]. Then, we show that lifting multiplication-friendly these codes over $R_\ell(r)$ heuristically boils down to solving ℓ instances of a *linear system* over $\mathbb{F}_{p^r}$ with $\Omega(n^6)$ coefficients. We illustrate efficiency of our method by lifting a strongly multiplicative secret sharing scheme over $\mathbb{F}_{16}$ for 64 players and adversary threshold $t = 13$, into a scheme over the Galois extension of degree four of $\mathbb{Z}/2^{100}\mathbb{Z}$, in a minute on a single processor.

Remark. Note that this extends the result from [CC06], which only works over any (large enough) finite fields, significantly. Concrete parameters we show here are at least as large, given the *same* overhead $\hat{r}(p)$.

Before we discuss protocol applications, we need two more technical results.

First, we need the functionality of hyper-invertible matrices [10] over *fixed* Galois-rings, with unbounded number of players and with asymptotically-good quality of extraction (i.e., number of "correct" random sharings extracted) and

[9] We can also conclude at this point that $C(D)^2$ inherits the *linear reconstruction* property of $C(2D)$ because the latter is a good lift

[10] A fundamental technique to extract many fully random sharings out of a pool of sharings only a fraction of which are random to the adversary, while at the same time exercising control over correctness of sharings, all in one go and at low amortized cost per random sharing produced; a key-ingredient in many efficient, secret-sharing-based, information-theoretic MPC protocols with active security.

similar privacy. In [Cas+18] (see Section 2.4) it is explained how to design alternatives for hyper-invertible matrices that avoid polynomial interpolation (thus avoiding limitations posed by the theory of MDS-codes) yet enjoy the same functionality. In fact, these alternatives, arising from a twist on codes and their duals, can be based on a fixed finite field in combination with unbounded number of players, yielding asymptotically-good extraction and privacy if the right codes are selected. To get what we want here, we just use the elementary lifting-theory developped in §2 (generalized by [Anob] over any local ring) in order to lift these alternatives fixed Galois-rings, with the desired parameters.

Second, we need asymptotically-good reverse multiplication-friendly embeddings (RFME) (see [Cas+18]) over fixed Galois-rings. This is a method to embed, for unbounded (and dense) m (m a positive integer), $\Omega(m)$ copies of $\mathbb{Z}/p^{\ell}\mathbb{Z}$ into a Galois-ring extension of degree $O(m)$ such that the coordinate-wise product of two elements in $\left(\mathbb{Z}/p^{\ell}\mathbb{Z}\right)^{m}$ is recovered by applying a fixed $\mathbb{Z}/p^{\ell}\mathbb{Z}$-linear map to the product of their respective embeddings in the Galois-ring extension. (In fact, this turns out to work for all m, efficiently). This is useful in the context of some parallellization of MPC computations. The asymptotics of the finite-field case was treated in [Cas+18]. Here, we use similar algebraic-geometric lifting as in the case of arithmetic secret sharing to get the desired result.

Finally, we give two applications to general arithmetic MPC over $\mathbb{Z}/p^{\ell}\mathbb{Z}$ (in the BGW-model with active, perfect security) with communication complexity significantly better than the obvious approach based on combining MPC over $\mathbb{F}_p$ with added circuitry for emulation of the basic $\mathbb{Z}/p^{\ell}\mathbb{Z}$-operations over $\mathbb{F}_p$. Concretely, recent results [Cas+18] on amortized complexity of MPC are now achievable over these rings instead of finite fields, with the same asymptotic complexity and adversary rates.

Concretely:

Main Theorem 3. In the BGW-model, for every $\epsilon > 0$, there is an efficient MPC protocol for n parties over $\mathbb{Z}/p^{\ell}\mathbb{Z}$ secure against a submaximal number of active corruptions $t < (1-\epsilon)n/3$ with an amortized communication complexity (per instance) of $O(n)$ elements of $\mathbb{Z}/p^{\ell}\mathbb{Z}$ per gate. More precisely, the constant communication overhead $\widehat{r}(\epsilon)$ grows in $O(\log(\epsilon))$ —the same as in the fields case.

Main Theorem 4. In the BGW-model, there is an efficient MPC protocol for n parties secure against the maximal number of active corruptions $t < n/3$ that computes $\Omega(\log n)$ evaluations of a single circuit over $\mathbb{Z}/p^{\ell}\mathbb{Z}$ in parallel with an amortized communication complexity (per instance) of $O(n)$ elements of $\mathbb{Z}/p^{\ell}\mathbb{Z}$ per gate. *combining with the Franklin-Yung paradigm [FY92], we get:*

In the BGW-model, for every $\epsilon > 0$, there is an efficient MPC protocol for n parties secure against a submaximal number of active corruptions $t < (1-\epsilon)n/3$ that computes $\Omega(n \log n)$ evaluations of a single circuit over $\mathbb{Z}/p^{\ell}\mathbb{Z}$ in parallel with an amortized communication complexity (per instance) of $O(1)$ elements of $\mathbb{Z}/p^{\ell}\mathbb{Z}$ per gate.

These theorems close a communication gap between secure computation in fields, and secure computation in rings emulated from field operations. For instance consider that so far, the state of the art protocols for secure comparison of integers [Dam+06] in the ring $\mathbb{Z}/2^\ell\mathbb{Z}$ involved $\ell \log \ell$ secure multiplications in the field $\mathbb{F}_2$, which means a *non constant communication overhead* $\log \ell$. Whereas our protocols have constant overhead per gate per element of $\mathbb{Z}/2^\ell\mathbb{Z}$.

In section 2 we gather elementary results on good lifts over Galois rings, building on [Wal99, §3]. In §2.3 we illustrate that the difficulty of the problem of finding codes with *multiplication friendly lifts* cannot be solved by elementary methods. We first illustrate that solution are not guaranteed to exist, and in any case very sparse. We come back later on this argument in Remark 3.5. Then we illustrate on a special toy example, for which a multiplication friendly lift exists, how to compute it. In §3.1 to §3.4 we prove the Main Theorem 1. In §3.5 we demonstrate practicality of lifting algebraic geometry codes on nontrivial examples. In §4.1 we deduce Corollary 2 and sketch how to *efficiently* share and reconstruct with errors a secret over rings, then in §4.2 how to lift the alternative to Beerliova-Hirt over *constant* rings. With these tools at hand, and from our asymptotically good schemes over rings with strong multiplication, we deduce in §4.3 our Main Theorem 3. Finally in 5 we show the existence and efficiency of liftings of the RMFE of [Cas+18]. We sketch how these can be applied to hyperinvertible matrices over Galois rings to deduce Main Theorem 4.

In the appendices we give a more detailed proof (from more elementary results) that furthermore yield *projective systems of codes* (33), from which we deduce multiplication friendly lifts over Witt vectors - §C Explain how Grothendieck's existence theorem gives the previous a geometric interpretation.

2 Codes over Galois rings, and the problem of finding multiplication-friendly lifts

This section introduces *good lifts* of codes, which are the natural object that replaces linear codes, when working over rings such as $\mathbb{Z}/p^l\mathbb{Z}$, instead of finite fields such as $\mathbb{F}_p$. We continue the exploration of their elementary properties begun in [Wal99, §3]. As will be recalled in Theorem 8 (ii) and Proposition 9 (iii), they have same dimension and distance than the codes reduced modulo p. Our contributions are that these codes can be constructed from any lift of any basis of reduced code (Thm 8 (ii)) and that, observing that Walker's results imply that these codes are direct summands (Thm 8 (0')), we deduce in Corollary 13 that they have furthermore *linear reconstruction*. In addition, although we observe that the highly technical result [Wal99, Theorem 5.10] yields equality of dual distance with the one of the reduced code, for all the codes considered in §3 and yielding our Main theorem 1, we show with elementary arguments that this fact actually holds for *any* good lift in Proposition 9 (iv). This last argument is borrowed from the unpublished and unsubmitted work [Anob], which we reproduce for convenience. Notice that all these results are extended to any local ring in [Anob], but then the definition of good lifts must be narrowed, since, e.g. over p-adic rings, not all free codes have the desirable properties enumerated above.

The second purpose of this section is to introduce the main problem of this paper, which is to find codes with good lifts that are compatible with taking the componentwise-square. In §2.3 we explain why the elementary methods *fail* to solve this problem.

2.1 Notations

The simplest example of Galois ring is $R_\ell = \mathbb{Z}/p^\ell\mathbb{Z}$, where p is a prime and ℓ an integer, they all have $\mathfrak{m} = (p)$ as unique maximal ideal, and residue field $\mathbb{F}_p$. Notice that [Anob] extends the theory over any local ring. In this larger context, the definition of good lift is narrowed, although in our present context it is synonym to be a free code.

More generally let us consider r a positive integer and the finite field:

$$\mathbb{F}_{p^r} = \mathbb{F}_p[X]/\overline{P} \ ,$$

where P is a monic irreducible polynomial of degree r. Just as with $\mathbb{F}_p$, we have that $\mathbb{F}_{p^r}$ is the reduction modulo (p) of the *Galois rings*:

$$R_\ell(r) = \mathbb{Z}/p^\ell\mathbb{Z}[X]\Big/P(X)$$

where $P(X) \in \mathbb{Z}/p^\ell\mathbb{Z}[X]$ is any monic lift of $\overline{P}$ (and thus is also irreducible). The rings $R_\ell(r)$ have also maximal ideal (p).

Throughout we let R be Galois ring, with maximal ideal $\mathfrak{m} = (p)$ and the quotient $\kappa = R/\mathfrak{m}$ the *residue field* of R. It is standard that any element a in R is invertible iff it is not in $\mathfrak{m}$ iff its reduction $\overline{a}$ is invertible in κ.

A *code* C of length n over R is a submodule of R^n.

Let us note $\pi : R^n \longrightarrow \kappa^n$ be the reduction modulo $\mathfrak{m}$ map. When C is a submodule of R^n, we also note $\pi : C \longrightarrow \overline{C}$ for the induced map onto the image $\overline{C}$, which is the *code reduced modulo* $\mathfrak{m}$.

The *componentwise product* of two codewords $\boldsymbol{c}$ and $\boldsymbol{d}$ of C is noted $\boldsymbol{c}*\boldsymbol{d}$. The *square* of C, noted C^{*2}, is the linear code generated by all the componentwise products between elements of C.

The *dual code* of C is defined, as usual, as the submodule of R^n:

$$C^\perp := \left\{\boldsymbol{d} \in R^n \ , \ \sum_{i=1}^{n} c_i d_i = 0 \text{ for all } \boldsymbol{c} \in C\right\}$$

2.2 Elementary theory of good lifts of codes over Galois rings

Definition 5 (Good lifts). Let C be a code —i.e. a submodule of R^n. Then we say that C is a *good lift* —or has *good reduction*— iff C is free, i.e. we have $C \cong R^k$ for a (uniquely determined) k, called the *rank* —or dimension— of C.

For example, the sub-$\mathbb{Z}/p^2\mathbb{Z}$-module $p\mathbb{Z}/p^2\mathbb{Z} \subset \mathbb{Z}/p^2\mathbb{Z}$ is *not* free.

Before stating the elementary properties of good lifts, let us recall the following standard consequence of Nakayama's lemma:

Lemma 6. *Let M be a* finitely generated *module over a local ring $(R, \mathfrak{m})$ with residue field κ. Consider the finite-dimensional κ-vector space $M/\mathfrak{m}M$. Take a basis of it and lift arbitrarily to M. Then the lift constitutes a (minimal) set of generators for M.*

We will also often use the following result. Notice that matrix inversion is effective over Galois rings, because they are principal ideal rings so we have the Gauss pivot.

Lemma 7. *Let M be a free R-module and $\phi : M \to R^n$ a map such that the map induced on the reductions*

$$M/\mathfrak{m}M \longrightarrow \kappa^n$$

is an injection. Then ϕ has a linear *left inverse (a "retraction") $R^n \to M$.*

Proof. Consider the $n \times m$ matrix of ϕ, say where the columns are the image in R^n of the m basis vectors of M. The map being an injection modulo $\mathfrak{m}$, there exists an invertible $m \times m$ minor. Reordering the basis of R^n so that the indices of this minor are $\{1 \dots m\}$, one obtains a retraction $G := (N^{-1}|0^{n-m})$.

Theorem 8. *Let C be a code in R^n, then the following are equivalent:*

(0) *C is a good lift;*
(0') *C is a direct summand in R^n;*
(i) *the inclusion $\mathfrak{m}C \subset \mathfrak{m}R^n \cap C$ is an equality;*
(ii) *C is free and generated by* any lift *in C of* any basis *of $\overline{C}$. In particular the rank equals dimension of the reduced:*

$$\mathrm{rk}\,(C) = \dim \overline{C}\ .$$

Proof. (0) => (0') is the first statement of [Wal99, Lemma 3.2] (notice that it is specific to Artinian rings), applied to the inclusion $C \hookrightarrow R^n$. Indeed recall that a map "splits" means that it has a left retraction. In particular it is then standard that the image of such a map, in R^n, is a direct summand.

(0') => (i) This is the second statement of [Wal99, Lemma 3.2]. Alternatively, let us prove it under the friendlier form: if $t \in R$, $z \in R^n$ are such that tz belongs to C, then there exists $c \in C$ such that $tz = tc$ (thus when t is a non-zero divisor: iff $c \in C$);

Proof: write $C \oplus C' = R^n$ (internal direct sum). Suppose tz in C. Write $z = c + c'$. Thus $tz = tc + tc'$ in C. Hence, $tc' = 0$. So $tz = tc$.

(i) => (ii) Take any basis $(\overline{e_i})$ of the k-vector space $C/\mathfrak{m}C$ and lift it arbitrarily to (e_i) in C. Then by Lemma 6, it forms a basis of C. But by assumption we have

$$\bar{C} := C/(\mathfrak{m}R^n \cap C) = C/\mathfrak{m}C$$

(ii) => (0) is immediate. □

The proof of the following proposition is extracted from another unpublished and unsubmitted work, that we copy here for convenience.

Proposition 9. *If C is a good lift, then we have*
(iii) $d(C) = d(\overline{C})$*;*
(iv) $C^{\perp}$ *is a good lift of* $\overline{C}^{\perp}$ *(thus is of rank equal to the co-rank of C).*

Proof. The first statement is [Wal99, Theorem 3.4] (notice that equality is specific to Artinian rings, in general we have $\geq$).

For the second, take a basis of C and arrange it in an $k \times n$ matrix A over R. It has a $k \times k$ minor B that is a unit in R (since C has good reduction by assumption). Wlog, $A = (B||B')$ for some $k \times (n-k)$-matrix B' over R.

Let us show at once that $Ax = 0$ has a solution space (= the dual) that is free of rank $n-k$. Clearly, this space is of the form: ${}^{trans}(-B^{-1}B'y, y)$ where y runs through R^{n-k}. So a basis is given by, e.g., the ${}^{trans}(-B^{-1}B'e_i, e_i)$ where the e_i form the standard unit basis for R^{n-k}.In conclusion, the space is of the form “free variables with the remaining ones uniquely determined by the free variables”. This provides a retraction map $R^n \to C^{\perp}$ showing that $C^{\perp}$ is a direct summand, from which we conclude by Theorem 8 (0’). □

Corollary 10. *If $E \subset G$ are two lifts R^n of the same code $\overline{G}$, and G is a good lift, then they are equal (in particular E is also a good lift).*

Proof. Indeed E contains a lift of a basis of $\overline{G}$ which, by item (ii) Theorem 8, generate the whole G. □

2.3 Main difficulty: an arbitrary good lift of a code of *small square* can *fail* to have its square being a good lift

Notice that for any lift C of a code $\overline{C}$, then the square C^{*2} is automatically a lift of the square $\overline{C}^{*2}$.

Definition 11. We say that a good lift C is a *multiplication friendly lift* if and only if the square C^{*2} is also a *good lift*.

The main difficulty we deal with in this paper is to find codes $\overline{C}$ over fields, with interesting parameters, which have a multiplication friendly lifts C. The purpose of this section is to illustrate why the elementary theory is helpless here, but also that it can be applied to compute a multiplication friendly lift *once* we are given such a code $\overline{C}$ with this property. Let us notice that the problem can be narrowed: from Corollary 10, applied to the square $D = C^{*2}$, we see that the problem boils down to finding C such that we have an *inclusion* of C^{*2} in a good lift of $\overline{C}$.

The easy case of generic codes, with large squares By a result of Cascudo-Cramer-Mirandola-Zémor IEEE Trans Inf. Th. 2015, *the squares of generic codes being of large dimension*, they are thus *bad for secret sharing*. More precisely they show that, if $\overline{C}$ is a random code of dimension k in κ^n, then the square is typically of *maximal dimension* (it “spreads maximally in the space”):

– either $\dim \overline{C}^{*2} = n$,
– or $\dim \overline{C}^{*2} = \frac{k(k+1)}{2}$

Remark. Although such codes are not interesting for us, let us notice anyway that if we take an arbitrary lift C, then the square C^{*2} will be of good reduction (this is precisely the property we would like for codes of small squares). Indeed:

- In the first case, extract from C^{*2} a subcode B which is generated by a lift of a basis of κ^n. By Lemma 6 the submodule B (and thus C^2) equals R^n.
- In the second case, by construction C is generated by a lift of a basis $(e_i)_i$ of $\overline{C}$. But the $k(k+1)/2$ codeword products $(e_i * e_j)$ are a basis of $\overline{C}^{*2}$ by assumption. So C^{*2} is generated by a lift of a basis, so is a good lift.

A first counterexample One the other let us consider a code $\overline{D}$ whose square is of dimension *strictly smaller* than the generic case, then we can build a counterexample from it:

Counterexample 12. *Let $\overline{C}$ and $\overline{D}$ be codes over κ of same dimension and let us assume that $\dim \overline{D}^{*2} < \dim \overline{C}^{*2}$. Let us now build a code E over R and of length equal to the sum of the lengths of $\overline{C}$ and $\overline{D}$. Let $(\overline{c_i})_i$ and $(\overline{d_i})_i$ be bases of $\overline{C}$ and $\overline{D}$, let $(c_i)_i$ and $(d_i)_i$ be arbitrary lifts and define E the code generated by the vectors $(d_i, pc_i)_i$. Then E is a good lift, because of dimension $\dim \overline{D} = \dim \overline{E}$. But E^2 is not a good lift, because of dimension*

$$\dim E^{*2} \geq \dim \overline{C}^{*2} > \dim \overline{D}^{*2} = \dim \overline{E}^{*2} \ .$$

Sparsity of solutions, if any, illustrated on a toy example We illustrate the multiplicative lifting problem on a tiny AG code. Consider the elliptic curve $y^2 + xy + y - x^3 + 1$ over

$$\mathbb{F}_{2^3} = \mathbb{F}_2 < \delta > \text{ with polynomial } \delta^3 + \delta + 1 = 0,$$

with 14 places, P_0 the place at infinity, the divisor $D_0 = 4P_0$ and the Riemann-Roch space $L(4P_0)$, with basis equal to the functions $(1, x, x^2, y)$. Let us define the evaluation code $C(D_0)$ at the $P_0, \ldots, P_{13}$, (see Remark 3.6 for evaluation at P_0) with basis $\overline{\boldsymbol{e_i}}$, $i = 1..4$, which form the following generating matrix:

$$\overline{G} = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ \delta & \delta & \delta^2 & \delta^2 & \delta^3 & \delta^3 & \delta^4 & \delta^4 & \delta^5 & \delta^5 & \delta^6 & \delta^6 & 1 \\ \delta^2 & \delta^2 & \delta^4 & \delta^4 & \delta^6 & \delta^6 & \delta & \delta & \delta^3 & \delta^3 & \delta^5 & \delta^5 & 1 \\ 1 & \delta & 1 & \delta^2 & \delta^2 & \delta^4 & 1 & \delta^4 & \delta & \delta^2 & \delta & \delta^4 & 0 \end{bmatrix}$$

Out of the 10 componentwise products $\overline{\boldsymbol{e_i}} * \overline{\boldsymbol{e_j}}$, 8 of them: $\overline{\mathcal{B}} := (\overline{\boldsymbol{e_k}} * \overline{\boldsymbol{e_l}})_{k,l \in B}$ generate $C(D_0)^{*2}$, B being defined as all unordered tuples (k, l) (cardinality $10 = 4 \times 5/2$) except $(2, 2)$ and $(4, 4)$. In particular $\overline{\boldsymbol{e_2}} * \overline{\boldsymbol{e_2}}$ and $\overline{\boldsymbol{e_4}} * \overline{\boldsymbol{e_4}}$ decompose themselves on this basis $\overline{\mathcal{B}}$, with decomposition coefficients $(\overline{\lambda_{2,2,k,l}})_{k,l \in B}$

and $(\overline{\lambda_{4,4,k,l}})_{k,l\in B}$ given by the following 2×8 matrix, called ”Reduc“ in the implementation:

$$\text{(2)} \qquad transp\Big(\overline{\lambda_{2,2,k,l}})_{k,l\in B}, (\overline{\lambda_{4,4,k,l}})_{k,l\in B}\Big) = \begin{bmatrix} 0\,0\,1\,0\,0\,0\,0\,0 \\ 1\,0\,0\,1\,1\,1\,0\,0 \end{bmatrix}$$

Then we repeated the following experiment 10^8 times: *randomly* lift the $(\overline{\boldsymbol{e_i}})_i$ modulo 2^2, to obtain vectors $(\boldsymbol{e_i})_i$ with coordinates in $R_4(8) = \mathbb{Z}/2^2\mathbb{Z} < \Delta >$. Let C_{bad} the code generated by these lifts. By Theorem 8 (ii), it is always a *good lift*. But we observed in *all the experiments* that $\boldsymbol{e_2} * \boldsymbol{e_2}$ and $\boldsymbol{e_4} * \boldsymbol{e_4}$ *do not* anymore decompose themselves on the lifts of the previous basis of $C(D_0)^{*2}$: $\mathcal{B} := (\boldsymbol{e_k} * \boldsymbol{e_l})_{k,l\in B}$ —see two paragraphs later for an explanation of how this checks were done efficiently with linear algebra. So in these situations C_{bad}^{*2} *is not* a good lift of the square $C(D_0)^{*2}$, because if it were, then by Theorem 8 (ii) the lifted basis $\mathcal{B}$ *would* generate it.

Why solutions may likely not exist at all Let us give a feeling of why most codes with small squares are likely to have no multiplication friendly lift. We will come over these arguments in more details in §3.5.

Let $\overline{C}$ be a code over, say, $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ of dimension k and length n, such that the square $\overline{C}^2$ has *small* dimension, say, $3k < n$. The goal is to find a multiplication friendly lift. That is, a code C over $\mathbb{Z}/p^2\mathbb{Z}$ (namely: a free sub-module of $(\mathbb{Z}/p^2\mathbb{Z})^n$) of same rank k, that lifts $\overline{C}$ modulo p^2, and such that the square C^2 is also a good lift of $\overline{C}^2$. As argued with the toy example, it follows from Theorem 8 (ii) that these requirements are equivalent to the following: let $(\boldsymbol{e_i})_i$ be any basis of C lifting a basis $(\overline{\boldsymbol{e_i}})$ of $\overline{C}$; let $\overline{\mathcal{B}} := (\overline{b_l})_l$ be a basis of $\overline{C^2}$; then $(\overline{b_l})_l$ lifts modulo p^2 to a basis of the square C^2, in particular generates the componentwise products $(\boldsymbol{e_i} * \boldsymbol{e_j})_{i,j}$. This equivalent condition translates itself into the fact that the equations expressing $\overline{\boldsymbol{e_i}} * \overline{\boldsymbol{e_j}}$ in terms of the $(\overline{b_l})_l$:

$$\overline{\boldsymbol{e_i}} * \overline{\boldsymbol{e_j}} = \sum_l \overline{\lambda_{i,j,k,l} b_l} \pmod p$$

lift modulo p^2. The number of degrees of freedom (the unknowns) are: (i) the choices of lifts for the $\overline{\boldsymbol{e_i}}$, so a total of nk coordinates to lift in $\mathbb{Z}/p^2\mathbb{Z}$; (ii) and lifts for the coefficients $\overline{\lambda_{l,i,j}}$: a total of $3k \times k(k+1)/2$ unknowns in $\mathbb{Z}/p^2\mathbb{Z}$. So the number of unknowns is asymptotically equivalent to (ii): $3k \times k(k+1)/2$. Whereas the number of equations is $nk(k+1)/2$ (namely: $k(k+1)/2$ vectorial equations with n coordinates in $\mathbb{Z}/p^2\mathbb{Z}$ each). Notice that $3k < n$, so that there are more constraints than variables. Finally, as will be detailed in the next paragraph, notice that this *quadratic* system over a *ring* simplifies modulo p^2 to a *linear system* over the *field* $\mathbb{F}_p$. Thus, the system being overdetermined, then a priori no solution is likely to exist.

A technique to find them when they exist, illustrated on the toy example We will formalize the general technique in §3.5 and justify that it returns all solutions when they exist. As a matter of fact, as will be demonstrated in general in Theorem §16, it is a remarkable property of AG codes, in particular the toy example, that they always have multiplication-friendly lifts —at least for all practical parameters. Putting this in perspective with the previous paragraph, this illustrates that AG codes seem *highly non-generic* among those with small square.

First, fix a good lift C_{bad} of $C(D_0)$ by lifting arbitrarily the basis to $(\boldsymbol{e_i}')_i$, for example by lifting the coordinates from $\mathbb{F}_2 < \delta >$ to $\mathbb{Z}/2^2\mathbb{Z} < \varDelta >$ by the dummy rule: $1 \to 1$ and $\delta \to \varDelta$. This gives formally the same generating matrix as $\overline{G}$, with δ replaced by $\varDelta$. With the same dummy rule, lift the decomposition coefficients $(\overline{\lambda_{2,2,k,l}})_{k,l \in B}$ and $(\overline{\lambda_{4,4,k,l}})_{k,l \in B}$ to $\lambda'_{2,2,k,l}$ and $\lambda'_{4,4,k,l}$, so that their matrix is formally the same as in (2). Now, there is *no reason* why $\boldsymbol{e'_2} * \boldsymbol{e'_2}$ and $\boldsymbol{e'_4} * \boldsymbol{e'_4}$ should decompose on $\mathcal{B} := (\boldsymbol{e_k}' * \boldsymbol{e_l}')_{k,l \in B}$, let alone with coefficients equal to $\lambda'_{2,2,k,l}$ and $\lambda'_{4,4,k,l}$, as we illustrated with our random tests two paragraphs above. As a matter of fact, we encounter nonzero error vectors $2\boldsymbol{D_{2,2}}$ and $2\boldsymbol{D_{4,4}}$ when trying to write the decompositions in $\mathbb{Z}/2^2\mathbb{Z} < \varDelta >$:

$$(3) \qquad \boldsymbol{e'_2} * \boldsymbol{e'_2} = \sum_{k,l} \lambda'_{2,2,k,l} \boldsymbol{e_k}' * \boldsymbol{e_l}' + 2\boldsymbol{D_{2,2}} \text{ and likewise for } \boldsymbol{e'_4} * \boldsymbol{e'_4}$$

Let us insist on the remarkable fact that the error vectors are multiples of 2, since the equalities (3) do hold without error term modulo 2. "Dividing" by 2, their coefficients are

$$transp(\boldsymbol{D_{2,2}}, \boldsymbol{D_{4,4}}) = \begin{bmatrix} 0 & 0 & \delta^4 & \delta^4 & \delta & \delta & 1 & 1 & \delta^5 & \delta^5 & \delta & \delta & 0 \\ 0 & 0 & \delta & \delta & 0 & 1 & \delta^2 & \delta^2 & \delta^4 & 0 & 0 & \delta^5 & 1 \end{bmatrix}$$

Which we express in $\mathbb{F}_{2^3}$ by abuse of notation (remember that an element $2x \in \mathbb{Z}/2^2\mathbb{Z} < \varDelta >$ is determined by the residue $\overline{x} \in \mathbb{F}_{2^3} \mod 2$). Now, let us look for corrective terms $2\boldsymbol{f'_i}$ and $2\mu'_{i,j,k,l}$, which we need only to find modulo 2:

$$(4) \qquad \boldsymbol{e_i} = e'i + 2\boldsymbol{f'_i} \text{ and } \lambda_{i,j,k,l} = \lambda'_{i,j,k,l} + 2\mu'_{i,j,k,l}$$

So that, replacing $\boldsymbol{e_i}'$ in (3) by the corrected $\boldsymbol{e_i}$ of (17) —where the corrective terms are treated as unknows—, simplifying and moding out the terms that are multiples of (2^2), we observe —a reminiscence of Hensel's trick— that all the terms remaining in the system are multiples of 2. So "dividing" the system by 2, we fall back to the following *linear* system in $\mathbb{F}_{2^3}$:

(5)

$$\overline{\boldsymbol{e_2}} * \boldsymbol{f'_j} + \overline{\boldsymbol{e_2}} * \boldsymbol{f'_i} - \boldsymbol{D_{2,2}} = \sum_{k,l} \mu'_{2,2,k,l} \overline{\boldsymbol{e_k}} * \overline{\boldsymbol{e_l}} + \overline{\lambda_{2,2,k,l}} (\overline{\boldsymbol{e_k}} * \boldsymbol{f'_l} + \overline{\boldsymbol{e_l}} * \boldsymbol{f'_k}) \ \ \text{(same for } \overline{\boldsymbol{e_4}} * \overline{\boldsymbol{e_4}}\text{)}$$

Solving this system for the correction terms, we deduce the corrected basis $(\boldsymbol{e_i})_i$ defined as in (4), that define the corrected code C_{good}, whose coordinates are given in the big left-hand matrix in Appendix §A. Likewise we deduce the corrected decomposition coefficients $(\lambda_{2,2,k,l})_{k,l \in B}$ and $(\lambda_{4,4,k,l})_{k,l \in B}$ as given in the centered right-hand formula.

We can finally check straightforwardly that, with these corrected values, then $\boldsymbol{e_2}*\boldsymbol{e_2}$ and $\boldsymbol{e_4}*\boldsymbol{e_4}$ now decompose themselves on $\mathcal{B}$ with the corrected coefficients, without anymore parasitic error vectors. So with these corrected lifts $(\boldsymbol{e_i})_i$, we have now that the square of the corrected code C_{good} is also a good lift. That is, we have succeeded in modifying the good lift C_{bad} into a *multiplication-friendly* lift C_{good}.

2.4 Decoding without errors and uniformly distributed projection on $d^{\perp} - 1$ coordinates

***Linear* decoding without errors (reconstruction)** Although theoretical results for error correction over rings are shown in [Anoa, Construction 1 & Proposition 1], it is not yet clear if there exists *effective algorithms* for even the simple task of reconstruction of a secret with only erasures. This is not a completely straightforward question: indeed we show in Counterexample 14 below that *there doesn't exist a linear reconstruction map* for a large class of linear codes over rings which are not good lifts.

Applying Lemma 7 to the puncturing map of a good lift, we deduce that we can *linearly* decode without error up to the minimal distance: i.e. there exists a linear reconstruction map.

Corollary 13. *Let C be a good lift over R, such that the reduced code $\overline{C}$ has distance $\overline{d}$. Then the puncturing map (e for "erasure"):*

$$e : C \longrightarrow R^{n-(\overline{d}-1)}$$

has a retraction, i.e. a linear *left inverse $R^{n-(\overline{d}-1)} \longrightarrow C$.*

Proof. C being a good lift, we have $C/\mathfrak{m}C = \overline{C}$ by Theorem 8 (i). Thus the reduced map

$$\overline{e} : \overline{C} = C/\mathfrak{m} \longrightarrow \kappa^{n-(\overline{d}-1)}$$

is exactly the puncturing map on $\overline{C}$, which is by assumption an *injection.* Thus we can apply Lemma 7. □

The following counterexample shows that, without the assumption to be a good lift, there exists submodules of R^n for which the puncturing map is an injection but for which *there doesn't exists any retraction.*

Counterexample 14. *Let C be a code in R^n with $d(\overline{C}) \geq 2$ such that there exists a punctured $C^* \subset R^{n-(\overline{d}-1)}$ which is* not *a good lift. [For example $C = \langle (p,p,p,0),(1,0,0,1) \rangle \in R^4$ (e.g. $R = \mathbb{Z}/p^{\ell}\mathbb{Z}$), with $d(\overline{C}) = 2$ and injectivity in R^3 when puncturing the last coordinate.] Then there* doesn't exist *any linear reconstruction map, i.e. any retraction $R^{n-(\overline{d}-1)} \to C$. [Indeed otherwise, compose the reconstruction map with the puncturing map: we obtain a retraction map to the inclusion $C^* \subset R^{n-(\overline{d}-1)}$, so C^* would be a direct summand, thus a good lift by Theorem 8 (0'), a contradiction.]*

Uniformly distributed projection on $d^\perp - 1$ coordinates

Proposition 15. *Let C be an* arbitrary submodule *(not necessarily free!) of R^n, then projection on up to $d(\overline{C}^\perp) - 1$ coordinates is uniformly distributed.*

Proof. Let U be an arbitrary index set with $|U| = \overline{d}^\perp - 1$. So $\overline{C}_U = \kappa^U$. Hence C_U contains $|U|$ vectors so that the matrix formed by them has an invertible determinant, thus has an inverse, thus these vectors generate R^U. □

3 Existence and efficient construction of multiplicative lifts of algebraic geometry codes

3.1 Roadmap of the proof of Main Theorem 1

We first prove the following algebraic-geometric theorem 16. Then, Main Theorem 1 will follow from Corollary 19, as explained at the end of the section.

Theorem 16. *Let X_0 be a function field of genus g over any finite field $\mathbb{F}_{p^r}$, $\left(P_0^{(j)}\right)_j$ the rational places (i.e. of degree one) of X_0 and $\mathcal{P}_0 = P_0^{(1)}, \ldots, P_0^{(n)}$ a subset of them. Consider any divisor D_0 on X_0 with support on rational places*[11]*, and degree*

$$2g + 1 \leq \deg(D_0) < \frac{n}{2} \, .$$

Then we can construct algebraic geometry codes $C(D_0)$ and $C(2D_0)$ defined by evaluation of the Riemann-Roch spaces $L(D_0)$ and $L(2D_0)$ on $\mathcal{P}_0$, and good lifts $C(D)$ and $C(2D)$ over $R_\ell(r)$ such that:

$$C(D)^{*2} = C(2D) \, . \tag{6}$$

For the proof, we first show in §3.2 below, that we have an inclusion in (6). Namely, that the trivial inclusion $C(D_0)^2 \subset C(2D_0)$ over fields carries over some well chosen good lifts $C(D)$ and $C(2D)$ over Galois rings as soon as $\deg(D_0) < n$.

We then show in §3.3 Theorem 18 that equality in (6) holds over fields: $C(D_0)^{*2} \subset C(2D_0)$ as soon as $\deg(D_0) \geq 2g + 1$. This results from a hard theorem of Mumford, which we generalize to nonnecessarily algebraically closed fields, as proven in appendix D, by standard arguments. Fortunately, we also obtain an elementary proof of Theorem 18 in the interesting cases where $\deg(D_0) \geq 4g$: see §3.4. We then deduce equality over rings: (6) from the elementary Corollary 10, finishing the proof of Theorem 16.

From the elementary theory we deduce Corollary 19, which, instantiated e.g. on Garcia Stichtenoth towers (or any other optimal family), immediatly yields Main theorem 1.

[11] Inluding possibly points of $\mathcal{P}_0$: see Remark 3.6

3.2 Proof of inclusion in (6) of Theorem 16

This section concentrates the algebraic geometry over rings needed in the proof of Main Theorem 1, which directly follows from the fundamental work [Wal99]. The goal is to justify that, as soon as we have $\deg(D_0) < n$, then we have good lifts $C(D)$ and $C(2D)$ such that inclusion in 6 holds:

$$C(D)^{*2} = C(2D) . \tag{7}$$

Roadmap of the proof. We first show the existence of good lifts $L(D)$ and $L(2D)$ of Riemann-Roch spaces, such that we have inclusions of products of spaces of global sections

$$L(D)^{\otimes 2} = L(2D) , \tag{8}$$

where the traditional notation $L(D)^{\otimes 2}$ stands for the space generated by all products fg of pairs of sections (f, g) in $L(D)$. Then, thanks to Judy Walker's Theorem 17 below —which is actually a direct consequence of Lemma 7— we deduce that the evaluation codes over rings $C(D)$ and $C(2D)$ arising from these good lifts are also good lifts.

Let us follow Walker's [Wal99] notations. Note $R = R_\ell(r)$ the noetherian local ring, with residue ring $\kappa = R/(p) = \mathbb{F}_{p^r}$. X_0 being a smooth projective curve over κ, then from [Ill05, Theorem 5.19 (ii)] (or [SGA1, III Corollaire 7.4]), X_0 has a smooth projective lift over the ring of Witt vectors $W(\kappa)$. Which, after reduction $\bmod p^\ell$, yields a projective lift X over R (because these properties are preserved by base change). Also, R being local, κ-points of X_0 lift to R-points of X by the formal smoothness criterion (see [Wal99, Remark 4.5] or next section for details). As a consequence, divisors with support on rational points (actually any divisor) lift to X —and thus also do the line bundles $\mathcal{L}_0$ arising from them.

An explicit procedure for simultaneous compatible good lifts of line bundles. By [Wal99, Lemma 4.4] we can construct lifts of Cartier divisors D_0 on X from the following recipe. First, for every rational point $P_0^{(j)}$ of X_0, fix a closed point of degree one $P^{(j)}$ of X above P_0, as described in [Wal99, Remark 4.5] (lift arbitrarily $P_0^{(j)}$ to an R-point, then choose $P^{(j)}$ inside the image).

Then we can simultaneously lift divisors D_0 and $2D_0$ on X_0 as follows. For every rational point P_0 of X_0 in the support of the line bundle D_0, let m be the valuation of D_0 at P_0 and let P be the closed point lying above P_0 as fixed earlier. Deduce from it a Cartier divisor mP, then sum over the points P_0 in the support of D_0, to obtain a lift D of D_0. Likewise for the Cartier divisor $2D$, equal to the same formal sum of R-points as in D and with twice the multiplicities. In particular, note $\mathcal{L} := \mathcal{L}(D)$ the line bundle associated to D, and likewise for $\mathcal{L}(2D)$. Then in a neighborhood U of P excluding the other points of the support of D, and small enough to have t_U a uniformizer of P (as in [Wal, Proposition 4.9]), we have that

$$\mathcal{L}_U = t_U^{-m} \mathcal{O}_U . \tag{9}$$

Thus $t_U^{-m} t_U^{-m} \in \mathcal{L}_U(2D)$, hence the claimed inclusion of products of global sections (8).

Deducing algebraic geometry codes by evaluation of the global sections. We then have the following compatibilities, as wrapped-up in [Wal99, Theorem 5.5]:

Theorem 17 (Lifts of Riemann-Roch spaces and AG codes). *Consider n rational points $\mathcal{P}_0 = \big(P_0^{(j)}\big)_{j=1\ldots n}$ on X_0, D_0 a divisor of degree:*

$$2g - 2 < \deg D_0 < n$$

with associated line bundle $\mathcal{L}_0$, and the injective evaluation map γ_0 yielding an algebraic geometry code $\overline{C}$ in κ^n. Then this data lifts to objects over R: X,$\mathcal{P}$ and D, with associated line bundle $\mathcal{L}$, yielding an evaluation code C, such that we have the following commutative diagram:

(10)
$$\begin{tikzcd}
\Gamma(X,\mathcal{L}) \arrow[r, two heads] \arrow[d, hook, "eval"'] & \Gamma(X,\mathcal{L}) \otimes_R \kappa \arrow[r, "\sim"] & \Gamma(X_0,\mathcal{L}_0) \arrow[d, hook, "eval"'] \\
\oplus_j \Gamma(P^{(j)}, \mathcal{L}|_{P^{(j)}}) \arrow[d, "\cong"', "\gamma"] & & \oplus_j \Gamma(P_0^{(j)}, \mathcal{L}_0|_{P_0^{(j)}}) \arrow[d, "\cong"', "\gamma_0"] \\
R^n \arrow[rr, "\bullet\otimes_R\kappa"] & & \kappa^n
\end{tikzcd}$$

Where: - the top left horizontal arrow and the bottom horizontal arrow are tensorisation by $\otimes_A \kappa$ - the top right isomorphism is constructed canonically as in the proofs of [Wal99, Lemma 4.6 & proof of Th 4.7]

- the top vertical arrows are the canonical restriction maps - the bottom left vertical arrow is a collection of arbitrary isomorphisms for all j:

$$\gamma_j : \Gamma(P^{(j)}, \mathcal{L}|_{P^{(j)}}) \longrightarrow A$$

that reduce to γ_0 by tensorisation by $\otimes_R \kappa$ (and if not, then redefine γ_0 accordingly without changing the code in κ^n).

Notice that the name "evaluation maps" of the top vertical arrows is abusive in general (because of poles, etc: see the first example of §3.6), but anyway they really play this role.

As explained in [Wal99], the code C is a good lift because it is the image of a free module: $\Gamma(X,\mathcal{L})$, under the evaluation map which is an injection modulo $\mathfrak{m}$, and thus is a direct summand in R^n by Lemma 7.

3.3 Proof of equality in (6) of Theorem 16

Firstly, *over fields*, the following theorem gives a criterion to have equality for the *reductions*:

$$C(D_0) * C(D_0') \;=\; C_0(D_0 + D_0')\;.$$

Theorem 18. *Let D_0, D_0' be two divisors of a function field X_0 of genus g over any field K. Suppose that $\deg D_0 \geq 2g$ and $\deg D_0' \geq 2g+1$. Then*

$$L(D_0)L(D_0') = L(D_0 + D_0') \tag{11}$$

This theorem is deduced in Appendix D from Mumford's normal generation criterion, which we extend to any field. See also the next section for more elementary proofs of Theorem 18 in particular cases.

From the inclusion in (7), and under the degree assumptions of Theorem (18), we can then apply Corollary 10 to

$$E := C(D) * C(D) \ \subset\ G := C(2D)$$

to deduce that equality (11) holds *over rings*, which proves Theorem 16.

From the properties on the distance and dual distance of good lifts stated in Theorem 8 (iii) and (iv), we can finally state:

Corollary 19. *Let X_0 be a function field of genus g over any finite field $\mathbb{F}_{p^r}$. Let D_0 be a divisor on X_0 with support on rational points (i.e. of degree one) and with degree*

$$2g + 1 \leq \deg{(D_0)} < \frac{n}{2}\ .$$

Let $L(D_0)$ be the Riemann-Roch space and $P_1, \ldots, P_n$ a collection of rational points on X_0. Define the algebraic geometry code $\overline{C}$ as the isomorphic image of $L(D_0)$ by the evaluation map on the $(P_i)_i$.

Then for any positive integer ℓ, $\overline{C}$ lifts to a free submodule C over the Galois ring $R_\ell(r)$, of same dimension and dual distance than $\overline{C}$, and such that the square *C^{*2} is also free of rank $\dim \overline{C}^{*2}$ and minimal distance $d(\overline{C}^{*2})$.*

Main Theorem 1 then follows as an immediate consequence (apply the previous to any asymptotically optimal family of curves, such as Shimura or Drinfeld or optimal recursive towers of function fields).

3.4 Elementary proof of Theorem 18 in a particular case

$D_0 = dP_0$ supported at a rational point, with degree $d \geq 4g$ We first prove two lemmas on gaps between Riemann-Roch spaces.

Lemma 20. *With the same assumptions, for any integer*

$$v \in \left[\left\lceil \frac{d}{2} \right\rceil, \ldots, d\right]$$

Then there exists a rational function $y_0 \in L(D)$ with exactly a pole of order v at P.

Proof. Claim: for all $i' \leq \left\lceil \frac{d}{2} \right\rceil + 1$, then we have that $l(K - (D - i')) = 0$ for degree reasons. Indeed:

$$\deg\left(K - (D - i')\right) \leq 2g - 2 - d + \left\lceil \frac{d}{2} \right\rceil + 1 < 2g - 1 - 4g + \left(\frac{d}{2} + 1\right) \leq 0 \, .$$

From the claim it follows that for all integer $i \leq \left\lceil \frac{d}{2} \right\rceil$, we have a gap in the sequence of dimensions:

$$l(D - iP) < l(D - (i+1)P) \, , \tag{12}$$

thus the result. □

Proof of the theorem: Consider f_0 a function in $L(2D) = L(2dP)$. Either it is in $L(D)$, and we are done. Or it has a pole at P with order strictly larger than d:

$$w := \mathrm{ord}_P(f) > d$$

(and by definition no other pole elsewhere). In this case, Lemma 20 implies that there exist y_0, y_0' in $L(D)$ such that

$$\mathrm{ord}_P(y_0) + \mathrm{ord}_P(y_0') = w$$

and thus, up to multiplying y_0 by a constant ρ_0, we have that the function:

$$f_1 = f_0 - y_0 y_0'$$

has a pole at P strictly lower than w (and by construction no pole elsewhere). Since $y_0 y_0'$ is in $L(D)^2$, we can conclude by recursion on the order of the pole of f_1 at P.

3.5 Practical method

The main result of this section, stated as Proposition 23, is that we can deduce a good multiplicative lift $C_{\ell+1} \in R_{\ell+1}(r)^n$ —if any— from a good multiplicative lift $C_\ell \in R_\ell(r)^n$, by just solving a *linear* system over $\mathbb{F}_{p^r}$ of size $O(n^3) \times O(n^3)$, so in *polynomial time*.

Furthermore, the key heuristic (unexplained) observation is that, for AG codes $\overline{C}$ satisfying the criterion of Theorem 16, then we have the following apparent *stronger property* than Theorem 16: *any* multiplicative lift C_ℓ of $\overline{C}$ over a given $R_\ell(r)$, has itself a multiplicative lift over $R_{\ell+1}(r)$ (whereas what is proven in Corollary 19 is only existence of such a multiplicative lift for the *base code* $\overline{C}$). Thus in practice we *can lift $\overline{C}$ sequentially in L steps into $R_L(r)^n$, each of these steps involving only one linear system (of same size in each step)*, so that the overall complexity is *linear in L*. We illustrate efficiency of our method by lifting a strongly multiplicative secret sharing scheme over $\mathbb{F}_{16}$ for 64 players and adversary threshold $t = 13$, into a scheme over $\mathbb{Z}/2^{100}\mathbb{Z}$, in a minute on a single processor.

Lemma 21. *Let C be a good lift in $R_\ell(r)^n$. Then C^{*2} is also a good lift if and only if there exists a basis $(\boldsymbol{e_i})_i$ of C, and a set B of unordered couples of indices (k,l) of cardinality $\dim C^{*2}$, such that the elementary products $(\boldsymbol{e_k} * \boldsymbol{e_l})_{(k,l)\in B}$ form a basis of C^{*2}. Namely, if and only if there exists coefficients $\lambda_{i,j,k,l}$ in $R_\ell(r)$ such that the following equalities in $R_\ell(r)^n$ hold:*

$$\boldsymbol{e_i} * \boldsymbol{e_j} = \sum_{k,l} \lambda_{i,j,k,l}\ \boldsymbol{e_k} * \boldsymbol{e_l} \ \text{ for all } i \leq j \tag{13}$$

Proof. Let $(\overline{\boldsymbol{e_i}})_i$ be *any* basis of $\overline{C}$. Let us chose $(\boldsymbol{e_i})_i$ *any* lifts of the $(\overline{\boldsymbol{e_i}})_i$ in C. By Theorem 8 (ii), C being a good lift, they form basis of C. The family $(\overline{\boldsymbol{e_i}} * \overline{\boldsymbol{e_j}})_{(i,j)}$ is a generating set of $\overline{C}^{*2}$. Extract from it a basis $(\overline{\boldsymbol{e_k}} * \overline{\boldsymbol{e_l}})_{(k,l)\in B}$ of $\overline{C}^{*2}$. The family $(\boldsymbol{e_k} * \boldsymbol{e_l})_{(k,l)\in B}$ is contained in C^{*2} and is a lift of a basis of $\overline{C}^{*2}$. But C^{*2} is by asumption a good lift, thus Theorem 8 (ii) implies that $(\boldsymbol{e_k} * \boldsymbol{e_l})_{(k,l)\in B}$ is a basis of C^{*2}.

As for the explicit equivalent conditions (13), let us simply call $\lambda_{i,j,k,l}$ the coefficients of the decomposition of a given $(\boldsymbol{e_i} * \boldsymbol{e_j})_{i,j}$ over the basis $(\boldsymbol{e_k} * \boldsymbol{e_l})_{(k,l)\in B}$. □

Lemma 22. *Let C_ℓ be a good lift in $R_\ell(r)^n$ such that C_ℓ^{*2} is also a good lift. Suppose that there exists a lift $C_{\ell+1}$ of C_ℓ in $R_{\ell+1}(r)^n$ such that the square $C_{\ell+1}^{*2}$ is still a good lift. Consider a basis $(\boldsymbol{e_i})_i$ of C_ℓ^{*2}, along with $(\boldsymbol{e_k} * \boldsymbol{e_l})_{(k,l)\in B}$ a basis of C_ℓ^{*2} and the explicit decomposition* (13)*, as granted by previous lemma.*

Then $C_{\ell+1}$ has a basis $(\widetilde{\boldsymbol{e_i}})_i$ formed of lifts *of the $\boldsymbol{e_i}$, such that there exists* lifts $\widetilde{\lambda_{i,j,k,l}}$ *of the coefficients $\lambda_{i,j,k,l}$, such that all the equalities* (13) lift *over $R_{\ell+1}(r)^n$:*

$$\widetilde{\boldsymbol{e_i}} * \widetilde{\boldsymbol{e_j}} = \sum_{k,l} \widetilde{\lambda_{i,j,k,l}}\ \widetilde{\boldsymbol{e_k}} * \widetilde{\boldsymbol{e_l}} \ \text{ for all } i \leq j \tag{14}$$

Proof. Consider *any* lift $(\widetilde{\boldsymbol{e_i}})_i$ of the $(\boldsymbol{e_i})_i$ in $C_{\ell+1}$, and the corresponding family $(\widetilde{\boldsymbol{e_k}} * \widetilde{\boldsymbol{e_l}})_{(k,l)\in B}$ in $C_{\ell+1}^{*2}$. Modulo p, they are bases of $\overline{C}$ and $\overline{C^{*2}}$, so by the same argument (Theorem 8 (ii)), they are bases of $C_{\ell+1}$ and $C_{\ell+1}$.

Now, define $\widetilde{\lambda_{i,j,k,l}}$ as coefficients of the decomposition (14), and let us show that they reduce mod p^ℓ to the $\lambda_{i,j,k,l}$. For this, reduce the equations (14) mod p^ℓ: we obtain a decomposition similar to (13), but with coefficients $\overline{\widetilde{\lambda_{i,j,k,l}}}$ instead of $\lambda_{i,j,k,l}$. By uniqueness of decomposition over a basis in a free module, they coincide. □

Proposition 23. *Let C_ℓ be a good lift in $R_\ell(r)^n$ such that the square C_ℓ^{*2} is also a good lift. Suppose we are explicitely given a basis of $(\boldsymbol{e_i})_i$, along with the explicit decomposition* (13) *granted by Lemma 22. Then finding —if any— a lift $C_{\ell+1}$ of C_ℓ in $R_{\ell+1}(r)^n$ such that the square $C_{\ell+1}^{*2}$ is still a good lift, falls back to solving* a linear *of size $O(n^3) \times O(n^3)$. More precisely,* the system returns all such lifts $C_{\ell+1}$*, and for each of them a lift in $R_{\ell+1}(r)^n$ of the explicit decomposition* (14)*.*

Proof. For sake of simplicity let us make the proof for $\ell = 1$, with thus $C_1 = \overline{C}$ and we are looking for a lift $C := C_2$ in $R_2(r)^n$ such that C^{*2} is a good lift. The situation for higher levels ℓ being similar (the situation is reminiscent of Hensel's lemma). By assumption we are given $(\overline{\boldsymbol{e_i}})_i$ a basis of $\overline{C}$, and a basis $(\overline{\boldsymbol{e_k}} * \overline{\boldsymbol{e_l}})_{(k,l)\in B}$ of $\overline{C}^{*2}$ along with the following (quadratic) equalities

$$\overline{\boldsymbol{e_i}} * \overline{\boldsymbol{e_j}} = \sum_{k,l} \overline{\lambda_{i,j,k,l}}\, \overline{\boldsymbol{e_k}} * \overline{\boldsymbol{e_l}} \text{ for all } (i,j) \tag{15}$$

in $\mathbb{F}_{p^r}$. Thanks to Lemma 22, the problem of finding C boils down to finding lifts $\boldsymbol{e_i}$ in $R_2(r)^n$ and $\lambda_{i,j,k,l}$ in $R_2(r)$, such that the equations (15) all lift to $R_2(r)^n$. Fix arbitrary lifts $\boldsymbol{e_i}'$ and $\lambda'_{i,j,k,l}$ of the $\overline{\boldsymbol{e_i}}$ and the $\overline{\lambda_{i,j,k,l}}$, over/in $R_2(r)$. We obtain error terms $pD_{i,j}$ when writing the system in $R_2(r)$:

$$\boldsymbol{e_i}' * \boldsymbol{e_j}' = \sum_{k,l} \lambda'_{i,j,k,l} \boldsymbol{e_k}' * \boldsymbol{e_l}' + pD_{i,j} \text{ for all } (i,j) \tag{16}$$

Solving the system means finding correct lifts $\boldsymbol{e_i}''$ and $\lambda''_{i,j,k,l}$ that anihilate the error terms $pD_{i,j}$. But $e''i$ and $\lambda''_{i,j,k,l}$ can always be deduced from $\boldsymbol{e_i}'$ and $\lambda'_{i,j,k,l}$, by adding corrective terms $p\boldsymbol{f'_i}$ and $p\mu'_{i,j,k,l}$, which we need only to find modulo p:

$$\boldsymbol{e_i}'' = e'i + p\boldsymbol{f'_i} \text{ and } \lambda''_{i,j,k,l} = \lambda'_{i,j,k,l} + p\mu'_{i,j,k,l} \tag{17}$$

So that, replacing $\boldsymbol{e_i}'$ in (16) by the corrected $\boldsymbol{e_i}$" of (17) (where the corrective terms are treated as unknows), simplifying and moding out the terms that are multiples of p^2, we observe (Hensel's trick) that all the terms remaining in the system are multiplies of p. So simplifying by p, we fall back to the following *linear* system in $\mathbb{F}_{p^r}$:

$$\overline{\boldsymbol{e_i}} * \boldsymbol{f'_j} + \overline{\boldsymbol{e_j}} * \boldsymbol{f'_i} - D_{i,j} = \sum_{k,l} \mu'_{i,j,k,l} \overline{\boldsymbol{e_k}} * \overline{\boldsymbol{e_l}} + \overline{\lambda_{i,j,k,l}}(\overline{\boldsymbol{e_k}} * \boldsymbol{f'_l} + \overline{\boldsymbol{e_l}} * \boldsymbol{f'_k})\ \forall i \leq j \tag{18}$$

Finally, as for the size of the system, each vectorial equation for (i,j) expands in n scalar (quadratic) equations, so a total of $nk(k+1)/2$. The lifts of the $(\boldsymbol{e_i})_i$ are n unknowns and the lifts of $\lambda_{i,j,k,l}$ are $k(k+1).\dim(C^{*2})$ unknowns. □

Remark. Then if $\dim(C^{*2})$ is smaller than n (which is the cases that we are interested in for multiplicative secret sharing), then the linear system is *overdetermined.* So it has a priori no solution, which further evidences the difficulty of finding multiplicative good lifts of codes.

Optimizations List the (i,j) for which the decomposition of $\overline{\boldsymbol{e_i}} * \overline{\boldsymbol{e_j}}$ is very simple: one single nonzero coefficient $\overline{\lambda_{i,j,k,l}}$ equal to one and the others equal to zero. Which includes, but far from exclusively, the basis vectors $\overline{\boldsymbol{e_k}} * \overline{\boldsymbol{e_l}}$ themselves. Then ask for these relations to hold modulo p^2, p^3 etc: this removes all the variables $\mu'_{i,j,k,l}$ from the system, for those "forced" relations on $\boldsymbol{e_i} * \boldsymbol{e_j}$. In practice this divides by two the dimension of the kernel while the system still yields solutions (actually one solution is enough for us, thanks to our lucky heuristic: see below) In practice, for algebraic geometry codes, this seems to make the number of equations drop from $k(k+1)/2$ to approximately $\dim(C^{*2}) \sim 2k$: see in the examples below.

Observation 24. *For all AG codes that we tried —such as those of Corollary 19, for which a multiplicative lift exists—, then* every solution *of the system* mod p^i *(i.e. a multiplicative lift in $R_i(r)^n$), lifts to a solution* mod p^{i+1}

Thanks to this unexplained fact, we need only solving the system ℓ times to find a multiplicative lift of $\overline{C}$ in $R_\ell(r)$, hence the overall strategy runs in *polynomial time in* n, and *linear in* ℓ.

3.6 Examples of multiplication friendly lifts modulo 2^{100}

The Magma program used to compute the two following examples (among others) is available on [Ano19].

Hermitian curve over $\mathbb{F}_{16}$ Let X_0 be the plane curve over $\mathbb{F}_{16}$ defined by equation $f(x,T) = T^4 + T - x^{4+1}$. Then it is well known that this curve has genus $g = 4(4-1)/2 = 6$ and $n+1 := |X_0(\mathbb{F}_{16})| = 1 + 4^3 = 65$ rational points (which reaches the Hasse-Weil upper-bound). Let us note these points $P_0, \dots, P_n$ (so $n = 64$), consider the divisor $D_0 = 25P_0$, whose Riemann-Roch space $L(D_0)$ is of dimension 20. We define the algebraic geometry code $\overline{C}$ of length $n+1$ defined as evaluations elements of $L(D_0)$ on all the rational points of X_0, *including the support* $\{P_0\}$ of D_0.

Remark. So with the notations of [CC06, §3], we allow in addition to evaluate at Q. We did this to make a little gain on the adversary bound. To be sure, solutions to overcome the problem with evaluating at the support of D_0 are well known. A standard trick would have been to choose instead D_0 equal to one point of degree 25, but this wouldn't fit in our simplistic assumption of Corollary 19, that D_0 is supported on rational points. So we do otherwise and keep $D = 25P_0$, compute t_0 a uniformizing parameter at P_0, and define the evaluation of $f \in L(D_0)$ at P_0 by:

$$(t_0^{23} f)(P_0) \ .$$

The intrinsic meaning of this formula is that we first compute the restriction (called "evaluation", in Theorem 17) of $\mathcal{L}(D_0)$ in a neighborhood of P_0: multiplying $\mathcal{L}(D_0)$ by t_0^{23} maps it to regular functions at P_0. Then we evaluate . The trick yields codes that still satisfy the conditions of Corollary 19 for the existence of finding multiplicative lifts [12]

[12] For the first trick they satisfy Corollary 19 since closed points of arbitrary degree do lift. For the second trick, consider $Z^{(0)}$ a $R_{100}(4)$-point of the lifted curve X

For the sake of illustration notice that, with $t = 13$, we have $\deg D_0 = 2g + t$ so that the condition $39 = 3t < n - 4g = 40$ of [CC06, Proposition 2] is satisfied, thus from $\overline{C}$ we can deduce a secret sharing scheme with strong multiplication for adversary bound $t = 13$.

Before going on, we compute the square code $\overline{C}^2$ and the (a priori larger) AG code associated to $L(2D_0)$, and check that both are equal —as predicted by equality in (7) since $\deg D_0 \geq 2g + 1$ — of dimension $2.25 + 1 - 6 = 45$. From the generating set $(\overline{\boldsymbol{e_i}} * \overline{\boldsymbol{e_j}})_{i \leq j}$ of $\overline{C}^2$ we extract a basis $(\overline{\boldsymbol{e_k}} * \overline{\boldsymbol{e_l}})_{(k,l) \in B}$. We now look at the matrix expressing the $(\overline{\boldsymbol{e_i}} * \overline{\boldsymbol{e_j}})_{i \leq j}$ in terms of this basis (with the previous notations, this is the matrix of the coefficients $\overline{\lambda_{i,j,k,l}}$). It has $(\dim(C)(\dim(C) + 1))/2 = 210$ lines (all ordered pairs $i \leq j$). Obviously the lines where the index (i, j) belongs to B contain a single coefficient, equal to one. And obviously these coefficients will remain equal to one in every lift mod p^ℓ so we can remove these $n \dim \overline{C}^2 = 64 \times 45$ relations (and the corresponding variables) from the system from now on.

Remark. But to our surprise, even when removing these lines from the matrix, the remaining matrix (which we call ”Reduc" in the program) contains many other lines (119, we call their list ”Fixed” in the program) that have also this property to have only one nonzero entry, equal to one. Looking at the global sections in $L(D_0)$ corresponding to these equalities $\overline{\boldsymbol{e_i}} * \overline{\boldsymbol{e_j}} = \overline{\boldsymbol{e_k}} * \overline{\boldsymbol{e_l}}$, we check that these equalities also hold for the underlying functions (which we already knew, since the evaluation map is injective). So, betting on the fact that this simple relations will also hold on the curve lifted over rings, we force these coefficients $\overline{\lambda_{i,j,k,l}} = 1$ to lift to 1 (and likewise the other coefficients on the line to lift to zero). Namely, in all iterations of the linear system $\bmod\ 2^\ell$, we force all the corresponding $\mu'_{i,j,k,l} = 0$, and $\lambda_{i,j,k,l} = 1$ for these special lines. As described in the paragraph “Optimizations” in the previous section, it seems that we still get many solutions to the system after this trick, which yields a significant drop in the number of unknowns in the system (18) .

Also, the rest of the matrix Reduc is also hollow, ($O(1)$ nonzero coefficients per line, from the other examples we tested), thus the overall system (18) is *sparse.*

Finally we end up with a system (18) of 10725 equations with 3305 unknowns but, surprisingly, of (still) very large kernel: dimension 83 (dimension 200 before applying the trick). We solve it in one second on a single processor.

Finally we repeat the operation, following the pattern of the proof of Proposition 23: we reinject the solution (the lifted vectors $\boldsymbol{e_i}$ and coefficients $\lambda_{i,j,k,l}$) in a system $\bmod\ 2^3$ (as in (14)), which is a multiple of 2^2 after simplification, thus falls back to a system mod 2 after “division by 2^2”. Note the general fact that the matrix of the new system obtained is exactly the same as the initial one (18),

above P_0 and t a uniformizing element as in [Wal, Proposition 4.9]. Then t^{23} is by construction the local equation of the lifted Cartier divisor D at the closed point $P^{(0)}$ in $Z^{(0)}$, and reduces to t_0.

because the coefficients depend only on the values modulo 2 of $\overline{\boldsymbol{e_i}}$ and $\overline{\lambda_{i,j,k,l}}$. To which we find again a solution (the mysterious lucky heuristic) —in one second as expected— then repeat exactly 97 times (always the lucky heuristic) to reach a multiplication friendly lift over $R_{100}(4)$.

The ManyPoints.org curve of genus 3 over $\mathbb{F}_{2^5}$ Here we want a comparatively larger adversary threshold so take an extension of $\mathbb{F}_2$ of larger size. Let δ be a root of the polynomial $1+T^2+T^5$ in $\mathbb{F}_2[T]$. Consider the plane curve X_0 over $\mathbb{F}_{2^5}$ defined as follows: let x, y be the affine coordinates, put $X := x^2+x$, $Y := y^2+y$ then X_0 is given by the equation:

$$X^2 + XY + \delta^3 Y^2 + Y + \delta^{26}$$

Its function field has

$$n = 64$$

places of degree one (i.e. a projective smooth model of X_0 would have 64 rational points). Consider the place at infinity $P_0(0, \delta, 1)$ and the divisor $D_0 = 22P_0$ (of degree $2g+16$). The Riemann Roch space $L(D_0)$ has dimension $22+1-3 = 21$, of which Magma can compute a basis E. We construct the AG code $\overline{C}$ obtained by evaluating these basis elements at all the rational points except the support P_0 (this time, avoiding the support doesn't harm the adversary bound).

Here the square $\dim \overline{C^2}$ is of dimension 42, after applying the same "special rows" trick the system contains 10584 equations and 5817 variables, and half of its rows are sparse. Surprisingly it (still) has very large kernel, of dimension 93. This time we solve it in 100 seconds and, thanks again to the lucky heuristic, need only iterating 98 times to finish with a lift mod 2^{100}.

4 Deducing arithmetic secret sharing schemes and MPC protocols with constant communication rate

4.1 Arithmetic secret sharing and reconstruction over rings

The goal of this paragraph is to describe efficient algorithms for secret sharing and decoding with errors for codes which are *good lifts* (which are very simple to construct, if we don't care about multiplicative properties). Recall also that general results for decoding without errors and adversary bound were obtained in §2.4 from the general theory of good lifts.

From multiplicative lifts (Main Theorem 1) to arithmetic secret sharing schemes with strong multiplication and uniformity (Corollary 2) From the elementary theory we can transpose easily over rings the general criterions of [Cas+09, §3-§4] [13] for Massey's secret sharing schemes with strong multiplication and uniformity.

Given a code C in R^{n+1}, suppose that we want to use the 0-th coordinate to store a secret s in R. We only need adapt the requirement of Definition 5 (and accordingly Definition 7) of $\mathcal{C}(R)$ in loc. cit. by asking that

- $(r, 0, \ldots, 0) \notin C$ for any $r \in R$. Notice that when C is a good lift, then this is equivalent to $(1, 0, \ldots, 0) \notin C$ by Theorem 8(i).
- And that $(r, 0, \ldots, 0) \notin C^{\perp}$ for all $r \in R$ —which is equivalent to the existence of a codeword with invertible coordinate at 0-th position. Notice that when C is a good lift, then this is equivalent to $(1, 0, \ldots, 0) \notin C^{\perp}$ by Theorem 8 (i) and (iv).

Recall that we established both *uniformity* of the projection on $d^{\perp}(\overline{C}) - 1$ coordinates (Proposition 15) —hence the adversary threshold satisfies:

$$t \geq d(\overline{C}^{\perp}) - 2 \tag{19}$$

— and, for *good lifts*, the existence of a *linear reconstruction map up to* $d(\overline{C}) - 1$ (Corollary 13). Thus, considering that the Main Theorem 1 provides simultaneous good lifts C, $C^{\perp}$ and C^2 (with asymptotically good parameters), we can construct from them arithmetic secret sharing schemes with *t-uniformity* and *strong multiplication* (efficient reconstruction in C^2 without errors from at least $n - d(\overline{C}^2) + 2$ shares).

Secret sharing protocol

Property 25 (Systematic form). *If C is a good lift then C has a generating matrix in systematic form.*

Proof. Choose a basis $\overline{\mathcal{B}}$ of $\overline{C}$ under which $\overline{C}$ is in systematic form $(\mathrm{Id}_k | \overline{N})$, where $k = \dim(\overline{C})$. Consider any lift $\mathcal{B}$ in C: it is a basis of C by item (ii) of Theorem 8. Its generating matrix is of the form $(\mathrm{Id}_k | N) + (M_1 | N_1)$ where M_1 (and N_1) has coefficients in $\mathfrak{m}$. Notice that the diagonal elements of $(Id_k + M_1)$ are invertible: up to multiplication of the rows by their inverses, one can assume that they are one. Then by elementary row operations, one can finally cancel all the terms outside of the diagonal. □

Algorithm 26 (Secret share). On input $s \in R$ and given $C =< \boldsymbol{e_1}, \ldots, \boldsymbol{e_k} >$ a good lift in R^{n+1} of dimension k in systematic form, do

- Select $\lambda_2, \ldots, \lambda_k$ uniformly at random in R
- Compute the codeword $\boldsymbol{c} = s\boldsymbol{e_1} + \lambda_2 \boldsymbol{e_2}, \ldots, \lambda_k \boldsymbol{e_k}$
- Send the first coordinate c_1 to Player 1, ... , c_n to Player n.

It is straightforward that the procedure above selects uniformly at random a codeword in C conditionned to the 0-th coordinate be equal to s.

[13] We could also recover arithmetic secret sharing over any $\mathbb{Z}/p^{\ell}\mathbb{Z}$ by the descent arguments of Crypto 2009, via multiplication friendly embedding of $R_{\ell}(r)$ into several copies of $\mathbb{Z}/p^{\ell}\mathbb{Z}$. Will not discuss this since we focus here on an adversary threshold close to $n/3$.

Decoding with errors Recall that decoding with errors was described in [Anoa] for the particular case of Reed-Solomon codes. Here we provide a general algorithm for decoding with errors in any code C over any principal ideal local ring (e.g. Galois or p-adic ring), as long as it is a good lift. It uses, as a black box subroutine, any given decoding algorithm for the reduction $\overline{C}$ over the residue field κ:

Proposition 27 (A compiler from error-correction over fields to rings). *Let $\big(R,(p)\big)$ be a principal ideal local ring and C be a code in R^n which is a* good lift. *Then we can compile any decoding algorithm $\overline{\phi}$ for the code $\overline{C}$ over the residue field (up to half of the minimum distance), into an algorithm ϕ for decoding-with-errors in C, with complexity equal to ℓ times the complexity of $\overline{\phi}$, where ℓ is such that $p^\ell = 0$.*

[For p-adic rings we have $\ell = \infty$: the decoding algorithm will return iteratively a solution, where the error term remains on the same support and has smaller and smaller p-adic norm.].

Let us describe informally the decoding algorithm (with justifications inline). Recall that the operation of lifting a codeword $\overline{c} \in \overline{C}$ to C can be done efficiently, thanks to the existence of a generating matrix for C in systematic form (Proposition 25).

Let $\boldsymbol{c} \in C$ be an unknown codeword, $\boldsymbol{e} \in R^n$ an error term with weight $< \overline{d}/2$ and $\boldsymbol{u} = \boldsymbol{c} + \boldsymbol{e}$ the corrupted codeword to be decoded. Repeat the following procedure:

- Decode $\overline{\boldsymbol{u}}$ into $\overline{\boldsymbol{c}}$ and deduce $\overline{\boldsymbol{u}} - \overline{\boldsymbol{c}} = \overline{\boldsymbol{e}}$.
- Choose any lift $\boldsymbol{c_1} \in C \pmod{p^2}$ of $\overline{\boldsymbol{c}}$ and $\boldsymbol{e_1} \in (R/p^2)^n$ any lift of $\overline{\boldsymbol{e}}$ with same support.
- Compute the difference $\boldsymbol{u} - (\boldsymbol{c_1} + \boldsymbol{e_1})$ modulo $(p)^2$: it is equal to
$$(\boldsymbol{c} - \boldsymbol{c_1}) + (\boldsymbol{e} - \boldsymbol{e_1})$$
where the left term is by construction a codeword in $C \cap (R/p^2)^n$, and thus in pC by Theorem 8 (i): let us call it $p\boldsymbol{c_2}$. Whereas the right term is in pR^n with at most the same support as $\overline{\boldsymbol{e}}$ (so $< \overline{d}/2$ nonzero coordinates): let us call it $p\boldsymbol{e_2}$.
- the difference computed is thus of the form $p\boldsymbol{u_1}$: dividing by p (that is: choosing any preimage under the multiplication by p) we obtain the equation modulo p
$$\boldsymbol{u_1} = \boldsymbol{c_2} + \boldsymbol{e_2}$$
- Apply the decoding algorithm to $\boldsymbol{u_1}$, deduce $\boldsymbol{c_2}$ and $\boldsymbol{e_2}$, lift them arbitrarily in $C \mod p^3$ and in $(R/(p^3))^n$ etc.

As an alternative, one could possibly lift over any local ring the generic decoding algorithm in [CDN15, §12.5.4].

4.2 Lifting Crypto 2018's alternative to hyperinvertible matrices for Beerliova-Hirt multiple random share

The arguments in Crypto 2018 §2.4 carry over local rings:

- $d^{\perp} - 1$ coordinates of a random codeword are uniformly distributed, by Proposition 15.
- linear recoverability from $2n - d + 1$ coordinates follows from Corollary 13
- The existence of a systematic form follows from Proposition 25.

4.3 Consequence for amortized MPC: Main Theorem 3

Main Theorem 3 follows from the elementary protocols above, including the alternative to Beerliova-Hirt, applied to the following secret sharing schemes over rings. Recall first the tradeoff of [CC06, §5] for secret sharing in finite fields $\mathbb{F}_p$. Let us cast a secret in $\mathbb{F}_p$, into the extension $\mathbb{F}_{p^r}$ of degree r, such that

$$p^r \geq 49 \; .$$

Then for adversary threshold $1/3 - \epsilon$, and for infinitely many number of players, there exists a secret sharing scheme over $\mathbb{F}_{p^r}$ with strong multiplication and constant size of shares, such that:

$$\epsilon < \frac{4}{3(p^{r/2} - 1)} \; ,$$

[CC06, §5] In particular, choosing $\widehat{r}(\epsilon) = -2\log(\epsilon)$ yields an adversary bound $1/3 - \epsilon$ when ϵ is sufficiently small. Taking a good lift of the underlying AG code and its (good) square over $R_\ell(r)$ —as provided by Corollary 19 and efficiently computed as above— yields the same adversary and reconstruction bounds, for the same constant communication overhead $\widehat{r}(\epsilon)$, so we have exactly the same parameters as in [CC06, §5].

5 Efficient constant rate lifts of reverse multiplication friendly embeddings (RMFE) and application to amortized MPC (Main theorem 4)

5.1 Definition and main result

Reverse multiplication friendly embeddings were introduced in [Cas+18, Definition 1]. They are the main tool for emulating several circuits in parallel over small finite fields $\mathbb{F}_p$, from a single circuit over a large extension $\mathbb{F}_{p^m}$. Let us adapt the definition over the rings $R_\ell = \mathbb{Z}/p^\ell\mathbb{Z}$, for sake of simplicity, and their extensions $R_\ell(m)$.

Definition 28. Let p be a prime and r a positive integer, let $k,\ n \geq 1$ be integers. A pair (ϕ, ψ) is called an $(k, m)_r$ -reverse multiplication friendly embedding (RMFE for short) iff $\phi : R_\ell^k \to R_\ell(m)$ and $\psi : R_\ell(m) \to R_\ell^k$ are two R_ℓ-linear maps satisfying

$$x * y = \psi(\phi(x)\phi(y))$$

for all $x, y \in R_\ell^k$.

The *existence* of RMFE over rings with the same rate than the algebraic-geometry construction in [Cas+18, Theorem], also follows from Theorem 1.

Theorem 29. *There exists a family of $(k, m)_q$-RMFE with $k \to \infty$ and $m = O(k)$. More concretely*

$$4m \to 2 + \frac{k}{A(q)}$$

Namely, following the construction done in the proof of loc. cit.: lift the curve and the Riemann-Roch spaces $L(D)$, and use Theorem 17 that states that Riemann-Roch spaces are good lifts. In particular, Riemann Roch spaces over rings arising from a divisor of strictly negative degree, e.g. the kernel of an evaluation map $L(G-R)$, are still equal to $\{0\}$ (see also the last sentence of §3.2).

5.2 An analogous linear system to efficiently lift RMFE

The definition of a *reverse multiplication embedding* of $\mathbb{F}_p^k$ (for sake of simplicity) into $\mathbb{F}_{p^m}$ may be rephrased as follows: Consider the multiplication tensor T in $\mathbb{F}_{p^m}$, its components $T_{i=1..m}$ are $\mathbb{F}_p$-bilinear forms from $\big(\mathbb{F}_{p^m} \times \mathbb{F}_{p^m}\big)$ to $\mathbb{F}_p$. Now fix a linear map

$$\phi : \mathbb{F}_p^k \longrightarrow \mathbb{F}_{p^m}$$

The pull back of T :

$$\phi^* T = T(\phi(.), \phi(.))$$

decomposes in $\mathbb{F}_{p^m}$ in m components which are symmetric bilinear forms

$$\phi^* T_i = T_i(\phi(.), \phi(.)) \ , i = 1..m$$

in the symmetric tensor space $S^2((\mathbb{F}_p^k)^*)$.

Definition 30. We say that ϕ is a reverse multiplication embedding iff these m bilinear forms $\phi^* T_i$ generate the components $(x_1^* \otimes x_1^*, ...x_k^* \otimes x_k^*)$ of the componentwise multiplication tensor in the (nonintegral) algebra $(\mathbb{F}_p)^k$.

Lifting of an algorithm ϕ modulo p^2: Suppose we are given a reverse multiplication friendly embedding ϕ, over $\mathbb{F}_p$ ($r = 1$ to make notations simple): for each $j = 1 \dots k$, we have coefficients $\lambda_{i,j}$ such that:

$$x_j^* \otimes x_j^* = \sum_{i=1}^{m} \lambda_{i,j} . \phi^* T_i \tag{20}$$

(it is a tensorial equality: it takes place in the space of symmetric bilinear forms of length k, so expands on coordinates as a set of $k(k+1)/2$ equations). We want to lift ϕ and the coefficients $\lambda_{i,j}$ such that the equalities (20) hold modulo p^2. (So we have $mk + mk$ unknowns and m equations, each of them taking place in a symmetric tensor space of dimension $k(k+1)/2$). Consider arbitrary lifts ϕ' and $\lambda'_{i,j}$ of ϕ and $\lambda_{i,j}$ over $\mathbb{Z}/p^2\mathbb{Z}$, we thus obtain the (tensorial) equalities modulo p^2 for $j = 1..k$:

$$x_j^* \otimes x_j^* = \sum_{i=1}^{m} \lambda'_{i,j} \phi'^* T_i + p\Delta_j$$

and we would like to eliminate the error terms $p\Delta_j$ modulo p^2 by choosing better lifts of ϕ and of $\lambda_{i,j}$:

$$\phi' + p\psi \text{ and } \lambda'_{i,j} + p\mu_{i,j} \tag{21}$$

After replacing (21) in (20) then simplification, the equation becomes the following (tensorial) *linear* equation modulo p (so with coordinates in $\mathbb{F}_p$):

$$\sum_{i=1}^{m} 2\lambda'_{i,j} T_i\big(\phi'(.), \psi(.)\big) + \mu'_{i,j} T_i\big(\phi'(), \phi'_i(.)\big) = -\Delta_j$$

where the unknowns are ψ and $\mu'_{i,j}$.

We will not state and prove that the previous systems returns all lifts modulo p^2, as it is very similar to Proposition 23, nor will we discuss again how to repeat and compute higher lifts modulo p^ℓ [14].

5.3 Consequence for amortized MPC: Main Theorem 4

From the existence of RMFE with constant rate over rings as shown above (which we also showed are efficiently computable), we can now compile a protocol for a circuit over a large Galois ring $R_\ell(r)$, into a protocol for many evaluations in parallel of this circuit in $\mathbb{Z}/p^\ell\mathbb{Z}$ by casting over rings the protocols of [Cas+18]. This could be applied to Main Theorem 3. But here in Main Theorem 4 we choose to restrict ourselves to the case of optimal adversary rate. So we really need hyperinvertible matrices over Galois rings for any number of players (not the previously discussed alternative with suboptimal adversary bound as used

[14] Let us notice that a generic argument of Forney's PhD thesis, that proves the existence of a polynomially constructible family of codes matching the Zyablov bound (i.e. optimal concatenated codes), could be instantiated to RMFE (but *not* to codes with both small $d^\perp(C)$ and small $d(C^2)$). The argument is recalled e.g. in [PW15, §24.4] (or [GI05]), and consists in concatenating an ”inner“ good code, found via exhaustive search, with an ”outer“ Reed-Solomon code. This idea was also applied to MFE in [Ram15]: in Table 2, $\mu_4(1,4)$ and $\mu_4(1,5)$ are found via exhaustive search. Here, one would apply concatenation Lemma 5 of [Cas+18] and perform exhaustive search over (ϕ_2, ψ_2), then concatenate with a Reed-Solomon RMFE as in [Cas+18, Remark 7].

in Main Theorem 3). Their existence will be detailed in a leter work. . We can thus cast the original protocol of Beerliova-Hirt over Galois rings, then compensate their bad asymptotic communication overhead by amortizing it over several instances in parallel, exactly as done in [Cas+18, Theorem 1 & 2], which thus yields our Main Theorem 4.

References

[Anoa] Anonymous. “Efficient Information-Theoretic Secure Multiparty Computation over $\mathbb{Z}/p^\ell\mathbb{Z}$ via Galois Rings”. Companion paper.

[Anob] Anonymous. “Elementary Lifting of Arithmetic Secret Sharing over Finite Fields to Local Rings, Its Limitations and Its Applications”. Companion paper.

[Ano19] Anonymous. *Magma program for multiplicative lifts of AG codes.* 2019.

[AZ18] C. Bachoc A. Couvreur and G. Zémor. “towards a function field version of Freiman’s Theorem”. In: *Algebraic Combinatorics* (2018).

[BLW08] Dan Bogdanov, Sven Laur, and Jan Willemson. “Sharemind: A Framework for Fast Privacy-Preserving Computations”. In: *ESORICS 2008*. Ed. by Sushil Jajodia and Javier Lopez. Springer, 2008.

[Cas+09] Ignacio Cascudo et al. “Asymptotically Good Ideal Linear Secret Sharing with Strong Multiplication over Any Fixed Finite Field”. In: *Advances in Cryptology - CRYPTO 2009*. Springer, 2009.

[Cas+18] Ignacio Cascudo et al. “Amortized Complexity of Information-Theoretically Secure MPC Revisited”. In: *Advances in Cryptology - CRYPTO 2018*. Springer, 2018, pp. 395–426.

[CC06] Hao Chen and Ronald Cramer. “Algebraic Geometric Secret Sharing Schemes and Secure Multi-Party Computations over Small Fields”. In: *Advances in Cryptology - CRYPTO 2006*. Springer, 2006.

[CDM00] Ronald Cramer, Ivan Damgård, and Ueli Maurer. “General Secure Multi-party Computation from Any Linear Secret-sharing Scheme”. In: *Proceedings of the 19th International Conference on Theory and Application of Cryptographic Techniques*. EUROCRYPT’00. 2000.

[CDN15] Ronald Cramer, Ivan Damgård, and Jesper Buus Nielsen. *Secure multiparty computation : an information-theoretic approach*. Cambridge University Press, July 1, 2015.

[Cra+03] Ronald Cramer et al. “Efficient Multi-party Computation over Rings”. In: *Advances in Cryptology — EUROCRYPT 2003*. Springer Berlin Heidelberg, 2003.

[Cra+18] Ronald Cramer et al. “SPD$\mathbb{Z}_{2^k}$: Efficient MPC mod 2^k for Dishonest Majority”. In: Lecture Notes in Computer Science (2018).

[Dam+06] Ivan Damgård et al. “Unconditionally Secure Constant-Rounds Multiparty Computation for Equality, Comparison, Bits and Exponentiation”. In: *Theory of Cryptography*. Springer, 2006.

[Dam+12] Ivan Damgård et al. "Multiparty Computation from Somewhat Homomorphic Encryption". In: *Advances in Cryptology – CRYPTO 2012*. Springer Berlin Heidelberg, 2012.

[Dam+19] Ivan Damgård et al. "New Primitives for Actively-Secure MPC mod 2^k with Applications to Private Machinen Learning". In submission. 2019.

[FY92] Matthew Franklin and Moti Yung. "Communication Complexity of Secure Computation (Extended Abstract)". In: *Proceedings of the Twenty-fourth Annual ACM Symposium on Theory of Computing*. STOC '92. ACM, 1992.

[GI05] V. Guruswami and P. Indyk. "Linear-time encodable/decodable codes with near-optimal rate". In: *IEEE Transactions on Information Theory* (2005).

[Ill05] Luc Illusie. "Grothendieck's existence theorem in formal geometry". In: *Fundamental Algebraic Geometry: Grothendieck's FGA Explained*. Ed. by AMS. Mathematical Surveys and Monographs vol. 123. AMS, 2005.

[Ish+07] Yuval Ishai et al. "Zero-knowledge from Secure Multiparty Computation". In: *Proceedings of the Thirty-ninth Annual ACM Symposium on Theory of Computing*. STOC '07. ACM, 2007.

[Mum11] David Mumford. "Varieties Defined by Quadratic Equations". In: *Questions on Algebraic Varieties*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2011, pp. 29–100.

[NW17] Anand Kumar Narayanan and Matthew Weidner. "Nearly linear time encodable codes beating the Gilbert-Varshamov bound". In: *CoRR* (2017). URL: `http://arxiv.org/abs/1712.10052`.

[PW15] Y. Polyanskiy and Y. Wu. *Lecture notes on information theory*. version of 2017, Aug. 29. 2015.

[Ram15] Matthieu Rambaud. "Finding Optimal Chudnovsky-Chudnovsky Multiplication Algorithms". In: *Arithmetic of Finite Fields*. See errata on the author's webpage. Springer, 2015.

[SGA1] Alexander Grothendieck. *Revêtements étales et groupe fondamental (SGA 1)*. Lecture Notes in Math., 224. 1960-61, with two papers by M. Raynaud. Springer-Verlag, Berlin, 1964.

[Sta18] The Stacks project authors. *The Stacks project*. `https://stacks.math.columbia.edu`. 2018.

[Wal] Judy Walker. "Algebraic geometry codes over rings". PhD thesis. Univ Illinois Champain.

[Wal99] Judy L. Walker. "Algebraic geometric codes over rings". In: *Journal of Pure and Applied Algebra* 144.1 (1999), pp. 91–110.

A Formulas for the toy example

$$\begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 2Dt^2+3Dt+2 & Dt+2 & Dt^2+2Dt & 3Dt^2+2Dt+2 & Dt+3 & Dt+1 & Dt^2+3Dt & 3Dt^2+Dt & Dt^2+Dt+1 & 3Dt^2+Dt+3 & 3Dt^2+1 & 3Dt^2+3 & 1 \\ Dt^2 & Dt^2 & 3Dt^2+3Dt & 3Dt^2+3Dt & Dt^2+2Dt+1 & Dt^2+2Dt+1 & Dt+2 & Dt+2 & 2Dt^2+3Dt+3 & 2Dt^2+3Dt+3 & Dt^2+3Dt+1 & Dt^2+3Dt+1 & 1 \\ 1 & Dt & 1 & Dt^2 & Dt^2 & Dt^2+Dt & 1 & Dt^2+Dt & Dt & Dt^2 & Dt & Dt^2+Dt & 0 \end{bmatrix}$$

$$transp\Big((\lambda_{2,2,k,l})_{k,l\in B},(\lambda_{4,4,k,l})_{k,l\in B}\Big)=\begin{bmatrix} 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 1 & 2 & 0 \end{bmatrix}$$

B Detailed proof with formal lifts of curves—from more elementary arguments, and projective limits of codes

B.1 Lifting smooth projective curves and algebraic geometry codes over local rings

Let us furthermore assume from now on that R *is noetherian.* Let $S = \operatorname{Spec} R$ be the corresponding affine scheme, we call *smooth projective curve over* S an irreducible scheme X with a smooth projective morphism $f : X \to \operatorname{Spec} S$ of relative dimension one [f being flat, Lemma [Sta18, 0AFE] implies that $\dim X = \dim R + 1$. So $\dim X = 2$ (an "arithmetic surface") if R is a DVR, and $\dim X = 1$ if R is a local Artinian ring].

Let us fix $(A, \mathfrak{m}, \kappa)$ a local noetherian ring (although A is "morally" the complete ring $\mathbb{Z}_p$ or $W(\mathbb{F}_q)$, the assumptions for A are actually the same as for the "generic" local noetherian ring R considered throughout, the completeness assumption being not necessary until the appendix). Consider the projective system of local Artinian rings:

$$\dots A_3 \to A_2 \to A_1 \to A_0 = \kappa \ ,$$

where $A_i = A/\mathfrak{m}^{i+1}$ and each arrow $A_{i+1} \to A_i$ is the reduction modulo $\overline{\mathfrak{m}^{i+1}}$. This corresponds to a direct system of affine schemes:

$$\operatorname{Spec} \kappa = S_0 \to S_1 \to S_2 \to S_3 \to \dots \ ,$$

where each arrow $S_i \to S_{i+1}$ is a closed immersion defined by the ideal $\overline{\mathfrak{m}^{i+1}}$ of square zero. Let X_0 be any flat scheme over $\operatorname{Spec} \kappa = S_0$, then a *formal lift* $\mathfrak{X}$ of X_0 over this direct system is the data of flat schemes X_i over each S_i, fitting into an infinite diagram where all squares are cartesian:

(22)
$$\begin{tikzcd}
X_0 \arrow[r, "j_0"] \arrow[d, "f_0"'] & X_1 \arrow[r, "j_1"] \arrow[d, "f_1"'] & X_2 \arrow[r, "j_2"] \arrow[d, "f_2"'] & \cdots \\
S_0 \arrow[r] & S_1 \arrow[r] & S_2 \arrow[r] & \cdots
\end{tikzcd}$$

In particular the X_i form a direct system and, by base-change, the maps $j_i : X_i \to X_{i+1}$ are closed immersions. They are given locally on $\operatorname{Spec} B_{i+1}$ by the ideal $\mathfrak{m}^{i+1} B_{i+1}$ of square zero .

Our principal addition to [Wal99], which studies reduction of AG codes over rings, is that we notice the possibility to go in the other direction:

Theorem 31 (Formal lifts of curves[15] ***[SGA1, III Theorem 6.3] or [Ill05, proof of 5.19 (i)]).*** *Let $(A, \mathfrak{m})$ be a local ring and consider X_0 a smooth projective curve over $S_0 = \operatorname{Spec} \kappa$, then X_0 admits a formal lift $\mathfrak{X}$ over the direct system $S_0 \to S_1 \to S_2 \to \cdots$. Moreover $\mathfrak{X}$ is projective.*

[15] About references: of course the clearest is https://amathew.wordpress.com/2011/06/18/lifting-smooth-curves-to-characteristic-zero/ . The small missing point is that he actually doesn't prove how to obtain a compatible system of lifts in Corollary 9, he only

Proof. Only the last point, about projectivity, is not stated in the references mentionned in the theorem. It is stated in the full FGA's existence theorem ([Ill05, Theorem 5.19 (ii)] or [SGA1, III Théorème 7.3]). But it can also be showed directly, as in the proof of [Ill05, Theorem 8.4.10], where a very ample sheaf on X_0 is lifted to each X_i by Nakayama.

Coming back to our generic (noetherian) local ring R and X a smooth projective curve over $S = \operatorname{Spec} R$, let us define an *$R$-point* of X as an S-morphism $Z : S \to X$.

Noting s the closed point of S and $Z(s)$ its image in X, one can prove that Z defines a regularly embedded subscheme of codimension one, which is contained in any sufficiently small affine neighborhood $U = \operatorname{Spec} B$ of $Z(s)$, and thus is a Cartier divisor (also noted Z) defined by:

$$\big\{(U, b), (1 \text{ outside of } Z(S))\big\}$$

where b is a suitable non-zero divisor in B. But actually for practical purposes (Main Theorem 1) we will only need the case where R is Artinian, whence Z is just a closed embedding to one closed point $Z(s)$: see [Wal99, Lemma 4.4], and Lemma 34 for the general case.

Thus in the situation of Theorem 31, the smooth morphisms $X_{i+1} \to S_{i+1}$ being in particular formally smooth, it is possible to lift any A_i-point Z_i on X_i to an A_{i+1}-point Z_{i+1} on X_{i+1} with compatibility relations. This boils down to [Wal99, Remark 4.5], see Proposition 36 below over general (local) rings. From here, d being any positive integer and $\mathcal{L}_i = [Z_i]^{\otimes d}$ (or $\mathcal{O}(d.Z_i)$) the line bundle class corresponding to the Cartier divisor $d.Z_i$, we immediatly deduce a lift $\mathcal{L}_{i+1} = [Z_{i+1}]^{\otimes d}$ of $\mathcal{L}_i$. [16] The key point is that *the line bundles surject to each other* in a compatible way with the projective system of rings. More precisely, considering affine open subsets where the line bundles become principal fractional ideals, we see that for each i the identity map on $\mathcal{O}_{X_i}$ induces the isomorphism of line bundles:

$$\mathcal{O}_{X_i} \otimes_{\mathcal{O}_{X_{i+1}}} \mathcal{L}_{i+1} \to \mathcal{L}_i \tag{23}$$

from which we deduce in particular the isomorphisms for all i:

$$\mathcal{O}_{X_0} \otimes_{\mathcal{O}_{X_i}} \mathcal{L}_i \to \mathcal{L}_0 \tag{24}$$

shows that X_0/k lifts to X_1/A_1. The trick that makes it possible is [Ill05, Remark 5.10 (b)] (see also [SGA1, p61]), which boils down to the standard base change formula for modules of differentials: let B be an A-algebra and $A \to A'$ a morphism of rings (here B is an affine subset algebra of X_{i+1}, $A = A_{i+1}$ and $A' = A_i$), then $A' \otimes \Omega_{B/A} = \Omega_{A' \otimes B/A'}$. We also mention that smoothness criterion [Ill05, 5.8 (ii)] is false and should be replaced by [SGA1, §II 1.1 & 4.8]. Hartshorne's Deformation theory, Corollary 10.3 recovers the result by more machinery (T functors).

[16] Notice also that it is actually possible to lift any line bundle, by [Ill05, §5.2] (see also Lemma 11 of Akhil Matthews' blog), although for our purpose it is enough to lift points, as we just did.

Finally, starting from a line bundle $\mathcal{L}_0 = [Z_0^{(0)}]^{\otimes d}$ on X_0 along with n distinct points of degree one $Z_0^{(1)}, \dots, Z_0^{(n)}$ outside of $Z_0^{(0)}$, defining a κ-linear evaluation code C_0, then we can lift this data to all X_i/S_i in a compatible way (the points and the line bundles embed/surject to each other), and obtain A_i-linear evaluation codes C_i of length n (see the explicit description of AG codes over Artinian rings at the beginning of [Wal99, §5]). What then remains to be shown is that these evaluation codes *reduce* to each other in a compatible way.

Theorem 32 (Projective systems of lifts of Riemann-Roch spaces and AG codes). *Consider the same situation as above: $\mathcal{L}_0$ any line bundle over X_0, n closed points $Z_0^{(j)}$, $j = 1 \dots n$ on X_0 and the evaluation map γ_0 yielding an algebraic geometry code. Then this data lifts to every X_i, such that we have the following commutative diagram:*

(25)
$$\begin{tikzcd}
\Gamma(X_{i+1}, \mathcal{L}_{i+1}) \arrow[r, twoheadrightarrow] \arrow[d] & \Gamma(X, \mathcal{L}_{i+1}) \otimes_{A_{i+1}} A_i \arrow[r, "\sim"] & \Gamma(X_i, \mathcal{L}_i) \arrow[d] \\
\oplus_j \Gamma(Z_{i+1}^{(j)}, \mathcal{L}_{i+1}|_{Z_{i+1}^{(j)}}) \arrow[d, "\gamma_{i+1}"] & & \oplus_j \Gamma(Z_i^{(j)}, \mathcal{L}_i|_{Z_i^{(j)}}) \arrow[d, "\gamma_i"] \\
A_{i+1}^n \arrow[rr, "\bullet \otimes_{A_{i+1}} A_i"] & & A_i^n
\end{tikzcd}$$

Where: - the top left horizontal arrow and the bottom horizontal arrow are tensorisation by $\otimes_{A_{i+1}} A_i$ - the top right arrow is constructed canonically as in [Wal99, Lemma 4.6 & proof of Th 4.7]

- the top vertical arrows are the canonical restriction maps, - the bottom left vertical arrow arizes from choices of isomorphisms for all j:

$$\gamma_{i+1} : \Gamma(Z_{i+1}^{(j)}, \mathcal{L}|_{Z_{i+1}^{(j)}}) \to A_{i+1}$$

under the (recursive) condition that it induces the bottom right isomorphism γ_i by tensorisation by $\otimes_{A_{i+1}} A_i$.

Proof. The lifting of $\mathcal{L}_0$ and of the points follows from the discussion above the theorem.

The proof that the top right arrow is an isomorphism is mutatis mutandis the arguments in [Wal99, Lemma 4.6 & proof of Th 4.7].

Maybe should I also explain how to obtain such a lift of γ_i for the bottom left vertical arrow.

Corollary 33 (Good lifts of AG codes). *The codes C_i form a projective system of codes, more precisely we have surjections for all i:*

(26)
$$C_{i+1} \twoheadrightarrow C_{i+1} \oplus_{A_{i+1}} A_i \cong C_i$$

Moreover the codes C_i are all free of rank $\dim C_0$ and thus good lifts of C_0:

(27)
$$\pi(C_i) = C_0$$

thus their projective limit $\hat{C} = \varprojlim C_i$ over $\widehat{A}$ is also a good lift of C_0.

Proof. The proof for (26) being the same as [Wal99, Theorem 5.5], let us describe it quickly.

The freeness and equality of ranks follows from [Wal99, Th 5.4], thus they are good lifts by definition, whence (27) (this is exactly the argument of [Wal99, Th 5.7]).

For the last assertion, the projective limit being an additive functor, it preserves direct summands so sends good lifts to good lifts. □

C Realizing the projective limit of codes as an AG code, thanks to the existence theorem

The following lemma states that [Wal99, Lemma 4.4] also holds over any local ring R, and that the situation is equally explicit.

Lemma 34. *An R-point is a regular immersion of codimension one. There exists a unique, well defined Cartier divisor (which we will also denote by Z) associated to Z. Furthermore let s be the closed point of S and $Z(s)$ be its (closed) image in X, then Z factors through a closed immersion in $\operatorname{Spec} \mathcal{O}_{Z(s)}$ followed by the open immersion in X. Thus there exists an affine neighborhood $U = \operatorname{Spec} B$ of $Z(s)$ and a regular element $b \in B$ such that $Z = \big\{(U, b), (1 \text{ outside of } Z(S))\big\}$.*

Proof. We firstly prove that the image of Z is contained in any (affine) neighborhood of $Z(s)$. Let $\operatorname{Spec} B$ be any affine neighborhood of the image $Z(s)$ in X, then $Z^{-1}(\operatorname{Spec} B)$ is an open subset of S containing s so is the whole S .

Let us now show that Z defines a closed immersion in $\operatorname{Spec} B$, which implies in particular that the image $Z(s)$ is a closed point. Let us restrict to $\operatorname{Spec} B$ the structural morphism $f : X \to S$, we now have the corresponding morphisms of rings $R \xrightarrow{f^\sharp} B \xrightarrow{Z^\sharp} R$ which by assumption compose to the identity of R. Thus in particular $Z^\sharp : B \to R$ is surjective.

Let us finally show the Cartier divisor description of Z. Z being an immersion, it is furthermore regular by [SGA1, II Corollaire 4.16]. In particular its ideal $I_{Z(s)} \subset \mathcal{O}_{Z(s)}$ is generated by a regular sequence. Let us remind why the codimension d —i.e. the size of this regular sequence— is one. The local ring $\mathcal{O}_{Z(s)}$ being noetherian, we have:

$$\dim R = \dim \mathcal{O}_{Z(s)}/I_{Z(s)} = \dim B - d = \dim R + 1 - d \ ,$$

where the second equality follows from [Sta18, 00KW] (see also [Liu], theorem 2.5.15) . All the other closed points of X being outside of $Z(S)$, Z is defined by 1 there. Thus by [Sta18, 00NX (5)] the sheaf of ideals of Z is locally free of rank one. The claimed description of Z follows by choosing a sufficiently small open affine neighborhood $U = \operatorname{Spec} B$ of $Z(s)$ and such that a regular generator b_B of $I_{Z(s)} \subset \mathcal{O}_{Z(s)}$ is a regular element of B. □

Theorem 35 (the existence theorem [Ill05, Theorem 5.19 (ii)] or [SGA1, III Corollaire 7.4]). *Under the assumptions of Theorem 31, if furthermore $A = \widehat{A}$ is* complete *(e.g. $\mathbb{Z}_p$ or more generally $W(\mathbb{F}_q)$), there exists a smooth projective curve X over $S = \operatorname{Spec} \widehat{A}$ that lifts X_0/S_0.*

Proposition 36 (Lifts of points). *Under the assumptions of Theorem 31, let $Z_0 : A_0 \to X_0$ be a A_0-point of X_0, then there exists a compatible direct system of A_i-points of X_i lifting Z_0. Namely we have a family of A_i-points $(Z_i)_i$ such that, noting j_i the closed immersion given by Theorem 31, then the following diagrams commute:*

(28)
$$\begin{tikzcd}
& X_i \arrow[rr, "j_i"] & & X_{i+1} \\
S_i \arrow[ur, "Z_i"] \arrow[rr] & & S_{i+1} \arrow[ur, "Z_{i+1}"] &
\end{tikzcd}$$

Proof. By induction, let us deduce Z_{i+1} assuming the existence of Z_i. Consider the composite map:

$$g_i : S_i \xrightarrow{Z_i} X_i \xrightarrow{j_i} X_{i+1} \ ,$$

which by Theorem 31 fits into the following commutative diagram:

(29)
$$\begin{tikzcd}
& & X_{i+1} \arrow[d] \\
S_i \arrow[r] \arrow[urr, "g_i"] & S_{i+1} \arrow[r, "\mathrm{id}"] \arrow[ur, dotted, "?"] & S_{i+1}
\end{tikzcd}$$

The vertical arrow being smooth and the bottom left arrow being a closed immersion of Artinian local rings defined by an ideal of square zero, [SGA1, III Th 3.1 (iii)] provides the existence of a dotted arrow Z_{i+1}, which is indeed a R_{i+1}-point making (28) commute. □

Under the assumptions of Theorem 35 we can also lift S_0 points of X_0 to S-points of X, this time as a consequence of [SGA1, III Th 3.1 (ii)]. Indeed as noticed in the proof of Lemma 34, any affine neighborhood of the closed point of S is actually the whole S.

Lifting n on X_0 points and a line bundle (of the form $O_{X_0}(dZ_0)$), we obtain an AG code C on X the smooth projective curve of 35. One can see that C surjects in a compatible way to the projective system of Corollary 33.

Remark. One can also show directly that C is a good lift of C_0. Indeed, we need only show the saturation criterion of Proposition 8 (i): if a codeword w in C is a multiple of $p : w = pw_1$ then w_1 is also a codeword of C . To prove this, use that all local rings in X are UFD (because X is smooth over the regular local ring R).

Question 1. So it would be very nice to find a counterexample of code C over a non smooth curve over $\mathbb{Z}_p$ (or Witt), such that C is not saturated (= the criterion that we just checked).

D Proof of Theorem 18: extending Mumford's normal generation criterion over any field

The following theorem is stated in [Mum11, Theorem 6] over any algebraically closed field. The goal of this section is to deduce that the theorem holds over any field, which is exactly the statement of Theorem 18 (formulated with function fields, see e.g. [AZ18, Theorem 6.1]).

Theorem 37. *Let X be a smooth projective curve over an algebraically closed field k. Let $\mathcal{L}$ and $\mathcal{M}$ be invertible sheaves on X, such that $\deg \mathcal{L} \geq 2g+1$ and $\deg \mathcal{M} \geq 2g$. Then the morphism*

$$\Gamma(\mathcal{L}) \otimes \Gamma(\mathcal{M}) \longrightarrow \Gamma(\mathcal{L} \otimes \mathcal{M})$$

is surjective.

Lemma 38. *Let k be a field, $k \subset K$ a field extension, X a variety over K and $f : X_K \to X$ the K-variety deduced from X by base-change. Let $\mathcal{F}$ be a sheaf of k-algebras over X (for example an invertible sheaf) and let $\mathcal{F}_K = f^{-1}\mathcal{F} \otimes_k K$ be its pull-back over X_K — where K is the constant sheaf over X_K. Then the morphism*

$$\Gamma(\mathcal{F}) \otimes_k K \longrightarrow \Gamma(\mathcal{F}_K)$$

is an isomorphism.

Let us first admit the lemma and prove Theorem 18. Let K be the algebraic closure of k. The property of being a proper —resp. smooth— morphism being stable by base change, the variety X_K is still proper and smooth over K. Mumford's Theorem 37, applied to the variety X_K and to the pulled-back sheafs $\mathcal{L}_K$ and $\mathcal{M}_K$, thus states that the morphism:

$$\Gamma(\mathcal{L}_K) \otimes \Gamma(\mathcal{M}_K) \longrightarrow \Gamma(\mathcal{L}_K \otimes \mathcal{M}_K)$$

is surjective. By the lemma, one can move out the $\otimes_k K$ from both from the right hand and left hand sides. The surjection therefore reads itself as:

$$\Gamma(\mathcal{L}) \otimes \Gamma(\mathcal{M}) \otimes_k K \longrightarrow \Gamma(\mathcal{L} \otimes \mathcal{M}) \otimes_k K.$$

But K being a k-vector space, it is faithfully flat, hence the theorem.

Let us now prove the lemma. Let $\rho_{UV} : \mathcal{F}(U) \to \mathcal{F}(V)$ the restriction morphisms of the sheaf $\mathcal{F}$. By definition, $\mathcal{F}_K$ is the sheaf associated to the following presheaf over X_K, whose sections over any open set U are the $\mathcal{F}(U) \otimes_k K$ and the restrictions equal to the $\rho_{UV,K} = \rho_{U,V} \otimes_k K : \mathcal{F}(U) \otimes_k K \to \mathcal{F}(V) \otimes_k K$.

Let us thus consider $\tilde{s}$ a section of $\mathcal{F}_K$. It consists in the data of a finite open covering $(U_i)_i$ of X_K, and of a collection of sections $\tilde{s_i} \in \mathcal{F}(U_i) \otimes_k K$ compatible between each other by the restriction maps $\rho_{UV,K}$. Explicitly, let U_i and U_j be two open sets. Let us abridge ρ_i and ρ_j the restriction morphisms $\rho_{U_i,\, U_i \cap U_j}$ and

$\rho_{U_j, U_i \cap U_j}$. Let us express the sections under the form of finite sums of elementary tensors:

$$\tilde{s_i} = \sum_{p \in P} m_p^i \otimes \lambda_p^i$$

$$\tilde{s_j} = \sum_{q \in Q} m_q^j \otimes \lambda_q^j \ ,$$

where P and Q are finite sets of indices, the $(\lambda_p^i)_p$ and $(\lambda_q^i)_q$ are elements of the field K, and the m_p^i (resp. m_q^j) sections of $\mathcal{F}(U_i)$ (resp. $\mathcal{F}(U_j)$). The glueing condition for the open sets U_i and U_j, noted (ij), is

$$\text{(ij)} \qquad \big(\rho_i \otimes_k K\big)\big(\sum_{p \in P} m_p^i \otimes \lambda_p^i\big) = \big(\rho_j \otimes_k K\big)\big(\sum_{q \in Q} m_q^j \otimes \lambda_q^j\big) \ .$$

Let $k \subset L \subset K$ a finite extension of k, large enough to contain all the coefficients $(\lambda_p^i)_{\substack{i,j,k,\ldots \\ p,q,r,\ldots}}$ which show up in the previous expressions of all the sections $\tilde{s_i}$, $\tilde{s_j}$, $\tilde{s_k}$ etc. Let $(l_1, \ldots, l_N)$ a basis of L over k and

$$\lambda_p^i = \lambda_{p,1}^i l_1 + \cdots + \lambda_{p,N}^i l_N,$$

$$\lambda_q^j = \lambda_{q,1}^j l_1 + \cdots + \lambda_{q,N}^j l_N$$

etc. The decompositions of each of these coefficients over the basis $(l_1, \cdots, l_N)$. L being a vector space over k —of dimension N—, every $\mathcal{F}(U) \otimes_k L$ is a direct sum of N copies of $\mathcal{F}(U)$ (by regrouping the components in $\cdot \otimes l_n$, $n = 1 \ldots N$). Consequently, the set of glueing conditions $(ij)_{i,j}$ is satisfied iff the set of projections of these glueing conditions $(ij, n)_{i,j,n}$, over all the components in $(\cdot \otimes l_n)_{n=1 \ldots N}$, is satisfied. For example, let us fix n, then the projection over $\cdot \otimes l_n$ of a glueing condition (ij) can be expressed as

$$\text{(ij,n)} \qquad \rho_i(\sum_{p \in P} m_p^i \otimes \lambda_{p,n}^i) = \rho_j(\sum_{q \in Q} m_q^j \otimes \lambda_{q,n}^j)$$

(Where we recall that the coefficients $(\lambda_{p,n}^i)_p$, $(\lambda_{q,n}^j)_q$ are in k). Consequently, the collection of the projected conditions $(ij, n)_{i,j}$, for a fixed n, defines a global section $s_n \in \mathcal{F}(X)$. But

$$\tilde{s} = s_1 \otimes_k l_1 + \cdots + s_N \otimes_k l_N \in \mathcal{F}(X) \otimes_k K,$$

which is what was to be proven.