Polynomial Reconstruction Based Cryptography
(A Short Survey)

Aggelos Kiayias[1] and Moti Yung[2]

[1] Graduate Center, CUNY, NY USA,
akiayias@gc.cuny.edu
[2] CertCo, NY USA
moti@cs.columbia.edu

Abstract. Cryptography and Coding Theory are closely knitted in many respects. Recently, the problem of Decoding Reed Solomon Codes (aka Polynomial Reconstruction) was suggested as an intractability assumption upon which the security of cryptographic protocols can be based. This has initiated a line of research that exploited the rich algebraic structure of the problem and related subproblems of which in the cryptographic setting. Here we give a short overview of recent works on the subject and the novel applications that were enabled due to this development.

1 Background

The polynomial reconstruction (PR) problem with parameters n, k, t is a natural way of expressing the problem of (list-)decoding Reed Solomon Codes: given a set of n points over a finite field, it asks for all polynomials of degree less than k that "fit" into at least t of the points. Translated to the coding theoretic context, PR asks for all messages that agree with at least t positions of the received codeword, for a Reed Solomon code of rate k/n.

Naturally, PR received a lot of attention from a "positive" side, i.e. how to solve it efficiently. When $t \geq \frac{n+k}{2}$ then PR has only one solution and it can be found with the algorithm of Berlekamp and Welch [BW86] ($\frac{n+k}{2}$ is the error-correction bound of Reed-Solomon codes). The problem has been investigated further for smaller values of t ([Sud97,GS98,GSR95]). These works have pointed to a certain threshold for the solvability of PR. Specifically, the problem appears to be hard if t is smaller than $\sqrt{kn}$, (the best algorithm known, by Guruswami and Sudan [GS98], finds all solutions when $t \geq \sqrt{kn}$).

We note here that apart from any direct implications of efficient list-decoding methods in the context of coding theory, these algorithms have proved instrumental in a number of computational complexity results such as the celebrated PCP theorem. There are numerous other works in computational complexity that utilize (list-)decoding techniques such as: the average-case hardness of the permanent [FL92,CPS99], hardness amplification [STV99], hardness of predicting witnesses for NP-predicates [KS99] etc.

S. Vaudenay and A. Youssef (Eds.): SAC 2001, LNCS 2259, pp. 129–133, 2001.

Perhaps the most notable work which applies the "negative" side of error-correction decoding (i.e., its inherent hardness for certain parameters) is the McEliece's cryptosystem [McE78]. Recently, in the work of Naor and Pinkas [NP99], the above well-studied Reed-Solomon list-decoding problem (namely: PR) has been looked at from a "negative" perspective, i.e. as a hard problem which cryptographic applications can base their security on.

It is important to stress that from a cryptographic perspective we are not interested in the worst-case hardness of PR but rather on the hardness of PR on the average. It is easy to see that PR on the average (termed also noisy PR) has only one solution with very high probability (note that we consider PR in a *large* prime finite field). It is believed that the noisy PR is not easier than the PR. This is because given an instance of the PR it is possible to randomize the solution polynomial (but it is not known how to randomize the noise, only to k-wise randomize it). This justification was presented by [NP99] who gave the basic suggestion to exploit the cryptographic intractability of this problem.

2 The Work of [NP99]

In [NP99] the PR problem is first exploited in concrete and efficient cryptographic protocol design. They presented a useful cryptographic primitive termed "Oblivious Polynomial Evaluation" (OPE) that allowed the secure evaluation of the value of a univariate polynomial between two parties. In their protocol the security of the receiving party was based on closely related problem to PR (later, due to the investigation of [BN00], the protocol of OPE was easily modified to be based directly on the PR problem [BN00,NP01]). We note here that a related intractability assumption appeared independently in [MRW99].

Various useful cryptographic applications based on OPE, were presented in [NP99] such as password authentication and secure list intersection computation. OPE proved to be a useful primitive in other settings, see e.g. [Gil99,KWHI01].

The assumption of [NP01] is essentially the following: given a (random) instance of PR, the value of the (unique with high probability) solution polynomial over 0 is pseudorandom for every polynomially bounded observer. Under this "pseudorandomness" assumption it can be easily shown that the receiving party in the OPE protocol is secure. Note that this assumption appears to be stronger than merely assuming hardness on the average.

3 Structural Investigation of PR

In [KY01b] we investigate cryptographic hardness properties of PR. The main theme of this work is outlined below.

Given a supposedly computationally hard problem, it is important to identify reasonable related (sub)problems upon which the security of advanced cryptographic primitives such as semantically-secure encryption and pseudorandom functions can be based. This practice is ubiquitous in cryptography, e.g. the

Decision-Diffie-Hellman problem is a subproblem related to the discrete-logarithm problem upon which the semantic security of ElGamal encryption is based; the Quadratic Residuosity Problem is a subproblem related to Factoring (and modular square roots) upon which the semantic security of [GM84] is based, etc. In [KY01b] a similar route is followed: first a suitable related subproblem of PR is identified and then advanced cryptographic primitives based on this problem are extracted. The problem is related to distinguishing one of the indices that correspond to the polynomial points in a PR-instance. Distinguishing between the points of the polynomial solution and the random points in a PR-instance appears to be naturally related to the supposed hardness of PR. The corresponding assumption is called Index-PR-Assumption (IPR). Subsequently under this assumption, we show

1. A PR instance conceals its solution in a semantic level: any algorithm that computes a function on a new value of the polynomial-solution (which is not given in the input) that is distributed according to an adversarially chosen probability distribution has negligible advantage.
2. The PR-Instances are pseudorandom.

Regarding the Polynomial Reconstruction Problem itself as the assumption, we show that it has interesting robustness properties under the assumption of almost everywhere hardness. In particular, solving PR with overwhelming probability of success is shown to be equivalent to:

1. Computing a value of the solution-polynomial at a new point with non-negligible success for almost all PR-instances.
2. Computing the least-significant-bit of a new value with non-negligible advantage for almost all PR-instances.

These results suggest that PR and its related subproblem are very robust in the cryptographic sense and seem to be suitable problems for further cryptographic exploitation. A direct application of our work is that the OPE protocol of [NP99,NP01] can be shown semantically secure (based on the IPR assumption instead).

4 Multisample Polynomial Reconstruction

A straightforward way to generalize PR so that additional cryptographic applications are allowed is the following: we can associate with any PR instance a set of indices (called the index-set) that includes the indices of the "good" points that correspond to the graph of the (with high probability unique) polynomial that "fits into" the instance. In the Multisample Polynomial Reconstruction (MPR) Problem, the given instance contains a set of r (random) PR-instances with the same index-set. The challenge is to solve all PR-instances.

MPR was defined in [KY01a] and further investigated in [BKY01]. This latter work points to a hardness threshold for the parameter r. Specifically MPR

appears to be hard when r is smaller than n/t. MPR has similar robustness properties as PR and is likewise sensitive to partial information extraction. These properties are investigated in [KY01c] under the corresponding Index-MPR-Assumption.

5 Cryptographic Applications

In [KY01a] a general family of two-player games was introduced together with an efficient protocol construction that allowed a variety of novel applications, such as a deterministically correct, polylogarithmic Private Information Retrieval (PIR) protocol. The security of these games, that involved the composition of many multivariate polynomials, bilaterally contributed by the two parties, was based on the hardness of MPR. Other applications of this work include: secure computation of the *Lists' Intersection Predicate* (a stringent version of the List Intersection Problem [NP99] where the two parties want to securely check if the two private lists have a non-empty intersection without revealing any items) and *Settlement Escrows* and *Oblivious Bargaining/Negotiations*, which are protocol techniques that are useful in the e-commerce setting.

In [KY01b,KY01c] PR and MPR are employed in the setting of symmetric encryption to produce stream/block ciphers with novel attributes including:

- Semantic Security.
- Error-Correcting Decryption.
- The capability of sending messages that are superpolynomial in the security parameter (namely, a cryptosystem with a very short (sublinear) key size).
- Double homomorphic encryption over the underlying finite field operations (with bounded number of multiplications).

6 Conclusion

The rich algebraic structure of Polynomial Reconstruction (PR), its related problem (IPR) and its multisample version (MPR), has proved valuable in the cryptographic setting. On the one hand, PR and its variants appear to be robust in the cryptographic sense and can be used as a basis for advanced cryptographic primitives (as exemplified in [KY01b,KY01c]). On the other hand, several interesting cryptographic protocols that take advantage of the algebraic properties of the problem have been introduced together with their applications in secure computing and e-commerce (as seen in [NP99,KY01a]).

References

[BW86] Elwyn R. Berlekamp and L. Welch, *Error Correction of Algebraic Block Codes.* U.S. Patent, Number 4,633,470 1986.

[BKY01] Daniel Bleichenbacher, Aggelos Kiayias and Moti Yung, *Batched Decoding of Reed-Solomon Codes with Correlated Errors*, work in progress, 2001.

[BN00] Daniel Bleichenbacher and Phong Nguyen, *Noisy Polynomial Interpolation and Noisy Chinese Remaindering.* In the Proceedings of EUROCRYPT2000, Lecture Notes in Computer Science, Springer, 2000.

[CPS99] Jin-Yi Cai, A. Pavan, and D. Sivakumar, *On the Hardness of the Permanent*, In the Proceedings of the 16th International Symposium on Theoretical Aspects of Computer Science, 1999.

[FL92] Uriel Feige and Carsten Lund, *On the Hardness of Computing the Permanent of Random Matrices*, In the Proceedings of the 24th ACM Symposium on the Theory of Computing, 1992.

[Gil99] Niv Gilboa, *Two Party RSA Key Generation*, CRYPTO 1999.

[GSR95] Oded Goldreich, Madhu Sudan and Ronitt Rubinfeld, *Learning Polynomials with Queries: The Highly Noisy Case.* In the Proceedings of the 36th Annual Symposium on Foundations of Computer Science, 1995.

[GM84] Shafi Goldwasser and Silvio Micali, *Probabilistic Encryption*, JCSS 28(2): 270-299, 1984.

[GS98] Venkatesan Guruswami and Madhu Sudan, *Improved Decoding of Reed-Solomon and Algebraic-Geometric Codes.* In the Proceedings of the 39th Annual Symposium on Foundations of Computer Science, 1998.

[KWHI01] Hirotaka Komaki, Yuji Watanabe, Goichiro Hanaoka, and Hideki Imai, *Efficient Asymmetric Self-Enforcement Scheme with Public Traceability*, International Workshop on Practice and Theory in Public Key Cryptography, 2001.

[KY01a] Aggelos Kiayias and Moti Yung, *Secure Games with Polynomial Expressions*, In the Proceedings of the 28th International Colloquium in Algorithms, Languages and Programming, 2001, pp. 939-950.

[KY01b] Aggelos Kiayias and Moti Yung, *Cryptographic Hardness based on the Decoding of Reed-Solomon Codes*, manuscript, 2001.

[KY01c] Aggelos Kiayias and Moti Yung, *Symmetric Encryption based on Polynomial Reconstruction*, manuscript, 2001.

[KS99] S. Ravi Kumar and D. Sivakumar, *Proofs, Codes and Polynomial-time Reducibilities*, In the Proceedings of the 14th IEEE Conference on Computational Complexity, 1999.

[McE78] Richard J. McEliece, *A Public-Key Cryptosystem Based on Algebraic Coding Theory*, JPL Deep Space Network Progress Report 42-44, pp. 114-116, 1978.

[MRW99] Fabian Monrose, Michael K. Reiter, and Suzanne Wetzel, *Password Hardening based on Keystroke Dynamics.* In the Proceedings of the 6th ACM Computer and Communications Security Conference, Singapore, November, 1999.

[NP99] Moni Naor and Benny Pinkas, *Oblivious Transfer and Polynomial Evaluation.* In the Proceedings of the 31th ACM Symposium on the Theory of Computing, 1999.

[NP01] Moni Naor and Benny Pinkas, *Oblivious Polynomial Evaluation*, manuscript 2001, available at `http://www.wisdom.weizmann.ac.il/ naor/onpub.html`.

[Sud97] Madhu Sudan, *Decoding of Reed Solomon Codes beyond the Error-Correction Bound.* Journal of Complexity 13(1), pp. 180–193, 1997.

[STV99] Madhu Sudan, Luca Trevisan and Salil Vadhan, *Pseudorandom Generators without the XOR Lemma*, In the Proceedings of the 31th ACM Symposium on the Theory of Computing, 1999.