IJISET - International Journal of Innovative Science, Engineering & Technology, Vol. 7 Issue 10, October 2020
ISSN (Online) 2348 – 7968 | Impact Factor (2020) – 6.72
www.ijiset.com

A Review Article on Correlated-Source Extractors in Cryptography

Simran Gade[1], Pragati Gupta[2]

[1&2]UG Department, Indian Institute of Science,
Bangalore, Karnataka, India

Abstract
This report is a summary for the research paper that introduces the notion of Correlated Source Extractors. The paper answers the question of security of cryptographic protocols in which correlated tapes are used over multiple executions of the protocol by introducing the notion of a 'Correlated Source Extractor' and giving a construction of that. They solve the mentioned problem in two settings, namely, Zero Knowledge and Multi Party Computational protocols. In the report, we attempt to 'extract' and present the main ideas and techniques from the paper.
Keywords: *Cryptography, Randomness, Extractors, Correlations, Zero Knowledge, Multi-Party Computation*

1. Introduction

Randomness is known to be crucial for cryptography. Several basic tasks in cryptography become impossible in the absence of randomness. However, perfect random sources are hard to achieve in practical applications. As a result, extractors are used to extract near to perfect random sources by using an impure source and a smaller pure seed. There is always a question of a trade-off between this seed length and the degree of randomness achieved via these extractors. Given this, a well-motivated direction is to understand the extent of randomness required for a given cryptographic protocol. Precisely, when correlated tapes are used in multiple executions of a cryptographic algorithm, is it still secure?

A practical scenario when this can happen is when the user has a defective random number generated that outputs correlated tapes over multiple invocations. In this scenario, the security tends to be compromised. Therefore, as a solution, the notion of 'Correlated Source Extractors (CsExt) is introduced [1]. It is proposed that this, along with Resettably-Secure Computational Protocols can be used to achieve Correlated Tape Zero Knowledge (ZK)[2][3] and Correlated Tape Multi Party Computation (MPC)[4]. The novel idea here is to break correlations between the correlated tapes and prove that such an intended result is achieved. In the review, we begin by giving a notion of Correlated Source Extractors. Then we switch to an explicit construction of a Correlated Source Extractors (CsExt) which uses a seed that doesn't depend on the number of tamperings. We provide an overview of the construction and a high level idea of its proof. In the concluding section, we give the notion of Correlated Tape ZK and MPC and demonstrate in brief how one can achieve security in these cryptographic protocols by using CsExt and Resettable Security

2. Correlated Source Extractors

In the view of various impossibility results known in cryptography, the seed will serve as the CRS in all the cryptographic applications. This accounts for the impossibility of cryptography with tamperable randomness [5] and also of approximate obfuscation and applications to resettable cryptography [6]

2.1 Model

To capture the limited control of Adversary A over the source, we model the correlations as t tampering functions on X, namely $A_1(X)$, ... , $A_t(X)$, which are specified by Adversary A such that $A_i(X) \neq X$ for any i. An additional constraint is that the A_i(s) are different.

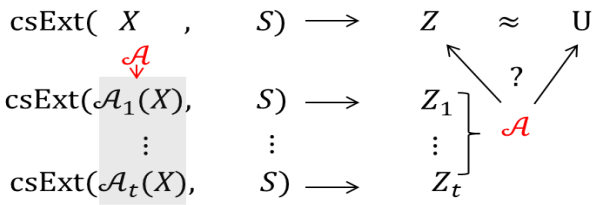

Figure 1 Correlated Source Extractor

The above setting captures the essence of Correlated Source Extractors (csExt). That is, A cannot distinguish computationally between uniform source U and Z even if it can observe Z_1, ..., Z_t.

Weak csExt is a csExt for which the seed length depends on the number of executions. Their existence is already implied by two source non-malleable extractors.[7]

Strong csExt is a csExt for which the seed length doesn't depend on the number of tamperings 't'. The paper [1] gives an explicit construction for such an extractor, which their most important technical contribution.

Why is seed length independence on t such an important result? If seed length depends on t, then each tampering will "fix" a part of the seed, causing significant decrease in its min-entropy [8](this is the measure of randomness of a given string) after a large number of runs. As a result, the independence eradicates this problem.

2.2 Overview of Construction

• We begin with our source X and random seed Y (the CRS). Define $X_i = A_i(X)$ for i∈ {1,...,t}. We then generate an advice adv of say length 'l' from the source X (and adv_i from X_i) such that it is unique w.h.p. across all the tampered executions.

•We then take a strong seeded extractor Ext. Using 2l fresh parts Y_1, . . .$Y_{2l}$of Y, we generate 2l sources from X, namely X_1, ..., X_{2l}, st X_i = Ext (X,Y_i).

•We repeat the above process for our tampered sources X_1, ... X_t such that, for every i ∈ {1, ... ,2l}, X_i is uniformly random given $\{X^j, X^j_1, ..., X^j_t\}$ st j ≠ i.

•Let adv_i denote the i^{th} bit of adv. Each bit adv^i corresponds to a pair of sources (X^{2i-1},X^{2i}). The extractor first uses one piece Z_0 of the original seed as the seed and extracts randomness from one source of the first pair(X^1,X^2) decided by the value of adv_1, then uses the result as the seed and extracts randomness from one source of the second pair (X^3, X^4)and so on, which is summarized in figure 2. The $Y_2{}^i$ is a fresh piece from the seed.

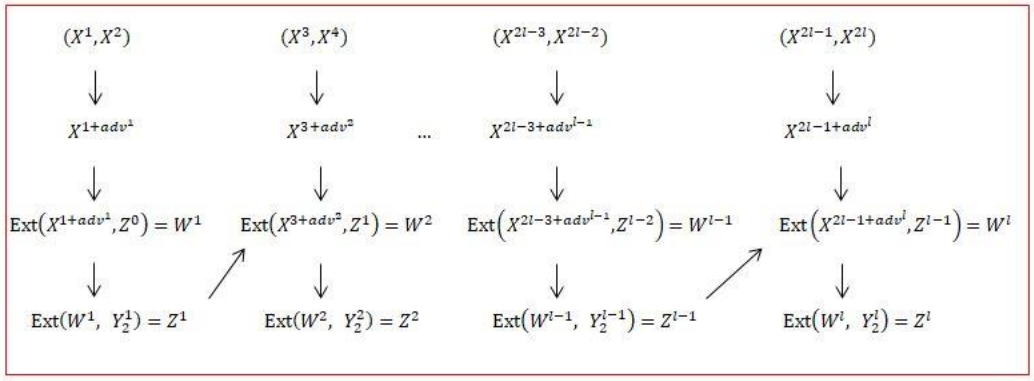

Figure 2 Overview of the Construction

2.3 Proof Overview

We prove that the above construction breaks the correlations by using following properties of extractors:

1. For two sources X and X', if given X', X has enough min-entropy, then Ext(X,Y) and Ext(X′,Y) are independent.

2. For two sources X and X', if X has enough min-entropy, then Ext(X,Y_1) and Ext(X′,Y_2)are independent whereY_1 and Y_2 are independent.

We know adv and $\{adv^i\}_{i\in[t]}$ are different. Which means that given any $\{adv_i\}$, there exists a 'j' st their j^{th} bits are different.

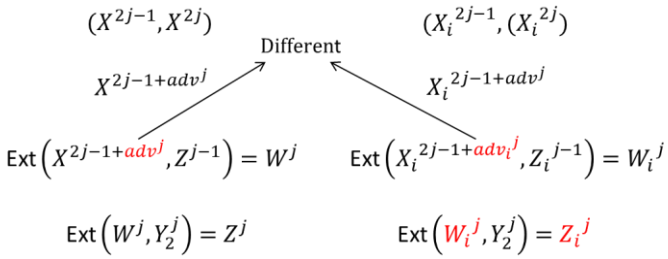

Figure 3 The case of different bits

Using Property 1 in step 3 above, we get that W^j and W_i^j are independent and therefore, Z^j and Z_i^j are independent (Correlation is broken!). We need to show that this 'break' in correlations gets carried to the next steps. We use induction.

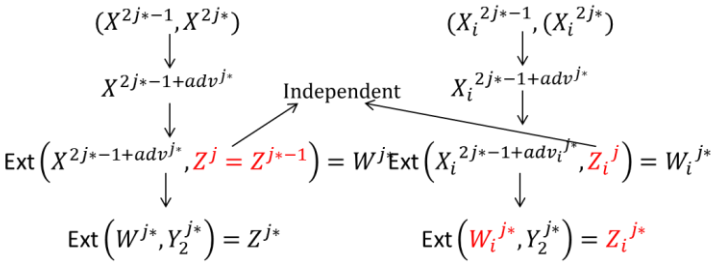

Figure 4 Induction step

For $j* = (j+ 1)$, in the third step, by using Property 2, we get that W^{j*} and W_i^{j*} and consequently Z^{j*} and Z_i^{j*} are independent. We can proceed like this inductively, and finally get that Z^l is independent of Z_i^l for all $i \in [t]$. As a result, we've broken the correlations!

3. Applications of Correlated Source Extractors

We need to remove the constraints on $A_i(s)$ in section 2.1 since we can't control what the adversary choses. So in order to handle the cases where same tapes are used, we incorporate Resettable Security to our model.

3.1 Correlated Tape Zero Knowledge

In order to preserve the zero knowledge property evenin the case of correlated tapes, we make our prover use $csExt(A_i(X))$ instead of $(A_i(X))$ in the i^{th} execution. We then invoke resettable ZK protocol as in [9] while interacting with the adversarial verifier.

3.2 Correlated Tape Multi Party Computation

In order to preserve the ideal/real model security, we use csExt and resettable multi-party computation protocol(π') based on [10] as building blocks. In correlated - tape secure MPC (π), we make each party run csExt with its secret random tape and CRS. Then use the output of csExt as the new random tape and follow the steps in π'.

3.3 Security of the Protocols

In a broad sense, we handle the cases with different and same random tapes by usingcsExt and Resettable Security respectively. We finally just need to take care of certain leakages, for eg. If there is some $A_i(X)$ which gives the same output as $A_1(X)$ with $Pr = {}^1/_2$ for random X. We try to 'mislead' the Adversary by revealing what we call the 'pattern' of X, which is a vector $\{s_1, \ldots, s_t\} \in [t]$ st $s_i = s_j \Leftrightarrow A_i(X) = A_j(X)$. Given the pattern, A bases their strategy on two tapes are either always the same(handled by the resp Resettable protocol) or always different(handled by csExt). So we deprive A of the advantage it could have had by its strategy before this knowledge. Also, this doesn't affect the min entropy of X by much since the number of bits revealed is bounded by tlogt. As a result, security is achieved!

4. Conclusion

Correlated source extractor provides a way to break correlations and can be applied to various setups where multiple executions of cryptographic algorithm from correlated sources is required. The correlated source extractor constructed above has parameters $k(t, d, m) = \Theta(t^3d + t^2m)$, where m is the length of the output. The authors prove a non-explicit existential result for correlated source extractor with $k(t, d, m) = \Theta(d + tm)$.

The future directions of work could be to realise an explicit csExt with optimal parameters and to find more applications of correlated source extractors. The idea can also be translated to correlated-tape secure encryption schemes with appropriate changes.

References

[1] Goyal V., Song Y. (2019) Correlated-Source Extractors and Cryptography with Correlated-Random Tapes. In: Ishai Y., Rijmen V. (eds) Advances in Cryptology – EUROCRYPT 2019. EUROCRYPT 2019. Lecture Notes in Computer Science, vol 11476. Springer, Cham. https://doi.org/10.1007/978-3-030-17653-2_19

[2] Barak, B., Goldreich, O., Goldwasser, S., Lindell, Y.: Resettably-sound zero-knowledge and its applications. In: Proceedings 2001 IEEE International Conference on Cluster Computing, pp. 116–125, October 2001

[3] Canetti, R., Goldreich, O., Goldwasser, S., Micali, S.: Resettable zero-knowledge (extended abstract). In: Proceedings of the Thirty-Second Annual ACM Symposium on Theory of Computing, STOC 2000, pp. 235–244. ACM, New York (2000)

[4] Goyal, V., Sahai, A.: Resettably secure computation. In: Joux, A. (ed.) EUROCRYPT 2009. LNCS, vol. 5479, pp. 54–71. Springer, Heidelberg (2009).

[5] Austrin, P., Chung, K.-M., Mahmoody, M., Pass, R., Seth, K.: On the impossibility of cryptography with tamperable randomness. In: Garay, J.A., Gennaro, R. (eds.) CRYPTO 2014. LNCS, vol. 8616, pp. 462–479. Springer, Heidelberg (2014).

[6] Bitansky, N., Paneth, O.: On the impossibility of approximate obfuscation and applications to resettable cryptography. In: Proceedings of the Forty-Fifth Annual ACM Symposium on Theory of Computing, STOC 2013, pp. 241–250. ACM, New York (2013)

[7] Li, X.: Non-malleable extractors, two-source extractors and privacy amplification. In: 2012 IEEE 53rd Annual Symposium on Foundations of Computer Science, pp. 688–697, October 2012

[8] Reyzin L. (2011) Some Notions of Entropy for Cryptography. In: Fehr S. (eds) Information Theoretic Security.

[9] Chung, K.-M., Ostrovsky, R., Pass, R., Venkitasubramaniam, M., Visconti, I.: 4-round resettably-sound zero knowledge. In: Lindell, Y. (ed.) TCC 2014. LNCS, vol. 8349, pp. 192–216. Springer, Heidelberg (2014).

[10] Chung, K.M., Ostrovsky, R., Pass, R., Visconti, I.: Simultaneous resettability from one-way functions. In: 2013 IEEE 54th Annual Symposium on Foundations of Computer Science, pp. 60–69, October 2013

Simran Gade is a BS + MS (Research) student majoring in Mathematics at the Indian Institute of Science, Bangalore.

Pragati Gupta is a BS + MS (Research) student majoring in Physics at the Indian Institute of Science, Bangalore.