7B-04

Implementation of Various Secret Sharing schemes in AC/NC

Sabyasachi DUTTA[1]
Kyushu University
saby.math@gmail.com

Kouichi SAKURAI[2]
Kyushu University & ATR
sakurai@inf.kyushu-u.ac.jp

1. Introduction

Secret sharing is an important primitive used heavily in Cryptography. Shamir (k, n) secret sharing scheme [22] gives an efficient way to distribute a secret into n pieces such that any k of those pieces can recover the secret whereas any k-1 pieces give absolutely no information about the secret. The work of Shamir was extended to general access structures by Ito et al. [12]. Most of the existing secret sharing schemes require either linear algebraic computation over finite fields e.g. [22] or exclusive-or operation e.g. [10, 9, 12. 17, 18, 16, 20, 23, 24, 25, 26, 28]. However, both of these operations cannot be implemented by AC^0 circuits.

2. Background

There is an existing literature on visual secret sharing schemes where the secrets are visual documents. Some are based solely on OR-operation e.g. [21] and some are based on XOR e.g. [27] and these can be implemented in a very low complexity classes. All of these aforementioned schemes are information-theoretically secure i.e. secure against infinitely powerful adversaries. Krawczyc [13] proposed a scheme to reduce the share size. However, the construction makes the scheme computationally secure i.e., the scheme is secure only against probabilistic polynomial time adversaries. We observe that in all of the above schemes, the honest parties have access to polynomial time algorithms whereas the adversary may have infinite computational power (information theoretic schemes) or probabilistic polynomial time algorithms (computational security). This observations naturally leads to the question of basing cryptography with minimal assumptions. The work of Hastad [11] is a classic example of constructing such cryptographic primitive - in particular, the author showed that one-way functions can be constructed in NC^0 which are secure against AC^0 adversaries. A recent work by Degwekar et al. [8] considers the area of fine-grained cryptography and showed some constructions of some (conditional) cryptographic primitives secure against NC^1 adversaries and also some (unconditional) primitives secure against AC^0adversaries.

Bogdanov et al. [2] proposed secret sharing implementable in $AC^0$and secure against unbounded adversaries. The work was followed up by a work of Cheng et al. [6] who achieved privacy threshold $k = \Omega(n)$ with binary alphabets by allowing negligible privacy error. They have also considered, based on a work by [7], robustness of the schemes in presence of honest majority with privacy threshold $\Omega(n)$, privacy error $2^{-n^{\Omega(1)}}$and reconstruction error 1/poly(n).

Recently, Boyle et al. [4] put forward the idea of sharing a function f into several shares $f_1, f_2, \dots, f_n$ such that any n-1 many f_b s completely hide f but f(x) = $f_1(x) + \cdots + f_n(x)$. The idea was soon forwarded to the idea of homomorphic secret sharing by Boyle et al. [3].In homomorphic secret sharing the function is kept as it is but the input is split into several parts and stored into different servers. The authors gave a scheme based on DDH assumption. Lai et al. [19] gave construction of homomorphic secret sharing schemes which can compute polynomial functionality on the input data. Their construction is based on degree k homomorphic public-key encryptions. The following table gives an overview of important secret sharing literature.

The classical secret sharing schemes assume that the number of participants and the access structure is known in advance. Komargodski et al. [14] introduced evolving secret sharing schemes where the dealer does not know in advance, the number of participants that will participate and no upper bound on their number. Thus, number of participants could be potentially infinite and the access structure may change with time. Komargodski et al. [14] considered the scenario when participants come one by one and receives their share from the dealer; the dealer however cannot update the shares that he has already distributed. The authors showed that for every evolving access structure there exists a secret sharing scheme. Komargodski and Paskin-Cherniavsky [15] forwarded the idea of evolving k-threshold schemes to evolving dynamic threshold schemes and provided a secret sharing scheme in which the share size is less than what is proposed in [14]. A very recent work by Beimel and Othman [1] considers the problem of ramp secret sharing for evolving threshold

[1] Sabyaachi Dutta is supported by an International Invitation Program of National Institute of Information and Communications Technology (NICT) Japan.
[2] Kouichi Sakurai is working with Graduate School and Faculty of Information Science and Electrical Engineering, Kyushu University Advanced Telecommunications Research Institute international (ATR)

schemes and drastically reduced the share size to constant size.

3. Our contribution

We try to make a critical analysis of the existing schemes in the literature. Most importantly, whether the secret sharing schemes in AC^0against AC^0 or NC^1 adversaries can give more efficient share size than the existing ones or not. One challenge is to study of secret sharing when the access structure is evolving with time such that both share generation and reconstruction algorithms can be implemented by AC^0 circuits. We give a concrete construction with some minor storage assumption. Furthermore, we consider the novel problem of robust redistribution of secret shares (in AC^0) to realize dynamic access structure by suitably modifying a construction of Cheng-Ishai-Li [6]. Our construction can be applied to the dealer-free situation.

Scheme	#clients	#servers	#corrupt	Function	Sec	Model	Adv power
[22]	n	m	m-1	$poly^{(m-1)}$	-	plain	inf
[16]	n	m	2	NC^1	-	plain	inf
[17]	n	m	m-1	NC^1	-	plain	inf
[18]	n	m	k-1	NC^1	-	plain	inf
[2]	n	m	$\Omega(\sqrt{m})$	AC^0	-	plain	inf
[4]	n	2	1	Point	OWF	plain	PPT
[3]	n	2	1	NC^1	DDH	PKI	PPT
[19]	n	m	1	$poly^{(k+1))m-1}$	K-HE	PKI	PPT

References

[1] Beimel, A. and Othman, H., Evolving Ramp Secret-Sharing Schemes, SCN'18: 313-332 (2018).
[2] Bogdanov, A., Ishai, Y., Viola, E. and Williamson, C., Bounded Indistinguishability and the Complexity of Recovering Secrets, CRYPTO(3) 2016: 593-618 (2016).
[3] Boyle, E., Gilboa, N. and Ishai, Y., Breaking the Circuit Size Barrier for Secure Computation Under DDH, CRYPTO (1) 2016: 509-539 (2016).
[4] Boyle, E., Gilboa, N. and Ishai, Y., Function Secret Sharing, EUROCRYPT (2) 2015: 337-367 (2015).
[5] Chaudhury, S. S., Dutta, S. and Sakurai, K., AC0 Secret Sharing for Evolving and Dynamic Access Structures, (under review).
[6] Cheng, K., Ishai, Y. and Li, X., Near-Optimal Secret Sharing and Error Correcting Codes in AC0, TCC(2) 2017: 424-458 (2017).
[7] Goldwasser, S., Gutfreund, D., Healy, A., Kaufman, T. and Rothblum, G., Verifying and decoding in constant depth, STOC'07: 440-449 (2007).
[8] Degwekar, A., Vaikuntanathan, V. and Vasudevan, P.N., Fine-Grained Cryptography, CRYPTO (3) 2016: 533-562 (2016).
[9] Fuji, Y., Tada, M., Hosaka, N., Tochikubo, K. and Kato, T., A Fast (2; n)-Threshold Scheme and Its Application, Proc. CSS2005, 631-636 (2005).
[10] Gong, X., Hu, P., Shum, K. W. and Sung, C. W., A Zigzag-Decodable Ramp Secret Sharing Scheme, IEEE Trans. Information Forensics and Security 13(8): 1906-1916 (2018).
[11] Hastad, J., One-way permutations in NC0, Information Processing Letters, 26(3):153-155 (1987).
[12] Ito, M., Saio, A. and Nishizeki, T., Multiple Assignment Scheme for Sharing Secret, J. Cryptology 6(1): 15-20 (1993).
[13] Krawczyk, H., Secret Sharing Made Short, CRYPTO 1993: 136-146 (1993).
[14] Komargodski, I., Naor, M. and Yogev, E., How to Share a Secret, Infinitely, TCC (B2) 2016: 485-514 (2016).
[15] Komargodski, I. and Paskin-Cherniavski, A., Evolving Secret Sharing: Dynamic Thresholds and Robustness, TCC (2) 2017: 379-393 (2017).
[16] Kurihara, J., Kiyomoto, S., Fukushima, K. and Tanaka, T., A Fast (3; n)-Threshold Secret Sharing Scheme Using Exclusive-OR Operations, IEICE Transactions 91-A(1): 127-138 (2008).
[17] Kurihara, J., Kiyomoto, S., Fukushima, K. and Tanaka, T., A New (k; n)-Threshold Secret Sharing Scheme and Its Extension, ISC 2008: 455-470 (2008).
[18] Kurihara, J., Kiyomoto, S., Fukushima, K. and Tanaka, T., A Fast (k; L; n)-Threshold Ramp Secret Sharing Scheme. IEICE Transactions 92-A(8): 1808-1821 (2009).
[19] Lai, R. W. F., Malavolta, G. and Schr• oder, D., Homomorphic Secret Sharing for Low Degree Polynomials, ASIACRYPT (3) 2018: 279-309 (2018).
[20] Matsuo, M. and Mutou, K., (k; n)-Threshold secret sharing scheme using Exclusive OR, Panasonic Tech. Journal, Vol. 59 (2), 115-120 (2013).
[21] Naor, M. and Shamir, A., Visual Cryptography, EUROCRYPT'94: 1-12 (1994).
[22] Shamir, A., How to Share a Secret, Commun. ACM 22(11): 612-613 (1979).
[23] Shima, K. and Doi, H., (f1; 3g; n) Hierarchical Secret Sharing Scheme Based on XOR Operations for a Small Number of Indispensable Participants, AsiaJCIS 2016: 108-114 (2016).
[24] Shima, K. and Doi, H., XOR-Based Hierarchical Secret Sharing Scheme, IWSEC 2018: 206-223 (2018).
[25] Suga, Y., New Constructions of (2; n)-Threshold Secret Sharing Schemes Using Exclusive-OR Operations, IMIS 2013: 837-842 (2013).
[26] Takaara, T. and Iwamura, K., A Fast (k; L; n)-Threshold Secret Sharing ramp Scheme using XOR Operations, Information Processing Society Symposium Proceedings, Vol. 2009 (11), 949-954 (2009).
[27] Tuyls, P., Hollmann, H. D. L., van Lint, J. H. and Tolhuizen, L. M. G. M., XOR-based Visual Cryptography Schemes, Des. Codes Cryptography 37(1): 169-186 (2005).
[28] Yoshihiro, F., Koya, T., Norikazu, H., Minako, T. and Takehisa, K., (k, n) Threshold Schemes Using XOR Operations, ISEC 2007, 31-38 (2007).