RESEARCH SUMMARY: DISTRIBUTED CRYPTOGRAPHY

ANIKET KATE

I. Distributed Key Generation and its Applications

A trusted authority, in some form, is essential for many secure systems. However, this requirement always leads to the liveness-related issue of single point of failure and sometimes to the more undesirable security issue of key escrow. Resolving these two issues is of paramount importance while designing secure systems for use over the Internet where denial-of-service attacks and malicious entities are widespread. Although distributed cryptography has emerged as a natural choice to mitigate these problems, the cryptography literature largely has failed to provide protocols suitable for the Internet. Namely, the aspects related to the practicality of these protocols have been largely ignored and usable implementations for most of the distributed cryptographic primitives are not yet available. This need for practical distributed cryptographic protocols motivated most of my PhD thesis work.

Distributed Key Generation. Distributed key generation (DKG) [19] is a fundamental building block of distributed cryptography, distributed pseudo-random functions and many other distributed computing primitives. It is a prominent example of a well-studied cryptographic protocol that lacks a practical design and implementation.

As our first contribution, we observed the need for a Byzantine agreement protocol for DKG over the Internet [12]. We then designed a DKG protocol by defining the verifiable secret sharing (VSS) and the agreement protocols in a system model that arguably depicts the Internet by considering Byzantine adversary with crash-recoveries and network failures in an asynchronous communication setting. We also obtained proactiveness as well as group modification primitives for our solutions. To verify the efficiency and the reliability of our protocols, we implemented and tested our DKG protocol on the PlanetLab platform [11, 14, 22]. While our above DKG protocol achieves the uniform randomness of the shared secret in the random oracle model [14], we are working towards in a protocol with the uniform randomness property in the standard model.

(a) Application to Identity-Based Cryptography. The key escrow and single point of failure properties of identity-based cryptography (IBC) necessitate the use of a distributed private-key generator (distributed PKG) [7] to make IBC suitable for systems outside the usual closed organizational settings. As the first application of our DKG protocol [13], we have designed provably secure protocols for three important identity-based encryption (IBE) schemes: Boneh and Franklin's BF-IBE, Sakai and Kasahara's SK-IBE, and Boneh and Boyen's BB_1-IBE. In the process, we have also formalized distributed PKG setup and private key extraction primitives for IBEs.

(b) Application to Distributed Hash Tables. As the second application, we have used our DKG protocol and threshold signatures to define two new efficient robust communication protocols for quorum-based distributed hash tables (DHTs) [22, 23]. Several analytical results exist on DHTs that can tolerate Byzantine faults. these results incur significant communication cost in order to achieve message routing. In this work, we obtain two robust communication protocols adding threshold digital signatures on top of our DKG system. Both of these protocols asymptotically reduce the communication costs of previous solutions against a computationally bounded Byzantine adversary, and importantly, no trusted third party is required in the system. We present results from microbenchmarks conducted over the PlanetLab platform, which show that our protocols are practical for deployment under significant levels of churn and adversarial behavior. Recently, using the concept of oblivious transfer, we extended our robust communication protocols to obtain privacy for queries keys [3].

(c) Application to Password Authentication. In password-based authentication, an authentication server maintains user passwords in a derived form (by employing a one-way function) in a so called “password file”. Given the scale and the frequency of server compromises over the Internet, *offline dictionary attacks* on these password files present a critical security challenge for the authentication systems. A threshold password authentication protocol mitigates this challenge by distributing password verification data among multiple servers. Recently, using our DKG protocol in a batched and offline manner, we designed and implemented a threshold password authentication protocol which unlike its all predecessors [5, 17] tolerates server-faults without restarting protocol instances [20].

II. Computational VSS

VSS is an important primitive in distributed cryptography that allows an untrusted dealer to share a secret among n parties in the presence of an adversary controlling at most t of them.

Non-homomorphic Commitments. In the computational complexity setting, the feasibility of VSS schemes based on commitments was established over two decades ago. However, all known computational VSS schemes relied on the homomorphic nature of these commitments or achieve weaker guarantees. As homomorphism is not inherent to commitments or to the computational setting in general, a closer look at its utility to VSS was called for.

In that direction, we demonstrated that homomorphism of commitments is not a necessity for computational VSS in the synchronous or in the asynchronous communication setting [4]. We presented new VSS schemes based only on the definitional properties of commitments that are almost as good as existing VSS schemes based homomorphic commitments. Furthermore, they have significantly lower communication complexities than their (statistical or perfect) unconditional counterparts. Considering the feasibility of commitments from any claw-free permutation, one-way function or collision-resistant hash function, our schemes can be an excellent alternative to unconditional VSS in the future.

VSS Round Complexity. In the same work, we also observed that a crucial interactive complexity measure of round complexity was never formally studied for computational VSS in the synchronous setting. Interestingly, for the optimal resiliency conditions of $n \geq 2t+1$, the least possible round complexity in the previously known computational VSS schemes was identical to that in the (statistical or perfect) unconditional setting: three rounds. Considering the strength of the computational setting, this equivalence was certainly surprising. We showed that three rounds are actually not mandatory for computational VSS, presented the first two-round VSS scheme for $n \geq 2t+1$, and lower-bound the result tightly by proving the impossibility of one-round computational VSS for $n \leq 3t$ given $t > 1$ [4]. Our efforts also resulted in a new *two-round* VSS scheme using homomorphic commitments that has the same communication complexity as the well-known *three-round* Feldman and Pedersen VSS schemes [19].

Polynomial Commitments. A polynomial commitment scheme allows a committer to commit to a polynomial with a short string that can be used by a verifier to confirm claimed evaluations of the committed polynomial. We introduced and formally defined polynomial commitment schemes, and provide two efficient constructions [15]. Although the commitment schemes such as discrete logarithm commitments or Pedersen commitments used in the VSS literature achieve this goal, the sizes of their commitments are linear in the degree of the committed polynomial. On the other hand, polynomial commitments in our schemes are of constant size (single elements), and the overhead of opening a commitment is also constant. Therefore, our schemes are useful tools to reduce the communication cost in VSS [15, 2]. The schemes have also been used in other verification primitives such as zero knowledge (ZK) sets [10, 18, 21].

III. Distributed Computing

In recent years, there have been a few proposals [8, 16] to add a small amount of trusted hardware at each party in a Byzantine fault tolerant system to cut back replication factors. These trusted components eliminate the ability for a malicious party to perform equivocation, which intuitively means making conflicting statements to different parties. In an ongoing work, we define *non-equivocation* and study its power in the context of distributed protocols that assume a malicious adversary model [9]. We show that non-equivocation alone does not allow for reducing the number of parties required to reach Byzantine agreement in the asynchronous communication setting, by proving a lower bound of $n > 3t$ parties for agreement with non-equivocation. However, when we add the ability to guarantee the transferable authentication of messages (e.g., using digital signatures), we showed that it is possible to use non-equivocation to transform any (honest-but-curious) protocol that works under the crash fault model into a protocol that tolerates malicious faults, without requiring an increase in the number of parties.

Our current transformation, however, does not immediately work for distributed cryptographic protocols such as asynchronous VSS and asynchronous multiparty computation (AMPC), where confidentially (or secrecy) is also required. In a recent effort, we have extended the utility of non-equivocation to VSS and MPC and improve the resiliency bound and efficiency for AMPC using non-equivocation [1]. In particular, using non-equivocation, we present an AMPC protocol in the asynchronous setting, tolerating $t < n/2$ faults. From a practical point of view, our AMPC protocol requires fewer setup assumptions than the previous AMPC protocol with $t < n/2$ by Beerliová-Trubíniová, Hirt and Nielsen [6]: unlike their AMPC protocol, it does not require any synchronous broadcast round at the beginning of the protocol and avoids the threshold homomorphic encryption setup assumption. Moreover, our AMPC protocol is also efficient and provides a gain of $\Theta(n)$ in the communication complexity per multiplication gate, over their AMPC protocol.

References

[1] M. Backes, F. Bendun, A. Choudhury, and A. Kate. Asynchronous MPC with $t < n/2$ Using Non-equivocation. Cryptology ePrint Archive, Report 2013/745, 2013. `http://eprint.iacr.org/`.

[2] M. Backes, A. Datta, and A. Kate. Asynchronous Computational VSS with Reduced Communication Complexity. In *CT-RSA*, pages 259–276, 2013.

[3] M. Backes, I. Goldberg, A. Kate, and T. Toft. Adding query privacy to robust DHTs. In *ASIACCS*, pages 30–31, 2012.

[4] M. Backes, A. Kate, and A. Patra. Computational Verifiable Secret Sharing Revisited. In *Advances in Cryptology - ASIACRYPT '11*, pages 590–609, 2011.

[5] A. Bagherzandi, S. Jarecki, N. Saxena, and Y. Lu. Password-protected secret sharing. In *ACM CCS '11*, pages 433–444, 2011.

[6] Z. Beerliová-Trubíniová, M. Hirt, and J. B. Nielsen. On the theoretical gap between synchronous and asynchronous MPC protocols. In *PODC*, pages 211–218, 2010.

[7] D. Boneh and M. K. Franklin. Identity-Based Encryption from the Weil Pairing. In *Advances in Cryptology—CRYPTO '01*, pages 213–229, 2001.

[8] B.-G. Chun, P. Maniatis, S. Shenker, and J. Kubiatowicz. Attested append-only memory: making adversaries stick to their word. In *ACM SOSP '07*, pages 189–204, 2007.

[9] A. Clement, F. Junqueira, A. Kate, and R. Rodrigues. On the (limited) power of non-equivocation. In *ACM PODC '12*, pages 301–308, 2012.

[10] R. Henry, F. G. Olumofin, and I. Goldberg. Practical PIR for electronic commerce. In *ACM CCS '11*, pages 677–690, 2011.

[11] A. Kate. *Distributed Key Generation and Its Applications*. PhD thesis, University of Waterloo, Waterloo, ON, Canada, June 2010.

[12] A. Kate and I. Goldberg. Distributed Key Generation for the Internet. In *IEEE ICDCS '09*, pages 119–128, 2009.

[13] A. Kate and I. Goldberg. Distributed Private-Key Generators for Identity-Based Cryptography. In *SCN '10*, pages 436–453, 2010.

[14] A. Kate, Y. Huang, and I. Goldberg. Distributed Key Generation in the Wild. *IACR Cryptology ePrint Archive*, 2012:377, 2012. Project Webpage: `http://crysp.uwaterloo.ca/software/DKG`.

[15] A. Kate, G. M. Zaverucha, and I. Goldberg. Constant-Size Commitments to Polynomials and Their Applications. In *Advances in Cryptology - ASIACRYPT '10*, pages 177–194, 2010.

[16] D. Levin, J. R. Douceur, J. R. Lorch, and T. Moscibroda. TrInc: Small Trusted Hardware for Large Distributed Systems. In *USENIX NSDI '09*, pages 1–14, 2009.

[17] P. MacKenzie, T. Shrimpton, and M. Jakobsson. Threshold password-authenticated key exchange. *Journal of Cryptology*, 19(1):27–66, 2006.

[18] C. Papamanthou, E. Shi, and R. Tamassia. Signatures of correct computation. Cryptology ePrint Archive, Report 2011/587, 2011.

[19] T. P. Pedersen. Non-Interactive and Information-Theoretic Secure Verifiable Secret Sharing. In *Advances in Cryptology—CRYPTO '91*, pages 129–140, 1991.

[20] I. Pryvalov and A. Kate. Threshold Password-Authenticated Key Exchange, Revisited. Under submission, November 2013.

[21] J. Xu and E.-C. Chang. Towards efficient proofs of retrievability. In *ASIACCS*, pages 79–80, 2012.

[22] M. Young, A. Kate, I. Goldberg, and M. Karsten. Practical Robust Communication in DHTs Tolerating a Byzantine Adversary. In *IEEE ICDCS '10*, pages 263–272, 2010.

[23] M. Young, A. Kate, I. Goldberg, and M. Karsten. Towards Practical Communication in Byzantine-Resistant DHTs. *IEEE/ACM Trans. Netw.*, 21(1):190–203, 2013.