Program of the NIST Workshop on Multi-Party Threshold Schemes

MPTS 2020 — Virtual event (November 4–6, 2020)

https://csrc.nist.gov/events/2020/mpts2020

		#	Hour	Speaker(s)	Topic (not the title)
November 4		—	09:15–09:35	—	Virtual arrival
	Talks	1a1	09:35–10:00	Luís Brandão	**Workshop introduction**
		1a2	10:00–10:25	Berry Schoenmakers	**Publicly verifiable secret sharing**
		1a3	10:25–10:50	Ivan Damgård	**Active security with honest majority**
		—	10:50–11:05	—	Break
	Talks	1b1	11:05–11:30	Tal Rabin	**MPC in the YOSO model**
		1b2	11:30–11:55	Nigel Smart	**Threshold HashEdDSA (deterministic)**
		1b3	11:55–12:20	Chelsea Komlo	**Threshold Schnorr (probabilistic)**
		—	12:20–12:30	—	Break
	Briefs	1c1	12:30–12:36	Yashvanth Kondi	**Threshold Schnorr (deterministic)**
		1c2	12:36–12:42	Akira Takahashi	**PQ Threshold signatures**
		1c3	12:42–12:48	Jan Willemson	**PQ Threshold schemes**
		1c4	12:48–12:54	Saikrishna Badrinarayanan	**Threshold bio-authentication**
		—	12:54–13:00$^+$	—	Day closing
November 5		—	09:15–09:35	—	Virtual arrival
	Talks	2a1	09:35–10:00	Yehuda Lindell	**Diverse multiparty settings**
		2a2	10:00–10:25	Ran Canetti	**General principles (composability, ...)**
		2a3	10:25–10:50	Yuval Ishai	**Pseudorandom correlation generators**
		—	10:50–11:05	—	Break
	Talks	2b1	11:05–11:30	Emmanuela Orsini & Peter Scholl	**Oblivious transfer extension**
		2b2	11:30–11:55	Vladimir Kolesnikov	**Garbled circuits**
		2b3	11:55–12:20	Xiao Wang	**Global scale threshold AES**
		—	12:20–12:30	—	Break
	Briefs	2c1	12:30–12:36	Xiao Wang	**Garbled circuits**
		2c2	12:36–12:42	Jakob Pagter	**MPC-based Key-management**
		2c3	12:42–12:48	Phillip Hallam-Baker	**Threshold key infrastructure**
		2c4	12:48–12:54	Ronald Tse	**Framework for threshold cryptography**
		2c5	12:54–13:00	Frank Wiener	**MPC Alliance**
		—	13:00–13:00$^+$	—	Day closing
November 6		—	09:15–09:35	—	Virtual arrival
	Talks	3a1	09:35–10:00	JP Aumasson & Omer Shlomovits	**Attacks to deployed threshold signatures**
		3a2	10:00–10:25	Kris Shrishak	**Threshold ECDSA**
		3a3	10:25–10:50	Nikolaos Makriyannis	**Threshold ECDSA**
		—	10:50–11:05	—	Break
	Talks	3b1	11:05–11:30	Schuyler Rosefield	**Distributed RSA key generation**
		3b2	11:30–11:55	Muthu Venkitasubramaniam	**Distributed RSA key generation**
		3b3	11:55–12:20	Marcella Hastings	**Implementation frameworks**
		—	12:20–12:30	—	Break
	Briefs	3c1	12:30–12:36	Damian Straszak	**Threshold ECDSA**
		3c2	12:36–12:42	Jack Doerner	**Threshold ECDSA**
		—	12:42–13:00$^+$	Various	Final comments

All times are expressed in Eastern Standard Time (EST) timezone.

Introduction

The MPTS 2020 workshop is intended as an informal consultation step to help with the development of criteria for evaluating multiparty threshold schemes for the cryptographic primitives identified in NISTIR 8214A. To that end, the workshop gathers several presentations with examples of threshold schemes and related topics, and welcomes suggestions and recommendations from the speakers.

The workshop is virtual, with presentations being made in "Webex Events" video-conference environment. Login details will be announced by email to the registered participants. Audio-video recordings of the presentations will be made publicly available online some time after the workshop.

The program is based on two types of contributions: invited talks (~20 min + Q&A) and briefs (~5 min). The invitation/selection of any particular talk/brief should not be construed as any preference for standardization of any particular technique. We hope the sample of viewpoints presented at the workshop serves as a motivation for subsequent feedback and engagement by other stakeholders.

After the workshop, the NIST Threshold Cryptography team will systematize the collected feedback and take it into consideration in the next step of the project, to be open for further public comments.

List of talks

The list is ordered according to the workshop schedule.

Talks in the 1st day (November 4, 2020)

Talk 1a1: Let's talk about multi-party threshold schemes

Speaker: Luís Brandão

Abstract: This talk will open the NIST workshop on multi-party threshold schemes (MPTS) 2020, presenting a viewpoint of the NIST Threshold Cryptography project on the potential for standardization of multi-party threshold schemes. In scope are threshold schemes for NIST-approved key-based cryptographic primitives, such as signing, encryption, decryption and key generation. As laid out in NISTIR 8214A, a necessary step moving forward is the definition of criteria for considering threshold schemes in a standardization effort. The talk will review the logic behind the workshop organization, describe its feedback-collection goal, and outline the program of ensuing talks.

Based on joint work with Apostol Vassilev and Michael Davidson.

Bio: Luís Brandão is a Foreign Guest Researcher at NIST since August 2017 (contractor via Strativia since February 2020). He holds a Ph.D. in Electrical & Computer Engineering obtained in the scope of the CMU|Portugal program between Carnegie Mellon University and Faculty of Sciences University of Lisbon. At NIST he is with the Cryptographic Technology Group, engaged with various projects: threshold cryptography; privacy-enhancing cryptography; interoperable randomness beacons; circuit complexity.

Talk 1a2: Publicly Verifiable Secret Sharing and Its Use in Threshold Cryptography

Speaker: Berry Schoenmakers

Abstract: Shamir's threshold scheme provides a simple and elegant solution for threshold secret sharing. Publicly verifiable secret sharing (PVSS) aims at enhancing Shamir's scheme to let anyone verify that all participants' shares are consistent with a unique secret. The basic solution is to accompany the public-key encrypted shares for the respective participants with a noninteractive zero-knowledge proof establishing the consistency of the shares. Every qualified set of participants is thus guaranteed to find the same secret when pooling their decrypted shares. Nonqualified sets of participants will gain no information about the secret from their decrypted shares due to the information-theoretic security of Shamir's threshold scheme. PVSS finds many applications in threshold cryptography. A major advantage of PVSS over the use of public-key threshold cryptosystems is the dynamic choice of participants each time one wishes to distribute shares of a secret, bypassing the need for any complicated protocols for distributed key generation commonly found in threshold cryptosystems.

In this talk we review the basic ideas behind PVSS and look into a range of applications in threshold cryptography. Many applications relate to secure multiparty computation (MPC) one way or another. For instance, PVSS can be used to secret-share input data among the parties running a (verifiable) MPC protocol. But PVSS can also be used to build an MPC protocol to let a number of parties jointly generate values for a randomness beacon (e.g., as in SCRAPE). In a different direction, modern scenarios pertaining to clouds and blockchains often rely on secure, replicated storage of secret values involving loosely related entities, which can be accommodated using PVSS.

Bio: Berry Schoenmakers is an Associate Professor with the Department of Mathematics & Computer Science at TU Eindhoven in the Netherlands. His main area of expertise is in privacy-protecting cryptographic protocols on which he published several influential papers. His research interests include electronic voting, electronic payment systems, secure multiparty computation, and work on implementation of such systems (most recently, on MPyC, a Python package for secure multiparty computation). Further research interests include pseudorandom generators, side-channel analysis and quantum cryptography as well as topics in algorithms and data structures.

Talk 1a3: Optimizing honest majority threshold cryptosystems

Speaker: Ivan Damgård

Abstract: We review some ideas that allows optimizing threshold implementations of well-known cryptographic primitives with honest majority and security against malicious adversaries. Specifically, full-fledged zero-knowledge proofs of correct behavior are often not necessary and can be replaced by weaker primitives.

Based on a paper with Kasper Dupont.

Bio: Ivan Damgård was born in 1956 and got his PhD in 1988 from Aarhus University, where he has also been professor since 1995. ID became a fellow of the IACR in 2010 and received the RSA conference award for excellence in mathematics in 2015. In 2018 he received the Villum Kann Rasmussen annual award and became member of the Danish Royal Society for sciences and letters. He was the editor in chief of Journal of Cryptology 2014-2016. He has been the supervisor for 20+ postdocs and 35 PhD students. ID has authored 170+ peer reviewed scientific papers that received more than 21000 citations in total. He is a co-founder of spin-off companies Cryptomathic, Partisia and Sepior.

Talk 1b1: You Only Speak Once – Secure MPC with Stateless Ephemeral Roles

Speaker: Tal Rabin

Abstract: The inherent difficulty of maintaining stateful environments over long periods of time gave rise to the paradigm of serverless computing, where mostly-stateless components are deployed on demand to handle computation tasks, and are teared down once their task is complete. Serverless architecture could offer the added benefit of improved resistance to targeted denial-of-service attacks. Realizing such protection, requires that the protocol only uses stateless parties. Perhaps the most famous example of this style of protocols is the Nakamoto consensus protocol used in Bitcoin.

We refer to this stateless property as the You-Only-Speak-Once (YOSO) property, and initiate the formal study of it within a new YOSO model. Our model is centered around the notion of roles, which are stateless parties that can only send a single message. Furthermore, we describe several techniques for achieving YOSO MPC; both computational and information theoretic. The talk will be self contained.

Based on joint works with: Fabrice Benhamouda, Craig Gentry, Sergey Gorbunov, Shai Halevi, Hugo Krawczyk, Chengyu Lin, Bernardo Magri, Jesper Nielsen, Leo Reyzin, Sophia Yakoubov.

Bio: Tal Rabin is a researcher whose general area focuses on cryptography and, more specifically, on secure multiparty computation, threshold cryptography, and proactive security. Her works have been instrumental in forming these areas. She is a professor at the University of Pennsylvania, Computer Science Dept and a consultant at the Algorand Foundation.

Prior to joining UPenn she has been the head of research and the Algorand Foundation and prior to that she had been at IBM Research for 23 years as a Distinguished Research Staff Member and the manager of the Cryptographic Research Group. She has a PhD from the Hebrew University.

Rabin is an ACM Fellow, an IACR (International Association of Cryptologic Research) Fellow and member of the American Academy of Arts and Sciences. She is the 2019 recipient of the RSA Award for Excellence in the Field of Mathematics. She was named by Forbes in 2018 as one of the Top 50 Women in Tech in the world. In 2014 Tal won the Anita Borg Women of Vision Award winner for Innovation and was ranked by Business Insider as the #4 on the 22 Most Powerful Women Engineers. Tal has served as the Program and General Chair of the leading cryptography conferences and is an editor of the Journal of Cryptology. She has initiated and organizes the Women in Theory Workshop, a biennial event for graduate students in Theory of Computer Science. She has served as a member of the SIGACT Executive Board and a council member of the Computing Community Consortium.

Talk 1b2: Thresholdizing DSA, Schnorr, EdDSA, HashEdDSA, ...

Speaker: Nigel Smart

Abstract: This talk will examine the methods to thresholdize the various DSA-based signature. With special emphasis on EdDSA and HashEdDSA. These are schemes in which the hash function required to produce a deterministic signature causes a particular problem for standard threshold methods.

Joint work with Charlotte Bonte and Titouan Tanguy.

Bio: Smart is a professor in the COSIC group at the KU Leuven. He has held two ERC Advanced grants. He was Vice President of the International Association for Cryptologic Research (2014-2016) and is a Fellow of the IACR. He is co-founder of Unbound Tech, the Real World Cryptography conference series.

Talk 1b3: FROST: Flexible Round-Optimized Schnorr Threshold Signatures and Extensibility to EdDSA

Speaker: Chelsea Komlo

Abstract: FROST is an improved threshold Schnorr signature scheme that allows for an optimization from a two-round signing protocol into a single-round protocol with preprocessing. FROST improves upon prior constructions as it is secure against forgery attacks which are demonstrated to be viable against similar schemes in the literature. Excitingly, there is already interest and plans for the use of FROST for practical use.

In this talk, we will introduce FROST and the motivations for its design. We will review the security model under which FROST is secure, and how this security model compares to practical deployments of threshold signatures. We will discuss how FROST is compatible with existing protocols such as those that require EdDSA compatibility, as well as next steps for FROST to be deployed and standardized.

Joint work with Douglas Stebila and Ian Goldberg.

Bio: Chelsea Komlo has nearly a decade of engineering experience and is a lead author on cryptographic designs ranging from multi-party signature schemes to post-quantum primitives with applications to secure messaging. She currently is completing her Ph.D at the University of Waterloo in the Cryptography, Security, and Privacy Lab, and is a Principal Technical Advisor and Researcher for the Zcash Foundation. Chelsea also serves as a member of the board of directors for the Tor Project.

Talks in the 2nd day (November 5, 2020)

Talk 2a1: Settings and Considerations for Standardizing Multi-Party Threshold Schemes

Speaker: Yehuda Lindell

Abstract: In this talk, we will present different commercial use cases for multiparty threshold schemes and show why these can actually be very diverse. We will then present a series of questions and considerations for standardisation based on different issues that have arisen in our work with customers and in building our products. These relate to both technical cryptographic aspects as well as to the security architecture of such solutions.

Bio: Yehuda Lindell is the CEO and co-founder of Unbound Tech. Yehuda is also a professor of Computer Science at Bar-Ilan University in Israel (on leave). Yehuda's research has focused on secure multiparty computation (MPC), and he has worked on both the theoretical foundations as well as making it efficient enough to be used in practice. At Unbound, Yehuda is working on the next step, which is commercialising MPC, and using it to solve acute problems of key protection and management for enterprises.

Talk 2a2: Standardizing Security: The case of threshold cryptography

Speaker: Ran Canetti

Abstract: Standardizing security mechanisms is a challenging and risky endeavor. When the mechanisms are as complex and multi-faceted as threshold cryptosystems, both the challenge and the risk amplify significantly. Still, the increasing dependence of society on the security of complex

cryptographic constructs makes such an endeavor essential.
I will attempt to highlight the potential gains and pitfalls in the current standardization effort, and propose some guidelines that will hopefully maximize the gain to society and the IT industry, while minimizing the risks. The focus will be on: (a) creating a common language and consensus; (b) the clarity, understandability, and compositionality of the requirements made and guarantees provided; (c) on the need in rigorous security analysis that asserts all that needs to be asserted.

Bio: Ran Canetti is a professor of Computer Science in Boston University, where he directs the center for Reliable Information System and Cyber Security. He is a Fellow of the International Association for Cryptologic Research, an incumbent of the RSA Award in Mathematics 2018. Canetti's research interests span multiple aspects of cryptography and information security, with emphasis on the design, analysis and use of cryptographic protocols. His contributions include, among others, the framework of Universally Composable security and the HMAC message authentication protocol. He has also was a founding co-chair of the Crypto Forum Research group of the IRTF and the Secure Multicast Working group of the IETF, and is serving on the steering committee of the ZKProof Standards effort.

Talk 2a3: Pseudorandom Correlation Generators: Secure Computation with Silent Preprocessing

Speaker: Yuval Ishai

Abstract: Correlated secret randomness is a useful resource for threshold cryptography and secure multiparty computation. A pseudorandom correlation generator (PCG) enables secure deterministic generation of long sources of correlated randomness from short, correlated seeds. The talk will cover the definition of a PCG, constructions of multiparty PCGs for linear correlations using symmetric cryptography (also known as "pseudorandom secret sharing"), and a recent line of work on PCGs for useful nonlinear correlations from different flavors of the Learning Parity with Noise (LPN) assumption. The latter includes practical methods for "silent" OT extension that use much less communication than alternative OT extension techniques.

Based on joint works with Elette Boyle, Geoffroy Couteau, Ronald Cramer, Ivan Damgård, Niv Gilboa, Lisa Kohl, Peter Rindal, and Peter Scholl.

Bio: Yuval Ishai is a professor of Computer Science at the Technion, Israel, working in the area of cryptography. He served as a program chair of the TCC 2011, Eurocrypt 2019 and Eurocrypt 2020 conferences and was inducted as an IACR Fellow in 2018. He published more than 150 research papers that were recognized by best paper awards at the FOCS 2004, Crypto 2007, and Crypto 2016 conferences and by a SIAM Outstanding Paper Prize.

Talk 2b1: Efficient Actively Secure OT Extension: 5 Years Later

Speakers: Emmanuela Orsini & Peter Scholl

Abstract: Oblivious Transfer (OT) is a fundamental cryptographic primitive that has been used as a building block in many efficient MPC protocols. Whilst OT inherently requires public-key cryptography, recent advances in the field show that in practice, OT can no longer be considered an expensive primitive. This is mainly due to the OT extension technique of Ishai, Kilian, Nissim and Petrank (CRYPTO 2003), which cheaply produces a large number of OTs starting from just

a few seed OTs. In this talk, we will describe the actively secure OT extension protocol of Keller, Orsini and Scholl (CRYPTO 2015) and some variants, and discuss lessons learnt and subsequent developments from the last few years.

Joint work with Marcel Keller.

Bios: Emmanuela Orsini is a Research Expert in the Computer Security and Industrial Cryptography (COSIC) research group at KU Leuven, Belgium. She is interested in a broad range of topics in cryptography, theory of error correcting codes and abstract algebra. Currently, her research is mainly focused on practical aspects of secure multiparty computation and its building blocks such as oblivious transfer and secret sharing schemes. Emmanuela is also particularly interested in post-quantum cryptographic constructions, both lattice and isogeny based, and was involved in the NIST Post-quantum standardization process with teams Lima and NewHope.

Peter Scholl is a tenure-track assistant professor in the Cryptography & Security group at Aarhus University. He has worked extensively on bringing the theory of secure multi-party computation into practice with more efficient protocols and implementations, as well as related technologies such as oblivious transfer and homomorphic secret sharing. His work on the popular SPDZ protocol won the best paper award at ESORICS 2013, and is now being used in several software frameworks.

Talk 2b2: Let's Standardize Garbled Circuits!

Speaker: Vladimir Kolesnikov

Abstract: Garbled Circuits (GC) is the classic, most popular and often the fastest approach to general secure two-party computation (2PC). In the semi-honest model, we can evaluate about two million AND gates per second on commodity devices and networks. This translates, for example, to approximately 330 shared-key AES evaluations per second. With specialized hardware or allowing precomputation, this number can be further greatly increased.

Since its introduction by Andrew Yao in 1986, there have been only a small number of improvements to the basic protocol. In this talk, time permitting, I will briefly review the basic protocol and some of the improvements, such as Free-XOR and our recent work Stacked Garbling. I will also talk about stronger security models, particularly cheap-to-achieve covert and publicly verifiable covert (PVC) models.

The stability, wide acceptance, simplicity, efficiency and generality of the GC protocol is unique among MPC protocols, and make it a strong candidate for standardization. A standardized GC variant would be a powerful and versatile tool, which would catalyze both wide practical adoption of rich cryptography and further MPC research.

This talk relied on joint works with David Heath and Thomas Schneider.

Bio: Vladimir Kolesnikov is an Associate Professor at Georgia Institute of Technology working in the area of cryptography and security. Prior to this appointment he was a researcher at Bell Labs, which he joined in 2006 after receiving his Ph.D. at the University of Toronto. His main current research interest is improving and applying secure computation and crypto techniques in practice. He has authored papers on garbled circuit, homomorphic encryption, related techniques and applications. He is also interested in zero-knowledge proofs (ZKP), blockchain, database security and privacy, key exchange and channel security. Dr. Kolesnikov has been involved in the design and analysis of Smart Grid networks, Storage Area Networks, wireless and biometric authentication, and other secure systems. His work has been supported by grants and contracts from DARPA, IARPA, ONR, NSF, and Sandia Labs.

Talk 2b3: Global-Scale Threshold AES (and SHA256)

Speaker: Xiao Wang

Abstract: Authenticated garbling is a set of protocols for maliciously secure two-party and multi-party computation based on garbled circuits. Implementations have verified its scalability in both the circuit size (e.g., computing billion-sized circuits) and the number of parties (e.g., computing over hundreds of nodes distributed globally). In this talk, I will give an overview of the protocol, a demo of it running on multiple nodes, and a discussion of future directions in the context of multi-party threshold schemes.

The talk is based on prior works join with Jonathan Katz, Xiao Lan, Samuel Ranellucci, Mike Rosulek, Chenkai Weng, Kang Yang, Jiang Zhang.

Bio: Xiao Wang is an assistant professor of computer science at Northwestern University. He was a postdoc researcher at MIT and Boston University and obtained his Ph.D. at the University of Maryland. His research interests include computer security, privacy, and cryptography. He has recently been working on practical multi-party computation, zero-knowledge proof, oblivious RAM, and post-quantum cryptography. He is in a team submitting to NIST post-quantum cryptography standardization, currently in round 3.

Talks in the 3rd day (November 6, 2020)

Talk 3a1: Attacks to deployed threshold signatures

Speakers: Jean-Philippe (JP) Aumasson and Omer Shlomovits

Abstract: Threshold wallets leverage threshold signature schemes (TSS) to distribute signing rights across multiple parties when issuing blockchain transactions. These provide greater assurance against insider fraud, and are sometimes seen as an alternative to methods using a trusted execution environment to issue the signature. This talk describes the authors' experience with building and analyzing TSS technology, notably the finding of attacks on TSS implementations used by leading organizations such as major exchanges.

Bios: Jean-Philippe (JP) Aumasson is co-founder and CSO of Taurus Group. JP is known for his work in cryptography including the reference book Serious Cryptography, the widely used algorithms BLAKE2 and SipHash, and talks at leading industry conferences. JP has been giving cryptography trainings since 2013 in multiple public and private settings. Find him on Twitter as @veorq.

Omer Shlomovits is a manager at ZenGo-X, a research hub focused on threshold cryptography. He is a co-founder of the MPC-Alliance and a member of the OpenMined MPC team.

Talk 3a2: Securing DNSSEC Keys via Threshold ECDSA from generic MPC

Speaker: Kris Shrishak

Abstract: While prior work has shown that computing k^{-1} is the main challenge for threshold ECDSA and often resort to specialized protocols in order to obtain k^{-1}, we show that out-of-the-box MPC suffices to compute a threshold ECDSA signature with essentially the same efficiency as the best existing schemes. To illustrate this generality, we implement our technique with all protocols supported by MP-SPDZ, allowing us to examine the trade-offs (in terms of efficiency) one has to

make when choosing between different corruption models (malicious vs. semi-honest) and corruption thresholds (honest vs. dishonest majority). Our technique in particular shines in the preprocessing model, where one wants to make many signatures with the same key.

At the center of our protocol is a generic transformation of a secret-sharing scheme based on the following observation: Let G be a generator of group $\mathcal{G}$ of order p. Then, given an additive secret-sharing $[x]$ over a field Z_p, the value $[x]G$ can be viewed as an additive secret-sharing over $\mathcal{G}$. Notice that this transformation is entirely local. We achieve active security for the protocol over $\mathcal{G}$ using regular SPDZ type MACs. If the base Z_p protocol is secured with SPDZ MACs, then the $\mathcal{G}$ protocol is secure as well, using the same MACs. Key generation, which has been costly in prior works, is simply generating a sharing of random element $[x]$, converting it to a sharing of $[xG]$ and opening it towards everyone to get the public key.

We use our threshold ECDSA protocol to secure DNSSEC keys. Very few domain owners run their own authoritative name servers and zone management is outsourced to DNS operators. Although outsourcing provides benefits such as increased availability of zones and fewer misconfigurations, several issues related to key management arise when DNSSEC is used. These issues extend from the domain owner relinquishing control of private keys to the DNS operator reusing keys for thousands of domains to the possibility of domain takedown by governments. We show how private keys can be secured in the outsourced DNS setting through threshold ECDSA.

Based on joint work with Anders Dalskov, Marcel Keller, Claudio Orlandi and Haya Shulman.

Bio: Kris Shrishak is a Ph.D. candidate at TU Darmstadt in Germany. His research interests are broadly in applied cryptography, privacy enhancing technologies and network security. His current focus is on cryptographic protocols and, in particular, practical aspects of secure multiparty computation.

Talk 3a3: UC Non-Interactive, Proactive, Threshold ECDSA with Identifiable Aborts

Speaker: Nikolaos Makriyannis

Abstract: Building on the Gennaro & Goldfeder and Lindell & Nof protocols (CCS '18), we present two threshold ECDSA protocols, for any number of signatories and any threshold, that improve as follows over the state of the art:

- For both protocols, only the last round requires knowledge of the message, and the other rounds can take place in a preprocessing stage, lending to a *non-interactive* threshold ECDSA protocol.
- Both protocols withstand adaptive corruption of signatories. Furthermore, they include a periodic refresh mechanism and offer full proactive security.
- Both protocols realize an ideal threshold signature functionality within the UC framework, in the global random oracle model, assuming Strong RSA, DDH, semantic security of the Paillier encryption, and a somewhat enhanced variant of existential unforgeability of ECDSA.
- Both protocols achieve accountability by identifying corrupted parties in case of failure to generate a valid signature.

The two protocols are distinguished by the round-complexity and the identification process for detecting cheating parties. Namely:

- For the first protocol, signature generation takes only 4 rounds (down from the current state of the art of 8 rounds), but the identification process requires computation and communication that is quadratic in the number of parties.

- For the second protocol, the identification process requires computation and communication that is only linear in the number of parties, but signature generation takes 7 rounds.

These properties (low latency, compatibility with cold-wallet architectures, proactive security, identifiable abort and composable security) make the two protocols ideal for threshold wallets for ECDSA-based cryptocurrencies.

Based on joint work with Ran Canetti, Rosario Gennaro, Steven Goldfeder and Udi Peled.

Bio: I received my BSc and MSc in Mathematics from Imperial College and EPFL, respectively. I obtained my Ph.D. from Universitat Pompeu Fabra, where I was working under the supervision of Vanesa Daza. The topic of my PhD thesis was Fairness in Secure Multi-Party Computation. In recent years I was a postdoc at Tel-Aviv University (hosted by Iftach Haitner) and at Technion (hosted by Yuval Ishai). I am currently a cryptography researcher at Fireblocks, a digital asset security platform. I have a broad interest in cryptography with a particular focus on MPC.

Talk 3b1: Multiparty Generation of an RSA Modulus

Speaker: Schuyler Rosefield

Abstract: We present a new multiparty protocol for the distributed generation of biprime RSA moduli, with security against any subset of maliciously colluding parties assuming oblivious transfer and the hardness of factoring. Our protocol is highly modular, and its uppermost layer can be viewed as a template that generalizes the structure of prior works and leads to a simpler security proof. We introduce a combined sampling-and-sieving technique that eliminates both the inherent leakage in the approach of Frederiksen et al. (Crypto'18), and the dependence upon additively homomorphic encryption in the approach of Hazay et al. (JCrypt'19). We combine this technique with an efficient, privacy-free check to detect malicious behavior retroactively when a sampled candidate is not a biprime, and thereby overcome covert rejection-sampling attacks and achieve both asymptotic and concrete efficiency improvements over the previous state of the art.

Based on joint work with Megan Chen, Ran Cohen, Jack Doerner, Yashvanth Kondi, Eysa Lee, and abhi shelat.

Bio: Schuyler is a PhD student at Northeastern University with abhi shelat. Their primary research interest is making novel cryptographic capabilities more practical so that they can benefit the larger community. So far, the research has taken the form of specialized efficient MPC protocols, with limited work on fully homomorphic encryption and searchable encryption.

Talk 3b2: Scaling Distributed RSA Modulus Generation with a Dishonest Majority

Speaker: Muthu Venkitasubramaniam

Abstract: In this work, we design and implement the first protocol for distributed generation of an RSA modulus that can support thousands of parties and offers security against active corruption of an arbitrary number of parties. In a nutshell, we first design a highly optimized protocol for this scale that is secure against passive corruptions, and then amplify its security to withstand active corruptions using lightweight succinct zero-knowledge proofs. Our protocol achieves security with "identifiable abort," where a corrupted party is identified whenever the protocol aborts, and supports public verifiability. Our protocol against passive corruptions extends the recent work of

Chen et al. (CRYPTO 2020) that, in turn, is based on the blueprint introduced in the original work of Boneh-Franklin protocol (CRYPTO 1997, J. ACM, 2001). Specifically, we reduce the task of sampling a modulus to secure distributed multiplication, which we implement via an efficient threshold additively homomorphic encryption scheme based on the Ring-LWE assumption. This results in a protocol where the (amortized) per-party communication cost grows logarithmically in the number of parties. In order to minimize the work done by the parties, we employ a "publicly verifiable" coordinator that is connected to all parties and only performs computations on public data. We implemented both the passive and the active variants of our protocol and ran experiments using 2 to 4,000 parties. This is the first implementation of any MPC protocol that can scale to more than 1,000 parties. For generating a 2048-bit modulus among 1,000 parties, our passive protocol executed in under 4 minutes and the active variant ran in 25 minutes.

Joint work with Megan Chen, Carmit Hazay, Yuval Ishai, Yuriy Kashnikov, Daniele Micciancio, Tarik Riviere, abhi shelat and Ruihan Wang.

Bio: Muthu Venkitasubramaniam is an associate professor at the University of Rochester and co-founder of Ligero Inc. He received his PhD from Cornell and pursued postdoctoral research at the Courant Institute of Mathematical Sciences (NYU) supported by the Computing Innovation Fellowship. He is a recipient of the Google Faculty Research Award and the ICDE Influential Paper Award. He is an expert on zero-knowledge proofs and secure computation with a special focus on composition. He currently serves as a steering committee member for Zero Knowledge Standardization.

Talk 3b3: How MPC Frameworks Use Threshold Cryptography

Speaker: Marcella Hastings

Abstract: Secure multi-party computation allows a group of mutually distrustful parties to compute a joint function on their inputs without revealing any information beyond the result of the computation. This type of computation is extremely powerful and has wide-ranging applications in academia, industry, and government. In recent years, general-purpose compilers for executing MPC on arbitrary functions have rapidly advanced the state of the art. However, the field is changing so rapidly that it is difficult even for experts to keep track of the varied capabilities of modern frameworks. In this talk, I will describe our survey of general-purpose compilers for secure multi-party computation. We evaluated the tools on a range of criteria, including language expressibility, capabilities of the cryptographic back-end, and accessibility to developers. I will discuss the limitations in documentation and software engineering we identified and discuss how the findings from this work can be used when evaluating multi-party threshold schemes.

Based on joint work with Brett Hemenway, Daniel Noble, and Steve Zdancewic

Bio: Marcella Hastings is a final-year PhD student at the University of Pennsylvania. Her research focuses on software tools for secure multi-party computation (MPC) and the challenges faced when using them in practice. She maintains an open-source repository that aims to make it easier to use the wide variety of available MPC frameworks. During her PhD, she has also collaborated with researchers and developers at Bolt Labs, Microsoft, and Boston University.

List of accepted briefs

Briefs in the 1st day (November 4, 2020)

Brief 1c1: Threshold Schnorr with Stateless Deterministic Signing

Speaker: Yashvanth Kondi

Abstract: Schnorr's signature scheme permits an elegant threshold signing protocol due to its linear signing equation. However each new signature consumes fresh randomness, which can be a major source of issues in practice. In order to mitigate security issues due to bad randomness in deployments, EdDSA (which is a special case of Schnorr) is specified to derive its nonces as a function of the message and the secret key. Implementing this deterministic nonce derivation in a threshold fashion while only using standardized primitives (eg. SHA, AES) is challenging. In this work, we construct protocols that enable such stateless deterministic nonce derivation in a threshold setting, albeit by combining evaluations of standardized PRFs rather than thresholdizing a standardized PRF. While we do not realize a functionally equivalent threshold version of EdDSA, we demonstrate that it is practically feasible to achieve stateless deterministic nonce derivation using standardized primitives in threshold Schnorr.

Based on joint work with François Garillot, Payman Mohassel, and Valeria Nikolaenko.

Brief 1c2: Lattice-based Distributed Signing Protocols from the Fiat–Shamir with Aborts Paradigm

Speaker: Akira Takahashi

Abstract: Most recent works on distributed signatures have focused on ECDSA and over variants of Schnorr signatures. However, little attention has been given to constructions based on post-quantum secure assumptions like the hardness of lattice problems. In this talk, we present several lattice-based multi-party signing protocols with low round complexity, following the FiatShamir with aborts paradigm due to Lyubashevsky (Asiacrypt 2009). Our constructions can be seen as distributed variants of the fast Dilithium-G signature scheme, or lattice-based counterparts of recent two-round multi-party signing protocol by Drijvers et al. (S&P 2019) in the discrete-log setting. Our result highlights several important similarities and differences which emerge when translating a discrete-log-based protocol to lattice-based one.

Based on joint work with Ivan Damgård, Claudio Orlandi, and Mehdi Tibouchi.

Brief 1c3: On the need for threshold post-quantum (signature) schemes

Speaker: Jan Willemson

Abstract: There are currently two standardization efforts running in parallel at NIST: Threshold Schemes for Cryptographic Primitives, and Post-Quantum Cryptography. Unfortunately, they do not overlap, and this is a problem, since easy thresholdizability is not a property that would magically appear for majority of the cryptographic schemes. In particular, the current post-quantum standard candidates can be thresholdized only with major performance penalty. The message of this brief is that there will be need for efficient threshold post-quantum cryptography as well, and there has to be an explicit call for obtaining such schemes.

Brief 1c4: BETA: Biometric Enabled Threshold Authentication

Speaker: Saikrishna Badrinarayanan

Abstract: Due to security and usability challenges with passwords, the industry is gradually moving to biometric-based authentication. While biometrics are user-friendly, a server-side breach of biometric data is more damaging because, unlike passwords, changing biometric information is difficult. FIDO Alliance, an industry-wide effort to enable biometric authentication, uses an approach where biometric templates and measurements are stored and matched on the client device. A successful match transmits a digital signature (on a fresh challenge) to the server which can verify this. Thus, a server-side breach does not lead to a loss of sensitve user data. We introduce a new framework for Distributing FIDO that securely distributes both the biometric template and signing key among multiple devices, who can collectively perform biometric matching and signature generation without reconstructing the template or signing key on any device. We model security via a real-ideal world UC definition and design several protocols that realize this.

Based on joint work with Shashank Agrawal, Payman Mohassel, Pratyay Mukherjee and Sikhar Patranabis.

Briefs in the 2nd day (November 5)

Brief 2c1: Better Concrete Security for Half-Gates Garbling (in the Multi-Instance Setting)

Speaker: Xiao Wang

Abstract: We study the concrete security of high-performance implementations of half-gates garbling, which all rely on (hardware-accelerated) AES. We find that current instantiations using k-bit wire labels can be completely broken, in the sense that the circuit evaluator learns all the inputs of the circuit garbler, in time $O(2^k/C)$, where C is the total number of gates, possibly across multiple independent executions. The attack can be applied to existing circuit-garbling libraries using $k = 80$ and would require 267 machine-months and cost about USD 3500. With this as our motivation, we seek a way to instantiate the hash function in the half-gates scheme to achieve better concrete security. We present a construction based on AES that achieves optimal security in the single-instance setting (when only a single circuit is garbled). We also show how to modify the half-gates scheme so that its concrete security does not degrade in the multi-instance setting.

Joint work with Chun Guo and Jonathan Katz and Chenkai Weng and Yu Yu.

Brief 2c2: MPC-based key management – Using threshold trust to address different threat models

Speaker: Jakob Pagter

Abstract: In key management based on Multi-Party Computation (MPC) cryptographic primitives are implemented through a distributed protocol executed by a set of MPC components. A fundamental but often ignored part of this, is the way in which control over the individual MPC components is used to address the threat model of the application. This allows the nice mathematical properties of threshold cryptography to address different trust models or different threat models. In this brief we will provide two examples (one where each MPC node is owned by the same enterprise, and one where nodes reflect different policy elements as well as end-user control) and use these to start a

discussion about constructing a taxonomy for how to align threats with what it offered by security architectures offered by MPC.

Brief 2c3: Towards a Threshold Key Infrastructure

Speaker: Phillip Hallam-Baker

Abstract: The Mathematical Mesh (Mesh) is a Threshold Key Infrastructure (TKI) that uses threshold techniques to manage public key pairs and threshold key shares. The resulting architecture shares many similarities to traditional Kohnfelder model PKIs (e.g. X.509) but with significant differences. The use of threshold techniques provides the 'key portability' advantage of using smartcards without the need for a physical token. Devices that are connected to a Mesh profile can decrypt data and authenticate to internal or external infrastructures as authorized by the user/administrator. Authorizations are expressed as threshold key shares mediated by a Mesh service. Through the use of threshold techniques, the service is zero-trust with respect to confidentiality and integrity concerns and limited trust with respect to availability. The Mesh may be used to manage keys for traditional PKI applications (SSH, OpenPGP, S/MIME) or as a platform for building new applications. Current applications include sharing of encrypted data-at-rest between groups of users, a password vault, a contact manager and a replacement for second factor authentication schemes that actually makes sense.

Brief 2c4: Confium: an open source framework to support threshold cryptography standardization

Speaker: Ronald Tse

Abstract: Confium is an open-source distributed trust store framework that bridges cryptographers with practical cryptography usage and supports the standardization efforts of threshold cryptography at NIST. It aims to provide a generalized environment with an extensible architecture for the development of trust stores and future cryptographic families. This presentation will briefly describe the framework, its goals and upcoming plans. Confium is a component of RNP, the openly-licensed high performance OpenPGP toolkit, selected by Mozillas Thunderbird to protect its 30+ million users to secure emails end-toend. RNP is a Ribose project. The Confium project is supported by the Next Generation Internet initiative of the European Commission; Ribose is a grantee of the Mozilla Open Source Support (MOSS) Foundational Technology award as well as the MOSS Secure Open Source award.

Jointly prepared with Daniel Wyatt, Nickolay Olshevsky and Jeffrey Lau.

Brief 2c5: The MPC Alliance (MPCA), Status and Roadmap

Speaker: Frank Wiener

Abstract: In this brief we want to introduce MPC Alliance (www.mpcalliance.org). We will present: Short term plans (e.g. community building, marketing, surveys, studies); Long term plans (e.g. involvement in MPC standardization); Stats on members (e.g MPCA has tripled its membership in less than a year); Stats on trends (e.g. Over 20 cryptocurrency wallet vendors now offer MPC-based wallets, demonstrating a dramatic increase since the first MPC wallet was introduced in 2018); MPCA structure (e.g. non-profit, present the board); How can workshop attendees can help.

Jointly prepared with Dan Bogdanov and Omer Shlomovits.

Briefs in the 3rd day (November 6)

Brief 3c1: Robustness for Dishonest Majority in Threshold ECDSA

Speaker: Damian Straszak

Abstract: An important application for threshold signature schemes and specifically for ECDSA is decentralized custody over digital assets. The main idea here is for a committee of nodes to jointly control an asset by maintaining a threshold key allowing to move or spend this asset. Decisions on what actions to perform come either from an external control system, or are made via some form of consensus within the group of nodes. Since we cannot assume that all nodes behave honestly in such systems, a property of crucial importance is "robustness" of signing. This means that whenever a decision to sign a message is made, the committee of nodes should succeed in producing a valid signature, despite adversarial behavior of a subset of them. We propose a new dishonest majority threshold ECDSA protocol that offers robustness and does not require choosing a subset of honest signers for a signature to be generated.

Based on joint work with Adam Ggol, Jdrzej Kula and Micha wietek.

Brief 3c2: A Multiparty Computation Approach to Threshold ECDSA

Speaker: Jack Doerner

Abstract: The Elliptic Curve Digital Signature Algorithm (ECDSA) is one of the most widely used schemes in deployed cryptography. Through its applications in code and binary authentication, web security, and cryptocurrency, it is likely one of the few cryptographic algorithms encountered on a daily basis by the average person. Standardizing a design for a threshold variant of ECDSA will be significant progress toward standardizing building blocks for threshold cryptosystems at large. However, the design of ECDSA is such that executing multi-party or threshold signatures in a secure manner is challenging: unlike other, less widespread signature schemes, secure multi-party ECDSA requires custom protocols, which has heretofore implied reliance upon additional cryptographic assumptions and primitives such as the Paillier cryptosystem. We introduce new protocols for multi-party ECDSA key-generation and signing with arbitrary thresholds that are secure against malicious adversaries in the Random Oracle Model assuming only the Computational Diffie-Hellman Assumption. We instantiate our protocols using the same hash function and elliptic curve group used by the ECDSA signature being computed. Our threshold t scheme requires $log(t) + 6$ rounds of communication with scope for adjustment to constant rounds if desired, and when $t = 2$ we provide an optimized two message protocol. Furthermore, our protocols are non-interactive in the preprocessing model. We evaluate our implementations and find that the wall-clock time for computing a signature through our two-party protocol comes to within a factor of 18 of local signatures. Concretely, two parties can jointly sign a message in just over three milliseconds. We also demonstrate the feasibility of signing with a low-power device (as in the setting of 2-factor authentication) by computing a signature between two Raspberry Pi devices in under 60 milliseconds.

Based on joint work with Yashvanth Kondi, Eysa Lee, and abhi shelat.