INVITED TALK : Public Good Crypto: funding last mile cryptography research to secure the internet and to push digital human rights forward.

Nicola Greco

Public Good Crypto (PGC) started in 2024 as an independent spin off from Protocol Labs by Nicola Greco, Luca Nizzardo and Irene Giacomelli, having Protocol Labs as the first funder.

PGC aims to fund last mile cryptography research to secure the internet and to push digital human rights forward in the following areas: decentralized systems, zero knowledge proofs, proof of storage, fully homomorphic encryption, multiparty computation, verifiable computing, private information retrieval and quantum cryptography.

We believe that it is hard for researchers to get small to medium size funding from large crypto foundations, DAOs and companies - instead, we believe it will be much easier for organizations such as PGC to act as a bridge and become a cross-organization funding vehicle.

We currently closed our first batch of "Microgrants" (up to 5k USD each) and will soon open more.

1. Refinement-based Verification of Protocols with Quantitative Values

Aoxuan Li, and Itsaka Rakotonirina

We present in this paper the Tidy prover, a fully automated tool for proving trace properties of cryptographic protocols relying on quantitative values such as real time. Its specification language is inspired by the \tidy logic, a framework for specifying security properties that rely on real-numbered mechanisms such as timeouts or timed cryptography.

We extend this idea with a generic procedure for arbitrary quantitative values (e.g., an account's balance), and provide a first prototype implementation. The tool uses an expressive specification language with a large range of convenient features for specifying protocols, including a notion of atomic composition and a ML-like static type checker.

2. Homomorphic Signature-based Witness Encryption and Applications

Alireza Kavousi, and István András Seres

Practical signature-based witness encryption (SWE) schemes recently emerged as a viable alternative to instantiate timed-release cryptography in the honest majority setting. In particular, assuming threshold trust in a set of parties that release signatures at a specified time, one can “encrypt to the future” using an SWE scheme. Applications of SWE schemes include voting, auctions, distributed randomness beacons, and more. However, the lack of homomorphism in existing SWE schemes reduces efficiency and hinders deployment. In this work, we introduce the notion of homomorphic SWE (HSWE) to improve the practicality of timed-release encryption schemes. We show one can build HSWE using a pair of encryption and signature schemes where the uniqueness of the signature is required when the encryption scheme relies on injective one-way functions. We then build three HSWE schemes in various settings using BLS, RSA, and Rabin signatures and show how to achieve a privacy-preserving variant that only allows extracting the homomorphically aggregated result while keeping the individual plaintexts confidential.

3. Dynamic-FROST: Schnorr Threshold Signatures with a Flexible Committee

Annalisa Cimatti, Francesco De Sclavis, Giuseppe Galano, Sara Giammusso, Michela Iezzi 2 , Antonio Muci, Matteo Nardelli, and Marco Pedicini

Threshold signatures enable any subgroup of predefined cardinality t out of a committee of n participants to generate a valid, aggregated signature. Although several (t, n)-threshold signature schemes exist, most of them assume that the threshold t and the set of participants do not change over time. Practical applications of threshold signatures might benefit from the possibility of updating the threshold or the committee of participants. Examples of such applications are consensus algorithms and blockchain wallets. In this paper, we present Dynamic-FROST (D-FROST, for short) that combines FROST, a Schnorr threshold signature scheme, with CHURP, a dynamic proactive secret sharing scheme. The resulting protocol is the first Schnorr threshold signature scheme that accommodates changes in both the committee and the threshold value without relying on a trusted third party. Besides detailing the protocol, we present a proof of its security: as the original signing scheme, D-FROST preserves the property of Existential Unforgeability under Chosen-Message Attack.

4. Jigsaw: Doubly Private Smart Contracts

Sanjam Garg, Aarushi Goel, Dimitris Kolonelos, and Rohit Sinha

Privacy is a critical concern in the execution of smart contracts on public ledgers. While current practical approaches to privacy-preserving smart contracts effectively address on-chain privacy, they rely heavily on off-chain trusted nodes or servers.

In these systems, clients submit their data to a trusted off-chain server, which is responsible for matching requests and performing the necessary contract computations. However, this setup grants the server full visibility into both client identities and their data, leading to significant privacy compromises. This limitation has become a major challenge in prominent blockchain applications, particularly in Decentralized Finance (DeFi).

We propose a novel framework for smart contracts that ensures doubly private execution, addressing both on-chain and off-chain privacy concerns. In our framework, clients submit their requests in a privacy-preserving manner to a group of (potentially mutually untrusting) servers. These servers collaboratively match client requests without learning any information about the data or identities of the clients.

We then present Jigsaw, an efficient cryptographic realization of our proposed framework. Jigsaw builds on the ZEXE architecture (Bowe et al., S&P 2020), which leverages zkSNARKs, and extends Collaborative zkSNARKs (Ozdemir and Boneh, USENIX 2022) to enable proof generation by a group of servers.

In Jigsaw, we introduce a novel collaborative zkSNARK construction that achieves low latency and reduced proving time, and showcase these advantages over sample applications ranging from trading in a decentralized exchange to auctions and voting. Our experiments demonstrate that Jigsaw is roughly 40 − 50x faster in proof generation and uses orders-of-magnitude less bandwidth than the naive approach of using off-the-shelf Collaborative zkSNARKs

Invited Talk: Anonymous Credentials: Past, Present and Future

Daniel Slamanig

Anonymous credentials are an important cryptographic concept, envisioned in the 1980s by Chaum, to enable privacy-friendly authentication. In recent years, they have experienced renewed interest, driven by new applications and increased attention from industry. In this talk, we will review the basic concept, explore different properties and types of such schemes (and their relation to blockchains), and examine current constructions of anonymous credentials. We will also take a look into the future — specifically the post-quantum setting — and discuss open research problems.

5. Putting Sybils on a Diet: Securing Distributed Hash Tables using Proofs of Space

Christoph U. Günther, and Krzysztof Pietrzak

Distributed Hash Tables (DHTs) are peer-to-peer protocols that act as components for more advanced applications. Recent examples, driven by blockchains, include decentralized storage networks (e.g., IPFS, Autonomi, Hypercore, and Swarm), data availability sampling, or Ethereum's peer discovery protocol.

In the blockchain setting, DHTs are susceptible to Sybil attacks, where an adversary disrupts the network by adding numerous malicious nodes. Preventing such attacks requires limiting the adversary's ability to create a large number of Sybil nodes. Surprisingly, the aforementioned applications implement no such measures. Seemingly, existing techniques are unsuitable for these applications.

For example, a straightforward technique described in the literature uses proof of work (PoW), where nodes periodically challenge their peers to solve computational puzzles. This approach, however, performs poorly in practice. Since these applications do not require honest nodes to have substantial computational power, the challenges cannot be too difficult. As a result, even moderately capable hardware can sustain many Sybil nodes.

In this work, we explore using Proof of Space (PoSp) to limit the number of Sybils in DHTs. While PoW proves that a node wastes computation, PoSp proves that a node wastes disk space. This aligns better with the resource needs of these applications: Many of them are storage-focused and rely on honest nodes contributing significant disk space to ensure functionality.

With this in mind, we propose a mechanism to limit Sybils where honest nodes dedicate a constant fraction of their disk space to PoSp. This ensures that an adversary cannot control a constant fraction of DHT nodes unless it contribute a constant fraction of the whole disk space contributed to the application overall. Since this is typically a considerable amount, Sybil attacks become economically unfeasible.

6. Nakamoto Consensus from Multiple Resources

Mirza Ahad Baig, Christoph U. Günther, Krzysztof Pietrzak

The blocks in the Bitcoin blockchain “record” the amount of work W that went into creating them through proofs of work. When honest parties control a majority of the work, consensus is achieved by picking the chain with the highest recorded weight. Resources other than work have been considered to secure such longest-chain blockchains. In Chia, blocks record the amount of disk-space S (via a proof of space) and sequential computational steps V (through a VDF).

In this paper, we ask what other weight functions $\Gamma(S,V,W)$ (that assign a weight to a block as a function of the recorded space, speed, and work) are secure in the sense that whenever the weight of the resources controlled by honest parties is larger than the weight of adversarial parties, the blockchain is secure.

We completely classify such functions in an idealized “continuous” model: $\Gamma(S,V,W)$ is secure if and only if it is homogeneous of degree one in the timed resources V and W, i.e., $\alpha\Gamma(S,V,W)=\Gamma(S,\alpha V,\alpha W)$. This includes the Bitcoin rule $\Gamma(S,V,W)=W$ and the Chia rule $\Gamma(S,V,W) = S \cdot V$. In a more realistic model where blocks are created at discrete time-points, one additionally needs some mild assumptions on the dependency on S (basically, the weight should not grow too much if S is slightly increased, say linear as in Chia).

Our classification is more general and allows various instantiations of the same resource. It provides a powerful tool for designing new longest-chain blockchains. E.g., consider combining different PoWs to counter centralization, say the Bitcoin PoW W_1 and a memory-hard PoW W_2. Previous work suggested to use W_1+W_2 as weight. Our results show that using e.g., √(W_1)·√(W_2) or min{W_1,W_2} are also secure, and we argue that in practice these are much better choices.

7. Traceable Verifiable Random Functions

Dan Boneh, Aditi Partap, and Lior Rotem

A threshold verifiable random function (threshold VRF) is a VRF where the evaluation key is secret shared among n parties, and a quorum of t parties is needed to evaluate the VRF. Threshold VRFs are used widely in practice in applications such as randomness beacons and deterministic wallets. Despite their long history, the question of accountability for leaking key shares in a threshold VRF has not been studied. Specifically, consider a set of f parties who use their key shares to create an evaluation box E that lets anyone evaluate the VRF at any point in the domain of the VRF. When f is less than the threshold t, this box E must also take as input t − f additional evaluation shares. Our goal is to design a threshold VRF where there is a tracing algorithm that can trace any such box E to the coalition of f parties that created it, using only blackbox access to E. The risk of tracing should deter the coalition from selling such a box. Questions in this vein were previously explored in the context of threshold decryption and secret sharing. Here we define and study traceability for a threshold VRF. Our traceable threshold VRF is built from a VRF based on Paillier encryption. The starting point for our tracing algorithm is the tracing technique of Boneh-Partap-Rotem (Crypto 2024) designed for tracing leaks in the context of secret sharing. However, there are multiple technical challenges in making this approach work, and we develop the necessary tools to overcome all these challenges. The end result is a threshold VRF with a provably secure tracing algorithm.

8. A Tale of Time Release powered by Blockchain and IBE

Gennaro Avitabile, Nico Döttling, Lucjan Hanzlik, Bernardo Magri, Christos Sakkas, Stella Wohnig

Blockchain protocols have revolutionized the way individuals and devices can interact and transact over the internet. More recently, a trend has emerged to harness blockchain technology as a catalyst to enable advanced security features in distributed applications, in particular fairness. However, the tools employed to achieve these security features were either resource wasteful (e.g., time-lock primitives) or only efficient in theory (e.g., witness encryption). To address this issue, Döttling et al. introduced the McFly protocol,which allows one to efficiently "encrypt a message to the future" such that the receiver can efficiently decrypt the message at the right time. In this talk, we will

1. introduce a primitive called signature-based witness encryption (SWE), which is at the heart of the McFly protocol. In a nutshell, SWE allows to encrypt a plaintext with respect to a tag and a set of signature verification keys. Once a threshold multi-signature of this tag under a sufficient number of these verification keys is released, this signature can be used to efficiently decrypt an SWE ciphertext for this tag.
2. show how SWE can be integrated with a BFT blockchain (or a blockchain finality layer) to achieve Time Release Encryption in the McFly construction. This approach enjoys a number of advantages over previous approaches: There is a very small computational overhead for all involved parties, the users of McFly do not need to actively maintain the blockchain, and are neither required to communicate with the committees, nor are they required to post on the blockchain.
3. discuss the relationship between SWE and Identity-Based-Encryption (IBE) in general and explain the concretely efficient construction of SWE which is based on the BLS signature and the Boneh-Franklin IBE scheme.
4. briefly discuss a novel (theoretical) result on SWE schemes with increased asymptotic efficiency due to Avitabile et al. This scheme's ciphertext size is sub-linear in the number of signers' verification keys used and relies on indistinguishability obfuscation iO and strongly puncturable signatures (SPS).
5. outline open directions.