WHITE PAPER

INTRODUCTION TO MULTIPARTY COMPUTATION (MPC)

FOR NON-CRYPTOGRAPHERS

SEPIOR

FRANK WIENER

JULY 2019

INTRODUCTION TO MULTIPARTY COMPUTATION

For Non-Cryptographers

1 Table of contents

2 Introduction

The need for effective digital security has never been greater than today. Virtually everyone is reliant on internet connected computers and services which store our personal and professional data and digital assets in on-line connected systems that can be hacked. Cryptography can be used protect data and digital assets even if the systems in which they are stored become compromised.

This white paper provides a conceptual introduction to Multiparty Computation (MPC) and its application in the field of threshold cryptography, a specialized subfield of cryptography. This paper is intended for general audiences who may not have a background in cryptography but seek to understand the concepts of MPC and its role in distributed and secure cryptographic operations such as encryption / decryption, and digital signature generation.

2.1 A Brief Introduction to Cryptography

Cryptography has been used to protect data for more than a thousand years, going back to the days of Julius Caesar and the Roman empire. The idea was simple, use an algorithm and a secret code to describe how to scramble data so that the data is meaningless to anyone who steals the data, but readable by anyone who knows the algorithm and secret code.

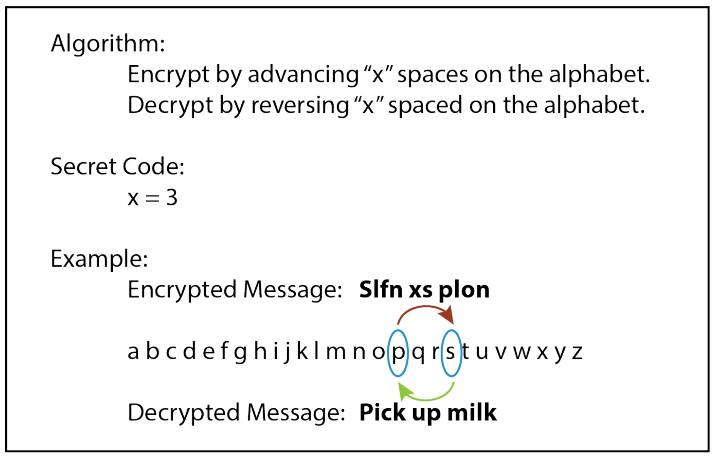

Fig 1) Visual example of simple encryption

As cryptographic algorithms advanced and became virtually unhackable by modern computers the primary concern for effective data security was protecting the secret codes, also known as private keys. ***These keys are used to create a unique scrambling of the data or to generate a unique digital signature. If the keys are stolen the data can be decrypted and digital signatures can be forged. Consequently, key management systems (KMS) which create, maintain and protect cryptographic keys have become the most critical component of today's cryptographic solutions.***

2.1.1 Right Fitting Security

In many cases the probability of having data stolen or a signature forged is low and the consequences if they do occur are also low. In those situations, cryptographic services may not be required. If they are employed, the solution should be as operationally simple and low cost as

possible, otherwise the cost or operational complexity of security can exceed the benefits of cryptographic security.

In other cases, the probability that a hacker will be both motivated and skilled enough to penetrate conventional security systems and steal confidential data or to forge an authorization signature is high, and the consequences when those events happen are also high. For those situations, we need to raise the bar on cryptography high enough so that adversaries determine it's not worth the time, effort, and/or money to hack your stuff.

Over the past two decades, highly specialized physical appliances known as hardware security modules (HSMs) were designed to generate and/or store private keys and provide cryptographic services when high security was deemed critical. HSMs are designed for placement in centralized, physically secured environments with highly restricted access by specially trained personnel to operate and maintain them. The systems are designed to be tamper-resistant and may even destroy locally stored data in the event that unauthorized tampering is detected.

To maximize security, documents requiring decryption or digital signatures may be forwarded to centralized HSMs for cryptographic services. With this process, the private keys used for these cryptographic services never leave the HSM. The assumption is that long as the HSM is physically secure, the keys are also secure which means the encrypted content is secure and signatures can be trusted.

2.1.2 MPC and Threshold Cryptography for MPC-based Key Management Services

Secure multiparty computation (MPC) was introduced in the 1980's. The original goal was to develop mathematical techniques allowing multiple parties to compute functions of their combined inputs, without revealing their corresponding inputs to one another or any other party.

The concept of MPC can be applied to virtually any problem involving confidential data from multiple parties. MPC is particularly useful for preserving the confidentiality of the private key used to decrypt data or to generate a digital signature. Threshold Cryptography is a term to describe cryptographic key management using MPC.

Rather than creating a whole private key and storing it on a device which can be compromised, MPC generates shares of a private key on the device used by each of multiple parties. MPC then computes across the shares held by participating parties to generate the digital signature or to decrypt data without ever having to produce or recreate a whole key on any appliance at any time.

By doing so, MPC eliminates the potential that one party becomes corrupted and misuses the key. It also eliminates the dependency on specialized secure hardware appliances, and assures accurate and secure cryptographic operations even with widely distributed, potentially untrusted devices or clouds, without any special forms of physical security.

While MPC offers tremendous hope and potential early implementations were computationally intensive and relatively slow compared to legacy key management systems. Early on, the algorithms required that all parties be online and interconnected concurrently to provide real-time cryptographic services. Iterative computations were executed across the multiple parties and the required compute resources, network connectivity, availability of mobile devices, and execution

time required were complicating factors for many use cases. Consequently, MPC was relegated to theory and academic studies until 2008 when some of Sepior's co-founders led the implementation of the world's first MPC systems in conjunction with the Danish Sugar Beet Auctions.

2.3 MPC Today

MPC has come a long way, but not all MPC systems are created the same. Modern implementations no longer require that all parties be concurrently online and communicating to execute cryptographic operations. However, many MPC implementations may be challenged to support sustainable high-performance operations at scale.

Multiple of Sepior's co-founders have been at the forefront of MPC for decades. They've been developing patent pending techniques and performance optimized implementations of multiple share models which provide equal to superior security effectiveness, with similar or better performance than legacy systems. And they've done so while achieving lower cost implementations. Perhaps more importantly, these MPC implementations can achieve industry leading performance while operating in a deeply distributed, software-defined operational framework which maintains security even when the reality of system failures and compromised participants occur.

Effectively implemented MPC-based key management systems provide threshold cryptographic services which are more effective, operationally compatible with today's distributed applications and decentralized services, and provide greater confidentiality, integrity, and availability than any other known key management alternative.

3 An MPC Description in Very General Terms

Multiparty computation (MPC) is a highly specialized mathematical approach used by cryptographers in the field of threshold cryptography to provide highly secure key management services. MPC is particularly compelling for this use case for two primary reasons:

- It provides cryptographic services without any reliance on sharing secrets with anyone, including a trusted third party which is subject to compromise,
- and it does so even when some parties become hacked or otherwise compromised.

Both of these attributes are profoundly different from conventional security paradigms. For cryptography there is historically a reliance on a trusted third party with which secrets are centrally shared and stored for some period of time. You can trust the system to the degree you can trust the trusted third party. If an insider acts maliciously or if systems become compromised, all trust can be violated.

3.1 An Oversimplified Example of MPC For Threshold Cryptography

As referenced in section 2.1 cryptography uses the combination of a standardized algorithm and a secret code. In that example, the secret code was the number 3. Following is an oversimplified

example of how MPC can break that code value into discrete shares which when collectively added up equals 3.

Party 1's Share: 401

Party 2's Share: 99

Party 3's Share: -497

Collective Value: 3

When we add all of those shares together, the value is 3, just like the secret code. The difference is, if a hacker breaks into Party 1's device they will find a value of 401. With that share alone they cannot deduce the value of the secret code. If they hack into two systems they have a value of 500. Once again this is interesting, but they still have no idea of the value of the secret code. If they break into all three party's devices they will have three values (401, 99, -497). However, they don't know if the MPC algorithm requires all three values to be added together, or if any other random combination of potential computations is required to determine the value.

Collectively, these attributes of MPC make the odds of a hacker breaking into all three party's systems, and correctly guessing the MPC algorithm low. This shifts the key protection concept from relying on a single trusted third party to keep your key secure and it eliminates the need to depend on physical device security to maintain the key security.

Above is an example of a three-party approval scheme where all members of system must participate to provide the private key to execute cryptographic operations. This is referred to as a 3 of 3 MPC model. As you might imagine, we could design MPC to have more than three or less than three (at least two) parties. There is also a way to design the computations where only a subset of the parties needs to be available to calculate the private key value. This is where the math becomes far more complex and is beyond the scope of this paper. However, this paper will elaborate on the general concepts and attributes of these more advanced MPC concepts.

3.1.1 Randomness and Range

While the above example is clever, a hacker could randomly guess different values to see what code might work. That's why cryptographic algorithms use random codes with a sufficiently large range of potential values to make it so impractical to randomly guess that it becomes virtually impossible. By choosing the proper cryptographic algorithms, the fastest computers could take years or longer and still not be able to generate and test every combination of possible alphanumeric codes. During that iterative code generation process, the value of the key will typically be changed multiple times, giving hackers a moving target which effectively resets the clock and further decreases the probability of converging on an accurate guess.

3.2 MPC Shifts Trust From Centralized to Decentralized

Traditional cryptography requires the user to place trust in either their own computing device to securely store the private key (without ever being hacked, lost, or otherwise compromised), or place their trust with a third party such as an HSM to securely store the private key. Threshold

cryptography eliminates the requirement to centrally trust any single party by using MPC to shift trust from a centralized to a decentralized model.

Threshold cryptography accomplishes this shift by operating highly specialized MPC algorithms across multiple devices to collectively provide lifecycle key management services. MPC algorithms generate each private key in the form of decentralized key shares which are natively created and stored on the device of each party. When cryptographic operations are required, MPC executes across the parties' devices to collectively confirm that a sufficient number of key shares are available to authorize and execute the operation. The MPC algorithm completes the operation without ever transferring data between any parties which could be used to derive the private key.

To maximize security, the devices should each be controlled by a different party and preferably in different networks. This approach would require an adversary to hack into multiple different computing devices, in different networks, concurrently. They would then have to develop MPC algorithms to properly compute across a sufficient number of key shares to execute the cryptographic operation, and they would need to complete all of this before the breech is detected or before the key is refreshed.

This decentralized trust attribute combines with several other MPC attributes to produce a security framework that supports the highest level of key management security available, without requiring costly and operationally constraining HSMs. It also aligns far more favorably and can scale dynamically as users scale.

3.3 Virtually Unlimited Implementation Models

The decentralized nature of threshold cryptography supports a virtually limitless number of applications and use case configurations. It's primarily up to the service providers to decide which implementation approach best satisfies their collective requirements for performance, scale, flexibility, and degrees of security.

For example, threshold cryptography is gaining widespread support for providing transaction signing services of cryptocurrencies and other digital assets. This is primarily because Threshold Signatures, a threshold cryptographic approach to digital signatures, provide better security, with better performance, and lower costs than alternative models.

Threshold Signatures can be implemented using a variety of multiparty approval schemes for digital signature authorization. In this application, the end customer of the service with the digital assets is likely to be one of the approving parties. The digital asset exchange or broker will likely be one of the parties. Exchanges seeking to elevate security above a two-party model may have a trusted third party which provides another independent level of authorization. If even higher security is required, additional parties may be added. In this scenario, at least three parties are likely to have different devices, under different administrative control, in different networks.

Another example might be to provide key management services for transaction signing and privacy control through encryption of smart contracts on permissioned blockchains. In this scenario, one of the likely parties may be the blockchain as a service provider, the party signing

off their portion of a smart contract, one or multiple enterprises with a primary interest in the integrity of the blockchain-based services, and/or independent cloud service providers.

As the number of parties increase, the diversity of device types, administrative domains, networks, and geographies increase which can incrementally increase the security levels. However, as with all network-based systems it's a matter of optimization across multiple considerations for a given use case and the ability of the MPC algorithms to efficiently balance the collective requirements.

3.4 Definable Thresholds – m of n Quorum Support

MPC supports the concept of thresholds under which certain services can be executed at the cryptographic operations layer (meaning the actual encryption, decryption, or digital signing). One of those threshold concepts is to require that a minimum of m parties out of a pool of n potentially available parties must participate with their shares of a private key before cryptographic operations are provided. This cryptographic quorum approval support assures operations even if some (n-m) of the parties are not available to authorize an operation, and it provides added degrees of security. In doing so it collectively increases availability and confidentiality for all cryptographic functions.

Certain implementations of MPC for threshold cryptography can support up to m=20 parties. N must be greater than or equal to m. As the number of parties increase the time required for collective computation can also increase, so current implementations which may be time sensitive tend to use two, three or four parties at the cryptographic quorum layer.

3.4.1 Definable Quorums at the Business Operations Layer

While two or three separate parties is widely regarded as sufficient for industry leading security at the cryptographic operations layer certain applications may require more approvers at the business operations layer. For example, a broker executing a very large digital asset trade may require multiple levels of in-house approval before the broker signs off with their approval. Depending on the value of the trade they may require one to three or more internal approvers.

This level of business operations quorum support is typically defined at a layer above the cryptographic quorum operations layer. As these business operations quorums are implemented and satisfied, the collective enterprise approval will then be presented at the cryptographic operations layer for cryptographic approval.

This disintermediation between quorums operating at the cryptographic operations layer and the business operation layer provides flexibility at the business level, with optimization and consistency at the cryptographic level.

3.5 Definable Thresholds – Corrupt Parties Tolerance

One of the principle requirements for any cryptographic service is to prevent unauthorized users from executing cryptographic operations. But what happens if one of the parties become compromised? Should all cryptographic services be prevented? With typical cryptography that would be the case. However, threshold cryptography introduces the ability to maintain safe and secure cryptographic operations even if one or potentially more of the parties' devices become

compromised. This allows for corrupt systems to be recovered without the service disruption that exists with conventional systems.

Threshold cryptographic supports the definition of a threshold t for the number of parties which may be corrupt, potentially deviating from the defined protocol, and still allow legitimate cryptographic operations to proceed as usual. Certain implementations of threshold cryptography will provide continued secure operations as long as the majority of parties remain honest or not corrupt. Other implementations support sustained secure operations even in the presence of a dishonest majority, where more than half of the parties are corrupt.

In either case, this dimension of threshold MPC enables a higher degree of operational integrity and operations availability as it enables proper operations even under non-ideal real-world conditions which conventional cryptographic systems cannot tolerate.

3.6 Definable Thresholds – Key/Share Regeneration

Yet another threshold cryptographic concept with MPC is to define a threshold t' for the minimum number of non-corrupted parties that must be available to generate key shares to replace lost shares of an existing key, or to generate new shares of an existing or new private key. This attribute of threshold cryptography is extremely powerful for flexible key management and restoring full system tolerances following the inevitable compromise of a party's device.

Let's look back at the example in Section 3.1. That example used three different share values (401, 99, -497) which were added together to compute the private key value of 3. If one party's device becomes compromised we should assume that the adversary learned the value of the key share. One approach would be to generate an entirely new private key in the form of new key shares on each party's device.

But what if the use case is for an enterprise wallet, where customers issue payments to a published account address? For cryptocurrencies like Bitcoin, generating a new private key will result in a new address which will have to be communicated to all customers seeking to make payments to the current account. For many businesses, changing a published address is undesirable. Fortunately, MPC introduces an attractive alternative.

Rather than changing the entire private key, MPC can simply generate new key shares on each party's device, which when added together still equals the value of the private key: 3. This way, the key shares can be refreshed but the integrity of the private key is retained and the published account number remains the same.

Key Share Refresh Example

Existing Key and Shares	Refreshed Key and Shares
Party 1: 401	Party 1: 100
Party 2: 99	Party 2: -400
Party 3: -497	Party 3: 303
Collective Value: 3	Collective Value: 3

Given a virtually infinite number of potential share combinations, key shares can be refreshed a virtually infinite number of times. This makes it feasible to publish and securely maintain a static account address if desired. In other cases, it may be preferable to change the value of the private key. MPC can facilitate private key generation as well.

This dimension of threshold cryptography further elevates the ability to assure availability, even in the event of key share losses and to assure integrity by generating the equivalent of new keys either on demand or on a pre-determined basis to further reduce the risk of a key compromise.

3.7 Native High Availability Architecture

The ability of MPC-based systems to maintain operations even where parties become corrupt, to continue with many operations even if one or potentially more parties become unavailable, and the ability to refresh or regenerate keys or key shares even when a subset of parties are corrupt provides a materially higher degree of system availability than traditional appliance-based key management solutions. If required, higher degrees of availability assurance are achievable with various threshold configurations and if preferred more conventional redundancy measures can be taken as well.

3.8 MPC Performance Optimizations

As we understand the operational concepts and flexibility of MPC we can begin to understand why it took time before performance optimized implementations were practical at scale. One of the biggest concerns with MPC was the speed at which cryptographic services can be rendered. No one wants to wait extra time for a document to be decrypted or a transaction to be signed before processing. Vendors such as Sepior have been hard at work on these optimizations for many years.

Sepior has applied a combination of published best practices, patent pending techniques, and trade secrets to provide threshold cryptographic systems to provide the compelling attributes above, with performance which is equal or superior to conventional alternative key management systems.

3.9 Collectively Compelling

MPC has many more definable attributes which are discussed in more detail in other documents. Collectively, these threshold and MPC-based system attributes establish threshold cryptographic services using MPC as the true next generation of key security and lifecycle key management for Web 2.0 and ultimately 3.0 based applications and services. The systems are fully virtualized,

software defined, capable of supporting effectively unlimited scale, with distributed parties and a uniquely secure and resilient operational framework which provides industry leading confidentiality, integrity, and availability (CIA).

4 Distributed Share Generation Versus Sharding

The concept of distributing shares of a key across multiple parties is not new. Sharding is a well-established technique which allows a key that is centrally generated to be broken into shards or fractions which can be distributed to multiple parties for distributed storage. While sharding is more secure than conventional key storage it is materially different from MPC. Sharding still has the problem of centrally creating and typically storing an entire key on one or more appliances, such as HSMs. Additionally, sharding requires all of the key shards to be recombined into a whole key before cryptographic operations can be executed. If any of the shards are lost or become unavailable, cryptographic operations may be prevented. It also results in the creation of a whole key on one or multiple devices which when hacked yields the private key and thus creates a single point of failure vulnerability.

MPC natively generates a unique share of a single private key on each of the n parties' devices, and it later uses at least m (a subset of n) of those key shares to conduct the required cryptographic operations. One of multiple fundamental differences between MPC and sharding is the fact that with MPC an entire key does not have to be created on any device at any time, and the shares are not required to be recombined to create a whole key at any time. Naturally, this attribute dramatically reduces the potential for key theft.

Furthermore, the ability of MPC to regenerate replacement shares for lost key shares or new keys, when desired, eliminates the requirements to store a copy of the key shares on HSMs. Of course, there is nothing to prevent one from storing copies of key shares on an HSM for backup if desired. But such backup copies should not be required unless if your security planning includes the potential for catastrophic events resulting in multiple concurrent system failures, such as the loss of more than t' devices with key shares concurrently. If the MPC ecosystem is designed and implemented properly this should be a highly unlikely scenario, baring wide ranging extreme natural disasters or manmade catastrophes. If such planning is within your scope, MPC fully supports this option.

5 NIST Threshold Cryptography Initiative

The National Institute of Standards and Technology (NIST) recently launched initiatives to develop formal standards which will enable customers to verify that various vendor implementations of threshold cryptographic systems comply with recommended guidelines. Those specifications are in process and will take time before completion and formal adoption. Until then, it's highly recommended to work with well established companies having a solid history in threshold cryptographic implementations of MPC.

6 World Renowned Leaders in MPC

Several of Sepior's co-founders and primary developers are recognized for their pioneering work in MPC and cryptography in general. One of numerous noteworthy examples is the 2008 paper on Asynchronous Multiparty Computation – Theory and Implementation by Ivan Bjerre Damgård, Martin Geisler, Mikkel Krøigaard, and Jesper Buus Nielsen.

The first publicly demonstrated implementation of MPC was the Danish Sugar Beet Auctions in 2008. The implementation provided a blind auction where the farmers and market buyers could settle on a price without the farmers ever disclosing how much they were willing to sell their beets for and without the buyers ever disclosing how much they would be willing to pay. What started out as a university project evolved into sustained implementation and operation for many years. Approximately half of the principles leading the above referenced paper and the sugar beet auction implementation came together to found Sepior several years later.

While that first implementation of MPC proved in the concepts and the value proposition for MPC, it also illustrated some of the challenges of effectively implementing MPC in a manner that is widely scalable, executes rapidly, and can be executed using standard off the shelf computing equipment.

Since 2014, Sepior has been developing trade secrets and patent pending techniques to apply MPC the threshold cryptographic key management services. After several years of implementation development and optimization with customers like SBI, Sepior's ThresholdSig implementations achieve transaction performance and scale that is directly comparable to the world's largest and fastest credit card networks.

Sepior's threshold cryptographic protocols have been evaluated for cryptographic integrity by highly respected independent cryptography experts like NCC Group sand CryptoExperts. These reports are available for inspection.

7 More Information

Sepior provides industry leading threshold cryptographic solutions for a range of applications such as securing digital asset and smart contract transactions, providing off-chain privacy controls for permissioned blockchain applications, and securing data and digital assets stored in public or private clouds. If you're interested in learning more about threshold cryptography or any of our solutions, please visit www.sepior.com or drop us an email at info@sepior.com.