INNOVATING FOR PROTECTION

MULTI-PARTY CRYPTOGRAPHY USE CASES

BASED ON SECURE MULTI-PARTY COMPUTATION

ABOUT TRIDENT

MULTI-PARTY

USECASES

GIST

ABOUT & BEYOND PKI
Feb 11, 2020

FERENC PETŐ
ferenc.peto@i4p.com

JOIN OUR PARTNER PROGRAM
AS RESELLER OR DISTRIBUTOR

TRIDENT HSM is the first in the world to offer multi-party cryptography

Verified by the globally recognized Common Criteria EAL 4+ certification

eIDAS Certified Qualified Signature and Seal Creation Device
Post-Quantum crypto support (Sphincs+)

JOIN OUR PARTNER PROGRAM AS RESELLER OR DISTRIBUTOR

INNOVATING FOR PROTECTION

MULTI-PARTY CRYPTOGRAPHY USE CASES

BASED ON SECURE MULTI-PARTY COMPUTATION

ABOUT TRIDENT

MULTI-PARTY

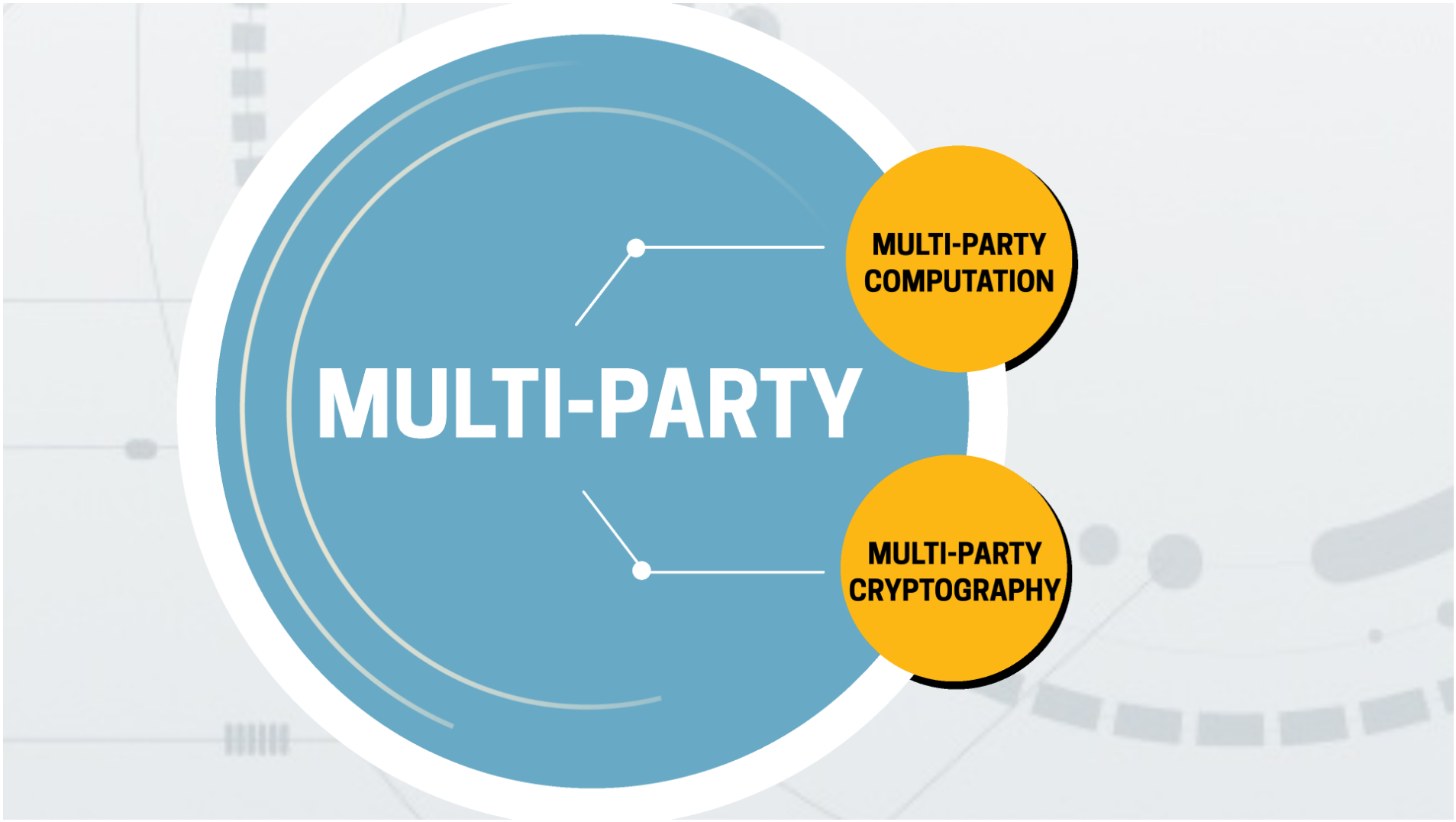
USECASES

GIST

ABOUT & BEYOND PKI
Feb 11, 2020

FERENC PETŐ
ferenc.peto@i4p.com

JOIN OUR PARTNER PROGRAM
AS RESELLER OR DISTRIBUTOR


MULTI-PARTY
MULTI-PARTY COMPUTATION
MULTI-PARTY CRYPTOGRAPHY

SECURE
MULTI-PARTY COMPUTATION

- methods for parties to jointly compute a function over their inputs while keeping those inputs private
- formally introduced in 1982 for the so-called Millionaires' Problem

https://en.wikipedia.org/wiki/Secure_multi-party_computation

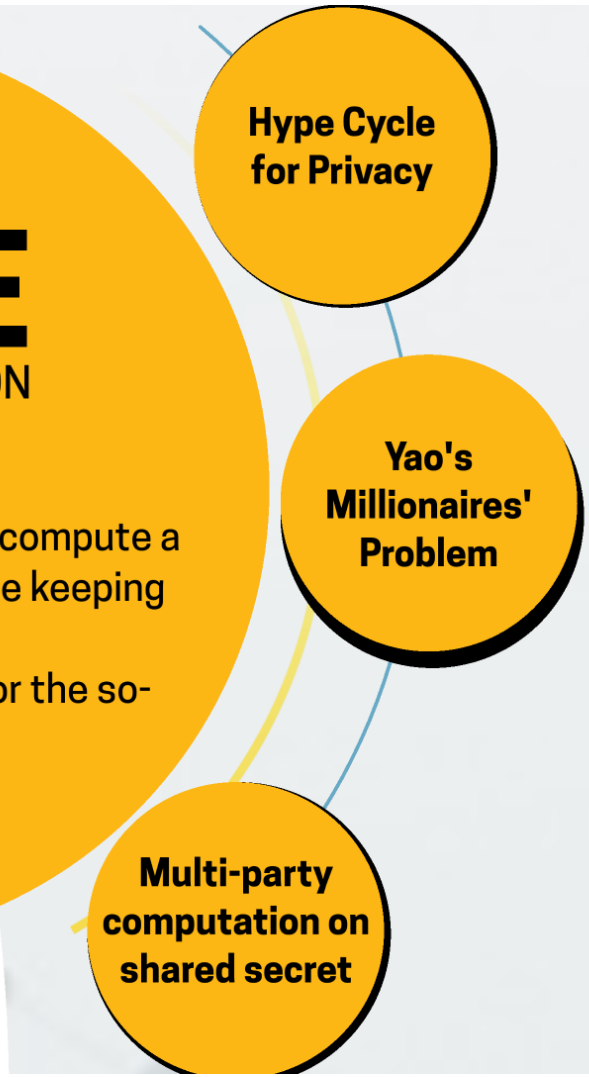
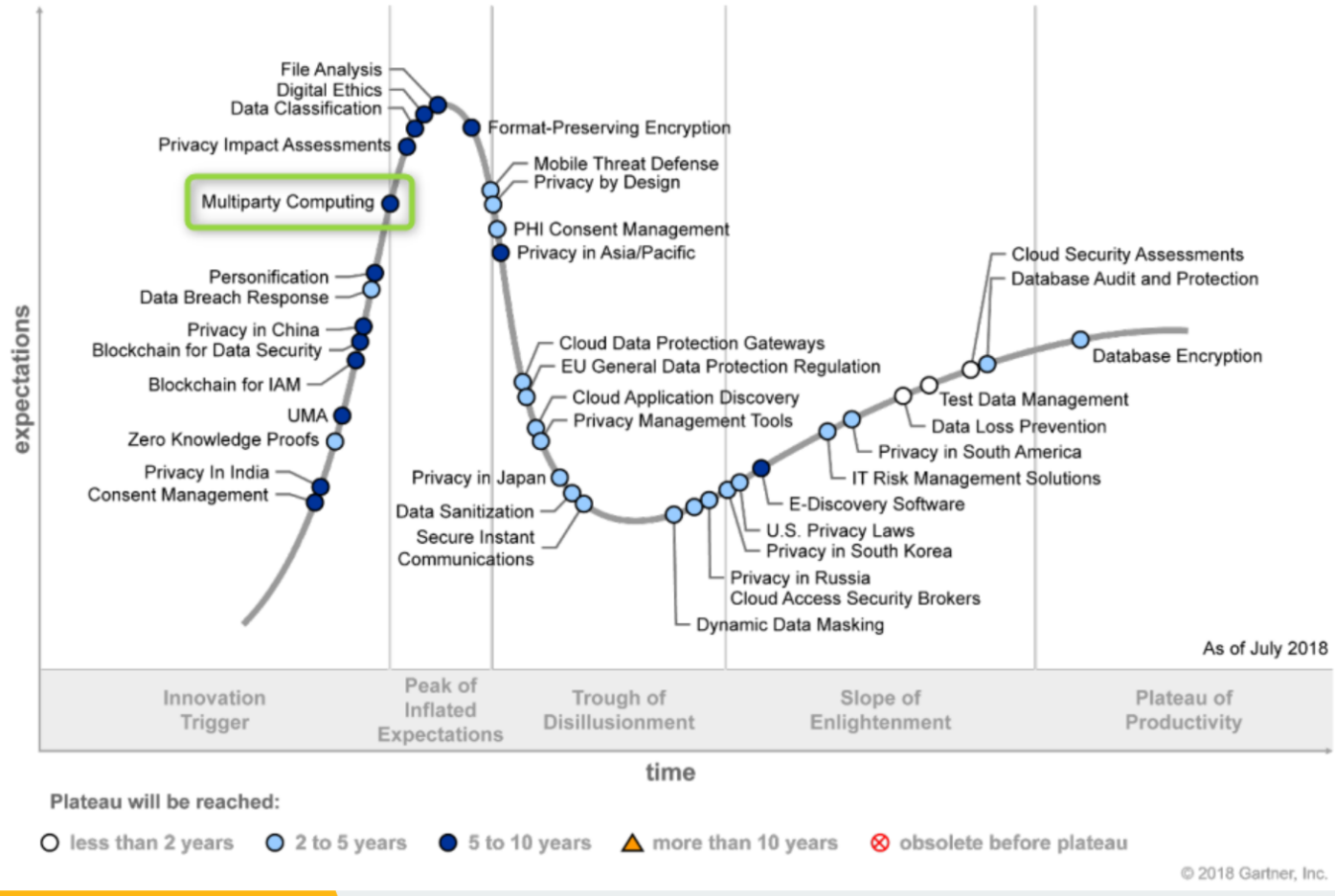
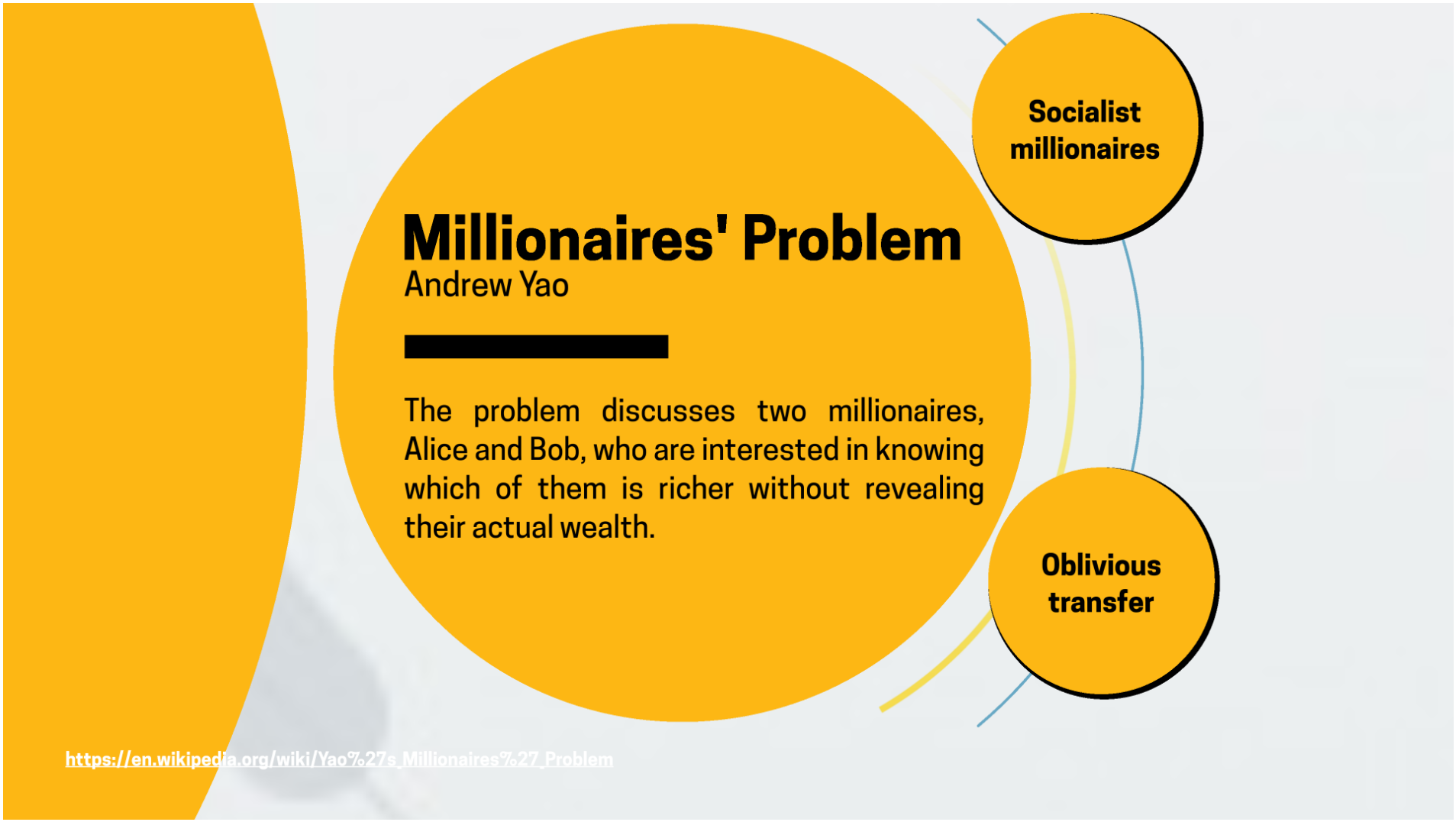


Figure 1. Hype Cycle for Privacy, 2018




Millionaires' Problem
Andrew Yao
The problem discusses two millionaires, Alice and Bob, who are interested in knowing which of them is richer without revealing their actual wealth.
Socialist millionaires
Oblivious transfer
https://en.wikipedia.org/wiki/Yao%27s_Millionaires%27_Problem


Socialist millionaires
It is a variant of the Millionaire's Problem. Two millionaires want to determine if their wealth is equal without disclosing any information about their riches to each other.
https://en.wikipedia.org/wiki/Socialist_millionaires
Alice and Bob
Suggestion boxes
Oblivious messages
Result

Alice and Bob

Suppose Alice and Bob each might be making either 10, 20, 30, or 40 $/hour.

Alice makes 30$/hour
Bob makes 20$/hour

https://en.wikipedia.org/wiki/Socialist_millionaires

Suggestion boxes

Lockable with different matching keys

Bob keeps only the key for the 20$ box and sends them to Alice

http://twistedoakstudios.com/blog/Post3724_explain-it-like-im-five-the-socialist-millionaire-problem-and-secure-multi-party-computation

Oblivious messages

Alice puts a slip of paper saying ‘yes’ into the 30$ box

Bob gets back the boxes and uses his key to unlock the 20$ box

http://twistedoakstudios.com/blog/Post3724_explain-it-like-im-five-the-socialist-millionaire-problem-and-secure-multi-party-computation

Result

Bob knows that Alice doesn't make 20$/hour like he does.

Alice knows Bob doesn't make 30$/hour (Bob shows Alice the slip he pulled out)

Nobody knows how much money the other party makes

http://twistedoakstudios.com/blog/Post3724_explain-it-like-im-five-the-socialist-millionaire-problem-and-secure-multi-party-computation

Oblivious transfer

In a 1-out-of-2 oblivious transfer protocol, the sender has two messages m0 and m1, and the receiver has a bit b, and the receiver wishes to receive mb, without the sender learning b, while the sender wants to ensure that the receiver receives only one of the two messages.

Suggestion boxes using RSA encryption

https://en.wikipedia.org/wiki/Oblivious_transfer

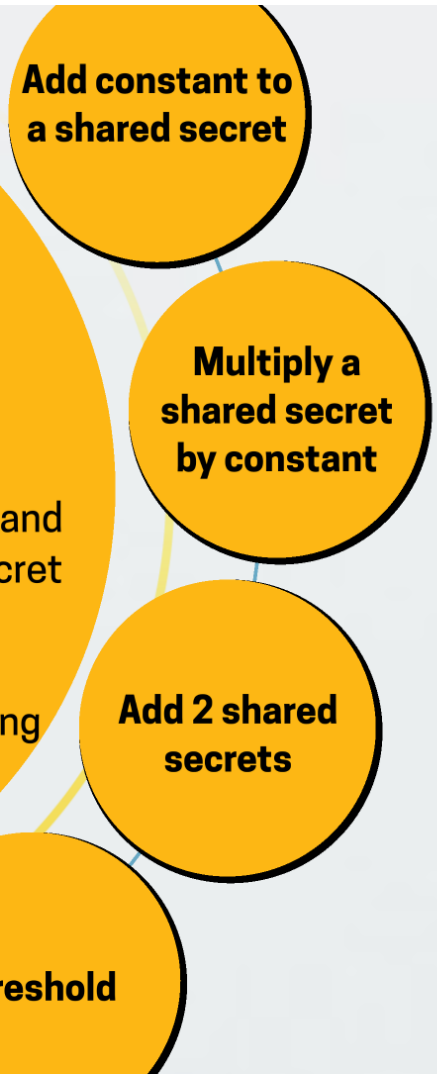
Alice				Bob		
Calculus	**Secret**	**Public**		**Public**	**Secret**	**Calculus**
Messages to be sent	m_0, m_1					
Generate RSA key pair and send public portion to Bob	d	N, e	$\Rightarrow$	N, e		Receive public key
Generate two random messages		x_0, x_1	$\Rightarrow$	x_0, x_1		Receive random messages
					k, b	Choose $b \in \{0, 1\}$ and generate random k
		v	$\Leftarrow$	$v = (x_b + k^e) \mod N$		Compute the encryption of k, blind with x_b and send to Alice
One of these will equal k, but Alice does not know which.	$k_0 = (v - x_0)^d \mod N$ $k_1 = (v - x_1)^d \mod N$					
Send both messages to Bob		$m'_0 = m_0 + k_0$ $m'_1 = m_1 + k_1$	$\Rightarrow$	m'_0, m'_1		Receive both messages
					$m_b = m'_b - k$	Bob decrypts the m'_b since he knows which x_b he selected earlier.

Shared secret

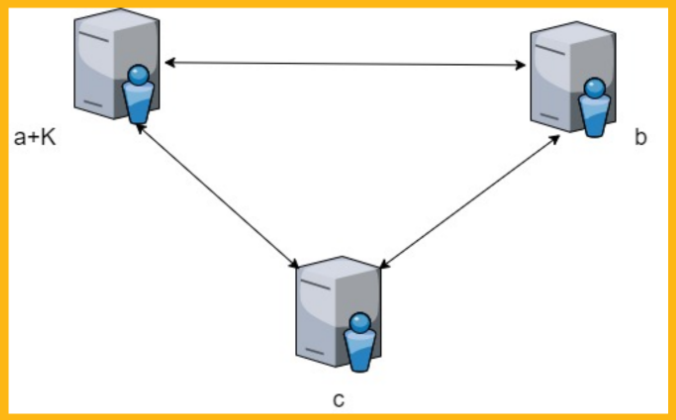
Additive sharing:

Each party has its own part of the secret and the sum of these parts is the global secret that is not known by any of the parties.

Other ways: e.g. Shamir's polynomial sharing

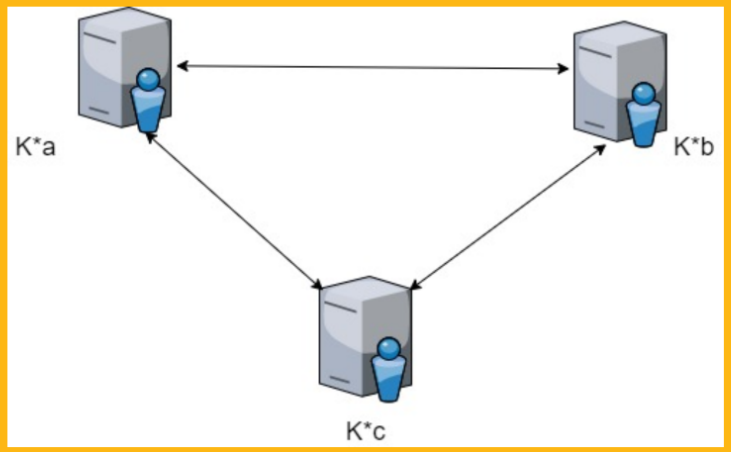


Add constant to a shared secret



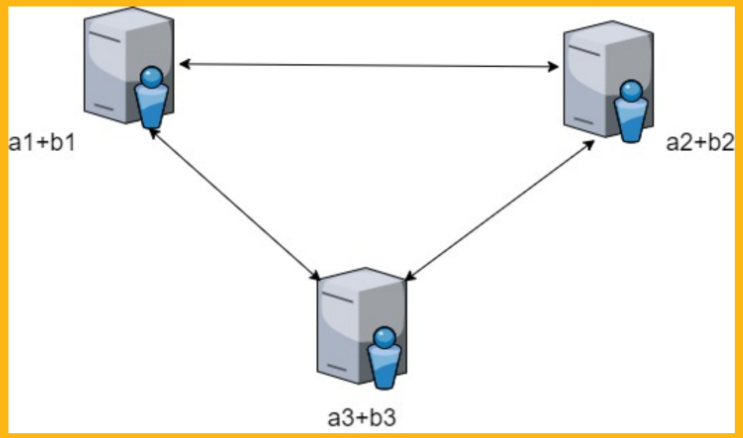
a+b+c+K=(a+K)+b+c

Multiply a shared secret by constant



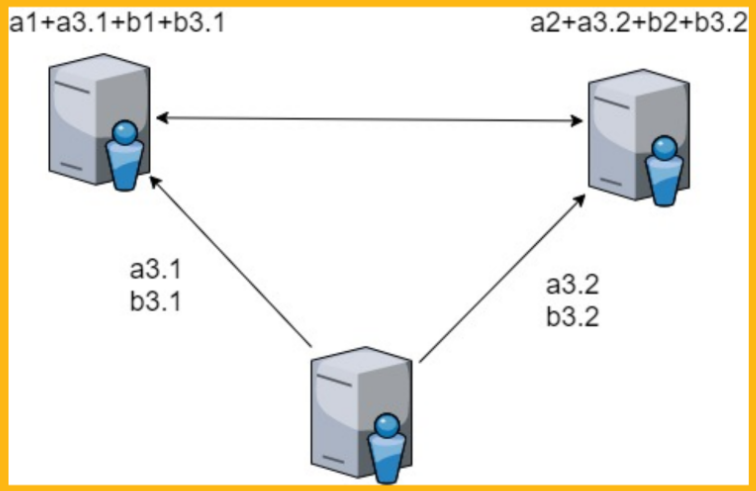
$$K*(a+b+c)=K*a+K*b+K*c$$

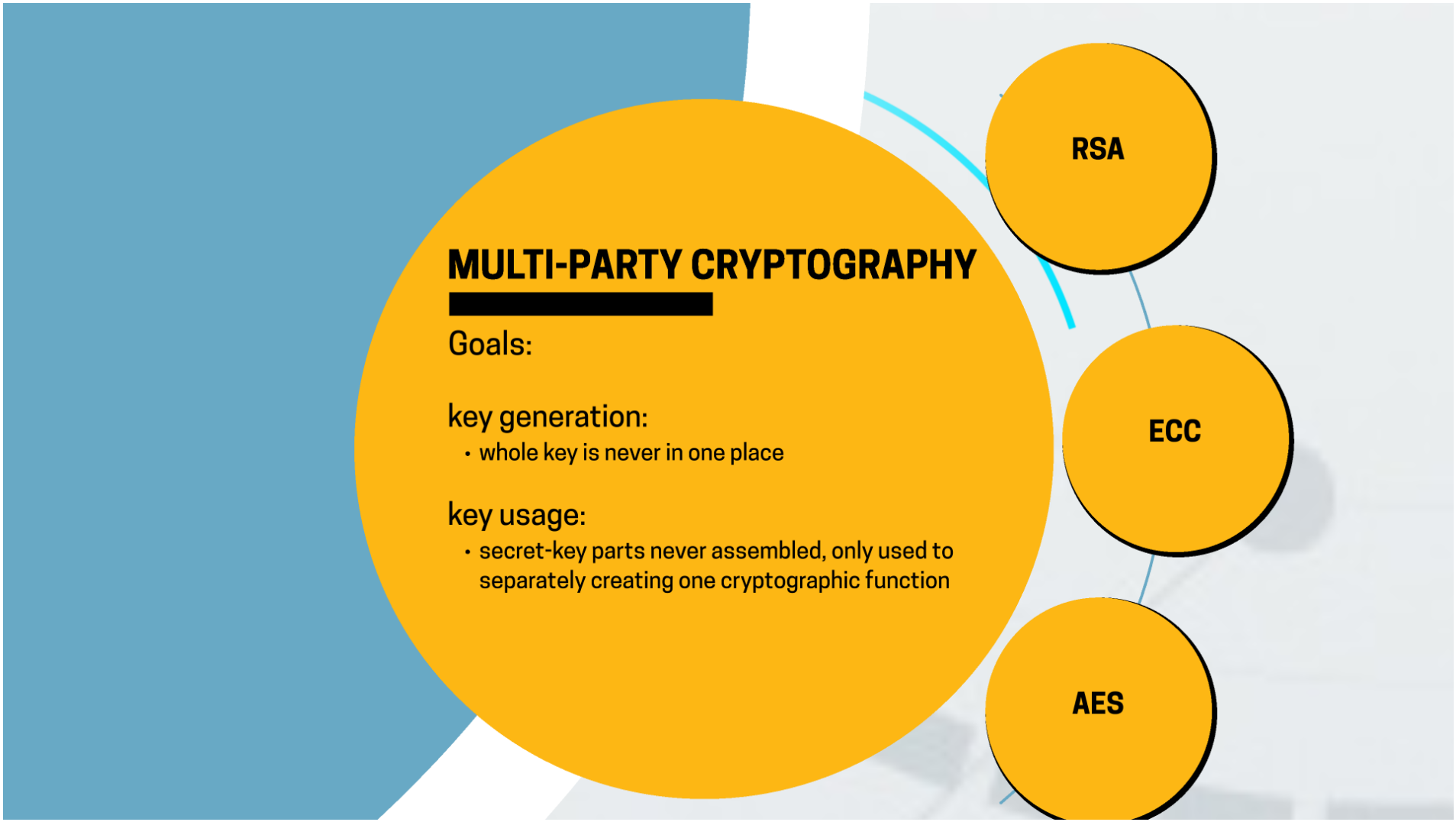
Add 2 shared secrets



(a1+b1+c1)+(a2+b2+c2) =
(a1+b1)+(a2+b2)+(a3+b3)

2 out of 3 threshold




MULTI-PARTY CRYPTOGRAPHY
Goals:
key generation:
• whole key is never in one place
key usage:
• secret-key parts never assembled, only used to separately creating one cryptographic function
RSA
ECC
AES

RSA

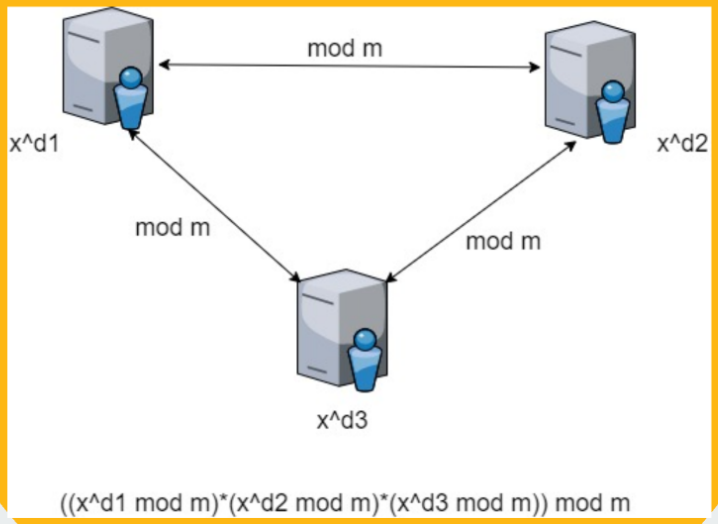
Key usage

Key generation:

Distributed Miller–Rabin primality test

Each of the parties have primes and so the private key (d) as shared secret

Multi-party modular exponentiation



ECC

Key generation:

No need for complex multi-party key generation methods
Random number generation by each parties

Key usage:
SMPC operations with the shared secrets and domain parameters

AES

Key generation:
Random number generation by each parties

Key usage:
SMPC operations

Exciting problem of using lookup tables with an index that is remaining shared secret

INNOVATING FOR PROTECTION

MULTI-PARTY CRYPTOGRAPHY USE CASES

BASED ON SECURE MULTI-PARTY COMPUTATION

ABOUT TRIDENT

MULTI-PARTY

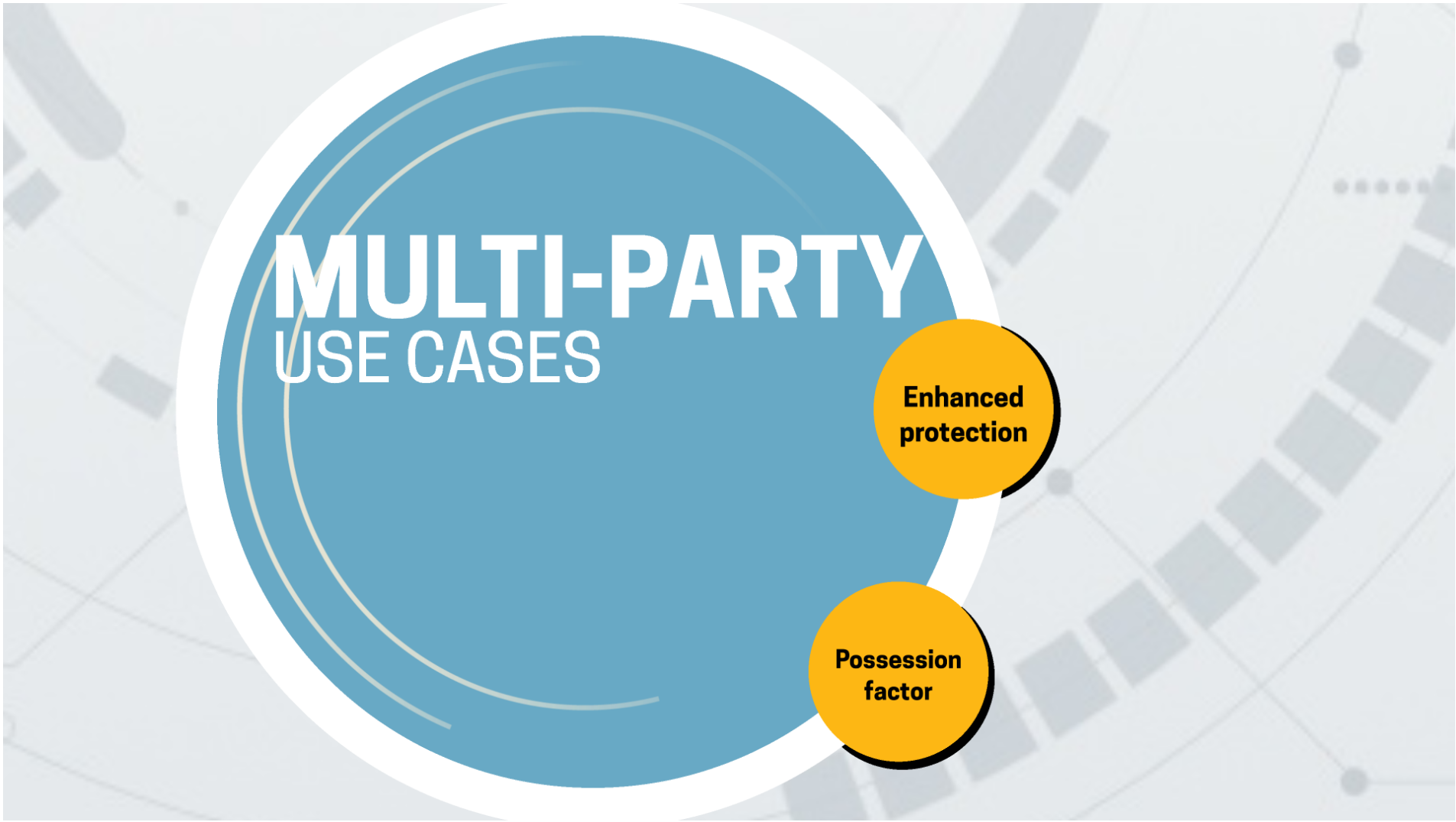
USECASES

GIST

ABOUT & BEYOND PKI
Feb 11, 2020

FERENC PETŐ
ferenc.peto@i4p.com

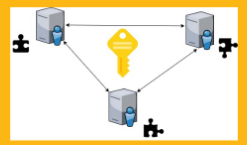
JOIN OUR PARTNER PROGRAM
AS RESELLER OR DISTRIBUTOR

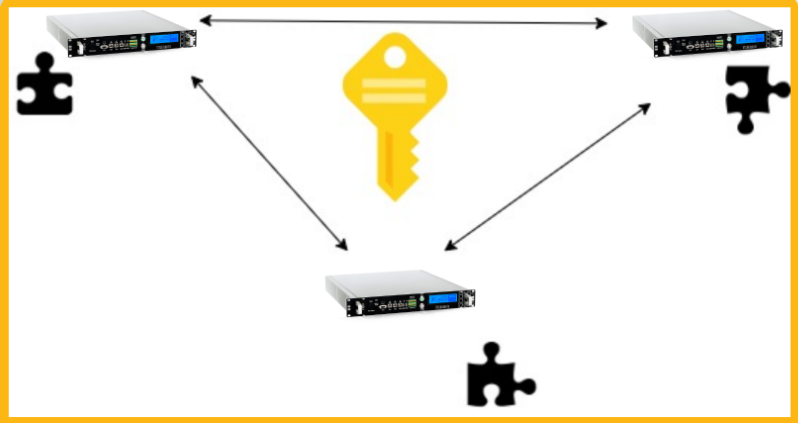

MULTI-PARTY
USE CASES
Enhanced protection
Possession factor

Enhanced protection of your crypto keys

Instead of storing your keys in one single place, you can store it in a distributed cluster

MOST VALUABLE KEYS

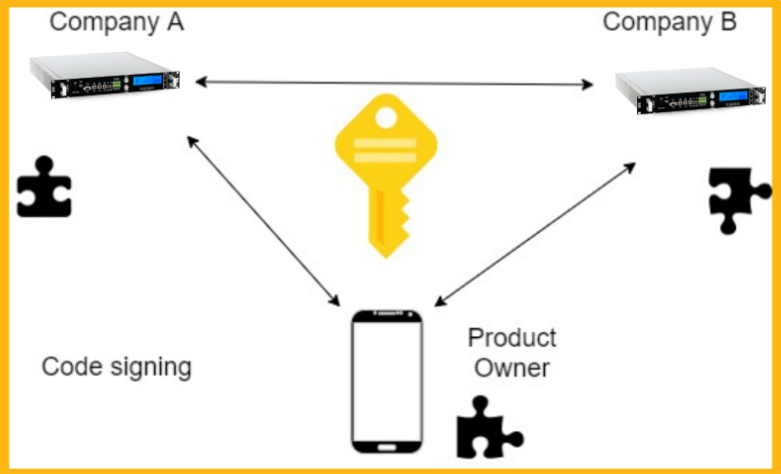


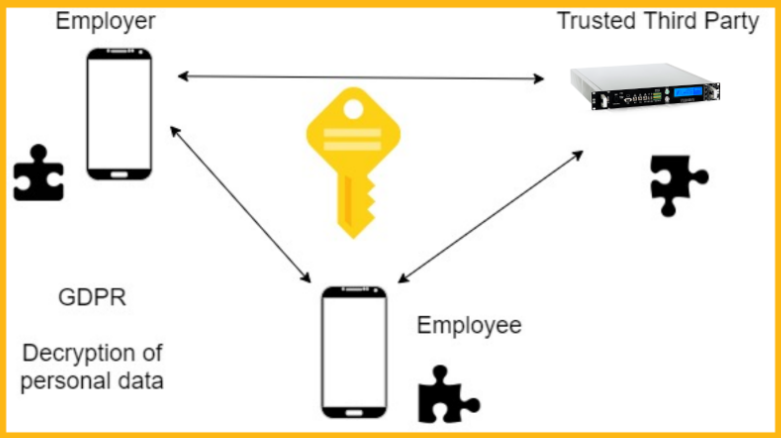


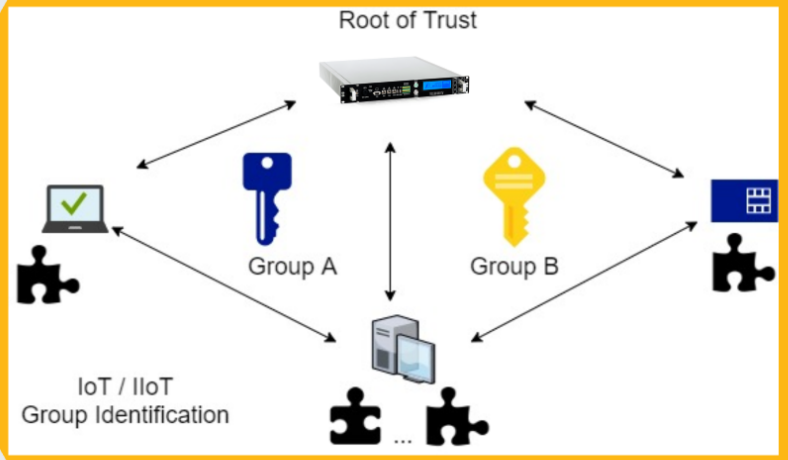
e.g. CA's root key,
master keys etc.

Possessing a key part

parties maybe in an untrusted environment and (even) with conflicting interests to perform a single crypto operation


Company A
Company B
Code signing
Product
Owner


Employer
Trusted Third Party
GDPR
Decryption of
personal data
Employee


Root of Trust
Group A
Group B
IoT / IIoT
Group Identification
...

INNOVATING FOR PROTECTION

MULTI-PARTY CRYPTOGRAPHY USE CASES

BASED ON SECURE MULTI-PARTY COMPUTATION

ABOUT TRIDENT

MULTI-PARTY

USECASES

GIST

ABOUT & BEYOND PKI
Feb 11, 2020

FERENC PETŐ
ferenc.peto@i4p.com

JOIN OUR PARTNER PROGRAM
AS RESELLER OR DISTRIBUTOR

JUST THE GIST

Secure multi-party computation helps you to protect your secret in a way that is never seen before

Possessing at least one part of your secret can provide you possessing the whole secret

Physical protection of that secret is essential

INNOVATING FOR PROTECTION

MULTI-PARTY CRYPTOGRAPHY USE CASES

BASED ON SECURE MULTI-PARTY COMPUTATION

ABOUT TRIDENT

MULTI-PARTY

USECASES

GIST

ABOUT & BEYOND PKI
Feb 11, 2020

FERENC PETŐ
ferenc.peto@i4p.com

JOIN OUR PARTNER PROGRAM
AS RESELLER OR DISTRIBUTOR