Group Homomorphism for Digital Signature privacy control

$$G \rightarrow H$$

$$\varphi_x(u+v) = \varphi_x(v) + \varphi_x(u)$$

Where is equal to means that it represents the same thing which is trust of the elements as a group.

φ is a function for a digital signature of data which includes X a unique identifier as part of the data.

If $\varphi_x(u+v)$ is a valid DSA with X a unique identifier then

$\varphi_x(u)+\varphi_x(v)$ is a valid DSA each having X and are equivalent in trust as belong to the same group.

Lets take an example of elements in two different groups Jane and Kris that should not share elements for trust.

Jane has two elements that define a group A which is a photo p and over 2 1 o.

φ is a function for a digital signature of data. Then

$\varphi(p+o)$ is a valid DSA from a Certificate Authority indicating this is a trusted group A all elements belong to each other.

Kris has two elements that define a group B which is a photo r and under 2 1 u.

$\varphi(r+u)$ is a valid DSA from a Certificate Authority indicating this is a trusted group B all elements belong to each other.

If the Certificate Authority creates a DSA for each element in Jane

$\varphi(p) + \varphi(o)$ the information can be trusted but the membership as a group cannot. If the Certificate Authority (CA) creates a DSA for each element in Kris

$\varphi(r) + \varphi(u)$ the information can be trusted it came from the CA but the membership as a group cannot. The elements could be traded between Jane and Kris such as over 2 1 and now Kris has compromised trust as a group though the data is trusted from a CA.

A Group Homomorphism for Digital Signature privacy control can be created such that the elements can stand on their own and knowledge of what group they belong to can be asserted.

$$G \rightarrow H$$

$$\varphi_x(u+v) = \varphi_x(v) + \varphi_x(u)$$

This is an important privacy control function for Identity. Identity contains many fields of information such as Photo, name, over 21 and address. If you simply need to prove Photo and over 21 there is no need to give your private home address out to strangers. For the case of Jane and Kris

Jane

$$\varphi_j(p+o) = \varphi_j(p) + \varphi_j(o)$$

Kris

$$\varphi_k(r+u) = \varphi_k(r) + \varphi_k(u)$$

Kris cannot trade an element of identity with Jane. This is not a valid DSA for a group

$$\varphi_k(r+u) \neq \varphi_k(r) + \varphi_j(o)$$

Kris cannot compromise his identity for age trading with Jane.

Lets show how this is done.

Jane has two privacy elements that define a group G which is a photo p and over 2 1 o.

φ_j is a function for a digital signature of data that will include j a unique identifier to Jane when creating a valid DSA for data.

Then φ_j (p+o) is a valid DSA from a Certificate Authority indicating this is a trusted group G all elements belong to each other.

A Group Homomorphism can be created for trust of the group using φ_j a function for a digital signature of data that will include j a unique identifier such as the following.

$$G \rightarrow H$$

$$\varphi_j(p+o) = \varphi_j(p) + \varphi_j(o)$$

The privacy elements $\varphi_j(p)$ can be trusted since it is a DSA and can be validated for its origin. The $\varphi_j(o)$ can be trusted also since it is a DSA and can be validated for its origin. The elements can be proven that they belong to each

as a group since the DSA derived from φ_j uses the same unique identifier.

Kris has two elements that define a group H which is a photo r and under 2 1 u.

For Kris φ_k is a function for a digital signature of data that will include k a unique identifier to Kris when creating a valid DSA for data.

Then φ_k (r+u) is a valid DSA from a Certificate Authority indicating this is a trusted group H all elements belong to each other.

The privacy elements $\varphi_k(r)$ can be trusted since it is a DSA and can be validated for its origin. The $\varphi_j(u)$ can be trusted also since it is a DSA and can be validated for its origin. The elements can be proven that they belong to each as a group H since the DSA derived from φ_k uses the same unique identifier.

Kris cannot trade an element of identity with Jane. This is not a valid DSA for a group since the unique Ids would be different.

$$\varphi_k(r+u) \neq \varphi_k(r) + \varphi_j(o)$$

In group theory, the most important functions between two groups are those that "preserve" the group operations, and they are called homomorphisms. A function f : G → H between two groups is a homomorphism when

$$f(xy) = f(x)f(y) \text{ for all } x \text{ and } y \text{ in } G$$

Here the multiplication in xy is in G and the multiplication in f(x)f(y) is in H, so a homomorphism from G to H is a function that transforms the operation in G to the operation in H.

Example homomorphisms are shown below:

$$e^{x+y} = e^x e^y$$

$$\log_a(xy) = \log_a(x) + \log_a(y)$$

The log function Homomorphism shows an excellent example of binary operation of multiplication can translate to a binary operation of addition for a function.

Group Theory

In general a Homomorphism is the function operating on the composition of u and v gives us the same answer as the composition of that function operating on u and composition of that function operating on v. We get the same results which in our case is defined as the trust of a group.

Some youtube videos

http://www.youtube.com/watch?v=dcM_AX82xIw

http://www.youtube.com/watch?v=IBBFHeKFuJM

Richard Redpath