Reducing Correlation: To What Degree is it Necessary?

by Brent Zundel, Avast Software s.r.o.

Proponents (such as myself) of zero-knowledge proofs and their use with Verifiable Credentials often assert that the additional complications introduced by such cryptographic techniques are necessary because they provide a means to reduce the number of correlating factors shared during the exchange of VCs.

These VC-related correlating factors may include: - claims made about a credential subject - credential metadata, such as: - subject identifiers - credential identifiers - revocation registry information - issuance and expiration timestamps - credential signatures

The purpose of this document is to stimulate a conversation around efforts to reduce correlating factors, for which use cases such efforts make sense, and to what extent a reduction in correlating factors should be sought.

Techniques for Reducing Correlation

Most techniques for reducing correlation involve either giving the holder power to only share subsets of verifiable data, or involve removing from interactions the necessity of sharing static values. There is an interest in finding ways to make it unnecessary to share such static values, and to put as much power to determine precisely what data to share into the hands of the holder as possible.

Selective Disclosure

Selective disclosure is the ability of a holder to only share a subset of data from a credential with a verifier. The fewer number of claims and pieces of metadata from a credential are shared, the fewer correlating factors end up in the databases of verifiers.

In addition to short group signatures, which are a class of digital signature that enables partial sharing of signed data, a number of other techniques have been invented that enable this capability, some of them even outside the realm of zero-knowledge proofs.

Private Holder Binding

Private holder binding is a technique that binds a credential to a hidden value, but a holder shows the credential is bound to them by proving they know the secret. This is in contrast to the standard technique of binding a credential to a revealed DID, which a holder shows is bound to them by proving they know the secret key. The difference is, in the case of private holder binding, no DID value or public key needs to be revealed.

Removing the need to share a DID removes a static value that could otherwise serve as a correlating factor.

Signature Blinding

Another value that in many cases is static, is the credential signature. Sharing the credential signature as part of the presentation of a credential provides the verifier with yet another correlating factor.

Short group signatures enable the holder to prove they know the signature, without revealing it.

Other Guidelines

Any other aspects of a credential exchange protocol that require static data to be shared that is unique to the credential, may provide correlating factors to a verifier. The privacy-enhancing capabilities introduced by short group signatures can be undone unless the data objects and protocols are also carefully designed with holder privacy in mind.

Use Cases

Use of any of the above techniques increases, sometimes significantly, the complexity of issuing, receiving, and verifying credentials. Are there use cases that justify such complexity? Hard-line privacy advocates might feel that even asking such a question takes the wrong stance. They may feel that every effort should be made to introduce these capabilities into every credential exchange, thereby minimizing as much as possible privacy harms that may come to an individual.

What of use cases that do not involve individuals? Are techniques that reduce correlation necessary for credentials about goods that travel along a supply chain? Are there use cases involving individuals where such extreme measures for reducing correlation aren't necessary?

I propose that time be spent exploring these use cases and examining them to determine to what degree it should be necessary to reduce correlation.

Is It Even Worth It?

Perhaps attempting to reduce correlating factors in credential exchange is a fool's errand. In light of the data that is already shared during credential exchange, does it matter if there are a few additional factors that may correlate? In light of the correlating factors that exist already within the systems used to enable credential exchange, what does it help to bend over backwards to avoid a few additional ones?

I propose that in conjunction with the above conversation around use cases, we explore other issues to determine whether attempts to reduce correlation are simply moot, or whether there is value in pursuing them, and to what extent.