Microsoft Research

Author: Mira Belenkiy

June 2014

© 2014 Microsoft Corporation. All rights reserved. This document is provided "as-is." Information and views expressed in this document, including URL and other Internet Web site references, may change without notice. You bear the risk of using it. This document does not provide you with any legal rights to any intellectual property in any Microsoft product. You may copy and use this document for your internal, reference purposes.

Summary
This document extends the U-Prove Cryptographic Specification [UPCS] by specifying bit decomposition proofs, useful for other extension protocols.
Contents
Summary ........................................................................................................................................... 1
1 Introduction .................................................................................................................................. 3
  1.1 Notation .................................................................................................................................. 3
  1.2 Feature overview .................................................................................................................... 4
2 Protocol specification .................................................................................................................. 4
  2.1 Presentation ............................................................................................................................ 4
  2.2 Verification ............................................................................................................................. 5
3 Security considerations .............................................................................................................. 6
References ........................................................................................................................................ 6

List of Figures
Figure 1: BitDecompositionProve ................................................................................................. 5
Figure 2: BitDecompositionVerify ................................................................................................. 5

Change history

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Revision 1</td>
<td>Initial draft</td>
</tr>
</tbody>
</table>
1 Introduction

This document extends the U-Prove Cryptographic Specification [UPCS] by specifying bit decomposition proofs, useful for other extension protocols.

The Prover and Verifier have as common input a list of values $C, C_0, C_1, ..., C_{n-1} \in G_q$ and a pair of generators $g, h \in G_q$. The Prover wants to show that the $C_i$ are Pedersen Commitments to the bit decomposition of the committed value in $C$.

$$
\pi = PK \{ (\alpha_i, \beta_i)_{i \in [0, n-1]}, y \} \left( \forall i: C_i = g^{\alpha_i} h^{\beta_i} \cap \alpha_i \in [0,1] \right) \cap C = h^y \prod_{i \in [0, n-1]} (C_i)^{x_i}
$$

The Prover knows a set of values $\{x_i, y_i\}_{i \in [0, n-1], z}$ that would satisfy the above relation. The Prover will create a special honest-verifier non-interactive zero-knowledge proof of knowledge using its witness $\{x_i, y_i\}_{i \in [0, n-1], z}$ that satisfies the above relation. The Prover will create $n$ separate set-membership proofs [EXSM] to show that $\forall i: C_i = g^{\alpha_i} h^{\beta_i} \cap \alpha_i \in [0,1]$. The Prover will create a separate equality proof [EXEO] to show that $C = h^y \prod_{i \in [0, n-1]} (C_i)^{x_i}$.

The U-Prove Cryptographic Specification [UPCS] allows the Prover, during the token presentation protocol, to create a Pedersen Commitment and show that the committed value is the equal to a particular token attribute. The Prover MAY use this Pedersen Commitment as either $C$ or any of the $C_i$ for the bit decomposition proof. The Issuance and Token Presentation protocols are unaffected by this extension. The Prover may choose to create a bit decomposition proof after these two protocols complete.

The committed value in $C$ and all of the $C_i$ MUST NOT be hashed. If any of these values are U-Prove token attributes, the attributes also MUST NOT be hashed.

1.1 Notation

In addition to the notation defined in [UPCS], the following notation is used throughout the document.

- $C$: Value of the Prover’s Pedersen Commitment.
- $x$: Committed value of Pedersen Commitment $C$.
- $y$: Opening of Pedersen Commitment $C$.
- $C_i$: Commitment to the $i^{th}$ bit of the decomposition of $x$.
- $x_i$: The $i^{th}$ bit of the decomposition of $x$, the committed value of Pedersen Commitment $C_i$.
- $y_i$: The opening of Pedersen Commitment $C_i$.
- $A$: Input to equality proof; $C$ divided by the composition of the $C_i$.
- $z$: Prover’s witness for equality proof, the discrete logarithm of $A$.
- $M$: Part of set membership proof: “response”.
- $\pi$: Equality proof.
- $\pi_i$: Set membership proof.
The key words “MUST”, “MUST NOT”, “SHOULD”, “RECOMMENDED”, “MAY”, and “OPTIONAL” in this document are to be interpreted as described in [RFC 2119].

1.2 Feature overview
The Bit Decomposition proof consists of a straightforward combination of a set membership proof and an equality proof.

To show that each value $C_i$ is a Pedersen Commitment to either 0 or 1, the Prover will create a set membership proof [EXSM] for the set $\{0, 1\}$.

To show that composing the committed values in the $C_i$ results in $C$, the Prover will create an equality proof [EXEQ]. The Prover knows witnesses $x, y, (x_0, y_0), (x_1, y_1), \ldots, (x_{n-1}, y_{n-1})$ that are the openings of $C, C_0, C_1, \ldots, C_{n-1}$. The Prover will compute

$$z := y - \sum_{i=0}^{n-1} 2^i y_i \mod q$$

It is easy to see that the following relation holds:

$$C = h^z \cdot \prod_{i=0}^{n-1} (C_i)^{2^i}$$

The Prover will create proof of knowledge of the discrete logarithm of $A = C / \prod (C_i)^{2^i}$ in terms of the generator $h$.

2 Protocol specification
As the bit decomposition proof can be performed independently of the U-Prove token presentation protocols, the common parameters consist simply of the group $G_q$, two generators $g$ and $h$, and a cryptographic function $\mathcal{H}$. The commitments $C, C_0, C_1, \ldots, C_{n-1}$ and their openings MAY be generated by the Prover.

2.1 Presentation
The presentation protocol consists of creating $n$ set membership proofs for the set $[0, 1]$, and an equality proof to prove valid decomposition.
2.2 Verification
The Verifier verifies the set membership and equality proofs.
3 Security considerations

The bit decomposition proof protocol is a composition of the set membership proof and the equality proof. The following restrictions apply:

1. The Prover and the Verifier MUST NOT know the relative discrete logarithm \( \log_g h \) of the generators \( g \) and \( h \). This is not an issue if the generators are chosen from the list of U-Prove recommended parameters.

References


