Errata

The following is a list of errata for my master's thesis. The updated version of my master's thesis can be found at:

`https://www.fogbunzel.dk/masters-thesis`

The original version of my master's thesis can be found at:

`https://www.fogbunzel.dk/masters-thesis-original`

- Corrected spelling and grammar throughout the whole thesis.
- Abstract: Changed the sentence "But an identification scheme is weaker than a sigma protocol since it only satisfies witness hiding instead of sHVZK. Furthermore, a sigma protocol also implies other useful protocols such as signature schemes, identification schemes, zero-knowledge protocols and commitment schemes." to "But an identification scheme is weaker than a sigma protocol since a sigma protocol can be used as a signature scheme, a zero-knowledge protocol, a commitment scheme or even an identification scheme.".
- Table of contents (page vii): Changed the headline of the following sections:
  - Changed Section 1.1 from "Overview" to "Chapter Overview".
  - Changed Section 2.8.1 from "Proofs of Knowledge Systems" to "Proof of Knowledge Systems".
  - Changed Section 4.2 from "A Statistically Secure Sigma Protocol based on the General Framework with Abort in the Standard Model" to "A Statistically Secure Sigma Protocol in the Standard Model based on the General Framework with Abort".
  - Changed Section 4.2 from "A Statistically Secure Non-Interactive Sigma Protocol based on the General Framework with Abort in the Random Oracle Model" to "A Statistically Secure Non-Interactive Sigma Protocol in the Random Oracle Model based on the General Framework with Abort".
- Section 2.7 (commitment schemes): Added a remark about why a commitment scheme can't achieve both unconditional binding and unconditional hiding.
- Section 2.10 (sigma protocols): Added a remark about that a sigma protocol can be used as an identification scheme, a signature scheme, a zero-knowledge protocol or a commitment scheme.
- DEFINITION 2.23: Updated the notation of the two accepting conversations in the definition of statistical special soundness from "(a, e, z) and (a, e', z')" to "(a, e, z) and (a', e', z')". Furthermore, updated the input to the knowledge extractor from (x, a, e, e', z, z') to (x, a, a', e, e', z, z').

- Proof of THEOREM 3.1: Corrected the probability $\Pr[\vec{z} \notin I^n]$ in the proof for completeness with abort from $\Pr[\vec{z} \notin I^n] = \left(\frac{1}{S+1}\right)^n$ to $\Pr[\vec{z} \notin I^n] = 1 - \left(\frac{2\cdot(S\cdot B-B)+1}{2\cdot(S\cdot B)+1}\right)^n$.
  - THEOREM 3.1: Changed $\left(\frac{1}{S+1}\right)^n$ to "$\Pr[\vec{z} \notin I^n]$ (see Equation (3.1))".
  - TABLE 3.2: Changed $\left(\frac{1}{S+1}\right)^n$ to "$\Pr[\vec{z} \notin I^n]$ (Eq. (3.1))".
- Proof of THEOREM 4.2: Updated the proof for statistical special soundness for an easier understanding.
  - FIGURE 4.3: Updated the figure according to the updated version of the proof.

Anders Fog Bunzel,
Aarhus, October 10, 2016.