Summary

Secure distribution and protection of digital content has become a crucial issue in the Digital Millennium. One of the most basic, but also most fundamental, questions is how to prove authorship on digital content and how to distribute rights on digital works, such that any transaction can be verified to be, directly or indirectly, authorised by the rightful author. These are the basic questions addressed in this thesis.

Towards answering these questions we provide, for the first time, formal definitions of authorship and discuss authorship proofs in different settings. We stress that it is important to distinguish between dispute resolving schemes and sound, direct authorship proofs. Furthermore, we present novel dispute resolving protocols that achieve additional security properties and, even more importantly, the first protocols for sound direct authorship proofs.

An important building block, which may be used in our protocols, are digital watermarking schemes. We provide computational definitions of robust watermarking schemes and discuss their use in dispute resolving and direct authorship proofs. Proving the presence of a watermark requires disclosure of security critical information. We propose a methodology to design zero-knowledge proof protocols, proving the presence or absence of watermarks. We show how to integrate these protocols in dispute resolving protocols and sound direct authorship proofs to improve their overall security and practicability.

Finally, we present a model for multilaterally secure distribution of rights, where we define rights, licensing and transfer transactions on rights and introduce a definition of rightful rights ownership. Furthermore we introduce protocols that implement these transactions and allow proving rightful rights ownership.

Results

The major results of this thesis are summarised below:

- **Novel Computational Definitions of Watermarking Schemes:**
  The need for formal security definitions of watermarking schemes is manifold, whereby the core need is to provide suitable abstractions to
construct, analyse and prove the security of applications that rely on watermarking schemes.

In recent years there has been a remarkable number of publications on such definitions. We review these proposals and point out their shortcomings. We present a formal framework of watermarking schemes, including rigorous definitions of detection errors and computational robustness. Our definitions provide suitable abstractions that are compatible with cryptographic definitions, enabling security proofs of protocols that combine cryptographic building blocks and watermarking schemes.

- **Novel Definition of Authorship:** For a long time copyright protection systems, such as dispute resolving or authorship proof schemes, have not been studied in a formal and rigorous way. Even the basic notion of „authorship“ itself was not defined formally. Therefore, early proposals for proof of authorship or dispute resolving lacked rigorous analysis and statements about the requirements achieved by these proposals. This makes it hard to assess their security and compare their overall properties.

We present the first formal definition of authorship (authorship model) by making reasonable abstractions from current copyright legislation and, thereby, lay the ground for a formal and rigorous treatment of authorship proofs, dispute resolving and sound rights management infrastructures. Based on our authorship model it is, for the first time, possible to define security requirements of these protocols and prove their security formally.

- **Dispute Resolving Schemes:** Building upon our authorship model, we present the first formal definitions of dispute resolving schemes, including formal definitions of their basic security requirements.

Furthermore, we present an extensive classification of dispute resolving schemes and identify important advanced requirements, such as „non-disclosing“ and „sound“ dispute resolving, which have been neglected in prior work. In addition, we discuss the security of non-invertible watermarking schemes, which have been proposed to resolve authorship disputes. We show that many non-invertibility constructions proposed in the literature are insecure unless the false-positive probability of the underlying watermarking schemes is negligible.

- **Direct, Sound Authorship Proofs:** Dispute resolving schemes known today are not „sound“, which means that the winner of an authorship dispute is not necessarily the rightful author of the disputed work. This observation is of utmost importance and, as such, is another major result of this thesis. The lack of soundness has strong
implications on the practical relevance of dispute resolving schemes: the winner of a dispute may not claim compensation as it is not clear that he is the rightful addressee of the compensation.

We propose a new type of protocol, which we refer to as „direct authorship proofs“. Its distinguishing features are that they provide soundness, i.e., our protocols guarantee that the claimant is really the rightful author of a work. Furthermore, our protocols work in a two-party scenario, which makes them suitable for e-commerce purchase scenarios, where the buyer of a work (or usage rights thereon) wants to make sure to purchase from the rightful author only.

Our authorship proofs are an important prerequisite for business with (digital) works or their usage rights. This holds especially for non-famous creators, who want to distribute their works themselves, i.e., without established well-known intermediaries. The basic question is: How can a potential customer be sure that he purchases a work from its rightful copyright holder? The answer to this question is addressed by authorship proofs.

- **Zero-knowledge Watermark Detection:** Most applications of watermarking schemes require at some point to prove the presence or absence of a watermark to some possibly untrusted party. When using standard, symmetric, watermarking schemes, this requires disclosure of security critical information such as the watermark and the watermarking key. Zero-knowledge watermark detection refers to cryptographic protocols that prove the presence of a watermark without disclosing such critical information.

We review previous work on zero-knowledge watermark detection and uncover serious limitations of the previous work. We propose a generally applicable methodology to construct provably secure and reasonably efficient zero-knowledge watermark detection protocols. Our protocols can be applied in several applications to overcome the drawbacks outlined above. We discuss their application in dispute resolving and direct authorship proofs in detail to achieve non-disclosing dispute resolving and offline direct authorship proofs.

- **Multilaterally Secure Rights Distribution Model and Protocols:** Current DRM systems focus mainly on rights holders’ security needs, but commonly neglect those of consumers or licensees. In particular, these systems even lack reliable means for users to verify that they purchase usage rights on works (licenses) from the rightful authors (rights holder). We introduce a formal model and the corresponding protocols for establishing a multilaterally secure rights distribution infrastructure.
The key features of our proposal are: firstly, consumers can directly verify that a seller is indeed authorised to grant certain usage rights. Secondly, authorship certificates and rights licenses are invariant with respect to perceptibly similar works, i.e., they are not only valid for the original work but also for a set of closely related similar works that are modifications of the original work (e.g., different resolutions or encodings of an image or a video). The reason for providing this property is that these works are still considered to be under the copyright of the author. Furthermore, the fact that licenses cover modified, processed versions of the work is an enabling feature for B2B digital rights management, where licensees may process works, while still being able to prove that the processed version of a work is covered by the same license. Our scheme provides an enabling technology for open, decentralised right distribution infrastructures for intellectual property with multilateral security.