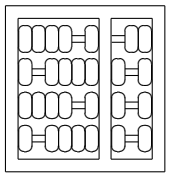


INSTITUTO DE COMPUTAÇÃO
UNIVERSIDADE ESTADUAL DE CAMPINAS

E-commerce and fair exchange:
The problem of item validation

Fabio Piva *Ricardo Dahab*

Technical Report - IC-11-05 - Relatório Técnico

February - 2011 - Fevereiro

E-commerce and fair exchange: The problem of item validation

Fabio Piva* Ricardo Dahab†

07 February 2011

Abstract

Fair exchange protocols have been widely studied since their proposal, but are still not implemented on most e-commerce transactions available. For several types of items, the current e-commerce business models fail to provide fairness to customers. The item validation problem is a critical step in fair exchange, and is yet to receive the proper attention from researchers. We believe these issues should be addressed in a comprehensive and integrated fashion before fair exchange protocols can be effectively deployed in the marketplace. This is the aim of our research, and drawing attention to this problems and possible solutions is the goal of this technical report.

1 Introduction

Fair exchange protocols were proposed [1] as a solution to the problem of two mutually distrusting parties interested in exchanging digital items atomically. Many variations of Asokan's original protocols have since been studied, but most of them were too cumbersome or required too many resources to be seriously considered for real applications. Probabilistic fair exchange [10], for instance, required a great number of messages to be transmitted, in order to achieve only a probabilistic, more relaxed form of fairness.

Arguably, the most successful instances of fair exchange in the real world are the optimistic fair exchange protocols – two-party protocols that rely on a mutually trusted third party (TTP) to handle exceptions that may arise during the exchange. Those protocols quickly became the focus of fair exchange research, and were used as the core of several pioneer e-commerce projects [12, 7].

Much work has been dedicated to the formalization of fair exchange protocols. Gärtner et. al. [4] give the first steps towards a formal definition of fairness; other authors follow similar approaches to different fair exchange properties, such as non-repudiation [5] and timeliness [15]. As for verification methods, very few of them seem able to handle optimistic fair exchange protocols appropriately, mostly due to their multi-protocol nature. Some

*Institute of Computing, University of Campinas, 13081-970 Campinas, SP. Research fully supported by FAPESP.

†Institute of Computing, University of Campinas, 13081-970 Campinas, SP.

recent works accomplished interesting results [16, 14, 13] with the adaptation of the Strand Spaces method [18] for supporting optimistic protocols.

However, most current e-commerce stores do not implement fair exchange in their business models; a simple web search reveals several Apple's iTunes Store user complaints about mistaken music files being purchased due to unaccurate description of the products; also, the Digital Downloads section on Amazon.com contains several customer comments on the same subject. To worsen the problem, most companies openly adopt a no-refund policy when it comes to selling digital products – even in the case of a mistaken purchase.

Such problems relate to an essential, but not sufficiently explored, aspect of fair exchange protocols: the **item validation** step. The original definition of fairness states that "*an exchange is fair if at the end of the exchange, either each player receives the item it expects or neither player receives any additional information about the other's item*" [1]. For that end, aside from ensuring the atomicity of the exchange, the protocol must specify when and how a party can check whether the item she just received (or is about to receive) is the one she desires. This is, however, a delicate process that may be influenced by the characteristics of the items being exchanged, by the available resources and by the structure of the protocol itself.

As such, we consider the item validation problem a very interesting and relevant topic of research, and that e-commerce would greatly benefit from a better understanding of its subtleties. We also believe that the lack of attention on this subject is the very reason why fair exchange protocols are not yet widely implemented in the current e-commerce business models.

1.1 Document organization

The remainder of this document is organized as follows: Section 2 describes our main motivation – namely the unsuitability of the current e-commerce model to today's consumer's and seller's needs – to consider item validation as an important topic of research. Section 3 presents our concept of reversible degradation, an elegant abstraction of how to solve the problem of fairly exchanging, validating and selling multimedia content over the Internet. In Section 4 we show a few alternative models for selling digital items, and discuss why they do not address the issues raised here. We conclude in Section 5 with some final remarks on the item validation problem and what future research on this topic should focus on.

2 Motivation: E-commerce in real-world

In this section we present our view on the current e-commerce model for digital items, and discuss why selling/purchasing digital items through the internet is a much more delicate process than it is for physical items – specially when multimedia (indescribable) files are the focus of the transaction.

2.1 Current model description

During the past ten years, selling digital content has become an atractive business, mainly due to the fast increase of consumers of that kind of media. The latest technological trends – such as cheaper and faster broadband internet connections, greater storage space, and gadgets that provided users with easier access to their data on-the-go – contributed to the development of a solid market for this so-called e-goods. And although several virtual retailers have emerged in order to supply this demand for digital content, most of them chose to adopt a real-world based business model that, however successful for selling physical products, is unsuitable for trading digital products; it is our belief that physical and digital items are too intrinsically different to be negotiated in the same way – maily because it is too easy to create an identical copy of a digital item, thus voiding any possibility of a returning policy in the case of an unsatisfying purchase.

The currently adopted model for electronic commerce of digital content is the following: First, the buyer registers with the seller, thus obtaining an account through which the transaction will be carried out. Then, while logged in the store's system (which might be a website or client software, for instance), the buyer chooses the product he desires to purchase; he must check carefully whatever descriptions – such as feature lists, pictures, or samples – are available for that product. Figure 1 illustrates a hypothetical digital item for sale and its possible description.

(a) Item i

- *Item Summary:* Portrait of model Lena Söderberg
- *Keywords:* hat, bust, plumes, portrait
- *File Specs:* PNG image (bitmap), RGB, 256x256 resolution

(b) Description $desc(i)$ of i

Figure 1: Desired item i and it's description as a list of specifications.

On this model, the item is not publicly available for the interested customer (otherwise he would be able to aquire it without paying for it). Instead, only the description, which in this example is the list of features ilustrated in Figure 1b, is available before payment.

Once satisfied by this description, the buyer places an order for that particular product – he now has a mental image of what he expects to receive. He must then pay for it; this may happen either by revealing his credit card number to the store, or by depositing money to an external account and then informing the seller, for instance. Either way, on the receiving of the payment, the seller finally releases the product to the buyer – maybe by

sending him a temporary link for downloading it or as an attachment in an email message.

If the buyer pays but never receives the product, dispute might be started. Most buyers would first try to contact the store, which will generally try to solve the problem to avoid bad reputation. Mostly, in the case of a digital file's purchase, the store would simply resend the item to the buyer, without losing any money. This is only the case because of the **idempotency** [1] property of e-goods: If a bit stream was to be received by a user, it wouldn't make a difference if that same bit stream was received multiple times, since this would mean that several exact copies of the same e-good was being received. For physical goods, this would not be the case: If the store was required to re-send a physical item, this would represent loss of money to the seller, and a malicous buyer would be able to retain two or more identical – but several, neverthless – instances of a product.

However, a completely different situation occurs if the buyer receives the product, but is not satisfied by it – which might happen if the description about a certain aspect of the product had been left vague or ambiguous by the store. In such cases, the buyer might find himself in an unfair situation – having paid for a product that does not meet his expectations. Figures 2a and 2b show two candidates for delivery that match the description shown in Figure 1b. One could point that the problem could be easily solved by adding the word "color" to the description, but then Figure 2(c) would still be a candidate for delivery.

(a) (b) (c)

Figure 2: Three different files that show pictures of the model Lena Söderberg. Figures (a) and (b) equally satisfy any description that does not mention color properties, and Figures (a) and (c) could be mistaken even if color is mentioned – which could lead to the wrong file being delivered.

In cases of mistaken delivery, both the store and any external judge might refuse to intervene in favor of the buyer, for it is his responsability to carefully check the product description before paying for it. The fact that the buyer is not able to return the wrong item – without possibly keeping a copy for himself – in exchange of the right one, makes the store unable to distinguish a genuine mistake from a pay-for-one-and-take-two con. We refer to this issue as the **unreturnability** property of digital items, and believe that it is one of the reasons why e-goods must be traded differently than physical products.

Unfortunately, if the digital product in question is also an **indescribable item** [2], there can be absolutely no guarantee to a buyer about the outcome of the purchase, in this model. Even if a sample of the file is used as description – a reduced thumbnail of an image file, or a lower bitrate fraction of a song file might be available for download beforehand,

for instance – the above mentioned problem might still occur, as we shall see in Section 2.2. In fact, most of the times, the buyer has no guarantee that the item corresponding to the sample is in fact the one to be delivered; as shown in Figure 3a, he might very well download a thumbnail sample of image file i, engage in a transaction for aquiring the larger version of it, and end up with a copy of image file i' illustrated in Figure 3b – possibly due to some internal error in the store system, or even human error when advertising the item.

(a) Buyer desires i from Figure 1a

(b) Item $i' \neq i$ which also satisfies $desc(i)$

Figure 3: The current model allows a buyer to pay for a file and receive a different one.

Dispute process for this kind of situation would be rather difficult, since the buyer would not be able to return file i' in exchange of desired file i; the store might rightfully allege that the buyer would be able to retain a copy of file i' for himself, which would leave it in an unfair situation. One should notice that even if the description from Figure 1b was used instead of the thumbnail to validate the transaction, the wrong item i' would still be a candidate for delivery.

Situations like this happen more often then one might imagine. In the next section we present a few examples of unsatisfied customers, gathered from communities of users of one of the most proeminent e-stores available – namely Amazon.com.

2.2 Real examples of unfairness in e-commerce

In this section we present a few examples of unsatisfied consumers of digital music. The fact that digital music files are examples of indescribable items (as we shall better define in Section 2.4) makes them very difficult to exchange fairly. Without a good description, item

validation becomes difficult and error prone – because the buyer is not able to accurately decide wether the item he is about to pay for is the one he desires, or not.

Currently, one of the most popular services for buying songs remains Amazon MP3 Downloads, which follows the business model described in Section 2.1. However, in order to strengthen item validation, the store also provides buyers with a limited preview of thirty seconds of each song – as illustrated in Figure 4.

(a)

(b)

Figure 4: Amazon MP3 Downloads description of an item. Figure (a) shows a list of details about the file, while Figure (b) shows a limited preview button.

One might think that, with the addition of a preview of the song to the description, the chances of someone buying the wrong file would be negligible. However, as Figure 5 shows, this may not always be true.

As we previousy stated, the current business model for multimedia, as well as several other special items, is anything but fair. In the following sections we intend to relate this issue to the problem of item validation, as well as to suggest a few possible, fair alternatives to the current e-commerce paradigm for digital items.

2.3 The item validation problem

Optimistic fair exchange protocols [1] usually follow a common sequence of events: Let us suppose that two parties P and Q are willing to exchange two generic items i_P and i_Q. A common requirement is that P and Q know beforehand the descriptions $desc(i_Q)$ and $desc(i_P)$, respectively, of their expected items; there must also be a publicly available function $validate(i, d)$ which takes an item i and a description d and returns $TRUE$, if d accurately describes i, or $FALSE$ otherwise.

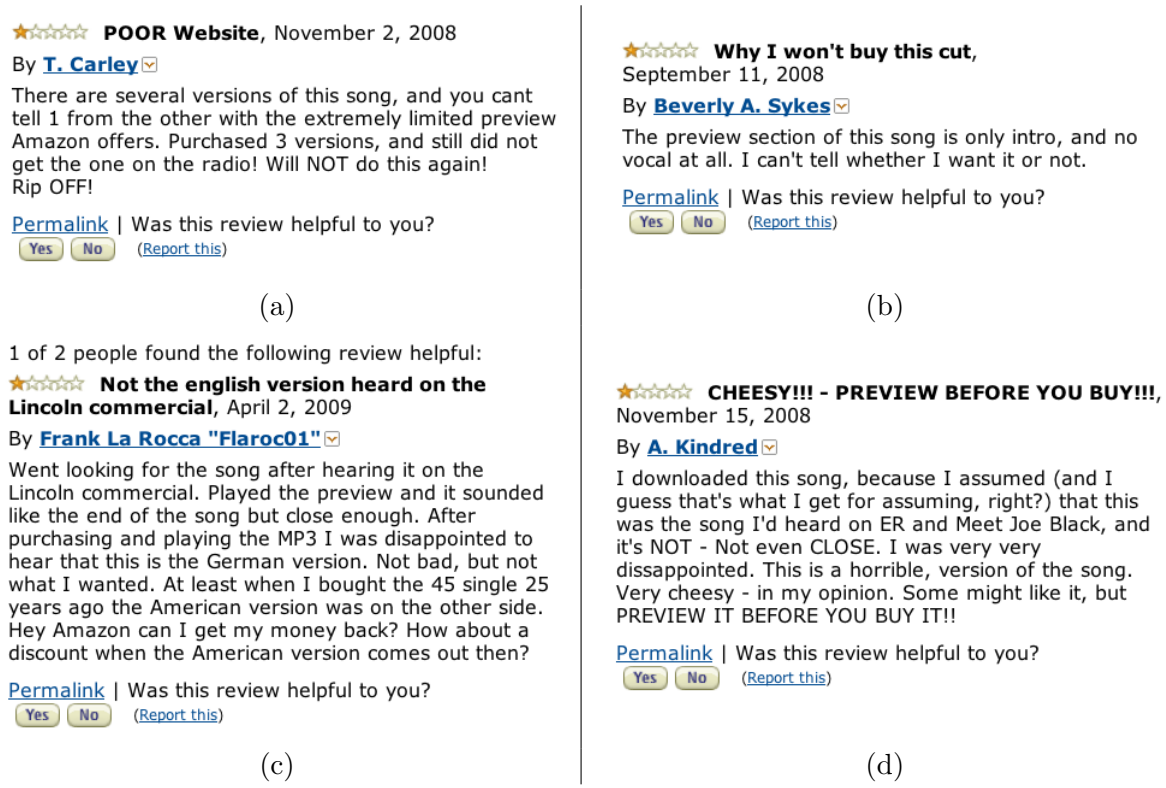


Figure 5: Four examples of unfair situations occured due to inaccurate validation of the purchased song (even when limited preview is available).

The parties then engage in the exchange, initially gathering sufficient information to prove the validity of the transaction; this step is crucial to allow for internal or external dispute resolution, in case of exceptions. After that, they proceed to the exchange of items. When a party receives an item, it executes *validate*() using the received item and the known description as parameters, and checks the result to decide whether the item is the expected one. If the function returns $FALSE$, then the protocol must be robust enough to either allow the cheated party to recover the correct item, usually by providing information about the unfair transaction to the TTP, or to stop her counterpart from getting the other item, if it has already been revealed.

One should notice that the availability of both the function *validate*() and accurate descriptions of the items are then essential to ensure fairness in this type of protocol. However, for some particular items, providing an accurate description can be a hard task [2]. We shall return to the issue of item (in)describability in Section 2.4.

Even for describable items, validation may not be trivial. The protocol designer must carefully ponder when in the protocol run the parties will be required to perform validation, and whether the item will be encrypted or unencrypted. Also, should the validation be performed by parties themselves, or should a TTP be assigned for this task? And if we transfer this responsability to a TTP, how can we describe the *validate()* function so that

we can ensure that parties will agree with its evaluation? All those questions must be taken into account when designing a fair exchange protocol, and are usually not so.

2.4 Special properties of items (and how they affect validation)

The first proposals for fair exchange protocols [1] regarded items as generic, forwardable digital goods, but soon researchers took interest in particular instances of the problem. Some special types of items, such as digital cash, multimedia files etc., may present special properties that should be considered during protocol design. A **strongly revocable item** [19], for instance, can be invalidated by its issuer, if some conditions are met. If the items being exchanged are both strongly revocable, fair exchange could become rather trivial, since unreturnability would no longer be an issue.

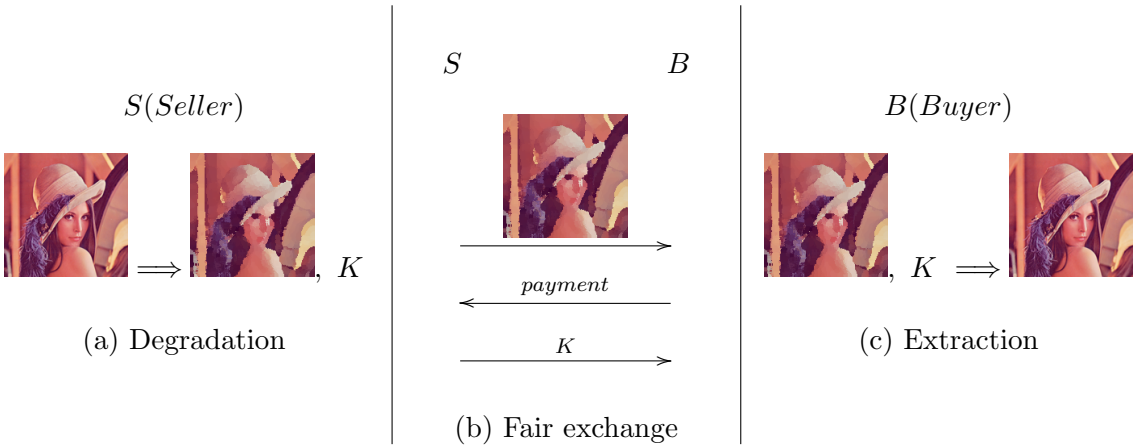
Not all special properties, however, assist the designer in the task of guaranteeing fairness. As we discussed in Section 2.3, protocol designers usually assume that a good description of each item will be available to parties before the exchange is initiated. Although little discussion can be found on what a good description would be, the fact is that descriptions may depend greatly on the nature of the item, and some items are particularly hard to describe. **Indescribable items** [2] present a real challenge to the fair exchange problem, simply because they are hard to validate. In fact, we believe that no currently known optimistic fair exchange protocol can be used to guarantee fairness to a party interested in an indescribable item. The discussion an example provided in Section 2.1 strengthens this claim.

3 Reversible degradation

In order to address this issue, we propose the concept of **reversible degradation** – an idea that might be the first solution for the fair exchange and validation of indescribable items. By transforming (*degrading*) the item in such a way that it becomes clearly deteriorated, but can still be distinguished by the receiving party, the owner could release it for validation without the risk of being cheated. If this degradation process could be made *reversible*, the buyer would be able to receive the degraded copy, validate it and then negotiate a key for recovering the original, full-quality item, as illustrated in Figure 6.

One interesting advantage of reversible degradation over other approaches is that it allows the buyer to obtain the item *before* paying for it – even if it is somehow degraded. Validation would then be performed by the user's own senses, since human perception is capable of ignoring degradation for the purpose of deciding whether that is, in fact, the desired item. Also, as we shall discuss in Section 4, reversible degradation does not require any singnificant additional bandwidth cost – as other methods do – or hardware changes on both ends of the transaction.

Another important property of the reversible degradation concept is that, after the degradation is reverted, the item is fully restored to its original form – no trace of the degrading information, perceivable or not, is left behind. This differs in essence from DRM methods and some removable watermarking techniques [9] that still leaves information embedded into the item and require the key on every subsequent access to its content. Such



(a) Degradation (b) Fair exchange (c) Extraction

Figure 6: Reversible degradation concept description.

techniques require the user to use special software or hardware to consume the purchased product, which is in general a problem if the user prefers a specific software player or intends to use a particular audio file on his portable digital music player.

There are several paradigms that might be good starting points for reversible degradation, such as error correcting codes [11], removable watermarking [9, 6] and perceptual cryptography [8]. The particular characteristics of these methods, as well as how they interact with fair exchange protocols, are yet to be studied and remain the focus of our current research. In this report, we limit ourselves to present the concept abstraction, compare it with other alternative models and discuss its main impacts on item validation and e-commerce of digital items.

4 Fair purchase of multimedia content without reversible degradation

In this section we present a few alternative models for the purchase/sell of multimedia items. We also point the main problems with each of them, and compare them to our reversible degradation model.

4.1 Full preview with embedded player

This is similar to the the limited preview model used by the major digital music stores available, specifically iTunes Store and Amazon. The limited preview model is presented in Section 2.2.

By allowing buyers to fully preview the song they are about to buy, the store reduces the problems that might arise if a bad section is chosen as a preview in the limited preview model. Buy listening to the whole song or watching the whole movie before buying, customers can better decide if that item is really what they are looking for. However, this would allow any malicious user to easily capture the video or audio stream and record it

without any quality loss, thus obtaining the item without having paid for it. This is unfair by definition, and would represent a great loss for media sellers.

4.2 Random preview with embedded player

If instead of providing a limited, fixed preview of the item, sellers provided a randomly-chosen portion of the file to be previewed, the bad portion problem of limited preview would also be solved. But since the full portion is not provided to the user, recording the stream to a new file would be harder.

Harder, but not impossible. Even if only a limited, randomly chosen portion of the item was made available each time the customer clicked on the presented preview button, a full copy of the file would be not that hard to obtain. By clicking the preview button several times, and by recording each part of the song, it wouldn't take long to the malicious user to obtain the whole song separated in several recordings. Reconstruction of the whole item would then be easily accomplished with a simple software editor.

We should notice that even if this system was smart enough to never select a particular portion of the item to be previewed – thus avoiding full item reconstruction by this method – the could be cases in which the hidden portion was exactly what the user wanted to preview to decide if the item is the one he desires. Some songs, for instance, have too many versions that can be very similar to each other, differing only by a few seconds from one another. The same might happen with a director's cut release of a movie, that may come with a few additional frames than the cinematic version. In such cases, hidding a particular portion of the item might present the buyer with an undecidable situation.

4.3 Lower bitrate samples

Instead of providing a preview of any kind, stores could provide the buyers with a full, downloadable, lesser quality version of the item. This is very similar to reversible degradation, with the only diference that the degradation is not reversible and is fixed as a proposital low bitrate. In image files, the equivalent would be a low resolution version of the item.

There are at least two problems with this model: First, by fixing the degradation method to lowering the bit rate/resolution of the item, the buyer would not be capable of deciding if the quality of the final item would be satisfactory. This violates the fairness property of the transaction – the customer could find himself unsatisfied by the outcome of the purchase, finding the acquired item poorer than he initially expected.

Second, this would almost double the required bandwidth in every successful purchase. The buyer would have to download each item twice – first, the low bitrate version; and finally, the full quallity one – instead of just one item download, as it is possible with reversible degradation. Specifically in the case of digital movie content purchase, this is significantly worse, since the items can be considerably large.

If reversible degradation was used, instead, only one large download would be required. The second download would be replaced of a small key file, that would allow full quallity reconstruction of the item. Also, other forms of degradation could be used instead of lowering the bitrate – thus leaving this property untouched.

4.4 DRM-based expiration date

Instead of degrading the file whatsoever, the store could provide the user with a full quallity download before the payment was made. The provided item would be rigged with some form of expiration date mechanism that would be triggered after some time, unless otherwise disabled by the user (possibly with some key provided after payment).

The problem here would be similar to the one discussed in Section 4.1. By playing the rigged item before the expiration date, the malicious buyer could simply record the output to another file without any perceivable quality loss. Besides that, DRM acceptance is becoming seriously undermined among digital media consumers – so we believe that DRM-based models are contemned to soon disappear.

4.5 Multimedia encryption, perceptual cryptography and partial encryption

Multimedia encryption [8] is a special field of research that concerns encryption/decryption schemes specifically designed for audio, video and image content. These schemes usually rely on some known cipher as the central component for a larger algorithm, taking into account the perceptual funcionality of multimedia. Another term commonly associated to multimedia encryption is *perceptual cryptography*.

The main idea behind perceptual cryptography is that multimedia content does not have to be fully encrypted to be protected. Its functionality depends exclusively on human perception, which is highly susceptible to small changes on the object. Such schemes are capable of making multimedia content completely unrecognizable to the human observer, by only encrypting a small fraction of data - a procedure refered to as *partial encryption* [3, 17]; this is particularly interesting for applications where efficiency is critical, such as video-on-demand, since the burden of real-time encryption/decryption can be highly reduced.

Partial encryption techniques seem to be very promissing in conjunction with fair exchange protocols. We have no knowledge of any study on the effects of perceptual cryptography on fair exchange of multimedia content, and we believe that a lot can be gained in the context of item validation.

5 Conclusion

The study of the item validation problem will certainly improve the chances of deployment of fair exchange protocols by making it adequate to today's e-commerce needs. Neither currently published fair exchange protocols, nor the currently implemented e-commerce business models, are able to provide fairness to both customers and sellers simultaneously, given the characteristics of current digital products and payment schemes. Specifically in the context of digital music and video selling, which is increasingly becoming the mainstream form of media consumption among the general public, new solutions should be proposed to reduce customer losses and increase reliance on e-commerce transactions.

We stress that, to the extent of our knowledge, the problem of item validation of fair exchange protocols has not been studied at all. The available techniques are barely described

on protocol specifications, if so. By treating validation techniques as not more then a byproduct of protocol design, researchers have neglected to approach a hard problem in protocol design – one that might lead to fruitful discussions and further enhancements on the state of art of diplomatic protocol design.

The fair exchange of indescribable items, for instance, has only been approached recently [2], and techniques for the optimistic fair exchange of those items are yet to be seem. Our reversible degradation model, presented in Section 3, shall produce the first solutions to address the exchange of indescribable items optimistically. Other alternative models for multimedia purchase, presented in Section 4, do not seem to address our concerns as well as our reversible degradation model in conjunction to fair exchange protocols.

The focus of our current work remains on evaluating several promising techniques, as well as proposing new ones, for reversible degradation of multimedia items. Concurrently, we are also giving the first steps towards the formalization of the item validation problem of fair exchange protocols, which remains an important open problem of cryptographic protocols design. We believe that, unless some atention is dedicated to the item validation problem and to how to accurately describe digital items, fairness will remain left aside from e-commerce and, as a consequence, reliance on e-commerce will never be as high as it should be in today's market needs.

References

[1] N. Asokan. Fairness in electronic commerce. *Research Report RZ3027*, Jan. 1998.

[2] A. Bottoni, G. Dini, and T. Stabell-Kulø. A methodology for verification of digital items in fair exchange protocols with active trustee. *Electronic Commerce Research*, 7(2), 2007.

[3] H. Cheng and X. Li. Partial encryption of compressed images and videos. *Signal Processing, IEEE Transactions on*, 48(8):2439–2451, 2000.

[4] F. C. Gartner, H. Pagnia, and H. Vogt. Approaching a Formal Definition of Fairness in Electronic Commerce. *SRDS*, 1999.

[5] S. Kremer, O. Markowitch, and J. Zhou. An intensive survey of fair non-repudiation protocols. *Computer Communications*, 25(17):1606–1621, Nov. 2002.

[6] S. Kwong. An algorithm for removable visible watermarking. *IEEE Transactions on Circuits and Systems for Video Technology*, 16(1):129–133, Jan. 2006.

[7] G. Lacoste, B. Pfitzmann, M. Steiner, and M. Waidner. SEMPER - Secure Electronic Marketplace for Europe. *Lecture Notes in Computer Science (LNCS)*, 1854, Aug. 2000.

[8] S. Lian. *Multimedia Content Encryption: Techniques and Applications*. 2009.

[9] M. Loytynoja, N. Cvejic, and T. Seppanen. Audio protection with removable watermarking. In *2007 6th International Conference on Information, Communications & Signal Processing*, pages 1–4. IEEE, 2007.

[10] O. Markowitch and Y. Roggeman. Probabilistic Non-Repudiation without Trusted Third Party. In *Second Workshop on Security in Communication Network˜99*, 1999.

[11] L. Minder. Cryptography based on error correcting codes. *algo.epfl.ch*, 2007.

[12] A. Nenadic, N. Zhang, and S. Barton. FIDES - a Middleware ECommerce Security Solution. In *The 3rd European Conference on Information Warfare and Security (ECIW*, pages 295–304, 2004.

[13] F. R. Piva. Verificação formal de protocolos de trocas justas utilizando o método de espaços de fitas. Master's thesis, UNICAMP, 2009.

[14] F. R. Piva, J. R. M. Monteiro, and R. Dahab. Strand spaces and fair exchange: More on how to trace attacks and security problems. In *Anais do VII SBSeg, Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais*, Sept. 2007.

[15] F. R. Piva, J. R. M. Monteiro, and R. Dahab. Regarding timeliness in the context of fair exchange. In *Network and Service Security, 2009. N2S '09. International Conference on*, pages 1–6, June 2009.

[16] F. R. Piva, J. R. M. Monteiro, A. J. Devegili, and R. Dahab. Applying Strand Spaces to Certified Delivery Proofs. In *Anais do VI SBSeg, Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais*, Sept. 2006.

[17] A. Servetti, C. Testa, and J. D. Martin. Frequency-selective partial encryption of compressed audio. *IEEE International Conference on Aucoustics*, Jan. 2003.

[18] F. J. Thayer, J. C. Herzog, and J. D. Guttman. Strand Spaces: Proving Security Protocols Correct. *Journal of Computer Security*, 7(2–3):191–230, 1999.

[19] H. Vogt. Asynchronous Optimistic Fair Exchange Based on Revocable Items. Apr. 2003.