Squealing Euros: Privacy Protection in RFID-Enabled Banknotes

Ari Juels[1] and Ravikanth Pappu[2]

[1] RSA Laboratories
Bedford, MA 01730, USA
e-mail: ajuels@rsasecurity.com
[2] ThingMagic, LLC
e-mail: ravi@thingmagic.com

Abstract. Thanks to their broad international acceptance and availability in high denominations, there is widespread concern that Euro banknotes may provide an attractive new currency for criminal transactions. With this in mind, the European Central Bank has proposed to embed small, radio-frequency-emitting identification (RFID) tags in Euro banknotes by 2005 as a tracking mechanism for law enforcement agencies. The ECB has not disclosed technical details regarding its plan. In this paper, we explore some of the risks to individual privacy that RFID tags embedded in currency may pose if improperly deployed. Acknowledging the severe resource constraints of these tags, we propose a simple and practical system that provides a high degree of privacy assurance. Our scheme involves only elementary cryptography. Its effectiveness depends on a careful separation of the privileges offered by optical vs. radio-frequency contact with banknotes, and full exploitation of the limited access-control capabilities of RFID tags.

Key words: banknotes, cryptography, RFID, privacy

1 Introduction

Issued under the aegis of the European Central Bank (ECB), the Euro now serves as a common currency for the second largest economic zone in the world, having supplanted the physical currency of member nations at the beginning of 2002. Among the many intricate policy decisions preceding the introduction of the Euro was the determination of banknote denominations. The ECB opted to issue banknotes up to the relatively high denominations of 200 and 500 Euro. At first, this may appear to be a straightforward decision addressing the convenience of consumers and financial institutions. It could ultimately prove, however, to have far reaching consequences as the Euro becomes a currency of international standing rivaling the U.S. dollar. Even before the introduction of the Euro, concern arose that the 500 Euro banknote might emerge as a magnet for international crime [31]. (Indeed, some economists even accused the ECB of trying to attract black-market activity to Europe as a financial stimulus.) At present, the physical currency of choice for international black market transactions is the United

States one-hundred-dollar bill. The 500 Euro note, however enjoys the advantage of superior portability. A simple observation is illustrative: enough one-hundred dollar bills to fill a briefcase will, when denominated in five-hundred-Euro notes, fit in a mere handbag.

As an apparent counterpoise to this threat, the ECB has disclosed plans to incorporate Radio Frequency ID (RFID) tags into Euro banknotes by 2005 [32]. An RFID tag is a tiny device capable of transmitting a piece of static information across short distances. While the ECB has not revealed specifics, it may be presumed that in this proposal, law enforcement officials would be able to employ monitoring equipment to learn the serial numbers of Euro banknotes surreptitiously at short distances. Deployed at highly trafficked locations such as airports, such a system would permit tracking of currency flows, providing a powerful tool for law enforcement monitoring illegal activity such as money laundering and narcotics trade. The difficulty of creating RFID tags is also seen as a potential deterrent to banknote forgery [29].

In this paper, we consider the impact of the ECB proposal on the privacy of bearers of banknotes carrying RFID tags. In brief, the problem is that RFID-tag readers are increasingly easy and inexpensive to buy. On the other hand, RFID tags are too limited in their capabilities to enforce sophisticated information disclosure policies as have been proposed for fully digital forms of cash (see, e.g., [8, 9, 11, 20] for examples). Indeed, the most likely candidate for deployment in Euro banknotes is the Hitachi μ-chip, which simply transmits a 128-bit serial number [29]. If banknotes transmit these serial numbers promiscuously, that is, to anyone possessing a reader, then it is possible for petty criminals easily to detect the presence of banknotes carried by passersby. This would be especially problematic if only high-denomination Euro notes were to be tagged, as might be the case given the additional expense of RFID tags. Worse still, it would possible for anyone to track banknotes, and thus the whereabouts and financial dealings of ordinary citizens. Such tracking would be feasible only at short distances, namely a few meters, but might be done without any knowledge on the part of the victim. The fact that serial numbers contain no consumer information would not provide a guarantee against privacy violations. We give a couple of hypothetical examples here to illustrate the problem:

Example 1. Bar X wishes to sell information about its patrons to local Merchant Y. The bar requires patrons to have their drivers' licenses scanned before they are admitted (ostensibly to verify that they are of legal drinking age). At this time, their names, addresses, and dates of birth are recorded.[3] At the same time, Bar X scans the serial numbers of the RFID tags of banknotes carried by its patrons, thereby establishing a link between identities and serial numbers. Merchant Y similarly records banknote serial numbers of customers from RFID

[3] The 2-D barcodes on drivers' licenses in certain states already carry demographic information [3]. The automated harvesting of consumer information by bars and restaurants is an emerging practice. Presumably the information on the front of cards, including the name of the card holder, can be harvested through optical character recognition.

tags. Bar X sells to Merchant Y the address and birthdate data it has collected over the past few days (over which period of time banknotes are likely not yet to have changed hands). In cases where Bar X and Merchant Y hold common serial numbers, Merchant Y can send mailings directly to customers – indeed, even to those customers who merely enter or pass by Merchant Y's shops without buying anything. Merchant Y can even tailor mailings according to the ages of targeted customers. Patrons of Bar X and Merchant Y might be entirely unaware of the information harvesting described in this example.

Example 2. A private detective wishes to know whether Bob is conducting large-value cash transactions at Carl's store. She surreptitiously intercepts the serial numbers on banknotes withdrawn by Bob and also records the serial numbers of those brought by Carl out of his store. If there is any overlap between sets of numbers, she concludes that Bob has given money to Carl. The private detective might reach the same conclusion if Bob leaves without banknotes that he carried into Carl's store. The private detective might also try to reduce her risk of detection by reading the banknotes of Bob and Carl at separate times, e.g., en route to or from the bank.

A slightly better proposal as regards consumer privacy, and still within the capability of even simple RFID tags, is for banknotes only to transmit serial numbers on receiving a special, static law enforcement key. The problem with this approach is that the key would almost certainly become public knowledge. Such a key would have to be universal, that is, embedded in every law enforcement monitoring device. Moreover, a monitoring device would operate by transmitting the key to target banknotes. This means that the law-enforcement key would need to be transmitted and might thus be easily intercepted. As banknotes cannot be reprogrammed in such cases, this approach seems unworkable.

Another possible approach is to employ a cryptographic form of privacy protection. RFID tags in banknotes could carry and transmit their serial numbers only in encrypted form. This approach is still flawed, however, in that the static ciphertext on a serial number is itself a unique identifier. In other words, the encrypted serial number may itself be viewed as a kind of meta-serial-number, itself permitting the promiscuous tracing of banknotes.

More sophisticated cryptographic solutions for privacy protection are possible in principle. For example, in lieu of a basic RFID tag, banknotes might carry small, clock-bearing devices that only respond to law enforcement queries bearing a digitally signed warrant valid within a certain period of time. Again, however, given the requirements for extremely low cost and size, the RFID tags embedded in banknotes will have to possess much more severely limited capabilities than this. Indeed, the most advanced current generation of cheap, passive RFID tags, such as the Atmel TK5552 carry only about 992 bits of user-accessible memory, and carry no internal power source [13].[4] These tags are capable of only rudimentary computation, such as bitstring comparisons on keys.

[4] Although the specified module size is 5mm × 8mm, this includes an indestructible casing for use in automobiles. The IC itself is about 1mm × 1mm in size, and thus

1.1 Our approach and goals

We propose an approach to privacy protection of RFID tags that does involve a certain amount of cryptographic design, but is fairly simple. Our solution, moreover, does not require any capabilities beyond the limited ones of the current generation of RFID tags. We assume that intensive cryptographic operations take place in relatively high-powered devices for handling banknotes, rather than in the banknotes themselves. We use public-key encryption of serial numbers (and associated digital signatures) in RFID tags in our scheme, with a corresponding private key stored appropriately by a law enforcement agency.

The basic idea in our proposal is to employ *re-encryption* to cause ciphertexts to change in appearance while the underlying plaintexts, i.e., the encrypted serial numbers, remain the same. We may view the global structure of our scheme as essentially analogous to that of a *mix network*, as introduced by [10]. One crucial difference, however, is that the entities performing re-encryption in our scheme have knowledge of the serial numbers, i.e., the plaintexts. Thus, we do not require any special homomorphic properties from the public-key encryption scheme. The term re-encryption generally refers in the literature to use of such homomorphic properties to enable transformation of a ciphertext value without knowledge of the plaintext. In this paper, though, we employ the term re-encryption with the unorthodox assumption that the plaintext is known.

Re-encryption of ciphertexts addresses the problem of their serving as meta-serial-numbers, thereby enforcing privacy even if banknotes transmit information promiscuously. The re-encryption operation might be performed by shops and retail banks, and even by consumers. Some shops now make use of optical scanning devices for electronic cheque conversion [14]. Devices of similar size and cost can perform exactly the operations required by our scheme for banknote privacy. This approach, though, introduces a couple of problems. First, how do we ensure that re-encryption is performed only at appropriate times and not, e.g., by a malicious passerby? Second, how to we ensure that re-encryption is performed properly, and that banknote holders or handlers are not deceptively embedding false information in RFID tags, or indeed, swapping information between banknotes? We address these two critical problems in this paper, among others.

One of the considerable advantages of our scheme is the flexibility it permits in law enforcement policy. For banknotes with which they have only made contact via RFID, law enforcement agents can only learn the serial number on performing an asymmetric decryption operation. Because the private decryption key for this operation can be distributed in a threshold manner using standard secret-sharing techniques [27], a broad range of policies can be used to restrict access to tracing information. In terms of management of this private key, our scheme may be viewed as a type of escrow on banknote serial numbers, analogous to key escrow of the traditional cryptographic type. Serial numbers are quasi-public values, however, unlike the keys that are handled by traditional escrow schemes. Thus

potentially suitable for embedding in banknotes. We cite the Atmel TK5552, though, merely as an example of the existing range of capabilities in RFID tags.

we employ rather different tools for creating and verifying the escrowed values to begin with.

Any approach of the kind we describe here – and indeed, we believe, any approach that provides effective privacy for RFID tagged banknotes – must permit fairly widespread alteration of RFID tag information. With this in mind, we now provide a rough enumeration of the properties that we feel a banknote-tracing system based on RFID tagging should provide:

1. **Consumer privacy:** Only law enforcement agencies (and not even the Central Bank) should be able to trace banknotes effectively using information transmitted by RFID tags. This should certainly be the case even if law-enforcement RFID signals are intercepted, and should even hold if law-enforcement field monitoring equipment is captured and successfully reverse engineered. Tracing should only be possible using an appropriately protected private key. We formalize this requirement in section 5.
2. **Strong tracing:** Given interception of valid RFID information from a given banknote, law enforcement should be able to determine the associated serial number.
3. **Minimal infrastructure:** Consumers should require no special equipment for the handling of banknotes. Merchants and banks should require only relatively inexpensive devices for this purpose, and should not require persistent network access. The system should be backward compatable, in the sense that banknotes can, if desired, be used and exchanged without reference to RFID tags.
4. **Forgery resistance:** A forger must at a minimum make optical contact with a banknote in order to be able to forge a copy bearing the same serial number and other data, e.g., associated digital signatures. A forger should be unable to forge new banknotes with previously unseen serial numbers, and should be unable to alter the denomination associated with a given banknote.
5. **Privilege separation:** So as to prevent wayward or malicious tampering with banknote information, RFID tag data should only be alterable given optical contact with banknotes, even if readable though RFID contact alone.
6. **Fraud detection:** If invalid law-enforcement information is written to an RFID tag on a banknote, this should be widely detectable, particularly by any merchant handling the banknote.

1.2 Organization

In section 2, we provide an introduction to RFID tags, describing their characteristics and capabilities. We describe our trust assumptions in section 3 as well as conceptual and cryptographic building blocks. We provide details of our proposed system in section 4. In section 5, we analyze the security of our scheme, proposing a definition of privacy and also touching on the range of non-cryptographic attacks possible in RFID-enabled systems. We conclude in section 6 with a discussion of some of the practical considerations in deploying our system and some

open issues. Formal definitions and additional notes are included in the appendix to the paper.

2 A Primer on RFID Tags

As explained above, an RFID tag is a device capable of transmitting radio-frequency signals, typically for the simple purpose of emitting a static identifier, that is, a uniquely identifying bit-string. In its simplest form, an RFID tag consists of a small silicon integrated circuit adjoined to an antenna, which may be printed on substrate roughly as thin as a piece of paper. Such tags presently cost in the vicinity of $0.50 per unit (U.S.). Thanks to emerging manufacturing techniques, however, the per-unit cost of RFID tags promises to drop to $0.05 or less [25, 26] in the next several years. Their physical form, while already quite compact, is in the process of reduction to a slender, paper-thin strip just several centimeters in length. Naturally, the computational capabilities of such small, inexpensive devices is quite constrained. As we will see below, most of the work in any communication with the tag is performed by the tag reader.

The cheap and compact RFID tags suitable for inclusion in banknotes are of a type known as *passive*. Passive tags do not have any internal power sources; rather, they are dependent on the RF field from the tag reader for their power. In a typical scenario, the reader first transmits RF radiation at a given frequency. This powers the tag which, after receiving a sufficient amount of power, modulates the incoming radiation with its stored data. The reader then demodulates and decodes the tag's response to recover the data. Examples of passive RFID tags include electronic article surveillance (or anti-theft) tags embedded in compact discs and books.

There are two other, more heavyweight categories of RFID tags known as *semi-passive* and *active* tags. Semi-passive tags have a battery on board. This allows them to be read from a longer range. Active tags, as distinct from passive and semi-passive tags, are capable of initiating the transmission from their location; they do not require a reader to interrogate them first. The only limitations on the range at which semi-passive and active tags can be read are power and reader sensitivity. A mobile telephone is an example of an active tag; it has a unique identity i.e., the phone number, and is capable of initiating transmission to a base station a long distance away. For size and cost reasons, however, it is impractical to include semi-passive or active tags in banknotes.

There are several bands of the spectrum in which RFID tags operate. These bands are usually regulated by quasi-governmental organizations in various countries. In the U.S., the Federal Communications Commission (FCC) is responsible for regulating all telecommunications by radio, television, wire, satellite and cable. The most commonly used unlicensed frequencies in RFID are 125 KHz (low frequency or LF), 13.56 MHz (high frequency or HF), 915 MHz (ultra high frequency or UHF), and 2.45 GHz (microwave). To many consumers, LF tags are familiar in the form of small plaques mounted on car windshields for the purpose of automatic toll payment. Although there has been no formal announcement

regarding the frequency at which ECB banknote tags will operate, there are several reasons to believe that these tags will operate in the microwave band. Among these reasons are: (1) The ICs of microwave tags are extremely small, allowing them to be manufactured at very low cost; (2) The antennae for these tags are also much smaller than those for tags operating at a lower frequency; and finally (3) These tags can be attached to paper substrates with ease [29].

In general, the necessary size of the tag decreases as the frequency increases, but this leads to a substantial increase in the complexity of the tag reader. Further, the rate at which information is transferred from the tag to the reader is directly proportional to the frequency. As a practical matter, this has implications for the amount of time the tag has to spend in the field of a given reader. The lower the data rate from the tag to the reader, the longer the tag has to spend in the field of the reader. For example, a commercially available tag operating at 125 KHz transmits its ID at 7.8 Kbps. This means that a tag has to remain in the field of the reader for approximately 128 ms. At 13.56 Mhz, the tag-to-reader data rate could be on the order of 50 Kbps, allowing a substantially diminished time in the field to read the same amount of data. At 915 MHz, the tag to reader data rate is higher still, on the order of 128 Kbps. The high tag-to-reader data rate assumes greater importance as the amount of information stored on the tag increases.

The small, passive tags suitable for inclusion in banknotes may be constructed with electrically-erasable programmable memory (EEPROM). A typical RFID communication protocol allows the reader to perform several operations on the memory of these tags. The simplest possible commands that the reader can issue are *read* and *write*, wherein the reader simply reads or writes the memory on the tag. Many protocols support anti-collision, that is, the ability for multiple tags with unique identities to be simultaneously read by the same reader. A tag may also receive a *sleep* command which renders it unresponsive to further commands from the reader. This state is maintained until the tag receives a *wake* command, accompanied by a tag-specific key. (*Sleep* is thus a keyed function.) Finally, a tag may be completely deactivated with a *kill* command, which renders the memory completely inaccessible forever. We note that typical passive tags available today have memory capacities of no more than a few kilobits and transmit at a maximum rate of about on the order of 100 Kbps.

Our proposed scheme is based on RFID tag functions at a slightly higher level of sophistication, namely *keyed-read* and *keyed-write*. These are access-control functions applied to particular memory cells. An RFID tag will only permit a keyed-read on a read-protected memory cell if it receives a static secret key, and likewise for write-protected memory cells. The current generation of RFID tags do not include keyed write. These functions, though, may be easily enabled in the manufacturing process, and are envisioned for near future generations of RFID tags. The Atmel TK5552 [13] is an example of a commercially available tag that supports a majority of these functions.

3 Preliminaries

We have stated our system goals in the list of requirements in section 1. Before presenting details, it is also useful for us to give a loose description of the trust model motivating our construction. In particular, we assume the participation of four entity types, characterized as follows:

1. **Central Bank:** The Central Bank, denoted by $\mathcal{B}$, is the organization empowered to create and issue banknotes. $\mathcal{B}$ also furnishes the digital signatures for banknotes, as we shall see. We assume that the principal security-related aim of the Central Bank is to prevent forgery. Thus, for example, the Central Bank has an interest in issuing banknotes with unique serial numbers and in protecting its digital signing key. We do not, however, assume an interest on the part of the Central Bank in protecting consumer privacy or ensuring effective tracing by law enforcement.
2. **Law Enforcement:** This entity, denoted by $\mathcal{L}$, consists of one or more agencies with an interest in tracing banknote flows. Our system aims to provide a high degree of assurance that the values embedded in banknote RFID tags facilitate this tracing. The law enforcement agency, we assume, wishes to ensure that its privileges are not infringed upon, i.e., that the ability of other entities to trace bills is minimized.
3. **Merchant:** Merchants are entities that handle banknotes, accepting them for payment and perhaps agreeing to anonymize them on behalf of consumers as a free service. We assume that most merchants seek to ensure compliance with law enforcement requirements, that is, that they will report irregularities in banknote information. We consider the possibility that merchants may attempt to compromise consumer privacy. We use $\mathcal{M}$ to denote a merchant, treating $\mathcal{M}$ as a generic label. Retail banks may perform the same range of banknote-handling operations as merchants.
4. **Consumer:** The bearer of a banknote, the consumer, denoted generically by $\mathcal{C}$, has an interest in protecting her own privacy. That is, the consumer seeks to restrict tracing of her banknotes in the highest possible degree. Toward this end, we consider that in some cases, consumers may even breach law enforcement regulations by corrupting the tracing information contained on banknote RFID tags.

3.1 Building blocks and concepts

Public-key encryption: Our scheme employs as its basis an arbitrary public-key cryptosystem providing chosen-ciphertext security against adaptive adversaries, of which many are known in the literature. We do not define the notion here, but instead refer the reader to, e.g., [4] for a discussion of cryptosystem security definitions. As explained above, the idea in our system is to generate a ciphertext C on the serial number S for a given banknote under a public key $PK_{\mathcal{L}}$ generated by $\mathcal{L}$. By employing the corresponding private key, $\mathcal{L}$ can extract S from C. In order to achieve the desired security guarantees, the encryption operation must

take as input a randomly generated value known as an *encryption factor*. We let **R** denote the set of valid encryption factors for a given security parameter.

Note that our privacy and practicality requirements (1-3) as stated in the introduction to this paper can be fully satisfied with a simple system in which a ciphertext C on a unique serial number S for a given banknote is the only information on the RFID tag. On receiving a bank note, a merchant can optically read the serial number from the note (using a scanning device), encrypt it under the public key $PK_{\mathcal{L}}$, and replace the existing ciphertext with this new one. Under the assumption of chosen-ciphertext security, it is infeasible for an adversary to determine whether the new ciphertext indeed corresponds with the old one. (In isolation, this property is known as semantic security [18].) Re-encryption thus provides the desired assurance of consumer privacy. The problem with this approach is that an attacker can create a ciphertext on any serial number she likes and place it on the RFID tag, causing this false serial number to be propagated. Thus our scheme requires some additional components for testing the validity of tracing information.

Digital signature: Rather than encrypting the serial number S for a given banknote, we instead propose encrypting a digital signature Σ on S produced by the Central Bank. This component of our system addresses requirement 4, namely *forgery resistance*. With use of a digital signature of this kind, an attacker cannot forge serial-number information from scratch for placement on any RFID tag. Our system can in principle accommodate any type of digital signature scheme secure against chosen-message attack, as defined in [19]. We discuss particular choices suitable for the limited memory of RFID tags in section 4.1.

Optical contact vs. RFID contact: The two requirements that are not satisfied by even the use of digital signatures are requirements 5 and 6, those of *privilege separation* and *fraud detection*. Privilege separation is important so as to prevent remote attacks on the banknotes of passersby, i.e., erasure or alteration of their RFID tag information through RF contact alone. Fraud detection is also quite important. Without it, a criminal can swap the information of RFID tags on different banknotes, while law enforcement agents will be unable to detect this type of attack without physical or at least optical contact with the banknote. Indeed, if an attacker plants a ciphertext in a banknote corresponding to an invalid signature, a merchant will be unable to detect this fact, since the merchant cannot decrypt it. Our view, however, is that the ability of merchants to detect invalid ciphertexts is critical in preventing criminal tampering with RFID tags, as law enforcement agencies may not often come in physical contact with individual banknotes in circulation.

To address these problems, we exploit in our system design the availability of two different channels, or data types, which we describe as *optical* and *transmission*. Optical information is simply data printed on a banknote, and presumed to be readable by the devices performing re-encryption, namely the banknote-handling machines of merchants. This information may be encoded in human readable form, and perhaps alternatively in machine-readable form as a 2-D bar

code. We assume that it includes a serial number S unique to the banknote and also a unique access-rights key D, whose form we specify later; other information such as the denomination, series, and origin of the note might also be included. By transmission information, we mean the contents of the RFID tag as released upon successful query by an RFID reader. Such a distinction between different types of physical contact with security-system components is not often formally identified in security architecture design, but arises from time to time. Some examples include systems using biometric authentication, digital-rights management systems for CD-ROMs, and the "resurrecting duckling" protocol described in [28].

As explained in our primer on RFID tags in section 2, one of their capabilities is control of read/write access privileges by means of static keys. In our proposed system, we thus restrict access privileges to two memory cells in the RFID tag for a banknote. Privileges for these two cells are protected under the key D, which, as stated above, can only be obtained through optical contact with the banknote. The first protected memory cell is that containing the ciphertext C on the serial number and associated digital signature for the banknote. This cell is universally readable via RF, but its write privileges are keyed to D. Our aim here is to satisfy requirement 5, that of privilege separation, thereby limiting adversarial alteration of the ciphertext C.

In the second protected memory cell is stored the encryption factor r particular to the current ciphertext C in the first memory cell. Both read and write privileges for this second cell are keyed under D. Access to this second cell permits verification of the ciphertext C, and does so without knowledge of the law-enforcement decryption key x, as explained below. Hence, by accessing the contents of this second memory cell, and reading S optically from a banknote, it is possible for a merchant to verify that the ciphertext C is correct. Thus, a merchant making optical contact with a banknote can verify the correctness of law-enforcement information. On the other hand, it is important to deny access to the encryption factor r to parties making RF contact alone with a banknote, as they could otherwise extract the serial number S. Hence, by placing the encryption factor in the second memory cell, we satisfy requirement 6, that of fraud detection, while not undermining the privacy requirements of our scheme. After verifying the correctness of the ciphertext C contained in a banknote she has received, $\mathcal{M}$ may then create a new ciphertext C' with a new, random encryption factor r', and use write access privileges obtained from knowledge of D to overwrite C with C' and r with r'.

Tracing attacks by the Central Bank: As discussed later, if the Central Bank $\mathcal{B}$ does not select a unique access key D for each banknote, this can facilitate an attack whereby the bank determines banknote serial numbers through RF contact alone. In the extreme case, $\mathcal{B}$ can assign the same key D to every banknote. In this case, $\mathcal{B}$ can successfully determine the re-encryption factor for the ciphertext C read from any banknote via RF contact, and then decrypt the associated serial number. We assume that the Central Bank wishes to ensure against forgery, and therefore assigns a unique serial number S to each ban-

knote. We do not, however, entrust $\mathcal{B}$ with the task of guarding against privacy abuses on its own part. Instead, we have $\mathcal{B}$ compute the key D in a manner such that merchants can verify its correct computation, but such that D still carries a sufficient cryptographic guarantee of uniqueness. To do so, we leverage the uniqueness of serial numbers assigned by $\mathcal{B}$, along with a special property on the digital signature scheme used to sign these serial numbers. This special property, known as *signature uniqueness*, means essentially that a signer cannot produce a single signature that is valid for two messages. Discussion of this property and a formal definition are given in appendix A.

4 Our Scheme

Setup: We let $CS = (\mathsf{KG}, \mathsf{Enc}, \mathsf{Dec})$ denote a public key cryptosystem with component algorithms performing key generation, encryption, and decryption respectively. We also make use of a digital signature system $DS = (\mathsf{SKG}, \mathsf{Sig}, \mathsf{Ver})$ whose constituent algorithms are key generation, signing, and verification respectively. For more formal and detailed definitions, see appendix A.

For a security parameter k_1 appropriate for long-term security, bank $\mathcal{B}$ generates a digital signing key pair $(PK_{\mathcal{B}}, SK_{\mathcal{B}}) \leftarrow \mathsf{SKG}(1^{k_1})$. Likewise the law enforcement agency $\mathcal{L}$ generates a cryptosystem key pair $(PK_{\mathcal{L}}, SK_{\mathcal{L}}) \leftarrow \mathsf{KG}(1^{k_1})$. The public keys $PK_{\mathcal{B}}$ and $PK_{\mathcal{L}}$ are published for availability to all participating entities. Also published is a collision-intractable hash function $h : \{0,1\}^* \rightarrow \{0,1\}^{2k_2}$ for an appropriate security parameter k_2. In what follows, we let $\|$ denote bitstring concatenation on plaintexts, and let $\in_R$ denote uniform random selection from a set.

Banknote creation: For every banknote i to be printed, $\mathcal{B}$ selects a unique serial number S_i and computes $\Sigma_i \leftarrow \mathsf{Sig}(SK_{\mathcal{B}}, [S_i \parallel den_i])$. Here, den_i is the banknote denomination, incorporated into the digital signature to prevent attacks involving forgery through alteration of a banknote denomination. A denomination specifier might alternatively be included in S_i. Additionally, $\mathcal{B}$ generates an access key $D_i \in \{0,1\}^{k_2}$ for the note. The key D_i is computed as $h(\Sigma_i)$. The *signature-uniqueness* of the digital signature scheme combined with the collision intractability of h together ensures that D_i is unique to each banknote.[5]

$\mathcal{B}$ prints S_i and Σ_i on the banknote in a manner to facilitate automated optical decipherment by merchant machines, e.g., 2-D barcodes. The serial number S_i might also be printed in human-readable form. Additionally, $\mathcal{B}$ computes

[5] It is important that D_i be computed from Σ_i, rather than S_i. Otherwise an attacker able to guess serial numbers successfully would be able to determine D_i values without even making optical contact with target banknotes. For example, it might be that batches of freshly printed banknotes carry consecutive serial numbers. In this case, an attacker making a withdrawal at a bank would be able to guess the serial numbers of other patrons making withdrawals at roughly the same time. If the D_i values of these banknotes are derived from serial numbers, the attacker can track the other patrons via RFID contact.

the ciphertext C_i as an encryption of Σ_i and S_i. In particular, $\mathcal{B}$ inserts a randomly selected encryption factor r_i into memory cell δ_i and the ciphertext $C_i = \mathsf{Enc}(PK_{\mathcal{L}}, [\Sigma_i \parallel S_i], r_i)$ into memory cell γ_i. It is useful to note that $\mathcal{B}$ need not store access keys or other special information for individual banknotes in order for our scheme to work. The bank may simply record serial numbers and denominations according to its normal policy.

Figure 1 provides a schematic layout of the data incorporated into a banknote in our scheme. For visual clarity, we omit subscripts in this figure.

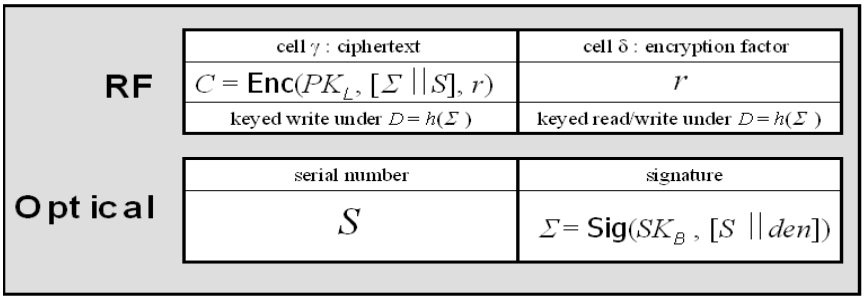

Figure 1. Banknote data

Banknote verification and anonymization: On receiving a banknote j for payment and/or anonymization, the Merchant $\mathcal{M}$ first verifies the correctness of the existing contents with the following steps:

1. $\mathcal{M}$ optically reads S_j, Σ_j, and D_j.
2. $\mathcal{M}$ computes $D_j = h(\Sigma_j)$.
3. $\mathcal{M}$ reads C_j from γ_j, and performs a keyed read of δ_j under key D_j, yielding the value r_j. If the keyed read fails, the banknote is submitted to law enforcement.
4. $\mathcal{M}$ checks $C_j = \mathsf{Enc}(PK_{\mathcal{L}}, [\Sigma_j \parallel S_j], r_j)$. If not, the invalid ciphertext is reported to law enforcement.

After verifying the contents of the banknote, $\mathcal{M}$ replaces the ciphertext C_j as follows.

5 $\mathcal{M}$ selects $r'_j \in_R \mathbf{R}$ and performs a keyed write of r'_j to δ_j under key D_j. If the keyed write fails, the banknote is submitted to law enforcement.
6 $\mathcal{M}$ computes $C'_j = \mathsf{Enc}(PK_{\mathcal{L}}, [\Sigma_j \parallel S_j], r'_j)$. $\mathcal{M}$ performs a keyed write of C'_j to γ_j under key D_j. $\mathcal{M}$ reports any failure in this step to law enforcement.

For a remark on reducing the computational costs for $\mathcal{M}$, see appendix B.

Banknote tracing: To obtain the ciphertext C from a target banknote, $\mathcal{L}$ need simply read the contents of the memory cell γ from the associated RFID tag. From the ciphertext C, $\mathcal{L}$ computes the plaintext $[\Sigma \parallel S] = \mathsf{Dec}(SK_{\mathcal{L}}, C)$. Then $\mathcal{L}$ checks whether Σ is a valid signature on S, i.e., whether $\mathsf{Ver}(PK_{\mathcal{B}}, \Sigma, [S \parallel den]) =$ '1'. (The security parameter 1^{k_1} is required here for technical reasons discussed in appendix A.) Provided that C was correct, then this will indeed be the case, and $\mathcal{L}$ will obtain the serial number S.

4.1 Algorithm and parameter choices

An especially attractive choice of encryption scheme CS for our system is the El Gamal cryptosystem [17], thanks primarily to its amenability to encoding over elliptic curves. When computed over appropriately parameterized elliptic curves, El Gamal ciphertexts can offer good security at quite compact sizes – on the order of 40 bytes. This is a useful feature given the limited storage available on RFID tags. Let $\mathcal{G}$ denote an appropriate elliptic-curve-based group with prime order q and published generator P. We assume throughout that all cryptographic operations take place over $\mathcal{G}$. For basic El Gamal encryption, we require a group $\mathcal{G}$ over which the Decision Diffie-Hellman problem is presumed to be hard; for the Fujisaki-Okamoto scheme, discussed below, the requirement on $\mathcal{G}$ can be relaxed to the Computational Diffie-Hellman assumption.

Let $SK_{\mathcal{L}} = x \in_R Z_q$ be a private decryption key held by law-enforcement. The value $PK_{\mathcal{L}} = Y = xP$ is the corresponding, published public encryption key. A message $m \in \{0,1\}^w$ for suitably small w is encrypted under $PK_{\mathcal{L}}$ as follows: $\mathsf{Enc}(PK_{\mathcal{L}}, m, r) = (\alpha, \beta) = (m + rY, rP)$, where $r \in_R Z_q$.

By itself, this form of El Gamal is not secure against adaptive chosen-ciphertext attacks. Provided that CS is a one-way encryption scheme, then it is possible to employ a technique due to Fujisaki-Okamato [16] toward this end. Let $h_1, h_2 : \{0,1\}^* \to \{0,1\}^w$ be two cryptographic hash functions. For public key PK, the Fujisaki-Okamoto system converts a basic encryption scheme Enc on plaintext $m \in \{0,1\}^w$ into a hybrid encryption scheme Enc^* as follows:

$$\mathsf{Enc}^*(PK, m, \sigma) = (\mathsf{Enc}(PK, \sigma, h_1(\sigma \parallel m)), h_2(\sigma) \oplus m),$$

where $\sigma \in_R \{0,1\}^w$ is a random encryption factor. The security of this scheme depends on the random oracle assumption on h_1 and h_2.

Although our system can in principle accommodate essentially any type of digital signature, it is important for practical purposes that the signature be short. A particularly attractive scheme is that of Boneh, Shachem, and Lynn [7], which yields signatures of roughly 20 bytes in length. The security is comparable to that of to ECDSA, for which signatures are about twice as long. This scheme makes use of the Weil pairing on a specially chosen elliptic-curve-based group; a signature consists of a single point on the elliptic curve. Another possible choice of digital signature scheme is QUARTZ [23], which yields signatures a mere 128 bits in length. This scheme, however, is based on a somewhat less well understood hardness assumption, and has a rather longer public key. Yet another scheme

that yields even shorter digital signatures is based on the McEliece cryptosystem [15]. The public key for this last, however, must be over 1Mb in length to achieve good security, and the scheme is somewhat slow.

Note: Chosen-ciphertext security may in fact be regarded as unnecessary in our system, depending on the extent to which law-enforcement information is likely to be divulged. In practice, a chosen-ciphertext attack would seem to be hard to mount against $\mathcal{L}$, as it would require access to private details of law-enforcement tracing activities. If plaintexts are indeed not likely to be available to an attacker, the basic El-Gamal cryptosystem would be deemed sufficient. Provided that the Decision Diffie-Hellman problem [6] is hard over $\mathcal{G}$, El Gamal possesses the property of semantic security [30], which is adequate for these purposes.

Sample parameters: European Central Bank plans presently call for a total availability of 14.5 billion banknotes [1]. Let us suppose that a maximum of one trillion (slightly less than 2^{40}) banknotes are to be printed over the lifetime of our scheme. Thus a serial number S_i might be encoded as a 40-bit value. For the Boneh *et al.* signature scheme, we might use a GDH (Gap Diffie-Hellman) group over E/F_{3^l} yielding a signature size of 154 bits (with discrete-log security equivalent to that of a subgroup of 151 bits) [7]. Thus, a plaintext $[\Sigma_i \parallel S_i]$ in our scheme would be 194 bits in length. We might therefore let $\mathcal{G}$ be an elliptic-curve-based group of 195-bit order. By employing the Fujisaki-Okamoto variant on El-Gamal with $n = 195$, we then achieve a ciphertext length of 585 bits. The encryption factor r for a ciphertext would be 195 bits in length. Thus the total memory requirement for our scheme would be 780 bits – well less than the 992-bit memory capacity of, e.g., the Atmel TK5552 RFID tag. As noted above, in the case that semantic security is deemed sufficient for the underlying cryptosystem CS, the total memory requirement can be reduced to 585 bits. Use of the QUARTZ digital signature scheme or the McEliece variant would further reduce memory requirements. Other optimizations are possible.

5 Security Analysis

The requirements of strong tracing and forgery resistance – indeed, more generally, requirements 2-6 – are straightforward enough from a cryptographic point of view so that we do not formally define them. For example, requirement 4 is fulfilled by the resistance of the underlying signature scheme to forgery. In contrast, the requirement of consumer privacy (requirement 1) is somewhat trickier to capture. The crux of the problem is that the key D_i for every banknote is known to the Central Bank $\mathcal{B}$. Additionally, a set of these keys may become known to a merchant $\mathcal{M}$, as they are read in the course of handling a banknote. In practice, banknote-handling machines could be rendered tamper-resistant so as to minimize disclosure of these keys. This, however, is not a foolproof approach,

particularly as an unscrupulous merchant can create his own banknote-handling machine.[6]

Thus, the strongest definition of consumer privacy regards an adversary with knowledge of a broad range of D_i values. Good privacy guarantees may still be attainable in this case by observing that an attack involving reading of a banknote using key D_i must take place *on the fly*, i.e., during RFID contact with the banknote. In other words, even if the adversary knows the keys D_i for all banknotes, she must guess which key D_i corresponds to a given, target banknote and then transmit that key to the banknote to learn the encryption factor r_i. Passive RFID tags generally transmit at a maximum rate of around 100 Kbps, as explained in section 2. Thus an adversary can expect to be able to make only a small number of on-line guesses in most cases – probably just several dozen with a fairly high-power reader operated against a passerby.

We should note additionally that if the Fujisaki-Okamoto construction is employed for encryption, then even knowledge of the encryption factor r_i for a ciphertext C_i does not immediately yield the corresponding serial number S_i. The serial number can be determined from the pair (C_i, r_i), but requires a potentially expensive brute-force attack. This attack may take place off-line, however, and is within the capabilities of a determined attacker. Thus, this partial concealment of S_i does not provide sufficient security *per se*.

Our definition of privacy aims to capture the capabilities of a very strong adversary. We consider the guessing success of an adversary with knowledge of *all* key values D_i. Additionally, as $\mathcal{B}$ itself might potentially constitute the adversary, we assume that this adversary may choose the digital signing keys and serial numbers of banknotes in the system. Another power we assume on the part of the adversary is that of mounting a chosen-ciphertext attack on the underlying cryptosystem.[7] The adversary may read the ciphertext C_i from a banknote, whereupon the aim of the adversary is to guess the corresponding key D_i. The key D_i in our scheme would yield the encryption factor for the associated ciphertext, and thus the serial number. Alternatively, the adversary might try to guess i or S_i directly, but given our strong assumptions about the power of the adversary, this implies the ability to guess D_i. We characterize the success of an adversary $\mathcal{A}$ in terms of the following experiment. We omit the value *den* here for clarity. Let H denote a family of hash functions and $\xleftarrow{f,k_2} H$ denote selection of a hash function from this family under a (possibly randomized) selection algorithm f and security parameter k_2.

[6] To prevent forgery of such machines, it is possible to create tamper-resistant modules that derive a re-encryption factor r'_j from an embedded, merchant-specific key $\kappa_{\mathcal{M}}$. For example, for banknote j, the machine might compute $r'_j = h'(\kappa_{\mathcal{M}}, S_j)$, where h' is a suitable cryptographic hash function. This would enable law enforcement authorities to detect unauthorized banknote-handling machines.

[7] As explained above, by removing the assumption that an adversary can mount an adaptive chosen-ciphertext attack, we can reduce the size of the ciphertext in our system from just over 800 to about 600 bits in practice.

Experiment $\mathsf{S\text{-}guess}(\mathcal{A}, \mathcal{G}, CS, DS, H, f); [k_1, k_2]$

1. The key pair $(PK_{\mathcal{L}}, SK_{\mathcal{L}}) \leftarrow \mathsf{KG}(1^{k_1})$ and hash function $h \xleftarrow{f,k_2} H$ are selected.
2. $\mathcal{A}$ receives as input the pair $(PK_{\mathcal{L}}, h)$.
3. $\mathcal{A}$ outputs a public signing key $PK_{\mathcal{B}}$.
4. $\mathcal{A}$ outputs a sequence $\{(S_i, \Sigma_i)\}_{i=1}^{n}$.
5. If $\mathsf{Ver}(PK_{\mathcal{B}}, S_i, \Sigma_i) =$'0' for any i, or $S_i = S_j$ for any $i \neq j$, then the output of the experiment is '0'.
6. For $i \in_R Z_n$ and $r \in_R \mathbf{R}$, $\mathcal{A}$ is given input $C = \mathsf{Enc}(PK_{\mathcal{L}}, [\Sigma_i \parallel S_i], r)$.
7. $\mathcal{A}$ outputs a guess $\tilde{D}$ at $D_i = h(\Sigma_i)$. If $\tilde{D} = D_i$, the output of the experiment is '1'. Otherwise, it is '0'.

Additionally in this experiment, $\mathcal{A}$ has access to encryption and decryption oracles for $PK_{\mathcal{L}}$ at any time during steps 2-5 on any ciphertext, and subsequently on any ciphertext other than C.

Note that an adversary that simply chooses $\tilde{D} \in_R \{D_i\}_{i=1}^{n}$ can succeed trivially with probability $1/n$. Thus, for any adversary $\mathcal{A}$, let us define the advantage of the adversary for fixed cryptographic primitive choices to $\mathsf{S\text{-}guess}$ as

$$\mathbf{Adv}_{\mathsf{S\text{-}guess}}(\mathcal{A}, k_1, k_2) = \mathsf{pr}[\mathsf{S\text{-}guess}(\mathcal{A}, \mathcal{G}, CS, DS, H, f); [k_1, k_2] = \text{'1'}] - 1/n.$$

Claim 1: Suppose that CS is a public-key cryptosystem with adaptive chosen-ciphertext security and DS a digital-signature scheme with resistance to adaptive chosen-message attack and signature uniqueness. Further, suppose that the hash function family H under f is collision-resistant.[8] Then the quantity $\max_{\mathcal{A}}[\mathbf{Adv}_{\mathsf{S\text{-}guess}}(\mathcal{A}, k_1, k_2)]$ is negligible when taken over all adversaries with running time polynomial in k_1 and k_2.

Proof: [sketch] Given the uniqueness of all elements in the set of serial numbers $\{S_i\}_{1=1}^{n}$, and the signature uniqueness of DS, the set $\{\Sigma_i\}_{i=1}^{n}$ comprises unique elements. It follows from the collision resistance of h, then, that all elements of the key set $\{D_i\}_{i=1}^{n}$ are unique with overwhelming probability. Under the adaptive-chosen-ciphertext security of CS, the adversary can determine the serial number S corresponding to ciphertext C with only negligible advantage. Hence, the adversary can successfully guess D_i with only negligible advantage. □

Our definition and proof are straightforwardly extensible to the scenario in which $\mathcal{A}$ is permitted multiple guesses at D_i, instead of just one. Another type of adversary worth considering is a casual one that does not have knowledge of any keys D_i. It is clear that such an adversary can determine S_i with overall probability only negligible in k_2, even if permitted a polynomial number of RFID tag queries.

[8] In practice use of a fixed, standard hash function like SHA-1 would be acceptable. If desired, this hash function can additionally be keyed with a random value bound to each individual banknote, effectively a kind of salt.

5.1 Further work: Other attacks

We have characterized the range of possible cryptographic attacks against consumer privacy in our system. Another potential problem for consumer privacy, as mentioned above, is the fact that RFID tags may betray the presence of Euro notes on a bearer. We do not have a comprehensive solution to this problem. One possible approach is for RFID tags to sit normally in a partially "sleep" state, in which they do not "wake" for transmission unless they receive either D_i or a universal law-enforcement key κ. We have already noted the shortcomings of employing a universal law-enforcement key, but this might still be a useful supplementary privacy-protecting measure. An alternative is to embed RFID tags in banknotes of different denominations - or to provide cheap spoofing tags by banks and shops or wallet manufacturers.

Another range of attacks to consider are possible evasions by consumers, that is, violations of the system requirement of strong tracing. Merchants are capable of detecting invalid ciphertexts in banknotes. It is easily possible for the bearer of a banknote, however, to insert a fake ciphertext into the banknote for use while subject to possible law-enforcement monitoring, e.g., before travelling through public places. The bearer can then reintroduce a valid ciphertext prior to spending or depositing the banknote. Indeed, the fake ciphertext used in this attack might be "lifted" from a passerby. One possibility for mitigating this risk is to omit Σ_i from the optical information on the banknote, and to construct ciphertexts so that they can be decrypted using r_i. In this case, an attacker who separates the valid signature Σ_i from a banknote and stores it externally runs some risk of losing the signature and thereby invalidating the banknote if she is not careful. Bank policy might require presentation of some proof of identity in order for invalidated banknotes to be exchanged for valid ones.

The possibility of introducing fake ciphertexts into banknotes results from the write capabilities in our proposed system. A very similar attack, however, would be easy to mount even in a system with RFID tags bearing static information. An attacker might with little difficulty create RF devices with the purpose of transmitting fake serial number information – information that may, again, be obtained from passersby. An even more basic attack is possible in any system employing RFID tags: An attacker can simply shield the tags from discovery. Isolation of banknotes in a Faraday cage would constitute a simple and effective attack of this kind. We stress, therefore, that any form of banknote tracing using RFID tags has shortcomings exploitable by a knowledgeable attacker, and that further work is required to address such problems.

6 Conclusion

We have proposed a banknote system design that appeals to the capabilities of the current generation of RFID tags to achieve stronger consumer privacy. It must be stressed that the system does not provide comprehensive privacy protection. Re-encryption of consumer banknotes by merchants, after all, may

not occur conveniently with as high a level of frequency as desired by some consumers. Our proposal does, however, go considerably farther than existing ones toward addressing a fundamental privacy issue.

Our observations may also provide some useful insight into how future RFID-tag architectures can offer enhanced functionality at the hardware level in support of both security and privacy. We would like RFID tags in our system to output read-protected information rapidly on presentation of a correct key D_i. On the other hand, an important feature in protecting consumer privacy in our system is the inability of an attacker to mount a rapid on-line attack involving guessing of D_i. In a sense, RFID tags naturally limit the rate of on-line attacks due to their slow processing and transmission capabilities. Ideally, however, this rate limiting might be improved. For example, an RFID tag might be designed to switch to a low data rate mode while transmitting all publicly available information on presentation of an invalid key D_i, thereby delaying subsequent guessing by an attacker. It is our belief that this feature could be incorporated into RFID tags at little cost.

Our definition of forgery resistance states that an attacker should be able to forge a banknote at a minimum only on making optical contact. This is the best that can be achieved based on data protection alone. Further protection against forgery must rely on physical protection mechanisms. There are a host of anti-forgery devices already incorporated into Euro and other banknotes [2]. By combining data security and physical security techniques, however, still better forgery resistance is possible. A number of researchers have investigated the use of distinctive characteristics of physical media as "fingerprints" to prevent device or object cloning, e.g., [12, 22]. It is our belief that the patterns of special fibers or other inclusions in banknotes may be used similarly. By incorporating such a "fingerprint" reading into the digital signature associated with a given banknote, a binding may be achieved between the physical embodiment of the note and the digital data. This binding might be checked by merchant scanning machines to create a truly formidable obstacle to banknote forgery. This represents just one of the many possible ways in which RFID tags might offer a closer integration of the physical and digital worlds.

Acknowledgments

The authors extend their thanks to Burt Kaliski and Markus Jakobsson for their helpful comments.

References

1. European Central Bank Euro FAQ, 2002. Euro circulation discussed at http://www.euro.ecb.int/en/section1/frequently/printing.html.
2. European Central Bank Euro FAQ, 2002. Euro security features discussed at http://www.euro.ecb.int/en/section/recog.html.

3. Registry of Motor Vehicles reforms: Progress report III, 2002. Available at http://www.state.ma.us/rmv/rmvnews/progrpt3.htm.
4. M. Bellare, A. Desai, D. Pointcheval, and P. Rogaway. Relations among notions of security for public-key encryption schemes. In *CRYPTO '98*, pages 26–45. Springer-Verlag, 1998. LNCS no. 1462.
5. M. Bellare and P. Rogaway. Random oracles are practical: A paradigm for designing efficient protocols. In *1st ACM Conference on Computer and Communications Security*, pages 62–73. ACM, 1993.
6. D. Boneh. The Decision Diffie-Hellman problem. In *ANTS '98*, pages 48–63. Springer-Verlag, 1998. LNCS no. 1423.
7. D. Boneh, H. Shacham, and B. Lynn. Short signatures from the Weil pairing. In *ASIACRYPT '01*, pages 514–532, 2001. LNCS no. 2139.
8. S. Brands. Untraceable off-line cash in wallets with observers (extended abstract). In *CRYPTO '93*, pages 302–318. Springer-Verlag, 1993. LNCS no. 773.
9. E. Brickell, P. Gemmell, and D. Kravitz. Trustee-based tracing extensions to anonymous cash and the making of anonymous change. In *SODA '95*, pages 157–166, 1995.
10. D. Chaum. Untraceable electronic mail, return addresses, and digital pseudonyms. *Communications of the ACM*, 24(2):84–88, 1981.
11. D. Chaum, A. Fiat, and M. Naor. Untraceable electronic cash. In *CRYPTO '88*, pages 319–327. Springer-Verlag, 1988. LNCS no. 403.
12. D. Clarke, B. Gassend, M. van Dijk, and S. Devadas. Secure hardware processors using silicon physical one-way functions. In R. Sandu, editor, *ACM CCS '02*, 2002. To appear.
13. Atmel Corporation. Atmel TK5552 data sheet, 2001. Available at http://www.atmel.com/atmel/products/prod227.htm.
14. Epson corporation. Epson cheque-imaging scanner: TM-H6000II with TransScan, 2002. Specifications available at http://pos.epson.com/pointofsale/station_printers/tmh6000iiTransScan.
15. M. Finiasz, N. Sendrier, and N. Courtois. How to achieve a McEliece-based digital signature scheme. In *Asiacrypt '01*, pages 157–174. Springer-Verlag, 2001. LNCS no. 2248.
16. E. Fujisaki and T. Okamoto. Secure integration of asymmetric and symmetric encryption schemes. In *CRYPTO '99*, pages 537–554. Springer-Verlag, 1999. LNCS no. 1666.
17. T. El Gamal. A public key cryptosystem and a signature scheme based on discrete logarithms. *IEEE Transactions on Information Theory*, 31:469–472, 1985.
18. S. Goldwasser and S. Micali. Probabilistic encryption. *J. Comp. Sys. Sci*, 28(1):270–299, 1984.
19. S. Goldwasser, S. Micali, and R. Rivest. A digital signature scheme secure against adaptive chosen-message attacks. *SIAM Journal on Computing*, 17(2):281–308, 1988.
20. M. Jakobsson. *Privacy vs. Authenticity*. PhD thesis, University of California at San Diego, 1997.
21. S. Jarecki and A. Odlyzko. An efficient micropayment system based on probabilistic polling. In R. Hirschfeld, editor, *Financial Cryptography '97*, pages 173–191. Springer-Verlag, 1997. LNCS no. 1318.
22. R. Pappu, B. Recht, J. Taylor, and N. Gerschenfeld. Physical one-way functions. *Science*, 2002. To appear.

23. J. Patarin, N. Courtois, and L. Goubin. QUARTZ, 128-bit long digital signatures. In *CT-RSA 2001*, pages 282–297. Springer-Verlag, 2001. LNCS no. 2020.
24. R. Rivest. Electronic lottery tickets as micropayments. In R. Hirschfeld, editor, *Financial Cryptography '97*, pages 307–314. Springer-Verlag, 1997. LNCS no. 1318.
25. S. Sarma. Towards the five-cent tag. Technical Report MIT-AUTOID-WH-006, MIT Auto ID Center, 2001. Available from http://www.autoidcenter.org/.
26. S. Sarma. Radio-frequency identification systems. In B. Kaliski, editor, *CHES '02*. Springer-Verlag, 2002. To appear.
27. A. Shamir. How to share a secret. *Communications of the Association for Computing Machinery*, 22(11):612–613, November 1979.
28. F. Stajano and R. Anderson. The resurrecting duckling: Security issues for ad-hoc wireless networks. In *7th International Workshop on Security Protocols*, pages 172–194. Springer-Verlag, 1999. LNCS no. 1796.
29. K. Takaragi, M. Usami, R. Imura, R. Itsuki, and T. Satoh. An ultra small individual recognition security chip. *IEEE Micro*, 21(6):43–49, 2001.
30. Y. Tsiounis and M. Yung. On the security of ElGamal-based encryption. In *PKC '98*, pages 117–134. Springer-Verlag, 1998. LNCS no. 1431.
31. C.P. Wallace. The color of money. *Time Europe*, 158(11). 10 September 2001. Available at http://www.time.com/time/europe/biz/magazine/0,9868,173522,00.html.
32. J. Yoshida. Euro bank notes to embed RFID chips by 2005. *EE Times*. 19 December 2001. Available at http://www.eetimes.com/story/OEG20011219S0016.

A Definitions

A randomized public-key cryptosystem comprises a triple of algorithms, $CS = (\mathsf{KG}, \mathsf{Enc}, \mathsf{Dec})$, denoting key generation, encryption, and decryption respectively. The system parameters include descriptions of $\mathbf{M}$ and $\mathbf{C}$, namely the message and ciphertext spaces for the algorithm, as well as a decryption of the set $\mathbf{R}$ of encryption factors (for discrete log systems, typically the set of integers Z_q, where q is the order of the group). We assume system parameters published in advance by a trusted party.

The key generation algorithm $(PK_{enc}, SK_{enc}) \leftarrow \mathsf{KG}(1^k)$ is randomized; it takes as input a security parameter k and outputs a public/private key pair (PK_{enc}, SK_{enc}). (As we assume the group $\mathcal{G}$ is fixed in advance, the security parameter k here may be regarded as having a predetermined upper bound.) The encryption algorithm $C \leftarrow \mathsf{Enc}(PK, m, r)$ is a deterministic algorithm that takes as input a public key PK, a message $m \in \{0,1\}^*$, and an encryption factor $r \in \mathbf{R}$. The algorithm Enc outputs a ciphertext $C \in \mathbf{C}$. Finally, the decryption algorithm $m \leftarrow \mathsf{Dec}(SK, C)$ takes as input a private key and ciphertext and outputs the corresponding plaintext. As explained above, we assume that CS has adaptive chosen-ciphertext security. (The most practical cryptosystems with chosen-ciphertext security achieve their security under the random-oracle model [5].)

A digital signature scheme is a triple of polynomial-time algorithms, $DS = (\mathsf{SKG}, \mathsf{Sig}, \mathsf{Ver})$, denoting key generation, signing, and verification respectively. We also assume a description $\mathbf{PK_{sig,k}}$ of the set of possible public keys PK_{sig} for

a given security parameter k; we assume an efficiently computable membership test thereon.

The key generation algorithm $(PK_{sig}, SK_{sig}) \leftarrow \mathsf{SKG}(1^k)$ takes as unary input a security parameter k and outputs a randomly selected public/private key pair (PK_{sig}, SK_{sig}) such that $PK_{sig} \in \mathbf{PK_{sig,k}}$. The signing algorithm $\Sigma \leftarrow \mathsf{Sig}(SK_{sig}, m)$ takes as input the private signing key $S\tilde{K}_{sig}$ and a message $m \in \{0,1\}^*$ and outputs a digital signature. The security parameter k is assumed to be known here or to be derivable from PK_{sig}. The verification algorithm $\{0,1\} \leftarrow \mathsf{Ver}(PK_{sig}, \Sigma, m)$ takes as input the public key and a purported digital signature / message pair. It outputs '1' if the signature is valid for m and also $PK_{sig} \in \mathbf{PK_{sig,k}}$; otherwise, it outputs '0'. The security parameter is input here to enable verification of the validity of the public signing key – a technical requirement to achieve privacy according to our definition above. We assume in our security analysis that the digital signature scheme employed in our system is fully resistant to chosen-message attacks. This property may be used to defend against forgery of banknotes bearing previously unseen serial numbers.[9]

As mentioned above, to prevent tracing attacks by $\mathcal{B}$ we do require an unorthodox property on the digital signature algorithm DS that we call *signature uniqueness*. In particular, it should be infeasible to generate keys, a message pair (m_1, m_2), and a signature such that the signature is valid for both messages. More formally:

Definition 1. Let DS be a digital signature scheme and $\mathcal{A}$ be an adversarial algorithm with running time polynomial in security parameter k. We define a *double signature* to be a tuple $\{(PK_{sig}, SK_{sig}), (m_1, m_2), \Sigma\}$ with the property that $\mathsf{Ver}(PK_{sig}, \Sigma, m_1) = 1$ and $\mathsf{Ver}(PK_{sig}, \Sigma, m_2) = 1$. In other words, the signature Σ is valid for two distinct messages under public key PK_{sig}. Let $\mathbf{Adv}_{DS}(\mathcal{A}, 1^k)$ be the probability under DS that the output $\mathcal{A}(1^k)$ for a given adversary $\mathcal{A}$ is a valid double signature. We say that DS has the property of *signature uniqueness* if $max_{\mathcal{A}}[\mathbf{Adv}_{DS}(\mathcal{A}, 1^k)]$ is negligible, i.e., less than $1/k^c$ for any positive integer c for sufficiently large k.

The property of signature uniqueness is an unusual one to consider in a digital signature scheme, as it assumes that the adversary may be the signer, rather than a forger.[10] Observe that even if, as is usually the case, a digital signature algorithm first involves application of a collision-intractable hash function h to

[9] In fact, one might argue that our system might employ a digital signature scheme that is resistant only to known, i.e., passive message attacks. This is because the process of printing banknotes and assigning serial numbers presumably does not admit input from an attacker. Nonetheless, given the minimal overhead required for a digital signature scheme that is fully resistant to chosen-message attacks, it makes sense to employ such a scheme.

[10] The attack might involve non-repudiation of an unorthodox kind in which the signer repudiates a signature on one message by evidencing another message with the same signature. As this would inculpate the signer, it is unclear whether this property should normally be of concern in a digital signature scheme.

a target message, the property of signature uniqueness does not immediately follow. This is because an adversary may still be able to generate a key pair and associated signature that are valid for both $h(m_1)$ and $h(m_2)$. Thankfully, most signature schemes naturally possess the property of signature-uniqueness under the assumption of collision-resistance on the underlying hash function. For example, the Boneh, Shachem, and Lynn [7] scheme, which fits into our proposed system quite naturally, may readily be seen to possess signature uniqueness. This is true given the collision-resistance on the underlying hash function for mapping to elliptic-curve points in the signature scheme, and provided that the trivial public key (l, q, P, P) (using the notation of [7]) is explicitly excluded, which we assume here.

For the RFID tag associated with the banknote bearing serial number i, we let γ_i denote the contents of the memory cell intended to contain the ciphertext C and let δ_i denote the memory cell intended to contain the encryption factor for the ciphertext. The cell γ_i is readable without any special privileges, but write-protected. The memory cell δ_i, on the other hand, has both read and write protection.

B Remark on Computational Costs for $\mathcal{M}$

The check by $\mathcal{M}$ in step 4 of the banknote verification and anonymization protocol is computationally expensive. It may be deemed sufficient, though, for $\mathcal{M}$ to perform this check on a probabilistic basis, so as to reduce on-line computational costs. The idea of probabilistic auditing of this kind has already been proposed in a similar setting, namely for electronic cash [21, 24].

To ensure merchant compliance, $\mathcal{M}$ should then be required to perform the check if the banknote data satisfy some predicate. It is important that this predicate not be computable by the holder $\mathcal{C}$ of a banknote, as $\mathcal{C}$ might then avoid presenting to $\mathcal{M}$ a banknote subject to verification. On the other hand, the behavior of the merchant and thus the predicate output must be auditable by law enforcement authorities. One possible approach is for each merchant $\mathcal{M}$ to hold a secret key $\kappa_{\mathcal{M}}$ assigned by $\mathcal{L}$. $\mathcal{M}$ would then be required to check the ciphertext on a banknote if $h''(\kappa_{\mathcal{M}}, S_i)/Z \leq p$, where Z is the maximum value in the range of a suitable cryptographic hash function h'' and $p \in [0, 1]$ is a minimum auditing probability selected by $\mathcal{L}$. In this case, if it becomes known in the course of a criminal investigation that $\mathcal{M}$ did not check a banknote with serial number S_i, $\mathcal{L}$ can determine whether or not $\mathcal{M}$ behaved correctly.

Probabilistic auditing is of limited benefit if the new encryption operation must be performed on-line by $\mathcal{M}$ in every instance. We note that if basic El Gamal is used, rather than the Fujisaki-Okamoto variant described below, however, then the computationally intensive step 6 can be largely performed offline. In particular, the encryption factor r' and the values $r'_j Y$ and $r'_j P$ may be precomputed. In this case, the online computational requirement of step 6 is only one modular multiplication (or addition, over an elliptic curve).