Using e-coins to ensure fair sharing of donor funds amongst HIV healthcare facilities

Martin S Olivier, JHP Eloff, Hein S Venter and Mariëtte E Botes

University of Pretoria, Pretoria, South Africa
martin@mo.co.za, eloff@cs.up.ac.za, hventer@cs.up.ac.za, mariette@mo.co.za

ABSTRACT

Donor funds are available for treatment of many diseases such as HIV. However, privacy constraints make it hard for donor organisations to verify that they have not sponsored the same patient twice — or sponsored a patient whose treatment was also sponsored by another donor.
This paper presents a protocol based on digital cash that enables donor organisations to obtain a proof (in the form of an e-coin) from healthcare providers for patients such a provider claims to have treated. These coins are distributed to patients at the beginning of a funding cycle.
The major challenge is to issue a unique coin to a patient — even if the coin is reissued. This is achieved without giving anyone access to a national database of identities; all databases contain effectively concealed information. Reissued coins will be identical to previous coins with a probability that can be decided beforehand.

CATEGORIES AND SUBJECT DESCRIPTORS:

KEYWORDS: Medical application security, privacy, digital cash

1 INTRODUCTION

For global pandemics, such as HIV, donor funds are often made available by various bodies. In the case of HIV funds have been made available by the World Health Organisation (WHO), the US president (PEPFAR, President's Emergency Plan for AIDS Relief), various national governments, private foundations and other bodies.

Usually healthcare providers who treat patients have to justify their share of such donor funds by reporting on the number of patients that they have treated with funds allocated to them.

Such reporting is not simple: HIV is the paradigm case for privacy, and providing donors with the identities of patients treated is not acceptable. In fact, if one uses identity as the basis of such reporting it will be necessary to provide each donor with identities of patients treated with funds from other donors as well; this would enable them to verify that a healthcare provider has not claimed for treatment of the same patient from multiple donors. This implies that the HIV status of patients have to be disclosed to donors with whom they have no relation at all.

In earlier work [1] we proposed an architecture that used a trusted third party to address the latter problem. However, the trusted third party now had access to a database of identities and the HIV status of each. It is well known that such large databases with sensitive information form a prime target for attack. In this case the database may have value for unscrupulous employers, life insurers, and other parties who may gain from misusing the information.

This paper considers an alternative strategy to enable healthcare providers to claim

donor funds that obviates the need for a large national database and does not disclose the identities of patients to donors. Yet, it ensures that donors will only pay for patients actually treated. Seen more abstractly, the paper proposes a protocol that will partition a set of people in a way that neither the elements of the original set, nor the elements of any given partition can be determined. However, the sizes of each of the partitions can be determined.

The strategy proposed in this paper is based on the use of electronic cash (or digital cash). We will refer to the tokens to be used as electronic coins (e-coins). At the point where a doctor determines that a patient qualifies for treatment under a sponsored program, an e-coin will be issued to the patient. This e-coin will then be presented to the healthcare provider (typically a hospital or clinic) in exchange for treatment. New coins may be required (and issued) on a periodic basis (eg annually) to ensure that the coins of patients who are no longer treated cannot be used ad infinitum. The healthcare providers then tender the coins to donors for payment (or justification of earlier payment).

The coins used in this application are similar to coins used for e-commerce in some respects. One obvious requirement is that coins cannot be spent twice — one healthcare provider should, for example, not be able to claim for the same patient's treatment twice. Neither should two healthcare providers be able to claim for the same patient.

Note that HIV is treated as a chronic disease, and the number of doctor visits cannot necessarily be predetermined for a given period. The intention of a coin is not to pay per visit, but to cover treatment for the entire sponsored period (including the relevant drugs).

In other respects the coins envisaged in this application are quite different from coins used elsewhere. In the case of e-commerce a customer may request as many coins as he or she wishes; the value of each coin is simply deducted from his or her bank account when requested. In the current application one cannot have an "account" for each patient, since such an account will imply that the identities of patients who qualify for treatment are stored in some database — contrary to the premises of this paper.

Besides our earlier work on this topic [1] we are not aware of any other research that has addressed this problem.

The remainder of the paper is structured as follows. Section 2 considers the threat and trust issues that we assume for the purposes of this paper. Section 3 then reviews the well known operation of e-coins and considers the modifications that need to be made to effectively use the coins in the new environment. The significant change that has to be made to a standard e-coin protocol is the requirement that subsequent coins should be identical to coins issued earlier because funds can only be claimed once from a donor for any given patient. Section 4 considers the suitability of the proposed protocol given the threats that were identified earlier. Section 5 revisits the need to identify patients anonymously. It is found that a suitable identification scheme depends on the solution of a statistical optimisation problem. Section 6 concludes the paper.

2 THREATS AND TRUST

E-coins in this application are worth (donor) money. Hence it has to be ensured that such coins cannot be falsified, cloned successfully or spent twice.

Since privacy is at stake, it should not be possible to infer the identity of the patient from the coin. It will be argued below that it should also not be possible to identify the identity of the certifying doctor from the coin.

In a typical e-coin application three parties are involved: The customer requests the coin from the bank and sends it to the merchant. The merchant then exchanges it for cash at the bank again.

In the medical environment five parties will be involved. The doctor (D) will request the coin from the bank and hand it to the patient (P). The patient will then exchange it at the healthcare provider (H) for treatment. The healthcare provider will then send it to the donor organisation (O) who will fund (or has funded) the patient's treatment. The donor

will present the coin to the bank to indicate that it has been spent. We assume multiple instances of D, P, H and O, but only one bank B.[1]

Of prime importance is the privacy requirement. It is assumed that the doctor knows the patient's identity and medical information. (It will be simple to modify the presented scheme for anonymous diagnosis and treatment, but we do not consider it in this paper — primarily due to medical complications that may result from such an approach.) It is assumed that the healthcare provider cannot infer the patient's details from the coin. Typically the financial staff at the healthcare provider deal with claims supported by coins, and they do not need access to clinical information. (In practice it may be assumed that many healthcare providers will know the identities of their patients, but this does not make a significant difference to the proposed scheme.) It is an absolute requirement that neither the bank nor the donor organisation should be able to determine the identity of the patient.

The primary monetary concern in the process is the dishonest healthcare provider who wants to obtain more coins than patients treated to exchange for donor funds — because the healthcare provider is the only party who can directly gain financially from "real" money in this process. (The doctor, patient and bank are not in a position to claim donor funds according to the current assumptions.) This implies that the healthcare provider should not be in a position to generate coins. Once this has been met, four financial threat scenarios remain:

1. Where the healthcare provider colludes with the doctor;
2. Where the healthcare provider colludes with the bank;
3. Where the healthcare provider colludes with a patient; and
4. Where stolen coins are used by the healthcare provider.

[1]In principle the donor may act as bank, but this would require the doctor to choose the donor for every patient; a single 'central' bank enables the doctor to obtain coins that may then be used to treat the patient using whatever donor funds are available.

The first option (collusion with the doctor) will not be treated as a significant threat in the current paper. This assumption is based on the professional status of the doctor. To address the issue of dishonest doctors, it is assumed that it should be possible to audit the doctor's actions to ensure that no false coins were authorised by the doctor. This is in line with society's trust in doctors to prescribe medicine that may be sold on the black market at high prices; if this trust is violated it has dire consequences for the doctor, and cases of such violations are relatively scarce.

The second option (collusion with the bank) also will be dealt with by trust. Note that the bank will not be entrusted with private information. Therefore the bank simply has to be trusted not to issue coins other than on a doctor's request. If suspicion exists that a bank has issued false coins, the bank has to show that the number of coins it has issued corresponds with the number of (signed) requests it has received from doctors. The number of coins may be determined by pooling the used coins from all service providers.[2] A bank may also cheat by informing a donor that a coin has not yet been spent, after it has, in fact, been spent, causing the donor to pay a second time for a patient that has already been sponsored. This will, however, be easy to detect as will be described below. The degree of trust placed in a bank therefore compares to the degree of trust currently placed in a chartered accounting (or certified professional accounting) firm. The bank is not entrusted with medical information.

The third option (colluding with a patient) will only occur if a patient is able to obtain more than one different coin. The challenge is therefore to ensure that the same coin will always be issued to the same patient, irrespective of which doctor requests it. (This will also deal with the issue of lost coins.)

The final problem to be considered is that of stolen coins. Only two financial incentives exist for stealing coins and using them. The first is again in collusion with a healthcare

[2]In general the bank should have more signed doctor requests than this because some coins may not have been used after all.

provider who is able to turn them into real money. The second is to get access to treatment for a patient who does not qualify for his or her own coin (such as an illegal immigrant who may not be accommodated in a country's medical system). The former is only a real threat if enough coins are stolen. Since a stolen coin can be identified when it is presented by a healthcare organisation, it is possible to identify healthcare organisations who present many stolen coins. Hence this is not considered as a real threat. Secondly, if eligibility for treatment is checked at the point of treatment, stolen coins are not worth much to 'illegal' patients, and this threat will not be considered in detail.

3 ISSUING COINS

Normally digital cash is used to spend money anonymously — an idea originally introduced by Chaum [2, 3] more than two decades ago. This section will briefly explain the original notion as introduced by Chaum. Then it will be adapted for the purposes of this paper to be pseudonomonous, rather than anonymous. The intention is to have a coin linked to a person's pseudonym in a way that the pseudonym cannot be translated to the person's real identity. However, under very special circumstances the person's real identity can be translated to the pseudonym.

In this section we will denote encrypting a message m with the public key of some party X as $e_X(m)$. Decrypting the message m' with the private key of X will be denoted as $d_X(m')$. Encrypting m with X's private key is equivalent to decrypting; hence this will also be indicated as $d_X(m)$.

In the (simple) usual case an e-coin is issued as follows [2, 3]: The customer (C) chooses a random number r. (r will typically be constrained in some way to have a recognisable form.) C now chooses a commuting function g and its inverse g^{-1}, such that $g^{-1}(d_X(g(x))) = g^{-1}(g(d_X(x))) = d_X(x)$ for any party X and any value x. A lack of space precludes a detailed discussion of commuting functions here; suffice it to note that such a function typically uses a random number known only to C and hence g is only known to C. (For examples see the paper by Chaum [3] again.)

The customer then forms a message that includes $g(r)$ and requests the bank to deduct money from C's account and to sign the included number. The bank encrypts the value with its private key, which yields $d_B(g(r))$. This value is returned to C. C now calculates $g^{-1}(d_B(g(r)))$. This is equal to $g^{-1}(g(e_C(r)))$, which is equal to $d_B(r)$. C now knows $\langle r, d_B(r)\rangle$, which is a signed version of r. C can now send $\langle r, d_B(r)\rangle$ to the merchant, who can easily verify that it has indeed been signed by B. When the merchant presents this value to B, the bank verifies that r has not yet been presented for payment and then credits the merchant.

The values sent between the various parties are also encrypted to ensure confidentiality. For the sake of simplicity this has not been shown above. Similarly messages in some cases need to be signed to ensure non-repudiation. This has also not been shown explicitly above.

For more details see the book by Wayner [4] or the paper by Panurach [5].

Whereas the protocol described above works where a bank customer is entitled to withdraw as many coins as he or she can afford, it has been argued earlier that each coin 'withdrawn' for a patient in the medical system has to be similar to all others 'withdrawn' for that patient. An initial version of the protocol will therefore not get a random value, r, signed, but some identifying value i. This i may, for example, be the national identity number or social security number of the patient. However, in the protocol above, r was exposed to the merchant and bank later in the transaction; as already argued, the identity of the patient should not be exposed to the donor, bank, or (perhaps even) the healthcare provider in the medical system.

A simple variation of this protocol uses $h(i)$ in the place of r where h is a suitable one-way hashing function. This, however, leads to the following problem (amongst others): If someone knows all the values $h(i)$ that exist, and wants to know whether some individual i' is in that list, it is simple to compute $h(i')$ and determine whether this individual is on this list.

This is so because, given the number of parties who has to know $h()$, it is not realistic to assume that h is secret. Note that, for h to be suitable for the intended it has to yield hashes that are 'recognisable' as a being in a special format. To do this, the simplest solution (following Chaum's [3] example) is to let h repeat a hash. That is, if h' is a function that has typical good hashing properties, let $h(i) = h'(i)||h'(i)$ where the vertical bars indicate concatenation. Without this property it may be too easy to find just any random number that happens to look like a signed random number [2].

We therefore need some value i to use here that is unique and constant for a given individual, but that is hard to obtain without a significant amount of information about the individual. By *unique* we mean that the value is guaranteed to be different for different individuals; by *constant* it is meant that the information should not change from one moment to the next; by *hard to obtain* it is meant that the information should indeed be easy to obtain from a cooperating patient, but that it should not be generally known about the patient, and should not be easy to determine without the cooperation of the patient.

One viable option is to use a compound value consisting of several subparts. The first subpart may indeed be the national identity number or social security number. On its own this will already ensure the uniqueness of the compound number.

To illustrate the qualities of other values that might be appended to this value, consider blood type. Individuals' blood is grouped into A, B, AB or O groups and further classified based on whether the Rhesus factor is present (+) or not (-). This provides eight possible values, resulting in three bits that may be added to the compound value. Some of the good points of using such a value is the fact that it is easily obtainable by a doctor, while it is not generally known to others. This value also remains constant over time. Drawbacks include the following. With only eight combinations it is easy for a nosy party to try a brute force attack where other parts of the identifying number is known. Moreover, the well-known frequency distribution of ABO blood groups (in most environments O predominate), and the fact that the vast majority of people are Rhesus positive, limit the search space.

A further complication is brought about by the fact that blood types are not absolutely constant. A person with A blood may receive O blood during a transfusion and a test shortly after that will determine that his or her blood is of type O. At worst this means that such an individual may be able to obtain two coins. However, the incidence of cases where a single blood type is not dominant is so low that this has little potential for fraud — remember that, as discussed above, such an individual needs to collude with a healthcare provider to derive economic benefit. The need is therefore not absolute uniqueness, but uniqueness with a high degree of probability.

The primary problem of using blood type is the size of the search space and the fact that its frequency distribution is skewed. We propose that a combination of biometric values be used to address this. The biometric data is collected from the patient at the point of where the coin is to be issued. For each biometric the feature vector is extracted. The identity number with the various feature vectors added forms the identifying string. Suitable biometrics need to be considered. Note that not only technical restrictions apply. Fingerprints may, for example, be an inappropriate biometric to use given the fact that the disease considered is already stigmatised.

Since the various components of i are merely used to identify the individual and are of no concern to the various parties who play a role in the protocol, it is hashed and $h(i)$ is used as the identifying value. Therefore no party (with the possible exception of the doctor) will be able to derive these values.

We are now ready to consider the full protocol, which consists of a simple application of the digital coin protocol described earlier. It is assumed that whenever a party X sends any message m to a party Y, X will encrypt the message with Y's public key. Formally this may be denoted as

$$X \overset{e_Y(m)}{\longrightarrow} Y$$

However, in this paper we will assume that

such encryption is implied and we will only write

$$X \xrightarrow{m} Y$$

We will also write $s_X(m)$ to denote a message m that is signed by X; therefore

$$s_X(m) = \langle m, d_X(m) \rangle$$

In what follows we will not indicate signed messages, except where the signing is an essential part of the protocol. Signing most messages will be useful for non-repudiation purposes during auditing. However, indicating below that each message is also signed will add unnecessary complexity to what follows.

The protocol proceeds as follows:

1. The doctor, D, determines i for the patient, P.
2. D calculates $h(i)$
3. D sends this value to the bank for signing; D signs the value to guarantee its authenticity:
$$D \xrightarrow{s_D(g(h(i)))} B$$
4. B signs the value $s_D(g(h(i)))$ and returns it:
$$B \xrightarrow{d_B(g(h(i)))} D$$
5. D calculates
$$g^{-1}(d_B(g(h(i)))) = g^{-1}(g(d_B(h(i)))) = d_B(h(i))$$
Let the coin, c, now be
$$c = \langle h(i), d_B(h(i)) \rangle = s_B(h(i))$$
6. D hands this signed coin to P:
$$D \xrightarrow{\text{c}} P$$
7. P exchanges this coin for treatment at a healthcare provider, H:
$$P \xrightarrow{c} H$$
8. H presents the coin to a donor organisation, O, for funding:
$$H \xrightarrow{c} O$$
9. O verifies with B that the coin has not yet been spent:
$$O \xrightarrow{c} B$$
10. B now marks the coin as spent and sends a confirmation to
$$B \xrightarrow{s_B(c, \text{confirm})} O$$
If the coin was not available it communicates this with O:
$$B \xrightarrow{s_B(c, \text{deny})} O$$
11. If availability of the coin is confirmed, O accepts responsibility for treating the patient:
$$O \xrightarrow{s_O(c, \text{confirm})} H$$
Else
$$O \xrightarrow{s_B(c, \text{deny})} H$$
12. If approved, H commences treatment of P.

As already noted the latter part of this protocol is a straightforward extension of a standard payment protocol and it will not be discussed in detail here. Relevant portions will be analysed in the next section.

The protocol above has been presented such that donor funds are requested per patient to be treated. In the real world, donor funds are often allocated and verification of patients only occur during a later reporting (or auditing) phase. The protocol is simple to modify to submit coins to the donor on a periodic basis irrespective of when treatment commenced. It might mean that some coins will be found be invalid if submitted after the treatment has already commenced. If this occurs infrequently enough it will still be sufficient for auditing purposes. It is expected that such cases will be spread proportionally over different healthcare providers, and hence will not affect the overall distribution of funds.

In many cases the healthcare providers do not communicate directly with the donor organisations, but via some national administrative fund administrators. Again the protocol is simple to adapt to include such a sixth party in the final part of the protocol.

4 ANALYSIS

The primary concern raised in Section 2 was that of privacy. None of the parties besides D

should be able to infer the identity of P. Since $h(i)$ forms an inherent part of c, all parties are able to determine $h(i)$. However, due to the one-way nature of $h()$ nobody can compute i from $h(i)$. Due to the complex composition of i, it is also unfeasible for an attacker to compute $h(i)$ from some i and match it against the known values of $h(i)$ to determine whether i is being treated (and from that infer the diagnosis of i).

The secondary concern was monetary. Since only H can access funds, either H has to forge the coin or collude with someone who can — as argued in Section 2. H cannot sign coins and therefore cannot forge them.

Suppose H colludes with D. It has already been argued that professional trust is placed in D — we now have to show that a forensic audit will indeed be able to expose D. If suspicion arises about D, all the requests signed by D may be recovered from B. D now has to be able to show the patient file and demonstrate how the request for each patient was derived. Patient files are detailed documents consisting of doctor notes, medical test results and, possibly, nursing notes (if the patient was treated in hospital). Moreover, specimen test results are linked to physical specimen results; blood tested for HIV is typically stored for years by the testing laboratory. Finally, participating in fraud will have severe consequences for D — such as being barred from further medical practice. Hence collusion between H and D is addressed in the manner professional trust is usually dealt with in society, rather than by a mathematical construct. It is based on trust that, when breached, is relatively simple to uncover with a forensic audit.

Whereas a normal bank will not issue fake coins (because it has to convert such coins to cash later), the bank B in this protocol may be enticed to issue such coins. We have to show — as argued in Section 2 — that (normal) auditing will expose B, if B engages in fraudulent activities. We assume that the number of coins cashed by donor organisations will be a matter of public record (since donor organisations typically report what has been accomplished with the funds donated by it). Hence it is easy to correlate the number of coins cashed with the number of signed requests received from doctors. Even if coins cashed are not a matter of public record, the bank can keep record of who cashed which coins. Its record of cashed coins then has to match the number of requests it had received from doctors. And it is easy to compare its record of cashed coins with any (random) donor's record of cashed coins. It is therefore possible to subject this to annual audit (and only to forensic audit if something is found to be amiss).

Collusion between H and P has already been dismissed in Section 2, unless enough patients are able to obtain multiple coins. This issue will be considered in the next section. Note that there will typically be a practical limit on the number of doctors a given patient can approach for coins, because policies typically limit patients to visit government facilities in their own region (or private doctors where they will have to pay for the visit and for the test).

5 ON THE CONSTRUCTION OF I

In Section 3 above, three necessary properties of the identity string i were identified, namely that it should be unique, constant and hard to obtain. Let i consist of m components k_j. In other words

$$i = k_1 \;||\; k_2 \;||\; k_3 \;||\; \ldots \;||\; k_m$$

The uniqueness of i was ensured by choosing k_1 as the national identity number of the person. This section considers the other two properties in more detail.

In order to be hard to obtain, multiple components, k_j (with $j \geq 2$) should be used to construct i. Ideally these components should be independent so that the value of one cannot be derived (or, ideally, not even estimated) from another. Preferably they should be chosen from a variety of domains, such as medicine, physical traits, behavioural traits and other characteristics. If only, say, medical characteristics are used, someone with access to medical data — such as a medical orderly — may be able to construct i from its components.

Secondly, enough viable values should exist for the components (in combination) that someone in a given domain is unlikely to know

many of them. Suppose any given person knows (or is able to guess) some components so that only a few components remain unknown, and those components cannot assume many values. Then, as has already been noted earlier, it is easy for this person to use a brute force attack to try to find a match in the database of $h(i)$ values. Hence i should have a large domain and, ideally, each k_j should have a large domain.

We will refer to the size of a component's domain as the component's *resolution*. A component with a high resolution is one that can assume many discrete values.

The requirement that i should be constant stems from the fact that variance in i allows a patient to obtain more than one coin. If this happens often enough, a market in excess coins may develop where such coins are supplied to a healthcare provider to exchange for donor funds. In order for i to be constant, each of the components needs to be constant. We will refer to this property as the component's *stability*.

As noted, k_1 is chosen as the patient's national identity number, which is assumed to remain constant. Similar numbers may be used as other components. Examples include the patient's driver licence number, cheque account number, passport number, etc. These examples, however, suffer from a few problems. Not all patients may have all these numbers. In some cases, numbers may be dependent; the driver licence may, for example, use the patient's national identity number as its number. And some numbers, such as a cheque account number, are easy to change and a given person is hardly ever restricted to only one such number. In other words, other numbers may be useful, but should only be used after careful consideration.

The other example used when i was introduced was that of blood type. This example is an ideal one: Repeated tests yield the same (discrete) value. Blood types hardly ever change — and the few cases where it does, are statistically insignificant because there simply are not enough cases to form a source of surplus coins.

Two concerns regarding this example should be raised. The first was already raised in Section 3. Using the terminology introduced in the current section, this component has a low resolution. However, that is easily dealt with using enough other components. The second concern is the fact that this type of biometric is considered invasive. Given the application context we argue that, although invasive, it is appropriate to use in a medical environment where such tests are standard.

Unfortunately not many examples exist that work as well as blood types. Many characteristics are measured on a continuous scale and the probability that one measurement will be identical to the next is extremely small. Consider a person's length. Assume, for the moment, that a person's length remains constant during the validity period of the coins and that the person therefore has a precise length. However, if the person's length is measured in millimetres (or some even smaller unit) small differences are likely to occur if the length is measured a second time. If larger units are used (or some larger interval is used), measurements are bound to categorise a person into the correct category more often. If, for example, we only determine a person's length to the nearest ten centimeters, relatively few categorisation errors will occur. Those people who are on the boundary of a category may still often be classified in the wrong category. However, if the categories are large enough, few cases will occur near the boundaries. Clearly, for such cases a tradeoff exists between resolution and stability.

As has already been argued, a small number of (potentially) double coins issued to the same individual is not a significant issue. Most patients will only request a single coin. Most of those who get a double coin will not realise it. It only becomes a significant issue once patients have a reasonable chance of obtaining a second coin that collusion between a sufficient number of patients and a healthcare provider becomes a significant threat.

In order to formalise this, assume that a potential fraction d of all patients may possibly receive a second (ie a different coin). This implies that at least $p = 1 - d$ patient's data identities should be determined correctly in the cat-

egories where they should be placed. For each k_j there is an expected proportion p_j of measurements that will be correctly classified. For k_1 (the national identity number) $p_1 = 1$. Similarly for blood type the corresponding value will be 1. For other measurements, p_j depends on the tradeoff made between resolution and stability. This will be explored formally below.

If the various components k_j are statistically independent (the ideal case, as has already been explained) then

$$p = p_1 \cdot p_2 \cdot p_3 \cdot \cdots \cdot p_m$$

If independence does not hold, the relationship is significantly more complex and is not considered in the current paper.

From this discussion it is clear that the problem will in practice be one of optimisation. The following constraints will typically apply:

- The number, m, of components that can realistically be incorporated;
- The empirically observed standard deviation, σ_{k_j}, for measurements of component k_j; note that we will simply write σ below when k_j is implied;
- The minimum resolution of i (which will be the product of the resolutions of its components k_j), and
- Possibly minimum resolutions of combinations of some components that exclude information that come from the same field (such as medicine).

The challenge then is to determine the sizes of categories to be used for each of the components such that the potential fraction d of all patients who may possibly receive a second coin is minimised (or at least ensured to be below some acceptable threshold).

This optimisation problem is not considered in the current paper. However, to conclude, we do explore the relationship between the value of e_{k_j} and the size of categories to be used for component k_j. Since k_j is implied in what follows, it is not explicitly written.

5.1 Balancing stability with resolution

Assume measurements of the physical trait under consideration are distributed according to some function ϕ with standard deviation σ. Consider any category that ranges from l (lower bound) to u (upper bound). Further assume that a trait is to be measured that has a true value v, with $l \leq v < u$. Then the actual measurements will be distributed around v. We will indicate the specific probability distribution function for measurements of v as ϕ_v. This is depicted in figure 1 (where, for purposes of illustration, it has been assumed that measurements are distributed normally around the actual value).

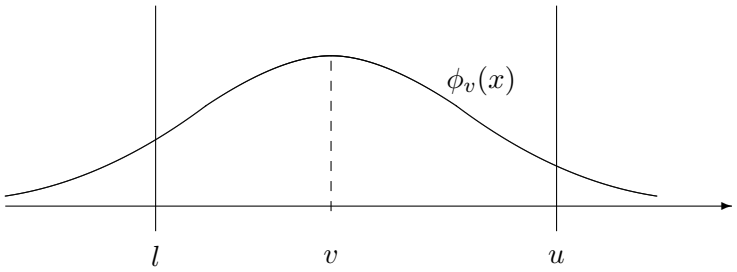

Figure 1: The distribution of expected measurements given an actual value v.

For such an actual value v the probability of placing the measurement in the correct category is given by

$$c_{l,u}(v) = \int_l^u \phi_v(x)\,\mathrm{d}x$$

Now suppose that the interval $[l, u)$ is subdivided into a number of discrete measurement units. Assume that there are n such discrete units in this interval. Further assume that the occurrence of these discrete values are distributed evenly over the interval. Then the expected *proportion* of values that will be correctly placed in this category is given by

$$p_{n,l,u} = \frac{1}{n}\sum_{i=0}^{n-1} c_{l,u}(l + i \cdot \delta)$$

with $\delta = (u - l)/n$ the distance between the subunits.

Where no discrete intervals exist — ie where measurements are taken on a continuous scale — this expected value is equal to

$$p_{l,u} = \lim_{n\to\infty} p_{n,l,u} = \int_l^u c_{l,u}(v)\,\mathrm{d}v$$

Assume now that the observed measurements of some true value v are indeed distributed normally with mean $\mu = v$ and standard deviation σ. Then, from the well-known normal distribution function, it follows that

$$\phi_v(x) = \frac{1}{\sigma\sqrt{2\pi}}\, e^{-\frac{1}{2}\left(\frac{x-v}{\sigma}\right)}$$

Therefore

$$\begin{aligned} p_{l,u} &= \int_l^u c_{l,u}(v)\,\mathrm{d}v \\ &= \int_l^u \int_l^u \phi_v(x)\,\mathrm{d}x\,\mathrm{d}v \\ &= \int_l^u \int_l^u \frac{1}{\sigma\sqrt{2\pi}}\, e^{-\frac{1}{2}\left(\frac{x-v}{\sigma}\right)}\,\mathrm{d}x\,\mathrm{d}v \end{aligned}$$

Note that the integrand does not depend on the values of x and v, but on the difference between them. Hence, if the integration areas over x and v are both moved by $-l$ and we let $\Delta = u - l$, then

$$p = \int_0^\Delta \int_0^\Delta \frac{1}{\sigma\sqrt{2\pi}}\, e^{-\frac{1}{2}\left(\frac{x-v}{\sigma}\right)}\,\mathrm{d}x\,\mathrm{d}v$$

This is the relationship between p and the size of the categories Δ that will serve as input to the optimisation problem identified earlier in the paper.

In order to derive this relationship a number of assumptions had to be made. We contend that those assumptions are reasonable, without considering each of them in detail here.

6 CONCLUSION

This paper considered a protocol based on digital cash to ensure equitable distribution of donor funds to healthcare providers for patient treatment. The problem was solved by using a fairly straightforward application of e-coins. However, to solve this problem, it was necessary to anonymously identify a patient in a manner that is unique, constant and hard to obtain.

The solution ensures uniqueness by incorporating a known unique value; it ensures that the identifier is (statistically) constant and ensures that it is hard to obtain by composing it of enough values from various domains.

The final solution is shown to be dependent on an optimisation problem — the details of which are left for future research.

Further work needs to be done to identify suitable biometrics to use in the construction of i. It is necessary to determine the value of σ for these biometrics empirically. It is then necessary to confirm that i can achieve a sufficient resolution by using (only) a reasonable number of components.

The solution presented here shows some similarities with the notion of multibiometrics [6]; the actual problem is indeed significantly different. However, one issue highlighted [6] as a problem for multibiometric systems is the fact that underlying measurements are not necessarily exposed to an application by current biometric hardware. This needs to be investigated in the context of the current paper as well.

Practical issues regarding communicating the protocol messages between the patient and other parties also needs further attention. It seems that smartcards might be useful.

Another potential avenue for future research is to consider the impact that trust models may have on the work presented in this paper. This might help to reduce the degree of trust currently vested in the doctor.

It also seems worth to investigate the use of related cryptographic protocols for this application, such as electronic voting and anonymous credentials. In fact, some models in the latter category already make use of biometrics [7]. However, it seems that application of such protocols here will also not be straightforward, given the requirement to partition an anonymous set of individuals.

REFERENCES

[1] H. S. Venter, M. S. Olivier, J. H. P. Eloff and M. E. Botes. "Balancing Patient Privacy and Treatment Facility Accountability using a Centralised Pseudonymous HIV/AIDS Database". In S. M. Furnell, P. S. Dowland and G. Kormentzas (editors), *Proceedings of the Fifth International Network Conference (INC2005)*, pp. 377–384. Samos, Greece, July 2005.

[2] D. Chaum. "Blind signatures for untraceable payments". In *Advances in Cryptology — Crypto '82*, pp. 199–203. Springer-Verlag, 1983.

[3] D. Chaum. "Security without identification: transaction systems to make big brother obsolete". *Commun. ACM*, vol. 28, no. 10, pp. 1030–1044, 1985. ISSN 0001-0782. doi:http://doi.acm.org/10.1145/4372.4373.

[4] P. Wayner. *Digital Cash: Commerce on the Net*. Morgan Kaufmann, 2nd edn., 1997.

[5] P. Panurach. "Money in electronic commerce: digital cash, electronic fund transfer, and Ecash". *Commun. ACM*, vol. 39, no. 6, pp. 45–50, 1996. ISSN 0001-0782. doi: http://doi.acm.org/10.1145/228503.228512.

[6] A. K. Jain and A. Ross. "Multibiometric systems". *Commun. ACM*, vol. 47, no. 1, pp. 34–40, 2004. ISSN 0001-0782. doi: http://doi.acm.org/10.1145/962081.962102.

[7] R. Impagliazzo and S. Miner More. "Anonymous credentials with biometrically-enforced non-transferability". In *WPES '03: Proceedings of the 2003 ACM workshop on Privacy in the electronic society*, pp. 60–71. ACM Press, New York, NY, USA, 2003. ISBN 1-58113-776-1. doi: http://doi.acm.org/10.1145/1005140.1005150.