Digital chips for an on-line casino*

J. Castellà-Roca
ETSE-URV, 43007 Tarragona (Catalonia), Spain
Email: jcaste@etse.urv.es

G. Navarro, J.A. Ortega-Ruiz, J. García
UAB, 08193 Bellaterra (Catalonia), Spain
Email: {gnavarro,jao,jgarcia}@ccd.uab.es

Abstract

Unlike in traditional environments, e-gambling players must make a beforehand payment to start a game. Most on-line casinos currently solve this problem using prepayment systems where the on-line casino has absolute control over all the transactions among the players. However, this solution poses a great number of problems because of the necessary trust relation between players and the on-line casino managers. To reduce this strong trust relationship with the on-line casino, we propose in this paper the use of a reliable digital chips system, which provides auditing facilities, and can be trusted by external parties. Digital chips, just like physical ones, will be used for players instead of legal course money. A set of cryptographic protocols will protect the different actions that players can perform using these digital chips.

1 Introduction

Real-world casino players do not use money of legal course. Instead, players change their money for tokens, known as *chips*, issued by the casino. Usually, chips are valid only in the casino where they are issued and are exchanged back to money by players leaving it.

The situation is different in an on-line casino. A player enrolling a game must make a pre-payment, not just an exchange of real money for chips. Only when the money is in the casino's bank account will the game start. In a way, the player must open an account on the casino's behalf to participate in the game.

This scenario offers ample opportunities for dishonest behavior, both on the casino's and the player's side. Let us describe some common sources of trouble in such a situation.

The player can use credit car to make the required prepayment on the casino's behalf, allowing players to quickly enter the game. But we should remember that credit card companies must offer the possibility of payment revocation. Dishonest players can just revoke their initial payment after loosing the game. As a result, credit card companies are very reticent to work with online casinos. For instance, American Express does not support any online money exchange with a casino, while other companies, such as Visa or MasterCard, charge high commissions to such transactions. Thus, casinos tend to avoid credit card usage, due to security and economy concerns, and honest players are deprived of a comfortable and quick access to online games. It is a lose-lose situation for both parties.

On the other hand, the prepayment system places casino managers on a privileged position. Not only have they the money beforehand, but control virtually all the mechanics and events (the player's cards, the roulette's results, and so on) of games of which they are an active part. And when the game is over, the casino still has absolute control over the player's money. There is little the player can do, except blindly trust in the casino's honesty.

Summing up, the simplistic prepayment systems currently used in on-line casinos impose an overly strong trust relationship between the involved parties, with no means of external control or verification.

In order to fix this undesirable state of affairs, we propose a reliable digital chips system, which provides auditing facilities, being thus verifiable by third parties. Players need no longer to trust in the casino's honesty. In addition, the digital chips are issued and managed by a credit card company and that the refund problem is avoided. Of course, our system should be used jointly with a cryptographic protocol that guarantees that game events are obtained fairly. Two efficient cryptographic suites for an on-line casino are [8] and [14].

1.1 Related work

Physical chips resemble, and in fact are used instead of, physical money. Thus, one may think that the best approach to implement digital chips is providing some sort of digital money.

*Part of this work has been founded by the Spanish Government, through its grant TIC2003-02041, and the project SEG-2004-04352-C04-01, and the Catalan Government with the grant 2003FI-126.

Digital money has received wide attention in the literature. Relevant research [1, 2, 3, 4, 5, 7, 10]. We refer the reader to [13] for a good survey on the field.

Despite the large number of proposals, the ability to transfer ownership of digital money is seldom supported, the most remarkable system offering this property being Okamoto's [12]. This digital cash system also provides user privacy, off-line payment and divisibility. While our proposal offers transferability, we shall not need the latter three properties (cf. Section 2.1). The main drawbacks of Okamoto's proposal are its complexity and the great computational cost of payments (every payment needs at least $3K/2$ exponentiations, where K is a security parameter with a typical value of 50).

An alternative to digital money systems are micropayment systems, which are, in principle, a more efficient solution. The most interesting micropayment systems allow some form of transferability [6, 11]. Here, transferability refers to the fact digital coins owned by an user can be transferred to another one, provided they have not been used. One of the main drawbacks of those systems is that used coins cannot be transferred anymore, or used in any other way for that matter. Even more important is the fact that, because they use hash chains to encode coins, to transfer a coin means to transfer a subchain. This normally involves revealing the seed of the hash chain to the receiving entity. In [11], one user can in principle transfer an unused subchain to another one, but they do not specify how to actually make this transfer, while in [6] the authors use the delegation capabilities of trust management systems (such as KeyNote or SPKI/SDSI) to delegate a subchain to another user. Summing up, these approaches are based on hash chain micropayments and the transferability of chips is severely limited. On-line e-gambling needs a digital system supporting an unlimited number of chip transfers among players (think for instance of an on-line poker game).

Finally, an interesting scheme is [16], where an optimistic third trusted party (TTP) is used to resolve guarantee payments. The TTP knows the credit card number of each player, and reveals it in case the player is dishonest to ensure that the payment is actually made. Our solution, based in [2], will also use an optimistic TTP to resolve any dispute arising during the game.

1.2 Paper organization

The rest of this paper is organized as follows. Section 2 describes the main properties and elements of our proposal, as well as the actions that players can perform on digital chips. Then, Section 3 presents a set of subprotocols, one for each of the above mentioned actions. An analysis on the security of the system is presented in Section 4. The paper closes with a list of conclusions in Section 5.

2 Overall system structure

2.1 Properties of digital chip systems

Any digital chip system for on-line casinos must provide, at least, the following guarantees:

Independence : the security of digital chips must not depend on any physical device. The use of devices such as smart cards or similar tamper proof devices should be avoided.

Resilience against forgery : only the on-line casino should be able to issue digital-chips.

Resilience against reuse : if one player transfers a digital chip, she must not be capable of reusing it for other transactions.

Resilience against robbery : digital chips must be usable only by their legitimate users. If robbery is avoided, a player can, for instance, show her digital chips as a proof that she has money enough to equal one bet.

Transferability : the digital chips must be transferable to other players. If one player loses a bet, she must pay (transfer) her digital chips to the winner.

Payment : players should always get the money they win.

Efficiency : the game is played on-line and chips transfers between players and the casino need to be performed in real time.

All of the above properties are covered in the digital chips system presented in the following sections, which thus provides a complete solution to the on-line gambling problems. Specially, the transferability issue (open in many other proposals) is fully solved. As pointed out in Section 1.1, strong privacy, dividability and off-line payments are provided by other systems. In our case, off-line payment is not an issue, since we focus on on-line chip usage. As for privacy, we need a system where it is revokable, because, if both transferability and privacy are granted, money laundering and tax evasion are hard to detect [9]. Finally, in a traditional casino, chips are never divided. Thus, in our proposal digital chips are indivisible.

2.2 Actors and actions

In our scenario, we shall be faced with interactions between five kinds of parties or actors, namely:

Bank : the entity, owned by the on-line casino, in charge of issuing digital chips.

Ownership Controller : this entity, introduced by this proposal, is in charge of managing the list of all valid chips (issued by the Bank), and the operations on them. All messages related to actions on digital chips are sent to the Ownership Controller (OC), which verifies and, when they are valid, publishes them on a bulletin board.

Time server : for an accurate accounting we use a time server providing a precise timestamp to each game event.

Dealer : the dealer is the casino's representer in the game table; more concretely, we will use the term *dealer* to refer to the software that acts in name of the on-line casino during the game.

Player : we will use the term player to refer to both a person taking part in the game and the software used to that end.

Before, during and after an on-line game, the above actors interact between them and use digital chips in the following ways:

Withdrawal : a player gives some money to the bank and indicates the value of her chips. The bank issues the chips.

Bet : in a traditional casino when one player makes a bet she places her chip on the table. We will refer to its virtual counterpart simply as a bet.

Transfer : a player transfers one of her chips to other player, as a result of her losing a bet.

Deposit : a player returns her chips to the bank, and the bank pays them.

In next section, we present a subprotocol for every action above, providing in this way a complete protocol for digital chip handling in on-line casinos.

3 Protocols

As we have seen, there are four actions involving digital chips during a typical game in an on-line casino: withdrawal, bet, transfer and deposit. A complete specification for a digital chips management system must provide a protocol for handling each of these actions, and the following subsections describe our proposed solution for them. To carry out these protocols, control and configuration data must be generated and a set of initialization tasks on these data is needed; in other words, we need to initialize our system before on-line gaming begins. Section 3.1 below details these initialitation steps, while the actual protocols are specified in Sections 3.2 to 3.5.

3.1 Initialization

Prior to the game, we shall generate the basic information that every actor must have to participate in our system. With the exception of the Bank, each system actor needs an asymmetric key pair. In addition, the Bank stores, for each possible digital chip value, an associated key pair and additional control data (see below). More concretely, these are the keys and data needed to setup of system:

Bank : The bank chooses how many chip values will be issued, and makes them public. Let us assume that there are t fixed prices for the chips. We shall denote the vector of available chip prices as $V = \{v_1, \ldots, v_t\}$. For each price v_i, the bank generates the following information:

- an asymmetric key pair (P_i, S_i);
- two large prime numbers, p_i and q_i, such that $p_i = 2q_i + 1$.

Ownership controller : the OC owns a key pair, (P_c, S_c)

Time server : the Time server owns a key pair (P_t, S_t).

Dealer : the dealer has a key pair (P_d, S_d).

Player : each player owns a key pair (P_p, S_p).

3.2 Withdrawal protocol

When a player $\mathcal{P}$ needs chips to play in the on-line casino, she will issue a withdrawal request to the Bank. We shall represent such as request using a list C of chip values:

$$C = \{c_1, \ldots, c_n\}, \ \forall c_i \in V$$

where n is the number of chips requested and V is the list of available chip values (cf. Section 3.1). The total amount s paid by the player will thus be $s = \sum_{i=1}^{n} c_i$

To satisfy a withdrawal request, the Bank will issue n digital chips, represented by as $X = \{x_1, \ldots, x_n\}$, according to the Protocol 1 below. This chip generation protocol involves the fulfillment of two subprotocols, one between the Bank and the player (Protocol 2) and a second one between the Bank and the OC (Protocol 3).

Protocol 1

1. *$\mathcal{P}$ performs the following steps:*
   (a) *Define the list of chip values requested, $C = \{c_1, \ldots, c_n\}$.*
   (b) *Send C in a secure way to the bank.*
2. *The Bank, upon receiving C, performs the following actions:*

(a) *Verify that all requested chip values are valid, i.e. that* $\forall c_j \in V$.

(b) *Substract s from P's account.*

(c) *For each* $c_j \in C$*:*

i. *Generate, completing Protocol 2 with* $v = c_j$*, the pair of values* $(I_j, I_j^{w_j})$.

ii. *Digitally sign* $I_j||c_j$ *(where* $||$ *denotes concatenation), using the key pair* (P_i, S_i) *associated with the token value* c_j*. Let us call this signature* γ_j*, i.e.* $\gamma_j = S_j\{I_j||v_j\}$.

iii. *Complete Protocol 3 with OC, using the previously computed values* $(I_j, I_j^{w_j})$*, to obtain the token* β_j.

iv. *Finally, construct the digital chip of value* c_j *according to the equation:* $x_j = (I_j, c_j, \gamma_j, I_j^{w_j}, \beta_j)$

(d) *Send the generated chips* (X) *to both* $\mathcal{P}$ *and OC.*

3. *Upon reception of* X*, the Ownership Controller will publish the new chips in its bulleting board, marking them as valid. At this point,* $\mathcal{P}$ *is ready to use them for on-line games or transfer.*

Thanks to the protocol completed between the player and the Bank, which yields th pair $(I_j, I_j^{w_j})$, $\mathcal{P}$ can use Schnorr's zero-knowledge algorithm [15] to prove that she is the owner of each chip. By virtue of the zero-knowledge property, there is no risk of the chip being stolen by the ownership verifier. The protocol between $\mathcal{P}$ and the Bank is parameterized by the chip's value v, and consists of the following steps:

Protocol 2 *[*$(v \in V)$*]*

1. *The Bank picks a generator* I *of a subgroup* G *of* Z_p^* *of order* q*, using a uniform distribution seeded by a random valued* σ_1*. Here,* p *and* q *are the random numbers associated to* v *during the initialization phase described in Section 3.1.*

2. *The Bank sends* I *to* $\mathcal{P}$

3. $\mathcal{P}$ *generates a random value* w*, such that* $2 < w < q$*, using a uniform distribution seeded by a random number* σ_2.

4. $\mathcal{P}$ *computes* $I^w \bmod p$*; and sends* I^w*;*

5. $\mathcal{P}$ *proves, using Schnorr's algorithm, that she knows* $\log_I I^w$.

The pair of values generated during the above protocol are signed by the Ownership Controller. As we have seen, this signature (β) is included in the digital chip, to assess its validity. This signature is obtained via the following simple exchange between the Bank and OC:

Protocol 3 *[*(I, I^w)*]*

1. *The Bank sends* (I, I^w) *to the OC.*

2. *The OC digitally signs the concatenation* $I||I^w$ *of the received values, using the OC's private key and yielding* β*:* $\beta = S_c\{I||I^w\}$.

3.3 Bet protocol

Once a player has withdrawn a number of chips, she can use them to bet in the on-line casino. Betting will be accomplished via a cryptographic protocol that must guarantee that bets are not changed after the fact and that winners get their money, just as in real-world casinos. To that end, we present two protocols. The first one (Protocol 4) is used to bet, and ensures that players cannot reuse chips lost in game or change in any way their bets after the game is over. On the other hand, Protocol 5 defines the procedure by which winners obtain their legitimate payment.

When a player $\mathcal{P}$ wants to make a bet using a digital chip x, the following protocol between $\mathcal{P}$, the game's Dealer, the Time Server and the Ownership Controller takes place:

Protocol 4

1. *The Dealer composes the message* $m_b = (T_b, N, H)$*, where* T_b *is the time available to bet,* N *is a nonce value, and* H *is an identifier of the hand or throw.*

2. *The Dealer digitally signs* m_b *using her key pair,* $m = S_d\{m_b\}$*, and sends* (m_b, m) *to the Time Server.*

3. *The Time Server stamps* (m_b, m)*, and returns* $T_1 = S_T\{m_b, m, T\}$ *to the Dealer, where* T *denotes the server time.*

4. *The Dealer sends* T_1 *to* $\mathcal{P}$*;*

5. $\mathcal{P}$ *composes a bet* $b = (R, \alpha, x_i, T_1)$*, where* R *is a Schnorr proof and* α *is the message of the bet.* R *can be used to prove that she knows* $\log_I I^w$ *(see Protocol 2), that is, that* $\mathcal{P}$ *is the chip's owner.*

6. $\mathcal{P}$ *sends* $m_p = S_p\{b\}$ *to the Time Server.*

7. *The Time Server stamps* m_p*, and returns* $T_2 = S_T\{m_p, T'\}$ *to* $\mathcal{P}$*, where* T' *is the current server time.*

8. $\mathcal{P}$ *sends* T_2 *to the Dealer, who verifies it.*

9. *The Dealer composes the message* $m_e = (m, m_b, T_2)$*; digitally signs* m_e *using her key pair, obtaining the value* $m' = S_d\{m_e\}$*, and sends* (m_e, m') *to the OC and to* $\mathcal{P}$.

10. *The OC blocks the chip x, so that x cannot neither be used in other bet nor deposited by $\mathcal{P}$, and places the bet in its bulletin board. Anybody can verify that the bet is correct.*

Note how the interaction with the Time Server ensures that bets are issued only during the time slot alloted to that end, while the OC plays a key role in ensuring the provability of the bet.

If $\mathcal{P}$ loses her bet, we must guarantee that the winner $\mathcal{P}'$ is able to proof that x was used in the bet, and that she won the game; i.e., we must prevent any attempt of cheating by $\mathcal{P}$, either by repudiating her bet or refusing to transfer x to the legitimate winner. The protocol used to that end will be fair provided a requisite cryptographic protocol is used to generate the games events whose outcome is at stake. Efficient game event handling schemes can be found in the literature [8, 14].

If $\mathcal{P}$ is honest, $\mathcal{P}'$ will obtain the chips she won using the nominal transfer protocol discussed in Section 3.4, with the mediation of the OC. Otherwise, subprotocol 6 will be used to force $\mathcal{P}$'s payment. Thus, $\mathcal{P}'$ will obtain his money by following the following protocol, which takes place when the game is over:

Protocol 5

1. *The Dealer sends the result of the game and the name of the winner $\mathcal{P}'$ to the OC.*
2. *The OC, $\mathcal{P}$ and $\mathcal{P}'$ run the transfer Protocol 7 (cf. Section 3.4) for every chip of $\mathcal{P}$ in the bet.*
3. *If $\mathcal{P}$ does not collaborate during the transfer protocol, the OC and the winner $\mathcal{P}$ run Protocol 6 to force $\mathcal{P}$'s payment.*

Let us assume that $X = \{x_1, \ldots, x_s\}$ is the set of chips that $\mathcal{P}'$ has won and some dishonest player has not paid. In this situation, the winner can reclaim her payment by completing the following dialog with the Ownership Controller:

Protocol 6

For each $x_j = \{I_j, c_j, \gamma_j, I_j^{w_j}, \beta_j\}$ in X, recall that p_i, and q_i are the random numbers associate to the value of each chip (v_i) during the initialization phase described in 3.1.

1. *$\mathcal{P}'$ generates a random value w'_j, such that $2 < w'_j < q_i$, using a uniform distribution seeded by a random value σ.*
2. *$\mathcal{P}'$ computes $I_j^{w'_j} \bmod p_i$ and sends it to the OC.*
3. *$\mathcal{P}'$ proves proves to the OC, using Schnorr's zero-knowledge proof, that she knows $\log_{I_j} I_j^{w'_j}$.*
4. *The OC computes $\beta'_j = S_c\{I_j, I_j^{w'_j}\}$, and replaces x_j with the new valid chip x'_j, where $x'_j = (I_j, c_j, \gamma_j, I_j^{w'_j}, \beta'_j)$.*

As a result, $\mathcal{P}'$ gets hold of the chips she won without $\mathcal{P}$'s intervention, who cannot help being deprived of them.

3.4 Transfer protocol

When a player $\mathcal{P}$ must transfer a chip $x = (I, c, \gamma, I^w, \beta)$ to another player $\mathcal{P}'$, the OC, $\mathcal{P}$ and $\mathcal{P}'$ will run the following protocol:

Protocol 7

1. *$\mathcal{P}$ sends w to $\mathcal{P}'$, and proves to OC, using Schnorr's algorithm, that she knows $\log_I I^w$.*
2. *$\mathcal{P}'$ generates a random value w' such that $2 < w' < q$, using a uniform distribution seeded by a random number seed.*
3. *$\mathcal{P}'$ computes $I^{w'} \bmod p$, and sends it to the OC.*
4. *$\mathcal{P}'$ proves proves in zero-knowledge to the OC that she knows $\log_I I^{w'}$;*
5. *The OC computes $\beta' = S_{oc}\{I||I^{w'}\}$, and replaces x' for x as a valid chip, where $x' = (I, c, \gamma, I^{w'}, \beta')$.*

3.5 Deposit protocol

A player $\mathcal{P}$ wanting to deposit a chip $x = (I, v, \gamma, I^w, \beta)$ will run the following simple protocol with the OC and the Bank:

Protocol 8

1. *$\mathcal{P}$ proves to the Bank, via Schnorr's algoritm, that she knows $\log_I I^w$.*
2. *The Bank deposits v in $\mathcal{P}$'s account.*
3. *The Bank sends x to the OC.*
4. *The OC removes x from the list of valid chips in the bulletin board.*

4 Security analysis

The security of our system is based on the Ownership Controller, which plays the role of an optimistic Trusted Third Party (TTP). Thus, the following security assesment for the digital chips management protocols presented in the previous sections relies on the assumption that the OC is honest. As will be shown, such assumption suffices to guarantee the detection of dishonest behaviour of any other actor in the system.

4.1 Withdrawal protocol

The Bank issues digital coins to players with the OC's involvement. The information that is exchanged between a player and the Bank ensures that digital chips cannot be stolen. Since the exponent w associated to every digital chip can be used to prove ownership to the OC, a hypothetical thief would need to know its value. But, as we have seen, this value is only known by the chip's legitimate owner, and can only be computed by solving a discrete algorithm.

4.2 Bet protocol

The use of a time server in the bet protocol ensures that all involved parties will respect the time schedule. A player's bet contains the initial and the bet's time, stamped by the time server. Therefore, it can be easily verified that the all parties have obeyed the game schedule.

Any player can verify, via the OC's bulletin board, the validity of bet chips, and zero-knowledge proofs assess chip ownership.

Bets are digitally signed by players. Therefore, nobody can modify them once they have been stamped by the time server.

Finally, a valid bet cannot be ignored when the game is over, because every bet is placed in the bulletin board.

4.3 Transfer and deposit protocols

The transfer protocol is run between honest players, so that no security concerns arise here. If a loser refuses to pay, the legitimate winner can recur to the OC via Protocol 6 to force the transfer of the corresping chips, and the (dishonest) loser cannot interfere or avoid this operation in any way, nor is his participation required for a succesful completion of the protocol. In sum, players are always able to obtain the chips that they win.

Finally, only the legitimate owner of a chip, barring the solution of a discrete logarithm, can proof to the Bank that she owns her chips.

5 Conclusions

We have presented in this paper an effective set of protocols for digital chip management in on-line casinos that offers a reasonable complexity and good time efficiency.

The use of digital chips for e-gambling is a relative novel topic. Currently, online casinos use prepaid systems and the casino manages internally all the transactions between the players. Such a scenario demands a very strong trust relation between players and the casino's management, which poses well-known security concerns. Our system introduces a TTP (the Ownership Controller) to greatly ameliorate these problems, and uses it through a set of relatively simple, feaseable cryptographic protocols.

References

[1] R. Anderson, H. Manifavas, and C. Shutherland. Netcard - a practical electronic cash system. In *Cambridge Workshop on Security Protocols*, 1995.

[2] S. Brands. Untraceable off-line cash in wallets with observers. In *Proceedings of CRYPTO'93*, pages 302–318, 1993.

[3] D. Chaum. Blind signatures for untraceable payments. In *Proceedings of CRYPTO'82*, pages 199–203, August 1982.

[4] D. Chaum. Security without identification: transactions systems to make big brother obsolete. *Communications of the ACM*, 28(10):1030–1044, october 1985.

[5] D. Chaum. Achieving electronic privacy. *Scientific american*, pages 96–101, August 1992.

[6] S. Foley. Using trust management to support transferable hash-based micropayments. In *Financial Cryptography 2003*, pages 1–14, 2003.

[7] S. Glassman, M. Manasse, M. Abadi, and G. Gauthier. The Millicent protocol for inexpensive electronic commerce. In *World Wide Web Journal: The Fourth International WWW Conference Proceedings*, pages 603–618, 1995.

[8] C. Hall and B. Schneier. Remote electronic gambling. In *13th Annual Computer Security Applications Conference*, pages 227–230. ACM, December 1997.

[9] M. Jahanian-Farsi. Digital cash. Master's thesis, Master's Thesis in Computer Science, Department of mathematics and computing science, Gteborg University, 1997.

[10] G. Medvinsky and B. C. Neuman. NetCash: A design for practical electronic currency on the internet. In *Proceedings of the First ACM Conference on Computer and Communications Security*, pages 102–106, 1993.

[11] K. Q. Nguyen, Y. Mu, and V. Varadharajan. Micro-digital money for electronic commerce. In *13th Annual Computer Security Applications Conference*, Dec. 1997.

[12] T. Okamoto and K. Ohta. Universal electronic cash. In Springer-Verlag, editor, *Advances in Cryptology Crypto '91*, LNCS 576, pages pp. 324–337, Berlin, 1992.

[13] D. O'Mahony, M. Pierce, and H. Tewari. *Electronic Payment Systems for E-Commerce*. Artech House, Norwood, MA, second edition, 2001.

[14] R. Oppliger and J. Nottaris. Online casinos. In *Kommunikation in verteilten Systemen*, pages 2–16, 1997.

[15] C. Schnorr. Efficient signature generation by smart cards. *Journal of Cryptology*, 4(3):pp. 161–174, 1991.

[16] W. Zhao, V. Varadharajan, and Y. Mu. Fair on-line gambling. In *16th IEEE Annual Computer Security Applications Conference (ACSAC'00)*, pages pp. 394–400, 2000.