Marking: A Privacy Protecting Approach Against Blackmailing

Dennis Kügler and Holger Vogt

Department of Computer Science*,
Darmstadt University of Technology,
D-64283 Darmstadt, Germany
{kuegler|hvogt}@cdc.informatik.tu-darmstadt.de

Abstract. Electronic payment systems based on anonymous coins have been invented as a digital equivalent to physical banknotes. However, von Solms and Naccache discovered that such anonymous coins are also very well suited to support criminals in blackmailing.
In this paper we present a payment system, which has an efficient tracing and revocation mechanism for blackmailed coins. The used tracing method is based on the idea of marking coins similar to marking banknotes with an invisible color. In contrast to previous solutions our payment system is unconditionally anonymous and thus protects the privacy of the users.

1 Introduction

Blind signature based anonymous payment systems [Cha83] have been invented for privacy protecting payments over the internet. However, it was discovered by von Solms and Naccache [vSN92] that *unconditional anonymity* may be misused by criminals: A blackmailer can exploit the properties of the used blind signature to receive blackmailed money from his victim so that neither the victim nor the bank are able to recognize the blackmailed coins later. Furthermore, the blackmailed coins can be transferred anonymously via an unobservable broadcast channel (e.g. a newsgroup). This attack is called the *perfect crime*, as it is impossible to identify or trace the blackmailer.

To solve anonymity related problems as blackmailing, money laundering, or illegal purchases, payment systems with *revokable anonymity* have been proposed [CMS96,JY96,FTY96,JY97]. In these payment systems trusted third parties are able to revoke the anonymity of the users at any time.

In our opinion blackmailing is the most serious drawback of the known payment systems offering unconditional anonymity. Attacks like money laundering and illegal purchases aren't a major problem in anonymous electronic payment systems, as these problems are even worse with physical cash [Fro96], because

* This work was supported by the Deutsche Forschungsgemeinschaft (DFG) as part of the PhD program (Graduiertenkolleg) "Enabling Technologies for Electronic Commerce" at Darmstadt University of Technology.

K. Kim (Ed.): PKC 2001, LNCS 1992, pp. 137–152, 2001.

in anonymous electronic payment systems the bank always knows how much a customer withdraws and how much a person deposits. Thus the bank is able to detect either the initiator or the recipient of a suspicious transaction.

In this paper we will show how to fight blackmailing without restricting the anonymity of users as it is done in systems with revokable anonymity. We present a new online payment scheme, which offers unconditional anonymity, but does not suffer from the blackmailing attack described above.

We stress that our proposed payment system is very practical as no trusted third parties are needed, and it is especially well suited for payments over the internet and for mobile payments using cellular phones. In our opinion, it is not a drawback that our system is an online system, as these systems minimize the risk of fraud and losses that may be caused by e.g. overspending.

The remainder is structured as follows: A new technique, which we call *marking*, is introduced in the next section. In Section 3 we show how marking is used in several scenarios to fight blackmailing. The implementation of a payment system using the marking technique is presented in section 4. The security and anonymity aspects are discussed in section 5. Furthermore, we sketch several improvements of the payment system in section 6, and we discuss how our approach relates to systems with revokable anonymity in section 7. Finally we conclude the paper with some open issues for further research.

2 Marking: A New Approach Against Blackmailing

Physical cash, particularly banknotes have two important features, which can be used to fight blackmailing:

- The serial numbers of the banknotes can be annotated.
- The banknotes can be marked, e.g. with a special invisible color.

The goal of both approaches is to support the investigation of blackmailings by enabling recognition of blackmailed banknotes after they are spent or discovered somewhere. As precondition for this method of investigation the victim of a blackmailing has to inform the bank and the police about the blackmailing **before** delivering the money.

Using the idea of annotating serial numbers for electronic payments results in payment systems with revokable anonymity, where a hint is kept in a database, which enables a trusted third party to recover the serial number. However, the knowledge of the serial numbers may be misused to trace users even if no blackmailing occurred.

As annotating serial numbers of electronic coins may violate anonymity, we base our approach for an anonymous payment system on the idea of marking coins. No electronic payment system with a similar mechanism has been proposed yet.[1]

[1] Note that the notion of marking with an invisible color should not be confused with magic ink signatures introduced in [JY97], which uses the approach of annotating serial numbers.

2.1 Marking of Electronic Coins

Our anonymous payment system implements a reliable marking mechanism for electronic coins and has the following properties:

- For every blackmailing the bank may issue coins with a different marking.
- Only the bank can determine whether a coin is marked or not. For every other person marked coins are indistinguishable from unmarked coins.
- At withdrawal the bank has to prove that a coin is unmarked. This proof cannot be used to convince anybody except the owner of the bank account.
- At deposit the bank can accept or reject marked coins, depending on the choice of the blackmailed person.

It follows directly that the anonymity of a customer is protected, as he always detects unsolicited marking. In case of blackmailing, a customer requests marked coins from the bank, and every spending of marked coins will immediately be noticed by the bank.

Compared to physical cash, our marking mechanism has several advantages:

- All unspent marked coins can be invalidated and refunded to the customer, after he instructs the bank to reject all marked coins. Thus the customer looses only the amount of the already spent marked coins.
- All spent marked coins can efficiently be detected at deposit. This enables tracing of the blackmailer.
- Marking cannot be misused to trace honest users.

2.2 A New Payment System Based on Undeniable Signatures

The typical approach for unconditional anonymous payment systems is based on blind signatures [Cha83]. However, in these systems it is hard to embed an undetectable mark in a coin, because the bank would have to generate a modified signature at the withdrawal, and as the validity of a coin's signature is publicly verifiable, such a modification of a blind signature is easy to detect.

Due to this shortcomings our aim is to restrict the verifiability of coins. We basically suggest the use of blind undeniable signatures [CvA89,Cha90] instead of blind signatures so that the verification of a signature can only be done by interacting with the bank in non-transferable zero-knowledge protocols:

Confirmation protocol: This protocol is used by the signer to prove the *validity* of an undeniable signature to another party.

Disavowal protocol: This protocol is used by the signer to prove the *invalidity* of an undeniable signature to another party.

The main idea of our payment system is that the bank issues coins consisting of undeniable signatures. This has the following consequences:

- At withdrawal, the bank must prove validity of a blindly withdrawn coin with a confirmation protocol. Without the confirmation protocol the bank may issue invalid or marked coins.

– At deposit, if the bank rejects a coin, it must prove the invalidity of this coin with a disavowal protocol. For an accepted coin the bank never proves the validity. Therefore, the bank may accept detected marked coins, but cannot deny a valid coin.

It is not a drawback in an online payment system that a coin cannot be verified without the issuing bank, because due to possible overspendings the validity of coins can only be checked by the bank.

2.3 Implementing Marking in Our Payment System

The bank can issue marked coins by using a different private key (we will also call this a *marking key*) instead of the normal private key to generate the undeniable signature. When the bank receives a coin, which was not generated with the normal private key, the bank has to check whether the coin has been created with a marking key.

Basically, we have to distinguish three different types of coins:

Valid coins: These coins are created with the normal private key of the bank. The bank always proves the validity of this type of coins with the confirmation protocol at withdrawal.

Marked coins: These coins are only issued in case of blackmailing and are created with a different marking key for each blackmailing. The confirmation protocol always fails for marked coins.

Invalid coins: These coins were neither generated with the normal private key nor with any of the marking keys. In other words, they were not generated by the bank. At deposit those coins are always rejected by the bank, which proves the invalidity with the disavowal protocol.

Some problems arise with these three types of coins, as a blackmailer must not be able to distinguish between marked and valid coins. The obvious way to test a coin to be valid, is to execute the confirmation protocol. Thus, we restrict the use of the confirmation protocol only to the withdrawal and we guarantee that for a specific coin the confirmation protocol is executed exactly once.

3 Cheating a Blackmailer to Accept Marked Coins

In this section we show how the customer and the bank together can cheat a blackmailer in the confirmation protocol to accept marked coins as valid coins. Depending on the power of the blackmailer, we have to distinguish three scenarios:

Perfect crime: The blackmailer contacts the victim via an anonymous channel and threatens him to withdraw some coins which are chosen and blinded by the blackmailer. The blackmailer communicates only with the victim but cannot observe the victim's communication with the bank.

Impersonation: The blackmailer gains access to the victim's bank account and withdraws coins by himself. The blackmailer communicates directly with the bank but cannot observe the victim's communication with the bank.

Kidnapping: The blackmailer has physical control over the blackmailed victim and withdraws the coins similar to the impersonation scenario. The blackmailer communicates directly with the bank and prevents the victim from communicating with the bank.

In all these scenarios the blackmailer hides his identity by using anonymous communication channels (e.g. remailer, broadcast communication or an anonymous communication endpoint).

We assume that the customer always tries to inform the bank about a blackmailing. If the customer notifies the bank about a blackmailing, the bank will issue marked coins in future withdrawals of the customer. Furthermore, we assume that the blackmailer is not able to observe the actions of the bank. The bank strictly follows the defined protocols for withdrawal and deposit and never cooperates with a blackmailer.

Next, we describe the different scenarios and their problems in detail and discuss our countermeasures when blackmailing occurs.

3.1 Perfect Crime

In this scenario the blackmailer threatens the victim to withdraw some coins which are chosen and blinded by the blackmailer. The victim contacts his bank and instructs it to mark these blinded coins during the withdrawal. The victim sends the marked coins back to the blackmailer, who unblinds the coins. In the subsequent confirmation protocol the blackmailer can choose the secret parameters and thus the challenge for the bank. Then the blackmailer instructs the customer to execute the confirmation protocol with this challenge to prove whether the coins are valid or marked/invalid.

Basically, we face the problem that the confirmation protocol is necessary to protect the customer from a cheating bank, but it also enables the blackmailer to detect marked coins. We solve this problem with a designated verifier proof [JSI96] in the confirmation protocol. Such a proof for the validity of the coins convinces only the designated verifier, who is in our case the owner of the bank account.

In the following we describe our generic confirmation protocol (see figure 1), which uses public key encryption as a trapdoor to extract the secret parameters of the challenge:

1. The customer generates a challenge from the coin and secretly chosen parameters. These parameters are encrypted with his own public key and sent together with the challenge to the bank.
2. For the given challenge the bank commits to a zero-knowledge proof for the validity of the coin and sends the committed proof to the customer.
3. The customer has to reveal his secret parameters to the bank. Then the bank checks, if the customer's challenge was built correctly.

4. Only then the bank opens the committed proof, which convinces the customer of the validity of the withdrawn coin.

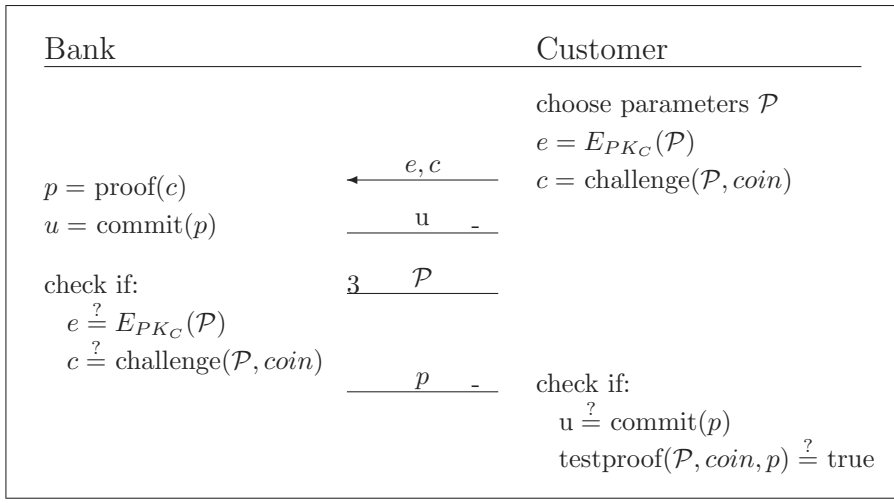

Fig. 1. This confirmation protocol convinces only the designated verifier of the validity of a coin.

In the case of a blackmailing the customer receives the challenge from the blackmailer. But as the customer can decrypt the secret parameters of the challenge, he can generate the answer that the blackmailer expects for an unmarked coin although the bank has issued a marked coin. Because the blackmailer cannot distinguish between the simulated and a real transcript of the confirmation protocol, he will always accept the proof.

A different solution for a designated verifier confirmation protocol, which is based on trapdoor commitments, is given in [JSI96]. In contrast to our solution the customer can open the commitment so that the revealed value is the correct answer for an unmarked coin. In the following we will focus on our solution, as it is more generic.

3.2 Impersonation of the Customer

In addition to the perfect crime scenario the blackmailer may even force the victim to reveal any private information including the information to access the victim's bank account. The blackmailer contacts the bank and pretends to be the owner of the victim's account. Thus the blackmailer can withdraw an arbitrary number of coins without the help of the victim.

However, the victim may communicate with the bank, as this is unobservable for the blackmailer. The customer gives his decryption key to the bank, who

can cheat the blackmailer as described in the perfect crime scenario. Note that transferring the decryption key to the bank will only enable the bank to mark coins in the future. Previously withdrawn coins are not affected and the privacy of the customer remains untouched. Alternatively, the customer can decrypt the parameters for the bank and keep his decryption key secret.

3.3 Kidnapping the Customer

In addition to the impersonation scenario the blackmailer has now physical control over the blackmailed victim. Thus the victim can only communicate with the blackmailer so that the victim is neither able to directly instruct the bank to issue marked coins nor to generate a faked confirmation protocol.

In this scenario a covert channel is needed to inform the bank about the kidnapping. For implementing such a covert channel we adopt the idea of a distress cash system [DFTY97]. Furthermore, we must enable the bank to generate a faked confirmation protocol by utilizing the trapdoor in the confirmation protocol, which is only possible, if the bank knows the private key for the decryption of the secret parameters.

A simple solution is to use secure hardware for the authentication at the beginning of the withdrawal. The main idea is that the hardware offers two different PINs, where one can be used to indicate a blackmailing. In this case the secure hardware informs the bank about the blackmailing and delivers the decryption key, which enables the bank to utilize the trapdoor to cheat the blackmailer. Due to the use of secure hardware, communication with the bank is encrypted and can be assumed to be unobservable. This means that it is impossible for the blackmailer to detect that his victim used the PIN, which enables the bank to issue marked coins.

A solution that does not depend on secure hardware is more complicated. For simplicity we assume that we use the same key pair for encryption of the challenge and for authentication of the customer. A covert channel is implemented by providing at least two different authentication key pairs. The first key pair should be used for ordinary withdrawals. All other key pairs are used only in the case of blackmailing, where both the public and the private key are already known to the bank, which enables it to decrypt the challenge given by the blackmailer in the confirmation protocol.

We suggest to generate all authentication key pairs dynamically from passphrases. Then it is impossible for the blackmailer to detect that his victim used a passphrase which instructs and enables the bank to issue marked coins.

4 Implementation of Our Payment System

In the following we will assume an attacker trying to commit the perfect crime, as the solution for this scenario can easily be transferred to the impersonation and the kidnapping scenario.

For the implementation of our payment system there are still some problems, which we will solve:

Comparing: A blackmailer can withdraw some coins in a regular withdrawal and the same coins in a blackmailing. For the regular withdrawal he knows that the coins are valid. If the blackmailed coins are marked, he will determine a difference between the blackmailed coins and the regularly withdrawn coins.

Transforming: A blackmailer must not be able to destroy marking. It cannot be assumed that a blackmailer follows the withdrawal protocol (e.g. he may use a different kind of blinding), but it must be guaranteed that marked coins cannot be transformed to invalid coins, while valid coins remain valid.

4.1 The Main Idea of Our Construction

To prevent the comparing attack we have to ensure that withdrawing the same coin two or more times always results in different signatures. This can be achieved with a randomized signature scheme.

We developed a new construction for a randomized undeniable signature, which uses the Okamoto-Schnorr blind signature scheme [Oka92,PS96] combined with the Chaum-van Antwerpen undeniable signature scheme [CvA89]. The main idea is to sign a random value with an undeniable signature, where the random value is a part of the blind signature. However, signing the commitment of a randomized blind signature does not work, as it is susceptible to the transforming attack. Instead we choose a system parameter of the blind signature randomly and sign it with the undeniable signature.

4.2 System Setup

In our payment system the system parameters are prime numbers p and q with $q|(p-1)$ and elements g_1, g_2 and g_3 of $(\mathbb{Z}/p\mathbb{Z})^*$ of order q. The bank chooses a key pair

$$SK_{\mathcal{B}} := (s_{1,}s_2) \in_R (\mathbb{Z}/q\mathbb{Z})^2$$
$$PK_{\mathcal{B}} := v = g_1^{s_1} g_2^{s_2} \bmod p$$

for the blind signature and a key pair

$$SK_{\mathcal{U}} := x \in_R \mathbb{Z}/q\mathbb{Z}$$
$$PK_{\mathcal{U}} := y = g_3^{x} \bmod p$$

for the undeniable signature scheme. Then it publishes the public keys $PK_{\mathcal{B}}$ and $PK_{\mathcal{U}}$.

4.3 The Withdrawal Protocol

The withdrawal protocol is shown in figure 2. For every new coin the bank creates a new random generator $\alpha = g_2^r \bmod p$ and sends this value to the customer. Then the bank and the customer interact in a blind Okamoto-Schnorr signature protocol, where the bank uses the generators g_1 and α. The customer transforms

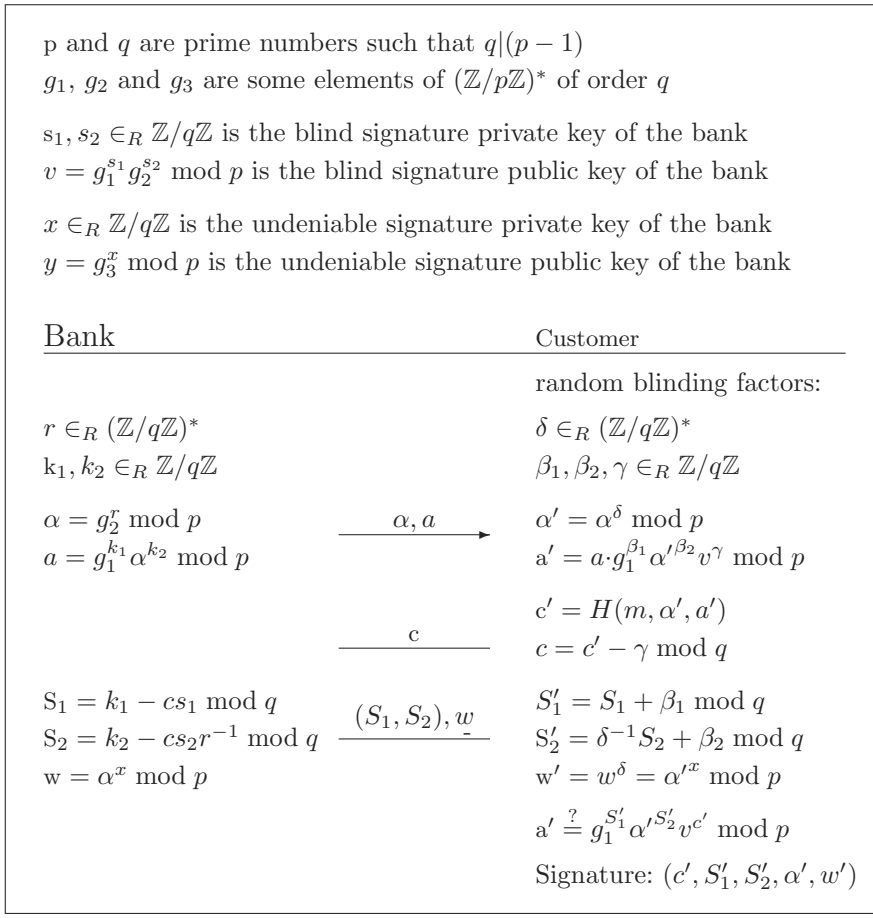

Fig. 2. Withdrawal of coins based on Okamoto-Schnorr blind signatures combined with Chaum-van Antwerpen undeniable signatures.

this signature to a signature based on the generators g_1 and $\alpha' = \alpha^\delta \bmod p$ using a randomly chosen $\delta \in_R (\mathbb{Z}/q\mathbb{Z})^*$. This transformation is needed, because otherwise the bank could recognize coins at deposit on behalf of the generator α.

Finally the bank issues an undeniable signature $w = \alpha^x \bmod p$ as a certificate for α. Again, the certificate has to be transformed to $w' = w^\delta = \alpha'^x \bmod p$ by the customer to circumvent recognition by the bank and to be a valid undeniable signature for α'. Note that for this transformation we have to omit the hashfunction on α. The impact on the security will be discussed in section 5.

At the end of the withdrawal protocol the customer possesses a valid coin $(m, c', S_1', S_2', \alpha', w')$, and the validity of the undeniable signature w has to be proven

in a confirmation protocol. Our confirmation protocol (see figure 3) is a designated verifier variant of the protocols described in [CvA89,Cha90]. If the customer follows the withdrawal protocol correctly, then the given proof is also valid for w'.

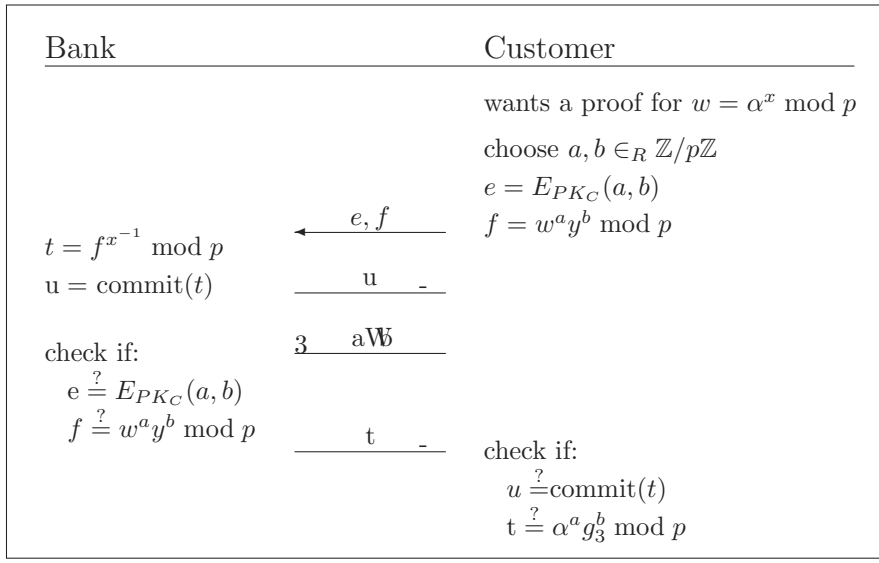

Fig. 3. This confirmation protocol proves the validity of the withdrawn coin only to the designated verifier.

4.4 Marking Blackmailed Coins

In the case of blackmailing marked coins are issued using a different private key $SK_{\mathcal{U}_\mathcal{M}} := x_\mathcal{M}$ to generate the undeniable signature. In order to recognize marked coins the bank has to maintain lists of all used marking keys:

1. The list $\mathbb{M}_A$ contains all marking keys for which the corresponding coins should be *accepted*.
2. The list $\mathbb{M}_R$ contains all marking keys for which the corresponding coins should be *rejected*.

When the customer instructs the bank to reject all his marked coins, the bank moves the corresponding marking key to $\mathbb{M}_R$ and refunds the amount of all unspent marked coins to the customer.

Our confirmation protocol for the Chaum-van Antwerpen undeniable signature used in the case of blackmailing is shown in figure 4. As the customer is able to decrypt the committed secret parameters a and b, he can give the correct answer $t = \alpha^a g_3^b \bmod p$, which the blackmailer expects for an unmarked coin.

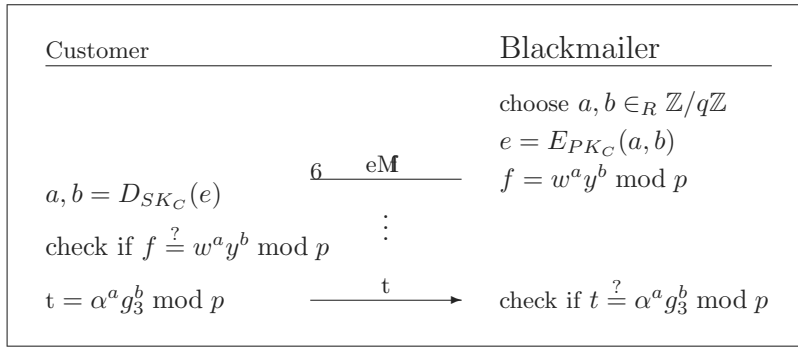

Fig. 4. In case of blackmailing the customer can even prove the validity of a marked coin.

4.5 Spending and Depositing Coins

When a customer spends a coin $(m, c', S_1', S_2', \alpha', w')$, the merchant is not able to check the validity of this coin alone, because he cannot verify the undeniable signature and cannot check for double spending. Thus he immediately has to deposit this coin at the bank.

For every coin to be deposited the bank first checks for double spending and then verifies the Okamoto-Schnorr signature and the corresponding Chaum-van Antwerpen undeniable signature.

Verification of the Okamoto-Schnorr signature: The bank verifies the signature by computing $a' = g_1^{S_1'} \alpha'^{S_2'} v^{c'} \bmod p$ and checking $c' \stackrel{?}{=} H(m, \alpha', a')$. If this test fails, the coin is rejected.

Verification of the Chaum-van Antwerpen undeniable signature: The bank verifies the undeniable signature by checking $w' \stackrel{?}{=} \alpha'^x \bmod p$. If this test also succeeds, then the coin is valid and will be accepted. If the test fails, the bank checks all previously used marking keys.

Checking the marking keys: The bank checks the marking keys $x_{\mathcal{M}} \in \mathbb{M}_A \cup \mathbb{M}_R$ by testing $w' \stackrel{?}{=} \alpha'^{x_{\mathcal{M}}} \bmod p$. If one of the marking keys fulfills this equation, the bank knows to which blackmailing this coin belongs and whether it has to accept or reject this coin. If the test fails for all marking keys, the coin is invalid and will be rejected.

Disavowal protocol: If the bank rejects a coin because of the undeniable signature, it has to prove that the undeniable signature was not generated with x. In our payment system we use Chaum's disavowal protocol [Cha90] for this proof.

5 Discussion of Security and Anonymity

In this section we discuss some aspects of security and anonymity of our payment system.

Unforgability of coins: It is sufficient to show that the blind signature is unforgeable, as this implies the unforgability of coins. Obviously, the security of the blind signature is not affected even if marking keys are published.

Our Okamoto-Schnorr blind signature differs from the original blind signature [Oka92,PS96], as it is possible to modify one generator by computing $\alpha' = \alpha^{\delta} \bmod p$. However, even if an attacker enforces this generator to be $\alpha' = 1$ by choosing $\delta = 0$ the signature remains witness-indistinguishable [FS90], as $k_1$and k_2 are always hidden in a. The security of witness-indistinguishable blind signatures is shown in [PS96]. Also note that no valid signature can be created with $\delta = 0$, as δ has to be invertible.

Undetectability of marking for blackmailers: Blinding of the undeniable signature is only possible as we omit the hashfunction on α, which makes the undeniable signature susceptible to the transforming attack described at the beginning of section 4. The goal of such a transformation is that marked coins are transformed to invalid coins, while valid coins remain valid. In this attack the undeniable signature (α, w) may be transformed to $(\alpha', w') = (\alpha^{\delta} h \bmod p, w^{\delta} h^{x} \bmod p)$ using a value h for which an undeniable signature $h^x \bmod p$ is available. In the verification of the blind signature $(a' = g_1^{S_1'} \alpha'^{S_2'} v^{c'} \bmod p)$ the value α' is raised to the power of S_2'. However, $h^{S_2'} \bmod p$ was not known at the time when a' was computed and thus the verification equation can only be fulfilled, if an attacker knows the discrete logarithm of h to the base of g_1 or g_2. As no undeniable signature of g_1 or g_2 is available to an attacker, no suitable h can be constructed. Thus h always has to be 1, which means that blackmailers cannot apply this attack to destroy marking.

Anonymity of customers: A unique property of our payment system is that the decision whether a coin is traceable or not has to be made at withdrawal and is unalterable afterwards.

If the customer receives unmarked coins at withdrawal, the views of the customer and the bank on the coins are unlinkable due to the blind signature. This means that payments with unmarked coins are unconditional anonymous for the customer.

The only way to degrade the anonymity of customers is to mark their coins. However, a polynominal time bounded bank has only a negligible chance to succeed in the confirmation protocol with a marked coin. If the bank is not polynominal time bounded, it may cheat the customer in the confirmation protocol by decrypting his challenge.

6 Improvements and Enhancements

After we described the basic version of our payment system, we now sketch several ideas how the system can be further improved.

- The efficiency of the withdrawal can be improved, if the bank uses the same random α and the same certificate w for all coins of a withdrawal session. This improvement has no impact on the linkability of the coins from one session, as long as the customer uses a different δ for every coin.
- As long as no marked coins are issued by the bank, the bank only needs to verify the blind signature. If this signature is correct, then it must have been issued by the bank, and thus the coin can be accepted without checking the undeniable signature.
- If the bank detects a coin generated with a marking key $x_{\mathcal{M}} \in \mathbb{M}_R$ at deposit, the bank may simply publish the key $x_{\mathcal{M}}$ instead of interacting in a disavowal protocol.
- When a blackmailer has been caught, the marking key used for this blackmailing can be removed from $\mathbb{M}_A$ or $\mathbb{M}_R$. If a coin with such a marking is deposited later, it is always rejected as invalid.
- There also exist other, less efficient implementations of our payment scheme, e.g. an Okamoto-Guillou-Quisquater blind signature [Oka92,PS96] combined with an undeniable RSA signature [GKR97].

7 A Comparison to Systems with Revocable Anonymity

In this section we compare our payment system to systems with revocable anonymity (e.g. [DFTY97,JY96,CMS96,JY97]), which are another well known solution to blackmailing attacks. In contrast to our solution these systems are based on trusted third parties.

The advantage of a system with revocable anonymity is that tracing is possible at any time after the withdrawal. This makes it always possible to trace blackmailed coins. In our system the customer has to decide at withdrawal, whether the coins should be traceable or not. But due to this restriction of our scheme, we do not suffer from *illegal tracing*, which may be possible in systems with revokable anonymity due to the following reasons:

- If the trusted third party illegally cooperates with the bank, they can trace the customer.
- Even if the trusted third party is honest, there is the danger that the bank gains access to the private data of the trusted third party and is able to trace the customer on its own. Vice versa, a dishonest trusted third party might get access to the bank's database and trace customers.
- Even if the private data of an honest trusted third party is protected carefully, the bank may be able to trace the customer alone: If anonymity revocation is implemented by trusted third party decryption (this applies to all offline trusted third parties, e.g. [CMS96,DFTY97]) and the cryptosystem is

broken, then the bank can trace any payment by computing the decryption key of the trusted third party.

In all of these cases illegal tracing is a serious threat for the privacy of a customer, as he has no possibility to detect illegal tracing. Moreover, it is always hard to prove that illegal tracing has happened.

In our payment system illegal tracing is impossible. Even if the cryptosystem used for the encryption in the confirmation protocol can be broken, the bank will not be able to trace previous payments. As long as the customer uses a secure encryption scheme at withdrawal the probability of illegal marking is negligible. Furthermore, any unmarked coin remains unconditionally anonymous in the future.

Last but not least we'd like to mention that most arguments against key escrow [AAB+98] (e.g. risk, complexity, costs) also apply for revocable anonymity.

8 Conclusions

We have sketched a novel anonymous payment system offering unconditional anonymity. In contrast to systems with revocable anonymity our approach does not rely on a trusted third party. In general a trusted third party causes additional costs, which the customer may not be willing to pay for. As the trusted third party manages sensitive personal data, it has to be protected carefully. However, the more secure the trusted third party is, the more expensive is the service of the trusted third party.

Our payment system protects private users against blackmailing attacks, by offering a marking mechanism similar to the well known marking of banknotes. Our marking mechanism is even more effective, because every transaction with a marked coin is immediately recognized by the bank. At deposit a detected marked coin may be accepted or rejected, depending on the choice of the customer.

As coins may only be marked in agreement with the customer, the bank cannot misuse marking to degrade anonymity. Nevertheless marked coins are undetectable for a blackmailer. This enables tracing of blackmailers and allows revocation of marked coins, without sacrificing anonymity.

An open question about our system is how it can be extended to other blackmailing scenarios (e.g. when the bank is blackmailed). Another question is whether the marking mechanism can also be applied to fight money laundering.

Acknowledgments

We like to thank Ingrid Biehl and the anonymous reviewers for their valuable suggestions and comments.

References

AAB+98. H. Abelson, R. Anderson, S. Bellovin, J. Benaloh, M. Blaze, W. Diffie, J. Gilmore, P. Neumann, R. Rivest, J. Schiller, and B. Schneier. The risks of key recovery, key escrow, and trusted third-party encryption. Online available at http://www.cdt.org/crypto/risks98, 1998. An earlier version appeared in World Wide Web Journal, v.2, n.3, 1997, pages 241–257.

Cha83. D. Chaum. Blind signatures for untraceable payments. In *Advances in Cryptology - CRYPTO '82*, pages 199–203. Plenum, 1983.

Cha90. D. Chaum. Zero-knowledge undeniable signatures. In *Advances in Cryptology - EUROCRYPT '90*, volume 473 of *Lecture Notes in Computer Science*, pages 458–464. Springer-Verlag, 1990.

CMS96. J. Camenisch, U. Maurer, and M. Stadler. Digital payment systems with passive anonymity-revoking trustees. In *Computer Security - ESORICS '96*, volume 1146 of *Lecture Notes in Computer Science*, pages 31–43. Springer-Verlag, 1996.

CvA89. D. Chaum and H. van Antwerpen. Undeniable signatures. In *Advances in Cryptology - CRYPTO '89*, volume 435 of *Lecture Notes in Computer Science*, pages 212–216. Springer-Verlag, 1989.

DFTY97. G. Davida, Y. Frankel, Y. Tsiounis, and M. Young. Anonymity control in e-cash systems. In *Financial Cryptography '97*, volume 1318 of *Lecture Notes in Computer Science*, pages 1–16. Springer-Verlag, 1997.

Fro96. A.M. Froomkin. Flood control on the information ocean: Living with anonymity, digital cash, and distributed databases. *15 U. Pittsburgh Journal of Law & Commerce 395*, 1996. Online available at http://www.law.miami.edu/~froomkin/articles/ocean.htm.

FS90. U. Feige and A. Shamir. Witness indistinguishable and witness hiding protocols. In *22nd Symposium on Theory of Computing (STOC '90)*, pages 416–426. ACM Press, 1990.

FTY96. Y. Frankel, Y. Tsiounis, and M. Young. "Indirect discourse proofs": Achieving efficient fair off-line e-cash. In *Advances in Cryptology - ASIACRYPT '96*, volume 1163 of *Lecture Notes in Computer Science*, pages 286–300. Springer-Verlag, 1996.

GKR97. R. Gennaro, H. Krawczyk, and T. Rabin. RSA-based undeniable signatures. In *Advances in Cryptology - CRYPTO '97*, volume 1294 of *Lecture Notes in Computer Science*, pages 132–149. Springer-Verlag, 1997.

JSI96. M. Jakobsson, K. Sako, and R. Impagliazzo. Designated verifier proofs and their applications. In *Advances in Cryptology - EUROCRYPT '96*, volume 1070 of *Lecture Notes in Computer Science*, pages 143–154. Springer-Verlag, 1996.

JY96. M. Jakobsson and M. Yung. Revokable and versatile electronic money. In *3rd ACM Conference on Computer Communication Security (CCCS '96)*, pages 76–87. ACM Press, 1996.

JY97. M. Jakobsson and M. Yung. Distributed "magic ink" signatures. In *Advances in Cryptology - EUROCRYPT '97*, volume 1233 of *Lecture Notes in Computer Science*, pages 450–464. Springer-Verlag, 1997.

Oka92. T. Okamoto. Provably secure and practical identification schemes and corresponding signature schemes. In *Advances in Cryptology - CRYPTO '92*, volume 740 of *Lecture Notes in Computer Science*, pages 31–53. Springer-Verlag, 1992.

PS96. D. Pointcheval and J. Stern. Provably secure blind signature schemes. In *Advances in Cryptology - ASIACRYPT '96*, volume 1163 of *Lecture Notes in Computer Science*, pages 252–265. Springer-Verlag, 1996.

vSN92. B. von Solms and D. Naccache. On blind signatures and perfect crimes. *Computers and Security*, 11(6):581–583, 1992.