Computers & Security, 11 (1992) 581–583

On Blind Signatures and Perfect Crimes

Sebastiaan von Solms[1] and David Naccache[2]

[1]*Rand Afrikaans University—Department of Computer Science, PO Box 524, Johannesburg 2000, South Africa*
[2]*Thomson Consumer Electronics R&D France, Parc d'Innovation # 1, PO Box 120, F-67403 Illkirch Cédex, France*

David Chaum has introduced the idea of blind signatures, an extension of the concept of digital signatures, as a way to protect the identity and privacy of a user in electronic payment and service networks. Blind signatures also prevent so-called "dossier creation" about users by organizations.

While the concept of blind signatures still allows authorities to distinguish between valid and false data, it prevents these authorities from connecting specific data or actions to specific users.

With the growing emphasis on the protection of the privacy of user data and user actions in electronic systems, blind signatures seem to be a perfect solution. This paper however, discusses a problematic aspect of blind signatures, showing that this perfect solution can potentially lead to perfect crime.

We use a real crime case as an example.

Keywords: Blind signatures, Digital signatures, Access control, Privacy, Network protection, Digital cash.

1. Introduction

Blind signatures can be used when a user wants to create legal electronic money, i.e. electronic money authorized by the bank. Once this money is created, it can be spent by the user without anybody anywhere being able to trace the money back to the user. This idea is described in detail in refs. 1 and 2.

The big (potential) benefit of the data is that individual surveillance (traceability) becomes impossible since it is not possible to determine who spends the electronic money.

Very much simplified, the concept works as follows.

Assume the public existence of a one-way function f and an RSA modulus n.

Step 1. The user requests electronic money from the bank:

1.1. The user chooses two random numbers:

a so-called blinding factor r, and x, and computes

$$B = r^3 f(x) \bmod n$$

B is sent to the bank.

1.2. The bank computes:

$$D = \sqrt[3]{B} \bmod n$$

Correspondence to: David Naccache, Philips TRT, Smart-Cards & Systems, 5 Avenue Réaumur, ZIPEC, PO Box 21, F-92352, Le Plessis Robinson Cédex, France.

and withdraws one "money unit" from the user's bank account, putting this "money unit" into a money pool. The bank sends D back to the user.

1.3. The user divides D by r (mod n), and keeps $C=\sqrt[3]{f(x)}$ mod n, the result of the division. $\{x, \sqrt[3]{f(x)} \text{ mod } n\}$ now represents one legal authorized "money unit" $\{x, C\}$.

Note that, although the bank knows it sent D back to the specific user, once D is divided by r, with only r known to the user, the resultant $\{x, C\}$ is in no way traceable to the specific user.

Step 2. The user spends his electronic money.

2.1. The user now offers $\{x, C\}$ as payment for one "money unit's" purchase to the shopkeeper/cash delivery machine/service selling entity.

2.2. The shopkeeper checks that $f(x)=C^3$ and if so, checks with the bank that $\{x, C\}$ has not been used previously.

2.3. The shopkeeper offers $\{x, C\}$ to the bank, who pays him one "money unit" from the money pool. It is totally impossible to trace this "money unit" back to our original user (in step 1).

Note that the user will, of course, use a smart card or similar technology to do the necessary calculations but for allowing the users to get convinced that the system is really blind, all such technological details are assumed to be public and only the factoring of the modulus n is kept secret by the authority.

2. The Kobayashi Credit Card Case

In his book *Dossiers d'Interpol 2*, Pierre Bellemare [3] reports the following criminal case.

In the early 1970s, a man opens bank account #1326387 in the Shinjubu branch of the First Kangyo Bank (Tokyo) and, after he has deposited ¥15,000 the bank supplies him with a credit card.

About a month later the baby of Mashahito Tsugawa, a famous Japanese TV actor, is kidnapped and a so-called "Kobayashi" threatens to kill the baby if an amount of 5 million Yen is not immediately accredited on the bank account #1326387.

A short enquiry shows that Kobayashi is a false identity.

The police identify the program of the central computer to trace ATM operations in real-time.

Policemen are placed near each machine and all withdrawal operations are filtered.

Some days later, Kobayashi is caught while trying to withdraw money with his card.

3. The Kobayashi Blind Signature Case

Suppose the First Kangyo Bank used a blind signature system, and Kobayashi decided to use it.

If he used the following strategy, he could have committed the perfect crime (as far as the financial aspect is concerned!).

Step 1. Open a bank account, receive the smart-card and kidnap the baby.

Step 2.

2.1. Choose a set of xs $(x_1, x_2, \ldots, x_p)$ and a set of rs $(r_1, r_2, \ldots, r_p)$.

2.2. Compute the set B_j where $B_j=r_j^3 f(x_j)$ mod n and mail the set B_j to the authorities with the threat to kill the baby if the following instructions are not complied with:

2.2.1. For all j, compute the set $D_j=\sqrt[3]{B_j}$ mod n

2.2.2. Publish the set D_j in a newspaper.

2.3. Buy the newspaper and compute the set $C_j=D_j/r_j$ mod n. $\{(x_j, C_j)\}$ now represents legal author-

ized money which can in no way be traced to Kobayashi.

Step 3. Free the baby.

Kobayashi can now freely spend all this money without any danger of ever being identified.

4. Discussion

Note that Kobayashi's first attempt failed because the credit card was an identity token which linked him to the bank account where the money was deposited. Withdrawing the money could therefore be traced back to him. In the second attempt this was impossible.

5. Conclusion

In this paper we tried to show that, while blind signatures can protect individuals from the "big brother is watching" situation, it may on the other hand create the situation where these same individuals may be deprived of some other type of protection.

Blind signatures can therefore provide potential problems for law enforcement of some types of crimes.

For the discussion above it is clear that blind signatures can be employed for successful criminal purposes that could not have been achieved without blind signatures.

On the other hand, blind signatures have beautiful properties which can be used to benefit mankind in general, and one should be careful not to throw out the baby with the bath water.

Maybe the moral of the story is, specifically in the area of information security research, to try to develop more formal ways in which new mechanisms and protocols can be proved to be sound, or at least analysed to determine if any conflicting conditions or situations do exist.

Promising work on these issues is being done, e.g. ref. 4.

References

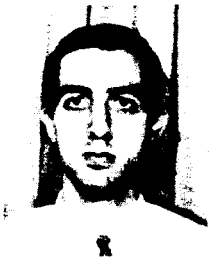
[1] D. Chaum, A. Fiat and M. Naor, Untraceable electronic cash. In S. Goldwasser (ed.), *Lecture Notes in Computer Science # 403, Proc. Crypto '88*, Springer-Verlag, Berlin, 1990, pp. 319–327.

[2] D. Chaum, Security without identification: Transaction systems to make big brother obsolete, *CACM 28/10*, 1985, pp. 1030–1044.

[3] P. Bellemare and J. Antoine, *Dossiers d'Interpol 2*, Editions N1, 1976, pp. 301–308.

[4] S. H. von Solms and N. Edwards, Designing and implementing a new security model, Int. J. Comp. Math., 29 (1989) 139–149.

Sebastiaan H. von Solms is Professor and Head of the Department of Computer Science at the Rand Afrikaans University in Johannesburg. He holds a Ph.D. degree in computer science. His main area of research is computer security and then specifically trying to find new and more powerful theoretical models for computer security. The field of formal languages and automata theory is used extensively in the description of such models.



David Naccache joined Thomson Consumer Electronics R&D, France, after gaining a degree in computer engineering and an M.Sc. in symbolic computation. He is presently with Philips TRT, where his interests are focused around smart-card technologies. He has authored or co-authored articles on number theory, cryptanalysis, combinatorics and hardware design.