Blind Signatures Based on the Discrete Logarithm Problem*

Jan L. Camenisch[1], Jean-Marc Piveteau[2], Markus A. Stadler[1]

[1] Institute for Theoretical Computer Science
ETH Zürich
CH-8092 Zürich, Switzerland
Email: {camenisch, stadler}@inf.ethz.ch
[2] Union Bank of Switzerland
Dep. UBILAB
Bahnhofstrasse 45
CH-8021 Zürich, Switzerland
Email: piveteau@ubilab.ubs.ch

Abstract. Blind signature schemes, an important cryptographic primitive, are useful in protocols that guarantee the anonymity of the participants. Two new blind signature schemes based on the discrete logarithm problem are presented.

1 Introduction

A blind signature scheme is a protocol allowing Bob to obtain a valid signature for a message m from a signer Alice without her seeing the message or its signature. If Alice sees m and its signature later, she can verify that the signature is genuine, but she is unable to link the message-signature pair to the particular instance of the signing protocol which has led to this pair.

The concept of a blind signature scheme was introduced by Chaum [2]. It allows to realize secure electronic payment systems protecting customer's privacy (e.g. [1],[3], [4], [5], [7], [10]) as well as other cryptographic protocols protecting the participants' anonymity (e.g. secure voting protocols [12]). Two proposals for blind signature schemes have been published: the first, presented in [2], is based on the RSA scheme [11], and the second is described in [6].

In this article, we present two new blind signature schemes. The first is derived from a variation of the DSA [8], the second is based on the Nyberg-Rueppel signature scheme [9].

2 Basic Signature Schemes

2.1 A Modification of DSA

The system parameters consist of a prime p, a prime factor q of $p-1$, and an element $g \in \mathbf{Z}_p^*$ of order q. The signer's private key is a random element $x \in \mathbf{Z}_q$,

* This work has been supported by the Swiss KWF Foundation, grant no. 2724.1.

while the corresponding public key is $y = g^x \pmod p$. To sign a message m, which is an integer relatively prime to q, the signer selects randomly $k \in \mathbf{Z}_q$, and computes R, r and s given by:

$$\begin{aligned} R &= g^k && \pmod p \\ r &= R && \pmod q \\ s &= km + rx && \pmod q \end{aligned}$$

The pair (r, s) is the signature of the message m. To check its validity, the receiver computes

$$T = (g^s y^{-r})^{m^{-1}} \pmod p$$

where m^{-1} denotes the inverse of m modulo q, and verifies that the following equality holds:

$$r = T \pmod q.$$

2.2 Nyberg-Rueppel Scheme

The following signature scheme has been published in [9]. The system parameters are the same as in the previous scheme. To sign a message $m \in \mathbf{Z}_p$, the signer selects $k \in \mathbf{Z}_q$ at random and computes r and s as follows:

$$\begin{aligned} r &= mg^k && \pmod p \\ s &= xr + k && \pmod q \end{aligned}$$

The pair (r, s) is the signature of the message m. To verify the validity of a signature, one checks that the following equality holds:

$$m = g^{-s} y^r r \pmod p.$$

Because this scheme provides message recovery, the signature need not to be accompanied by the message m.

3 Blind Signature Schemes

First we give a formal definition of the blindness for a signature scheme. Let $\mathcal{V}$ denote Alice's complete view of an execution of the protocol, i.e. her random coin tosses and all exchanged values; and let $(m, sig(m))$ denote the message-signature pair generated in that particular execution.

Definition 1. A signature scheme is called blind if Alice's view $\mathcal{V}$ and the message-signature pair $(m, sig(m))$ are statistically independent.

3.1 Blinding the Modification of DSA

The following protocol is a blind version of the modification of DSA described in Section 2.1.

1. a) Alice randomly chooses $\tilde{k} \in \mathbf{Z}_q$ and computes $\tilde{R} = g^{\tilde{k}} \pmod p$.
   b) Alice checks whether $gcd(\tilde{R}, q) = 1$. If this is not the case, she goes back to step a). Otherwise, she sends $\tilde{R}$ to Bob.
2. a) Bob checks that $gcd(\tilde{R}, q) = 1$.
   b) Bob randomly chooses $\alpha,\ \beta \in \mathbf{Z}_q$ and computes $R = \tilde{R}^\alpha g^\beta \pmod p$.
   c) Bob checks whether $gcd(R, q) = 1$. If this is not the case, he goes back to step b). Otherwise, he computes $\tilde{m} = \alpha m \tilde{R} R^{-1} \pmod q$ and sends $\tilde{m}$ to Alice.
3. Alice forwards $\tilde{s} = \tilde{k}\tilde{m} + \tilde{R}x \pmod q$ to Bob.
4. Bob determines $s = \tilde{s} R \tilde{R}^{-1} + \beta m \pmod q$ and $r = R \pmod q$.

Theorem 2. *The pair (r, s) is a valid signature of message m for the modification of DSA presented in Section 2.1 and the above protocol is a blind signature scheme.*

Proof: The validity of the signature (r, s) can easily be shown as follows. Let T be as in Section 2.1. Then

$$T = (g^s y^{-r})^{m^{-1}} = g^{(\tilde{s} r \tilde{R}^{-1} + \beta m - xr)m^{-1}} = g^{\tilde{k}\alpha + \beta} = R \qquad \pmod p$$

It follows that $r = T \pmod q$ which means that (r, s) is a valid signature of m.

In order to proof the blindness of the protocol, we show that given any view $\mathcal{V}$ and any valid message signature pair $(m, (r, s))$ with $r \neq 0 \pmod q$, there exists a unique pair of blinding factors α and β. Because Bob chooses the blinding factors α and β at random, the blindness of the signature scheme follows.

If the signature (r, s) of m has been generated during an execution of the protocol with view $\mathcal{V}$ consisting of $\tilde{k}$, $\tilde{R} = g^{\tilde{k}} \pmod p$, $\tilde{m}$, and $\tilde{s} = \tilde{k}\tilde{m} + \tilde{R}x \pmod q$, then the following equations must hold for α and β:

$$\begin{aligned} \tilde{m} &= \alpha m \tilde{R} r^{-1} && \pmod q \\ s &= \tilde{s} r \tilde{R}^{-1} + \beta m && \pmod q \\ r &= \tilde{R}^\alpha g^\beta && \pmod p \pmod q \end{aligned}$$

Because m, $\tilde{R}$, and r are relatively prime to q, the blinding factors α and β are uniquely determined by the first two equations:

$$\begin{aligned} \alpha &= \tilde{m} m^{-1} r \tilde{R}^{-1} && \pmod q \\ \beta &= (s - \tilde{s} r \tilde{R}^{-1}) m^{-1} && \pmod q \end{aligned}$$

By substituting $\tilde{s} = \tilde{k}\tilde{m} + \tilde{R}x \pmod q$, we obtain:

$$\tilde{k}\alpha + \beta = \tilde{k}\tilde{m} m^{-1} r \tilde{R}^{-1} + s m^{-1} - \tilde{s} r \tilde{R}^{-1} m^{-1} = (s - rx) m^{-1} \pmod q$$

We therefore have:

$$\tilde{R}^\alpha g^\beta = \tilde{R}^\alpha g^\beta = g^{\tilde{k}\alpha + \beta} = g^{(s - rx)m^{-1}} = (g^s y^{-r})^{m^{-1}} = T \pmod p$$

which implies $r = T \pmod q$. □

3.2 Blinding the Nyberg-Rueppel Scheme

In this Section we present the blind version of the Nyberg-Rueppel signature scheme.

1. Alice selects $\tilde{k} \in \mathbf{Z}_q$, computes $\tilde{r} = g^{\tilde{k}} \pmod p$, and sends $\tilde{r}$ to Bob.
2. a) Bob randomly selects $\alpha \in \mathbf{Z}_q$ and $\beta \in \mathbf{Z}_q^*$, computes $r = mg^{\alpha}\tilde{r}^{\beta} \pmod p$ and $\tilde{m} = r\beta^{-1} \pmod q$.
   b) Bob checks whether $\tilde{m} \in \mathbf{Z}_q^*$. If this is not the case, he goes back to step a). Otherwise, he sends $\tilde{m}$ to Alice.
3. Alice computes $\tilde{s} = \tilde{m}x + \tilde{k} \pmod q$ and forwards $\tilde{s}$ to Bob.
4. Bob computes $s = \tilde{s}\beta + \alpha \pmod q$.

Theorem 3. *The pair (r, s) is a Nyberg-Rueppel signature of the message m and the above protocol is a blind signature scheme.*

Proof: The validity of the signature (r, s) for message m follows from

$$g^{-s}y^r r = mg^{-\tilde{s}\beta-\alpha+xr+\tilde{k}\beta+\alpha} = mg^{-\tilde{m}x\beta-\tilde{k}\beta+xr+\tilde{k}\beta} = m \qquad \pmod p.$$

In order to proof the blindness of the protocol we show that given a valid signature (r, s) and any view $\mathcal{V}$, there exists a unique pair of blinding factors $\alpha \in \mathbf{Z}_q$ and $\beta \in \mathbf{Z}_q^*$. Since Bob chooses the blinding factors α and β randomly, the blindness of the signature scheme follows.

Assume that the signature (r, s) has been generated during the protocol with view $\mathcal{V}$ consisting of $\tilde{k}$, $\tilde{r} = g^{\tilde{k}} \pmod p$, $\tilde{m}$, and $\tilde{s} = \tilde{m}x + \tilde{k} \pmod q$): then the following equations must hold for α and β (where $m = g^{-s}y^r r \pmod p$):

$$\begin{aligned} r &= mg^{\alpha}\tilde{r}^{\beta} && \pmod p \\ \tilde{m} &= r\beta^{-1} && \pmod q \\ s &= \tilde{s}\beta + \alpha && \pmod q \end{aligned}$$

Since we have $\tilde{m} \in \mathbf{Z}_q^*$, a unique solution for α and β satisfying the last two of the above equations is given by:

$$\begin{aligned} \beta &= r\tilde{m}^{-1} && \pmod q \\ \alpha &= s - \tilde{s}\beta && \pmod q \end{aligned}$$

It remains to show that the first of the three equations holds:

$$mg^{\alpha}\tilde{r}^{\beta} = g^{-s+rx+\alpha+\tilde{k}\beta}r = g^{-\tilde{s}\beta+rx+\tilde{k}\beta}r = g^{-\tilde{m}x\beta+rx}r = r \qquad \pmod p$$

□

Acknowledgements

The authors would like to thank Ueli Maurer for helpful remarks and discussions.

References

1. S. Brands: Electronic Cash Systems Based On The Representation Problem In Groups of Prime Order, to appear in *Advances in Cryptology, Crypto '93*.
2. D. Chaum: Blind Signature Systems, *Advances in Cryptology, Crypto '83*, Plenum, p. 153.
3. D. Chaum, A. Fiat, M. Naor: Untraceable Electronic Cash, *Advances in Cryptology, Crypto '88*, LNCS 403, Springer Verlag, pp. 319-327.
4. D. Chaum: Privacy Protected Payment, SMART CARD 2000, Elsevier Science Publishers B.V. (North-Holland), 1989, pp. 69-93.
5. D. Chaum, B. den Boer, E. van Heyst, S. Mjølsnes, A. Steenbeek: Efficient Offline Electronic Checks, *Advances in Cryptology, Eurocrypt '89*, LNCS 434, Springer Verlag, pp. 294-301.
6. D. Chaum, T. Pedersen: Wallet databases with observers, *Advances in Cryptology, Crypto '92*, LNCS 740, Springer Verlag, pp. 89-105.
7. N. Ferguson: Single Term Off-line Coins, *Advances in Cryptology, Eurocrypt '93*, LNCS 765, Springer Verlag, pp. 318-328.
8. NIST FIPS PUB XX, Digital Signature Standard (DSS), National Institute of Standards and Technology, U.S. Department of Commerce, DRAFT, 1993
9. K. Nyberg, R.A. Rueppel: A New Signature Scheme Based on the DSA Giving Message Recovery, *1st ACM Conference on Computer and Communications Security*, November 3-5, Fairfax, Virginia.
10. T. Okamoto, K. Ohta: Universal Electronic Cash, *Advances in Cryptology, Crypto '91*, LNCS 576, Springer Verlag, pp. 324-337.
11. R.L. Rivest, A. Shamir, L. Adleman: A Method for Obtaining Digital Signatures and Public Key Cryptosystems, *Comm. ACM*, **21**, 1978, pp. 120-126.
12. B. Schneier, Applied Cryptography, J. Wiley, 1993.