University of Technology Chemnitz-Zwickau

Department of Computer Science

Theoretical Computer Science
and Information Security

Technical Report

TR-95-11-D

Comment: "Cryptanalysis" of the blind signatures based on the discrete logarithm problem

Patrick Horster · Markus Michels · Holger Petersen

July 1995

Straße der Nationen 62
D-09111 Chemnitz, Germany

Phone: (+49) 371-531-1479
Fax: (+49) 371-531-1810

Comment: "Cryptanalysis" of the blind signatures based on the discrete logarithm problem

Patrick Horster · Markus Michels · Holger Petersen

Theoretical Computer Science and Information Security,
University of Technology Chemnitz-Zwickau,
Straße der Nationen 62, D-09111 Chemnitz, Germany
E-mail: {pho,mmi,hpe}@informatik.tu-chemnitz.de

July 19, 1995

Abstract

In [Harn95], Harn claims, that the signature schemes in [CaPS94] and [HoMP94] are not true blind signatures. In this comment, we prove, that this claim is fortunately totally wrong. His attempt to cryptanalyse the schemes in [CaPS94, HoMP94] is incorrect, as the proposed relationship, which is used to trace the signature by the signer, is an invariant that is satisfied by *any* two pairs of signed messages.

We assume, that the reader is familar with the notation in [Harn95] and the notation of the Meta-blind signature scheme in [HoMP94]. The true anonymity of the signature with respect to the signer has already been proven in [CaPS94] and for the Meta-blind signature scheme in [HoMP94]. In the following theorem, we show, that for *any* two signatures of the signature scheme described in [CaPS94], Harn's checking equation is *always* satisfied. Therefore the blind signature can't be traced by this equation.

Theorem 1: Given large primes p and q, $q|(p-1)$, a generator α of a multiplicative subgroup of order q of $\mathbf{Z}_p$ and a public key $y \in \mathbf{Z}_p$ of order q. Assume, we have two (arbitrary) signed messages (m_i, r_i, s_i) with $\alpha^{s_i} \equiv y^{r_i} \cdot r_i^{m_i} \pmod p$, for $i \in \{1,2\}$, and the two relations $a := m_2 \cdot m_1^{-1} \cdot r_2^{-1} \cdot r_1 \pmod q$ and $b := m_1^{-1} \cdot (s_1 - s_2 \cdot r_1 \cdot r_2^{-1}) \pmod q$. Then the equation (1) holds:

$$r_1 \equiv r_2^a \cdot \alpha^b \pmod p. \qquad (1)$$

is straightforward:

$$\begin{aligned}
r_2^a \cdot \alpha^b \equiv\ & r_2^{m_2 \cdot m_1^{-1} \cdot r_2^{-1} \cdot r_1} \cdot \alpha^{m_1^{-1} \cdot (s_1 - s_2 \cdot r_1 \cdot r_2^{-1})} \\
\equiv\ & (\alpha^{s_2} \cdot y^{-r_2})^{m_1^{-1} \cdot r_2^{-1} \cdot r_1} \cdot \alpha^{s_1 \cdot m_1^{-1} - m_1^{-1} \cdot s_2 \cdot r_1 \cdot r_2^{-1}} \\
\equiv\ & \alpha^{s_2 \cdot m_1^{-1} \cdot r_2^{-1} \cdot r_1} \cdot y^{-r_2 m_1^{-1} \cdot r_2^{-1} \cdot r_1} \cdot (y^{r_1} \cdot r_1^{m_1})^{m_1^{-1}} \cdot \alpha^{-m_1^{-1} \cdot s_2 \cdot r_1 \cdot r_2^{-1}} \\
\equiv\ & y^{-m_1^{-1} \cdot r_1} \cdot (y^{r_1} \cdot r_1^{m_1})^{m_1^{-1}} \\
\equiv\ & r_1 \pmod p
\end{aligned}$$

Furthermore (a, b) is the unique solution for equation (1) for two given valid signed messages (m_1, r_1, s_1) and (m_2, r_2, s_2), because of cardinality reasons: There exist $(q-1)^2$ possibilities for choosing $a, b \in \mathbf{Z}_q^*$. Fixing (m_1, r_1, s_1) we have $(q-1)$ choices of $m_2 \in \mathbf{Z}_q^*$ and $(q-1)$ choices of r_2 in the subgroup generated by α $(r_2 \neq 1)$. The computation of s_2 is uniquely fixed as $s_2 := \log_\alpha(y^{r_2} \cdot r_2^{s_2}) \pmod p$. As a result, it's impossible, to find two different tupels (a_1, b_1) and (a_2, b_2), that satisfy equation (1) for these messages. Together with theorem 1, this proves untraceability. Clearly this result can be generalized for the Meta-blind signature scheme in [HoMP94]. Thus both blind signature schemes remain secure.

Harn further states, that the blind signature scheme proposed in [CaPS94] was the first blind signature scheme based on the discrete logarithm problem. This statement is inaccurate, as e.g. Okamoto published the blind Schnorr signature scheme and other blind signature schemes already in [Okam92].

References

[CaPS94] J.L.Camenisch, J.-M.Piveteau, M.A.Stadler, “Blind signature schemes based on the discrete logarithm problem”, Preprint, presented at the Rump session of Eurocrypt ’94, (1994), 5 pages.

[Harn95] L.Harn, “Cryptanalysis of the blind signatures based on the discrete logarithm problem”, Electronics Letters, Vol. 31, No. 14, (1995), pp. 1136.

[HoMP94] P.Horster, M.Michels, H.Petersen, “Meta-Message recovery and Meta-blind signature schemes based on the discrete logarithm problem and their applications”, Lecture Notes in Computer Science 917, Advances in Cryptology: Proc. Asiacrypt ’94, Berlin: Springer Verlag, 1995, pp. 224 – 237.

[Okam92] T.Okamoto, “Provable secure and practical identification schemes and corresponding signature schemes”, Lecture Notes in Computer Science 740, Advances in Cryptology: Proc. Crypto ’92, Berlin: Springer Verlag, (1993), pp. 31–53.