Centrum voor Wiskunde en Informatica
**REPORT***RAPPORT*

# More on restrictive blind issuing of secret-key certificates in parallel mode

S.A. Brands

Computer Science/Department of Algorithmics and Architecture

**CS-R9534 1995**

Report CS-R9534
ISSN 0169-118X

CWI
P.O. Box 94079
1090 GB Amsterdam
The Netherlands

# More on Restrictive Blind Issuing of Secret-Key Certificates in Parallel Mode

Stefan Brands

*CWI*

*P.O. Box 94079, 1090 GB Amsterdam, The Netherlands*

## Abstract

A minimal variation is proposed of a recently described secret-key certificate scheme that is derived from the Schnorr signature scheme. The issuing protocol of the variation is conjectured to be restrictive blind in parallel mode, motivated by a recent argument of Schoenmakers. The variation demonstrates that the double use of a generator is not problematic in any way, contrary to the belief expressed by Schoenmakers. A more profound argument for the conjectured security in parallel mode is provided, and similar variations are described for secret-key certificates based on Brickell-McCurley signatures. To create some order in the variety of restrictive blind certificate schemes that have been proposed to date, their specific merits and limitations are categorized and discussed.

*AMS Subject Classification (1991)*: 94A60
*CR Subject Classification (1991)*: D.4.6
*Keywords and Phrases*: Cryptography, Certificates.
*Note:* Preliminary version, April 7, 1995.

## 1. Introduction

Since this report is a direct continuation of [9, 10], the reader is referred to those references for motivation and background information.

In [3, 4, 5] generally applicable techniques have been described for designing restrictive blind issuing protocols for secret-key certificates derived from Fiat-Shamir type signatures. There are many essentially equivalent ways to define the certificate verification relations of these restrictive blind secret-key certificate schemes. To prove that a certificate issuing scheme is restrictive blind *in sequential mode*, for an "isolated" receiver, a generally applicable proof technique has been demonstrated in [4, 5]. This proof technique is made possible by the simulatability of certified public keys, a property that is characteristic to secret-key certificate schemes [3]. The importance of provable security for isolated receivers in sequential mode is that it provides solid evidence in support of the conjecture that the restrictive blind issuing protocol at hand is *generally* secure in sequential mode.

Unfortunately, such solid evidence is not known for the security of restrictive blind certificate schemes *in parallel mode*: it seems that one cannot do much better than assess the security of restrictive blind issuing schemes in parallel mode on an ad hoc basis, by submitting them to algebraic attacks. For instance the parallel mode security of the restrictive blind (public-key) certificate scheme in [1] has been conjectured on the basis of an ad hoc assessment.

A conjecture for parallel mode security of an issuing protocol is much more plausible if the security of that protocol in sequential mode can be proven under some reasonable intractability assumption, because this rules out the majority of possible attack strategies, namely those that also apply in sequential mode. Only attacks that are typical for parallel mode have to be assessed, which is a significant advantage: "algebraic" parallel mode attacks are fairly specialized, and one can form a pretty good picture of what they must look like. This observation has been put to good use in [10], where an immunization technique for preventing typical algebraic attacks in parallel mode has been proposed. The immunization technique consists of destroying certain multiplicative relations that are believed to be typical for algebraic attacks in parallel mode [4, 9], by "masking" these multiplicative relations with an additional one-way function in such a way that all the properties of the unmodified schemes are preserved.

Although the immunization technique of [10] is generally applicable, both to RSA and Discrete Log based schemes, it negatively affects notably the on-line efficiency for the receivers. It therefore is worthwhile to assess whether the immunization technique is really required; perhaps there are simple variations of the secret-key certificate schemes of [4] for which parallel mode security can be argued. It will be shown in this report that such variations indeed exist for the Discrete Log based schemes, motivated by a recent argument provided by Schoenmakers [13], but unfortunately do not seem to exist for RSA based schemes.

The organization of this report is as follows. In Section 2 a minimal variation of the Schnorr-based secret-key certificate scheme of [4, 5] is described. This variation demonstrates that the belief expressed by Schoenmakers, namely that the double use of a generator is problematic (see Section 7 of [13]), is false. In fact, there are various alternative definitions of the certificate verification relation that all result in issuing protocols that are believed to be restrictive blind in parallel mode, by the same argument.

The attackers in the algebraic parallel attacks described in [4, 9] can retrieve a certified key pair with an uncorrelated blinding-invariant part by combining powers of

their respective verification relations, and solving relations that are expressed in terms of their respective challenge values and their secret or public keys. The argument of Schoenmakers in essence is that these algebraic attacks should not work for variations in which the relations can be made to be expressed in terms of the respective *responses* instead of in terms of the respective challenges, since the responses cannot be anticipated on by the attackers. Ad hoc assessment of security properties is always a delicate affair, and so it is of great importance that more convincing arguments are provided. A step in this direction is made in Section 3, where a more profound argument than that of Schoenmakers [13] is provided for the conjectured security in parallel mode.

In Section 4 it is shown that there are similar variations for secret-key certificates based on Brickell-McCurley signatures, whose corresponding restrictive blind issuing protocols are believed to be secure in parallel mode on the basis of the same argument; since the Brickell-McCurley identification scheme is known to be witness hiding, the security for the issuer in these schemes is at least as high as that in the Schnorr-based schemes. It is then argued that there are no variations for RSA-based secret-key certificate schemes that are restrictive blind in parallel mode.

A disadvantage of the variants described in Section 2 and Section 4 is that they cannot be used in conjunction with a variety of useful credential techniques, including techniques for implementing framing protection [1], currency exchange [2] and anonymous accounts and electronic checks [6], and for updating and demonstrating predicates of credentials [7]. To bring some structure in the many restrictive blind certificate schemes (and their variations) that have been proposed to date, their specific merits and limitations are discussed in Section 5.

## 2. Secret-Key Certificates Based on the Schnorr Signature Scheme

In view of the following discussion, we will first summarize the particular variation of Schnorr-based secret-key certificates that has been described in detail in [3, 5].

Signer $\mathcal{S}$ generates a public key $(\mathrm{desc}(G_q), g, h, g_1, \mathcal{H}(\cdot))$ and a corresponding secret key $(\log_g h, \log_g g_1)$, denoted by $(x, y)$. Here, $\mathrm{desc}(G_q)$ denotes the polynomial-size description (including the specification of $q$) of a group $G_q$ of prime order $q$ for which polynomial-time algorithms are known to multiply, determine equality of elements, test membership, and to randomly select elements, and for which no feasible algorithms for computing discrete logarithms are known. Furthermore, $g$, $h$ and $g_1$ are elements of $G_q$, and $\mathcal{H}(\cdot)$ is a polynomial-size description of a correlation-free one-way hash-function that maps its inputs to $\mathbb{Z}_{2^t}$ for some appropriate $t$. A secret key of receiver $\mathcal{R}_i$ corresponding to a public key $h_i$ is a pair $(s_{0i}, s_{1i}) \in \mathbb{Z}_q \times \mathbb{Z}_q$ such that $h_i = g_1^{s_{0i}} g^{s_{1i}}$,

and a secret-key certificate of $\mathcal{S}$ on $h_i$ is a pair $(r, c) \in \mathbb{Z}_q \times \mathbb{Z}_{2^t}$ such that the following *certificate verification relation* holds:

$$c = \mathcal{H}(h_i, g^r (h\, h_i)^{-c}).$$

Clearly there are a great many essentially equivalent definitions of the certificate verification relation (as well as of the key pair definition for $\mathcal{R}_i$). It is easy to see that for instance the following alternative definitions of the certificate verification relation all provide the same security in case the corresponding certificates are issued according to a non-interactive issuing protocol, or according to a two-move protocol (which can be designed as in [3]) that prevents the issuer from learning the secret key of $\mathcal{R}_i$:

$$\begin{aligned}
c &= \mathcal{H}(h_i, g^r h^{-c} h_i^{-1}) \\
c &= \mathcal{H}(h_i, (g^r h^{-1})^{1/c} h_i^{-1}) \\
c &= \mathcal{H}(h_i, g^r (h\, h_i)^{-c}) \\
c &= \mathcal{H}(h_i, (g^r (h\, h_i)^{-1})^{1/c}) \\
c &= \mathcal{H}(h_i, (g h_i)^r h^{-c}) \\
c &= \mathcal{H}(h_i, ((g h_i)^r h^{-1})^{1/c}).
\end{aligned}$$

(In the variations where $1/c$ appears in the exponent, $\mathcal{H}(\cdot)$ should not map its inputs to zero.) It will hardly be a surprise that there are many more variations. An example of a variation in which the key pair definition for $\mathcal{R}_i$ is modified is to take $c = \mathcal{H}(h_i, g^r h_i^{-c})$, where $h$ is a representation with respect to, say, $(h, g_1)$ instead of $(g, g_1)$.

For any of these and other variations, a *three-move* issuing protocol can be designed by applying the technique presented in [4, 5] for designing restrictive blind issuing protocols described. However, the exemplary variations in that case do not all provide equivalent security; of the exemplary variations described above, all but the first two are *restrictive* blind for an isolated receiver in sequential mode. For the remaining variations, results similar to those provided in [4, 5] can be proven straightforwardly, by using the proof techniques of these references. In this way the conjectured security of each of these variants of the Schnorr-based restrictive blind certificate issuing schemes in sequential mode can be established.

Although many of the minor variations in the definition of the certificate verification relation result in issuing protocols that are restrictive blind in *sequential mode*, not all of the issuing protocols preserve this property when run in *parallel mode*; see the parallel mode attacks in [4, 9]. Which protocols remain secure in parallel mode and which don't can only be established on an ad hoc basis, by trying out whether they

can be subjected to "algebraic" parallel mode attacks such as those in [4, 9]. The security in parallel mode of one particular variation has recently been conjectured by Schoenmakers [4], based on the observation that the parallel mode attacks described in [4, 9] do not seem to work for this particular variation. This belief stems from the fact that the attacks in [4, 9] for Schoenmakers' variation require the attackers to solve relations that involve the respective *responses* of the issuer, instead of the respective challenges of the attackers.

It will hardly come as a surprise that the observation of Schoenmakers applies also to several other variations, such as for instance the fifth and sixth of the alternative forms described above. Consider for example the fifth of the variations described above; the certificate verification relation

$$c = \mathcal{H}(h_i, g^r (h\, h_i)^{-c})$$

is modified by this variation into

$$c = \mathcal{H}(h_i, (g\, h_i)^r h^{-c}).$$

No further changes are needed. As with all variations, a corresponding three-move issuing protocol can be designed by applying the technique of [4]. Denoting $g_1^{s_{0i}}$ by $h_i$ as in [5], consider the following issuing protocol:

**Step 1.** $\mathcal{S}$ generates at random a number $w \in \mathbb{Z}_q$, and sends $a := g^w$ to $\mathcal{R}_i$.

**Step 2.** $\mathcal{R}_i$ generates at random a number $\alpha \in \mathbb{Z}_q^*$ and two random numbers $t_1, t_2 \in \mathbb{Z}_q$. $\mathcal{R}_i$ computes $h_i' := h_i^\alpha g^{\alpha - 1}$, $c' := \mathcal{H}(h_i', a\,(g h_i)^{t_1} h^{t_2})$, and sends $c := c' + t_2 \bmod q$ to $\mathcal{S}$.

**Step 3.** $\mathcal{S}$ sends $r := (cx + w)\,(y s_{0i} + 1)^{-1} \bmod q$ to $\mathcal{R}_i$.

$\mathcal{R}_i$ accepts if and only if $(g h_i)^r h^{-c} = a$. If this verification holds, $\mathcal{R}_i$ computes $r' := (r + t_1)\,\alpha^{-1} \bmod q$. Note that $(y s_{0i} + 1)^{-1} \bmod q$ in Step 3 can be pre-computed by $\mathcal{S}$, and that $\mathcal{R}_i$ likewise can pre-compute almost all his computations.

As the reader can easily work out for himself by applying the proof techniques of [4], in sequential issuing mode $\mathcal{R}_i$ cannot obtain representations of $h_i'$ with respect to $(g_1, g)$ other than $(\alpha\, s_{0i}, \alpha - 1)$ for random $\alpha$. Note also that, as in [1], the case $\alpha = 0$ can be recognized publicly from $h_i'$, and must be declared invalid.

Contrary to the belief expressed by Schoenmakers [13] the double usage of a generator, as in the variations used in [4, 5], is not problematic. In fact, if we sweep the

occurrence of $g$ in the certificate verification relation $c = \mathcal{H}(h_i, (g\,h_i)^r h^{-c})$ into $h_i$, then the variation described by Schoenmakers has the same certificate verification relation as that described here.

## 3. Security Assessment

The proof techniques that pertain to the particular variations considered in [4, 5] apply straightforward to the variation considered in the preceding section. For this reason the security results for sequential mode are omitted here; they are analogues of those in [4]. The argument presented below for parallel mode security of the issuing protocol for the considered variation improves on that of Schoenmakers [13].

As in [4], we will only consider "algebraic" attacks on the parallel version of the issuing protocol. For the sake of simplicity we will furthermore restrict ourselves to two parallel executions of the issuing protocol, each with respect to a different blinding-invariant number; the argument can easily be generalized to any number of attackers.

To facilitate comparison with the security argument provided by Schoenmakers [13], we will consider the verification relation

$$c = \mathcal{H}(h_i, h_i^r h^{-c})$$

instead of $c = \mathcal{H}(h_i, (g\,h_i)^r h^{-c})$; it is easy to provide the corresponding three-move issuing protocol, applying the technique of [4], and it is therefore omitted here. We will let $s_{0i}$ and $s_{0j} \neq s_{0i} \bmod q$ denote the presumed blinding-invariant parts of the two receivers. After the two executions of the issuing protocol, the attackers should be able to compute a representation $(s, t)$ of a public key unequal to 1, and a secret-key certificate $(c, r)$ on that public key, such that

$$s \neq t\,s_{0i} \bmod q, \quad s \neq t\,s_{0j} \bmod q.$$

It will now be argued that this task is infeasible, *assuming sequential mode security.* In other words, it will be argued that the blinding-invariant predicate can be recovered from the blinded secret key $(s, t)$ according to $s/t \bmod q$, when the public key is not equal to 1.

The following result plays a vital role in the argument.

**Proposition 1** *If the Schnorr identification scheme is witness hiding, then no conspiracy in the defined secret-key certificate scheme can compute with non-negligible probability of success a non-trivial representation of* 1 *with respect to* $(g, g_1, h)$*, even when polynomially many executions of the issuing protocol are performed in parallel.*

**Sketch of proof** Consider the following algorithm $A$, that takes as input a randomly chosen public key $(\mathrm{desc}(G_q), g_0, h_0, \mathcal{H}(\cdot))$ of the honest prover in the blind Schnorr signature protocol (see [5]). In its first step, $A$ randomly performs one of the following two simulations of the public key for $\mathcal{S}$ (where each of the two alternatives has probability weight, say, 1/2):

- Set $g := g_0$, $g_1 := h_0$. Generate at random an element $x \in \mathbb{Z}_q$, and set $h := g^x$. The simulated public key for $\mathcal{S}$ is $(\mathrm{desc}(G_q), g, h, g_1, \mathcal{H}(\cdot))$.
- Set $g := g_0$, $h := h_0$. Generate at random an element $y \in \mathbb{Z}_q$, and set $g_1 := g^y$. The simulated public key for $\mathcal{S}$ is $(\mathrm{desc}(G_q), g, h, g_1, \mathcal{H}(\cdot))$.

Next, using the simulated public key for $\mathcal{S}$, $A$ simulates for each receiver the actions that $\mathcal{S}$ would perform in the issuing protocol, by making use of the prover in the blind Schnorr signature scheme. Regardless of how the public key for $\mathcal{S}$ has been simulated, this can easily be done with identical probability distribution (*cf.* Lemma 3 of [4] and Lemma 5 of [5], technical report versions).

Suppose that, after polynomially many executions of the issuing protocol, the conspiracy outputs with non-negligible probability of success a non-trivial representation of 1 with respect to $(g, g_1, h)$. Denoting this representation by $(a_1, a_2, a_3)$, two cases can be discerned:

1. $a_3 = 0 \bmod q$. Since the simulated probability distribution in the issuing protocol is independent of the particular way in which $A$ simulated the public key for $\mathcal{S}$, with probability 1/2 did $A$ apply the first simulation method. In that case, $A$ can output the witness of the prover in the blind Schnorr signature protocol, because $\log_{g_0} h_0 = \log_g g_1 = -a_1/a_2 \bmod q$.
2. $a_3 \neq 0 \bmod q$. Since the simulated probability distribution in the issuing protocol is independent of the particular way in which $A$ simulated the public key for $\mathcal{S}$, with probability 1/2 did $A$ apply the second simulation method. In that case, $A$ can output the witness of the prover in the blind Schnorr signature protocol, because $1 = g^{a_1} g_1^{a_2} h^{a_3} = g^{a_1 + y a_2} h^{a_3}$ and so $\log_{g_0} h_0 = \log_g h = -(a_1 + y a_2)/a_3 \bmod q$.

Taking both cases into consideration, it follows that the probability that $A$ outputs the secret key of the prover in the blind Schnorr signature scheme is non-negligible. Since the blind Schnorr signature protocol is witness hiding if the Schnorr identification scheme is witness hiding, this contradicts the assumption. □

Our first observation is that knowing $(c, r)$ such that $c = \mathcal{H}(g_1^s g^t, (g_1^s g^t)^r h^{-c})$ is equivalent to knowing $(a, r)$ such that $(g_1^s g^t)^r h^{-\mathcal{H}(g_1^s g^t, a)} = a$; the proof is trivial and hence omitted here. This allows us to specify the target of the attack as being a triple $(s, t), g_1^s g^t, (a, r)$ such that $(g_1^s g^t)^r h^{-c} = a$, where $c$ denotes $\mathcal{H}(g_1^s g^t, a)$.


Two parallel mode attacks are known, the first of which has been described in [4] (see also [5]) and the second in [9], and it will be assumed that these are the only possible types of attack. Because the attackers know their respective blinding-invariant numbers in advance, it follows that the first of these attacks is the most powerful. In particular, *if it is feasible to make parameter choices that make the second attack work then it is feasible to make parameter choices that make the first attack work.* It therefore suffices to consider only the first type of attack.

Raising the verification relations for each of the two protocol executions to a power $l_i$ and $l_j$, respectively, and multiplying the results, we obtain

$$\left.\begin{array}{l}(g_1^{s_{0i}} g)^{l_i r_i} h^{-l_i c_i} = a_i^{l_i} \\ (g_1^{s_{0j}} g)^{l_j r_j} h^{-l_j c_j} = a_j^{l_j}\end{array}\right\} \Rightarrow g_1^{s_{0i} l_i r_i + s_{0j} l_j r_j} g^{l_i r_i + l_j r_j} h^{-(l_i c_i + l_j c_j)} = a_i^{l_i} a_j^{l_j}.$$

Following the attack of [4, 5], the attackers must determine a pair $s, t$, and numbers $l_i$, $l_j$, $c_i$, $c_j$ for which the information provided by the issuer can be combined into a pair $(a, r)$ such that

$$g_1^{sr} g^{tr} h^{-c} = a,$$

where $c = \mathcal{H}(g_1^s g^t, a)$.

Assume first that the attackers compute $a := a_i^{l_i} a_j^{l_j}$, for $l_i, l_j \neq 0 \bmod q$ that need not be explicitly known at the time $c_i$ and $c_j$ have to be provided. (Note that $l_i = 0 \bmod q$ or $l_j = 0 \bmod q$ can be excluded because these choices result in sequential mode attacks.) They then must ensure that

$$g_1^{s_{0i} l_i r_i + s_{0j} l_j r_j} g^{l_i r_i + l_j r_j} h^{-(l_i c_i + l_j c_j)} = g_1^{sr} g^{tr} h^{-c}.$$

Assuming furthermore that $l_i$ and $l_j$ will be computable by the attackers once the attack has been completed successfully (a plausible assumption given the algebraic nature of the attack), it follows from Proposition 1 that the attackers have to (implicitly) solve

$$s_{0i} l_i r_i + s_{0j} l_j r_j = sr \bmod q, \quad l_i r_i + l_j r_j = tr \bmod q, \quad l_i c_i + l_j c_j = c \bmod q$$

for $(l_i, l_j, s, t, c_i, c_j)$ and $r$; other assignments for the exponents imply the ability of the attackers to compute a non-trivial representation of 1 with respect to $(g, g_1, h)$. According to the algebraic attack in [4] the implicit choices for $(l_i, l_j, s, t, c_i, c_j)$ have to be made *before* $r_i$ and $r_j$ are provided; only $r$ may be computed afterwards.

We now get to the heart of our argument. We concentrate on the first two relations, $s_{0i} l_i r_i + s_{0j} l_j r_j = sr \bmod q$ and $l_i r_i + l_j r_j = tr \bmod q$. Since $r$ can be computed by the attackers after $r_i$ and $r_j$ have been received, it seems at first sight that there are many workable choices for $l_i, l_j, s, t$. This is not true, since the attackers in fact have to solve, in terms of $l_i, l_j, s, t$, a single relation *that does not involve $r$ but does involve $r_i$ and $r_j$*. More precisely, two cases can be distinguished:

- $t = 0 \bmod q$. In that case the equality $l_i r_i + l_j r_j = 0 \bmod q$ must hold for the choices for $l_i, l_j$ of the attackers. Since $r_i, r_j$ cannot be anticipated, the only feasible non-zero choices seem to be to take $l_i = A r_i^{-1} \bmod q$ and $l_j = -A r_j^{-1} \bmod q$, or $l_i = A r_j \bmod q$ and $l_j = -A r_i \bmod q$ for some suitable constant $A$.

- $t \neq 0 \bmod q$. Multiplying both sides of $l_i r_i + l_j r_j = tr \bmod q$ by $s/t \bmod q$, and subtracting from $s_{0i} l_i r_i + s_{0j} l_j r_j = sr \bmod q$, we get

  $$(l_i (s_{0i} - s/t)) r_i + (l_j (s_{0j} - s/t)) r_j = 0 \bmod q.$$

  Because $r_i$ and $r_j$ cannot be anticipated on, and because $s/t \bmod q$ cannot be equal to both $s_{0i}$ and $s_{0j}$, the only workable non-zero choices for $l_i, l_j, s, t$ seem to be to take $l_i = A_i r_i^{-1} \bmod q$ and $l_j = A_j r_j^{-1} \bmod q$, or $l_i = A_i r_j \bmod q$ and $l_j = A_j r_i \bmod q$ for some suitable constants $A_i$ and $A_j$ that can depend on $s$ and $t$.

Now, it is not immediately clear (although it seems to be true) that the attackers cannot compute $a := a_i^{l_i} a_j^{l_j}$ for such a choice for $l_i$, $l_j$, because $l_i$ and $l_j$ need not be known explicitly for this computation (the attackers know for instance that $a_i^{1/r_i} = (g_1^{s_{0i}} g)\, h^{-c_i/r_i}$). Instead, we focus on the third relation, $l_i c_i + l_j c_j = c \bmod q$. Even if $a$ could be computed, the fact that $c$ is a one-way correlation-free function of $a$ implies that its value cannot be expressed in terms of $r_i$ and $r_j$. Consequently, $l_i c_i + l_j c_j = c \bmod q$ can only be solved for values $c_i$ and $c_j$ that are expressed in terms of $r_i, r_j$. Because $c_i$ and $c_j$ have to be provided by the attackers before $r_i$ and $r_j$ become known, workable choices for $l_i$ and $l_j$ should be infeasible.

We assumed in this argument that the attackers compute $a := a_i^{l_i} a_j^{l_j}$. The information contained in

$$g_1^{s_{0i} l_i r_i + s_{0j} l_j r_j} g^{l_i r_i + l_j r_j} h^{-(l_i c_i + l_j c_j)} = a_i^{l_i} a_j^{l_j}$$

can be combined into

$$g_1^{sr} g^{tr} h^{-c} = a$$

in a more general way. The most general form seems to take

$$a := a_i^{l_i} a_j^{l_j} g_1^{\alpha} g^{\beta} h^{\gamma}$$

for smart choices for $\alpha, \beta, \gamma$. Applying Proposition 1, we can derive as before three relations. From the first two of these we can again derive one relation that involves $r_i$ and $r_j$ but not $r$, and that must be solved (implicitly) for $l_i, l_j, s, t$. The only way to arrive at a relation in which $l_i$ and $l_j$ are not expressions in terms of $r_i, r_j$ (for which the above argument applies), seems to be by choosing $\alpha, \beta$ such that $s_{0i} l_i r_i + s_{0j} l_j r_j + \alpha = sr \bmod q$ and $l_i r_i + l_j r_j + \beta = tr \bmod q$ are linearly dependent in $r$; in that case $r$ cannot be made to drop out of the equations. Such choices for $\alpha, \beta$ seem to require expressions in terms of $r_i$ and $r_j$ that cannot be anticipated on; whether it is indeed true that there are no implicit choices for $\alpha, \beta, s, t$ for which $g_1^s g^t$, $g_1^{\alpha}$ and $g^{\beta}$ can be computed before $r_i, r_j$ become known can only be conjectured.

## 4. Secret-Key Certificates Based on Other Signature Schemes

In light of the fact that the presumed security of certain variations in parallel mode is dependent on the assumption that the underlying identification scheme is witness hiding, it may be worthwhile to assess whether there are variations for secret-key certificates that are derived from Brickell-McCurley signatures [11]. The following variant is at least as secure as the variant of Section 2.

Signer $\mathcal{S}$ generates a public key $(p, g, h, g_1, \mathcal{H}(\cdot))$, with $h = g^x$, $g_1 = g^y$ for a randomly chosen secret key $(x, y) \in \mathbb{Z}_{p-1} \times \mathbb{Z}_{p-1}$. Here, $p$ is a prime number such that $p - 1$ is a

multiple of two distinct primes $q$ and $q'$ of roughly equal size. Furthermore, $g$, $h$ and $g_1$ are elements of order $q$ in $\mathbb{Z}_p^*$, and $\mathcal{H}(\cdot)$ is a polynomial-size description of a correlation-free one-way hash-function that maps its inputs to $\mathbb{Z}_{2^t}$ for some appropriate $t$. A secret key of $\mathcal{R}_i$ corresponding to a public key $h_i \neq 1$ is a pair $(s_{0i}, s_{1i}) \in \mathbb{Z}_{p-1} \times \mathbb{Z}_{p-1}$ such that $h_i = g_1^{s_{0i}} g^{s_{1i}}$, and a secret-key certificate of $\mathcal{S}$ on $h_i$ is a pair $(r, c) \in \mathbb{Z}_{p-1} \times \mathbb{Z}_{2^t}$ such that

$$c = \mathcal{H}(h_i, h_i^r h^{-c}).$$

Denoting the not-yet-blinded public key $g_1^{s_{0i}} g$ by $h_i$, consider the following issuing protocol:

**Step 1.** $\mathcal{S}$ generates at random a number $w \in \mathbb{Z}_{p-1}$, and sends $a := g^w$ to $\mathcal{R}_i$. (Note that $\mathcal{S}$ can compute $a$ as $a := g^{w \bmod q}$ in case it saves $q$ as part of its public key.)

**Step 2.** $\mathcal{R}_i$ generates at random a number $\alpha \in \mathbb{Z}_{p-1} \setminus \{0\}$ and two random numbers $t_1, t_2 \in \mathbb{Z}_{p-1}$. $\mathcal{R}_i$ computes $h_i' := h_i^\alpha$, $c' := \mathcal{H}(h_i', a\, h_i^{t_1} h^{t_2})$, and sends $c := c' + t_2 \bmod p-1$ to $\mathcal{S}$.

**Step 3.** $\mathcal{S}$ sends $r := (cx + w)\,(ys_{0i} + 1)^{-1} \bmod p-1$ to $\mathcal{R}_i$.

$\mathcal{R}_i$ accepts if and only if $h_i^r h^{-c} = a$. If this verification holds, $\mathcal{R}_i$ computes $r' := (r + t_1)\,\alpha^{-1} \bmod p-1$. As before, it can be argued that the blinding-invariant part of a secret key $(s, t)$ is defined by $s/t \bmod p-1$.

Similar variations also exist for secret-key certificates based on Okamoto's Discrete-Log based signature scheme; one such variation has been sketched by Schoenmakers [13]. Oddly enough, the three-move issuing protocols of similar variations based on Fiat-Shamir type signature schemes in RSA groups, including the schemes of Guillou-Quisquater, Fiat-Shamir, Feige-Fiat-Shamir, and Okamoto, are not restrictive blind in parallel mode; they in fact are not even restrictive blind in sequential mode. Consider for instance secret-key certificates derived from the Guillou-Quisquater signature scheme. The particular variation described in detail in [4] is as follows: Signer $\mathcal{S}$ generates a public key $(n, v, h, g, \mathcal{H}(\cdot))$ and a corresponding secret key $(h^{1/v} \bmod n, g^{1/v} \bmod n)$, denoted by $(x, y)$. Here, $n$ denotes the product of two distinct prime numbers; $v$ is a prime number that is co-prime with $\varphi(n)$; $h$ and $g$ are elements of $\mathbb{Z}_n^*$; and $\mathcal{H}(\cdot)$ is a polynomial-size description of a correlation-free one-way hash-function that maps its inputs to $\mathbb{Z}_{2^t}$ for some appropriate $t$. A secret key of $\mathcal{R}_i$ corresponding to a public key $h_i$ is a pair $(s_{0i}, s_{1i}) \in \mathbb{Z}_v \times \mathbb{Z}_n^*$ such that $h_i = g^{s_{0i}} s_{1i}^v$, and a secret-key certificate of $\mathcal{S}$ on $h_i$ is a pair $(r, c) \in \mathbb{Z}_n^* \times \mathbb{Z}_{2^t}$ such that $c = \mathcal{H}(h_i, r^v (h\, h_i)^{-c})$. Now consider the

variation in which

$$c = \mathcal{H}(h_i, (h_i\, r)^v h^{-c});$$

in the corresponding three-move issuing protocol, designed according to the techniques of [4], $\mathcal{R}_i$ can multiply arbitrary powers of $g$, as well as arbitrary $v$-th powers, into $h_i$. Similar disappointing results hold for other conceivable RSA-based variations as well. The only approach currently available for designing restrictive blind issuing schemes for the RSA-based schemes is to apply the *immunization* method described in [10].

## 5. General Applicability

Various restrictive blind secret-key certificate schemes have been proposed to this date. For comparison, a summary is presented below of the peculiarities of each.

We will distinguish between RSA and Discrete Log based schemes. For instance, in the Guillou-Quisquater based schemes [7] a representation of a public key $h_i$ with respect to a basis $(g_1, \ldots, g_k; v) \in \mathbb{Z}_n^* \times \cdots \times \mathbb{Z}_n^* \times \mathbb{Z}_{\lambda(n)}$ is a tuple $(a_1, \ldots, a_k; a_{k+1}) \in \mathbb{Z}_v \times \cdots \mathbb{Z}_v \times \mathbb{Z}_n^*$ such that $h_i = g_1^{a_1} \cdots g_k^{a_k} a_{k+1}^v \bmod n$; and in the Schnorr based schemes a representation of a public key $h_i$ with respect to a basis $(g_1, \ldots, g_k) \in G_q \times \cdots \times G_q$ is a tuple $(a_1, \ldots, a_k) \in \mathbb{Z}_q \times \cdots \times \mathbb{Z}_q$ such that $h_i = g_1^{a_1} \cdots g_k^{a_k}$.

For both RSA based schemes and Discrete-Log based schemes one can consider a first blinding mode in which $h_i$ can be blinded, for random $\alpha$ in $\mathbb{Z}_v$ (RSA) or in $\mathbb{Z}_q$ (Discrete Log), to $h_i' = h_i^\alpha \bmod n$ and $h_i' = h_i^\alpha$, respectively, and a second blinding mode in which the receiver can obtain $h_i' = h_i \alpha^v \bmod n$ (RSA) or $h_i' = h_i g^\alpha$ (Discrete Log). In issuing protocols that allow the receiver to blind according to the combination of the two modes, the issuer can easily enforce one of them by a suitable choice of the basis tuple that must be used in executions of a successive showing protocol.

One can furthermore consider the case in which the issuer needs to know information about the not-yet-blinded secret key of the receiver, typically $h_i^{1/v} \bmod n$ in the RSA situation or $\log_g h_i$ in the Discrete Log based systems, and the case in which the issuer does not need to know such information. Since RSA has a trapdoor (the factorization of the modulus), the first case never needs to apply to the RSA-based schemes.

Based on these characteristics, the various types of restrictive blind certificate issuing protocols known to date can be categorized as follows:

- The restrictive blind certificate issuing scheme in [1, 8]. This is the only one known thus far for issuing *public-key* certificates. It is Discrete Log based, and allows both modes of blinding: for a public key of the form $h_i = g_1^{a_1} \cdots g_k^{a_k}$, the issuer can ensure either that $h_i$ can be blinded at best to $h_i' = h_i^\alpha$ or to

$h_i' = h_i g^\alpha$ (or the combination of the two methods). In general, the first mode can be enforced by working in successive showing protocols with representations of $h_i'$ with respect to bases in which $g$ does not appear; and the second mode can be enforced by setting, say, $a_1$ equal to 1 and working in successive showing protocols with representations of $h_i'/g_1$ with respect to bases in which $g_1$ does not appear.

Since the issuer does not need to know any information about the not-yet-blinded secret key of the receiver in order to perform the issuing protocol, this scheme has the most general applicability of all known restrictive blind issuing schemes. On the downside, the security of the issuing protocol is not well understood even in sequential mode and no RSA based analogues are known (which were the main causes for the development of secret-key certificates), and the on-line computational requirement for the receiver in the issuing protocol equals several hundreds of modular multiplications.

- The RSA-based schemes that can be developed by the techniques of [4, 10] allow the preferable second mode of blinding. The issuer does not need to be provided with information about the not-yet-blinded secret key of the receiver in order to perform the issuing protocol, since use can be made of the factorization of the modulus. The sequential mode security of all variants can be proved for an isolated receiver, assuming merely a plausible intractability assumption. The variants that are secure only in sequential mode require the receiver to perform merely a single on-line multiplication (neglecting a small addition and computation of a hashvalue). On the downside, the immunized variants [10], which are secure also in parallel mode, require the receiver in the issuing protocol to perform several hundreds of on-line modular multiplications.

- The Discrete-Log based schemes that can be developed by the techniques of [4, 10] allow the preferable second mode of blinding. There are also variants that allow the first mode of blinding, as shown in [13] and this report. The sequential mode security of all variants can be proved for an isolated receiver, assuming merely a plausible intractability assumption.

  The variants that are secure in parallel mode, and that require the receiver to perform merely a single on-line multiplication, only allow the first mode of blinding; the variants that are secure in parallel mode and allow the preferable second mode of blinding (namely those that are the result of applying the immunization technique of [10]) require the receiver in the issuing protocol to perform several

hundreds of on-line modular multiplications; and the variants that require the receiver to perform merely a single on-line multiplication and allow the second blinding mode are only secure in sequential mode.

A disadvantage of all schemes is that the issuer must know certain information about the not-yet-blinded secret key of the receiver, typically $\log_g h_i$, in order to be able to perform the issuing protocol. It is not known whether there is a *practical* protocol that allows the receiver and the issuer to compute this information together in such a way that neither the issuer nor the receiver leaks additional information about its secret key. (The alternative of using a trusted party that must know the secret key of the issuer is highly undesirable.) More generally, it is not known whether there is a practical protocol which allows two parties, that both know a vector over $\mathbb{Z}_q$, to determine the standard inner product of the vectors without either party leaking additional information to the other party.

For both RSA-based schemes and Discrete Log based schemes a variety of credential showing and transferring techniques exists [7]; the off-line electronic cash techniques developed in [1, 2, 5, 8] are special cases of these techniques. Each of the various schemes has its own merits, and the choice for one particular scheme will in general depend on the application at hand. For instance, for the applicability of the updating technique the issuer should not need to know information about the not-yet-blinded secret key of the receiver, and for the techniques for demonstrating predicates of credentials (single values, NOT, OR, AND, linear relations, ...) in general the issuer should be able to enforce the second blinding mode. To gain some more appreciation for this, it may help to study the following examples.

*Example 1.* In the credential mechanism described in [7], a special authority issues digital pseudonyms by performing a restrictive blind certificate issuing protocol. The issued public keys serve as pseudonyms, and the pseudonyms of one individual are all related because they have the same blinding-invariant part of the secret key. When the second mode of blinding is used, a pseudonym of an individual $i$ at an organization $j$ is a public key $h_{ij} = g^{s_i} r_{ij}^v \bmod n$ (RSA) or $h_{ij} = g_1^{s_i} g^{r_{ij}}$ (Discrete Log); the $r_{ij}$'s make the pseudonyms unconditionally unlinkable. (The issuer could instead use an issuing protocol in which the first mode of blinding is possible, but then the general credential showing techniques of [7] cannot be used.) To establish a pseudonym with an organization, the individual must show along with the public key the issued certificate of the special authority (and perform a proof of knowledge of a secret key, in case of secret-key certificates). To give out a credential to individual $i$, organization $j$ computes

a certificate on a blinded form of the pseudonym of $i$ with $j$. This certificate must be recognizable by other parties as corresponding to that organization (unless one central facility computes all signatures). To ensure that $i$ can only transfer a credential to one of his own pseudonyms (which need not be known at credential issuing time), credential issuing must also be performed by means of a restrictive blind issuing protocol. Note that a pseudonym can be seen as a special type of credential.

If we use the Discrete-Log based restrictive blind issuing protocol of [1, 8] for credential issuing, then each organization can issue its own credentials *without assistance of a central facility*. Hereto, the public key of organization $j$ comprises a unique generator $h_j = g^{x_j}$, preferably certified by a special authority, which performs the same function as $h$ in [1]. All the credentials of organization $j$ that are issued to individual $i$ can be maintained and *updated* in the same number, using the techniques of [7].

With the RSA-based secret-key certificate schemes, use can be made of the fact that the issuer may know the factorization of the modulus (and so does not need to know information about issued secret keys). In this way the techniques for maintaining and updating credentials can be realized, in the same way as when the scheme of [1] is used, at one cost: for security all the credential issuing must be performed by a central facility that knows the factorization of the modulus (much as in [12]). This need not be much of a drawback at all, considering that the public key, in which an individual maintains his credentials, in general has to be re-blinded once it has been shown, in order to maintain unlinkability between pseudonyms.

If no use is made of knowledge of the factorization, or when the Discrete-Log based secret-key certificate schemes are used (for which no trapdoor information for the issuer is known), then credential issuing can only be performed using a protocol for determining inner products; as mentioned, no practical such protocol is known.

*Example 2.* Consider in an off-line electronic cash system the encoding of values, that may not become known to the issuer, into the blinding-invariant part of the secret key. This is for instance required in the method for framing protection described in [1], and in the method for anonymous accounts described in [6]. The Discrete-Log based scheme of [1, 8] can be used because the issuer in that scheme does not need to know anything about the secret keys of issued triples. Likewise, the RSA-based certificate schemes can be used for this purpose, since we can let the bank know the trapdoor information (although it must then be ensured that this does not reveal the particular secret key known by the receiver, which can be done by ensuring that there are many secret keys corresponding to the same public key). However, none of the Discrete-Log

based secret-key certificate schemes are suitable (unless we can find a practical protocol for determining inner products).

*Example 3.* Consider in off-line electronic cash systems the encoding into coins or checks of additional fixed values known to the bank (such as exchange rates, expiration dates, check denominations, and so on), that have to be released at least in part in the payment protocol (see [2, 6, 7]). If a great many values can be taken on, then it is impractical to let the bank use a different public key for each possible value; the values will therefore have to be encoded by the bank into the blinding-invariant part of the issued secret keys. Because the identity of account holders has to be encoded independently into the issued coins, the issuing protocol should allow (and enforce) the second mode of blinding; certificate issuing schemes that enable only the first mode of blinding are unsuitable in general (*cf.* the check extension in [1], extended pre-print).

## 6. Conclusion

It seems that one cannot improve much on the argument for parallel mode security that has been provided in Section 3. More generally no reductions for the parallel mode security of any of the restrictive blind certificate schemes proposed to date are known. It is an open problem to design a restrictive blind signature scheme whose security in parallel mode can be proven, at least to a great extent, with respect to a plausible intractability assumption.

## References

1. Brands, S., "Untraceable Off-Line Cash in Wallet with Observers," Advances in Cryptology – CRYPTO '93, Lecture Notes in Computer Science, no. 773, Springer-Verlag, pp. 302–318. An extended pre-print appeared as: "An efficient off-line electronic cash system based on the representation problem," Centrum voor Wiskunde en Informatica (CWI), Report CS-R9323, March 1993. Available by anonymous ftp from: ftp.cwi.nl:/pub/CWIreports/AA/CS-R9323.ps.Z.
2. Brands, S., "Off-line Cash Transfer by Smart Cards," Proceedings of the First Smart Card Research and Advanced Application Conference, Lille (France), Oct. 1994, pp. 101–117. See also: Centrum voor Wiskunde en Informatica (CWI), Report CS-R9455, September 1994. Available by anonymous ftp from: ftp.cwi.nl:/pub/CWIreports/AA/CS-R9455.ps.Z.
3. Brands, S., manuscript (1993) part (i): "Secret-Key Certificates," Centrum voor Wiskunde en Informatica (CWI), Report CS-R9510, February 1995. Available by anonymous ftp from: ftp.cwi.nl:/pub/CWIreports/AA/CS-R9510.ps.Z.

4. Brands, S., manuscript (1993) part (ii): "Restrictive Blinding of Secret-Key Certificates," Centrum voor Wiskunde en Informatica (CWI), Report CS-R9509, February 1995. Available by anonymous ftp from: ftp.cwi.nl:/pub/CWIreports/AA/CS-R9509.ps.Z. Extended abstract in: Advances in Cryptology – EUROCRYPT '95, Lecture Notes in Computer Science, Springer-Verlag.

5. Brands, S., manuscript (1993) part (iii): "Off-Line Electronic Cash Based on Secret-Key Certificates," Centrum voor Wiskunde en Informatica (CWI), Report CS-R9506, January 1995. Available by anonymous ftp from: ftp.cwi.nl:/pub/CWIreports/AA/CS-R9506.ps.Z. See also: Proc. of the Second International Symposium of Latin American Theoretical Informatics (LATIN '95), Valparaíso, Chili, April 3–7, 1995.

6. Brands, S., manuscript (1993) part (iv):"Extensions of Off-Line Cash," to appear.

7. Brands, S., manuscript (1993) part (v): "Privacy-protecting Digital Credentials Based on Restrictive Blinding," to appear.

8. Brands, S., "Electronic Cash on the Internet," Proceedings of the Internet Society 1995 Symposium on Network and Distributed System Security, San Diego, California, Februari 16-17, 1995.

9. Brands, S., "A Note on Parallel Executions of Restrictive Blind Issuing Protocols for Secret-Key Certificates," Centrum voor Wiskunde en Informatica (CWI), Report CS-R9519, March 1995. Available by anonymous ftp from: ftp.cwi.nl:/pub/CWIreports/AA/CS-R9519.ps.Z.

10. Brands, S., "Restrictive Blind Issuing of Secret-Key Certificates in Parallel Mode," Technical report, Centrum voor Wiskunde en Informatica (CWI), March 30, 1995. (Report number not yet available.)

11. Brickell, E., McCurley, K., "An Interactive Identification Scheme Based on Discrete Logarithms and Factoring," Journal of Cryptology, Vol. 5, No. 1 (1992), pp. 29–39.

12. Chaum, D., Evertse, J. H., "A secure and privacy-protecting protocol for transmitting personal information between organizations," Advances in Cryptology – CRYPTO '86, Lecture Notes in Computer Science, Springer-Verlag 1986, pp. 118-168.

13. Schoenmakers, B., "An Efficient Electronic Payment System Withstanding Parallel Attacks," Technical report, Centrum voor Wiskunde en Informatica (CWI), March 31, 1995. (Report number not yet available.)