Centrum voor Wiskunde en Informatica
REPORT*RAPPORT*

Restrictive blind issuing of secret-key certificates in parallel mode

S.A. Brands

Computer Science/Department of Algorithmics and Architecture

CS-R9523 1995

Report CS-R9523
ISSN 0169-118X

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

Restrictive Blind Issuing of Secret-Key Certificates in Parallel Mode

Stefan Brands

CWI

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

Abstract

Recently a class of secret-key certificate issuing protocols has been proposed that is believed to be restrictive blind when run in sequential mode. In this report an immunization technique is proposed for modifying these secret-key certificate issuing protocols in order to make them restrictive blind even when run in parallel mode. All the proofs of correctness for the underlying, unmodified protocols are fully preserved under the modification, as is their applicability to privacy-protecting mechanisms for value transport.

AMS Subject Classification (1991): 94A60
CR Subject Classification (1991): D.4.6
Keywords and Phrases: Cryptography, Certificates.
Note: Preliminary report, March 30, 1995.

1. Introduction

For highly demanding transaction environments it is desirable to have certificate issuing protocols that are secure even when run in parallel. This allows, for instance, the issuing to be performed by distributed agents without needing central coordination between these agents.

Recently a generally applicable technique [4] has been described for designing restrictive blind issuing protocols [1] for a certain type of secret-key certificates [3], and it has been shown [4, 6] that the resulting issuing protocols should not be run in parallel because that would enable an attack in which completely blinded triples can be retrieved. In this report an immunization technique is proposed for modifying these issuing protocols such that they are restrictive blind even in parallel mode.

The new immunization technique preserves all the correctness proofs that have been provided [4] for the (unmodified) issuing protocols. In fact, if the one-way function, $f(\cdot)$, that is introduced by this technique is broken then we are back in the situation of the unmodified protocols. Since the immunization technique does not change the definition of what constitutes a key pair for a receiver, but only the definition of what

constitutes a certificate on a public key, the new issuing protocols can be used in privacy-protecting mechanisms for signature transport in exactly the same way as the unmodified issuing protocols [1, 2, 5].

2. The Immunization Technique

In each of the secret-key certificate issuing protocols provided in [4], the signer $\mathcal{S}$ starts by sending to the receiver $\mathcal{R}_i$ some "initial" information, a; following this, $\mathcal{R}_i$ blinds its public key and computes a challenge number that it sends to $\mathcal{S}$; $\mathcal{S}$ then computes a response which it sends to $\mathcal{R}_i$; and, finally, $\mathcal{R}_i$ verifies the correctness of the response by using the public key of $\mathcal{S}$, and corrects the response to obtain the blinded certificate on the blinded public key.

These issuing protocols should not generally be performed in parallel [4, 6], since that would allow an adversary to retrieve a completely blinded triple by engaging in two parallel executions of the issuing protocol, each of which involves a different blinding-invariant number. This unfortunate situation is due to the fact that certain algebraic relations (in particular, multiplicative relations), pertaining to such parallel executions of the issuing protocol, can be exploited to algebraically combine the respective certificate verification relations into a new one, with a new "blinding-invariant" number.

To enable $\mathcal{S}$ to perform executions of any of these issuing protocols in parallel, without any restrictions, the immunization technique proposed in this report can be used to immunize the issuing protocols against algebraic attacks in parallel mode. Informally, the immunization technique amounts to letting $\mathcal{S}$ send $f(a)$, instead of a, in its first transmission; accordingly we must correct for this in the definition of the certificates, and in the issuing protocol. Here, $f(\cdot)$ is a function (actually, a family of functions) that meets the following two requirements:

1. it is easy to compute $f(ab)$ from $f(a)$ and b; and
2. it is unfeasible to compute $f(a^{\alpha}b^{\beta})$ from $f(a)$ and $f(b)$, for known non-trivial α, β.

For convenience we will take $f(\cdot)$ to be one-to-one; it can then instantly be seen that the security of the immunized protocols will reduce to that of their underlying, unmodified counterparts in case $f(\cdot)$ becomes easy to invert. It will be clear from studying the immunization technique described below that this property can easily be relaxed.

Since a, b in this specification are generated from some mathematical group, such as the multiplicative group $\mathbb{Z}_n^*$ of integers modulo a composite n that is the product of at least two large primes, or the multiplicative group of integers modulo a large prime p, the product ab in $f(ab)$ must be the group product. Note that the domain of $f(\cdot)$ is the group in which a, b reside.

The first of the two requirements for $f(\cdot)$ ensures that receivers still can retrieve public keys and corresponding certificates in a perfectly blinded manner, in effect in exactly the same manner as in the unmodified issuing protocols [4], while the second condition prevents attacks in which multiplicative relations are exploited between the initial information provided in different executions of the issuing protocol.

The requirement for $f(\cdot)$, and how to apply the immunization technique, are best motivated by describing some examples. For this reason we will now take a look at how to apply the immunization technique to two different secret-key certificate issuing protocols, one RSA-based and one Discrete Log-based. For the sake of explicitness we will use the following realization of $f(\cdot)$. Let F be an element in some appropriate finite group in which it is unfeasible to compute discrete logarithms with respect to the basis F, and in which the order of F is equal to the modulus of the group in which a and b reside. The function $f(\cdot)$ is then specified to assign F^a to $f(a)$. After the two examples we will return to the requirements for $f(\cdot)$, and assess whether the chosen realization of $f(\cdot)$ meets these requirements. The general modification technique, applied to both examples, is described in the form of protocol figures in the appendix.

First example. In the restrictive blinding issuing protocol for the Guillou-Quisquater secret-key certificate scheme [4], $\mathcal{S}$ uses 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}) such that

$$h_i = g^{s_{0i}} s_{1i}^v \bmod n.$$

With the new immunization technique, $\mathcal{S}$ in addition publishes a pair (M, F), as part of its public key (in general, the description of $f(\cdot)$). Here, M is a prime number such that n divides $M-1$, and F is an element of order n in $\mathbb{Z}_M^*$. Note that this construction ensures that in expressions such as, for instance, $F^{ab} \bmod M$, the computation in the exponent is performed modulo n. Indeed, a computation such as $F^{w^v} \bmod M$ can be

performed by first computing $w^v \bmod n$, and then raising F modulo M to the outcome of $w^v \bmod n$. The first requirement for $f(\cdot)$ is met, because given $f(a) = F^a \bmod M$ and b, for $a, b \in \mathbb{Z}_n^*$, one can easily compute $f(ab \bmod n)$, by raising F^a modulo M to the power b. An assessment of the second requirement for $f(\cdot)$ is provided in the next section.

A *secret-key certificate* of $\mathcal{S}$ on a public key h_i of $\mathcal{R}_i$ is a pair $(r, c) \in \mathbb{Z}_n^* \times \mathbb{Z}_{2^t}$ such that

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

Note that $f(a)$ is included in the hash-function, as opposed to a in the unmodified issuing scheme.

As in the unmodified issuing protocol, in an execution of the immunized issuing protocol $\mathcal{R}_i$ receives a certified key pair (s_{0i}, s_{1i}), h_i', (r', c'), with the blinding-invariant predicate of the secret key being equal to $s_{0i} \bmod v$. The number $g_1^{s_{0i}} \bmod n$ will be denoted by h_i; it can be thought of as the "not-yet-blinded" public key that is to be blinded to h_i'.

$\boxed{\mathcal{R}_i}$		$\boxed{\mathcal{S}}$
		$w \in_{\mathcal{R}} \mathbb{Z}_n^*$
		$a := F^{w^v} \bmod M$
	$\xleftarrow{a}$	
$s_{1i}, t_1 \in_{\mathcal{R}} \mathbb{Z}_n^*$		
$t_2 \in_{\mathcal{R}} \mathbb{Z}_v$		
$h_i' := h_i s_{1i}^v \bmod n$		
$c' := \mathcal{H}(h_i', a^{t_1^v (h\, h_i)^{t_2}} \bmod M)$		
$c := c' + t_2 \bmod v$		
	$\xrightarrow{c}$	
		$r := (x y^{s_{0i}})^c w \bmod n$
	$\xleftarrow{r}$	
$F^{r^v (h\, h_i)^{-c}} \stackrel{?}{=} a \bmod M$		
$r' := r\, t_1 (h\, h_i)^{c' + t_2 \operatorname{div} v} s_{1i}^{c'} \bmod n$		

Figure 1

The immunized issuing protocol is as follows (see Fig. 1):

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

Step 2. $\mathcal{R}_i$ generates at random two numbers $s_{1i}, t_1 \in \mathbb{Z}_n^*$, and a number $t_2 \in \mathbb{Z}_v$. $\mathcal{R}_i$ computes $h_i' := h_i s_{1i}^v \bmod n$, $c' := \mathcal{H}(h_i', a^{t_1^v (h\, h_i)^{t_2}} \bmod M)$, and sends $c := c' + t_2 \bmod v$ to $\mathcal{S}$.

Step 3. $\mathcal{S}$ sends $r := (xy^{s_{0i}})^c w \bmod n$ to $\mathcal{R}_i$.

$\mathcal{R}_i$ accepts if and only if $F^{r^v (h\, h_i)^{-c}} = a \bmod M$. If this verification holds, $\mathcal{R}_i$ computes $r' := r\, t_1 (h\, h_i)^{c' + t_2 \operatorname{div} v} s_{1i}^{c'} \bmod n$.

Second example. In the restrictive blinding issuing protocol for the Schnorr secret-key certificate scheme [4, 5], $\mathcal{S}$ uses a public key $(p, q, g, h, g_1, \mathcal{H}(\cdot))$, and a secret key (x, y) in $\mathbb{Z}_q \times \mathbb{Z}_q$. Here, p and q are prime numbers such that q divides $p - 1$; g is an element of order q in the group $\mathbb{Z}_p^*$; h_0 is equal to $g^x \bmod p$; g_1 is equal to $g^y \bmod p$; 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 is a pair $(s_{0i}, s_{1i}) \in \mathbb{Z}_q \times \mathbb{Z}_q$ such that

$$h_i = g_1^{s_{0i}} g^{s_{1i}} \bmod p.$$

Note that we could use any group G_q of prime order q in [5], without needing to specify a particular type; here we have to specify a type, because we otherwise cannot define $f(\cdot)$ explicitly.

Applying the immunization technique, $\mathcal{S}$ now also publishes a pair (M, F) as part of its public key. Here, M is a prime number such that p divides $M - 1$; and F is an element of order p in $\mathbb{Z}_M^*$. This construction ensures that in computations such as, for instance, $F^{ab} \bmod M$, the computation in the exponent is performed modulo p.

A *secret-key certificate* of $\mathcal{S}$ on a public key h_i of $\mathcal{R}_i$ is a pair $(r, c) \in \mathbb{Z}_q \times \mathbb{Z}_{2^t}$ such that

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

As in the unmodified issuing protocol, in an execution of the immunized issuing protocol $\mathcal{R}_i$ receives a certified key pair (s_{0i}, s_{1i}), h_i', (r', c'), with the blinding-invariant predicate of the secret key being equal to $s_{0i} \bmod q$. The number $g^{s_{0i}} \bmod p$ will be denoted by h_i.

The immunized issuing protocol is as follows (see Fig. 2):

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

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

Step 3. $\mathcal{S}$ sends $r := c\,(x + y s_{0i}) + w \bmod q$ to $\mathcal{R}_i$.

$\mathcal{R}_i$ accepts if and only if $F^{g^r (h\,h_i)^{-c}} = a \bmod M$. If this verification holds, then $\mathcal{R}_i$ computes $r' := r + t_1 + c' s_{1i} \bmod q$.

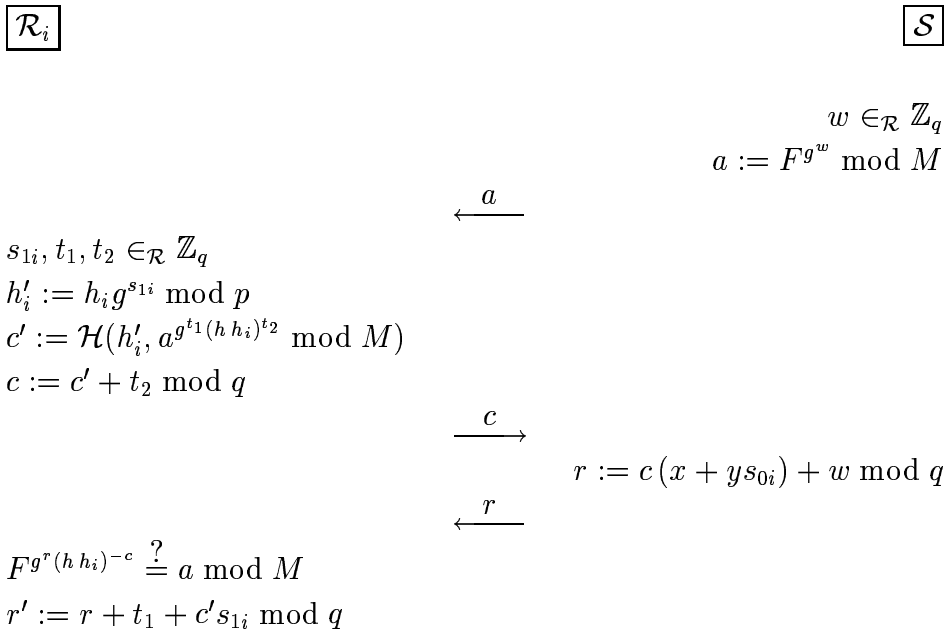

Figure 2

3. Rationale

As a little thought will reveal, all the proofs that pertain to the unmodified issuing protocols [4] are fully preserved, since $f(\cdot)$ is one-to-one. In fact, should $f(\cdot)$ become easy to invert (more specifically, if the second requirement is not met), then we are back in the case of the unmodified issuing protocols (the small change in the definition of a certificate on a public key does not make any difference in this respect).

It is also easy to see that all the techniques that have been introduced in [1, 2, 5], for applying restrictive blind certificate issuing protocols to privacy-protecting mechanisms

for value transport, can be used straightforwardly in conjunction with their immunized counterparts; this is because the definition of what constitutes a key pair for a receiver is not affected by the immunization technique. (The value transport techniques are not based on the structure of the certificates, only on the structures of the key pairs.)

Methods for generating triples (M, n) (first example) and (M, p, q) (second example) have been well-studied in the literature. With respect to the first example, finding a prime M, for which n (the product of two primes) divides $M - 1$, using trial and error is expected [10] to result in M satisfying $M < n \log^2 n$ (although the evidence is only heuristic). It is interesting to note that such pairs (M, n) are also required in the construction of the Brickell-McCurley identification scheme [7]. As for triples (M, p, q), it is known for instance [9] that the fraction of n-bit numbers that are special primes (i.e., primes M such that $M - 1 = 2p$ and $p - 1 = 2q$ for primes p, q) is asymptotically $1/n^3 \log^3 2$, and hence they can easily be found by trial and error. The task in our case is even (much) simpler, since we do not need special primes. Note also that it is often recommended, for high security, to use RSA moduli that are the product of two primes that both meet the requirements that we imposed on the prime M.

Before explaining why this immunization technique should be effective, let's first assess whether the chosen realization of $f(\cdot)$ satisfies the two requirements. It is obvious that the function is one-to-one, and we have already seen that the first requirement is met. The proof of the following proposition will appear in the full paper. (It is stated in terms of the second example; a similar proposition for the first example can be proved in the same way.)

Proposition 1 *Let M, p and q denote prime numbers such that q divides $p-1$ and p divides $M-1$, and let F be an element of order p in $\mathbb{Z}_M^*$. Suppose there exist constants α, β, with (α, β) unequal to $(1, 0)$ or $(0, 1)$, and a polynomial-time algorithm that, on given as input a randomly chosen tuple (M, p, q, F) and a pair $(F^a \bmod M, F^b \bmod M)$ for randomly chosen a, b of order q in $\mathbb{Z}_p^*$, outputs $F^{a^\alpha b^\beta} \bmod M$ with probability of success non-negligibly greater than $1/2$. Then the Diffie-Hellman problem for groups $\mathbb{Z}_M^*$, with M of the specified form, is tractable.*

The lower bound of $1/2$ here stems from the fact that the seeming intractability of the Decision Diffie-Hellman problem (see the pre-print of [1]) prevents one from recognizing correct outputs of the algorithm, and so the proof uses the well-known idea of working with polynomially many randomly self-reduced copies of each input and taking the majority vote. Whether the proof can be made to work for any non-negligible success probability is an open question. Likewise, it is not clear whether the proposition

holds for any non-trivial (α, β) in $\mathbb{Z}_q^* \times \mathbb{Z}_q^*$ (since q grows exponentially). Moreover, the proposition only considers algorithms that perform the task of outputting $F^{a^\alpha b^\beta} \bmod M$ for fixed α, β; it does not exclude the possibility that there exists an algorithm that, on input the specified information, outputs non-trivial constants α, β and $F^{a^\alpha b^\beta} \bmod M$.

Nevertheless, the proposition strongly suggests that if the Diffie-Hellman problem [8] in groups $\mathbb{Z}_M^*$ is intractable, for moduli M of the specified form, then the described realization of the function $f(\cdot)$ meets the second requirement. Since such moduli M are believed to be among the best possible choices for making the discrete log problem as hard as possible, the proposition provides good evidence in favor of the chosen realization for $f(\cdot)$.

Finally, we'll address why the proposed immunization technique should be effective. Consider, without loss of generality, two executions of any one of the unmodified issuing protocols, with challenges c_i and c_j, respectively, and initial information a_i and a_j, respectively. The crucial observation is that, if the unmodified issuing protocols are restrictive blind in sequential mode, then any successful attack for retrieving completely blinded triples in parallel mode must be such that each of the two challenges c_i, c_j depends on each of a_i, a_j. Algebraic attacks that can exploit this [4, 6] make use of the fact that the respective verification relations for each of the two considered executions of the issuing protocol can be combined algebraically (by raising each to some appropriate power, and taking the product). These algebraic attacks amount to combining $a_i^\alpha a_j^\beta$ into a new a_k. If one tries to apply such algebraic attacks to the immunized protocols, which as mentioned above are at least as secure as the unmodified protocols, then one must find multiplicative relations $f(a_i^\alpha a_j^\beta)$ from $f(a_i)$ and $f(a_j)$, i.e., one must perform this task through the "masked" forms, with $f(\cdot)$ serving as the mask. The second requirement for $f(\cdot)$ ensures that this task is infeasible.

We can weaken the second requirement for $f(\cdot)$ by, in addition, building in the following timing mechanism into the immunized issuing protocols. $\mathcal{S}$ initially determines some appropriate time bound (which may vary per execution of the issuing protocol, or per receiver). If the delay in time between sending out the number a and receiving the challenge c exceeds this time bound, then $\mathcal{S}$ will not provide its response r. $\mathcal{S}$ can time this delay by means of a sufficiently accurate clock. Failure to provide a challenge in time then means that the receiver must try again, in a new execution of the issuing protocol. If this timing mechanism is used, then it suffices that computing algebraic relations of the form $f(a^\alpha b^\beta)$ be unfeasible *within the imposed time bound* (which may not be more than a second, or a fraction thereof).

4. Conclusion

In the introduction of [4] three advantages of the unmodified protocols were mentioned. Clearly the first of these, namely that the receiver needs to perform only a single on-line multiplication, no longer holds for the immunized protocols. On the other hand, the immunized protocols have the following advantage over the unmodified protocols. To download, say, 1000 certified key pairs, $\mathcal{R}_i$ and $\mathcal{S}$ perform 1000 executions of the certificate issuing protocol in parallel. After having received the 1000 initial numbers from $\mathcal{S}$, $\mathcal{R}_i$ disconnects. $\mathcal{R}_i$ then computes 1000 challenges (which may take some time on a slow computer). Once finished, $\mathcal{R}_i$ connects again, sends the 1000 challenges, and receives the matching 1000 responses. This clearly is an important advantage of interactive issuing protocols that may be performed in parallel over those that may not. Another advantage is that the immunized issuing protocols can be run by distributed agents, without central coordination between the agents.

Whether it is favorable to use the unmodified protocols, because they are extremely efficient with respect to on-line computational requirements, or their somewhat less efficient immunized counterparts, which can be run in parallel mode, depends completely on the application at hand.

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 (extended abstract)," Advances in Cryptology – EUROCRYPT '95, Lecture Notes in Computer Science, Springer-Verlag. See for full paper: 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.

5. Brands, S., manuscript (1993) part (iii): "Off-Line Electronic Cash Based on Secret-Key Certificates," Proc. of the Second International Symposium of Latin American Theoretical Informatics (LATIN '95), Valparaíso, Chili, April 3–7, 1995. See also: 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.
6. 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.
7. 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.
8. Diffie, W., Hellman, M.E., "New Directions in Cryptography," IEEE Trans. Info. Theory IT-22, Nov. 1976, pp. 644-654.
9. Shanks, D., *Solved and Unsolved Problems in Number Theory*, Chelsea, New York, 1976.
10. Wagstaff, S.S. Jr., "Greatest of the least primes in arithmetic progressions having a given modulus," Mathematics of Computation, No. 33, 1979, pp. 1073–1080.

1. Appendix

In this appendix the application of the immunization technique to both the Guillou-Quisquater based certificate scheme (first example) and the Schnorr-based certificate scheme (second example) is described in general terms of the function $f(\cdot)$. In both cases first the unmodified, original protocol is shown, and then its immunized counterpart is shown below it. To emphasize the simple mechanics of the immunization technique, no symbolic name has been introduced for $f(a)$, so that by comparing the unmodified protocol to the immunized protocol it can instantly be seen how to apply the function $f(\cdot)$ to the unmodified protocols. Remember that in the immunized protocols, the second argument of $\mathcal{H}(\cdot)$, when computing c', can be computed from $f(a)$ and b (the blinding factor, equal to $t_1^v(h\,h_i)^{t_2} \bmod n$ in the first example and $g^{t_1}(h\,h_i)^{t_2} \bmod p$ in the second), due to the first requirement for $f(\cdot)$. To make this more explicit, the blinding of a is described using the "$\cdot$" symbol, denoting multiplication.

$\boxed{\mathcal{R}_i}$		$\boxed{\mathcal{S}}$
		$w \in_{\mathcal{R}} \mathbb{Z}_n^*$
		$a := w^v \bmod n$
	$\xleftarrow{a}$	
$s_{1i}, t_1 \in_{\mathcal{R}} \mathbb{Z}_n^*$		
$t_2 \in_{\mathcal{R}} \mathbb{Z}_v$		
$h_i' := h_i s_{1i}^v \bmod n$		
$c' := \mathcal{H}(h_i', a \cdot t_1^v (h\, h_i)^{t_2} \bmod n)$		
$c := c' + t_2 \bmod v$		
	$\xrightarrow{c}$	
		$r := (x y^{s_{0i}})^c w \bmod n$
	$\xleftarrow{r}$	
$r^v (h\, h_i)^{-c} \bmod n \stackrel{?}{=} a$		
$r' := r\, t_1 (h\, h_i)^{c' + t_2 \operatorname{div} v} s_{1i}^{c'} \bmod n$		

Original issuing protocol (first example)

$\boxed{\mathcal{R}_i}$		$\boxed{\mathcal{S}}$
		$w \in_{\mathcal{R}} \mathbb{Z}_n^*$
		$a := w^v \bmod n$
	$\xleftarrow{f(a)}$	
$s_{1i}, t_1 \in_{\mathcal{R}} \mathbb{Z}_n^*$		
$t_2 \in_{\mathcal{R}} \mathbb{Z}_v$		
$h_i' := h_i s_{1i}^v \bmod n$		
$c' := \mathcal{H}(h_i', f(a \cdot t_1^v (h\, h_i)^{t_2} \bmod n))$		
$c := c' + t_2 \bmod v$		
	$\xrightarrow{c}$	
		$r := (x y^{s_{0i}})^c w \bmod n$
	$\xleftarrow{r}$	
$f(r^v (h\, h_i)^{-c} \bmod n) \stackrel{?}{=} f(a)$		
$r' := r\, t_1 (h\, h_i)^{c' + t_2 \operatorname{div} v} s_{1i}^{c'} \bmod n$		

Immunized issuing protocol (first example)

$\boxed{\mathcal{R}_i}$		$\boxed{\mathcal{S}}$
		$w \in_{\mathcal{R}} \mathbb{Z}_q$
		$a := g^w \bmod p$
	$\xleftarrow{a}$	
$s_{1i}, t_1, t_2 \in_{\mathcal{R}} \mathbb{Z}_q$		
$h_i' := h_i g^{s_{1i}} \bmod p$		
$c' := \mathcal{H}(h_i', a \cdot g^{t_1} (h\, h_i)^{t_2} \bmod p)$		
$c := c' + t_2 \bmod q$		
	$\xrightarrow{c}$	
		$r := c\,(x + y s_{0i}) + w \bmod q$
	$\xleftarrow{r}$	
$g^r (h\, h_i)^{-c} \bmod p \stackrel{?}{=} a$		
$r' := r + t_1 + c' s_{1i} \bmod q$		

Original issuing protocol (second example)

$\boxed{\mathcal{R}_i}$		$\boxed{\mathcal{S}}$
		$w \in_{\mathcal{R}} \mathbb{Z}_q$
		$a := g^w \bmod p$
	$\xleftarrow{f(a)}$	
$s_{1i}, t_1, t_2 \in_{\mathcal{R}} \mathbb{Z}_q$		
$h_i' := h_i g^{s_{1i}} \bmod p$		
$c' := \mathcal{H}(h_i', f(a \cdot g^{t_1} (h\, h_i)^{t_2} \bmod p))$		
$c := c' + t_2 \bmod q$		
	$\xrightarrow{c}$	
		$r := c\,(x + y s_{0i}) + w \bmod q$
	$\xleftarrow{r}$	
$f(g^r (h\, h_i)^{-c} \bmod p) \stackrel{?}{=} f(a)$		
$r' := r + t_1 + c' s_{1i} \bmod q$		

Immunized issuing protocol (second example)