Security of Blind Discrete Log Signatures against Interactive Attacks

Claus Peter Schnorr

Fachbereiche Mathematik/Informatik, Universität Frankfurt, PSF 111932,
D-60054 Frankfurt am Main, Germany. schnorr@cs.uni-frankfurt.de

Abstract. We present a novel parallel one-more signature forgery against blind Okamoto-Schnorr and blind Schnorr signatures in which an attacker interacts some l times with a legitimate signer and produces from these interactions $l + 1$ signatures. Security against the new attack requires that the following ROS-problem is intractable: find an $\underline{\text{o}}$verdetermined, $\underline{\text{s}}$olvable system of linear equations modulo q with $\underline{\text{r}}$andom inhomogenities (right sides).

There is an inherent weakness in the security result of Pointcheval and Stern. Theorem 26 [PS00] does not cover attacks with 4 parallel interactions for elliptic curves of order 2^{200}. That would require the intractability of the ROS-problem, a plausible but novel complexity assumption. Conversely, assuming the intractability of the ROS-problem, we show that Schnorr signatures are secure in the random oracle and generic group model against the one-more signature forgery.

1 Introduction and Summary

We study the security of blind Schnorr signatures and blind Okamoto-Schnorr signatures against the one-more signature forgery in which an attacker interacts some l times with the legitimate signer and produces from these l interactions $l + 1$ signatures. Let these signatures be based on the discrete logarithm of an arbitrary group G of prime order q, e.g. an elliptic or hyperelliptic curve or a subgroup of units in $\mathbf{Z}_n^*$ for a composite or prime module n. We introduce the novel parallel attack that succeeds in a one-more signature forgery against blind Schnorr signatures and blind Okamoto-Schnorr signatures with the same efficiency. The attack is in the Random Oracle and Generic Group Model (ROM + GM) explained in Section 3. The new attack merely requires a solution of the ROS-problem, a possibly intractable problem: find an $\underline{\text{o}}$verdetermined, $\underline{\text{s}}$olvable system of linear equations modulo q with $\underline{\text{r}}$andom inhomogenities. Specifically, given a system of $t \gg l$ linear equations modulo q in l unknowns with random inhomogenities (right sides) find a solvable subsystem of $l + 1$ equations — a solvable subsystem corresponds to a $(l + 1) \times l$-submatrix of rank l.

The new parallel attack has the interesting feature not to depend on the public key. Traditional security proofs do not seem to work in the presence of such an attack. Usually, traditional security proofs use the attacker to solve a DL-problem or a decisional Diffie-Hellman-problem associated with the public

S. Qing, T. Okamoto, and J. Zhou (Eds.): ICICS 2001, LNCS 2229, pp. 1–12, 2001.

key. However, the generic parallel attack uses a solution of the ROS-problem that is not related to the public key and thus the attacker cannot be used to solve a DL- or a DDH-problem. How could [PS00,PS96b] prove security ? Theorem 26 of [PS00] only covers cases where solutions of the ROS-problem exist with negligible probability. While Theorem 26 [PS00] is optimal in the traditional security model, the new attack points to an inherent weakness of this result.

Theorem 26 of [PS00] shows that an attacker mounting a one-more signature forgery with a probability of success $\varepsilon > 4Q^{l+1}/q$ can be used to compute a discrete logarithm.[1] Here Q is the number of hash queries, l is the number interactions with the signer and q is the prime order of the group G. For an elliptic curve G of order $q \approx 2^{200}$ and $Q = 2^{50}$ we must have $l \leq 3$ as $\varepsilon \leq 1$. For a subgroup G of units of order $\leq 2^{1000}$ we must have $l \leq 20$. The security for larger values of l is an open problem [PS00]. Our generic parallel attack shows that the security of blind DL-signatures against one-more signature forgeries requires the intractability of the ROS-problem. The ROS-problem is related to a NP-complete problem [H97].

Conversely, assuming the intractability of the ROS-problem Theorem 2 gives a practical security guarantee for blind Schnorr signatures in the ROM + GM. A generic attacker performing t generic steps, including some l interactions with the signer, cannot produce $l+1$ signatures with a better probability than $\binom{t}{2}/q$. For elliptic curves G of order $q \approx 2^{200}$ this guarantee covers up to $t = 2^{100}$ generic steps including up to 2^{100} parallel signer interactions that can be interleaved in an arbitrary way. Blind Schnorr signatures have the same security level in the ROM + GM as the double-keyed blind Okamoto-Schnorr signatures, thus reducing a considerable overhead.

Our result suggests to use blind Schnorr signatures in connection with strong elliptic/hyperelliptic curves rather than double-keyed blind Okamoto-Schnorr signatures with subgroups of units. We prove security of the most practical schemes under reasonable assumptions. The less practical schemes of [P98], [AO 00] are provably secure for a polynomial number of interactions, but some restrictions apply. [2] The security proofs of [P98], [AO 00] do not use the GM. The new attack does not apply to the less simple signatures of [A01].

Is the GM-assumption to strong ? Contrary to claims of previous anonymous referees we are not aware of a practical cryptographic scheme that is secure in the

[1] In terms of asymptotic bounds the security results of Pointcheval, Stern [PS96b,PS00] show that blind Okamoto-Schnorr signatures are secure against parallel interactive attacks provided that the number of interactions with the signer is poly-logarithmic — $polylog(|q|)$ for the binary length $|q|$ of q. The polylog bound on the number of signer interactions has not been explicitly mentioned in [P00] but it is required as the proof is based on the results of [PS00].

[2] In [P98] a third party — the *checker* — has been introduced, and it is shown that the resulting three-party signature protocol is secure for a polynomial number of *synchronized* signer interactions, where the synchronization forces the completion of each step for all the different protocol invocations before the next step of any other invocation is started. The [AO 00] scheme uses the [P98] scheme, thus the same restrictions apply.

ROM + GM but is insecure in reality. [CGH98] give a very intricate example of a secure scheme in ROM (only) that does not have a secure implementation. Of course the random hash function must be independent of the generic group [F00]. Moreover, FISCHLIN [F00] shows that generic verifier zeroknowledge is provably weaker than black-box TM verifier zeroknowledge. There are two reasons [Sc01b]: firstly, generic verifiers are more restricted than TM-verifiers, secondly black-box simulators are less powerful than generic verifier simulators that control the generic group steps. Fischlin's result does not amount to a security break as we do not know that generic verifier zeroknowledge is weaker than "general" TM-verifier zeroknowledge. The restriction via the black-box mode may be to rigid.

The paper is organized as follows. We present in Section 2 blind Schnorr signatures and the novel parallel attack against blind Schnorr and against blind Okamoto-Schnorr signatures. We determine in Theorem 1 the probability for the existence of a solution for the ROS-problem. In Section 3 we describe the ROM + GM as introduced in [SJ00]. Assuming the intractability of the ROS-problem we give in Section 4, Theorem 2 a practical security guarantee for blind Schnorr signatures in the ROM + GM.

2 Blind Schnorr Signatures and the Parallel Attack

We are interested in blind signatures as required for anomymous digital cash. Blind signatures are generated by an interaction with the signer who controls the secret signature key.

Schnorr signatures refer to an arbitrary group G of prime order q and an arbitrary message space M. We describe signer interactions, an interactive protocol that enables a user to generate Schnorr signatures of messages of its choice. We first describe the setting and the structure of the signatures, after which we review the protocol for generation of signatures. We also show how to generate blind signatures of the same type. Signatures will be based on an ideal hash function $H : G \times M \to \mathbf{Z}_q$, where M is the set of messages.

Private/public key pairs. The *private key* x of the signer is random in $\mathbf{Z}_q$. The corresponding *public key* is $h = g^x \in G$, a random group element. We have $x = \log_g h$.

Signatures. A Schnorr signature on a message m is a triple $(m, c, z) \in M \times \mathbf{Z}_q^2$ such that $H(g^z h^{-c}, m) = c$. For this paper, we let signatures (m, c, z) comprise the message.

Signing a message $m \in M$: Pick a random $r \in_R \mathbf{Z}_q$, compute g^r, $c := H(g^r, m)$ and $z := r + cx$. Output the signature: (m, c, z). The result is a valid signature since we have $g^z h^{-c} = g^{r+cx} h^{-c} = g^r$, and thus $H(g^z h^{-c}, m) = c$. We call a signature (m, c, z) constructed by this protocol a *standard signature.*

A signer interaction is a three round interactive protocol between the signer and a user. The signer picks a random $r \in_R \mathbf{Z}_q$ and sends the commitment g^r to the user. The user selects a challenge $c \in \mathbf{Z}_q$ and sends c. The signer responses by sending $z := r + cx \in \mathbf{Z}_q$. We let $(r, c, z) \in \mathbf{Z}_q^3$ denote the signer interaction consisting of the signer's random coin r, the user's *challenge* c and the signer's *response* z. A signer interaction (r, c, z) can be used to generate the *standard signature* (m, c, z), where $c := H(g^r, m)$ or a transformation (m, c', z') of this signature.

Blind Signature Protocol. We call the signature protocol *blind* if it generates a signature (m, c', z') that is statistically independent of the interaction (r, c, z) that provides the view of the signer. Lateron, blind signatures cannot be identified and related to the signer interaction. The blindness concept is from [CP92].

To generate a blind signature (m, c', z') the user picks random numbers $\alpha, \beta \in_R \mathbf{Z}_q$, and responses to the commitment g^r by sending the challenge $c = H(g^{r+\alpha} h^{\beta}, m) + \beta \in \mathbf{Z}_q$. After receiving $z = r + cx \in \mathbf{Z}_q$ he computes $z' = z + \alpha, c' = c - \beta$.

Validity. For the output of the interaction $(m, c', z') = (m, c - \beta, z + \alpha)$ we have $g^{z'} h^{-c'} = g^{r+cx+\alpha} h^{-c+\beta} = g^{r+\alpha} h^{\beta}$. Hence $H(g^{z'} h^{-c'}, m) = c - \beta = c'$, and thus (m, c', z') is a valid signature.

Blindness Property. The generated signature $(m, c - \beta, z + \alpha)$ is — for a constant interaction (r, c, z) — uniformly distributed over all signatures on message m due to the random $\alpha, \beta \in_R \mathbf{Z}_q$. Each signature (m, c', z') is produced for a unique pair $(\alpha, \beta) \ : \alpha = z' - z, \ \beta = c - c'$.

2.1 A New Parallel Attack against Blind Schnorr Signatures

We present a variant of the attack that does not even use the generator g and the public key h. We first present the attack for Schnorr signatures. Thereafter, we extend it to Okamoto-Schnorr signatures. We show that Okamoto-Schnorr signatures do not protect better against the attack than plain Schnorr signatures. The new attack uses a solution of the following

ROS-problem: Find an overdetermined, solvable system of linear equations modulo q with random inhomogenities. Specifically, given an oracle random function $F : \mathbf{Z}_q^l \to \mathbf{Z}_q$, find coefficients $a_{k,\ell} \in \mathbf{Z}_q$ and a solvable system of $l+1$ distinct equations (1) in the unknowns $c_1, ..., c_l$ over $\mathbf{Z}_q$:

$$a_{k,1}\, c_1 + ... + a_{k,l}\, c_l = F(a_{k,1}, ..., a_{k,l}) \ \text{ for } k = 1, ..., t. \tag{1}$$

We evaluate the expected number of solvable subsystems consisting of $l+1$ out of t equations (1).

Theorem 1. *For arbitrary coefficients $a_{k,\ell} \in \mathbf{Z}_q$, the average number of solvable subsystems of $l+1$ out of the t equations* (1) *is at most $\binom{t}{l+1}/q$. For statistically independent coefficients $a_{k,\ell} \in_R \mathbf{Z}_q$ the average number of solvable subsystems is $\binom{t}{l+1} q^{-1}\ (1 - q^{-1} + O(q^{-2}))$.*

Proof. Consider a constant selection of $l+1$ out of the t equations (1) with arbitrary coefficients $a_{k,\ell}$. Let the subsystem have s linearly independent vectors

$(a_{k,1}, ..., a_{k,l}) \in \mathbf{Z}_q^l$. The subsystem is solvable if and only if the rank of the submatrix of the corresponding vectors $(a_{k,1}, ..., a_{k,l},\ F(a_{k,1}, ..., a_{k,l}))$ is s. The probability that the subsystem is solvable has a maximum q^{-1} for $s = l$. For $s = l$ the l linearly independent equations have a unique solution and that solution satisfies the remaining equation with probability q^{-1}. As there are $\binom{t}{l+1}$ selections out of t, the average number of solvable subsystems is at most $\binom{t}{l+1}/q$.

Next, consider random coefficients $a_{k,\ell} \in_R \mathbf{Z}_q$. Then l vectors $(a_{k,1}, ..., a_{k,l})$ are linearly independent with probability $(1 - q^{-1})(1 - q^{-2}) \cdot ... \cdot (1 - q^{-l+1})$. Hence, a constant selection of $l + 1$ equations (1) is solvable with probability $q^{-1}(1 - q^{-1} + O(q^{-2}))$.

Consider two distinct selections of $l + 1$ equations. The solvability of two systems of $l + 1$ equations is (nearly) statistically independent as the systems differ in at least one random value $F(a_{k,1}, ..., a_{k,l})$. The law of large numbers holds for a sequence of pairwise independent, identically distributed random variables. Therefore, the expected number of solvable subsystems with $l + 1$ equations is $\binom{t}{l+1}q^{-1}(1 - q^{-1} + O(q^{-2}))$. □

The attack against Schnorr signatures. The signer sends commitments $g_1 = g^{r_1}, ..., g_l = g^{r_l}$. The attacker $\mathcal{A}$ selects $a_{k,1}, ..., a_{k,l} \in \mathbf{Z}_q$ and messages $m_1, ..., m_t$, and computes $f_k = g_1^{a_{k,1}} \cdot ... \cdot g_l^{a_{k,l}}$ and $H(f_k, m_k)$ for $k = 1, ..., t$. Then $\mathcal{A}$ solves $l + 1$ of the t equations (2) in the unknowns $c_1, .., c_l$ over $\mathbf{Z}_q$:

$$H(f_k, m_k) = \textstyle\sum_{\ell=1}^{l} a_{k,\ell}\, c_\ell \quad \text{for } k = 1, ..., t. \tag{2}$$

$\mathcal{A}$ sends the solutions $c_1, ..., c_l$ as challenges to the signer. The signer sends back $z_\ell := r_\ell + c_\ell x \in \mathbf{Z}_q$ for $\ell = 1, .., l$. For each solved equation (2), the attacker gets a valid signature (m_k, c'_k, z'_k) by setting

$$c'_k := \textstyle\sum_{\ell=1}^{l} a_{k,\ell}\, c_\ell = H(f_k, m_k) \quad \text{and} \quad z'_k := \textstyle\sum_{\ell=1}^{l} a_{k,\ell} z_\ell.$$

Correctness. The equations (2) imply that

$$g^{z'_k} h^{-c'_k} = g_1^{a_{k,1}} \cdot ... \cdot g_l^{a_{k,l}} = f_k \quad \text{and} \quad H(g^{z'_k} h^{-c'_k}, m_k) = c'_k.$$

In the ROM the values $H(f_k, m_k)$ are random. The coefficients $a_{k,\ell}$ selected by the attacker are arbitrary values. The solution $(c_1, ..., c_l)$ of $l + 1$ of the t equations (2) does not depend on g, h. As $\mathcal{A}$ does not use g, h, $\mathcal{A}$ cannot help in black-box mode to compute $\log_g h$ or to solve a Diffie-Hellman or a decisional Diffie-Hellman problem related to h.

The new attack is generic, it works for arbitrary groups with an efficient multiplication. We call it the *generic, parallel attack*. The attack is intrinsic parallel. Theorem 1 shows that the number l of parallel interactions with the signer must be at least logarithmic in q. Otherwise, the probability $\binom{t}{l+1}/q$ for the existence of a solvable subsystem of $l + 1$ equations (2) is negligible.

The attack against Okamoto-Schnorr signatures. We follow the notation of [PS00]. There are two public keys h and $y = g^{-r}h^{-s}$ for random secret keys $r, s \in_R \mathbf{Z}_q$ while $\log_g h$ is unknown. A signature of message m is a tuple $(m, \varepsilon, \sigma, \rho) \in M \times \mathbf{Z}_q^3$ satisfying $H(g^\rho h^\sigma y^\varepsilon, m) = \varepsilon$.

The signer picks random $t_\ell, u_\ell \in_R \mathbf{Z}_q$ and sends commitments $g_\ell = g^{t_\ell} h^{u_\ell}$ for $\ell = 1, .., l$. The attacker $\mathcal{A}$ selects coefficients $a_{k,\ell} \in \mathbf{Z}_q$ and messages $m_1, ..., m_t$, and computes $f_k = g_1^{a_{k,1}} \cdot ... \cdot g_l^{a_{k,l}}$ and $H(f_k, m_k)$ for $k = 1, ..., t$. $\mathcal{A}$ solves $l+1$ of the t linear equations (2) modulo q in the unknowns $c_1, ..., c_l$. $\mathcal{A}$ sends the solutions $c_1, ..., c_l$ as challenges to the signer. The signer sends back $R_\ell := t_\ell + c_\ell r$, $S_\ell := u_\ell + c_\ell s \in \mathbf{Z}_q$ for $\ell = 1, .., l$. For each solved equation (2) $\mathcal{A}$ gets a valid signature $(m_k, \varepsilon_k, \rho_k, \sigma_k)$ by setting

$$\varepsilon_k = H(f_k, m_k) = \textstyle\sum_{\ell=1}^{l} a_{k,\ell}\, c_\ell, \;\; \rho_k = \sum_{\ell=1}^{l} a_{k,\ell}\, R_\ell, \;\; \sigma_k = \sum_{\ell=1}^{l} a_{k,\ell}\, S_\ell.$$

Correctness. From the equations (2) we get that

$$g^{\rho_k} h^{\sigma_k} y^{\varepsilon_k} = \textstyle\prod_{\ell=1}^{l} g_\ell^{a_{k,\ell}} = f_k \quad\text{and}\quad H(g^{\rho_k} h^{\sigma_k} y^{\varepsilon_k}, m_k) = \varepsilon_k.$$

Conclusion. The generic parallel attack $\mathcal{A}$ does not use the public g, h, y. Thus, it is impossible to use a successful attacker to solve a DL- DH- or DDH-problem. The generic, parallel attack has been excluded in Theorem 26 [PS00] by assuming that the attacker has a probability of success $4t^{(l+1)}/q$ which is greater than the probability $\binom{t}{l+1}/q$ for the existence of a solvable subsystem of $l+1$ equations (2). The second part of Theorem 1 shows that solutions to the ROS-problem are very likely to exist for $l = 4, t = 2^{50}$ and $q \approx 2^{200}$. The generic parallel attack is possible for $l = 4$ parallel interactions, $t = 2^{50}$ hash queries for elliptic curves of order $q \approx 2^{200}$. A meaningful security guarantee for elliptic curves of order $\approx 2^{200}$ requires that solvable subsystems of $l+1$ equations (2) are hard to find.

3 The Random Oracle and the Generic Group Model

The Random Oracle Model (ROM). Let G be a group of prime order q with generator g, a range M of messages, and let $\mathbf{Z}_q$ denote the field of integers modulo q. Let H be an *ideal* hash function with range $\mathbf{Z}_q$, modelled as an oracle that given an input (query) in $G \times M$, outputs a random number in $\mathbf{Z}_q$. Formally, H is a random function $H : G \times M \to \mathbf{Z}_q$ chosen at random over all functions of that type with uniform probability distribution.

The Generic Group Model (GM). Generic algorithms for G do not use the binary encodings of the group elements, as they access group elements only for group operations and equality tests. Nechaev [Ne94] proves that the discrete logarithm problem is hard in such a model, see [Sc01a] for a stronger result. The generic model of algorithms was further elaborated on by Shoup [Sh97]. We present the Shoup model in a slightly different setup[3] and we extend it

[3] We count the same generic steps as in [Sh97]; however, we allow arbitrary multivariate exponentiations while Shoup merely uses multiplication and division. The technical setup in [Sh97] looks different as groups G are *additive* and associated with a random injective encoding $\sigma : G \to S$ of the group G into a set S of bit strings — the generic algorithm performs arbitrary computations on these bit strings. Addition/subtraction is done by an oracle that computes $\sigma(f_i \pm f_j)$ when given $\sigma(f_i), \sigma(f_j)$ and the specified sign bit. As the encoding σ is random it contains only the information about which group elements coincide — this is what we call the set of *collisions*.

to algorithms that interact with a decryption oracle. Encryptions are for the private/public key pair (x, h), where x is random in $\mathbf{Z}_q$ and $h = g^x$. We describe the extended generic model in detail, first focusing on non-interactive algorithms and thereafter on algorithms interacting with oracles for hashing and signing.

The *data of a generic algorithm* is partitioned into group elements in G and non-group data. The *generic steps* for group elements are multivariate exponentiations:

- mex: $\mathbf{Z}_q^d \times G^d \to G,\ (a_1, ..., a_d, g_1, ..., g_d) \mapsto \prod_i g_i^{a_i}$ with $d \geq 0$.

The cases $d = 2, a_1 = 1, a_2 = \pm 1$ present multiplication/division. The case $d = 0$ presents *inputs* in G — e.g., g, h are inputs for the DL-computation.

Def. A (non-interactive) *generic algorithm* is a sequence of t generic steps[4]

- $f_1, \ldots, f_{t'} \in G$ (inputs) $1 \leq t' < t$,
- $f_i = \prod_{j=1}^{i-1} f_j^{a_j}$ for $i = t' + 1, \ldots, t$, where $(a_1, \ldots, a_{i-1}) \in \mathbf{Z}_q^{i-1}$ depends arbitrarily on i, the non-group input and the set $\mathcal{CO}_{i-1} := \{(j, \ell) \mid f_j = f_\ell,\ 1 \leq j < \ell \leq i-1\}$ of previous *collisions* of group elements.

Typical non-group inputs are various integers in $\mathbf{Z}_q$ contained in given ciphertexts or signatures. $\mathcal{CO}_t$ is the set of all collisions of the algorithm.

Some group inputs f_i depend on random coin flips, e.g., the random public key $h = g^x$ depends on the random secret key $x \in_R \mathbf{Z}_q$. The *probability space* consists of the random group elements of the input. The logarithms $\log_g f_i$ of the random inputs f_i play the role of *secret parameters*. Information about the secret parameters can only be revealed by collisions. E.g., $g^a = f_i^b$ implies $\log_g f_i = a/b$. We let the non-group input and the generator g not depend on random bits.

The *output* of a generic algorithm consists of

- non-group data that depend arbitrarily on the non-group input and on the set $\mathcal{CO}_t$ of all collisions,
- group elements $f_{\sigma_1}, \ldots, f_{\sigma_d}$ where the integers $\sigma_1, \ldots, \sigma_d \in \{1, \ldots, t\}$ depend arbitrarily on the non-group input and on $\mathcal{CO}_t$.

Next, we elaborate on *interactive, generic algorithms.* We count the following generic steps :

- group operations, mex: $\mathbf{Z}_q^d \times G^d \to G,$ $(a_1, ..., a_d, g_1, ..., g_d) \mapsto \prod_i g_i^{a_i}$,
- queries to the hash oracle H,
- interactions with a signature oracle (*signer* for short).

A *generic adversary* $\mathcal{A}$ — mounting a one-more signature forgery — is an interactive algorithm that interacts with a signer. It performs some t generic steps resulting in $t' \leq t$ group elements $f_1, ..., f_{t'}$. $\mathcal{A}$ iteratively selects the next generic step — a group operation, a query to H, an interaction with the signer

Shoup's random encoding allows for an efficient sorting of group elements. We do not need such efficient sorting as equality tests are for free.

[4] We can allow that the number t of generic steps varies with the input. We can let the algorithm decide after each step whether to terminate depending arbitrarily on the given non-group data.

— depending arbitrarily on the non-group input and on previous collisions of group elements.

The *input* consists of the generator g, the public key $h \in G$, the group order q, a collection of messages and ciphertexts and so on, all of which can be broken down into group elements and non-group data.

The computed *group elements* $f_1, ..., f_{t'} \in G$ are the group elements contained in the input, such as g, h. When counting the number of group operations, we count each input as one operation. As a signer interaction is counted as a generic step the number t' of group elements is bounded by the number t of generic steps, $t' \leq t$. We have $t = t'$ for a non-interactive $\mathcal{A}$.

The given *non-group data* consists of the non-group data contained in the input, the previous hash replies $H(Q)$ of queries Q, and the set of previous collisions of group elements. *Signer interactions* are described in Section 2.

$\mathcal{A}$'s *output* and *transmission* to the signer consists of non-group data NG and previously computed group elements f_σ, where NG and σ, $1 \leq \sigma \leq t'$, depend arbitrarily on given non-group data.

$\mathcal{A}$'s *transmission* to the hash oracle H depends arbitrarily on given group elements and given non-group data. The *probability space* consists of the random H, the random input group elements and the random coin flips of the signer.

The *restriction of the generic model* is that $\mathcal{A}$ can use group elements only for generic group operations, equality tests and for queries to the hash oracle, whereas non-group data can be arbitrarily used without charge. The computed group elements $f_1, ..., f_{t'}$ are given as explicit multiplicative combinations of given group elements. Let $g_\ell = g^{r_\ell}$ for $\ell = 1, ..., l$ be the group elements that $\mathcal{A}$ gets from the signer. A computed $f_j \in G$ is of the form $f_j = g^{a_{j,-1}} h^{a_{j,0}} g_1^{a_{j,1}} \cdot ... \cdot g_l^{a_{j,l}}$, where the exponents $a_{j,-1}, ..., a_{j,l} \in \mathbf{Z}_q$ depend arbitrarily on given non-group data. $\mathcal{A}$ can arbitrarily use the coefficients $a_{j,-1}, ..., a_{j,l}$ from this explicit representation of f_j. A generic adversary does not use internal coin flips, this is not a restriction as internal coin flips would be useless.[5]

Trivial collisions. We call a collision $(i, j) \in \mathcal{CO}_t$ *trivial* if $f_i = f_j$ holds with probability 1, i.e., if it holds for all choices of the secret data such as the secret key x and the random bits r of the encipherer. We write $f_i \equiv f_j$ for a trivial collision. Trivial collisions do not release any information about the secret data while non-trivial collisions can completely release some secret data. Trivial collisions can be excluded from $\mathcal{CO}_t$. Therefore, we ignore trivial collisions.

[5] $\mathcal{A}$ could select interior coin flips that maximize the probability of success — there is always a choice for the internal coin flips that does not decrease $\mathcal{A}$'s probability of success. Moreover, it would be useless for $\mathcal{A}$ to generate random group elements — in particular ones with unknown DL. Using one generic step, $\mathcal{A}$ could replace random elements in G by some deterministic g^a where $a \in \mathbf{Z}_q$ is chosen as to maximize the probability of success.

4 Security of Signatures against Interactive Attacks

Assuming the intractability of the ROS-problem and the ROM + GM we give in Theorem 2 a practical security guarantee for blind Schnorr signatures against one-more signature forgeries.

This section refers to a generic adversary $\mathcal{A}$ performing some t generic steps — including some l interactions $(r_1, c_1, z_1), ..., (r_l, c_l, z_l)$ with the signer — producing some t' group elements and some t'' queries to the hash oracle. We let $\mathbf{r} = (r_1, ..., r_l)$ denote the signers random coins. Let $f_1 = g,\ f_2 = h = g^x$, $f_3, ...f_{t'} \in G$ denote the group elements of $\mathcal{A}$'s computation. The generic $\mathcal{A}$ computes $f_j = g^{a_{j,-1}} h^{a_{j,0}} g_1^{a_{j,1}} \cdot ... \cdot g_l^{a_{j,l}}$, where $g_1 = g^{r_1}, ..., g_l = g^{r_l}$ are the signer's commitments and the exponents $a_{j,\ell} \in \mathbf{Z}_q$ depend arbitrarily on the previously computed non-group data. As each signer interaction yields one group element g^{r_ℓ} we have that $t'' = t - t' \geq 0$ is the number of interactions with the hash oracle. We first present the basic Lemma 1 and 2 that extend results of [SJ00] from a non-interactive attacker to an adversary using a hash oracle and a signature oracle.

Lemma 1. *Collisions among $f_1, ..., f_{t'}$ occur at most with probability $\binom{t'}{2}/q$. The probability refers to the random h, H and the random coins $\mathbf{r}$ of the signer.*

Proof. We show for $i < j$ that $\Pr_{x,\mathbf{r},H}[f_i = f_j] \leq \frac{1}{q}$ under the condition that there is no prior collision of group elements. So let us assume that there is no such prior collision. The main point is to show that f_i, f_j are either statistically independent or f_i/f_j is constant with $f_i \neq f_j$. Considering x and $r_1, ..., r_l$ as indeterminates over $\mathbf{Z}_q$, $\log_g f_j = a_{j,-1} + a_{j,0}\, x + \sum_{\ell=1}^{l} a_{j,\ell}\, r_\ell$ is a linear polynomial in $\mathbf{Z}_q[x, r_1, ..., r_l]$.

For a *non-interactive* $\mathcal{A}$, where $l = 0$ and $\mathbf{r} = (r_1, ..., r_l)$ is empty we have $f_i = f_j$ iff $a_{i,-1} - a_{j,-1} + (a_{i,0} - a_{j,0})\, x = 0$. Therefore, x is statistically independent of the $a_{i,\ell}, a_{j,\ell}$, and thus $\Pr_{x,H}[f_i = f_j] \leq \frac{1}{q}$.[6]

Next, consider an *interactive* $\mathcal{A}$. We call r_ℓ, g^{r_ℓ} *prior* to f_j if the value $a_{j,\ell}$ depends on the signer's response $z_\ell = r_\ell + c_\ell x$, otherwise r_ℓ is *subsequent* to f_j. When given $f_j = g^{a_{j,-1}} h^{a_{j,0}} g_1^{a_{j,1}} \cdot ... \cdot g_l^{a_{j,l}}$ the probability space — from $\mathcal{A}$'s point of view — consists of x, H and the r_ℓ subsequent to f_j. The $r_\ell = z_\ell - c_\ell x$ prior to f_j are linear functions in x, with given coefficients z_ℓ, c_ℓ. Consider $\log_g f_j = a_{j,-1} + a_{j,0}\, x + \sum_{\ell=1}^{l} a_{j,\ell}\, r_\ell$ as a linear function in x and the r_ℓ subsequent to f_j. The coefficients $a_{j,\ell}, c_\ell, z_\ell \in \mathbf{Z}_q$ depend on $x, H, \mathbf{r}$ only via prior r_ℓ and prior hash values. Thus x is statistically independent of the given coefficients. Therefore, the values of the function $\log_g f_i - \log_g f_j$ are either constant or uniformly distributed over $\mathbf{Z}_q$. The case that $\log_g f_i - \log_g f_j = 0$ for all x and all r_ℓ subsequent to f_j has been excluded as $f_i \not\equiv f_j$. This shows that $\Pr_{x,\mathbf{r},H}[f_i = f_j] \leq \frac{1}{q}$, which implies the claim of Lemma 1 as there are $\binom{t'}{2}$ pairs $i < j$. □

Lemma 2. *If there are no collisions among $f_1, ..., f_{t'}$ the random x is statistically independent of the computed non-group data except that the random coins $(\mathbf{r}, x)$ leading to collisions are excluded.*

[6] The equality $f_i = f_j$ holds with zero probability if $a_{i,-1} \neq a_{j,-1}$ and $a_{i,0} = a_{j,0}$. As $f_j \not\equiv f_i$ we cannot have that $(a_{i,-1}, a_{i,0}) = (a_{j,-1}, a_{j,0})$.

Proof. The random x enters into the generic computation only via the the random values $z_\ell = r_\ell + c_\ell x$, random hash values and $h = g^x$. In a signer interaction $\mathcal{A}$ gets the pair (g^{r_ℓ}, z_ℓ). Due to the random r_ℓ the distribution of z_ℓ does not depend on $h = g^x$. The probability distribution of the non-group data generated from hash values and signer responses does not depend on x. Therefore, x is statistically independent of all non-group data ($h = g^x$ is NOT statistically independent of (g^{r_ℓ}, z_ℓ), however g^{r_ℓ} enters into the computation of non-group data only by collisions of group elements and via random hash values). □

Theorem 2 shows that Schnorr signatures are secure against the one-more signature forgery in the ROM + GM. Theorem 2 covers blind signatures as required for anonymous electronic cash. This is the first sharp security result for simple DL-signatures in the interactive setting.

Theorem 2. *Let a generic adversary $\mathcal{A}$ be given the generator g, the public key h, an oracle for H. Let $\mathcal{A}$ interact with the signer some l times and perform t generic steps including l signer interactions. If $\mathcal{A}$ succeeds in a* parallel *attack to produce $l+1$ signatures with a better probability of success than $\binom{t}{2}/q$ then $\mathcal{A}$ must solve the* ROS*-problem : solve $l+1$ distinct equations* (2) *in the unknowns $c_1, ..., c_l \in \mathbf{Z}_q$. The probability space consists of h, H and the random coins of the signer.*

Proof. In the interaction (r_ℓ, c_ℓ, z_ℓ) the signer correctly transmits $g_\ell := g^{r_\ell}$ and responds to $\mathcal{A}$'s challenge c_ℓ by $z_\ell = r_\ell + c_\ell x$. It is assumed that $\mathcal{A}$ outputs distinct triples $(m_i, c_i', z_i') \in M \times \mathbf{Z}_q^2$ for $i = 1, ..., l+1$. We study the probability that the $l+1$ outputs are all signatures. Let there be t'' (distinct) queries to the hash oracle resulting in independent hash values $H(f_{\sigma_k}, m_k) \in \mathbf{Z}_q$ for $k = 1, ..., t''$ for an arbitrary function $k \mapsto \sigma_k$ that selects f_{σ_k} from the computed group elements f_j. Lemma 3 shows that the group element $g^{z_i'}h^{-c_i'}$ corresponding to a signature (m_i, c_i', z_i') must be among $f_{\sigma_1}, ..., f_{\sigma_{t''}}$. We let $f_{\sigma_i} = g^{z_i'}h^{-c_i'}$.

Lemma 3. *Let the output (m_i, c_i', z_i') be a signature with a better probability than $\frac{1}{q}$. Then we have that $c_i' = H(f_{\sigma_i}, m_i)$ for some hash query satisfying $f_{\sigma_i} = g^{z_i'}h^{-c_i'}$. Moreover, c_i', z_i', σ_i satisfy the equations $z_i' = a_{\sigma_i,-1} + \sum_{\ell=1}^{l} a_{\sigma_i,\ell}\, z_\ell$ and*

$$H(f_{\sigma_i}, m_i) = -a_{\sigma_i,0} + \textstyle\sum_{\ell=1}^{l} a_{\sigma_i,\ell}\, c_\ell. \qquad (3)$$

Conversely, given a solution $(c_1, ..., c_l)$ of equation (3) *one easily gets a signature (m_i, c_i', z_i') for each solved equation.*

Proof. The first claim follows from the equation $c_i' = H(g^{z_i'}h^{-c_i'}, m_i)$ required for signatures (m_i, c_i', z_i'). In the ROM this equation necessitates that $\mathcal{A}$ selects c_i' from given hash values $H(f_{\sigma_k}, m_k)$ — otherwise the equality only holds with probability $\frac{1}{q}$ as the hash value is random. W.l.o.g. let $c_i' = H(f_{\sigma_i}, m_i)$ where $f_{\sigma_i} = g^{z_i'}h^{-c_i'}$ holds for the output (m_i, c_i', z_i') which determines σ_i. [7] The equations $g^{z_i'}h^{-c_i'} = f_{\sigma_i} = g^{a_{\sigma_i,-1} + a_{\sigma_i,0}\, x + \sum_{\ell=1}^{l} a_{\sigma_i,\ell}\, r_\ell}$ and $r_\ell = z_\ell - c_\ell x$ imply

[7] For simplicity we abbreviate $f_{\sigma_i} = g^{z_i'}h^{-c_i'}$ even though that equation only holds a posteriori. The output (m_i, c_i', z_i') defines σ_i except that there is a collision $H(f_{\sigma_i}, m_i) = H(f_{\sigma_j}, m_j)$ with $m_i = m_j$.

$$z_i' \;=\; \log_g g^{z_i'} h^{-c_i'} + c_i' x$$
$$z_i' \;=\; a_{\sigma_i,-1} + \textstyle\sum_{\ell=1}^{l} a_{\sigma_i,\ell}\, z_\ell + (\, a_{\sigma_i,0} - \sum_{\ell=1}^{l} a_{\sigma_i,\ell}\, c_\ell \; + c_i')x, \tag{4}$$

If $c_i' = -a_{\sigma_i,0} + \sum_{\ell=1}^{l} a_{\sigma_i,\ell}\, c_\ell$ then $\mathcal{A}$ can easily compute the correct z_i' . In this case, the equation (4) does not depend on the secret key x and we have $z_i' = a_{\sigma_i,-1} + \sum_{\ell=1}^{l} a_{\sigma_i,\ell}\, z_\ell$, where the signers responses $z_1, ..., z_l$ and the coefficients $a_{\sigma_i,-1}, \ldots, a_{\sigma_i,l}$ are known to $\mathcal{A}$.

Conversely, $\mathcal{A}$ must select $c_1, ..., c_l$ as to zero the coefficient of the secret key x in (4). Otherwise, Equation (4) holds with probability $\frac{1}{q}$ as x is by Lemma 2 statistically independent of the non-group data $z_i', a_{\sigma_i-,1}, ..., a_{\sigma_i,l}, c_1, ..., c_l$, and thus $\mathcal{A}$'s probability of success is not better than $\frac{1}{q}$. This proves that $\mathcal{A}$ must solve the equation □

We see that the parallel attacker $\mathcal{A}$ can only succeed in either of four cases:

- $\mathcal{A}$ solves $l+1$ out of t'' distinct equations
  $$H(f_{\sigma_i}, m_i) = -a_{\sigma_i,0} + \textstyle\sum_{\ell=1}^{l} a_{\sigma_i,\ell}\, c_\ell. \tag{3}$$
  Each solved equation (3) yields a corresponding signature (m_i, c_i', z_i') by setting $z_i' = a_{\sigma_i,-1} + \sum_{\ell=1}^{l} a_{\sigma_i,\ell}\, z_\ell$. This is the *generic, parallel attack.*
- For some i, $1 \le i \le l+1$ equation (3) does not hold but equation (4) holds. This event has probability $\frac{1}{q}$.
- There is a collision of group elements. This event has probability $\le \binom{t'}{2}/q$.
- There is a collision of hash values $H(f_{\sigma_i}, m_i) = H(f_{\sigma_j}, m_j)$, where $m_i = m_j$, $f_{\sigma_i} \ne f_{\sigma_j}$ and $a_{\sigma_i,0} = a_{\sigma_j,0}, ..., a_{\sigma_i,l} = a_{\sigma_j,l}$. In this case the equations (3) with indices i and j coincide. This event has probability $\le \binom{t''}{2}/q$.

W.l.o.g. we can assume that $t', t'' \ge 1$, and thus $\binom{t'}{2} + \binom{t''}{2} + 1 \le \binom{t}{2}$. We see that $\mathcal{A}$ succeeds in the last three cases with no better probability than $\binom{t}{2}/q$. This proves Theorem 2 as $\mathcal{A}$ does not succeed with a better probability than $\binom{t}{2}/q$, except that $\mathcal{A}$ solves $l+1$ out of t'' distinct equations (3). □

Security against sequential attacks. It can be seen from the above proof that a sequential attack cannot succeed in the GM + ROM with a better probability than $\binom{t}{2}/q$. Here, the intractability of the ROS-problem is not needed. This characterizes the different power of sequential and of parallel attacks.

For a sequence of l sequential attacks, each with a single signer interaction, $\mathcal{A}$ selects the coefficients $a_{i,\ell}$ in (3) such that there is for each k at most one non-zero coefficient $a_{k,\ell}$ with $\ell \ge 1$.

References

[A01] *M. Abe*: A Secure Three-move Blind Signature Scheme for Polynomially Many Signatures. Proc. Eurocrypt'01, LNCS 2045, pp. 136–151, 2001.

[AO00] *M. Abe and T. Okamoto*: Provably Secure Partially Blind Signatures. Proc. Crypto'00, LNCS 1880, pp. 271–286, 2000.

[CP92] *D. Chaum and T.P. Pedersen* Wallet Databases with Observers. Proc. Crypto'92, LNCS 740, pp. 89–105, 1992.

[BL96] *D. Boneh and R.J. Lipton* : Algorithms for black-box fields and their application in cryptography. Proc. Crypto'96, LNCS 1109, pp. 283–297, 1996.

[BR93] *M. Bellare and P. Rogaway* : Random Oracles are Practical: a Paradigms for Designing Efficient Protocols. Proc. 1st ACM Conference on Computer Communication Security, pp. 62–73, 1993.

[CGH98] *R. Canetti, O. Goldreich and S. Halevi* : The Random Oracle Methodology, Revisited. Proc. STOC'98, ACM Press, pp. 209–218, 1998.

[F00] *M. Fischlin* : A Note on Security Proofs in the Generic Model. Proc. Asiacrypt'00, LNCS 1976, Springer-Verlag, pp. 458–469, 2000.

[FFS88] *U. Feige, A. Fiat and A. Shamir* : Zero-knowledge proofs of identity. Journal of Cryptology, 1 , pp. 77–94, 1988.

[FS87] *A. Fiat and A. Shamir* : How to Prove Yourself: Practical Solutions of Identification and Signature Problems. Proc. Crypto'86, LNCS 263, pp. 186–194, 1987.

[H97] *J. Håstad*: Some Optimal Inapproximability Results. Proc. ACM Symposium on Theory of Computing 1997, ACM Press, pp. 1–10, 1997.

[Ne94] *V.I. Nechaev*: Complexity of a Determinate Algorithm for the Discrete Logarithm. Mathematical Notes 55, pp. 165-172, 1994.

[O92] *T. Okamoto* : Provably Secure Identification Schemes and Corresponding Signature Schemes. Proc. Crypto'92, LNCS 740, Springer-Verlag, pp. 31–53, 1992.

[P98] *D. Pointcheval* : Strengthened Security for Blind Signatures. Proc. Eurocrypt'98 LNCS 1403, Springer Verlag, pp. 391–405, 1998.

[P00] *D. Pointcheval* : The Composite Discrete Logarithm and Secure Authentication. Proc. PKC'2000, LNCS 1751, Springer-Verlag, pp. 113–128, 2000.

[PS96a] *D. Pointcheval and J. Stern* : Security Proofs for Signature Schemes. Proc. Eurocrypt'96, LNCS 1070, Springer-Verlag, pp. 387–398, 1996.

[PS96b] *D. Pointcheval and J. Stern* : Provably Secure Blind Signature Schemes. Proc. Asiacrypt'96, LNCS 1163, Springer Verlag, pp. 387–393, 1996.

[PS00] *D. Pointcheval and J. Stern* : Security Arguments for Digital Signatures and Blind Signatures. Journal of Ctyptology, 13, 3, pp. 361–396, 2000.

[Sc91] *C.P. Schnorr* : Efficient Signature Generation for Smart Cards. Journal of Cryptology 4, pp. 161–174, 1991.

[SJ00] *C.P. Schnorr and M. Jakobsson* : Security of Signed ElGamal Encryption. Proc. Asiacrypt'00, LNCS, Springer-Verlag, 2000.

[Sc01a] *C.P. Schnorr* : Small Generic Hardcore Subsets for the Discrete Logarithm: Short Secret DL-Keys. Information and Processing Letters, 79, pp. 93–98, 2001.

[Sc01b] *C.P. Schnorr* : Security of DL-Encryption and Signatures Against Generic Attacks, a Survey. Proc. of Public-Key Cryptography and Computational Number Theory Conference, Warsaw Sept. 2000, Eds. K. Alster, H.C. Williams, J. Urbanowicz. De Gruyter GMBH, July, 2001.

[Sh97] *V. Shoup* : Lower Bounds for Discrete Logarithms and Related Problems. Proc. Eurocrypt'97, LNCS 1233, Springer-Verlag, pp. 256-266, 1997.