Enhancing the Security of Perfect Blind DL-Signatures.

Claus Peter Schnorr

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

December, 2003
Preliminary Version

Abstract. We enhance the security of Schnorr blind signatures against the novel one-more-forgery of SCHNORR [Sc01] and WAGNER [W02] which is possible even if the discrete logarithm is hard to compute. We show two limitations of this attack. Firstly, replacing the group G by the s-fold direct product $G^{\times s}$ increases the work of the attack, for a given number of signer interactions, to the s-power while increasing the work of the blind signature protocol merely by a factor s. Secondly, we bound the number of additional signatures per signer interaction that can be forged effectively. That fraction of the additional forged signatures can be made arbitrarily small.

1 Introduction and Summary

Blind signatures are a basic primitive for anonymous electronic cash. We study the security of SCHNORR blind signatures and OKAMOTO-SCHNORR blind signatures against the one-more-forgery in which an attacker interacts some l times with the legitimate signer and produces from these l interactions $l+1$ signatures. Let G be a group of prime order q for which the discrete logarithm (DL) is hard to compute, e.g. an elliptic / hyperelliptic curve or a group of units. The security of Schnorr blind signatures over G does not only require the hardness of the DL-problem. SCHNORR [Sc01] introduces the ROS-problem and shows that one-more-forgeries are easy for Schnorr blind and Okamoto-Schnorr blind signatures when an algorithm is given to solve the ROS-problem. WAGNER [W02] solves the ROS-problem for $l+1=2^t$ in $O(2^t\, q^{1/(t+1)})$-average time and space by a tree-like *general birthday method*. For $t=9$, $|G| \approx 2^{160}$ this attack succeeds in $O(2^{25})$ average time performing 2^9-1 interactions with the signer. We show two limitations of this attack.

Firstly, replacing a group G by its non-cyclic s-fold direct product $G^{\times s}$ enhances the security against general birthday attacks. For a given number of signer interactions, the work of the attack increases to the s-power while the work of the blind signature protocol merely increases by a factor s. E.g., the general birthday attack that succeeds in $O(2^{25})$ average time and $2^9 - 1$ interactions for a group G, $|G| \approx 2^{160}$, requires $O(2^{25\,s})$ average time for the product group $G^{\times s}$, for the same number of interactions.

Secondly, we bound the number of additional signatures per interaction that can be forged effectively by the new attack. The fraction of the additional forged signatures can be made arbitrarily small. For a given number of signer interactions, forging s additional signatures in an interleaved way requires work proportional to the s-power of the work for forging a single signature. Blind signatures differ from standard signatures in that forging two additional signatures may be infeasible, for a given number of signer interactions, even if a single additional signature can be forged with moderate work.

The critical resource for the general birthday attack is the number of interactions with the signer. The birthday attack requires many signer interactions to become efficient. This makes the attack pointless if the signer is willing to give away a few signatures for free rewarding a high volume of paid signatures. The birthday attack that forges a single signature in time 2^{25} with $2^9 - 1$ signer interactions amounts to an enforced 0.2 % *free rate* for a volume of 2^9 signatures. Such a small rebate for a high business volume is reasonable, if the attacker cannot easily increase the enforced rebate. We show that increasing the 0.2 % free rate by a factor s either increases the work 2^{25} of the attack to $2^{25\,s}$ or else requires to perform several, separate attacks with fewer interactions.

There are provably secure blind DL-signature protocols where the general birthday attack does not apply. However, the blind DL-signature protocols of Abe [A01] and of Pointcheval [P98] require additional public parameters and additional work. The [A01] scheme provides merely computational blindness, the [P98] scheme requires a third party checker and its security covers only synchronous attacks. This poses the question whether perfectly blind DL-signatures exist. Simplicity of the scheme is also important as it furthers its acceptance. A clear security result may help to combine the scheme with other cryptographic primitives. Therefore, Schnorr blind signatures remain attractive compared to more complicated blind signature schemes of [A01, P98].

2 Schnorr Blind Signatures for Direct Product Groups

We consider blind signatures as required for anonymous digital cash. Blind signatures are generated by an interaction with the signer in such a way that the signer cannot link the generated signature to the interaction.

Schnorr signatures refer to an arbitrary group G of prime order q, a generator g of G, an arbitrary message space M, and the field $\mathbf{Z}_q$ of integers modulo q. We first describe Schnorr signatures for the group G, and thereafter for the direct product group $G^{\times s}$, where signature verification consists of s independent verifications over G. Signatures will be based on strong hash functions $H : G \times M \to \mathbf{Z}_q$, resp., $\bar{H} : G^{\times s} \times M \to \mathbf{Z}_q^s$. Our security analysis assumes that $H, \bar{H}$ are modeled as random oracles.

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

Signatures. A Schnorr signature of a message m is a triple $(m, c, z) \in M \times \mathbf{Z}_q^2$ such that $H(g^z h^{-c}, m) = c$.

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 $H(g^z h^{-c}, m) = c$.

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 transmits a challenge $c \in \mathbf{Z}_q$, the signer replies 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 *reply* 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 that signature.

Extension to the s-fold direct product $G^{\times s}$. Let $G^{\times s} = G \times \cdots \times G$ denote the s-fold product of the group G with the componentwise group action.

Signatures for $G^{\times s}$. A Schnorr signature of message m is a triple $(m, \bar c, \bar z) \in M \times \mathbf{Z}_q^{s\times 2}$ such that $\bar H(g^{\bar z} h^{-\bar c}, m) = \bar c$. Here let $g^{\bar z} h^{-\bar c}$ denote $(g^{z_1} h^{-c_1}, ..., g^{z_s} h^{-c_s}) \in G^{\times s}$ for $\bar z = (z_1, ..., z_s)$, $\bar c = (c_1, ..., c_s) \in \mathbf{Z}_q^s$.

To sign a message m the signer picks a random $\bar r \in_R \mathbf{Z}_q^s$, computes $g^{\bar r} = (g^{r_1}, ..., g^{r_s})$, $\bar c := \bar H(g^{\bar r}, m)$ and $\bar z := \bar r + \bar c x$, and outputs the signature $(m, \bar c, \bar z)$.

Note that Schnorr signatures for $G^{\times s}$ merely use the secret/public parameters of Schnorr plain signatures. All further concepts like blind signatures translate in the obvious way from the group G to $G^{\times s}$.

Blind Signature Protocol for $G^{\times s}$. A protocol for generating a signature is called (perfectly) *blind* if the generated signature $(m, \bar c', \bar z')$ is statistically independent of the interaction $(r, \bar c, \bar z)$ that provides the view of the signer. Blind signatures cannot be linked to the signer interaction. The blindness concept is from [CP92].

To generate a blind signature $(m, \bar c', \bar z')$ the user picks random s-tuples $\bar\alpha, \bar\beta \in_R \mathbf{Z}_q^s$, and replies to the commitment $g^{\bar r} \in G^{\times s}$ of the legitimate signer by sending the challenge $\bar c = \bar H(g^{\bar r + \bar\alpha} h^{\bar\beta}, m) + \bar\beta \in \mathbf{Z}_q^s$. The signer answers by sending $\bar z = \bar r + \bar c x \in \mathbf{Z}_q^s$. Upon receipt the user computes $\bar z' := \bar z + \bar\alpha$, $\bar c' := \bar c - \bar\beta$, and gets the signature $(m, \bar c', \bar z')$.

signer $x \in \mathbf{Z}_q$		*user* $h = g^x \in G$
picks $\bar r \in_R \mathbf{Z}_q^s$	$\xrightarrow{g^{\bar r}}$	picks $\bar\alpha, \bar\beta \in_R \mathbf{Z}_q^s$
computes $g^{\bar r}$	$\xleftarrow{\bar c}$	$\bar c := H(g^{\bar r+\bar\alpha} h^{\bar\beta}, m) + \bar\beta$
$\bar z := \bar r + \bar c\, x$	$\xrightarrow{\bar z}$	$\bar z' := \bar z + \bar\alpha$, $\bar c' := \bar c - \bar\beta$

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

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

Informal Argument for the Enhanced Security by $G^{\times s}$. For a random function $\bar{H}$ the components $H_1(\bar{f}, m), ..., H_s(\bar{f}, m) \in \mathbf{Z}_q$ of

$$\bar{H}(\bar{f}, m) = (H_1(\bar{f}, m), ..., H_s(\bar{f}, m))$$

are statistically independent even for particular choices of $\bar{f}$ where e.g., $f_1 = ... = f_s$. The verification $\bar{H}(g^{\bar{z}} h^{-\bar{c}}, m) = \bar{c}$ consists of statistically independent equations $H_i(g^{\bar{z}} h^{-\bar{c}}, m) = c_i$ for $i = 1, ..., s$.

Informally, the birthday method of [W02] applies to random $(s \lg q)$-bit strings $\bar{H}(\bar{f}, m)$ whereas, in the case of signatures for G, it applies to the $\lg q$-bit string $H(f, m)$. This increases the work of the attacks to the s-power, see Section 4.1 for a formal proof. While $G^{\times s}$ improves the security against the birthday attack the complexity of the DL-problem remains unchanged. The s-fold DL-problem for $G^{\times s}$ amounts to solve s DL-problems for G.

3 The Generic Parallel Attack on Blind Signatures

We recall in Section 3.1 the generic attack from [Sc01] when given an algorithm to solve the ROS-problem. We review in Section 3.2 WAGNER's solution of the ROS-problem as a 2^t-sum problem over $\mathbf{Z}_q$.

3.1 One-More-Forgeries by Solving the ROS-Problem.

First, we present the generic attack for Schnorr blind signatures, and thereafter for Okamoto-Schnorr blind signatures. Okamoto-Schnorr signatures do not protect better against the generic attack than Schnorr blind signatures. The generic attack for Schnorr blind signatures uses a solution of the

ROS-problem over $\mathbf{Z}_q$: 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 $c_1, ..., c_l \in \mathbf{Z}_q$:

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

For the generic attack we let $F(a_{k,1}, ..., a_{k,l}) = H(f_k, m_k)$ for $f_k = g_1^{a_{k,1}} \cdots g_l^{a_{k,l}}$ and an arbitrary message m_k.

The attack against Schnorr blind 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_k, and computes $f_k = g_1^{a_{k,1}} \cdots g_l^{a_{k,l}}$, $H(f_k, m_k)$ for $k = 1, ..., \tau$. Then $\mathcal{A}$ solves $l+1$ out of the τ equations (2) in the unknowns $c_1, .., c_l$ over $\mathbf{Z}_q$:

$$a_{k,1}\, c_1 + \cdots + a_{k,l}\, c_l = H(f_k, m_k). \tag{2}$$

$\mathcal{A}$ 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

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

Correctness. The equations (2) imply that

$$g^{z_k'} h^{-c_k'} = g_1^{a_{k,1}} \cdots g_l^{a_{k,l}} = f_k \quad \text{and} \quad H(g^{z_k'} h^{-c_k'}, m_k) = c_k'.$$

The attack is generic, it works for arbitrary groups with an efficient multiplication, it is intrinsic parallel. We call it the *generic, parallel attack*.

The aattack against Okamoto-Schnorr blind 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 $(m, \varepsilon, \rho, \sigma)$
$\in M \times \mathbf{Z}_q^3$ 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 $f_k = g_1^{a_{k,1}} \cdots g_l^{a_{k,l}}$ and $H(f_k, m_k)$ for $k = 1, ..., \tau$. $\mathcal{A}$ solves $l+1$ of the τ 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

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

$\mathcal{A}$ gets a valid signature $(m_k, \varepsilon_k, \rho_k, \sigma_k)$ by setting

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

Correctness. From the equations (2) we get that

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

3.2 The ROS-Problem and the 2^t-Sum Problem.

The classic birthday method finds a collision in a large list of n bit integers that are drawn uniformly at random in $O(2^{n/2})$ average time. *Wagner's 2^t-sum algorithm* [W02] generalizes the birthday method to solve the following
2^t*-sum problem* over $\mathbf{Z}_2^n \cong \{0,1\}^n$: Given 2^t lists $L_1, \ldots, L_{2^t}$ of elements drawn uniformly and independently at random from $\{0,1\}^n$ find $x_1 \in L_1, \ldots, x_{2^t} \in L_{2^t}$ such that $x_1 \oplus \cdots \oplus x_{2^t} = 0$.

Wagner's algorithm solves the 2^t-sum problem over $\mathbf{Z}_2^n$ in $O(2^t\, 2^{\frac{n}{1+t}})$ average time and space. For $t = 2$ the algorithm runs in $O(2^{n/3})$ time improving the $O(2^{n/2})$ bound of previous algorithms. Wagner's algorithm extends to the case that the group $\mathbf{Z}_2$ is replaced by the group $\mathbf{Z}_q$ for an arbitrary integer q.

For the 2^t-*sum problem* over $\mathbf{Z}_q^n$ we are given lists $L_1, ..., L_{2^t}$ of independent random elements of $\mathbf{Z}_q^n$ and search for $x_1 \in L_1, ..., x_{2^t} \in L_{2^t}$ such that $x_1 + \cdots + x_{2^t} = 0$. The general birthday method solves this problem in $O(2^t q^{\frac{n}{t+1}})$ average time. This upper bound is also a lower bound for Wagner's algorithm which requires $2^t q^{\frac{n}{t+1}}$ average time. The 2^t-sum problem gets easier as t increases. While this holds for powers of 2, the m-sum problem for $2^t < m < 2^{t+1}$ can be solved as the harder 2^t-sum problem, and more efficient solutions are unknown.

It is open whether Wagner's general birthday method is optimal for the 2^t-sum problem. The 2^t-sum problem over $\mathbf{Z}_q^s$ has an information theoretic lower bound $\Omega(q^{s/2^t})$, and thus its complexity is likely to be $\Theta(q^{s/c(t)})$ for some function $c(t)$.

Solution of the ROS-*problem with* $l + 1 = 2^t$. Consider for simplicity the case $l = 3$. Solving the ROS-problem means to find a matrix

$$A = \begin{bmatrix} a_{1,1}, & a_{1,2}, & a_{1,3}, & H(f_1, m_1) \\ a_{2,1}, & a_{2,2}, & a_{2,3}, & H(f_2, m_2) \\ a_{3,1}, & a_{3,2}, & a_{3,3}, & H(f_3, m_3) \\ a_{4,1}, & a_{4,2}, & a_{4,3}, & H(f_4, m_4) \end{bmatrix} \in \mathbf{Z}_q^{4 \times 4}$$

so that the corresponding four linear equations (2) in c_1, c_2, c_3 are solvable. Solvability means that the last column vector of A is a linear combination of the first three columns. If the first three columns of A are linearly independent the four linear equations (2) are solvable if and only if $\det(A) = 0$. Developing the determinant along the 4-th column yields the equation

$$\textstyle\sum_{k=1}^{4} (-1)^k A_k H(f_k, m_k) = 0, \tag{3}$$

where A_k is the determinant of the 3×3-submatrix obtained from A by removing the k-th row and the last column. Solving the linear equation (3) for given constant non-zero coefficients A_k is an instance of the 4-sum problem over $\mathbf{Z}_q$: fill list L_k with candidates for $A_k H(f_k, m_k)$ for $k = 1, ..., 4$ and search for a solution to $x_1 + \cdots + x_4 = 0$ with $x_k \in L_k$. The 4-list algorithm solves Equation (3) in $O(q^{1/3})$ average time. Note that we let m_k vary for distinct candidates of L_k while keeping $f_k, a_{1,k}, a_{2,k}, a_{3,k}$ determined by k. So we get many candidate values $H(f_k, m_k)$ for each k. Alternatively, we can let $f_k, a_{1,k}, a_{2,k}, a_{3,k}$ vary for distinct candidates of L_k while keeping m_k determined by k.

Extending this method to arbitrary values $l + 1 = 2^t$ proves Theorem 1.

Theorem 1. [W02] *The ROS-problem for $l + 1 = 2^t$ can be solved as a 2^t-sum problem over $\mathbf{Z}_q$.*

Simplification of Equation (3). The ROS-solution of Theorem 1 allows to freely choose the matrix entries $a_{k,\ell} \in \mathbf{Z}_q$ so that the coefficients A_k in (3), resp. in (4) for general l, are all non-zero. Zero coefficients A_k must be avoided as sum problems with fewer terms are harder to solve.

The particular matrix choice $a_{l+1,i} := -a_{i,i}$ for $i = 1, ..., l$, $a_{i,j} := 0$ for $i \neq j$, $i \leq l$ yields the equation $\sum_{k=1}^{l+1} H(f_k, m_k) = 0$ for arbitrary l.

Reducing the 2^t-sum problem to the ROS-problem. Solving the 2^t-sum problem as an ROS-problem is possible for a particular class of ROS-algorithms and for a novel type of reduction. Consider the particular ROS-algorithms that generate constant coefficients A_k in (3), (4) that do not depend on H.

Solving the 2^t-sum problem by ROS-algorithms with constant coefficients A_k. Consider an arbitrary ROS-algorithm producing an ROS-solution matrix $A' = [a_{k,\ell}]_{k,\ell} \in \mathbf{Z}_q^{(l+1)\times l}$ with right sides $H(f_k, m_k)$. Assuming that A' has maximal rank l this yields a solution of the equation

$$\sum_{k=1}^{l+1} (-1)^k A_k H(f_k, m_k) = 0, \tag{4}$$

where A_k is the determinant of the $l \times l$-submatrix obtained from A' by removing the k-th row.

Suppose that the A_k do not depend on H. We can assume w.l.o.g. that all A_k are non-zero, otherwise Equation (4) gets harder to solve. The ROS-algorithm must try many candidates for each random element $H(f_k, m_k)$. If the ROS-algorithm tries q_k candidates for $H(f_k, m_k)$ we must have that $q_1 \cdots q_{l+1} \geq q$ because Equation (4) holds with probability $\frac{1}{q}$ for each choice of candidates. Let L_k denote the set of candidates for $H(f_k, m_k)$. Then the ROS-algorithm solves the 2^t-sum problem for the lists $A_1 L_1, ..., A_{2^t} L_{2^t}$. This proves the reduction as the lists $A_k L_k$ consist of random elements that are drawn independently from $\mathbf{Z}_q$.

This is a novel type of reduction for computational problems with random inputs. The coefficients $A_1, ..., A_{l+1}$ generated by the ROS-algorithm are used to transform the probability space of the 2^t-sum problem consisting of the lists $L_1, ..., L_{2^t}$. This transform multiplies the elements of L_k by A_k, it preserves probabilities since the transform is invertible.

The case of non-constant coefficients A_k. In general the coefficients A_k in (4) may depend on H as the coefficients $a_{k,\ell}$ may arbitrarily depend on previously drawn random elements $H(f_{k'}, m_{k'})$. However, $H(f_k, m_k)$ is statistically independent of $a_{k,1}, ..., a_{k,l}$. A coefficient vector $\boldsymbol{A} = (A_1, ..., A_{l+1})$ associated with the ROS-solution occurs with some probability $\Pr_H[\boldsymbol{A}]$ depending on the random H and the choices of the ROS-algorithm. For an ROS-algorithm running in average time $q^{1/t+1}$ some coefficient vector $\boldsymbol{A}$ must have probability $\Pr_H[\boldsymbol{A}] \geq q^{-\frac{1}{l+1}}$. Such $\boldsymbol{A}$ must be tested by the ROS-algorithm for at least $q^{1-\frac{1}{l+1}}$ hash tuples $\boldsymbol{H} = (H(f_1, m_1), ..., H(f_{l+1}, m_{l+1}))$ since Equation (4) holds with probability $\frac{1}{q}$ for each hash tuple. Therefore, ROS-algorithms running in time $q^{1/t+1}$ must select the matrix entries $a_{k,\ell}$ to focus the resulting $\boldsymbol{A}$ on a few vectors.

It seems that testing hash tuples $\boldsymbol{H}$ for several coefficient vectors $\boldsymbol{A}$ is more difficult than testing for a single $\boldsymbol{A}$ as does the 2^t-sum algorithm. This indicates that variable vectors $\boldsymbol{A}$ dont help. We conjecture that the most efficient general ROS-algorithms generate constant vectors $\boldsymbol{A}$ that do not depend on H.

3.3 Complexity of the Generic Attack.

The Generic Group Model with Random Hashes. Generic group algorithms for G do not use the binary encodings of the group elements, they access group elements only for group operations, equality tests, and random hashes. NECHAEV [Ne94] proves that the discrete logarithm problem is hard in such a model. SHOUP [Sh97] extends the Nechaev argument to further generic complexity lower bounds. He introduces a random encoding $\sigma : G \to S$ of group elements into random binary strings. Curiously, the security proofs of Shoup [Sh97] do not depend on the random σ even though [Sh97] suggests otherwise. SCHNORR AND JAKOBSSON [SJ00],[Sc01] have eliminated the random σ from the generic group model. In addition they assume that hash functions, required for various applications, are independent random functions modeled as random oracles. We call this the *generic group model with random hashes* (GM+ROM). Security proofs in this strong proof model merely exclude *generic attacks.* Contrary to the claims of some anonymous referees, we are not aware of any non generic attack to a reasonable cryptosystem. However, non generic attacks are known for artificial protocols [CGH98, F00].

Theorem 2 [Sc01, Thm 2] gives a sharp security lower bound for generic attacks on Schnorr blind signatures. It shows that Schnorr signatures are secure against generic attacks if both the DL-problem and the ROS-problem are computationally hard.

Theorem 2. [Sc01, Thm 2] *Let a generic adversary $\mathcal{A}$ be given the generator g, the random public key h, an oracle for H. Let $\mathcal{A}$ perform τ generic steps including l signer interactions. If $\mathcal{A}$ succeeds to produce $l+1$ blind signatures for G with a better probability of success than $\binom{\tau}{2}/q$ then $\mathcal{A}$ must find a solvable system of $l+1$ equations (2) for the unknowns $c_1, ..., c_l \in \mathbf{Z}_q$. The probability space consists of h, H and the random coins of the signer.*

4 Security of Blind Signatures for $G^{\times s}$.

The generic attack, with l interactions and τ generic steps, on Schnorr blind signatures requires a solution of the

ROS-problem over $\mathbf{Z}_q^s$: Given an oracle random function $\bar{F} : \mathbf{Z}_q^{l \times s} \to \mathbf{Z}_q^s$, find coefficients $\bar{a}_{k,\ell} \in \mathbf{Z}_q^s$ and a solvable system of $l+1$ out of τ distinct equations $(\bar{1})$ in the unknowns $\bar{c}_1, ..., \bar{c}_l \in \mathbf{Z}_q^s$:

$$\bar{a}_{k,1}\,\bar{c}_1 + \cdots + \bar{a}_{k,l}\,\bar{c}_l = \bar{F}(\bar{a}_{k,1}, ..., \bar{a}_{k,l}). \tag{$\bar{1}$}$$

For the generic attack let $\bar{F}(\bar{a}_{k,1}, ..., \bar{a}_{k,l}) = \bar{H}(\bar{f}_k, m_k)$ for $\bar{f}_k = \bar{g}_1^{\bar{a}_{k,1}} \cdots \bar{g}_l^{\bar{a}_{k,l}}$ and for an arbitrary message m_k.

The attack against Schnorr blind signatures for $G^{\times s}$. The signer sends commitments $\bar{g}_1 = g^{\bar{r}_1}, ..., \bar{g}_l = g^{\bar{r}_l} \in G^{\times s}$. The attacker $\mathcal{A}$ selects $\bar{a}_{k,1}, ..., \bar{a}_{k,l} \in \mathbf{Z}_q^s$ and messages m_k, and computes $\bar{f}_k = \bar{g}_1^{\bar{a}_{k,1}} \cdots \bar{g}_l^{\bar{a}_{k,l}}$ and $\bar{H}(\bar{f}_k, m_k)$ for $k = 1, ..., \tau$.

Then $\mathcal{A}$ solves $l+1$ out of the τ equations $(\bar{2})$ in the unknowns $\bar{c}_1, .., \bar{c}_l$ over $\mathbf{Z}_q^s$:

$$\sum_{\ell=1}^{l} \bar{a}_{k,\ell}\, \bar{c}_\ell = \bar{H}(\bar{f}_k, m_k). \qquad (\bar{2})$$

$\mathcal{A}$ sends the solutions $\bar{c}_1, ..., \bar{c}_l$ as challenges to the signer. The signer sends back $\bar{z}_\ell := \bar{r}_\ell + \bar{c}_\ell x \in \mathbf{Z}_q^s$ for $\ell = 1, ..., l$. For each solved equation $(\bar{2})$, the attacker gets a valid signature $(m_k, \bar{c}'_k, \bar{z}'_k)$ by setting

$$\bar{c}'_k := \sum_{\ell=1}^{l} \bar{a}_{k,\ell}\, \bar{c}_\ell = \bar{H}(\bar{f}_k, m_k) \quad \text{and} \quad \bar{z}'_k := \sum_{\ell=1}^{l} \bar{a}_{k,\ell} \bar{z}_\ell.$$

Correctness. The equations $(\bar{2})$ imply that

$$g^{\bar{z}'_k} h^{-\bar{c}'_k} = \bar{g}_1^{\bar{a}_{k,1}} \cdots \bar{g}_l^{\bar{a}_{k,l}} = \bar{f}_k \quad \text{and} \quad \bar{H}(g^{\bar{z}'_k} h^{-\bar{c}'_k}, m_k) = \bar{c}'_k.$$

Corollary 1. *A generic adversary that performs τ generic steps and produces from l signer interactions $l+1$ Schnorr blind signatures for $G^{\times s}$ with a better probability of success than $\binom{\tau}{2}/q$ must find a solvable system of $l+1$ out of τ linear equations $(\bar{2})$ in l unknowns, with unknowns and coefficients in $\mathbf{Z}_q^s$, and statistically independent right sides.*

Proof. The proof of Theorem 2 [Sc01] extends from G to $G^{\times s}$. Schnorr blind signatures for $G^{\times s}$ of message m_k, constructed from l signer interactions with challenges $\bar{c}_1, ..., \bar{c}_l \in \mathbf{Z}_q^s$, require distinct equations $\sum_{\ell=1}^{l} \bar{a}_{k.\ell}\, \bar{c}_\ell = \bar{H}(\bar{f}_k, m_k)$. A generic attack that generates $l+1$ signatures from l signer iteractions must find $l+1$ solvable equations $(\bar{2})$ for $\bar{c}_1, ..., \bar{c}_l$. The right side $\bar{H}(\bar{f}_k, m_k)$ of these equations consists of independent random numbers in $\mathbf{Z}_q^s$. Hence the claim. □

Theorem 3. *Finding a solvable system of $l+1$ linear equations $(\bar{2})$ as in Corollary 1 can be solved as an $l+1$-sum problem over $\mathbf{Z}_q^s$, and requires $2^t q^{\frac{s}{t+1}}$ average time for the general birthday method with $l+1 = 2^t$.*

Proof. The attacker must find a solvable system of $l+1$ equations

$$\sum_{\ell=1}^{l} \bar{a}_{k,\ell}\, \bar{c}_\ell = \bar{H}(\bar{f}_k, m_k), \qquad (\bar{2})$$

with coefficients and unknowns in $\mathbf{Z}_q^s$. Consider the matrix

$$\bar{A} = \begin{bmatrix} \bar{a}_{1,1} & \cdots & \bar{a}_{1,l} & \bar{H}(\bar{f}_1, m_1) \\ \vdots & & \vdots & \vdots \\ \bar{a}_{l,1} & \cdots & \bar{a}_{l,l} & \bar{H}(\bar{f}_l, m_l) \\ \bar{a}_{l+1,1} & \cdots & \bar{a}_{l+1,l} & \bar{H}(\bar{f}_{l+1}, m_{l+1}) \end{bmatrix}.$$

The matrix $\bar{A} = (A_1, ..., A_s) \in (\mathbf{Z}_q^s)^{(l+1)\times(l+1)}$ consists of component matrices $A_i \in \mathbf{Z}_q^{(l+1)\times(l+1)}$ whose entries are the i-th components of the entries of $\bar{A}$. Each linear equation for $\bar{c}_1, ..., \bar{c}_l \in \mathbf{Z}_q^s$ corresponds to s separate linear equations for the components $c_{\ell,i} \in \mathbf{Z}_q$ of $\bar{c}_\ell$ for $i = 1, ..., s$. W.l.o.g. let the matrices A_i all have rank l. Then the $l+1$ equations $(\bar{2})$ are solvable if and only if $\det(A_i) = 0$ for $i = 1, ..., s$.

These determinant equations can be written as a system of s linear equations

$$\sum_{k=1}^{l+1}(-1)^k A_{k,i} H_i(\bar{f}_k, m_k) = 0 \quad \text{for } i = 1, ..., s, \tag{5}$$

where the coefficient $A_{k,i} \in \mathbf{Z}_q$ is the determinant of the $l \times l$-submatrix that is obtained from A_i by removing the k-th row and the last column. While the $A_{k,i}$ may depend on H we consider the case that the $A_{k,i}$ are constant. Solving the equations (5) for given $\bar{A} \in \mathbf{Z}_q^{s \times (l+1) \times (l+1)}$ amounts to solve an $l+1$-sum problem over $\mathbf{Z}_q^s$. For this we fill the list L_k with candidates $((-1)^k A_{k,i} H_i(\bar{f}_k, m_k))_{i=1,...,s} \in \mathbf{Z}_q^s$ for $k = 1, ..., l+1$. These candidates are independent random elements in $\mathbf{Z}_q^s$. Note that we let m_k vary for distinct candidates while keeping $\bar{a}_{k,1}, ..., \bar{a}_{k,l}, \bar{f}_k$ determined by k. Hence, the claim. □

5 Forging s Additional Signatures in an Interleaved Way.

We study the problem of forging s additional signatures for a given number l of interactions by the general birthday method. Theorem 2 yields the following

Corollary 2. *Any generic attack that performs τ generic steps and produces from l signer interactions $l + s$ Schnorr blind signatures for G with a better probability of success than $\binom{\tau}{2}/q$ must find a solvable system of $l + s$ out of τ linear equations (2) over $\mathbf{Z}_q$.*

Proof. A Schnorr signature (m_k, c', z') that is constructed by the generic parallel attack using l signer interactions with challenges $c_1, ..., c_l$ is of the form $c' = \sum_{\ell=1}^{l} a_{k,\ell} c_\ell$, $z' = \sum_{\ell=1}^{l} a_{k,\ell} z_\ell$ and the challenges $c_1, ..., c_l$ must satisfy the corrresponding equation

$$\sum_{\ell=1}^{l} a_{k,\ell}\, c_\ell = H(f_k, m_k) \quad \text{for} \quad f_k = g_1^{a_{k,1}} \cdots g_l^{a_{k,l}} \tag{2}$$

from a system of τ such equations for $k = 1, ..., \tau$, see the proof of Theorem 1 [Sc01]. A generic attack that generates $l + s$ signatures from l signer iteractions must set up the corresponding $l + s$ equations so that they are solvable. The right sides $H(f_k, m_k)$ are independent random numbers as H is a random function. □

By Corollary 2 an efficient generic attacker must generate a solvable system of $l + s$ linear equations (2) over $\mathbf{Z}_q$. The fastest known attack is to forge in s separate attacks one additional signature per attack. For this the attacker solves s ROS-problems for $l_1, ..., l_s$ signer interactions, where $\sum_{i=1}^{s} l_i = l$. Of course one-more-forgeries with fewer interactions are less efficient and s separate attacks require that $s \leq l$. Next, we study fully interleaved attacks.

Theorem 4. *The problem of producing a solvable system of $l+s$ linear equations as required in Corollary 2 can be solved as an $(l+1)$-sum problem over $\mathbf{Z}_q^s$ in $O(\,2^t q^{\frac{s}{t+1}})$ average time by the general birthday method for $l + 1 = 2^t$.*

Proof. We show how to construct a solvable system of $l+s$ equations (2) with an $(l+s)\times l$–matrix $A' = [a_{k,\ell}]_{k,\ell} \in \mathbf{Z}_q^{(l+s)\times l}$ of rank l. If $rank(A') = l$ the corresponding $l+s$ equations (2) are solvable if and only if the $(l+s)\times(l+1)$-matrix A, extending A' by the right sides $H(f_k, m_k)$, has rank l too. That means that the following determinants must vanish

$$\det \begin{bmatrix} a_{1,1} & \cdots & a_{1,l} & H(f_1, m_1) \\ \vdots & & \vdots & \vdots \\ a_{l,1} & \cdots & a_{l,l} & H(f_l, m_l) \\ a_{l+j,1} & \cdots & a_{l+j,l} & H(f_{l+j}, m_{l+j}) \end{bmatrix} = 0 \quad \text{for } j = 1, \ldots, s.$$

We simplify these determinant equations by setting $a_{i,j} := 0$ for $i \neq j$, $i \leq l$, and $a_{l+j,k} = -a_{k,k} \cdot b_{k,j}$ for $k = 1,..,l$ and independent random multipliers $b_{k,j} \in_R \mathbf{Z}_q$. Then the determinant equations become

$$\textstyle\sum_{k=1}^{l} b_{k,j} H(f_k, m_k) + H(f_{l+j}, m_{l+j}) = 0 \quad \text{for } j = 1, \ldots, s. \tag{6}$$

In order to solve these equations as an $l+1$-sum problem over $\mathbf{Z}_q^s$ for $l+1 = 2^t$ we apply the 2^t-sum algorithm to the following lists $L_1, \ldots, L_{l+1}$ with elements

$$(b_{k,1}H(f_k, m_k), ..., b_{k,s}H(f_k, m_k)) \in \mathbf{Z}_q^s \quad \text{for } L_1, ..., L_l,$$
$$(H(f_{l+1}, m_{l+1}), \ldots, H(f_{l+s}, m_{l+s})) \in \mathbf{Z}_q^s \quad \text{for } L_{l+1}.$$

Here we let $H(f_1, m_1), ..., H(f_l, m_l) \in \mathbf{Z}_q \setminus \{0\}$ be constant whereas the $b_{k,j}$ and the $H(f_{l+j}, m_{l+j})$ vary over independent random numbers in $\mathbf{Z}_q$. The list L_{l+1} consists of independent random elements in $\mathbf{Z}_q^s$ due to the random H. The lists $L_1, ..., L_l$ consist of independent random elements due to the random multipliers $b_{k,j}$. As the lists $L_1, ..., L_{l+1}$ consist of independent random elements os $\mathbf{Z}_q^s$ the general birthday method solves the equations (6) in $O(\,2^t q^{\frac{s}{t+1}})$ average time. □

Theorem 4 studies a typical fully interleaved attack to forge s additional signatures. For an arbitrary attack the equations (6) take the form

$$\textstyle\sum_{k=1}^{l} A_{k,j} H(f_k, m_k) + A_{0,0} H(f_{l+j}, m_{l+j}) = 0 \quad \text{for } j = 1, ..., s,$$

where $A_{k,j}$ for $k \neq 0$ is the determinant of the $l \times l$-submatrix obtained from A' by removing row (numbered) k and rows $l+1, ..., l+s$ except for row $l+j$, and $A_{0,0}$ is the determinant of the $l \times l$-matrix consisting of the first l rows of A'. Particular easy instances of such equations occur for constant coefficients $A_{k,j}$ that partition the s equations into classes depending on disjoint sets of hash values. No other easy instances exist for constant $A_{k,j}$, and we conjecture that this is also true for non-constant $A_{k,j}$ that depend on H.

5.1 The Enforcable Free Rate

We study the maximal *free rate* that an attacker can enforce in $\sqrt{q}$ average time. The free rate is the number of additionally forged Schnorr blind signatures divided by the number of signer interactions. Using $\tau = \sqrt{q}$ generic steps the attacker can recover the secret key $x = \log_g h$ from h with no better probability than $\binom{\tau}{2}/q \approx \frac{1}{2}$ (Theorem 2). Therefore, the attacker is bound to one-more-forgeries via ROS-solutions (Theorem 2).

Solving the ROS-problem over $\mathbf{Z}_q$ for $l = 2^t - 1$ signer interactions via Wagner's general birthday method requires $2^t q^{\frac{1}{t+1}}$ average time. Forging one additional signature for $G^{\times s}$ and $2^t - 1$ interactions requires $2^t q^{\frac{s}{t+1}}$ average time (Theorem 3), surpassing the $\sqrt{q}$ time bound for $t \leq 2s - 1$. We see that $2^{2s} - 1$ interactions with the signer are required to forge one additional signature for $G^{\times s}$ in $\sqrt{q}$ time by the general birthday method. Forging more than one additional signature in a fully interleaved way is even more difficult (Theorem 4). This proves

Theorem 5. *The free rate of Schnorr blind signatures for $G^{\times s}$ that is enforcable by the general birthday method in $\sqrt{q}$ average time is at most* $1/(2^{2s} - 1)$.

E.g., at most one additional signature for $G^{\times 3}$ can be forged using $2^6 - 1 = 65$ signer interactions. This corresponds to an enforced free rate of $\frac{1}{65} \approx 1.5\%$ for a volume of 65 paid signatures. If the signer accepts an 1.5% free rate then Schnorr blind signatures are more efficient than the computationally blind signatures of Abe [A01]. Schnorr blind signature generation costs 3 exponentiations for each of the signer and the user, i.e., 6 exponentiations in total. Signature generation according to [A01] requires a total of 9 exponentiations and additional overhead for the public parameters.

References

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

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

[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.

[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.

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

[PS00] *D. Pointcheval and J. Stern* : Security Arguments for Digital Signatures and Blind Signatures. Journal of Cryptology, 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 1976, Springer-Verlag, pp. 73-89, 2000.

[Sc01] *C.P. Schnorr* : Security of Blind Discrete Log Signatures Against Interactive Attacks. ICICS 2001, LNCS 2229, Springer-Verlag, pp. 1-12, 2001.

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

[W02] *D. Wagner*, A Generalized Birthday Problem. Proceedings Crypto'02, LNCS 2442, Springer-Verlag, pp. 288-303, 2002.