

The Digital Signature Scheme MQQ-SIG

Intellectual Property Statement and Technical Description

10 October 2010

Danilo Gligoroski¹ and Svein Johan Knapskog² and Smile Markovski³ and Rune Steinsmo Ødegård²
and Rune Erlend Jensen² and Ludovic Perret⁴ and Jean-Charles Faugère⁵

¹ Department of Telematics, Faculty of Information Technology, Mathematics and Electrical Engineering,
The Norwegian University of Science and Technology (NTNU), O.S.Bragstads plass 2E, N-7491 Trondheim,
NORWAY, daniilog@item.ntnu.no

² Norwegian University of Science and Technology Centre for Quantifiable Quality of Service in
Communication Systems. O.S. Bragstads plass 2E, N-7491 Trondheim, NORWAY, knapskog@q2s.ntnu.no,
rune.odegard@q2s.ntnu.no, runeerle@stud.ntnu.no

³ “Ss Cyril and Methodius” University, Faculty of Natural Sciences and Mathematics, Institute of
Informatics, P.O.Box 162, 1000 Skopje, MACEDONIA, smile@ii.edu.mk

⁴ Pierre and Marie Curie University - Paris, Laboratory of Computer Sciences, Paris 6, 104 avenue du
Président Kennedy 75016 Paris FRANCE, ludovic.perret@lip6.fr

⁵ UPMC, Université Paris 06, LIP6 INRIA, Centre Paris-Rocquencourt, SALSA Project-team CNRS, UMR
7606, LIP6 4, place Jussieu 75252 Paris, Cedex 5, FRANCE jean-charles.faugere@inria.fr

Abstract: This document contains the Intellectual Property Statement and the technical description of the MQQ-SIG - a new public key digital signature scheme. The complete scientific publication covering the design rationale and the security analysis will be given in a separate publication. MQQ-SIG consists of $n - \frac{n}{4}$ quadratic polynomials with n Boolean variables where $n = 160, 196, 224$ or 256 .

Keywords: Public Key Cryptosystems, Fast signature generation, Multivariate Quadratic Polynomials, Quasigroup String Transformations, Multivariate Quadratic Quasigroup

1 Intellectual Property Statement

We, the seven names given in the title of this document and undersigned on this statement, the authors and designers of MQQ-SIG digital signature scheme, do hereby agree to grant any interested party an irrevocable, royalty free licence to practice, implement and use MQQ-SIG digital signature scheme, provided our roles as authors and designers of the MQQ-SIG digital signature scheme are recognized by the interested party as authors and designers of the MQQ-SIG digital signature scheme.

Name	Signature	Place	Date
1. Danilo Gligoroski	-----	Trondheim	-----
2. Svein Johan Knapskog	-----	Trondheim	-----
3. Smile Markovski	-----	Skopje	-----
4. Rune Steinsmo Ødegård	-----	Trondheim	-----
5. Rune Erlend Jensen	-----	Trondheim	-----
6. Ludovic Perret	-----	Paris	-----
7. Jean-Charles Faugère	-----	Paris	-----

2 Description of the MQQ-SIG digital signature scheme

A generic description for our scheme can be expressed as a $\frac{3}{4}$ truncation of a typical multivariate quadratic system: $\mathbf{S} \circ P' \circ \mathbf{S}' : \{0, 1\}^n \rightarrow \{0, 1\}^n$ where $\mathbf{S}' = \mathbf{S} \cdot \mathbf{x} + \mathbf{v}$ (i.e. \mathbf{S}' is a bijective affine transformation), \mathbf{S} is a nonsingular linear transformation, and P' is a bijective multivariate quadratic mapping on $\{0, 1\}^n$.

The bijective multivariate quadratic mapping $P' : \{0, 1\}^n \rightarrow \{0, 1\}^n$ is defined in Table 1.

Bijjective multivariate quadratic mapping $P'(\mathbf{x})$
Input: A vector $\mathbf{x} = (f_1, \dots, f_n)$ of n linear Boolean functions of n variables. We implicitly suppose that a multivariate quadratic quasigroup $*$ is previously defined, and that $n = 32k$, $k \in \{5, 6, 7, 8\}$ is also previously determined.
Output: 8 linear expressions $P'_i(x_1, \dots, x_n), i = 1, \dots, 8$ and $n - 8$ multivariate quadratic polynomials $P'_i(x_1, \dots, x_n), i = 9, \dots, n$
<ol style="list-style-type: none"> 1. Represent a vector $\mathbf{x} = (f_1, \dots, f_n)$ of n linear Boolean functions of n variables x_1, \dots, x_n, as a string $\mathbf{x} = X_1 \dots X_{\frac{n}{8}}$ where X_i are vectors of dimension 8; 2. Compute $\mathbf{y} = Y_1 \dots Y_{\frac{n}{8}}$ where: $Y_1 = X_1$, $Y_{j+1} = X_j * X_{j+1}$, for even $j = 2, 4, \dots$, and $Y_{j+1} = X_{j+1} * X_j$, for odd $j = 3, 5, \dots$ 3. Output: \mathbf{y}.

Table 1. Definition of the bijective multivariate quadratic mapping $P' : \{0, 1\}^n \rightarrow \{0, 1\}^n$

The algorithm for generating the public and private key is defined in the Table 2.

Algorithm for generating Public and Private key for the MQQ-SIG scheme
Input: Integer n , where $n = 32 \times k$ and $k \in \{5, 6, 7, 8\}$.
Output: Public key \mathbf{P} : $n - \frac{n}{4}$ multivariate quadratic polynomials $P_i(x_1, \dots, x_n), i = 1 + \frac{n}{4}, \dots, n$, Private key: Two permutations σ_1 and σ_K of the numbers $\{1, \dots, n\}$, and 81 bytes for encoding a quasigroup $*$.
<ol style="list-style-type: none"> 1. Generate an MQQ $*$ according to equations (1) ... (4). 2. Generate a nonsingular $n \times n$ Boolean matrix \mathbf{S} and affine transformation \mathbf{S}' according to equations (5), ..., (11). 3. Compute $\mathbf{y} = \mathbf{S}(P'(\mathbf{S}'(\mathbf{x})))$, where $\mathbf{x} = (x_1, \dots, x_n)$. 4. Output: The public key is \mathbf{y} as $n - \frac{n}{4}$ multivariate quadratic polynomials $P_i(x_1, \dots, x_n) i = 1 + \frac{n}{4}, \dots, n$, and the private key is the tuple $(\sigma_1, \sigma_K, *)$.

Table 2. Generating the public and private key

The algorithm for signing by the private key $(\sigma_1, \sigma_K, *)$ is defined in Table 3.

Algorithm for digital signature with the private key $(\sigma_1, \sigma_K, *)$
Input: A document M to be signed.
Output: A signature $\mathbf{sig} = (x_1, \dots, x_n)$.
<ol style="list-style-type: none"> 1. Compute $\mathbf{y} = (y_1, \dots, y_n) = H(M) _n$, where M is the message to be signed, $H()$ is a standardized cryptographic hash function such as SHA-1, or SHA-2, with a hash output of not less than n bits. The notation $H(M) _n$ denotes the least significant n bits from the hash output $H(M)$. 2. Set $\mathbf{y}' = \mathbf{S}^{-1}(\mathbf{y})$. 3. Represent \mathbf{y}' as $\mathbf{y}' = Y_1 \dots Y_{\frac{n}{8}}$ where Y_i are Boolean vectors of dimension 8. 4. By using the left and right parastrophes \backslash and $/$ of the quasigroup $*$ compute $\mathbf{x}' = X_1 \dots X_{\frac{n}{8}}$, such that: $X_1 = Y_1$, $X_j = X_{j-1} \backslash Y_j$, for even $j = 2, 4, \dots$, and $X_j = Y_j / X_{j-1}$, for odd $j = 3, 5, \dots$ 5. Compute $\mathbf{x} = \mathbf{S}^{-1}(\mathbf{x}') + \mathbf{v} = (x_1, \dots, x_n)$. 6. The MQQ-SIG digital signature of the document M is the vector $\mathbf{sig} = (x_1, \dots, x_n)$.

Table 3. Digital signing

The algorithm for signature verification with the public key $\mathbf{P} = \{P_i(x_1, \dots, x_n) \mid i = 1 + \frac{n}{4}, \dots, n\}$ is given in Table 4.

Algorithm for signature verification with a public key $\mathbf{P} = \{P_i(x_1, \dots, x_n) \mid i = 1 + \frac{n}{4}, \dots, n\}$
Input: A document M and its signature $\mathbf{sig} = (x_1, \dots, x_n)$.
Output: TRUE or FALSE.
1. Compute $\mathbf{y} = (y_{1+\frac{n}{4}}, \dots, y_n) = H(M) _{n-\frac{n}{4}}$, where M is the signed message, $H()$ is a standardized cryptographic hash function such as SHA-1, or SHA-2, with a hash output of not less than n bits, and the notation $H(M) _{n-\frac{n}{4}}$ denotes the least significant $n - \frac{n}{4}$ bits from the hash output $H(M)$.
2. Compute $\mathbf{z} = (z_{1+\frac{n}{4}}, \dots, z_n) = \mathbf{P}(\mathbf{sig})$.
3. If $\mathbf{z} = \mathbf{y}$ then return TRUE, else return FALSE.

Table 4. Digital verification

3 Multivariate Quadratic Quasigroups

A Multivariate Quadratic Quasigroup (MQQ) $*$ of order 2^d used in this version of MQQ-SIG can be described shortly by the following expression:

$$\mathbf{x} * \mathbf{y} \equiv \mathbf{B} \cdot \mathbf{U}(\mathbf{x}) \cdot \mathbf{A}_2 \cdot \mathbf{y} + \mathbf{B} \cdot \mathbf{A}_1 \cdot \mathbf{x} + \mathbf{c} \quad (1)$$

where $\mathbf{x} = (x_1, \dots, x_d)$, $\mathbf{y} = (y_1, \dots, y_d)$, the matrices \mathbf{A}_1 , \mathbf{A}_2 and \mathbf{B} are nonsingular in $GF(2)$, of size $d \times d$, the vector \mathbf{c} is a random d -dimensional vector with elements in $GF(2)$ and all of them are generated by a uniformly random process. The matrix $\mathbf{U}(\mathbf{x})$ is an upper triangular matrix with all diagonal elements equal to 1, and the elements above the main diagonal are linear expressions of the variables of $\mathbf{x} = (x_1, \dots, x_d)$. It is computed by the following expression:

$$\mathbf{U}(\mathbf{x}) = I + \sum_{i=1}^{d-1} \mathbf{U}_i \cdot \mathbf{A}_1 \cdot \mathbf{x}, \quad (2)$$

where the matrices \mathbf{U}_i have all elements 0 except the elements in the rows from $\{1, \dots, i\}$ that are strictly above the main diagonal. Those elements can be either 0 or 1.

Once we have a multivariate quadratic quasigroup

$$*_{vv}(x_1, \dots, x_d, y_1, \dots, y_d) = (f_1(x_1, \dots, x_d, y_1, \dots, y_d), \dots, f_d(x_1, \dots, x_d, y_1, \dots, y_d))$$

we will be interested in those quasigroups that will satisfy the following conditions:

$$\forall i \in \{1, \dots, d\}, \text{Rank}(\mathbf{B}_{f_i}) \geq 2d - 4, \quad (3a)$$

$$\exists j \in \{1, \dots, d\}, \text{Rank}(\mathbf{B}_{f_j}) = 2d - 2 \quad (3b)$$

where matrices \mathbf{B}_{f_i} are $2d \times 2d$ Boolean matrices defined from the expressions f_i as

$$\mathbf{B}_{f_i} = [b_{j,k}], \quad b_{j,d+k} = b_{d+k,j} = 1, \text{ iff } x_j y_k \text{ is a term in } f_i. \quad (4)$$

Proposition 1. For $d = 8$, a multivariate quadratic quasigroup that satisfies the conditions (1), ..., (4) can be encoded in a unique way with 81 bytes.

4 Nonsingular Boolean matrices in MQQ-SIG

In MQQ-SIG the nonsingular matrices \mathbf{S} are defined by the following expression:

$$\mathbf{S}^{-1} = \sum_{i=1}^K I_{\sigma_i}, \quad (5)$$

where I_{σ_i} , $i = \{1, 2, \dots, K\}$ are permutation matrices of size $n = 32 \times k$ and where permutations σ_i are permutations on n elements. They are defined by the following expressions:

$$K = \begin{cases} k & , \text{ if } k \text{ is odd,} \\ k + 1 & , \text{ if } k \text{ is even} \end{cases} \quad (6)$$

$$\begin{cases} \sigma_1 - \text{random permutation on } \{1, 2, \dots, n\} \text{ satisfying the condition (8),} \\ \sigma_2 = \text{RotateLeft}(\sigma_1, 32) \text{ satisfying the condition (8),} \\ \sigma_3 = \text{RotateLeft}(\sigma_2, 64) \text{ satisfying the condition (8),} \\ \sigma_j = \text{RotateLeft}(\sigma_{j-1}, 32), \text{ for } j = 4, \dots, K-1, \text{ satisfying the condition (8),} \\ \sigma_K - \text{random permutation on } \{1, 2, \dots, n\} \text{ satisfying the condition (8)} \end{cases} \quad (7)$$

$$\sigma_\nu = \left(\begin{array}{cccccccc} 1 & 2 & \dots & 8 & 9 & \dots & n-1 & n \\ s_1^{(\nu)} & s_2^{(\nu)} & \dots & s_8^{(\nu)} & s_9^{(\nu)} & \dots & s_{n-1}^{(\nu)} & s_n^{(\nu)} \end{array} \right), \{s_1^{(\nu)}, s_2^{(\nu)}, \dots, s_8^{(\nu)}\} \cap \{1, 2, \dots, 8\} = \emptyset \quad (8)$$

where $\text{RotateLeft}(\sigma, l)$ denotes a permutation obtained from the permutation σ by rotating it to the left for l positions.

We require an additional condition to be fulfilled by the permutations $\sigma_1, \dots, \sigma_K$:

$$L = \begin{bmatrix} \sigma_1 \\ \sigma_2 \\ \vdots \\ \sigma_{K-1} \\ \sigma_K \end{bmatrix}, \text{ is a Latin Rectangle.} \quad (9)$$

Once we have a nonsingular matrix \mathbf{S}^{-1} we will compute its inverse obtaining

$$\mathbf{S} = (\mathbf{S}^{-1})^{-1}$$

and from there we will obtain the affine transformation

$$\mathbf{S}'(\mathbf{x}) = \mathbf{S} \cdot \mathbf{x} + \mathbf{v}, \quad (10)$$

where the vector \mathbf{v} is n -dimensional Boolean vector defined from the values of the permutation σ_K by the following expression:

$$\mathbf{v} = (v_1, v_2, \dots, v_n), \text{ where } v_i = \left(\frac{s_{64 + \lceil \frac{i}{4} \rceil}^{(K)}}{2^i \bmod 4} \right) \bmod 2. \quad (11)$$

In words: we construct the bits of the vector \mathbf{v} by taking the four least significant bits of the values $s_{65}^{(K)}, \dots, s_{64 + \frac{n}{4}}^{(K)}$ in the permutation σ_K .

Proposition 2. *The linear transformation \mathbf{S}^{-1} can be encoded in a unique way with $2n$ bytes.*

5 Characteristics of the MQQ-SIG digital signature scheme

The main characteristics of our MQQ-SIG digital signature scheme can be briefly summarized as follows:

- there is no message expansion;
- the length of the signature is n bits where ($n = 160, 192, 224$ or 256);
- its conjectured security level is $2^{\frac{n}{2}}$;
- its verification speed is comparable to the speed of other multivariate quadratic PKCs;
- in software its signing speed is in the range of 500–5,000 times faster than RSA and ECC schemes;
- in hardware its signing or verification speed is more than 10,000 times faster than RSA and ECC schemes;
- it is also well suited for producing short signatures in smart cards and RFIDs;

5.1 The size of the public and the private key

The size of the public key is $0.75 \times n \times (1 + \frac{n(n+1)}{2})$ bits. The private key of our scheme is the tuple $(\sigma_1, \sigma_K, *)$. The corresponding memory size needed for storage of the private key is $2n + 81$ bytes. In Table 5 we give the size of the public key (in KBytes) and the size of the private key (in bytes) for $n \in \{160, 192, 224, 256\}$.

n	Size of the public key (KBytes)	Size of the private key (bytes)
160	188.69	401
192	325.71	465
224	516.82	529
256	771.02	593

Table 5. Memory size in KBytes for the public key and in bytes for the private key

The Digital Signature Scheme MQQ-SIG

Intellectual Property Statement and Technical Description

10 October 2010

Danilo Gligoroski¹ and Svein Johan Knapskog² and Smile Markovski³ and Rune Steinsmo Ødegård² and Rune Erlend Jensen² and Ludovic Perret⁴ and Jean-Charles Faugère⁵

¹ Department of Telematics, Faculty of Information Technology, Mathematics and Electrical Engineering, The Norwegian University of Science and Technology (NTNU), O.S.Bragstads plass 2E, N-7491 Trondheim, NORWAY, danilog@item.ntnu.no

² Norwegian University of Science and Technology Centre for Quantifiable Quality of Service in Communication Systems. O.S. Bragstads plass 2E, N-7491 Trondheim, NORWAY, knapskog@q2s.ntnu.no, rune.odegard@q2s.ntnu.no, runeerle@stud.ntnu.no

³ "Ss Cyril and Methodius" University, Faculty of Natural Sciences and Mathematics, Institute of Informatics, P.O.Box 162, 1000 Skopje, MACEDONIA, smile@ii.edu.mk

⁴ Pierre and Marie Curie University - Paris, Laboratory of Computer Sciences, Paris 6, 104 avenue du Président Kennedy 75016 Paris FRANCE, ludovic.perret@lip6.fr

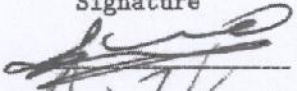
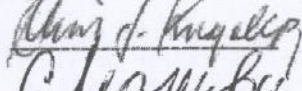
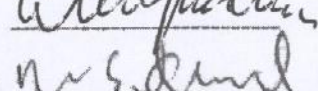
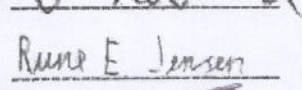
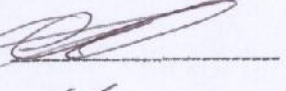
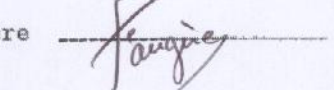
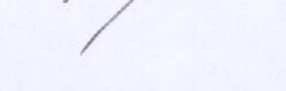
⁵ UPMC, Université Paris 06, LIP6 INRIA, Centre Paris-Rocquencourt, SALSA Project-team CNRS. UMR 7606, LIP6 4, place Jussieu 75252 Paris, Cedex 5, FRANCE jean-charles.faugere@inria.fr

Abstract: This document contains the Intellectual Property Statement and the technical description of the MQQ-SIG - a new public key digital signature scheme. The complete scientific publication covering the design rationale and the security analysis will be given in a separate publication. MQQ-SIG consists of $n - \lfloor \frac{n}{7} \rfloor$ quadratic polynomials with n Boolean variables where $n = 160, 196, 224$ or 256 .

Keywords: Public Key Cryptosystems, Fast signature generation, Multivariate Quadratic Polynomials, Quasigroup String Transformations, Multivariate Quadratic Quasigroup

1 Intellectual Property Statement

We, the seven names given in the title of this document and undersigned on this statement, the authors and designers of MQQ-SIG digital signature scheme, do hereby agree to grant any interested party an irrevocable, royalty free licence to practice, implement and use MQQ-SIG digital signature scheme, provided our roles as authors and designers of the MQQ-SIG digital signature scheme are recognized by the interested party as authors and designers of the MQQ-SIG digital signature scheme.

Name	Signature	Place	Date
1. Danilo Gligoroski		Trondheim	5.10.2010
2. Svein Johan Knapskog		Trondheim	06.10.2010
3. Smile Markovski		Skopje	07.10.2010
4. Rune Steinsmo Ødegård		Trondheim	06/10-2010
5. Rune Erlend Jensen		Trondheim	07.10.2010
6. Ludovic Perret		Paris	13/10/2010
7. Jean-Charles Faugère		Paris	13.10.2010