Generic Attacks and the Security of Quartz[⋆],[⋆⋆]

Nicolas T. Courtois

CP8 Crypto Lab, SchlumbergerSema
36-38 rue de la Princesse, BP 45, 78430 Louveciennes Cedex, France
courtois@minrank.org

Abstract. The signature scheme Quartz is based on a trapdoor function G belonging to a family called HFEv-. It has two independent security parameters, and we claim that if d is big enough, no better method to compute an inverse of G than the exhaustive search is known. Such a (quite strong) assumption, allows to view Quartz as a general construction, that transforms a trapdoor function into a short signature scheme. The main object of this paper is the concrete security of this construction. On one hand, we present generic attacks on such schemes. On the other hand, we study the possibility to prove or justify the security with some well chosen assumptions. Unfortunately for Quartz, our lower and upper security bounds do not coincide. Still the best attack known for Quartz is our generic attack using $\mathcal{O}(2^{80})$ computations with $\mathcal{O}(2^{80})$ of memory. We will also propose an alternative way of doing short signatures for which both bounds do coincide.

Keywords: Asymmetric cryptography, finite fields, Hidden Field Equations (HFE), MQ, HFEv-, short signatures, Quartz, Flash, Sflash, Nessie.

1 Introduction

The shortest signature scheme known in the "classical cryptography" is based on Weil pairing and achieves 160 bits with the security of 2^{80} [1]. Only recently schemes with signatures shorter than 160 bits have been proposed. These new schemes belong to the multivariate cryptography. Quartz, proposed for standardisation in the European Nessie project, achieves signatures of 128 bits with a claimed security level of 2^{80}. The McEliece-based signature scheme CFS gives signatures of about 80 bits [4] but has a substantially bigger public key than Quartz. Both Quartz and McEliece have features that make them a unique choice for some applications, while remain excluded from other applications. It seems that, see [4], the security of McEliece signatures can be proven in the random oracle model and the lower and upper bounds coincide with respect to two well known problems. In the present paper we will try to see what are the

[⋆] The work described in this paper has been supported by the French Ministry of Research under RNRT Project "Turbo-signatures".

[⋆⋆] An early version of this paper has been presented at the second Nessie workshop, September 2001, Royal Holloway University of London.

Y.G. Desmedt (Ed.): PKC 2003, LNCS 2567, pp. 351–364, 2003.

lower and upper bounds on the security of Quartz, based on some well-chosen (but plausible) assumptions.

The paper is organized as follows: First we overview the hardness properties that are believed to hold for such multivariate trapdoor functions as HFEv- and we formulate the Assumption 2.0.2 which is the basis of all our subsequent security considerations. In the section 3 we study generic attacks on such meta signature schemes. Then in the Section 4 and in the Appendix we study if the security of Quartz can be proved, or justified, based on our Assumption 2.0.2. Finally we give our conclusions.

2 Multivariate Quadratic Trapdoor Functions

In this paper we study a security of signature schemes based on multivariate quadratic trapdoor functions $GF(q)^n \rightarrow GF(q)^m$. For example for Quartz, described in [13], we only need to know that it uses a trapdoor quadratic function of type HFEv-, with $n = 107$ variables and $m = 100$ equations over $GF(2)$. The HFEv- cryptosystem has an important second security parameter d that can be adjusted independently of m and n, so that all structural attacks disappear, and all attacks that remain are generic attacks that behave as if G was random without any trapdoor:

Theorem 2.0.1 (Generic Attack on a Trapdoor Function).
Let $G : GF(q)^n \rightarrow GF(q)^m$ be an efficiently computable function. For all $0 \leq T \leq q^m$ there is an adversary that computes an inverse of G for a random $y \leftarrow GF(q)^m$ with success probability of about:

$$\varepsilon \approx T/q^m.$$

For HFEv-, it is believed that if the parameter d is sufficiently high, then we have a sort of converse of this Theorem, as follows:

Critical Assumption 2.0.2 (Strong One-Wayness of HFEv-).
Let G a random public key $G \leftarrow \text{HFEv}^-(q, n, m)$ with $m \approx n$, $n \geq m$ and $m \leq 100$. For any Adversary A running in T CPU clocks, given random $y \leftarrow GF(q^m)$, the probability that A outputs some $x = G^{-1}(y)$ is at most:

$$\varepsilon \leq T/q^m.$$

This assumption is a consequence of the current state of knowledge in multivariate cryptography. A full and detailed explanation of this assumption is quite long and appears in the extended version of this paper.

In the remaining part of this paper we will study the upper and lower bounds that may be given for the security of Quartz (and also of other multivariate signature schemes), given, on one hand this (very strong) assumption, and on the other hand, using the generic attack above.

3 Feistel-Patarin Construction

3.1 Generic Threats

The classical way to compute digital signatures with a trapdoor function $G : GF(q)^n \rightarrow GF(q)^m$ is to compute a hash H, and the signature is given as:

$$\sigma = G^{-1}(H)$$

As a direct consequence of 2.0.1, such a signature can be forged in the square root of exhaustive search. This attack is generic: it does not depend on G. We produce a lists of $q^{m/2}$ $G(\sigma_i)$ and a list of $q^{m/2}$ hashes of different messages (or different versions of the same message). Then we expect to be able to produce at least one valid pair (message, signature), which is an existential forgery.

Remark: This generic attack is not an issue for most well-known signature schemes such as RSA, DSA, McEliece etc. It is because for all these functions there already exists an attack in the square root of exhaustive search (or less) and the parameters have already been chosen sufficiently large to avoid it. The situation is somewhat different for multivariate quadratic schemes such as HFE. For several such schemes, there is no attack known noticeably smaller than the exhaustive search. Therefore if the signature is computed as $\sigma = G^{-1}(H)$ for a scheme such as HFE or HFEv-, $q^{m/2}$ should be at least 2^{80} and it implies that the signatures should have at least 160 bits. For this reason, when it comes to shorter signatures, multivariate quadratic schemes usually compute a signature in different, somewhat strange way.

3.2 Removing Existential Forgeries

We assume $m = n$ (this condition will be relaxed later). How to compute a signature using a trapdoor function ? On one hand, the owner of the private key should use the computation of $G^{-1}()$ at least once, so that he will be the only person to be able to compute a signature. On the other hand, the verification should be in the implicit form Verif(σ, H) in order to avoid meet-in-the middle attacks. On the Figure 1 we show an example of such a construction derived from the Feistel scheme, in which the hash is divided in two pieces and the signature is computed as (cf. Fig. 1):

$$H(M) = (H_1(M), H_2(M))$$
$$\sigma = H_1 \oplus G^{-1}(H_2 \oplus G^{-1}(H_1))$$

Now, the meet-in-the middle attack fails: we can still produce two lists of candidate messages and candidate signatures, but we are unable to detect which signature correspond to which message by just sorting two lists. It is necessary to run the verification algorithm on each pair (message, signature) and it gives a complexity of q^m.

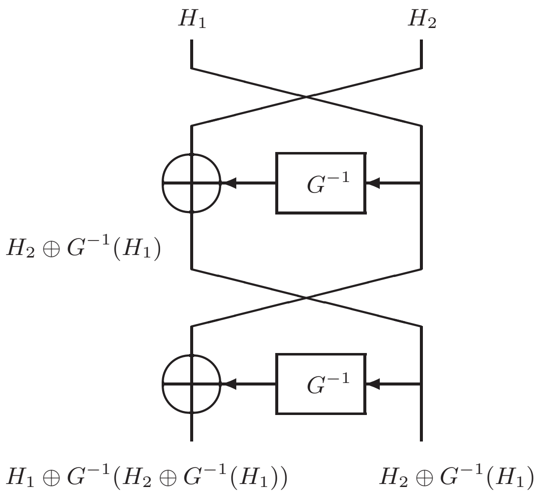

Fig. 1. 2-round Feistel applied to signature generation

Security: Clearly, the Feistel-based (meta) signature scheme described above is better than the (ordinary) signature scheme, but still not perfect. In [10] Patarin explains that that a signature can still be forged in $q^{\frac{2m}{3}}$ instead of $q^{\frac{m}{2}}$ previously. For this, we precompute $q^{\frac{2m}{3}}$ values $f(X)$ for some $q^{\frac{2m}{3}}$ values for X. It allows to compute an inverse of G with probability $q^{-\frac{m}{3}}$. Thus one can compute two consecutive inverses with probability $q^{-\frac{2m}{3}}$. Then, given $q^{\frac{2m}{3}}$ messages we are able to forge a signature of (about) one of them. In general we have:

Theorem 3.2.1 (Generic Attack on Signature Schemes).
Let $G : GF(q)^n \rightarrow GF(q)^m$. Any deterministic signature scheme that combines K inverses and message hash values can be broken in $q^{\frac{K}{K+1}m}$.

Proof. We precompute $q^{\frac{K}{K+1}m}$ values $f(X)$ for some $q^{\frac{K}{K+1}m}$ values for X. It allows to compute an inverse of G with probability $q^{-\frac{1}{K+1}m}$ and thus to compute iteratively K inverses with probability $q^{-\frac{K}{K+1}m}$. Thus with $q^{\frac{K}{K+1}m}$ messages we are able to forge a signature. □

Remark: For a function $G : GF(q)^n \rightarrow GF(q)^m$ the complexity is $q^{\frac{K}{K+1}m}$ with $q^{\frac{K}{K+1}m}$ of memory. It is in fact the best known attack against Quartz and gives 2^{80} computations with 2^{80} of memory.

It is obvious that when K grows, the complexity of the attacks tends to q^m of the exhaustive search. Unfortunately using the Feistel structure cannot easily be extended to more rounds: we will not have enough information to verify the signature anymore. Still the formula it gives can be generalized and in many different ways:

```
$\sigma \leftarrow 0$
for $i = 1$ to $K$ do
    {
        $\sigma \leftarrow \sigma \oplus H_i(M)$
        $\sigma \leftarrow G^{-1}(\sigma)$
    }
return $\sigma$
```

Fig. 2. Basic Feistel-Patarin scheme with K inverses

3.3 Extending to any Number of Inverses

For example we may consider the following (cf. Fig. 2):

$$H(M) = (H_1(M), H_2(M), \ldots, H_K(M))$$

$$\sigma = G^{-1}(H_K \oplus \ldots \oplus G^{-1}(H_3 \oplus G^{-1}(H_2 \oplus G^{-1}(H_1)) \ldots)$$

We call it the Feistel-Patarin signature scheme, though it has little to do (now) with the original Feistel scheme.

3.4 Extending to $m \neq n$

We need to generalize the above construction to trapdoor functions with input and output spaces of different sizes $G : GF(q)^n \rightarrow GF(q)^m$, and $m \neq n$. In this paper we limit to $m \leq n$, see [5] for the case $m > n$. The adaptation consists of cutting off and publishing the additional $(m - n)$ symbols obtained in every round, as they are a necessary ingredient in the signature verification process. It makes signatures somewhat longer. More precisely we do the following (Fig. 3):

This is precisely used in Quartz with $K = 4$, as represented on Fig. 4.

```
$\sigma \leftarrow 0$
for $i = 1$ to $K$ do
{
        $\sigma \leftarrow \sigma \oplus H_i(M)$
        $U \in G^{-1}(\sigma)$
        $\sigma \leftarrow U_{1 \rightarrow m}$
        $X_{i1}|| \ldots ||X_{i(n-m)} \leftarrow U_{(m+1) \rightarrow n}$
}
return $\sigma||X_{11}|| \ldots ||X_{K(n-m)}$
```

Fig. 3. Generalized Feistel-Patarin with $m \leq n$

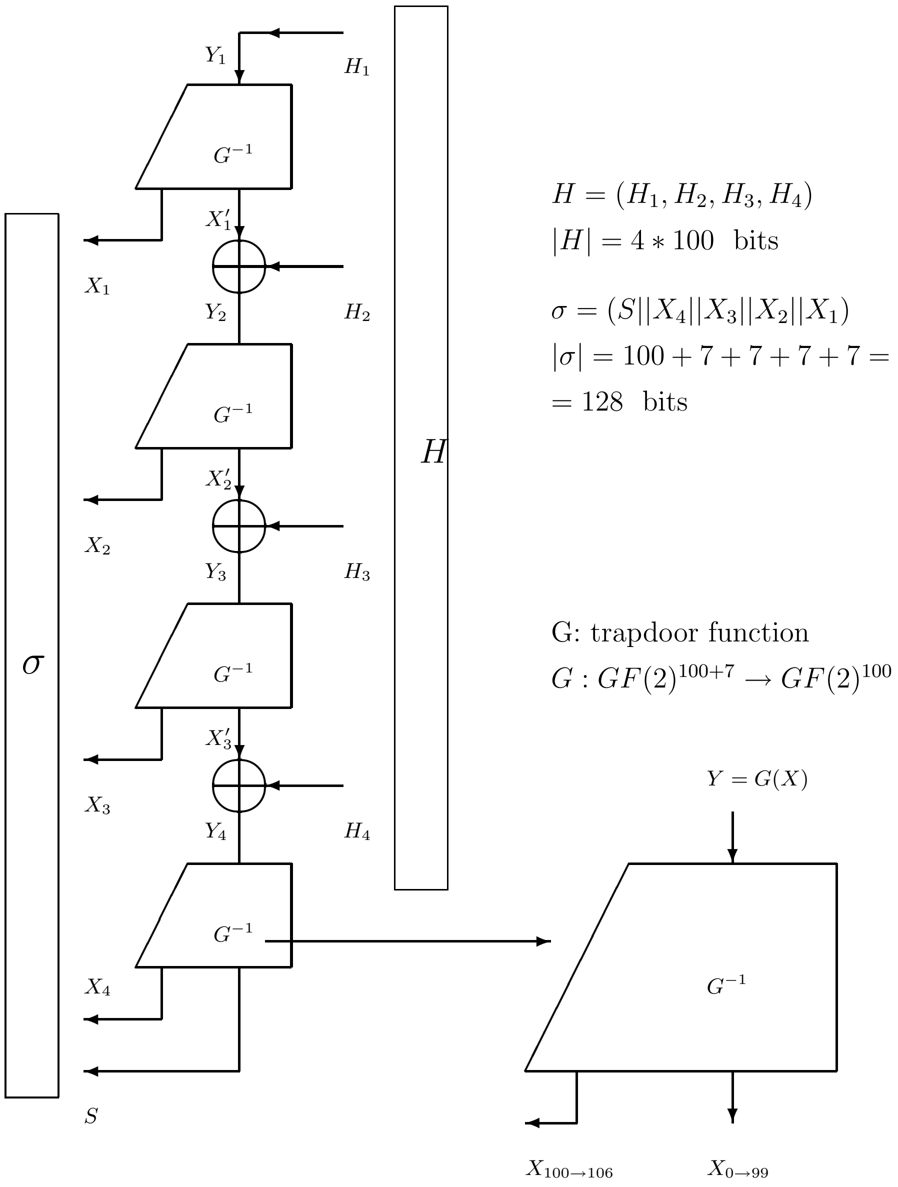

Fig. 4. Signature generation in Quartz

3.5 The Signature Length

The signature length in the generalized Feistel-Patarin construction is:

$$|\sigma| = (\ m + K(n-m)\ ) \cdot \log_2(q) \ \text{ bits}$$

Given the Theorem 3.2.1, the signature length at a given security level 2^{SF} is:

$$|\sigma| = \left\lceil \frac{K+1}{K} \cdot SF \right\rceil + K(n-m)\log_2(q) \ \text{ bits}$$

We note that the length decreases for small K, and then it increases. Therefore at some point the signature is the shortest. In Quartz the minimum is $|\sigma| = 128$ bits, achieved for both[1] $K = 3$ and $K = 4$.

4 Is It Possible to Prove the Security of Quartz ?

We established lower bounds for the attacks on signature schemes such as Quartz. The question is now whether these lower bounds are also upper bounds, and more importantly, can the perfect correspondence between the generic attack 2.0.1 and the Assumption 2.0.2, be extended to Quartz ? This problem is studied in this section, and in more details in the Appendix. Though several open problems remain, we will prove several interesting results about the security of Quartz, Flash and Sflash.

We restrict to no-message attacks. The goal is to prove that an adversary cannot compute a valid pair (message, signature) given the public key. We assume the random oracle model with Q being the number of queries. It is a very powerful tool for security proofs. It allows an immediate reduction for a signature scheme of the form $G^{-1}(h)$: if the adversary computes a valid pair (message, signature) for some h taken out of the Q oracle answers, then we can transform this adversary into a machine that computes $G^{-1}(h)$ for one out of Q given values. This remains true not only for Q random values, but also for with probability very close to 1 to any set of chosen Q values. Indeed our reduction must behave exactly in the same way as with truly random values, provided that this set cannot be distinguished from random (which is in most cases easily achieved).

Thus we get machine that given some Q random (or chosen, but randomly looking values), outputs $G^{-1}(h)$ for one of them. By injecting a chose value into a list of length Q, we get a a machine able to invert G with probability at least $1/Q$. However from the Assumption 2.0.2 we know that this success probability cannot be bigger than T/q^m, and thus $1/Q \leq T/q^m$. Reading the oracle takes time and thus we have $Q \leq T$. Combining these two equations gives: $T \geq Q \geq q^m/T$ and thus $T \geq q^{m/2}$. A signature cannot be forged in less than $q^{m/2}$ for no-message attacks.

[1] The reasons for which the $K = 4$ has been chosen, and not $K = 3$, is that the authors wanted some internal value, namely $h = m + r$ to be a prime, with $m = \left\lceil \frac{K+1}{K} \cdot 80 \right\rceil$ and $r = 3$, see [14, 13].

We note that this argument applies also to Sflash [15, 16] and shows that if it satisfies our (quite strong) Assumption 2.0.2, then a signature cannot be forged in less than 2^{91}, again only for no-message attacks.

It also applies for the first G^{-1} in Quartz: its entry is given entirely by the oracle, see Fig. 4. A Quartz signature cannot be forged in less than 2^{50}, quite disappointing compared to the claimed security level of 2^{80}.

Now let us assume that in a signature scheme, several inverses G^{-1}, say K inverses, are computed for several H_i, such that all the H_i are independent parts of an output of one single application of a hash function. Then an adversary that can do an existential forgery, is able, with probability $1/Q$, to solve the inversion problem simultaneously for K independent instances H_i. Our Assumption 2.0.2 says that the probability of finding an inverse is at most T/q^m. It is therefore legitimate to think that the probability to compute K inverses in parallel will [2] be at most $(T/q^m)^K$. The adversary does with probability $1/Q$ something that can only be done with probability $(T/q^m)^K$. Thus, we get $1/T \geq 1/Q \geq (T/q^m)^K$. This gives $T \geq q^{\frac{K}{K+1}m}$. We obtain a lower bound that is the exact converse of our generic attack 2.0.1 !

From this one might think that it is possible to prove the security of Quartz and obtain an upper and a lower bound that coincide, thus achieving the exact security level of 2^{80} for no-message attacks. Unfortunately our argument does not apply to Quartz, the entries of the three other G^{-1} functions are not given by the random oracle, see Fig. 4. We are here at the heart of the problem of short signatures. Is it possible to have a signature scheme for which a lower bound on an attack can be proven that is more than $q^{\text{signature size}/2}$? The answer is yes and in Section A.4 we show a very surprising way to compute signatures, in which the signer does compute G^{-1} for two independent values H_1 and H_2, but in which the signature length is only the size of one $G^{-1}(H_i)$.

5 Conclusion

Quartz is based on a trapdoor function G that belongs to a family called HFEv-. It has two independent security parameters and if d is sufficiently large, there is no better method known to compute inverses of G, than simple guessing. We formalized this, and we studied what kind of security can be achieved by a general class of (short) signature schemes, under this assumption and in the

[2] It is not a consequence of our Assumption 2.0.2 and requires an additional assumption (cf. Assumption A.2.1 in the Appendix). It does not contradict any known attacks for Quartz. We need to assume that K is small. We may deduce this result, assuming that the only way to compute K inverses is to use the best algorithm to compute one inverse K times. For example the owner of the private key can compute 1 inverse with probability 1, and K inverses with probability at most $1^K = 1$, even here there is no contradiction. For the algorithms that does not contain the private key, we expect it to be true, because it seems that the only thing they can do to find solutions is to guess them, and our assumption is obviously true for any algorithm that is just guessing.

random oracle model. On one side we studied generic attacks on such signature schemes and gave exact lower security bounds. On the other side, we studied the security reductions that could give security upper bounds under some well chosen assumptions. Unfortunately for Quartz, our lower and upper bounds do not coincide. We also proposed a new method for computing short signatures for which the two bounds do coincide, however it is less general than the scheme of Quartz.

In practice it seems that Quartz, though lacking a tight security reduction, is still a correct way to achieve short signatures. The best attack known for Quartz is our generic attack using $\mathcal{O}(2^{80})$ computations with $\mathcal{O}(2^{80})$ of memory. In practice memory is very expensive and the fastest ”memoryless” attack known requires as much as 2^{100} computations.

References

[1] Dan Boneh, H. Shacham, and B. Lynn: *Short signatures from the Weil pairing,* Asiacrypt 2001, LNCS 2139, Springer, pp. 514-532. 351

[2] Nicolas Courtois: *The security of Hidden Field Equations (HFE)*; Cryptographers' Track Rsa Conf. 2001, LNCS2020, Springer-Verlag, pp. 266-281.

[3] N. Courtois, L. Goubin, W. Meier, J.-D. Tacier: *Solving Underdefined Systems of Multivariate Quadratic Equations;* PKC 2002, LNCS 2274, Springer, pp. 211-227.

[4] Nicolas Courtois, Matthieu Finiasz and Nicolas Sendrier: *How to achieve a McEliece-based Digital Signature Scheme*; Asiacrypt 2001, LNCS2248, Springer, pp. 157-174. 351

[5] Nicolas Courtois: *La sécurité des primitives cryptographiques basées sur les problèmes algébriques multivariables MQ, IP, MinRank, et HFE*, PhD thesis, Paris 6 University, 2001, in French. 355

[6] Michael Garey, David Johnson: *Computers and Intractability, a guide to the theory of NP-completeness*, Freeman, p. 251.

[7] S. Goldwasser, S. Micali and R. Rivest: *A Secure Digital Signature Scheme;* Siam Journal on Computing, Vol. 17, 2 (1988), pp. 281-308.

[8] Neal Koblitz: *Algebraic aspects of cryptography;* Springer-Verlag, ACM3, 1998, Chapter 4: ”Hidden Monomial Cryptosystems”, pp. 80-102.

[9] Jacques Patarin: *Hidden Fields Equations (HFE) and Isomorphisms of Polynomials (IP): two new families of Asymmetric Algorithms;* Eurocrypt'96, pp. 33-48.

[10] Jacques Patarin: *La Cryptographie Multivariable*; Mémoire d'habilitation à diriger des recherches de l'Université Paris 7, 1999. 354

[11] Jacques Patarin, Louis Goubin, Nicolas Courtois, + papers of Eli Biham, Aviad Kipnis, T. T. Moh, et al.: *Asymmetric Cryptography with Multivariate Polynomials over a Small Finite Field*; known as ”orange script”, compilation of different papers with added materials. Available from Jacques.Patarin@louveciennes.tt.slb.com

[12] Jacques Patarin, Nicolas Courtois, Louis Goubin: *C*-+ and HM - Variations around two schemes of T. Matsumoto and H. Imai;* Asiacrypt 1998, pp. 35-49. *Unbalanced Oil and Vinegar Signature Schemes;* Eurocrypt 1999, Springer-Verlag.

[13] Jacques Patarin, Louis Goubin, Nicolas Courtois: *Quartz,* 128*-bit long digital signatures*; Cryptographers' Track Rsa Conference 2001, San Francisco 8-12 April 2001, LNCS2020, Springer. See [14] for the updated Quartz specification. 352, 357

[14] Jacques Patarin, Louis Goubin, Nicolas Courtois: *Quartz,* **128**-*bit long digital signatures*; An updated version of Quartz specification. available at `http://www.cryptosystem.net/quartz/` 357, 359

[15] Jacques Patarin, Louis Goubin, Nicolas Courtois: *Flash, a fast multivariate signature algorithm*; Cryptographers' Track Rsa Conference 2001, LNCS2020, Springer. 358, 362

[16] An updated version of Sflash specification. Available at `http://www.cryptosystem.net/sflash/` 358, 362

[17] D. Pointcheval, J. Stern: *Security arguments for Digital signatures and Blind Signatures;* Journal of Cryptology, Vol.13(3), Summer 2000, pp. 361-396. *Efficient signature schemes based on birational permutations;*

[18] Nicolas Courtois, Adi Shamir, Jacques Patarin, Alexander Klimov, *Efficient Algorithms for solving Overdefined Systems of Multivariate Polynomial Equations*, Eurocrypt'2000, LNCS 1807, Springer-Verlag, pp. 392-407.

[19] Adi Shamir, Aviad Kipnis: *Cryptanalysis of the HFE Public Key Cryptosystem*; Crypto'99.

A Black-Box Reductions For No-Message Attacks

In this section we study the security of some signature schemes based, as in Quartz on computation of one or several inverses $y \mapsto G^{-1}(y)$, provided that the trapdoor function G is difficult to inverse, as specified by the Strong Onewayness Assumption 2.0.2. We limit ourselves to no-message attacks, i.e. for the usual case with the adversary trying to forge a valid pair (message, signature) given (only) the public key (and no signature oracles). We need to build a black-box reduction, from the forger, to a machine that solves some difficult problem. It is done for a scheme that is similar to Quartz, but not identical: the signature is longer and it does not involve chaining of the G^{-1} as in Quartz. Later we will see if the result can be extended to Quartz.

A.1 The Black-Box Reduction

First of all, it is easy to prove the security of the usual signature scheme $\sigma = G^{-1}(H(M))$ in the random oracle model. The point is that the value $H(M)$ on which the trapdoor function G is inverted, is produced by the hash function. It does not only mean that it is completely random, and therefore G is inverted on random y, but also that the value may in fact be **chosen** by the random oracle, and as long its probability distribution is indistinguishable from random source, the adversary cannot say the difference. Therefore the adversary may as well be used to compute inverses of some **chosen** values: we have a black-box reduction that is achieved by replacing the random oracle by a given source (if it is random-looking).
Similar black-box reduction works for signature schemes that compute several inverses and we have the following:

Theorem A.1.1 (Security Reduction for Signatures Scheme that Compute Inverses of Hashed Values). Let G be a trapdoor one-way function. Assume that a signature scheme satisfies:

- it computes $G^{-1}(H_i)$ for some K values $H_i \in GF(q)^m$,
- all the H_i are independent parts of a (single) output of a hash function:

$$H(M) = (H_1, H_2, \ldots, H_K)\,.$$

- all the K values $G^{-1}(H_1), .., G^{-1}(H_K)$ can be completely recovered in the signature verification,

If an attacker having (only) the access to the public key is able to compute a valid pair (message, signature) with probability ε, in random oracle model, and with Q queries to the hashing oracle.
Then it can be then transformed into a machine than given a random K-tuple $(y_1, y_2, \ldots, y_K)$ will with probability ε/Q output all the K inverses: $\big(G^{-1}(y_1), G^{-1}(y_2), \ldots, G^{-1}(y_K)\big)$.

Proof. In the adversary's interaction with the hash oracle, the oracle gives a random and independent K-tuple $(H_1^{(i)}, H_2^{(i)}, \ldots, H_K^{(i)})$ each time it is called for $i = 1..Q$. We replace a randomly chosen K-tuple by $(y_1, y_2, \ldots, y_K)$. Since both lists are random and independent, even a computationally unbounded adversary cannot distinguish between two situations. Consequently the result will be the same: he will, with probability ε output, a valid pair (message, signature), and with probability ε/Q it will contain the inverse of the chosen K-tuple.

A.2 Security Arguments

It turns out that our Strong One-wayness Assumption 2.0.2 is not enough.

Assumption A.2.1 (Super-Strong One-Wayness of HFEv-).
Let K be a small integer. Let G a random public key $G \leftarrow \mathrm{HFEv}^{-}(q, n, m)$ with $m \approx n$, $n \geq m$ and $m \leq 100$. For any Adversary A running in T CPU clocks, given random K-tuple $(y_1, \ldots, y_K) \leftarrow GF(q^m)^k$, the probability that A computes all the inverses $x_i = G^{-1}(y_i)$ with probability ε' is upper-bounded by:

$$\varepsilon' \leq (T/q^m)^K\,.$$

It is not a consequence of the Assumption 2.0.2. There may be algorithms that compute all K inverses $x_i = G^{-1}(y_i)$ faster than applying K times, the best algorithm to compute one inverse. Cf. also the footnote 2, p. 358.

Theorem A.2.2. Let K be a small integer. Let G be a trapdoor one-way function $G : GF(q)^n \rightarrow GF(q)^m$ with $m \leq n$. Assume that G satisfies the Assumption A.2.1. Assume that in a signature scheme, given a valid (pair message, signature), K inverses $G^{-1}(H_i)$ can be computed, with $H(M) = (H_1, H_2, \ldots, H_K)\,.$ We assume that H is a random oracle. Let A be an Adversary, having (only) the access to the public key, running in time T, and able to compute a valid pair (message, signature) with a success probability ε. Then:

$$T \geq \varepsilon^{\frac{1}{K+1}} \cdot q^{m \cdot \frac{K}{K+1}}\,.$$

Proof. From Theorem A.1.1, we obtain a machine that inverts G in parallel for K random values $y_1, \ldots, y_K$ and with probability $\varepsilon' = \varepsilon/Q$. Following our Assumption, the attacker is able to do with probability ε/Q something that can only be done with a probability at most $(T/q^m)^K$. Thus:

$$\varepsilon/Q \leq (T/q^m)^K.$$

Finally, since the oracle queries take time, we have $Q \leq T$ and obtain:

$$\varepsilon/T \leq \varepsilon/Q \leq (T/q^m)^K, \text{ from this we get } T^{K+1} \geq \varepsilon(q^m)^K, \text{ and finally}$$

$$T \geq \varepsilon^{\frac{1}{K+1}} \cdot q^{m \cdot \frac{K}{K+1}}.$$

□

Corollary A.2.3. Let G be a trapdoor one-way function $G : GF(q)^n \rightarrow GF(q)^m$ with $m \leq n$. Assume that the only method known for to obtain $G^{-1}(y_i)$ for some values y_i is to guess them and apply G. Assume that in a signature scheme, given a valid pair (message, signature), K inverses $G^{-1}(H_i)$ are be computed, with $H(M) = (H_1, H_2, \ldots, H_K)$. Let A be an Adversary having (only) the access to the public key and running in time T that is able to compute a valid pair (message, signature). Then, under the random oracle assumption,

$$T \geq q^{m \cdot \frac{K}{K+1}}.$$

We obtained an exact, tight converse of the Theorem 3.2.1. It gives the exact security level of the described signature schemes (but not for Quartz).

A.3 Applications, $K = 1$, Consequences on Flash and Sflash

All well known signature schemes constructed as $\sigma = G^{-1}(H)$ satisfy the assumption of the signature scheme we used in Theorems A.1.1 and A.2.2. However that trapdoor functions they use, for example RSA encryption, admit attacks asymptotically much faster than the exhaustive search, and therefore **do not** satisfy our very strong hardness Assumption 2.0.2 used in Theorems A.2.2.

Currently the only convincing trapdoor functions that seem to satisfy our Strong One-wayness Assumption 2.0.2 are multivariate cryptographic trapdoor functions. For example the signature scheme Flash and Sflash [3], submitted to European call for cryptographic primitives [15, 16], use a trapdoor function $G : GF(q)^{37} \rightarrow GF(q)^{26}$ with respectively $q = 256$ for Flash and $q = 128$ for Sflash. Thus by the Theorem A.2.2 and the converse given by the Theorem 3.2.1 we have:

Corollary A.3.1 (Exact Security of Flash and Sflash). If the trapdoor function used in Flash/Sflash satisfies the Strong One-wayness Assumption 2.0.2, the security of these respective signature schemes [15, 16] against no-message attacks is exactly:

$$q^{m/2} = 2^{104} \text{ for Flash} \quad \text{ and } 2^{91} \text{ for Sflash.}$$

[3] We refer here to the updated version of Sflash that is very similar to Flash, see [16].

A.4 Applications with $K \geq 2$, Differential Signature Scheme

It is trivial to construct a signature scheme for which the Theorem A.2.2 applies, for any small K, and based on any trapdoor function. For this we need just to compute in parallel K signatures $\sigma_i = G^{-1}(H_i)$ and the signature will be given by a K-tuple $\left(G^{-1}(H_1(M)), \ldots, G^{-1}(H_K(M))\right)$. Unfortunately such a signature will be K times as long as when $K = 1$.

Differential Signatures It is highly non-trivial to construct a signature scheme for which the Theorem A.2.2 applies, but with shorter signatures. For $K = 2$, it is possible to have a complete signature compression. For example we may compute the signature as follows:

$$\boxed{\sigma = F^{-1}(H_2) - F^{-1}(H_1)}$$

This surprising signature scheme has a non-trivial verification procedure. The signature compression is based on the fact that the two values $x = F^{-1}(H_1)$ and $x + \sigma = F^{-1}(H_2)$ can be completely recovered given their difference σ, as the equation $F(x+\sigma) - F(x) = H_2 - H_1$ becomes linear in the x_i after σ, H_1 and H_2 are known (the degree 2 terms will just cancel out). This scheme is called the "Differential Signature" scheme. It is not completely generic: it works only when G is a Multivariate Quadratic (MQ) function and only for $K = 2$.
Example: For example we may use the differential signature scheme with the following set of parameters for HFEv-: q=2, h=127, r=7, v=1, d=257, n=128, m=120. For these parameter values[4], we have:

Corollary A.4.1. Let $\varepsilon = 1$, $m = 120$, $n \geq m$, $K = 2$. Then the exact security of the differential signature scheme for no-message attacks is

$$Security = 2^{\frac{2}{3}m} = 2^{80}.$$

This follows immediately from Theorems A.2.2 and 3.2.1. The differential signature scheme allows, unlike Quartz, to have digital signatures of 128 bits with proven exact security of 2^{80} (for no-message attacks).

A.5 Application to Quartz and Similar Schemes

Unfortunately, in the construction used in Quartz as represented on Fig. 4 and more generally for generalized Feistel-Patarin with $K > 1$, only one of the values for which we have to compute the inverse G^{-1} is given by the hashing oracle. Our reduction, the Theorem A.1.1, cannot be applied for $K = 4$. We may however apply the Theorem A.1.1 and thus A.2.2 with $K = 1$, only considering the first inverse, that is indeed given by the random oracle. This shows that the security of this scheme is at least $q^{m/2}$, which is not very satisfactory, knowing that the the Theorem 3.2.1 gives an attack in $q^{m\frac{K}{K+1}}$. Concretely, our lower bound for the security of Quartz under the Assumption 2.0.2 is 2^{50}, and the upper bound is 2^{80}. They do unfortunately not coincide.

[4] We note that $h = 127$ is a prime as in Quartz (though yet no attacks are known when it isn't).

B Chosen-Message Security

The chosen-message security of schemes such as Quartz remains an open problem. In the extended version of this paper, available from the author, it is shown that, for some special trapdoor function, and without an additional assumption, they are not in general secure against such attacks. However, it is conjectured that if the signature is computed in deterministic way, with random coins being derived from the message by a pseudo-random generator using an additional secret key, such schemes should be secure also against this (the most general) class of attacks. Such a solution is used in Quartz.