A Generic Scheme Based on Trapdoor One-Way Permutations with Signatures as Short as Possible

Louis Granboulan**

École Normale Supérieure

Abstract. We answer the open question of the possibility of building a digital signature scheme with proven security based on the one-wayness of a trapdoor permutation and with signatures as short as possible. Our scheme is provably secure against existential forgery under chosen-message attacks (with tight reduction) in the ideal cipher model. It is a variant of the construction used in QUARTZ [11], that makes multiple calls to the trapdoor permutation to avoid birthday paradox attacks. We name our scheme the *generic chained construction* (GCC) and we show that the k-rounds GCC based on a k-bit one-way permutation with k-bit security generates k-bit signatures with almost k-bit security.

1 Introduction

The size of the signature is one of the measures of the efficiency of a digital signature scheme. In the security model where the threat is existential forgery, one obvious lower bound is that k-bit signatures cannot provide better than k-bit security, because the probability that a signature is valid is at least 2^{-k}.

The quest for short signatures is long and many schemes have been proposed. One approach to obtain signatures as short as possible for a given security level of k bits has been initiated by Boneh et al. [5, 4], who use pairing in elliptic curves to generate $2k$-bit signatures. This approach permits relatively fast signature generation and signature verification, its main drawback is that the signature have twice the minimal possible length. Other schemes with short signatures based on the hardness of the elliptic curve discrete logarithm have been proposed [17, 18] but they use message recovery and the signed message is not shorter than with Boneh et al.. The approach of Patarin, Courtois et al. [11, 9, 10] is to use new hard problems (based on multivariate equations or coding theory) to generate αk-bit signatures with $\alpha < 2$. But their security is based on ad hoc assumptions (see section 4.3 for more details). Granboulan [13] uses the ideal cipher model to generate k-bit signatures based on any trapdoor one-way permutation, but the main weakness of his technique is that these are signature schemes with message recovery. This result is extended in [14].

** This work is supported in part by the French government through X-Crypt, in part by the European Commission through ECRYPT.

In this paper, we introduce a new technique, which can be seen as a mix of [11, 9] and [13], that allows to have k-bit signatures with appendix with security based on the sole one-wayness of a permutation, in the ideal cipher model.

The next section recalls classical definitions and previous results. It includes well known results on Full Domain Hash schemes and emphasises the fact that its generic security proof is optimal. It describes the Chained Patarin (or Feistel-Patarin) construction for digital signature schemes and makes an overview of its known properties. The material of this section is similar to the one that introduces Courtois' study of Quartz [9].

The third section describes our new *generic chained construction* for digital signature schemes, and shows that it can have an optimal generic security proof and that it can be used to design schemes that are as close as needed to the theoretical lower bound on the length of signatures. Our chained construction is based on iterating a trapdoor permutation, and therefore can be linked to the techniques by Lysyanskaya et al. [16] that generate aggregate signatures.

The fourth section compares GCC with some other techniques, and gives some comments and open questions.

2 Preliminaries

2.1 Definitions

Digital signatures schemes. A digital signature scheme ("with appendix", not "with message recovery") is defined by the following sets and algorithms:

- $\mathcal{M}$ is the set of messages,
- $\mathcal{PK}$ is the set of public keys and $\mathcal{SK}$ the set of secret keys,
- for any $pk \in \mathcal{PK}$, $\mathcal{S}_{pk}$ is the (finite) set of possible signatures,
- Gen is a randomised key generation algorithm that outputs a pair $(pk, sk) \in \mathcal{PK} \times \mathcal{SK}$,
- $\mathsf{Sign}_{pk,sk} : \mathcal{M} \to \mathcal{S}_{pk}$ is the signature algorithm for the public key pk,
- $\mathsf{Ver}_{pk} : \mathcal{M} \times \mathcal{S}_{pk} \to \{0, 1\}$ is the corresponding verification algorithm.

The scheme is consistent if for all (pk, sk) generated by Gen and all m we have $\mathsf{Ver}_{pk}(m, \mathsf{Sign}_{pk,sk}(m)) = 1$.

Security of a digital signatures scheme. The scheme is secure under chosen message attack with q_S queries if no attacker allowed to adaptively ask q_S signatures of chosen messages can with high success probability output a valid signature that was not one of the q_S answers. Such a machine is called an existential forger[1]. For $q_S = 0$ it is said that the scheme is secure under a no-message attack.

[1] A slightly less strong definition is more common in the literature, where the forgery needs to be with a new message. We prefer the stronger definition even if it may not be necessary [1].

Exact security. The scheme is (t, ϵ)-secure if no forger is a (t, ϵ)-forger, where a (t, ϵ)-forger is a forger running in expected time at most t (where the unit for time measurement is e.g. the average time necessary to run Ver_{pk}) and with a probability of successfully outputting a forgery less than ϵ.

The scheme is said to have k-bit security if there is no (t, ϵ)-forger such that $t/\epsilon < 2^k$.

To avoid technical subtleties about the exact running time and success probability, we will introduce a new definition: a scheme is $[t, \epsilon]$-secure if it is $(\alpha_t t, \alpha_\epsilon \epsilon)$-secure for $1/\beta < \alpha_t, \alpha_\epsilon < \beta$, for a small β (typically 2 or 10). Another equivalent definition of $[t, \epsilon]$-security applies to the case where the scheme depends on a complexity parameter n (e.g. the size of the public key), and the condition is that β is a constant independent of n. $[k]$-bit security is defined in a similar way.

Trapdoor one-way permutations. For any $pk \in \mathcal{PK}$, let $\mathcal{S}_{pk}$ be a set of $2^{\ell_{pk}}$ elements. The family $\mathsf{f}_{pk} : \mathcal{S}_{pk} \to \mathcal{S}_{pk}$ is said to be a family of trapdoor one-way permutations if f_{pk} is easy to compute for any pk and if pk can be randomly generated by some algorithm Gen in such a way that it comes with a trapdoor sk that makes easy to compute f_{pk}^{-1}. It is (t, ϵ)-secure if any machine running in expected time t (the unit for time measurement is e.g. the average time necessary to compute f_{pk}) on a random input pk and $s \in \mathcal{S}_{pk}$ cannot compute f_{pk}^{-1} with better probability than ϵ. Such a machine is called an inverter. The permutation is said to have k-bit security if there is no (t, ϵ)-inverter such that $t/\epsilon < 2^k$.

It is obvious that an exhaustive search can be used to invert f_{pk}, therefore it is impossible to have k-bit security for $k > \ell$ where ℓ is the average value of ℓ_{pk} for random pk generated by Gen. It is an open problem whether if it is possible to reach this lower bound or not. The best candidates are some discrete logarithm-based functions, which apparently have $[\ell/2]$-bit security, and some specific functions (e.g. based on quadratic multivariate equations [11] or error correcting codes [10]) that may have $[\alpha\ell]$-bit security for $\alpha > 1/2$.

Another obvious property is that trapdoor one-way permutations that are random-self-reducible or based on claw-free functions have another upper bound for their security: an attack based on the birthday paradox shows that it is impossible to have k-bit security for $k > \ell/2$. It is the case for trapdoor one-way permutations based on classical number theoretical problems (factorisation or discrete logarithm).

A $[\ell]$-bit secure trapdoor one-way permutation is called *optimal trapdoor one-way permutation.*

2.2 Previous results on Full Domain Hash

Full Domain Hash (FDH) has been named by Bellare and Rogaway [2] and is one of the most classical techniques to construct digital signature schemes.

Definition 1 (FDH). *Let* $\mathsf{H}_{pk} : \mathcal{M} \to \mathcal{S}_{pk}$ *be a family of cryptographic hash functions and* $\mathsf{f}_{pk} : \mathcal{S}_{pk} \to \mathcal{S}_{pk}$ *be a family of trapdoor one-way permutations. A* *valid signature s of a message m under the key pk is the unique value such that* $\mathsf{H}_{pk}(m) = \mathsf{f}_{pk}(s)$. *It can be generated using the trapdoor by* $s = \mathsf{f}_{pk}^{-1} \circ \mathsf{H}_{pk}(m)$.

Generic attack by birthday paradox. The forger computes $2^{\ell_{pk}/2}$ hash on random messages and $2^{\ell_{pk}/2}$ images of random signatures. Birthday paradox[2] shows that there is probably a collision such that $\mathsf{H}_{pk}(m) = \mathsf{f}_{pk}(s)$.

Therefore FDH cannot have better than $[\ell/2]$-bit security.

Security proof. The classical security proof for FDH needs the random oracle model. This means that the forger is forced to use an external *oracle* when it wants to compute the hash function. The number of queries to this oracle is bounded by q_H. The security proof shows that if there exists a (t, ϵ) forger against FDH that makes q_S signature queries and q_H hash queries, then one can design an algorithm that uses this forger as a black box, that controls the oracle for H_{pk}, and that is a $[t, \epsilon/q_H]$-inverter for the trapdoor permutation.

Therefore FDH based on a k-bit secure trapdoor one-way permutation has at least $[k/2]$-bit security.

Conclusion. If there exists an optimal family of trapdoor one-way permutations, then the security proof and the generic attack show that FDH based on this family has exactly $[\ell/2]$-bit security. Therefore the previous security proof is optimal, because a better proof would imply the non-existence of optimal trapdoor one-way permutations. It can be improved only with additional properties of f_{pk}, e.g. claw-free function [7, 12].

2.3 Previous results on Chained Patarin construction

It has been introduced for the QUARTZ signature scheme [11], and is named The Chained Patarin Construction (CPC) [19] or Feistel-Patarin Construction [9]. It depends on an integer parameter r (the number of rounds). QUARTZ uses $r = 4$ and FDH is the special case where $r = 1$. Here we describe the basic CPC. QUARTZ uses a generalisation of CPC to trapdoor functions that are not permutations.

Definition 2 (CPC). *For any $pk \in \mathcal{PK}$ let $\mathcal{S}_{pk}$ be a set of $2^{\ell_{pk}}$ elements with a group operation $\oplus$. For $i = 1...r$ let $\mathsf{H}_{pk,i} : \mathcal{M} \to \mathcal{S}_{pk}$ be a cryptographic hash function and $\mathsf{f}_{pk,i} : \mathcal{S}_{pk} \to \mathcal{S}_{pk}$ be a trapdoor one-way permutation. A signature $s \in \mathcal{S}_{pk}$ for the message m under the key pk is checked with the following procedure: let $s_r = s$ and for $i > 0$ let $s_{i-1} = \mathsf{f}_{pk,i}(s_i) \oplus \mathsf{H}_{pk,i}(m)$, the signature is valid if $s_0 = 0$. The signature is generated using the trapdoors by $s_0 = 0$, for $i = 1...r$, $s_i = \mathsf{f}_{pk,i}^{-1}(s_{i-1} \ominus \mathsf{H}_{pk,i}(m))$ and $s = s_r$.*

[2] Usually the birthday paradox is invoked when looking at collisions when randomly selecting a single set from a larger superset. Here collisions between two independently selected sets from the same superset are examined. The same principle applies, up to a small constant in the probability of collision ($1/\sqrt{2}$).

Generic attack by birthday paradox. The forger chooses $2^{\frac{r}{r+1}\ell_{pk}}$ random messages and computes $\mathsf{H}_{pk,1}(m)$ and chooses $2^{\frac{r}{r+1}\ell_{pk}}$ random values x_1 and computes their images $y_1 = \mathsf{f}_{pk,1}(x_1)$. Birthday paradox shows that there are $2^{\frac{r-1}{r+1}\ell_{pk}}$ collisions such that $\mathsf{f}_{pk,r}(x_1) = \mathsf{H}_{pk,1}(m)$. After one round, we have $2^{\frac{r-1}{r+1}\ell_{pk}}$ candidate pairs (m, x_1). Then the forger chooses $2^{\frac{r}{r+1}\ell_{pk}}$ random values x_2 and computes their images $y_2 = \mathsf{f}_{pk,2}(x_2)$. For each candidate pair, there is a probability $2^{-\frac{1}{r+1}\ell_{pk}}$ that $x_1 \ominus \mathsf{H}_{pk,2}(m)$ is equal to some y_2. Therefore after 2 rounds we have $2^{\frac{r-2}{r+1}\ell_{pk}}$ candidate pairs (m, x_2). And after i rounds we have $2^{\frac{r-i}{r+1}\ell_{pk}}$ candidate pairs (m, x_i). After r rounds all candidate pairs (m, x_r) are valid signatures, and the expected number of such pairs is roughly one.

Therefore the r-rounds CPC cannot have better than $[\frac{r}{r+1}\ell]$-bit security.

Security proof. The security proof of FDH applies to CPC. There is no known better security proof for CPC. The most comprehensive study of the security of CPC is by Courtois [9].

Conclusion. There is a gap between the security proof and the best generic attack known on CPC.

3 The generic chained construction and its security

3.1 Introduction

The Generic Chained Construction (GCC) is a generalisation of CPC where a block encryption is used instead of just xoring the current value with the result of a hash function.

Definition 3 (GCC). *For any $pk \in \mathcal{PK}$ and let $\mathcal{S}_{pk}$ be a set of $2^{\ell_{pk}}$ elements. For $i = 1...r$ let $\mathsf{E}_{pk,i} : \mathcal{M} \times \mathcal{S}_{pk} \to \mathcal{S}_{pk}$ be a block cipher and $\mathsf{f}_{pk,i} : \mathcal{S}_{pk} \to \mathcal{S}_{pk}$ be trapdoor one-way permutations. A signature $s \in \mathcal{S}_{pk}$ for the message m under the key pk is generated using the trapdoors by $s = \mathsf{f}_{pk,r}^{-1} \circ \mathsf{E}_{pk,r}^{-1}[m] \circ ... \circ \mathsf{f}_{pk,1}^{-1} \circ \mathsf{E}_{pk,1}^{-1}[m](0)$. The signature verification computes $v = \mathsf{E}_{pk,1}[m] \circ \mathsf{f}_{pk,1} \circ ... \circ \mathsf{E}_{pk,r}[m] \circ \mathsf{f}_{pk,r}(s)$. The signature is valid if $v = 0$.*

The special case where $\mathsf{E}_{pk,i}[m](x) = x \oplus \mathsf{H}_{pk,i}(m)$ is exactly the chained Patarin construction.

The public key should contain the description of all $\mathsf{E}_{pk,i}$ and of all $\mathsf{f}_{pk,i}$. NB: the security proof of theorem 1 below shows that these r functions don't need to be distinct.

Generic attack by birthday paradox. This is the same attack as the attack against CPC.

The forger chooses $2^{\frac{r}{r+1}\ell_{pk}}$ random messages and computes $\mathsf{E}_{pk,1}^{-1}[m](0)$ and chooses $2^{\frac{r}{r+1}\ell_{pk}}$ random values x_1 and computes their images $y_1 = \mathsf{f}_{pk,1}(x_1)$.

Birthday paradox shows that there are $2^{\frac{r-1}{r+1}\ell_{pk}}$ collisions such that $\mathsf{f}_{pk,1}(x_1) = \mathsf{E}^{-1}_{pk,1}[m](0)$. After one round, we have $2^{\frac{r-1}{r+1}\ell_{pk}}$ candidate pairs (m, x_1). Then the forger chooses $2^{\frac{r}{r+1}\ell_{pk}}$ random values x_2 and computes their images $y_2 = \mathsf{f}_{pk,2}(x_2)$. For each candidate pair, there is a probability $2^{-\frac{\ell_{pk}}{r+1}}$ that $\mathsf{E}^{-1}_{pk,2}[m](x_1)$ is equal to some y_2. Therefore after 2 rounds we have $2^{\frac{r-2}{r+1}\ell_{pk}}$ candidate pairs (m, x_2). And after i rounds we have $2^{\frac{r-i}{r+1}\ell_{pk}}$ candidate pairs (m, x_i). After r rounds all candidate pairs (m, x_r) are valid signatures, and the expected number of such pairs is roughly one.

Therefore the r-rounds GCC cannot have better than $[\frac{r}{r+1}\ell]$-bit security.

3.2 Security proof against a chosen message attack

Theorem 1. *If there exists a (t, ϵ)-forger against r-rounds GCC based on trapdoor one-way permutations of 2^ℓ elements that makes at most q_E cipher queries and q_S signature queries then one can design an algorithm that uses this forger as a black box, that controls the oracle for $\mathsf{E}_{pk,i}$, and is a $[t, (q_E + q_S)^{-1/r}\epsilon]$-inverter against one of the trapdoor one-way permutations.*

Proof. The forger receives a public key and makes at most q_E cipher queries and q_S signature queries, corresponding to $N \le q_E + q_S$ messages m. The algorithm that answers those queries should simulate the behaviour of an algorithm that knows the secret key, it is called the simulator. The challenge is pk and a value $\bar{x} \in \mathcal{S}_{pk}$, and the simulator wins the game if it computes one of the $\mathsf{f}^{-1}_{pk,i}(\bar{x})$.

We denote y_j the intermediate values that occur in the computation of the signature. They depend on the message, and are denoted $y_j[m]$. More precisely, for each message m that appear in some query, we let $y_0[m] = 0$ and for $j = 1...r$, let $x_j[m] = \mathsf{E}^{-1}_{pk,j}[m](y_{j-1}[m])$ and $y_j[m] = \mathsf{f}^{-1}_{pk,j}[m](x_j[m])$. The last value $y_r[m]$ is the signature.

- Simulation

  Game 0. For each m, the simulator chooses random values for $y_j[m]$, computes $x_j[m] = \mathsf{f}_{pk,j}[m](y_j[m])$, and fixes $\mathsf{Sign}(m) = y_r[m]$ and $\mathsf{E}_{pk,j}[m] : x_j[m] \mapsto y_{j-1}[m]$. All other cipher queries are answered with random values. All the answers to cipher queries are kept in a table, that restricts the choice of the random answers to the queries to the ones such that all $\mathsf{E}_{pk,j}[m]$ are permutations. It is a perfect simulator.

  Game j, for $j = 1...r$. This game is similar to Game j-1, but the values $y_j[m]$ are not fixed in advance but only when needed. Therefore, $y_j[m]$ is fixed only if $\mathsf{Sign}(m)$ or $\mathsf{E}^{-1}_{pk,j}[m](y_{j-1}[m])$ are queried.
  All values $y_{j+1}[m]$, ..., $y_r[m]$ are still fixed in advance. That means that all $x_{j+1}[m]$, ..., $x_r[m]$ are computed in advance, but that $x_j[m]$ is unknown. Therefore (unless $y_j[m]$ is fixed) the simulator does not know when a $\mathsf{E}_{pk,j}[m]$ for $x_j[m]$ is made, and answers random values to all $\mathsf{E}_{pk,j}[m]$ queries.
  Event Bad(j) happens when some $\mathsf{E}_{pk,j}[m](\hat{x})$ query is answered $y_{j-1}[m]$ and afterwards the signature of m is queried, because the simulator needs

to know the value of $y_j[m]$ hence needs to find $\mathsf{f}_{pk,j}^{-1}(\hat{x})$. For each $\mathsf{E}_{pk,j}[m]$ cipher query, the probability that the answer is $y_{j-1}[m]$ is $2^{-\ell}$.

– A study of Game r.

There are at most q_E queries that may cause some event Bad(j), therefore this failure happens with probability less than $q_E 2^{-\ell}$. But we can make the hypothesis that the forger is at least as efficient as the one based on the birthday paradox, therefore $(q_E + q_S) \leq 2^{\frac{r}{r+1}\ell}$. Game 0 and Game r can be distinguished with probability at most $2^{-\frac{\ell}{r+1}}$, which is less than $\frac{1}{2}$ if $r \leq l-1$.

Let $X(j)$ be the set of the messages such that $y_1[m], ..., y_j[m]$ are fixed by cipher queries. Let n_j be the size of $X(j)$.
If m is a random message in $X(j)$ with $j < r$, then with probability $\frac{n_{j+1}}{n_j}$ it is also an element of $X(j+1)$ and the simulator does not need to know $y_j[m]$ when answering $x_j[m]$ to the cipher query $\mathsf{E}_{pk,j}[m](y_{j-1}[m])$, because it will learn it when $\mathsf{E}_{pk,j}[m](y_j[m])$ is queried.
If m is a random message in $X(r)$, then with probability $\frac{1}{n_r}$ it is the message that is output by the forger and the simulator does not need to know $y_r[m]$ when answering $x_r[m]$ to the cipher query $\mathsf{E}_{pk,r}[m](y_{r-1}[m])$, because it will learn it when the forger outputs its forgery.

– Inversion.

Game j' for $j = 1...r$. The simulator runs a game identical to Game j with the exception of one value $y_j[m]$ that is unknown to the simulator but fixed with $x_j[m] = \bar{x}$. Therefore with probability $\frac{n_{j+1}}{n_j}$ the simulator learns the value of $\mathsf{f}_{pk,j}^{-1}(\bar{x})$.

Last Game. The simulator runs at random one of the Games j'.
One of the probabilities $\frac{n_2}{n_1}, ..., \frac{n_{j+1}}{n_j}, ..., \frac{n_r}{n_{r-1}}, \frac{1}{n_r}$ is greater than $n_1^{-1/r}$, which is greater than $(q_E + q_S)^{-1/r}$, therefore, if $r \leq l-1$, the probability of successfully learning one of the $\mathsf{f}_{pk,j}^{-1}(\bar{x})$ is greater than $\frac{1}{2r}(q_E + q_S)^{-1/r}$

□

This theorem shows that r-rounds GCC based on a $[t, \epsilon]$-bit secure trapdoor one-way permutation has $(t, (q_E + q_S)^{1/r}\epsilon)$-bit security in a chosen-message attack. This implies that for k-bit secure permutations the scheme is $[k - \frac{1}{r}\log_2(q_E + q_S)]$-secure. The running time of an attacker is necessarily greater than $q_E + q_S$, therefore $\log_2(q_E + q_S) \leq k - \frac{1}{r}\log_2(q_E + q_S)$ or equivalently $\log_2(q_E + q_S) \leq \frac{r}{r+1}k$, which means that the scheme is $[k - \frac{1}{r+1}k]$-secure.

Our theorem shows that r-rounds GCC based on a k-bit secure trapdoor one-way permutation has $[\frac{r}{r+1}k]$-bit security in a chosen-message attack. Therefore r-rounds GCC based on optimal trapdoor one-way permutations has at least $[\frac{r}{r+1}\ell]$-bit security, which is the efficiency of the generic attack by birthday paradox.

One surprising fact is that chosen-message attacks of GCC are not more powerful than no-message attacks.

4 Comments on GCC

4.1 Optimality

k-round GCC has almost the best possible security for a generic scheme based on trapdoor one-way permutations. If a scheme can be based on any k-bit secure trapdoor one-way permutation, then it should be secure in the case where there exist an algorithm that computes inverses of the permutation in time 2^k and with probability 1. Then, the forger that uses this algorithm to implement the signature algorithm runs in time $r2^k$ where r is the number of inverses needed to sign. This proves that a digital signature scheme based on a k-bit secure trapdoor one-way permutation cannot have better than $[k]$-bit security.[3]

For any constant α, αk-round GCC has asymptotically $[k-\log k]$-bit security, which is almost the best possible result.

k-round GCC based on an optimal trapdoor one-way permutation is a digital signature scheme with the shortest possible signatures. This is a consequence from the previous remark. If there exists an optimal trapdoor one-way permutation, we can obtain $[k]$-bit security with signature as short as $k + \log k$ bits.

This seems to contradict the result of Coron [8, annex E], which implies that a hash-and-sign digital signature with k-bit security cannot have shorter signature than $k + \log q_S$ bits. But our scheme is not a hash-and-sign scheme.

4.2 Implementation and practical use

The ideal cipher model. The ideal cipher model is a technique to prove the security of a cryptographic scheme in an *idealised world* where an oracle exists which implements random permutations. It is similar to the random oracle model, where the oracle implements random functions. The random oracle model has been proven[4] to be impossible to instantiate in general [6], and it is very likely that this result extends to the ideal cipher model. However, there is no reason for a block cipher with no other properties than being a strong pseudo-random permutation generator to fail to instantiate the ideal cipher in GCC.

[3] A scheme based on a k-bit secure trapdoor one-way permutation may have better than $[k]$-bit security if there is no such inverter for the permutation. For example if the best k-bit inverter runs in time 2^{k-1} and succeeds with probability $1/2$, the previous argument describes a forger that succeeds with probability 2^{-r}, which is a $[k+r]$-bit forger.

[4] The applicability of this proof to realistic cryptographic schemes is debatable [15], because it uses a specific ad hoc and unrealistic construction of a counter-example.

Choosing the cipher. The key space of the cipher is the set of all possible messages. No cipher has such an infinite key space, but this problem can easily be solved. For k-bit security, we need a collision-resistant hash function H with a $2k$-bit output, and a block cipher C with $2k$-bit keys and, then $\mathsf{E}[m](x) = \mathsf{C}_{\mathsf{H}(m)}(x)$ can be used in GCC.

A more difficult problem is that the cipher should encrypt blocks that are in the set $\mathcal{S}_{pk}$ of $2^{\ell_{pk}}$ elements permuted by the $\mathsf{f}_{pk,i}$. Current block cipher only handle the cases where $\ell_{pk} \in \{64, 128, 256\}$, while we may want to use arbitrary integer and non-integer values. There is some literature on the subject [3] but no well-established solution exist.

A problem may arise if the domain $\mathcal{S}_{pk}$ depends on pk, because implementing a block cipher depending on pk is costly.

The trapdoor one-way permutations. The description of the r-round scheme uses r trapdoor permutations $\mathsf{f}_{pk,i}$. But the security proof does not make the hypothesis that these permutations are distinct ones. If the size of the public key matters, we recommend to use the same trapdoor permutation for all rounds. This is also true for CPC, and for example Quartz uses a unique $\mathsf{f}_{pk,i}$.

However, if the attacker is able to easily invert one of the $\mathsf{f}_{pk,i}$, then the effect is that one round of GCC is cancelled. Therefore the attack by birthday paradox is more efficient and the security proof is less efficient. The use of distinct permutations for $\mathsf{f}_{pk,i}$ allows to combine their one-wayness without increasing the size of the signature.

4.3 Comparison with some other schemes

Theoretical design	Message recovery	Signature length	Heuristic security	Proven security[5]	Based on
r-round GCC		k	$\frac{r}{r+1}k$	$\frac{r}{r+1}k$	one-way
r-round CPC [11]		k	$\frac{r}{r+1}k$	$k/2$	one-way
CFS-like scheme [10]		k	k	$k/2$	one-way
FDH		$2k$	k	k	one-way
Improved PSS [14]		$2k$	k	$k-1$	claw-free
OPSS-R [13, 14]	X	k	k	k	one-way
Boneh et al. [5, 4]		$2k$	k	k	pairing
Naccache-Stern [17]	X	$2.5k$	k	k	discrete log
Pintsov-Vanstone [18]	X	$2k$	k	k	discrete log

Quartz. Our security proof for GCC is different from the study of CPC made by Courtois, because the security proof in [9, section 4] is based on an additional assumption for the underlying one-way function: the assumption that the best algorithm that computes many inverses is the one that computes them

[5] If the underlying function is one-way.

independently. This assumption is likely to hold for optimal trapdoor one-way permutations, but does not hold in general.

Moreover, both the structure of Quartz and of the Differential Signature Scheme [9, annex A.4] are insecure if the underlying one-way function F is homomorphic (i.e. $F(x+y) = F(x)+F(y)$) while our structure makes no hypothesis other than the one-wayness.

It is an open problem to prove the security of the CPC construction under the hypothesis of non-homomorphism and one-wayness.

Code-based schemes [10]. The authors describe a scheme that generates 81-bit signatures and claims to have 83-bit security against no-message attacks. The scheme is constructed using a non-proven generalisation of FDH to trapdoor injective functions where $\mathsf{f}_{pk} : \mathcal{S}_{pk} \rightarrow \mathcal{H}_{pk}$ where membership in $\mathsf{f}_{pk}(\mathcal{S}_{pk})$ is difficult to test without the trapdoor. It is likely that a security proof for this scheme will suffer the same problem as the security proof of FDH: that it is not tight.

4.4 Conclusion

We decribe a new technique that allows to generate digital signature schemes based on trapdoor one-way permutations, that are secure in the ideal cipher model and have a signature length as short as possible. However, their running time (for k-bit security) is k times the running time of Full Domain Hash.

An open question is whether it is possible to have short signatures with less than k calls to the trapdoor function or not. Another open question is whether it is possible to have signatures of similar length that are provably secure without an idealised model or not.

References

1. J. H. An, Y. Dodis, and T. Rabin, "On the security of joint signature and encryption." in *Proceedings of Eurocrypt'02* (L. R. Knudsen, ed.), no. 2332 in Lecture Notes in Computer Science, pp. 83–107, Springer-Verlag, 2002.
2. M. Bellare and P. Rogaway, "The exact security of digital signature – how to sign with RSA and Rabin." in *Proceedings of Eurocrypt'96* (U. Maurer, ed.), no. 1070 in Lecture Notes in Computer Science, pp. 399–416, Springer-Verlag, 1996. Revised version available at `http://www-cse.ucsd.edu/users/mihir/papers/exactsigs.html`.
3. J. Black and P. Rogaway, "Ciphers with arbitrary finite domains." in *Proceedings of CT-RSA'02* (B. Preneel, ed.), no. 2271 in Lecture Notes in Computer Science, pp. 114–130, Springer-Verlag, 2002.
4. D. Boneh and X. Boyen, "Short signatures without random oracles." in *Proceedings of Eurocrypt'04* (C. Cachin and J. Camenisch, eds.), no. 3027 in Lecture Notes in Computer Science, pp. 56–73, Springer-Verlag, 2004.
5. D. Boneh, B. Lynn, and H. Shacham, "Short signature from the Weil pairing." in *Proceedings of Asiacrypt'01* (C. Boyd, ed.), no. 2248 in Lecture Notes in Computer Science, pp. 514–532, Springer-Verlag, 2001.

6. R. Canetti, O. Goldreich, and S. Halevi, "The random oracle methodology, revisited." in *Proceedings of Symposium on Theory of Computing – STOC'98*, pp. 209–218, ACM Press, 1998.
7. J.-S. Coron, "On the exact security of Full Domain Hash." in *Proceedings of Crypto'00* (M. Bellare, ed.), no. 1880 in Lecture Notes in Computer Science, pp. 229–235, Springer-Verlag, 2000.
8. J.-S. Coron, "Optimal security proofs for PSS and other signature schemes." in *Proceedings of Eurocrypt'02* (L. R. Knudsen, ed.), no. 2332 in Lecture Notes in Computer Science, pp. 272–287, Springer-Verlag, 2002. Also available at `http://eprint.iacr.org/2001/062/`.
9. N. T. Courtois, "Generic attacks and the security of Quartz." in *Proceedings of Public Key Cryptography – PKC'03* (Y. Desmedt, ed.), no. 2567 in Lecture Notes in Computer Science, pp. 351–364, Springer-Verlag, 2003.
10. N. T. Courtois, M. Finiasz, and N. Sendrier, "How to Achieve a McEliece-Based Digital Signature Scheme." in *Proceedings of Asiacrypt'01* (C. Boyd, ed.), no. 2248 in Lecture Notes in Computer Science, pp. 157–175, Springer-Verlag, 2001.
11. N. T. Courtois, L. Goubin, and J. Patarin, "Quartz, 128-bit long digital signature." in *Proceedings of CT-RSA'01* (D. Naccache, ed.), no. 2020 in Lecture Notes in Computer Science, pp. 282–297, Springer-Verlag, 2001. See also `http://www.minrank.org/quartz/`.
12. Y. Dodis and L. Reyzin, "On the power of claw-free permutations." in *Proceedings of SCN'02* (S. Cimato, C. Galdi, and G. Persiano, eds.), vol. 2576 of *Lecture Notes in Computer Science*, Springer-Verlag, 2002. Also available at `http://eprint.iacr.org/2002/103/`.
13. L. Granboulan, "Short signatures in the random oracle model." in *Proceedings of Asiacrypt'02* (Y. Zheng, ed.), no. 2501 in Lecture Notes in Computer Science, pp. 364–378, Springer-Verlag, 2002.
14. J. Katz and N. Wang, "Efficiency improvements for signature schemes with tight security reductions." in *Proceedings of CCS'03*, ACM Press, 2003.
15. N. Koblitz and A. Menezes, "Another Look at 'Provable Security' ". 2004. Available at `http://eprint.iacr.org/2004/152/`.
16. A. Lysyanskaya, S. Micali, L. Reyzin, and H. Shacham, "Sequential aggregate signatures from trapdoor permutations." in *Proceedings of Eurocrypt'04* (C. Cachin and J. Camenisch, eds.), no. 3027 in Lecture Notes in Computer Science, pp. 74–90, Springer-Verlag, 2004.
17. D. Naccache and J. Stern, "Signing on a postcard." in *Proceedings of Financial Cryptography – FC'00* (Y. Frankel, ed.), no. 1962 in Lecture Notes in Computer Science, pp. 121–135, Springer-Verlag, 2000.
18. L. A. Pintsov and S. A. Vanstone, "Postal revenue collection in the digital age." in *Proceedings of Financial Cryptography – FC'00* (Y. Frankel, ed.), no. 1962 in Lecture Notes in Computer Science, pp. 105–120, Springer-Verlag, 2000.
19. NESSIE consortium, "NESSIE Security report." Deliverable report D20, NESSIE, 2002. Available from `http://www.cryptonessie.org/`.