Making Conditionally Secure Cryptosystems Unconditionally Abuse-Free in a General Context

(Extended Abstract)

Yvo G. Desmedt

Dept. EE & CS, Univ. of Wisconsin - Milwaukee

P.O. Box 784, WI 53201 Milwaukee, U.S.A.

Abstract. *[Sim84] introduced the concept of subliminal channel in the context of signature systems. [Des88b] presented a solution against subliminal channels and extended in [Des88a] the solution to abuse-free coin-flipping, abuse-free generation of public keys, and abuse-free zero-knowledge. In this paper we demonstrate that a whole family of systems (generalized Arthur-Merlin games) can be made abuse-free, avoiding the exhaustive approach of [Des88a]. We will hereto formalize the concept of abuse.*

1 Introduction

[Sim84] found that a secret message can be hidden in a subliminal way through the authentication process. Simmons called the hidden channel the *subliminal channel* Simmons illustrated it, by comparing it with two prisoners who are communicating authenticated messages in full view of a warden. The warden is able to read the messages. The subliminal consists in hiding a message through the authentication scheme such that the warden cannot detect its use nor read the hidden part (for other subliminal channels see [JS86,Sim85,Sim86]).

[Des88b] demonstrated that subliminal-free authentication and signature systems can be made by introducing the concept of active warden (a warden who modifies the authenticator). [Des88a] studied subliminal channels in different contexts (which was then called abuses). [Des88a]'s solutions against abuses are exhaustive, discussing particular solutions to particular problems. The *goal of this paper* is to prove, in a *constructive way*, that *all* cryptosystems can be made abuse-free using a compiler which will transform a given cryptosystem into an abuse-free version (similarly as [GMW86, p. 185], but keeping the solution practical). However, our solution could ruin the security specifications, in other words, it could be that the abuse-free version is no longer a secure cryptosystem. Therefore, we can only prove our theorem for a family of cryptosystems.

G. Brassard (Ed.): Advances in Cryptology - CRYPTO '89, LNCS 435, pp. 6-16, 1990.

2 Formal model for abuses and abuse-freeness

We assume that the reader is familiar with terminology of [GMR89] (will be briefly overviewed in final paper) and notations in [CEvdGP87]. We now introduce a formal description of an active and a passive warden, covering them together to avoid long-windedness. The model has similarities with the one in [BOGKW88].

Definition 1 Let $A_1, \ldots, A_m, A_{m+1}$ be probabilistic Turing machines. If all machines A_i have a shared common read-only tape C and in addition:

- all A_i $(1 \leq i \leq m+1)$ have their own work-tape and own random tape,
- each A_i $(1 \leq i \leq m+1)$ has a private read-only tape H_i and the content of these tapes has been written before the machines run,
- for all i such that $1 \leq i \leq m$, A_i has $m-1$ write-only communication tapes $T_{i,j}$ $(1 \leq j \leq m$ and $i \neq j)$ and A_{m+1} has $m(m-1)$ read only communication tapes $R'_{i,j}$ such that $R'_{i,j} = T_{i,j}$ (for all i and j such that $i \neq j$ and $1 \leq i \leq m$ and $1 \leq j \leq m$),
- for all i such that $1 \leq i \leq m$, A_i has $m-1$ read-only communication tapes $R_{i,j}$ $(1 \leq j \leq m$ and $i \neq j)$ and A_{m+1} has $m(m-1)$ write only-communication tapes $T'_{i,j}$ such that $T'_{i,j} = R_{i,j}$ (for all i and j such that $i \neq j$ and $1 \leq i \leq m$ and $1 \leq j \leq m$),
- the order in which these machines write on the tapes is fixed (*e.g.*, A_1 starts),

then we call $\mathbf{A} = (A_1, \ldots, A_m, A_{m+1})$ an *m-participant system with warden*, A_{m+1}, or for short *m-participant system*. We will denote A_{m+1} mostly as W. If m could be an indeterminate, we call $\mathbf{A}$ a *multi-participant system* with warden, W. *If* the warden, W, does not read the common tape C, his random tape, his private read-only tape H_{m+1}; but only writes on tape $T'_{i,j}$ the same symbol which he reads from tape $R'_{j,i}$ (for all i and j, $i \neq j$), *then* we say that the warden is *passive*. In all other cases we say that the warden, W, is *active*.

We remark that the case that the actual communication links don't exist corresponds with machines that don't write on these tapes. Adapting the above model could be useful in other contexts. The private read-only tape H_i can be used *e.g.*, to store *secret keys*. We assume mostly that the length of H_i is polynomial in x, where x is the common input. Simplification of notations is possible by giving each A_i $(1 \leq i \leq m)$ only one tape T_i and one tape R_i. However, in our model in the case that the warden is passive the network corresponds with a complete directed graph. It depends on the context which power the probabilistic Turing machines $A_1, \ldots, A_m$ and W have.

Definition 2 Let $S(x, \mathbf{A})$ be a predicate, (specifications of the security), where $\mathbf{A}$ is a k-participant system and $x \in \{0,1\}^*$. If for a multi-participant system, $\mathbf{B}$ holds that $S(x, \mathbf{B}) = 1$ for all sufficiently long (large) $x \in L$, where $L \subset \{0,1\}^*$, then we call $\mathbf{B}$ an *$S(L)$-system with* (active or passive) *warden, W*, or shorter an *S-system* if there is no ambiguity. We will also say that the m-participant system $\mathbf{B}$ is S-secure.

Definition 2 allows us to speak about authentication-systems, signature-systems and so on. For our purposes, we now adapt notations introduced in [GMR89]. For a run of $\mathbf{A}$, an m-participant system, with x on the shared common tape (C) and with h_l on A_l's private read-only tape, *the l-participant's view* corresponds with all that can be seen from his random tape and from the read-only communication tapes $R_{l,j}$ (for all $j \in \{1, \ldots, l-1, l+1, \ldots, m+1\}$). Let $\mathrm{Pview}_{\mathbf{A},l}(x, h_l)$ be the random variable whose value is the l-participant's view. If the warden, W, is an *active* one, we define *the warden's view* to be everything that can be seen from W's random tape and from *all* read only communication tapes $R'_{i,j}$, for $i \neq j$. If the warden is *passive*, and x is on the shared common tape (C), we define *the warden's view* to be everything that can be seen from *all* read only communication tapes, $R'_{i,j}$ ($i \neq j$). $\mathrm{Wview}_{\mathbf{A}}(x)$ is the random variable whose value is the warden's view. To simplify notations, we did not specify the input h_{m+1} in the expression $\mathrm{Wview}_{\mathbf{A}}(x)$.

Definition 3 Let $\mathbf{A} = (A_1, \ldots, A_m, W)$ be an $S(L)$-system, with warden W. Let $\mathbf{A}' = (A'_1, \ldots, A'_m, W)$ be an m-participant system. $\mathbf{A}'$ is a *perfect (statistical) (computational) abuse of the $S(L)$-system* $\mathbf{A}$ if:

1. **Warden-indistinguishable:** $\{\mathrm{Wview}_{\mathbf{A}}(x)\}$ and $\{\mathrm{Wview}_{\mathbf{A}'}(x)\}$ (families of random variables) are *equal (statistically indistinguishable) (computational indistinguishable)* on L', where $L' = L$ if the warden is passive, else $L' = \{(x, h_{m+1}) \mid x \in L \text{ and } |h_{m+1}| = |x|^c\}$.

2. **k-Participant-distinguishable:** $\exists k, h_k$ $(1 \leq k \leq m)$: the families of random variables $\{\mathrm{Pview}_{\mathbf{A}''_{\mathbf{k}},k}(x, h_k)\}$ and $\{\mathrm{Pview}_{\mathbf{A}',k}(x, h_k)\}$ are *not* computationally indistinguishable on L'', where $\mathbf{A}''_{\mathbf{k}} = (A''_1, \ldots, A''_m, W)$ is an m-participant system such that $A''_i = A_i$ for all $i \neq k$ and $A''_k = A'_k$ and $L'' = \{(x, h_k) \mid x \in L \text{ and } |h_k| = |x|^c\}$.

We denote $\mathbf{A}''_{\mathbf{k}}$ as: $\mathbf{A} \star A'_k$ ($\star$ is non-commutative). The aforementioned participant k is called the *subliminal receiver. If there exists* an m-participant system $\mathbf{A}'$, which is an abuse of the m-participant system $\mathbf{A}$, we say that $\mathbf{A}$ *can be abused.*

Definition 4 Let $\mathbf{A} = (A_1, \ldots, A_m, W)$ be an $S(L)$-system, with warden W. We call $\mathbf{A}$ an *abuse-free* $S(L)$-system if for all m-participant systems $\mathbf{A}' = (A'_1, \ldots, A'_m, W)$, $\mathbf{A}'$ is *not* an abuse of the $S(L)$-system $\mathbf{A}$. We call $\mathbf{A}$ a *strong (weak) abuse-free* $S(L)$-system if for all m-participant systems $\mathbf{A}' = (A'_1, \ldots, A'_m, W)$ holds $\forall k, h_k$ $(1 \leq k \leq m)$: *if* the families of random variables $\{\mathrm{Wview}_{\mathbf{A}}(x)\}$ and $\{\mathrm{Wview}_{\mathbf{A}'}(x)\}$ are computationally indistinguishable on L', *then* $\{\mathrm{Pview}_{\mathbf{A}\star A'_k,k}(x, h_k)\}$ and $\{\mathrm{Pview}_{\mathbf{A}',k}(x, h_k)\}$

are statistically (computationally) indistinguishable on L'', where L' and L'' were defined in Definition 3.

Informal interpretation

In an abuse, the passive warden, W, is listening to all communications going on during the run of the system. However, the passive warden, W, has no access to the tapes H_i. The subliminal receiver k is waiting to receive hidden information and is therefore running his special program A'_k instead of running the normal one, namely A_k.

Abuse-freeness means that one does not exclude that a different system is used than the one intended, but the warden will detect it (almost always). Strong abuse-freeness means that a polynomial-bounded warden will (almost always) detect an abuse even if the other participants have all infinite computer power.

3 A general solution

3.1 A BUILDING BLOCK

Let us first discuss a slightly modified version of [Des88a] abuse-free generation of public keys (the main difference is that W will always publish the public key). In the final paper we will formally define what a public-key generation system is also considering [GMR88, pp. 290–291]'s definition.

Lemma 1 *If $G(\cdot)$ forms a group and r is chosen out of G according to a uniform probability distribution, (the probability to select a given r is $p(r) = 1/|G|$), then: $\forall x \in G : p(x \cdot r) = 1/|G|$ and $p(r \cdot x) = 1/|G|$, or $x \cdot r$ and $r \cdot x$, with x fixed, have uniform distributions.*

Proof. Trivial: based on group theory and [Sha49]. □

Theorem 1 *If a polynomial-time operation $\oplus$ is defined on G such that $G(\oplus)$ forms a group and f is hard to invert, then the protocol of Figure 1 is a strong abuse-free public-key generation system. The abuse-freeness is unconditional. (If the zero-knowledge protocol used is non-interactive, the length of the input $|x|$ has an upperbound similar as in [BFM88].)*

Proof. (Sketch) First observe that such a zero-knowledge protocol exists, because what has to be proven is an **NP** problem [GMW86]. (The fact that the zero-knowledge aspect in [GMW86] is based on unproven assumptions does *not* influence our proof, because its soundness is unconditional.)

Let us call the public-key generation system, which is presented in Figure 1, $\mathbf{A} = (A, B_2, \ldots, B_m, W)$. It is sufficient to prove that for all 2-participant systems $\mathbf{A}'$ holds that: *if* $\{\mathrm{Wview}_{\mathbf{A}}(x)\}$ and $\{\mathrm{Wview}_{\mathbf{A}'}(x)\}$ are computationally indistinguishable on L' *then* $\left\{\mathrm{Pview}_{\mathbf{A}*A'_2,2}(x, h_2)\right\}$ and $\{\mathrm{Pview}_{\mathbf{A}',2}(x, h_2)\}$ are statistically indistinguishable

Participant A		**Warden** W
$r \in_{(R)} G$ and $k \in_{(R)} K$ and $m := c(r,k)$	$\xrightarrow{m}$	
	$\xleftarrow{r'}$	$r' \in_R G$
$s := r \oplus r'$, $n := f(s)$	$\xrightarrow{n}$	
A proves to W that $\exists r \in G, k \in K$: $m = c(r,k) \quad \wedge \quad n = f(r \oplus r')$, using zero-knowledge.	$\xrightarrow{\text{proof}}$	If proof is interactive W asks questions and proof is repeated.
		W verifies A's proof. W publishes A's public key n.

FIGURE 1. Abuse-free generation of public key

on L'', where x specifies a description of G (as its size and so on), and where L' and L'' are similar as in Definition 3. Because the warden doesn't use his private read-only tape H_{m+1}, we replace L' by L without problems. We denote $\mathbf{A}$ as $\mathbf{A} = (A, B, W)$. Observe that $\{\text{Pview}_{\mathbf{A}\star A'_2,2}(x, h_2)\} = \{\text{Pview}_{\mathbf{A},2}(x, h_2)\}$ because B is not sending and thus not influencing. We will prove more than required; which is that there exists a poly-size family of circuits C such that *if* $\{\text{Wview}_{\mathbf{A}}(x)\}$ and $\{\text{Wview}_{\mathbf{A}'}(x)\}$ are C-computationally indistinguishable then, $\{\text{Pview}_{\mathbf{A},2}(x, h_2)\}$ and $\{\text{Pview}_{\mathbf{A}',2}(x, h_2)\}$ are statistically indistinguishable on L''.

Consider the circuit which the warden will use to check the zero-knowledge proof. Let the circuit return a 1 if the warden accepts the proof and a 0 otherwise. For this particular circuit, saying that $\{\text{Wview}_{\mathbf{A}}(x)\}$ and $\{\text{Wview}_{\mathbf{A}'}(x)\}$ are C-computational indistinguishable means that for all constants $e > 0$ and all sufficiently long strings $x \in L$: $|p(\text{warden rejects}) - p'(\text{warden rejects})| < |x|^{-e}$, where $p'(\text{warden rejects})$ and $p'(\text{warden rejects})$ denote respectively the probability that the warden will reject (the proof) when A and A' is executed. (A correct proof is not necessarily accepted with probability one, due to the definition of completeness, which is important for non-interactive proofs.)

$\text{Pview}_{\mathbf{A}',2}(x, h_2)$ is nothing else than n sent by W and the probability that a specific n_i is sent is denoted as $p'(n = n_i)$. Similarly $p(n = n_i)$ corresponds to the probability that B receives n_i when A is executed.

Using our reformulations, it is sufficient to prove that *if* (1) holds for all $e > 0$ and all sufficiently long $x \in L$, *then* (2) holds for all $d > 0$ and all sufficiently long $x \in L$.

$$p'(\text{warden rejects}) \;<\; |x|^{-e} \tag{1}$$

$$\sum_{n_i} |p(n = n_i) - p'(n = n_i)| \;<\; |x|^{-d} \tag{2}$$

We first describe how n is made. First A' makes a string m, not necessarily as specified. So there is a probability that A' returns a specific $m \in \{0,1\}^*$. Then W gives a $r' \in G$. Given this r' and his previous information, A' will make an n. n does not necessarily correspond with $f(s)$. Similarly, A' will make a proof, but nothing guarantees that this proof is correct. We will denote the string (A''s random, r', σ) as α, where σ is the string of W's questions in the zero-knowledge protocol when it is interactive, and when the zero-knowledge proof system is non-interactive, σ corresponds with the shared common random string [BFM88]. The string(s) that A' sends during the zero-knowledge proof is(are) denoted as γ. So:

$$p'(n = n_i) \quad = \quad \sum_{m_j} \sum_{\gamma_l} \sum_{\alpha_z} p'(n = n_i, m = m_j, \gamma = \gamma_l | \alpha = \alpha_z) \cdot p(\alpha = \alpha_z). \qquad (3)$$

Remark that $p(\alpha = \alpha_z)$ remains the same independently if A or A' is executed (and independent of h_2).

Let us denote $p'(\lambda = 1)$ the probability that machine A' will return at one or another stage of the protocol something different than it should have returned when it would have followed the protocol. We then prove that:

$$\sum_{n_i} |p(n = n_i) - p'(n = n_i)| \quad \leq \quad 2p'(\lambda = 1).$$

Let us denote p'(warden rejects) as $p'(\rho = 1)$. The problem remaining now is to relate $p'(\lambda = 1)$ with $p'(\rho = 1)$ and then to finally prove the theorem.

We prove that:

$$p'(\lambda = 1) \quad = \quad 1 + \frac{p'(\rho = 1) + p'(\rho = 0 | \lambda = 1) - 1}{(p'(\rho = 0 | \lambda = 0) - p'(\rho = 0 | \lambda = 1))} \qquad (4)$$

Assuming (1), this means $p'(\rho = 1) < |x|^{-e}$ for all $e > 0$ and x large enough, and using the definition of completeness and soundness we obtain that for all $t > 0$ and sufficiently large x: $p'(\lambda = 1) < |x|^{-t}$. Then follows that *if* (1) holds for all $e > 0$ and all sufficiently long $x \in L$, *then* (2) holds for all $d > 0$ and all sufficiently long $x \in L$. □

We have used the symbol $\oplus$ for a visualization aid in case $G = GF(2^n)$, but the group G does *not* have to be Abelian.

3.2 Our solution

Let us first introduce a special case of a sequential multi-participant system. (What we describe can be run in parallel under some circumstances, but our definition of a multi-participant system requires an order in which the machines write on their communication tapes.)

Definition 5 Let **A** be a sequential m-participant system with *passive* warden W. Let us call x the input of the common input tape, h_i and $q^s_{i,j}$ the content of respectively

the private tape H_i and the read-only communication tape $R_{i,j}$ at stage s. The binary string r_i contains the string read by A_i during the protocol from the random tape. We assume that the length of h_i, $q^s_{i,j}$ and r_i and the number of stages (this last requirement could be relaxed) are polynomial in function of the length of x. $q^s_{i,j}$ could be empty. During stage s, $A_{\pi(s)}$ writes n_s on tape $T_{\pi(s),\phi(s)}$. *If* $\pi(s) \neq l$ (l fixed), *then* $n_s \in_R G_{x,s}$ or $n_s = f_s(x, q^1_{\pi(s),1}, q^1_{\pi(s),2}, \ldots, q^1_{\pi(s),m}, \ldots, q^{s-1}_{\pi(s),1}, q^{s-1}_{\pi(s),2}, \ldots, q^{s-1}_{\pi(s),m})$, such that:

- the form of n_s is known beforehand in a deterministic way,
- $\forall x, s : G_{x,s}(+)$ forms a group, such that in polynomial-time (in function of the length of x) one can: execute the operations $+$, check if $x \in G_{x,s}$, and select a random element of $G_{x,s}$,
- the functions f_s are executable in polynomial time.

If $\pi(s) = l$, *then* $n_s = f_s(x, r_l, h_l, q^1_{l,1}, q^1_{l,2}, \ldots, q^1_{l,m}, \ldots, q^{s-1}_{l,1}, q^{s-1}_{l,2}, \ldots, q^{s-1}_{l,m})$, and the predicate $B_s(h_l) = 1$ is satisfied, such that:

- checking if an input exists such that $f_s(\text{input}) = \text{output}$ is an **NP** problem,
- the length of r_l, g, is fixed for a given x.

If **A** satisfies all the described properties here; we call **A** a *generalized Arthur-Merlin game*, with A_l being Merlin [Bab85].

Observe that if A_s is not Merlin *its output is either truly random or a deterministic function of its inputs*, so in the last case the random tape is not used. We would like to prove now that all $S(L)$-systems which are generalized Arthur-Merlin games can be made abuse-free. However, our solution could ruin its (security) specifications; therefore we can only prove a restricted form of it, which is based on a repetitive use of Theorem 1. We claim that most practical, conditionally secure cryptosystems can be made abuse-free if one allows interaction with the warden. Giving a proof of this claim is impossible due to a lack of an adequate formal description of all possible cryptosystems.

Corollary 1 If **A** *is a generalized Arthur-Merlin game and an* $S(L)$*-system, then there exists a multi-participant system* **A'** *(with active warden), such that either:*

- **A'** *is an unconditionally strong abuse-free* $S(L)$*-system, or*
- **A'** *isn't an* $S(L)$*-system.*

Proof. Our proof will be constructive by describing the multi-participant system **A'**. A generalized Arthur-Merlin game can be considered to be a system which is mainly publishing public keys, random numbers and/or deterministic calculations. In an initial stage, A'_l sends W a commitment ($m_l = c(r_l, k_l)$) for the bit string r_l.

Then the warden sends his random choice of his bit string r'_l (with length g). Let us now describe what is executed in $\mathbf{A}'$ instead of the execution of stage s in $\mathbf{A}$. We distinguish three different cases. *If* $\pi(s) \neq l$ *and* n_s has the form $f_s(x, q^1_{\pi(s),1}, q^1_{\pi(s),2}, \ldots, q^1_{\pi(s),m}, \ldots, q^{s-1}_{\pi(s),1}, q^{s-1}_{\pi(s),2}, \ldots, q^{s-1}_{\pi(s),m})$, *then* A'_s sends the warden n_s and the warden verifies if n_s is correct (if it is not, the warden calculates n_s himself) and sends n_s (writes $q^s_{\phi(s),\pi(s)} = n_s$ on the tape $T'_{\phi(s),\pi(s)}$). *If* $\pi(s) \neq l$, *and* n_s had to be chosen randomly from $G_{x,s}$, *then* the following steps are executed:

1. $A'_{\pi(s)}$ chooses $n_s \in_{(R)} G_{x,s}$ and sends W a commitment $(m_{\pi(s)} = c(n_s, k_{\pi(s)}))$,
2. the warden sends $A'_{\pi(s)}$: $n'_s \in_R G_{x,s}$,
3. $A'_{\pi(s)}$ sends the warden: n_s and $k_{\pi(s)}$.
4. the warden verifies the commitment. *If* correct, *then* the warden writes $q^s_{\phi(s),\pi(s)} = n_s + n'_s$, *else* sends a random $q^s_{\phi(s),\pi(s)} \in_R G_{x,s}$.

If $\pi(s) = l$, *then* A'_l sends $n_s = f_s(x, r_l \oplus r'_l, h_l, q^1_{l,1}, q^1_{l,2}, \ldots, q^1_{l,m}, \ldots, q^{s-1}_{l,1}, q^{s-1}_{l,2}, \ldots, q^{s-1}_{l,m})$ (where $\oplus$ is the bit-by-bit exclusive-or) and gives a zero-knowledge proof to W that:

$$\exists k_l \in K, r_l \in \{0,1\}^g, h_l : \quad m_l = c(r_l, k_l) \quad \wedge \quad B_s(h_l) = 1$$
$$\wedge \quad n_s = f_s(x, r_l \oplus r'_l, h_l, q^1_{l,1}, q^1_{l,2}, \ldots, q^1_{l,m}, \ldots, q^{s-1}_{l,1}, q^{s-1}_{l,2}, \ldots, q^{s-1}_{l,m}).$$

The warden verifies then A'_l's proof and writes $q^s_{\phi(s),l} = n_s$.

Let us now prove that $\mathbf{A}'$ is abuse-free. It holds that $\forall \mathbf{A}'' : \{\text{Pview}_{\mathbf{A}' * A''_l, i}(x, h_i)\}$ and $\{\text{Pview}_{\mathbf{A}', i}(x, h_i)\}$ are equal, when $i \neq l$; due to the independency of the warden's random choices. Also $\forall \mathbf{A}'' : \{\text{Pview}_{\mathbf{A}' * A''_l, l}(x, h_l)\}$ and $\{\text{Pview}_{\mathbf{A}'', l}(x, h_l)\}$ are equal. This implies that the rest of the proof follows easily from the proof of Theorem 1 (because the remark made after (3) is still valid).

Let us discuss some improvements. Sometimes, it is sufficient for the warden to check once and for all (or at the beginning of the protocol) that h_l satisfies the appropriate predicates. Instead of r_l being modified at the beginning of the protocol, it could be done during the different stages of the protocol. It is then necessary to guarantee independency of randomness when appropriate and to treat earlier altered random as deterministic variables instead of random ones. If a function f_s is deterministic, it means r_l is not used, then there is no need for interaction if A'_l's zero-knowledge proof is non-interactive. □

We make the important observation that *all* the unconditionally abuse-free cryptosystems discussed in [Des88a,Des88b] are generalized Arthur-Merlin games and therefore special cases of ours and that therefore the *proof of their abuse-freeness has not to be given for each separately.*

Let us discuss the consequences of Corollary 1 by analyzing which cryptosystems can be made abuse-free. One first has to realize that, so far, most cryptosystems have been defined without taking a (passive) warden into consideration. So first, one has to convert them into a definition in which the warden's role and privileges are defined. Mostly, one considers such a warden as an opponent. In particular the above corollary also implies (after a careful redefinition, as mentioned) that *abuse-free interactive proof systems and zero-knowledge systems for* **NP** *languages exist*, using Goldreich–Micali–Wigderson [GMW86] proof for 3-colourability and Corollary 1, *however the verifier's soundness collapses to a conditional soundness, instead of an unconditional one.* It is possible to make abuse-free zero-knowledge proofs for all languages in **NP** such that the soundness of the verifier remains unconditional, as was recently demonstrated [BD89]. This solution is however not based on the above compiler. The protocol described in [Des88a] to make zero-knowledge proof systems for **NP** languages abuse-free is only conditionally abuse-free, while the one here is unconditional.

4 Conclusions and open problems

Our approach to abuse-freeness allows one to make all (generalized Arthur-Merlin games) cryptosystems abuse-free. It is an open problem of whether Corollary 1 can be generalized to more general multi-participant systems (excluding the obvious generalizations). If so, a different proof technique will be necessary.

Trying to apply Corollary 1 on unconditionally secure authentication systems as *e.g.*, [GMS74], ruins the unconditionality of the authentication. The question whether it can be solved in one or another way is an open problem, even if the abuse-freeness would only be weak abuse-freeness (as defined). A similar remark was made related to soundness of zero-knowledge schemes, there also the unconitionality of the soundness was ruined by using above compiler. For zero-knowledge, the same problem could be solved [BD89], but the solution is not based on the above compiler.

The approach followed in this paper is constructive as well as general. It avoids the exhaustive character followed in [Des88a] but gives a global solution to the problem, useful for many situations. One of the advantages of this approach is the reduction of proofs required to demonstrate the abuse-freeness of different cryptosystems to mainly one proof.

5 REFERENCES

[Bab85] L. Babai. Trading group theory for randomness. In *Proceedings of the seventeenth ACM Symp. Theory of Computing, STOC*, pp. 421–429, May 6-8, 1985.

[BD89] M. V. D. Burmester and Y. G. Desmedt, June 1989. Text in preparation.

[BFM88] M. Blum, P. Feldman, and S. Micali. Non-interactive zero-knowledge and its applications. In *Proceedings of the twentieth ACM Symp. Theory of Computing, STOC*, pp. 103–112, May 2–4, 1988.

[BOGKW88] M. Ben-Or, S. Goldwasser, J. Kilian, and A. Wigderson. Multi-prover interactive proofs: How to remove intractability assumptions. In *Proceedings of the twentieth ACM Symp. Theory of Computing, STOC*, pp. 113–131, May 2–4, 1988.

[CEvdGP87] D. Chaum, J.-H. Evertse, J. van de Graaf, and R. Peralta. Demonstrating possession of a discrete logarithm without revealing it. In A. Odlyzko, editor, *Advances in Cryptology. Proc. Crypto'86 (Lecture Notes in Computer Science 263)*, pp. 200–212. Springer-Verlag, 1987. Santa Barbara, California, U.S.A., August 11–15.

[Des88a] Y. Desmedt. Abuses in cryptography and how to fight them. Presented at Crypto'88, Santa Barbara, California, U.S.A., to appear in: Advances in Cryptology. Proc. of Crypto'88 (Lecture Notes in Computer Science), Springer-Verlag, August 1988.

[Des88b] Y. Desmedt. Subliminal-free authentication and signature. In C. G. Günther, editor, *Advances in Cryptology, Proc. of Eurocrypt'88 (Lecture Notes in Computer Science 330)*, pp. 23–33. Springer-Verlag, May 1988. Davos, Switzerland.

[GMR88] S. Goldwasser, S. Micali, and R. Rivest. A digital signature scheme secure against adaptive chosen-message attacks. *Siam J. Comput.*, 17(2), pp. 281–308, April 1988.

[GMR89] S. Goldwasser, S. Micali, and C. Rackoff. The knowledge complexity of interactive proof systems. *Siam J. Comput.*, 18(1), pp. 186–208, February 1989.

[GMS74] E. Gilbert, F. MacWilliams, and N. Sloane. Codes which detect deception. *The BELL System Technical Journal*, 53(3), pp. 405–424, March 1974.

[GMW86] O. Goldreich, S. Micali, and A. Wigderson. Proofs that yield nothing but their validity and a methodology of cryptographic protocol design. In *The Computer Society of IEEE, 27th Annual Symp. on Foundations of Computer Science (FOCS)*, pp. 174–187. IEEE Computer Society Press, 1986. Toronto, Ontario, Canada, October 27–29, 1986.

[JS86] T. C. Jones and J. Seberry. Authentication without secrecy. *ARS Combinatoria*, 21(A), pp. 115–121, May 1986.

[Sha49] C. E. Shannon. Communication theory of secrecy systems. *Bell System Techn. Jour.*, 28, pp. 656–715, October 1949.

[Sim84] G. J. Simmons. The prisoners' problem and the subliminal channel. In D. Chaum, editor, *Advances in Cryptology. Proc. of Crypto 83*, pp. 51–67. Plenum Press N.Y., 1984. Santa Barbara, California, August 1983.

[Sim85] G. J. Simmons. The subliminal channel and digital signatures. In T. Beth, N. Cot, and I. Ingemarsson, editors, *Advances in Cryptology. Proc. of Eurocrypt 84 (Lecture Notes in Computer Science 209)*, pp. 364–378. Springer-Verlag, Berlin, 1985. Paris, France, April 9–11, 1984.

[Sim86] G. J. Simmons. The secure subliminal channel (?). In H. C. Williams, editor, *Advances in Cryptology. Proc. of Crypto 85 (Lecture Notes in Computer Science 218)*, pp. 33–41. Springer-Verlag, 1986. Santa Barbara, California, August 18–22, 1985.