Secure canonical identification schemes yield Fiat-Shamir signature schemes secure in the random oracle model

Victor Glazer

March 8, 2005

Background

- An identification scheme $ID = (G, P, V)$ is said to be *canonical* if it is a three-round, public-coin scheme. The prover P goes first; his move is called the *commitment*, denoted by $\textsc{Cmt}$. The verifier V replies with a random *challenge* $\textsc{Ch}$, consisting of his random bits. P then sends a *response* $\textsc{Rsp}$ to V, who either accepts or rejects the transcript $(\textsc{Cmt}, \textsc{Ch}, \textsc{Rsp})$.

  Remark. To streamline the presentation, we assume throughout that $n \leq |pub| \leq |pri|$ and $|\textsc{Ch}| = n$, where n is the security parameter.

- The *Fiat-Shamir transform* takes a canonical identification scheme $ID = (G, P, V)$ and a hash function $h : \{0,1\}^* \to \{0,1\}^n$, and outputs the following signature scheme $SIG_h(ID) = (GEN, SIGN, VER)$.

  The key generation algorithm, GEN, is identical to G[1].

  To sign a message $m \in \{0,1\}^*$, $SIGN_{pri}$ obtains a commitment $\textsc{Cmt}$ by running P on pri, computes $y = h(\textsc{Cmt}, m)$ and gives y to P as the challenge $\textsc{Ch}$. P responds with $\textsc{Rsp}$ (recall that the *completeness* property of ID ensures that P can correctly answer any challenge $\textsc{Ch}$). $SIGN_{pri}$ then outputs $\sigma = (\textsc{Cmt}, \textsc{Rsp})$ as the signature of m.

  To determine whether $\sigma = (\textsc{Cmt}, \textsc{Rsp})$ is a legitimate signature of m, VER_{pub} computes $y = h(\textsc{Cmt}, m)$ and runs V_{pub} on $(\textsc{Cmt}, y, \textsc{Rsp})$.

- The random oracle model is a popular approach to analyzing the security of cryptographic protocols involving hash functions. Let $h : \{0,1\}^* \to \{0,1\}^n$ be a hash function and $\pi(h)$ be a protocol which utilizes h. To prove that $\pi(h)$ is secure in the random oracle model, we proceed as follows. All parties — including the adversary — are equipped with a random oracle $\mathcal{R} : \{0,1\}^* \to \{0,1\}^n$, and evaluations of h are replaced with queries to $\mathcal{R}$. The adversary's success probability, now also taken over the randomness of $\mathcal{R}$, is then shown to be negligible in n under plausible hardness assumptions.

[1] Strictly speaking, the Fiat-Shamir transform should be defined with respect to an ensemble $\{\mathcal{H}_n\}_{n\in\mathbb{N}}$ rather than an individual function h. This is because, for any fixed h, it's easy to come up with (contrived) secure canonical id schemes which yield insecure Fiat-Shamir signature schemes. In this setting, GEN randomly chooses a key $k \in \mathcal{H}_n$ and appends it to pub to form the public key PK. The private key SK is simply set to pri.

Results

Theorem. *Let $ID = (G, P, V)$ be a secure canonical identification scheme and $h : \{0,1\}^* \to \{0,1\}^n$ be a hash function. Then the signature scheme $SIG_h(ID) = (GEN, SIGN, VER)$ is secure in the random oracle model.*

Proof. Let F be a forger that breaks the security of $SIG_h(ID)$ in the random oracle model. F has access to a random oracle $\mathcal{R} : \{0,1\}^* \to \{0,1\}^n$ and a signature oracle $\mathcal{S}$.

When queried on a string s for the first time, $\mathcal{R}$ chooses $r \in \{0,1\}^n$ uniformly at random and sets $\mathcal{R}(s) = r$. Subsequently, $\mathcal{R}$ responds with r whenever queried on s. To produce a signature $\sigma = (\textsc{Cmt}, \textsc{Rsp})$ of message m, $\mathcal{S}$ first obtains a commitment $\textsc{Cmt}$ from P_{pri} and then gives him a challenge $\mathcal{R}(\textsc{Cmt}, m)$, to which P_{pri} responds with $\textsc{Rsp}$. Observe that $\mathcal{R}$'s replies must be consistent with those of $\mathcal{S}$. For instance, if $\mathcal{S}(m) = (\textsc{Cmt}, \textsc{Rsp})$ it should be the case that $V_{pub}(\textsc{Cmt}, \mathcal{R}(\textsc{Cmt}, m), \textsc{Rsp}) = 1$.

Let $\varnothing \subset \mathcal{C} \subset \{0,1\}^*$ be the space P draws his commitments from. We make no additional assumptions about $\mathcal{C}$, so that $\mathcal{C} = \{0,1\}^n$ and $\mathcal{C} = \{\lambda\}$ are equally legitimate choices. Also, denote the message whose signature F tries to forge by m^*, and its supposed signature by $\sigma^* = (\textsc{Cmt}^*, \textsc{Rsp}^*)$.

We make a few simplifying assumptions about F, insisting that he have the following "normal form":

(i) F never queries $\mathcal{R}$ on the same string more than once.

(ii) All of F's random oracle queries are of the form $\mathcal{R}(\textsc{Cmt}, m)$, where $\textsc{Cmt} \in \mathcal{C}$ and $m \in \{0,1\}^*$.

(iii) F queries $\mathcal{R}$ on $(\textsc{Cmt}^*, m^*)$ at some point. This special query is called the "crucial query".

It isn't too hard to show that if a successful forger exists, then there exists one satisfying the above three properties.

Suppose that F fails to have property (i), so that he queries $\mathcal{R}$ on some string s multiple times. Let F' be the same as F, except that F' writes $ans = \mathcal{R}(s)$ down on an unused portion of his working tape the first time $\mathcal{R}$ is queried on s, and all subsequent random oracle queries about s are answered by looking ans up. Since $\mathcal{R}$ is a function, F''s success probability is unchanged, yet he only queries $\mathcal{R}$ on s once. If there is another string s' on which F' queries $\mathcal{R}$ multiple times, we can repeat the above process to get a new forger F'' which queries $\mathcal{R}$ on s' once. Proceeding in this fashion, we eventually obtain a forger who doesn't query $\mathcal{R}$ on any string more than once, and whose success probability is identical to that of F. This assumption guarantees that F doesn't repeat random oracle queries, so that $\mathcal{R}$'s answers are always random.

Now suppose that F fails to have property (ii), so that at least one of his random oracle queries is not of the form $\mathcal{R}(\textsc{Cmt}, m)$. Let F' be the same as F, except that all malformed $\mathcal{R}$ queries are answered randomly. Since $\mathcal{R}$'s replies are also random, these answers have exactly the right distribution. Notice that there is no interplay between answers to $\mathcal{S}$ queries and malformed $\mathcal{R}$ queries, so no inconsistencies are introduced. The new forger's success probability is therefore identical to that of F, and all of his $\mathcal{R}$ queries are well-formed.

Finally, suppose that F fails to have property (iii), namely that he never queries $\mathcal{R}$ on $(\textsc{Cmt}^*, m^*)$. Let F' be the same as F, except that instead of outputting (m^*, σ^*) right away, F' first queries $\mathcal{R}$

on $(\textsc{Cmt}^*, m^*)$. F''s success probability is identical to that of F, since the extra $\mathcal{R}$ query does not affect his output. It is also worth noting that the new forger doesn't violate assumptions (i) and (ii), because the extra $\mathcal{R}$ query is both new and well-formed.

We are now ready to describe an impersonator I which breaks the security of ID. Recall that I's goal is to get the verifier V to accept by interacting with him in the role of the prover P. I is allowed to first interact with P in the role of V polynomially many times. Since I is trying to break the *active* security of ID, he can send P whatever messages he likes.

Consider the experiment where a pair of keys (pub, pri) is generated by running G on 1^n, and I is given the public key pub.

Let $q_{\mathcal{R}}(n)$ and $q_{\mathcal{S}}(n)$ denote the number of times F queries $\mathcal{R}$ and $\mathcal{S}$, respectively, and set $q(n) = q_{\mathcal{R}}(n) + q_{\mathcal{S}}(n)$. I first interacts with P_{pri} $q(n) \cdot q_{\mathcal{S}}(n)$ times in order to construct "transcript blocks" $\mathcal{B}_1, \ldots, \mathcal{B}_{q(n)}$. Each block is made up of $q_{\mathcal{S}}(n)$ transcripts of the form $(\textsc{Cmt}, r, \textsc{Rsp})$, obtained as follows. I first receives a commitment $\textsc{Cmt} \in \mathcal{C}$ from P_{pri}. Next, I sends a challenge $r \in \{0,1\}^n$ to P_{pri}. If $\textsc{Cmt}$ does not appear in any of the transcripts added to the block so far, r is chosen randomly. Otherwise, r is set to the challenge associated with $\textsc{Cmt}$. P_{pri} responds with $\textsc{Rsp}$, and the transcript $(\textsc{Cmt}, r, \textsc{Rsp})$ is added to the block.

I next guesses the index of F's "crucial query" by randomly choosing $k \in \{1, \ldots, q_{\mathcal{R}}(n)\}$.

I now begins to simulate F. Note that assumption (ii) above enables us to associate a unique message with every $\mathcal{R}$ query F makes. Since $\mathcal{S}$ queries explicitly reference a message, every oracle query made by F therefore has a message unambiguously associated with it.

Let $m_1, m_2, m_3, \ldots$ be the *distinct* messages associated with F's oracle queries. There are at most $q(n)$ of these, since in the worst case every query concerns a different message. I answers queries associated with m_i using transcripts stored in block $\mathcal{B}_i$. The answer to the j^{th} $S(m_i)$ query is $(\textsc{Cmt}, \textsc{Rsp})$, where $(\textsc{Cmt}, r, \textsc{Rsp})$ is the j^{th} transcript in $\mathcal{B}_i$. If $\textsc{Cmt}$ appears in any of the transcripts stored in $\mathcal{B}_i$, then the answer to $\mathcal{R}(\textsc{Cmt}, m_i)$ is r, the challenge associated with $\textsc{Cmt}$. Otherwise, $\mathcal{R}(\textsc{Cmt}, m_i)$ is answered randomly.

The k^{th} random oracle query, $\mathcal{R}(\textsc{Cmt}', m')$, is handled specially. I sends $\textsc{Cmt}'$ to V_{pub}, receives a challenge $\textsc{Ch}$ in reply and gives $\textsc{Ch}$ to F as the answer to $\mathcal{R}(\textsc{Cmt}', m')$. Let k^* denote the *true* index of the "crucial query". Observe that if $k \neq k^*$, then I's simulation of F may break down. What if F requests to see some signatures of m'? One of these could well involve $\textsc{Cmt}'$. In that case, the correct answer to $\mathcal{R}(\textsc{Cmt}', m')$ is the corresponding challenge, r, which almost certainly differs from $\textsc{Ch}$. On the other hand, if $k = k^*$ then $m' = m^*$ and $\textsc{Cmt}' = \textsc{Cmt}^*$. F won't query $\mathcal{S}$ on m^* since that is the message whose signature he is trying to forge, and I's simulation of F is perfect.

Eventually, F outputs a message m^* together with an alleged signature $\sigma^* = (\textsc{Cmt}^*, \textsc{Rsp}^*)$ of m^*. I then sends $\textsc{Rsp}^*$ to V_{pub}, who either accepts or rejects the transcript $(\textsc{Cmt}', \textsc{Ch}, \textsc{Rsp}^*)$.

Let $p_F(n)$ and $p_I(n)$ denote the success probabilities of F and I, respectively. Note that $q_{\mathcal{R}}(n) \leq q(n) \leq t_F(n) \leq n^c$ for some c, where $t_F(n)$ is the running time of F. Also observe that $p_F(n) \geq \frac{1}{n^d}$ for some d and infinitely many n, because F breaks the security of $SIG_h(ID)$ in the random oracle model.

Since I's simulation of F is perfect provided he correctly guesses the index of the "crucial query", we have:

$$\begin{aligned}
p_I(n) &= \Pr[V_{pub}(\textsc{Cmt}', \textsc{Ch}, \textsc{Rsp}^*) = 1] \\
&= \Pr[V_{pub}(\textsc{Cmt}', \textsc{Ch}, \textsc{Rsp}^*) = 1 \wedge k' = k^*] + \Pr[V_{pub}(\textsc{Cmt}', \textsc{Ch}, \textsc{Rsp}^*) = 1 \wedge k' \neq k^*] \\
&\geq \Pr[V_{pub}(\textsc{Cmt}', \textsc{Ch}, \textsc{Rsp}^*) = 1 \wedge k' = k^*] \\
&= \Pr[V_{pub}(\textsc{Cmt}', \textsc{Ch}, \textsc{Rsp}^*) = 1 | k = k^*] \cdot \Pr[k' = k^*] \\
&= p_F(n) \cdot \frac{1}{q_{\mathcal{R}}(n)} \geq \frac{p_F(n)}{n^c} \geq \frac{1}{n^{c+d}} \text{ for infinitely many } n.
\end{aligned}$$

This shows that $p_I(n)$ is non-negligible in n, so I breaks the security of ID. ■