A REMARK ON A SIGNATURE SCHEME WHERE FORGERY CAN BE PROVED

Gerrit Bleumer Birgit Pfitzmann Michael Waidner

Institut für Rechnerentwurf und Fehlertoleranz, Universität Karlsruhe
Postfach 6980, D-7500 Karlsruhe 1, F. R. Germany

I. INTRODUCTION

A new type of signature scheme, *a signature scheme where forgery by an unexpectedly powerful attacker is provable*, was suggested in [11]: if the signature of an honest participant Alice is forged, she can *prove* this forgery with arbitrarily high probability.

The possibility of proving forgeries does not depend on any unproven assumptions. The impossibility of forgery is based on the existence of pairs of claw-free permutations.

We improve this scheme for the special case that the GMR-generator for pairs of claw-free permutations is used [5]: During the set-up phase, Bob generates a pair (f_0, f_1). Alice's security depends entirely on the sufficiency of Bob's choice. Therefore, in the general case, Bob has to prove to Alice the sufficiency of his choice by a zero-knowledge proof (ZKP). We show that for the GMR-generator, this expensive ZKP can be replaced by the simple condition that the modulus chosen by Bob is odd.

In Section II, we sketch a simplified version of the signature scheme of [11]. Section III contains the necessary notations. The GMR-generator is described in Section IV. In Section V we present our result.

II. A SIMPLE SIGNATURE SCHEME WHERE FORGERY CAN BE PROVED

The signature scheme where forgery can be proved of [11] is based on the idea of LAMPORT's one-time signatures [3]:

Assume two parties, the signer Alice and the recipient of her signatures, Bob. If Alice has to sign at the most L bits, she chooses a one-way function g and $2{\bullet}L$ values $r_{i,0}, r_{i,1}, i = 1,\ldots,L$, randomly from dom($g$), the domain of g. She publishes g and the $2{\bullet}L$ images

$$g(r_{1,0})\ g(r_{1,1}) \ldots g(r_{L,0})\ g(r_{L,1}).$$

To sign the t-th bit with value $b \in \{0,1\}$, Alice sends the preimage $r_{t,b}$ of $g(r_{t,b})$ to Bob. As usual, if the forger Felix can invert g, Alice's security is lost completely.

The new idea was that in such a case Alice should be able to prove to Bob or a judge Judy that someone has inverted g [11, 10]. For this, function g has to fulfil two conditions:

i. for a fixed value $\sigma > 0$, and for each $x \in \mathrm{dom}(g)$, the value $g(x)$ has at least 2^σ preimages,
ii. g is (computationally) collision-free for Alice, i.e. it is hard for Alice to find a pair (x, y) with $g(x) = g(y)$ and $x \neq y$.

If Felix (or even Bob) forges a signature, at least for one image $g(r_{t,b})$ he computes a new preimage x. Since $r_{t,b}$ was randomly chosen from dom(g), with probability $(1\text{-}2^{-\sigma})$ the pair $(x, r_{t,b})$ is a g-collision. Each g-collision convinces Bob and Judy that condition ii. is violated, i.e. that the signature scheme is broken.

Condition i. guarantees that with high probability Alice can prove a forgery. This is called *Alice's (information theoretical) security.*

Conditon ii. guarantees that it is hard to forge signatures or proofs of forgery. Since Alice can almost always prove a forgery, her security is not influenced by forgeries. Conversely, after a proved forgery, all of Alice's signatures become invalid, i.e. Bob's security depends completely on this condition. Thus the (computational) impossibility of forgery is called *Bob's security.*

Such a function g can be constructed from each pair (f_0, f_1) of claw-free permutations (as defined in [5]): Let $D := \mathrm{dom}(f_i)$. Then define

$$g: \{0,1\}^\sigma \times D \rightarrow D$$

$$(\alpha_0, \ldots, \alpha_{\sigma\text{-}1}, x) \rightarrow f_{\alpha_0}(f_{\alpha_1}(\ldots f_{\alpha_{\sigma\text{-}1}}(x)\ldots)). \tag{1}$$

Since g hides the first argument in an unconditional way, g is called *hiding function* in [11].

Finding claws is only proved to be hard for parties who cannot observe the process of generation. Thus instead of Alice, Bob has to generate the pair for Alice.

(Please note that now nothing prevents Bob from inverting g and forging signatures, i.e. nobody but Bob can be sure that a signature was really created by Alice. Therefore, to sign a message for n recipients $\mathrm{Bob}_1, \ldots, \mathrm{Bob}_n$, Alice has to sign the message n times, each time using a different function g_i generated by Bob_i. Alice can prove a forgery by presenting collisions for each function g_i.)

Bob's security is now ensured by Bob himself.

Alice's security depends completely on condition i. Thus Bob must prove the sufficiency of his choice. In general, this can be done by an unconditionally correct zero-knowledge proof [6, 1]. In Section V, we show that for the GMR-generator this expensive proof can be omitted.

Some efficiency improvements are mentioned in [11]. Since they are all based on the function g, they all cause the same problem, thus we only mention that most of the improvements for ordinary one-time signatures described in [7, 9, 8] can be applied. The most important one is MERKLE's tree-authentication for decreasing the length of the public key. To apply this idea, a collision-free hash-function, chosen by Bob, must be used [2], and each collision of the hash-function must be accepted as a proof of forgery.

For a complete description and a formal proof of the security of the signature scheme, see [10, 1].

III. NOTATIONS

For $m \in \mathbb{N}$, $\mathbb{Z}_m$ denotes the ring of all residues modulo m, and $\mathbb{Z}_m{}^*$ the set of all residues x modulo m with $\gcd(x, m) = 1$. We use the symmetric representation for $\mathbb{Z}_m$, i.e. for odd m, we use the set $\{-(m-1)/2, \ldots, -1, 0, 1, \ldots, (m-1)/2\}$ to represent $\mathbb{Z}_m$.

$(\frac{x}{m})$ denotes the JACOBI-Symbol. QR_m denotes the set $\{x^2 \mid x \in \mathbb{Z}_m{}^*\}$ of all quadratic residues modulo m, $-\mathrm{QR}_m$ the set $\{-z \mid z \in \mathrm{QR}_m\}$.

For odd m and $x \in \mathbb{Z}_m$, define the absolute value of x by

$$|x| := \begin{cases} x & \text{if } x \in \{0,\ldots,(m-1)/2\} \\ -x & \text{if } x \in \{-1,\ldots,-(m-1)/2\} \end{cases}$$

For a set M, the symbol $|M|$ denotes the cardinality of M.

IV. THE GMR-GENERATOR FOR PAIRS OF CLAW-FREE PERMUTATIONS

Let $k \in \mathbb{N}$ be the security parameter for the GMR-generator. On input k, the generator randomly selects a number m from the set

$$H_k := \{p \cdot q \mid p, q \text{ prime} \wedge \lfloor \log_2(p) \rfloor = \lfloor \log_2(q) \rfloor = k - 1 \wedge p \equiv 3 \bmod 8 \wedge q \equiv 7 \bmod 8\}$$

of BLUM-integers of length $2 \cdot k$ or $2 \cdot k - 1$.

The functions $f_i \colon D \rightarrow D$ are then defined by

$$f_0(x) := |x^2|$$
$$f_1(x) := |4 \cdot x^2|.$$

Their common domain D is given by

$$D := \{\, x \mid x \in \mathbb{Z}_m{}^* \wedge (\tfrac{x}{m}) = 1 \wedge x \in \{1,\ldots,\tfrac{m-1}{2}\}\}. \qquad (2)$$

Both functions are permutations of D. Finding a claw, i.e. a triple (x_0, x_1, z) with $z = f_0(x_0) = f_1(x_1)$, is as hard as factoring m [5].

In this case, the hiding function $g \colon \{0,1\}^\sigma \times D \rightarrow D$ defined in (1) can be described by

$$g(\alpha, x) = |4^\alpha \cdot x^{2^\sigma}|,$$

where $\alpha = (\alpha_0, \ldots, \alpha_{\sigma-1})$ is interpreted as the integer $\alpha_{\sigma-1} \cdot 2^{\sigma-1} + \ldots + \alpha_1 \cdot 2 + \alpha_0$ (similar to [4], proof by induction on σ).

Finding a g-collision, i.e. a pair $((\alpha, x), (\beta, y))$ with $g(\alpha, x) = g(\beta, y)$ and $(\alpha, x) \neq (\beta, y)$, is as hard as finding a claw.

V. NUMBER OF PREIMAGES OF g

To guarantee that Alice can prove each forgery with probability at least $(1\text{-}2^{-\sigma})$, each $z \in \mathrm{im}(g)$, the image of g, must have at least 2^{σ} preimages.

If (f_0, f_1) are permutations of D, e.g. because Bob is honest and uses the GMR-generator, this is satisfied since then the functions $g(\alpha,\bullet)$, $\alpha \in \{0,1\}^{\sigma}$, are permutations of D, too. Thus for each value $z \in D$ and each $\alpha \in \{0,1\}^{\sigma}$, there is exactly one x with $g(\alpha, x) = z$. Thus $|g^{-1}(z)| = 2^{\sigma}$.

In the following, we show that to be convinced of condition i, Alice just has to check that m is odd.

For general odd m, instead of using the domain D defined in (2), we use the domain

$$E := \{\, |x^2| \mid x \in \mathbb{Z}_m^{\,*} \,\},$$

from which it is also easy to choose a random element.

Lemma 1. If $m \in H_k$, the domains D and E are equal.

Proof. Let $m = p \bullet q$, where $p \equiv q \equiv 3 \pmod 4$. Hence $(\frac{-1}{m}) = (\frac{-1}{p}) \bullet (\frac{-1}{q}) = (-1) \bullet (-1) = +1$.

$E \subseteq D$: Assume $y := |x^2(\mathrm{mod}\ m)| \in E$. From $(\frac{-1}{m}) = (\frac{x^2}{m}) = 1$, it follows that $(\frac{|x^2|}{m}) = 1$.

Since $|x^2| \in \{1,\ldots,\frac{m-1}{2}\}$ by definition, we have $y \in D$.

$D \subseteq E$: Assume $y \in D$, i.e. $(\frac{y}{m}) = 1$, $y \in \{1,\ldots,\frac{m-1}{2}\}$.

If $y \in \mathrm{QR}_m$ then there is an x such that $y = x^2 = |x^2| \pmod m$.

Otherwise $(\frac{-y}{p}) = (\frac{-y}{q}) = -1$ holds. In this case there is an x such that $y = -x^2 = |x^2|$ (mod m),

because $(\frac{-y}{p}) = (\frac{-y}{q}) = (\frac{-1}{p}) \bullet (\frac{y}{p}) = (\frac{-1}{q}) \bullet (\frac{y}{q}) = (-1)^2 = 1$ which means $-y \in \mathrm{QR}_m$. □

Lemma 1 says that nothing is changed if Bob is honest, thus Bob's security is not influenced. We only need to consider Alice's security.

Lemma 2. If m is an arbitrary odd integer, then for all $z \in E$, $|g^{-1}(z)| \geq 2^{\sigma}$.

Proof. The proof is in four steps. Each one can be proved by basic algebraic calculations omitted here for shortness.

1st step. The sets $\{+1,-1\}$ and $\mathrm{QR}_m \cup \text{-}\mathrm{QR}_m$ are subgroups of $(\mathbb{Z}_m^{\,*},\bullet)$. Consider the quotient group $G := (\mathrm{QR}_m \cup \text{-}\mathrm{QR}_m) / \{+1, -1\}$.

Set E is a representation system of G, the element $\pm x^2 \bullet \{+1,-1\} \in G$ is represented by $|x^2| \in E$. Multiplication in E is defined by $|x| \bullet |y| := |x \bullet y|$.

2nd step. For all $\alpha, \beta \in \{0,1\}^{\sigma}$ and $x, y \in G$, let

$$(\alpha, x) * (\beta, y) := (\alpha + \beta \bmod 2^{\sigma}, |x \bullet y \ \bullet 4^{(\alpha+\beta)\,\mathrm{div}\,2^{\sigma}}|)$$

Then $(\{0,1\}^{\sigma} \times G\ , *)$ is an ABELian group.

3rd step. Function g is a group-homomorphism from $(\{0,1\}^{\sigma} \times G\ , *)$ into G.

Proof: For all $\alpha, \beta \in \{0,1\}^\sigma$ and $x, y \in E$

$$\begin{aligned}
g((\alpha, x) * g(\beta, y)) &= g(\alpha + \beta \bmod 2^\sigma, |x \bullet y \bullet 4^{(\alpha+\beta)\operatorname{div} 2^\sigma}|) \\
&= |4^{\alpha+\beta \bmod 2^\sigma} \bullet (x \bullet y \bullet 4^{(\alpha+\beta)\operatorname{div} 2^\sigma})^{2^\sigma}| \\
&= |4^{\alpha+\beta \bmod 2^\sigma + 2^\sigma \bullet ((\alpha+\beta)\operatorname{div} 2^\sigma)} \bullet (x \bullet y)^{2^\sigma}| \\
&= |4^{\alpha+\beta} \bullet (x \bullet y)^{2^\sigma}| \\
&= ||4^\alpha \bullet x^{2^\sigma}| \bullet |4^\beta \bullet y^{2^\sigma}|| \\
&= |g(\alpha, x) \bullet g(\beta, y)|
\end{aligned}$$

4th step. Since g is a group-homomorphism, each $z \in \operatorname{im}(g) \subseteq G$ has the same number of preimages. Thus

$$|g^{-1}(z)| = \frac{|\{0,1\}^\sigma \times G|}{|\operatorname{im}(g)|} = 2^\sigma \bullet \frac{|G|}{|\operatorname{im}(g)|} \geq 2^\sigma. \qquad \square$$

VI. SUMMARY

If the signature scheme where forgery can be proved of [11] is implemented using the claw-free permutation-pairs of [5], the signer Alice just needs to check whether the modulus m chosen by the recipient Bob is odd. The zero-knowledge proof used in [11] to convince Alice that Bob has generated a suitable m can be omitted.

REFERENCES

[1] Gerrit Bleumer: Vertrauenswürdige Schlüssel für ein Signatursystem, dessen Brechen beweisbar ist; Studienarbeit, Universität Karlsruhe 1990 (in preparation).

[2] Ivan Bjerre Damgård: Collision free hash functions and public key signature schemes; Eurocrypt '87, LNCS 304, Springer-Verlag, Berlin 1988, 203-216.

[3] Whitfield Diffie, Martin E. Hellman: New Directions in Cryptography; IEEE Transactions on Information Theory 22/6 (1976) 644-654.

[4] Oded Goldreich: Two Remarks Concerning the Goldwasser-Micali-Rivest Signature Scheme; Crypto '86, LNCS 263, Springer-Verlag, Berlin 1987, 104-110.

[5] Shafi Goldwasser, Silvio Micali, Ronald L. Rivest: A Digital Signature Scheme Secure Against Adaptive Chosen-Message Attacks; SIAM J. Comput. 17/2 (1988) 281-308.

[6] Oded Goldreich, Silvio Micali, Avi Wigderson: Proofs that Yield Nothing But their Validity and a Methodology of Cryptographic Protocol Design; 27th FOCS, IEEE 1986, 174-187.

[7] Ralph C. Merkle: Protocols for Public Key Cryptosystems; Symposium on Security and Privacy, Oakland 1980, 122-134.

[8] Ralph C. Merkle: A digital signature based on a conventional encryption function; Crypto '87, LNCS 293, Springer-Verlag, Berlin 1988, 369-378.

[9] Ralph C. Merkle: Secrecy, authentication, and public key systems; UMI Research Press 1982.

[10] Birgit Pfitzmann: Für den Unterzeichner sichere digitale Signaturen und ihre Anwendung; Diplomarbeit, Universität Karlsruhe 1989.

[11] Michael Waidner, Birgit Pfitzmann: The Dining Cryptographers in the Disco: Unconditional Sender and Recipient Untraceability with Computationally Secure Serviceability; Universität Karlsruhe 1989; presented at Eurocrypt '89.