Nonce-Misuse Resistant Signatures

Laurane Marco

EPFL

In this report, we give an overview of the literature on misuse resistance, focusing on digital signatures. We first define this notion in the context of symmetric cryptography, as it was originally introduced and then focus to its later applications in public-key cryptography on digital signatures.

1 The implications of nonce-misuse

In cryptography, "nonce" stands for "number only used once". It is therefore natural to wonder what happens when that one-time use property isn't respected. It can happen as a result of a bad implementation or a bad randomness generator, when a counter eventually repeats, as a result of random sampling, or as a deliberate ignorance of the protocol's specification. We briefly describe the implications of nonce-misuse in the context of symmetric cryptography and then in that of public-key cryptography focusing on signatures.
In symmetric cryptography, some modes of operations require an IV, and in certain cases it is crucial that it shouldn't be re-used. This is the case, for the OFB, CTR and GCM modes in particular. In OFB and CTR mode, reusing an IV has the same implication as reusing a key in a Vernam cipher, since their construction is similar. This means that it will leak some information about the plaintexts, and it can be especially bad if those have low entropy. However, the problem is limited to the two sent messages. In GCM mode, reusing a nonce directly allows for a universal forgery. Hence, it affects the entire forthcoming communication.
In the context of public key cryptography, nonces are also essential for security. In particular, DSA-type signatures' security, such as DSA and ECDSA signatures heavily relies on the fact that the nonce is never re-used. Indeed, using the same nonce for two signatures under the same key-pair allows a total break by recovering the secret key solving only a linear equation. This has led to several attacks in practice, e.g. on Sony PS3 ([4]) or on Bitcoin wallets for Android devices ([7]).

2 Misuse Resistance in Symmetric Cryptography

The notion of misuse-resistance comes from symmetric cryptography. It was first introduced in the context of authenticated encryption by Rogaway and Shrimpton ([10]). They define the notion of misuse resistant authenticated encryption (MRAE) in the following way :

Definition 1 (Misuse resistant Authenticated Encryption [10]). *Let* $\Pi = (\mathcal{K}, \mathsf{Enc}, \mathsf{Dec})$ *be an IV-based encryption scheme that can handle an associated header* hd *and let* $\mathcal{A}$ *be an adversary. Then, the* MRAE-advantage *of* $\mathcal{A}$ *is*

$$\mathrm{Adv}^{\mathsf{MRAE}}_{\Pi}(\mathcal{A}) = \Pr[\mathsf{MRAE}_1(\mathcal{A}) \to 1] - \Pr[\mathsf{MRAE}_0(\mathcal{A}) \to 1]$$

where the $\mathsf{MRAE}_b, b = 0, 1$ *game is defined in Figure 1.*

MRAE_b		$\mathsf{OEnc}(hd, IV, X)$	
1 :	$K \leftarrow\$\, \mathcal{K}$	1 :	**if** $(hd, IV, X) \in$ Used :
2 :	Used $\leftarrow \emptyset$	2 :	**return** $\perp$
3 :	Encrypted $\leftarrow \emptyset$	3 :	Used $\leftarrow$ Used $\cup \{(hd, IV, X)\}$
4 :	$\mathcal{A}^{\mathsf{OEnc},\mathsf{ODec}} \to z$	4 :	**if** $b = 0$:
5 :	**return** z	5 :	$ct \leftarrow\$\, \{0,1\}^{n+\lvert X\rvert}$
		6 :	**else** :
		7 :	$ct \leftarrow \mathsf{Enc}(hd, IV, X)$
		8 :	Encrypted $\leftarrow$ Encrypted $\cup \{(hd, IV, ct)\}$
		9 :	**return** ct
		10 :	
		$\mathsf{ODec}(hd, IV, Y)$	
		1 :	**if** $(hd, IV, Y) \in$ Encrypted or $b = 0$
		2 :	**return** $\perp$
		3 :	**else**
		4 :	**return** $\mathsf{Dec}(hd, IV, Y)$

Fig. 1: The MRAE_b security game for authenticated encryption.

The difference with respect to traditional security is that usually the adversary is not allowed to repeat an IV to an encryption/random query whereas in this definition it can. In OEnc, n is the overhead of the AE scheme, arising from the header.
Furthermore, they show how to construct a misuse resistant-AE scheme from a vector-input pseudo-random function (which is easily constructed from a regular string-input PRF) and an IND$-secure encryption scheme.

In [1], Bellare and Keelveedhi distinguish two notions of MRAE. In the first one, let us call it MRAE1 they allow the nonce not to be random, but still require it to be unique. In the second one, MRAE2, they do not make any assumption on the nonce, i.e. the adversary can provide any nonce it feels like. They show that these two security notions can't be achieved in general for

key dependent message-encryption (KDM). They propose a generic transform **R**andomized**H**ash**t**hen**E**ncrypt (RHtE), that takes as input a symmetric encryption scheme, a key generation algorithm and an integer, and returns a scheme that is random-nonce secure for key dependent messages and key-independent header if the base scheme is (one-time) secure for key independent header and messages.

They show security under MRAE1 and MRAE2 under some restriction for KDM encryption namely output unpredictability and collision resistance.

The concept of misuse resistance has also been extended to other constructions like MACs.

In [8], they provide an efficient nonce-based MAC that provides security up to the birthday bound in case of nonce misuse (i.e. nonce repetition), and past that bound if nonces aren't reused. Their construction uses a Wegman-Carter hash function H_{K_h} together with an encrypted Davies-Meyer construction in the following way :

$$E_{K'}(E_K(N) \oplus N \oplus H_{K_h}(M))$$

3 Misuse-resistant signatures ([3])

As explained in 1, bad randomness in signatures can lead to disastrous consequences. A generic way to eliminate randomness in signing is introduced in [9]. Consider a pseudo-random function F, and a digital signature scheme Σ, then Figure 2 gives the transform to make it deterministic.

$\mathsf{DeterministicKeyGen}(\lambda)$	$\mathsf{DeterministicSign}(\mathsf{sk}', m)$
1 : $(\mathsf{sk}, \mathsf{pk}) \leftarrow \mathsf{KeyGen}_\Sigma(\lambda)$	1 : $(\mathsf{sk}, \mathsf{fk}) \leftarrow \mathsf{sk}'$
2 : $\mathsf{fk} \leftarrow \mathsf{KeyGen}_F(\lambda)$	2 : $r \leftarrow F(\mathsf{fk}, m)$
3 : $\mathsf{sk}' \leftarrow (\mathsf{sk}, \mathsf{fk})$	3 : $\sigma \leftarrow \mathsf{Sign}_\Sigma(\mathsf{sk}, m; r)$
4 : **return** $(\mathsf{sk}', \mathsf{pk})$	4 : **return** σ

Fig. 2: A transform for deterministic signing [9]

The verification is unchanged.
Given that F is a PRF and Σ is EUF-CMA, then this new scheme remains EUF-CMA. However, the secret key is changed which we might want to avoid in some applications.
Another way to achieve deterministic signatures without changing the secret key is to obtain the coins r by applying a random oracle to sk and m. Security of this transform was proven in [2] for any EUF-CMA scheme.
It is used in the Ed25519 signature scheme [6], which is a specific instance of the EdDSA (Edwards-curve Digital Signature Algorithm) applied to the curve Curve25519 [5].

We describe the EdDSA signature scheme in Figure 3. It takes as parameters a field $\mathbb{F}_q$ for a prime power q, an elliptic curve $E/\mathbb{F}_q$ such that $\#E(\mathbb{F}_q) = 2^c \cdot \ell$ for a large prime ℓ, a point B of order ℓ on the curve and a hash function H with a $2b$-bits output such that $2^{b-1} > q$. We use the following notation : $H_{i,\dots j}(.)$, $i < j$ denotes an integer represented by bits from i to j of $H(.)$ (See [6] for details of the representation).

$\mathsf{KeyGen}(\lambda)$

1 : $k \leftarrow\$ \{0,1\}^b$
2 : $\mathsf{sk} \leftarrow H_{0,\dots,b-1}(k)$
3 : $\mathsf{pk} \leftarrow \mathsf{sk} \cdot B$
4 : **return** $(\mathsf{sk}, \mathsf{pk})$

$\mathsf{Sign}(\mathsf{sk}, m)$

1 : $r \leftarrow H(H_{b,\dots,2b-1}(k)||M)$
2 : $R \leftarrow r \cdot B$
3 : $S \leftarrow r + H(R||\mathsf{pk}||m)s \mod \ell$
4 : $\sigma \leftarrow (R, S)$
5 : **return** σ

$\mathsf{Verify}(\sigma, \mathsf{pk}, m)$

1 : **return** $2^c SB = 2^c R + 2^c H(R||\mathsf{pk}||M)\mathsf{pk}$

Fig. 3: The EdDSA signature scheme.

In [3], Bellare and Tackmann define the concept of *nonce-based signatures*, in which the signer possesses both a secret key and a seed. The signing process uses both these and a nonce and is deterministic. If the key and seed are kept private (MR1), this provides the same level of security as deterministic signatures. However, if the seed is compromised (MR2), the additional security property is that security is also preserved as long as nonces are unpredictable. A formal definition of nonce based signatures is given in Definition 2

Definition 2 (Nonce-based signatures). *A nonce-based signature scheme* NDS *with message space* $\mathcal{M}$*, nonce space* $\mathcal{N}$ *consists of three polynomial time algorithm* $(\mathsf{KeyGen}_{\mathsf{NDS}}, \mathsf{Sign}_{\mathsf{NDS}}, \mathsf{Verify}_{\mathsf{NDS}})$ *defined in the following way :*

– $(\mathsf{sk}, \mathsf{pk}, \mathsf{xk}) \leftarrow\$ \mathsf{KeyGen}_{\mathsf{NDS}}(\lambda)$ *: It is a probabilistic algorithm that takes as input the security parameter* λ*, and outputs a secret key* sk*, a public key* pk *and a seed* xk*.*

– $\sigma \leftarrow \mathsf{Sign}_{\mathsf{NDS}}(\mathsf{sk}, \mathsf{xk}, m, n)$*: It is a deterministic algorithm that takes as input the secret key* sk*, the seed* xk*, the message to be signed* $m \in \mathcal{M}$ *and a nonce* $n \in \mathcal{M}$*.*
– $0/1 \leftarrow \mathsf{Verify}(\sigma, \mathsf{pk}, m)$*: It is a deterministic algorithm that takes as input the signature* σ*, the public key* pk*, and the message* m *and returns* 1 *if the signature is valid and 0 otherwise.*

The security of a nonce-based signature scheme is captured by the following games :

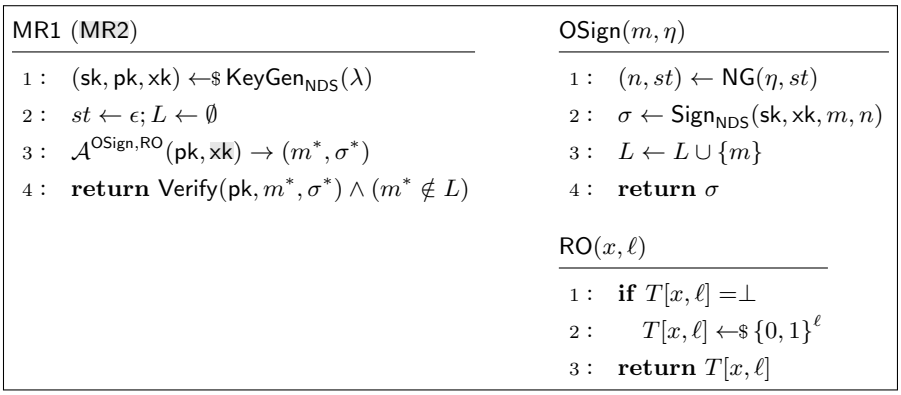

Fig. 4: The MR1 and MR2 (in grey) security games for nonce-based signature security [3]. (NG stands for Nonce Generator)

Furthermore, they show how to instantiate a nonce-based signature scheme by giving a transform R2NDS that takes as input a digital signature scheme σ, and a hedged extractor HE and returns a nonce-based signature scheme.

Definition 3 (Hedged extractor [3]). *A hedged extractor* HE *takes as input a seed* xk*, a message* m *and a nonce* n *and deterministically returns a string* $r = \mathsf{HE}(\mathsf{xk}, (m, n))$*. It has two properties :*

1. *It is a pseudo-random function (PRF).*
2. *It is an extractor.*

The PRF property ensures that if xk is random and hidden the output looks random to an adversary. The extractor property ensure that if xk is random but leaked then r looks random if (m, n) is unpredictable. We call the latter RoR security.

Given such a hedge extractor HE and a digital signature scheme Σ then the $\mathsf{R2NDS}(\Sigma, \mathsf{HE})$ transform is quite simple :

$\mathsf{KeyGen}_{\mathsf{R2NDS}}(\lambda)$	$\mathsf{Sign}_{\mathsf{R2NDS}}(\mathsf{sk}', m)$
1 : $\mathsf{xk} \leftarrow \mathsf{KeyGen}_{\mathsf{HE}}(\lambda)$	1 : $r \leftarrow \mathsf{HE}^{\mathsf{RO}}(\mathsf{xk}, (m, n))$
2 : $(\mathsf{sk}, \mathsf{pk}) \leftarrow \mathsf{KeyGen}_{\Sigma}(\lambda)$	2 : $\sigma \leftarrow \mathsf{Sign}_{\sigma}(\mathsf{sk}, m; r)$
3 : $\mathsf{sk}' \leftarrow (\mathsf{sk}, \mathsf{xk})$	3 : **return** σ
4 : **return** $\mathsf{sk}', \mathsf{pk}$	

They show that in the random oracle model the transform is MR1 secure if Σ is unforgeable and HE is a pseudo random function. They show MR2 security, still in the random oracle model, under the additional assumption of RoR security of HE.

4 Conclusion

We gave an introduction to the concept of misuse resistance and its consequences in Section 1. We formally define it, as it was originally introduced, in the context of symmetric cryptography in Section 2. We explain how this concept extends to public key cryptography and signatures in particular in Section 3. Nonce-misuse can have disastrous consequences for signatures since they lead to a total break of the scheme, but we show that cheap and practical solutions exist to address this issue.

References

1. Bellare, M., Keelveedhi, S.: Authenticated and misuse-resistant encryption of key-dependent data. In: Rogaway, P. (ed.) Advances in Cryptology – CRYPTO 2011. pp. 610–629. Springer Berlin Heidelberg, Berlin, Heidelberg (2011)
2. Bellare, M., Poettering, B., Stebila, D.: From identification to signatures, tightly: A framework and generic transforms. In: Cheon, J.H., Takagi, T. (eds.) Advances in Cryptology – ASIACRYPT 2016. pp. 435–464. Springer Berlin Heidelberg, Berlin, Heidelberg (2016)
3. Bellare, M., Tackmann, B.: Nonce-based cryptography: Retaining security when randomness fails. In: Fischlin, M., Coron, J.S. (eds.) Advances in Cryptology – EUROCRYPT 2016. pp. 729–757. Springer Berlin Heidelberg, Berlin, Heidelberg (2016)
4. Bendel, M.: Hackers describe ps3 security as epic fail, gain unrestricted access (2010), `https://www.exophase.com/20540/hackers-describe-ps3-security-as-epic-fail-gain-unrestricted-access/`
5. Bernstein, D.J.: Curve25519: New diffie-hellman speed records. In: Yung, M., Dodis, Y., Kiayias, A., Malkin, T. (eds.) Public Key Cryptography - PKC 2006. pp. 207–228. Springer Berlin Heidelberg, Berlin, Heidelberg (2006)
6. Bernstein, D.J., Duif, N., Lange, T., Schwabe, P., Yang, B.Y.: High-speed high-security signatures. In: Preneel, B., Takagi, T. (eds.) Cryptographic Hardware and Embedded Systems – CHES 2011. pp. 124–142. Springer Berlin Heidelberg, Berlin, Heidelberg (2011)
7. Bitcoin.org: Android security vulnerability (2013), `https://bitcoin.org/en/alert/2013-08-11-android`

8. Cogliati, B., Seurin, Y.: Ewcdm: An efficient, beyond-birthday secure, nonce-misuse resistant mac. In: Robshaw, M., Katz, J. (eds.) Advances in Cryptology – CRYPTO 2016. pp. 121–149. Springer Berlin Heidelberg, Berlin, Heidelberg (2016)
9. M'Raïhi, D., Naccache, D., Pointcheval, D., Vaudenay, S.: Computational alternatives to random number generators. In: Tavares, S., Meijer, H. (eds.) Selected Areas in Cryptography. pp. 72–80. Springer Berlin Heidelberg, Berlin, Heidelberg (1999)
10. Rogaway, P., Shrimpton, T.: A provable-security treatment of the key-wrap problem. In: Vaudenay, S. (ed.) Advances in Cryptology - EUROCRYPT 2006. pp. 373–390. Springer Berlin Heidelberg, Berlin, Heidelberg (2006)