UNIVERSITÀ POLITECNICA DELLE MARCHE

DII Dipartimento di Ingegneria dell'Informazione

Clearing Fuzzy Signatures: a Proof of Work Blockchain Protocol for Biometric Identification

Paolo Santini, Giulia Rafaiani, Massimo Battaglioni, Franco Chiaraluce
Marco Baldi
Dipartimento di Ingegneria dell'Informazione
Università Politecnica delle Marche

5th Distributed Ledger Technology Workshop (DLT 2023) Thursday 25th May 2023

Introduction

- Extracting secrets from a physical source is often tricky, since the source can be noisy
- For authentication purposes, different readings of the same secret will be *close*, but still not identical, one to each other
- When data from fuzzy sources are used as the secret key for multiple digital signatures, the resulting signatures will fail verification with the originally enrolled public key, if some techniques to reduce noise are not employed

Aim of the work

- As for authentication, an increasing trend is that of relying on decentralization
- Existing fuzzy authentication schemes are not directly linked to the problem of reconciling with a stored template and use noise-reduction techniques, like error-correcting codes

Aim of the work

- As for authentication, an increasing trend is that of relying on decentralization
- Existing fuzzy authentication schemes are not directly linked to the problem of reconciling with a stored template and use noise-reduction techniques, like error-correcting codes

- *Our aim is to create a decentralized fuzzy system for authentication purposes fully leveraging blockchain technology*

System features

- Users are simply required to *digitally sign* some random message using fuzzy keys

System features

- Users are simply required to *digitally sign* some random message using fuzzy keys
- The system will *not* use noise-reducing techniques

System features

- Users are simply required to *digitally sign* some random message using fuzzy keys
- The system will *not* use noise-reducing techniques
- The blockchain will be actively part of the noise removal, providing the basis for a special instance of Proof of Work in which the mining process corresponds to the de-noising process

System features

- Users are simply required to *digitally sign* some random message using fuzzy keys
- The system will *not* use noise-reducing techniques
- The blockchain will be actively part of the noise removal, providing the basis for a special instance of Proof of Work in which the mining process corresponds to the de-noising process
- We consider classic RSA digital signatures, showing that fuzziness in the secret key translates into some noise affecting the derived signatures

Fuzzy Signature Scheme

- sk is sampled from the discrete distribution $\mathcal{D}$ of the fuzzy source

Fuzzy Signature Scheme

- sk is sampled from the discrete distribution $\mathcal{D}$ of the fuzzy source
  - $\mathrm{KeyGen}_{\mathcal{D}}()$: sample $\mathrm{sk} \leftarrow \mathcal{D}$, then compute the corresponding public key $\mathrm{pk} \in \mathcal{P}$;

Fuzzy Signature Scheme

- sk is sampled from the discrete distribution $\mathcal{D}$ of the fuzzy source
  - $\mathrm{KeyGen}_{\mathcal{D}}()$: sample $\mathrm{sk} \leftarrow \mathcal{D}$, then compute the corresponding public key $\mathrm{pk} \in \mathcal{P}$;
  - $\mathrm{Sign}_{\mathcal{D}}(m)$: on input a message $m \in \mathcal{M}$, sample $\mathrm{sk} \leftarrow \mathcal{D}$, then run $\mathrm{Sign}(m, \mathrm{sk})$ on input the sampled sk

Fuzzy Signature Scheme

- sk is sampled from the discrete distribution $\mathcal{D}$ of the fuzzy source
  - $\mathrm{KeyGen}_{\mathcal{D}}()$: sample $\mathrm{sk} \leftarrow \mathcal{D}$, then compute the corresponding public key $\mathrm{pk} \in \mathcal{P}$;
  - $\mathrm{Sign}_{\mathcal{D}}(m)$: on input a message $m \in \mathcal{M}$, sample $\mathrm{sk} \leftarrow \mathcal{D}$, then run $\mathrm{Sign}(m, \mathrm{sk})$ on input the sampled sk
- The input secret key is another sample sk' from the same fuzzy distribution. When sk and sk' are close, *the associated signatures are also similar*, according to some distance metric

Signature Clearing

- Let $\mathrm{dist} : \mathcal{S} \times \mathcal{S} \longmapsto \mathbb{R}_+$ be a distance function for which there exists some $\theta \in \mathbb{R}_+$ such that, for every pair of signatures σ, σ' on the same message m, computed respectively with keys $\mathrm{sk}, \mathrm{sk}'$ it holds that $\mathrm{dist}(\sigma, \sigma') \leq \theta$

Signature Clearing

- Let $\mathrm{dist} : \mathcal{S} \times \mathcal{S} \longmapsto \mathbb{R}_+$ be a distance function for which there exists some $\theta \in \mathbb{R}_+$ such that, for every pair of signatures σ, σ' on the same message m, computed respectively with keys $\mathrm{sk}, \mathrm{sk}'$ it holds that $\mathrm{dist}(\sigma, \sigma') \leq \theta$
- Then, we call ClearSignature an algorithm that, on input a triplet (m, σ, pk), returns a signature $\sigma' \in \mathcal{S}$ such that $\mathrm{dist}(\sigma, \sigma') \leq \theta$ and $\mathrm{Verify}(m, \sigma', \mathrm{pk})$ = True

RSA Clear Signature

- Let p_i and q_i be two primes, and $n_i = p_i\, q_i$. We define $\mathcal{D}_{\mathcal{S}_i}$ as the distribution that returns samples of the form $x \equiv \hat{x}_i + e \bmod n_i$, where e is uniformly distributed over $[-w; w]$

RSA.ClearSign$\big(m, s, (n, \delta)\big)$:

1) compute $c = \mathsf{Hash}(m)$;
2) compute $y \equiv s^{\delta} \mod n$;
3) sample $\Delta e \xleftarrow{\$} [-2w; 2w]$;
4) compute $\widehat{c} \equiv y c^{-\delta \Delta e} \mod n$;
5) return Δe if $\widehat{c} = c$, else restart from Step 3.

System procedure

Distributed Network		Source $\mathcal{S}_i$
		Enter string $\mathcal{S}_i$
	$\xleftarrow{\quad \mathcal{S}_i \quad}$	
Recover n_i from $\mathcal{L}$		
	$\xrightarrow{\quad n_i \quad}$	
		Set $m = (\mathcal{S}_i \| \texttt{Context})$
		Compute $s = \mathsf{Sign}_{\mathscr{D}_i}(m)$
	$\xleftarrow{\texttt{RawTx} = (m, s)}$	
Run $\mathsf{RSA.ClearSign}(m, s, \mathsf{pk}_i)$		
If $\Delta e \in [-2w; 2w]$ is found:		
Set $\texttt{MinedTx} = (m, s, \Delta e)$		

Modified RSA Clear Signature

- If users collude, malicious miners can skip the clearing process (since they know the secret keys and, so, Δe) and produce blocks faster than honest miners, which execute RSA.ClearSign

Modified RSA Clear Signature

- If users collude, malicious miners can skip the clearing process (since they know the secret keys and, so, Δe) and produce blocks faster than honest miners, which execute RSA.ClearSign

$\mathsf{RSA.ClearSign}^{(\mathsf{PRNG})}(m, \mathtt{aux}, s, (n, \delta))$:

1) compute $c = \mathsf{Hash}(m)$;
2) compute $y \equiv s^{\delta} \mod n$;
3) sample $\mathtt{seed} \xleftarrow{\$} \mathcal{R}$;
4) compute $\Delta e = \mathsf{PRNG}(m || \mathtt{seed} || \mathtt{aux})$;
5) compute $\widehat{c} \equiv y c^{-\Delta e} \mod n$;
6) return $\mathtt{seed}$ if $\widehat{c} = c$, else restart from Step 3.

Byzantine Fault Tolerance

- If all malicious miners $\widetilde{M}$ know in advance the value of Δe, but do not know its pre-image seed, all works until

$$\frac{(4w+1)t_{\mathrm{PRNG}}}{\widetilde{M}} > \frac{(4w+1)(t_{\mathrm{PRNG}}+t_{\mathrm{RSA}})}{M-\widetilde{M}}$$

Byzantine Fault Tolerance

- If all malicious miners $\widetilde{M}$ know in advance the value of Δe, but do not know its pre-image seed, all works until

$$\frac{(4w+1)t_{\text{PRNG}}}{\widetilde{M}} > \frac{(4w+1)(t_{\text{PRNG}}+t_{\text{RSA}})}{M-\widetilde{M}}$$

$$\widetilde{M} < \mathrm{M} \cdot \frac{t_{\text{PRNG}}}{2t_{\text{PRNG}}+t_{\text{RSA}}} = M \cdot \frac{1}{2+\frac{t_{\text{RSA}}}{t_{\text{PRNG}}}}$$

Byzantine Fault Tolerance

- If all malicious miners $\widetilde{M}$ know in advance the value of Δe, but do not know its pre-image seed, all works until

$$\frac{(4w+1)t_{\text{PRNG}}}{\widetilde{M}} > \frac{(4w+1)(t_{\text{PRNG}}+t_{\text{RSA}})}{M-\widetilde{M}}$$

$$\widetilde{M} < \mathrm{M} \cdot \frac{t_{\text{PRNG}}}{2t_{\text{PRNG}}+t_{\text{RSA}}} = M \cdot \frac{1}{2+\frac{t_{\text{RSA}}}{t_{\text{PRNG}}}}$$

- *PRNG cannot be much more efficient than RSA*

Conclusion

- The authentication process is delegated to a distributed network and executes the task of removing noise from fuzzy signatures

Conclusion

- The authentication process is delegated to a distributed network and executes the task of removing noise from fuzzy signatures
- The design of an ad-hoc PRNG leads to BFT $\sim \frac{\tilde{M}}{M} \approx \frac{1}{2+{}^{1}/_{X}}$

Conclusion

- The authentication process is delegated to a distributed network and executes the task of removing noise from fuzzy signatures
- The design of an ad-hoc PRNG leads to BFT $\sim \frac{\tilde{M}}{M} \approx \frac{1}{2+{}^{1}/_{X}}$
- Mining and verification times grow respectively as $O\left(\frac{X+1}{M}\right)$ and $O(X)$

Conclusion

- The authentication process is delegated to a distributed network and executes the task of removing noise from fuzzy signatures
- The design of an ad-hoc PRNG leads to BFT $\sim \frac{\widetilde{M}}{M} \approx \frac{1}{2+{}^{1}/_{X}}$
- Mining and verification times grow respectively as $\mathrm{O}\left(\frac{X+1}{M}\right)$ and $\mathrm{O}(X)$
- Security analysis and application to RSA signature scheme show the feasibility of the approach

UNIVERSITÀ
POLITECNICA
DELLE MARCHE

DII
Dipartimento di Ingegneria
dell'Informazione

Thanks for your kind attention!

g.rafaiani@univpm.it