Schnorr Signatures are Tightly Secure in the ROM under a Non-Interactive Assumption

Gavin Cho (UMass Amherst)
Georg Fuchsbauer (TU Wien)
Adam O'Neill (UMass Amherst)
Marek Sefranek (TU Wien)

https://ia.cr/2024/1528

Motivation

- Provable security: break security of scheme $\Pi \implies$ solve problem P

Motivation

- Provable security: break security of scheme $\Pi \Longrightarrow$ solve problem P
- Reduction: for every efficient adversary A that breaks Π with probability ϵ_A, there is efficient adversary B that solves P with probability ϵ_B

TU WIEN CYSEC CYBERSECURITYCENTER S&P Security & Privacy

Motivation

- Provable security: break security of scheme $\Pi \implies$ solve problem P
- Reduction: for every efficient adversary A that breaks Π with probability ϵ_A, there is efficient adversary B that solves P with probability ϵ_B
- Tight reduction: $\epsilon_A \approx \epsilon_B$ (importance recognized since [BR93, BR94, BR96…])

TU WIEN CYSEC CYBERSECURITYCENTER S&P Security & Privacy

Motivation

- Provable security: break security of scheme $\Pi \implies$ solve problem P
- Reduction: for every efficient adversary A that breaks Π with probability ϵ_A, there is efficient adversary B that solves P with probability ϵ_B
- Tight reduction: $\epsilon_A \approx \epsilon_B$ (importance recognized since [BR93, BR94, BR96…])
- Hardness of problem P then determines parameters (e.g. key length) for instantiating scheme Π in real world

Motivation

- Provable security: break security of scheme $\Pi \implies$ solve problem P
- Reduction: for every efficient adversary A that breaks Π with probability ϵ_A, there is efficient adversary B that solves P with probability ϵ_B
- Tight reduction: $\epsilon_A \approx \epsilon_B$ (importance recognized since [BR93, BR94, BR96…])
- Hardness of problem P then determines parameters (e.g. key length) for instantiating scheme Π in real world
- Unfortunately, for many schemes we only have loose reductions (i.e., adversary B needs to spend much more effort than adversary A)

Our Focus: Schnorr Signatures [Sch90]

Our Focus: Schnorr Signatures [Sch90]

- One of the most widely deployed pieces of cryptography today

Our Focus: Schnorr Signatures [Sch90]

- One of the most widely deployed pieces of cryptography today
- Often in the form of the EdDSA scheme over twisted Edwards curves (currently standardized by NIST)

Our Focus: Schnorr Signatures [Sch90]

- One of the most widely deployed pieces of cryptography today
- Often in the form of the EdDSA scheme over twisted Edwards curves (currently standardized by NIST)
- Algebraic properties of Schnorr signatures have been instrumental in achieving advanced functionalities, such as threshold, blind, adaptor signatures…

Our Focus: Schnorr Signatures [Sch90]

- One of the most widely deployed pieces of cryptography today
- Often in the form of the EdDSA scheme over twisted Edwards curves (currently standardized by NIST)
- Algebraic properties of Schnorr signatures have been instrumental in achieving advanced functionalities, such as threshold, blind, adaptor signatures…
- Existentially unforgeable (EUF-CMA-secure) in the ROM under DL

Tightness

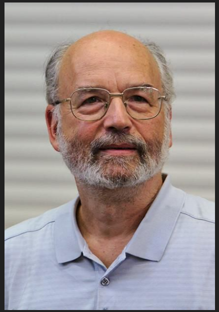
- Suppose we want to use Schnorr signatures over twisted Edwards curves with 128-bit security – how large does the group order need to be?

TU WIEN CYSEC CYBERSECURITYCENTER S&P Security & Privacy

Tightness

- Suppose we want to use Schnorr signatures over twisted Edwards curves with 128-bit security – how large does the group order need to be?

We should use a group order of 256 bits!



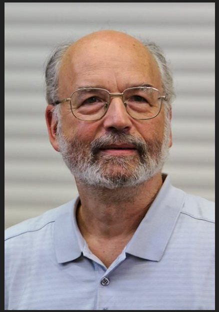
Practitioners

TU WIEN CYSEC CYBERSECURITYCENTER S&P Security & Privacy

Tightness

- Suppose we want to use Schnorr signatures over twisted Edwards curves with **128-bit security** – how large does the **group order** need to be?

We should use a group order of **256** bits!



Practitioners

Best known attack is breaking DL, which on twisted Edwards curves takes time $O(\sqrt{|\mathbb{G}|})$

Tightness

- Suppose we want to use Schnorr signatures over twisted Edwards curves with 128-bit security – how large does the group order need to be?

We should use a group order of 768 bits!

Theoreticians

Tightness

- Suppose we want to use Schnorr signatures over twisted Edwards curves with 128-bit security – how large does the group order need to be?

We should use a group order of 768 bits!

[PS96] in **ROM**:

$$\mathsf{Adv}^{\text{euf-cma}}_{\mathsf{Sch}[\mathbb{G}]} \leq q_h \cdot \sqrt{\mathsf{Adv}^{\text{dl}}_{\mathbb{G}}} + \ldots$$

Theoreticians

Tightness

- Suppose we want to use Schnorr signatures over twisted Edwards curves with **128-bit security** – how large does the **group order** need to be?

We should use a group order of **768** bits!

[PS96] in **ROM**:

$$\mathrm{Adv}^{\text{euf-cma}}_{\mathsf{Sch}[\mathbb{G}]} \leq 2^{64} \cdot \sqrt{\mathrm{Adv}^{\text{dl}}_{\mathbb{G}}}$$

Theoreticians

Tightness

- Suppose we want to use Schnorr signatures over twisted Edwards curves with 128-bit security – how large does the group order need to be?

We should use a group order of 768 bits!

[PS96] in ROM:

$$\mathsf{Adv}^{\text{euf-cma}}_{\mathsf{Sch}[\mathbb{G}]} \leq 2^{64} \cdot \sqrt{\sqrt{2^{-768}}}$$

Theoreticians

CYBERSECURITYCENTER

Tightness

- Suppose we want to use Schnorr signatures over twisted Edwards curves with 128-bit security – how large does the group order need to be?

We should use a group order of 768 bits!

[PS96] in **ROM**:

$$\mathsf{Adv}^{\text{euf-cma}}_{\mathsf{Sch}[\mathbb{G}]} \leq 2^{64} \cdot 2^{-192}$$

Theoreticians

Tightness

- Suppose we want to use Schnorr signatures over twisted Edwards curves with **128-bit security** – how large does the **group order** need to be?

We should use a group order of **768** bits!

[PS96] in **ROM**:

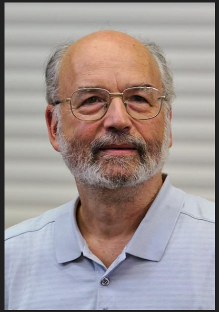
$$\mathsf{Adv}^{\text{euf-cma}}_{\mathsf{Sch}[\mathbb{G}]} \leq 2^{-128}$$

Theoreticians

Tightness

- Suppose we want to use Schnorr signatures over twisted Edwards curves with **128-bit security** – how large does the **group order** need to be?

We should use a group order of **256** bits!



Practitioners

We should use a group order of **768** bits!

Theoreticians

Our Question

Is there a ***tight security proof*** *for Schnorr signatures?*
If so, under what ***assumption****?*

Prior Work: Positive Results

Paper	ROM?	Tight?	Asm./model	Notion
[PS96]	Yes	No	DL	EUF-CMA

Prior Work: Positive Results

Paper	ROM?	Tight?	Asm./model	Notion
[PS96]	Yes	No	DL	EUF-CMA
[PV05]	No	Yes	OMDL	KR-CMA
[BD20]	Yes	Semi	MBDL	EUF-CMA
[FPS20]	Yes	Yes	DL+AGM	EUF-CMA
[RS21]	Yes	No	HMDL	EUF-CMA

Prior Work: Positive Results

Paper	ROM?	Tight?	Asm./model	Notion
[PS96]	Yes	No	DL	EUF-CMA
[PV05]	No	Yes	OMDL	KR-CMA
[BD20]	Yes	Semi	MBDL	EUF-CMA
[FPS20]	Yes	Yes	DL+AGM	EUF-CMA
[RS21]	Yes	No	HMDL	EUF-CMA

$\Longrightarrow$ Getting even a *semi*-tight reduction requires interactive, non-falsifiable assumptions!

TU WIEN CYSEC CYBERSECURITYCENTER S&P Security & Privacy

Prior Work: Positive Results

Paper	ROM?	Tight?	Asm./model	Notion
[PS96]	Yes	No	DL	EUF-CMA
[PV05]	No	Yes	OMDL	KR-CMA
[BD20]	Yes	Semi	MBDL	EUF-CMA
[FPS20]	Yes	Yes	DL+AGM	EUF-CMA
[RS21]	Yes	No	HMDL	EUF-CMA

adversary has oracle access

$\Longrightarrow$ Getting even a *semi*-tight reduction requires interactive, non-falsifiable assumptions!

Prior Work: Positive Results

Paper	ROM?	Tight?	Asm./model	Notion
[PS96]	Yes	No	DL	EUF-CMA
[PV05]	No	Yes	OMDL	KR-CMA
[BD20]	Yes	Semi	MBDL	EUF-CMA
[FPS20]	Yes	Yes	DL+AGM	EUF-CMA
[RS21]	Yes	No	HMDL	EUF-CMA

adversary has oracle access

impossible to efficiently “prove” you found an attack

⟹ Getting even a *semi*-tight reduction requires interactive, non-falsifiable assumptions!

TU WIEN CYSEC CYBERSECURITYCENTER S&P Security & Privacy

Prior Work: Positive Results

Paper	ROM?	Tight?	Asm./model	Notion
[PS96]	Yes	No	DL	EUF-CMA
[PV05]	No	Yes	OMDL	KR-CMA
[BD20]	Yes	Semi	MBDL	EUF-CMA
[FPS20]	Yes	Yes	DL+AGM	EUF-CMA
[RS21]	Yes	No	HMDL	EUF-CMA

adversary has oracle access

impossible to efficiently "prove" you found an attack

⟹ Getting even a *semi*-tight reduction requires interactive, non-falsifiable assumptions or additional idealized models!

TU WIEN CYSEC CYBERSECURITYCENTER S&P Security & Privacy

Prior Work: Negative Results

- [PV05, GBL08, Seu12, FJS19]: no tight & generic reduction from representation-independent (RI), non-interactive problem to EUF-CMA of Schnorr signatures

Prior Work: Negative Results

- [PV05, GBL08, Seu12, FJS19]: no tight & generic reduction from representation-independent (RI), non-interactive problem to EUF-CMA of Schnorr signatures
  - Generic: reduction treats underlying group as a black-box

Prior Work: Negative Results

- [PV05, GBL08, Seu12, FJS19]: no tight & generic reduction from representation-independent (RI), non-interactive problem to EUF-CMA of Schnorr signatures
  - Generic: reduction treats underlying group as a black-box
  - RI: instance-solution pairs invariant to changes of group representation

Prior Work: Negative Results

- [PV05, GBL08, Seu12, FJS19]: no tight & generic reduction from representation-independent (RI), non-interactive problem to EUF-CMA of Schnorr signatures
  - Generic: reduction treats underlying group as a black-box
  - RI: instance-solution pairs invariant to changes of group representation
- All usual assumptions like DL, CDH, DDH, Uber assumption… are RI

Prior Work: Negative Results

- [PV05, GBL08, Seu12, FJS19]: no tight & generic reduction from representation-independent (RI), non-interactive problem to EUF-CMA of Schnorr signatures
  - Generic: reduction treats underlying group as a black-box
  - RI: instance-solution pairs invariant to changes of group representation
- All usual assumptions like DL, CDH, DDH, Uber assumption… are RI

Is there such a representation-dependent assumption or non-generic reduction that gets around the above?

Schnorr Signature Scheme

- Group $(\mathbb{G}, p, g)$, hash function $H\colon \{0,1\}^* \to \mathbb{Z}_p$

Schnorr Signature Scheme

- Group $(\mathbb{G}, p, g)$, hash function $H\colon \{0,1\}^* \to \mathbb{Z}_p$

KeyGen():

1. $sk := x \xleftarrow{\$} \mathbb{Z}_p$
2. $vk := g^x$
3. Return (vk, sk)

Schnorr Signature Scheme

- Group $(\mathbb{G}, p, g)$, hash function $H: \{0,1\}^* \rightarrow \mathbb{Z}_p$

KeyGen():

1. $sk := x \xleftarrow{\$} \mathbb{Z}_p$
2. $vk := g^x$
3. Return (vk, sk)

Sign(x, m):

1. $r \xleftarrow{\$} \mathbb{Z}_p$; $R := g^r$
2. $c := H(R, m)$
3. $s := r + cx \bmod p$
4. Return (R, s)

Schnorr Signature Scheme

- Group $(\mathbb{G}, p, g)$, hash function $H : \{0,1\}^* \rightarrow \mathbb{Z}_p$

KeyGen():

1. $sk := x \xleftarrow{\$} \mathbb{Z}_p$
2. $vk := g^x$
3. Return (vk, sk)

Sign(x, m):

1. $r \xleftarrow{\$} \mathbb{Z}_p;\ R := g^r$
2. $c := H(R, m)$
3. $s := r + cx \bmod p$
4. Return (R, s)

Verify$(vk, m, (R, s))$:

1. $c := H(R, m)$
2. $g^s = R \cdot vk^c$?

New Assumption: Circular Discrete-Logarithm (CDL)

- Let $\mathbb{G} = \langle g \rangle$ be a group of prime order p

New Assumption: Circular Discrete-Logarithm (CDL)

- Let $\mathbb{G} = \langle g \rangle$ be a group of prime order p

Discrete-Logarithm Problem:

1. $x \xleftarrow{\$} \mathbb{Z}_p;\ h := g^x$
2. $x' \xleftarrow{\$} \mathrm{A}(h)$
3. $x = x'$?

TU WIEN CYSEC CYBERSECURITYCENTER S&P Security & Privacy

New Assumption: Circular Discrete-Logarithm (CDL)

- Let $\mathbb{G} = \langle g \rangle$ be a group of prime order p
- Let $f : \mathbb{G} \to \mathbb{Z}_p$ be an efficiently computable function

Discrete-Logarithm Problem:

1. $x \xleftarrow{\$} \mathbb{Z}_p;\ h := g^x$
2. $x' \xleftarrow{\$} \mathrm{A}(h)$
3. $x = x'$?

TU WIEN CYSEC CYBERSECURITYCENTER S&P Security & Privacy

New Assumption: Circular Discrete-Logarithm (CDL)

- Let $\mathbb{G} = \langle g \rangle$ be a group of prime order p
- Let $f : \mathbb{G} \to \mathbb{Z}_p$ be an efficiently computable function

Discrete-Logarithm Problem:

1. $x \xleftarrow{\$} \mathbb{Z}_p;\ h := g^x$
2. $x' \xleftarrow{\$} \mathrm{A}(h)$
3. $x = x'$?

Circular Discrete-Logarithm Problem:

1. $x \xleftarrow{\$} \mathbb{Z}_p;\ h := g^x$
2. $(R, z) \xleftarrow{\$} \mathrm{A}(h)$
3. $f(R) \neq 0 \wedge g^z = R \cdot h^{f(R)}$?

Circular Discrete-Logarithm (CDL) Assumption

- CDL solution: $(R, z) \in \mathbb{G} \times \mathbb{Z}_p$ such that $f(R) \neq 0 \wedge g^z = R \cdot h^{f(R)}$

TU WIEN CYSEC CYBERSECURITYCENTER S&P Security & Privacy

Circular Discrete-Logarithm (CDL) Assumption

- CDL solution: $(R, z) \in \mathbb{G} \times \mathbb{Z}_p$ such that $f(R) \neq 0 \wedge g^z = R \cdot h^{f(R)}$
- CDL is:
  - ✅ non-interactive

Circular Discrete-Logarithm (CDL) Assumption

- CDL solution: $(R, z) \in \mathbb{G} \times \mathbb{Z}_p$ such that $f(R) \neq 0 \wedge g^z = R \cdot h^{f(R)}$
- CDL is:
  - ✅ non-interactive
  - ✅ falsifiable

Circular Discrete-Logarithm (CDL) Assumption

- CDL solution: $(R, z) \in \mathbb{G} \times \mathbb{Z}_p$ such that $f(R) \neq 0 \wedge g^z = R \cdot h^{f(R)}$
- CDL is:
  - ✅ non-interactive
  - ✅ falsifiable
  - ✅ representation-dependent

TU WIEN CYSEC CYBERSECURITYCENTER S&P Security & Privacy

Circular Discrete-Logarithm (CDL) Assumption

- CDL solution: $(R, z) \in \mathbb{G} \times \mathbb{Z}_p$ such that $f(R) \neq 0 \wedge g^z = R \cdot h^{f(R)}$
- CDL is:
  - ✅ non-interactive
  - ✅ falsifiable
  - ✅ representation-dependent
- Does it correspond to a no-message attack on the empty message?

TU WIEN CYSEC CYBERSECURITYCENTER S&P Security & Privacy

Circular Discrete-Logarithm (CDL) Assumption

- CDL solution: $(R, z) \in \mathbb{G} \times \mathbb{Z}_p$ such that $f(R) \neq 0 \wedge g^z = R \cdot h^{f(R)}$
- CDL is:
  - ✅ non-interactive
  - ✅ falsifiable
  - ✅ representation-dependent
- Does it correspond to a no-message attack on the empty message?
  - No, because f doesn't have to be the same as hash function used by Schnorr!

TU WIEN CYSEC CYBERSECURITYCENTER S&P Security & Privacy

Circular Discrete-Logarithm (CDL) Assumption

- CDL solution: $(R, z) \in \mathbb{G} \times \mathbb{Z}_p$ such that $f(R) \neq 0 \land g^z = R \cdot h^{f(R)}$
- CDL is:
  - ✅ non-interactive
  - ✅ falsifiable
  - ✅ representation-dependent
- Does it correspond to a no-message attack on the empty message?
  - No, because f doesn't have to be the same as hash function used by Schnorr!
  - In fact, we don't even need to know what f is!

Main Result

Theorem (in ROM):

$$\mathsf{Adv}^{\text{euf-cma}}_{\mathsf{Sch}[\mathbb{G}]} \leq \mathsf{Adv}^{\text{cdl}}_{\mathbb{G},f} + \frac{q_s(q_s + q_h) + q_h \cdot |f^{-1}(0)|}{p}$$

Main Result

Theorem (in ROM):

$$\mathsf{Adv}^{\text{euf-cma}}_{\mathsf{Sch}[\mathbb{G}]} \leq \mathsf{Adv}^{\text{cdl}}_{\mathbb{G},f} + \frac{q_s(q_s+q_h)+q_h\cdot|f^{-1}(0)|}{p}$$

- Arbitrary efficiently computable function $f:\mathbb{G}\to\mathbb{Z}_p$!

TU WIEN CYSEC CYBERSECURITYCENTER S&P Security & Privacy

Main Result

Theorem (in ROM):

$$\mathsf{Adv}^{\text{euf-cma}}_{\mathsf{Sch}[\mathbb{G}]} \leq \mathsf{Adv}^{\text{cdl}}_{\mathbb{G},f} + \frac{q_s(q_s + q_h) + q_h \cdot |f^{-1}(0)|}{p}$$

- Arbitrary efficiently computable function $f : \mathbb{G} \to \mathbb{Z}_p$!
- Take f that minimizes advantage

Applicability of CDL to Threshold Schnorr Signatures

- Sparkle+ [CKM23] is a recent 3-round threshold Schnorr signature scheme

Applicability of CDL to Threshold Schnorr Signatures

- Sparkle+ [CKM23] is a recent 3-round threshold Schnorr signature scheme
- NIST is currently standardizing threshold Schnorr

TU WIEN CYSEC CYBERSECURITYCENTER S&P Security & Privacy

Applicability of CDL to Threshold Schnorr Signatures

- Sparkle+ [CKM23] is a recent 3-round threshold Schnorr signature scheme
- NIST is currently standardizing threshold Schnorr
- Sparkle+ has a loose reduction from static security to DL (in the ROM)

Applicability of CDL to Threshold Schnorr Signatures

- Sparkle+ [CKM23] is a recent 3-round threshold Schnorr signature scheme
- NIST is currently standardizing threshold Schnorr
- Sparkle+ has a loose reduction from static security to DL (in the ROM)
- We give a tight proof of static security under CDL (in the ROM)

TU WIEN CYSEC CYBERSECURITYCENTER S&P Security & Privacy

Justifying CDL

1. Idealized group:

Justifying CDL

1. Idealized group:
   - We show CDL is as hard as DL in the elliptic-curve GGM [GS22] for any function f that has small preimage sets

Justifying CDL

1. Idealized group:
   - We show CDL is as hard as DL in the elliptic-curve GGM [GS22] for any function f that has small preimage sets
2. Idealized function:

Justifying CDL

1. Idealized group:
   - We show CDL is as hard as DL in the elliptic-curve GGM [GS22] for any function f that has small preimage sets
2. Idealized function:
   - We show that for the ECDSA conversion function

$$f : (x, y) \mapsto x \bmod p$$

   CDL reduces to DL in the algebraic bijective ROM [FKP16, QCY21]

TU WIEN CYSEC CYBERSECURITYCENTER S&P Security & Privacy

Summary

- We introduce the circular discrete-logarithm problem, a new non-interactive and falsifiable variant of DL which uses a function $f : \mathbb{G} \to \mathbb{Z}_p$

TU WIEN CYSEC CYBERSECURITYCENTER S&P Security & Privacy

Summary

- We introduce the circular discrete-logarithm problem, a new non-interactive and falsifiable variant of DL which uses a function $f : \mathbb{G} \to \mathbb{Z}_p$
- We show a tight reduction from EUF-CMA of Schnorr signatures to CDL in the ROM

TU WIEN CYSEC CYBERSECURITYCENTER S&P Security & Privacy

Summary

- We introduce the circular discrete-logarithm problem, a new non-interactive and falsifiable variant of DL which uses a function $f : \mathbb{G} \to \mathbb{Z}_p$
- We show a tight reduction from EUF-CMA of Schnorr signatures to CDL in the ROM
- We conjecture that the ECDSA conversion function works as f for a suitable elliptic-curve group and give evidence by proving it in suitable idealized models

Summary

- We introduce the circular discrete-logarithm problem, a new non-interactive and falsifiable variant of DL which uses a function $f: \mathbb{G} \to \mathbb{Z}_p$
- We show a tight reduction from EUF-CMA of Schnorr signatures to CDL in the ROM
- We conjecture that the ECDSA conversion function works as f for a suitable elliptic-curve group and give evidence by proving it in suitable idealized models
- We give a tight proof of (static) security of the Sparkle+ threshold signature scheme [CKM23] under CDL

Future Directions

- Is there a function for which CDL reduces to a standard assumption, maybe even DL?
- Is CDL applicable to:
  - Additional threshold Schnorr schemes?
  - Additional advanced primitives based on Schnorr signatures like adaptor signatures, multisignatures, or blind signatures?
- Could CDL be useful for instantiating Schnorr signatures under EUF-CMA in the standard model?

TU WIEN CYSEC CYBERSECURITYCENTER S&P Security & Privacy

Thanks!

Questions?

https://ia.cr/2024/1528

TU WIEN CYSEC CYBERSECURITYCENTER S&P Security & Privacy

Proof Intuition

- On CDL instance h, we run the forger with public key h
- We simulate signing queries as in [PS96]
- For hash queries, we want to embed outputs of f in responses such that:
  1. Responses are independent and uniform
  2. The forgery can be used to extract a CDL solution
- On the i-th hash query (R, m), we set $R' := R \cdot h^{a_i} \cdot g^{b_i}$ for random $a_i, b_i \in \mathbb{Z}_p$ and return

$$f(R') + a_i \bmod p$$

Proof Intuition

- Now adversary's forgery $m, (R, s)$ will correspond to a hash query, so:

$$g^s = R \cdot h^c = R \cdot h^{f(R \cdot h^a \cdot g^b)+a}$$

- Multiplying both sides by g^b gives:

$$g^{s+b} = R \cdot h^a \cdot g^b \cdot h^{f(R \cdot h^a \cdot g^b)}$$

- So, we can return the CDL solution:

$$(R \cdot h^a \cdot g^b,\ s + b \bmod p)$$

TU WIEN CYSEC CYBERSECURITYCENTER S&P Security & Privacy