



Provable security:

main concepts, significance
and open problems

OR WHAT DOES «PROVABLE SECURITY» PROVE?

Evgeny Alekseev

Liliya Akhmetzyanova



Global history

- Global history – two major milestones:
 - First papers for asymptotically defined objects:
 - M. Rabin. «Digitalized signatures and public-key functions as intractable as factorization», **1979**.
 - A. C. Yao. «Theory and applications of trapdoor functions», **1982**.
 - S. Goldwasser and S. Micali. «Probabilistic encryption», **1984**.
 - M. Blum and S. Micali. «How to generate cryptographically strong sequences of pseudorandom bits», **1984**.

Global history

- Global history – two major milestones:
 - Papers for concrete mechanisms and protocols:
 - M. Bellare, A. Desai, E. Jokipii and P. Rogaway. «A Concrete Security Treatment of Symmetric Encryption: Analysis of the DES Modes of Operation», **1997**.
 - M. Bellare and P. Rogaway, «Practice-Oriented Provable-Security», **1998**.
 - M. Bellare and P. Rogaway. «The security of triple encryption and a framework for code-based game-playing proofs», **2006**.
- Today: 63 of the 105 papers on EUROCRYPT 2024 are related to provable security

Global history

- Global history – two major milestones:
 - Papers for concrete mechanisms and protocols:
 - M. Bellare, A. Desai, E. Jokipii and P. Rogaway. «A Concrete Security Treatment of Symmetric Encryption: Analysis of the DES Modes of Operation», **1997**.
 - M. Bellare and P. Rogaway, «Practice-Oriented Provable-Security», **1998**.
 - **M. Bellare and P. Rogaway. «The security of triple encryption and a framework for code-based game-playing proofs», 2006. EUROCRYPT in Russia!**
- Today: 63 of the 105 papers on EUROCRYPT 2024 are related to provable security

Russian history

- First papers:
 - N.P. Varnovskii. «Provable security of digital signatures in the tamper-proof device model», **2008**.
 - A.G. Stolbunov. «On the provable security of cryptosystems based on elliptic curve isogenies», **2008**.
- First papers on security of practical mechanisms:
 - G.K. Sedov «The security of GOST R 34.11-2012 against preimage and collision attacks», **2015**.
 - E.K. Alekseev, I.B. Oshkin, V.O. Popov, S.V. Smyshlyaev. «On the cryptographic properties of algorithms accompanying the applications of standards GOST R 34.11-2012 and GOST R 34.10-2012», **2016**.
 - L.R. Ahmetzyanova, E.K. Alekseev, I.B. Oshkin, S.V. Smyshlyaev, L.A. Sonina. «On the properties of the CTR encryption mode of Magma and Kuznyechik block ciphers with re-keying method based on CryptoPro Key Meshing», **2017**.

Russian history

- Modern research:
 - **LLC «SFB Lab», JSC «InfoTeCS».** V.A. Kiryukhin, A.A. Scherbachenko: papers on symmetric schemes (PRF, KDF, MAC) based on the Streebog hash function and a block cipher;
 - **Security Code.** A.M. Koreneva, G.V. Firsov: papers on full disk encryption block cipher modes of operation;
 - **Kryptonite.** K. Tsaregorodtsev: evaluation of the security level of protocols used within the 5G technology and other cryptographic mechanisms;
 - **QApp.** M. Kudinov, S. Grebnev, Yu.V. Kosolapov, O.Yu. Turchenko: papers on post-quantum mechanisms;
 - **Aktiv.** A.R. Vasin, M.A. Skorobogatova, B.Yu. Buinov: research on security of AEAD-modes of operation;
 - **TC26.** V.I. Nozdrunov, I.V. Lavrikov, V.A. Shishkin: research on block cipher modes of operations and hash-based symmetric schemes (KDF, PRF).

Russian history

- First dissertations:
 - Doctoral: S.V. Smyshlyaev. «Mathematical methods of assessment of the security level of cryptosystems operating in a low-trust environment», **2022**.
 - PhD: L.R. Akhmetzyanova. «Combinatorial properties of schemes providing confidentiality and integrity», **2022**.

What is «provable security» and what is not

We can't prove statements like
«**there not exists an efficient algorithm for solving
this math problem**»
in realistic calculation model.



What is «provable security» and what is not

- Basic idea – proof by contradiction:

«If **A is true**, then **B is true**»

$\Leftrightarrow$

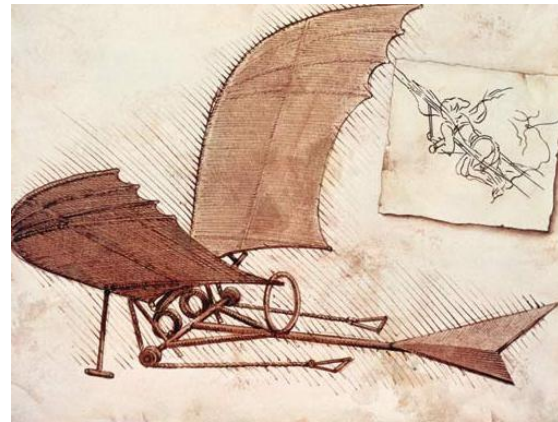
«If **not-B is true**, then **not-A is true**»

- In the language of cryptography:

«If **basic math problem is hard**, then
cryptosystem can't be broken»

$\Leftrightarrow$

«If **cryptosystem can be broken**, then
efficient algorithm for solving basic math problem exists»



What is «provable security» and what is not

- Basic idea – proof by contradiction:

«If **A is true**, then **B is true**»

$\Leftrightarrow$

«If **not-B is true**, then **not-A is true**»

- In the language of cryptography:

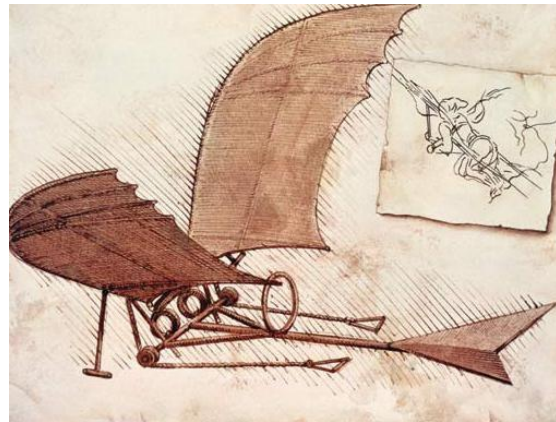
«If **basic math problem is hard**, then
cryptosystem can't be broken»

$\Leftrightarrow$

«If **cryptosystem can be broken**, then
efficient algorithm for solving basic math problem exists»

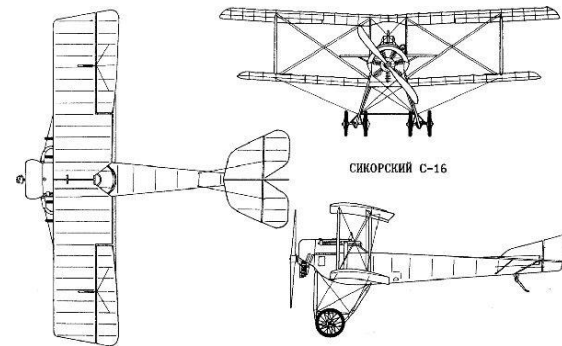
We need to prove
non-existence

We need to construct
concrete algorithm



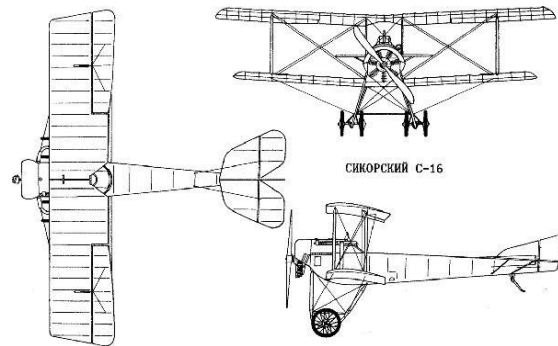
What is «provable security» and what is not

- More common and practice-oriented task is **to estimate the security level of cryptosystem**
- Definitions:
 - Let $A_{M,S}$ – an adversary (= algorithm) who is trying to break cryptosystem (or solve math problem) S in the sense M
 - $T(A_{M,S})$ – computation resources of algorithm $A_{M,S}$
 - **Security level** of S in sense M : $Sec_M(S) = \min_{A_{M,S}} T(A_{M,S})$
- We will use just A instead $A_{M,S}$ for short because it will be clear it mean every time.



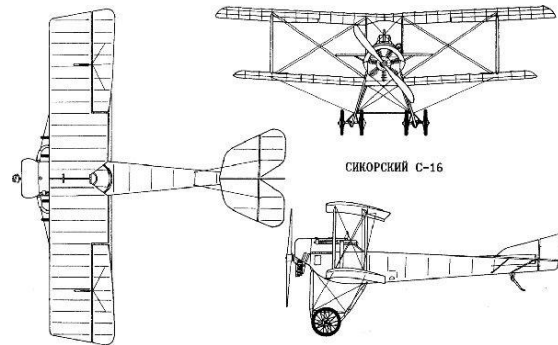
What is «provable security» and what is not

- We need to prove the statement «if cryptosystem can be broken, then efficient algorithm for solving basic math problem exists»
- What we have:
there exist some algorithm A which breaks the cryptosystem S in sense M
- What we need to do:
construct as efficient an algorithm B for solving math problem S' in sense M' as possible using algorithm A as «black box»



What is «provable security» and what is not

- Ok, we done it! What does this give us?
- We need to get nontrivial upper bound for $T(B)$ as a function of $T(A)$.
For example:
 - $T(B) \leq T(A) + \delta$
- A is a «black box», which mean it is arbitrary $\Rightarrow$ we can put it equal to most efficient one for breaking S in sense M :
 - $A' = \underset{A}{\operatorname{argmin}} T(A)$, so $T(A') = \operatorname{Sec}(S)$
- B is concrete, so the following inequality holds:
 - $\operatorname{Sec}(S') \leq T(B)$
- Finally we have:
 - $\operatorname{Sec}(S') \leq T(B) \leq T(A) + \delta = \operatorname{Sec}(S) + \delta$
 - $\operatorname{Sec}(S) \geq \operatorname{Sec}(S') - \delta$

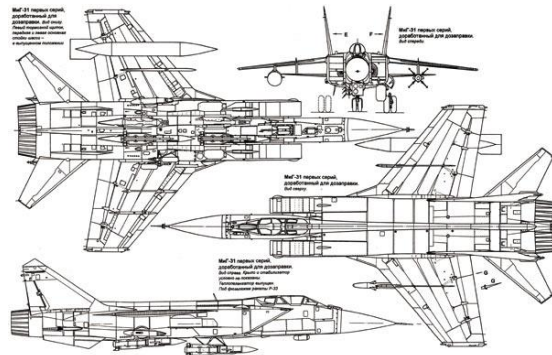


What is «provable security» and what is not

- In real world we work not only with computational resources but also with success probability and other system and model parameters
- $Adv_S^M(A)$ – measure of adversary success (like $T(A)$)
- $Insec_S^M(t, \dots) = \max_{A \in \mathcal{A}(t, \dots)} Adv_S^M(A)$ – insecurity of the system S in sense M (like $Sec(S)$)
- The result of reduction is:

$$Insec_S^M(t, \dots) \leq F\left(params, Insec_{S'}^{M'}(t', \dots)\right)$$

L.R. Ahmetzyanova, E.K. Alekseev, G.A. Karpunin, S.V. Smyshlyaev.
«On cryptographic properties of the CVV and PVV parameters
generation procedures in payment systems», 2018.



What is «provable security» and what is not

- Mihir Bellare («Practice-oriented provable security»): What provable security give us?

NOMENCLATURE. In some ways the term “provable security” is misleading. As the above indicates, what is probably the central step is providing a model and definition, which does not involve proving anything. And one does not “prove a scheme secure:” one provides a reduction of the security of the scheme to the security of some underlying atomic primitive. For that reason, I sometimes use the term “reductionist security” to refer to this genre of work.

- Reduction in provable security is a concrete attack against base atomic primitive by the adversary equipped with a «function», which can break the cryptosystem.

Power of provable security

- Saving researchers attentions:
 - We can evaluate the security by concrete attacks not for all cryptosystems, but just for basic math problems and mechanisms.
- Modularity:
 - We can evaluate the security of cryptosystems not for each atomic components, but for classes united by the security requirement.
- Predictions:
 - Reductions can predict existence of concrete attacks.
 - Examples: security bound for CTR-ACPKM predicts the Dunkelman-Ghosh-Lambooij attack of 2023.

Critics of provable security

Critics

Feelings of cryptographers
practicing concrete methods



Critics

Feelings of cryptographers
practicing provable security



Critic abroad

Critical perspectives on provable security: Fifteen years of "Another Look" papers

Neal Koblitz and Alfred Menezes

Advances in Mathematics of Communications, 13 (2019), 517-558.



Another Look at Provable Security

Ever since Thomas Kuhn's *The Structure of Scientific Revolutions* appeared a half-century ago, historians of science and technology have viewed the challenging — and occasionally the overthrowing — of reigning paradigms as an essential part of scientific progress. In contrast, complacency, arrogance, and efforts to suppress alternative viewpoints (for example, by dominating program committees or editorial boards) are antithetical to the scientific spirit.

This very general observation applies with special force to cryptography. Throughout history the most successful cryptographers have been those who've been aware of the need to be constantly questioning assumptions, searching for new vulnerabilities, and critiquing exaggerated claims of security.

In our time one of the dominant paradigms in cryptographic research goes by the name "provable security." This is the notion that the best (or, some would say, the *only*) way to have confidence in the security of a cryptographic protocol is to have a mathematically rigorous theorem that establishes some sort of guarantee of security (defined in a suitable way) under certain conditions and given certain assumptions.

The purpose of this website is to encourage the emergence of a more skeptical and less credulous attitude toward this notion and to contribute to a process of critical analysis of the positive and negative features of the "provable security" paradigm.

Neal Koblitz and Alfred Menezes

Articles

Main page

Overview

Critical perspectives on provable security
"Another Look" papers **UPDATED!!**

Concrete analysis of approximate ideal
Ring-LWE reduction **NEW!!**

Cryptography 101 online course **NEW!**

Kyber and Dilithium online course **NEW!**

Another look at "provable security"

Another look at "provable security" II

Another look at generic groups

Another look at HMQV

Another look at non-standard DL and CDH

Another look at automated theorem-proving

Another look at automated theorem-proving II

Another look at security definitions

Another look at tightness

Another look at tightness II

Another look at HMAC

Another look at 1-key nested MACs

Another look at non-uniformity

Another look at XCB

Another look at normal approximations

On the security of the WOTS-PRF signature

The uneasy relationship between mathematics and cryptography

The brave new world of bodacious asymptotic security in cryptography

Critic in Russia

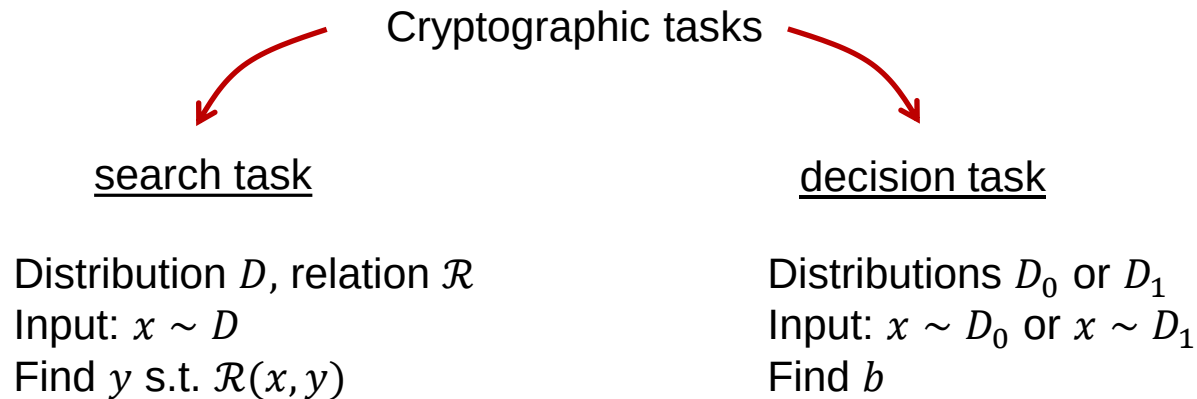
«Эффект плацебо в криптографии», Denis Fomin, RusCrypto 2023.

«Показуемая стойкость в задаче обфускации криптографических исследований», Grigory Marshalko and Denis Fomin, RusCrypto 2024.

Critics

- unclear advantages
- uncovered concrete methods
- non-tight bounds

1 what do advantages mean



1 what do advantages mean

Cryptographic tasks

search task

Examples:

- Make forgery
- Recover key
- Recover plaintext

decision task

Examples:

- «distinguish» «real» output from «ideal» output

Advantage of adversary

$$Adv(A) = \Pr_{x \sim D} [A(x) \rightarrow y]$$

probability of success

$$Adv(A) = \Pr_{x \sim D_0} [A(x) \rightarrow 1] - \Pr_{x \sim D_1} [A(x) \rightarrow 1]$$

«computational» distance



1 what do advantages mean

$$Adv(A) = \Pr_{x \sim D_0} [A(x) \rightarrow 1] - \Pr_{x \sim D_1} [A(x) \rightarrow 1]$$

«computational» distance

practical meaning?

Informal idea:

f there exists an algorithm that
recover «**dangerous**» **amount** of info with **high** probability than there exists a
distinguisher with **high** advantage

1 what do advantages mean

Example: pseudorandom generator PRG: $\{0,1\}^n \rightarrow \{0,1\}^m, m > n$, and its security model

$$D_0 = \{\text{PRG}(s)\}_{s \sim U_n} \quad \text{vs} \quad D_1 = U_m$$

s – initial seed, U_l – uniform distribution over $\{0,1\}^l$.

1 what do advantages mean

Suppose that there exists an algorithm that for a given PRG can predict (recover):

the $wt(PRG(s))$ with probability 1 (Hamming weight)

✓ there exists A s.t $Adv(A) \approx 1$

the first bit of $PRG(s)$ with probability 1

✓ there exists A s.t $Adv(A) = \frac{1}{2}$

} dangerous

that $PRG(s) \neq 0^m$ with probability $1/2$

✓ there exists A s.t $Adv(A) = 1/2^m$

} for big m not so dangerous?



1 what do advantages mean

Suppose that there exists an algorithm that for a given PRG can predict (recover):

the $wt(PRG(s))$ with probability 1 (Hamming weight)

✓ there exists A s.t $Adv(A) \approx 1$

the first bit of $PRG(s)$ with probability 1

✓ there exists A s.t $Adv(A) = \frac{1}{2}$

} dangerous

that $PRG(s) \neq 0^m$ with probability $1/2$

✓ there exists A s.t $Adv(A) = 1/2^m$

} for big m not so dangerous?

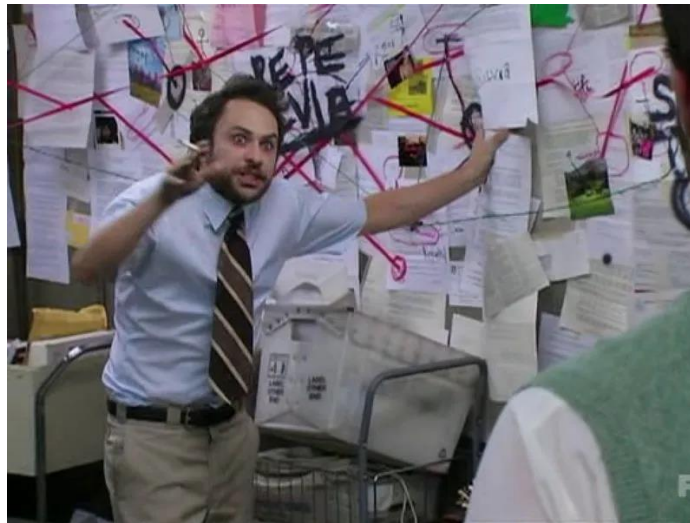
Open question: how exactly $Adv(A)$ correlates with probability of success and amount of recovered info?



2 it does not cover known concrete methods

It can happen, it is OK and
it is complicated...

Let's get into the details



2 it does not cover known concrete methods

Reason #1 Inaccurate/different security model

1. Inaccurate assumptions about adversary goal or capabilities (qualitative and quantitative)

2 it does not cover known concrete methods

Reason #1 Inaccurate/different security model

1. Inaccurate assumptions about adversary goal or capabilities (qualitative and quantitative)

Example 1: Blindness property for blind signatures [1]

«The adversarial signer cannot obtain any info about...»

Incorrect

«...signed message»

Correct

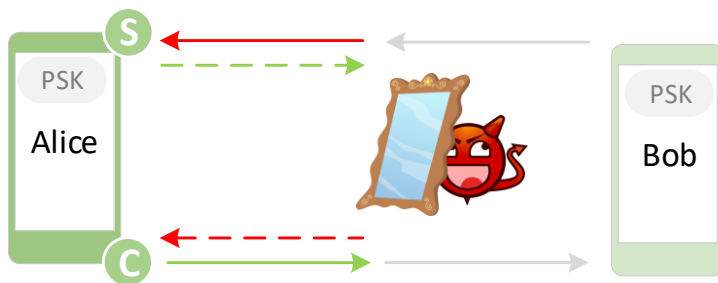
«... signed message **and its signature**»

2 it does not cover known concrete methods

Reason #1 Inaccurate/different security model

1. Inaccurate assumptions about adversary goal or capabilities (qualitative and quantitative)

Example 2: Using the same PSK for client-side and server-side secret in TLS 1.3



2 it does not cover known concrete methods

Reason #1 Inaccurate/different security model

1. Inaccurate assumptions about adversary goal or capabilities (qualitative and quantitative)

For more details see

«What bad things can happen by using crypto algorithms incorrectly?», E.K. Alekseev, CTCrypt 2019.

2 it does not cover known concrete methods

Reason #1 Inaccurate/different security model

2. Model idealizations

Examples:

- Random Oracle model
- Ideal Cipher model
- Generic/algebraic group model

2 it does not cover known concrete methods

Reason #1 Inaccurate/different security model

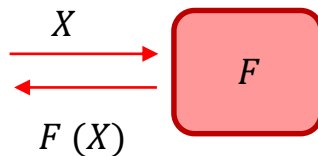
2. Model idealizations

Examples:

- **Random Oracle model**
- Ideal Cipher model
- Generic/algebraic group model

Hash function $H: \{0,1\}^* \rightarrow \{0,1\}^n$ is replaced with an «ideal» random function

$$F \stackrel{U}{\leftarrow} \text{Func}(\{0,1\}^*, \{0,1\}^n)$$



2 it does not cover known concrete methods

Reason #1 Inaccurate/different security model

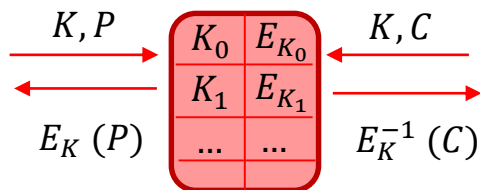
2. Model idealizations

Examples:

- Random Oracle model
- **Ideal Cipher model**
- Generic/algebraic group model

Block cipher $E: \{0,1\}^k \times \{0,1\}^n \rightarrow \{0,1\}^n$
is replaced with a set of 2^k «ideal»
random permutations

$$\{E_K \stackrel{U}{\leftarrow} \text{Perm}(\{0,1\}^n)\}_{K \in \{0,1\}^k}$$



2 it does not cover known concrete methods

Reason #1 Inaccurate/different security model

2. Model idealizations

Examples:

- Random Oracle model
- Ideal Cipher model
- **Generic/algebraic group model**

Group $\mathbb{G} = \langle g \rangle$ is replaced with
a randomly chosen encoding of
the group

2 it does not cover known concrete methods

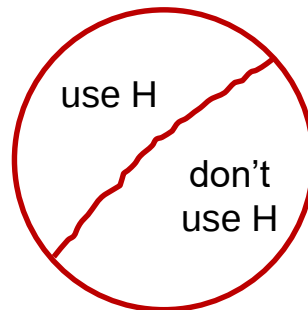
Reason #1 Inaccurate/different security model

2. Model idealizations

How to interpret results: this security models «cover» only those adversaries that do not use specific properties of

- hash function
- block cipher
- group

All adversaries



2 it does not cover known concrete methods

Reason #1 Inaccurate/different security model

2. Model idealizations

BE CAREFUL:

Theorem (Informal) [1] There exists a signature scheme that is secure in ROM but is insecure with any «real» hash function.

(similar result on GGM model is presented in [2])

Provide concrete method analysis regarding adversaries «uncovered» by model

[1] Canetti R., Goldreich O., Halevi S. «The Random Oracle Methodology, Revisited», 1998.

[2] Dent A. «Adapting the weaknesses of the Random Oracle model to the Generic Group model», 2002.

2 it does not cover known concrete methods

Reason #1 Inaccurate/different security model

2. Model idealizations

Why we need idealizations?

Sometimes we cannot construct reduction without idealizations

2 it does not cover known concrete methods

Reason #1 Inaccurate/different security model

Example: Schnorr signatures

→ ROM, reduction to dl (discrete logarithm) [1]:

$$Adv_{Schnorr}^{uf}(A) \leq f\left(params, Adv_{\mathbb{G}}^{dl}(A')\right)$$

→ GGM, reduction to rpp and rpsp (random-prefix preimage and second preimage) [2]:

$$Adv_{Schnorr}^{uf}(A) \leq f\left(params, Adv_H^{rpp}(A'), Adv_H^{rpsp}(A'')\right)$$

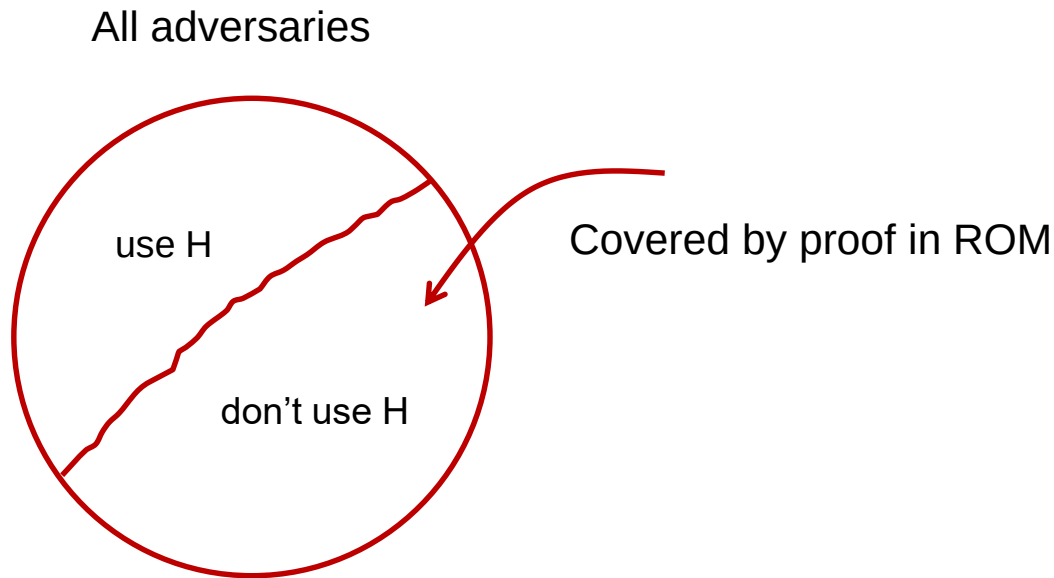
[1] Pointcheval D., Stern J. Security Proofs for Signature Schemes, EUROCRYPT'96.

[2] Neven G., Smart N.P., Warinschi B. Hash function requirements for Schnorr signatures, Journal of Mathematical Cryptology, 2009.

2 it does not cover known concrete methods

Reason #1 Inaccurate/different security model

Example: Schnorr signatures



2 it does not cover known concrete methods

Reason #1 Inaccurate/different security model

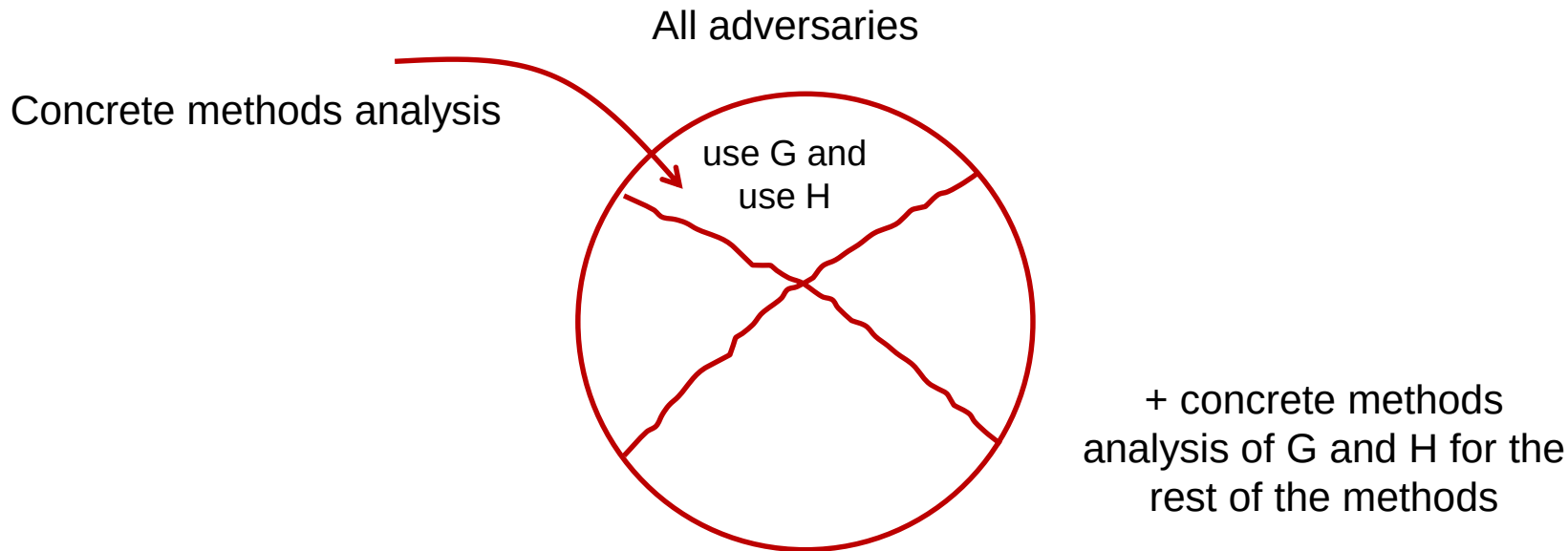
Example: Schnorr signatures



2 it does not cover known concrete methods

Reason #1 Inaccurate/different security model

Example: Schnorr signatures



2 it does not cover known concrete methods

Reason #1 Inaccurate/different security model

For more details about meaning of reductions see

«Practical significance of security bounds for standardized internally re-keyed block cipher modes», Ahmetzyanova L., Alekseev E., Sedov G., Griboedova E., Smyshlyaev S. 2019.

2 it does not cover known concrete methods

Reason #2

Insecurity of basic problem/mechanism

$$Adv_S^M(A) \leq f(\text{params}, Adv_{\Pi}^{M'}(A'))$$

Total break

ROS-attack on blind signatures [1]

Proofs allow to predict this attack

Reducing security (current params are not OK)

Discrete logarithm for finite fields [2]

[1] Benhamouda F. On the (In)security of ROS. Security Proofs for Signature Schemes, IACR Cryptol, ePrint Arch, 2020.

[2] Adleman L., Huang M.D. Function Field Sieve Method for Discrete Logarithm over Finite Fields. Inf. Comput, 1999.

2 it does not cover known concrete methods

Reason #3

Inaccurately evaluated bounds

2 it does not cover known concrete methods

Reason #3

Inaccurately evaluated bounds

1 Carefully chose computational model (time, memory, precomputations, parallelism), it can be important for e.g. light-weight crypto with small security parameters [1].

2 it does not cover known concrete methods

Reason #3

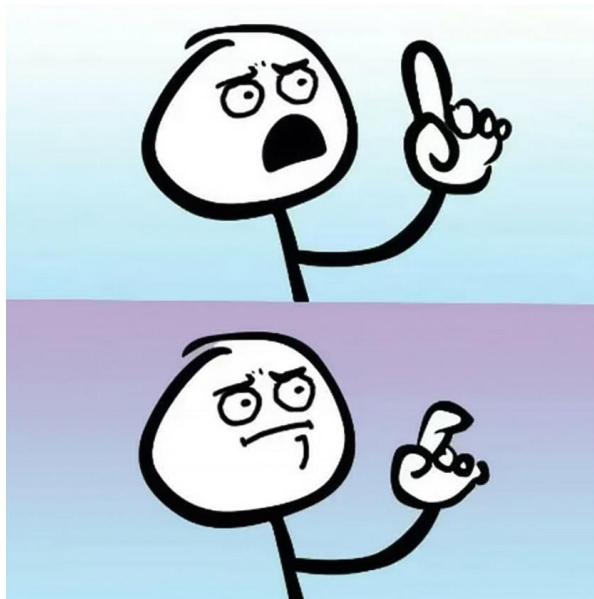
Inaccurately evaluated bounds

2 Carefully choose «heuristic» upper bounds for basic problems, take into account all known methods

DL – Pollard's rho-method (easy)

LWE (Learning with Errors) – a lot of different methods that depend differently on different parameters [1]

3 non-tight security bounds



OK, we are ready
to use provably security results,
but ... how?

3 non-tight security bounds

Example: Schnorr signatures, upper bound provable in ROM [1]

$$Adv_{Schnorr}^{uf}(A) \leq f(params) + \underbrace{\sqrt{q_0 Adv_{\mathbb{G}}^{dl}(A')}}_{\text{Pollard's rho-method}}$$

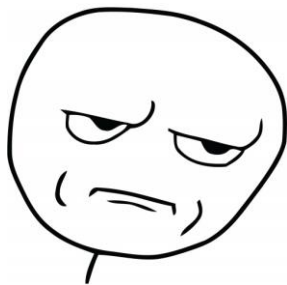
Let the best method for discrete logarithm be
Pollard's rho-method with time complexity
 $\approx \sqrt{q}$, where $q = |\mathbb{G}|$

The bounds «predicts» that there exist methods
breaking Schnorr with time complexity $\approx \sqrt[4]{q}$

3 non-tight security bounds

Example: Schnorr signatures, upper bound provable in ROM

$$Adv_{Schnorr}^{uf}(A) \leq f(params) + \underbrace{\sqrt{q_0 Adv_{\mathbb{G}}^{dl}(A')}}_{\text{red bracket}}$$



Are really there?

Let the best method for discrete logarithm be
Pollard's rho-method with time complexity
 $\approx \sqrt{q}$, where $q = |\mathbb{G}|$

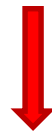
The bounds «predicts» that there exist methods
breaking Schnorr with time complexity $\approx \sqrt[4]{q}$

3 non-tight security bounds

Example: Schnorr signatures

$$Adv_{Schnorr}^{uf}(A) \leq f(params) + \underbrace{\sqrt{q_0 Adv_{\mathbb{G}}^{dl}(A')}}_{\text{no known methods corresponding to this term}}$$

no known methods
corresponding to this term



If there is a «gap» between lower and upper bound
then the upper (insecurity) bound is **non-tight**

3 non-tight security bounds

If the gap is big



Bounds provides non-optimal security parameters

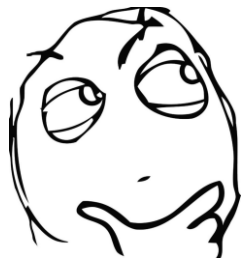


Reduces performance

Example: for Schnorr signatures we should choose 512-bits q to guarantee 128-bit security.

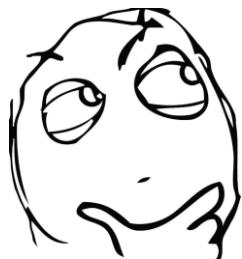


3 non-tight security bounds



Push yourself, try harder and construct better reductions!

3 non-tight security bounds



Push yourself, try harder and construct better reductions!

Not so fast, sometimes it's not easy at all...

Theorem 1 [1] (informal). For almost any natural non-interactive computational problem Π , there is *no tight generic reduction* from solving Π to breaking the Schnorr signatures, unless solving Π is easy.

3 non-tight security bounds

These kinds of results are proven using

Meta-reduction

3 non-tight security bounds

These kinds of results are proven using

Meta-reduction

«Ordinary» reduction

reduction R ■
breaking
problem Π



adversary A
breaking
scheme S

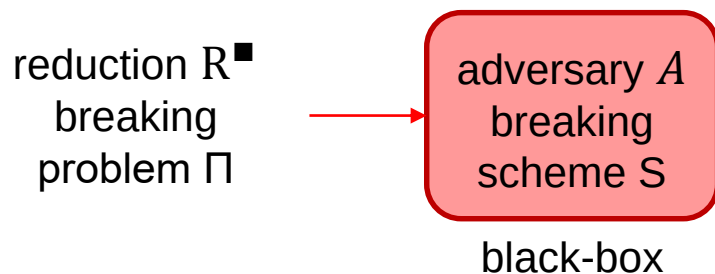
black-box

3 non-tight security bounds

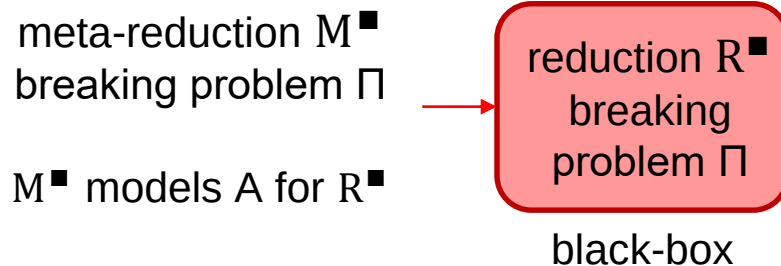
These kinds of results are proven using

Meta-reduction

«Ordinary» reduction



Meta-reduction



3 non-tight security bounds

What is a profit in such bounds?

$$Adv_{Schnorr}^{uf}(A) \leq f(params) + \sqrt{q_0 Adv_{\mathbb{G}}^{dl}(A')}$$

They provide strong arguments for absence of «polynomial-time» attacks

But BE CAREFUL with choosing concrete security parameters

3 non-tight security bounds

What is a profit in such bounds?

$$Adv_{Schnorr}^{uf}(A) \leq f(params) + \sqrt{q_0 Adv_{\mathbb{G}}^{dl}(A')}$$

They provide strong arguments for absence of «polynomial-time» attacks

But BE CAREFUL with choosing concrete security parameters

Wrong way

1. Provide concrete methods analysis for basic problems/mechanisms
2. Choose parameters using only p.1

! Often practiced in PQ world

3 non-tight security bounds

What is a profit in such bounds?

$$Adv_{Schnorr}^{uf}(A) \leq f(params) + \sqrt{q_O Adv_{\mathbb{G}}^{dl}(A')}$$

They provide strong arguments for absence of «polynomial-time» attacks

But BE CAREFUL with choosing concrete security parameters

Good way [1]

1. Provide concrete methods analysis for basic problems/mechanisms
2. *Provide concrete methods analysis for scheme*
3. Choose parameters using p.1 and p. 2

Instead of conclusion!

Over 50 years of active study

Powerful instrument that should be
correctly and carefully used

Critic is always good



What to read?

1. Oded Goldreich. Foundations of Cryptography
2. Mihir Bellare and Phillip Rogaway. Introduction to Modern Cryptography
3. Dan Boneh and Victor Shoup. A Graduate Course in Applied Cryptography
4. Neal Koblitz and Alfred Menezes. "Another Look" papers
5. Seminar «Mathematical methods of cryptanalysis»
<https://yadi.sk/d/c00VAq9mhTeuFQ>





**Thank you for your
attention!**

