# On One-Pass Key Establishment

Colin Boyd

Information Security Institute
Queensland University of Technology

Joint work with Juan González and M. Choudary Gorantla

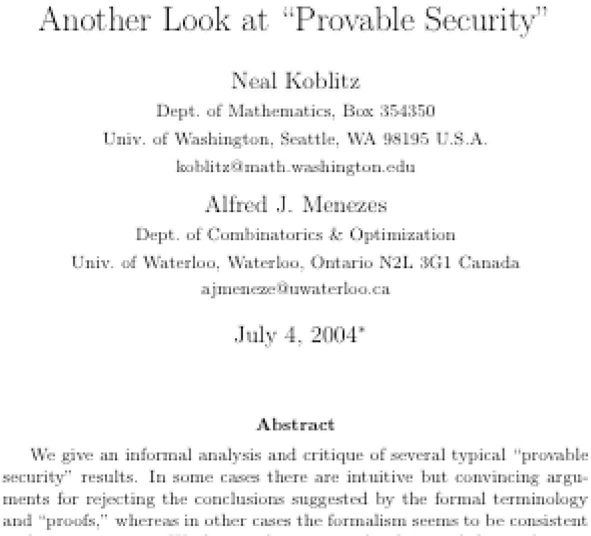
# Outline

1. A Few Comments on Provable Security
2. One-Pass Key Establishment — What and Why
    - Key establishment and one-pass variants
    - HMQV Protocol
    - Identity-Based OPKE
3. Relating One-Pass Key Establishment to Signcryption
    - Signcryption and its Security Models
    - Equivalence Theorems

# Security Reductions

1. Define what constitutes the cryptographic primitive (algorithms and their inputs and outputs)
2. Define a security model:
   - what the adversary is allowed to do (access to oracles)
   - what it means for the primitive to be secure
3. Show that if the primitive is not secure then some (presumably) hard problem can be solved

# Recent Controversy



## Another Look at “Provable Security”

Neal Koblitz
Dept. of Mathematics, Box 354350
Univ. of Washington, Seattle, WA 98195 U.S.A.
koblitz@math.washington.edu

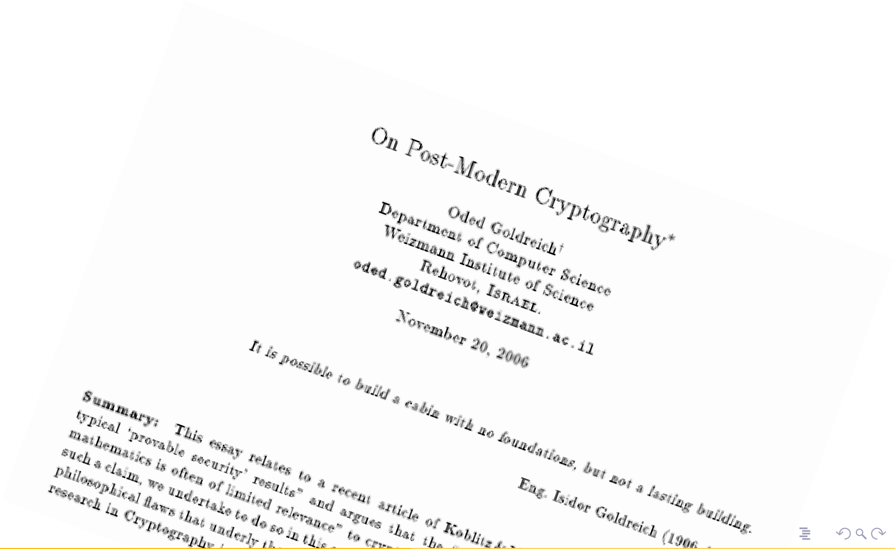
Alfred J. Menezes
Dept. of Combinatorics & Optimization
Univ. of Waterloo, Waterloo, Ontario N2L 3G1 Canada
ajmeneze@uwaterloo.ca

July 4, 2004*

**Abstract**

We give an informal analysis and critique of several typical “provable security” results. In some cases there are intuitive but convincing arguments for rejecting the conclusions suggested by the formal terminology and “proofs,” whereas in other cases the formalism seems to be consistent

# Recent Controversy



## On Post-Modern Cryptography*

Oded Goldreich†
Department of Computer Science
Weizmann Institute of Science
Rehovot, ISRAEL.
oded.goldreich@weizmann.ac.il

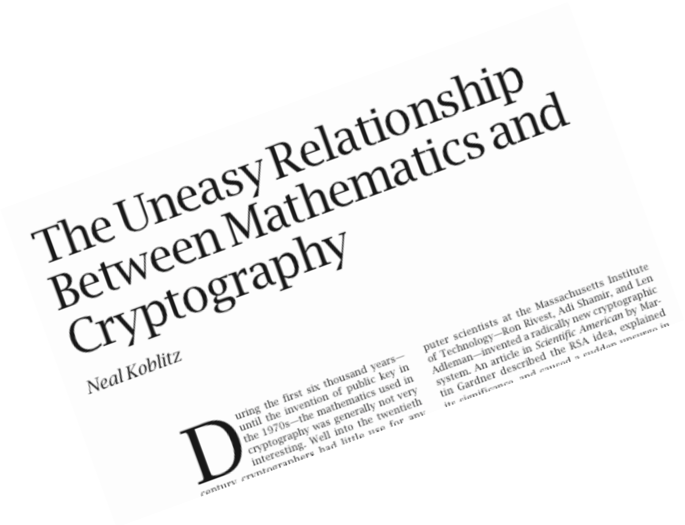
November 20, 2006

*It is possible to build a cabin with no foundations, but not a lasting building.*

Eng. Isidor Goldreich (1906

**Summary:** This essay relates to a recent article of Koblitz
typical 'provable security' results" and argues that the
mathematics is often of limited relevance" to cry
such a claim, we undertake to do so in this
philosophical flaws that underly th
research in Cryptography

# Recent Controversy



## The Uneasy Relationship Between Mathematics and Cryptography

*Neal Koblitz*

During the first six thousand years—until the invention of public key in the 1970s—the mathematics used in cryptography was generally not very interesting. Well into the twentieth century cryptographers had little use for any

puter scientists at the Massachusetts Institute of Technology—Ron Rivest, Adi Shamir, and Len Adleman—invented a radically new cryptographic system. An article in *Scientific American* by Martin Gardner described the RSA idea, explained its significance, and caused a sudden upsurge in

# Provable Security Myths

- A proof is a cast-iron guarantee of security
- Nobody reads the proofs
- The proofs are usually wrong

# Provable security = reductionist security?

> In my opinion, provable computational security is a myth! Not only do we have no proofs of computational security today, but we are so far from such proofs that it seems unlikely that we will have any in the forseeable future — if ever!

James Massey, 2006

# Dangers of Provable Security

- Too many models
- Too many assumptions
- Proofs become more important than innovation
- Most proofs are not composable

# Provable security – a personal view

- Provable (reductionist) security has two aspects:
  1. a theoretical side (computer science)
  2. a practical side (engineering)
- On the theoretical side provable security is a theory (collection of theorems)
- On the practical side provable security is a tool, one of many
- The two aspects should not be confused

# Outline

1. A Few Comments on Provable Security
2. One-Pass Key Establishment — What and Why
    - Key establishment and one-pass variants
    - HMQV Protocol
    - Identity-Based OPKE
3. Relating One-Pass Key Establishment to Signcryption
    - Signcryption and its Security Models
    - Equivalence Theorems

# One-Pass Key Establishment

- Here we identify passes and message — one-pass = one message
- One-pass key establishment (OPKE) is practical and efficient
- Only consider public key scenario
- Very many two-pass protocols
  - MTI
  - UM
  - MQV, HMQV
- These all have one-pass versions

# Models for Security of Key Establishment

- First proposed by Bellare and Rogaway (1993)
- Extensions and variations by various authors: Bellare and Rogaway 1995, Shoup 1998, Bellare, Pointcheval, Rogaway 2000, Canetti and Krawczyk 2001, LaMacchia, Lauter and Mityagin 2007, . . .
- Adversary controls multiple parties and has access to various oracles
- Supports reductionist proofs

# Properties for Key Establishment

- Indistinguishability of session key (adversary cannot distinguish session key in target session from random)
- Many users involved (allow *corrupt* queries)
- Known key security (allow *reveal* queries)
- Forward secrecy (allow *corrupt* query to target)
- Resilience to key compromise impersonation (allow *corrupt* query to partner of target)
- Resilience to compromise of ephemeral data (allow *state reveal* queries)

# Limitations of One-Pass Key Establishment

- Key *agreement* is not possible
- Recipient needs to rely on time-varying parameter to detect replays
- It is not possible to provide forward secrecy for the recipient

# Freshness in Canetti–Krawczyk Model

- Freshness in CK model relies on *session identifier* (SID)
- SID must be different for each session that adversary runs
- In practice often define SID to be concatenation of messages sent
- For OPKE this means that messages cannot be replayed!
- Seems like cheating – probably model is too weak

# Outline

1. A Few Comments on Provable Security
2. One-Pass Key Establishment — What and Why
    - Key establishment and one-pass variants
    - HMQV Protocol
    - Identity-Based OPKE
3. Relating One-Pass Key Establishment to Signcryption
    - Signcryption and its Security Models
    - Equivalence Theorems

# HMQV

- MQV protocol due to (Law,) Menezes, Qu and Vanstone, originally in 1995
- Widely implemented and standardised (including IEEE P1363)
- HMQV (hashed MQV) published by Krawczyk at Crypto 2005

"...provides the same (almost optimal) performance of MQV but also delivers, in a provable way, the original security goals of MQV (and even more)."

# HMQV

$$\begin{array}{ccc}
A & & B \\
(y_A = g^{x_A}) & & (y_B = g^{x_B}) \\
 & & \\
r_A \in_R \mathbb{Z}_q & & \\
t_A = g^{r_A} & & \\
 & \xrightarrow{\quad t_A \quad} & \\
 & & r_B \in_R \mathbb{Z}_q \\
 & & t_B = g^{r_B} \\
 & \xleftarrow{\quad t_B \quad} & \\
S_A = r_A + \bar{t}_A x_A \bmod q & & S_B = r_B + \bar{t}_B x_B \bmod q \\
Z_{AB} = (t_B y_B^{\bar{t}_B})^{S_A} & & Z_{AB} = (t_A y_A^{\bar{t}_A})^{S_B}
\end{array}$$

$\bar{t}_A = \overline{H}(t_A, B)$ and $\bar{t}_B = \overline{H}(t_B, A)$

# XCR Signature

- Krawczyk defined *exponential challenge-response* signatures as part of HMQV design
- Related to Schnorr identification protocol
- Challenger $A$ chooses message $m$ and challenge $t_A = g^{r_A}$.
- Signature produced by signer $B$ consists of the pair

  $$t_B, t_A^{r_B + \bar{t}_B x_B}$$

  where $\bar{t}_B = \overline{H}(t_B, m)$.
- Signature $(t_B, \sigma)$ is valid if $t_B \neq 0$ and $(t_B y_B^{\bar{t}_B})^{r_A} = \sigma$.
- HMQV uses two intertwined copies of XCR where $m$ is the identity of the signer (sender).

# One-pass HMQV

$$\begin{array}{ccc} A & & B \\ r_A \in_R \mathbb{Z}_q & & \\ t_A = g^{r_A} & & \\ & \xrightarrow{t_A} & \\ Z_{AB} = y_B^{r_A+\bar{t}_A x_A} & & Z_{AB} = (t_A y_A^{\bar{t}_A})^{x_B} \end{array}$$

$$\bar{t}_A = \overline{H}(t_A, A, B)$$

The shared secret is the XCR signature of $A$ on the message consisting of the identities $A, B$ using challenge $y_B$ (public key of $B$).

# Outline

1. A Few Comments on Provable Security
2. One-Pass Key Establishment — What and Why
    - Key establishment and one-pass variants
    - HMQV Protocol
    - Identity-Based OPKE
3. Relating One-Pass Key Establishment to Signcryption
    - Signcryption and its Security Models
    - Equivalence Theorems

# Identity-based cryptography

- First proposed by Shamir in 1982 in order to simplify management of public keys
- The public key can be chosen as any bit string, even before private key is known
- By choosing public key as identity of owner, no certificate is required
- Practical identity-based encryption first achieved in 2000 using bilinear mapping derived from pairings on elliptic curves

# Why ID-based OPKE?

- ID-based cryptography very fashionable?!
- Two pass ID-based key establishment (agreement) goes back to 1984
- Can make *any* two pass protocol into ID-based protocol simply by adding certificates!
- Cannot be done with OPKE — similar to why IBE is far harder to achieve than ID-based signatures
- Forward secrecy less important?

# ID-based OPKE (GBG 08)

- Pairing-based using an admissable bilinear pairing

  $$e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$$

  where $\mathbb{G}$ is an additive group and $\mathbb{G}_T$ is a multiplicative group of prime order $q$.
- The key generation centre selects a master secret $s \in_R \mathbb{Z}_q$ and an arbitrary generator $P$ of $\mathbb{G}$.
- The public key $P_{pub} \in \mathbb{G}$ is computed as $P_{pub} = sP$.
- Specify hash functions $H_1 : \{0,1\}^* \to \mathbb{G}$ and $H_2 : \mathbb{G} \times \{0,1\}^* \to \mathbb{Z}_q^*$ and a key derivation function $\mathcal{K} : \mathbb{G}_T \to \{0,1\}^k$, where $k$ is the required length of the key.

# ID-based OPKE (GBG 08)

$$\begin{array}{ccc} A & & B \\ r \in_R \mathbb{Z}_q & & \\ R = rQ_A & & \\ & \xrightarrow{R} & \\ h = H_2(R, ID_A \| ID_B) & & h = H_2(R, ID_A \| ID_B) \\ k_{AB} = e((r+h)S_A, Q_B) & & k_{BA} = e(R + hQ_A, S_B) \end{array}$$

$$k_{AB} = k_{BA} = e(Q_A, Q_B)^{s(r+h)}$$

# Security Theorem

**Theorem**

*The above ID-based OPKE protocol is secure assuming the hardness of Bilinear Diffie-Hellman (BDH) problem with $H_1$, $H_2$ and $\mathcal{K}$ modelled as random oracles.*

- Strongly related to two-pass protocol of Choo and Chow (2007)
- Choo and Chow define ID-based version of exponential challenge signature (XCR) used by Krawczyk.

# Outline

1. A Few Comments on Provable Security
2. One-Pass Key Establishment — What and Why
   - Key establishment and one-pass variants
   - HMQV Protocol
   - Identity-Based OPKE
3. Relating One-Pass Key Establishment to Signcryption
   - Signcryption and its Security Models
   - Equivalence Theorems

# Signcryption

- Achieving the following security services at the same time:
  - confidentiality
  - integrity
  - authentication
  - (non-repudiation)
- May also be called public key authenticated encryption
- Aims to save on cost of signing and encrypting separately

# Hybrid Construction

- Key Encapsulation Mechanism (KEM) generates a symmetric key $K$ and its encapsulation $C$
- Data Encapsulation Mechanism (DEM) encrypts a message through a symmetric cipher using $K$
- KEM + DEM = hybrid encryption

## Hybrid Signcryption

- Extended by Dent to signcryption
- Definitions for Outsider and Insider security (considers only insider unforgeability)
- Security notions in the two-user setting

# Signcryption KEM (SKEM)

- Generates a mutually authenticated symmetric key
- The key generated should be indistinguishable from any other key
- Should be unforgeable

# OPKE and Signcryption

- We already noted:
    - signcryption is a cryptographic primitive designed to provide confidentiality and integrity (possibly non-repudiation too) to sender data
    - signcryption often uses a KEM (key encapsulation) technique to establish a symmetric key
- Sounds very much like OPKE!
- Are the models the same?
- Can signcryption KEMs work as OPKE and *vice versa*?

# Security for Signcryption

- Signcryption is designed to provide both *confidentiality* and *unforgeability* of sender data.
- Two notions of security are considered:
  1. *Outsider security* assumes that the adversary is neither sender nor receiver.
  2. *Insider security* allows the adversary to be the sender or receiver
- Dent did not consider insider security for confidentiality

# Security for Signcryption

The models for key establishment suggest some stronger security definitions for signcryption.

- Multi-user setting rather than two user setting
- Forward secrecy can be provided through insider security for confidentiality
- State reveal queries could be allowed

# Security for signcryption KEMs

## Security notions

| | Outsider unforgeability | Insider unforgeability |
|---|---|---|
| Outsider confidentiality | Authenticated encryption | Signcryption (with non-repudiation) |
| Insider confidentiality | Forward secrecy | ? |

No signcryption KEM is known that provides both insider unforgeability and insider confidentiality

# Outline

# Equivalence Theorems (GBG 07)

**Theorem**

*If $\pi$ is a one-pass key establishment protocol SK-secure with sender forward secrecy in the CK model, then it can be used as a signcryption KEM that is secure in the insider confidentiality and outsider unforgeability notions.*

**Theorem**

*If a signcryption KEM is secure in the insider confidentiality and outsider unforgeability notions, then it can be used as a one-pass key establishment protocol $\pi$ that is SK-secure with sender forward secrecy in the CK model.*

# New signcryption KEM

By applying the second theorem we can obtain a new signcryption KEM from one-pass HMQV

- Encapsulation
  1. Choose $r \in_R Z_q^*$
  2. Set $t = g^r$
  3. Set $\bar{t} = \overline{H}(t, A, B)$
  4. Set $K = H_1((y_B)^{r + x_A \bar{t}})$
  5. $t$ is encapsulation of key $K$
- Decapsulation
  1. Set $\bar{t} = \overline{H}(t, A, B)$
  2. Set $K = H_1\left((t y_A^{\bar{t}})^{x_B}\right)$
  3. Output $K$

# Compromise of Ephemeral Data

- Session state reveal queries allow ephemeral protocol data to become available to adversary
- Is this reasonable for one-pass protocols?
- No existing signcryption KEM can allow this sort of query

# Summary

- A new ID-based one-pass protocol — a useful new primitive?
- A duality between OPKE and signcryption KEM
- Future work:
  - can we unify more models?
  - are our models as strong as they could and should be?

# References

- Ivan Damgård A “proof-reading” of Some Issues in Cryptography, ICALP, Lecture Notes in Computer Science, Vol. 4596, pp. 2-11, Springer, 2007.
- A. W. Dent. Fundamental problems in provable security and cryptography. In Phil Trans R Soc A, vol. 364, no. 1849, pp. 3215–3230, 2006. `http://www.isg.rhul.ac.uk/~alex/papers/roysoc.pdf`
- Neal Koblitz and Alfred Menezes, Another Look at “Provable Security”, Journal of Cryptology, Vol. 20, 2007.
- Neal Koblitz, The Uneasy Relationship Between Mathematics and Cryptography, Notices of the American Mathematical Society, Vol. 54, 2007. `http://www.ams.org/notices/200708/tx070800972p.pdf`

# References

- Hugo Krawczyk, HMQV: A High-Performance Secure Diffie-Hellman Protocol, CRYPTO, LNCS Vol. 3621, pp. 546-566, Springer, 2005.
- James L. Massey, Provable Security — Myth or Reality (slides only), `http://ispec2006.i2r.a-star.edu.sg/Massey_Provable%20Security%20Myth%20or%20Reality.pdf`
- M. Choudary Gorantla, Colin Boyd, Juan González, On the Connection between Signcryption and One-Pass key Establishment, Eleventh IMA International Conference on Cryptography and Coding, Springer 2007, to appear.
- M. Choudary Gorantla, Colin Boyd and Juan González. ID-based One-pass Authenticated Key Establishment, AISC 2008, to appear.