

A generalization of DDH with applications to protocol analysis and computational soundness

Emmanuel Bresson¹, Yassine Lakhnech², Laurent Mazaré³,
Bogdan Warinschi⁴

DCSSI Crypto Lab, emmanuel@bresson.org

VERIMAG Grenoble, yassine.lakhnech@imag.fr

Amadeus SAS, laurent.mazare@m4x.org

University of Bristol, bogdan@cs.bris.ac.uk

November 8, 2007

Generalizing DDH

$$\text{DDH: } (g, g^x, g^y, g^{xy}) \approx (g, g^x, g^y, g^z)$$

- From 2-party to multi-party key exchange: Group Diffie-Hellman [[Ste96](#), [BCP02b](#)]
 - given $g^{\prod_i x_i}$, for up to $n - 1$ exponents, decide $g^{x_1 \cdots x_n}$ vs. g^r
- More general polynomials expressions [[Kil01](#)]
 - g^a and g^b , and a (single) challenge $g^{P(a,b)}$
- Other extensions:
 - General Diffie-Hellman Exponent (GDHE) [[BBG05](#)]
 - Square Exponent [[MW96](#), [CS00](#), [Shp02](#)]
 - Inverse Exponent [[SS01](#)]

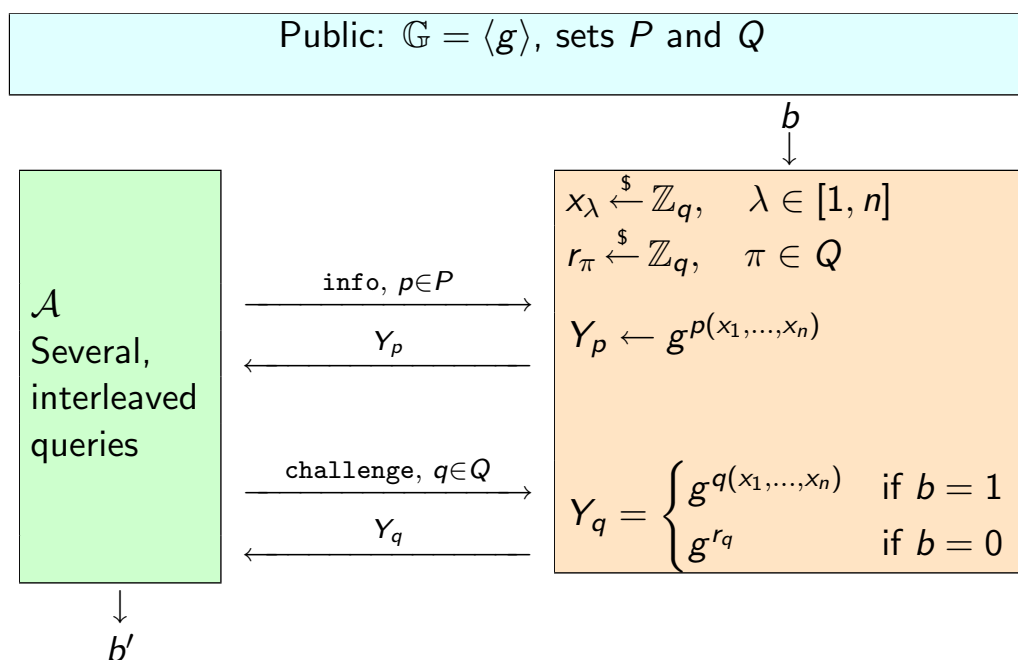
Our Generalization of DDH

- 1 Adversary sees some $g^{p(x_1, x_2, \dots, x_n)}$, where p in a fixed set P of power-free polynomials
 - *polynomials* instead of *monomials*

- 2 Adversary receives challenges $g^{q(x_1, x_2, \dots, x_n)}$, where q in a fixed set Q of power-free polynomials
 - multiple challenges allowed
 - can be interleaved with $g^{p(x_1, x_2, \dots, x_n)}$

- 3 Adversary must decide between challenges and random elements

The (P, Q) -DDH Experiment



Our Main Result

Theorem (Informal)

Under conditions on P and Q that we identify, the (P, Q) -DDH problem is:

- either trivial
- or hard provided the DDH assumption holds in \mathbb{G}
- or impossible (unconditionally hard)

More formally: $\mathbf{Adv}^{(P,Q)\text{-DDH}} \leq \Lambda \cdot \mathbf{Adv}^{\text{DDH}}$

\implies loss factor Λ to be studied...

Applications of our Result

Application to protocols security

Key exchange

- direct/better proofs for previous assumptions (GDDH)
- “one-line” proof of Burmester-Desmedt

Computational Soundness

- symbolic, mechanical reasoning about protocols
- symbolically derived results imply cryptographic security

Extension of Abadi-Rogaway symbolic language [AR00]

- incorporate DH-like keys (previously missing)
- symbolic proofs of indistinguishability

(Non)-Trivial Challenges

Sometimes (P, Q) -DDH is trivial:

- eg, $P = \{x_1, x_2\}$ and $Q = \{x_1 + x_2\}$
- **We restrict to linearly independent P and Q**

Definition (Non-trivial challenge)

Challenge (P, Q) is **non-trivial** if $\text{Span}(P) \cap \text{Span}(Q) = \{0\}$ and polynomials in Q are linearly independent.

Impossible Challenges

Other extreme: adversary has 0 advantage

- eg, $P = \{x_1, x_2, x_1x_2\}$ and $Q = \{x_3\}$

Definition (Impossible challenge)

Challenge (P, Q) is **impossible** if for **any** adversary \mathcal{A} ,
 $\text{Adv}_{\mathcal{A}}^{(P,Q)\text{-DDH}} = 0$

Intuitively: *cannot “reach” polynomials in Q from those in P*

- We formally identify such condition in the paper

Proving the “Main” Part of the Theorem

Use ℓ successive transformations from a non-trivial challenge (P, Q) into an impossible one

If \mathcal{A} succeeds in the original challenge significantly better than in the final one, then DDH is easy

Theorem

Let (P, Q) be a non-trivial challenge. Assume the adversary makes at most N oracle queries. Then (P, Q) - DDH is (ϵ, t) -hard, with

$$\epsilon = 2\ell \cdot \epsilon_{DDH} \quad \text{and} \quad t_{DDH} = t + N \cdot t_{\text{oracle}}$$

Proving the Theorem — Strategies

Build a sequence of challenges $(P_0, Q_0), \dots, (P_\ell, Q_\ell)$:

- 1 Start from $(P, Q) = (P_0, Q_0)$ on variables X_1, \dots, X_n
- 2 Obtain (P_{i+1}, Q_{i+1}) out of (P_i, Q_i) :
 - select X_u and X_v occurring in a monomial $m \in \text{mon}(P \cup Q)$
 - merge them into a new variable $X_{u \cup v}$

$$\forall \mathcal{A}, \exists \mathcal{B} : \mathbf{Adv}_{\mathcal{A}}^{(P_i, Q_i)\text{-DDH}} \leq 2 \cdot \mathbf{Adv}_{\mathcal{B}}^{DDH} + \mathbf{Adv}_{\mathcal{A}}^{(P_{i+1}, Q_{i+1})\text{-DDH}}$$

- 3 (P_ℓ, Q_ℓ) is an impossible challenge on variables X_1, \dots, X_{2^n}

Improving the Tightness

The Random Self-Reducibility (RSR) property comes into play:

All “independence” of variables allows to use a single *DDH* challenge to deal with all the steps (X_{u_i}, X_{v_i}) at once

—details omitted

Limitation: in the worst case, the loss of security may be exponential

- a factor $2^{\#(\text{“bad” monomials})}$. . .

Most often the set of “bad” elements is empty: linear loss!

Application: Group Key Exchange

Applications to Key Exchange Protocols

Group Diffie-Hellman (GDDH): challenge (P, Q) :

- $P = \{\prod_{i \in E} X_i \mid E \subsetneq [1, n]\}$, that is, P contains all the monomials of order up to $n - 1$
 - $Q = \{\prod_{1 \leq i \leq n} X_i\}$
- 1 $\text{Span}(P) \cap \text{Span}(Q) = \{0\}$
 - 2 P and Q contain only monomials

The reduction is linear !

$$\epsilon' = 2(n - 1)\epsilon_{DDH}$$

The Burmester-Desmedt Protocol [BD94, KY03]

Overview of the protocol:

- 1 Each U_i broadcasts g^{X_i}
- 2 Each U_i broadcasts $g^{X_i X_{i+1} - X_{i-1} X_i}$
- 3 The common secret is $g^{X_1 X_2 + \dots + X_n X_1}$.

Security analysis in the passive setting:

- Adversary observe transcripts (Execute queries)
- Adversary try to distinguish a key (Test query)
- These queries can be intertwined

This actually corresponds to (P, Q) -DDH assumption

- $P = \{X_i\}_{1 \leq i \leq n} \cup \{X_i X_{i+1} - X_{i-1} X_i\}_{1 \leq i \leq n}$: broadcasted stuff
- $Q = \{\sum_{i=1}^n X_i X_{i+1}\}$: the shared secret

$$\text{Span}(P) \cap \text{Span}(Q) = \{0\}, |Q| = 1$$

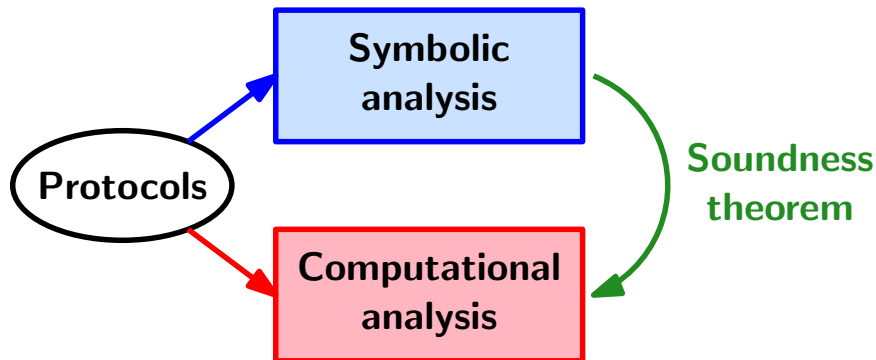
Theorem gives $\epsilon' = 2n\epsilon_{DDH}$

Not optimal: use Random Self-Reducibility

⇒ Obtain improved bounds matching **[BD94, KY03]**

Application: Computational
Soundness

Application to Symbolic Logic



We propose a symbolic language that includes exponentiation
Allows *automatic* reasoning on indistinguishability of distributions

Computational Soundness — Motivation

Three-party protocol (F is an arbitrary expression):

$$E(F) = (g^{X_1}, g^{X_2}, g^{X_3}, \{F\}_{h(g^{X_1 X_2 X_3})})$$

More sophisticated: Burmester-Desmedt

$$E(F) = (g^{X_1}, g^{X_2}, g^{X_3}, g^{X_3 X_1 - X_1 X_2}, g^{X_1 X_2 - X_2 X_3}, g^{X_2 X_3 - X_3 X_1}, \{K\}_{h(g^{X_1 X_2 + X_2 X_3 + X_3 X_1})}, \{F\}_K)$$

For security it suffices to show that $E(F)$ and $E(0)$ are “indistinguishable”

Our Symbolic Syntax

Start from **Keys**, **Nonce** and **Exponents**

Let **Poly** := power-free polynomials on **Exponents**

Define **Msg** set of expressions: $g^{\text{Poly}} \mid (\text{Msg}, \text{Msg}) \mid \{\text{Msg}\}_{\text{Keys}}$

Security is captured *via* a deduction relation \vdash [DY83]

Rules:

$$\frac{E \vdash \{m\}_K \quad E \vdash K}{E \vdash m} \quad \dots$$

Additional rules:

$$\frac{E \vdash g^p \quad E \vdash g^q}{E \vdash g^{\lambda p + q}} \quad \lambda \in \mathbb{Z}_q$$

Equivalence vs Associated Distributions

Each expression has a **pattern** = information revealed via the \vdash relation [AR00, Mic05]

E_1, E_2 symbolically equivalent: $E_1 \equiv E_2$, if same pattern

Defined inductively: $pat((E', E'')) = (pat(E'), pat(E''))$, etc.

Each expression E maps to a distribution \hat{E} on bitstrings

- Induced by sampling **Keys**, **Nonce**, **Exponents** in appropriate space
- Computed in an inductive manner

Soundness Theorem

Theorem (Symbolic equivalence implies indistinguishability)

Let E_1 and E_2 be two arbitrary expressions. If $E_1 \equiv E_2$ (symbolically equivalent), then $\widehat{E}_1 \approx \widehat{E}_2$ (computationally indistinguishable).

Polynomials however need more care...

On the Equivalence Condition

Some subtleties in defining equivalence for expressions that contain polynomials...

DDH: identify $E_1 = (g^{X_1}, g^{X_2}, g^{X_1 X_2})$ and $E_2 = (g^{X_1}, g^{X_2}, g^{X_3})$ by renaming polynomial $X_1 X_2$ to X_3

Renamings of polynomials are not all valid:

- E_1 and $E_3 = (g^{X_1}, g^{X_2}, g^{X_1 + X_2})$: distinguishable, **should not** be made indistinguishable by a mapping $X_1 X_2$ to $X_1 + X_2$

Soundness Theorem

We define **Equivalence up to Renaming** (denoted $E_1 \cong E_2$) as a relaxed equivalence notion, in which linear dependency of polynomials is preserved.

Theorem (Symbolic equivalence implies indistinguishability)

Let E_1 and E_2 be acyclic expressions. If $E_1 \cong E_2$, then $\widehat{E}_1 \approx \widehat{E}_2$.

Acyclic expressions: avoid encryptions in which plaintext and key are linearly dependent, as in $\{g^{X_1}, g^{X_1+X_2}\}_{h(g^{X_2})}$

Soundness Theorem — Illustration

$$E(F) = (g^{X_1}, g^{X_2}, g^{X_3}, g^{X_3X_1 - X_1X_2}, g^{X_1X_2 - X_2X_3}, g^{X_2X_3 - X_3X_1}, \{K\}_{h(g^{X_1X_2 + X_2X_3 + X_3X_1})}, \{F\}_K)$$

with F an arbitrary expression.

It is now clear how to prove the security automatically:

- Use the (P, Q) -DDH assumption to transform the expression into a “*equivalent-up-to-renaming*” one
- The obtained expression $E'(F)$ is trivially equivalent to $E'(0)$
- Use the soundness theorem to go to the computational world!

Conclusion

In this paper we propose

- a significant generalization of the DDH problem
 - essentially not harder than standard DDH

We offer two applications:

- simple and tight security proofs for key exchange protocols
- a computational soundness theorem that deals with exponentiation and Diffie-Hellman-like keys

In progress: how to extend this last result to the case of active adversaries

talk \vdash question

answer \vdash satisfaction

References I



M. Abadi and P. Rogaway.

Reconciling two views of cryptography (the computational soundness of formal encryption).
In *IFIP TCS2000*, pp. 3–22.



F. Bao, R. Deng, and H. Zhu.

Variations of Diffie-Hellman problem.
In *ICICS 2003*, pp. 301–312.



M. Blum and S. Micali.

How to generate cryptographically strong sequences of pseudo-random bits.
SIAM J. of Computing, 13:850–864, 1984.



D. Boneh, X. Boyen, and E.-J. Goh.

Hierarchical identity based encryption with constant size ciphertext.
In *EUROCRYPT '05*, pp. 440–456.



E. Bresson, O. Chevassut, and D. Pointcheval.

Group Diffie-Hellman key exchange secure against dictionary attacks.
In *ASIACRYPT '02*, pp. 497–514.



E. Bresson, O. Chevassut, and D. Pointcheval.

Dynamic group Diffie-Hellman key exchange under standard assumptions.
In *Eurocrypt 02*, pp. 321–336.



E. Bresson, O. Chevassut, and D. Pointcheval.

The group Diffie-Hellman problems.
In *SAC 2002*, pp. 325–338.

References II



M. Burmester and Y. Desmedt.

A secure and efficient conference key distribution system (extended abstract).
In *EUROCRYPT '94*, pp. 275–286.



R. Canetti.

Towards realizing random oracles: Hash functions that hide all partial information.
In *CRYPTO '97*, pp. 455–469.



D. Coppersmith and I. Shparlinski.

On polynomial approximation of the discrete logarithm and the Diffie-Hellman mapping.
J. of Cryptology, 13(2):339–360, 2000.



R. Cramer and V. Shoup.

A practical public key cryptosystem provably secure against adaptive chosen ciphertext attack.
In *CRYPTO '98*, pp. 13–25.



W. Diffie and M. Hellman.

New directions in cryptography.
IEEE Trans. on Information Theory, IT-22(6):644–654, November 1976.



D. Dolev and A. Yao.

On the security of public key protocols.
IEEE IT, 29(12):198–208, 1983.



T. ElGamal.

A public key cryptosystem and a signature scheme based on discrete logarithm.
IEEE IT, 31(4):469–472, 1985.

References III



J. Katz and M. Yung.

Scalable protocols for authenticated group key exchange.
In *CRYPTO '03*, pp. 110–125.



E. Kiltz.

A tool box of cryptographic functions related to the Diffie-Hellman function.
In *Indocrypt '01*, pp. 339–350.



U. Maurer and S. Wolf.

Diffie-Hellman oracles.
In *CRYPTO '96*, pp. 268–282.



D. Micciancio and S. Panjwani.

Adaptive security of symbolic encryption.
In *TCC 2005*, pp. 245–263.



M. Naor and O. Reingold.

Number-theoretic constructions of efficient pseudo-random functions.
In *FOCS '97*, pp. 458–467.



A.-R. Sadeghi and M. Steiner.

Assumptions related to discrete logarithms: Why subtleties make a real difference.
In *EUROCRYPT '01*, pp. 244–261.



V. Shoup.

Lower bounds for discrete logarithms and related problems.
In *EUROCRYPT '97*, pp. 256–266.

References IV



I. Shparlinski.

Security of most significant bits of g^{x^2} .
IPL, 83(2):109–113, 2002.



M. Steiner, G. Tsudik, and M. Waidner.

Diffie-Hellman key distribution extended to group communication.
In *ACM CCS 96*, pp. 31–37.