

# DESIGN AND ANALYSIS OF HUMAN IDENTIFICATION PROTOCOLS

By

Hassan Jameel Asghar

A THESIS SUBMITTED TO MACQUARIE UNIVERSITY  
FOR THE DEGREE OF  
DOCTOR OF PHILOSOPHY  
DEPARTMENT OF COMPUTING, FACULTY OF SCIENCE  
MAY 2012



MACQUARIE  
UNIVERSITY  
FACULTY OF SCIENCE



This thesis is submitted in fulfillment of the requirements of the degree of Doctor of Philosophy at Macquarie University. I certify that this work has not been submitted for a higher degree to any other university or institution. To the best of my knowledge, all sources of information used in the preparation of this thesis have been acknowledged and the utilization of others' works, wherever applicable, has been properly cited.

---

Hassan Jameel Asghar



# Abstract

Human identification protocols are authentication protocols that enable a human using an insecure terminal to authenticate to a remote server. The goal of such protocols is to ensure secure authentication in the presence of an adversary who can not only view the user's inputs, and the internal computations and display of the terminal, but also eavesdrop on the communication link between the terminal and the server. An active adversary can in addition actively interfere with this communication link. However, protocols secure against active adversaries fall well short of usability. As a result, the focus of recent research has been on security against passive adversaries. Traditional authentication methods such as password-based authentication are not secure under this model, since the adversary can impersonate the user by learning the user's password after observing a single authentication session.

Since the introduction of the problem by Matsumoto and Imai in 1991, there have been sporadic attempts at constructing secure human identification protocols. However, to date there is no accepted solution, mainly because such protocols require mental computations from humans, and therefore the tradeoff between security and usability is huge. State-of-the-art protocols take between one to three minutes for authentication, but guarantee stronger security than traditional authentication methods. While this authentication time is not acceptable for most practical purposes, many interesting new mathematical problems and ideas have resulted in search for usable protocols.

This thesis aims to further the research in human identification protocols by focusing on the mathematical and analytical aspects of such protocols. We generalize some aspects of these protocols by analyzing their general structure. We give detailed security analysis of two protocols from literature, showing that without a thorough security analysis, these protocols are vulnerable to simple but innovative attacks. We also give the construction of two protocols with detailed security analysis and clearly defined design goals. Finally, we analyze the link between fixed-parameter intractability and human identification protocols. It is suggested that problems that are fixed-parameter intractable can be natural candidates for primitives in human identification protocols.



# Acknowledgements

For all the delightful discussions, constructive criticism and auspicious advice, I am grateful to Josef Pieprzyk, whose keen interest in this area of research kept my motivation rolling. I am greatly indebted to Shujun Li, who has been my research partner for a major portion of this thesis, and whose contribution, commentary and (at times, cold) criticism has polished this research to its current quality. Indeed, he is the main contributor to the work presented in Chapter 3.

I am also thankful to Huaxiong Wang for his encouragement and suggestions for improvement on an important component of this thesis, without which that part was dead and buried. I would also like to thank Ron Steinfeld for his help in improving a crucial piece of work in this thesis by pointing me to new areas of research in applied mathematics and cryptography, thus making me dig deep into unfamiliar mathematical territory despite my efforts to the contrary.

I am also grateful to my parents, not the least for refraining from exerting too much pressure on me to quickly complete my studies. Likewise, I am thankful to my brother and sister, who with high probability, won't bother reading this thesis. Special thanks to my circle of friends, of which the Internet, due to its immense knowledge, is a salient member.





# List of Publications

- S. Li, H. J. Asghar, J. Pieprzyk, A.-R. Sadeghi, R. Schmitz, and H. Wang. *On the Security of PAS (Predicate-Based Authentication Service)*. In *Proceedings of ACSAC '09*, pp. 209-218, (IEEE Computer Society, 2009).
- H. J. Asghar, J. Pieprzyk, and H. Wang. *A New Human Identification Protocol and Coppersmith's Baby-Step Giant-Step Algorithm*. In *Proceedings of ACNS '10*, vol. 6123, pp. 349-366, (Springer-Verlag, Berlin, 2010).
- H. J. Asghar, S. Li, J. Pieprzyk, and H. Wang. *Cryptanalysis of the Convex Hull Click Human Identification Protocol*. In *Proceedings of ISC '10*, vol. 6531, pp. 24-30, (Springer-Verlag, Berlin, 2011).
- H. J. Asghar, J. Pieprzyk, and H. Wang. *On the Hardness of the Sum of  $k$  Mins Problem*. *The Computer Journal* **54**, 1652 (2011).



# Contents

<b>Abstract</b>	<b>v</b>
<b>Acknowledgements</b>	<b>vii</b>
<b>List of Publications</b>	<b>ix</b>
<b>List of Figures</b>	<b>xv</b>
<b>List of Tables</b>	<b>xvii</b>
<b>1 Introduction</b>	<b>1</b>
<b>2 Preliminaries and Related Work</b>	<b>9</b>
2.1 Notation . . . . .	9
2.2 Human Identification Protocols . . . . .	10
2.2.1 Challenge-Response Protocols . . . . .	11
2.2.2 Security Definitions . . . . .	12
2.3 Some General Results and Attacks . . . . .	13
2.3.1 Random Guesses . . . . .	13
2.3.2 Information Theoretic Bound on $m$ . . . . .	14
2.3.3 Computational Security . . . . .	16
2.4 An Example Protocol . . . . .	17
2.4.1 Security Analysis . . . . .	17
2.4.2 Implementation . . . . .	19
2.5 Related Work . . . . .	22
<b>3 Security Analysis of PAS (Predicate-based Authentication Service)</b>	<b>29</b>
3.1 Predicate-based Authentication Service . . . . .	29
3.2 Re-Evaluating Security and Usability . . . . .	34
3.2.1 Security against Brute Force Attack Targeting Predicates . . . . .	35
3.2.2 Security against Brute Force Attack Targeting Password . . . . .	36
3.2.3 Security against Random Guess Attack . . . . .	37
3.2.4 Security against SAT Attack . . . . .	37
3.2.5 Usability . . . . .	38
3.3 A Probabilistic Attack . . . . .	39
3.3.1 Description of the Attack . . . . .	40

3.3.2	Theoretical Analysis . . . . .	41
3.3.3	Time Complexity of the Attack . . . . .	45
3.3.4	Experimental Results . . . . .	45
3.3.5	Consequences of the Probabilistic Attack . . . . .	46
3.4	Conclusion . . . . .	47
<b>4</b>	<b>Security Analysis of CHC (Convex Hull Click)</b>	<b>49</b>
4.1	The CHC Human Identification Protocol . . . . .	50
4.1.1	The Protocol . . . . .	51
4.1.2	Mitigating Random Guesses . . . . .	52
4.2	Attack 1: Difference in Distributions . . . . .	53
4.3	Number of Candidates Satisfying a Challenge-Response Pair . . . . .	56
4.4	Attack 2 . . . . .	58
4.4.1	The Attack . . . . .	59
4.4.2	Simulation Results for Attack 2 . . . . .	62
4.4.3	Why does Attack 2 Work . . . . .	62
4.4.4	Impersonation using Attack 2 . . . . .	67
4.4.5	Discussion . . . . .	70
4.5	Conclusion . . . . .	71
<b>5</b>	<b>Protocol Construction 1: Kangaroo Hopping</b>	<b>73</b>
5.1	Proposed Protocol . . . . .	74
5.1.1	User Friendly Implementations . . . . .	74
5.1.2	Different Ways of Computation . . . . .	75
5.2	Security Analysis . . . . .	76
5.2.1	Some Obvious Attacks . . . . .	77
5.2.2	Algebraic Interpretation . . . . .	78
5.2.3	Time-Memory Tradeoff . . . . .	80
5.2.4	Comparative Time Complexities . . . . .	83
5.2.5	Significance of the Jump Constant $a$ . . . . .	83
5.3	Usability Analysis . . . . .	86
5.3.1	Handling Errors . . . . .	87
5.3.2	Suggested Values of Parameters . . . . .	87
5.4	Conclusion . . . . .	88
<b>6</b>	<b>Protocol Construction 2: Counting Edges</b>	<b>91</b>
6.1	Fixed-Parameter Intractable Problems . . . . .	92
6.2	The Counting Edges Protocol: First Construction . . . . .	93
6.3	Security Analysis . . . . .	94
6.3.1	Impersonation without the knowledge of $K$ . . . . .	94
6.3.2	Randomly Guessing the Secret . . . . .	95
6.3.3	Finding $K$ . . . . .	95
6.4	Drawbacks of the Basic Protocol . . . . .	97
6.5	The Counting Edges Protocol: Main Construction . . . . .	100
6.6	Security Analysis . . . . .	100

6.6.1	Fine-tuning Protocol Parameters . . . . .	101
6.6.2	Meet-in-the-middle Attack . . . . .	102
6.6.3	Attacks from Coding Theory . . . . .	102
6.6.4	Coskun and Herley's Divide-and-Conquer Attack . . . . .	104
6.7	Usability Analysis . . . . .	104
6.8	Conclusion . . . . .	105
<b>7</b>	<b>Fixed-Parameter Intractable Problems in Human Identification Pro-</b>	
	<b>ocols</b>	<b>107</b>
7.1	A Motivating Example: The HB Protocol . . . . .	108
7.2	Parameterized Complexity Theory . . . . .	109
7.2.1	Parameterized Counting Problems . . . . .	111
7.3	The Sum of $k$ Mins Protocol . . . . .	111
7.3.1	The Sum of $k$ Mins Problem . . . . .	112
7.3.2	The Protocol . . . . .	112
7.3.3	Matrix Representation . . . . .	113
7.3.4	Generalized Sum of $k$ Mins . . . . .	114
7.3.5	Modular Sum of $k$ Mins . . . . .	118
7.3.6	A Short Digression: The Case when $d = 2$ . . . . .	121
7.4	HB and the Example Protocol . . . . .	123
7.5	The Counting Edges Protocol . . . . .	123
7.6	The Foxtail Protocol . . . . .	124
7.7	Conclusion . . . . .	127
<b>8</b>	<b>Conclusion and Future Research Directions</b>	<b>129</b>
<b>A</b>	<b>Appendix</b>	<b>137</b>
A.1	Turk's Method of Generating a Random Point Inside a Triangle . . . . .	137
A.2	Optimum Value of $m$ . . . . .	137
A.3	Graphs . . . . .	139
A.4	Coding Theory . . . . .	140
A.5	Coskun and Herley's Attack . . . . .	141
A.5.1	The Attack on Counting Edges Protocol . . . . .	142
	<b>References</b>	<b>149</b>



# List of Figures

1.1	Authentication under Matsumoto and Imai's threat model. . . . .	2
2.1	A challenge and response from the Example Protocol. . . . .	20
2.2	An iteration of Matsumoto and Imai's protocol. . . . .	23
3.1	A challenge and response table from PAS. . . . .	32
4.1	The convex hull of a set of points $\Pi$ . . . . .	50
4.2	One iteration of the Convex Hull Click protocol. . . . .	52
4.3	The distribution of $P$ . . . . .	57
4.4	The 2 partitions $\Pi_1$ and $\Pi_2$ . . . . .	64
4.5	The high and low frequency regions. . . . .	65
4.6	A simulation run showing the low and high frequency regions. . . . .	67
5.1	An example challenge grid. . . . .	76
5.2	The jump constant $a$ makes the distribution nearly uniform over $n$ . . .	85
6.1	Two graphs $G_1$ and $G_2$ on the vertex set $V = \{1, 2, 3, 4\}$ . . . . .	98
6.2	An example implementation of the basic Counting Edges Protocol. . .	99
A.1	A simple undirected graph $G$ . . . . .	140
A.2	$k - e$ icons between $s$ and $s'$ are the same, and $e$ are different. . . . .	142
A.3	Graphical illustration of neighbours of $s'$ . . . . .	145





# List of Tables

2.1	Suggested parameter values for the Example Protocol. . . . .	21
3.1	List of parameters/notations used in the description of PAS. . . . .	33
3.2	The security of PAS, estimated by Bai et al. . . . .	34
3.3	Re-evaluated security of PAS against three attacks. . . . .	35
3.4	The ratio of sizes of re-represented versus original password space. . . .	37
3.5	The minimal value of $\hat{t}$ against $q$ to ensure $\Pr[ \mathbb{C}^*  = 1] \geq q$ . . . . .	43
3.6	Lower bounds of $\Pr [\max_{i=2}^N(\#(O_i)) \leq \#(O_1) + \hat{t}]$ against $\hat{t}$ . . . . .	44
3.7	Theoretical upper bounds of $E[N_{max}]$ and estimated values. . . . .	45
3.8	Success rate of finding the secret and estimated number of candidates. .	46
4.1	Simulation results for Attack 1. . . . .	55
4.2	Values of $\gamma$ . . . . .	58
4.3	Expected and actual values of the number of combinations and labels. .	61
4.4	Output of Attack 2. . . . .	63
4.5	Output of the Chosen Test Set Attack. . . . .	68
5.1	The time and space complexity of the time-memory tradeoff attack. . .	83
5.2	Time complexity of time-memory tradeoff attacks on three protocols. .	84
5.3	The statistical distance $\Delta(Q, U)$ against $n$ and $k$ . . . . .	86
5.4	Suggested parameter values for the Kangaroo Hopping Protocol. . . . .	88
6.1	Suggested values of parameters for the Counting Edges Protocol. . . . .	105
7.1	The min function in $\mathbb{Z}_2$ is simply bit multiplication. . . . .	122
A.1	Number of neighbours with differences $e - 1$ , $e$ and $e + 1$ . . . . .	146

