Robust Privacy-Preserving Fingerprint Authentication

Ye Zhang and Farinaz Koushanfar

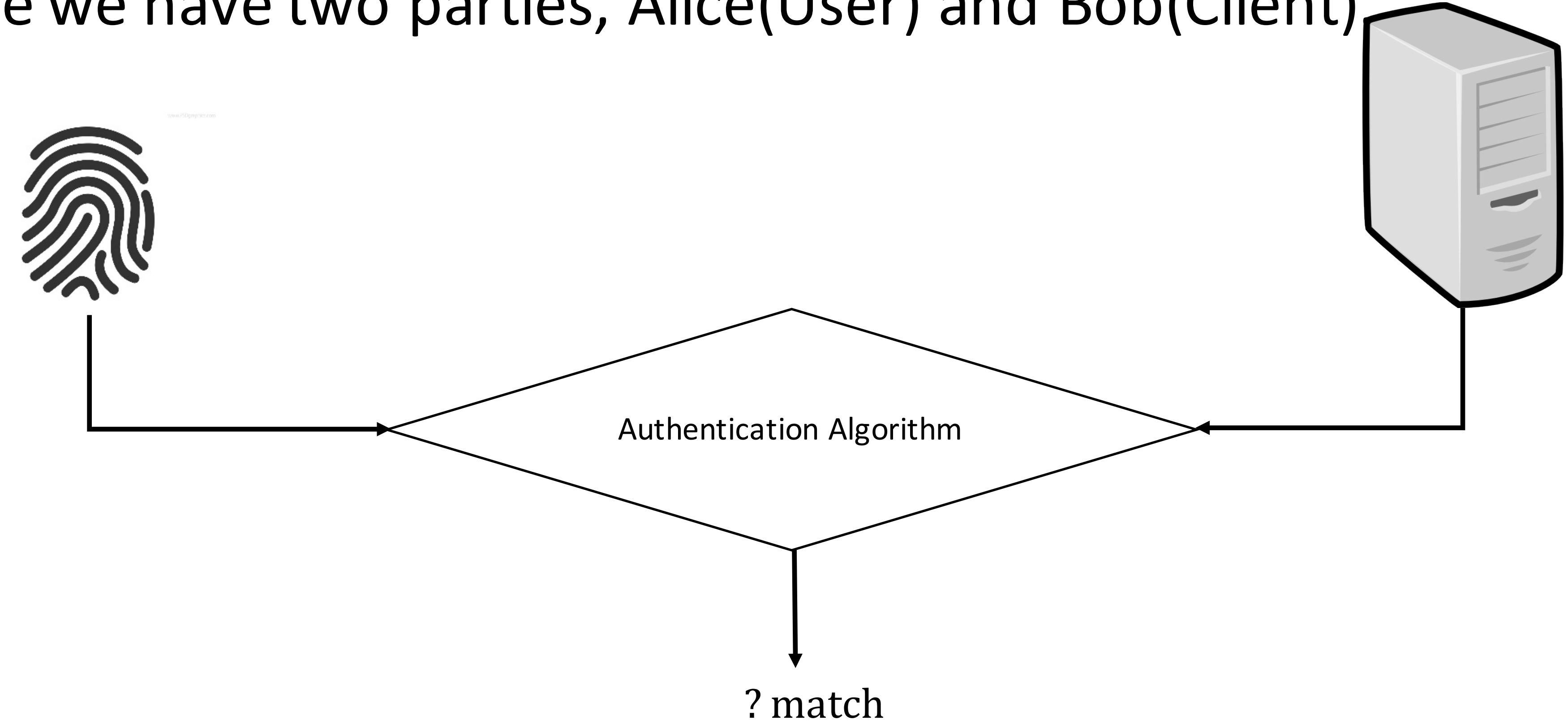
Rice University and University of California, San Diego

May 3rd, 2016

Problem Statement

Privacy Concerns: mutually untrusted parties

Suppose we have two parties, Alice(User) and Bob(Client)



Security Model

- Authentication algorithm is publicly available
- Threshold r_s is privately held by Bob

- After the authentication:
  - Alice learns a 0/1 result
  - Both parties know nothing more than what the protocol reveals to them

- Semi-honest model

Prior Work

- M. Blanton *et.al.* 2015
  - Minutiae:
    - Location(x,y) and Orientation(t)
  - Metrics: Euclidean Distance
  - Privacy preservation: Yao's Garbled Circuits(GC)

  - Matching algorithm → Unreliable

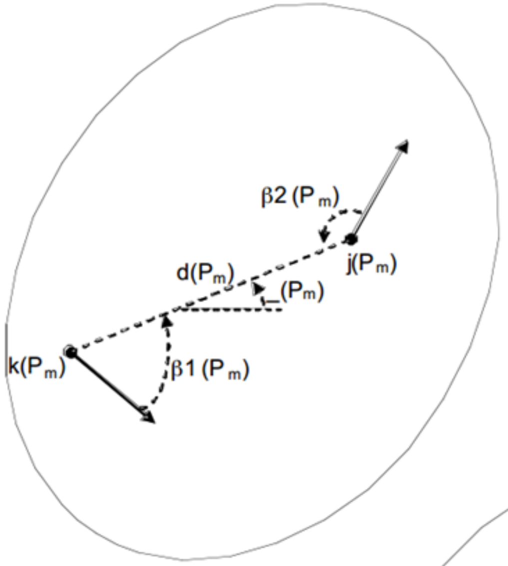
$\{x, y, t\}$

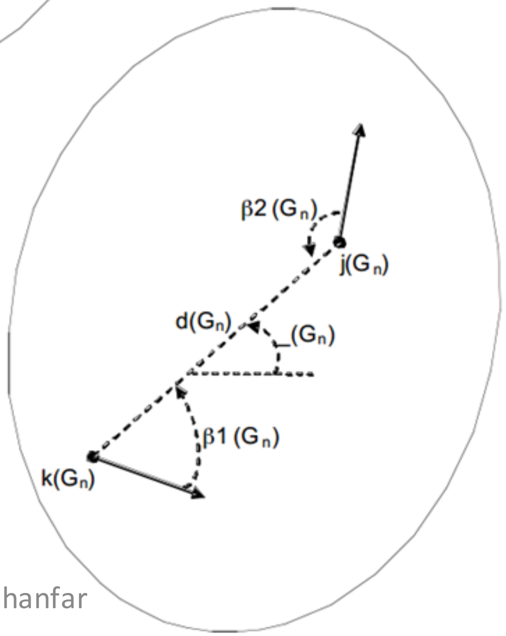
[1] M. Blanton et al., "Secure and Efficient Iris and Fingerprint Identification," Cambridge Scholars Publishing, 1 2015,ch.~9

Outline

- Motivation – Practical Methodology
  - Reliability
  - Efficiency
  - Scalability
- Our Approach:
  - Minutiae based algorithm – Customized Bozorth Matcher
  - Privacy-preserving Protocol
  - Implementation and Evaluation
- Privacy-Preservation: Yao's GC

Bozorth Algorithm – Step1





- Construct Minutia-pair comparison tables for two fingerprints

- d_{ij} → relative distance
- β_1, β_2 → relative angles
- i, j → indices of a minutia-pair
- θ_{ij} → global orientation

- Minutia file $\{x, y, t\}$ → Compatibility table $\{d_{ij}, \beta_1, \beta_2, i, j, \theta_{ij}\}$

Bozorth Algorithm – Step2

- Construct a minutia-pair compatible table

- A compatible minutia-pair is determined by:
  - $\Delta_d\big(d(P_m), d(G_n)\big) < T_d$
  - $\Delta_\beta\big(\beta 1(P_m), \beta 1(G_n)\big) < T_\beta$
  - $\Delta_\beta\big(\beta 2(P_m), \beta 2(G_n)\big) < T_\beta$

- $\{\Delta(\theta_{ij,c}, \theta_{ij,s})\ , i_c, j_c, i_s, j_s, \}$

Bozorth Algorithm – Step3

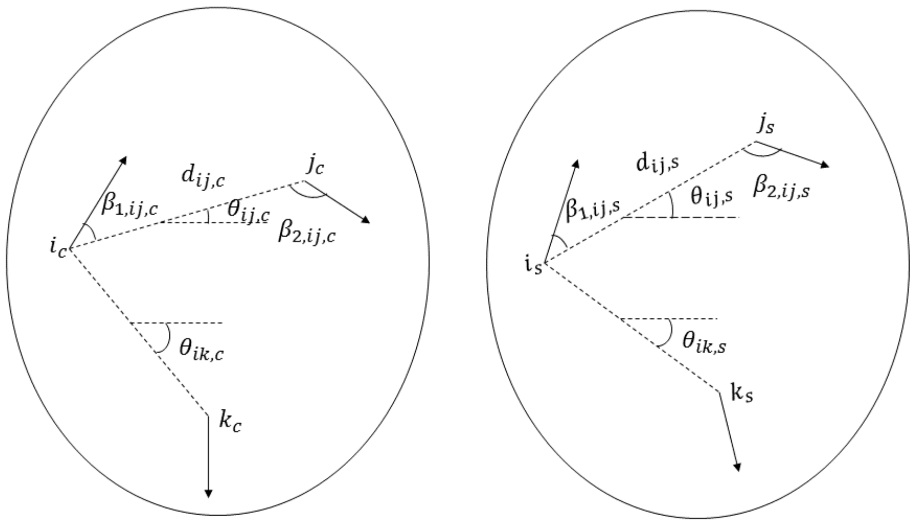
- Traverse the compatibility table:
  - Longest Path
- Problems:
  - NP hard → Garbling?

Our Adaptation

- New Objective:

  Longest path →

  # of compatible minutia-triplets



- Minutia-Triplet:
  - Compatibility Table: $\{\Delta(\theta_{ij,c},\theta_{ij,s}), i_c, j_c, i_s, j_s,\}$
  - A compatible minutia-triplet is determined by:
    - $i_c' = i_c''$ and $i_s' = i_s''$
    - $\Delta\left(\Delta(\theta_{ij,c},\theta_{ij,s})\right) < t$
  - Incomplete Compatibility Table: $\{\Delta(\theta_{ij,c},\theta_{ij,s}), i_c, i_s\}$

-124	3	12	10	5
-122	5	7	17	22
-132	5	8	17	25
71	6	9	22	17
-145	7	15	17	14
178	8	12	12	6
-155	8	15	17	10
-136	8	21	17	14

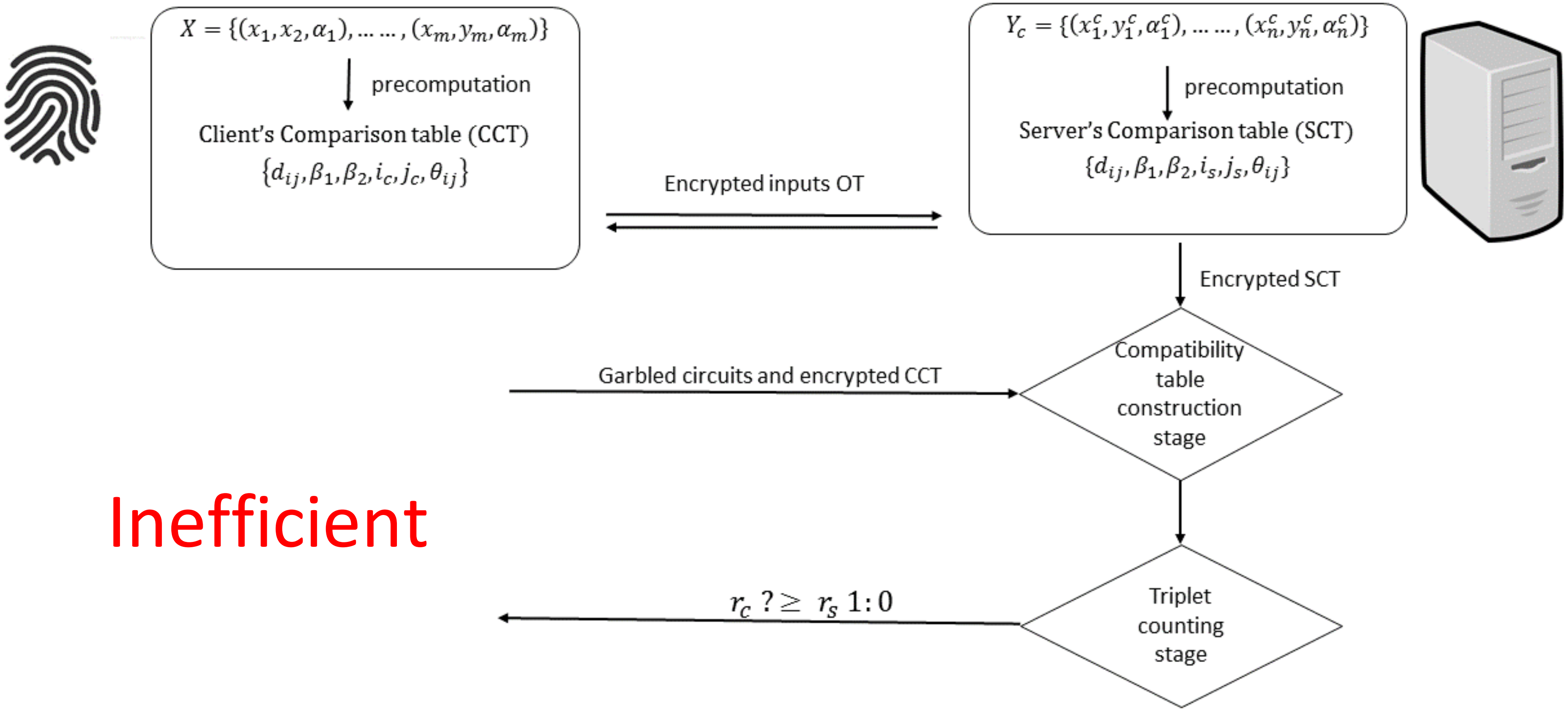
Our Adaptation

- Minutia-Triplet:
  - A Discriminative local structure

- Incomplete minutia-pair compatibility table
  - Saving Memory
  - Reducing Circuit Size

Secure Protocol Construction

- Intuition



Inefficient

Secure Protocol Construction

- Improved Protocol:
  - Release the compatible minutia-triplet counting phase
  - Privacy Concern – Incomplete Compatibility Table

    $\{\Delta(\theta_{ij,c}, \theta_{ij,s}), i_c, i_s\}$

    → Client's minutia-pair comparison table $\{d_{ij_c}, \beta_{1_c}, \beta_{2_c}, i_c, j_c, \theta_{ij_\downarrow c}\}$

  - Encrypted Incomplete Compatibility Table: $\{\Delta(\theta_{ij,c}, \theta_{ij,s}), Enc(i_c), i_s\}$

Implementation and Evaluation - Reliability

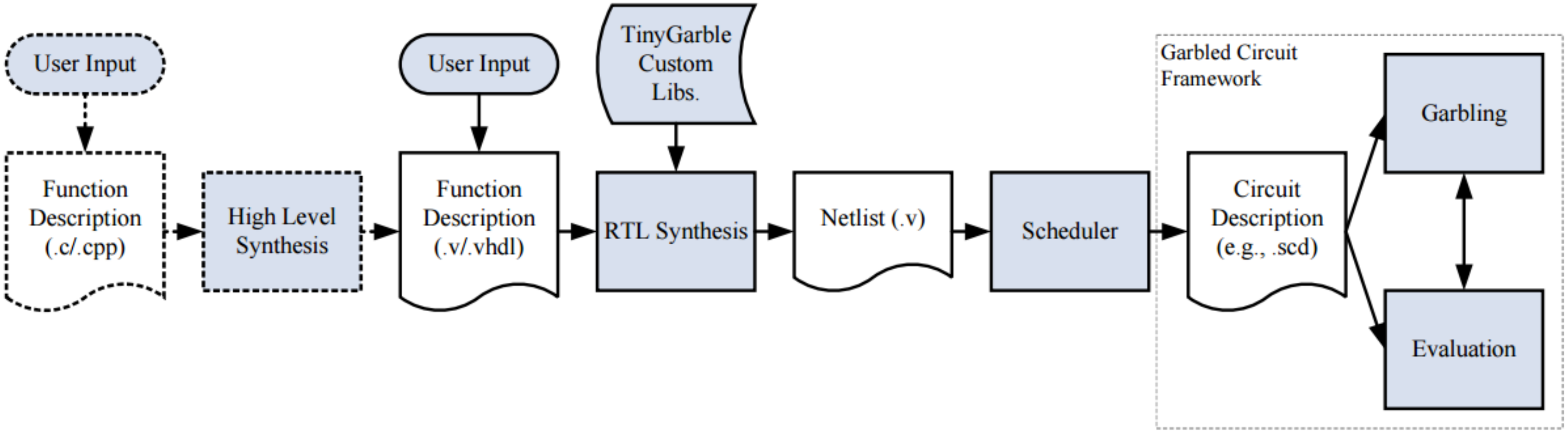
- Metrics :
  - Genuine Acceptance Rate(GAR)
  - False Acceptance Rate(FAR)

- Results:

FAR \ l	64	72	80	88	96	104	112	120	128
0%	74.2%	75.9%	81.8%	83.2%	84.7 %	87.3%	87.3%	87.5%	90.2%
0.1%	84.2%	85.5%	86.3 %	87.3%	88.8 %	90.4%	91.0%	91.6%	92.0%
1.0%	89.4%	89.8%	90.0%	91.9%	93.4 %	95.5 %	95.7%	96.1%	96.5%

TABLE I
GAR VS FAR FOR DIFFERENT NUMBER OF MINUTIA-PAIRS

Implementation and Evaluation – Efficiency and Scalability



Global Flow for TinyGarble

[2] Songhori et al., "TinyGarble: Highly Compressed and Scalable Sequential Garbled Circuits," IEEE S&P 2015

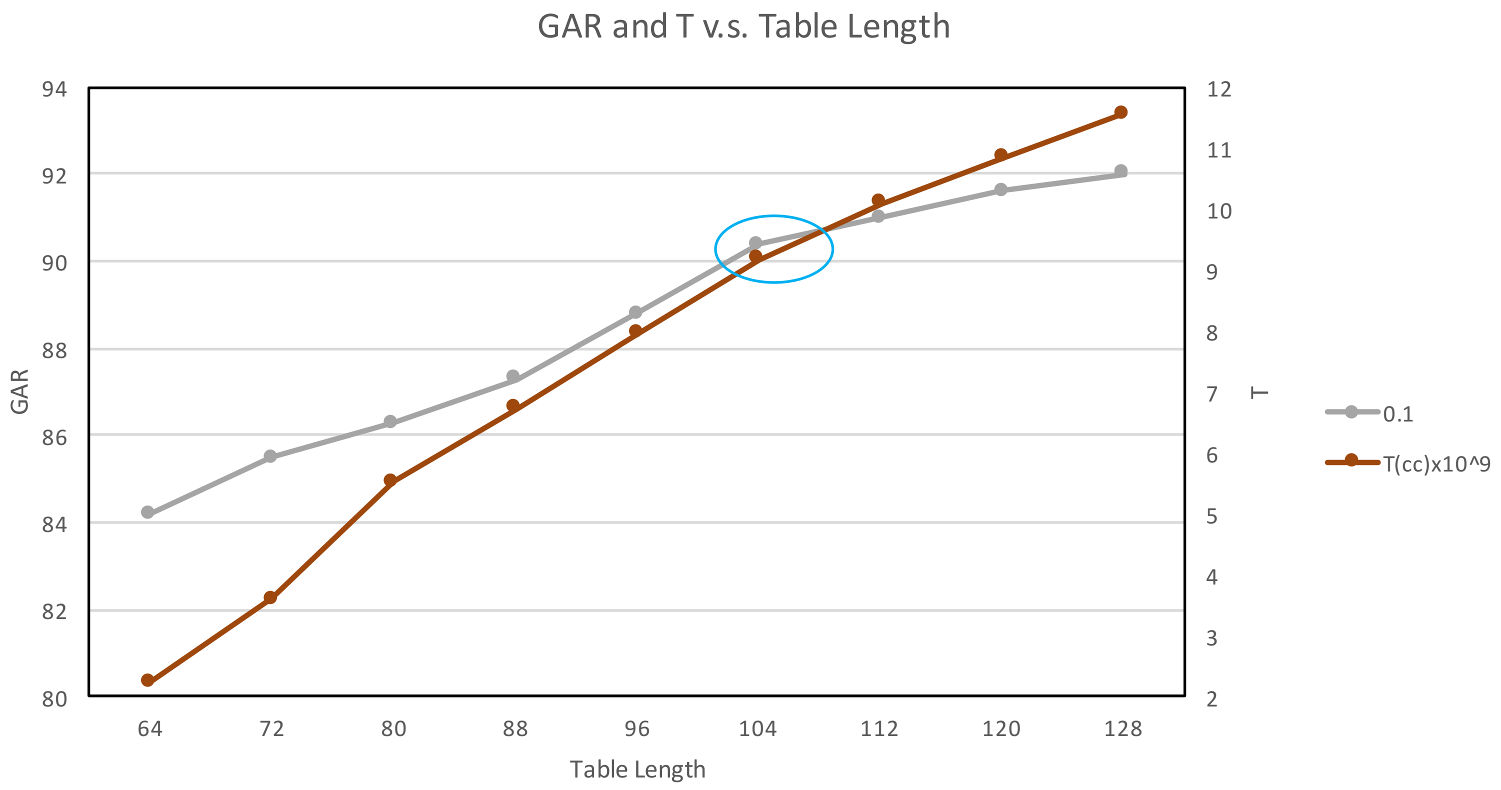
Evaluation – Timing and Circuit Size

- The largest CS we achieved is 255 KB($l = 128$)
- A highly compact and efficient design(0.67sec/match)

l	64	72	80	88	96	104	112	120	128
total gates	5175	6406	7041	7684	8320	8963	9607	10281	10886
non-XOR	2055	2319	2541	2767	2982	3190	3410	3678	3880
CS(KB)	134	150	165	180	195	210	225	241	255
$T(cc) \times 10^9$	2.24	3.61	5.53	6.73	7.95	9.18	10.09	10.85	11.57

TABLE II
CIRCUIT SIZE AND TIMING EVALUATION FOR CUSTOMIZED BOZORTH MATCHER

Evaluation – Best Point



Best Point: $l = 104$ | $T_{total} = 9.18 * 10^9 cc$ | CS = 210KB | GAR = 90.4%

Conclusion

- Introduce the first reliable, efficient and scalable methodology for privacy-preserving fingerprint authentication
- Develop an efficient and reliable fingerprint matching algorithm
- Construct a privacy-preserving protocol for performing our matching algorithm
- Implementation and evaluation

Acknowledgements

- Funding Agencies:
  - Office of Naval Research
  - National Science Foundation
  - U.S. Army Research Office

- Reviewers for HOST 2016

Thanks for Your Attention!